iMG/RG Gateway
Release 3-7-04
Software Reference Manual
Document Issue 1.4

i. Preface

I Introduction

I.I Purpose of this manual

The Allied Telesis Gateway product set delivers multiple IP-based broadband services to home over high speed, always-on broadband connection. This family of devices enables the delivery of voice, data, and video to customer premises, offering benefits both to service providers and to final users. Service providers can quickly deliver to their customers advanced services such as fast Internet, VoIP, and video on demand in a full scalable way that is remotely manageable. End users get the benefit of a unique device interconnecting all peripherals, computers, and telephones using a single uplink broadband connection.

This manual is the complete reference to the configuration, management, and operation of the AT-Gateway family of devices. It includes detailed descriptions of all management commands.

It is assumed that the reader is familiar with:

- The topology of the network in which the Intelligent Business Gateway is to be used.
- Basic principles of computer networking, protocols and routing, and interfaces.
- Administration and operation of a computer network.

II Intended audience

This manual is intended for the system administrator, network manager or communications technician who will configure and maintain AT-iMG600 devices, or who manages a network of AT-iMG600 Gateways.

It is assumed that the reader is familiar with:

- The topology of the network in which the intelligent Multiservice Gateway is to be used;
- Basic principles of computer networking, protocols and routing, and interfaces;
- Administration and operation of a computer network.

III How this Document is Organized

This preface provides an overview of the supported devices and the documentation sections that are relevant to these devices. Using this preface, the customer should be able to see where the device fits within the ATI iMG portfolio - and at a high level - how it is different from the other members of the family. This Preface has four main subsections:

1. A description of the different types of devices, grouped by Network Interface Technology (ADSL, Active Fiber, EPON, Modular).
2. A detailed list of the individual models supported - including the type of Network Interface, Number of Ethernet LAN interfaces and the number and type of Telephony ports.
3. A list of functional groupings of devices that describes the unique traits of this set of devices - exclusive of network interfaces.
4. A list of the different sections within the document and based on the above defined grouping - an indication of which sections apply.

The intent of the functional groupings is to allow the customers to use the appropriate group to determine which sections within the document apply to that set of devices, as well as identify what specific differences there may be between the different groupings when discussing a specific topic - such as File System structure or Switch functionality.

IV Allied Telesis Gateway Family Feature Summary

IV.I VLAN OPERATION

This family of devices supports IEEE 802.1Q tagged VLAN operation across its all switch ports. It therefore offers a powerful combination of wirespeed Layer 2 switching between VLANs as well as high performance Layer 3 routing between VLANs in one highly cost effective unit.

IV.II FIREWALL

This family of devices integrates a Stateful Inspection Firewall with Network Address Translation (NAT) and Denial of Service intrusion detection and blocking for protecting customer networks. Each VLAN can be configured to be external, internal, or DMZ. With the Virtual Server features, a web or e-mail server can sit beyond the NAT and appear like being on the public interface. The NAT implementation supports the most popular protocols and applications including NetMeeting (H.323 and SIP), IPSec and PPPtp.

IV.III PORT RATE LIMITING

This family of devices offers the possibility to limit the egress and ingress bandwidth on each port. This feature allows the Service Operator to offer differentiated services to each customer and protect its network from malicious packet flooding.

IV.IV VOICE OVER IP (VOIP)

This family of devices offer a choice of Voice over IP signaling methods, namely SIP and MGCP including NCS 1.0 profile. SIP and MGCP are optimized for operation over IP networks. This multiple protocol support provides maximum flexibility for service providers, allowing them to provide an IP telephony service based on cost and feature set, rather than being limited by the protocol used.

Similarly, a choice of different voice and data encoding algorithms is also available comprising G.711 A-law, µ-law (64kbps), G.729 (8kbps,) and T.38, so that maximum VoIP interworking is assured with carrier class IP Gateways and network switches. Quality of Service is provided through mechanisms such as the Type of Service (ToS) field in the IP packet, priority tagging of voice traffic using IEEE 802.1p, as well as silence suppression and local generation of comfort noise – the result is excellent voice quality.

Class 5 services are supported and the VoIP inter-operability has been certified versus major soft-switch vendors.

IV.V VIDEO STREAMING

Video Streaming offers unique features to optimize the delivery of Video contents to customers, namely VLAN, IGMP snooping, and proxying. This family of devices supports full IGMP snooping capability (v1/v2), and individual LAN ports can receive different multicast transmissions e.g. different movies or TV channels. The gateway 'snoops' IGMP packets in-transit, so it knows which port to forward the particular multicast data to.

This results in high-quality, high-bandwidth video streaming without affecting Internet surfing or IP telephony on adjacent ports. The gateway also supports IGMP proxying to allow forwarding of multicast packets at Layer 3 with or without NAT.

IV.VI MANAGEMENT & CONFIGURATION

This family of devices is designed for high volume deployment, this is reflected in the Zero Touch Configuration model, whereby no user intervention is required when installing a unit. ZTC provides intelligent and automatic configuration of remote RG units. It analyses incoming status information from each RG unit and dynamically creates the appropriate configuration file or operating system download as required, it then selects the appropriate download mechanism (e.g. TFTP,HTTP, HTTPS etc.) to complete the process. The ZTC client in the RG initiates the download process on power up, or on expiry of its DHCP lease timer. ZTC provides secure authentication of client devices, resilience through distributed server operation and in-built scalability for very large networks.

V Gateway Types

V.I ADSL Gateways

Asymmetric Digital Subscriber Line (ADSL) is used to provide cost-effective, high speed local loop access for Internet and other applications where data flows downstream to end users faster that it does upstream from end users. ADSL provides asymmetric transmission over one pair of copper telephone wires with downstream data transmission rates ranging from 32 Kbps to 26 Mbps with ADSL2+. One single telephone line can be used simultaneously for voice and data transmission.

The ADSL interface is designed to meet the following standards:

- ANSI T1.413 (8 Mbps)
- ITU G.992.1Annex A also known as G.dmt (10 Mbps)
- ITU G.992.2 also known as G.lite (4Mbps)
- ITU G.992.3/4 also known as ADSL2 or G.dmt.bis (12Mbps)
- ITU G.992.5 also known as ADSL2+ (24 Mbps).

These gateways typically support 4 Ethernet 10/100TX ports plus 2 Voice ports.:

V.II Active Fiber Gateways

Allied Telesis Active Fiber Gateways offer a full range of optical interfaces to fit the requirements of FTTx applications. In full compliance with the optical performance requirements of 100 Base-FX version of IEEE 802.3u, both multi-mode and single-mode fibers are available. In addition, the bi-directional optical interface over a single fiber, allows the best exploitation of the cabling infrastructure.

TABLE i-1 Active Fiber Gateways

OPTICAL PARAMETER	SH	LH	BD
Fiber type	Multi-mode	Single-mode	Single-mode
Operating wavelength	1300 nm	1300 nm	TX 1310 nm RX 1550 nm

These gateways support from 3 to 6 Ethernet 10/100TX ports plus 2 to 4 voice ports and are available in both indoor and outdoor versions.

There is also a subset of this family of devices that support RF Overlay. These are derivations of base models - with an "RF" suffix in the model name. This is supported by the addition of a second fiber and an optical module that supports Analog Fiber to RF Conversion. The devices are connected to the WAN via a dual single-mode fibre optical interface: one fibre delivers triple-play services similarly to the iMG613BD, the second fibre receives the video broadcast channels.

TABLE i-2 Active Fiber Gateways with RF Overlay

OPTICAL PARAMETER	Fiber to Eth/VoIP	Fiber-to-RF
Fiber type	Single-mode	Single-mode
Operating wavelength	TX 1310 nm RX 1550 nm	RX 1550 nm

The separated passive unit named RG001 where the optical cable is terminated, allows easy installation, maintenance and replacement thanks to a plug-and-play optical connection.

V.III Passive Optical Network Fiber Gateways

Allied Telesyn has expanded the portfolio to include an EPON Active Fiber Outdoor Gateway. This device is an evolution of the Active Fiber Outdoor Gateway - supporting 6 Ethernet 10/100TX ports and 4 voice ports.

A passive optical network (PON) is a point-to-multipoint, fiber to the premises network architecture in which unpowered optical splitters are used to enable a single optical fiber to serve multiple premises, typically 32-128. A PON consists of an Optical Line Terminal (OLT) at the service provider's central office and a number of Optical Network Units (ONUs) near end users. A PON configuration reduces the amount of fiber and central office equipment required compared with point to point architectures.

Downstream signals are broadcast to each premises sharing a fiber. Encryption is used to prevent eavesdropping.

Upstream signals are combined using a multiple access protocol, invariably time division multiple access (TDMA). The OLTs "range" the ONUs in order to provide time slot assignments for upstream communication.

V.IV Active Fiber Business Gateways

Allied Telesyn Active Fiber Business Gateways offer a full range of optical interfaces via an SFP or 100M TX interface to fit the requirements of FTTx or MDU applications. This family boasts higher performance and a larger number of Voip interfaces. Being AC Powered - it is perfectly adapted for installation in business or MDU applications:

V.V Modular Gateways

Allied Telesyn Modular Outdoor Gateways offer a full suite of choices to the customer - for both WAN interfaces and for LAN interfaces. This hardened device is designed for ease of installation - and long lasting robust service. It allows the customer to select a Base platform for deployment and management - that can be enhanced as needs evolve. This base platform supports 2 or 4 Voice ports and 6 10/100M TX Ports.

The following Modular WAN interfaces are supported:

- 100M Active Fiber
- 1000M Active Fiber
- EPON Fiber

The following Modular LAN interfaces are Supported in addition.

- 1000M Copper Ethernet
- T1/E1 Circuit Emulation
- HPNA V3.1

VI Supported Products

The following table lists all the Gateway Series devices supported by this software release along with information indication the types of interfaces available.

TABLE i-3 RG/iMG Models

Type	iMG/iBG Model[a]	Customer[b]	Network[c]	2-5	3-5	3-6	3-7
Fiber	RG613TX BD/LH/SH	FXS=2, LAN=3	SM, SF	RG600	-	-	RG600E
	RG656BD	FXS=3, LAN=6	SM, SF	RG600	-	-	RG6x6E
	iMG606BD LH/SH	LAN=6	SM, SF	RG600	-	-	RG6x6E
	iMG616BD LH/SH	FXS=2, LAN=6	SM, SF	-	iMG616E	-	iMG616E
	iMG616RF, RF+, iMG616SRF, SRF+	FXS=2, LAN=6, RF O'lay	SM, SF	-	iMG616E	-	iMG616E
	iMG616W	FXS=2, LAN=6, RF O'lay, 802.11b/g	SM, SF	-	-	-	iMG616W
	iMG646BD LH/SH	FXS=4, LAN=6	SM, SF	RG600	-	-	RG6x6E
	iMG646BD-ON	FXS=4, LAN=6	SM, SF	RG600	-	-	RG6x6E
	iMG646PX-ON	FXS=4, LAN=6	EPON[d]	RG600	-	-	RG6x6E
	iBG915-FX	FXS=8, LAN=5	SFP/TX	-	-	-	iBG915FX
ADSL	iMG624A iMG624B	LAN=4	ADSL2+ (A/B)	-	iMG624A iMG624B	-	iMG624A iMG624B
	iMG634A iMG634B	FXS=2, LAN=4	ADSL2+ (A/B)	-	iMG634A iMG634B	-	iMG634A iMG634B
	iMG624A-R2	LAN=4	ADSL2+(A)	-	-	-	iMG624A-R2
	iMG634A-R2 iMG634B-R2	FXS=2, LAN=4	ADSL2+ (A/B)	-	-	-	iMG634A-R2 iMG634B-R2
	iMG634WA iMG634WB	FXS=2, LAN=4, 802.11b/g	ADSL2+ (A/B)	-	iMG634WA iMG634WB	-	iMG634WA iMG634WB

TABLE i-3 RG/iMG Models

Type	iMG/iBG Model[a]	Customer[b]	Network[c]	2-5	3-5	3-6	3-7
	iMG634WA-R2 iMG634WB-R2	FXS=2, LAN=4 802.11b/g	ADSL2+ (A/B)	-	-	-	iMG634WA-R2 iMG634WB-R2
	iBG910A	FXS=4, ISDN=2, LAN=8	ADSL2+(A)	-	-	iBG910A	iBG910A
Mod-ular	iMG646MOD iMG626MOD	FXS=4 or 2, LAN=6, HPNA/T1.	BD, PON	-	-	iMG626 iMG646	iMG626 iMG646
	iMG746MOD iMG726MOD	FXS=4 or 2, LAN=6, Gig Lan=1, HPNA/T1.	100M-BD, 1000M-BD PON	-	-	-	iMG726 iMG746

d. Refer to the iMAP User Guide for configuring the EPON2 card and Optical Network Unit (ONU).

VII Functional Groupings

Below is a table that lists all the iMG models that are supported in 3-7. They are grouped by distinguishing characteristics - such as hardware resources available on the device. There is also a column which identifies what is unique regarding this grouping.

TABLE i-4 iMG Models Supported in 3-7

Group	Model	Load Name	Characteristics	Uniqueness
Fiber A	rg613TX, BD, LH, SH	rg600E	4/16 Meg Flash/Ram	Initial product offering
			Kendin Switch	
			Ni-210 Processor	
Fiber B	rg656BD, LH, SH	RG6x6E	4/16 Meg Flash/Ram	More efficient routing when VLANs configured.Similar service offering to Modular Devices
	iMG606BD, LH, SH		Broadcom Switch	
	iMG646BD, LH, SH		Ni-210 Processor	
	iMG646BD-ON/PX-ON			
Fiber C	iMG616BD, LH, SH	iMG616E	4/16 Meg Flash/Ram	Base Platform that provides capability for RF overlay.
	iMG616RF, RF+,		Broadcom Switch	
	iMG616SRF, SRF+		Ni-210 Processor	
Fiber D	iMG616W	iMG616W	8/32 Meg Flash/RAM	New indoor wireless product - greater processing capacity - plus wireless support
			Broadcom Switch	
			Solos Processor	
Fiber E	iBG915FX	iBG915	8/32 Meg Flash/RAM	New Multi port Tel port offering. SFP provides for WAN flexibility.
			Marvell Switch	
			He-520 Processor	
Modular	iMG626MOD	iMG626	8/32 Meg Flash/RAM	Modular outdoor devices - provide support for different WAN services - and additional LAN interfaces.
	iMG646MOD	iMG646	Marvell Switch	
	iMG726MOD	iMG726	He-520 Processor	
	iMG746MOD	iMG746		
ADSL A	iMG624A/B	iMG624A/B	8/32 Meg Flash/RAM	Second Generation ADSL CPE.
	iMG634A/B	iMG634A/B	Kendin Switch	
	iMG634WA/B	iMG634WA/B	Argon Processor	
ADSL B	iMG624A-R2	iMG624A-R2	8/32 Meg Flash/RAM	Third Generation ADSL CPE - Greater performance - able to support 2 INP.
	iMG634A/B-R2	iMG634A/B-R2	Marvell Switch	
			Solos Processor	
ADSL C	iBG910A/B	iBG910A/B	8/32 Meg Flash/RAM	Multi-line ADSL Gateway supporting both ISDN and POTS.
			Marvell Switch	
			Argon Processor	

VIII Documentation Structure

In the table below is a high level index of the remainder of the document - along with columns for each of the groupings defined above. Where a section applies to that group of devices, an X is placed in the cell. If it is left blank, then that section does not apply. Minor differences are managed via note sections within the different sections.

TABLE i-5 Main Features and where they apply to Product Type

		Fiber					Modular	ADSL		
Chapter	Section	A	B	C	D	E		A	B	C
1 "System Configuration"	" System Management" page 1	x	x	x	x	x	x	x	x	
	" Webserver" page 36	x	x	x	x	x	x	x	x	x
	" Emergency" page 47	x	x	x						
	" Software update" page 54	x	x	x	x	x	x	x	x	x
	" ZTC" page 74	x	x	x	x	x	x	x	x	x
	" SNMP" page 84	x	x	x	x	x	x	x	x	x
2 "Switching"	" Switching" page 1	x	x	x	x	x	x	x	x	x
	" BRIDGE" page 37	x	x	x	x	x	x	x	x	x
	" VLAN" page 84	x	x	x	x	x	x	x	x	x
3 "IGMP"	" IGMP snooping" page 1	x	x	x	x	x	x	x	x	x
4 "IPNetwork Functions"	" IP" page 1	x	x	x	x	x	x	x	x	x
	" Security" page 57	x	x	x	x	x	x	x	x	x
	" Firewall" page 105	x	x	x	x	x	x	x	x	x
	" Network address translation - NAT" page 134	x	x	x	x	x	x	x	x	x
5 "System Administration"	" Dynamic Host Configuration Protocol" page 1	x	x	x	x	x	x	x	x	x
	" Domain name system - DNS" page 83	x	x	x	x	x	x	x	x	x
	" SNTP" page 93	x	x	x	x	x	x	x	x	x
6 "Voice Service"	" VoIP MGCP" page 1	x	x	x	x	x	x	x	x	x
	" VoIP SIP" page 16	x	x	x	x	x	x	x	x	x
	" VoIP phone ports" page 59	x	x	x	x	x	x	x	x	x
	" Common VoIP attributes: QoS, Media and DTMF-Relay" page 120	x	x	x	x	x	x	x	x	x
7 "Quality of Service"	" QOS" page 1 - Includes Classifier, Meter, and Scheduler for Ingress									
	" Classifying packets" page 3	x	x	x	x	x	x	x	x	x
	" Meter" page 5	x	x	x	x	x	x	x	x	x
	" Scheduler" page 9							x	x	x
	" L2Filter" page 60		x		x	x	x	x	x	x
8 "ADSL Port"	" ADSL System description" page 2							x	x	x
	" Port a1" page 5							x	x	x
	" Bridge" page 36							x	x	x
	" Transports" page 49							x	x	x
	" Ethernet" page 58							x	x	x
	" PPPoE" page 62									
	" PPPoA" page 114							x	x	x
	" RFC1483" page 151							x	x	x
9 "Wireless"	" Wireless Interface" page 1				x			x	x	

TABLE i-5 Main Features and where they apply to Product Type

		Fiber					Modular	ADSL		
Chapter	Section	A	B	C	D	E		A	B	C
10 "LAN Module Management"	" HPNA LAN Module" page 2						x			
	" HPNA Command Reference" page 3						x			
	" CES LAN Module" page 8						x			
	" Circuit Emulation Command Reference" page 9						x			

IX Reason for Update

The following table lists the updates that have occurred for this release, due to hardware, software, and document changes.

Note: Document errors have also been corrected where necessary.

TABLE i-6

Feature	3-7-03 and Before	3-7-04	Notes
QoS functions for iMG devices	Present on Ethernet-based devices	Includes the: iMG634-A/B iMG634-WA/WB iMG624-A/B iMG624-A R2 iMG634-A/B R2	Refer to TABLE i-5
Split Management	Not available	Provides	Refer to 1.1.2.3
AT-616W	Not available, but documented	Available	Refer to TABLE i-4
Fast UDP Support	Supported in 3-5	Removed	Removed from document
Time Zone	Supported	EDT is no longer displayed and cannot be set. Time that is set depends on time zone, date, and daylight savings time setting	
Customer Products and Wireless Features			Refer to the Release Notes for any compatibility issues. Features are listed in 9.1.1.
Configuring EPS			Note added on using SECURITY ADD ALG. Refer to 6.2.3.

TABLE i-6

PPPoE and TCP MSS value S			On the iMG or the PPPoE concentrator/RA should be configured to clamp the maximum TCP MSS value. Refer to 8.7.2.5
SIP EPS Configuration			Note that each EPS allows a maximum of three calls per line. The number of SIP users and media port limit is clarified. Refer to 6.2.3
IGMP			Included is a description of the new IGMP functionality (including also extended IGMP messages flow charts) plus the description of the old IGMP functionality. Changes to default values are included Refer to 3.1.

Table of Contents

i Preface - *i-1*

1 System Configuration - *1-1*

1.1 System Management - **1-1**

1.1.1 System Configuration - 1-1

1.1.1.1 Access to the Gateway - 1-1

1.1.1.2 Default Factory Configuration - 1-1

1.1.1.3 Minimal Configuration - 1-2

1.1.2 Command Line Interface and Console - 1-3

1.1.2.1 Access permissions to CLI - 1-3

1.1.2.2 Access permissions to WEB interface - 1-4

1.1.2.3 Split management - 1-5

1.1.3 File system - 1-5

1.1.3.1 Gateway with 4Mbytes of FLASH - 1-6

1.1.3.2 Gateway with 8MBytes of FLASH with and without EEPROM - - - - - - - - - - 1-7

1.1.3.3 Boot partition - 1-8

1.1.3.4 Recovery partition - 1-8

1.1.3.5 Main partition - 1-9

1.1.3.6 Configuration partitions - 1-9

1.1.4 Configuration Management - 1-9

1.1.4.1 Configuration File Saving and Backup Process- 1-10

1.1.5 System command reference - 1-12

1.1.5.1 System CLI commands- 1-12

1.2 Webserver - **1-36**

1.2.1 Introduction- 1-36

1.2.2 Web pages- 1-36

1.2.2.1 Home page - 1-36

1.2.2.2 Configuration page - 1-37

1.2.2.3 Security page - 1-37

1.2.2.4 Services page - 1-37

1.2.2.5 Admin page - 1-37

1.2.3 Webserver command reference - 1-38

1.2.3.1 Webserver CLI commands - 1-38

1.3 Emergency - **1-47**

1.3.1 Introduction- 1-47

1.3.2 Emergency configuration ---- 1-47
1.3.3 Save and activate emergency configuration. ---- 1-48
1.3.4 -Emergency command reference ---- 1-49
1.3.4.1 Emergency CLI commands ---- 1-49

1.4 Software update ---- 1-54
1.4.1 Windows™ Loader ---- 1-57
1.4.2 Upgrade via Web Interface ---- 1-58
1.4.3 SwUpdate module ---- 1-60
1.4.3.1 Start Time scheduling ---- 1-63
1.4.3.2 Retry Period scheduling ---- 1-64
1.4.3.3 Stop Time scheduling ---- 1-64
1.4.3.4 Manually enabling SwUpdate ---- 1-66
1.4.3.5 Plug-and-play ---- 1-66
1.4.3.6 Server access ---- 1-67
1.4.4 SwUpdate command reference ---- 1-68
1.4.4.1 SwUpdate commands ---- 1-68

1.5 ZTC ---- 1-74
1.5.1 Functional blocks ---- 1-75
1.5.1.1 ZTC network architecture ---- 1-75
1.5.2 ZTC Client ---- 1-76
1.5.2.1 Storing unit configuration ---- 1-77
1.5.2.2 Pull-at-startup ---- 1-77
1.5.2.3 Scheduled-pull ---- 1-78
1.5.3 ZTC command reference ---- 1-81
1.5.3.1 ZTC Client commands ---- 1-81

1.6 SNMP ---- 1-84
1.6.1 SNMP configuration within the SNMPv3 administration framework ---- 1-86
1.6.1.1 Security ---- 1-86
1.6.1.2 Mechanisms used by SNMPv3 security ---- 1-86
1.6.1.3 Local configuration datastore ---- 1-88
1.6.1.4 Configuration file format ---- 1-88
1.6.1.5 Configuration for all SNMPv3 entities ---- 1-88
1.6.2 Additional configuration for SNMPv3 agent entities ---- 1-92
1.6.2.1 Configuring view-based access control ---- 1-92
1.6.2.2 Defining families of view subtrees ---- 1-92
1.6.2.3 Defining groups and access rights ---- 1-94
1.6.2.4 Assigning principals to groups ---- 1-95
1.6.3 Configuring notifications ---- 1-96
1.6.3.1 Defining notifications ---- 1-96
1.6.3.2 Defining target addresses ---- 1-97
1.6.3.3 Defining target parameters ---- 1-98

1.6.4 Configuring notification filters - - - 1-99
1.6.4.1 Creating a notification filter - - - 1-99
1.6.4.2 Associating a filter with a notification parameter - - - 1-101
1.6.5 Configuring source address checking - - - 1-101
1.6.5.1 Matching exactly one source address - - - 1-103
1.6.5.2 Matching any source address - - - 1-103
1.6.5.3 Matching a source address in a subnet - - - 1-104
1.6.6 Examples - - - 1-105
1.6.6.1 noAuthNoPriv SNMPv3 users - - - 1-105
1.6.7 authNoPriv SNMPv3 users - - - 1-106
1.6.8 Additional configuration for SNMPv3 agent entities - - - 1-107
1.6.8.1 Configuring context names - - - 1-107
1.6.9 Additional configuration for SNMPv1 and SNMPv2 agent entities - - - 1-108
1.6.9.1 Configuring communities - - - 1-108
1.6.9.2 Examples - - - 1-109
1.6.10 MIB - - - 1-110
1.6.10.1 Standard (public) MIB - - - 1-110
1.6.10.2 Standard traps - - - 1-114
1.6.10.3 Enterprise (private) MIB - - - 1-115

2 Switching - - - 2-1

2.1 Overview - - - 2-1
2.1.1 Layer 2 Switching in the Network - - - 2-1
2.1.2 Documentation Structure - - - 2-1

2.2 Switching - - - 2-1
2.2.1 Overview - - - 2-1
2.2.2 Layer 2 switch functional description - - - 2-2
2.2.2.1 Port Management - - - 2-2
2.2.2.2 Ingress Filtering - - - 2-2
2.2.2.3 Address management - - - 2-3
2.2.2.4 Rate limiting support - - - 2-3
2.2.2.5 Loop Detection - - - 2-3
2.2.2.6 Layer 3 Routing Rate Limiting - - - 2-4
2.2.2.7 Quality of Service Classification - - - 2-4
2.2.2.8 Power Conservation Mode - - - 2-6
2.2.2.9 Port Diagnostics - - - 2-7
2.2.3 Functional Differences for Switching in Product Categories - - - 2-7
2.2.4 Switch command reference - - - 2-9
2.2.4.1 Switch CLI commands - - - 2-9

2.3 BRIDGE - - - 2-37
2.3.1 Overview - - - 2-37

2.3.2 Bridge Functional Description - - - 2-37
2.3.2.1 Source MAC based forwarding - - - 2-37
2.3.2.2 Destination MAC based forwarding - - - 2-37
2.3.2.3 Port based forwarding - - - 2-38
2.3.2.4 Traffic Prioritization - - - 2-38
2.3.2.5 Multicast Traffic - - - 2-39
2.3.2.6 Learning - - - 2-39
2.3.3 Functional Differences in Product Categories - - - 2-40
2.3.4 Bridge command reference - - - 2-40
2.3.4.1 Bridge commands - - - 2-41

2.4 VLAN - - - 2-84
2.4.1 Overview - - - 2-84
2.4.1.1 VLAN tagging - - - 2-85
2.4.2 VLAN Functional Description - - - 2-88
2.4.2.1 VLAN support on Ethernet interfaces - - - 2-88
2.4.2.2 VLAN support on ADSL interface - - - 2-89
2.4.2.3 VLAN versus IP interface - - - 2-90
2.4.2.4 VLAN Translations - - - 2-91
2.4.3 Functional Differences in Product Categories - - - 2-92
2.4.4 VLAN command reference - - - 2-93
2.4.4.1 VLAN CLI commands - - - 2-93

3 IGMP - - - 3-1

3.1 IGMP snooping - - - 3-1
3.1.1 Multicasting overview - - - 3-1
3.1.1.1 Multicast Group addresses - - - 3-1
3.1.1.2 IGMP protocol - - - 3-2
3.1.1.3 Multicast MAC addresses - - - 3-2
3.1.2 IGMP snooping Functional Overview (Includes New Functionality) - - - 3-3
3.1.2.1 Multicast router port discovery - - - 3-4
3.1.2.2 Snoop-Only Operation Mode - - - 3-4
3.1.2.3 Proxy Operational Mode - - - 3-6
3.1.3 Old IGMP Snooping Functionality - - - 3-13
3.1.3.1 Multicast router port discovery - - - 3-13
3.1.3.2 Snoop-Only Operation Mode - - - 3-13
3.1.3.3 Proxy Operation Mode - - - 3-14
3.1.3.4 IP source address masking – Secondary IP Interface - - - 3-15
3.1.3.5 IGMP snooping security - - - 3-15
3.1.3.6 Routed IGMP proxy - - - 3-15
3.1.4 Functional Differences in Product Categories - - - 3-16
3.1.5 IGMP Snooping command reference - - - 3-16
3.1.5.1 IGMP snooping CLI commands - - - 3-17

4 IPNetwork Functions -4-1

4.1 IP - 4-1
4.1.1 Overview - 4-1
4.1.2 IP Interfaces - 4-1
4.1.3 IP support on AT-iMG Models - 4-2
4.1.3.1 Adding and attaching IP interfaces - 4-2
4.1.3.2 IP stack and incoming packets - 4-3
4.1.3.3 Locally received packets - 4-3
4.1.3.4 Forwarding packets - 4-3
4.1.4 Unconfigured interfaces - 4-4
4.1.5 Unnumbered interfaces - 4-4
4.1.5.1 Unconfigured interfaces vs unnumbered interfaces - - - - - - - - - - - - - - - - - - 4-4
4.1.5.2 Configuring unnumbered interfaces - 4-5
4.1.5.3 Creating a route - 4-5
4.1.6 Virtual interfaces - 4-6
4.1.6.1 Configuring virtual interfaces - 4-6
4.1.6.2 Similarities between virtual interfaces and real interfaces - - - - - - - - - - - - - - - 4-7
4.1.6.3 Differences between virtual interfaces and real interfaces - - - - - - - - - - - - - - - 4-7
4.1.7 Secondary IP addresses - 4-7
4.1.7.1 Configuring secondary IP addresses - 4-8
4.1.7.2 Functionality of secondary IP addresses - 4-8
4.1.8 TCP/IP command reference - 4-8
4.1.8.1 IP Tracing commands - 4-8
4.1.8.2 IP CLI commands - 4-9

4.2 Security - 4-57
4.2.1 Overview - 4-57
4.2.2 Security support on AT-iMG Models - 4-58
4.2.3 Security interfaces - 4-58
4.2.3.1 Security Triggers - Dynamic Port Opening - 4-60
4.2.4 Intrusion Detection Settings - 4-62
4.2.4.1 Port Scan Attacks - 4-63
4.2.4.2 How Port Scanning works - Configuring Port Scanning - - - - - - - - - - - - - - - 4-64
4.2.4.3 Denial of Service (DoS) Attacks - 4-64
4.2.4.4 IDS Trojan Database - 4-67
4.2.5 Management stations - Remote Management - 4-67
4.2.6 Security logging - 4-68
4.2.7 Security command reference - 4-68
4.2.7.1 Command Set - 4-68

4.3 Firewall - 4-105
4.3.1 Overview - 4-105
4.3.1.1 Policy - 4-106
4.3.1.2 Portfilter - 4-106

4.3.2 Firewall command reference - - - - 4-106

4.4 Network address translation - NAT- - - - 4-134
4.4.1 Overview - - - - 4-134
4.4.2 NAT support on AT-iMG Models - - - - 4-135
4.4.2.1 Reserved mappings - - - - 4-136
4.4.2.2 Application level gateways (ALGs) - - - - 4-136
4.4.3 Interactions of NAT and other security features - - - - 4-136
4.4.3.1 Firewall filters and reserved mappings. - - - - 4-136
4.4.3.2 NAT and dynamic port opening - - - - 4-137
4.4.4 NAT and secondary IP addresses - - - - 4-137
4.4.5 NAT command reference - - - - 4-137
4.4.5.1 NAT CLI commands - - - - 4-137

5 System Administration - - - - 5-1

5.1 Dynamic Host Configuration Protocol - - - - 5-1
5.1.1 DHCP support - - - - 5-1
5.1.2 DHCP server - - - - 5-2
5.1.2.1 Example - - - - 5-2
5.1.3 DHCP client - - - - 5-4
5.1.3.1 Lease requirements and requests - - - - 5-5
5.1.3.2 Support for AutoIP - - - - 5-6
5.1.3.3 Additional DHCP client modes - - - - 5-6
5.1.3.4 Propagating DNS server information - - - - 5-6
5.1.3.5 Automatically setting up a DHCP server- - - - 5-6
5.1.3.6 Example - - - - 5-7
5.1.4 DHCP Relay- - - - 5-8
5.1.5 DHCP Server command reference - - - - 5-8
5.1.5.1 DHCP server CLI commands - - - - 5-8
5.1.6 DHCP Client command reference - - - - 5-55
5.1.6.1 DHCP client CLI commands - - - - 5-55
5.1.7 DHCP Relay Command Reference- - - - 5-79
5.1.7.1 DHCP relay CLI commands - - - - 5-80

5.2 Domain name system - DNS - - - - 5-83
5.2.1 DNS Relay - - - - 5-84
5.2.2 DNS Client- - - - 5-84
5.2.3 DNS Relay command reference - - - - 5-84
5.2.3.1 DNS Relay CLI commands - - - - 5-84
5.2.4 DNS Client command reference- - - - 5-89
5.2.4.1 DNS Client CLI commands - - - - 5-89

5.3 SNTP - - - - 5-93

5.3.1 SNTP features - - - - - - - 5-93
5.3.2 Time zones and daylight savings (summer time) conversion - - - - - - - 5-94
5.3.3 SNTP command reference - - - - - - - 5-94
5.3.3.1 SNTP CLI commands - - - - - - - 5-94

6 Voice Service - - - - - - - 6-1

6.1 VoIP MGCP - - - - - - - 6-1
6.1.1 MGCP Functional Description - - - - - - - 6-1
6.1.1.1 Endpoints - - - - - - - 6-1
6.1.1.2 Custom endpoints syntax - - - - - - - 6-2
6.1.2 Piggyback - - - - - - - 6-2
6.1.3 Wildcard - - - - - - - 6-3
6.1.4 Heartbeat - - - - - - - 6-3
6.1.5 Call Agent Failover - - - - - - - 6-4
6.1.6 Functional Differences for VoIP MGCP in Product Categories - - - - - - - 6-4
6.1.7 VOIP MGCP command reference - - - - - - - 6-5
6.1.7.1 VoIP MGCP CLI commands - - - - - - - 6-5
6.1.7.2 VOIP MGCP PROTOCOL SET ENDPOINT-SYNTAX - - - - - - - 6-8

6.2 VoIP SIP - - - - - - - 6-16
6.2.1 iMG SIP Overview - - - - - - - 6-16
6.2.1.1 iMG call processes - - - - - - - 6-16
6.2.1.2 Calls involving another terminal - - - - - - - 6-16
6.2.1.3 Calls Involving a Terminal and a SIP Endpoint - - - - - - - 6-17
6.2.2 VoIP SIP Servers, Users & the Forwarding Database - - - - - - - 6-18
6.2.2.1 SIP servers - - - - - - - 6-19
6.2.2.2 Users - - - - - - - 6-20
6.2.2.3 Forwarding database (FDB) - - - - - - - 6-22
6.2.3 VoIP SIP Embedded Proxy Server - - - - - - - 6-24
6.2.4 VoIP SIP command reference - - - - - - - 6-24
6.2.4.1 VoIP SIP protocol CLI commands - - - - - - - 6-24
6.2.5 VoIP SIP Locationserver command reference - - - - - - - 6-37
6.2.5.1 VoIP SIP Locationserver CLI commands - - - - - - - 6-37
6.2.6 VoIP SIP Proxyserver command reference - - - - - - - 6-41
6.2.6.1 VoIP SIP Proxyserver CLI commands - - - - - - - 6-41
6.2.7 VoIP SIP Embeddedserver command reference - - - - - - - 6-44
6.2.7.1 VoIP SIP Embeddedserver CLI commands - - - - - - - 6-44
6.2.8 VoIP SIP User command reference - - - - - - - 6-48
6.2.8.1 VoIP SIP User CLI commands - - - - - - - 6-48
6.2.9 VoIP SIP FDB command reference - - - - - - - 6-54
6.2.9.1 VoIP SIP FDB CLI commands - - - - - - - 6-54

6.2.10 VoIP SIP ALERTINFO command reference - - - 6-57
6.2.10.1 VoIP SIP ALERTINFO CLI commands - - - 6-57

6.3 VoIP phone ports - - - 6-59
6.3.1 Port configuration - - - 6-60
6.3.1.1 Digit map - - - 6-62
6.3.1.2 Dial mask - - - 6-63
6.3.1.3 Voice coder/decoder - - - 6-63
6.3.1.4 Voice quality management - - - 6-64
6.3.1.5 Country-specific telecom tones - - - 6-66
6.3.1.6 Port enable/disable - - - 6-67
6.3.2 VoIP ADMIN Command Reference - - - 6-67
6.3.2.1 VoIP ADMIN commands - - - 6-67
6.3.3 VoIP EP command reference - - - 6-75
6.3.3.1 VoIP EP CLI commands - - - 6-75

6.4 Common VoIP attributes: QoS, Media and DTMF-Relay - - - 6-120
6.4.1 QoS - - - 6-120
6.4.2 Media - - - 6-120
6.4.2.1 Media Timeout - - - 6-121
6.4.3 DTMF-RELAY - - - 6-121
6.4.4 Functional Differences for Common VoIP attributes in Product Categories - - - 6-121
6.4.5 VOIP QOS command reference - - - 6-122
6.4.5.1 VoIP QoS CLI commands - - - 6-122
6.4.6 VoIP Media command reference - - - 6-126
6.4.6.1 VoIP Media CLI commands - - - 6-126
6.4.7 VoIP DTMF-RELAY command reference - - - 6-129
6.4.7.1 VoIP DTMF-RELAY CLI commands - - - 6-129

7 Quality of Service - - - 7-1

7.1 QOS - - - 7-1
7.1.1 Introduction - - - 7-1
7.1.2 QoS architecture overview - - - 7-1
7.1.3 QoS implementation for DIFFSERV - - - 7-2
7.1.3.1 The Classifier - - - 7-2
7.1.3.2 Classifying packets - - - 7-3
7.1.3.3 Meter - - - 7-5
7.1.3.4 Scheduler - - - 7-9
7.1.4 ATM QoS Feature - - - 7-15
7.1.4.1 ATM Packet Prioritization - - - 7-15
7.1.4.2 How ATM packet prioritization works - - - 7-16
7.1.4.3 Configuring priority handling support - - - 7-17

7.1.5 Classifier command reference ---------- 7-17
7.1.5.1 Classifier CLI commands ---------- 7-17
7.1.6 Meter command reference ---------- 7-42
7.1.6.1 Meter CLI commands ---------- 7-42
7.1.6.2 Scheduler CLI commands ---------- 7-51

7.2 L2Filter ---------- 7-60
7.2.1 Overview ---------- 7-60
7.2.1.1 Packet Flow ---------- 7-60
7.2.2 L2Filter Command Reference ---------- 7-61
7.2.2.1 L2 Filter CLI commands ---------- 7-61

8 ADSL Port ---------- 8-1

8.1 Overview ---------- 8-1
8.1.1 ADSL upload interface ---------- 8-1
8.1.2 Documentation Structure ---------- 8-1

8.2 ADSL System description ---------- 8-2
8.2.1 Overview ---------- 8-2
8.2.2 ADSL connection via RFC1483 bridged mode ---------- 8-2
8.2.3 ADSL connection via RFC1483 routed mode ---------- 8-4
8.2.4 ADSL connection via Point to Point Protocol over ATM (PPPOA) ---------- 8-4

8.3 Port a1 ---------- 8-5
8.3.1 Port a1 command reference ---------- 8-5
8.3.1.1 Port a1 CLI commands ---------- 8-5

8.4 Bridge ---------- 8-36
8.4.1 Basic bridge configuration ---------- 8-36
8.4.2 Multiple VLAN support ---------- 8-38
8.4.3 Bridge command reference ---------- 8-39
8.4.3.1 Bridge CLI commands ---------- 8-39

8.5 Transports ---------- 8-49
8.5.1 Transports command reference ---------- 8-50
8.5.1.1 Transports CLI commands ---------- 8-50

8.6 Ethernet ---------- 8-58
8.6.1 Ethernet command reference ---------- 8-58
8.6.1.1 Ethernet CLI commands ---------- 8-59

8.7 PPPoE ---------- 8-62
8.7.1 PPPoE Overview ---------- 8-62

8.7.2 PPPoE Functional Overview - - - 8-64
8.7.2.1 PPPoE Connections - - - 8-64
8.7.2.2 PPPoE connections over ATM - VLAN Unaware - - - 8-65
8.7.2.3 PPPoE connections - VLAN Aware - - - 8-65
8.7.2.4 Populating automatically routing table and DNS server table - - - 8-66
8.7.2.5 Configuration Option to Clamp Maximum TCP MSS Value - - - 8-67
8.7.3 Functional Differences in Product Categories - - - 8-67
8.7.4 PPPoE command reference - - - 8-67
8.7.4.1 PPPoE CLI commands - - - 8-67

8.8 PPPoA - - - 8-114
8.8.1 PPPoA command reference - - - 8-114
8.8.1.1 PPPoA CLI commands - - - 8-114

8.9 RFC1483 - - - 8-151
8.9.1 RFC1483 command reference - - - 8-151
8.9.1.1 RFC1483 CLI command - - - 8-151

9 Wireless - - - 9-1

9.1 Wireless Interface - - - 9-1
9.1.1 Wireless LAN module - - - 9-1
9.1.2 Layer 2 switch on wireless port - - - 9-1
9.1.2.1 Layer 2 CPE Configuration for ADSL A group wireless products - - - 9-2
9.1.2.2 Layer 2 CPE Configuration for ADSL B group wireless products - - - 9-6
9.1.3 Layer 3 routing on wireless port - - - 9-10
9.1.3.1 Layer 3 CPE Configuration for ADSL A group wireless products - - - 9-11
9.1.3.2 Layer 3 CPE Configuration for ADSL B group wireless products - - - 9-15
9.1.4 Authentication Configuration - - - 9-18
9.1.4.1 Open Authentication Configuration - - - 9-18
9.1.4.2 Shared Authentication Configuration - - - 9-19
9.1.4.3 WPA-PSK Authentication and TKIP Encryption - - - 9-20
9.1.4.4 WPA2-PSK Authentication and AES_CCMP Encryption - - - 9-21
9.1.4.5 WPA2 Mixed Mode Authentication - - - 9-21
9.1.5 Summary of wireless attribute and configurations - - - 9-21
9.1.6 Wireless Interface CLI commands - - - 9-22
9.1.6.1 802.1x Authenticator commands - - - 9-22
9.1.6.2 Port Wireless commands - - - 9-25
9.1.6.3 WPA Commands - - - 9-35

10 LAN Module Management - - - 10-1

10.1 System Overview - - - 10-1

10.1.1 Default Factory Configuration - **10-1**
10.1.2 Adding/Removing & Changing LAN Modules - 10-1
10.1.3 Device and Module Compatibility - 10-1
10.1.4 Functional Differences for LAN Modules Management in Product Categories - - - 10-2

10.2 HPNA LAN Module - 10-2
10.2.1 HPNA Deployment Model - 10-2

10.3 HPNA Command Reference - 10-3
10.3.1 Overview - 10-3
0.0.1 System CLI commands - 10-3

10.4 CES LAN Module - 10-8
10.4.1 CES Deployment Model - 10-8

10.5 Circuit Emulation Command Reference - 10-9
10.5.1 Overview - 10-9
10.5.1.1 CES CLI commands - 10-9

List of Tables

Table i-1 Active Fiber Gateways - i-5
Table i-2 Active Fiber Gateways with RF Overlay - i-6
Table i-3 RG/iMG Models - i-8
Table i-4 iMG Models Supported in 3-7 - i-10
Table i-5 Main Features and where they apply to Product Type - i-11
Table i-6 - i-13
Table 1-1 System Commands -1-13
Table 1-2 Webserver Commands Provided by the CLI -1-39
Table 1-3 Emergency CLI Commands -1-50
Table 1-4 SwUpdate Commands -1-69
Table 1-5 ZTC Client Commands -1-81
Table 2-1 Functional Mapping for Switching- 2-7
Table 2-2 *Switch* commands - 2-9
Table 2-3 Functional Mapping for Bridge -2-40
Table 2-4 *Bridge* commands -2-41
Table 2-5 Reserved VID Values -2-88
Table 2-6 -2-92
Table 3-1 Functional Mapping for Bridge -3-16
Table 3-2 *Bridge* IGMP Snooping Commands- -3-17
Table 4-1 *IP CLI* commands- 4-9
Table 4-2 Security Commands and Product Category -4-68
Table 4-3 Firewall commands and Product Type -4-107
Table 4-4 Default Policies Enabled in the Firewall - High Security -4-111
Table 4-5 Default Policies Enabled in the Firewall - Medium Security -4-112
Table 4-6 Default Policies Enabled in the Firewall - Low Security -4-112
Table 4-7 NAT CLI Commands and Product Category -4-138
Table 5-1 DHCP server CLI commands
- 5-9
Table 5-2 DHCP client CLI commands -5-55
Table 5-3 DHCP Relay Commands
- -5-80
Table 5-4 DNS Relay Commands
- -5-85
Table 5-5 DNS Client Commands
- -5-90
Table 5-6 DNS Client Commands
- -5-95
Table 5-7 Time Abbreviations when Setting Timezone Difference -5-98
Table 6-1 Functional Mapping for VoIP MGCP- 6-5
Table 6-2 *VoIP MGCP* commands - 6-5
Table 6-3 Possible Combinations for MGCP Profile- 6-9
Table 6-4 VoIP SIP Protocol CLI Commands

- 6-25
Table 6-5 VoIP SIP Location Server CLI Commands - 6-38
Table 6-6 Commands for VoIP Proxy Server - 6-41
Table 6-7 Commands for VoIP Embeddedserver - 6-44
Table 6-8 Commands for VoIP SIP User - 6-48
Table 6-9 VoIP SIP SDB CLI Commands - 6-54
Table 6-10 VoIP SIP Alertinfo CLI commands - 6-58
Table 6-11 Codecs Available for iMGs - 6-64
Table 6-12 Country-specific Telecom tones - 6-66
Table 6-13 Commands for VoIP Admin- 6-68
Table 6-14 Commands for VoIP EP - 6-76
Table 6-15 Functional Mapping for Common VoIP attributes - 6-122
Table 6-16 *VoIP QoS* commands - 6-122
Table 6-17 *VoIP Media* commands - 6-126
Table 6-18 *Commands for VoIP DTMF* - 6-129
Table 7-1 *Classifier* commands - 7-17
Table 7-2 Meter commands - 7-42
Table 7-3 *Scheduler* commands - 7-51
Table 7-4 L2filter commands - 7-61
Table 8-1 Port a1 Commands - 8-5
Table 8-2 Options for ADSL Port Attributes- 8-7
Table 8-3 Bridge commands - 8-39
Table 8-4 Transport commands - 8-50
Table 8-5 Ethernet commands - 8-59
Table 8-6 Functional Mapping for PPPoE - 8-67
Table 8-7 PPPoE commands provided by the CLI - 8-68
Table 8-8 PPPOA Command - 8-114
Table 8-9 RFC1883 Commands - 8-151
Table 9-1 Summary of wireless port attributes versus wireless security schemes - 9-22
Table 9-2 802.1x Authenticator Commands - 9-23
Table 9-3 Port Wireless Commands - 9-25
Table 9-4 Port Wireless Commands - 9-36
Table 10-1 Functions for Modular iMGs - 10-2
Table 10-2 HPNA Commands - 10-4
Table 10-3 *CES* commands - 10-10

List of Figures

Figure 1-1 4 MByte Flash Memory partitions - 1-6
Figure 1-2 8 MByte Flash Memory partition - 1-8
Figure 1-3 Configuration files backup process - example - 1-11
Figure 1-4 The Windows™ Loader - 1-58
Figure 1-5 The Web Interface main page - 1-59
Figure 1-6 The Web Interface Firmware Update page - 1-60
Figure 1-7 Normal *SwUpdate* operation mode - 1-62
Figure 1-8 SwUpdate scheduling example 1 - 1-65
Figure 1-9 *SwUpdate* scheduling example 2 - 1-66
Figure 1-10 ZTC network architecture - 1-75
Figure 1-11 *Pull-at-Startup* ZTC phase - 1-78
Figure 1-12 *Scheduled-pull* ZTC phase - 1-80
Figure 1-13 A manager Entity - 1-85
Figure 1-14 An agent Entity - 1-85
Figure 1-15 hmac expression - 1-87
Figure 1-16 vacmViewTreeFamilyMask - 1-94
Figure 1-17 vacmViewTreeFamilyMask (continued) - 1-94
Figure 1-18 snmpNotifyFilterMask - 1-100
Figure 1-19 snmpNotifyFilterMask (continued) - 1-100
Figure 1-20 snmpTargetAddrTMask - 1-103
Figure 1-21 snmpTargetAddrTMask (continued) - 1-104
Figure 1-22 snmpTargetAddrTMask (continued) - 1-104
Figure 1-23 snmpTargetAddrTMask (continued) - 1-104
Figure 1-24 snmpTargetAddrTMask (continued) - 1-105
Figure 2-1 IP packet overview - 2-6
Figure 2-2 Tagged frame format according to IEEE 802.3ac standard - 2-86
Figure 2-3 IP interface over LAN - first steps - 2-91
Figure 3-1 IGMP messages flow when Snoop-Only mode is active - 3-5
Figure 3-2 Two Hosts Join Two Different Mulitcast Channels - 3-8
Figure 3-3 Two Hosts Join Two Different Multicast Channels - 3-10
Figure 3-4 Host Disconnects - No Leave Message - 3-11
Figure 3-5 One and Two Hosts Leave the Same Multicast Stream - 3-12
Figure 4-1 Security modules on AT-iMG Models - 4-58
Figure 4-2 Security interfaces on AT-iMG Models - 4-59
Figure 4-3 Address Conservation Using NAT - 4-135
Figure 5-1 Domain Name System - 5-83
Figure 6-1 Phone --> iMG(A) --> iMG(B) --> Phone - 6-17
Figure 6-2 Phone --> iMG(A) --> SIP IP Phone - 6-18
Figure 6-3 VoIP subsystem configuration - basic steps - 6-19

Figure 6-4 VoIP subsystem configuration - basic steps ---------- 6-61
Figure 7-1 Gateway Architecture ---------- 7-2
Figure 7-2 Metering for Traffic Control ---------- 7-8
Figure 7-3 Overview of Scheduler Functionality ---------- 7-10
Figure 7-4 Scheduling Process for Packet Enqueuing ---------- 7-13
Figure 7-5 Scheduling Process for Packet Dequeuing ---------- 7-14
Figure 7-6 The ADSL Driver ---------- 7-16
Figure 8-1 ADSL upload interface module ---------- 8-2
Figure 8-2 Basic software bridge configuration ---------- 8-37
Figure 8-3 Example of system architecture to support multiple vlan management ---------- 8-38
Figure 8-4 Example of PPPoE connection ---------- 8-64
Figure 9-1 Wireless interface usage on a bridged scenario ---------- 9-2
Figure 9-2 Wireless interface usage on a routed scenario ---------- 9-11
Figure 10-1 HPNA Section of LAN Module Diagram ---------- 10-3
Figure 10-2 Typical CES Deployment Model: ---------- 10-8

1. System Configuration

1.1 System Management

This section provides information regarding access to the gateway, the login process, command line interface (CLI) and the different types of user access.

1.1.1 System Configuration

1.1.1.1 Access to the Gateway

The gateway can be configured in different ways,either through the CLI or using the web interface.

The CLI is accessible through the serial interface, Telnet, or an SSH connection.

The web interface is accessible through the Microsoft Internet Explorer WEB browser.

Each different gateway family has a different configuration and access capability according to the following table:

Group	Serial interface	Telnet	SSH	WEB
Fiber A	NO	YES	NO	NO
Fiber B	YES	YES	NO	YES
Fiber C	YES	YES	NO	NO
Fiber D	YES	YES	YES	YES
Fiber E	YES	YES	YES	YES
Modular	YES	YES	YES	YES
ADSL A	NO	YES	YES	YES
ADSL B	YES	YES	YES	YES

1.1.1.2 Default Factory Configuration

The default configuration stored on the gateway when delivered to the customer is called “factory”.

The default "factory" configuration has the DHCP client enabled on all interfaces, including xDSL in the xDSL-based modem with a bridged RFC1483 over PVC 0.35.

The IP management interface is set dynamically at startup.

It is possible to connect remotely to the gateway using Telnet of SS4 once an IP address has been assigned to the gateway.

In order to access the gateway, the user is required to enter a username and password.

The following default values give super-user access to the CLI commands and must be used only by administrators to configure the system and create user access with restricted privileges:

- IP address: dynamically assigned by the DHCP server
- Telnet port: 23
- Login: manager
- Password: friend

For gateways with a serial interface, it is possible to connect using a suitable cable and serial terminal program.

The following configuration parameters must be set on the terminal program for serial access:

- Baud rate: 38400
- Data: 8 bit
- Parity: none
- Stop: 1 bit
- Flow control: none

Serial access uses the same security credentials as for remote access.

1.1.1.3 Minimal Configuration

To access the gateway CLI when no DHCP server is available on the network, it is possible to load the gateway with a well known configuration - called the "minimal" configuration.

A default minimal configuration exists on the gateway. This can be customized or replaced with a minimal configuration created by the customer.

The minimal configuration is accessible from the serial interface. To start the gateway using the minimal configuration, first power-off the unit. Then keep the "R" button pressed on the PC keyboard for at least 30 seconds was the unit is powered-on.

If the default minimal configuration has not been replaced by a customised version, once the system has completed the bootstrap phase it will be possible to connect remotely (via Telnet or SSH) and serially to the gateway using the following parameters:

- IP address: 192.168.1.1

- Login: *manager*
- Password: *friend*
- To install a custom minimal configuration on the gateway see the section related to the software update module.

1.1.2 Command Line Interface and Console

On the gateway two types of consoles are available:

- ***Standard CLI (Command Line Interface): this is used to configure and manage the system. It provides full access to the system modules included in this manual.***
- ***Debug console: this is a special console (also named simply as console), available to users with super-user rights for access to hidden debug commands that are not available in the standard command line. Console commands are not documented in this administration guide. Access to console is possible only from inside a CLI session.***

1.1.2.1 Access permissions to CLI

There are three CLI access levels (via local craft interface, telnet or SSH), each providing different levels of allowed operations:

- ***Default user*** - can use CLI commands. Only "show" and "list" commands are available. Cannot access console commands.
- ***Engineer user*** - can use most of CLI commands without restriction. Cannot create or modify CLI users. Cannot access console commands.
- ***Super user*** - can use all CLI commands without restriction. Can create or modify CLI users, changing their passwords. Can access console commands without restriction.

The following table maps the user properties to the corresponding CLI credentials. User properties can be configured via CLI commands by setting the *user access level* (default, engineer, administrator) and the *mayconfigure* flag (enabled, disabled)

access level	mayConfigure	Allowed CLI operations
default	disabled	No access to CLI
default	enabled	Limited CLI commands access (only read operations)
engineer	disabled	No access to CLI
engineer	enabled	Full CLI commands access except user creation/modify and debug console

access level	mayConfigure	Allowed CLI operations
superuser	disabled	No access to CLI
superuser	enabled	Full CLI commands access (read and write operations)

To create new user accounts, use the SYSTEM ADD USER or SYSTEM ADD LOGIN commands. The accounts created by these commands default to low privileges.

To change user privileges, use the SYSTEM SET USER ACCESS or SYSTEM SET LOGIN ACCESS commands.

To list the current user or login accounts, use the SYSTEM LIST USER or SYSTEM LIST LOGIN commands, respectively.

The user-related commands are details in Section 1.1.5

1.1.2.2 Access permissions to WEB interface

Similarly to CLI permission, the access to WEB interface is controlled by the user access level and by the *mayconfigureweb* flag:

- ***Default user*** - can access to Status pages, Wireless configuration and user password settings. Cannot access to the other configuration pages.
- ***Engineer or Super user*** - can access to Status , Wireless configuration, Security configuration, firmware upgrade pages.

The following table maps the user properties to the corresponding WEB credentials. User properties can be configured via CLI commands by setting the *user access level* (default, engineer, administrator) and the *mayconfigureweb* flag (enabled, disabled).

access level	mayConfigureWeb	Allowed CLI operations
default	disabled	No access to WEB interface
default	enabled	Status pages, Statistics, Wireless settings (basic & advanced), User password change Configuration saving
engineer/ superuser	disabled	No access to WEB interface

access level	mayConfigureWeb	Allowed CLI operations
engineer/ superuser	enabled	Status pages, Statistics, Wireless settings (basic & advanced), Security (NAT and Firewall) Settings DHCP server settings Routing configuration User password change Firmware Upgrade Configuration saving

1.1.2.3 Split management

Split management is part of the NMS provisioning framework.

Split management allows the end-user to perform configurations via WEB interface while the management of the system is kept under the network administrator control (NMS).

When split management is enabled, a login user is created with login "admin" and default password "admin".

The end-user can access to WEB pages to configure wireless parameters and to change his own password.

The end-user cannot configure other system parameters like security, dhcpserver and he cannot execute firmware upgrade. These configuration changes are still under the network administrator control.

When split management is disabled, the end-user doesn't have access to the system WEB pages at all.

1.1.3 File system

The file system differs according to the gateway memory capacity and the presence or absence of an EEPROM.

There are three different file system cofigurations:

- Gateways with 4Mbytes of FLASH (Fiber A, Fiber B, Fiber C)
- Gateways with 8MBytes of FLASH with EEPROM (Modular, ADSL A)
- Gateways with 8MBytes of FLASH without EEPROM (Fiber E, ADSL B, ADSL C)

The software running on the gateway is a multi thread application where each task typically needs to load configuration information when it starts, and store configuration changes for future use.

To support the above requirements, two dedicated file systems are provided. These are called the ***In Store File System*** and the ***Flash File System***. The two file systems provide a standard file interface to application processes. These two file systems are referred to as ***isfs*** and ***flashfs*** respectively in this document. The ***isfs*** provides volatile run-time file storage whereas the ***flashfs*** provides non-volatile file storage. The flash memory is partitioned according to sections Section 1.1.3.1 and Section 1.1.3.2

1.1.3.1 Gateway with 4Mbytes of FLASH

The file system on the gateway with 4 Mbytes fo FLASH is depicted in the Figure 1-1

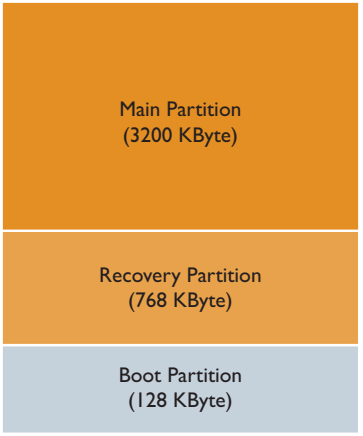


FIGURE 1-1 4 MByte Flash Memory partitions

1.1.3.1.1 Boot partition

The *Boot ROM* program resides in a special partition (the *Boot Partition*) on the flash device. This is the first code that runs when the system is started and provides self-test code as well as the ability to load the main run-time images.

The boot partition cannot be read or written by the *flashfs process,* and typically doesn't require upgrade. The boot partition is automatically over-written when the gateway is upgraded using a flash image. In all other cases the boot ROM program and boot partition are never altered.

1.1.3.1.2 Recovery partition

The *Recovery Partition* is a reserved partition on the flash device where a minimal operating system named *Recovery Application code* is installed. This operating system runs only if the boot ROM code is not able to

start the main application code because, if for example the main partition has been corrupted by a system power-off during software upgrade.

Services available in the Recovery Application Code are a subset of those available in the Main Application Code: for example VoIP modules, SSH and SNMP access are not available.

Note: Recovery Application Code uses the same configuration file as the Main Application Code. Configuration parameters for modules not available on Recovery Application Code are simply ignored when the CPE runs in recovery mode.

1.1.3.1.3 Main partition

The gateway operating system is named *Main Application code* and is stored in a third ***flashfs*** partition area (the *Main Partition*) that provides permanent storage for the *Main Application code,* and for files that are normally used only during system bootstrap.

During the system bootstrap the files stored in the main partition are copied into ***isfs*** in order to make them available to all application processes. Processes typically use the ***isfs*** to store temporary configuration data.

The configuration is stored within the main partition.

1.1.3.2 Gateway with 8MBytes of FLASH with and without EEPROM

The main difference between models with and without the EEPROM is the location of unit-specific information like MAC address, serial number, model name etc.

Figure 1-2 below depicts the two different partitions side-by-side. 8 MByte Flash Memory partitioned with and without EEPROM

FIGURE 1-2 8 MByte Flash Memory partition

1.1.3.3 Boot partition

The ***Boot ROM*** program resides in a special partition (the *Boot Partition*) on the flash device. This is the first code that runs when the system is booted and provides self-test code as well as the ability to load the main run-time images.

The boot partition cannot be read or written by the ***flashfs*** process and typically doesn't require upgrade. The boot partition is automatically over-written when the gateway is upgraded using a flash image. In all the other cases the boot ROM program and boot partition are never altered.

1.1.3.4 Recovery partition

The *Recovery Partition* is a reserved partition on the flash device where a minimal operating system named *Recovery Application code* is installed. This operating system runs only if the boot ROM code is not able to start the main application code if for example, because the main partition has been corrupted by a system power-off during software upgrade.

Services available in Recovery Application Code are a subset of those available in the Main Application Code: for example VoIP modules, SSH and SNMP access are not available.

Note: Recovery Application Code uses the same configuration file used by Main Application Code. Configuration parameters for modules not available on Recovery Application Code are simply ignored when the CPE runs in recovery mode.

1.1.3.5 Main partition

The gateway operating system is named *Main Application code* and is stored in a third ***flashfs*** partition area (the *Main Partition*) that provides permanent storage for the *Main Application code* and for files that are normally used only during system bootstrap.

During the system bootstrap, the files stored in the main partition are copied into ***isfs*** in order to make them available to all application processes. Processes typicallyuse the ***isfs*** to store temporary configuration data.

1.1.3.6 Configuration partitions

This gateway adopts a partition architecture based on two Configuration Partitions.

One configuration partition is used to backup the other one in case of flash corruption during configuration update. Any time a configuration partition needs to be changed, an identical backup copy is created.

To increase system robustness and avoid loss of configuration when the CPE runs in recovery or is rebooted during a configuration save process, configuration files are saved in separate partitions from the main application code.

*Note: The **Command Line Interface** doesn't allow access to the **flashfs** file system or to the **isfs** in store file system because this is not typically required by user.*
*The Flash file system **flashfs**, in store file system **isfs** and special debug functions are available only through the debug console command line.*

1.1.4 Configuration Management

Each active gateway configuration can be saved as configuration file for future reference, or as bootstrap configuration file.

Up to two custom configuration files can be permanently stored in the system, with one of them marked as the active configuration file to be executed during the bootstrap phase.

Configurations are not stored as a sequence of commands but in a proprietary format.
The format of the configuration files follows the Information Model used by the main application code where a typical object tree representation is used to categorize and map system objects attributes.

The following example shows a snapshot of a generic configuration file.

```
# Information Model configuration file
version 4
N ImGwaAdmins ImGwaAdmins
N ImGwaAdmin ImGwaAdmins.gwa_admin
      A Profile none
```

```
N ImGwaSips ImGwaSips
N ImGwaSip ImGwaSips.gwa
      A ControlProtocol SIP
      A Enable true
      A Authentication proxy
      A DefaultPort 5060
      A KeepAlive disabled
      A KeepAlive_Time 300
      A NAT none
      A NetInterface ip0
      A RTT 500
      A SE 1800
      A Support none
      A TimerB 32
```

To create a configuration that stores the current running system configuration, simply use the system config create command. This command will create a file with the filename specified by the user in the Information Model format and will save it permanently in the flash.

To extend configuration flexibility, it is possible at bootstrap time to force the gateway to execute a configuration file written in standard CLI syntax. As it is not possible to save a running configuration directly into a file in CLI syntax, a special set of commands has been provided that allow the loading of a configuration file (written in CLI syntax) from a remote ftp or tftp server.

To set a configuration file as the bootstrap configuration file (irrespective of whether it has been written in Information Model format or CLI syntax), use the `system config set` command.

To display the list of the existing configuration files use the `system config list` command.

To retrieve the bootstrap configuration filename or to display the content of a configuration file use the `system config show command.`

It is also possible set the gateway to a default factory configuration (see Section 1.1.5.1.10) using the `system config set factory` command and then restarting the gateway.

It is possible set the gateway to a minimal configuration (see Section 1.1.5.1.10) using the `system config set none` command, and then restart the device.

1.1.4.1 Configuration File Saving and Backup Process

On the units with 8 MBytes of FLASH configuration partitions are duplicated to support redundancy. Each configuration partition includes the same files as its peer partition.

A special file named “version” is present within each configuration partition. This stores an incremental number that differs between the two partitions by one. During the bootstrap phase the configuration partition having the version file with the higher value is nominated to be the active configuration partition while the other is assumed to be the backup partition.

Figure 1-3 details the backup process executed when a configuration file is created and set as bootstrap configuration.

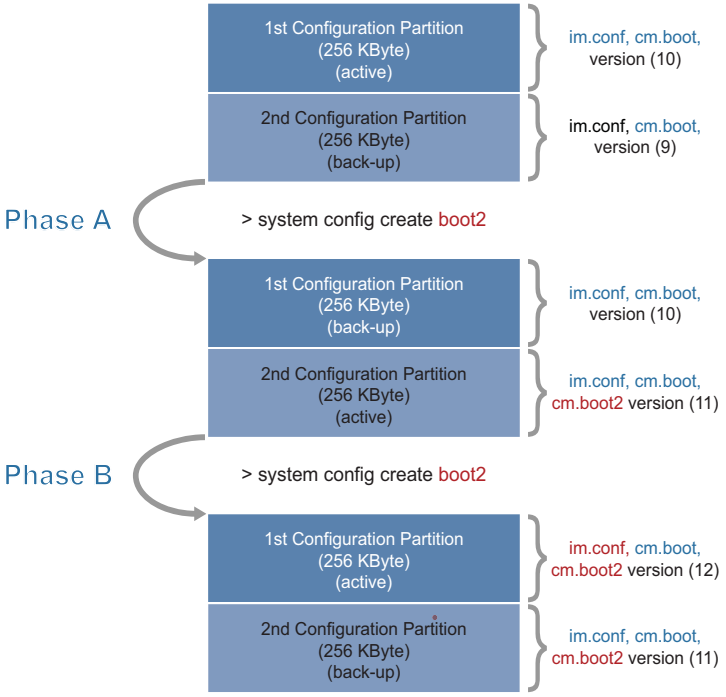


FIGURE 1-3 Configuration files backup process - example

At the bootstrap phase the gateway activates the configuration stored in the active configuration partition, based on the higher value stored in the "version" file available on both the two configuration partitions.

In Figure 1-3, when the configuration file "boot2" is generated via the `system config create` command (phase A), the backup process first copies the content of the active configuration partition to the current backup configuration partition. It then updates the backup configuration partition with the new configuration file "boot2" and increments the content of file version in the backup configuration partition to be one value higher than the active configuration partition.

At this point, if the gateway restarts the role of the two partitions is swapped. The second partition will be the active configuration partition while the other will be the backup.

Note also that if during the `system config create` command the gateway restarts or power-cycles, only the backup configuration partition (the second in the example) will be corrupted, leaving the first configuration partition responsible for configuring the gateway.

Following the example in Figure 1-4; when the configuration file "boot2" is set to be the bootstrap configuration file via the `system config set` command (phase B), the backup process first copies the content of the active configuration partition (now the second partition) to the backup configuration partition (the first partition). It then updates the im.conf file in the backup configuration partition to be a copy of the new configuration file "boot2" and increments the content of file version in the backup config partition to be one value higher than the active configuration partition.

At this point, if the gateway restarts the rule of the two partitions are swapped yet again. The first partition will be the active configuration partition while the second will be the backup.

If during the system config set command, the gateway restarts or power-cycles, only the backup configuration partition (the first in the example) will be corrupted, leaving the second configuration partition responsible for configuring the gateway and preserving the original bootstrap configuration file as well as the newly generated (from Phase A) configuration file.

Note: When a configuration partition is corrupted, the first system config create or set command will cause the backup process to format and restore the invalid partition so it can receive a copy of the current active configuration partition.

1.1.5 System command reference

This section describes the commands available on the gateway to configure and manage the ***system*** module.

1.1.5.1 System CLI commands

Table 1-1 ***lists all system*** commands provided by the CLI:

TABLE 1-1 System Commands

Option	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SYSTEM ADD USER	X	X	X	X	X	X	X	X	X
SYSTEM ADD LOGIN	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG CREATE	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG DELETE	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG GET	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG HELP	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG LIST	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG PUT	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG RESTORE	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG SET	X	X	X	X	X	X	X	X	X
SYSTEM CONFIG SHOW	X	X	X	X	X	X	X	X	X
SYSTEM CONTACT	X	X	X	X	X	X	X	X	X
SYSTEM CPULOAD	X	X		X	X	X	X	X	X
SYSTEM DELETE USER	X	X	X	X	X	X	X	X	X
SYSTEM INFO	X	X	X	X	X	X	X	X	X
SYSTEM LEGAL	X	X	X	X	X	X	X	X	X
SYSTEM LIST ERRORS	X	X	X	X	X	X	X	X	X
SYSTEM LIST OPENFILES	X	X	X	X	X	X	X	X	X
SYSTEM LIST USERS	X	X	X	X	X	X	X	X	X
SYSTEM LIST LOGINS	X	X	X	X	X	X	X	X	X
SYSTEM LOCATION	X	X	X	X	X	X	X	X	X
SYSTEM LOG	X	X	X	X	X	X	X	X	X
SYSTEM LOG ENABLE|DISABLE	X	X	X	X	X	X	X	X	X
SYSTEM LOG LIST	X	X	X	X	X	X	X	X	X

Option	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SYSTEM NAME	X	X	X	X	X	X	X	X	X
`--> system name AT-iMG616BD-Routed`	X	X	X	X	X	X	X	X	X
SYSTEM LOCATION	X	X	X	X	X	X	X	X	X
SYSTEM RESTART	X	X	X	X	X	X	X	X	X
SYSTEM SET LOGIN ACCESS	X	X	X	X	X	X	X	X	X
SYSTEM SET LOGIN MAYCONFIGURE	X	X	X	X	X	X	X	X	X
SYSTEM SET LOGIN MAYCONFIGUREWEB	X	X	X	X	X	X	X	X	X
SYSTEM SET LOGIN MAYDIALIN	X	X	X	X	X	X	X	X	X
SYSTEM SET USER ACCESS	X	X	X	X	X	X	X	X	X
SYSTEM SET USER MAYCONFIGURE	X	X	X	X	X	X	X	X	X
SYSTEM SET USER MAYDIALIN	X	X	X	X	X	X	X	X	X
SYSTEM SET USER PASSWORD	X	X	X	X	X	X	X	X	X

1.1.5.1.1 SYSTEM ADD USER

Syntax `SYSTEM ADD USER <name> ["comment"]`

Description This command adds a user to the system. Only a user with *superuser* rights can use this command. This command is typically used to create a PPP user on the system.

The default settings in the table below are applied to new accounts that are added using the SYSTEM ADD USER command. (A different set of defaults is applied to a new account added using the SYSTEM ADD LOGIN command.)

New account settings	Default Value
Dialing to the system	Enabled
Login to the system	Disabled
Login to the	Disabled
Access permissions	default user

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	A unique user name made up of more than one character that identifies an individual user and lets the user access the system.	N/A
COMMENT	An optional comment about the user that is displayed when you type the commands SYSTEM LIST USERS and SYSTEM LIST LOGINS.	No comment added

Example `--> system add user ckearns "Typical user"`

See also
```
SYSTEM SET USER ACCESS
SYSTEM SET USER MAYDIALIN
SYSTEM SET USER MAYCONFIGURE
SYSTEM LIST USERS
SYSTEM DELETE USER
```

1.1.5.1.2 SYSTEM ADD LOGIN

Syntax `SYSTEM ADD LOGIN <name> ["comment"]`

Description This command adds a user to the system. Only a a user with *superuser* rights can use this command.

The default settings in the table below are applied to new accounts that are added using the SYSTEM ADD LOGIN command. (A different set of defaults is applied to a new account added using the SYSTEM ADD USER command.)

New account settings	Default Value
Dialing to the system	Disabled
Login to the system	Enabled
Login to the web pages	Enabled
Access permissions	default user

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	A unique login name made up of more than one character that identifies an individual user and lets the user access the system.	N/A
COMMENT	An optional comment about the user that is displayed when you type the commands SYSTEM LIST USERS and SYSTEM LIST LOGINS.	Blank (No comment added)

Example `--> system add login ckearns "temporary contractor"`

See also
```
SYSTEM DELETE LOGIN
SYSTEM LIST LOGINS
```

1.1.5.1.3 SYSTEM CONFIG CREATE

Syntax `SYSTEM CONFIG CREATE <filename>`

Description This command creates a configuration file named <filename> storing the current running system configuration and save permanently it in the flash.

It is possible create up to two configuration files. If a configuration with the same name already exists, the new one will overwrite the previous configuration file without warning.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
FILENAME	The name of the file where the current running configuration is saved. The following filenames are reserved and cannot be used: factory none	N/A

Example `--> system config create myfile`

See also
```
SYSTEM CONFIG DELETE
SYSTEM CONFIG GET
SYSTEM CONFIG LIST
```

```
SYSTEM CONFIG SET
SYSTEM CONFIG SHOW
```

1.1.5.1.4 SYSTEM CONFIG DELETE

Syntax `SYSTEM CONFIG DELETE <filename>`

Description This command deletes the configuration file named <filename> from the flash.

It's not possible delete a configuration file that has been set as bootstrap configuration file. In this case it's necessary change the bootstrap configuration file (for example setting it to none) before deleting it.

To retrieve the configuration file list use the SYSTEM CONFIG LIST command. To display the current bootstrap configuration file use the SYSTEM CONFIG SHOW command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
FILENAME	The name of an existing configuration file. The following filenames are reserved and cannot be used: factory none	N/A

Example `--> system config delete myfile.cfg`

See also
```
SYSTEM CONFIG CREATE
SYSTEM CONFIG GET
SYSTEM CONFIG LIST
SYSTEM CONFIG SET
SYSTEM CONFIG SHOW
```

1.1.5.1.5 SYSTEM CONFIG GET

Syntax `SYSTEM CONFIG GET <url>`

Description This command retrieves a configuration file from a remote TFTP or FTP server and save it permanently in the configuration file list.

If the retrieved configuration file has the same filename as an existing file, the new file will overwrite the old one even if it is the bootstrap configuration file without warning. On a

device can be present a maximum of two configuration files (factory + two more configuration files).

The address of the remote file to be downloaded is expressed accordingly to the following url syntax depending by the protocol used for the remote connection: ftp or tftp.

If tftp protocol is used, the url format is the following:

```
tftp://host[:port]/path/filename
```

If ftp protocol is used, the url format is the following:

```
ftp://login:password@host[:port]/path/filename
```

Where:

- *host* is the address of the TFTP / FTP server. Can be used expressed as hostname or as IPv4 address.
- *port* is the port where the TFTP / FTP server is listening for incoming connections.
- *path* is the relative path on the TFTP / FTP server root directory where the configuration file is stored.
- *login* and *password* are the username and password to get access on the FTP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
URL	The name of the file and address of the remote server where the configuration file must be downloaded. The url format depends by the protocol used for the remote connection: ftp or tftp. If tftp protocol is used, the url format is the following: tftp://host[:port]/path/filename In ftp protocol is used, the url format is the following: ftp://login:password@host[:port]/path/filename	N/A

Example The following command retrieves a configuration file named myconf.cfg from the TFTP server 192.168.1.100 located in the directory iMG600, and saves it into the flash memory:

```
--> system config get tftp://192.168.1.100/img600/myconf.cfg
```

The following command retrieves a configuration file named myconf.cfg from the TFTP server tftp.atkk.com root directory:

```
-->system config get tftp://tftp.atkk.com/myconf.cfg
```

The following command retrieves the configuration file named my.cfg from the FTP server ftp.atkk.it. User "manager" and password "friend" are used to log on the FTP server:

```
--> system config get ftp://manager:friend@ftp.atkk.it/
my.cfg
```

See also

```
SYSTEM CONFIG CREATE
SYSTEM CONFIG DELETE
SYSTEM CONFIG LIST
SYSTEM CONFIG SET
SYSTEM CONFIG SHOW
```

1.1.5.1.6 SYSTEM CONFIG HELP

Syntax `SYSTEM CONFIG HELP`

Description This command show the help for the system config commands

Example `--> system config help`

1.1.5.1.7 SYSTEM CONFIG LIST

Syntax `SYSTEM CONFIG LIST`

Description This command lists all the configuration files stored in flash memory.

Example `--> system config list`

```
Configuration Management file list:
 ID  |    Size    |    Name
-----|------------|-------------------------------------------
   1 |        669 | factory
   2 |       7343 | bootstrap.cfg
   3 |      10177 | mgcp.cfg
-----------------------------------------------------------------
```

See also

```
SYSTEM CONFIG CREATE
SYSTEM CONFIG DELETE
SYSTEM CONFIG LIST
SYSTEM CONFIG SET
SYSTEM CONFIG SHOW
```

1.1.5.1.8 SYSTEM CONFIG PUT

Syntax `SYSTEM CONFIG PUT <filename> <url>`

Description This command store a configuration file on a remote TFTP server.

filename is the name of the local file

url is the address of the remote server accordingly to the following url syntax.

`tftp://host[:port]/path/filename`

Where:

- *host* is the address of the TFTP server. Can be used expressed as hostname or IPv4 address.
- *port* is the port where the TFTP server is listening for incoming connections.
- *path* is the relative path on the TFTP server root directory where the configuration file is stored.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
FILENAME	The name of the file to be saved on the remote server	N/A
URL	The name of the file and address of the remote server where the configuration file must be downloaded.	N/A

Example The following command writes a configuration file named myconf.cfg from the gateway to a TFTP server 192.168.1.100 on a directory iMG600:

```
--> system config put myconf.cfg tftp://192.168.1.100/img600/
```

The following command writes a configuration file named myconf.cfg on TFTP server tftp.atkk.com root directory:

```
-->system config put myconf.cgf tftp://tftp.atkk.com/
```

See also
```
SYSTEM CONFIG CREATE
SYSTEM CONFIG DELETE
SYSTEM CONFIG LIST
SYSTEM CONFIG SET
SYSTEM CONFIG SHOW
```

1.1.5.1.9 SYSTEM CONFIG RESTORE

Syntax `SYSTEM CONFIG RESTORE <factory>`

Description This command tries to restore the configuration to factory without the need to reboot the units.

1.1.5.1.10 SYSTEM CONFIG SET

Syntax `SYSTEM CONFIG SET { <filename> | factory | none }`

Description This command set one of the existing configuration files as bootstrap configuration file. If *factory* is selected, the gateway is set to the default factory configuration (see Section 1.1.1.2).
If *none* is selected, the CPE is set to the minimal configuration (see Section 1.1.1.3).

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
FILENAME	The name of an existing configuration file. To retrieve the configuration file list use the SYSTEM CONFIG LIST command.	NA
FACTORY	When factory is selected the CPE is set to the default factory configuration having the management IP interface (ip0) with a dynamic IP address.	NA
NONE	When none is selected the CPE is set to the minimal configuration having the management IP interface (ip0) a static ip address: 192.168.1.1/24	NA

Example The following command set the configuration file named myconf as bootstrap configuration file:

```
--> system config set myconf
```

The following command restores the bootstrap configuration file to the default factory:

```
--> system config set factory
```

See also
```
SYSTEM CONFIG CREATE
SYSTEM CONFIG DELETE
SYSTEM CONFIG GET
SYSTEM CONFIG LIST
SYSTEM CONFIG SHOW
```

1.1.5.1.11 SYSTEM CONFIG SHOW

Syntax `SYSTEM CONFIG SHOW [ <filename> ]`

Description This command returns the name of the bootstrap configuration file. If filename is specified the command displays the contents of the configuration file.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
FILENAME	The name of an existing configuration file to be displayed. To retrieve the configuration file list use the SYSTEM CONFIG LIST command.	NA

Example `--> system config show myconf.cfg`

See also
```
SYSTEM CONFIG CREATE
SYSTEM CONFIG DELETE
SYSTEM CONFIG GET
SYSTEM CONFIG LIST
SYSTEM CONFIG SET
```

1.1.5.1.12 SYSTEM CONTACT

Syntax `SYSTEM CONTACT <NONE/sys-contact>`

Description This command set the system contact information on the gateway

Example `--> system contact info@company.com`

1.1.5.1.13 SYSTEM CPULOAD

Syntax `SYSTEM CPULOAD`

Description This command displays the cpu usage details of the system that you are using.

Example `--> system cpuload`

```
cpu usage: PP 3%, NP 1%
```

See also `SYSTEM INFO`

1.1.5.1.14 SYSTEM DELETE USER

Syntax `SYSTEM DELETE USER <name>`

Description This command deletes a user that has been added to the system using the SYSTEM ADD USER command or the SYSTEM ADD LOGIN command. Only a ***Super*** user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A

Example `--> system delete user ckearns`

See also `SYSTEM ADD USER`
`SYSTEM ADD LOGIN`

1.1.5.1.15 SYSTEM INFO

Syntax `SYSTEM INFO`

Description This command displays the vendor ID, URL, base MAC address and hardware and software version details of the current gateway system.

Example `--> system info`

```
Global System Configuration:
          Vendor : Allied Telesis
             URL : http://www.alliedtelesis.com
     MAC address : 00:0d:da:45:16:14
           Build : RG6X6E-MAIN
    Hardware ver : RG606BD
    Software ver : 3-7_01_26
    Recovery ver : 2-2_19
       Dsp clock : 98 Mhz
      Build type : RELEASE
 System Name     : dt-905S-Routed
 System Location : Inter AT labs
 System Contact  : admin@his_desk
 System Uptime   : 04:19:36
```

1.1.5.1.16 SYSTEM LEGAL

Syntax `SYSTEM LEGAL`

Description This command displays copyright information about the software that you are using.

Example `--> system legal`

```
(C) Copyright 2009 Allied Telesis Holdings K.K. - All rights
reserved.
```

1.1.5.1.17 SYSTEM LIST ERRORS

Syntax `SYSTEM LIST ERRORS`

Description This command displays a system error log. The error log contains the following information:

- The time (in minutes) that an error occurred, calculated from the start of your login session
- The module that was affected by the error
- A brief description of the error itself

Example `--> system list errors`

```
Error log:
    When    |    Who     |    What
------------|------------|-----------------------------------------------
104  |webserver|webserver:Failedtocreatenodetype'ImRfc1483'
104  | webserver  | webserver:Invalid argument: Failed to open port a4
     (may already be in use, or invalid port name)
-------------------------------------------------------------------------
```

See also `SYSTEM LIST USERS`
`SYSTEM LIST LOGINS`

1.1.5.1.18 SYSTEM LIST OPENFILES

Syntax `SYSTEM LIST OPENFILES <name>`

Description This command allows you to display low-level debug information about specific open file handles.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of a file that has open file handles associated with it.	N/A

Example `--> system list openfiles bun`

```
qid         devuse   appuse   colour   flags    lasterrno
console     0000004b 00000000 00400000 3        0
console     00000027 00000000 00400000 5        0
console     00000003 00000000 00400000 5        0
```

See also `SYSTEM LOG ENABLE|DISABLE`

1.1.5.1.19 SYSTEM LIST USERS

Syntax `SYSTEM LIST USERS`

Description This command displays a list of users and logins added to the system using the SYSTEM ADD USER and SYSTEM ADD LOGIN commands. The same information is displayed by the SYSTEM LIST LOGINS command.

The list contains the following information:

- user ID number
- user name
- configuration permissions (enabled or disabled)
- engineer or customer web pages configuration permissions (enabled or disabled)
- dialing permissions (enabled or disabled)
- access level (default, engineer or super user)
- comment (any comments that were included when the user was added to the system)

Example `--> system list users`

```
Users:
                May       May Conf  May
  ID | Name  | Conf.   | web     | Dialin   | Level     | Comment
-----|-------|---------|---------|----------|--------- -|------------
  1  | admin | ENABLED | ENABLED | disabled | superuser | Admin user
-------------------------------------------------------------------
```

See also `SYSTEM LIST ERRORS`
`SYSTEM LIST LOGINS`

1.1.5.1.20 SYSTEM LIST LOGINS

Syntax `SYSTEM LIST LOGINS`

Description This command displays a list of logins and users added to the system using the SYSTEM ADD LOGIN and SYSTEM ADD USER commands. The same information is displayed by the SYSTEM LIST USERS command.

The list contains the following information:

- user ID number
- user name
- configuration permissions (enabled or disabled)
- engineer or customer web pages configuration permissions (enabled or disabled)
- dialin permissions (enabled or disabled)
- access level (default, engineer or super user)
- comment (any comments that were included when the user was added to the system)

Example `--> system list users`

```
Users:
                 May       May Conf  May
  ID | Name  | Conf.   | web     | Dialin   | Level     | Comment
-----|-------|---------|---------|----------|--------- -|------------
  1  | admin | ENABLED | ENABLED | disabled | superuser | Admin user
-------------------------------------------------------------------------
```

See also `SYSTEM LIST ERRORS`
`SYSTEM LIST LOGINS`

1.1.5.1.21 SYSTEM LOCATION

Syntax `SYSTEM LOCATION <NONE/sys-location>`

Description This command sets the location info for the gateway.

Example `--> system location milan`

1.1.5.1.22 SYSTEM LOG

Syntax `SYSTEM LOG {NOTHING|WARNINGS|INFO|TRACE|ENTRYEXIT|ALL}`

Description This command sets the level of output that is displayed by the CLI for various modules. Setting a level also implicitly displays the level(s) below it.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NOTHING	No extra output is displayed.	N/A
WARNINGS	Non-fatal errors are displayed.	N/A
INFO	Certain program messages are displayed. Also displays the values for the ***warnings*** option.	N/A
TRACE	Detailed trace output is displayed. Also displays the values for ***info*** and ***warnings*** options.	N/A
ENTRYEXIT	A message is displayed every time a function call is entered or left. Also displays the values for ***trace, info*** and ***warnings*** options.	N/A
ALL	All output is displayed. Also displays the values for ***entryexit, trace***, ***info*** and ***warnings*** options.	N/A

Example `--> system log all`

1.1.5.1.23 SYSTEM LOG ENABLE|DISABLE

Syntax

```
SYSTEM LOG {ENABLE|DISABLE} RIP {ERRORS|RX|TX}
SYSTEM LOG {ENABLE|DISABLE} IP {ICMP|RAWIP|UDP|TCP|ARP|SOCKET}
SYSTEM LOG {ENABLE|DISABLE} VOIP {DEP|SEP|CA|MGCP-TRACE|MGCP-
EVENT|MGCP-MSG|SIP-TRACE|SIP-EVENT|SIP-MSG|SIP-EPS|GWADRV|MEP}
```

Description This command enables/disables the tracing support output that is displayed by the CLI for a specific module and module category. The command is used for debugging purposes. The values available for module and category are displayed by the SYSTEM LOG LIST command. The current list of supported modules is ***RIP*** and ***IP***.

Each individual module has its own specific module category (see Examples). The output produced when a particular option is enabled depends on that option, and on the trace statements in the module that are executed. The general purpose of this tracing is to:

- Show how data packets pass through the system
- Demonstrate how packets are processed and what they contain
- Display any error conditions that occur

For example IP RAWIP tracing shows that an IP packet has been received, sent or discarded due to an error. Brief details of the packet are displayed to identify it.

The RIP and IP modules provide separate categories that are enabled and disabled independently. For example, if you enable IP RAWIP, it does not affect IP UDP, and so on.

To display a list of modules and categories and their enable/disable status, see SYSTEM LOG LIST.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ENABLE	Enables tracing support output for a specified specific module and module category.	Disable
DISABLE	Disables tracing support output for a specified specific module and module category.	Disable

Example
```
--> system log enable rip rx
```
enabled logging for the receiving of RIP packets

See also
```
SYSTEM LOG LIST
SYSTEM LOG
```

1.1.5.1.24 SYSTEM LOG LIST

Syntax
```
SYSTEM LOG LIST [<module>]
```

Description The system log list command displays the tracing options for the modules available in the current image that you are using. The SYSTEM LOG LIST MODULE command displays the tracing options for an individual module specified in the command. Both commands display the current status of the tracing options set using the command SYSTEM LOG ENABLE|DISABLE.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
MODULE	The name of a module that exists in your current image build. This can be either RIP or IP.	N/A

Example
```
--> system log list
```

```
 --> sys log list
ip        arp             (disabled)
```

```
ip        config          (disabled)
ip        icmp            (disabled)
ip        l2cyan          (disabled)
ip        rawip           (disabled)
ip        socket          (disabled)
ip        tcp             (disabled)
ip        udperr          (disabled)
ip        udp             (disabled)
isdn      aft             (disabled)
isdn      aftbg           (disabled)
isdn      aux00           (disabled)
isdn      iapi            (disabled)
isdn      indtol4         (disabled)
isdn      isdnmod         (disabled)
isdn      msgh            (disabled)
isdn      msgnisdn        (disabled)
isdn      ss              (disabled)
isdn      statin          (disabled)
rip       errors          (disabled)
rip       rx              (disabled)
rip       tx              (disabled)
snmp      packet          (disabled)
sshd      fatal           (ENABLED)
sshd      error           (ENABLED)
sshd      info            (disabled)
sshd      verbose         (disabled)
sshd      debug           (disabled)
sshd      debug1          (disabled)
sshd      debug2          (disabled)
sshd      debug3          (disabled)
upload    info            (disabled)
upload    preserve        (disabled)
upload    get             (disabled)
voip      aep             (disabled)
voip      ca              (disabled)
voip      dep             (disabled)
voip      gwadrv          (disabled)
voip      mep             (disabled)
voip      mgcp-event      (disabled)
voip      mgcp-msg        (disabled)
voip      mgcp-trace      (disabled)
voip      mod             (disabled)
voip      sep             (disabled)
```

```
voip      sip-event        (disabled)
voip      sip-msg          (disabled)
voip      sip-trace        (disabled)
webserver access           (disabled)
webserver file             (disabled)
```

Example `--> system log list voip`

```
voip      aep              (disabled)
voip      ca               (disabled)
voip      dep              (disabled)
voip      gwadrv           (disabled)
voip      mep              (disabled)
voip      mgcp-event       (disabled)
voip      mgcp-msg         (disabled)
voip      mgcp-trace       (disabled)
voip      mod              (disabled)
voip      sep              (disabled)
voip      sip-event        (disabled)
voip      sip-msg          (disabled)
voip      sip-trace        (disabled)
```

See also `SYSTEM LOG`
`SYSTEM LOG ENABLE|DISABLE`

1.1.5.1.25 SYSTEM NAME

Syntax `SYSTEM NAME [<sys-name>]`

Description This command sets the system name.

To show the current system name use the system info command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
SYS-NAME	The name of the system.	none

Example `--> system name AT-iMG616BD-Routed`

1.1.5.1.26 SYSTEM CONTACT

Syntax `SYSTEM CONTACT [<sys-contact>]`

Description This command sets the system contact reported by system info command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
SYS-CONTACT	Usually a reference to some contacts.	none

Example `--> system contact admin@his_desk`

1.1.5.1.27 SYSTEM LOCATION

Syntax `SYSTEM LOCATION [<sys-location>]`

Description This command sets the system location reported by system info command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
SYS-LOCATION	Usually a reference to the location where the system is installed.	none

Example `--> system location “Inter AT labs”`

1.1.5.1.28 SYSTEM RESTART

Syntax `SYSTEM RESTART`

Description This command forces a warm restart on the gateway

Example `--> system restart`

1.1.5.1.29 SYSTEM SET LOGIN ACCESS

Syntax `SYSTEM SET LOGIN <name> ACCESS {DEFAULT|ENGINEER|SUPERUSER}`

Description This command sets the access permissions of a user who has been added to the system using the SYSTEM ADD LOGIN command. Only a ***Super*** user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
DEFAULT/ ENGINEER/ SUPERUSER	Access permissions for a user.	Default

Example `--> system set login ckearns access engineer`

See also `SYSTEM SET LOGIN MAYCONFIGURE`
`SYSTEM SET LOGIN MAYDIALIN`

For more information on the types of user access permissions, see Section 1.1.2.1.

1.1.5.1.30 SYSTEM SET LOGIN MAYCONFIGURE

Syntax `SYSTEM SET LOGIN <name> MAYCONFIGURE {ENABLED|DISABLED}`

Description This command sets configuration permissions for a user who has been added to the system using the ADD SYSTEM LOGIN or the ADD SYSTEM USER command. Only a Super user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
ENABLED/ DISABLED	Determines whether a user can configure the system.	enabled

Example `--> system set login ckearns mayconfigure disabled`

See also `SYSTEM SET LOGIN ACCESS`
`SYSTEM SET LOGIN MAYDIALIN`

1.1.5.1.31 SYSTEM SET LOGIN MAYCONFIGUREWEB

Syntax `SYSTEM SET LOGIN <name> MAYCONFIGUREWEB {ENABLED|DISABLED}`

Description This command sets configuration permissions for a user who has been added to the system using the SYSTEM ADD LOGIN or the SYSTEM ADD USER command. Only a Super user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
ENABLED/ DISABLED	Determines whether or not a user can configure the system via the Engineer or Customer web pages.	enabled

Example `--> system set login ckearns mayconfigure disabled`

See also `SYSTEM SET LOGIN ACCESS`
`SYSTEM SET LOGIN MAYDIALIN`

1.1.5.1.32 SYSTEM SET LOGIN MAYDIALIN

Syntax `SYSTEM SET LOGIN <name> MAYDIALIN {ENABLED|DISABLED}`

Description This command sets dial in permissions for a user who has been added to the system using the SYSTEM ADD LOGIN command. Only a Super user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
ENABLED/ DISABLED	Determines whether a user can dial in to the system.	disabled

Example `--> system set login ckearns maydialin enabled`

See also `SYSTEM SET LOGIN ACCESS`
`SYSTEM SET LOGIN MAYCONFIGURE`

1.1.5.1.33 SYSTEM SET USER ACCESS

Syntax `SYSTEM SET USER <name> ACCESS {DEFAULT|ENGINEER|SUPERUSER}`

Description This command sets the access permissions of a user who has been added to the system using the SYSTEM ADD USER command. Only a Super user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
DEFAULT/ ENGINEER/ SUPERUSER	Lets you to set the access permissions for a user.	default

Example `--> system set user ckearns access default`

See also `SYSTEM SET USER MAYCONFIGURE`
`SYSTEM SET USER MAYDIALIN`

1.1.5.1.34 SYSTEM SET USER MAYCONFIGURE

Syntax `SYSTEM SET USER <name> MAYCONFIGURE {ENABLED|DISABLED}`

Description This command sets configuration permissions for a user who has been added to the system using the ADD SYSTEM USER command. Only a Super user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
ENABLED/ DISABLED	Determines whether a user can configure the system.	disabled

Example `--> system set user ckearns mayconfigure enabled`

See also `SYSTEM SET USER ACCESS`
`SYSTEM SET USER MAYDIALIN`

1.1.5.1.35 SYSTEM SET USER MAYDIALIN

Syntax `SYSTEM SET USER <name> MAYDIALIN {ENABLED|DISABLED}`

Description This command sets dial in permissions for a user who has been added to the system using the SYSTEM ADD USER command. Only a Super user can use this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
ENABLED/ DISABLED	Determines whether a user can dialin to the system (functionality not available on current software version).	enabled

Example `--> system set user ckearns maydialin enabled`

See also `SYSTEM SET USER ACCESS`
`SYSTEM SET USER MAYCONFIGURE`

1.1.5.1.36 SYSTEM SET USER PASSWORD

Syntax `SYSTEM SET USER <name> PASSWORD <password>`

Description This command sets the user password that was previously created using the user password command. Only a Super user can use this command..

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
NAME	The name of an existing user.	N/A
PASSWORD	The password for the user	N/A

1.2 Webserver

1.2.1 Introduction

The gateway also offers an alternative management interface to the one depicted in the sections above, and the process in charge of managing this access (parsing CLI commands and remote management using Telnet, SSH and SNMP) is the webserver.

The webserver module can be use to mange and restrict access to the gateway modifying the configuration of the main services, including changing the default access port or restricting the access to specific IP address or subnet.

1.2.2 Web pages

Access to WEB pages can be controlled by means of user access level and *mayconfigureweb* flag as described in Section 1.1.2.2.

WEB pages are organized in 6 main sections. A menu on the left frame can be used to navigate through them:

- Home
- Configuration
- Security
- Services
- Port Statistics
- Admin

1.2.2.1 Home page

The Home page section summarizes basic and advanced informations about the operative status of the system.

Basic information are::

- Model type
- Main Application code version
- WAN Upstream/Downstream speed (only for ADSL devices)
- Wireless status and wireless network name

Advanced informations are:

- Recovery Application code version
- System Name, Location and Contact
- Routing and ARP table
- Wireless stations

1.2.2.2 Configuration page

The Configuration page is used to access Wireless and DHCP Server configuration parameters.

On the Wireless configuration pages it's possible to specify both Basic and Advanced parameters.

- Wireless Mode
- Network Name and preferred channels
- Authentication and Encryption protocols
- MAC adddress filtering (white and black list)

On the DHCP Server configuration page it's possible configure the dhcp server address ranges, fixed hosts and additional dhcp options.

1.2.2.3 Security page

The Security page includes settings related to Firewall rules, NAT reserved mapping rules and Domain Filtering.

It's possible therefore enable or disable the firewall and define for the three available policies the traffic blocking rules separately.

It's also possible configure NAT reserved mapping schemes to allow specific and-user programs to accept incoming connections even if behind the NAT engine.

It's also possible configure a virtual server that can abe accessed from public network keeping protected the internal end-user network from external attacks.

1.2.2.4 Services page

The Services page allows to configure the routing table.

It's possible enter manually static routes or enable the RIP support over the existing IP interfaces.

1.2.2.5 Admin page

The Admin page is used to perform the following operations:

- Firmware upgrade (Main Application code or Recovery Application code)

- Configuration save
- Users password settings
- System date and time setting

1.2.3 Webserver command reference

This section describes the commands available on the gateway to configure and manage the ***webserver*** module.

1.2.3.1 Webserver CLI commands

The table below lists all webserver commands provided by the CLI:

TABLE 1-2 Webserver Commands Provided by the CLI

Option	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
WEBSERVER ENABLE/DISABLE	X	X	X	X	X	X	X	X	X
WEBSERVER ADD MANAGEMENTSUBNET	X	X	X	X	X	X	X	X	X
WEBSERVER LIST MANAGEMENTSUBNETS	X	X	X	X	X	X	X	X	X
WEBSERVER CLEAR MANAGEMENTSUBNET	X	X	X	X	X	X	X	X	X
WEBSERVER DELETE MANAGEMENTSUBNET	X	X	X	X	X	X	X	X	X
WEBSERVER CLEAR STATS	X	X	X	X	X	X	X	X	X
WEBSERVER SET MANAGEMENTIP	X	X	X	X	X	X	X	X	X
WEBSERVER SET INTERFACE	X	X	X	X	X	X	X	X	X
WEBSERVER SET TELNET	X	X	X	X	X	X	X	X	X
WEBSERVER SET PORT	X	X	X	X	X	X	X	X	X
WEBSERVER SET TELNETPORT	X	X	X	X	X	X	X	X	X
WEBSERVER SET SECCLASSES	X	X	X	X	X	X	X	X	X
WEBSERVER SET TELNETSECCLASSES	X	X	X	X	X	X	X	X	X
WEBSERVER SHOW INFO	X	X	X	X	X	X	X	X	X
WEBSERVER SHOW STATS	X	X	X	X	X	X	X	X	X
WEBSERVER SHOW MANAGEMENTSUBNETS	X	X	X	X	X	X	X	X	X
WEBSERVER SHOW MEMORY	X	X	X	X	X	X	X	X	X

1.2.3.1.1 WEBSERVER ENABLE/DISABLE

Syntax `WEBSERVER {ENABLE|DISABLE}`

Description This command enables or disables the Web Server process. By default, the Web Server process is enabled. The webserver does not control only the web interface, disabling it causes serious problem to the gateway.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ENABLE	Enables the Web Server process.	enable
DISABLE	Disables the Web Server process.	

Example `--> webserver disable`

`WebServer is disabled`

See also `WEBSERVER SHOW INFO`

1.2.3.1.2 WEBSERVER ADD MANAGEMENTSUBNET

Syntax `WEBSERVER ADD MANAGEMENTSUBNET <NAME> <IPADDRESS> <NETMASK> <STARTADDR> <ENDADDR>`

Description This command restricts the telnet access to the gateway only on the specified IP addresses. It is possible to define a subnet or a list of subnets that are allowed to telnet to the gateway, denying attempts from all other subnets.

Example `--> webserver add managementsubnet fortelnet 192.168.1.0 255.255.255.0 192.168.1.10 192.168.1.100`

See also `WEBSERVER LIST MANAGEMENTSUBNET`

1.2.3.1.3 WEBSERVER LIST MANAGEMENTSUBNETS

Syntax `WEBSERVER LIST MANAGEMENTSUBNETS`

Description This command lists all the managementsubnets configured.

Example `--> webserver list managementsubnets`

```
Webserver trusted subnets:
 ID  |    IP Address   |    Netmask      |    StartAddr    |   EndAddr  |
-----|-----------------|-----------------|-----------------|------------|
  1  | 192.168.1.0     | 255.255.255.0   | 192.168.1.10    |192.168.1.110|
--------------------------------------------------------------------------
```

See also `WEBSERVER ADD MANAGEMENTSUBNETS`

1.2.3.1.4 WEBSERVER CLEAR MANAGEMENTSUBNET

Syntax `WEBSERVER CLEAR MANAGEMENTSUBNET`

Description This command delete all the active management subnets

Example `--> webserver clear managementsubnet`

See also `WEBSERVER LIST MANAGEMENTSUBNET`

1.2.3.1.5 WEBSERVER DELETE MANAGEMENTSUBNET

Syntax `WEBSERVER DELETE MANAGEMENTSUBNET <NAME>`

Description This command delete a specific management subnet

Example `--> webserver delete managementsubnet fortelent`

See also `WEBSERVER LIST MANAGEMENTSUBNET`

1.2.3.1.6 WEBSERVER CLEAR STATS

Syntax `WEBSERVER CLEAR STATS`

Description This command delete all the statistics related to any management subnet

Example `--> webserver clear stats`

See also `WEBSERVER LIST MANAGEMENTSUBNET`

1.2.3.1.7 WEBSERVER SET MANAGEMENTIP

Syntax `WEBSERVER SET MANAGEMENTIP <IPADDRESS>`

Description This command allows connection requests to be restricted to only one IP address, (e.g. from an IP address that is used by a management entity) or from any IP address (by setting the IP address to 0.0.0.0).

This command has been superseded by webserver add managementsubnets command that extends configuration flexibility.

Example `--> webserver set managementip 192.168.1.10`

See also `WEBSERVER ADD MANAGEMENTSUBNETS`

1.2.3.1.8 WEBSERVER SET INTERFACE

Syntax `WEBSERVER SET INTERFACE <INTERFACE>`

Description This command specifies the name of an IP interface that an ISOS IGD (Internet Gateway Device) will use for UPnP (Universal Plug and Play) communication with other devices on the local area network. By default, your system creates an IP interface with an Ethernet transport attached to it. This interface is called *iplan,* and it is the default interface that UPnP uses for its communication. Once you have set the UPnP interface, the IGD moni-

tors the interface. The IGD can handle changes to the interface definition (for example, if the IP address changes through a DHCP update, the IGD will use the newly assigned address)
This command has been superseded by webserver add managementsubnets command that extends configuration flexibility.

Example `--> webserver set interface ip0`

See also `WEBSERVER ADD MANAGEMENTSUBNETS`

1.2.3.1.9 WEBSERVER SET TELNET

Syntax `WEBSERVER SET TELNET { ENABLED | DISABLED }`

Description This command enable or disable the telnet service on the gateway. Once disabled, only remote access via SSH is available.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ENABLED	Enable telnet access to the CPE.	ENABLED
DISABLED	Disable totally the telnet access to the CPE.	N/A

Example `--> webserver set telnet disabled`

See also `WEBSERVER SHOW INFO`
`WEBSERVER SET TELNETSECCLASSES`

1.2.3.1.10 WEBSERVER SET PORT

Syntax `WEBSERVER SET PORT <PORT>`

Description This command sets the HTTP port number that the Web Server process will use to transfer data.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
PORT	A valid port number that must be between 0 and 65535.	80

Example `--> webserver set port 1080`

1.2.3.1.11 WEBSERVER SET TELNETPORT

Syntax `WEBSERVER SET TELNETPORT <PORT>`

Description This command sets the telnet port number that the Web Server process will use to answer telent connection requests.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
PORT	A valid port number that must be between 0 and 65535.	23

Example `--> webserver set port 24`

1.2.3.1.12 WEBSERVER SET SECCLASSES

Syntax `WEBSERVER SET SECCLASSES <SECCLASSES>`

Description This command allows you to set the security class(es) associated with the HTTP AppService. Entering this command will overwrite any existing security class(es) configured for the HTTP AppService. This has the same effect as entering the command ip set appservice http secclasses <secclasses>.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
SECCLASSES	Supported secclasses values are as follows: all- allows access to the HTTP AppService via all existing security interfaces none- prevents access to the HTTP AppService via any existing security interface internal- allows access to the HTTP AppService via the existing internal security interface external- allows access to the HTTP AppService via the existing external security interface dmz - allows access to the HTTP AppService via the existing dmz security interface To allow access to the HTTP AppService via two security interface types, type the secclass values separated by a comma (for example, internal, external) or separated by a space and enclosed in double-quotation marks (for example, "internal external"). To specify all three internal, external and dmz secclasses, use the all value.	all

Example `--> webserver set secclasses external`

See also `WEBSERVER SHOW INFO`

1.2.3.1.13 WEBSERVER SET TELNETSECCLASSES

Syntax `WEBSERVER SET TELNETSECCLASSES <SECCLASSES>`

Description This command allows you to set the security class(es) associated with the Telnet AppService. Entering this command will overwrite any existing security class(es) configured for the Telnet AppService. This has the same effect as entering the command ip set appservice telnet secclasses <secclasses>.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
SECCLASSES	all- allows access to the Telnet AppService via all existing security interfaces none- prevents access to the Telnet AppService via any existing security interface internal- allows access to the Telnet AppService via the existing internal security interface external- allows access to the Telnet AppService via the existing external security interface dmz - allows access to the Telnet AppService via the existing dmz security interface To allow access to the Telnet AppService via two security interface types, type the secclass values separated by a comma (for example, internal, external) or separated by a space and enclosed in double-quotation marks (for example, "internal external"). To specify all three internal, external and dmz secclasses, use the all value.	all

Example `--> webserver set telnetsecclasses external`

See also `WEBSERVER SHOW INFO`

1.2.3.1.14 WEBSERVER SHOW INFO

Syntax `WEBSERVER SHOW INFO`

Description This command displays the following information about the Web Server process:

- EmWeb (Embedded Web Server) release details
- Web Server enabled status (true or false)
- Archive file set
- Interface set
- HTTP port set
- UPnP port set
- Telnet port set
- Auxiliary HTTP port setting

- Permitted HTTP Security Classes
- Permitted UPnP Security Classes
- Permitted Telnet security Classes
- Management IP address

1.2.3.1.15 WEBSERVER SHOW STATS

Syntax `WEBSERVER SHOW STATS`

Description This command tells you how many bytes have been transmitted and received by the Web Server.

Bytes transmitted: bytes sent by the webserver.

Bytes received: bytes received by the webserver.

Example
```
--> webserver show stats
Web Server statistics:
Bytes transmitted: 2122
Bytes received: 0
```

See also `WEBSERVER SHOW INFO`

1.2.3.1.16 WEBSERVER SHOW MANAGEMENTSUBNETS

Syntax `WEBSERVER SHOW MANAGEMENTSUBNETS <NAME>`

Description This command tells you the information on a specific management subnet

Bytes received: bytes received by the webserver.

Example
```
--> webserver show smanagementsubnet fortelnet
```

See also `WEBSERVER SHOW INFO`

1.2.3.1.17 WEBSERVER SHOW MEMORY

Syntax `WEBSERVER SHOW MEMORY`

Description This command displays the memory allocation from variable and fixed buffer pools for the webserver.

total pool size: The total size of variable or fixed memory pool.

free: Free memory in the variable or fixed memory pool.

Allocated: Memory allocated to variable or fixed memory pool.

mean alloc chunk: Mean of the allocated chunk to variable or fixed memory pool.

max free chunk: Maximum free chunk available in variable or fixed memory pool.

Example

```
--> webserver show memory
Variable allocation pool:
total pool size139968
free57840
allocated82128
mean alloc chunk82
max free chunk55088
Buffer pool:
total pool size25568
free 24480
allocated 1088
mean alloc chunk217
max free chunk 24464
```

See also WEBSERVER SHOW INFO

1.3 Emergency

This chapter describes the AT-iMG600 emergency module used to configure the system connectivity when the intelligent Multiservice Gateway runs in recovery mode. Emergency module is available only on AT-RG613 and AT-iMG616.

1.3.1 Introduction

If the intelligent Multiservice Gateway flash file system is corrupted, the system will start running a minimal operating system simply named *recovery*.

From the recovery mode, it's possible load remotely the complete system application image and any additional file to recover the unit into a full operative default system configuration.

1.3.2 Emergency configuration

The connectivity between the intelligent Multiservice Gateway and the remote network operation centre (NOC) can operate both via any intelligent Multiservice Gateway Ethernet port and via the ADSL port.

When Ethernet connection is used, the intelligent Multiservice Gateway Ethernet ports are set to belong to the default vlan as untagged port. When running in recovery mode, there is no support to tagged VLANs on the Ethernet interfaces.

When ADSL connection is used, the intelligent Multiservice Gateway tries to connect to the remote NOC via an RFC1483 LLC/SNAP Bridged connection type with VPI/VCI = 0/35 without any tagging scheme.

It's possible configure the IP address used to connect remotely to the intelligent Multiservice Gateway when recovery application is running.

To set a static IP address use the `EMERGENCY SET IPINTERFACE IPADDRESS NETMASK` command and to set the default gateway use the `EMERGENCY SET IPINTERFACE GATEWAY` command.

To set a dynamic IP address uses the `EMERGENCY SET DHCP ENABLE` command. The intelligent Multiservice Gateway will get the IP address from any external DHCP server as well as the interface subnet and the default gateway.

Note: Note that if no DHCP server is discovered, the intelligent Multiservice Gateway will use the autoip feature to autonomously assign a random IP address in the range 169.254.0.0/16. If a DHCP server becoms available later, the IP interface will then change the IP address to the value offered by the DHCP server.

1.3.3 Save and activate emergency configuration.

The emergency configuration data set in the previous section is not active until saved permanently in the intelligent Multiservice Gateway e2prom. Emergency configuration data are saved in an e2prom instead in the flashfs filesystem to increase the system robustness to any flashfs failure.

To save emergency configuration data in e2prom use the `EMERGENCY UPDATE` command.

Emergency configuration data is also saved in the system configuration any time the command `SYSTEM CONFIG CREATE` or `SYSTEM CONFIG SET` are entered. In this way the information is stored in two different areas: the e2prom and the file bootstrap configuration file in the main partition.

In the case where the system starts in recovery mode because the main application partition is considered corrupted, only the information stored in the e2prom will be used to configure the recovery application.

During normal system bootstrap initialization the recovery configuration data stored in the bootstrap configuration file is considered the current emergency settings. This information is also stored automatically in the e2prom to be immediately active.

To display the active recovery configuration data use the `EMERGENCY SHOW` command.

To avoid any misalignment between the configuration stored in the E2PROM and the configuration reported in the bootstrap configuration file, the following situations are managed during the system bootstrap:

Optione2prom recovery config. data → bootstrap file recovery config. data ↓	NOT AVAILABLE	AVAILABLE
NOT AVAILABLE	If the system restarts in recovery mode, the recovery application will then use the default configuration data coded within the recovery application.	The e2prom recovery configuration data is removed and if the system restarts in recovery mode, the recovery application will then use the default configuration data coded within the recovery application.
AVAILABLE	The im.conf recovery configuration data is copied into the e2prom. In this way, if the system restarts in recovery mode, the recovery application will then use the same configuration data reported by the im.conf recovery configuration data.	The im.conf recovery configuration data is copied into the e2prom overriding any previous configuration present in the e2prom. In this way, if the system restarts in recovery mode, the recovery application will then use the same configuration data reported by the im.conf recovery configuration data.

1.3.4 Emergency command reference

This chapter describes the Emergency CLI module commands.

1.3.4.1 Emergency CLI commands

The table below lists the *Emergency* commands provided by the CLI:

TABLE 1-3 Emergency CLI Commands

Option	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
EMERGENCY ADD									
EMERGENCY CREATE									
EMERGENCY DELETE									
EMERGENCY SET DHCP									
EMERGENCY SET IPINTERFACE GATEWAY									
EMERGENCY SET IPINTERFACE IPADDRESS									
EMERGENCY SHOW									
EMERGENCY UPDATE									

1.3.4.1.1 EMERGENCY ADD

Syntax `EMERGENCY ADD VLAN <vlan_vid> PORT <port_name> FRAME TAGGED`

Description This command adds and tags an Ethernet port to the specified vlan. The vlan must be already defined in the Emergency module using the EMERGENCY CREATE VLAN command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
vlan_id	The vlan identifier (VID) previously created with the EMERGENCY CREATE VLAN command. To display the existing vlan, use the EMERGENCY SHOW command.	N/A
port_name	The name of an Ethernet port. Available values are: lan1, lan2, lan3 and lan4.	N/A

Example Example .. `emergency add vlan 2 port lan4 frame tagged`

See also
`EMERGENCY CREATE`
`EMERGENCY SHOW`
`EMERGENCY UPDATE`

1.3.4.1.2 EMERGENCY CREATE

Syntax `EMERGENCY CREATE LAN <vlan_vid>`

Description This command defines a new vlan on which will be attached the ip interface used to reach the system when running in recovery mode. Creating a new vlan requires also the definition of which Ethernet port must be tagged for this vlan. To add an Ethernet port to the new vlan, use the EMERGENCY ADD command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
vlan_id	The vlan identifier (VID) of the new vlan to be created. Only tagged frame with this VID will be processed by the upper layer (IP layer) when recovery application runs.	N/A

Example `emergency create vlan 2`

See also `EMERGENCY ADD`
`EMERGENCY SHOW`
`EMERGENCY UPDATE`

1.3.4.1.3 EMERGENCY DELETE

Syntax `EMERGENCY DELETE VLAN <vlan_vid> [ PORT <port_name> ]`

Description This command is used to delete an Ethernet port from a previously created vlan and delete any vlan different from the default. It's not possible delete a vlan if an Ethernet port is assigned to this vlan as tagged port. In this case it's necessary delete first the Ethernet port with the command EMERGENCY DELETE VLAN PORT and then remove the vlan with the command EMERGENCY DELETE VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
vlan_id	he vlan identifier (VID) of the vlan used when recovery application runs.	N/A

Option	Description	Default Value
port_name	The name of an Ethernet port. Available values are: lan1, lan2, lan3 and lan4. To display the current tagged port configured in the emergency module, use the EMERGENCY SHOW command.	N/A

Example `emergency delete vlan 2 port lan4`
`emergency delete vlan 2`

See also `EMERGENCY ADD`
`EMERGENCY SHOW`
`EMERGENCY UPDATE`

1.3.4.1.4 EMERGENCY SET DHCP

Syntax `Syntax EMERGENCY SET DHCP { ENABLE | DISABLE }`

Description This command is used to set the ip interface address used when the system runs in recovery mode to be dynamic or static. If the interface is set statically and no ipaddress is set with the command EMERGENCY SET IPINTERFACE command, the recovery default ip address 192.168.1.1/24 will be used.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ENABLE	Set the recovery ip interface address dynamically. If no DHCP server is available or cannot be reached, the ip address will get an autoip address in the subnet 169.254.0.0.	N/A
DISABLE	Turn off the dhcpclient on the recovery ip interface.	N/A

Example `emergency set dhcp enable`

See also `EMERGENCY SET IPINTERFACE IPADDRESS`
`EMERGENCY SHOW`
`EMERGENCY UPDATE`

1.3.4.1.5 EMERGENCY SET IPINTERFACE GATEWAY

Syntax `Syntax EMERGENCY SET IPINTERFACE GATEWAY <ip_address>`

Description This command sets the default gateway ip address to be used when the system runs in recovery mode.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ip_address	The default gateway ipaddress in IPv4 format (e.g. 192.168.1.254)	N/A

Example `emergency set ipinterface gateway 192.168.1.254`

See also
```
EMERGENCY SET IPINTERFACE
EMERGENCY SHOW
EMERGENCY UPDATE
```

1.3.4.1.6 EMERGENCY SET IPINTERFACE IPADDRESS

Syntax `EMERGENCY SET IPINTERFACE IPADDRESS <ip_address> NETMASK <netmask>`

Description This command sets the ip interface address and netmask to be used when the system runs in recovery mode.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
p_address	The ip interface address in IPv4 format (e.g. 192.168.1.1)	N/A
netmask	Network for the interface	N/A

Example
```
emergency set ipinterface ipaddress 192.168.1.1 netmask
255.255.255.0
```

See also EMERGENCY SET IPINTERFACE GATEWAY
EMERGENCY SHOW
EMERGENCY UPDATE

1.3.4.1.7 EMERGENCY SHOW

Syntax EMERGENCY SHOW

Description This command displays the current emergency configuration settings. These settings are not active until the EMERGENCY UPDATE command is entered or the Residential Gateway configuration is saved and then the system is restarted.

Example emergency show

```
EMERGENCY CONFIGURATION
- GENERAL PARAMETERS
device ip address: 192.168.1.1
device netmask: 255.255.255.0
gateway ip address: 192.168.1.254
vlan tag id: 2
vlan tagged port: LAN4
```

Syntax EMERGENCY UPDATE

1.3.4.1.8 EMERGENCY UPDATE

Syntax EMERGENCY UPDATE

Description This command update the Residential Gateway e2prom with the new emergency configuration data. To display the current emergency configuration settings use the EMERGENCY SHOW command.

Example emergency update

See also EMERGENCY SHOW

1.4 Software update

Gateway software consists of the Main Application code plus additional support files and the Recovery Application code. All these files are stored permanently into the ***flash*** memory under the main partition or recovery partition depending on the file type.

To upgrade software or simply load into the gateway a specific file, it's possible use one of the following solutions depending on the type of upgrade requested:

- Web Interface, when available is designed to update the Main Application code or the Recovery Application code. Web interface is available only on the main code (not on recovery)

- SwUpdate module, available both on Main Application code and Recovery Application Code designed to update the Main Application code or the Recovery Application code and to upload any configuration file

Product Name	Loader	SwUpdate	Web Interface
AT-RG613	Loader_RG600E_x-y_z.exe	rg600E-x-y_z.zip	N/A
AT-iMG616	Loader_IMG616E_x-y_z.exe	iMG616E-x-y_z.zip	N/A
AT-iMG634A AT-iMG634WA	N/A	iMG634A-x-y_z.zip	iMG634A-main-x-y_z.bin
AT-iMG634B AT-iMG634WB	N/A	iMG634B-x-y_z.zip	iMG634B-main-x-y_z.bin
AT-iMG624A	N/A	iMG624A-x-y_z.zip	iMG624A-main-x-y_z.bin
AT-iMG624B	N/A	iMG624B-x-y_z.zip	iMG624B-main-x-y_z.bin
AT-iMG634A-R2 AT-iMG634WA-R2	N/A	iMG634A-R2-x-y_z.zip	iMG634A-R2-main-x-y_z.bin
AT-iMG634B-R2 AT-iMG634WB-R2	N/A	iMG634B-R2-x-y_z.zip	iMG634B-R2-main-x-y_z.bin
AT-iMG624A-R2	N/A	iMG624A-R2-x-y_z.zip	iMG624A-R2-main-x-y_z.bin
AT-iMG626MOD	N/A	iMG626-x-y_z.zip	iMG626-main-x-y-z.bin
AT-iMG646MOD	N/A	iMG646-x-y_z.zip	iMG646-main-x-y-z.bin
AT-iMG726MOD	N/A	iMG726-x-y_z.zip	iMG726-main-x-y-z.bin
AT-iMG746MOD	N/A	iMG746-x-y_z.zip	iMG746-main-x-y-z.bin
AT-iBG915FX	N/A	iBG915FX-x-y_z.zip	iBG915FX-main-x-y-z.bin

- **Recovery Application Software Naming Convention table**

Product Name	Loader	SwUpdate	Web Interface
AT-RG613	RecLoader_RG600_a-b_c.exe	rg6xx-rec-a-b_c.zip	N/A
AT-iMG616	RecLoader_IMG616E_a-b_c.exe	iMG616E-rec-a-b_c.zip	N/A
AT-iMG634A AT-iMG634WA	N/A	iMG634A-rec-a-b_c.zip	iMG634A-recovery-a-b_c.bin
AT-iMG634B AT-iMG634WB	N/A	iMG634B-rec-a-b_c.zip	iMG634B-recovery-a-b_c.bin
AT-iMG624A	N/A	iMG624A-rec-a-b_c.zip	iMG624A-recovery-a-b_c.bin
AT-iMG624B	N/A	iMG624B-rec-a-b_c.zip	iMG624B-recovery-a-b_c.bin
AT-iMG634A-R2 AT-iMG634WA-R2	N/A	iMG634A-R2-rec-a-b_c.zip	iMG634A-R2-recovery-a-b_c.bin
AT-iMG634B-R2 AT-iMG634WB-R2	N/A	iMG634B-R2-rec-a-b_c.zip	iMG634B-R2-recovery-a-b_c.bin
AT-iMG624A-R2	N/A	iMG624A-R2-rec-a-b_c.zip	iMG624A-R2-recovery-a-b_c.bin
AT-iMG626MOD	N/A	iMG626-rec-a-b_c.zip	iMG626-recovery-a-b_c.bin
AT-iMG646MOD	N/A	iMG646-rec-a-b_c.zip	iMG646-recovery-a-b_c.bin
AT-iMG726MOD	N/A	iMG726-rec-a-b_c.zip	iMG726-recovery-a-b_c.bin
AT-iMG746MOD	N/A	iMG746-rec-a-b_c.zip	iMG746-recovery-a-b_c.bin
AT-iBG915FX	N/A	iBG915FX-rec-a-b_c.zip	iBG915FX-recovery-a-b_c.bin

- **FLASH image Naming Convention table**

Product Name	Flash Image
AT-RG613	rg600E-image-2-2_y-3-7_x.bin
AT-iMG616	iMG616E-image-2-2_y-3-7_x.bin
AT-iMG634A AT-iMG634WA	iMG634A-image-3-7_x.bin
AT-iMG634B AT-iMG634WB	iMG634B-image-3-7_x.bin
AT-iMG624A	iMG624A-image-3-7_x.bin
AT-iMG624B	iMG624B-image-3-7_x.bin
AT-iMG634A-R2 AT-iMG634WA-R2	iMG634A-R2-image-3-7_x.bin
AT-iMG634B-R2 AT-iMG634WB-R2	iMG634B-R2-image-3-7_x.bin
AT-iMG624A-R2	iMG624A-R2-image-3-7_x.bin
AT-iMG626MOD	iMG626-image-3-7_x.bin
AT-iMG646MOD	iMG646-image-3-7_x.bin
AT-iMG726MOD	iMG726-image-3-7_x.bin
AT-iMG746MOD	iMG726-image-3-7_x.bin
AT-iBG915FX	iBG915FX-image-3-7_x.bin

1.4.1 Windows™ Loader

To upgrade the AT-RG600 Residential Gateway, a special Windows™ based application has been developed, the Loader.

The loader uses the TFTP services provided by the gateway to download on the unit the application file plus all other support files avoiding the user to download each file separately.

The loader can be used to upgrade an existing software version or can be used to download a new complete software release if the gateway is running in recovery mode.

When the Loader is used to upgrade the gateway from a previous software release, all the existing configuration files are kept.

Note: Starting with release 3-1-0, a special Loader application has been developed to also upgrade the recovery application code installed in the recovery partition. The graphical interface is the same as that used for the main application code.

When using the Loader, the IP address of the residential Gateway must be selected and the SNMPv2 community write name is requested as session password.

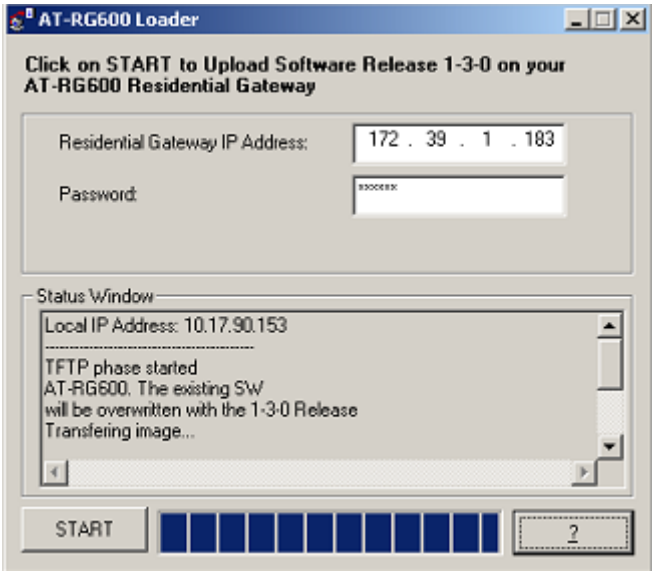


FIGURE 1-4 The Windows™ Loader

1.4.2 Upgrade via Web Interface

Some gateways provide a web interface to load the Main Application code or the Recovery Application code.

Figure 1-4 shows the Web Interface main page. To load a software, click the Firmware Update menu.

On the Firmware Update page (See Figure 1-6) push the “Browse” button, select the software file to be uploaded and click OK:

- iMG634xxx-main-x-y_z.bin to load the Main Application code.

- iMG634xxx-recovery-x-y_z.bin to load the Recovery Application code.
- After the file has been selected, the software will be uploaded and written on the device. A progress bar will be displayed on the web interface. When the process is finished the web interface will display a “Restart” button. Click it to restart the device and run the loaded software version.

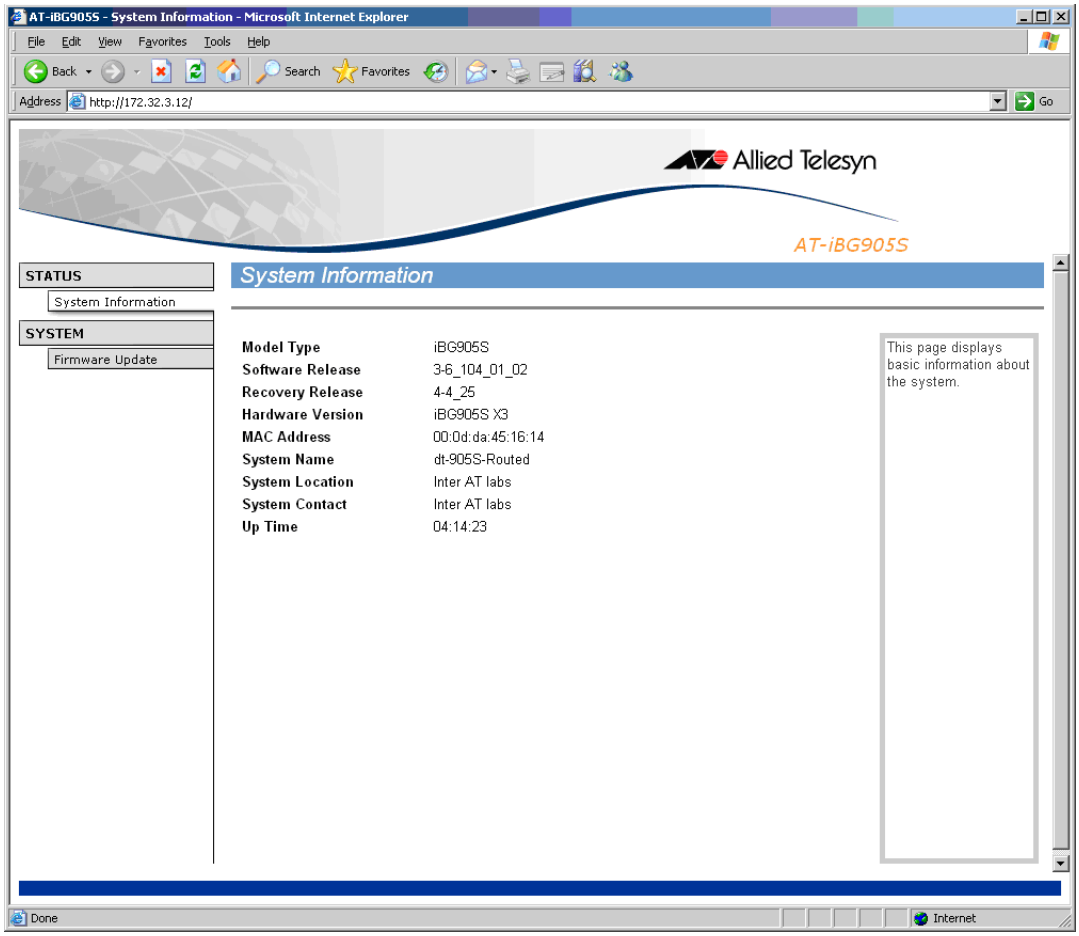


FIGURE 1-5 The Web Interface main page

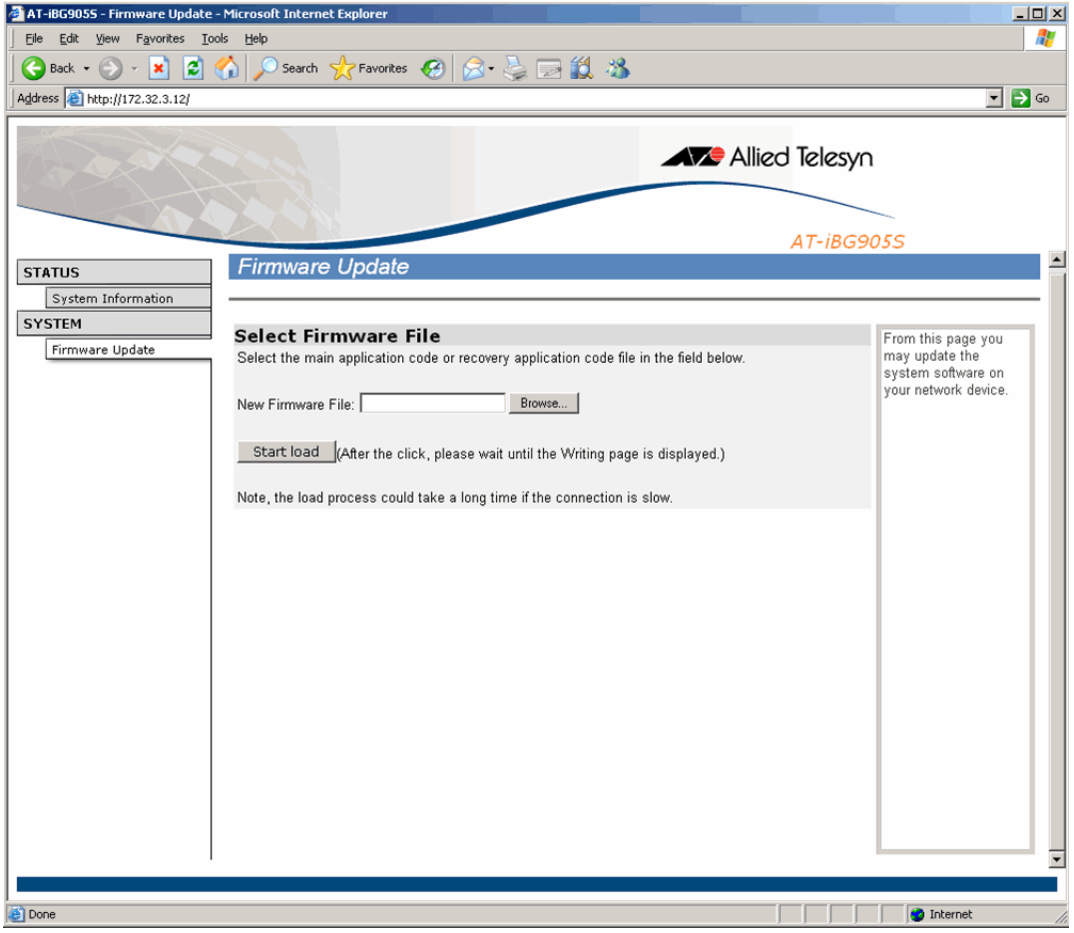


FIGURE 1-6 The Web Interface Firmware Update page

1.4.3 SwUpdate module

SwUpdate module is a basic FTP/TFTP client module running on the gateway that contacts periodically a pre-defined FTP/TFTP server and retrieves from it the required software or support files.

SwUpdate can retrieve the IP address of the FTP server dynamically, resolving the FTP server name through look-up requests to an existing DNS server, or can be configured statically accordingly to network design implementation.

When working in the TFTP mode, ***SwUpdate*** retrieves the TFTP Server address from the value of a specific dhcp option (option 66 'tftp-server-name') passed by the external DHCP server to the gateway IP interface. It then uses the path passed as *filename* string to navigate into the TFTP server.

In order to distinguish the correct DHCP Offer (in case more than one DHCP server is present in the network), the gateway will consider only DHCP Offers that include the option 60 ('dhcp-class-identifier') with one of the following possible values depending on the product code:

Product code Legacy RG	Product code Ethernet Uplink	Product code ADSL Uplink	Product code Outdoor and Business
AT-RG613	AT-iMG606TX	AT-iMG624A	AT-iMG646MOD
AT-RG623	AT-iMG606BD	AT-iMG624B	AT-iMG626MOD
AT-RG613TXJ	AT-iMG606LH	AT-iMG634A	AT-iMG746MOD
AT-RG656	AT-iMG606SH	AT-iMG634B	AT-iMG726MOD
AT-RG613LH	AT-iMG616RF	AT-iMG634WA	AT-iBG915FX
AT-RG613SH	AT-iMG616BD	AT-iMG634WB	AT-iMG646BD-ON
AT-RG623LH	AT-iMG616LH		AT-iMG646PX-ON
AT-RG623SH	AT-iMG616SH		
AT-RG613BD	AT-iMG616SRF		
	AT-iMG616RF+		
AT-RG624A	AT-iMG616SRF+	AT-iMG624A-R2	
AT-RG624B	AT-iMG616W	AT-iMG624B-R2	
AT-RG634A	AT-iMG616CRFW	AT-iMG634A-R2	
AT-RG634B	AT-iMG616TX	AT-iMG634B-R2	
AT-RG656LH		AT-iMG634WA-R2	
AT-RG656SH		AT-iMG634WB-R2	
AT-RG656TX			
AT-RG646BD			
AT-RG613RF			

SwUpdate is designed to download only the files that differ or are not present into the file-system.

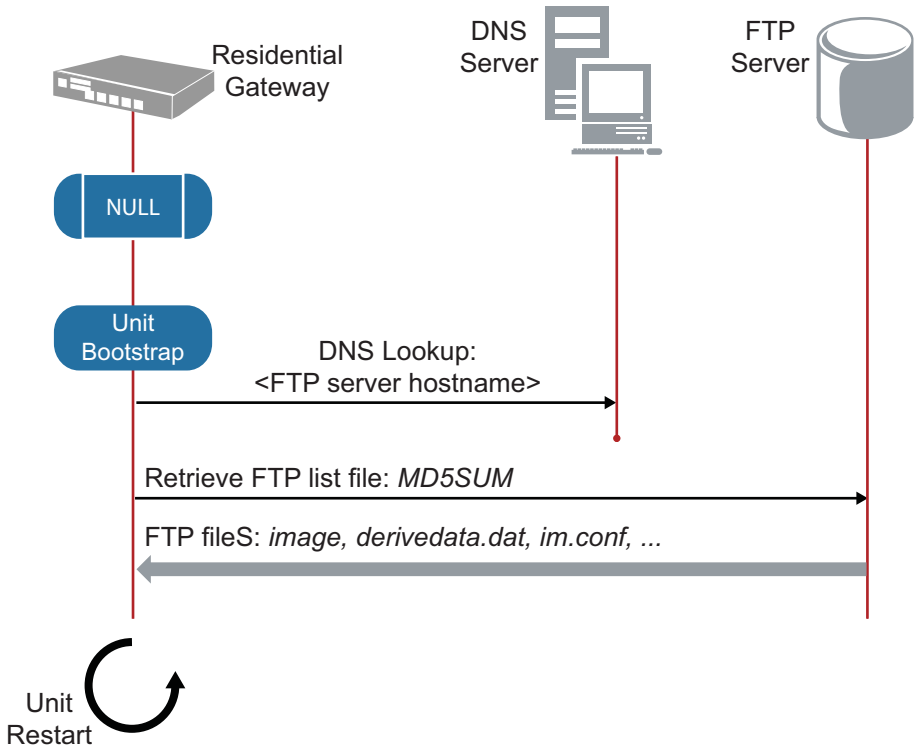


FIGURE 1-7 Normal *SwUpdate* operation mode

In order to inform the ***SwUpdate*** module about which files it must download from the FTP/TFTP server, a special file named MD5SUM must be created on the FTP/TFTP server.

When the ***SwUpdate*** module connects to the FTP/TFTP server, it retrieves immediately this file and then it downloads each file reported in this list.

The MD5SUM file is a list of filenames where each file name has associated the MD5 value.

To create the MD5SUM file it's possible use the md5sum command available under standard Linux platforms (free md5sum applications are available also under ***Windows™ Operating System***).

If a file reported in the MD5SUM list is already present into the gateway file-system with the same MD5 value, the ***SwUpdate*** skip this download, otherwise it will download it.

Example

Assuming the all the files included in the current directory must be downloaded into the gateway; the following command must be used to generate the MD5SUM file:

```
root# md5sum * >  MD5SUM
the MD5SUM file will list the following informations:
```

```
d99f017e2652516d9146dd14f787f16e  iMG616BD-recovery-4-4_25.bin
7e722ffb74af07265b3e22d51496d1c3  iMG616BD-main-3-7-01_26.bin
d90657f8851b761d8336fbd0b34156df  snmpd.cnf.orig
ec6fc5ddc6adaa1e7943ce463de283c3  snmpinit
```

The above procedure is valid both for upgrade the Main Application code, the Recovery Application code and any configuration file requested by the CPE. The swupdate module is able to detect based on the file type, on which flash partition the file will be stored.

1.4.3.1 Start Time scheduling

It is possible set the ***SwUpdate*** starting time at any minute/hour/day/week of the year.

The ***Start Time*** command uses syntax similar to the ***crontab*** files syntax

The ***Start Time*** is composed of five time and date fields (minute, hour, day-of-month, month, day-of-week respectively). The ***SwUpdate*** is started when the minute, hour and month of year fields match the current gateway time and when at least one of the two day fields (day-of-month or day-of-week) match the current gateway time.

Field	Allowed Values
MINUTE	0-59
HOUR	0-23
DAY-OF-MONTH	1-31
MONTH	1-12
DAY-OF-WEEK	0-7 (0 or 7 is Sunday)

A field may be an asterisk ('*'), which always stands for 'first-last'.

Ranges of numbers are allowed. Ranges are two numbers separated by a hyphen. The specified range is inclusive.

For example, 8-11 for the 'hours' entry specifies execution at hours 8, 9, 10 and 11.

Lists are allowed. A list is a set of numbers (or ranges) separated by commas.

Examples: '1,2,5,9', '0-4,8-12.

When the local gateway time equals the start time, ***SwUpdate*** executes the following actions:

It retrieves the list of files available into the non-volatile memory and for each file calculates the MD5 value.

It then connects to the FTP/TFTP server and retrieves a file named MD5SUM from the directory defined by the path parameter (and eventually by the MAC parameter). This file contains a list of all files available on the server, with the corresponding MD5 value that the ***SwUpdate*** module must retrieve from the FTP server.

It compares the MD5SUM file downloaded from the server with the local MD5 file calculated on the current flash file system.

For each file in the MD5SUM file that differ from the list in the local MD5 file or it not present, the ***SwUpdate*** retrieves it from the FT/TFTP server.

When all the files have been downloaded, they are saved permanently into the gateway file-system and the gateway is restarted. The next time it starts, the gateway will use the new files.

Non-existing times, such as 'missing hours' during daylight savings conversion, will never match, causing ***SwUpdate*** scheduled during the 'missing times' not to be started.

1.4.3.2 Retry Period scheduling

If ***SwUpdate*** fails a download, it reschedules the next request using the retry-period timeout.

The retry-period timeout specifies the Maximum time within the ***SwUpdate*** will reschedule the next request.

The exact time when the ***SwUpdate*** will perform the next request is randomly selected between 15secs and the retry-period timeout. This computation is performed every time ***SwUpdate*** fails and a new request must be scheduled.

When the download finishes successfully, ***SwUpdate*** is rescheduled using the start timetable. If the current time is in the time window between two consecutive start and stop time, the ***SwUpdate*** suspends any download.

The start time has precedence over the ***Retry Period*** schedule. If the start time happens while the ***Retry Period*** is running, ***SwUpdate*** starts immediately the download and only if it fails, it will reschedule the download.

1.4.3.3 Stop Time scheduling

It is possible stop ***SwUpdate*** at any minute/hour/day/week of the year.

Stop time is typically used when ***SwUpdate*** fails a download and as result a new request has been scheduled prior to the next start time.

To prevent continuous re-transmissions, stop time forces the ***SwUpdate*** to stop any scheduled retry during specific (configurable) time of day or day of week.

SwUpdate will be active only in timeslots defined by two consecutive start and stop times.

The time period between a stop time and the consecutive start time is the inactive (idle) period where ***SwUpdate*** does NOT contacts any server.

If the retry-period timer was running before the stop time, this timer is stopped when the local time match the stop time.

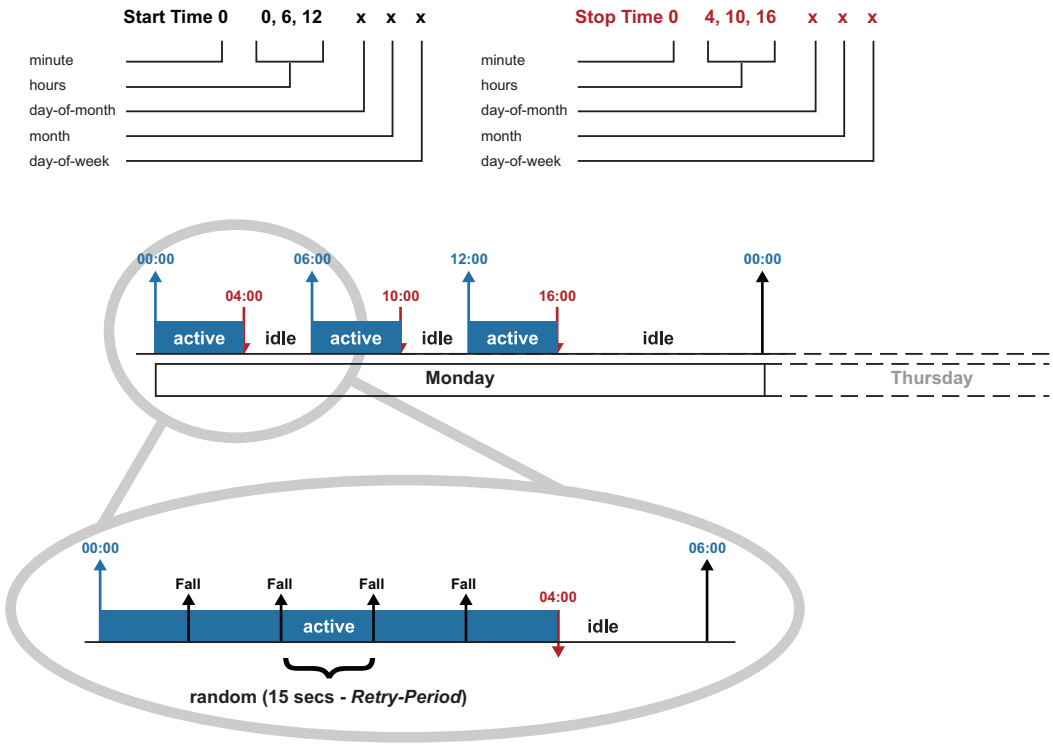


FIGURE 1-8 ***SwUpdate*** **scheduling example 1**

Figure 1-8 above shows a schedule example where the ***SwUpdate*** is started every day of the week at hours 0, 6, 12 and is stopped after 4 hours from each start time.

The following figure (Figure 1-9) shows a schedule example where the ***SwUpdate*** is started every day of the week at hours 0, 6, 12 and is stopped in specific time of the day.

It the stop time is set inside an idle period, ***SwUpdate*** stay in the inactive state waiting for the next start time.

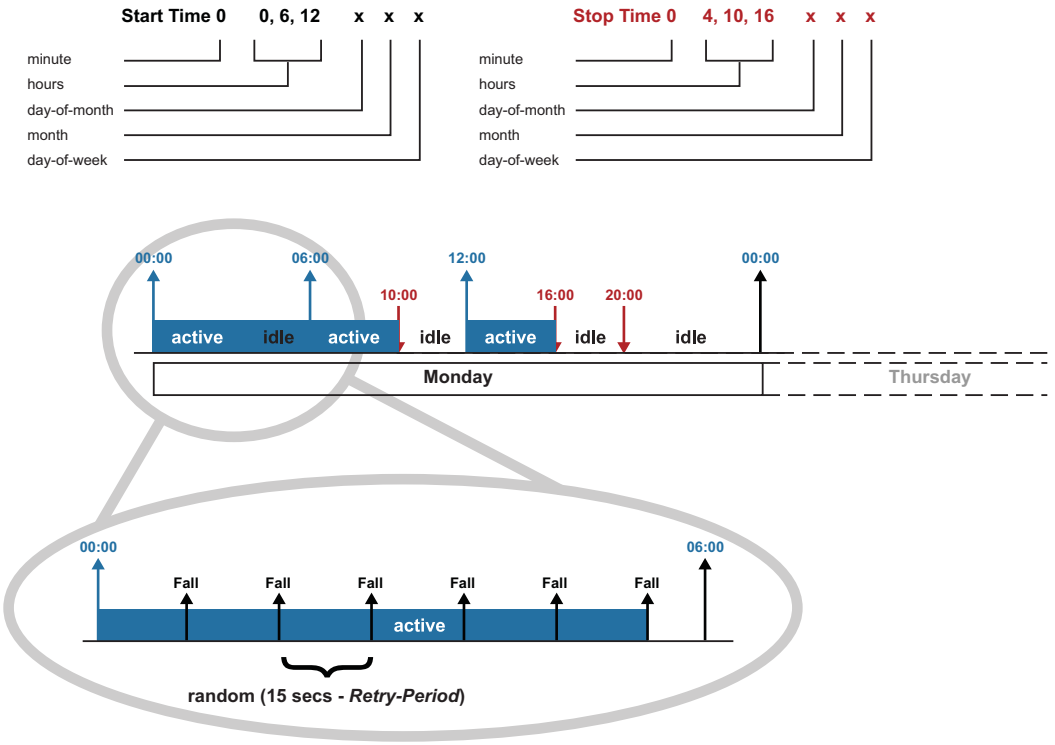


FIGURE 1-9 *SwUpdate* scheduling example 2

1.4.3.4 Manually enabling SwUpdate

It is possible turn on (disable) and turn off the ***SwUpdate*** module manually using the `swupdate start` and `swupdate stop` command.

If ***SwUpdate*** was disabled and the download finish successfully, ***SwUpdate*** returns to the disable state.

If ***SwUpdate*** was disabled and the download fails, ***SwUpdate*** stays enabled and scheduled with the same rules defined in previous sections.

If ***SwUpdate*** was enabled and the download finish successfully, ***SwUpdate*** stays enabled with the schedule time defined by the Start and Stop Time.

If ***SwUpdate*** was enabled and the download fails, ***SwUpdate*** stays enabled and scheduled with the same rules defined in section previous sections.

1.4.3.5 Plug-and-play

Default operational mode

By default SwUpdate module is set to work in TFTP mode trying to get all the TFTP server parameters from the DHCP parameters list option passed by the external DHCP server

When working in TFTP mode, the gateway requires that the IP interface connected to the swupdate network is set dynamically. Swupdate will use the feature of the dhcpclient to request the DHCP option 66 ("tftp-file-name") and the DHCP option 60 (dhcp-class-identifier).

The swupdate module will then use the tftp-file-name option and the DHCP *filename* field value passed in the DHCP ACK message to set the TFTP server address and the server path respectively.

During the interface IP address discover or renewal, the DHCP client notifies to the server the Residential gateway model type and MAC address in the dhcp-class-identifier and dhcp-client-identifier options respectively.

Notification of dhcp-class-identifier and dhcp-client-identifier options allow DHCP server to discover dynamically the type of unit and perform selective choice of TFTP server parameters (for example select a different server path to download different code versions or different unit configuration files).

Note: The swupdate module needs the dhcp-class-identifier option to be present in the DHCP ACK message with the same value sent in the DHCP Discover and Request messages. If this value is different or the option is not present, the swupdate doesn't start.

1.4.3.6 Server access

FTP server account

SwUpdate is able to access FTP server using the server access login.

The FTP server login account and login password are configurable into the ***SwUpdate*** module.

FTP/TFTP working directory

SwUpdate is able to navigate into the FTP/TFTP server directory.

The working directory can be specified defining in the ***SwUpdate*** module a parameter named path. It identifies the relative path respect the login home directory where the ***SwUpdate*** module expects to found the files.

For example if the home directory is:

```
/home/manager
```

and the gateway path address is set to:

```
at-iMG616BD-software-xxx
```

the working directory will be:

```
/home/manager/at-iMG616BD-software-xxx
```

The working directory can be specified also using the gateway MAC address in the format:

```
aa_bb_cc_dd_ee_ff.
```

In this case the working directory will be the login home directory plus the MAC address.

This feature is useful when network administrators need to create specific configuration for each residential gateway.

To enable this feature a special flag named MAC can be used.

For example if the home directory is:

```
/home/manager
```

and the gateway MAC address is:

```
10:20:30:40:50:60
```

enabling the MAC field, the working directory will be:

```
/home/manager/10_20_30_40_50_60
```

If both the path field and the MAC flag are set, the working directory will be the login home directory plus the path string plus MAC address.

For example if the home directory is:

```
/home/manager
```

and the gateway MAC address is:

```
10:20:30:40:50:60
```

and the gateway path address is set to:

```
at-iMG616BD-software-xxx
```

the working directory will be:

```
/home/manager/at-iMG616BD-software-xxx/10_20_30_40_50_60
```

1.4.4 SwUpdate command reference

This section describes the commands available on the gateway to configure and manage the ***SwUpdate*** module.

1.4.4.1 SwUpdate commands

The table below lists the ***SwUpdate*** commands provided by the CLI:

TABLE 1-4 SwUpdate Commands

Option	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SWUPDATE MAC	X	X	X	X	X	X	X	X	X
SWUPDATE SET LOGIN	X	X	X	X	X	X	X	X	X
SWUPDATE SET PASSWORD	X	X	X	X	X	X	X	X	X
SWUPDATE SET PATH	X	X	X	X	X	X	X	X	X
SWUPDATE SET RETRY PERIOD	X	X	X	X	X	X	X	X	X
SWUPDATE SET SERVER	X	X	X	X	X	X	X	X	X
SWUPDATE SHOW	X	X	X	X	X	X	X	X	X
SWUPDATE START	X	X	X	X	X	X	X	X	X
SWUPDATE START TIME	X	X	X	X	X	X	X	X	X
SWUPDATE STOP	X	X	X	X	X	X	X	X	X
SWUPDATE STOP TIME	X	X	X	X	X	X	X	X	X

1.4.4.1.1 SWUPDATE MAC

Syntax `SWUPDATE MAC {ENABLE | DISABLE}`

Description This command forces the ***SwUpdate*** module to look for the MD5SUM file on the FTP server into a directory having the same value as the unit MAC address.

The working directory is therefore the home directory followed by the unit MAC address.

If the path value is set using SWUPDATE SET PATH command, the working directory is the user home directory + the MAC address + the path.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
ENABLED	Enable the use of MAC address as qualifier for the working directory. The name of the working directory will be for example:00_20_30_40_50_60	Enabled

Option	Description	Default Value
DISABLED	Disable the use of MAC address as qualifier for the working directory.	

Example `--> swupdate mac enable`

See also `SWUPDATE SET PATH`
`SWUPDATE SHOW`

1.4.4.1.2 SWUPDATE SET LOGIN

Syntax `SWUPDATE SET LOGIN < login>`

Description This command set the login name used when ***SwUpdate*** connects to an FTP server.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
LOGIN	The login name used to access ftp server.	manager

Example `--> swupdate set login administrator`

See also `SWUPDATE SET PATH`
`SWUPDATE SET PASSWORD`
`SWUPDATE SHOW`

1.4.4.1.3 SWUPDATE SET PASSWORD

Syntax `SWUPDATE SET PASSWORD < password>`

Description This command set the password key used when ***SwUpdate*** connects to an FTP server.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
PASSWORD	The password key used to access ftp server.	friend

Example `--> swupdate set password superuser`

See also SWUPDATE SET LOGIN
SWUPDATE SHOW

1.4.4.1.4 SWUPDATE SET PATH

Syntax SWUPDATE SET PATH <path>

Description This command set the path used when ***SwUpdate*** navigate into the FTP server.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
PATH	The path used when ***SwUpdate*** navigate into the FTP server. '***none***' means no path is used.	none

Example --> swupdate set path rel-x-y-z

See also SWUPDATE MAC ENABLE
SWUPDATE SHOW

1.4.4.1.5 SWUPDATE SET RETRY PERIOD

Syntax SWUPDATE SET RETRY PERIOD <secs>

Description This command set the maximum retry period when a download fails.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
SECS	The maximum retry period (in secs) used when the download fails and ***SwUpdate*** tries to contact the FTP/TFTP server.	60

Example --> swupdate set retry-period 120

See also SWUPDATE SHOW

1.4.4.1.6 SWUPDATE SET SERVER

Syntax `SWUPDATE SET SERVER <server_address>`

Description This command set the server address to which ***SwUpdate*** tries to connect.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
SERVER_ADDRESS	The hostname or IPv4 address of the ftp server. Host can be a maximum of 256 chars long (when using hostname format).	swupdate

Example `--> swupdate set server 10.17.90.101`

See also
```
SWUPDATE SET PATH
SWUPDATE SET PASSWORD
SWUPDATE SHOW
```

1.4.4.1.7 SWUPDATE SHOW

Syntax `SWUPDATE SHOW`

Description This command displays the ***SwUpdate*** module configuration parameters.

Example `--> swupdate show`

```
FTP SWUPDATE CONFIGURATION
   - GENERAL PARAMETERS
   Retry period set to: 40
   start time passed to cron: 0-59 * * * *
   stop time passed to cron: none
   - FTP SERVER PARAMETERS
   server address in use:  swupdate
   login:  manager
   password:  friend
   pathname:  none
   mac:  false
```

See also
```
SWUPDATE SET PATH
SWUPDATE SET PASSWORD
```

1.4.4.1.8 SWUPDATE START

Syntax SWUPDATE START

Description This command forces the software update to start immediately and remain active until the next stop command is sent or the download is executed successfully.

Example `--> swupdate start`

See also SWUPDATE STOP

1.4.4.1.9 SWUPDATE START TIME

Syntax `SWUPDATE START TIME {NONE | MINUTE <minute> HOUR <hour> DAY-OF-MONTH <day-of-month> MONTH <month> DAY-OF-WEEK <day-of-week> }`

Description This command set the scheduled starting time. See the relative section about the syntax used for the starting time.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
MINUTES	The minute(s) in the hour when swupdate must start.	N/A
HOUR	The hour(s) in the day when swupdate must start.	N/A
DAY-OF-MONTH	The day(s) in the month when swupdate must start.	N/A
MONTH	The month(s) in the year when swupdate must start.	N/A
DAY-OF-WEEK	The day(s) in the week when swupdate must start.	N/A

Example `--> swupdate set start_time minute * hour [0-7] day-of-month * month * day-of-week *`

See also SWUPDATE SHOW

1.4.4.1.10 SWUPDATE STOP

Syntax SWUPDATE STOP

Description This command force the software update to stop immediately and remain in idle state until a start command is set.

Example `--> swupdate stop`

See also SWUPDATE START

1.4.4.1.11 SWUPDATE STOP TIME

Syntax SWUPDATE STOP TIME {NONE | MINUTE <minute> HOUR <hour> DAY-OF-MONTH <day-of-month> MONTH <month> DAY-OF-WEEK <day-of-week> }

Description This command set the scheduled stop time. See the relative section about the syntax used for the stop time.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
MINUTES	The minute(s) in the hour when swupdate must stop.	N/A
HOUR	The hour(s) in the day when swupdate must stop.	N/A
DAY-OF-MONTH	The day(s) in the month when swupdate must stop.	N/A
MONTH	The month(s) in the year when swupdate must stop.	N/A
DAY-OF-WEEK	The day(s) in the week when swupdate must stop.	N/A

Example `--> swupdate set stop_time minute 0 hour [21-24] day-of-month * month * day-of-week *`

See also SWUPDATE SHOW

1.5 ZTC

Wide Area Networks consist of a lot of components (hubs, switches, routers, residential gateways, set top boxes, PCs) that need to be configured.

The number of components can be very high and often the configuration of these devices to get them up and running requires a lot of work for network administrators.

As a result, network administrator operations can be very expensive with in-field configuration taking a lot of time.

The ***Zero Touch Configurator*** (ZTC) is a tool designed to enable a network administrator to configure and manage network devices remotely and automatically without end-user intervention.

The ***Zero Touch Configurator*** is able to update image software and unit configuration on multiple devices simultaneously, so administrators can avoid having to connect to each device separately and repeat the same sequence of actions for each of them.

1.5.1 Functional blocks

The ZTC is a component-based application, which consists of different logical blocks that can be distributed on independent runtime environments or machines (see Figure 1-10).

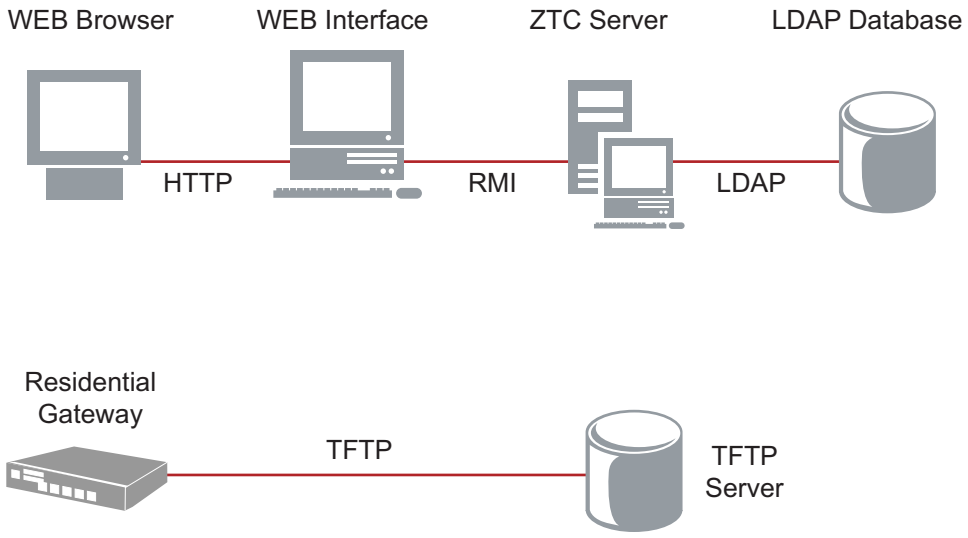


FIGURE 1-10 ZTC network architecture

1.5.1.1 ZTC network architecture

The ZTC Network Architecture consists of the following parts:

- An ***LDAP Directory Serv***ice in which data is stored.
- The *ZTC Server*, that contains all the application logic for:
- User authentication and authorization
- Data consistency and syntax checking when requesting to add a new device configuration
- Application logic for creating new configuration scripts
- Application logic to execute commands on the device
- Data Access Object layer to access the data tier
- Several protocols for supporting different kind of clients
- The *ZTC WEB Interface*. This application lest users interact with the ZTC Server. Through this interface they can view or update existing configurations, or add new ones.

- The *ZTC Embedded Client*. This client is installed on the devices to communicate with the ZTC Server. Typically, the devices connect to ZTC Server to perform the following operations:
- Communicate their actual configuration to ZTC Server
- Download, if existing, new configurations from ZTC Server

The components of ZTC are independent, and they can run on different machines and platforms, in a three-tiered architecture fashion.

The core of the application is the ZTC Server. It manages the dialogue with the directory service backend and performs all operations on data. The ZTC WEB Interface, used to interact with the ZTC Server, is decoupled from the ZTC server, and can run on different machines.

1.5.2 ZTC Client

The ZTC Embedded Client, or, shortly, the ZTC Client, is the module running on the gateway in charge to communicate with the ZTC server.

ZTC client works accordingly to the so-called ***Configuration PULL*** method. ZTC Client is in charge to contact the ZTC server passing the current configuration, the unit identifier and retrieves the new configuration if necessary. ZTC server has the responsibility to allow the download only of the correct configuration file depending on the unit identifier (the unit MAC address) and on the configuration rules defined inside the ZTC Server.

The following three ZTC Clients – ZTC Server communication phases are possible:

- ***Pull-at-startup*** – This phase is executed when the unit startup
- ***Scheduled-pull*** - This phase is executed every time the ***ztcclient*** polling timeout expires

ZTC Client and ZTC Server communicate through TFTP protocol.

The ZTC Server IP address can be configured in the ZTC Client module in two ways: either *statically* or *dynamically.*

When a ***static configuration*** is used, the ZTC Server IPv4 address is defined explicitly using the ZTCCLIENT ENABLE STATIC ZTCSERVERADDR command. This command set the server IP address that will be used by all the next queries and also turns on the ***ztcclient*** module forcing the module to query the server to retrieve the unit configuration file.

When a ***dynamic configuration*** is used, the ZTC client module is bind to an existing IP interface using the ZTCCLIENT ENABLE DYNAMIC LISTENINTERFACE command.

In this way the ZTC client module uses the facilities offered by the *dhcpclient* module to force the IP interface to ask to an external DHCP server the ZTC Server address. When the ZTC Client needs to know the ZTC Server address, a DHCP request is generated by the IP interface requesting a value for option 67 'bootfile-name'. The ZTC Client module as ZTC Server IP address uses the value returned by the DHCP server for option 67.

Similarly to the static configuration, ZTCCLIENT ENABLE DYNAMIC LISTENINTERFACE command turns on the ztcclient module forcing the module to query the server to retrieve the unit configuration file.

Note: ZTC client can be enabled dynamically only if the IP interface where it is bind, it's a dynamic IP interface. Attempting to enable ZTC client module dynamically on a static IP interface results is an error.

1.5.2.1 Storing unit configuration

The configuration file downloaded from ZTC Server is never stored permanently into the unit flash file system. This solution prevents memory flash failure when too many write requests are executed.

If the unit restarts, it loses the previous downloaded configuration and starts from the bootstrap configuration. This behavior allows network administrator to control the unit configuration based only on the configuration file defined by the ZTC Server framework.

When ZTC Client is enabled, the current running configuration is the result of the bootstrap configuration plus the unit configuration downloaded from ZTC Server. Any action that save permanently the configuration (e.g. the system configuration save command) could change the bootstrap configuration file and therefore the resulting configuration when ZTC Client runs could be unpredictable.

Note: When ZTC client is enabled, any CLI commands that can cause a change in the system configuration are inhibited. To enter these types of commands, it's necessary disable the ZTC client with the ZTCCLIENT DISABLE command.

1.5.2.2 Pull-at-startup

Figure 1-11 shows the ***Pull-at-startup*** phase executed by the ZTC client module when the gateway bootstraps.

Considering a scenario where ZTC Client is bind to a dynamic IP interface, during the bootstrap process, the gateway uses the facilities provided by the DHCP client module to setup the IP interface configuration.

The dynamic IP interface receives the new network configuration and the ZTC Server address in the 'bootfilename' DHCP option.

As soon the network is configured, the ZTC Client runs.

The ZTC Client contacts the ZTC Server, passing in the parameters list the Residential Gateway's MAC address, the application filename and a value derived from the current running configuration (that, at bootstrap, it is null). This information defines the current device status.

The ZTC Server checks if there is a configuration for the gateway looking for the device MAC address into the LDAP server, and if necessary, it returns the configuration file to the device.

The device executes the configuration file and starts the ZTC Client timeout. The timeout defines the polling period before ZTC Server will be contacted.

When the timeout expires the ***Scheduled-pull*** phase is executed.

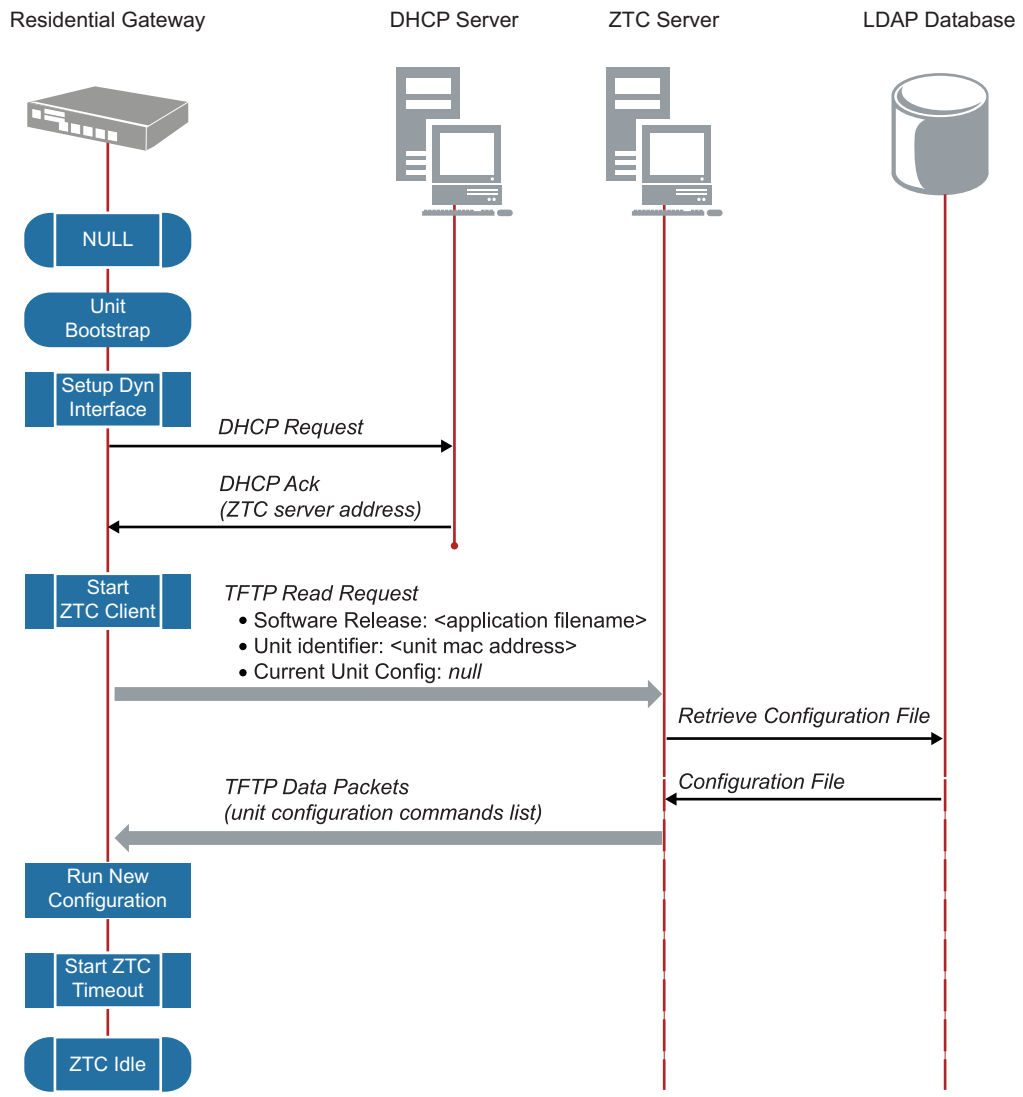


FIGURE 1-11 ***Pull-at-Startup*** **ZTC phase**

1.5.2.3 Scheduled-pull

Figure 1-11 shows the ***Scheduled-pull*** phase executed by the ZTC client module when the ztcclient polling timeout expires.

The ZTC Client contacts the ZTC Server, passing in the parameters list the Residential gateway MAC address, the application filename and the hash key derived from the current running configuration. This information defines the actual state of the device.

The ZTC Server checks whether there is a configuration for the gateway looking for the device MAC address into the LDAP server, and if necessary, it returns the configuration file to the device.

When the device receives the new configuration, it reboots in order to execute the new configuration starting from a "well known" status: the bootstrap configuration.

Since the gateway never stores the configuration downloaded from ZTC Server, the ZTC Client contacts again the ZTC Server and execute exactly the same procedure defined in the ***Pull-at-startup*** phase.

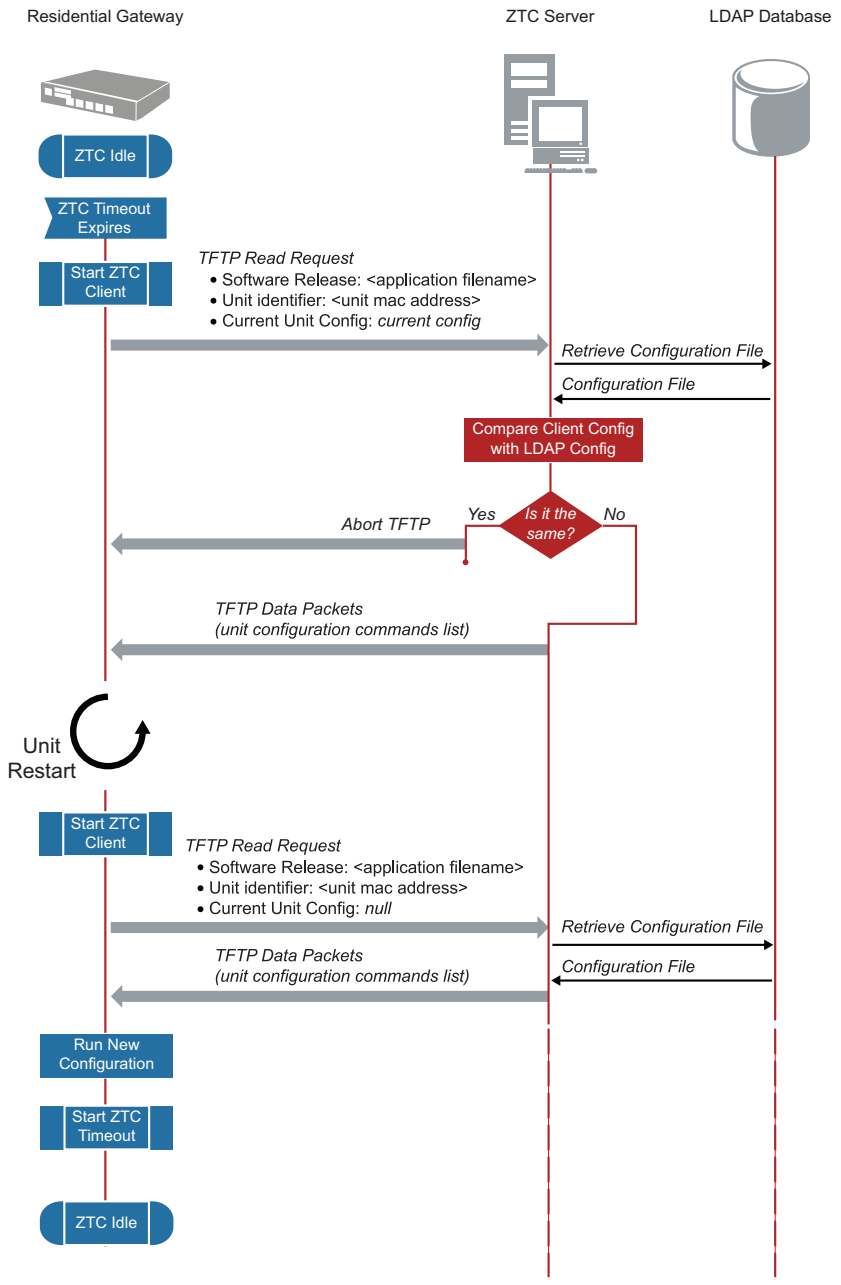


FIGURE 1-12 ***Scheduled-pull*** **ZTC phase**

1.5.3 ZTC command reference

This section describes the commands available on the gateways to configure and manage the ***ZTC Client*** module.

1.5.3.1 ZTC Client commands

The table below lists the ***ztcclient*** commands provided by the CLI:

TABLE 1-5 ZTC Client Commands

Option	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
ZTCCLIENT ENABLE DYNAMIC	X	X	X	X	X	X	X	X	X
ZTCCLIENT ENABLE STATIC	X	X	X	X	X	X	X	X	X
ZTCCLIENT DISABLE	X	X	X	X	X	X	X	X	X
ZTCCLIENT SHOW	X	X	X	X	X	X	X	X	X
ZTCCLIENT SET CONFIGTIMEOUT	X	X	X	X	X	X	X	X	X
ZTCCLIENT SET POLLINGTIMEOUT	X	X	X	X	X	X	X	X	X
ZTCCLIENT UPDATE	X	X	X	X	X	X	X	X	X

1.5.3.1.1 ZTCCLIENT ENABLE DYNAMIC

Syntax `ZTCCLIENT ENABLE DYNAMIC LISTENINTERFACE <ipinterface>`

Description This command enables the ztcclient and binds it on an existing dynamic IP interface. This command automatically creates a specific configuration rule that applies to the IP interface in order to force the ***dhcpclient*** module to request the ZTC server address inside the option list of the DHCP discover request sent to the external DHCP server.

Note: This command requires that <ipinterface> is defined as dynamic interface, thus it must have the DHCP flag enabled.

To apply changes to the ZTC client module and turn on it, use the ZTCCLIENT UPDATE command.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
IPINTERFACE	The name of an existing IP interface.To see the list of existing interfaces, use the IP LIST INTERFACE command.	N/A

Example `--> ztcclient enable dynamic listeninterface ip0`

See also `ZTCCLIENT DISABLE`

1.5.3.1.2 ZTCCLIENT ENABLE STATIC

Syntax `ZTCCLIENT ENABLE STATIC ZTCSERVERADDR <ztcserveraddr>`

Description This command enables the ztcclient, and set the ZTC Server IP address.

To apply changes to the ZTC client module and turn on it, use the ZTCCLIENT UPDATE command.

Options The following table gives the range of values for each option that can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
ZTCSERVERADDR	The IP address of the interface used to connect to the ZTC Server. The IP address must be specified in IPv4 format (e.g. 192.168.102.3)	N/A

Example `--> ztcclient enable static ztcserveraddr 192.168.102.3`

See also `ZTCCLIENT DISABLE`

1.5.3.1.3 ZTCCLIENT DISABLE

Syntax `ZTCCLIENT DISABLE`

Description This command disables the ztcclient module.

Example `--> ztcclient disable`

See also `ZTCCLIENT ENABLE`

1.5.3.1.4 ZTCCLIENT SHOW

Syntax `ZTCCLIENT SHOW`

Description This command shows the ZTC Client configuration parameters.

Example The following example shows the ZTC client parameters when a dynamic configuration is set.

```
ZTC CLIENT CONFIGURATION
   - GENERAL PARAMETERS
   enabled: false
   dynamic: true
   configuration timeout:  60 seconds
   server address in use:  192.168.1.10
   - DYNAMIC CONFIGURATION
   interface:  ip0
   - STATIC CONFIGURATION
   server address for static configuration:  0.0.0.0
```

1.5.3.1.5 ZTCCLIENT SET CONFIGTIMEOUT

Syntax `ZTCCLIENT SET CONFIGTIMEOUT <configtimeout>`

Description This command changes the value of the ***configtimeout***, which is the polling time interval used by the ztcclient when it check if new configurations are available on the ZTC server.

Options The following table gives the range of values for each option that can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
CONFIGTIMEOUT	The polling time (in minutes) used by the ztcclient module when the gateway is already configured. Acceptable values are from 1 to 120 minutes,	1

Example `--> ztcclient set configtimeout 30`

See also `ZTCCLIENT SHOW`

1.5.3.1.6 ZTCCLIENT SET POLLINGTIMEOUT

Syntax `ZTCCLIENT SET POLLINGTIMEOUT <pollingtimeout>`

Description This command changes the value of the ***pollingtimeout***, which is the polling time interval used by the ztcclient when it attempts the first synchronization. After the gateway is synchronized, the ztc client switches to the configtimeout polling time to check if new configurations are available on the ZTC server. The timer is used to force a fast synchronization without generate high network traffic when the gateway is already configured.

Options The following table gives the range of values for each option that can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
POLLINGTIMEOUT	The polling time (in secs) used by the ztc client module when it tries to make the first server synchronization.	5

Example `--> ztcclient set pollingtimeout 10`

See also `ZTCCLIENT SHOW`

1.5.3.1.7 ZTCCLIENT UPDATE

Syntax `ZTCCLIENT UPDATE`

Description This command saves the changes made with ZTCCLIENT SET CONFIGTIMEOUT and ZTCCLIENT ENABLE DYNAMIC or ZTCCLIENT ENABLE DYNAMIC commands and turn on the polling timeout.

Example `--> ztcclient update`

1.6 SNMP

This chapter introduces the configuration of SNMP module on the gateway.

To describe the SNMP configuration process the following terminology is used:

- entity
- a network management element that consists of an SNMP engine and one or more applications.
- engine
- a component of an SNMP entity that consists of a message processing subsystem, a security subsystem, an access control subsystem (as appropriate), and a dispatcher.
- application

- a component of an SNMP entity that determines the function of the entity. Applications include a command generator, command responder, notification originator, notification receiver, proxy forwarder, etc.

The SNMP entity that is commonly called a MANAGER is an engine plus a command generator application and a notification receiver application.

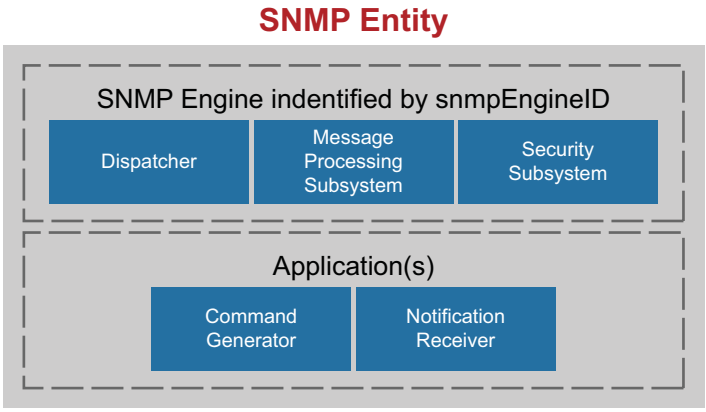


FIGURE 1-13 A manager Entity

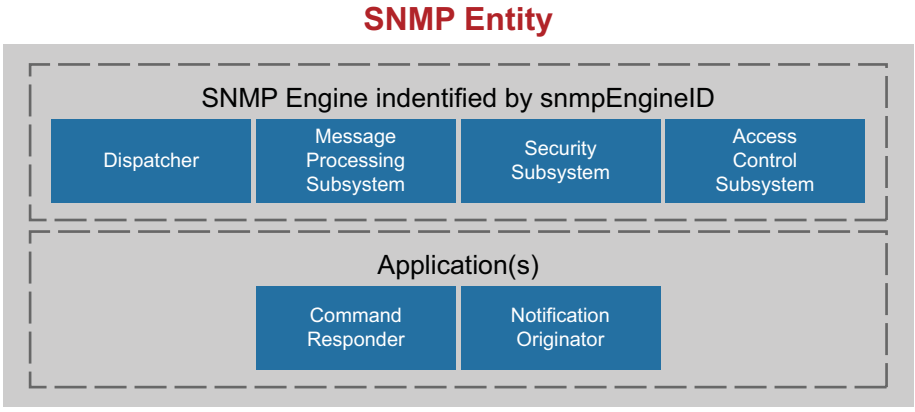


FIGURE 1-14 An agent Entity

The SNMP entity that is commonly called an AGENT is an engine plus a command responder and a notification originator. Other types of entities are possible, because other combinations of engine and applications are viable.

1.6.1 SNMP configuration within the SNMPv3 administration framework

The SNMPv3 Administration Framework is a configuration infrastructure for SNMPv3 users, but it can also be used to remotely configure and administer SNMPv1 and SNMPv2c community strings.

The SNMPv3 security administration framework provides a strong authentication mechanism, authorization with fine granularity, complete access control, security level controls which include two authentication algorithms[1] and an optional privacy protocol, and a MIB document for remote configuration.

1.6.1.1 Security

SNMPv3 provides advanced security mechanisms for protecting against threats to management operations. These security mechanisms are not new: they are taken from the SNMPv2 Draft Standards. The following sections describe the potential threats and how SNMPv3 protects against these threats.

SNMPv3 addresses in particular the following four threats:

- MASQUERADE
  the masquerade threat is when an unauthorized user attempts to carry out management operations by assuming the identity of an authorized user. SNMPv3 can verify the identity of the originator of the SNMPv3 message.
- MODIFICATION OF INFORMATION
  modification of information is the threat that a user will (by malice or error) alter a message in transit between the source and the destination, thereby carrying out unauthorized management activity. SNMPv3 can verify that the SNMPv3 message was not altered in transit between the originator and the recipient.
- MESSAGE STREAM MODIFICATION
  message stream modification occurs when (by malice or error) management messages are reordered, replayed, or delayed. SNMPv3 can verify that a received message is timely.

1.6.1.2 Mechanisms used by SNMPv3 security

SNMPv3 security protects against masquerade, modification of information, and message stream modification by using the Hash-based Message Authentication Code (HMAC) with MD5 Message Digest Algorithm (MD5) in a symmetric, i.e. private, key mode. MD5, defined in RFC1321, takes "as input a message of arbitrary length and produces as output a fingerprint or 'message digest' of the input."

- Computes an MD5 hash (H)on the concatenation of
  - The shared secret key (K), which has been `xored` with the hexadecimal value '36 '(ipad),
  - The SNMP message (text), which contains zero bytes in the digest field, to produce an intermediate digest, and
- Computes an MD5 hash on the concatenation of

1. Trivial authentication requiring only a correct user names and strong authentication based on an MD5 hash algorithm.

- The shared secret key, which has been xored with the hexadecimal value ‘5C ’(opad),
- The intermediate digest to produce the final digest.

The HMAC function is summarized by the following expression:

$$H(K \otimes opad \text{ , } H(K \otimes ipad \text{ , } text))$$

FIGURE 1-15 hmac expression

HMAC is used in the following manner to protect against threats to management operations:

- The sender and intended recipient of the SNMPv3 message share a secret key.
- When the sender constructs the outgoing message, the sender’s notion of the SNMP agent’s time is inserted into the message, and the digest field is padded with zeros. The HMAC function is then used to compute a digest (“fingerprint”) over the concatenation of the sender‘s notion of the shared secret key and SNMPv3 message.
- The digest is then inserted into the message at the position where the padding previously had been.
- The message is then sent.
- When the recipient receives the message, the digest in the incoming message is saved.
- The recipient inserts zeros into the incoming message at the position where the shared secret key previously had been.
- In the same manner as the sender, the recipient uses HMAC to compute a digest of the incoming message (with padding instead of a digest) and the recipient’s notion of the shared secret key.

The recipient then compares:

- The digest computed over the incoming message,
- The digest that was saved from the incoming message.

If the shared secret key has not been compromised[2], and if the two digests above exactly match, then there is a high degree of confidence[3] that the following statements about the message are true:

- The message origin is authentic. That is, the user that claims to have sent the message did in fact send it. Otherwise, the digests would have been different.
- The message contents have not been altered in transit. Otherwise, the digests would have been different.

2. SNMPv3 cannot protect against the threat of compromised keys. If an unauthorized user knows a shared secret key, then that user can masquerade as another user, modify messages in transit, and modify the message stream.
3. It is computationally infeasible to threaten a system by trying all possible keys, especially if the administration policy for the system includes a periodic changing of the keys which are configured.

When an SNMP agent receives a message, it verifies that the received message is timely by comparing the time value inside the packet with the current time. If the time value from the packet is within a "safe"window of the actual current time, the packet is accepted. If the time value from the packet is not within the specified window, a Report PDU containing the agent's notion of current time is transmitted to the sender of the received packet, and the agent discards the received packet.

If the original message was authentic, then the sender of the original message has the ability to resend the request. The sender of the original message will update its notion of the SNMP agent's time using the time value from the Report PDU. Then, the HMAC calculations will be performed again to obtain the digest for the same request packet containing an updated time value.

If the original message was the result of message stream modification, and if the shared secret key has not been compromised, then the sender would not find the time value from the Report PDU to be useful. Without the secret key, the packet digest cannot be correctly recalculated.

1.6.1.3 Local configuration datastore

SNMP configuration information must be stored locally on the gateway filesystem in a plain ASCII text file named `snmpd.cnf`.

It's possible upload such file via a ftp session (using the ftp daemon facility available on the Residential Gateway) or via the `swupdate` feature.

1.6.1.4 Configuration file format

Each line of the configuration file has the format <TAG> <VALUE> where <TAG> is a keyword and <VALUE> is a valid configuration value.

Entries may be continued across multiple lines by using a backslash (\). White space (tabs, spaces, line-feeds/ carriage-returns) and blank lines in the file are ignored. Values that are strings containing white space must be delimited with quotation marks (").

1.6.1.5 Configuration for all SNMPv3 entities

1.6.1.5.1 Configuring SNMPv3 users

Configuration for at least one SNMPv3 user must be provided for an SNMP engine to send or receive SNMPv3 messages on behalf of certain SNMP applications.

To configure an SNMPv3 user, add an `usmUserEntry` definition in the `snmpd.cnf` file accordingly the following syntax:

```
usmUserEntry <usmUserEngineID> <usmUserName> <usmUserAuthProtocol>
<usmUserStorageType> <usmTargetTag> <AuthKey>
```

usmUserEngineID
is an OctetString which is the authoritative SNMP engine's administratively-unique identifier. For a detailed explanation of snmpEngineID, refer to the next section.

For Get, GetNext, GetBulk, and Set requests, the SNMP entity containing the command responder application is authoritative. Therefore, the value of the usmUserEngineID field of the usmUserEntry in the agent 's configuration file will be localSnmpID.

For Trap messages, the SNMP entity containing the notification generator application is authoritative. Therefore, the value of the usmUserEngineID field of the usmUserEntry in the agent's configuration file will be localSnmpID.

usmUserName
is a human readable string representing the name of the user. This is the user-based security model dependent security ID.

UsmUserAuthProtocol
is an OBJECT IDENTIFIER that indicates whether messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be authenticated, and if so, the type of authentication protocol which is used. The value of usm-UserAuthProtocol can be usmNoAuthProtocol or usmHMACMD5AuthProtocol.

usmUserPrivProtocol
is an OBJECT IDENTIFIER that indicates whether messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be protected from disclosure, and if so, the type of privacy protocol which is used. The value of usmUserPrivProtocol must be usmNoPrivProtocol.

UsmUserStorageType
is nonVolatile, permanent, or readOnly.

usmTargetTag
is a human readable string that is used to select a set of entries in the snmpTargetAddrTable for source address checking. If the SNMP entity should not perform source address checking, then this field should contain a dash (-).

AuthKey
is an OctetString represented as a sequence of hexadecimal numbers separated by colons. Each octet is within the range 0x00 through 0x. If usmUserAuthProtocol is usmNoAuthProtocol, this user does not have an AuthKey, and this field should contain a dash (-).

This field can also be set to a human readable string representing the user's authentication password; the password will be converted to a key at run time.

It's possible define more than one SNMPv3 user. The list of all the SNMPv3 user entries is named usmUserTable.

1.6.1.5.2 Breakdown of an snmpEngineID

An `snmpEngineID` is a globally unique identifier for an SNMP entity. All SNMPv3 entities must possess an `snmpEngineID`. The `snmpEngineID` of an SNMP agent can be retrieved by sending a `Get` request to the agent for the MIB object `snmpEngineID`.

The following `snmpEngineID` are registered for Allied gateways models:

Model	OID	Model	OID
AT-RG613	1.3.6.1.4.1.207.1.17.1	***AT-iMG634B***	1.3.6.1.4.1.207.1.17.45
AT-RG623	1.3.6.1.4.1.207.1.17.4	***AT-iMG634WA***	1.3.6.1.4.1.207.1.17.46
AT-RG613TXJ	1.3.6.1.4.1.207.1.17.5	***AT-iMG634WB***	1.3.6.1.4.1.207.1.17.47
AT-RG656	1.3.6.1.4.1.207.1.17.6	***AT-iMG664WA***	1.3.6.1.4.1.207.1.17.50
AT-RG613LH	1.3.6.1.4.1.207.1.17.7	***AT-iMG664WB***	1.3.6.1.4.1.207.1.17.51
AT-RG613SH	1.3.6.1.4.1.207.1.17.8	***AT-iMG664A***	1.3.6.1.4.1.207.1.17.48
AT-RG623LH	1.3.6.1.4.1.207.1.17.9	***AT-iMG664B***	1.3.6.1.4.1.207.1.17.49
AT-RG623SH	1.3.6.1.4.1.207.1.17.10	***AT-iMG616RF+***	1.3.6.1.4.1.207.1.17.54
AT-RG613BD	1.3.6.1.4.1.207.1.17.11	***AT-iMG646MOD***	1.3.6.1.4.1.207.1.17.55
AT-RG623BD	1.3.6.1.4.1.207.1.17.12	***AT-iMG626MOD***	1.3.6.1.4.1.207.1.17.64
AT-RG624A	1.3.6.1.4.1.207.1.17.13	***AT-iMG616SRF***	1.3.6.1.4.1.207.1.17.62
AT-RG624B	1.3.6.1.4.1.207.1.17.14	***AT-iMG616SRF+***	1.3.6.1.4.1.207.1.17.63
AT-RG634A	1.3.6.1.4.1.207.1.17.15	***AT-iBG915FX***	1.3.6.1.4.1.207.1.17.65
AT-RG634B	1.3.6.1.4.1.207.1.17.16	***AT-iMG624A-R2***	1.3.6.1.4.1.207.1.17.66
AT-RG656LH	1.3.6.1.4.1.207.1.17.17	***AT-iMG624B-R2***	1.3.6.1.4.1.207.1.17.67
AT-RG656SH	1.3.6.1.4.1.207.1.17.18	***AT-iMG634A-R2***	1.3.6.1.4.1.207.1.17.68
AT-RG656TX	1.3.6.1.4.1.207.1.17.19	***AT-iMG634B-R2***	1.3.6.1.4.1.207.1.17.69
AT-RG644A	1.3.6.1.4.1.207.1.17.20	***AT-iMG634WA-R2***	1.3.6.1.4.1.207.1.17.70
AT-RG644B	1.3.6.1.4.1.207.1.17.21	***AT-iMG634WB-R2***	1.3.6.1.4.1.207.1.17.71
AT-RG646BD	1.3.6.1.4.1.207.1.17.24	***AT-iMG616W***	1.3.6.1.4.1.207.1.17.72
AT-RG632SA	1.3.6.1.4.1.207.1.17.25	***AT-iMG616CRF***	1.3.6.1.4.1.207.1.17.73
AT-RG632SB	1.3.6.1.4.1.207.1.17.26	***AT-iMG616CRFW***	1.3.6.1.4.1.207.1.17.74
AT-RG613RF	1.3.6.1.4.1.207.1.17.30	***AT-iMG616TX***	1.3.6.1.4.1.207.1.17.75

Model	OID	Model	OID
AT-iMG606TX	1.3.6.1.4.1.207.1.17.31	***AT-iMG616TXW***	1.3.6.1.4.1.207.1.17.76
AT-iMG606BD	1.3.6.1.4.1.207.1.17.32	***AT-iMG616LHW***	1.3.6.1.4.1.207.1.17.77
AT-iMG606LH	1.3.6.1.4.1.207.1.17.33	***AT-iMG616BD-R2***	1.3.6.1.4.1.207.1.17.78
AT-iMG606SH	1.3.6.1.4.1.207.1.17.34	***AT-iMG616LH-R2***	1.3.6.1.4.1.207.1.17.79
AT-iMG646BD-ON	1.3.6.1.4.1.207.1.17.35	***AT-iMG606W***	1.3.6.1.4.1.207.1.17.80
AT-iMG646PX-ON	1.3.6.1.4.1.207.1.17.36	***AT-iMG606CRF***	1.3.6.1.4.1.207.1.17.81
AT-iMG616RF	1.3.6.1.4.1.207.1.17.38	***AT-iMG606TX-R2***	1.3.6.1.4.1.207.1.17.82
AT-iMG616BD	1.3.6.1.4.1.207.1.17.39	***AT-iMG606TXW***	1.3.6.1.4.1.207.1.17.83
AT-iMG616LH	1.3.6.1.4.1.207.1.17.40	***AT-iMG606LHW***	1.3.6.1.4.1.207.1.17.84
AT-iMG616SH	1.3.6.1.4.1.207.1.17.41	***AT-iMG606BD-R2***	1.3.6.1.4.1.207.1.17.85
AT-iMG624A	1.3.6.1.4.1.207.1.17.42	***AT-iMG606LH-R2***	1.3.6.1.4.1.207.1.17.86
AT-iMG624B	1.3.6.1.4.1.207.1.17.43	***AT-iMG746MOD***	1.3.6.1.4.1.207.1.17.72
AT-iMG634A	1.3.6.1.4.1.207.1.17.44	***AT-iMG726MOD***	1.3.6.1.4.1.207.1.17.73

1.6.1.5.3 Configuring an agent to receive requests and send traps

This section describes how to configure SNMPv3 user information only. Additional configuration is required for an SNMP agent to actually receive SNMP requests and send SNMP Traps.

When an SNMP agent receives an SNMPv3 request from an SNMP manager, the user sending the message must be known to the agent's SNMP engine. If the request is sent in a secure packet, the agent must use the use's security key to authenticate the message. For this operation, the keys must be pre-configured in the `snmpd.cnf` con figuration file.

When an SNMP agent sends an SNMPv3 Trap to an SNMP manager, the recipient user must be known to the agent's SNMP engine. If the Trap is sent in a secure packet, the agent must use the user's security key to compute an authentication digest for the message. For this operation, the keys must be pre-configured in the `snmpd.cnf` configuration file.

Note: For each the following examples, the `snmpEngineID` *for the agent is used (*`localSnmpID`*), because the receiving SNMP engine is authoritative for the security of SNMP request messages, and the sending SNMP engine is authoritative for the security of SNMP Trap messages.*

1.6.1.5.4 Configuration for authentication

The following `usmUserEntry` configures an SNMP agent engine with information about an SNMPv3 user whose name is "myV3AuthNoPrivUser". This entry contains the user's authentication password. An SNMP

request message from this user (originating from another SNMP entity) can be received if the message was sent using no security or using MD5 authentication. The SNMP agent can send Trap messages to this user using no security or using MD5 authentication.

```
usmUserEntry localSnmpID myV3AuthNoPrivUser usmHMACMD5AuthProtocol
usmNoPrivProtocol nonVolatile whereValidRequestsOriginate
myV3UserAuthPassword
```

1.6.1.5.5 Configuration for no authentication

The following `usmUserEntry` configures an SNMP agent engine with information about an SNMPv3 user whose name is "myV3NoAuthNoPrivUser". This user does not have an authentication password, so the last field contains a dash (-). An SNMP request message from this user (originating from another SNMP entity) can be received if the message was sent using no security.

The SNMP agent can send Trap messages to this user using no security.

```
usmUserEntry localSnmpID myV3NoAuthNoPrivUser usmNoAuthProtocol usm-
NoPrivProtocol nonVolatile whereValidRequestsOriginate –
```

1.6.2 Additional configuration for SNMPv3 agent entities

Certain SNMP applications (which are normally associated with an SNMP entity acting in the "agent" role) require more information in addition to the information about SNMPv3 users.

1.6.2.1 Configuring view-based access control

Configuration of view-based access control must be provided for the SNMP engine to correctly process SNMPv1, SNMPv2c, or SNMPv3 messages. Configuring view-based access control is a process that requires three steps:

- Define a family of view subtrees.
- Define a group and its associated access rights.
- Assign an SNMPv3 user (or SNMPv1 community string, etc.) to the group defined in step2.

The following sections describe each step of this process in more detail.

1.6.2.2 Defining families of view subtrees

To configure an view tree family, add an `vacmViewTreeFamily` definition in the `snmpd.cnf` file accordingly the following syntax:

```
vacmViewTreeFamily <vacmViewTreeFamilyViewName> <vacmViewTreeFam-
ilySubtree> <vacmViewTreeFamilyMask> <vacmViewTreeFamilyType> <vacm-
ViewTreeFamilyStorageType>
```

`vacmViewTreeFamilyViewName`
is a human readable string representing the name of this family of view subtrees.

`vacmViewTreeFamilySubtree`
is an OBJECT IDENTIFIER that identifies a subtree of the MIB; e.g. enterprises.207. This value and `vacmViewTreeFamilyMask` are used to determine if an OBJECT IDENTIFIER is in this family of view subtrees.

`vacmViewTreeFamilyMask`
is an `OctetString` represented as a sequence of hexadecimal numbers separated by colons. Each octet is within the range 0x00 through 0xFF. A zero length `OctetString` is represented with a dash (-).

`vacmViewTreeFamilyType`
is included or excluded and indicates if the `vacmViewTreeFamilySubtree` is explicitly accessible or not accessible in this family of view subtrees.

`VacmViewTreeFamilyStorageType`
is `nonVolatile`, `permanent`, or `readOnly`.

It's possible define more than one `vacmTreeFamily`. The list of all the `vacmTreeFamily` entries is named `vacmTreeFamilyTable`.

Example:

```
vacmViewTreeFamilyEntry All iso - included non-Volatile
```

defines a subtree for the view named "All" that includes the entire set of MIB objects (iso is the root node of the MIB tree).

The `vacmViewTreeFamilyMask` field allows restriction of the MIB view at a finer granularity than that of the `vacmViewTreeFamilySubtree` and `vacmViewTreeFamilyType` pair. For instance, a view can be restricted to one row of a table (see the example below).

The value - causes the corresponding `vacmViewTreeFamilyMask` to be a NULL string, which in turn allows all entries 'below' the `vacmViewTreeFamilySubtree` entry to be visible, unless cancelled by another `vacmViewTreeFamilyEntry`.

The `vacmViewTreeFamilyMask` is built using octets that correspond to the OID being restricted. For example, one may wish to restrict a user's view of the `ifTable` to only the second row, all columns. The OID for `ifEntry.0.2` is:

```
1.3.6.1.2.1.2.2.1.0.2
```

The `vacmViewTreeFamilyMask` is a series of ones and zeros used for masking out parts of the tree. A zero indicates a WILD CARD (i.e, matches anything), and a one indicates an exact match must be made. So:

OID	1 . 3 . 6 . 1 . 2 . 1 . 2 . 2 . 1 . 0 . 2
vacmViewTreeFamilyMask	1 1 1 1 1 1 1 1 1 0 1

FIGURE 1-16 vacmViewTreeFamilyMask

would require an exact match on all fields except the table column (i.e., the 0 in `ifEntry.0.2`).

Using the above example, the bits of the `vacmViewTreeFamilyMask` would be grouped into bytes, and then the right end padded with ones if necessary to fill out the last byte:

byte 1		byte 2		
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	original mask
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	padded with 1's
ff		bf		hex value

FIGURE 1-17 vacmViewTreeFamilyMask (continued)

So the `vacmViewTreeFamilyMask` entry would be:

```
ff:bf
```

1.6.2.3 Defining groups and access rights

To configure a group and its associated access rights, add a `vacmAccessEntry` definition in the `snmpd.cnf` file accordingly the following syntax:

```
vacmAccessEntry <vacmGroupName> <vacmAccessContextPrefix> <vacmAc-
cessSecurityModel> <vacmAccessSecurityLevel> <vacmAccessContext-
Match> <vacmAccessReadViewName> <vacmAccessWriteViewName>
<vacmAccessNotifyViewName> <vacmAccessStorageType>
```

`vacmGroupName`
is a human readable string which is the groupname.

`vacmAccessContextPrefix`
is a human readable string which is an entire or partial context name used to match the context name in (or derived from) a management request. A dash (-) represents the default context.

`vacmAccessSecurityModel`
is `snmpv1` for SNMPv1, `snmpv2c` for SNMPv2c, or `usm` for SNMPv3.

`vacmAccessSecurityLevel`
is `noAuthNoPriv` for no authentication and no privacy, and `authNoPriv` is for MD5 authentication with no privacy.

`vacmAccessContextMatch`
is *exact* or `prefix` to indicate how the context of a request must match `vacmAccessContextPrefix`.

For example, if an authenticated management request is sent in context "AT-iMG646MOD", and if the value of `vacmAccessContextPrefix` and `vacmAccessContextMatch` are "AT-iMG646MOD" and "prefix", then the context name in (or derived from) the request is determined to be a correct match to the values in this `vacmAccessEntry`.

`vacmAccessReadViewName`
is a `vacmViewTreeFamilyViewName` (defined by at least one `vacmViewTreeFamilyEntry`) identifying the view subtrees accessible for `Get, GetNext, and GetBulk` requests.

`vacmAccessWriteViewName`
is a `vacmViewTreeFamilyViewName` (defined by at least one `vacmViewTreeFamilyEntry`) identifying the view subtrees accessible for `Set` requests.

`vacmAccessNotifyViewName`
is a `vacmViewTreeFamilyViewName` (defined by at least one `vacmViewTreeFamilyEntry`) identifying the view subtrees from which objects may be included as `VarBinds` in `Trap` messages and `Inform` requests.

`vacmAccessStorageType`
is `nonVolatile, permanent, or readOnly`.

1.6.2.4 Assigning principals to groups

A PRINCIPAL is generic term to refer to an SNMPv3 user or an SNMPv2c or SNMPv1 community string (see RFC2571).

To assign a principal to a group, add one or more `vacmSecurityToGroupEntry` definition in the `snmpd.cnf` file accordingly the following syntax:

```
vacmSecurityToGroupEntry <vacmSecurityModel> <vacmSecurityName> <vac-
mGroupName> <vacmSecurityToGroupStorageType>
```

`vacmSecurityModel`
is `snmpv1` for SNMPv1, `snmpv2c` for SNMPv2c, or `usm` for SNMPv3.

`vacmSecurityName`
is a human readable string which is the principal.

`vacmGroupName`
is a human readable string which is the groupname. The groupname must be defined by at least one `vacmAccessEntry`.

vacmSecurityToGroupStorageType
is nonVolatile, permanent, or readOnly.

It's possible define more than one vacmSecurityToGroupEntry. The list of all the vacmSecurityToGroupEntry entries is named vacmSecurityToGroupTable.

1.6.3 Configuring notifications

SNMP agent is designed to support SNMPv1 Traps, SNMPv2c Traps, or SNMPv3 Traps. To send TRAPs, it's necessary perform some basic SNMP engine configuration as defined in the following sections.

Configuring notification is a process that requires four steps:

- Define a notification.
- Define a set of network addresses to which a notification should be sent.
- Define parameters to use when sending notifications to each of the target addressed identified in step2.
- Optionally, define notification filters to reduce the amount of traps sent to the target addresses.

The following sections describe each step of this process in more detail.

1.6.3.1 Defining notifications

To configure a notification, add an snmpNotifyEntry definition in the snmpd.cnf file accordingly the following syntax:

```
snmpNotifyEntry <snmpNotifyName> <snmpNotifyTag> <snmpNotifyType>
<snmpNotifyStorageType>
```

snmpNotifyName
is a human readable string representing the name of this notification.

snmpNotifyTag
is a human readable string that is used to select a set of entries in the snmpTargetAddrTable.

snmpNotifyType
is 1(trap) or 2(inform).

nmpNotifyStorageType
is nonVolatile, permanent or readOnly.

It's possible define more than one notification. The list of all the notification entries is named snmpNotifyTable.

Example:

```
snmpNotifyEntry myFirstNotify myFirstNotifyTag 1 nonVolatile
snmpNotifyEntry mySecondNotify mySecondNotifyTag 1 nonVolatile
```

1.6.3.2 Defining target addresses

To configure a target address (to which a notification should be sent), add one or more `snmpTargetAddrEntry` definition in the `snmpd.cnf` file accordingly the following syntax:

```
snmpTargetAddrEntry <snmpTargetAddrName> <snmpTargetAddrTDomain>
<snmpTargetAddrTAddress> <snmpTargetAddrTimeout> <snmpTargetAddrRe-
tryCount> <snmpTargetAddrTagList> <snmpTargetAddrParams> <snmpTar-
getAddrStorageType> <snmpTargetAddrTMask> <snmpTargetAddrMMS>
```

`snmpTargetAddrName`
is a human readable string representing the name of this target.

`snmpTargetAddrTDomain`
is an OID which indicates the network type (UDP/IP,IPX,etc.). For UDP/IP transport type, the OID value (in dotted format) is `1.3.6.1.6.1.1` or equivalent (in English name) `snmpUDPDomain`.

`snmpTargetAddrTAddress`
is a valid address in the `snmpTargetAddrTDomain`. For `snmpTargetAddrTDomain` equal to `snmpUDPDomain`, a valid address would be `192.147.142.35:0`, where the value after the colon is the UDP port number. This address is used as the destination address for outgoing notifications.

Note: If the port number is specified as zero, the actual destination port used for the outgoing notification message is set to the default 162

`snmpTargetAddrTimeout`
is an integer which identifies the expected maximum round-`trip time` (in hundredths of seconds) for communicating with the `snmpTargetAddrTAddress`.

When an Inform is sent to this address, and a response is not received within this time period, the SNMP entity will assume that the response will not be delivered. The default value of 1500 (15 seconds) is suggested by RFC2573. If the outgoing message type is not Inform then this field is ignored.

`snmpTargetAddrRetryCount`
is an integer which identifies the number of times the SNMP entity will attempt to retransmit an Inform when a response is not received. The default value of 3 is suggested by RFC2573. If the outgoing message type is not Inform, then this field is ignored.

`snmpTargetAddrTagList`
is a quoted string containing one or more (space-separated) tags. These tags correspond to the value of `snmpNotifyTag` in the `snmpNotifyTable`. A notification defined in the `snmpNotifyTable` will be sent to the address specified in `snmpTargetAddrTDomain` if the notification's `snmpNotifyTag` appears in this list of tags.

`snmpTargetAddrParams`
is a human readable string that is used to select a set of entries in the `snmpTargetParamsTable`

`snmpTargetAddrStorageType`
is `nonVolatile, permanent`, or `readOnly`.

snmpTargetAddrTMask
is a bitfield mask for the snmpTargetAddrTAddress and appears in the snmpd.cnf file in the same format as the snmpTargetAddrTAddress For notifications, the value must be 255.255.255.255:0 to indicate that the Trap or Inform message will be sent to a specific address.

*Note: SNMP does not allow for the broadcasting of notifications. However, a notification may be sent to more than one specific address by configuring more than one **snmpTargetAddrEntry** with the same tag(s)in the **snmpTargetAddrTagListfield***

snmpTargetAddrMMS
is an integer which is the maximum message size (in bytes)that can be transmitted between the local host and the host with address snmpTargetAddrTAddress without risk of fragmentation. The default value is 2048.

1.6.3.3 Defining target parameters

To configure parameters to be used when sending notifications, add one or more snmpTargetParamsEntry definition in the snmpd.cnf file accordingly the following syntax:

```
snmpTargetParamsEntry <snmpTargetParamsName> <snmpTargetParamsMP-
Model> <snmpTargetParamsSecurityModel> <snmpTargetParamsSecuri-
tyName> <snmpTargetParamsSecurityLevel>
<snmpTargetParamsStorageType>
```

snmpTargetParamsName
is a human readable string representing the name of this parameter.

snmpTargetParamsMPModel
is 0 for SNMPv1, 1 for SNMPv2c, or 3 for SNMPv3.The value of this field together with the value of snmpTargetParamsSecurityModel indicates which type of notification should be sent.

snmpTargetParamsSecurityModel
is snmpv1 for SNMPv1, snmpv2c for SNMPv2c, or usm for SNMPv3.The value of this field together with the value of snmpTargetParamsMPModel indicates which type of notification should be sent.

snmpTargetParamsSecurityName
is a human readable string which is the principal (an SNMPv3 user, or an SNMPv2c or SNMPv1 community string) to be used in the notification.

snmpTargetParamsSecurityLevel
identifies the security level of the notification to send. When an SNMPv1 or SNMPv2c notification is configured, the only valid value is noAuthNoPriv. When an SNMPv3 notification is configured, the value of this field is noAuthNoPriv for no authentication and no privacy, or authNoPriv for authentication without privacy.

snmpTargetParamsStorageType
is nonVolatile, permanent or readOnly.

1.6.4 Configuring notification filters

After the SNMP entity has been properly configured to send notifications, the SNMP engine will dutifully send SNMPv1, SNMPv2c, and SNMPv3 notification messages on behalf of the notification generator application.

Depending upon the nature of the specific notification generator application, this may result in the sending of few or many notifications.

A well-designed notification generator application will send enough notifications to be useful to a notification receiver application, but not too many notifications that it produces "noise".

The SNMPv3 administration framework allows an SNMP entity which contains both a notification receiver application and a command generator application to "turn down the noise" by filtering notifications at the source.

In the SNMP entity containing the notification originator, there are two MIB tables which control notification filtering: the `snmpNotifyFilterProfileTable` and the `snmpNotifyFilterTable`. By sending SNMP Set requests to create new rows in these tables, the SNMP entity with the notification receiver application can specify what kinds of notifications should not be sent to it.

This section describes the `snmpNotifyFilterProfileTable` and the `snmpNotifyFilterTable` in terms of the corresponding entries in the `snmpd.cnf` file. Using this information, some notification filters can be pre-configured before the AGENT entity is launched.

Configuring a notification filter is a process that requires two steps:

- Create a notification filter.
- Associate the notification filter with one or more notification parameters.

1.6.4.1 Creating a notification filter

To create a notification filter, add one or more `snmpNotifyFilterEntry` definition in the `snmpd.cnf` file accordingly the following syntax:

```
snmpNotifyFilterEntry.<snmpNotifyFilterProfileName> <snmpNotifyFil-
terSubtree> <snmpNotifyFilterMask> <snmpNotifyFilterType> <snmpNoti-
fyFilterStorageType>
```

`snmpNotifyFilterProfileName`
is a human readable string representing the name of this notification filter.

`snmpNotifyFilterSubtree`
is an OID which specifies the MIB sub-tree containing notifications objects to be filtered. The value of this OID may be specified in dotted-decimal format or by the English name.

`snmpNotifyFilterMask`
modifies the set of notifications and objects identified by `snmpNotifyFilterSubtree` (a detailed explanation follows).This object is an `OctetString` represented as a sequence of hexadecimal numbers separated by

colons. Each octet is within the range 0x00 through 0xff. A zero-length `OctetString` is represented with a dash (-).

`snmpNotifyFilterType`
is included or excluded. This object indicates whether the family of filter sub-trees defined by this entry are included in or excluded from a filter.

`snmpNotifyFilterStorageType`
is `nonVolatile`, `permanent`, or `readOnly`.

The `snmpNotifyFilterMaskfield` allows filtering of MIB view at a finer granularity than that of the `snmpNotifyFilterSubtree` and `snmpNotifyFilterType` pair alone. For instance, a filter can be made to apply to one row of a table only (see the example below).

The value causes the corresponding `snmpNotifyFilterMask` to be a NULL string, which in turn allows all objects 'below' the `snmpNotifyFilterSubtree` entry to be filtered.

The `snmpNotifyFilterMask` is built using octets that correspond to the OID being filtered.

For example, one may wish to restrict a filter of the `ifTable` to only the second row, all columns. The OID for `ifEntry.0.2` is: `1.3.6.1.2.1.2.2.1.0.2`

The `snmpNotifyFilterMask` is a series of ones and zeros used for masking out parts of the filter.

A zero indicates a WILD CARD (i.e. matches anything), and a one indicates an exact match must be made. So:

OID	1	.	3	.	6	.	1	.	2	.	1	.	2	.	2	.	1	.	0	.	2
snmpNotifyFilterMask	1		1		1		1		1		1		1		1		1		0		1

FIGURE 1-18 snmpNotifyFilterMask

would require an exact match on all fields except the table column (i.e. the 0 in `ifEntry.0.2`).

Using the above example, the bits of the `snmpNotifyFilterMask` would be grouped into bytes, and then the right end padded with ones if necessary to fill out the last byte:

byte 1		byte 2		
1 1 1 1	1 1 1 1	1 0 1		original mask
1 1 1 1	1 1 1 1	1 0 1 1	1 1 1 1	padded with 1's
ff		bf		hex value

FIGURE 1-19 snmpNotifyFilterMask (continued)

So the snmpNotifyFilterMask entry would be

```
ff:bf
```

With this value for snmpNotifyFilterMask and all other appropriate entries in the con figuration file, a notification containing values from any of the following ifTable objects would match the filter and would not be sent:

```
ifIndex.2
ifDescr.2
ifType.2
ifMtu.2
ifSpeed.2
ifPhysAddress.2
ifAdminStatus.2
ifOperStatus.2
ifLastChange.2
ifInUcastPkts.2
ifInErrors.2
ifOutUcastPkts.2
ifOutErrors.2
ifOutQLen.2
ifSpecific.2
```

1.6.4.2 Associating a filter with a notification parameter

To create a notification filter, add one or more snmpNotifyFilterProfileEntry definition in the snmpd.cnf file accordingly the following syntax:

```
snmpNotifyFilterProfileEntry <snmpTargetParamsName> <snmpNotifyFil-
terProfileName> <snmpNotifyFilterProfileStorageType>
```

snmpTargetParamsName
is a snmpTargetParamsName defined in the snmpTargetParamsTable

snmpNotifyFilterProfileName
is a snmpNotifyFilterProfileName defined in the snmpNotifyFilterTable

snmpNotifyFilterProfileStorageType
is nonVolatile, permanent, or readOnly.

1.6.5 Configuring source address checking

A feature of SNMP Research software allows the SNMP engine to perform additional authentication of an incoming SNMPv1, SNMPv2c, or SNMPv3 message by checking the source address of the message.

To configure a source address (from which a message will be received), add one or more snmpTargetAddrEntry definition in the snmpd.cnf file accordingly the following syntax:

```
snmpTargetAddrEntry <snmpTargetAddrName> <snmpTargetAddrTDomain>
<snmpTargetAddrTAddress> <snmpTargetAddrTimeout> <snmpTargetAddrRe-
tryCount> <snmpTargetAddrTagList> <snmpTargetAddrParams> <snmpTar-
getAddrStorageType> <snmpTargetAddrTMask> <snmpTargetAddrMMS>
```

snmpTargetAddrName
is a human readable string representing the name of this target.

snmpTargetAddrTDomain
is an OID which indicates the network type (UDP/IP, IPX, etc.). For UDP/IP transport type, the OID value (in dotted format) is 1.3.6.1.6.1.1 or equivalent (in English name) snmpUDPDomain.

snmpTargetAddrTAddress
is a valid address in the snmpTargetAddrTDomain. For example, if the snmpTargetAddrTDomain is snmpUDPDomain, a valid address would be 192.147.142.35:0. This address is compared to the source address of an incoming message to determine if the message should be received or rejected. The scope of this comparison is controlled by the value of snmpTargetAddrTMask (see below).

snmpTargetAddrTimeout
is an integer which must be present but is ignored by the SNMP engine. This field should be set to zero.

snmpTargetAddrRetryCount
is an integer which must be present but is ignored by the SNMP engine. This field should be set to zero.

snmpTargetAddrTagList
is a quoted string containing one or more (space-separated) tags. These tags correspond to the value of usmTargetTag in the usmUserTable and to the value of snmpCommunityTransportTag in the snmpCommunityTable.

An incoming SNMPv1 or SNMPv2c message will not be rejected if:

- The community string in the incoming message matches a con figured snmpcommunityname, and
- The snmpcommunityentry has a snmpcommunitytransporttag with one or more corresponding tag(s) in the snmptargetaddrtable, and
- The source address of the incoming message is validated by snmptargetaddrtaddress (masked by snmptargetaddrtmask) of a corresponding snmptargetaddrentry

An incoming SNMPv3 message will not be rejected if:

- The user identified by the incoming message matches a configured usmusername, and
- The usmuserentry has a usmtargettag with one or more corresponding tag(s) in the snmptargetaddrtable,
- The source address of the incoming message is validated by snmptargetaddrtaddress (masked by snmptargetaddrtmask) of a corresponding snmptargetaddrentry

`snmpTargetAddrParams`
is a human readable string which must be present but is ignored by the SNMP engine. This field should be set to a dash (-).

`snmpTargetAddrStorageType`
is `nonVolatile`, `permanent`, or `readOnly`.

`snmpTargetAddrTMask`
is a bit field mask for the `snmpTargetAddrTAddress` and appears in the `snmpd.cnf` file in the same format as the `snmpTargetAddrTAddress`. For example, if `snmpTargetAddrTDomain` is '`snmpUDPDomain` ', a valid mask would be `255.255.255.0:0`. This mask is used in conjunction with the `snmpTargetAddrTAddress` to determine if an incoming request has arrived from an authorized address.

Note: The value trailing the colon should ALWAYS be zero

The value of `snmpTargetAddrTMask` identifies which bits of the source address should be compared to the value of `snmpTargetAddrTAddress`. A bit value of '1'in the mask means that the corresponding bit in the source address should be compared to the corresponding bit in the value of `snmpTargetAddrTAddress`. A bit value of 0 in the mask means that corresponding bit in the source address is a "don't care" case in the comparison.

`snmpTargetAddrMMS`
is an integer which is the maximum message size (in bytes) that can be transmitted between the local host and the host with address `snmpTargetAddrTAddress` without risk of fragmentation. The default value is 2048.

1.6.5.1 Matching exactly one source address

If `snmpTargetAddrTMask` is `255.255.255.255:0`, then all bits have '1' as value

byte 1		byte 2		byte 3		byte 4		
255		255		255		255		decimal
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	binary

FIGURE 1-20 snmpTargetAddrTMask

This indicates that the source address must exactly match the value of `snmpTargetAddrTAddress`, or the incoming SNMP request will be rejected.

1.6.5.2 Matching any source address

If `snmpTargetAddrTMask` is `0.0.0.0:0`, then all bits have '0' as value:

byte 1		byte 2		byte 3		byte 4		
0		0		0		0		decimal
0000	0000	0000	0000	0000	0000	0000	0000	binary

FIGURE 1-21 snmpTargetAddrTMask (continued)

This indicates that none of the bits of the source address will be compared to the value of `snmpTargetAddrTAddress`, and consequently, an incoming SNMP request will not be reject based on its source address.

1.6.5.3 Matching a source address in a subnet

If the high-order bits of `snmpTargetAddrTMask` are set to '1' and the low-order bits are set to '0', the mask can be used to reject an SNMP request that does not come from a particular subnet. For example, if `snmpTargetAddrTMask` is `255.255.255.128:0`, then only the most significant 25 bits of the source address must match the most significant 25 bits of the value of `snmpTargetAddrTAddress`.

byte 1		byte 2		byte 3		byte 4		
255		255		255		128		decimal
1111	1111	1111	1111	1111	1111	1000	0000	binary

FIGURE 1-22 snmpTargetAddrTMask (continued)

Consider the case where the value of `snmpTargetAddrTAddress` is `192.147.142.35`:

byte 1		byte 2		byte 3		byte 4		
192		147		142		35		decimal
1100	0000	1001	0011	1000	1110	0010	0011	binary

FIGURE 1-23 snmpTargetAddrTMask (continued)

in order not to be rejected, the source address of an incoming SNMP request must begin with `192.147.142` In the fourth byte, only the first bit will be compared to the same bit of the value of `snmpTargetAddrTAddress`. The remaining bits are "don't care" cases (shown in Figure 1-24).

byte 4		
0 0 1 0	0 0 1 1	snmpTargetAddrTMask (binary)
0 0 1 0	0 0 1 1	snmpTargetAddrTAddress (binary)
0 ? ? ?	? ? ? ?	source address of SNMP request

FIGURE 1-24 snmpTargetAddrTMask (continued)

Therefore, to not be rejected, the source address of an incoming SNMP request must be `192.147.142.xxx` where 'xxx' is a value between 0 (expressed as '00000000'in binary) and 127 (expressed as '01111111' in binary).

1.6.6 Examples

This section contains examples of SNMP configuration for SNMP agent entities.

1.6.6.1 noAuthNoPriv SNMPv3 users

To authorize the receipt of SNMPv3 `noAuthNoPriv Get` and `Set`[4] requests from the user "`myV3NoAuthNoPrivUser`" from exactly one manager station (one IP address), add the following lines to the *snmpd.cnf* configuration file together with the `usmUserEntry` for the user "`myV3NoAuthNoPrivUser`".

```
vacmAccessEntry myV3NoAuthNoPrivGroup -usm noAuthNoPriv exact All All
-nonVolatile
vacmSecurityToGroupEntry usm myV3NoAuthNoPrivUser
myV3NoAuthNoPrivGroup nonVolatile
vacmViewTreeFamilyEntry All iso -included nonVolatile
snmpTargetAddrEntry myV3Manager_allRequests snmpUDPDomain
192.147.142.35:0 0 0 whereValidRequestsOriginate -nonVolatile
255.255.255.255:0 2048
```

To relax the agent configuration so that this user can access the MIB objects from additional hosts, change the `snmpTargetAddrTMask` to perform wildcard matching of the source address of the incoming request message.

To relax the agent configuration so that this user can access the MIB objects from any host, change "`whereValidRequestsOriginate`" in the `usmUserEntry` to a dash (-).

```
usmUserEntry localSnmpID myV3NoAuthNoPrivUser usmNoAuthProtocol usmNo-
PrivProtocol nonVolatile - - -
```

4. To authorize Get request without authorizing Set requests, the fields "All All –" in the vacmAccessEntry should be changed to "All - - "

To authorize the sending of SNMPv3 `noAuthNoPriv Trap` messages to a user at exactly one SNMP manager station (one IP address), add the following lines to the `snmpd.cnf` configuration file together with the `usmUserEntry` for the user "`myV3NoAuthNoPrivUser`".

```
vacmAccessEntry myV3NoAuthNoPrivGroup -usm noAuthNoPriv exact - - All
nonVolatile
vacmSecurityToGroupEntry usm myV3NoAuthNoPrivUser
myV3NoAuthNoPrivGroup nonVolatile
vacmViewTreeFamilyEntry All iso -included nonVolatile
snmpNotifyEntry myTrap whereMyNotificationsGo trap nonVolatile
snmpTargetAddrEntry myV3Manager_noAuthNoPrivNotifications snmpUDPDo-
main 192.147.142.35:0 100 3 whereMyNotificationsGo
myV3NoAuthNoPrivParams nonVolatile 1.2.3.4:0 2048
snmpTargetParamsEntry myV3NoAuthNoPrivParams 3 usm
myV3NoAuthNoPrivUser noAuthNoPriv non-Volatile
```

To configure additional Trap destinations (additional IP addresses where the user is authorized to operate a management station), add additional `snmpTargetAddrEntry` entries to the `snmpd.cnf` configuration file. For example, to authorize 192.147.142.111 as an additional Trap destination, add the following line to the `snmpd.cnf` configuration file.

```
snmpTargetAddrEntry anotherV3Manager_noAuthNoPrivNotifications snm-
pUDPDomain 192.147.142.111:0 100 3 whereMyNotificationsGo
myV3NoAuthNoPrivParams nonVolatile 1.2.3.4:0 2048
```

1.6.7 authNoPriv SNMPv3 users

To authorize the receipt of SNMPv3 `authNoPriv Get` and `Set`[5] requests from the user "`myV3AuthNoPrivUser`" from exactly one manager station (one IP address), add the following lines to the `snmpd.cnf` configuration file together with the `usmUserEntry` for the user "`myV3AuthNoPrivUser`".

```
vacmAccessEntry myV3AuthNoPrivGroup -usm authNoPriv exact All All -
nonVolatile
vacmSecurityToGroupEntry usm myV3AuthNoPrivUser myV3AuthNoPrivGroup
nonVolatile
vacmViewTreeFamilyEntry All iso -included nonVolatile
snmpTargetAddrEntry myV3Manager_allRequests snmpUDPDomain
192.147.142.35:0 0 0 whereValidRequestsOriginate -nonVolatile
255.255.255.255:0 2048
```

5. To authorize Get request without authorizing Set requests, the fields "All All –" in the vacmAccessEntry should be changed to "All - - "

To relax the agent configuration so that this user can access the MIB objects from additional hosts, change the `snmpTargetAddrTMask` to perform wildcard matching of the source address of the incoming request message.

To relax the agent configuration so that this user can access the MIB objects from any host, change "`whereValidRequestsOriginate`" in the `usmUserEntry` to a dash (-).

To authorize the sending of SNMPv3 `authNoPriv Trap` messages to a user at exactly one SNMP manager station (one IP address), add the following lines to the `snmpd.cnf` configuration file together with the `usmUserEntry` for the user "`myV3AuthNoPrivUser`".

```
vacmAccessEntry myV3AuthNoPrivGroup -usm authNoPriv exact - - All
nonVolatile
vacmSecurityToGroupEntry usm myV3AuthNoPrivUser myV3AuthNoPrivGroup
nonVolatile
vacmViewTreeFamilyEntry All iso -included nonVolatile
snmpNotifyEntry myTrap whereMyNotificationsGo trap nonVolatile
snmpTargetAddrEntry myV3Manager_authNoPrivNotifications snmpUDPDomain
192.147.142.35:0 100 3 whereMyNotificationsGo myV3AuthNoPrivParams
nonVolatile 1.2.3.4:0 2048
snmpTargetParamsEntry myV3AuthNoPrivParams 3 usm myV3AuthNoPrivUser
authNoPriv non-Volatile
```

To configure additional Trap destinations (additional IP addresses where the user is authorized to operate a management station), add additional snmpTargetAddrEntry entries to the *snmpd.cnf* configuration file. For example, to authorize 192.147.142.111 as an additional Trap destination, add the following line to the `snmpd.cnf` configuration file.

```
snmpTargetAddrEntry anotherV3Manager_authNoPrivNotifications snmpUDP-
Domain 192.147.142.111:0 100 3 whereMyNotificationsGo
myV3AuthNoPrivParams nonVolatile 1.2.3.4:0 2048
```

1.6.8 Additional configuration for SNMPv3 agent entities

1.6.8.1 Configuring context names

A context is a collection MIB objects. An SNMP entity can potentially provide access to many contexts and a particular MIB object instance can exist in multiple contexts. A context is often associated with a particular physical or logical device, so a context name is an identifier to distinguish MIB object instances for one device from MIB object instances for another device.

When a management request is sent to an SNMP agent, the context name which appears in the SNMPv3 message (or which is derived from the SNMPv1 or SNMPv2c message) must exist in the agent, or the command responder application will return a `noSuchContext` error.

The configuration of context names is static and must be performed before the SNMP agent is launched for the first time.

To configure a context name, add a `vacmContextEntry` line to the `snmpd.cnf` file accordingly the following syntax:

```
vacmContextEntry <vacmContextName>
```

`vacmContextName`
is a human readable string representing the name of a context to be supported by this configuration.

Note: Note that the default context is always supported by an SNMPv3 agent.

1.6.9 Additional configuration for SNMPv1 and SNMPv2 agent entities

This section describes SNMP configuration that is required for SNMP entities that support SNMPv1 and/or SNMPv2c in addition to SNMPv3.

1.6.9.1 Configuring communities

Configuration of at least one community string must be provided for an SNMP engine to send or receive SNMPv1 or SNMPv2c messages. To configure an SNMPv1 or SNMPv2c community, add a `snmpCommunityEntry` line to the `snmpd.cnf` file accordingly the following syntax:

```
snmpCommunityEntry <snmpCommunityIndex> <snmpCommunityName> <snmpCom-
munitySecurityName> <snmpCommunityContextEngineID> <snmpCommunity-
ContextName> <snmpCommunityTransportTag> <snmpCommunityStorageType>
```

`snmpCommunityIndex`
is a human readable string which is an arbitrary index. The value of this field is unimportant, other than it must unique from other values in this field in other `snmpCommunityEntry` entries.

`snmpCommunityName`
is the community string, which may be a human readable string or a hexadecimal representation containing unprintable characters.

For example, if the community string was the word "public" with an unprintable 'bell' character (ASCII code 7) at the end, then the value of this field would be `70:75:62:6c:69:63:07` (the ASCII codes for 'p,''u,''b,''l,''i,''c,' and 'bell').

`snmpCommunitySecurityName`
is a human readable string which identifies the security name for this community string. This string should appear in at least one `vacmSecurityToGroupEntry` to assign the community string (principal) to an access control group.

`snmpCommunityContextEngineID`
is an `OctetString`, usually "`localSnmpID`".

`snmpCommunityContextName`
is the SNMPv3 context implied by the community string. A dash (-) in this field represents the default context.

`snmpCommunityTransportTag`
is a human readable string that is used to select a set of entries in the `snmpTargetAddrTable` for source address checking. Entries in the `snmpTargetAddrTable` are selected if the value of `snmpCommunityTransportTag` appears in the list of (space-separated) tags in `snmpTargetAddrTagList`. If the SNMP entity should not perform source address checking, then this field should contain a dash (-).

`snmpCommunityStorageType`
is `nonVolatile`, `permanent`, or `readOnly`.

1.6.9.2 Examples

To receive SNMPv1 requests from exactly one SNMP manager station:

```
snmpCommunityEntry 61 targetV1Community targetV1Community localSnmpID
- whereValidRequestsOriginate nonVolatile vacmAccessEntry myV1Group -
snmpv1 noAuthNoPriv exact All All All nonVolatile
vacmSecurityToGroupEntry snmpv1 targetV1Community myV1Group nonVola-
tile
vacmViewTreeFamilyEntry All iso -included nonVolatile
snmpTargetAddrEntry myV1Manager_allRequests snmpUDPDomain
192.147.142.35:0 0 0 whereValidRequestsOriginate -nonVolatile
255.255.255.255:0 2048
```

To send SNMPv1 Trap messages to exactly one SNMP manager station:

```
vacmAccessEntry myV1Group -snmpv1 noAuthNoPriv exact All All All non-
Volatile
vacmSecurityToGroupEntry snmpv1 targetV1Community myV1Group nonVola-
tile
vacmViewTreeFamilyEntry All iso -included nonVolatile
snmpNotifyEntry myTrap whereMyNotificationsGo trap nonVolatile
snmpTargetAddrEntry myV1Manager_allNotifications snmpUDPDomain
192.147.142.35:0 100 3 whereMyNotificationsGo myV1ExampleParams non-
Volatile 1.2.3.4:0 2048
snmpTargetParamsEntry myV1ExampleParams 0 snmpv1 targetV1Community
noAuthNoPriv non-Volatile
```

To receive SNMPv2c requests from exactly one SNMP manager station:

```
snmpCommunityEntry 62 targetV2cCommunity targetV2cCommunity localSnm-
pID - whereValidRequestsOriginate nonVolatile
vacmAccessEntry myV2cGroup -snmpv2c noAuthNoPriv exact All All All
nonVolatile
vacmSecurityToGroupEntry snmpv2c targetV2cCommunity myV2cGroup non-
Volatile
vacmViewTreeFamilyEntry All iso -included nonVolatile
```

```
snmpTargetAddrEntry myV2cManager_allRequests snmpUDPDomain
192.147.142.35:0 0 0 whereValidRequestsOriginate -nonVolatile
255.255.255.255:0 2048
```

To send SNMPv2c Trap messages to exactly one SNMP manager station:

```
vacmAccessEntry myV2cGroup -snmpv2c noAuthNoPriv exact All All All
nonVolatile
vacmSecurityToGroupEntry snmpv2c targetV2cCommunity myV2cGroup non-
Volatile
vacmViewTreeFamilyEntry All iso -included nonVolatile
snmpNotifyEntry myTrap whereMyNotificationsGo trap nonVolatile
snmpTargetAddrEntry myV2cManager_allNotifications snmpUDPDomain
192.147.142.35:0 100 3 whereMyNotificationsGo myV2cExampleParams non-
Volatile 1.2.3.4:0 2048
snmpTargetParamsEntry myV2cExampleParams 1 snmpv2c targetV2cCommunity
noAuthNoPriv nonVolatile
```

1.6.10 MIB

Beginning with software release 2-0-0, the AT-RG600 Series supports SNMP v1, v2c and v3 for configuration commands. Notification messages are restricted to SNMP v1.

1.6.10.1 Standard (public) MIB

The gateway supports the standard MIB defined in RFC 1213 (RFC1213-MIB) with the following limitations:

[report here a table that details which public objects are supported by each family]

OID	RFC1213	Implementation
SYSDESCR	Read-Only	Read-Only
SYSOBJECTID	Read-Only	Read-Only
SYSUPTIME	Read-Only	Read-Only
SYSCONTACT	Read-Write	Read-Write
SYSNAME	Read-Write	Read-Write
SYSLOCATION	Read-Write	Read-Write
SYSSERVICES	Read-Only	Read-Only
IFDESCR	Read-Only	Read-Only
IFTYPE	Read-Only	Read-Only

OID	RFC1213	Implementation
IFMTU	Read-Only	Read-Only
IFSPEED	Read-Only	Read-Only
IFPHYSADDRESS	Read-Only	Read-Only
IFADMINSTATUS	Read-Write	Read-Write
IFOPERSTATUS	Read-Only	Read-Only
IFLASTCHANGE	Read-Only	Read-Only
IFINOCTETS	Read-Only	Read-Only
IFINUCASTPKTS	Read-Only	Read-Only
IFINNUCASTPKTS	Read-Only	Read-Only
IFINDISCARDS	Read-Only	Read-Only
IFINERRORS	Read-Only	Read-Only
IFINUNKNOWNPROTOS	Read-Only	Read-Only
IFOUTOCTETS	Read-Only	Read-Only
IFOUTUCASTPKTS	Read-Only	Read-Only
IFOUTNUCASTPKTS	Read-Only	Read-Only
IFOUTDISCARDS	Read-Only	Read-Only
IFOUTERRORS	Read-Only	Read-Only
IFOUTQLEN	Read-Only	Read-Only
IFSPECIFIC	Read-Only	Read-Only
ATPHYSADDRESS	Read-Write	Read-Only
ATNETADDRESSS	Read-Write	Read-Only
IPFORWARDING	Read-Write	Read-Only
IPDEFAULTTTL	Read-Write	Read-Only
IPINRECEIVES	Read-Only	Read-Only
IPINHDRERRORS	Read-Only	Read-Only
IPINADDRERRORS	Read-Only	Read-Only
IPFORWDATAGRAMS	Read-Only	Read-Only

OID	RFC1213	Implementation
IPINUNKNOWNPROTOS	Read-Only	Read-Only
IPINDISCARDS	Read-Only	Read-Only
IPINDELIVERS	Read-Only	Read-Only
IPOUTREQUESTS	Read-Only	Read-Only
IPOUTDISCARDS	Read-Only	Read-Only
IPOUTNOROUTES	Read-Only	Read-Only
IPREASMTIMEOUT	Read-Only	Read-Only
IPREASMREQDS	Read-Only	Read-Only
IPREASMOKS	Read-Only	Read-Only
IPREASMFAILS	Read-Only	Read-Only
IPFRAGOKS	Read-Only	Read-Only
IPFRAGFAILS	Read-Only	Read-Only
IPFRAGCREATES	Read-Only	Read-Only
IPADENTADDR	Read-Only	Read-Only
IPADENTIFINDEX	Read-Only	Read-Only
IPADENTNETMASK	Read-Only	Read-Only
IPADENTBCASTADDR	Read-Only	Read-Only
IPADENTREASMMAXSIZE	Read-Only	Read-Only
IPROUTEDEST	Read-Write	Read-Only
IPROUTEIFINDEX	Read-Write	Read-Only
IPROUTEMET1RIC1	Read-Write	Read-Only
IPROUTEMETRIC2	Read-Write	Read-Only
IPROUTEMETRIC3	Read-Write	Read-Only
IPROUTEMETRIC4	Read-Write	Read-Only
IPROUTENEXTHOP	Read-Write	Read-Only
IPROUTETYPE	Read-Write	Read-Only
IPROUTEPROTO	Read-Only	Read-Only

OID	RFC1213	Implementation
IPROUTEAGE	Read-Write	Read-Only
IPROUTEMASK	Read-Write	Read-Only
IPROUTEMETRIC5	Read-Write	Read-Only
IPROUTEINFO	Read-Write	Read-Only
IPNETTOMEDIAIFINDEX	Read-Write	Read-Only
IPNETTOMEDIAPHYSADDRESS	Read-Write	Read-Only
IPNETTOMEDIANETADDRESS	Read-Write	Read-Only
IPNETTOMEDIATYPE	Read-Write	Read-Only
IPROUTINGDISCARDS	Read-Only	Read-Only
ICMPINMSGS	Read-Only	Read-Only
ICMPINERRORS	Read-Only	Read-Only
ICMPINDESTUNREACHS	Read-Only	Read-Only
ICMPINTIMEEXCDS	Read-Only	Read-Only
ICMPINPARMPROBS	Read-Only	Read-Only
ICMPINSRCQUENCHS	Read-Only	Read-Only
ICMPINREDIRECTS	Read-Only	Read-Only
ICMPINECHOS	Read-Only	Read-Only
ICMPINECHOREPS	Read-Only	Read-Only
ICMPINTIMESTAMPS	Read-Only	Read-Only
ICMPINTIMESTAMPREPS	Read-Only	Read-Only
ICMPINADDRMASKS	Read-Only	Read-Only
ICMPINADDRMASKREPS	Read-Only	Read-Only
ICMPOUTMSGS	Read-Only	Read-Only
ICMPOUTERRORS	Read-Only	Read-Only
ICMPOUTDESTUNREACHS	Read-Only	Read-Only
ICMPOUTTIMEEXCDS	Read-Only	Read-Only
ICMPOUTPARMPROBS	Read-Only	Read-Only

OID	RFC1213	Implementation
ICMPOUTSRCQUENCHS	Read-Only	Read-Only
ICMPOUTREDIRECTS	Read-Only	Read-Only
ICMPOUTECHOS	Read-Only	Read-Only
ICMPOUTECHOREPS	Read-Only	Read-Only
ICMPOUTTIMESTAMPS	Read-Only	Read-Only
ICMPOUTTIMESTAMPREPS	Read-Only	Read-Only
ICMPOUTADDRMASKS	Read-Only	Read-Only
ICMPOUTADDRMASKREPS	Read-Only	Read-Only
TCPRTOALGORITHM	Read-Only	Read-Only
TCPRTOMIN	Read-Only	Read-Only
TCPRTOMAX		
TCPMAXCONN		
TCPACTIVEOPENS		
TCPPASSIVEOPENS		
TCPATTEMPTFAILS		
TCPESTABRESETS		
TCPCURRESTAB		
TCPINSEGS		
TCPOUTSEGS		
TCPRETRANSSEGS		
TCPCONNSTATE	Read-Write	Read-Only

1.6.10.2 Standard traps

Only the standard ***ColdStart TRAP*** is supported.

*Note: Standard **ColdStart TRAP** can be sent only in SNMPv1 format. It is therefore necessary that the* `snmpd.cnf` *file is correcty configured to generate this trap using the SNMPv1 protocol.*

1.6.10.3 Enterprise (private) MIB

The gateway implements private objects in order to give access to specific unit configuration parameters that are not mapped in any standard MIB.

All the private MIB objects are located under the following OID: `enterprise.207.8.44`.

The following private objects are available starting from software release 2-0-0:

`sysInfo group`

This group collects generic information about the unit

OID	Max-Access	Description
SYSVENDOR	Read-Only	The vendor company name
SYSURL	Read-Only	The vendor company URL
SYSMAC	Read-Only	The unit MAC address
SYSHARDWARE	Read-Only	The unit Hardware version
SYSSOFTWARE	Read-Only	The unit Software version

`sysUsers group`

This group collects the list of the users defined in the system and the login/password for each user.

OID	Max-Access	Description
SYSUSERNAMER	Read-Only	The user name/login
SYSUSERCONFIG	Read-Write	The user may configure
SYSUSERACCESS	Read-Write	The user may configure
SYSUSERCOMMENT	Read-Write	Additional comment associated with this user
SYSUSERPASSWORD	Read-Write	The user password

`sysAdmin group`

This group collects basic objects used to force a unit restart, configuration saving, power status (only on AT-RG656 models) and a special object (sysAdminCLIEntry) that acts like a shell where is possible send CLI-like commands.

OID	Max-Access	Description
SYSRESTART	Read-Write	If set to 1 (true), this object force a system restart. The value returned by get requests is always 2 (false)
SYSCONFIGSAVE	Read-Write	If set to 1 (true) this object force a system configuration save. The value returned by get requests is always 2 (false)
SYSPOWERBACKUPSYSTEM	Read-Only	The object returns the value 1 if the backup battery system is present otherwise it returns a value of 2.
SYSPOWERBACKUPBATTERYSTATUS	Read-Only	The object returns the value 1 if the battery is charged otherwise it returns a value of 3.
SYSPOWERBACKUPPRIMARYSUPPLY	Read-Only	The object returns the value 1 if the backup battery system is correctly externally powered, otherwise it returns a value of 2.

1.6.10.3.1 Private traps

The following private (enterprise specific) traps are generated:

OID	Specific Trap Code	Description
POWERBACKPUPBATTERYON	1	This trap indicates that the external backup power supply is disconnected.
POWERBACKPUPBATTERYMISSING	2	This trap indicates that the battery backup system is disconnected.
POWERBACKPUPBATTERYLOW	3	This trap indicates that the battery is low or missing.
VOIPMGCPPROTOCOLENABLETRAP	4	This trap indicates that MGCP protocol has been enabled.
VOIPMGCPPROTOCOLDISABLETRAP	5	This trap indicates that MGCP protocol has been disabled.

OID	Specific Trap Code	Description
VOIPMGCPPROTOCOLRESTARTTRAP	6	This trap indicates that MGCP protocol has been restarted.
VOIPMGCPENDPOINTPH0RESTARTTRAP	7	This trap indicates that MGCP endpoint #1 has been restarted.
VOIPMGCPENDPOINTPH1RESTARTTRAP	8	This trap indicates that MGCP endpoint #2 has been restarted.
VOIPMGCPENDPOINTPH2RESTARTTRAP	9	This trap indicates that MGCP endpoint #3 has been restarted.
IGMPSNOOPINGVLANENABLETRAP	10	This trap indicates that igmp snooping has been enabled on a VLAN. The VLAN VID is reported inside the variable-binding field.
IGMPSNOOPINGVLANDISABLETRAP	11	This trap indicates that igmp snooping has been disabled on a VLAN. The VLAN VID is reported inside the variable-binding field.
IGMPSNOOPINGGROUPJOINTRAP	12	This trap indicates that a new multicast group has been joined. The multicast group address is reported inside the variable-binding field.
IGMPSNOOPINGGROUPLEAVETRAP	13	This trap indicates that a multicast group has been left. The multicast group address is reported inside the variable-binding field.

Note: Private TRAPs *can only be sent in SNMPv1 format. It is therefore necessary that the* `snmpd.cnf` *file is correctly configured to generate this trap using the SNMPv1 protocol.*

2. Switching

2.1 Overview

2.1.1 Layer 2 Switching in the Network

The System consists of a Layer 2 switch coupled to a Network Processor. The aggregate is viewable as a single Layer 2 switch, but this functionality is spread across the two devices - switch and the bridge - with interconnectivity being provided by the CPU port.

Rate Limiting, QOS - and VLAN Tag management is provided at the edge of the system - via port configuration.

By default - all traffic flows in one single VLAN - however an extension to this model is to use VLANs to segregate traffic flows to certain ports.

2.1.2 Documentation Structure

The Preface listed all of the iMG/RG/iBG devices and to which product category they belong. Keeping this in mind, the user can better use the remainder of this section, which is organized as follows:

- An overview of an area and its main attributes.
- The functions within an area. These are explained in some detail, usually with accompanying figures.
- A table that lists these functions and to which product category they apply. Notes help the user understand why a function may or may not be relevant.
- A table that lists the commands and to which product category they apply.
- A command reference for each command and its parameters.

Note: The command reference subsection is generic for all product categories. The user should refer to the the function and command tables to see how a command or parameter applies to a specific product.

2.2 Switching

2.2.1 Overview

The iMG/RG/iBG product includes an integrated layer 2 managed switch providing Fast Ethernet transceivers supporting 10Base-T, 100Base-TX and 1000Base-TX modes, high performance memory bandwidth (wire speed) and an extensive feature set including Rate Limiting, QoS priority, VLAN tagging and MIB counters.

The layer 2 switch uses one additional 100Mbps or 1000Mbps port as an internal port to communicate to the central processor in order to access layer 3 services such as routing, VoIP protocols, firewall and NAT security modules.

The following is the complete set of features available in the switch module:

- IEEE 802.1q tag based VLAN (up to 16 VLANs)
- VLAN ID tag/untag options, per port basis
- Programmable rate limiting, ingress port, egress port, per port basis.
- IGMP v1/v2 snooping for multicast packet filtering
- QoS packet prioritization support: per port, IEEE 802.1p and DiffServ based
- Integrated look-up engine with dedicated 1 K unicast MAC addresses
- Automatic address learning, address aging and address migration
- Full duplex IEEE 802. flow control
- Automatic MDI/MDI-X crossover for plug-and-play on all the ports

2.2.2 Layer 2 switch functional description

A summary of the general switch functions is included below.

2.2.2.1 Port Management

All ports on the switch are numbered sequentially from "lan1" up to the max number of Lan based 10/100 Ethernet ports. For the available number, please see the summary table in the preface. There can be special function LAN interfaces - such as HPNA - that are addressed where that function is discussed. The admin status of the port can be set - as well as the Port Status and Counter value being displayed.

The port speed can also be set - as one of the following options: 100MFull, 100MHalf, 10MFull, 10MHalf, Auto, Coax. The Coax mode is used when connecting an Ethernet to Coax Balun to the device.

2.2.2.2 Ingress Filtering

The infiltering parameter enables or disables Ingress Filtering of frames admitted on the ports.

If a port has only TAGGED VLANs associated with it - then when InFiltering is set to:

- ON - Only TAGGED packets with a VLAN ID matching VLANs associated with the port are admitted. UNTAGGED Packets are not admitted.
- OFF - Both TAGGED packets with a VLAN ID Matching VLANS associated with the port are admitted - as well as UNTAGGED packets. UNTAGGED Packets are tagged with the Default VLAN ID.

2.2.2.3 Address management

The primary function of the layer 2 switch is to receive good packets from the ports, process them and forward them to the appropriate ports for transmission. This frame processing involves the Ingress Policy, Queue Controller, Output Queues and Egress Policy.

The normal packet flow involves learning how to switch packets only to the correct ports. The switch learns which port and end station is connected to by remembering each packet's Source Address along with the port number on which the packet arrived - and the vlan that it is on.

When a packet is directed to a new, unlearned MAC address, the packet is flooded out of all the ports (as long as they belong on the same VLAN) except for the one on which it arrived. Once a MAC address/port number is learned, all future packets directed to that end station's MAC addresses are directed to the learned port number only. This ensures that the packet is sent to the correct end station. This table can be displayed via the CLI

The address database is stored in the embedded switch memory and has a default aging time of about 300 seconds (5 minutes). If no packets are received from that MAC Address during that aging interval, then the address is purged from the database. If a MAC Address is received from a different port during this time, then the MAC address is learned on that new port and all traffic is then routed to that new port.

The number of MAC addresses that can be learned differs between devices. (Kendin, BCM, Marvell, Marvell Gig)

2.2.2.4 Rate limiting support

The integrated layer 2 switch supports hardware rate limiting on receive and transmit independently on a per port basis. The rate limiting applies to all the frame types: unicast, broadcast and multicast.

Some devices do provide the ability to rate limit the Multicast and Broadcast traffic. (BCM and Gig Marvell)

If the number of bytes exceeds the programmed limit, the switch will stop receiving or transmitting packets on the port. In the transmit direction, extra packets are placed in one or more FIFO queues and sent as soon as possible given the configured limit. Note that when multiple queues are configured, the highest priority queue is emptied first.

In the receive direction, on some devices, there is an option provided for flow control to prevent packet loss. In this case, if the configured limit is reached, and Flow Control is enabled, then a PAUSE frame will be sent to the peer device. This will stop transmission of packets until the Gateway is ready to receive packets again.

2.2.2.5 Loop Detection

Loop detection is a feature available at layer 2 used to disable automatically one or more switch ports when a loop is verified on one or more of these ports.

Ethernet loops are likely to happen when a Ethernet-to-Coax balun is used in installations where there are appliances connected to coax cable that need to the6 ethernet ports. In this case, if the coax cable is not properly terminated, a signal reflection is generated on the coax cable segment and then reported to the ethernet segment too causing high network degradation.

To detect a loop on ethernet ports, the Gateway periodically sends a "special" ping message. If the gateway receives the same ping message back, it means that a loop is present. In this case the Gateway disables all the traffic to/from the port (except the "special" ping) until the loop has been removed.

2.2.2.6 Layer 3 Routing Rate Limiting

The integrated layer 2 switch can limit traffic that goes to the Gateway network processor where routing tasks need to be performed.

Limitation on the maximum routing rate is necessary to preserve system resources for high priority tasks like VoIP and IGMP.

If the number of frames per seconds that need to be routed to the network processor are higher than the selected maximum rate, the layer 2 switch discards packets addressed to the network processor in order to force the average traffic rate to be below the target rate.

2.2.2.7 Quality of Service Classification

QoS switching policy is performed by the Queue Controller. The priority of a frame is determined in priority order by:

- The IEEE 802.3ac Tag containing IEEE 802.1p priority information: this IEEE 802.1p priority information is used in determining frame priority when IEEE 802.3ac tagging is enabled on the port.
- The IPv4 Type of Service (TOS)/DiffServ field when enabled on the port. IPv4 priority classification can be configured on a port basis to have a higher priority then IEEE Tag.

The user can enable these classification individually or in combination.

All untagged frames entering a port have their priority set to the port's default priority. This priority is then used to manage the traffic from that port.

There are two different models in place:

1. A two Queue scheme- where by the user specifies which Priority settings go into the high priority queue and which go into the low queue.
2. A four Queue scheme where the user actually maps the different priority values to one of the four queues.

Highest priority queues are emptied first before the lower priority queues…and as such, it is possible for the low priority traffic to get starved out.

The integrated layer 2 switch supports two ***Class of Service*** (CoS) mechanisms: ***IEEE 802.1p*** tagging (Layer 2) and ***Differentiated Services*** (DS) as an advanced architecture of ToS (Layer 3).

2.2.2.7.1 802.1p traffic priority

The IEEE 802.1p signalling technique is an IEEE endorsed specification for prioritizing network traffic at the data-link/MAC sub-layer (OSI Reference Model Layer 2).

IEEE 802.1p is a spin-off of the IEEE 802.1q (VLAN tagging) standard and they work in tandem (see Figure 1).

The 802.1q standard specifies a VLAN tag that appends to a MAC frame. The VLAN tag carries VLAN information. The VLAN tag has two parts: The VLAN ID (12-bit) and User Priority (3-bit). The User Priority field was never defined in the VLAN standard. The 802.1q implementation defines this prioritizing field.

Switches, routers, servers, even desktop systems, can set these priority bits in the three-bit user priority field, which allows packets to be grouped into various traffic classes. If a packet is received that does not have this tag added, then the switch adds it to the packet and uses the default priority associated with the port.

In the two queue systems, the user priority field in the TAG header is compared with an internal value inthe switch called the base priority - and all values equal or greater to this base priority are put into the high priority egress queue - while all others are put into the low priority queue.

In the four queue systems, the value in the user priority is used to determine which queue to place the packet into directly. This mapping is configurable.

2.2.2.7.2 Differentiated services code point (DSCP)

The IEEE 802.1p signalling technique is an IEEE endorsed specification for prioritizing network traffic.

The DSCP octet in the IP header classifies the packet service level. The DSCP replaces the ToS Octet in the IPv4 header (see Figure 2-1).

Currently, only the first six bits are used. Two bits of the DSCP are reserved for future definitions. This allows up to 64 different classifications for service levels.

In the two queue systems, the DSCP field is compared with an internal value in the switch called the base priority - and all values equal or greater to this base priority are put into the high priority egress queue - while all others are put into the low priority queue.

In the four queue systems, the value in the user priority used to determine which queue to place the packet into directly. This mapping is configurable.

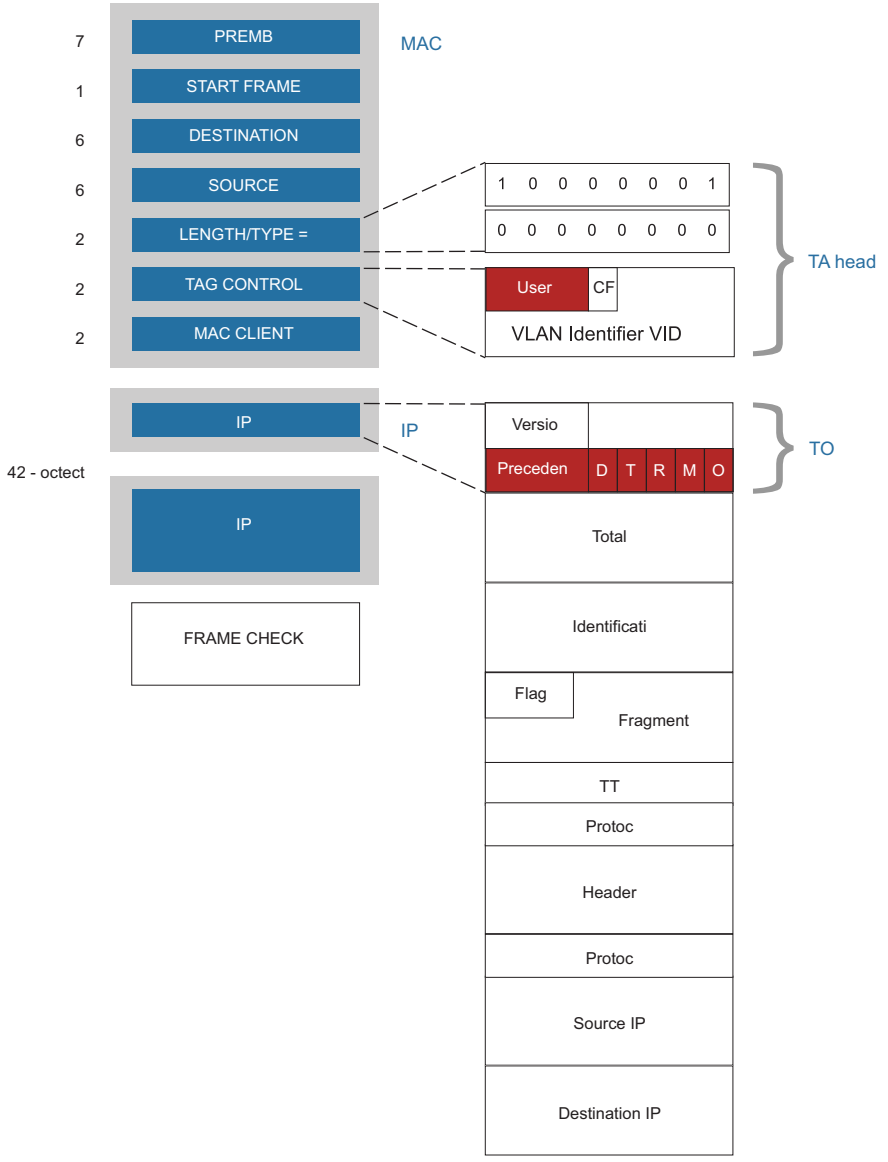


FIGURE 2-1 IP packet overview

2.2.2.8 Power Conservation Mode

In order to provide longer back-up battery life during power-failure situations, some devices support a mode in which -30 minutes after an AC Power failure is detected, all but the Lan1 interface will be powered off. This enables the device to reduce battery consuption.

2.2.2.9 Port Diagnostics

On some devices, it is possible to perform diagnostics on the physical wiring that is connected to the Gateway's ethernet port. This is in effect a TDR mechanism - that can detect opens, shorts or good connections - and can also determine the distance to the terminating point.

2.2.3 Functional Differences for Switching in Product Categories

The table below is intended to identify what is common amongst the product families - as well as where there are differences - to highlite those differences. To determine which family your device belongs to - please refer to the preface.

TABLE 2-1 Functional Mapping for Switching

Option	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
Port Management	15	15, 12	15, 21	12, 15	12, 15, 18	12, 15, 16	15, 17	12, 15, 17	12, 15
Ingress Filtering	13	X	X	X	X	X	13	X	X
Address management	1	3	3	3	2	2	1	2	2
Rate limiting support	10	7, 14, 19	11, 14, 19	7, 14, 19	8, 9	7, 8, 9, 14, 20, **22**	10	8, 9	8, 9
Loop Detection	X		X				X		
Layer 3 Routing Rate Limiting						6			
Quality of Service Classification	4	5	**5**	5	5	5	4	5	5
802.1p traffic priority	X	X	X	X	X	**23**	X	X	X
Differentiated services code point (DSCP)	X	X	X	X	X	X	X	X	X
Power Conservation Mode		X				X			
Port Diagnostics						X			

1. Supports 1K MAC Addresses
2. Supports 2K MAC Addresses
3. Supports 4K MAC Addresses
4. Supports 2 Queues

5. Supports 4 Queues
6. Fixed value that is not provisionable - only supported on 7x6MOD
7. Up to thirty different rate limits are supported: 128Kbps, 256Kbps, 512Kbps, 756Kbps, 1Mbps, 1.5Mbps 2Mbps, 3Mbps, 4 Mbps, 5Mbps, 6Mbps, 7Mbps, 8Mbps, 9Mbps, 10Mbps, 12Mbps, 14Mbps, 16Mbps, 18Mbps, 20Mbps, 25Mbps 30Mbps, 35Mbps, 40Mbps, 45Mbps, 50Mbps, 60Mbps, 70Mbps, 80Mbps and 90Mbps independently on each port and on the frame direction: Tx or Rx
8. On non-gig capable versions - Up to seven different rate limits are supported: 128Kbps, 256Kbps, 512Kbps, 1Mbps, 2Mbps, 4 Mbps and 8Mbps independently on each port and on the frame direction: Tx or Rx. If additional granularity or higher limits are needed, please see the section on Network Processor Based Rate Limiting.
9. On Non Gig capable versions - If it is necessary to rate limit TCP traffic - then it is recommended to use the Network Processor Based Rate Limiting. Rate Limiting in the RX direction can result in packet loss - which results in lower throughput than configured for TCP sessions.
10. Rate limiting on these devices is based on 64Kb granularity - the user is able to enter values between 0 and 100Mbps
11. Rate limiting on these devices is based on 64Kb granularity - the user is able to enter values between 0 and 100Mbps.
12. Coax Mode is not supported.
13. When assigning VLANs - these ports can be defined as TAGGED or UNTAGGED - it is not possible to support both.
14. Supports BroadCast Rate Limiting and MultiCast Rate Limiting
15. Ports supported are from Lan1 up to a max of LAN6 - depending on the number of Ethernet ports available.
16. Additional ports can be present depending on the Module added - for example hpna - if the HPNA Lan module is present; CESC and CESD if the T1/E1 Circuit emulation module is present; Glan if the Gig WAN Module is present. All these ports can be managed like a normal LAN port - but it is not recommended that any changes be made to the CESC port.
17. It is possible ot use the LAN4 port as a WAN port.
18. It is possible to use the LAN6 port as a Wan port - if the Fiber port is not being used.
19. Supported Rate Limits for Broadcast and multicast data are 3.5%, 5%, 10% and 20% or the total port capacity.
20. On Gig Enabled devices, Supported Rate Limits for Broadcast and Multicast data are 128Kbps, 256Kbps, 512Kbps, 756Kbps, 1Mbps, 1.5Mbps, 2Mbps, 3Mbps, 4Mbps, 5Mbps, 6Mbps, 7Mbps, 8Mbps, 9Mbps, 10Mbps 12Mbps, 14Mbps, 16Mbps, 18Mbps, 20Mbps, 25Mbps, 30Mbps, 35Mbps, 40Mbps, 45Mbps, 50Mbps, 60Mbps, 70Mbps, 80Mbps, 90Mbps.
21. Supports FLOW and JAMMING Control of flow-control options.
22. **On Gig Ports the same rates are supported below 100Mbps. In addtion the following rates are supported: 100Mbps, 150MBps, 200Mbps, 250Mbps, 300Mbps, 350MBps, 400Mbps, 450Mbps, 500Mbps, 600Mbps, 700Mbps, 800Mbps, 900Mbps.**

23. **For 6x6MOD and 7x6MOD devices when 802.1P is Disabled, the P-Bit Setting on any received packet is converted to 0. So if a packet is received with a P-Bit setting of 3 - the P-Bit of the packet when transmitted is 0. To assist in managing the implications of this - the default setting for the WAN and the CPU port 802.1p port attributes is Enabled.**

2.2.4 Switch command reference

This section describes the commands available on configure and manage switch ports and the address look up table.

Throughout are references back to 2.2.3

2.2.4.1 Switch CLI commands

The table below lists the ***switch*** commands provided by the CLI:

TABLE 2-2 ***Switch*** commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SWITCH DIAGNOSE PORT						X			
SWITCH DISABLE AGEINGTIMER	X		X				X		
SWITCH DISABLE LEARNING	X		X				X		
SWITCH DISABLE LOOPDETECTION	X		X				X		
SWITCH DISABLE PORT	X		X				X		
SWITCH ENABLE AGEINGTIMER	X		X				X		
SWITCH ENABLE LEARNING	X		X				X		
SWITCH ENABLE LOOPDETECTION	X		X				X		
SWITCH ENABLE PORT	X		X				X		
SWITCH LIST PORTS		X		X	X	X		X	X
SWITCH RESET	X	X	X	X	X	X	X	X	X
SWITCH RESET COUNTERS	X		X				X		
SWITCH RESET PORT	X	X	X	X	X	X	X	X	X
SWITCH SET 802.1P PRIORITY			X						
SWITCH SET AGE-TIMER		X		X	X	X		X	X

TABLE 2-2 *Switch* commands **(Continued)**

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SWITCH SET AGING-TIME		X		X	X	X		X	X
SWITCH SET AGINGTIMER	X		X				X		
SWITCH SET LEARNING		X		X	X	X		X	X
SWITCH SET LOOPDETECTION	X		X				X		
SWITCH SET PORT 802.1P		X		X	X	X		X	X
SWITCH SET PORT BROADCASTLIMIT		X	X	X		X			
SWITCH SET PORT DEFAULTPRIORITY	X	X	X	X	X	X	X	X	X
SWITCH SET PORT DEFAULTVID	X	X	X	X	X	X	X	X	X
SWITCH SET PORT DSCP		X		X	X	X		X	X
SWITCH SET PORT DSCP/NODSCP	X		X				X		
SWITCH SET PORT FLOW	X						X		
SWITCH SET PORT FLOWCONTROL		X		X	X	X		X	X
SWITCH SET PORT INFILTERING	X	X	X	X	X	X	X	X	X
SWITCH SET PORT MULTICASTLIMIT		X	X	X		X			
SWITCH SET PORT QOS/NOQOS	X		X				X		
SWITCH SET PORT RCVLIMIT	X	X	X	X	X	X	X	X	X
SWITCH SET PORT RCVLIMIT-HIGH	**X**						**X**		
SWITCH SET PORT RCVLIMIT-LOW	**X**						**X**		
SWITCH SET PORT SPEED	X	X	X	X	X	X	X	X	X
SWITCH SET PORT STATUS		X		X	X	X		X	X
SWITCH SET PORT TRSLIMIT	X	X	X	X	X	X	X	X	X
SWITCH SET PORT TRSLIMIT-HIGH	**X**						**X**		
SWITCH SET PORT TRSLIMIT-LOW	**X**						**X**		
SWITCH SET PORT TRSLIMIT-HIGH	X		X				X		
SWITCH SET QOS 802.1P		X		X	X	X		X	X
SWITCH SET QOS DSCP		X		X	X	X		X	X

TABLE 2-2 *Switch* commands **(Continued)**

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SWITCH SET QOS PRIORITY	X		X				X		
SWITCH SET ROUTING-LIMIT			X						
SWITCH SHOW	X	X	X	X	X	X	X	X	X
SWITCH SHOW 802.1P			X						
SWITCH SHOW FDB	A	B	A	B	B	B	A	B	B
SWITCH SHOW PORT	X	X	X	X	X	X	X	X	X
SWITCH SHOW QOS	X		X				X		
SWITCH SHOW QOS 802.1P		X		X	X	X		X	X
SWITCH SHOW QOS DSCP		X		X	X	X		X	X

2.2.4.1.1 SWITCH DIAGNOSE PORT

Syntax `SWITCH DIAGNOSE PORT`

Description This command executes the Time Domain Reflection test - that is used to determine whether or not an Etherenet Cable connected to the port has a fault..

The results are whether or not there is an “open”, “short” or “good term”.for each pair. It also prints the distance to the fault if the result is not “good term”. The accuracy is to within approximately 10%.

Options None.

Example --> switch diagnose port lan6

```
Port 2 Tx: open [0ft] Rx: open [0ft]
```

2.2.4.1.2 SWITCH DISABLE AGEINGTIMER

Syntax `SWITCH DISABLE AGEINGTIMER`

Description This command stops the aging timer used by the look up engine to remove expired FDB entries.

If the ageing timer is disabled the look up entries in the FDB are kept permanently until the SWITCH ENABLE AGEINGTIMER command entered or the switch is reset.

To show the current switch status, use the SWITCH SHOW command.

Example `switch disable ageingtimer`

See also `SWITCH ENABLE AGEINGTIMER`
`SWITCH SHOW`

2.2.4.1.3 SWITCH DISABLE LEARNING

Syntax `SWITCH DISABLE LEARNING`

Description This command stops the learning engine used to update the look up table when frame are received from new *Source Addresses*.

To restore the learning process, use the SWITCH ENABLE LEARNING command.

To show the current switch status, use the SWITCH SHOW command.

Example `switch disable learning`

See also `SWITCH ENABLE LEARNING`
`SWITCH SHOW`

2.2.4.1.4 SWITCH DISABLE LOOPDETECTION

Syntax `SWITCH DISABLE LOOPDETECTION`

Description This command stops the loop detection on the Ethernet ports. Special "ping" messages used to detect loop are stopped.

Any port that was set to coax mode still remain configured in this mode forcing the port speed to 10M Full Duplex.

To show the current port status, use the SWITCH SHOW command.

Example `switch disable loopdetection`

See also `SWITCH ENABLE LOOPDETECTION`
`SWITCH SHOW`

2.2.4.1.5 SWITCH DISABLE PORT

Syntax `SWITCH DISABLE PORT <port-name> [FLOW JAMMING]`

Description This command disables the selected switch port, or disables a flow control mechanism on the port.

If jamming is specified the jamming signal used for flow control on half duplex ports will be disabled.

To show the current port status, use the SWITCH SHOW PORT command.

Please see notes under Port management for the applicability of the FLOW and JAM-MING options.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A

Example `switch disable port lan1`

See also `SWITCH ENABLE PORT`
`SWITCH SHOW PORT`

2.2.4.1.6 SWITCH ENABLE AGEINGTIMER

Syntax `SWITCH ENABLE AGEINGTIMER`

Description This command restarts the aging timer used by the look up engine to update the aging of FDB entries.

To show the current switch status, use the SWITCH SHOW command.

Example `switch enable ageingtimer`

See also `SWITCH DISABLE AGEINGTIMER`
`SWITCH SHOW`

2.2.4.1.7 SWITCH ENABLE LEARNING

Syntax `SWITCH ENABLE LEARNING`

Description This command restarts the learning process used by the look up engine to update the FDB when frames from new addresses are received.

To show the current switch status, use the SWITCH SHOW command.

Example `switch enable learning`

See also `SWITCH DISABLE LEARNING`
`SWITCH SHOW`

2.2.4.1.8 SWITCH ENABLE LOOPDETECTION

Syntax `SWITCH ENABLE LOOPDETECTION`

Description This command turns on the loop detection feature on the switch. The Residential Gateway will start sending special "ping" messages to all the switch ports configured as "coax".

All the switch ports having a speed valued different from "coax" will not be involved in the loop detection process.

To add an Ethernet port to the list of ports where loop detection is controlled, use the SWITCH SET PORT SPEED COAX command.

Example `switch enable loopdetection`

See also `SWITCH DISABLE LOOPDETECTION`
`SWITCH SHOW`

2.2.4.1.9 SWITCH ENABLE PORT

Syntax `SWITCH ENABLE PORT <port-name> [FLOW [JAMMING] ]`

Description This command enables the selected switch port.

If SWITCH ENABLE PORT FLOW is entered, pause flow control is enabled when the port speed is configured to full duplex.

If SWITCH ENABLE PORT FLOW JAMMING is entered, jamming flow control is enabled when the port speed is configured to half duplex.

To show the current port status, use the SWITCH SHOW PORT command.

Please see notes under Port management for the applicability of the FLOW and JAMMING options.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A

2.2.4.1.10 SWITCH LIST PORTS

Syntax `SWITCH LIST PORTS`

Description This command current status of all the Ethernet Ports on the device.

The port ID and current state are also displayed - this allows the user to gather a broad view of the state of the system.

Options None.

Example--> switch list ports

```
Switch Ports:

   Name    | Port ID   |   State   | Connected |   Speed
-----------|-----------|-----------|-----------|-----------
lan1       | 4         | Enabled   | false     | N/C
lan2       | 1         | Enabled   | false     | N/C
lan3       | 5         | Enabled   | false     | N/C
lan4       | 0         | Enabled   | false     | N/C
lan5       | 3         | Enabled   | false     | N/C
lan6       | 2         | Enabled   | false     | N/C
cpu        | 6         | Enabled   | true      | 100F
-------------------------------------------------------------
```

2.2.4.1.11 SWITCH RESET

Syntax `SWITCH RESET [PORT <port-name> [COUNTERS]]`

Description This command resets completely the switch .

All internal switch counters are reset and FDB entries removed.

Options None.

Example `switch reset`

```
    --> switch reset
```

2.2.4.1.12 SWITCH RESET COUNTERS

Syntax `SWITCH RESET COUNTERS`

Description This command resets completely the switch counters.

Options None

Example switch reset counters

2.2.4.1.13 SWITCH RESET PORT

Syntax `SWITCH RESET PORT <port-name> COUNTERS`

Description This command resets the counters of the switch port if a port is specified.

Only the counters related to the selected port are reset without removing any FDB entries.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A

Example switch reset port lan1 counters

See also `switch show`

2.2.4.1.14 SWITCH SET 802.1P PRIORITY

Syntax `SWITCH SET 802.1P <802.1P_value> PRIORITY <queue>`

Description This command is used to map an incoming tagged frame with a specific 802.1p value in the priority field of the tag header into one of the four egress queues available on the switch. To show the current 802.1p value/queue mapping, use the SWITCH SHOW 802.1p command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)..

Option	Description	Default Value
802.1P_value	The value of the 802.1p field used to map incoming frames into a well defined outgoing queue. Possible values are from 0 to 7.	N/A
queue	The name of the egress priority queue where frame will be forwarded. Allowed values are: low (lowest priority queue) med-low med-high high (highest priority queue).	low for 802.1p values 0 to 3 high for 802.1p values 4 to 7

Example swtich set 802.1P 0 PRIORITY

2.2.4.1.15 SWITCH SET AGE-TIMER

Syntax `SWITCH SET AGE-TIME <agetimer>`

Description This command sets the value of the ageing timer, after which an un-refreshed dynamic entry in the ***Forwarding Database*** is automatically removed.

Acceptable values are from 16 secs to 4080 secs.

To show the current switch status, use the SWITCH SHOW command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Agetimer	Number of seconds. (16 to 4080)	304 (secs)

Example --> switch set ageingtimer 180

See also `switch show`

See also `SWITCH SHOW PORT`

2.2.4.1.16 SWITCH SET AGING-TIME

Syntax `SWITCH SET AGING-TIME { Enabled | Disabled }`

Description This command enables or disables the aging time process. Once disabled all the FDB entries already learned are kept until aging-time is re-enabled or a switch reset command is entered.

To show the current switch status, use the SWITCH SHOW command.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Enabled | Disabled	When Enabled, the aging time process will flush out any entry older than the age-timer value. When Disabled, the aging time process keep all the entries already learned. No additional entries are learned in this status.	Enabled

Example --> switch set aging-time disabled

See also `switch show`

2.2.4.1.17 SWITCH SET AGINGTIMER

Syntax `SWITCH SET AGINGTIMER [fast|normal|value] <agetimer>`

Description This command sets the value of the ageing timer, after which an un-refreshed dynamic entry in the ***Forwarding Database*** is automatically removed.

FAST sets the aging timer to 800 µSec, while NORMAL sets the aging timer to 300 Sec

Acceptable values are from 16 secs to 4080 secs.

To show the current switch status, use the SWITCH SHOW command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Agetimer	Number of seconds. (16 to 4080)	none

Example --> switch set ageingtimer 180

See also `switch show`

2.2.4.1.18 SWITCH SET LEARNING

Syntax `SWITCH SET LEARNING { Enabled | Disabled }`

Description This command enables or disables the learning process on the switch.

When learning is disabled, any frame having a new source mac address will not be stored on the switch fdb. The existing fdb entries instead will be flushed out accordingly to the age-timer value.

To show the current switch status, use the SWITCH SHOW command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Enabled | Disabled	When Enabled, the learning engine learns source addresses of incoming frames. When Disabled, no learning process will take place.	Enabled

Example --> switch set learning disabled

2.2.4.1.19 SWITCH SET LOOPDETECTION

Syntax `SWITCH SET LOOPDETECTION POLLINGTIME <polling-time>`

Description This command changes the rate of the "special" ping messages used to detect loop condition on one or more Ethernet ports.

If more then one port is configured for loop detection, each port will generate a "ping" message rate equal to the polling time multiplied by the number of "coax" ports.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
polling-time	The loop detection "ping" rate in milliseconds. Available values are between 50msec up to 5000 msec.	50

Example `switch set loopdetection pollingtime 100`

See also `switch show`

2.2.4.1.20 SWITCH SET PORT 802.1P

Syntax `SWITCH SET PORT <portname> 802.1P { Enabled | Disabled }`

Description This command enables the support of 802.1p priority field on the incoming frames.

This command is usually used in conjunction with the switch set qos 802.1p command to specify on which egress queue an incoming tagged frames having a specific value on the priority field will be forwarded.

When 802.1p is is disabled, no specific forwarding policy is applied on incoming tagged frames except the normal forwarding process.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A

Option	Description	Default Value
Enabled | Disabled	When Enabled, the incoming packets are placed in the appropriate priority queue based on the P-Bit setting. When Disabled, there is no prioritization based on P-Bit.	Disabled
default_vlanid	The VLAN identifier to be associated to untagged frames that arrive to this port. This valid range is from 1 to 4095.	Disabled

Example --> switch set port lan1 802.1p Enabled

See also SWITCH SHOW PORT

2.2.4.1.21 SWITCH SET PORT BROADCASTLIMIT

Syntax SWITCH SET PORT <portname> BROADCASTLIMIT < bcastlimit >

This command specifies the ingress data rate limit for broadcast traffic. These limits apply only to broadcast frame types entering on the selected switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
bcastlimit	The maximum bit rate for broadcast traffic that is allowed on a switch port in the receive direction. See Section 2.3 for a list of possible values - depending on product family.	None

Example --> switch set port lan8 broadcastlimit 4Mbps

2.2.4.1.22 SWITCH SET PORT DEFAULTPRIORITY

Syntax `SWITCH SET PORT <portname> DEFAULTPRIORITY <priority>`

Description This command sets the priority value on the 802.1p priority field for all the frames that arrive on the switch port as untagged frames.

This command works only if the 802.1p support has been previously enabled via the switch set port 802.1p enable command.

When an untagged frame arrives to a port where the default priority value has not been specified, and the egress port is tagged, the 802.1p priority field of the outgoing frame frame will be set to 0.

This command can be used to set the port priority, with the priority queue for the specified port depending on the queue that the port is associated with. This association is shown using the SWITCH SHOW 802.1p command. Refer to the example, below, where using the example command `switch set port lan1 defaultopriority 5`, the port priority for lan1 will be set for 5. To know the priority queue for lan1, use the command `SWITCH SHOW 802.1p`. This shows that the queue associated to the value 5 is H (high priority) so lan1 port outgoing packets will be put in the high priority queue.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
defaultpriority	The default priority value to be set when untagged frames are forwarded to a tagged egress port. Valid range is 0 to 7.	0

Example --> switch set port lan1 defaultopriority 5

```
-> switch show 802.1p
802.1p Queue Map
-------------------------------------------------------------------
PID   |  0 1 2 3 4 5 6 7
       -----------------
QUEUE |  . . . . H H H H
-------------------------------------------------------------------
```

See also `SWITCH SHOW PORT`

2.2.4.1.23 SWITCH SET PORT DEFAULTVID

Syntax `SWITCH SET PORT <portname> DEFAULTVID { default_vlanid }`

Description This command specifies the vlan identifier used as IEEE Tagged VID added during egress to untagged frames that arrived at this port. Frames will be processed as frames.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
default_vlanid	The VLAN identifier to be associated to untagged frames that arrive to this port. This valid range is from 1 to 4095.	N/A

Example --> switch set port lan1 defaultvid 100

See also `SWITCH SHOW PORT`

2.2.4.1.24 SWITCH SET PORT DSCP

Syntax `SWITCH SET PORT <portname> DSCP { Enabled | Disabled }`

Description This command enable the support of DSCP IP field on the incoming frames.

This command is usually used in conjunction with the switch set qos dscp command to specify on which egress queue an incoming frames having a specific value on the DSCP field will be forwarded.

When DSCP support is disabled, no specific forwarding policy is applied on incoming frames except the normal forwarding process.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
Enabled | Disabled	When Enabled, the support of DSCP IP field management is active. When Disabled, any QoS policy based on DSCP field is disabled.	Disabled

Example --> switch set port lan1 DSCP Enabled

2.2.4.1.25 SWITCH SET PORT DSCP/NODSCP

Syntax `SWITCH SET PORT <portname> { dscp | nodscp }`

Description This command enable/disable the DSCP based priority on the selected switch port .

When DSCP based priority is enabled, the DSCP value of each incoming frame is search in the switch DSCP table to check if the frame must be forwarded to High or Low Priority egress queue. If the switch DSCP table reports that for a specific DSCP value the frame must be managed as high priority frame, than the switch will forward the frame to the high priority queue otherwise the frame will be forwarded to the low priority queue.

To change the switch DSCP table use the SWITCH SET QOS PRIORITY command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
dscp | nodscp	When dscp, the support of DSCP IP field management is active. When nodscp, any QoS policy based on DSCP field is disabled.	nodscp

Example `switch set port wan dscp`

See also `SWITCH SHOW PORT`
`SWITCH SET QOS PRIORITY`

2.2.4.1.26 SWITCH SET PORT FLOW

Syntax `SWITCH SET PORT <portname> FLOW { Enabled | Disabled }`

Description This command enables/disables full duplex flow control on the selected switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
Enabled | Disabled	When Enabled, the flow control support is active. When Disabled, the flow control support is deactivated.	Enabled

Example --> switch set port wan flow Enabled

See also `SWITCH SHOW PORT`

2.2.4.1.27 SWITCH SET PORT FLOWCONTROL

Syntax `SWITCH SET PORT <portname> FLOWCONTROL { Enabled | Disabled }`

Description This command enables/disables full duplex flow control on the selected switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
Enabled | Disabled	When Enabled, the flow control support is active. When Disabled, the flow control support is deactivated.	Enabled

Example --> switch set port wan flowcontrol enabled

See also

See also `SWITCH SHOW PORT`

2.2.4.1.28 SWITCH SET PORT INFILTERING

Syntax `SWITCH SET PORT <portname> INFILTERING { Enabled | Disabled }`

Description This command enables/disables the infiltering process on incoming tagged frames.

When infiltering is enabled, an incoming tagged frame having a VLAN identifier different from the vlan where the switch port is configured will be dropped.

When infiltering is disabled, an incoming tagged frame having a VLAN identifier different from the vlan where the switch port is configured is accepted and will be processed accordingly to the standard forwarding process.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
Enabled | Disabled	When Enabled, ingress filtering support is active. When Disabled, ingress filtering is deactivated.	Enabled

Example --> switch set port lan1 infiltering disabled

See also `SWITCH SHOW PORT`

2.2.4.1.29 SWITCH SET PORT MULTICASTLIMIT

Syntax `SWITCH SET PORT <portname> MULTICASTLIMIT < mcastlimit >`

Description This command specifies the ingress data rate limit for multicast traffic. These limits apply only to multicast frame types entering on the selected switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
mcastlimit	The maximum rate if ingress multicast traffic that will be accepted on the switch port. See Section 2.3 for a list of possible values - depending on product family.	none

2.2.4.1.30 SWITCH SET PORT QOS/NOQOS

Syntax `SWITCH SET PORT <portname> {QOS | NOQOS}`

Description This command enables/disables the 802.1p scheme priority on the selected switch port.

When 802.1p scheme priority is enabled, the 802.1p priority field value of each incoming frame is compared with the switch base priority. If it is higher, the switch will forward the frame to the high priority queue otherwise the frame will be forwarded to the low priority queue.

To change the switch base priority use the SWITCH SET PRIORITY command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
qos | noqos	When qos, the support of 802.1p IP field management is active. When noqos, any QoS policy based on 802.1p field is disabled.	noqos

Example --> switch set port wan qos

See also `SWITCH SHOW PORT`
`SWITCH SET PRIORITY`

2.2.4.1.31 SWITCH SET PORT RCVLIMIT

Syntax `SWITCH SET PORT <portname> RCVLIMIT < rcvlimit >`

Description This command specifies the ingress data rate limit. These limits apply to all frame types entering on the selected switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
rcvlimit	The maximum bit rate allowed on a switch port in the receive direction. See Section 2.3 for a list of possible values - depending on product family.	None

Example --> switch set port lan8 rcvlimit 4Mbps

2.2.4.1.32 SWITCH SET PORT RCVLIMIT-HIGH

Syntax `SWITCH SET PORT <portname> RCVLIMIT-HIGH < rcvlimit >`

Description This command specifies the ingress data rate limit for high priority traffic. These limits apply to all frame types entering on the selected switch port that are high priority.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
rcvlimit	The maximum bit rate allowed on a switch port in the receive direction. See Section 2.3 for a list of possible values - depending on product family.	None

Example --> switch set port lan8 rcvlimit-high 4Mbps

2.2.4.1.33 SWITCH SET PORT RCVLIMIT-LOW

Syntax `SWITCH SET PORT <portname> RCVLIMIT-LOW < rcvlimit >`

Description This command specifies the ingress data rate limitfor the low priority traffic. These limits apply to all frame types entering on the selected switch port that are categorized as low prirority.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
rcvlimit	The maximum bit rate allowed on a switch port in the receive direction. See Section 2.3 for a list of possible values - depending on product family.	None

Example --> switch set port lan8 rcvlimit-low 4Mbps

2.2.4.1.34 SWITCH SET PORT SPEED

Syntax `SWITCH SET PORT <portname> SPEED <port-speed>`

Description This command set the speed value and mode on the selected switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Port-name	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
port-speed	The port speed and mode. Allowed values are: AUTO (Autonegotiate) COAX (10Mbps Half Duplex) 10H (10Mbps Half Duplex) 10F (10Mbps Full Duplex) 100H (100Mbps Half Duplex) 100F (100Mbps Full Duplex) 1000H (1000Mbps Half Duplex) 1000F (1000Mbps Full Duplex)	AUTO

Example --> switch set port lan1 speed 10F

See also SWITCH SHOW PORT

2.2.4.1.35 SWITCH SET PORT STATUS

Syntax `SWITCH SET PORT <portname> STATUS { Enabled | Disabled }`

Description This command disables or enables the switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
portname	he name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
Enabled | Disabled	When Enabled, the link is up and traffic can be sent or received to/from the switch port. When Disabled, the link is forced to be down.	Enabled

Example --> switch set port lan1 status Disabled

2.2.4.1.36 SWITCH SET PORT TRSLIMIT

Syntax `SWITCH SET PORT <portname> TRSLIMIT < trslimit >`

Description This command specifies the ingress data rate limit. These limits apply to all frame types entering on the selected switch port.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
portname	he name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
trslimit	The maximum bit rate allowed on a switch port in the transmit direction. See Section 2.3 for a list of possible values - depending on product family.	None

Example --> switch set port lan1 trslimit 8Mbps

2.2.4.1.37 SWITCH SET PORT TRSLIMIT-HIGH

Syntax `SWITCH SET PORT <portname> TRSLIMIT-HIGH < trslimit >`

Description This command specifies the ingress data rate limit for high priority packets. These limits apply to all frame types entering on the selected switch port that are high priority.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
portname	he name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
trslimit	The maximum bit rate allowed on a switch port in the transmit direction. See Section 2.3 for a list of possible values - depending on product family.	None

Example --> switch set port lan1 trslimit-high 8Mbps

2.2.4.1.38 SWITCH SET PORT TRSLIMIT-LOW

Syntax `SWITCH SET PORT <portname> TRSLIMIT-LOW < trslimit >`

Description This command specifies the ingress data rate limit for low priority packets. These limits apply to all frame types entering on the selected switch port that are low priority.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
portname	he name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A
trslimit	The maximum bit rate allowed on a switch port in the transmit direction. See Section 2.3 for a list of possible values - depending on product family.	None

Example --> switch set port lan1 trslimit-low 8Mbps

2.2.4.1.39 SWITCH SET PRIORITY

Syntax `SWITCH SET PRIORITY <802.1p_base_priority>`

Description This command sets the switch base priority. If an 802.1p bit value is higher than or equal to this value - then it goes into the high priority queue. Otherwise - it goes into the low priority queue.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
802.1p_base_priority	The system priority value. Available values are in the range 0 to 7.	4

Example --> switch set priority 7

2.2.4.1.40 SWITCH SET QOS 802.1P

Syntax `SWITCH SET QOS 802.1P < 802.1p_value > PRIORITY < queue >`

Description This command is used to map an incoming tagged frame with a specific 802.1p value in the priority field of the tag header into one of the four egress queues available on the switch.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
802.1p_value	The value of the 802.1p field used to map incoming frames into a well defined outgoing queue. Possible values are from 0 to 7.	N/A
queue	The name of the egress priority queue where frame will be forwarded. Allowed values are: P0 (lowest priority queue) P1 P2 P3 (highest priority queue).	P0

Example --> switch set qos 24,37 priority high

2.2.4.1.41 SWITCH SET QOS DSCP

Syntax `SWITCH SET QOS DSCP < dscp_value > PRIORITY < queue >`

Description This command is used to map an incoming frame with a specific TOS/DiffServ/Traffic class value in the IP header into one of the four egress queues available on the switch.

To show the current port status, use the SWITCH SHOW PORT command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
dscp_value	The value of the TOS/DiffServ/Traffic class field used to map incoming frames into a well defined outgoing queue. Possible values are from 0 to 6.	N/A
queue	The name of the egress priority queue where frame will be forwarded. Allowed values are: P0 (lowest priority queue) P1 P2 P3 (highest priority queue).	P0

2.2.4.1.42 SWITCH SET QOS PRIORITY

Syntax `SWITCH SET QOS <dscpcode> PRIORITY {HIGH | LOW}`

Description This command maps the priority levels for Quality of Service.

The six-bit TOS field in the IP header is decoded as 64 entries and for each one it is possible to specify the priority.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
dscpcode	dscpcode-list is a comma-separate list of numbers in the range 0-63 which represent the DSCP (Differentiated Service Code Point) value in the most significant 6 bits of the TOS field in IPv4 header.	N/A

Example To set the high priority for DSCP values 24 and 37, use the command:

```
switch set qos 24,37 priority high
```

2.2.4.1.43 SWITCH SET ROUTING-LIMIT

Syntax `SWITCH SET ROUTING-LIMIT <limit>`

Description This command set the maximum number of frame per seconds that the layer 2 switch forward to the Residential Gateway network processor for routing purposes.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
limit	It's the traffic maximum rate (frame per seconds) sent to the network processor. Available values are: 1.0Kfps 1.5Kfps 2.0Kfps 2.5Kfps 3.0Kfps 3.5Kfps 4.0Kfps 4.5Kfps 5.0Kfps 5.5Kfps 6.0Kfps None (disable the routing limit)	none

2.2.4.1.44 SWITCH SHOW

Syntax `SWITCH SHOW`

Description This command shows a summary of the switch parameters:

Example --> switch show

```
Actual configuration:
     Switch MAC:      00:0d:da:08:78:d4
     Status:          Enabled
     Aging Time:      Enabled
     Age Timer:       304
     Learning Status: Enabled
Status summary:
```

```
Max Ports:       10
Max VLANS:       16
Max Queues:      4
```

See also SWITCH SHOW PORT

2.2.4.1.45 SWITCH SHOW 802.1P

Syntax SWITCh SHOW 802.1P

Description This command displays the current mapping of the switch egress queues respect the 802.1p priority field value of the tag header of the an incoming tagged frame. Please note that the four queues are shown in the following way:

- low queue --> .
- med-low queue --> L
- med-high queue --> M
- high queue --> H

Example switch show 802.1p

```
802.1p Queue Map
-------------------------------------------------------------------
PID   |  0 1 2 3 4 5 6 7
       ----------------
QUEUE |  . . . . H H H H
-------------------------------------------------------------------
```

2.2.4.1.46 SWITCH SHOW FDB

Syntax (A) SWITCH SHOW FDB [ADDRESS <mac-address>|PORT <port-name> | vlan <vlan-id>
(B) SWITCH SHOW FDB

Description This command displays the whole contents of the ***Forwarding Database (ordered by VLAN identifier)***.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
mac-address	The MAC Address of the device that it is of interest to see the FDB entry for.	N/A

Option	Description	Default Value
port-name	The name of the switch port to be that entries are to be displayed for..	N/A
vlan-id	The VLAN Identifier that it is of interest to show all the FDB entries for.	N/A

Example To display the FDB content:

```
--> switch show fdb
VLAN         MAC           Port          Status
 204  00:0d:da:00:79:0f    lan8          Dynamic
 204  00:0d:da:01:2c:68    lan8          Dynamic
 204  00:0d:da:02:33:d2    lan8          Dynamic
 204  00:0d:da:05:51:94    lan8          Dynamic
 202  00:0d:da:01:2c:68    lan8          Dynamic
 202  00:0d:da:06:f4:23    lan8          Dynamic
 202  00:0d:da:08:6c:b6    cpu           Dynamic
 202  00:30:84:ee:40:7e    lan8          Dynamic
   1  00:30:84:ee:40:80    lan8          Dynamic
```

2.2.4.1.47 SWITCH SHOW PORT

Syntax `SWITCH SHOW PORT <port-name> [COUNTERS]`

Description This command displays the status of the selected switch port and eventually the value of the associated counters.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
portname	The name of the switch port to be configured. See Section 2.3 for a list of possible port names.	N/A

Example --> switch show port lan6

2.2.4.1.48 SWITCH SHOW QOS

Syntax `SWITCH SHOW QOS`

Description This command displays the current mapping of user priority level to QOS egress queue for the switch.

```
Switch Quality Of Service configuration
-----------------------------------------------------------------------
  Priority Map:

    Addr | 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
    ---------------------------------------------
     00  | . . . . . . . . . . . . . . . . . . . .
     20  | . . . . . . . . . . . . . . . . . . . .
     40  | H H H H H H H H H H H H H H H H H H H H
     60  | H H H H
-----------------------------------------------------------------------
```

2.2.4.1.49 SWITCH SHOW QOS 802.1P

Syntax `SWITCH SHOW QOS 802.1P`

Description This command displays the current mapping of the switch egress queues with respect to the 802.1p priority field value of the tag header of the an incoming tagged frame.

Example --> switch show qos 802.1p

```
Tag Que Map:
Queue Range: 0-3
PID   |  0    1    2    3    4    5    6    7
      ---------------------------------------
QUEUE |  0    0    1    1    2    2    3    3
```

2.2.4.1.50 SWITCH SHOW QOS DSCP

Syntax `SWITCH SHOW QOS DSCP`

Description This command displays the current mapping of the switch egress queues respect the TOS/DiffServ/Traffic class value in the IP header of the an incoming frame.

Example --> switch show qos dscp

```
DSCPQue Map:
Queue Range: 0-3
DSCP   |   0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5   6   9
-------------------------------------------------------------------------------
 00    |   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   1   1
 20    |   1   1   1   1   1   1   1   1   1   1   1   1   2   2   2   2   2   2
 40    |   2   2   2   2   2   2   2   2   3   3   3   3   3   3   3   3   3   3
 60    |   3   3   3   3
```

2.3 BRIDGE

2.3.1 Overview

The Bridge module acts as an extension to the existing Layer 2 switch - providing connectivity between the applications and services provided in the CPU and the devices connected to the LAN ports also provides support for virtual LANs in order to create multiple domains in which the packets are forwarded. The Bridge module also provides standard interfaces for attachment to the system TCP/IP Stack allowing the termination of IP frames belonging to a specific VLAN to a well defined IP interface.

A key point of interest here is that the port associated with the Bridge is not the Ethernet Port from the switch - there is a single interface between the switch and the bridge, and then additional connections to the different functions - such as the ADSL interface - or the IP interface.

2.3.2 Bridge Functional Description

2.3.2.1 Source MAC based forwarding

The source based MAC forwarding entries are unicast entries configured to forward packets on the specified port that is configured for the MAC address, which matches the destination MAC address of the packet. They are also used to restrict forwarding of packets to the ports specified in the entry if MAC address and source port matches the source MAC address of the packet and the port on which packet is received.

The source based MAC entries (named also static unicast entries source based) can be created/deleted by the user through. These entries have higher priority over the dynamic entries, meaning that the learned entry does not overwrite the static unicast entry with the same MAC address.

A static unicast entry serves the following purpose in packet forwarding:

- For a packet received from the port with its source MAC address and received port matching the static unicast entry's MAC address and the source port respectively, then the packet will be forwarded to the respective ports as specified by the entry's destination mask;
- For a packet received from a port with its source MAC address matching but withdifferent source port, the packet will be discarded;
- For a packet received from a port with its destination MAC address matching a static unicast entry, the packet will be forwarded to the source port of the entry.

2.3.2.2 Destination MAC based forwarding

The destination based MAC forwarding entries are configured to forward packets to the ports specified in the entry whose MAC address matches the destination MAC address of the packet. In the absence of a static unicast entry or a dynamic entry, it provides the capability to forward unicast packets to the ports on which the

particular destination might be present. It is also used to create multicast entries and forward multicast packets to all ports listening for that particular multicast address.

The destination based MAC entries (named also static unicast entries destination based) can be created/deleted by the user.

For a specific MAC address, there can exist either a static unicast entries source based or a destination unicast entries source based. However, a destination based MAC entry is updated to be of type static + dynamic if a packet is received with the source MAC address matching the destination based MAC entry's MAC address. In that case, the source port field that was unused for destination based MAC entry type is updated to the source port on which the MAC address is learnt.

A destination based MAC entry serves the following purpose in packet forwarding:

- For a packet received from a port with its destination MAC address matching a destination based MAC entry entry's MAC address, the packet will be forwarded to the ports as specified by the entry's destination mask;
- For a packet received from a port with its destination MAC address matching a destination based MAC entry + dynamic entry's MAC address, the packet will be forwarded to the source port specified in the entry;

2.3.2.3 Port based forwarding

Port based forwarding is an additional mechanism to forward packets based on the port on which the packets are received. This forwarding applies to all packets received, irrespective of their source and destination MAC addresses.

Port based forwarding is the first level of forwarding applied to the received packets. The destination mask is set to the forwarding mask of the port on which the packets are received. It serves the following purpose in packet forwarding:

- If a source based MAC entry or a dynamic MAC entry matching the destination MAC address is found, the packet is forwarded to the specified source port only if the port exists in the port forwarding mask of the port on which packet is received.
- If a source based MAC entry matching the source MAC address is found, the packet is forwarded to all the ports that exist in the destination mask as well as the port forwarding mask of the port on which packet is received.
- If a destination based MAC entry, matching the destination MAC address is found, the packet is forwarded to the all the ports that exist in the destination mask of the entry as well as the port forwarding mask of the port on which packet is received.

2.3.2.4 Traffic Prioritization

The bridge module provides support for traffic prioritization in conformance to the IEEE 802.1p specifications.

To regenerate priority mapping, it can be configured for each port such that, whenever a tagged packet is received with a specified priority in the tag header, it is mapped to the corresponding regenerated priority and the tag header is reset with the new priority.

Additionally, it can be configured to prioritize traffic based on certain traffic classes defined for each outgoing port. Based on these mappings, the regenerated priority is mapped to the corresponding traffic class priority, which is set as the system buffer priority such that the transmitted packets are appropriately prioritized by the lower layers. The actual priority transmission of packets is performed by the Scheduler device. The scheduler device transmits packets with highest priority first, followed by lower priority packets and finally the lowest priority packets.

Priority handling has the following effect on the forwarding path:

- If the packet receive is untagged, assign the default priority of the port on which packet is received else obtain the user priority from the tag header.
- Maps the user priority to the regenerated priority based on the configuration of the received port.
- If the packet is forwarded as tagged, it sets the regenerated priority in the tag header.
- If traffic class mapping is enabled, it obtains the traffic class mapping based on the configuration of the outgoing port and sets the priority in the system buffer.

2.3.2.5 Multicast Traffic

The system supports configuration and handling of multicast MAC forwarding entries, forward all and forward unregistered entries. Forwarding of the multicast packets is done based on these entries. By default, multicast traffic is forwarded to all ports. With the addition of support for IGMP snooping in the Bridge, multicast forwarding is further optimized, by intelligent forwarding of multicast traffic in the network..

Additionally, the system provides configuration of forward all and forward unregistered ports.

Forward all ports are the ports to which all multicast data will always be forwarded. Forward unregistered ports are the ports to which the multicast data needs to be forwarded, for which there exists no multicast filtering entry.

2.3.2.6 Learning

Learning is carried out for each unicast packet received by the bridge. Based on the source MAC address and the source port on which the packet is received, the bridge updates it forwarding database so that whenever a packet with destination as the learnt MAC address is received, it sends it to the appropriate port on which it had learnt that MAC address.

The entries are aged out with a periodicity of filter age time configured by the user.

The entries are learnt only on those ports that are in either learning or forwarding state.

Learning is carried out in the following manner:

- If there already exists an Dynamic entry with MAC address that matches the source MAC address, it updates the last seen time and the source port for the entry.
- If there exists a Static entry with MAC address that matches the source MAC address, it updates entry's source port field with the received port.

2.3.3 Functional Differences in Product Categories

A key difference between the different models is the incorporation of a VLAN Aware Bridge implementation. As a part of this enhancement - additional flexibility was added to support MAC Filtering. Note that some commands described here - presume support for multiple VLANs w/in the Bridge. For more information on the VLAN specific functions - please see the VLAN section.

It is not often that a user would need to manipulate the forwarding databases. This capability is there...but not anticipated to be widely utilized.

TABLE 2-3 Functional Mapping for Bridge

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
Port based forwarding		X		X	X	X		X	X
Traffic Prioritization		X		X	X	X		X	X
Multicast Traffic	1	X	1	X	X	X	1	X	X
Learning	X	X	X	X	X	X	X	X	X

Note 1) On these devices - Multicast traffic is forwarded to all ports with no options for filtering/restriction.

Note 2) For these devices there is only one Forwarding DataBase - the DefaultFDB - for other devices - it is possible to create multiple Forwarding Databases via the Bridge Add VLAN command.

Note 3) Dynamic Destination MAC based forwarding is the only mechanism supported here. The Bridge learns which MAC addresses come from which ports - and forwards packets with that MAC as a Destination MAC to those ports. There is no support for static configuration of MAC Addresses.

2.3.4 Bridge command reference

This section describes the commands available for Bridge.

2.3.4.1 Bridge commands

The table below lists the Bridge commands provided by the CLI:

TABLE 2-4 ***Bridge*** commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
BRIDGE ADD FWDALLINTERFACE SHARED	X	X	X	X	X	X	X	X	X
BRIDGE ADD FWDUNREGINTERFACE SHARED									
BRIDGE ADD INTERFACE	X	X	X	X	X	X	X	X	X
BRIDGE ADD MCASTENTRY SHARED		X		X	X	X		X	X
BRIDGE ADD MCASTINTERFACE SHARED		X		X	X	X		X	X
BRIDGE ADD UCASTENTRY DEST		X		X	X	X		X	X
BRIDGE ADD UCASTENTRY SRC		X		X	X	X		X	X
BRIDGE ADD UCASTINTERFACE		X		X	X	X		X	X
BRIDGE ATTACH	X	X	X	X	X	X	X	X	X
BRIDGE CLEAR FWDALLINTERFACES SHARED	X	X	X	X	X	X	X	X	X
BRIDGE CLEAR FWDUNREGINTERFACES SHARED									
BRIDGE CLEAR INTERFACE STATS	X	X	X	X	X	X	X	X	X
BRIDGE CLEAR INTERFACES	X	X	X	X	X	X	X	X	X
BRIDGE CLEAR MCASTENTRIES SHARED		X		X	X	X		X	X
BRIDGE CLEAR MCASTINTERFACES SHARED		X		X	X	X		X	X
BRIDGE CLEAR UCASTENTRIES		X		X	X	X		X	X
BRIDGE CLEAR UCASTINTERFACES		X		X	X	X		X	X
BRIDGE DELETE FWDALLINTERFACE SHARED	X	X	X	X	X	X	X	X	X
BRIDGE DELETE FWDUNREGINTERFACE SHARED									
BRIDGE DELETE INTERFACE	X	X	X	X	X	X	X	X	X
BRIDGE DELETE MCASTENTRY SHARED		X		X	X	X		X	X
BRIDGE DELETE MCASTINTERFACE SHARED		X		X	X	X		X	X

TABLE 2-4 *Bridge* commands **(Continued)**

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
BRIDGE DELETE UCASTENTRY		X		X	X	X		X	X
BRIDGE DELETE UCASTINTERFACE		X		X	X	X		X	X
BRIDGE DETACH	X	X	X	X	X	X	X	X	X
BRIDGE FLUSH	X	X	X	X	X	X	X	X	X
BRIDGE LIST FDBS		X		X	X	X		X	X
BRIDGE LIST FWDALL SHARED		X		X	X	X		X	X
BRIDGE LIST FWDUNREG SHARED									
BRIDGE LIST INTERFACE STATS	X	X	X	X	X	X	X	X	X
BRIDGE LIST INTERFACES	X	X	X	X	X	X	X	X	X
BRIDGE LIST MCASTENTRIES SHARED		X		X	X	X		X	X
BRIDGE LIST STATIC FWDALL SHARED									
BRIDGE LIST STATIC FWDUNREG SHARED									
BRIDGE LIST STATIC MCASTENTRIES SHARED		X		X	X	X		X	X
BRIDGE LIST STATIC UCASTENTRIES		X		X	X	X		X	X
BRIDGE LIST UCASTENTRIES	X	X	X	X	X	X	X	X	X
BRIDGE SET FILTERAGE	X	X	X	X	X	X	X	X	X
BRIDGE SET INTERFACE ACCEPTFRAMETYPE		X		X	X	X		X	X
BRIDGE SET INTERFACE DEFAULTUSERPRIORITY		X		X	X	X		X	X
BRIDGE SET INTERFACE FILTETYPE	X	X	X	X	X	X	X	X	X
BRIDGE SET INTERFACE INGRESSFILTERING		X		X	X	X		X	X
BRIDGE SET INTERFACE NUMTRAFFICCLASSES		X		X	X	X		X	X
BRIDGE SET INTERFACE NUMTRAFFICCLASSES	X	X	X	X	X	X	X	X	X
BRIDGE SET INTERFACE PVID		X		X	X	X		X	X
BRIDGE SET INTERFACE REGENPRIORITY		X		X	X	X		X	X
BRIDGE SET INTERFACE TRAFFICCLASSTATUS		X		X	X	X		X	X

TABLE 2-4 *Bridge* commands **(Continued)**

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
BRIDGE SET INTERFACE TRAFFICCLASSTATUS	X	X	X	X	X	X	X	X	X
BRIDGE SET WANTOWANFORWARDING	X	X	X	X	X	X	X	X	X
BRIDGE SHOW	X	X	X	X	X	X	X	X	X
BRIDGE SHOW FDB		X		X	X	X		X	X
BRIDGE SHOW INTERFACE	X	X	X	X	X	X	X	X	X
BRIDGE SHOW INTERFACE REGENPRIORITY		X		X	X	X		X	X
BRIDGE SHOW INTERFACE TRAFFICCLASSMAP		X		X	X	X		X	X
BRIDGE SHOW INTERFACESTATS	X	X	X	X	X	X	X	X	X
BRIDGE SHOW MCASTENTRY SHARED		X		X	X	X		X	X
BRIDGE SHOW UCASTENTRY		X		X	X	X		X	X

2.3.4.1.1 BRIDGE ADD FWDALLINTERFACE SHARED

Syntax `BRIDGE ADD FWDALLINTERFACE SHARED { <fdbname> | <fdbnumber> } <interfacename>`

Description This command adds an interface to the egress interface list of the Forward All Group of the named Filtering Database. The Forward All Group represents the set of interfaces to which all the multicast frames would be forwarded.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Option	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database..	N/A

Option	Description	Default Value
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	N/A
interface name	The name of a bridge interface that has previously been added and attached to a transport using the *bridge add interface* and *bridge attach*	N/A

Example bridge add fwdallinterface shared FDB_1 bridge1

See also `BRIDGE DELETE FWDALLINTERFACE SHARED`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.2 BRIDGE ADD FWDUNREGINTERFACE SHARED

Syntax `BRIDGE ADD FWDUNREGINTERFACE SHARED { <fdbname> | <fdbnumber> } <interfacename>`

Description This command adds an interface to the egress interface list of the Forward Unregistered Group of the named Forwarding Database. The Forward Unregistered Group represents the set of interfaces to which all the multicast frames would be forwarded whose respective destination MAC addresses have no other forwarding information available..

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Option	Description	Default Value
fdbname	The name of an existing Forwarding Database. See bridge add vlan CLI command to configure a new Forwarding Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the bridge list fdbs command. The number appears in the first column under the heading ID.	
interface name	The name of a bridge interface that has previously been added and attached to a transport using the bridge add interface and bridge attach CLI commands, respectively.	

Example bridge add fwdunreginterface shared FDB_1 bridge1

See also `BRIDGE ADD FWDALLINTERFACE`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.3 BRIDGE ADD INTERFACE

Syntax `BRIDGE ADD INTERFACE < name >`

Description This command adds a named interface to the bridge.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Name	An arbitrary name that identifies an object. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit..	N/A

Example --> bridge add interface bridge1

See also `BRIDGE LIST INTERFACES`
`BRIDGE ATTACH`

2.3.4.1.4 BRIDGE ADD MCASTENTRY SHARED

Syntax `BRIDGE ADD MCASTENTRY SHARED <name> { <fdbname> | <fdbnumber> } <mac>`

Description This command adds a multicast forwarding entry to a Forwarding Database. On receiving a multicast frame, if the multicast MAC address matches the address given in this command, that frame is forwarded to all the interfaces in the egress interface list of this entry. See *bridge add mcastinterface shared* to add an egress interface to a multicast entry.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Option	Description	Default Value
name	An arbitrary name that identifies the entry. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit	N/A

fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	N/A
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	N/A
mac	A valid multicast Ethernet MAC address displayed in the following format:##:##:##:##:##:##	N/A

Example bridge add mcastentry shared MCAST_1 DefaultFdb 01:00:00:00:00:00

See also `BRIDGE DELETE MCASTENTRY SHARED`

2.3.4.1.5 BRIDGE ADD MCASTINTERFACE SHARED

Syntax `BRIDGE ADD MCASTINTERFACE SHARED { <entryname> | <entrynumber> } { <fdbname> | <fdbnumber> } egress <interfacename>`

Description This command adds an interface to the egress interface list of the named multicast forwarding entry for the given Forwarding Database.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Dafault Value
entryname	Name of an existing Multicast Forwarding Entry. To display the list of all statically configured multicast entries, that the user can delete, use *bridge list static mcastentries*. This command also displays the entire egress interface list for that entry.	N/A
entrynumber	A number that identifies an existing Multicast Forwarding Entry. To display the list of statically configured multicast entries, use *bridge list static mcastentries*. The number appears in the first column under the heading ID.	N/A
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	N/A
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	N/A
interfacename	The name of a bridge interface that has previously been added and attached to a transport using the *bridge add interface* and *bridge attach* CLI commands, respectively.	N/A

Example bridge add mcastinterface shared MCAST_1 FDB_1 egress bridge1

See also `BRIDGE CLEAR MCASTENTRIES SHARED`
`BRIDGE ADD MCASTENTRY SHARED`
`BRIDGE DELETE MCASTENTRY SHARED`

2.3.4.1.6 BRIDGE ADD UCASTENTRY DEST

Syntax `BRIDGE ADD UCASTENTRY DEST <name> { <fdbname> | <fdbnumber> } <macaddress>`

Description This commands creates a destination MAC address based unicast forwarding entry in the named forwarding database.

When the system receives an ethernet frame, the system examines the destination MAC address of the frame. If the destination MAC address matches the address specified in this command, the system forwards the frame to the egress interfaces configured for this entry.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Dafault Value
name	An arbitrary name that identifies the entry. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit The name has to be unique for all unicast entries (source MAC and destination MAC based) in a Filtering Database.	
fdbname	The name of an existing forwarding database to which the entry will be added.	
fdbn umber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	
macaddress	A valid unicast Ethernet MAC address displayed in the following format:##:##:##:##:##:##	

Example Example bridge add ucastentry dest UCAST_2 DefaultFdb 00:00:00:00:00:02

See also
```
BRIDGE ADD UCASTENTRY SRC
BRIDGE ADD UCASTENTRY DEST
BRIDGE LIST UCASTENTRIES
```

2.3.4.1.7 BRIDGE ADD UCASTENTRY SRC

Syntax `BRIDGE ADD UCASTENTRY SRC <name> {<fdbname>| <fdbn umber>) <macaddress> <recvin terface>`

Description This commands creates a source MAC address based unicast filtering entry in the named filtering database.

When the system receives an ethernet frame, the system examines the source MAC address of the frame. If both the source MAC address and source interface matches the <macaddress> and <recvinterface> specified in this command, the system forwards the frame to the egress interfaces configured for this entry. .

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the entry. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit The name has to be unique for all unicast entries (source MAC and destination MAC based) in a Forwarding Database.	
fdbname	The name of an existing forwarding database to which the entry will be added.	
fdbn umber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	
macaddress	A valid unicast Ethernet MAC address displayed in the following format:##:##:##:##:##:##	
recvinterface	The name of the existing bridge interface that Ethernet frames is received on. The interface must be attached to a valid transport. To display interface names and their transport attachment details, use the *bridge list interfaces* command.	

Example -->bridge add ucastentry src UCAST_1 FDB_1 00:00:00:00:00:01 bridge1

See also `BRIDGE ADD UCASTENTRY DEST`
`BRIDGE LIST STATIS UCASTENTRIES`

2.3.4.1.8 BRIDGE ADD UCASTINTERFACE

Syntax `BRIDGE ADD UCASTINTERFACE {<entryname>| <entryn umber>) {<fdbname>| <fdbn umber>) <interfacename>`

Description This commands adds an interface to the egress interface list of a statically configured unicast forwarding entry. This command can be invoked multiple times to add more interfaces to the egress interface list of the entry.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
entryname	Name of an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*.	

entryn umber	A number that identifies an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing filtering database to which the filtering entry will be added. See Note on filtering database in this command.	
fdbn umber	A number that identifies an existing Filtering Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	
interface-name	The name of a bridge interface that has previously been added and attached to a transport using the *bridge add interface* and *bridge attach* CLI commands, respectively.	

Example bridge add ucastinterface UCAST_I DefaultFdb bridge

See also
```
BRIDGE ADD UCASTENTRY SRC
BRIDGE ADD UCASTENTRY DEST
BRIDGE LIST UCASTENTRIES
```

2.3.4.1.9 BRIDGE ATTACH

Syntax `BRIDGE ATTACH { <name> | <number> } <transport>`

Description This command attaches an existing transport to an existing bridge interface to allow data to be bridged via the transport. Only one transport can be attached to an interface. If you use this command when there is already a transport attached to the interface, the previous transport is replaced by the new one.

This command implicitly enables the transport being attached. This command also adds the interface to the untagged port list of the default VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created.	N/A
Number	The numerical identifier automatically assigned to the object when it was created.	N/A

Name	Description	Default Value
Transport	A name that identifies an existing transport. To display transport names, use the <transport type> list transports command.	N/A

Example --> bridge attach bridge1 my1483

See also `BRIDGE LIST INTERFACES`

2.3.4.1.10 BRIDGE CLEAR FWDALLINTERFACES SHARED

Syntax `BRIDGE CLEAR FWDALLINTERFACES SHARED {<fdbname> | <fdbnumber>}`

Description This commands removes all the interfaces from the egress interface list of the Forward All Group of the named Forwarding Database. The Forward All Group represents the set of interfaces to which all the multicast frames would be forwarded.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge clear fwdallinterfaces shared FDB_1

See also `BRIDGE DELETE FWDALLINTERFACE SHARED`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.11 BRIDGE CLEAR FWDUNREGINTERFACES SHARED

Syntax `BRIDGE CLEAR FWDUNREGINTERFACES SHARED { <fdbname> | <fdbnumber> }`

Description This command removes all of the interfaces from the egress interface list of the Forward Unregistered Group of the named Forwarding Database (previously added using the *bridge add fwdunreginterface shared* CLI command). The Forward Unregistered Group represents the set of interfaces to which all the multicast frames would be forwarded, whose respective destination MAC addresses have no other forwarding information available.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge clear fwdunreginterfaces shared FDB_I

See also `BRIDGE ADD FWDALLINTERFACE`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.12 BRIDGE CLEAR INTERFACE STATS

Syntax `BRIDGE CLEAR INTERFACE STATS [ < name | number > ]`

Description This command clears either the interface statistics for all interfaces or the interface statistics for a single specified interface. It resets all of the statistical information displayed by bridge list interface stats CLI command to zero.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created.	N/A

Example --> bridge clear interface stats

See also `BRIDGE ADD INTERFACE`
`BRIDGE ATTACH`
`BRIDGE LIST INTERFACE STATS`

2.3.4.1.13 BRIDGE CLEAR INTERFACES

Syntax `BRIDGE CLEAR INTERFACES`

Description This command deletes all bridge interfaces previously created using the bridge add interface command.

All source/ destination MAC address based unicast forwarding entries associated with the interfaces are also deleted by this command. The interfaces are also deleted from the

egress interface list of all VLANs, multicast filtering entries and Forward All/Unregistered group entries.

Example --> bridge clear interfaces

See also BRIDGE ADD INTERFACE
BRIDGE DELETE INTERFACE

2.3.4.1.14 BRIDGE CLEAR MCASTENTRIES SHARED

Syntax BRIDGE CLEAR MCASTENTRIES SHARED { <fdbname> | <fdbnumber>)

Description This command deletes the entire statically configured multicast forwarding entries from the named Forwarding Database, that were added by *bridge add mcastentry shared* CLI command. Also, all the interfaces in the egress interface list of entries (added by *bridge add mcastinterface shared* CLI command) are deleted.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge clear mcastentries DefaultFdb

See also BRIDGE ADD MCASTENTRY SHARED
BRIDGE DELETE MCASTENTRY SHARED

2.3.4.1.15 BRIDGE CLEAR MCASTINTERFACES SHARED

Syntax BRIDGE CLEAR MCASTINTERFACES SHARED {<entryname>| <entrynumber>) {<fdbname> | <fdbnumber>)

Description This command deletes all the interfaces from the egress interface list of the named multicast Forwarding entry in the given Forwarding Database. The following table gives the range of values for each option that can be specified with this command and a default-value (if applicable)

Name	Description	Default Value
entryname	Name of an existing Multicast Forwarding Entry. To display the list of all statically configured multicast entries, that the user can delete, use *bridge list static mcastentries*. This command also displays the entire egress interface list for that entry.	
entrynumber	A number that identifies an existing Multicast Forwarding Entry. To display the list of statically configured multicast entries, use *bridge list static mcastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the	

Example bridge clear mcastinterfaces shared MCAST_I DefaultFDB

See also `BRIDGE ADD MCASTENTRY SHARED`
`BRIDGE DELETE MCASTENTRY SHARED`

2.3.4.1.16 BRIDGE CLEAR UCASTENTRIES

Syntax `BRIDGE CLEAR UCASTENTRIES{<fdbname>| <fdbn umber>}`

Description This commands deletes all the statically configured unicast forwarding entries in the named forwarding database. For each unicast entry, it also deletes their egress interfaces.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
fdbname	The name of an existing forwarding database to which the entry will be added.	
fdbn umber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first col-	

Example bridge clear ucastentries DefaultFdb

See also BRIDGE ADD UCASTENTRY SRC
BRIDGE ADD UCASTENTRY DEST

2.3.4.1.17 BRIDGE CLEAR UCASTINTERFACES

Syntax BRIDGE CLEAR UCASTINTERFACES {<entryname>| <entrynumber>) {<fdbname>| <fdbnumber>)

Description This command removes all the interfaces from the egress interface list of the named unicast forwarding entry.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
entryname	Name of an existing unicast filtering entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*.	
entryn umber	A number that identifies an existing unicast filtering entry. To display the list of statically configured unicast entries, use *bridge list static ucastentrie*s. The number appears in the first column under the heading ID.	
fdbname	The name of an existing filtering database to which the filtering entry will be added. See Note on filtering database in this command.	
fdbn umber	A number that identifies an existing Filtering Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge clear ucastinterfaces DefaultFdb

See also BRIDGE ADD UCASTENTRY SRC
BRIDGE ADD UCASTENTRY DEST
BRIDGE LIST UCASTENTRIES

2.3.4.1.18 BRIDGE DELETE FWDALLINTERFACE SHARED

Syntax BRIDGE DELETE FWDALLINTERFACE SHARED {<fdbname>| <fdbnumber>} <interfacename>

Description This command removes an interface from the egress interface list of the Forward All Group of the named Forwarding Database (previously added using the *bridge add fwdallinterface shared*

CLI command). The Forward All Group represents the set of interfaces to which all the multicast frames would be forwarded.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	
interface name	The name of a bridge interface that has previously been added and attached to a transport using the *bridge add interface* and *bridge attach* CLI commands, respectively.	

Example bridge delete fwdallinterface shared FDB_1 bridge1

See also `BRIDGE ADD FWDALLINTERFACE SHARED`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.19 BRIDGE DELETE FWDUNREGINTERFACE SHARED

Syntax `BRIDGE DELETE FWDUNREGINTERFACE SHARED {<fdbname> | <fdbnumber>} <interfacename>`

Description This command removes an interface from the egress interface list of the Forward Unregistered Group of the named Forwarding Database which was added by bridge add fwdunreginterface shared CLI command. The Forward Unregistered Group represents the set of interfaces to which all the multicast frames would be forwarded whose respective destination MAC addresses have no other forwarding information available.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database.	

fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	
interface name	The name of a bridge interface that has previously been added and attached to a transport using the *bridge add interface* and *bridge attach* CLI commands, respectively.	

Syntax `bridge delete fwdunreginterface shared FDB_1 bridge1`

See also `BRIDGE ADD FWDALLINTERFACE`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.20 BRIDGE DELETE INTERFACE

Syntax `BRIDGE DELETE INTERFACE < name | number >`

Description This command deletes a single interface from the bridge.

All source/ destination MAC address based unicast filtering entries associated with the interfaces are also deleted by this command. The interface is also deleted from the egress interface list of all VLANs, multicast filtering entries and Forward All/Unregistered group entries.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created.	N/A
Number	The numerical identifier automatically assigned to the object when it was created.	N/A

Example --> bridge delete interface qbridge1

See also `BRIDGE LIST INTERFACES`

2.3.4.1.21 BRIDGE DELETE MCASTENTRY SHARED

Syntax `BRIDGE DELETE MCASTENTRY SHARED {<entryname>| <entrynumber>) {<fdbname> | <fdbnumber>)`

Description This command deletes a single multicast forwarding entry created using the *bridge add mcastentry shared* CLI command. Also, this command deletes all of the interfaces in the

egress interface list of the entry (previously added using the *bridge add mcastinterface shared* CLI command).

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)bridge list mcastentries shared

Name	Description	Default Value
entryname	Name of an existing Multicast Forwarding Entry. To display the list of all statically configured multicast entries, that the user can delete, use *bridge list static mcastentries.* This command also displays the entire egress interface list for that entry.	
entrynumber	A number that identifies an existing Multicast Forwarding Entry. To display the list of statically configured multicast entries, use *bridge list static mcastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge delete mcastentry shared MCAST_I DefaultFDB

See also `BRIDGE CLEAR MCASTENTRIES SHARED`
`BRIDGE DELETE MCASTENTRY SHARED`

2.3.4.1.22 BRIDGE DELETE MCASTINTERFACE SHARED

Syntax `BRIDGE DELETE MCASTINTERFACE SHARED {<entryname>| <entrynumber>) {<fdbname>| <fdbnumber>) <interfacename>`

Description This command removes an interface from the egress interface list of a multicast Forwarding entry.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
entryname	Name of an existing Multicast Forwarding Entry. To display the list of all statically configured multicast entries, that the user can delete, use *bridge list static mcastentries*. This command also displays the entire egress interface list for that entry.	
entrynumber	A number that identifies an existing Multicast Forwarding Entry. To display the list of statically configured multicast entries, use *bridge list static mcastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	
interface name	The name of a bridge interface that has previously been added and attached to a transport using the *bridge add interface* and *bridge attach* CLI commands, respectively.	

Example bridge delete mcastinterface shared MCAST_1 FDB_1 bridge1

See also `BRIDGE ADD MCASTENTRY SHARED`
`BRIDGE CLEAR MCASTENTRY SHARED`

2.3.4.1.23 BRIDGE DELETE UCASTENTRY

Syntax `BRIDGE DELETE UCASTENTRY {<entryname>| <entryn umber>) {<fdbname>| <fdbnumber>)`

Description This command deletes a statically configured unicast forwarding entry. Also, all the egress interfaces of the unicast entry are also deleted by this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value

entryname	A name that identifies an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*. This command also displays the egress interface list for each unicast entry.	
entryn umber	A number that identifies an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing forwarding database to which the entry will be added.	
fdbn umber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge delete ucastentry UCAST_I DefaultFdb

See also `BRIDGE ADD UCASTENTRY DEST`
`BRIDGE LIST STATIS UCASTENTRIES`

2.3.4.1.24 BRIDGE DELETE UCASTINTERFACE

Syntax `BRIDGE DELETE UCASTINTERFACE {<entryname>| <entryn umber>) {<fdbname>| <fdbn umber>) <interfacename>`

Description This command removes an interface from the egress interface list of the named unicast forwarding entry.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable

Name	Description	Default Value
entryname	Name of an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*.	
entryn umber	A number that identifies an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing forwarding database to which the entry will be added.	

fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the	
interface-name	The name of a bridge interface that has previously been added and attached to a transport using the *bridge add inter-*	

Example bridge delete ucastinterface UCAST_1 FDB_1 bridge1

See also
```
bridge add ucastentry
bridge add ucastentry dest
bridge add ucastinterface
bridge list static ucastentries
bridge list ucastentries
```

2.3.4.1.25 BRIDGE DETACH

Syntax `BRIDGE DETACH INTERFACE { <name> | <number> }`

Description This command detaches the transport that was attached to the bridge interface using the bridge attach interface command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created.	N/A
Number	The numerical identifier automatically assigned to the object when it was created.	N/A

Example --> bridge detach interface bridge1

See also `BRIDGE LIST INTERFACES`

2.3.4.1.26 BRIDGE FLUSH

Syntax `BRIDGE FLUSH < portname >`

Description This command deletes all the dynamic unicast filtering entries across all filtering databases for the given bridge interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Portname	The name of a bridge interface that has previously been added and attached to a transport using the bridge add interface and bridge attach CLI commands respectively.	N/A

Example --> bridge flush bridge1

See also
```
BRIDGE ADD INTERFACE
BRIDGE ATTACH
BRIDGE LIST INTERFACE STATS
```

2.3.4.1.27 BRIDGE LIST FDBS

Syntax `BRIDGE LIST FDBS`

Description This command displays statistical information of all the filtering databases in the bridge. It displays the following information about the filtering database:

- Filtering database ID (FID)
- Number of dynamic unicast entries within it
- Number of VLANs associated with it
- Number of frames discarded due to filtering database overflow
- Type, indicating whether the filtering database is statically configured or dynamically created (by default, FDBs are created statically using the bridge add vlan command)

See also `BRIDGE ADD VLAN`

2.3.4.1.28 BRIDGE LIST FWDALL SHARED

Syntax `BRIDGE LIST FWDALL SHARED {<fdbname>|<fdbnumber>}`

Description This command lists the statically added interfaces (See *bridge add fwdallinterface shared* CLI command) and dynamically learnt interfaces in the egress interface list of the Forward All Group for the named Forwarding Database. The Forward All Group represents the set of interfaces to which all the multicast frames would be forwarded.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Filtering Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	
fdbnumber	A number that identifies an existing Filtering Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge list fwdall shared FDB_1

```
Forward All Egress Interfaces for : FDB_1
Egress Interfaces:bridge1
```

See also `BRIDGE ADD FWDALLINTERFACE`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.29 BRIDGE LIST FWDUNREG SHARED

Syntax `BRIDGE LIST FWDUNREG SHARED {<fdbname>| <fdbnumber>}`

Description This command lists statically added (See bridge add fwdunreginterface shared CLI command) and dynamically learnt interfaces in the egress interface list of the Forward Unregistered Group for the named Filtering Database. The Forward Unregistered Group represents the set of interfaces to which all the multicast frames would be forwarded whose respective destination MAC addresses have no other forwarding information available..

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge list fwdunreg shared FDB_1

See also BRIDGE ADD FWDALLINTERFACE
BRIDGE LIST FWDALL SHARED

2.3.4.1.30 BRIDGE LIST INTERFACE STATS

Syntax BRIDGE LIST INTERFACE STATS

Description This command displays the statistical information of all the configured bridge interfaces.

- ID: The numerical identifier automatically assigned to the object when it was created.
- Name: The name manually assigned to the object when it was created.
- Rx Frames: Number of frames received on the interface.
- Tx Frames: Number of frames transmitted from the interface.
- Transmit Delay Discards: Number of frames discarded due to transmit delay.
- Buffer O/F Discards: Number of frames discarded due to buffer overflow.
- Unknown VLAN Discards: Number of frames discarded due to unknown VLAN Id in the frames.
- Ingress Discards: Number of frames discarded due to ingress filtering.
- Frame Type Discards: Number of frames discarded due to the acceptable frame type setting on the interface.

Example --> bridge list interface stats

```
ID|Name| Rx     | Tx     | Transmit | Unknown |Buffer  |Ingress |Frame Type
  |    | Frames | Frames | Delay    | VLAN    | O/F    |Discards|Discards
  |    |        |        | Discards |Discards |Discards|        |
--|----|--------|--------|----------|---------|--------|--------|--------
1 |eth |3686117 |3236443 |0         |0        |0       |0       |0
2 |usb |0       |3236399 |0         |0        |0       |0       |0
-------------------------------------------------------------------------
```

See also BRIDGE ADD INTERFACE
BRIDGE ATTACH
BRIDGE SHOW INTERFACESTATS

2.3.4.1.31 BRIDGE LIST INTERFACES

Syntax BRIDGE LIST INTERFACES

Description This command lists information about all of the bridge interfaces created using the bridge add interface command.

Example --> bridge list interfaces

```
ID:      1
Name: defaulti
Filter| PVID  | Accept    | Ingress   | User  | Transport
Type  |       | FrameType | Filtering | Prio  |
------|-------|-----------|-----------|-------|--------------
All   | 1     | ALL       | disabled  | 0     | default
```

See also BRIDGE SET INTERFACE FILTERTYPE
BRIDGE SET INTERFACE PORTFILTER
BRIDGE SET INTERFACE PVID
BRIDGE SET INTERFACE INGRESSFILTERING
BRIDGE SET INTERFACE ACCEPTFRAMETYPE
BRIDGE SET INTERFACE DEFAULTUSERPRIORITY
BRIDGE SET INTERFACE NUMTRAFFICCLASSES
BRIDGE SET INTERFACE REGENPRIORITY

2.3.4.1.32 BRIDGE LIST MCASTENTRIES SHARED

Syntax BRIDGE LIST MCASTENTRIES SHARED {<fdbname>| <fdbnumber>}

Description This command displays all the statically configured and dynamically learnt multicast forwarding entries for the named Forwarding Database.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	
fdbn mber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge list mcastentries DefaultFdb

```
ID | Type|MAC Address| Egress Interfaces
1 | static|1:0:0:0:0:1| br1
```

See also BRIDGE CLEAR MCASTENTRIES SHARED
BRIDGE ADD MCASTENTRY SHARED
BRIDGE DELETE MCASTENTRY SHARED

2.3.4.1.33 BRIDGE LIST STATIC FWDALL SHARED

Syntax `BRIDGE LIST STATIC FWDALL SHARED {<fdbname>|<fdbnumber>}`

Description This command lists the interfaces added statically (See *bridge add fwdallinterface shared* CLI command to add an egress interface) in the egress interface list of the Forward All Group for the named Forwarding Database. The Forward All Group represents the set of interfaces to which all the multicast frames would be forwarded.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See bridge add vlan CLI command to configure a new Filtering Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the bridge list fdbs command. The number appears in the first column under the heading ID.	

Example bridge list static fwdall shared FDB_I

See also `BRIDGE ADD FWDALLINTERFACE`
`BRIDGE LIST FWDALL SHARED`

2.3.4.1.34 BRIDGE LIST STATIC FWDUNREG SHARED

Syntax `BRIDGE LIST STATIC FWDUNREG SHARED {<fdbname>| <fdbnumber>}`

Description This command lists the statically added interfaces (See *bridge add fwdunreginterface shared* CLI command to add an egress interface) in the egress interface list of the Forward Unregistered Group for the named Forwarding Database. The Forward Unregistered Group represents the set of interfaces to which all the multicast frames would be forwarded whose respective destination MAC addresses have no other forwarding information available.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database.	

fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge list static fwdunreg shared FDB_I

See also BRIDGE ADD FWDALLINTERFACE
BRIDGE LIST FWDALL SHARED

2.3.4.1.35 BRIDGE LIST STATIC MCASTENTRIES SHARED

Syntax BRIDGE LIST STATIC MCASTENTRIES SHARED {<fdbname>|<fdbnumber>}

Description This command displays all the statically configured multicast forwarding entries along with the forward all and forward unregistered groups in the named Filtering Database.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Forwarding Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge list static mcastentries shared DefaultFdb

```
Multicast Entries for : DefaultFdb1
ID        | Name|              MAC Address
1         | FWDALLMCAST|     00:00:00:00:00:FE
Egress Interfaces:
2         | FWDUNREGMCAST|   00:00:00:00:00:FC
```

See also BRIDGE CLEAR MCASTENTRIES SHARED
BRIDGE ADD MCASTENTRY SHARED
BRIDGE DELETE MCASTENTRY SHARED

2.3.4.1.36 BRIDGE LIST STATIC UCASTENTRIES

Syntax BRIDGE LIST STATIC UCASTENTRIES {<fdbname>|<fdbnumber>}

Description This command displays information about the statically configured unicast forwarding entries for the named Forwarding Database. The fields are listed below:

- IDA number that identifies an existing unicast forwarding entry.
- NameA name that identifies an existing unicast forwarding entry.
- TypeIndicates whether the entry is a source MAC address or destination MAC address based forwarding entry.
- MAC AddressEthernet MAC address associated with the entry.
- Receive PortReceive interface for source MAC address based entries. See the bridge add ucastentry src for more information.
- Egress InterfacesEgress interface list.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
fdbname	The name of an existing forwarding database to which the entry will be added.	
fdbn umber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge list static ucastentries DefaultFdb

```
.ID. | .Name........|.Type..........|.MAC Address..........| .Receive Port
-------------------------------------------------------------------------
..1..|.x............| .Dest Static. |.00:00:00:00:00:00...|

Egress Interfaces:                          bridge1
.........................................................
```

See also `BRIDGE ADD UCASTENTRY SRC`
`BRIDGE ADD UCASTENTRY DEST`
`BRIDGE LIST UCASTENTRIES`

2.3.4.1.37 BRIDGE LIST UCASTENTRIES

Syntax `BRIDGE LIST UCASTENTRIES <fdbname>`

Description This command displays all of the statically configured and dynamically learnt unicast filtering entries in the named filtering database.

- ID: The numerical identifier automatically assigned to the object when it was created.
- Type: One of the following types:
- source MAC address-based
- destination MAC address-based, statically configured
- destination MAC address-based, dynamically learnt
- Special Entry
- destination MAC address-based, statically configured and dynamically learnt.
- MAC Address: Ethernet MAC address associated with the entry.
- Receive Port: Receive port for source MAC address-based entries. See the bridge add ucastentry src CLI command for more information.
- Egress Interface: Egress interface list..

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Fdbname	The name of an existing filtering database.	N/A

Example --> bridge list ucastentries bridge1

```
Filtering entries for the FDB: FDB_1
ID| Type      | MAC Address | Receive Port
-----------------------------------------------------
 1| Dest Static| 0:0:0:0:0:0 |
Egress Interfaces: bridge1
-----------------------------------------------------
```

See also BRIDGE ADD UCASTENTRY SRC
BRIDGE ADD UCASTENTRY DEST
BRIDGE LIST STATIC UCASTENTRIES
BRIDGE ADD VLAN

2.3.4.1.38 BRIDGE SET FILTERAGE

Syntax `BRIDGE SET FILTERAGE < filterage >`

Description This command specifies the maximum age of filter table entries for the bridge. The filter age for the bridge is displayed by the bridge show command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Filterage	The time (in seconds) after which MAC addresses are removed from the filter table when there has been no activity. The time may be an integer value between 10 and 100,000 seconds..	300

Example --> bridge set filterage 1000

See also `BRIDGE SHOW`

2.3.4.1.39 BRIDGE SET INTERFACE ACCEPTFRAMETYPE

Syntax `BRIDGE SET INTERFACE { <name>|number } ACCEPTFRAMETYPE { acceptall | accepttaggedonly }`

Description This command specifies whether the bridge interface accepts only VLAN tagged frames or it accepts all the incoming frames. If the interface accepts all incoming frames, it assigns its PVID to the untagged or priority tagged frames.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command.	N/A
Number	A number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A
Acceptall	Accepts all the incoming frames.	Acceptall
accepttaggedonly	Accepts only VLAN tagged frames. See the bridge show interfacestats command. to know the incoming frames discarded due to acceptable frame type filtering	

Example --> bridge set interface bridge1 acceptframetype acceptall

See also `BRIDGE SET INTERFACE PVID`
`BRIDGE LIST INTERFACES`

2.3.4.1.40 BRIDGE SET INTERFACE DEFAULTUSERPRIORITY

Syntax `BRIDGE SET INTERFACE {<name>|<number>} DEFAULTUSERPRIORITY <defaultpriority>`

Description This command specifies the user priority that should be assigned to untagged frames, received on the interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	An arbitrary name that identifies an object. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
Number	Number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A
Defaultpriority	A value that assigns priority to untagged frames received on the interface.	0

Example --> bridge set interface bridge1 defaultuserpriority 4

See also `BRIDGE LIST INTERFACES`

2.3.4.1.41 BRIDGE SET INTERFACE FILTETYPE

Syntax `BRIDGE SET INTERFACE {<name> | <number>} FILTERTYPE {all | ip | pppoe}`

Description This command specifies the type of Ethernet filtering performed by the named bridge interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created..	N/A
Number	The numerical identifier automatically assigned to the object when it was created.	N/A
All	Allows all types of ethernet packets through the port.	All

Name	Description	Default Value
IP	Allows only IP/ARP types of ethernet packets through the port.	
Pppoe	Allows only PPPoE type of ethernet packets through the port.	

Example --> bridge set interface bridge1 filtertype ip

See also BRIDGE LIST INTERFACES

2.3.4.1.42 BRIDGE SET INTERFACE INGRESSFILTERING

Syntax BRIDGE SET INTERFACE {<name>|<number>} INGRESSFILTERING {disable|enable}

Description This command adds a named interface to the bridge.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	An arbitrary name that identifies an object. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
Number	A number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A
Disable	Accepts all incoming frames.	Disable
Enable	Accepts VLAN tagged frames, only if the VLAN Id in the frame has this interface in its egress interface list. See bridge show interfacestats to know the incoming frames discarded due to ingress filtering.	

Example --> bridge set interface bridge1 ingressfiltering disable

See also BRIDGE LIST INTERFACES
BRIDGE SHOW INTERFACESTATS

2.3.4.1.43 BRIDGE SET INTERFACE NUMTRAFFICCLASSES

Syntax BRIDGE SET INTERFACE {<name>|<number>} NUMTRAFFICCLASSES <numtrafficclasses>

Description This command specifies the number of traffic classes supported by the bridge interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command.	N/A
Number	A number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A
pri0	The traffic class to which the regenerated priority of value 0 is mapped.	0
pri1	The traffic class to which the regenerated priority of value 1 is mapped.	1
pri2	The traffic class to which the regenerated priority of value 2 is mapped.	2
pri3	The traffic class to which the regenerated priority of value 3 is mapped.	3
pri4	The traffic class to which the regenerated priority of value 4 is mapped.	4
pri5	The traffic class to which the regenerated priority of value 5 is mapped.	5
pri6	The traffic class to which the regenerated priority of value 6 is mapped.	6
pri7	The traffic class to which the regenerated priority of value 7 is mapped.	7

Example --> bridge set interface bridge1 trafficclassmap 7 6 5 4 3 2 1 0

See also `BRIDGE SHOW INTERFACE TRAFFICCLASSMAP`
`BRIDGE LIST INTERFACES`

2.3.4.1.44 BRIDGE SET INTERFACE PORTFILTER

Syntax `BRIDGE SET INTERFACE {<name> | <number>} PORTFILTER {all | <port>}`

Description This command controls the bridge's forwarding and broadcasting behavior. It allows you to set a portfilter on a bridge interface to determine which port or ports unknown packets should be forwarded to. This command sets one destination port at a time. If you

want to forward packets to several ports, enter a bridge set interface portfilter <port> command for each port. If you want to forward packets to all ports, enter the command and specify the all value.

If a unicast packet is received by an interface with a portfilter set to all, the portfilter rule is ignored. The unicast packet is still only sent to one port. If the bridge itself is attached to the router, the bridge itself will always forward to all ports and will always be forwarded to by all ports. Port Filter is not restored by the system config save command. If the LAN to LAN forwarding is disabled, then no packet received on a lan side bridge interface will be bridged to any other lan side bridge interface irrespective of the portfilter. If the WAN to WAN forwarding is disabled, then no packet received on a wan side bridge interface will be bridged to any other wan side bridge interface irrespective of the portfilter.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created.	N/A
Number	The numerical identifier automatically assigned to the object when it was created.	N/A
Port	The name of the existing port that you want packets, received on a specified bridge interface, to be forwarded to. To display port names, use the bridge list interfaces CLI command.	All
All	Allows only IP/ARP types of ethernet packets through the port.	

Example --> bridge set interface bridge1 portfilter ethernet

See also
```
BRIDGE LIST INTERFACES
BRIDGE SET LANTOLANFORWARDING ENABLE/DISABLE
BRIDGE SET WANTOWANFORWARDING ENABLE/DISABLE
```

2.3.4.1.45 BRIDGE SET INTERFACE PVID

Syntax `BRIDGE SET INTERFACE {<name>|<number>} PVID <pvid>`

Description This command specifies the VLAN Id, that should be assigned to untagged or priority-tagged frames received on this interface..

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	An arbitrary name that identifies an object. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
Number	A number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A
Pvid	The Id of the VLAN to which the user wants to associate the untagged/priority-tagged frames received on the given interface. See bridge list vlans CLI command to find the VLAN Ids for all the statically configured and dynamic VLANs.	1

Example --> bridge set interface bridge1 pvid 2

See also `BRIDGE LIST INTERFACES`
`BRIDGE ADD VLAN`

2.3.4.1.46 BRIDGE SET INTERFACE REGENPRIORITY

Syntax `BRIDGE SET INTERFACE {<name>|<number>} REGENPRIORITY <pri0> <pri1> <pri2> <pri3> <pri4> <pri5> <pri6> <pri7>`

Description This command adds a named interface to the bridge.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command.	N/A
Number	A number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A
pri0	The regenerated user-priority to which the user priority with value 0 in the incoming frame should be mapped.	0

Name	Description	Default Value
pri1	The regenerated user-priority to which the user priority with value 1 in the incoming frame should be mapped.	1
pri2	The regenerated user-priority to which the user priority with value 2 in the incoming frame should be mapped.	2
pri3	The regenerated user-priority to which the user priority with value 3 in the incoming frame should be mapped.	3
pri4	The regenerated user-priority to which the user priority with value 4 in the incoming frame should be mapped.	4
pri5	The regenerated user-priority to which the user priority with value 5 in the incoming frame should be mapped.	5
pri6	The regenerated user-priority to which the user priority with value 6 in the incoming frame should be mapped.	6
pri7	The regenerated user-priority to which the user priority with value 7 in the incoming frame should be mapped.	7

Example --> bridge set interface bridge1 regenpriority 3 2 4 0 0 0 0 0

See also `BRIDGE SHOW INTERFACE REGENPRIORITY`
`BRIDGE LIST INTERFACES`

2.3.4.1.47 BRIDGE SET INTERFACE TRAFFICCLASSTATUS

Syntax `BRIDGE SET TRAFFICCLASSSTATUS { enable | disable | prioritybased }`

Description This command specifies the mapping of regenerated priority to their traffic class values. See bridge show interface trafficclassmap to see the traffic class mapping.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Enable	Enable the mapping of regenerated priority to its traffic class.	Disable
Disable	Disable the mapping of regenerated priority to its traffic class.	
Prioritybased	Traffic class mapping would happen only if traffic class has not been already set.	

Example --> bridge set trafficclassstatus enable

See also BRIDGE SET INTERFACE NUMTRAFFICCLASSES
BRIDGE SET INTERFACE TRAFFICCLASSMAP
BRIDGE SET INTERFACE REGENPRIORITY

2.3.4.1.48 BRIDGE SET LANTOLANFORWARDING

Syntax BRIDGE SET LANTOLANFORWARDING ENABLE/DISABLE

Description This command is used to enable/disable LAN to LAN forwarding (where data received on a LANside bridge interface is forwarded to other LAN-side bridge interface.).

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Enable	Enables LAN to LAN forwarding on the bridge.	N/A
Disable	Disables LAN to LAN forwarding on the bridge.	N/A

Example --> bridge set lantolanforwarding enable

See also BRIDGE SET WANTOWANFORWARDING ENABLE/DISABLE

2.3.4.1.49 BRIDGE SET WANTOWANFORWARDING

Syntax BRIDGE SET WANTOWANFORWARDING ENABLE/DISABLE

Description This command is used to enable/disable WAN to WAN forwarding (where data received on a WANside bridge interface is forwarded to other WAN-side bridge interface.)

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Enable	Enables WAN to WANforwarding on the bridge.	N/A
Disable	Disables WAN to WAN forwarding on the bridge.	N/A

Example --> bridge set wantowanforwarding enable

See also BRIDGE SET LANTOLANFORWARDING ENABLE/DISABLE

2.3.4.1.50 BRIDGE SHOW

Syntax BRIDGE SHOW

Description This command displays the global configuration settings for the bridge.

Example --> bridge show

See also BRIDGE LIST INTERFACES

2.3.4.1.51 BRIDGE SHOW FDB

Syntax BRIDGE SHOW FDB {<fdbname>|<fdbnumber>}

Description This command displays the statistical information of a single user-configured filtering database.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Fdbname	The name of an existing Filtering Database. See bridge add vlan CLI command to configure a new filtering database.	N/A
Fdbnumber	A number that identifies an existing filtering database. To display the list of FDBs, use the bridge list fdbs command. The number appears in the first column under the heading ID.	N/A

Example --> bridge show fdb FDB_I

```
Filtering Database Statistics:
ID | FDB Name | FID | Num VLANs | Num Entries |Num Discards | Type
-------------------------------------------------------------------------
1  | FDB1     | 1   | 1         | 0           | 0           | static
```

See also BRIDGE ADD VLAN
BRIDGE LIST FDBS

2.3.4.1.52 BRIDGE SHOW INTERFACE

Syntax BRIDGE SHOW INTERFACE {<name>|<number>}

Description This command displays configuration settings of a named bridge interface.

This command does not show the current contents of the bridge's filter table. See the CLI command bridge list ucastentries. If the LAN to LAN forwarding is disabled, then no packet received on a lan side bridge interface will be bridged to any other lan side bridge interface irrespective of the port-filter. If the WAN to WAN forwarding is disabled, then no packet received on a wan side bridge interface will be bridged to any other wan side bridge interface irrespective of the port-filter. Hence Port Filter should be interpreted accordingly.

- Filter Type: The type of Ethernet filtering performed by the named bridge interface, by default it is set to All.
- Port Filter: The list of bridge interfaces that the frames can go through, if the frames are received on this bridge interface.
- Transport: The name of the transport attached to the bridge using the bridge attach CLI command.
- PVID: Port VLAN ID associated with the interface.
- Acceptable Frame Type: Acceptable Frame Type Setting which is non-configurable and always enabled, i.e. each bridge interface can be configured to accept all frames or only tagged frames.
- User Priority: Default User Priority.
- Leave Mode: IGMP Snoop Leave Processing mode.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created.	N/A
Number	The numerical identifier automatically assigned to the object when it was created.	N/A

Example --> bridge show interface bridge1

```
Filtering entries for the FDB: FDB_1
ID| Type      | MAC Address | Receive Port
------------------------------------------------------
 1| Dest Static| 0:0:0:0:0:0 |
Egress Interfaces: bridge1
------------------------------------------------------
```

See also BRIDGE ADD UCASTENTRY SRC
BRIDGE ADD UCASTENTRY DEST
BRIDGE LIST STATIC UCASTENTRIES
BRIDGE ADD VLAN

2.3.4.1.53 BRIDGE SHOW INTERFACE REGENPRIORITY

Syntax BRIDGE SHOW INTERFACE {<name>|<number>} REGENPRIORITY

Description This command adds a named interface to the bridge.

- User Priority: It is the priority that comes in the VLAN tagged or priority tagged incoming packets as per the 802.1p.
- Regenerated priority:

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command.	N/A
Number	A number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A

Example --> bridge show interface bridge1 regenpriority

```
Bridge Interface: bridge1
-------------------------
User | Regenerated
Priority | Priority
-----------|-------------
0 | 0
1 | 1
2 | 2
3 | 3
4 | 4
5 | 5
6 | 6
7 | 7
```

See also BRIDGE LIST INTERFACES
BRIDGE ATTACH

2.3.4.1.54 BRIDGE SHOW INTERFACE TRAFFICCLASSMAP

Syntax `BRIDGE SHOW INTERFACE {< name >|< number >} TRAFFICCLASSMAP`

Description This command displays the regenerated priority to traffic class mapping. It also displays the number of traffic classes supported by the interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command.	N/A
Number	A number that identifies an existing bridge interface. To display interface names, use the bridge list interfaces command. The number appears in the first column under the heading ID.	N/A

Example --> bridge show interface bridge1 trafficclassmap

```
Bridge Interface: bridge1
Number of Traffic Classes: 8
--------------------------
Regenerated| Traffic
Priority   | Class
-----------|-------------
0 | 0
1 | 1
2 | 2
3 | 3
4 | 4
5 | 5
6 | 6
7 | 7
```

See also BRIDGE SET INTERFACE ACCEPTFRAMETYPE
BRIDGE SET INTERFACE DEFAULTUSERPRIORITY
BRIDGE SET INTERFACE NUMTRAFFICCLASSES
BRIDGE SET INTERFACE REGENPRIORITY
BRIDGE LIST INTERFACES

2.3.4.1.55 BRIDGE SHOW INTERFACESTATS

Syntax `BRIDGE SHOW INTERFACESTATS { < name > | < number > }`

Description This command displays the statistical information of one bridge interface configured by the user.

- Rx Frames: Number of frames received on the interface.
- Tx Frames: Number of frames transmitted from the interface.

- Transmit Delay Discards: Number of frames discarded due to transmit delay.
- Unknown VLAN Discards: Number of frames discarded due to unknown VLAN
- Buffer O/F Discards: Number of frames discarded due to buffer overflow.
- Ingress Discards: Number of frames discarded due to ingress filtering.
- Frame Type Discards: Number of frames discarded due to the acceptable frame type setting on the interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	The name manually assigned to the object when it was created..	N/A
Number	The numerical identifier automatically assigned to the object when it was created.	N/A

Example --> bridge show interfacestats I

```
Bridge Interface: ethernet0
Rx Frames|Tx Frames|Transmit      |Unknown VLAN|Buffer O/F|Ingress |Frame Type
         |         |Delay Discards|Discards    |Discards  |Discards|Discards
---------|---------|--------------|------------|----------|--------|----------
3686117  |3236443  |0             |0           |0         |0       |0
-------------------------------------------------------------------------------
```

See also BRIDGE ADD INTERFACE
BRIDGE ATTACH
BRIDGE LIST INTERFACE STATS

2.3.4.1.56 BRIDGE SHOW MCASTENTRY SHARED

Syntax BRIDGE SHOW MCASTENTRY SHARED {<entryname>| <entrynumber>) {<fdbname>| <fdbnumber>)

Description This command displays a statically configured multicast Forwarding entry with the given name in the named Forwarding Database.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
entryname	Name of an existing Multicast Forwarding Entry. To display the list of all statically configured multicast entries, that the user can delete, use *bridge list static mcastentries*. This command also displays the entire egress interface list for that entry.	
entrynumber	A number that identifies an existing Multicast Forwarding Entry. To display the list of statically configured multicast entries, use *bridge list static mcastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing Forwarding Database. See *bridge add vlan* CLI command to configure a new Filtering Database.	
fdbnumber	A number that identifies an existing Forwarding Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge show mcasten try shared MCAST_1 DefaultFdb

```
 Mcast Entry Name:MCAST_1
MAC Address:01:00:00:00:00:00
Egress Interfaces:bridge1
```

Description BRIDGE CLEAR MCASTENTRIES SHARED
BRIDGE ADD MCASTENTRY SHARED
BRIDGE DELETE MCASTENTRY SHARED

2.3.4.1.57 BRIDGE SHOW UCASTENTRY

Syntax `BRIDGE SHOW UCASTENTRY {<entryname>| <entryn umber>) {<fdbname>| <fdbn umber>)`

Description This command displays information about a statically configured, unicast filtering entry for a given filtering database. The fields are listed below:

- User Entry NameUser-configured filtering entry name.
- TypeType, indicating if it is a source MAC address or destination MAC address based filtering entry
- TypeEthernet MAC address associated with the entry.
- MAC AddressEthernet MAC address associated with the entry.

- Receive InterfaceReceive interface for source MAC address based entries. See the bridge add ucastentry src for more information.
- Egress InterfacesEgress interface list.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
entryname	A name that identifies an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*. This command also displays the egress interface list for each unicast entry.	
entrynumber	A number that identifies an existing unicast forwarding entry. To display the list of statically configured unicast entries, use *bridge list static ucastentries*. The number appears in the first column under the heading ID.	
fdbname	The name of an existing filtering database to which the filtering entry will be added. See Note on filtering database in this command.	
fdbn umber	A number that identifies an existing Filtering Database. To display the list of FDBs, use the *bridge list fdbs* command. The number appears in the first column under the heading ID.	

Example bridge show ucastentry UCAST_1 FDB_1

```
Output Ucast Entry Name: UCAST_1
Type:  Dest Static
MAC Address:00:00:00:00:00:01
Receive Interface:
Egress Interfaces:
```

See also `BRIDGE ADD UCASTENTRY SRC`
`BRIDGE ADD UCASTENTRY DEST`

2.4 VLAN

2.4.1 Overview

VLAN is a networking technology that allows networks to be segmented logically without having to be physically rewired.

Many Ethernet switches support virtual LAN (VLAN) technologies. By replacing hubs with VLAN switches, the network administrator can create a virtual network within existing network. With VLAN, the network logical topology is independent of the physical topology of the wiring. Each computer can be assigned a VLAN identification number (ID), and computers with the same VLAN ID can act and function as though they are all on the same physical network.

So, the traffic on a VLAN is isolated and thus all communications remain within the VLAN. The assignment of VLAN IDs is done by the switches and can be managed remotely using network management software.

VLAN switches can function in different ways. They can be switched at the data-link layer (layer 2 of the Open Systems Interconnection reference model) or the network layer (layer 3), depending on the type of switching technology used. The main advantage of using VLAN technologies is that users can be grouped together according to their need for network communication, regardless of their actual physical locations. This isolation will help to reduce unnecessary traffic so better network performance. The disadvantage is that additional configuration is required to set up and establish the VLANs when implementing these switches.

2.4.1.1 VLAN tagging

VLAN technology introduces the following three basic types of frame:

- Untagged frames
- Priority-tagged frames
- VLAN-tagged frames

An untagged frame or a priority-tagged frame does not carry any identification of the VLAN to which it belongs. Such frames are classified as belonging to a particular VLAN based on parameters associated with the receiving port.

This classification mechanism requires the association of a specific VLAN ID, the Port VLAN Identifier, or PVID, with each of the switch ports.

The PVID for a given port provides the VID for untagged and priority-tagged frames received through that port. The PVID for each port shall contain a valid VID value, and shall not contain the value of the null VLAN ID (see Table 8)

A VLAN-tagged frame carries an explicit identification of the VLAN to which it belongs; i.e., it carries a non-null VID. Such a frame is classified as belonging to a particular VLAN based on the value of the VID that is included in the tag header. The presence of a tag header carrying a non-null VID means that some other device, either the originator of the frame or a VLAN-aware switch, has mapped this frame into a VLAN and has inserted the appropriate VID.

Tagging of frames is performed for the following purposes:

- To allow user priority information to be added to frames carried on IEEE 802 LAN MAC types that have no inherent ability to signal priority information at the MAC protocol level;
- To allow a frame to carry a VID;

- To allow the frame to indicate the format of MAC Address information carried in MAC user data;
- To allow VLANs to be supported across different MAC types.

Tagging a frame requires:

- The addition of a tag header to the frame. This header is inserted immediately following the destination MAC Address and source MAC Address fields of the frame to be transmitted;
- Recomputation of the Frame Check Sequence (FCS).

When relaying a tagged frame between 802.3/Ethernet MACs, a switch may adjust the PAD field such that the minimum size of a transmitted tagged frame is 68 octets.

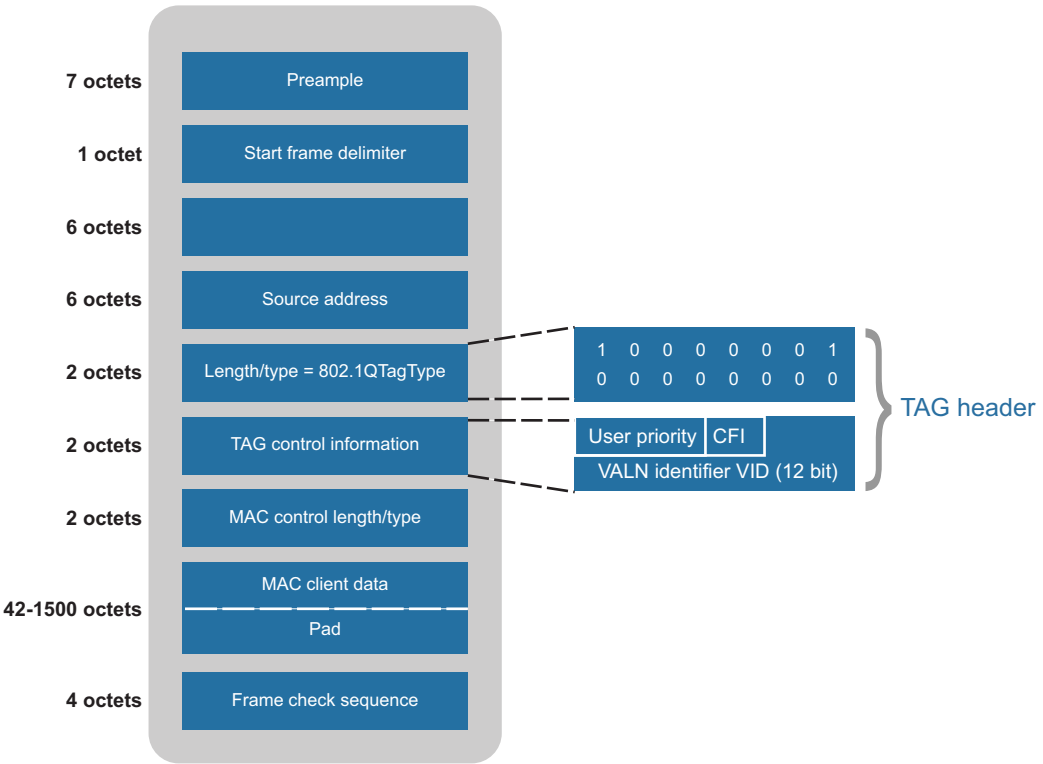


FIGURE 2-2 Tagged frame format according to IEEE 802.3ac standard

The tag header carries the following information (see Figure 2-2):

- The Tag Protocol Identifier (TPID) carrying an Ethernet Type value (802.1QTagType), which identifies the frame as a tagged frame. The value of 802.1QTagType is 81-00

- Tag Control Information (TCI). The TCI field is two octets in length, and contains user priority, CFI and VID (VLAN Identifier) fields. Figure ... illustrates the structure of the TCI field:
- User priority. The user priority field is three bits in length, interpreted as a binary number. The user priority is therefore capable of representing eight priority levels, 0 through 7. This field allows the tagged frame to carry user priority information across Bridged LANs in which individual LAN segments may be unable to signal priority.
- Canonical Format Indicator (CFI). The Canonical Format Indicator (CFI) is a single bit flag value. CFI reset indicates that all MAC Address information that may be present in the MAC data carried by the frame is in Canonical format.
- The meaning of the CFI when set depends upon the variant of the tag header in which it appears.
- In an Ethernet-encoded tag header, transmitted using 802.3/Ethernet MAC methods, CFI has the following meanings:
  - When set, indicates that the E-RIF field is present in the tag header, and that the NCFI bit in the RIF determines whether MAC Address information that may be present in the MAC data carried by the frame is in Canonical (C) or Non-canonical (N) format;
  - When reset, indicates that the E-RIF field is not present in the tag header, and that all MAC Address information that may be present in the MAC data carried by the frame is in Canonical format (C).
- VLAN Identifier (VID). The twelve-bit VLAN Identifier field uniquely identifies the VLAN to which the frame belongs. The VID is encoded as an unsigned binary number. In Table 8 are described the values of the VID field that have specific meanings or uses; the remaining values of VID are available for general use as VLAN identifiers.

A priority-tagged frame is a tagged frame whose tag header contains a VID value equal to the null VLAN ID.

TABLE 2-5 Reserved VID Values

VID Value (Hexadecimal)	Meaning/Use
0	The null VLAN ID. Indicates that the tag header contains only user priority information; no VLAN identifier is present in the frame. This VID value shall not be configured as a PVID, configured in any Filtering Database entry, or used in any Management operation.
1	The default PVID value used for classifying frames on ingress through a switch port. The PVID value can be changed by management on a per-port basis.
FFF	Reserved for implementation use. This VID value shall not be configured as a PVID, configured in any Filtering Database entry, used in any Management operation, or transmitted in a tag header.

2.4.2 VLAN Functional Description

2.4.2.1 VLAN support on Ethernet interfaces

The Gateway supports up to 16 VLANs (irrespective of whether they are carrying tagged or untagged frames) from VID=1 up to VID=4094.

If a non-tagged or null-VID tagged packet is received, the ingress port VID is used for look up.

The look up process starts with a VLAN table look up to determine whether the VID is valid.

If the VID is not valid the packet will be dropped and its address will not be learned.

If the VID is valid, FID is retrieved for further look up.

FID + DA is used to determine the destination port. FID + SA is used for learning purposes.

2.4.2.1.1 VLAN definition and port tagging

By default the Gateway starts with only one VLAN defined with name default and VID=1.

All the system ports are members of the default VLAN.

Creating and configuring a new VLAN is a two-step process:

- A VLAN is created by specifying a name for the VLAN and its VID value.
- The ports are added to the VLAN. When a port is added it's necessary to specify the frame format in which packets associated with that VLAN will be transmitted from that port: untagged or tagged.

Note that a physical port can be a member of one or more VLANs.

- A port can be member of two or more VLANs only if it is tagged on all the VLANs or it is untagged on one VLAN only and tagged on all the other VLANs. A port cannot be member of two or more VLANs as untagged port.

To change the tagged/untagged frame format of a port for a specific VLAN it's necessary remove the port from the VLAN and then re-add the port to the VLAN, specifying the required frame format.

When a port is removed from a VLAN and the same port is not a member of any other VLAN, the port is automatically added to the default VLAN with the untagged attribute.

2.4.2.2 VLAN support on ADSL interface

The ADSL Residential Gateways extend the support on tagged frames from the Ethernet ports to the ADSL port.

Specifically, only on ADSL connections that use RFC1483 encapsulation method, it's possible assign a connection to manage tagged traffic for one or more VLANs and simultaneously manage also untagged frames for one VLAN only.

2.4.2.2.1 Untagged RFC1483 connections

To assign an RFC1483 to manage untagged frames for one VLAN, use the command RFC1483 SET TRANSPORT FRAME UNTAGGED.

- All the incoming untagged frames that from the ADSL port arrive to the residential gateway on the PVC channel specific for the RFC1483 transport, are forwarded internally to the bridge software as tagged frames with the VLAN identifier equal to the VID value of VLAN specified.
- If the same RFC1483 transport has not been assigned to manage any tagged frame, any tagged incoming frames are silently discharged.
- All the outgoing tagged frames that from the bridge software must be sent outside on the ADSL port, are filtered to discharge not valid tagged frames:
- If the frame VID value in the 802.1Q header equals the VID value of VLAN specified, the 802.1Q header is removed and the frame is sent as untagged frame, otherwise the frame is silently discharged.

2.4.2.2.2 Tagged RFC1483 connections

To assign an RFC1483 to manage tagged frames for one VLAN, use the command rfc1483 set transport frame tagged.

All the incoming tagged frames that from the ADSL port arrive to the residential gateway on the PVC channel specific for the RFC1483 transport and having the VID value equal to the VID value of VLAN specified, are simply forwarded internally to the bridge software as tagged frames maintaining the same VLAN identifier.

All the incoming tagged frames that from the ADSL port arrive to the residential gateway on the PVC channel specific for the RFC1483 transport and having the VID value different to the VID value of VLAN specified are silently discharged.

Note that it's possible assign the same RFC1483 transport to manage tagged frames for more than one VLAN simply entering multiple times the command RFC1483 SET TRANSPORT FRAME TAGGED for each VLAN to be configured.

All the incoming untagged frames that from the ADSL port arrive to the residential gateway on the PVC channel specific for the RFC1483 transport, are silently discharged if the RFC1483 transport has not being assigned any VLAN as untagged transport.

- All the outgoing tagged frames that from the bridge software must be sent outside on the ADSL port, are filtered to discharge not valid tagged frames:

If the frame VID value in the 802.1Q header equals the VID value of VLAN specified, the frame is sent as tagged frame maintaining the same VLAN identifier; otherwise the frame is silently discharged.

2.4.2.3 VLAN versus IP interface

One of the major constraints when using VLANs is that packets exchanged between hosts that are members of the same VLAN cannot be received by hosts that are members of a different VLAN.

The Gateway solves this limitation by offering a packet routing service between different VLANs.

The routing of packets between VLANs is based on the classical layer 3 routing method as, for example, a typical router performs between IP interfaces.

Based on this approach, there is the requirement that each VLAN that you wish to be involved in the routing of packets must have an associated IP interface.

In this way, the Layer 3 routing process is able to treat VLAN IP interfaces as though they were distinct Ethernet ports, and route rules apply as they would for a multi-port router.

Each primary IP interface uses the VLAN data transport services (frame tagging and untagging and related layer 2 forwarding) as though it were an Ethernet port.

For the system point of view, when a VLAN is used to support an IP interface, the VLAN becomes a transport device supporting Ethernet traffic (see Figure 2-3).

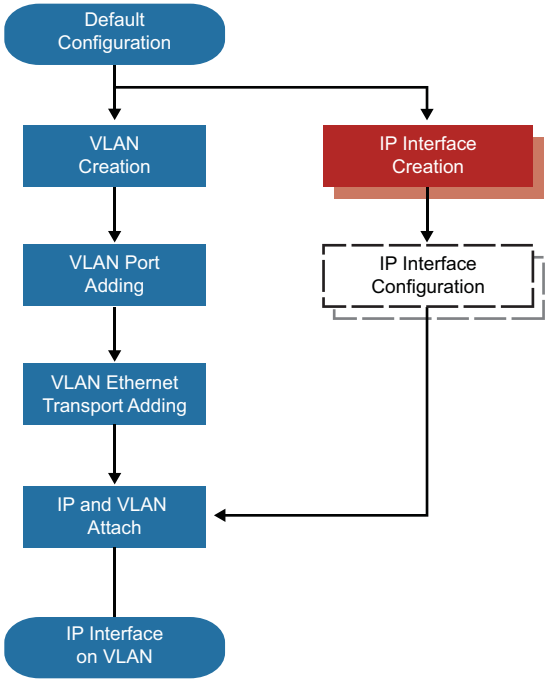


FIGURE 2-3 **IP interface over LAN - first steps**

The maximum number of primary IP interfaces that can be defined is 16 and is equal to the maximum number of VLANs that it is possible to create on the residential gateway.

When more than one IP interfaces is defined, routing between these interfaces is immediately enabled without requiring any route to be explicitly defined.

By default, the Gateway starts with one IP interface attached to the default VLAN in order to provide remote access to the system via telnet.

The default VLAN and the IP interface attached to it cannot be removed. It's possible to remove all the ports from the default VLAN if one or more other VLANs exist.

2.4.2.4 VLAN Translations

An additional feature that can be of use - when trying to match Network specified VLAN id's to a customer's network - is the use of VLAN translations. This mechanism allows the user take all traffic received from the WAN interface - on a given VLAN - and convert the VLAN TAG to an internal VID - for transfer to the LAN interfaces.

2.4.3 Functional Differences in Product Categories

There are a number of different options that are available to manage VLANs in the newer devices, however the Basics for creating and configuring a VLAN - are simplified into a small subset of commands that are described below. For more sophisticated users, access to the BRIDGE VLAN commands can provide additional flexibility.

TABLE 2-6

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VLAN tagging	X	X	X	X	X	X	X	X	X
VLAN support on Ethernet interfaces	X	X	X	X	X	X	X	X	X
VLAN support on ADSL interface							X	X	X
VLAN versus IP interface	1	2	1	2	2	2	1	2	2
VLAN Translations				X	X	X		X	X

Note 1:

To create a primary IP interface and connect it to a VLAN, the following steps must be performed.

- Create a VLAN using the VLAN ADD VID command
- Add ports to the VLAN using the VLAN ADD PORT command
- Add the VLAN to the Ethernet transports list using the ETHERNET ADD TRANSPORT command. This command instructs the system that a new (virtual) transport device has been added to the system.
- Create an IP interface with the IP ADD INTERFACE command. This command constructs a new IP interface with the specified IP address and net mask but doesn't bind the IP interface to any port.
- Bind the IP interface to the VLAN using the IP ATTACH TRANSPORT command.
  ***** It is not necessary to add the VLAN to the CPU port - when the VLAN is attached to the bridge, it is automatically added to the CPU port.

Note 2:

To create a primary IP interface and connect it to a VLAN, the following steps must be performed.

- Create a VLAN using the VLAN CREATE command - the VLAN is automatically created on the Bridge.
- Add switch ports to the VLAN using the VLAN ADD command
- Create an IP interface with the IP ADD INTERFACE command. This command constructs a new IP interface with the specified IP address and net mask but doesn't bind the IP interface to any port.
- Bind the IP interface to the VLAN using the IP ATTACH command.
  ***** If it is desired that the CPU recieve traffic in a particular VLAN, it is necessary to add the VLAN to the CPU port - in the tagged mode - using the VLAN ADD command.

2.4.4 VLAN command reference

This section describes the commands available to create, configure and manage VLANs.

2.4.4.1 VLAN CLI commands

The table below lists the VLAN commands provided by the CLI:

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
BRIDGE ADD VLAN		X		X	X	X		X	X
BRIDGE CLEAR VLANS		X		X	X	X		X	X
BRIDGE DELETE VLAN		X		X	X	X		X	X
BRIDGE LIST STATIC VLANS		X		X	X	X		X	X
BRIDGE LIST VLANS		X		X	X	X		X	X
BRIDGE SHOW VLAN		X		X	X	X		X	X
BRIDGE CLEAR INTERFACEVLAN-STATS		X		X	X	X		X	X
BRIDGE LIST INTERFACEVLANSTATS		X		X	X	X		X	X
BRIDGE SHOW INTERFACEVLAN-STATS		X		X	X	X		X	X
BRIDGE ADD VLANINTERFACE		X		X	X	X		X	X
BRIDGE CLEAR VLANINTERFACES		X		X	X	X		X	X
BRIDGE DELETE VLANINTERFACE		X		X	X	X		X	X
BRIDGEVLAN ADD TRANSPORT		X		X	X	X		X	X
BRIDGEVLAN CLEAR TRANSPORTS		X		X	X	X		X	X
BRIDGEVLAN DELETE TRANSPORT		X		X	X	X		X	X
BRIDGEVLAN LIST TRANSPORTS		X		X	X	X		X	X
VLAN ADD		X		X	X	X		X	X
VLAN ADD PORT	X		X				X		
VLAN ADD VID	X		X				X		
VLAN CREATE		X		X	X	X		X	X

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VLAN DELETE	X	X	X	X	X	X	X	X	X
VLAN LIST		X		X	X	X		X	X
VLAN SHOW	X		X				X		
VLAN TRANSLATE				X	X	X		X	X

2.4.4.1.1 BRIDGE ADD VLAN

Syntax `BRIDGE ADD VLAN <name> <vlanid> <fdb>`

Description This command adds a named VLAN (either the default VLAN or a user-defined VLAN) to the bridge. By default, all of the bridge interfaces are added to the untagged interface list of the default VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Name	An arbitrary name that identifies the VLAN. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit. Set to 'DefaultVlan' to add the default VLAN.	N/A
Vlanid	The VLAN Id that the user wants to assign to the named VLAN. The valid values for the VLAN Id ranges between 1 and 4094. Set to 1 to add the default VLAN. (VLAN Id 1 is used only for the default VLAN.)	
Fdb	The name of an existing Filtering Database with which the user wants the VLAN to be associated. If the FDB already exists, the VLAN becomes associated with that FDB. If the FDB does not exist, it is created and the VLAN becomes associated with it. See bridge list fdbs CLI commands to display all the existing filtering databases configured in the bridge and their corresponding statistics. Set to DefaultFdb' to add the default VLAN.	

Example --> bridge add vlan VLAN_1 2 FDB_1

See also BRIDGE DELETE VLAN
BRIDGE LIST STATIC VLAN
BRIDGE LIST VLANS

2.4.4.1.2 BRIDGE CLEAR VLANS

Syntax BRIDGE CLEAR VLANS

Description This command deletes the statically configured VLANs from the bridge. The egress interfaces and multicast filtering entries (for an IVM configuration) associated with the VLANs are also deleted by this command. If a VLAN is the last VLAN associated with its FDB, the FDB along with the unicast and multicast filtering entries and forward all/unregistered group entries are also deleted from the bridge.

Example --> bridge add interface bridge1

See also BRIDGE ADD VLANS
BRIDGE DELETE VLAN

2.4.4.1.3 BRIDGE DELETE VLAN

Syntax BRIDGE DELETE VLAN {<name>|<number>}

Description This command deletes a single statically configured VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing VLAN. To display the list of statically configured VLANs, use bridge list static vlans. To display the list of all the static and dynamic VLANs in the bridge use bridge list vlans CLI command	N/A
Number	A number that identifies an existing VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A

Example --> bridge delete vlan VLAN_1

See also BRIDGE ADD VLAN
BRIDGE LIST STATIC VLANS
BRIDGE LIST VLANS

2.4.4.1.4 BRIDGE LIST STATIC VLANS

Syntax `BRIDGE LIST STATIC VLANS`

Description This command displays all of the statically configured VLANs. See bridge add vlan CLI command to statically configure a VLAN. For each of the VLANs, the command displays all of the statically added egress interfaces. See the bridge add vlaninterface CLI command to add an interface to the named VLAN.

- ID: The sequence number given by the CLI system for the VLAN in the CLI listing.
- VLAN ID: A number that identifies an existing statically-configured VLAN.
- VLAN Name: A name that identifies an existing statically-configured VLAN.
- FDB Name: The name of an existing filtering database to which the filtering entry will be added. See Note on filtering database in this command.
- Tagged Interfaces: Tagged egress interface list.
- Untagged Interfaces: Untagged egress interface list.

Example --> bridge list static vlans

```
..ID..|...VLAN ID....|......VLAN Name.......|...FDB Name
------|--------------|----------------------|---------------
...1..|......2.......|.......VLAN_1.........|....FDB_1
Tagged Interfaces: bridge1
Untagged Interfaces: bridge2
-------------------------------------------------------------
```

See also `BRIDGE LIST INTERFACES`
`BRIDGE ATTACH`

2.4.4.1.5 BRIDGE LIST VLANS

Syntax `BRIDGE LIST VLANS`

Description This command adds a named interface to the bridge.

- ID: The sequence number given by the CLI system for the VLAN in the CLI listing.
- VLAN ID: A number that identifies an existing statically-configured VLAN.
- VLAN Name: A name that identifies an existing statically-configured VLAN.
- FDB Name: The name of an existing filtering database to which the filtering entry will be added. See Note on filtering database in this command.
- Type: Indicates whether the VLAN is either statically configured or dynamically learnt.
- Tagged Interfaces: Tagged egress interface list.

Example --> bridge list vlans

```
.ID.|.VLAN ID.|.VLAN Name..|.FDB Name..|.Type....|
-------------------------------------------------------------
..1.|.2.......|.VLAN_1.....|.FDB_1.....|.static..|
Tagged Interfaces: bridge1
Untagged Interfaces: bridge2
-------------------------------------------------------------
```

See also `BRIDGE ADD VLAN`
`BRIDGE ADD VLANINTERFACE`
`BRIDGE LIST STATIC VLANS`

2.4.4.1.6 BRIDGE SHOW VLAN

Syntax `BRIDGE SHOW VLAN {< name >|<number>}`

Description This command displays a single statically configured VLAN. See bridge add vlan CLI command to statically configure a VLAN. The command displays all the statically added egress interfaces of the VLAN. See bridge add vlaninterface CLI command to add an interface to a VLAN.

- VLAN: A name that identifies an existing statically-configured VLAN.
- VLAN ID: A number that identifies an existing statically-configured VLAN.
- Filtering Database: The name of an existing filtering database to which the filtering entry will be added. See Note on filtering database in this command.
- Tagged Interfaces: Tagged egress interface list.
- Untagged Interfaces: Untagged egress interface list.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable)

Name	Description	Default Value
Name	A name that identifies an existing VLAN. To display the list of statically configured VLANs, use bridge list static vlans. To display the list of all the static and dynamic VLANs in the bridge use bridge list vlans CLI command. This command also displays the egress interface list for each VLAN.	N/A

Name	Description	Default Value
Number	A number that identifies an existing VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A

Example --> bridge show vlan VLAN_I

```
VLAN: VLAN_1
VLAN Id: 2
Filtering Database: FDB_1
Tagged Interfaces: bridge1
Untagged Interfaces: bridge2
```

See also BRIDGE ADD VLAN
BRIDGE ADD VLANINTERFACE
BRIDGE LIST STATIC VLANS
BRIDGE LIST VLANS

2.4.4.1.7 BRIDGE CLEAR INTERFACEVLANSTATS

Syntax BRIDGE CLEAR INTERFACEVLANSTATS [{<vlanname>|<vlannumber>} [<interfacename>]]

Description This command clears the statistics for:

- All the egress interfaces across all the VLANs.
- All the egress interfaces for the named VLAN.
- A particular egress interface for the named VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Vlanname	The name of an existing VLAN. See bridge add vlan CLI command to configure a new VLAN.	N/A
Vlannumber	A number that identifies an existing VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A
Interfacename	The name of an egress interface of the VLAN.	N/A

Example --> bridge clear interfacevlanstats

```
--> bridge clear interfacevlanstats VLAN_1
--> bridge clear interfacevlanstats VLAN_1 bridge1
```

See also BRIDGE ADD VLAN
BRIDGE ADD VLANINTERFACE
BRIDGE LIST INTERFACEVLANSTATS

2.4.4.1.8 BRIDGE LIST INTERFACEVLANSTATS

Syntax `BRIDGE LIST INTERFACEVLANSTATS { < vlanname > | < vlannumber > }`

Description This command displays the statistical information of the egress interfaces of the named VLAN.

- Name: The name of an existing VLAN. See bridge add vlan CLI command to configure a new VLAN.
- Rx Frames: The number of frames received on the interface for the named VLAN.
- Tx Frames: The number of frames transmitted from the interface for the named VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Vlanname	The name of an existing VLAN. See bridge add vlan CLI command to configure a new VLAN.	N/A
Vlannumber	A number that identifies an existing VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A

Example --> bridge list interfacevlanstats VLAN_I

```
Interfaces Stats for the VLAN: VLAN_1
Name | Rx Frames | Tx Frames
---------|-----------|-------------
bridge1 | 56 | 72
-----------------------------------
```

See also BRIDGE ADD VLAN
BRIDGE ADD VLANINTERFACE
BRIDGE CLEAR INTERFACEVLANSTATS

2.4.4.1.9 BRIDGE SHOW INTERFACEVLANSTATS

Syntax `BRIDGE SHOW INTERFACEVLANSTATS {< vlanname > | < vlannumber >} <interfacename>`

Description This command adds a named interface to the bridge.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Vlanname	The name of an existing VLAN. See bridge add vlan CLI command to configure a new VLAN.	N/A
Vlannumber	A number that identifies an existing VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A
Interfacename	The name of an egress interface of the VLAN.	N/A

Example --> bridge show interfacevlanstats VLAN_1 bridge1

```
VLAN Interface Name: ethernet
Rx Frames | Tx Frames
|--------------------|-----------------
22 | 1056
-------------------------------------
```

See also `BRIDGE ADD VLAN`
`BRIDGE ADD VLANINTERFACE`
`BRIDGE LIST INTERFACEVLANSTATS`

2.4.4.1.10 BRIDGE ADD VLANINTERFACE

Syntax `BRIDGE ADD VLANINTERFACE {<name>|<number>} {tagged|untagged} <interfacename>`

Description This command adds an interface in the egress interface list of the named VLAN. The egress interface list for a VLAN is the union of tagged interfaces and the untagged interfaces. For the default VLAN, all the bridge interfaces, are automatically configured as its untagged egress interfaces. The user need not explicitly add untagged interfaces for the DefaultVlan. See bridge add vlan to add a default or a new VLAN. However, the user is free to add/delete the interfaces from the default VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing VLAN. To display the list of statically configured VLANs, use bridge list static vlans. To display the list of all the static and dynamic VLANs in the bridge use bridge list vlans CLI command.	N/A
Number	A number that identifies an existing VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A
Tagged	To add a port in the tagged port list of the named VLAN.	N/A
Untagged	To add a port in the untagged port list of the named VLAN.	N/A
interface name	The name of a bridge interface that has previously been added and attached to a transport using the bridge add interface and bridge attach CLI commands, respectively.	N/A

Example --> bridge add vlaninterface VLAN_1 tagged bridge1

See also `BRIDGE ADD INTERFACE`
`BRIDGE ATTACH`
`BRIDGE ADD VLAN`

2.4.4.1.11 BRIDGE CLEAR VLANINTERFACES

Syntax `BRIDGE CLEAR VLANINTERFACES {<name>|<number>} [{ tagged | untagged }]`

Description This command provides three different option to delete:

- All tagged interfaces.
- All untagged interfaces.
- All the egress interfaces, i.e., all tagged and untagged interfaces of the named VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing VLAN. To display the list of statically configured VLANs, use bridge list static vlans. To display the list of all the static and dynamic VLANs in the bridge use bridge list vlans CLI command. This command also displays the egress interface list for each VLAN.	N/A
Number	A number that identifies an existing VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A
Tagged	Removes all the tagged interfaces from the egress interface list of the VLAN. If no tagged / untagged option is given in this command, all the egress interfaces are removed from the VLAN.	N/A
Untagged	Removes all the untagged interfaces from the egress interface list of the VLAN. If no tagged / untagged option is given in this command, all the egress interfaces are removed from the VLAN.	N/A

Example --> bridge clear vlaninterfaces

See also
```
BRIDGE ADD VLAN
BRIDGE ADD VLANINTERFACE
BRIDGE LIST STATIC VLANS
BRIDGE LIST VLANS
```

2.4.4.1.12 BRIDGE DELETE VLANINTERFACE

Syntax `BRIDGE DELETE VLANINTERFaCE {<name>|<number>} <interfacename>`

Description This command removes an interface from the egress interface list of the named VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Name	A name that identifies an existing VLAN. To display the list of statically configured VLANs, use bridge list static vlans. To display the list of all the static and dynamic VLANs in the bridge use bridge list vlans CLI command.	N/A
Number	A number that identifies an existing VLAN which is an egress interface in the VLAN. To display the list of statically configured VLANs, use the bridge list static vlans command. The number appears in the first column under the heading ID.	N/A
Interfacename	The name of a bridge interface, which belongs to the egress interface list of the VLAN.	N/A

Example --> bridge delete vlaninterface VLAN_I bridgeI

See also
```
BRIDGE ADD VLAN
BRIDGE ADD VLANINTERFACE
BRIDGE LIST STATIC VLANS
BRIDGE LIST VLANS
```

2.4.4.1.13 BRIDGEVLAN ADD TRANSPORT

Syntax `BRIDGE VLAN ADD TRANSPORT <name> <vlanid>`

Description This command adds a named VLAN transport corresponding to a VLAN Id. By attaching an IP interface to this transport, the IP interface will be able to send and receive traffic on the VLAN with Id as <vlanid>. Section 23.5 describes the CLI command to attach an IP interface to a VLAN transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
name	A name that identifies a VLAN transport. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	

vlanid	VLAN Id on which the transport is created. A VLAN corresponding to the vlanid should be already created for this command to be successful. Use *bridge add vlan* CLI command to add a VLAN.	

Example bridgevlan add transport vt1 2

See also `bridgevlan delete transport`
`bridgevlan list transports`

2.4.4.1.14 BRIDGEVLAN CLEAR TRANSPORTS

Syntax `BRIDGEVLAN CLEAR TRANSPORTS`

Description *This command deletes all the configured VLAN transports from the system.*

Options None

Example bridgevlan clear transports

See also `bridgevlan add transport`
`bridgevlan list transports`

2.4.4.1.15 BRIDGEVLAN DELETE TRANSPORT

Syntax `BRIDGEVLAN DELETE TRANSPORT {<name> | <number>}`

Description This command deletes a single configured VLAN transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
name	A name that identifies an existing VLAN transport. To display the list of configured VLAN transports, use *bridgevlan list transports* CLI command.	
number	A number that identifies an existing VLAN transport. To display the list of configured VLAN transports, use *bridgevlan list transports*. The number appears in the first column under the heading ID.	

Example bridgevlan delete transport vt1

See also `bridgevlan add transport`
`bridgevlan list transports`

2.4.4.1.16 BRIDGEVLAN LIST TRANSPORTS

Syntax `BRIDGEVLAN LIST TRANSPORTS`

Description This command displays information about all of the configured VLAN transports. See bridgevlan add transport on page 62. The following fields are displayed:

- IDThe numerical identifier automatically assigned to the object when it was created.
- NameThe name that identifies an existing VLAN transport.
- VLAN IDThe numerical identifier automatically assigned to the VLAN object when it was created.
- IP InterfaceIP interface associated with the transport, if any.

Options None

Example bridgevlan list transports

See also `bridgevlan add transport`
`ip interface attachbridgevlan`

2.4.4.1.17 VLAN ADD

Syntax `VLAN ADD < vlanname > < portname > FRAME { TAGGED | UNTAGGED }`

Description This command adds an Ethernet port to an existing named VLAN that has been created with the command VLAN ADD VID.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Vlanname	An existing VLAN. To display the existing VLANs, use the VLAN LIST command.	N/A
Portname	The name of the switch port to be configured. Available ports are: lan1 lan2 lan3 lan4 lan5 lan6 cpu	N/A

Name	Description	Default Value
TAGGED/ UNTAGGED	Specify if the switch port must be set as tagged or untagged port for the selected vlan.	N/A

Example --> vlan add voip lan1 frame tagged

See also VLAN LIST

2.4.4.1.18 VLAN ADD PORT

Syntax VLAN ADD <vlanname> PORT <portname> FRAME {TAGGED | UNTAGGED}

Description This command adds an Ethernet port to an existing named VLAN that has been created with the command VLAN ADD VID.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
vlanname	An existing VLAN. To display the existing VLANs, use the VLAN SHOW command.	N/A
portname	A name that identifies an Ethernet port. Valid port names (case insensitive) are lan1, lan2, lan3 and lan4.	N/A
FRAME	The FRAME parameter specifies whether a VLAN tag header is included in each frame transmitted on the specified ports. If tagged is specified, a VLAN tag is added to frames prior to transmission. The port is then called a tagged port for this VLAN. If untagged is specified, the frame is transmitted without a VLAN tag. The port is then called an untagged port for this VLAN.	N/A

Example vlan add voip port lan1 frame untagged

See also VLAN SHOW

2.4.4.1.19 VLAN ADD VID

Syntax VLAN ADD <vlanname> VID <vlanID> [802.1p_priority <priority>]

Description This command defines a new VLAN that has the specified VID value.

The VLAN name can be 16 characters length; it cannot start with a digit and cannot contain dots '.' or the slash symbols '/'.

This command specifies also the priority value of the tagged packets that from the network processor are sent to the layer 2 switch and then to the network.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
vlanname	An arbitrary name that identifies the VLAN. The name must not be already in use for another VLAN. The VLAN name can be at most 16 chars long.	N/A
vlanID	The VLANID parameter specifies a unique VLAN Identifier (VID) for the VLAN. If tagged ports are added to this VLAN, the specified VID is used in the VID field of the tag in outgoing frames. If untagged ports are added to this VLAN, the specified VID only acts as an identifier for the VLAN in the Forwarding Database. The default port based VLAN has a VID of 1.	N/A
priority	It's the priority value as defined in 802.1p of the tagged packets that from the Residential Gateway network processor are sent to the switch and then outside to the network. Available values are in the range 0 to 7.	0

Example `vlan add voip vid 10 802.1p_priority 7`

See also `VLAN SHOW`

2.4.4.1.20 VLAN CLEAR

Syntax `VLAN CLEAR < vlanname >`

Description This command removes an existing vlan from the vlan database.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Vlanname	An existing VLAN. To display the existing VLANs, use the VLAN LIST command.	N/A

Example --> vlan clear voip

See also `VLAN LIST`

2.4.4.1.21 VLAN CREATE

Syntax `VLAN CREATE < vlanname > < vlanid >`

Description This command defines a new VLAN and specifies the corresponding VLAN identifier (VID).

The VLAN name can be 16 characters length; it cannot start with a digit and cannot contain dots '.' or the slash symbols '/'.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Vlanname	An arbitrary name that identifies the VLAN. The name must not be already in use for another VLAN. The VLAN name can be at most 16 chars long.	N/A
Vlanid	The VLANID parameter specifies a unique VLAN Identifier (VID) for the VLAN. If tagged ports are added to this VLAN, the specified VID is used in the VID field of the tag in outgoing frames. If untagged ports are added to this VLAN, the specified VID only acts as an identifier for the VLAN in the Forwarding Database. The default port based VLAN has a VID of 1.	N/A

Example
--> vlan create voip vid 10
--> vlan create wan_net 20
--> vlan create lan_net 20
--> vlan add interface wan_net wan frame tagged
--> vlan add interface lan_net lan1 frame untagged

```
--> vlan add interface wan_net  cpu frame tagged
--> vlan add interface lan_net  cpu frame tagged
--> vlan translate lan_net 20
--> vlan translate wan_net 10
```

See also `VLAN LIST`

2.4.4.1.22 VLAN DELETE

Syntax `VLAN DELETE <vlanname> <portname>`

Description This command removes a switch port to be membership of an existing VLAN.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Vlanname	An existing VLAN. To display the existing VLANs, use the VLAN LIST command.	N/A
Portname	The name of the switch port to be configured. Available ports are: lan1 lan2 lan3 lan4 lan5 lan6 cpu wan cesc cesd	N/A

Example --> vlan delete voip lan1

See also `VLAN ADD PORT`
`VLAN ADD VID`
`VLAN SHOW`

2.4.4.1.23 VLAN LIST

Syntax `VLAN LIST`

Description This command display the following information about all the VLANs defined in the system:

- VLAN Name: The name of the VLAN.
- VLAN ID: The numerical VLAN identifier of the VLAN (VID).
- Untagged port(s): A list of untagged ports that belong to the VLAN.
- Tagged port(s): A list of tagged ports that belong to the VLAN.

Example --> vlan list

```
VLANs:
  ID | VLAN ID | VLAN   Name     |
-----|---------|-----------------|-
   1 | 1       | DefaultVlan     |
Tagged Ports:    cpu
Untagged Ports:
-----------------------------------
   2 | 200     | vlan_int        |
Tagged Ports:    cpu
Untagged Ports:  lan1  lan2  lan3  lan4
-----------------------------------
   3 | 1200    | vlan_dmz        |
Tagged Ports:    cpu
Untagged Ports:  lan5  lan6
-----------------------------------
```

See also `VLAN ADD PORT`
`VLAN ADD VID`

2.4.4.1.24 VLAN SHOW

Syntax `VLAN SHOW`

Description This command display the following information about all the VLANs defined in the system:

- **Name**- The name of the VLAN.
- **Identifier**- The numerical VLAN identifier of the VLAN (VID).
- **Status -** The status of the VLAN (only static VLAN are supported)
- **Untagged port(s) -** A list of untagged ports that belong to the VLAN.
- **Tagged port(s) -** A list of tagged ports that belong to the VLAN.
- **802.1p priority -** The value of the 802.1.p priority assigned to packets sent from the Residential Gateway processor.

Example `vlan show`

```
VLAN information
-----------------------------------------
Name: default
   Identifier                1
   Status                    static
   802.1p Priority           7
   Untagged port(s)          lan3, lan2
   Tagged port(s)            cpu
Name: voip
   Identifier                10
   Status                    static
   802.1p Priority           7
   Untagged port(s)          lan2
   Tagged port(s)            lan1

-----------------------------------------
```

See also VLAN ADD PORT
VLAN ADD VID

2.4.4.1.25 VLAN TRANSLATE

Syntax VLAN TRANSLATE<vlanname> <vlanid>

Description This command will create a software base VLAN translation. This process can be CPU intensive and should not be used for video:

- VLAN Name: The name of the VLAN.
- VLAN ID: The numerical VLAN identifier of the VLAN (VID).
- Untagged port(s): A list of untagged ports that belong to the VLAN.
- Tagged port(s): A list of tagged ports that belong to the VLAN.

Example

```
--> vlan create wan_net 20
--> vlan create lan_net 20
--> vlan add interface wan_net  wan frame tagged
--> vlan add interface lan_net  lan1 frame untagged
--> vlan add interface wan_net  cpu frame tagged
--> vlan add interface lan_net  cpu frame tagged
--> vlan translate lan_net 20
--> vlan translate wan_net 10
```

This command defines a new VLAN and specifies the corresponding VLAN identifier (VID).

The VLAN name can be 16 characters length; it cannot start with a digit and cannot contain dots '.' or the slash symbols '/'.

Options

The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Name	Description	Default Value
Vlanname	An arbitrary name that identifies the VLAN. The name must not be already in use for another VLAN. The VLAN name can be at most 16 chars long.	N/A
Vlanid	The VLANID parameter specifies a unique VLAN Identifier (VID) for the VLAN. If tagged ports are added to this VLAN, the specified VID is used in the VID field of the tag in outgoing frames. If untagged ports are added to this VLAN, the specified VID only acts as an identifier for the VLAN in the Forwarding Database. The default port based VLAN has a VID of 1.	N/A

3. IGMP

3.1 IGMP snooping

3.1.1 Multicasting overview

Multicasting is a technique developed to send packets from one location in the Internet to many other locations, without any unnecessary packet duplication. In multicasting, one packet is sent from a source and is replicated as needed in the network to reach as many end-users as necessary.

The concept of a group is crucial to multicasting. Every multicast stream requires a multicast group; the sender (or source) transmits to the group address, and only members of the group can receive the multicast data. A group is defined by a Class D address.

Multicasting is useful because it conserves bandwidth by replicating packets as needed within the network, thereby not transmitting unnecessary packets. Multicasting is the most economical technique for sending a packet stream (which could be audio, video, or data) from one location to many other locations on the Internet simultaneously.

Of course, multicasting has to be a connectionless process. The server simply sends out its multicast UDP packets, with no idea of whom will be receiving them, and whether they get received. It would be quite impossible for the server to have to wait for ACKs from all the recipients, and remember to retransmit to those recipients from whom it does not receive ACKs. Apart from anything else the server does not know who the recipients are, or how many there are.

3.1.1.1 Multicast Group addresses

A multicast stream is a stream of data whose destination address is a multicast address – i.e. an IP address with the first byte having a value of 224 to 240. The destination address used by a stream is referred to as its Group address. These Group Addresses, like all IP addresses, are a limited resource, and there are all sorts of rules about who may use addresses from which address ranges.

A server sends out a multicast stream to a group multicast address but the way it is routed to the hosts that actually want to receive it is a very different process to routing unicast packets. With unicast packets, the destination address of the packet uniquely identifies the host who should receive the packet and all the routers along the path just need to look in their routing tables to work out which is the correct route to send the packet down.

However, in the case of multicast, the stream is simply being sent out, with no particular knowledge of who wants to receive it, and where the recipients are. One approach would be for every router that receives a multicast stream on one interface to just retransmit that stream out ALL its other interfaces. In that way it would be guaranteed to eventually reach every host that might be interesting in receiving it. However, that would be an inefficient use of bandwidth, as a lot of the time the routers would sending the streams out along paths that do

not contain any hosts that want to receive them. Given that the main reason for having multicasting is to make efficient use of bandwidth, this would not be a good approach.

So, a more efficient approach is needed. This is where IGMP comes in.

3.1.1.2 IGMP protocol

IGMP (*Internet Group Management Protocol*) is the protocol whereby hosts indicate that they are interested in receiving a particular multicast stream. When a host wants to receive a stream (in multicast jargon, this is called '*joining a group*') it sends to its local router an IGMP packet containing the address of the group it wants to join – this is called an IGMP Membership report (sometimes called a *Join packet*).

Now, the local router is generally going to be a long way from the server that is generating the stream. So, having received the IGMP join packet, the router then knows that it has to forward the multicast stream onto its LAN (if it is not doing so already). However, if the router is not already receiving the multicast stream from the server (probably many hops away) what does the router do next in order to ensure that the multicast stream gets to it? This is achieved by elaborate process involving multicast routing protocols like PIM, DVMRP, and MOSPF.

The IGMP packet exchange works as described in the following paragraphs.

At a certain period (default is 125 seconds), the router sends an IGMP query message onto the local LAN. The destination address of the query message is a special '*all multicast groups*' address. The purpose of this query is to ask, "Are there any hosts on the LAN that wish to remain members of Multicast Groups?"

Hosts on the LAN receive the query, if any given host wishes to remain in a Multicast group; it sends a new IGMP Membership report (Join message) for that group (of course some hosts may be members of more than one group – so they will send join messages for all the groups that they are members of).

The router looks at the responses it receives to its query, and compares these to the list of Multicast streams that it has currently registered to receive. If there are any items in that list for which it has not received query responses, it will send a message upstream, asking to no longer receive that stream – i.e. to be 'pruned' from the tree through which that stream is flowing.

In IGMP version 2, the IGMP leave message was added. So, a host can now explicitly inform its router that it wants to leave a particular multicast group. So, the router keeps a table of how many hosts have joined particular groups, and removes hosts from the table when it receives leave messages, then it can know straight away when there are no hosts on its LAN that are still members of a given group. So, it can ask to be pruned from that tree straight away, rather than having to wait until the next query interval.

3.1.1.3 Multicast MAC addresses

Multicast IP addresses are Class D IP addresses. So, all IP addresses from 224.0.0.0 to 239.255.255.255 are multicast IP addresses. They are also referred to as *Group Destination Addresses* (GDA).

For each GDA there is an associated MAC address. This MAC address is formed by 01-00-5e, followed by the last 23 bits of the GDA translated in hex. Therefore:

230.20.20.20 corresponds to MAC 01-00-5e-14-14-14

224.10.10.10 corresponds to MAC 01-00-5e-0a-0a-0a

Consequently, this is not a one-to-one mapping, but a one-to-many mapping:

224.10.10.10 corresponds to MAC 01-00-5e-0a-0a-0a

226.10.10.10 corresponds to MAC 01-00-5e-0a-0a-0a, as well.

It is required that when an IP multicast packet is sent onto an Ethernet, the destination MAC address of the packet must be the MAC address that corresponds to the packet's GDA. So, it is possible, from the destination MAC address of a multicast packet, to know the set of values that its GDA must fall within.

3.1.2 IGMP snooping Functional Overview (Includes New Functionality)

IGMP snooping is a filtering process performed at layer 2 to reduce the amount of multicast traffic on a LAN.

It is designed to solve the problem when a multicast traffic is received from a layer 2 switch due to join requests performed by hosts connected to some of the switch ports.

If individual hosts on the LAN (i.e. hosts connected to ports on the switches) wish to receive multicast streams, then they will send out IGMP joins, which will get up to the multicast router; and the router will join into the appropriate multicast trees; and the multicast flows will then reach the router, and it will forward them into the LAN.

By default, when a switch receives a multicast packet, it must forward it out all its ports (except the port upon which it was received). So, considering the example where only host number 1 actually requests to join a particular multicast group, what will happen is that all the hosts on the LAN will start receiving the multicast packets, as all the switches will forward the multicast packets to all their ports.

This is rather a waste of bandwidth, and the purpose of multicasting is to make efficient use of bandwidth.

The solution to this problem is to make the layer-2 switch aware of the IGMP packets that are being passed around. That is, although the IGMP packets are destined for the router, the layer-2 switch needs to 'snoop' them as they go past. Then the layer-2 switch can know which hosts have asked to join which multicast groups, and only forward the multicast data to the places where it really needs to go.

Because the uplink interface can be connected to the network through an ADSL port, the igmp snooping feature is extended to include also the ADSL port when it is used on RFC1483 (bridged) connections.

IGMP snooping is designed to work in a network environment where both multicast router(s) and multicast host(s) are present.

Note: Multicast packets having as destination IP the following range: 224.0.0.[0-255] and 224.0.1.[0-255] will NOT be blocked in the upstream direction since belonging to reserved traffic (OSPF, RIPv2, PIM etc…)

The goal is to construct an internal view of the multicast network based on the IGMP messages received both from multicast router(s) and multicast host(s).

The following sections describe the IGMP snooping functionality for iMG models belonging to group Fiber-B, Fiber-D, Fiber-E, Modular and ADSL-B, ADSL-C.

3.1.2.1 Multicast router port discovery

The system listens for IGMP General Query messages and records the port(s) where any such message has been received.

In this way the Gateway knows where multicast routers are located in order to forward IGMP report and leave messages only to the correct uplink port(s).

Once the Residential Gateway has detected where the multicast router is located, it keeps the entry for a period of time defined by the Bridge Multicast Interface Aging Time attribute.

If a new IGMP General Query is received, the multicast router timer is refreshed and the corresponding uplink port is updated if needed.

If the multicast entry expires before any IGMP General Query is received, forwarding of any multicast stream to internal hosts is stopped.

It's therefore recommended that the multicast uplink interface timer is longer than the query interval configured on the multicast router (two times the query interval, at least).

Then the forwarding of IGMP queries from multicast router and the forwarding of IGMP report/leave messages from internal multicast hosts follows different schemes depending if the IGMP process on the

Residential Gateway is working in Snoop-Only mode or it is configured to work in Proxy mode.

Independently on the operational mode, the IGMP process on the Residential Gateway keeps always a view of the multicast network updating the local multicast group database

3.1.2.2 Snoop-Only Operation Mode

Snoop-Only mode is the default operational mode for IGMP snooping. It's possible to force the IGMP snooping to work in Snoop-Only mode via the bridge set igmp snooping mode snooponly command.

Before changing the igmp operational mode it's always recommended to disable the IGMP process via the bridge set igmpsnooping disable command and then re-enable it after the configuration changes have been entered.

When operating in Snoop-Only mode, the IGMP process does not act any change on IGMP messages. IGMP source IP and MAC addresses are left unchanged and they are forwarded through the Residential Gateway as they arrive to the CPE.

IGMP process checks only if there are hosts that have joined or left multicast streams in order to update the local multicast group database.

The following picture shows an example of IGMP messages flow when Snoop-Only mode is active.

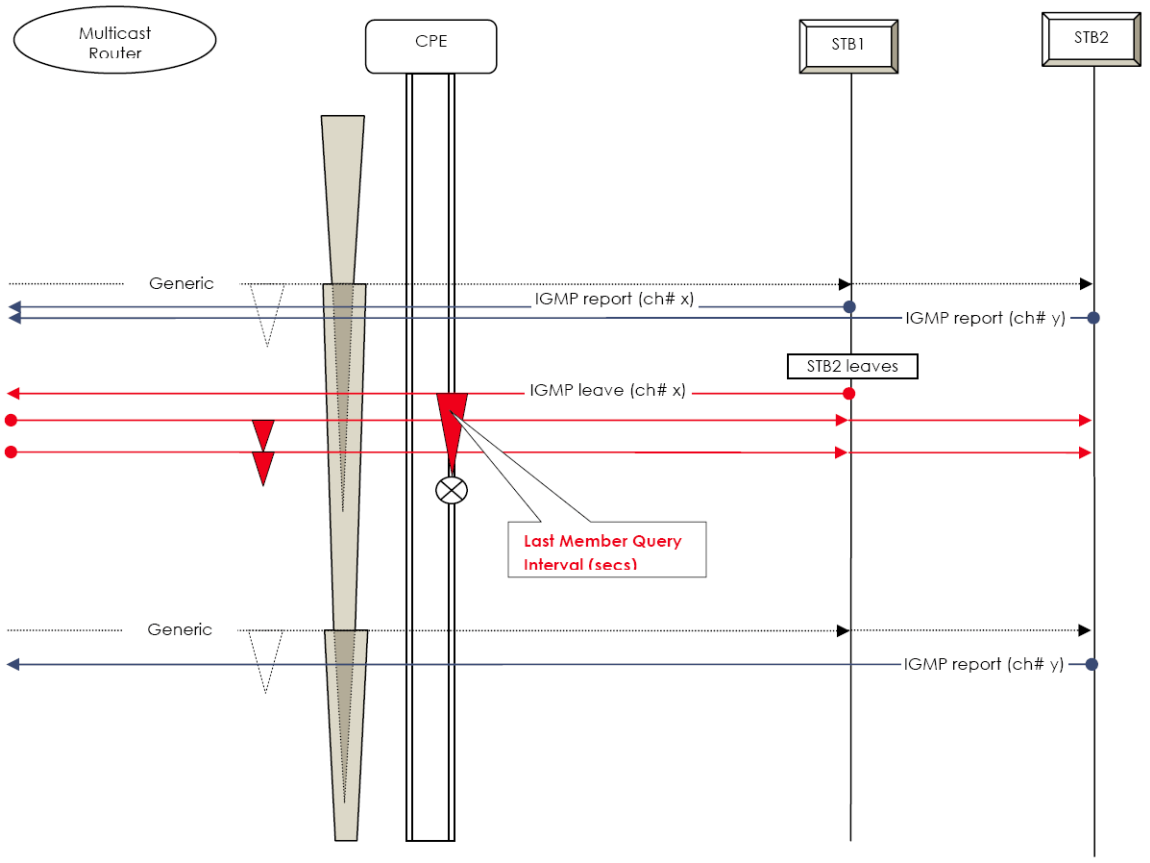


FIGURE 3-1 **IGMP messages flow when Snoop-Only mode is active**

3.1.2.2.1 Joining a Multicast Group

The Residential Gateway detects unsolicited IGMP Report messages that hosts send to join a multicast channel.

The Residential Gateway updates the local multicast group database storing the information about the requested stream and the requesting port.

The IGMP process then forwards immediately the IGMP Report message to the multicast router.

Local igmp entries can be displayed via the bridge list igmpsnooping groupinfo command.

As soon the multicast router opens the multicast stream towards the Residential Gateway, the port that requested that stream starts to receive it.

3.1.2.2.2 Leaving a multicast group

Periodically the multicast router sends Generic Queries to check whether there are multicast hosts that are still active.

If one or most hosts are still interested to receive multicast streams, they will reply with IGMP Report messages and the corresponding entries on the local multicast group database will be refreshed.

When an host wants to leave group, it sends an IGMP Leave message specific for the group it wants to leave.

The IGMP Leave message is then forwarded to the upstream multicast router and a timer equals to the Last Member Query Interval secs is started for the corresponding local igmp entry.

When this timer expires, the IGMP process stops the forwarding of the multicast stream on the port that has received the IGMP leave message.

This mechanism is used to reduce the flooding of unsolicited multicast streams in case the multicast upstream router takes a long time before closing the multicast stream towards the Residential Gateway.

The upper multicast router can decide to keep open the multicast stream towards the Residential Gateway if it has detected that there are other hosts interested to receive the multicast stream.

This is usually done by the upper multicast router upon the reception of an IGMP leave messages sending one or more specific queries for the multicast stream just left.

3.1.2.3 Proxy Operational Mode

Proxy Mode is an operational mode where the Residential Gateway takes a more active roll in the management of the IGMP messages.

IGMP messages received from the upper multicast router or from the internal hosts are always terminated into the Residential Gateway.

IGMP messages sent by the Residential Gateway to the internal hosts or to the upper multicast router will use the CPE source IP and MAC addresses creating in this way a demarcation point between the access and the user network.

3.1.2.3.1 Joining a Multicast Group

As for IGMP Snoop-Only mode, the system listens for unsolicited IGMP Report messages that hosts send to join a multicast group.

The Residential Gateway updates the local multicast group database storing the information about the requested stream and the requesting port.

If the received IGMP report message is the first one (i.e. no other hosts have requested the same multicast stream), then the IGMP process forwards immediately the IGMP Report message to the upper multicast router (replacing the source IP and MAC addresses).

Instead, if the received IGMP report message refers to a multicast channel that is already registered in the local database, the IGMP process will drop it without forwarding it to the multicast router and will update the local database, if needed.

Periodically the multicast router sends Generic Queries to check the presence of active multicast hosts.

Then the IGMP process answers to each IGMP query notifying all the multicast stream registered on the local multicast group database without querying the internal hosts.

The upper multicast router does not have therefore any knowledge of the internal lan configuration. IGMP reports (and leaves) messages are always sent by the CPE IGMP process using the Residential Gateway IP and MAC source address.

In order to keep the local multicast group database up to date, the IGMP process sends periodically IGMP generic queries to the internal hosts. The period IGMP queries are sent, is called Query Interval. Each host still interested to receive multicast streams must respond with one or more IGMP Report messages within a time-frame called Query Response Interval.

The picture here below shows an example scenario where two hosts join two different multicast channels.

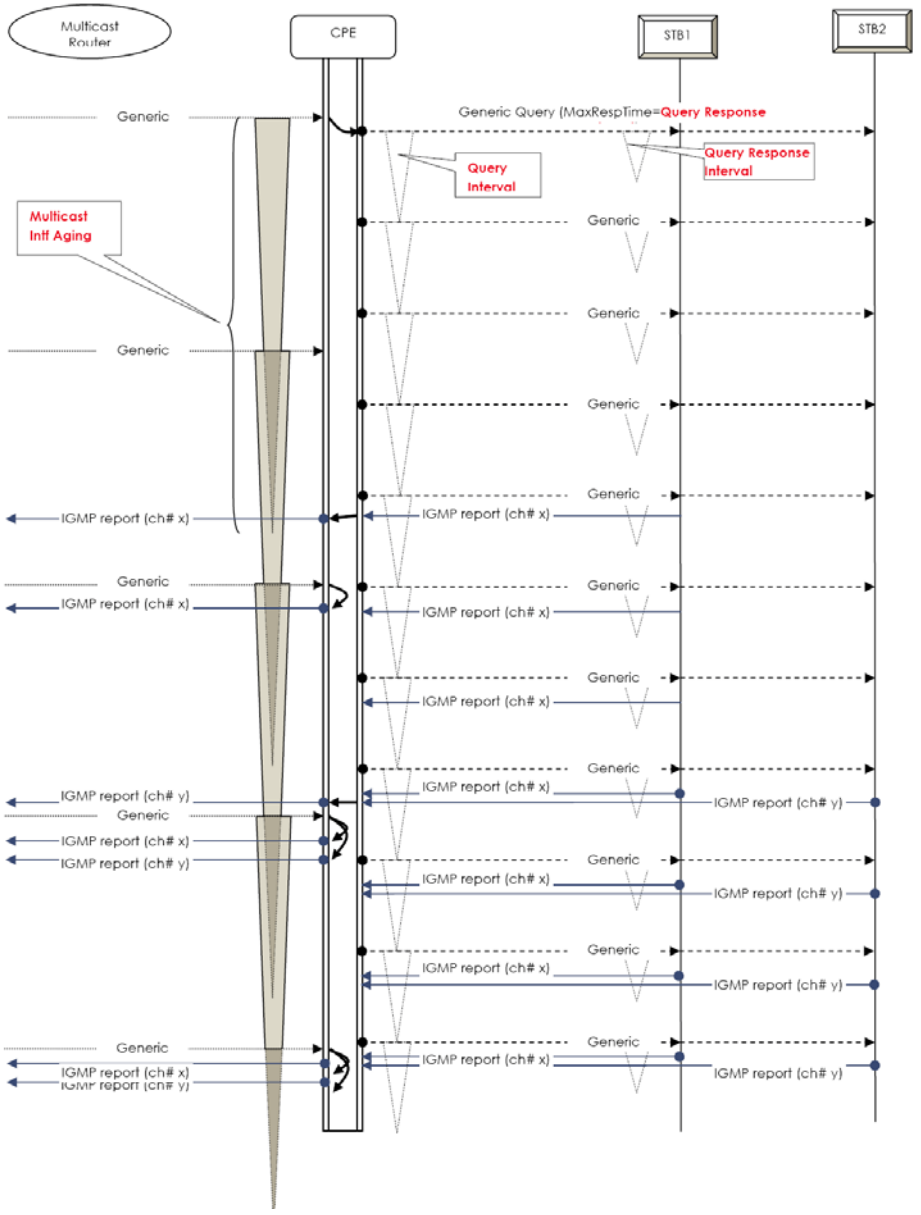


FIGURE 3-2 Two Hosts Join Two Different Mulitcast Channels

3.1.2.3.2 Leaving a Multicast Stream

Under Proxy operational mode, when an host wants to leave a multicast group and sends an IGMP Leave message, the IGMP process takes different actions depending if the Fast Leave feature is enabled or disabled.

- Fast Leave Disabled

Upon the reception of an IGMP leave message, the IGMP process starts sending IGMP Specific Queries to the port that has received the leave message to double check whether that there are other hosts still interested to receive the multicast stream.

The number of IGMP specific queries sent by the Residential Gateway is defined by the Robustness attribute. The max response time that the IGMP process wait for an answer is defined by the Last Member Query Interval value.

If no hosts answer to the Residential gateway in a timeframe less than Last Member Query Interval times the Robustness variable, the Residential Gateway will purge from the local igmp database the entry that matches the multicast stream and the corresponding port.

Then, if there are no other hosts on the other ports that are listening the same multicast stream, the IGMP process will send an IGMP leave message to the multicast router to inform it that it can close the multicast stream towards the Residential Gateway.

The picture here below shows an example scenario where two hosts join two different multicast channels.

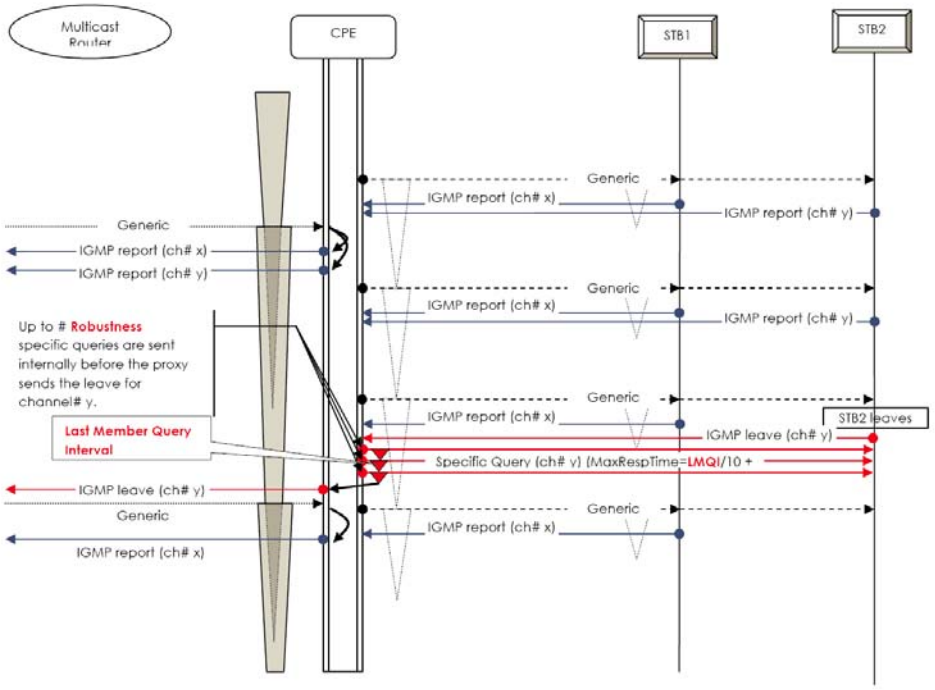


FIGURE 3-3 Two Hosts Join Two Different Multicast Channels

In case a multicast host is disconnected from the network, the IGMP process is able to detect such condition checking the absence of IGMP reports on the port where the host left.

This process takes a time that is usually longer than the case where the host leaves the network in a gracefully way. The IGMP process has to wait for no answers to the internal Generic Queries a number of times equals to the Robustness attribute value.

The picture here below shows an example where an host disconnects from the network without sending any IGMP leave message.

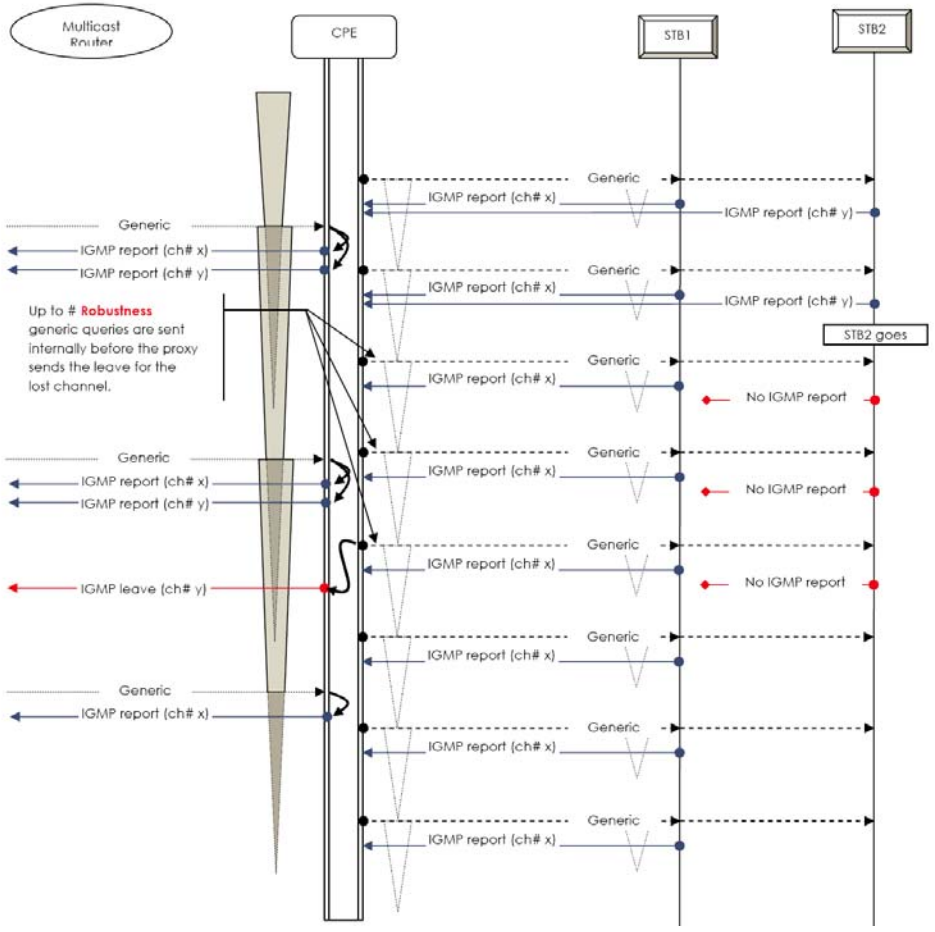


FIGURE 3-4 Host Disconnects - No Leave Message

- Fast Leave Enabled

When Fast Leave support is enabled, upon the reception of an IGMP leave message, the IGMP process stops immediately the forwarding of multicast stream towards the internal host.

The IGMP process does not send any specific query to check if there are other hosts still interested to receive the multicast stream.

When the IGMP process receives the IGMP leave message, if there are no other hosts receiving the same stream on other ports, it sends immediately an IGMP leave message to the multicast router.

In case other hosts have joined the same multicast stream, the IGMP process purges only the entry matching the corresponding lan port and drop the IGMP leave message.

The picture here below shows an example scenarios where an host leaves a multicast stream and a scenario where two hosts leave the same multicast stream.

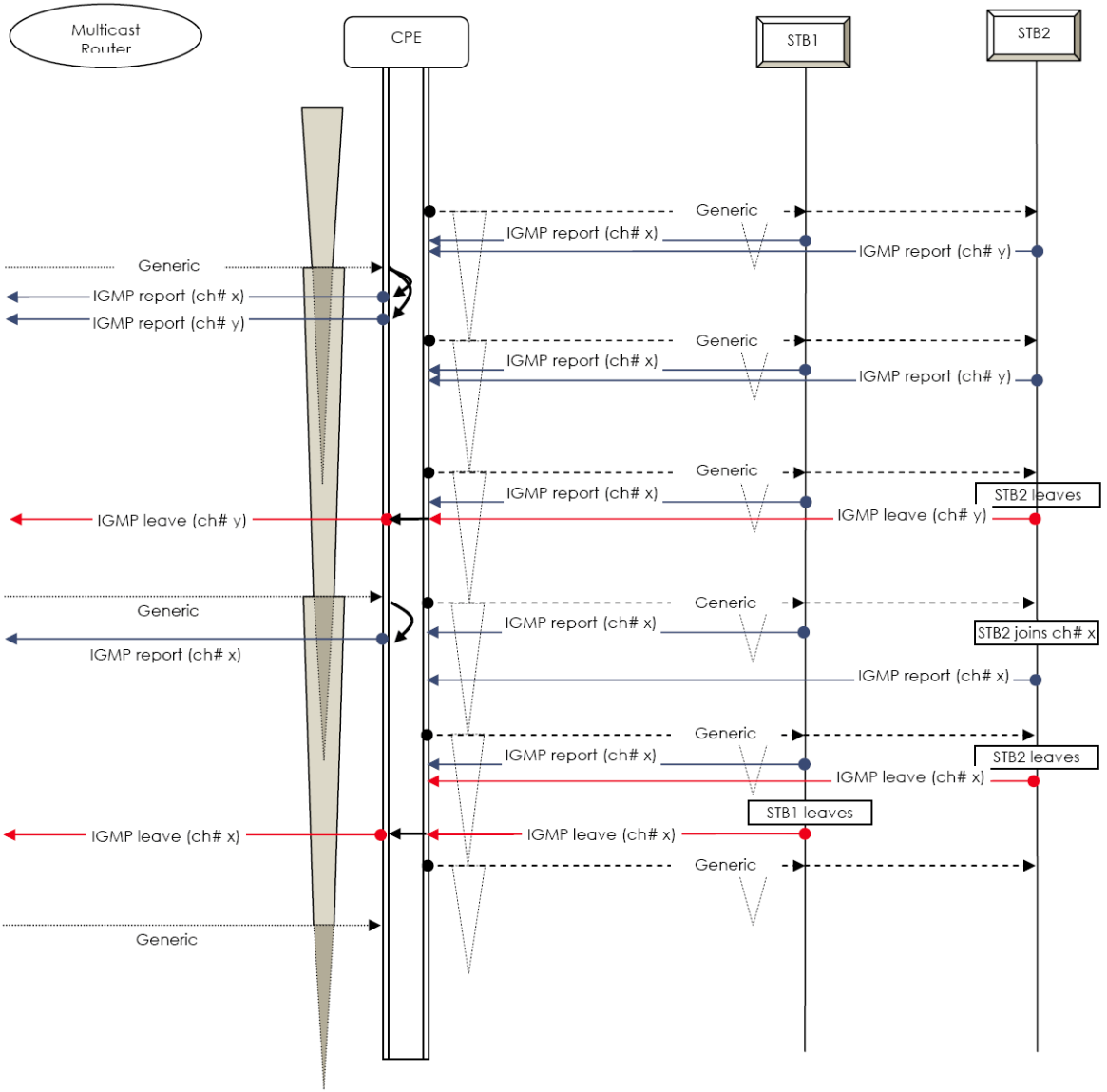


FIGURE 3-5 One and Two Hosts Leave the Same Multicast Stream

3.1.3 Old IGMP Snooping Functionality

The following sections describe the IGMP snooping functionality for iMG models belonging to group Fiber-A, Fiber-C, and ADSL-A.

3.1.3.1 Multicast router port discovery

IGMP snooping is activated using the IGMP SNOOPING ENABLE command.

The system listens for IGMP Membership General Query packets sent to the address 01-00-5e-00-00-01 and records the port(s) where any such message has been received.

In this way the Residential Gateway knows where multicast routers are located in order to forward report and leave messages only to the correct port(s).

Note that even if multiple VLANs can be present in the system, the IGMP snooping feature can be turned on only on one VLAN at time.

3.1.3.2 Snoop-Only Operation Mode

3.1.3.2.1 Joining a Multicast Group

The system listens for unsolicited IGMP Report messages that hosts send to join a multicast group and records the port where each message has been received. What happens next depends on the circumstances in which the packet is received. To understand this, let us consider two possible scenarios:

- First Scenario:

Host A is the first host in an Ethernet segment to join a group.

Host A sends an unsolicited IGMP Membership report.

The Residential Gateway intercepts the IGMP membership report sent Host A and creates a multicast entry for the group that host A was requesting. It then links this entry to the port on which it has received the report.

It also sets, for this port and this multicast group , a local Timeout timer to the Timeout Interval value This timer is used to refresh the multicast membership table periodically.

The system then forwards the IGMP report on to the multicast router. In this way the router will also receive the IGMP report and will update its multicast routing table accordingly. If no Multicast router has been detected, then it does nothing.

Immediately multicast traffic for the requested group address is forwarded only to the port where the report from Host A has been received.

- Second Scenario:

Another host B, on the same Ethernet segment as host A joins the same multicast group as host A.

Host B sends an unsolicited IGMP Membership report.

The Gateway intercepts the IGMP membership report sent by Host B.

As a multicast entry for this group already exists, the Gateway simply adds the port to the already existing entry for that multicast group. It also adds another Timeout timer specific for this port to the multicast group.

If another host joins another multicast group or the same multicast group, the same procedures described in the first and second scenarios are performed, respectively. A new Group entry will be added whenever a new group has been joined.

Note: In order to maintain group membership, the multicast router sends IGMP queries periodically. This query is intercepted and forwarded to all ports on the switch. All hosts that are members of the group will answer that query. The IGMP protocol was designed in such a way that only one member of any group on any VLAN would have to respond to any given query. But, because the reports are intercepted, the hosts do not see each other's reports, and thus, all hosts send a report (instead of one per group). These reports are then forwarded to the router; one report per group from among all received responses.

3.1.3.2.2 Leaving a multicast group

When a host wants to leave group it sends an IGMP Leave message specific for the group it wants to leave.

The IGMP Leave message is captured and if no other devices are known to be joined to that multicast group on that port - then the multicast stream is removed from that port. If no other ports have hosts joined to the same multicast group, then the leave messages is forwarded to the multicast router. In this way the multicast traffic the router is asked to stop sending the multicast stream.

If more than one port has hosts that have joined the multicast group, then the host that sent the IGMP Leave message is removed from the multicast membership record without forwarding the leave message to the multicast router.

- Time-out interval expiring

When the Time-out Interval expires, the Residential Gateway removes that entry from the multicast membership records and that multicast stream from the associated port - if it is the last entry registered against that port.

3.1.3.3 Proxy Operation Mode

Proxy mode is the default operational mode for the old IGMP snooping mode. It's possible to force the IGMP snooping to work in proxy mode via the igmp snooping set mode proxy command.

The Gateway responds to the IGMP Group Specific Query from the Multicast Router based on it's internal multicast records - replying with an IGMP Membership report for each multicast stream that the hosts that it is managing are subscribed to.

It also periodically sends IGMP Group Specific Query messages to all ports that are not known multicast router ports - in order to understand which multicast streams are subscribed to on which ports. The frequency with which this happens is based upon the Query interval that is configured on the device.

Upon receiving an IGMP Leave message, the system can either process it immediately - as described above (This is known as FastLeave) - or if configured to do so - send an IGMP Group Specific Query to the port where the IGMP Leave message was received from. The Leave Time value is used in the query message to request a fast response from other hosts that may be present on the same Ethernet segment. This can be used to ensure that when one host asks for a multicast stream to be stopped - it does not adversely impact another host on the same port that is subscribed to that multicast stream.

If no answer is received to the IGMP Group Specific Query and if no other ports have hosts joined to the same multicast group, then an IGMP leave messages is sent to the multicast router. In this way the multicast traffic the router is asked to stop sending any multicast data for that particular group.

The IGMP leave message forwarded by the Gateway will have as source MAC address the Gateway's MAC address and will have as source IP address the ipaddress of the ip interface associated with the VLAN that is associated with the IGMP service.

3.1.3.4 IP source address masking – Secondary IP Interface

If the Interface associated with the VLAN that the IGMP module is associated with does not have an IP address, it is possible to refer, as source IP address for upstream IGMP signalling messages, the IP address of any other existing IP interface. This interface is not required to be attached to the VLAN where IGMP snooping has been enabled.

3.1.3.5 IGMP snooping security

This feature allows the iBG/iMG/RG to limit accepted IGMP signalling to that from designated STB identified by their MAC addresses. These MAC addresses will be learned automatically by the software up to a configured number and saved in a non volatile memory. They are specifically named in the configuration. with the maximum number of STB MAC addresses supported being 10. It is possible to manually configure the allowed MAC addresses - so that via a provisioning action - the security of the Video network is maintained.

3.1.3.6 Routed IGMP proxy

An alternative to Bridged IGMP snooping is routed IGMP.

This is a layer-3 feature that allows multicast traffic to be routed between multiple IP interfaces.

IGMP traffic is typically limited to the VLAN where it is received. If a host joins a multicast group but multicast traffic is received on another VLAN to which the host is not connected, the multicast traffic will never reach the host.

Routed IGMP overrides this limitation with the only constraint that multicast traffic must be received only on one IP interface called the *upstream* interface.

In this case, when a host joins a multicast group, the IP interface attached to the transport (VLAN) where the host is located, becomes a downstream interface. It will receive all the multicast traffic related to the group that the host has joined.

It is possible to statically define the upstream IP interface.

3.1.4 Functional Differences in Product Categories

There are two different implementations of IGMP that are encountered in these ATI Gateways. The original implementation is configured using IGMP SNOOPING and IGMP PROXY commands. It is a separate application that IGMP packets are sent to - and is not integrated with the Bridge - that is an integral part of the Packet processing on the CPU. The newer implementation is configured using BRIDGE IGMPSNOOP and IGMP commands.It is integrated into the CPU based Bridge - which supports VLAN segregation of traffic flows.

In addition the IGMP PROXY commands have been superseded by the IGMP commands that are now available to manage Routed IGMP Proxy. The IGMP PROXY commands are retained in older devices for backward compatibility - but are not recommended.

TABLE 3-1 Functional Mapping for Bridge

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
Multicast router port discovery	1	2	1	2	2	2	1	2	2
Joining a Multicast Group	1	2	1	2	2	2	1	2	2
Leaving a multicast group	1	2	1	2	2	2	1	2	2
Multicast router port discovery	1	2	1	2	2	2	1	2	2
Proxy Operation Mode	1	2	1	2	2	2	1	2	2
IP source address masking – Secondary IP Interface	1	2	1	2	2	2	1	2	2
IGMP snooping security	1	2	1	2	2	2	1	2	2
Routed IGMP proxy	1	2	1	2	2	2	1	2	2

1) Utilizes IGMP SNOOPING command set. IGMP Command set recommended in place of IGMP PROXY command set.

2) Utilizes integrated BRIDGE IGMPSNOOP and the IGMP command set.

3.1.5 IGMP Snooping command reference

This section describes the commands available to enable, configure and manage the *IGMP snooping* feature.

3.1.5.1 IGMP snooping CLI commands

The table below lists the *IGMP snooping* commands provided by the CLI:

TABLE 3-2 ***Bridge*** IGMP Snooping Commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
BRIDGE ADD IGMPSNOOP MCASTROUTERINTF		X		X	X	X		X	X
BRIDGE ADD IGMPSNOOP SECURITY		X		X	X	X		X	X
BRIDGE DELETE IGMPSNOOP MCASTROUTERINTF		X		X	X	X		X	X
BRIDGE DELETE IGMPSNOOP SECURITY		X		X	X	X		X	X
BRIDGE LIST IGMPSNOOP GROUPINFO		X		X	X	X		X	X
BRIDGE LIST IGMPSNOOP INTERFACESTATS		X		X	X	X		X	X
BRIDGE LIST IGMPSNOOP STATIC MCASTROUTERINTFS		X		X	X	X		X	X
BRIDGE LIST IGMPSNOOP SECURITY		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP DEFAULTFASTLEAVE		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP LASTMBERQUERYINTVL		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP MCASTROUTERTIMEOUT		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP MODE		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP NETINTERFACE		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP QUERYINTVL		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP QUERYRESPONSEINTVL		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP ROBUSTNESSVAR		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP SECURITY		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP AUTOLEARNING		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP SECURITY MAXMACNUMBER		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP VLAN		X		X	X	X		X	X
BRIDGE SET IGMPSNOOP V1TIMER		X		X	X	X		X	X

TABLE 3-2 *Bridge* IGMP Snooping Commands **(Continued)**

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
IGMP SET FORWARDALL	X	X	X	X	X	X	X	X	X
IGMP SET LASTMBERQUERYINTVL	X	X	X	X	X	X	X	X	X
IGMP SET QUERYINTVL	X	X	X	X	X	X	X	X	X
IGMP SET QUERYRESPONSEINTVL	X	X	X	X	X	X	X	X	X
IGMP SET ROBUSTNESS	X	X	X	X	X	X	X	X	X
IGMP SET UPSTREAMINTERFACE	X	X	X	X	X	X	X	X	X
IGMP SHOW FORWARDALL	X	X	X	X	X	X	X	X	X
IGMP SHOW STATUS	X	X	X	X	X	X	X	X	X
IGMP SHOW TIMERCONFIGURATION	X	X	X	X	X	X	X	X	X
IGMP SHOW UPSTREAMINTERFACE	X	X	X	X	X	X	X	X	X
IGMP SNOOPING DISABLE	X		X				X		
IGMP SNOOPING ENABLE	X		X				X		
IGMP SNOOPING SET SECONDARY-NETINTERFACE	X		X				X		
IGMP SNOOPING SET MODE	X		X				X		
IGMP SNOOPING SET LEAVETIME	X		X				X		
IGMP SNOOPING SET TIMEOUT	X		X				X		
IGMP SNOOPING SHOW	X		X				X		
IGMP SNOOPING SECURITY	X		X				X		
IGMP SNOOPING SECURITY SET MAXMACNUMBER	X		X				X		
IGMP SNOOPING SECURITY LEARNING	X		X				X		
IGMP SNOOPING SECURITY ADD	X		X				X		
IGMP SNOOPING SECURITY DELETE	X		X				X		
IGMP SNOOPING SECURITY SHOW	X		X				X		
IGMP PROXY SET UPSTREAMINTERFACE	X						X		
IGMP PROXY SHOW UPSTREAMINTERFACE	X						X		
IGMP PROXY SHOW STATUS	X						X		

3.1.5.1.1 BRIDGE ADD IGMPSNOOP MCASTROUTERINTF

Syntax `BRIDGE ADD IGMPSNOOP MCASTROUTERINTF <interface name>`

Description This command allows the user to add a static multicast router interface. A multicast router interface is also called an upstream interface and a multicast router is connected to this interface. The upstream interface implements the Host portion of the IGMP protocol. The IGMP membership reports and leave group messages are forwarded on the upstream interfaces.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
interface_name	The name of a bridge interface that has previously been added and attached to a transport using the bridge add interface and bridge attach CLI commands.	N/A

Example --> bridge add igmpsnoop mcastrouterintf eth0

See also `BRIDGE SHOW`

3.1.5.1.2 BRIDGE ADD IGMPSNOOP SECURITY

Syntax `BRIDGE ADD IGMPSNOOP SECURITY <mac_name> MAC <mac_address>`

Description This command allows the user to add a static mac address into the list of mac addresses that are authorized to be provided video service via IGMP. When an IGMP packet is received, the source MAC address is validated against this list of MAC Addresses - and if a match if found - it is processed as normal - if not - then it is dropped.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
mac_name	The name of this particular entry in the MAC table	N/A
mac_address	The MAC Address of the Set Top Box that is authorized to receive video. It is of the format: <XX:XX:XX:XX:XX:XX>	N/A

Example --> bridge add igmpsnoop security firstSTB mac 00:01:02:03:04:05

See also BRIDGE LIST IGMPSNOOP SECURITY

3.1.5.1.3 BRIDGE DELETE IGMPSNOOP MCASTROUTERINTF

Syntax BRIDGE DELETE IGMPSNOOP MCASTROUTERINTF <interface name>

Description This command allows the user to delete a previously added static multicast router interface. The interface reverts to a downstream interface after deletion.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
interface_name	The name of a bridge interface that has previously been added and attached to a transport using the bridge add interface and bridge attach CLI commands.	N/A

Example --> bridge delete igmpsnoop mcastrouterintf eth0

3.1.5.1.4 BRIDGE DELETE IGMPSNOOP SECURITY

Syntax BRIDGE DELETE IGMPSNOOP SECURITY <mac_name|mac_number|ALL>

Description This command allows the user to delete one or all static mac address from the list of mac addresses that are authorized to be provided video service via IGMP.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
mac_name	The name of this particular entry in the MAC table	N/A
mac_number	The number of the particular entry in the MAC Table	N/A
ALL	All entries	

Example --> bridge delete igmpsnoop security All

See also BRIDGE LIST IGMPSNOOP SECURITY

3.1.5.1.5 BRIDGE LIST IGMPSNOOP GROUPINFO

Syntax `BRIDGE LIST IGMPSNOOP GROUPINFO`

Description This command displays all of the multicast groups in the IGMP database.

Example --> bridge set igmpsnoop groupinfo

3.1.5.1.6 BRIDGE LIST IGMPSNOOP INTERFACESTATS

Syntax `BRIDGE LIST IGMPSNOOP INTERFACESTATS`

Description This command displays IGMP packet statistics collected for each interface on the bridge.

3.1.5.1.7 BRIDGE LIST IGMPSNOOP STATIC MCASTROUTERINTFS

Syntax `BRIDGE LIST IGMPSNOOP STATIC MCASTROUTERINTFS`

Description This command allows the user to list all previously added static multicast router interfaces and the manner in which they were added.

Description --> bridge list igmpsnoop static mcastrouterintfcs

```
Bridge Interfaces:
Name  | Type
---------------
ethe0 | static
---------------
```

3.1.5.1.8 BRIDGE LIST IGMPSNOOP SECURITY

Syntax `BRIDGE LIST IGMPSNOOP SECURITY`

Description This command allows the user to display the IGMP information associated with IGMP Seccurity to include the configuration - enabled or disabled, the maximum number of MAC Addresses allowed and whether or not MAX Addresses can be learned. Learned MACs are sticky - in that if one is learned, then a system restart - or provisioning action is required to remove it.

Example --> bridge list igmpsnoop security

```
IGMP Snoop Configuration:

        IGMP Snoop:                  Disable
        IGMP Net Interface:          ip0
        IGMP Enabled Vlan:           -1
        Default Fast Leave           Enable
        Last Member Query Interval:  0
```

```
Query Interval:                 41
Robustness Variable:            2
Query Response Interval:        3
V1 Timer Value:                 133
Multicast Intf Aging Time:      133
IGMP Snoop Mode:                snooponly
IGMP MAC Security:              Disable
IGMP MAC Security Learning:     Disable
IGMP MAC Security Max Number:   5
     MAC Address 1:             Empty
     MAC Address 2:             Empty
     MAC Address 3:             Empty
     MAC Address 4:             Empty
     MAC Address 5:             Empty
     MAC Address 6:             Empty
     MAC Address 7:             Empty
     MAC Address 8:             Empty
     MAC Address 9:             Empty
```

3.1.5.1.9 BRIDGE SET IGMPSNOOP

Syntax `BRIDGE SET IGMPSNOOP { Enable | Disable | Drop }`

Description This command turns on/off the IGMP snooping processes.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
Enabled | Disabled | Drop	When Enabled, the IGMP process will intercept all IGMP frames on the bridge and performs multicast trunking by adding static multicast entries to the FDB. When Disabled, the IGMP process removes all static entries from the FDB and floods all multicast frames. When Drop, the IGMP process will intercept all IGMP frames on the bridge and not forward the packets.	Disabled

Example --> bridge set igmpsnoop enabled

See also `BRIDGE SHOW`

3.1.5.1.10 BRIDGE SET IGMPSNOOP DEFAULTFASTLEAVE

Syntax `BRIDGE SET IGMPSNOOP DEFAULTFASTLEAVE { defaultfastleave }`

Description Set the default fast leave state when enabling IGMP. Fast leave, proxy mode only, will force leaves out the WAN facing network upon receipt of a leave on the LAN facing network. If DEFAULTFASTLEAVE is disabled, then when in Proxy mode, the system will send an IGMP Query down the LAN side to make sure that no other device is receiving the specific multicast stream- prior to sending the IGMP Leave message out the WAN interface.

Note: You must disable and re-enable IGMP before this command will take effect.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
Defaultfastleave	Enable/disable	Enabled

3.1.5.1.11 BRIDGE SET IGMPSNOOP LASTMBERQUERYINTVL

Syntax `BRIDGE SET IGMPSNOOP LASTMEMBERQUERYINT<lastmberqueryintvl>`

Description This command sets the value for the last member query interval. When the Gateway receives the what it believes is an IGMP Leave from the last device in a Multicast Group on a particular port- the Last Member Query Interval is used to specify the time the Gateway waits for an IGMP Report after sending an IGMP Query message for that multicst stream down that port. If the Gateway does not receive an IGMP Report in that interval then it sends an IGMP leave to the Multicast Router.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
lastmberqueryintvl	The last member query interval value in seconds. Valid range is 0 to 255. 0 is a special case, 333 ms.	1

Example --> bridge set igmpsnoop lastmberqueryintvl 5

See also `BRIDGE LIST IGMPSNOOP`

3.1.5.1.12 BRIDGE SET IGMPSNOOP MCASTROUTERTIMEOUT

Syntax `BRIDGE SET IGMPSNOOP MCASTROUTERTIMEOUT < mcastroutertimeout >`

Description This command sets the value for the multicast router time out interval which is the time a dynamic multicast router interface remains an upstream interface after receiving an IGMP Query with a non-zero source IP address. If an IGMP Query with a non-zero source IP address is not received on the dynamic multicast router interface during this time interval, the dynamic multicast router interface is reverted back to a downstream interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
mcastroutertimeout	The aging time for multicast interfaces in seconds. Valid range is 1 to 65535	400

Example --> bridge set igmpsnoop mcastroutertimeout 500

See also `BRIDGE LIST IGMPSNOOP`

3.1.5.1.13 BRIDGE SET IGMPSNOOP MODE

Syntax `BRIDGE SET IGMPSNOOP MODE { Proxy | Snooponly }`

Description This command specifies the mode of operation for the IGMP process.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
Proxy | Snooponly	When in snooponly mode, the IGMP process samples IGMP packets without interference, using the data to trunk multicast streams. When in proxy mode, the IGMP process intercepts all IGMP packets and re-sources and times the reports and queries base on IGMP configuration.	Snooponly

Example --> bridge set igmpsnoop mode proxy

See also `BRIDGE SHOW`

3.1.5.1.14 BRIDGE SET IGMPSNOOP NETINTERFACE

Syntax `BRIDGE SET IGMPSNOOP NETINTERFACE <ip interface name>`

Description This command specifies the IP interface from which IGMP proxy messages should be sourced. Uses IP address 0.0.0.0 if not specified.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
Name	A name that identifies an existing ip interface as seen with ip list interfaces	ip0

Example --> bridge set igmpsnoop netinterface ip0

See also `IP LIST INTERFACES`

3.1.5.1.15 BRIDGE SET IGMPSNOOP QUERYINTVL

Syntax `BRIDGE SET IGMPSNOOP QUERYINTVL < queryintvl >`

Description This command sets the value for the query interval. The Query Interval is the time between General Queries sent by the proxy Querier.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
Queryintvl	The query interval value in seconds. Query interval cannot be less than or equal to the query response interval. Valid range is 2 to 255	125

Example --> bridge set igmpsnoop queryintvl 200

See also `BRIDGE SHOW`
`BRIDGE SET IGMPSNOOP QUERYRESPONSEINTVL`

3.1.5.1.16 BRIDGE SET IGMPSNOOP QUERYRESPONSEINTVL

Syntax `BRIDGE SET IGMPSNOOP QUERYRESPONSEINTVL < queryresponseintvl >`

Description This command sets the value for the query response interval. The Max Response Time inserted into the periodic General Queries.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
queryrespon-seintvl	The query response interval value in seconds. Query response interval cannot be greater than or equal to the query interval. Valid range is 1 to 254.	3

Example --> bridge set igmpsnoop queryresponseintvl 20

See also `BRIDGE SET IGMPSNOOP QUERYINTVL`

3.1.5.1.17 BRIDGE SET IGMPSNOOP ROBUSTNESSVAR

Syntax `BRIDGE SET IGMPSNOOP ROBUSTNESSVAR < robustnessvar >`

Description This command sets the value for the network robustness, allowing tuning based upon expected packet loss on the network. This robustness value will modify the time, in proxy mode only, between the leave on the LAN facing network and the leave being sent on the WAN facing network will be robustness times the lastmemberqueryintvl. It functions by forcing multiple IGMP Packet transmissions.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
robustnessvar	The the robustness variable value is a retry count for IGMP packet transmissions. Valid range is 2 to 255.	2

Example --> bridge set igmpsnoop robustnessvar 3

3.1.5.1.18 BRIDGE SET IGMPSNOOP SECURITY

Syntax `BRIDGE SET IGMPSNOOP SECURITY <enable|disable>`

Description This command enabled or disables IGMP Security for the device. When enabled - all IGMP messaging is validated against the MAC Addresses in the IGMP Security table to ensure that they are authorized to receive video service..

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
enable/disable	Activates or deactivates the service	disable

Example --> bridge set igmpsnoop security enable

See also `BRIDGE LIST IGMPSNOOP SECURITY`

3.1.5.1.19 BRIDGE SET IGMPSNOOP AUTOLEARNING

Option	Description	Default value
enable/disable	Activates or deactivates the service	disable

Syntax `BRIDGE SET IGMPSNOOP SECURITY AUTOLEARNING <enable|disable>`

Description This command activates or deactivates the ability of the security mechanism to learn MAC addresses. When the system starts - only configured MAC addresses are populated in the list of allowed MAC addresses. If AutoLearning is enabled, as new MAC addresses are encountered, they are added to the list of valid MAC addresses - until the table has reached the maximum size allowed. Once in the table, they cannot be removed, unless the system is restarted. Once in the table - and the config is saved, they cannot be removed except by a manual action.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
enable/disable	Activates or deactivates the autolearning feature	disable

Example --> bridge set igmpsnoop security autolearning enable

See also `BRIDGE LIST IGMPSNOOP SECURITY`

3.1.5.1.20 BRIDGE SET IGMPSNOOP SECURITY MAXMACNUMBER

Syntax `BRIDGE SET IGMPSNOOP SECURITY MAXMACNUMBER < num_macs >`

Description This command sets the limit on the number of MAC addresses that the IGMP Securitiy feature will allow to be populated in it's internal table - and thus the number of devices that can get video service..

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
num_macs	The maximum number of MACs that IGMP Security is allowed to be configured with - or learn..	5

Example --> bridge set igmpsnoop security maxmacnumber 3

See also `BRIDGE LIST IGMPSNOOP SECURITY`

3.1.5.1.21 BRIDGE SET IGMPSNOOP VLAN

Syntax `BRIDGE SET IGMPSNOOP VLAN < vlan_id >`

Description This command restricts all IGMP messaging to the specified VLAN. If IGMP messages are received on a different VLAN then they are forwarded as normal messages.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
vlan_id	The integer number of the VLAN - from 1 to 4094.	No restrictions (-1)

Example --> bridge set igmpsnoop vlan 313

See also `BRIDGE LIST IGMPSNOOP`

3.1.5.1.22 BRIDGE SET IGMPSNOOP V1TIMER

Syntax `BRIDGE SET IGMPSNOOP V1TIMER < v1timer >`

Description This command sets the value for the v1 timer. The Version 1 Router Present Timeout is how long a host must wait after hearing a Version 1 Query before it may send any IGMP version 2 messages.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
v1timer	The v1timer variable value in seconds. Valid range is 1 to 65535.	400

Example --> bridge set igmpsnoop v1timer 200

See also `BRIDGE SHOW`

3.1.5.1.23 IGMP SET FORWARDALL

Syntax `IGMP SET FORWARDALL < enabled|disabled >`

Description This command allows you to enable/disable your router's ability to forward multicast traffic to ALL interfaces. By default, multicast traffic is only forwarded to interfaces on which there is IGMP Proxy group membership.

Setting froward all is an alternative to IGMP Proxy. If you set forwardall enabled, it unsets the upstream interface and disables IGMP proxy.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
enabled/disabled	Enabled forwards multicast traffic to all interfaces. Disabled forwards multicast traffic only to interfaces on which there are IGMP Proxy group members	disabled

Example --> igmp set forwardall enabled

See also `IGMP SHOW FORWARDALL`

3.1.5.1.24 IGMP SET LASTMBERQUERYINTVL

Syntax `IGMP SET LASTMEMBERQUERYINT <lastmberqueryintvl>`

Description This command sets the value for the last member query interval. When the Gateway receives the what it believes is an IGMP Leave from the last device in a Multicast Group on a particular port- the Last Member Query Interval is used to specify the time the Gateway waits for an IGMP Report after sending an IGMP Query message for that multicst stream down that port. If the Gateway does not receive an IGMP Report in that interval then it sends an IGMP leave to the Multicast Router.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
lastmberqueryintvl	The last member query interval value in seconds. Valid range is 1 to 255.	1

Example --> igmp set lastmberqueryintvl 5

See also `IGMP SHOW STATUS`

3.1.5.1.25 IGMP SET QUERYINTVL

Syntax `IGMP SET QUERYINTVL < queryintvl >`

Description This command sets the value for the query interval. The Query Interval is the time between General Queries sent by the proxy Querier.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
Queryintvl	The query interval value in seconds. Query interval cannot be less than or equal to the query response interval. Valid range is 2 to 255	125

Example --> igmp set queryintvl 200

See also `IGMP SET QUERYRESPONSEINTVL`

3.1.5.1.26 IGMP SET QUERYRESPONSEINTVL

Syntax `IGMP SET QUERYRESPONSEINTVL < queryresponseintvl >`

Description This command sets the value for the query response interval. The Max Response Time inserted into the periodic General Queries.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
queryresponseintvl	The query response interval value in seconds. Query response interval cannot be greater than or equal to the query interval. Valid range is 1 to 254.	10

Example --> igmp set queryresponseintvl 20

See also `IGMP SET QUERYINTVL`

3.1.5.1.27 IGMP SET ROBUSTNESS

Syntax `IGMP SET ROBUSTNESS < robustness >`

Description This command sets the value for the network robustness, allowing tuning based upon expected packet loss on the network. This robustness value will modify the time, in proxy mode only, between the leave on the LAN facing network and the leave being sent on the WAN facing network will be robustness times the lastmemberqueryintvl.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
robustness	The the robustness variable value is a retry count for IGMP packet transmissions. Valid range is 2 to 255.	2

Example --> igmp set robustness 3

3.1.5.1.28 IGMP SET UPSTREAMINTERFACE

Syntax `IGMP SET UPSTREAMINTERFACE < ip_interface|none >`

Description This command enables the router's IGMP Proxy, and sets one of the router's existing IP interfaces as teh upstream interface; all other router interfaces are designated downstream interfaces. The upstream interface implements the Host portion of the IGMP protocol, and the downstream interfaces implement the Router portion of the IGMP protocol. The IGMP Proxy may be disabled by setting the upstream interface to none.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
ip_interface	The name of an existing router interface that you want to set as the upstream interface	N/A
none	Disables IGMP proxy	N/A

Example --> igmp set upstream interface ip1

See also `IGMP SHOW`

3.1.5.1.29 IGMP SHOW FORWARDALL

Syntax `IGMP SHOW FORWARDALL`

Description This command displays the status of the ForwardAll configuration.

Example --> iigmp show forwardall

```
IGMP Forwarder:
            Forward All : false
```

See also `IGMP SET FORWARDALL`

3.1.5.1.30 IGMP SHOW STATUS

Syntax `IGMP SHOW STATUS`

Description This command displays the following information about the status of IGMP proxy:

- IGMP Proxy group membership per interface details
- Interface name and querier status
- Group address

Example --> igmp proxy show status

```
Multicast group membership:
Interface (querier)  | Group address
---------------------|-----------------
ip_video (yes)       | 239.255.255.250
--------------------------------------
```

3.1.5.1.31 IGMP SHOW TIMERCONFIGURATION

Syntax `IGMP SHOW TIMERCONFIGURATION`

Description This command displays the All the timer settings for the IGMP Proxy. This includes the Robustness setting, Query Interval, Query response interval and the last member query interval.

Example --> igmp proxy show status

```
IGMP Proxy configuration:

              Robustness : 2
               Query Int : 125
           Query Rsp Int : 10
    Last Member Query Int : 1
```

See also IGMP SET LASTMEMBERQUERYINT
IGMP SET QUERYINTERVAL|
IGMP SET QUERYRSPINTERVAL
IGMP SET ROBUSTNESS

3.1.5.1.32 IGMP SHOW UPSTREAMINTERFACE

Syntax IGMP SHOW UPSTREAMINTERFACE

Description This command displays the status of the upstream interface. If an upstream interface has been set using the IGMP SET UPSTREAMINTERFACE command, this command displays the current setting.

Example --> igmp show upstreaminterface

```
IGMP Proxy configuration
Upstream If : ip0
```

See also IGMP SET UPSTREAMINTERFACE

3.1.5.1.33 IGMP SNOOPING DISABLE

Syntax IGMP SNOOPING DISABLE <vlan_name>

Description This command disables the layer- 2 IGMP snooping feature previously enabled with the IGMP SNOOPING ENABLE command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
vlan_name	The name of an existing vlan where igmp snooping has been previously enabled.	N/A

Example → `igmp snooping disable vlan_video`

See also `IGMP SNOOPING ENABLE`

3.1.5.1.34 IGMP SNOOPING ENABLE

Syntax `IGMP SNOOPING ENABLE`

Description This command enables the layer-2 IGMP snooping feature.

Default timeout values are used:

- leavetime10secs
- timeout270secs

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
vlan_name	The name of an existing vlan where igmp snooping has been previously enabled.	N/A

Example → `igmp snooping enable vlan_video`

See also `IGMP SNOOPING DISABLE`
`IGMP SNOOPING SET`

3.1.5.1.35 IGMP SNOOPING SET SECONDARY-NETINTERFACE

Syntax `IGMP SNOOPING SET SECONDARY-NETINTERFACE <secondary_net_interface>`

Description This command sets the ip address interface used as reference for the ip address value to be replaced in the upstream IGMP signalling messages. The IGMP module will use this secondary ip interface ONLY if the ip interface attached to the vlan where IGMP snooping has been enabled has null value (0.0.0.0). In the contrary all upstream IGMP signalling

messages will use the ip address of the IP interface immediately attached to the multicast vlan.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
secondary_net_interface	The name of an existing IP interface to be used as reference source IP address.	N/A

Example → `igmp snooping set secondary-netinterface ip_mgmt`

See also `IGMP SNOOPING SHOW`

3.1.5.1.36 IGMP SNOOPING SET MODE

Description IGMP SNOOPING SET MODE <mode>

This command sets the mode to forward IGMP packets. When mode is set to "proxy", the original Source MAC address and the original Source IP address are substituted with the gateway's own MAC and IP addresses. When mode is set to "snooping", the IGMP packets are forwarded with no changes.

When IGMP snooping is enabled, by default this parameter is set "snooping".

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default value
mode	Implemented different igmpsnooping mode: *proxy*: Substitutes Source MAC Address and Source MAC address with its own addresses forwarding received IGMP packets. *snooping*: Forwards received IGMP packets with no changes.	snooping

Example --> igmp snooping set mode proxy

See also IGMP SNOOPING ENABLE

3.1.5.1.37 IGMP SNOOPING SET LEAVETIME

Syntax `IGMP SNOOPING SET LEAVETIME <leavetime>`

Description This command sets the duration of the Leave Period timer for the IGMP snooping process. The timer controls the maximum allowed time before hosts must send a response to Query message issued by the Gateway.

When IGMP snooping is enabled, by default this value is set to 10 sec.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
leavetime	The leavetime value expressed in seconds. Valid values are between 0 and 65535.	10

Example ◊ igmp snooping set leavetime 50

See also `IGMP SNOOPING ENABLE`

3.1.5.1.38 IGMP SNOOPING SET TIMEOUT

Syntax `IGMP SNOOPING SET TIMEOUT <timeout>`

Description This command sets the longest interval, in seconds, for which a group will remain in the local multicast group database without the Residential Gateway receiving a *Host Membership Report* for this multicast group.

When IGMP snooping is enabled, by default this value is set to 270 sec.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default value
timeout	The timeout interval value expressed in seconds. Valid values are from 1 to 65535.	270

Example igmp snooping set timeout 125

See also `IGMP SNOOPING ENABLE`

3.1.5.1.39 IGMP SNOOPING SHOW

Syntax `IGMP SNOOPING SHOW`

Description This command shows IGMP snooping status.

The following information are reported:

- Timeout Interval
  Interval after which entries will be removed from the group database
- Interface Name
  VLAN reference
- Multicast Router
  Recognized Multicast route
- Group List
  Membership list for this VLAN
- Group
  The group multicast address. Multicast Filter highlights members useful to stop
- Port
  Port where the member is attached
- Last Adv
  The last host to advertise the membership report or query
- Refresh time
  The time interval (in seconds) before the membership group is deleted

See also IGMP SNOOPING ENABLE

3.1.5.1.40 IGMP SNOOPING SECURITY

Syntax `IGMP SNOOPING SECURITY <enable/disable>`

Description This command enables/disables the security feature

3.1.5.1.41 IGMP SNOOPING SECURITY SET MAXMACNUMBER

Syntax `IGMP SNOOPING SECURITY SET MAXMACNUMBER <max_mac_number>`

Description This command sets the maximum number of MAC addresses that can be statically (via the "add" command) or dynamically (via auto-learning) managed by the CPE. Range is 1-10, default 5. In case of some MACs have been already learned/set, a new value of this parameter is accepted if equal or greater than registered MAC numbers.

3.1.5.1.42 IGMP SNOOPING SECURITY LEARNING

Syntax `IGMP SNOOPING SECURITY LEARNING <enable/disable>`

Description This command enables/disables the auto-learning option

3.1.5.1.43 IGMP SNOOPING SECURITY ADD

Syntax `IGMP SNOOPING SECURITY ADD <name> max <mac_address>`

Description This command statically adds a new MAC address.

3.1.5.1.44 IGMP SNOOPING SECURITY DELETE

Syntax `IGMP SNOOPING SECURITY DELETE {<name> | ALL }`

Description This command deletes a MAC entry, either statically or dynamically added

3.1.5.1.45 IGMP SNOOPING SECURITY SHOW

Syntax `IGMP SNOOPING SECURITY SHOW`

Description This command shows the security info the MAC list and the status

3.1.5.1.46 IGMP PROXY SET UPSTREAMINTERFACE

Syntax `IGMP PROXY SET UPSTREAMINTERFACE {<ip_interface> | NONE}`

Description This command enables the gateway's IGMP Proxy Routing function, and sets one of the existing IP interfaces as the upstream interface; all other interfaces are designated downstream interfaces. The upstream interface implements the *Host* portion of the IGMP protocol, and the downstream interfaces implement the *Router* portion of the IGMP protocol. Setting upstream interface to none may disable the IGMP Proxy.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default value
ip_interface	The name of an existing interface that you want to set as the upstreaminterface.	N/A
none	Disables IGMP proxy	N/A

Options --> igmp proxy set upstreaminterface ip0

See also IGMP PROXY SHOW STATUS

3.1.5.1.47 IGMP PROXY SHOW UPSTREAMINTERFACE

Syntax `IGMP PROXY SHOW UPSTREAMINTERFACE`

Description This command displays the status of the upstream interface. If an upstream interface has been set using the IGMP PROXY SET UPSTREAMINTERFACE command, this command displays the current setting.

Example --> igmp proxy show upstreaminterface

```
IGMP Proxy configuration
Upstream If : ip0
```

See also `IGMP PROXY SET UPSTREAMINTERFACE`

3.1.5.1.48 IGMP PROXY SHOW STATUS

Syntax `IGMP PROXY SHOW STATUS`

Description This command displays the following information about the status of IGMP proxy:

- IGMP Proxy group membership per interface details
- Interface name and querier status
- Group address

Example --> igmp proxy show status

```
Multicast group membership:
Interface (querier)  | Group address
---------------------|-----------------
ip_video (yes)       | 239.255.255.250
--------------------------------------
```

See also `IGMP PROXY SHOW UPSTREAMINTERFACE`

4. IPNetwork Functions

4.1 IP

4.1.1 Overview

This chapter describes the main features of the Internet Protocol (IPv4) and how to configure and operate the AT-iMG models IP interface.

Before you start configuring the IP Stack for your own network requirements, it is essential that you are familiar with the basic functionality of the IP Stack

The IP Stack allows you to configure basic connectivity for your network to provide IP routing between interfaces and to support local applications, such as Telnet, web server, DHCP and so on.

The dual IP Stack implements the following IPv4 protocols:

- Internet Protocol (IP), including RFC 791.
- Includes support for Fragmentation and Reassembly (*RFC 0791* and *RFC 1812* (section 4.2.2.7))
- Includes support for Subnetting and Classless Interdomain Routing. • Internet Control Message Protocol (ICMP) (*RFC 0792*); see *ICMP (RFC 972)*.
- User Datagram Protocol (UDP) - *RFC 768*
- Transmission Control Protocol (TCP) - *RFC 793*
- featuring also TCP MSS Clamp;
- Address Resolution Protocol (ARP) for Ethernet - *RFC 826* and *RFC 894*.
- Internet Group Management Protocol (IGMP), Version 2 - *RFC 236*. Multicast forwarding and IGMP Proxy (*RFC 2236*);
- Routing Information Protocol (RIP), Version 2 - *RFC 1723*; see *RIP v2 (for IPv4)*.

4.1.2 IP Interfaces

In order to use the IP stack, one or more interfaces must be added to the IP stack and attached to a transport.

For IPv4 interfaces, each interface must be configured with an IP address and a subnet mask. Together, these define the range of addresses which can be reached via the interface withoutpassing through any other routers

Each interface (real and virtual) must have a unique subnet; the range of addresses on each interface must not overlap with any other interface. The only exception to this is unnumbered interfaces, which may be configured on point to point links when there is no local subnet associated with the interface.

4.1.3 IP support on AT-iMG Models

In order to use the IP stack, one or more interfaces must be added to the IP stack and attached to a transport.

Each interface must be configured with an IP address and a subnet mask. Together, these define the range of addresses that can be reached via the interface without passing through any other routers.

Each interface (real and virtual) must have a unique subnet; the range of addresses on each interface must not overlap with any other interface. In situations where there is no local subnet associated with an interface, unnumbered interfaces may be used.

4.1.3.1 Adding and attaching IP interfaces

IP interfaces are added and attached using the commands provided in the IP and Ethernet module respectively.

IP interfaces use typically the services provided by Ethernet transports. Ethernet transport is an abstraction layer used to classify the format of the IP packets that will be transferred through the network. Another type of transport is, for example, is PPPoE. Packets transmitted through a PPPoE connection or Ethernet connection will have different frame format even if the convey the same type of information to the IP layer.

Because the system supports VLANs, the same Ethernet port can be shared between different VLANs. Therefore it's not possible map an Ethernet transport directly to a physical Ethernet port.

Instead Ethernet transports are mapped to VLANs that from a logical point of view they act like an Ethernet segment, as an Ethernet port would do in a simple system without VLANs

The way a transport is attached to the gateway depends on the kind of core switching type.

On FIBER A/C and ADSL A devices it happens like depicted in steps here below.

- Create an Ethernet transport using the command:
  ```
  ethernet add transport eth1 myvlan
  ```
- Create an interface to the IP stack: using, for example, the command:
  ```
  ip add interface ip1 192.168.101.2 255.255.255.0
  ```
- Attach the transport to the interface using the command:
  ```
  ip attach ip1 eth1
  ```

Things are slightly different on the remaining models. A Vlan is handled as a bridgeport. Each bridgeport is a transport of type Qbridge. therefore step 1) is not necessary.

- Create an interface to the IP stack: using, for example, the command:
  ```
  ip add interface ip1 192.168.101.2 255.255.255.0
  ```
- Attach the transport to the interface using the command:
  ```
  ip attach ip1 myvlan
  ```

The **maximum number of IP interfaces is set to 16**, which means that there are up to 16 IP interfaces internally numbered one to 16. Since one interface is reserved for use as a loopback interface, this means up to 15 IP interfaces can be added by the user

When a packet arrives on an IP interface, the IP stack determines what to do with the packet. There are two options:

- Receive the packet locally;
- Forward the packet to another interface

4.1.3.2 IP stack and incoming packets

When a packet arrives on an IP interface, the IP stack determines whether:

- The packet should be received locally
- The packet should be forwarded to another interface

4.1.3.3 Locally received packets

A packet will be received locally if:

- The destination address of the packet matches any of the IP stack interface addresses (real or virtual interface, primary or secondary addresses)
- The packet is a broadcast
- The packet is a multicast to a group that the IP stack belongs to
- The packet has the ***Router Alert*** option set

The packet is either processed internally within the IP stack (for example, ICMP or IGMP control messages), or passed up to an application via the appropriate protocol processing (for example, TCP or UDP data).

For a local application to successfully send a packet back to another host, the IP stack must be able to find a suitable route to that host.

4.1.3.4 Forwarding packets

If the IP stack determines that a packet should not be received locally, it will try to forward the packet. The packet will be forwarded if:

- The destination of the packet can be reached directly via any of the IP stack's interfaces
- A route has been added, either manually or by a routing protocol, specifying a suitable gateway via which that destination may be reached

Several address tests are applied before forwarding a packet, for example to prevent broadcast packets from being forwarded. For more information about these tests, see ***RFC1122: Requirements for Internet - Hosts***.

If the packet cannot be forwarded, an ICMP ***Destination Unreachable*** error will be returned to the sender.

By default, the checksum of forwarded IP packets is not checked. This is for reasons of efficiency, because calculating the checksum on all packets adds significantly to the forwarding time and reduces throughput. This default setting is common in most IP routers. Locally terminated packets always have their checksum checked.

4.1.4 Unconfigured interfaces

An interface with an IP address of 0.0.0.0 is unconfigured. An interface is added as unconfigured when it is to be configured at a later time, for example, by IPCP or DHCP.

No traffic will be forwarded from an unconfigured interface. However, an unconfigured interface may still receive certain types of traffic, such as responses to DHCP requests.

An unconfigured interface should not be confused with an unnumbered interface.

4.1.5 Unnumbered interfaces

In a routed network, consider two routers that are joining two different subnets via a point-to-point link. It would usually be necessary to allocate a whole subnet just for the link between the routers, in addition to the other two subnets.

An unnumbered interface does not have a subnet associated with it and simply serves as one end of a point-to-point link. An unnumbered link does not have an IP address, but a router ID THAT is the IP address of one of the router's other interfaces.

You can have multiple unnumbered interfaces as long as you have at least one normal (numbered) IP interface in your router so that you can use its IP address as the router ID. The unnumbered interfaces can either use different router ID values, or use the same router ID value. WhaTEVER THEIR VALUE, THE ROUTER ID(s) must match the address of a normal interface.

Note: Unnumbered interfaces can only be used on point-to-point links. This includes PPP. You cannot use unnumbered interfaces with Ethernet

4.1.5.1 Unconfigured interfaces vs unnumbered interfaces

An unnumbered interface is not the same as an unconfigured interface.

An unconfigured interface is created by adding an interface without specifying an IP address (ip add interface myinterface), or by specifying an IP address of 0.0.0.0 (ip add interface myinterface 0.0.0.0).

You would add an unconfigured interface if the interface address were to be set automatically later, for example, by IPCP or DHCP. It cannot be used for normal traffic.

An unnumbered interface is different - it is used for normal traffic but does not have its own IP address or a local subnet associated with it.

4.1.5.2 Configuring unnumbered interfaces

Unnumbered interfaces are created using the following CLI command:

IP ADD INTERFACE <name> <ipaddress> 255.255.255.255

For example:

```
ip add interface myinterface 192.168.101.3 255.255.255.255
```

In this command:

- ***myinterface*** is the unnumbered interface name.
- 192.168.101.3 is the ***router id***. The router ID must be set to the IP address of one of the router's normal interfaces. The main use of the router ID is as the source address for packets sent on an unnumbered interface from local applications or routing protocols. Router IDs are described in ***RFC1812 Requirements for IP v4 Routers***.
- 255.255.255.255 is a special subnet mask that identifies an unnumbered interface and distinguishes it from any other type of interface.

You must also add a route before your unnumbered interface can send packets.

4.1.5.3 Creating a route

Because an unnumbered interface does not have a local subnet associated with it, no packets can be routed to an unnumbered interface until a route is added. Let us just consider how this is done.

Usually, for Ethernet interface, routes are added with a gateway to be used for a particular destination.

For example:

```
ip add route myroute 10.0.0.0 255.0.0.0 gateway 192.168.101.10
```

This means that all packets for the 10.0.0.0 subnet will be sent to the address 192.168.101.10 as their next hop. The gateway must be reachable directly, so 192.168.101.10 must be on a subnet served by one of the local interfaces.

But, for point-to-point links, you can add a route through the interface, without specifying a gateway address, for example:

```
ip add route myroute 10.0.0.0 255.0.0.0 interface myinterface
```

All packets for the specified destination will be sent via the unnumbered interface called ***myinterface***. This type of route can be used for all interfaces with point-to-point links, not just for unnumbered interfaces.

On devices of the type `FIBER B/D/E, MODULAR` and `ADSL B/C` routes can be disabled and enabled.Unless explicitely set: routes are created and enabled.

4.1.6 Virtual interfaces

Usually, each transport only has one router interface associated with it, and each router interface has only one IP address and local subnet associated with.

Virtual interfaces allow you to attach more than one IP interface to the same transport. Secondary IP addresses allow you to associate more than one IP address with the same IP interface. Together, these features allow many configurations that would not otherwise be possible.

Virtual interfaces allow you to create multiple router interfaces on the same transport, for example, on the same Ethernet port. This allows the IP stack to communicate with and route between multiple subnets existing on the same LAN.

4.1.6.1 Configuring virtual interfaces

To configure a virtual interface you need to create an IP interface, but instead of attaching it to a transport, you need to attach it to a second IP interface that already has a transport attached to it.

In this way, the two interfaces share the transport that is only attached to one of the interfaces.

The original interface attached directly to a transport is called the real interface, and the interface that is attached to the real interface is called the virtual interface.

To configure a virtual interface using the CLI:

- Create the real interface, then create an Ethernet transport and attach the IP interface to the transport:

```
ip add interface real_ip 192.168.101.2 255.255.255.0

On FIBER A/C and ADSL A devices:

ethernet add transport eth1 myvlan
ip attach real_ip eth1
```

On the remaining models it's enough to:

```
ip attach real_ip myvlan
```

- Create the virtual interface:

```
ip add interface virtual_ip 192.168.50.10 255.255.255.0
```

- Attach the virtual interface to the real interface:

```
ip attachvirtual virtual_ip real_ip
```

You can add more than one virtual interface to the same real interface.

Attaching them to a real interface instead of to a transport directly creates virtual interfaces. If the real interface is deleted, then all associated virtual interfaces are detached automatically.

4.1.6.2 Similarities between virtual interfaces and real interfaces

A virtual interface is similar to a real interface:

- Virtual interfaces may be manipulated in the same way as real interfaces using the CLI.
- The IP stack will route between virtual interfaces and real interfaces in the same way that it routes between real interfaces.

Note: Like real interfaces, virtual interfaces must have a unique subnet that does not overlap with other interfaces. In order to have the router respond to more than one IP address on the same subnet, secondary addresses must be used instead of virtual interfaces.

4.1.6.3 Differences between virtual interfaces and real interfaces

When the IP stack receives a packet from a transport that has associated virtual interfaces, the IP stack must decide which interface the packet arrived on.

The source address of the incoming packet is compared with the subnet of each virtual interface on that transport. If there is no match, the IP stack assumes that the packet arrived on the real interface.

The interface that the packet arrived on is important in two scenarios:

- When the Firewall is in use - different rules (such as policies, portfilters and validators) are configured between different interfaces, so you need to know which interfaces the packet passes between.
- Some applications are written to only respond to traffic received on a specific interface. For example, DHCP server.

Because the traffic for all virtual interfaces is received in the same way as the real interface, the only reasonable way of selecting an interface is based on source address as described above. This means that:

- A virtual interface only receives packets with a source address matching its interface subnet, providing packets arrive via the real interface that the virtual interface is attached to.
- Packets that arrive with a source address that does not match a local subnet are deemed to have been received on the real interface, even if the next hop would be reached through the virtual interface when sending to that destination.
- Any packets from an unconfigured host, for example DHCP or BOOTP requests, are deemed to be received on the real interface.

Note: Remember that the sender can spoof the source address of the packet; therefore security-related decisions should not be based on the ability to distinguish between virtual interfaces on the same transport.

4.1.7 Secondary IP addresses

Secondary IP addresses differ from virtual interfaces because there is no concept of a separate local subnet associated with a secondary address.

The secondary addresses share the same subnet with the interface.

Secondary addresses therefore allow the IP stack to have more than one address on the same subnet. After setting the main interface address, one or more additional addresses on the same subnet can be added to the interface.

4.1.7.1 Configuring secondary IP addresses

You can create and configure secondary IP addresses using the CLI.

The following CLI commands allow you to create and configure secondary IP addresses:

```
ip interface add secondaryipaddress
ip interface clear secondaryipaddresses
ip interface delete secondaryipaddress
ip interface list secondaryipaddresses
```

Note: FThe ability to specify a subnet mask with a secondary address is superseded by the functionality of virtual interfaces. You should use virtual interfaces instead.

Support for adding secondary IP addresses including subnet mask specification will be withdrawn in a future software release.

4.1.7.2 Functionality of secondary IP addresses

On Ethernet interfaces, secondary IP addresses must be on the same subnet as the interface. Secondary addresses may be added to virtual interfaces, as well as real interfaces.

On Point-to-Point links, secondary addresses may be added on a different subnet to the main interface address. This will provide an additional address that the IP stack will respond to for traffic arriving on that interface, but with no associated local subnet.

This is similar to configuring a virtual interface as an unnumbered interface. This is not a common configuration.

4.1.8 TCP/IP command reference

This section describes the commands available on AT-iMG models to manage the TCP/IP module.

4.1.8.1 IP Tracing commands

You can carry out tracing in the IP stack using the following system commands:

- SYSTEM LOG ENABLE|DISABLE; enables/disables the tracing support output for a specific module and category.
- SYSTEM LOG LIST; displays the tracing options for the modules available in the current image

4.1.8.2 IP CLI commands

The table below lists the IP commands provided by the CLI:

TABLE 4-1 IP CLI commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
IP ATTACH	X	X	X	X	X	X	X	X	X
IP ATTACHBRIDGE	X	X	X	X	X	X	X	X	X
IP ATTACHVIRTUAL	X	X	X	X	X	X	X	X	X
IP CLEAR ARPENTRIES	X	X	X	X	X	X	X	X	X
IP CLEAR INTERFACES	X	X	X	X	X	X	X	X	X
IP CLEAR RIPROUTES	X	X	X	X	X	X	X	X	X
IP CLEAR ROUTES	X	X	X	X	X	X	X	X	X
IP DELETE INTERFACE	X	X	X	X	X	X	X	X	X
IP DELETE ROUTE	X	X	X	X	X	X	X	X	X
IP DETACH INTERFACE	X	X	X	X	X	X	X	X	X
IP INTERFACE ADD PROXYARPENTRY	X	X	X	X	X	X	X	X	X
IP INTERFACE ADD PROXYARPEXCLUSION	X	X	X	X	X	X	X	X	X
IP INTERFACE ADD SECONDARYIPADDRESS	X	X	X	X	X	X	X	X	X
IP INTERFACE ADD STATICARPENTRY	X	X	X	X	X	X	X	X	X
IP INTERFACE CLEAR PROXYARPENTRIES	X	X	X	X	X	X	X	X	X
IP INTERFACE CLEAR SECONDARYIPADDRESSES	X	X	X	X	X	X	X	X	X
IP INTERFACE CLEAR STATICARPENTRIES	X	X	X	X	X	X	X	X	X
IP INTERFACE DELETE PROXYARPENTRIES	X	X	X	X	X	X	X	X	X
IP INTERFACE DELETE PROXYARPEXCLUSION	X	X	X	X	X	X	X	X	X
IP INTERFACE DELETE SECONDARYIPADDRESSES	X	X	X	X	X	X	X	X	X
IP INTERFACE DELETE STATICARPENTRY	X	X	X	X	X	X	X	X	X
IP INTERFACE LIST PROXYARPENTRIES	X	X	X	X	X	X	X	X	X
IP INTERFACE LIST SECONDARYIPADDRESSES	X	X	X	X	X	X	X	X	X

TABLE 4-1 IP CLI commands (Continued)

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
IP INTERFACE LIST STATICARPENTRIES	X	X	X	X	X	X	X	X	X
IP LIST APPSERVICES	X	X	X	X	X	X	X	X	X
IP LIST ARPENTRIES	X	X	X	X	X	X	X	X	X
IP LIST CONNECTIONS	X	X	X	X	X	X	X	X	X
IP LIST INTERFACES	X	X	X	X	X	X	X	X	X
IP LIST RIPROUTES	X	X	X	X	X	X	X	X	X
IP LIST ROUTES	X	X	X	X	X	X	X	X	X
STOP PING	X	X	X	X	X	X	X	X	X
IP PING	X	X	X	X	X	X	X	X	X
IP SET APPSERVICE	X	X	X	X	X	X	X	X	X
IP SET INTERFACE IPADDRESS	X	X	X	X	X	X	X	X	X
IP SET INTERFACE NETMASK	X	X	X	X	X	X	X	X	X
IP SET INTERFACE MTU	X	X	X	X	X	X	X	X	X
IP SET INTERFACE DHCP	X	X	X	X	X	X	X	X	X
IP SET INTERFACE GATEWAY	X	X	X	X	X	X	X	X	X
IP SET INTERFACE RIP ACCEPT	X	X	X	X	X	X	X	X	X
IP SET INTERFACE RIP MULTICAST	X	X	X	X	X	X	X	X	X
IP SET INTERFACE RIP SEND	X	X	X	X	X	X	X	X	X
IP SET INTERFACE TCPMSSCLAMP	X	X	X	X	X	X	X	X	X
IP SET RIP ADVERTISEDEFAULT	X	X	X	X	X	X	X	X	X
IP SET RIP AUTHENTICATION	X	X	X	X	X	X	X	X	X
IP SET RIP DEFAULTROUTECOST	X	X	X	X	X	X	X	X	X
IP SET RIP HOSTROUTES	X	X	X	X	X	X	X	X	X
IP SET RIP PASSWORD	X	X	X	X	X	X	X	X	X
IP SET RIP POISON	X	X	X	X	X	X	X	X	X
IP SET ROUTE	X	X	X	X	X	X	X	X	X

TABLE 4-1 IP CLI commands (Continued)

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
IP SET ROUTE	X	X	X	X	X	X	X	X	X
IP SET ROUTE	X	X	X	X	X	X	X	X	X
IP SET ROUTE ADVERTISE	X	X	X	X	X	X	X	X	X
IP SET ROUTE DESTINATION	X	X	X	X	X	X	X	X	X
IP SET ROUTE GATEWAY	X	X	X	X	X	X	X	X	X
IP SET ROUTE COST	X	X	X	X	X	X	X	X	X
IP SET ROUTE INTERFACE	X	X	X	X	X	X	X	X	X
IP SET TTL	X	X	X	X	X	X	X	X	X
IP SHOW	X	X	X	X	X	X	X	X	X
IP SHOW APPSERVICE	X	X	X	X	X	X	X	X	X
IP SHOW INTERFACE	X	X	X	X	X	X	X	X	X
IP SHOW ROUTE	X	X	X	X	X	X	X	X	X

(*) Those commands are avalaible on FIBER B,D,E, MODULAR and ADSL B,C devices

4.1.8.2.1 IP ADD DEFAULTROUTE GATEWAY

Syntax `IP ADD DEFAULTROUTE GATEWAY <gateway_ip>`

Description This command creates a default route. It acts as a shortcut command that you can use instead of typing the following:

```
ip add route default 0.0.0.0 0.0.0.0 gateway 192.168.103.3
```

Note: You can only create one default route. A default route will not be created if you have already created a default route using the IP ADD ROUTE command or the IP ADD DEFAULTROUTE INTERFACE command.

If you want RIP to advertise a default route with a default cost metric, see the IP SET RIP ADVERTISEDEFAULT and IP SET RIP DEFAULTROUTECOST commands.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
gateway_ip	The IP address of the gateway that this route will use by default, in the format: 192.168.103.3	gateway_ip

Example --> ip add defaultroute gateway 192.168.103.3

See also
```
ip add route
ip add defaultroute interface
ip set rip advertisedefault
ip set rip defaultroutecost
```

4.1.8.2.2 IP ADD DEFAULTROUTE GATEWAY DISABLED

Syntax `IP ADD DEFAULTROUTE GATEWAY <gateway_ip> DISABLED`

Description This command creates a default route and but prevents its activation. It acts as a shortcut command that you can use instead of typing the following:

```
ip add route default 0.0.0.0 0.0.0.0 gateway 192.168.103.3 DISABLED
```

Note: You can only create one default route. A default route will not be created if you have already created a default route using the IP ADD ROUTE command or the IP ADD DEFAULTROUTE INTERFACE command.

If you want RIP to advertise a default route with a default cost metric, see the IP SET RIP ADVERTISEDEFAULT and IP SET RIP DEFAULTROUTECOST commands

Note: This command are avalable on FIBER B,D,E MODULAR and ADSL B,C models only.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
gateway_ip	The IP address of the gateway that this route will use by default, in the format: 192.168.103.3	gateway_ip

Example --> ip add defaultroute gateway 192.168.103.3

See also
```
ip add route disabled, ip add route, ip set route enabled
ip add defaultroute interface, ip add default route inter-
face disabled
ip set rip advertisedefault
ip set rip defaultroutecost
```

4.1.8.2.3 IP ADD DEFAULTROUTE INTERFACE

Syntax `IP ADD DEFAULTROUTE INTERFACE <interface>`

Description This command creates a default route. It acts as a shortcut command that you can use instead of typing the following:

```
ip add route default 0.0.0.0 0.0.0.0 interface ip3
```

Note: You can only create one default route. A default route will not be created if you have already created a default route using the ip add route command or the ip add defaultroute gateway command.

If you want RIP to advertise a default route with a default cost metric, see the IP SET RIP ADVERTISEDEFAULT and IP SET RIP DEFAULTROUTECOST commands.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
interface	The name of the existing interface that this route will use. To display interface names, use the IP LIST INTERFACES command.	N/A

Example --> ip add defaultroute interface ip3

See also
```
ip add route
ip add defaultroute gateway
ip set rip advertisedefault
ip set rip defaultroutecost
```

4.1.8.2.4 IP ADD DEFAULTROUTE INTERFACE DISABLED

Syntax `IP ADD DEFAULTROUTE INTERFACE <interface> DISABLED`

Description This command creates a default route but prevents its activation. It acts as a shortcut command that you can use instead of typing the following:

```
ip add route default 0.0.0.0 0.0.0.0 interface ip3 disabled
```

Note: You can only create one default route. A default route will not be created if you have already created a default route using the ip add route command or the ip add defaultroute gateway command.

If you want RIP to advertise a default route with a default cost metric, see the IP SET RIP ADVERTISEDEFAULT and IP SET RIP DEFAULTROUTECOST commands.

Note: This command is avalable on FIBER B,D,E MODULAR and ADSL B,C models only.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
interface	The name of the existing interface that this route will use. To display interface names, use the IP LIST INTERFACES command.	N/A

Example --> ip add defaultroute interface ip3

See also `ip add route, ip add route disabled, ip set route enabled`
`ip add defaultroute gateway, ip add defaultroute gateway disabled`
`ip set rip advertisedefault`
`ip set rip defaultroutecost`

4.1.8.2.5 IP ADD INTERFACE

Syntax `IP ADD INTERFACE <name> [<ipaddress> [<netmask>]]`

Description This command adds a named interface and optionally sets its IP address. The IP address is not mandatory at this stage, but if it is not specified in this command, the interface will be unconfigured. There are three ways that the IP address can be set later:

- Using the IP SET INTERFACE IPADDRESS command
- You can set the interface to obtain its configuration via dynamic host configuration protocol (DHCP) using the IP SET INTERFACE DHCP ENABLED command. By default, DHCP is disabled.

This interface can obtain its IP configuration via PPP IPCP (***Internet Protocol Control Protocol***) negotiation. See PPPoA CLI commands or PPPoE CLI commands .

The IP stack automatically creates a loopback interface for address 127.0.0.1 subnet mask 255.0.0.0. This interface is not displayed by the IP LIST INTERFACES command.

You can use this command to add unnumbered interfaces.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the ip interface. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A

Option	Description	Default Value
ipaddress	The interface IP address in the format 192.168.102.3 If the IP address is set to the special value 0.0.0.0, the interface is marked as unconfigured. This value is used when the interface address is obtained automatically. For an unnumbered interface, the IP address parameter is used to specify the router-id of the interface. The router-id should be the same as the IP address of one of the router's numbered interfaces.	0.0.0.0
netmask	The netmask address of the interface displayed in the following format 255.255.255.0 The special value 255.255.255.255 is used to indicate an unnumbered interface. An unnumbered interface is configured by setting the IP address to the interface's router-id value, and setting netmask to 255.255.255.255.	If no IP address is supplied, the natural mask of the IP address is used.

Example --> ip add interface ip1 192.168.103.3 255.255.255.0

See also
```
ip attach
ip show interface
ip set interface ipaddress
ip set interface dhcp
```

Note: For information on setting DHCP client configuration options, see DHCP Client command reference.

4.1.8.2.6 IP ADD ROUTE

Syntax `IP ADD ROUTE <name> <dest_ip> <netmask> {[GATEWAY <gateway_ip>]|[INTERFACE <interface>]}`

Description This command creates a static route to a destination network address via a gateway device or an existing interface. It also allows you to create a default route.

Note: You can only create one default route. A default route will not be created if you have already created a default route using the IP ADD DEFAULTROUTE GATEWAY command or the IP ADD DEFAULTROUTE INTERFACE command.

A route specifies a destination network (or single host), together with a mask to indicate what range of addresses the network covers, and a next-hop gateway address or interface. If there is a choice of routes for a destination, the route with the most specific mask is chosen.

Routes are used when sending datagrams as well as forwarding them, so they are not relevant only to routers. However, a system with a single interface is likely to have a single route as a default route to the router on the network that it most often needs to use. If

the interface can communicate more efficiently with a particular destination by using a different router, then it will learn this fact from an ***Internet Control Message Protocol*** (ICMP) redirect message.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the route. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit. To create a default static route to a destination address, type default as the route name. You can only create one route called default.	N/A
dest_ip	The IP address of the destination network displayed in the following format: 192.168.102.3	N/A
netmask	The destination netmask address (format: 255.255.255.0)	N/A
gateway_ip	The IP address of the gateway that this route will use, displayed in the following format: 192.168.102.3	N/A
interface	The existing interface that this route will use. To display interface names, use the IP LIST INTERFACES command.	N/A

Example Example 1 routes through a gateway.
--> ip add route route1 192.168.103.3 255.255.255.0 gateway 192.168.102.3

Example 2 is a default route.
--> ip add route default 0.0.0.0 0.0.0.0 interface ip1

See also
```
ip list interfaces
ip add defaultroute gateway
ip add defaultroute interface
```

4.1.8.2.7 IP ADD ROUTE DISABLED

Syntax
```
IP ADD ROUTE <name> <dest_ip> <netmask> {[GATEWAY
<gateway_ip>]|[INTERFACE <interface>]} DISABLED
```

Description This command creates a static route to a destination network address via a gateway device or an existing interface. It also allows you to create a default route.

Note: You can only create one default route. A default route will not be created if you have already created a default route using the IP ADD DEFAULTROUTE GATEWAY command or the IP ADD DEFAULTROUTE INTERFACE command.

A route specifies a destination network (or single host), together with a mask to indicate what range of addresses the network covers, and a next-hop gateway address or interface. If there is a choice of routes for a destination, the route with the most specific mask is chosen.

Routes are used when sending datagrams as well as forwarding them, so they are not relevant only to routers. However, a system with a single interface is likely to have a single route as a default route to the router on the network that it most often needs to use. If the interface can communicate more efficiently with a particular destination by using a different router, then it will learn this fact from an ***Internet Control Message Protocol*** (ICMP) redirect message.

Note: This command is avalable on FIBER B,D,E MODULAR and ADSL B,C models only.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the route. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit. To create a default static route to a destination address, type default as the route name. You can only create one route called default.	N/A
dest_ip	The IP address of the destination network displayed in the following format: 192.168.102.3	N/A
netmask	The destination netmask address (format: 255.255.255.0)	N/A
gateway_ip	The IP address of the gateway that this route will use, displayed in the following format: 192.168.102.3	N/A
interface	The existing interface that this route will use. To display interface names, use the IP LIST INTERFACES command.	N/A

Example Example 1 routes through a gateway.
--> ip add route route1 192.168.103.3 255.255.255.0 gateway 192.168.102.3

Example 2 is a default route.
--> ip add route default 0.0.0.0 0.0.0.0 interface ip1

See also `ip list interfaces`
`ip add defaultroute gateway`
`ip add defaultroute interface`

4.1.8.2.8 IP ATTACH

Syntax `IP ATTACH {<name>|<number>} <transport>`

Description This command attaches an existing transport to an existing IP interface (e.g., a bridge or router) so that data can be transported via the selected transport method.

This command implicitly enables the transport being attached.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the ip list interfaces command.	N/A
number	An existing IP interface. To display interface numbers, use the ip list interfaces command. The number appears in the first column under the heading ID.	N/A
transport	An existing transport.	N/A

Example In the example below, ***eth1*** is the name of an Ethernet transport created using the ETHERNET ADD TRANSPORT command:

--> ip attach ip1 eth1

See also `IP ADD INTERFACE`
`IP LIST INTERFACES`

4.1.8.2.9 IP ATTACHBRIDGE

Syntax `IP ATTACHBRIDGE {<name>|<number>}`

Description This command attaches the bridge to the router via an existing IP interface.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the ip list interfaces command.	N/A
number	An existing IP interface. To display interface numbers, use the ip list interfaces command. The number appears in the first column under the heading ID.	N/A

See also `IP ADD INTERFACE`
`IP LIST INTERFACES`

4.1.8.2.10 IP ATTACHVIRTUAL

Syntax `IP ATTACHVIRTUAL <name> <real_interface>`

Description This command creates a virtual interface. The virtual interface is associated with a 'real' IP interface that has already been attached to a transport using the IP attach command. You can attach multiple virtual interfaces to one 'real' IP interface.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface to be used as a virtual interface. The IP interface should not have a transport attached to it. To display interface names, use the IP LIST INTERFACES command.	N/A
real_interface	An existing 'real' IP interface, attached to a transport, to which the virtual interface is associated with an existing 'real' IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A

Example --> ip attachvirtual ip_virtual ip_real

See also `ip list interfaces`

4.1.8.2.11 IP CLEAR ARPENTRIES

Syntax `ip clear arpentries`

Description This command clears all ARP entries.

Example --> ip clear arpentries

See also `IP LIST ARPENTRIES`

4.1.8.2.12 IP CLEAR INTERFACES

Syntax `ip clear interfaces`

Description This command clears all IP interfaces that were created using the IP ADD INTERFACE command.

Example --> ip clear interfaces

See also `ip delete interface`

4.1.8.2.13 IP CLEAR RIPROUTES

Syntax `ip clear riproutes`

Description This command deletes all the existing dynamic routes that have been obtained from RIP. It does not delete the static routes; see the IP CLEAR ROUTES command.

Example --> ip clear riproutes

See also
```
ip clear routes
ip set rip hostroutes
ip set interface rip accept
ip set interface rip send
```

4.1.8.2.14 IP CLEAR ROUTES

Description This command clears all static routes that were created using the IP ADD ROUTE command.

Example --> ip clear routes

See also `IP DELETE ROUTE`

4.1.8.2.15 IP DELETE INTERFACE

Syntax `IP DELETE INTERFACE {<name>|<number>}`

Description This command deletes a single IP interface that was created using the IP ADD INTERFACE command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> ip delete interface ip1

See also `IP CLEAR INTERFACES`
`IP LIST INTERFACES`

4.1.8.2.16 IP DELETE ROUTE

Syntax `IP DELETE ROUTE {<name>|<number>}`

Description This command deletes a single route that was created using the IP ADD ROUTE command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing route. To display route names, use the IP LIST ROUTES command.	N/A
number	An existing route. To display route numbers, use the IP LIST ROUTES command. The number appears in the first column under the heading ID.	N/A

Example --> ip delete route route1

See also `IP LIST ROUTES`

4.1.8.2.17 IP DETACH INTERFACE

Syntax `IP DETACH {<name>|<number>}`

Description This command detaches a transport from an IP interface that was previously attached using the IP ATTACH INTERFACE command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the ip list interfaces command.	N/A
number	An existing IP interface. To display interface numbers, use the ip list interfaces command. The number appears in the first column under the heading ID.	N/A

Example --> ip detach ip1

See also `ip list interfaces`

4.1.8.2.18 IP INTERFACE ADD PROXYARPENTRY

Syntax `IP INTERFACE {<name>|<number>} ADD PROXYARPENTRY <ipaddress> [<netmask>]`

Description This command configures proxy ARP functionality on an existing IP interface. This means that an interface responds to ARP requests for both its own address and for any address that has been configured as a proxy ARP address.

You can configure proxy ARP functionality on a single address or a range of addresses. Once you have configured a range of proxy ARP interfaces, you can set one or more addresses in the range to NOT respond to proxy ARP using the IP INTERFACE ADD PROXYARPEXCLUSION command.

Options The following table gives the range of values for each option thatcan be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
ipaddress	The IP address/range of addresses of the interface to be set as a proxy ARP entry, in the format: 192.168.102.3	N/A
netmask	The netmask address (or range of addresses) of the interface, displayed in the following format: 255.255.255.0	N/A

Example The following command adds proxy ARP support to the entire subnet 192.168.100.0:

--> ip interface ip1 add proxyarpentry 192.168.100.0 255.255.255.0

See also `ip interface add proxyarpexclusion`
`ip interface list proxyarpentries`

4.1.8.2.19 IP INTERFACE ADD PROXYARPEXCLUSION

Syntax `IP INTERFACE {<name>|<number>} ADD PROXYARPEXCLUSION <ipaddress> [<netmask>]`

Description This command configures proxy ARP exclusion functionality on an existing IP interface. This means that once you have configured an interface with a range of proxy ARP interfaces, you can set one or more addresses in the range to NOT respond to proxy ARP.

The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use THE IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
ipaddress	The IP address (or range of addresses) of the interface that you want to set as a proxy ARP exclusion entry, displayed in the following format: 192.168.102.3	N/A
netmask	The netmask address (or range of addresses) of the interface, displayed in the following format: 255.255.255.0	N/A

Example Example 1 adds proxy ARP support to the subnet 192.168.100.0 :

--> ip interface ip1 add proxyarpentry 192.168.100.0 255.255.255.0

Example 2 adds proxy ARP exclusion support to 192.168.100.10 255.255.255.254:

--> ip interface ip1 add proxyarpexclusion 192.168.100.10 255.255.255.254

This means that the entire 192.168.100.0 subnet supports proxy ARP, EXCEPT for addresses 192.168.100.10 and 192.168.100.11.

See also `IP INTERFACE ADD PROXYARPENTRY`
`IP INTERFACE LIST PROXYARPENTRIES`

4.1.8.2.20 IP INTERFACE ADD SECONDARYIPADDRESS

Syntax `IP INTERFACE {<name>|<number>} ADD SECONDARYIPADDRESS <ipaddress> [<netmask>]`

Description This command adds a secondary IP address to an existing IP interface. A secondary address may be used to create an extra IP address on an interface for management purposes, or to allow the IP stack to route between two subnets on the same interface.

The functionality of secondary IP addresses depends on several parameters including the type of IP interface and the netmask:

- If a secondary address is on the same subnet as the primary interface address, you do not need to specify a subnet mask for that secondary address. This applies to all interface types.
- If a secondary address is on a different subnet to the primary address, and the interface is Ethernet or a transport using a bridged encapsulation, you must specify the subnet mask. The IP stack will listen on the new address for connections to local services (e.g., for management purposes), and will also route packets to the new subnet.
- If a secondary address is on a different subnet to the primary address, and the interface is a point-to-point interface, specifying a netmask is optional.
- For the same behavior as described for Ethernet interfaces above, the subnet mask should be specified.
- If the subnet mask is not specified, the IP address will not be associated with any subnet, but will still be recognized as one of the IP stack's own addresses for local traffic.

Note: The ability to specify a subnet mask with a secondary address is still supported, but superseded by the functionality of virtual interfaces. You should USE VIRTUAL INTERFACES instead; see IP ATTACHVIRTUAL. Support for adding secondary IP addresses including subnet mask specification will be withdrawn in a future releases.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Option	Description	Default Value
ipaddress	A secondary IP address that you want to add to the main IP interface. You can add any number of secondary IP addresses. The IP address is displayed in the following format: 192.168.102.3 To display the secondary IP addresses, use the IP INTERFACE LIST SECONDARYIPADDRESSES command.	N/A
netmask	The netmask of the secondary IP address displayed in the following format: 255.255.255.0 To display the secondary IP addresses, use the IP INTERFACE LIST SECONDARYIPADDRESSES command.	none specified

Example --> ip interface ip1 add secondaryipaddress 192.168.102.3 255.255.255.0

See also `IP LIST INTERFACES`
`IP INTERFACE LIST SECONDARYIPADDRESSES`

4.1.8.2.21 IP INTERFACE ADD STATICARPENTRY

Syntax `IP INTERFACE {<name>|<number>} ADD STATICARPENTRY <ipaddress> <macaddr>`

Description This command allows you to add a static ARP entry. This is useful for testing purposes.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
ipaddress	The IP address/range of addresses of the interface to be set as a static ARP entry, in the format: 192.168.102.3	N/A
macaddr	A valid MAC address in the format: ##:##:##:##:##:##	N/A

Example --> ip interface ip1 add staticarpentry 192.168.1.1 00:20:2b:e0:03:87

See also `ip list interfaces`
`ip interface list staticarpentries`

4.1.8.2.22 IP INTERFACE CLEAR PROXYARPENTRIES

Syntax `IP INTERFACE {<name>|<number>} CLEAR PROXYARPENTRIES`

Description This command clears all proxy ARP entries and exclusions that were created using the IP INTERFACE ADD PROXYARPENTRY and IP INTERFACE ADD PROXYARPEXCLUSION commands.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> ip interface ip1 clear proxyarpentries

See also `IP INTERFACE ADD PROXYARPENTRY`
`IP INTERFACE ADD PROXYARPEXCLUSION`

4.1.8.2.23 IP INTERFACE CLEAR SECONDARYIPADDRESSES

Syntax `IP INTERFACE {<name>|<number>} CLEAR SECONDARYIPADDRESSES`

Description This command deletes all additional IP addresses that have been added to an existing IP interface using the IP INTERFACE ADD SECONDARYIPADDRESS command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> ip interface ip1 clear secondaryipaddresses

See also `IP LIST INTERFACES`
`IP INTERFACE ADD SECONDARYIPADDRESS`

```
IP INTERFACE DELETE SECONDARYIPADDRESS
IP INTERFACE LIST SECONDARYIPADDRESSES
```

4.1.8.2.24 IP INTERFACE CLEAR STATICARPENTRIES

Syntax `IP INTERFACE {<name>|<number>} CLEAR STATICARPENTRIES`

Description This command clears all static ARP entries that were created using THE IP INTERFACE ADD STATICARPENTRY command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> ip interface ip1 clear staticarpentries

See also `ip list interfaces`

4.1.8.2.25 IP INTERFACE DELETE PROXYARPENTRIES

Syntax `IP INTERFACE {<name>} DELETE PROXYARPENTRIES <number>`

Description This command deletes a single proxy ARP entries that was created using the IP INTERFACE ADD PROXYARPENTRY command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing proxy ARP entry. To display proxy ARP entry numbers, use the IP INTERFACE LIST PROXYARPENTRIES command.	N/A

Example --> ip interface ip1 delete proxyarpentry 1

See also IP INTERFACE ADD PROXYARPENTRY
IP INTERFACE LIST PROXYARPENTRIES

4.1.8.2.26 IP INTERFACE DELETE PROXYARPEXCLUSION

SyntaxIP INTERFACE {<name>} DELETE PROXYARPEXCLUSION <number>

Description This command deletes a single proxy ARP exclusion entry that was created using the IP INTERFACE ADD PROXYARPEXCLUSION command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing proxy ARP exclusion entry. To display proxy ARP exclusion numbers, use the IP INTERFACE LIST PROXYARPENTRIES command.	N/A

Example --> ip interface ip1 delete proxyarpexclusion 2

See also IP INTERFACE ADD PROXYARPEXCLUSION
IP INTERFACE LIST PROXYARPENTRIES

4.1.8.2.27 IP INTERFACE DELETE SECONDARYIPADDRESSES

Syntax IP INTERFACE {<name>|<number>} DELETE SECONDARYIPADDRESS <secondaryipaddress number>

Description This command deletes a single secondary IP address that has previously been added to an existing IP interface using the IP INTERFACE ADD SECONDARYIPADDRESS command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use THE IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Option	Description	Default Value
secondary ipaddress number	The number that identifies a secondary IP address that you want to delete from the main IP interface. To display secondary IP address numbers, use THE IP INTERFACE LIST SECONDARYIPADDRESSES command. The number appears in the first column under the heading ID.	N/A

Example --> ip interface ip1 delete secondaryipaddress 1

See also `IP LIST INTERFACES`
`IP INTERFACE LIST SECONDARYIPADDRESSES`

4.1.8.2.28 IP INTERFACE DELETE STATICARPENTRY

Syntax `IP INTERFACE <name> DELETE STATICARPENTRY <number>`

Description This command deletes a single static ARP entry that was created using the IP INTERFACE ADD STATICARPENTRY command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing static ARP entry. To display static ARP entry numbers, use the IP INTERFACE LIST STATICARPENTRIES command.	N/A

Example --> ip interface ip1 delete staticarpentry 2

See also `ip list interfaces`
`ip interface list staticarpentries`

4.1.8.2.29 IP INTERFACE LIST PROXYARPENTRIES

Syntax `IP INTERFACE {<name>|<number>} LIST PROXYARPENTRIES`

Description This command displays information about proxy ARP entries and exclusions that were created using the IP INTERFACE ADD PROXYARPENTRY and IP INTERFACE ADD PROXYARPEXCLUSION commands.

The following information is displayed:

- Interface ID numbers
- IP address and netmask of proxy ARP entries and exclusions
- Exclusion status: true for exclusions, false for inclusions

Options The following table gives the range of values for each option THAT can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> ip interface ip1 list proxyarpentries

```
 ID  |    IP Address  |   Netmask      |  Exclude
-----|----------------|----------------|----------
   1 | 192.168.100.0  | 255.255.255.0  | false
   2 | 192.168.100.8  | 255.255.255.254| true
-------------------------------------------------
```

See also `IP INTERFACE ADD PROXYARPENTRY`
`IP INTERFACE ADD PROXYARPEXCLUSION`
`IP LIST INTERFACES`

4.1.8.2.30 IP INTERFACE LIST SECONDARYIPADDRESSES

Syntax `IP INTERFACE {<name>|<number>} LIST SECONDARYIPADDRESSES`

Description This command lists the secondary IP addresses (and netmasks if applicable) that have been added to an existing IP interface using the IP INTERFACE ADD SECONDARYI-PADDRESS command.

Options The following table gives the range of values for each option THAT can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example In the example output below, secondary IP addresses without associated netmasks appear as 0.0.0.0 by default.

--> ip interface ip1 list secondaryipaddresses

```
 ID  |    IP Address   |    Netmask
-----|---------------------------------
   1 | 192.168.104.6   |  255.255.255.0
   2 | 192.168.103.4   |  0.0.0.0
   3 | 192.168.103.2   |  0.0.0.0
-------------------------------------
```

See also `ip list interfaces`
`ip interface list secondaryipaddresses`

4.1.8.2.31 IP INTERFACE LIST STATICARPENTRIES

Syntax `IP INTERFACE {<name>|<number>} LIST STATICARPENTRIES`

Description This command displays information about static ARP entries that were created using the IP INTERFACE ADD STATICARPENTRY command.

The following information is displayed:

- Interface ID numbers
- IP address of static ARP entries
- MAC address of static ARP entries

Options The following table gives the range of values for each option THAT can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> ip interface ip1 list staticarpentries

```
 ID  |    IP Address  |   Mac Address
-----|----------------|-------------------
   1 | 192.168.100.0  | 00:20:2b:e0:03:87
   2 | 192.168.100.8  | 00:20:2b:03:0a:72
-----------------------------------------
```

See also `IP LIST INTERFACES`

4.1.8.2.32 IP LIST APPSERVICES

Syntax `ip list aPPSERVICES`

Description A number of system processes use the IP stack to provide services, such as SNMP agent and TFTP server. These services are called AppServices.

This command lists the AppServices that are available and have configurable security classes. It displays the following information:

- AppService ID numbers
- AppService names
- the Security Class(es) configured on a specific AppService.

Example --> ip list appservices

```
-------------------------------------------------------------------
 ID  |AppService| Security Classes
-----|----------|--------------------------------------------------
   1 | ssh      | all
   2 | snmp     | all
   3 | http     | all
   4 | telnet   | all
-------------------------------------------------------------------
```

See also `IP SHOW APPSERVICE`

4.1.8.2.33 IP LIST ARPENTRIES

Syntax `ip list arpentries`

Description This command displays the ARP table that lists the following information:

- IP addresses and corresponding MAC addresses obtained by ARP.
- IP interface on which the host is connected
- Static status - 'no' for dynamically generated ARP entries; 'yes' for static entries added by the user.

Example --> ip list arpentries

IP ARP table entries:

```
 IP address      | MAC address       | Interface    | Static
-----------------|-------------------|--------------|--------
 10.10.10.10     | 00:20:2b:e0:03:87 | ip3          | no
```

```
-----------------|--------------------|--------------|--------
 20.20.20.20     | 00:20:2b:03:0a:72 | ip2          | no
-----------------|--------------------|--------------|--------
 30.30.30.30     | 00:20:2b:03:09:c4 | ip1          | no
-------------------------------------------------------------
```

See also IP CLEAR ARPENTRIES

4.1.8.2.34 IP LIST CONNECTIONS

Syntax ip list connections

- This command lists the active TCP/UDP connections in use by applications running on the device. It displays the following information:
- Protocol type (TCP or UDP)
- Local connection address
- Remote connection address
- Connection state for TCP connections

This command does not show raw socket connections or UDP connections opened internally within the IP stack.

Example The example below shows an active telnet connection, WebServer, TFTP server and SNMP:

--> ip list connections

```
Local TCP/UDP connections:

 Prot | Local address        | Remote address       | State       | Owner
------|----------------------|----------------------|-------------|------------
 tcp  | *:8008               | *:*                  | LISTEN      | webserver
 tcp  | *:22                 | *:*                  | LISTEN      | sshd
 tcp  | *:23                 | *:*                  | LISTEN      | webserver
 tcp  | *:80                 | *:*                  | LISTEN      | webserver
 udp  | 255.255.255.255:3913 | <2> *:*              |             | grsp
 udp  | *:68                 | *:*                  |             | dhcpclient
 udp  | *:68                 | <1> *:*              |             | dhcpclient
 udp  | *:55001              | *:*                  |             | tftp
 udp  | *:55000              | *:*                  |             | tftp
 udp  | *:50001              | *:*                  |             | snmpr
 udp  | *:161                | *:*                  |             | snmpr
 udp  | *:50000              | *:*                  |             | dnsrelay
 udp  | *:53                 | *:*                  |             | dnsrelay
 udp  | *:520                | *:*                  |             | rip
 udp  | *:123                | *:*                  |             | sntp
```

4.1.8.2.35 IP LIST INTERFACES

Syntax `ip list interfaces`

Description This command lists information about IP interfaces that were added using the IP ADD INTERFACE command. The following information is displayed:

- Interface ID numbers
- Interface names
- IP addresses (if previously specified)
- DHCP status
- Whether a transport is attached to the interface, and if so, the name of the transport
- Whether a virtual interface is attached to a real interface. The name of the attached virtual interface is displayed in the *Transport* column in square brackets, for example [ip2]

Example --> ip list interfaces

```
IP Interfaces:

 ID  |    Name      |    IP Address    |   DHCP   |  Transport
-----|--------------|------------------|----------|--------------
   1 | ppp_device   | 192.168.102.2    | disabled | pppoe1
   2 | ip2          | 192.168.102.3    | disabled | Not attached
   3 | ip_real      | 192.168.101.2    | disabled | ethernet1
   4 | ip_virtual   | 192.168.150.1    | disabled | [ip_real]
-------------------------------------------------------------------
```

See also `IP SHOW INTERFACE`
`IP SET INTERFACE DHCP`

4.1.8.2.36 IP LIST RIPROUTES

Syntax `ip list riproutes`

Description This command lists information about the routes that have been obtained from RIP. It displays the following:

- Destination IP addresses
- Destination netmask address
- Gateway address
- Cost - The number of hops counted as the cost of the route.

- Timeout - the number of seconds that this RIP route will remain in the routing table unless updated by RIP
- Source interface - the name of the existing interface that this route uses

Example --> ip list riproutes

IP RIP routes:

```
 Destination   | Mask          | Gateway       | Cost | Time |Source
---------------|---------------|---------------|------|------|------
 192.168.101.1 | 255.255.255.0 | 10.10.10.10   | 1    | 3000 | ip2
-------------------------------------------------------------------
```

See also `IP SET RIP HOSTROUTES`
`IP SET INTERFACE RIP ACCEPT`
`IP SET INTERFACE RIP SEND`

4.1.8.2.37 IP LIST ROUTES

Syntax `ip list routes`

Description This command lists information about existing routes. It displays the ID, name, destination IP address (if applicable), netmask address (if applicable), and gateway address or interface name (whichever is applicable).

- Route ID numbers
- Route names
- Destination IP addresses (if previously specified)
- Destination netmask address (if previously specified)
- Either the gateway address or the name of the destination interface (whichever is set)

Example --> ip list routes

IP routes:

```
 ID  |    Name  | Destination    | Netmask        |Gateway/Interface
-----|----------|----------------|----------------|-----------------
   2 | route2   | 192.168.102.3  | 255.255.255.0  | ip1
   1 | route1   | 192.168.50.50  | 255.255.255.0  | 192.168.68.68
-------------------------------------------------------------------
```

See also `ip show route`

4.1.8.2.38 STOP PING

Syntax `STOP PING`

Description This command is used to stop a running ping request. In case, you specify a high number of attempts for the ping request and then intend to stop the running ping request cycle, you need to use the stop ping command to obtain the required functionality.

This command involves no parameters. On entering a stop ping request, the statistics for the number of pings attempted so far shall be displayed. These statistics are displayed, once the ping task completes the last ping request it was processing at the time when the stop ping command was triggered.

Example --> ip ping 192.168.0.12 iplan 644 (644 specifies the numberOfAttempts)

ping: PING 192.168.0.12: 32 data bytes ping: 40 bytes from 192.168.0.12: seq = 0, ttl=128, rtt<10ms ping: 40 bytes from 192.168.0.12: seq = 0, ttl=128, rtt<10ms ping: 40 bytes from 192.168.0.12: seq = 0, ttl=128, rtt<10ms ping: 40 bytes from 192.168.0.12: seq = 0, ttl=128, rtt<10ms

stop ping

ping: MANUALLY STOPPING THE RUNNING PING REQUEST !!!!!

ping: 40 bytes from 192.168.0.11: seq = 0, ttl=128, rtt<10ms ping: Ping stopped manually by the user

ping: Ping statistics:

ping: Packets: Sent = 5, Recieved = 5, Lost = 0 ping: Round-trip times:

ping: Minimum = 0ms, Maximum = 0ms, Average < 1ms

See also `Domain name system - DNS`

4.1.8.2.39 IP PING

Syntax `IP PING <destination> [<ifname>] [<numberofattempts>] [<timeoutval>] [<blocksize>] [<tos>]`

Description This command pings a specified destination. If you are using a DNS client, you can ping either an IP address or a host name. If you are not using DNS client, you only ping a destination IP address.

It's possible specify the name of the interface over which the ping is sent. The ping request message will use the IP address of this interface as source IP address.

In addition to these, you can configure certain additional parameters for the ping request. These include the number of ping attempts [<numberOfAttempts>], the timeout value for a ping request [<timeoutVal>], the data block size for an outgoing ping request [<blockSize>] and the type of service or diffServCodePoint parameter [<TOS>]. The

type of service (TOS) parameter is used for test packets, and to specify the type of service provided to the outgoing ping request at the IP level.

All these additional parameters are optional and hence when these are not specified, the Default Values are used instead.

Options The following table gives the range of values for each option THAT can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
destination	Either the IP address or host name (if you are using DNS client) of the destination machine that you want to ping.	N/A
ifname	A name that identifies an existing IP interface. To display interface names, use the ip list interfaces command.	
numberOfAttempts	A number that identifies the number of ping attempts for the ping operation. t ranges from 0-65534.	1
timeoutVal	A number that identifies the value in seconds, for which the ping response will be awaited. In case the destination specified in the destination parameter is not reachable, then the request will be taken as timed out after the specified number of seconds have elapsed. It ranges from 0-60 (seconds).	4
blockSize	A number that identifies the payload size for a ping request. It ranges from 0-65534.	32
TOS	A number that identifies the type of service for the ping request message. This shall be used for the test packets. It ranges from 0- 64.	0

Example --> ip ping 192.168.102.3

```
ip: ping - reply received from 192.168.102.3
```

If ping was unsuccessful, the following output is displayed:

ip: ping - no reply received.

See also Domain name system - DNS

4.1.8.2.40 IP SET APPSERVICE

Syntax `IP SET APPSERVICE <name> SECCLASSES <secClasses>`

Description A number of system processes use the IP stack to provide services, such as SNMP agent and TFTP server. These services are called AppServices. This command allows you to set the security class(es) associated with an AppService. A security class is synonymous with a security interface type. It is assumed that you have already assigned security interfaces to your IP interfaces, using the command security show alg.

Setting the security class(es) for an AppService defines the interface(s) through which the AppService will be provided.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing AppService. To display AppService names, use the ip list appservices command.	N/A
number	A number that identifies an existing AppService. To display AppService numbers, use the ip list appservices command. The number appears in the first column under the heading ID.	N/A
secClasses	Supported secClasses values are as follows: all - allows access to the AppService via all existing security interfaces none - prevents access to the AppService via any existing security interface internal - allows access to the AppService via existing internal security interfaces external - allows access to the AppService via existing external security interfaces dmz - allows access to the AppService via existing dmz security interfaces To allow access to an AppService via two security interface types, type the secClass values separated by a comma (for example, internal,external) or separated by a space and enclosed in double-quotation marks (for example, “internal external”). To specify all three internal, external and dmz secClasses, use the all value.	0.0.0.0

Example --> ip set appservice tftp secclasses external,dmz

Example --> ip set appservice http secclasses none

See also `IP SET INTERFACE MTU`
`IP SET INTERFACE DHCP`
`IP LIST INTERFACES`
`IP SET INTERFACE NETMASK`

4.1.8.2.41 IP SET INTERFACE IPADDRESS

Syntax `IP SET INTERFACE {<name>|<number>} IPADDRESS <ipaddress> [<netmask>]`

Description This command sets the IP address for an existing IP interface.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
ip address	The IP address of the interface displayed in the following format: 192.168.102.3. If the IP address is set to the special value 0.0.0.0, the interface is marked as unconfigured. This value is used when the interface address is obtained automatically. For unnumbered interfaces, the IP address parameter is used to specify the router-id of the interface. The router-id should be the same as the IP address of one of the router's numbered interfaces.	0.0.0.0
netmask	The netmask address of the interface displayed in the following format: 255.255.255.0. The special value 255.255.255.255 indicates an unnumbered interface, that is configured by setting the IP address to the interface's router-id value, and setting netmask to 255.255.255.255.	If no IP address is supplied, the natural mask of the IP address is used.

Example --> ip set interface ip4 ipaddress 192.168.102.3 255.255.255.0

See also `IP SET INTERFACE MTU`
`IP SET INTERFACE DHCP`
`IP LIST INTERFACES`
`IP SET INTERFACE NETMASK`

4.1.8.2.42 IP SET INTERFACE NETMASK

Syntax `IP SET INTERFACE {<name>|<number>} NETMASK <netmask>`

Description This command sets the netmask for an existing IP interface.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use THE IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
netmask	The netmask address of the interface in the format: 255.255.255.0 The special value 255.255.255.255 is used to indicate an unnumbered interface, that is configured by setting the IP address to the interface's router-id value, and setting netmask to 255.255.255.255.	N/A

Example --> ip set interface ip6 netmask 255.255.255.0

See also `IP SET INTERFACE IPADDRESS`
`IP LIST INTERFACES`

4.1.8.2.43 IP SET INTERFACE MTU

Syntax `IP SET INTERFACE {<name>|<number>} MTU <mtu>`

Description This command sets the MTU (***Maximum Transmission Unit***) for an existing IP interface.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	1500

Option	Description	Default Value
mtu	***Maximum Transmission Unit***: maximum packet size (in bytes) an interface can handle. The MTU should be set to a value appropriate for the transport attached to the interface (typically from 576 to 1500 bytes). For example, Ethernet and most other transports support an MTU of 1500 bytes, whereas PPPoE supports an MTU of 1492 bytes.	1500

Example --> ip set interface ip2 mtu 800

See also
```
IP SET INTERFACE IPADDRESS
IP SET INTERFACE DHCP
IP LIST INTERFACES
```

4.1.8.2.44 IP SET INTERFACE DHCP

Syntax `IP SET INTERFACE {<name>|<number>} DHCP {ENABLED|DISABLED}`

Description This command specifies whether a named interface should obtain its configuration via DHCP.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the ip list interfaces command.	N/A
number	An existing IP interface. To display interface numbers, use the ip list interfaces command. The number appears in the first column under the heading ID.	N/A
enabled	The interface obtains configuration information from DHCP client.	Disabled
disabled	The interface does not use DHCP client configuration information.	

Example --> ip set interface ip2 dhcp enabled

See also
```
IP SET INTERFACE IPADDRESS
IP SET INTERFACE MTU
IP LIST INTERFACES
```

Description For information on setting DHCP client configuration options, see DHCP Client command reference.

4.1.8.2.45 IP SET INTERFACE GATEWAY

Syntax `IP SET INTERFACE {<name>|<number>} GATEWAY {<IP-ADDRESS>}`

Description This command specifies the gateway ip-address associated to the given interface

Note: This command is avalable on FIBER B,D,E MODULAR and ADSL B,C models only.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the ip list interfaces command.	N/A
number	An existing IP interface. To display interface numbers, use the ip list interfaces command. The number appears in the first column under the heading ID.	N/A
ip-address	The gateway ip-address	N/A

Example --> ip set interface ip2 dhcp enabled

See also
```
IP ADD ROUTE
IP SET INTERFACE MTU
IP LIST INTERFACES
```

For information on setting DHCP client configuration options, see DHCP Client command reference.

4.1.8.2.46 IP SET INTERFACE RIP ACCEPT

Syntax `IP SET INTERFACE {<name>|<number>} RIP ACCEPT {NONE|V1|V2|ALL}`

Description This command specifies whether an existing interface accepts RIP messages. You can specify what version of RIP messages are accepted by the interface.

When receiving RIP v1 messages, the IP stack tries to use the information it has available to determine the appropriate subnet mask for the addresses received.

Options The following table gives the range of values for each option THAT can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACE COMMAND. The number appears in the first column under the heading ID.	N/A
none	The interface does not accept RIP messages.	None
v1	The interface only accepts RIP v. 1 messages (RFC1058)	
v2	The interface only accepts RIP v. 2 messages (RFC1723)	
all	The interface accepts RIP version 1 (RFC1058) and RIP version 2 (RFC1723) messages	

Example --> ip set interface ip3 rip accept none

See also
```
IP SET INTERFACE RIP SEND
IP SET INTERFACE RIP MULTICAST
IP SET RIP HOSTROUTES
IP SET RIP POISON
IP SHOW
IP LIST INTERFACES
```

4.1.8.2.47 IP SET INTERFACE RIP MULTICAST

Syntax `IP SET INTERFACE {<name>|<number>} RIP MULTICAST {ENABLED | DISABLED}`

Description This command allows you to enable/disable whether RIP version 2 messages are sent via multicast.

RIP version 2 messages sent via multicast are only received by the hosts on the network that have a multicast network address. If this command is disabled, RIP version 2 messages are sent via broadcast and are received by all the hosts on the network.

You need to set RIP to send v2 messages using the IP SET INTERFACE RIP SEND command in order for the IP SET INTERFACE RIP MULTICAST ENABLED command to send version 2 messages via multicast.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
enabled	Allows RIP version 2 messages to be sent via multicast.	Disabled
disabled	Disables RIP version 2 messages being sent via multicast. Messages are sent via broadcast instead.	

Example --> ip set interface ip1 rip multicast enabled

See also `IP LIST INTERFACES`
`IP SET INTERFACE RIP SEND`

4.1.8.2.48 IP SET INTERFACE RIP SEND

Syntax `IP SET INTERFACE {<name>|<number>} RIP SEND {NONE|V1|V2|ALL}`

Description This command specifies whether an existing interface can send RIP messages. You can specify which version of RIP messages will broadcast routing information on the interface. Routing information is broadcast every 30 seconds or when the RIP routing table is changed.

Note: RIP version 1 does not allow specification of subnet masks; a RIP version 1 route that appears to be to an individual host might in fact be to a subnet, and treating it as a route to the whole network may be the best way to make use of the information.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A

Option	Description	Default Value
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
rip send none	The interface does not accept RIP messages.	rip send none (this command affects all interfaces except loopback interfaces)
rip send v1	The interface only sends RIP v. 1 messages (RFC1058)	
rip send v2	The interface only sends RIP version 2 messages (RFC1723). If set, RIP version 2 is used on all non-loop-back interfaces.	
rip send all	The interface sends RIP version 1 (RFC1058) and RIP version 2 (RFC1723) messages.	

Example --> ip set interface ip1 rip send v1

See also
```
IP SET INTERFACE RIP ACCEPT
IP SET RIP HOSTROUTES
IP SET RIP POISON
IP SHOW
IP LIST INTERFACES
```

For information on RFC1058 and RFC1723, see http://www.ietf.org/rfc/rfc1723.txt

4.1.8.2.49 IP SET INTERFACE TCPMSSCLAMP

Syntax `IP SET INTERFACE <name> TCPMSSCLAMP {ENABLED|DISABLED}`

Description This command enables/disables TCP MSS (***Maximum Segment Size***) Clamp functionality on an existing IP interface. When TCP MSS Clamp is enabled on an interface, all TCP traffic routed through that interface will be examined. If a TCP SYN (synchronize/start) segment is sent with a maximum segment size larger than the interface MTU (***Maximum Transmission Unit***), the MSS option will be rewritten in order to allow TCP traffic to pass through the interface without requiring fragmentation.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
enabled	TCP SYN segments routed through this interface will be examined and, if necessary, modified.	Disabled
disabled	The IP stack will not examine or modify TCP traffic routed through this interface.	

Example --> ip set interface ip2 tcpmssclamp enabled

See also `IP SET INTERFACE MTU`
`IP SHOW`

4.1.8.2.50 IP SET RIP ADVERTISEDEFAULT

Syntax `ip set rip advertisedefault {enabled | disabled}`

Description This command enables/disables the advertising of a default route via RIP. If you set this to ***enabled***, then create a default route using the IP ADD DEFAULTROUTE commands, the route will also be added to those advertised by the RIP protocol. The cost associated with the route is the value set using the IP SET RIP DEFAULTROUTECOST command.

You must enable default advertising before you create the default route.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	Enables RIP to advertise a default route with the cost metric set using the IP SET RIP DEFAULTROUTE-COST command.	Disabled
disabled	Disables advertisement of a default route.	

Example --> ip set rip advertisedefault enabled

See also `ip add defaultroute gateway`
`ip add defaultroute interface`
`ip set rip defaultroutecost`
`ip set route advertise`

4.1.8.2.51 IP SET RIP AUTHENTICATION

Syntax `ip set rip authentication {enabled | disabled}`

Description This command enables/disables RIP v2 plain text authentication.

If ***enabled***, a plain text authentication string is placed in RIP v2 packets. RIP v2 packets will only be accepted if they contain an authentication entry with the correct password string. Packets with no authentication or the wrong password will be rejected.

To set an authentication password, use the IP SET RIP PASSWORD command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Example --> ip set rip authentication enabled

See also
```
ip set rip password
ip show
```

4.1.8.2.52 IP SET RIP DEFAULTROUTECOST

Syntax `IP SET RIP DEFAULTROUTECOST <cost>`

Description This command sets the number of hops counted as the cost of a default route advertised via RIP.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
cost	The number of hops counted as the cost of the default route. It can be any positive integer between 1 and 15.	1

Example --> ip set rip defaultroutecost 10

See also
```
IP ADD DEFAULTROUTE GATEWAY
IP ADD DEFAULTROUTE INTERFACE
IP SET RIP ADVERTISEDEFAULT
IP SET ROUTE ADVERTISE
```

4.1.8.2.53 IP SET RIP HOSTROUTES

Syntax `ip set rip hostroutes {enabled | disabled}`

Description Specifies whether IP interfaces will accept RIP routes to specific routes.

Note: RIP version 1 does not allow specification of subnet masks; a RIP version 1 route that appears to be to an individual host might in fact be to a subnet, and treating it as a route to the whole network may be the best way to make use of the information.

To display the current state of RIP hostroutes, use the IP SHOW COMMAND.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	Sets the hostroutes flag to on. The interface accepts RIP routes to specific routes.	Disabled
disabled	Sets the hostroutes flag to off: RIP version 1 routes to individual hosts are treated as routes to the network containing the host. RIP version 2 routes to individual hosts are ignored.	

Example --> ip set rip hostroutes enabled

See also
```
IP SET INTERFACE RIP ACCEPT
IP SET INTERFACE RIP SEND
IP SHOW
```

4.1.8.2.54 IP SET RIP PASSWORD

Syntax `IP SET RIP PASSWORD <password>`

Description This command sets an authentication string that is placed in RIP v2 packets if IP SET RIP AUTHENTICATION is enabled.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
password	An authentication password used by RIP v2 packets if IP SET RIP AUTHENTICATION is enabled. The password is a string of 0 to 16 characters.	N/A

Example --> ip set rip password vancouver

See also `IP SET RIP AUTHENTICATION`
`IP SHOW`

4.1.8.2.55 IP SET RIP POISON

SyntaxIP SET RIP POISON {ENABLED | DISABLED}

Description Enables or disables the poisoned reverse flag. If this flag is on, TCP/IP performs poisoned reverse as defined in RFC 1058; see that RFC for discussion.

To display the current state of the poisoned reverse flag, use the IP SHOW command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	Sets the poisoned reverse flag to on. TCP/IP performs poisoned reverse as defined in RFC 1058.	Disabled
disabled	Sets the poisoned reverse flag to off.	

Example --> ip set rip poison enabled

See also `IP SET INTERFACE RIP ACCEPT`
`IP SET INTERFACE RIP SEND`
`IP SET RIP HOSTROUTES`
`IP SHOW`

4.1.8.2.56 IP SET ROUTE

Syntax `IP SET ROUTE {<name>|<number>} <ENABLED|DISABLED>`

Description This command enables/disables an existing static route (including a default route).

If the route being operated on by this command is a default route then the command also might have the effect of making the device not reachable

Note: This command is avalable on FIBER B,D,E MODULAR and ADSL B,C models only.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	Enables a static route.	Disabled

Option	Description	Default Value
disabled	Disables a static route.	

Example --> ip set route myroute enabled

See also `ip list routes, ip add route, ip show route`

4.1.8.2.57 IP SET ROUTE ADVERTISE

Syntax `IP SET ROUTE {<name>|<number>} ADVERTISE <ENABLED|DISABLED>`

Description This command enables/disables the advertising of an existing static route (including a default route) via RIP. The cost advertised with this route is the cost specified by the IP SET ROUTE COST command.

If the route being operated on by this command is a default route then the setting of the IP SET RIP ADVERTISEDEFAULT command also has an effect:

- If the IP SET RIP ADVERTISEDEFAULT command is enabled, then it controls the advertising of the route and uses the cost set by the IP SET DEFAULTROUTECOST command.
- If the IP SET RIP ADVERTISEDEFAULT command is disabled, then the IP SET ROUTE ADVERTISE command controls the advertising of the route and uses the cost set by the IP SET ROUTE COST command as described above.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	Enables RIP to advertise a static route.	Disabled
disabled	Disables advertisement of a static route.	

Example --> ip set route myroute advertise enabled

See also
`IP SET ROUTE COST`
`IP LIST ROUTES`
`IP SET RIP ADVERTISEDEFAULT`
`IP SET RIP DEFAULTROUTECOST`

4.1.8.2.58 IP SET ROUTE DESTINATION

Syntax `IP SET ROUTE {<name>|<number>} DESTINATION <dest-network> <netmask>`

Description This command sets the destination network address of a route previously created using the IP ADD ROUTE COMMAND.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing route. To display route names, use the IP LIST ROUTES command.	N/A
number	An existing route. To display route numbers, use the IP LIST ROUTES command. The number appears in the first column under the heading ID.	N/A
dest-network	The IP address of the destination network in the format: 192.168.102.3	N/A
netmask	The destination netmask address (format: 255.255.255.0)	N/A

Example --> ip set route route1 destination 192.168.103.3 255.255.255.0

See also `IP SET ROUTE GATEWAY`
`IP SET ROUTE COST`
`IP LIST ROUTES`

4.1.8.2.59 IP SET ROUTE GATEWAY

Syntax `IP SET ROUTE {<name>|<number>} GATEWAY <gateway>`

Description This command sets the gateway address of a route previously created using the IP ADD ROUTE command. If you want the route to go directly to its destination and not via a gateway, specify 0.0.0.0 as the gateway.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing route. To display route names, use the IP LIST ROUTES command.	N/A
number	An existing route. To display route numbers, use the IP LIST ROUTES command. The numbers appear in the first column under the heading ID.	N/A

Option	Description	Default Value
gateway	The IP address of the gateway that the IP routes through, displayed in the following format: 192.168.102.3 If you added a route directly to an interface, the gateway address is set by default to 0.0.0.0 so that no gateway is specified.	N/A

Example --> ip set route route1 gateway 192.168.102.3

See also
```
IP ADD ROUTE
IP SET ROUTE DESTINATION
IP SET ROUTE COST
IP LIST ROUTES
```

4.1.8.2.60 IP SET ROUTE COST

Syntax `IP SET ROUTE {<name>|<number>} COST <cost>`

Description This command sets the number of hops counted as the cost of the route for a route previously created using the IP ADD ROUTE command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing route. To display route names, use the IP LIST ROUTES command.	N/A
number	An existing route. To display route numbers, use the IP LIST ROUTES command. The number appears in the first column under the heading ID.	N/A
cost	The number of hops counted as the cost of the route. This may affect the choice of route when the route is competing with routes acquired from RIP. (Using a mixture of RIP and static routing is not advised). The cost value can be any positive integer.	1

Example --> ip set route route1 cost 3

See also
```
IP ADD ROUTE
IP LIST ROUTES
IP SET ROUTE ADVERTISE
```

4.1.8.2.61 IP SET ROUTE INTERFACE

Syntax `IP SET ROUTE {<name>|<number>} INTERFACE {<interface>|NONE}`

Description This command sets the interface used by a route previously created by the IP ADD ROUTE command. If you want the existing route to route to an address via a gateway device, use none so that no interface is set.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing route. To display route names, use the IP LIST ROUTES command.	N/A
number	An existing route. To display route numbers, use the IP LIST ROUTES command. The number appears in the first column under the heading ID.	N/A
interface	The name of the existing interface that the IP routes through, displayed in the following format: 192.168.102.3 To display interface names, use the IP LIST INTERFACES command.	N/A
none	No interface is set. This is used for routes that route via a gateway device instead of an interface.	N/A

Example --> ip set route r1 interface eth1

See also `IP LIST INTERFACES`
`IP LIST ROUTES`

4.1.8.2.62 IP SET TTL

Syntax `IP SET TTL {<number>}`

Description This command sets the default time-to-live (ttl) value in the IP header of a generated IP packet. To display the current state of *ttl*, use the *ip show* command.

Note: This command is avalable on FIBER B,D,E MODULAR and ADSL B,C models only.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
number	A number that specifies the time-to-live (ttl) value for the IP header of all transmitted packets	128

Example --> ip set ttl 60

See also `ip show`

4.1.8.2.63 IP SHOW

Syntax `ip show`

Description Shows current RIP configuration and any other information global to the router.

Example --> ip show

```
Global IP configuration:

          Host routes: false
      Poison reverse: false
      Authentication: false
       Auth password:
   Advertise default: false
  Default Route Cost: 1
         Default TTL: 128
```

See also `IP SET RIP HOSTROUTES`
`IP SET RIP POISON`

4.1.8.2.64 IP SHOW APPSERVICE

Syntax `IP SHOW APPSERVICE {<name>|<number>}`

Description This A number of ISOS processes use the IP stack to provide services, such as SNMP agent and TFTP server. These services are called AppServices.

This command shows system related information about the specified AppService. The command is typically used for debugging purposes than for normal system configuration.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing AppService. To display AppService names, use the ip list appservices command.	N/A
number	A number that identifies an existing AppService. To display AppService numbers, use the ip list appservices command. The number appears in the first column under the heading ID.	N/A

4.1.8.2.65 IP SHOW INTERFACE

Syntax `IP SHOW INTERFACE {<name>|<number>}`

Description This command displays the following information about a named interface:

- IP address and netmask address (if set). For virtual interfaces, the name of the real interface that the virtual interface is attached to is also displayed.
- MTU (Maximum Transmission Unit)
- Status of DHCP
- Status of TCP MSS Clamp
- Status of RIP send and RIP accept
- Status of RIP multicast

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A
number	An existing IP interface. To display interface numbers, use the IP LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example Real IP interface

```
--> ip show interface ip0

IP Interface: ip0

                  IPaddr : 10.17.90.153
                    Mask : 255.255.255.0
          Rx Packet Count : 210
          Tx Packet Count : 5
                     MTU : 1500

                    Dhcp : true

            TCP MSS Clamp : false
    Source Addr Validation : false
     Icmp Router Advertise : false
                Accept V1 : false
```

```
                    Send V1 : false
                  Accept V2 : false
                    Send V2 : false
               Send Multicast : false
```

Example Virtual IP interface

```
-> ip show interface ip1

IP Interface: ip1 - virtual [ip0]

                   IPaddr : 192.168.10.1
                     Mask : 255.255.255.0
           Rx Packet Count : 0
           Tx Packet Count : 0
                       MTU : 1500

                      Dhcp : false

             TCP MSS Clamp : false
    Source Addr Validation : false
     Icmp Router Advertise : false
                 Accept V1 : false
                   Send V1 : false
                 Accept V2 : false
                   Send V2 : false
            Send Multicast : false
```

See also IP SHOW
IP SHOW ROUTE
IP LIST INTERFACES

4.1.8.2.66 IP SHOW ROUTE

Syntax `IP SHOW ROUTE {<name>|<number>}`

Description This command displays the following information about a named route:

- Destination IP address
- Netmask address
- Gateway IP address
- Cost: the number of hops counted as the cost of the route
- Interface name

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing route. To display route names, use the IP LIST ROUTES command.	N/A
number	An existing route. To display route numbers, use the IP LIST ROUTES command. The number appears in the first column under the heading ID.	N/A

Example --> ip show route route3

```
IP route: DHCP-DefRt1

   Destination: 0.0.0.0
       Netmask: 0.0.0.0
       Gateway: 10.17.90.1
          Cost: 1
     Interface: ip0
     Advertise: false

 Route enabled: true
   Route valid: true
```

See also IP SHOW
IP LIST ROUTES

4.2 Security

This section describes the AT-iMG models built-in security facilities, and how to configure and monitor them.

4.2.1 Overview

The aim of this chapter is to teach you how to configure security services to manage and restrict the traffic that passes between the Internet and your network, and protect your network infrastructure from attacks. The components of the package are:

- *Network Address Translation (NAT)* component; maps multiple addresses on a private network to an externally-visible address (or range of addresses) on the outside network
- *Firewall* component; blocks certain traffic between interfaces based on stateful packet information (SPI)

- *Intrusion Detection Settings (IDS)* component; implements security measures to protect your network from suspicious hosts
- *Security* component; manages the Security package, and enables security features such as management stations, triggers, security applications, session tracking and application services

4.2.2 Security support on AT-iMG Models

The ***Security module*** is the main module in the AT-iMG Models that acts as a server to the other two ***security*** modules; ***Firewall*** and ***NAT***, forming the Security System (see Figure 7).

This component allows you to:

- **enable/disable** all modules in the Security package (including the child modules; NAT and Firewal, that cannot otherwise be configured)
- add IP interfaces to the Security package to create **security interfaces** that are used to configure the NAT and Firewall child modules
- configure **triggers** to allow applications to open secondary port sessions
- configure **IDSs** (Intrusion Detection Settings)
- configure **management stations** to allow a specific host (or range of hosts) remote access to the device without having to go through NAT and/or Firewall
- configure **application services**; to restrict access to a specific application service on a specific IP interface once the interfaces have been defined as security interface
- configure **logging**: (On FIber D,E Modular and ADSL A,B,C models only) to track intrusion events, blocking-events and session-events.

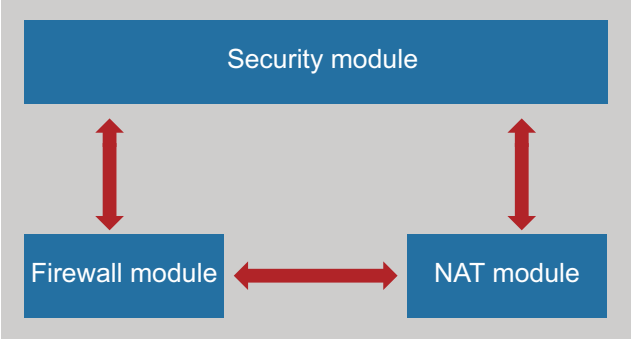


FIGURE 4-1 Security modules on AT-iMG Models

4.2.3 Security interfaces

A security interface is an existing IP interface that has been defined as either as ***Internal***, ***External*** and ***DMZ*** (see Figure To Be Supplied)

- An ***Internal interface*** is an IP interface that is attached to a network that needs to be protected from the network attached to the ***External interface***. For example, an interface attached to a private LAN is an internal interface.
- The ***External interface*** is an IP interface that is attached to a network, for example the Internet, containing hosts that may pose a security threat to hosts on the ***internal interfaces***.
- A ***DMZ*** (demilitarized zone) is an IP interface serving a small network that acts as a neutral zone between the inside network and the outside network. A DMZ is a portion of the local network that is almost completely open to the external network. There may be some restriction at external access to the DMZ, but much less than the restriction of access to the ***internal interface.***

To define an IP interface use the IP ADD INTERFACE command. (ref to ip command list)

To define an existing IP interface as a ***security*** interface use the SECURITY ADD INTERFACE command.

To show the ***security*** interfaces currently defined, use the SECURITY LIST INTERFACES command.

Note: Only one external security interface and one DMZ security interface can be defined

Note: Security interfaces must be created before you can configure the majority of the features of the security package

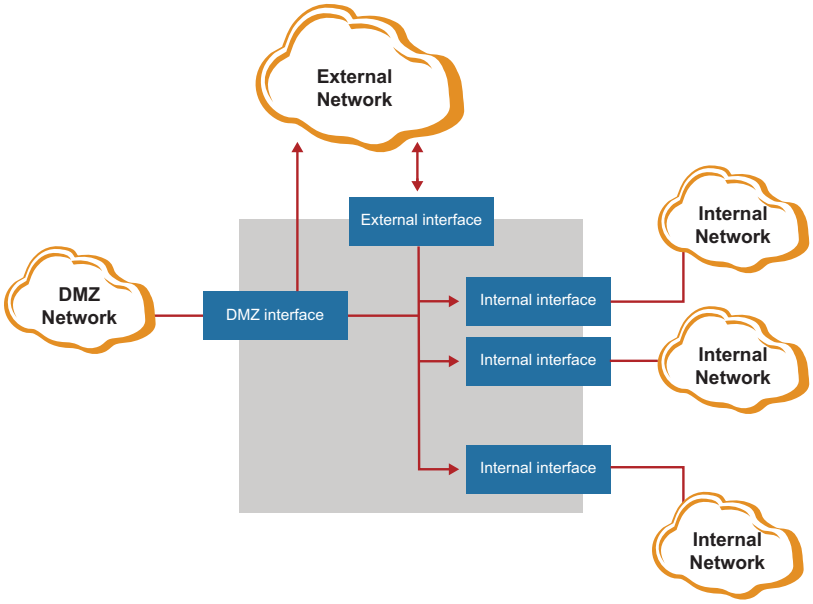


FIGURE 4-2 Security interfaces on AT-iMG Models

4.2.3.1 Security Triggers - Dynamic Port Opening

The ***Dynamic Port Opening (aka Security Trggers)*** feature solves a typical security problem related to Internet applications that require secondary ports to be open in order for a session to operate or need to have binary IP addresses in the payload translated and do not have an Application Level Gateway (ALG)

For example, an FTP control session operates on port 21, but FTP uses port 20 as a secondary port for the data transfer process. The more ports that are open, the greater the security risk. So, the ***Dynamic Port Opening*** service makes it possible to designate certain secondary ports that will only be opened when there is an active session on their associated ***primary port***.

AT-iMG Models use triggers to inform the security mechanism to expect secondary sessions and how to handle them. Rather than allowing a range of port numbers, triggers handle the situation dynamically, allowing the secondary sessions only when appropriate.

The trigger mechanism works without having to understand the application protocol or reading the payload of the packet, (although the payload does need to be read when using NAT if address replacement has to be performed).

4.2.3.1.1 CONFIGURING TRIGGERS

To create a trigger for a TCP or UDP application, enter:

```
security add trigger <name> {tcp|udp} <startport> <endport> <maxactinterval>
```

The <*startport*> and <*endport*> attributes allow you to configure the port range used by the application to open a primary session. Most applications use a single port to open a primary session, in which case you can enter the same port value for both attributes. For example, to create a trigger for Windows Media Player, enter:

```
security add trigger WMP tcp 1755 1755 30000
```

In this command, notice that the <*maxactinterval*> attribute has been set to 30000. This attribute determines the maximum interval time in milliseconds between the use of secondary port sessions. It prevents the security threat posed by ports remaining open unnecessarily for long periods of time. If a secondary port remains inactive for the duration set, the port is automatically closed.

4.2.3.1.2 CONFIGURING SESSION CHAINING

The majority of applications that require triggers only open one additional (secondary) session, however a small number of rare applications (like WS NetMeeting) open a secondary session which in turn opens additional sessions after the primary session has ended. This is called session chaining; multi-level session are triggered from a single trigger. To configure session chaining, use the command:

```
security set trigger <name> sessionchaining {enable|disable}
```

This command enables session chaining for TCP packets only. If you also want to configure session chaining for UDP packets, use the command:

```
security set trigger <name> UDPsessionchaining {enable|disable}
```

Note: TCP session chaining must be always enabled if UDP session chaining is to be used. It's not possible define a UDP session chaining without previously enabling TCP session chaining. Disabling TCP session chaining also automatically disables UDP session chaining.

Note: For the majority of applications, you do not need to enable session chaining and should do so only if you are certain that they are required: because NetMeeting is so commonly used, an apposite command-macro is provided to create a NetMeeting trigger with minimal configuration requirements: **security add trigger <name> netmeeting** *. You do not have to set a port range or maximum activity interval for this trigger; the security module automatically sets this for you.*

4.2.3.1.3 CONFIGURING ADDRESS REPLACEMENT

If your device is configured as a NAT router, you may need to configure triggers for certain protocols to replace the embedded binary IP addresses of incoming packets with the correct inside host IP addresses. This ensures that addresses are translated correctly. To enable/disable binary address replacement, enter:

```
security set trigger <name> binaryaddressreplacement {enable|disable}
```

Once enabled, you can enable address replacement on TCP, UDP or both types of packet:

```
security set trigger <name> addressreplacement {none|tcp|udp|both}
```

4.2.3.1.4 CONFIGURING ADDRESS REPLACEMENT

By default, a trigger can only initiate a secondary session requested by the same host that initiated the primary session. Certain applications, such as SSL, may initiate secondary sessions from different remote hosts. This is called *multihosting*. To enable/disable multihosting, enter:

```
security set trigger <name> multihost {enable|disable}
```

The commands below allow you to determine the range of ports that a secondary session can use. In the majority of cases, you **do not** need to configure the secondary port ranges because triggers will only open specific port numbers for secondary sessions within the range 1024 - 65535.

To configure a secondary port range, enter:

```
security set trigger <name> secondarystartport <portnumber> security
set trigger <name> secondaryendport <portnumber>
```

4.2.3.1.5 APPLICATION LEVEL GATEWAYS (ALGS)

Essentially, triggers and ALGs perform the same function; they deal with difficult applications that your NAT or Firewall configuration cannot manage. However, certain applications prove too difficult for triggers and must be handled by ALGs. The Security module is configured with ALGs for certain well-known applications (see table below).

Security triggers can be configured to deal with some applications, but only when ALGs are not available

An ALG provides a service for a specific application such as FTP (File Transfer Protocol). Incoming packets are checked against existing NAT rules or Firewall filters, IP addresses are evaluated and detailed packet analysis is performed. If necessary, the contents of a packet is modified, and if a secondary port is required, the ALG will open one. The ALG for each application does not require additional configuration.

Application	TCP Port	UDP Port
AOL Instant Messenger (AIM)	5190	N/A
File Transfer Protocol (FTP)	21	N/A
Internet Key Exchange (IKE)	N/A	500
Internet Locator Service (ILS) (a directory service based on Lightweight Directory Access Protocol (LDAP))	389 (+1002)	N/A
Microsoft Networks (MSN)	1863	N/A
Point to Point Tunnelling Protocol (PPTP)	1723	N/A
Resource Reservation Protocol (RSVP (protocol 46))	N/A	N/A
Real Time Streaming Protocol (RTSP)	N/A	N/A
Layer Two Tunnelling Protocol (L2TP)	N/A	1701
Session Initiation Protocol (SIP) (includes Session Description Protocol (SDP))	5060	5060

4.2.4 Intrusion Detection Settings

Intrusion Detection is a feature that looks for traffic patterns that correspond to certain known types of attack from suspicious hosts that attempt to damage the network or to prevent legitimate users from using it.

The ***Intrusion Detection*** protects the system from the following kinds of attacks:

- ***DOS (Denial of Service)*** attacks - a DOS attack is an attempt by an attacker to prevent legitimate hosts from accessing a service.
- ***Port Scanning*** - an attacker scans a system in an attempt to identify any open ports, that are listening for a particular service
- ***Web Spoofing*** - an attacker creates a 'shadow' of the World Wide Web on their own machine, however a legitimate host sees this as the 'real' WWW. The attacker uses the shadow WWW to monitor the host's activities and send false data to and from the host's machine.

Intrusion Detection works differently for each type of attack.

Once an intrusion attempt is detected and the attacker is blocked and blacklisted for a set time limit. The length of time that a blacklisted host remains blocked depends on the kind of attack:

- For **Denial of Service** attacks by the SECURITY SET IDS DOSATTACKBLOCK command and by the SECURITY SET IDS MALICIOUSATTACKBLOCK (default is 30 minutes in both cases)
- For ***Port Scan*** attacks by the SESECURITY SET IDS SCANATTACKBLOCK command.(default is 24 hours)
- For ***Web Spoofing*** attacks by the SECURITY SET IDS VICTIMPROTECTION command (default is 10 minutes.)

4.2.4.1 Port Scan Attacks

Scans are performed by sending a message to each port in turn with certain TCP flag headers set. The response received from each port indicates whether the port is in use and can be probed further in an attempt to violate the network. For example, if a weak port is found, the attacker may attempt to send a DoS attack to that port.

The Security module offers protection from the port scan attacks listed in the table below. Certain port scan attacks are classed as *Trojan Horse* attacks. These are programs that may appear harmless, but once executed they can cause damage to your computer and/or allow remote attackers access to it

The default protection measures are the same for each scan attack:

Scan Attack	Description
Echo scan	The attacker sends scanning traffic to the standard Echo port (TCP port 7).
Xmas Tree scan	The attacker sends TCP packets with FIN, URG and PSH flags set. If a port is closed, the device responds with an RST. If a port is open, the device does not respond.
IMAP scan	The attacker exploits vulnerability of the IMAP port (TCP port 143) once a TCP packet is received from the victim with the SYN and FIN flag set.
TCP SYN ACK scan	The attacker sends a SYN packet and the device responds with a SYN and ACK to indicate that the port is listening, or an RST if it is not listening.
TCP FIN RST scan	The attacker sends a FIN packet to close an open connection. If a port is closed, the device responds with an RST. If a port is open, the device does not respond
NetBus scan	NetBus is a Trojan Horse attack for Windows 95/98/NT. Once installed on the victim's PC, the attacker uses TCP port 12345, 12346 or 20034 to remotely perform illicit activities.

Scan Attack	Description
Back Orifice scan	Back Orifice and Back Orifice 2k are Trojan Horse attacks for Windows 95/98/NT. Once installed on the victim's PC, the attacker commonly listens on UDP ports 31337, 31338 (Back Orifice) and 54320, 54321 (Back Orifice 2k). The attacker can then remotely perform illicit activities.
SubSeven attack	SubSeven and SubSeven 2.1 are Trojan Horse attacks for Windows platforms. Once installed on the victim's PC, the attacker uses TCP ports 1243, 6711, 6712, 6713 (SubSeven) and 27374 (SubSeven 2.1) to remotely perform illicit activities

4.2.4.2 How Port Scanning works - Configuring Port Scanning

The device detects an attempted port scan if it receives more than 5 scanning packets (e.g., SYN/ ACK, FIN or RST packets) per second from a single host. To modify this default threshold:

```
security set IDS scanthreshold <max>
```

The device counts the maximum number of scan packets allowed per second over a 60 second period. To modify this default duration

```
security set IDS scanperiod <duration>
```

If the number of scanning packets counted within the specified duration is greater than the scan threshold set, the suspected attacker is blocked for 86400 seconds (24 hours). To modify this default duration, enter:

```
security set IDS SCANattackblock <duration>
```

Echo scan, Xmas Tree scan, IMAP scan on the contrary are blocked using the MaliciousAttack attribute. Block duration default is set to 30 minutes, to change it:

```
security set IDS MaliciousAttackBlock <duration>
```

4.2.4.3 Denial of Service (DoS) Attacks

There are two main types of DoS attack:

- *Flood attacks* - an attacker tries to overload your device by flooding it with packets. Whilst your device tries to cope with this sudden influx of packets, it causes delays to the transport of legitimate packets or prevents the network from transporting legitimate traffic altogether.
- *Logic* or *software attacks* - a small number of corrupt packets are designed to exploit known software bugs on the target system.

The Security module can detect the early stages of the following DoS attacks:

Dos Attack	Description
SMURF Attack	Attacker sends pings (Echo Requests) to a host with a destination IP address of broadcast (protocol 1, type 8). The broadcast address has a spoofed return address which is the address of the intended victim, and the replies cause the system to crash
SYN/FIN/RST Flood	Attackers send unreachable source addresses in SYN packets, so your device sends SYN/ACK packets to the unreachable address, but does not receive any ACK packets in return. This causes a back-log of half-opened sessions.
ICMP Flood	The attacker floods the network with ICMP packets that are not Echo requests, stealing bandwidth needed for legitimate services. The device detects an attempted ICMP flood if it receives more than 100 ICMP packets per second from a single host
Ping Flood	The attacker floods the network with pings, using bandwidth needed for legitimate services. The device detects an attempted ping flood if it receives more than 15 pings per second from a single host
Ascend Kill	The attacker sends a UDP packet containing special data to port 9 (the discard port), causing your Ascend router to reboot and possi-bly crash continuously
WinNuke Attack	The attacker sends invalid TCP packets which disable networking on many Microsoft Windows 95 and Windows NT machines. Bad data is sent to an established connection with a Windows user. NetBIOS (TCP port 139) is often used
Echo Chargen	A chargen attack exploits character generator (chargen) service (UDP port 19). Sessions that appear to come from the local sys-tem's Echo service are spoofed and pointed at the chargen service to create an endless loop of high volume traffic that will slow your network down
Echo Storm	Attackers send oversized ICMP datagrams to your device using ping in an attempt to crash, freeze or cause a reboot. The device detects an attempted Echo Storm attack if it receives more than 15 ICMP datagrams per second from a single host.
Boink	An attacker sends fragmented TCP packets that are too big to be reassembled on arrival, causing Microsoft Windows 95 and Win-dows NT machines to crash.

Dos Attack	Description
Land Attack	This attack targets Microsoft Windows machines. An attacker sends a forged packet with the same source and destination IP address which confuses the victim's machine, causing it to crash or reboot.
Ping of Death	It is possible to crash, reboot or otherwise kill a large number of systems by sending a ping of a certain size from a remote machine. A ping is defined as a ping of death when the ping payload exceeds 65535 bytes.
Overdrop	This attack uses incorrect IP packet fragmentation to exploit vulnerabilities in networked devices. Fragmented IP packets are sent and the fragment information indicates that the packet length is over 65535 bytes (including IP header), but the actual data in the payload is much less than this amount.

For each DoS attack there are different IDS settings, summarized in the the table below:

Dos Attack	Related Detection settings	Block duration setting / (Default)
SMURF Attack	security enable IDS victimprotection	security set IDS victimprotection <duration> /(10 min)
SYN/FIN/RST Flood	security set IDS floodthreshold <max> security set IDS portfloodthreshold <max> security set IDS floodperiod <duration> security set IDS MaxTCPopenhandshake <max>	security set IDS DOSattackblock <duration> / (30 min)
ICMP Flood	security set IDS MaxICMP <max>	security set IDS DOSattackblock <duration> / (30 min)
Ping Flood	security set IDS MaxPING <max>	security set IDS DOSattackblock <duration> / (30 min)
Ascend Kill	N/A	security set IDS MaliciousAttackBlock <duration> / (30 min
WinNuke Attack	N/A	security set IDS MaliciousAttackBlock <duration> / (30 min

Dos Attack	Related Detection settings	Block duration setting / (Default)
Echo Chargen	N/A	security set IDS DOSattackblock <duration> / (30 min)
Echo Storm	security set IDS MaxPING <max>	security set IDS DOSattackblock <duration> / (30 min)
Boink	N/A	security set IDS DOSattackblock <duration> / (30 min)
Land Attack	N/A	security set IDS DOSattackblock <duration> / (30 min)
Ping of Death	N/A	security set IDS DOSattackblock <duration> / (30 min)
Overdrop	N/A	security set IDS DOSattackblock <duration> / (30 min)

4.2.4.4 IDS Trojan Database

Trojan attacks are detected by scanning for packets on pre-defined Trojan attack ports, using a pre-defined Database includes commonly attacked Trojan Ports.

To enter a new Trojan name in the IDS Trojan Database

```
security IDS add trojan <trojan name>
```

Once you have added a Trojan name to the database, you may need to identify the attack port that might be used by that Trojan. Use the following command to add a port to the IDS Trojan Database against the Trojan name specified in the previous command:

```
security IDS add trojanport <trojan name> <ident> <udp|tcp> <port>
```

In order to start scanning you must enable the Trojan with the following CLI command:

```
security IDS enable trojan <trojan name>
```

4.2.5 Management stations - Remote Management

A management station is a host or range of hosts that can remotely access your device from the public Internet for a certain period of time. Once your device has been configured to allow remote access, the management station sends IP traffic on a specific transport/port to the device's external port. Any NAT or Firewall configuration is bypassed. This allows a network administrator access to the device's configuration without having to visit the site

Note: It is important for ISPs to configure management stations as precisely as possible to reduce the chance of malicious access.

The exact IP address (or range of addresses) for the management station device(s) must be defined in the following command:

```
security add mgmt-station <name> {range <start_addr> <end_addr> |
subnet <address> <mask>} <transport_type> <port> <idle_timeout>
```

Once you have configured a management station and want to enable a remote session to the device's external port, enter:

```
security set mgmt-station <name> enabled
```

4.2.6 Security logging

Note: Security logging is avalaible on FIber D,E Modular and ADSL A,B,C models only

Configuring the security logging module allows you to track:

- *intrusion events;* logs details of attempted DoS, port scanning and web spoofing attacks including the name of the attack, the port number used and the source/destination IP addresses.
- *blocking events*; if an intrusion has been detected, this logs details of the blocked/blacklisted host including their IP address and the length of time they will be blocked/blacklisted for.
- *session events*; logs details of session activity when a session is timed-out when it finishes naturally and is removed from the session list.

Before you can log intrusion, blocking and session events, enable the logging module by entering:

```
security enable logging
```

4.2.7 Security command reference

This section describes the commands available on the AT-iMG Models to enable, configure and manage the ***Security*** module.

4.2.7.1 Command Set

The table below lists the ***security*** commands provided by the CLI.

TABLE 4-2 Security Commands and Product Category

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SECURITY ENABLE | DISABLE	X	X	X	X	X	X	X	X	X
SECURITY ENABLE | DISABLE {LOGGING|blockinglog| intrusionlog| sessionlog}				X	X	X	X	X	X

TABLE 4-2 Security Commands and Product Category (Continued)

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SECURITY ENABLE | DISABLE {blockinglog| intrusionlog| sessionlog} CONSOLEPRINTIng				X	X	X	X	X	X
SECURITY SET BLOCKINGLOG|INTRUSIONLOG|SESSIONLOG LEVEL				X	X	X	X	X	X
SECURITY ADD ALG	X	X	X	X	X	X	X	X	X
SECURITY DELETE ALG	X	X	X	X	X	X	X	X	X
SECURITY LIST ALG	X	X	X	X	X	X	X	X	X
SECURITY LIST LOGGING				X	X	X	X	X	X
SECURITY SHOW ALG	X	X	X	X	X	X	X	X	X
SECURITY STATUS	X	X	X	X	X	X	X	X	X
SECURITY ADD INTERFACE	X	X	X	X	X	X	X	X	X
SECURITY CLEAR INTERFACES	X	X	X	X	X	X	X	X	X
SECURITY DELETE INTERFACE	X	X	X	X	X	X	X	X	X
SECURITY LIST INTERFACES	X	X	X	X	X	X	X	X	X
SECURITY SHOW INTERFACE	X	X	X	X	X	X	X	X	X
SECURITY ADD MGMT-STATION RANGE	X	X	X	X	X	X	X	X	X
SECURITY DELETE MGMT-STATION	X	X	X	X	X	X	X	X	X
SECURITY SET MGMT-STATION	X	X	X	X	X	X	X	X	X
SECURITY LIST MGMT-STATION	X	X	X	X	X	X	X	X	X
SECURITY ADD TRIGGER TCP|UDP	X	X	X	X	X	X	X	X	X
SECURITY ADD TRIGGER NETMEETING	X	X	X	X	X	X	X	X	X
SECURITY CLEAR TRIGGERS	X	X	X	X	X	X	X	X	X
SECURITY DELETE TRIGGER	X	X	X	X	X	X	X	X	X
SECURITY LIST TRIGGERS	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER ADDRESSREPLACEMENT	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER MULTIHOST	X	X	X	X	X	X	X	X	X

TABLE 4-2 Security Commands and Product Category (Continued)

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SECURITY SET TRIGGER BINARYADDRESSREPLACE-MENT	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER MAXACTINTERVAL	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER ENDPORT	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER STARTPORT	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER SECONDARYENDPORT	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER SECONDARYSTARTPORT	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER SESSIONCHAINING	X	X	X	X	X	X	X	X	X
SECURITY SET TRIGGER UDPSESSIONCHAINING	X	X	X	X	X	X	X	X	X
SECURITY SHOW TRIGGER	X	X	X	X	X	X	X	X	X
SECURITY SET SESSIONTIMEOUT	X	X	X	X	X	X	X	X	X
SECURITY ADD WAITINGSESSION	X	X	X	X	X	X	X	X	X
SECURITY DELETE WAITINGSESSION	X	X	X	X	X	X	X	X	X
SECURITY SET WAITINGSESSION	X	X	X	X	X	X	X	X	X
SECURITY SHOW WAITINGSESSION	X	X	X	X	X	X	X	X	X
SECURITY ENABLE|DISABLE IDS	X	X	X	X	X	X	X	X	X
SECURITY ENABLE|DISABLE IDS BLACKLIST	X	X	X	X	X	X	X	X	X
SECURITY CLEAR IDS BLACKLIST	X	X	X	X	X	X	X	X	X
SECURITY ENABLE|DISABLE IDS VICTIMPROTECTION	X	X	X	X	X	X	X	X	X
SECURITY SET IDS VICTIMPROTECTION	X	X	X	X	X	X	X	X	X
SECURITY SET IDS DOSATTACKBLOCK	X	X	X	X	X	X	X	X	X
SECURITY SET IDS MALICIOUSATTACKBLOCK	X	X	X	X	X	X	X	X	X
SECURITY SET IDS MAXICMP	X	X	X	X	X	X	X	X	X
SECURITY SET IDS MaxPING	X	X	X	X	X	X	X	X	X
SECURITY SET IDS MAXTCPOPENHANDSHAKE	X	X	X	X	X	X	X	X	X
SECURITY SET IDS SCANATTACKBLOCK	X	X	X	X	X	X	X	X	X

TABLE 4-2 Security Commands and Product Category (Continued)

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SECURITY SET IDS FLOODPERIOD	X	X	X	X	X	X	X	X	X
SECURITY SET IDS FLOODTHRESHOLD	X	X	X	X	X	X	X	X	X
SECURITY SET IDS PORTFLOODTHRESHOLD	X	X	X	X	X	X	X	X	X
SECURITY SET IDS SCANPERIOD	X	X	X	X	X	X	X	X	X
SECURITY SET IDS SCANTHRESHOLD	X	X	X	X	X	X	X	X	X
SECURITY SET AEMLOGGINGINTERVAL				X	X		X	X	X
SECURITY SHOW IDS	X	X	X	X	X	X	X	X	X

4.2.7.1.1 SECURITY ENABLE | DISABLE

Syntax `security {enable | disable}`

Description This command explicitly enables/disables all modules in the ***Security*** package (including the child modules; NAT and Firewall). You must enable the ***Security*** package if you want to use the ***NAT*** and/or ***Firewall*** modules to configure security for your system.

If you disable the ***Security*** package during a session, any configuration changes made to the ***Security, NAT*** or ***Firewall*** modules when the package was enabled remain in the system, so that you can re-enable them later in the session. If you need to reboot your system but want to save the security configuration between sessions, use the SYSTEM CONFIG CREATE and SYETM CONFIG SET command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	Enables all modules in the ***Security*** package (***Security, NAT and Firewall*** modules).	Disabled
disabled	Disables all modules in the ***Security*** package (***Security, NAT and Firewall*** modules).	

Example --> security enable

See also `firewall ENABLE logging`

4.2.7.1.2 SECURITY ENABLE | DISABLE {LOGGING|BLOCKINGLOG| INTRUSIONLOG| SESSIONLOG}

Syntax `security {enable | disable} {logging|blockinglog|intrusionlog|sessionlog}`

Description This command enables/disables logging of:

- logging activit
- blocking activity
- intrusion activity
- session events

This command is not present on FIBER A,B,C devices

Note: Before you can log intrusion, blocking and session events, logging module must be enabled

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	Logging is enabled.	N/A
disabled	Logging is disabled.	
logging	generic logging module reference	Enabled
blockinglog	Details of blocking activity are logged.	Enabled
intrusionlog	Details of intrusion activity are logged.	Disabled
sessionlog	Details of session events are logged.	Disabled

Example --> security enable blockinglog

See also `firewall set securitylevel`

4.2.7.1.3 SECURITY ENABLE | DISABLE {BLOCKINGLOG| INTRUSIONLOG| SESSIONLOG} CONSOLEPRINTING

Syntax `security {enable | disable} {blockinglog|intrusionlog|sessionlog} CONSOLEPRINTING`

Description This command allows you to set whether blocking, intrusion or session logging is sent to the console instead of to the event log. Note that you must first enable logging using the command security enable|disable logging|blockinglog|intrusionlog|sessionlog. This command is not present of FIBER A,B,C devices

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enabled	The specified logging activity is displayed at the console.	Disable
disabled	The specified logging activity is sent to the event log.	
blockinglog	Specifies where blocking activity is displayed.	N/A
intrusionlog	Specifies where intrusion activity is displayed..	
sessionlog	Specifies where session activity is displayed.	
consoleprinting	Enabling consoleprinting sends logging to the console instead of to the event log. Disabling consoleprinting sends logging to the event log instead of to the console.	N/A

Example --> security enable blockinglog consoleprinting

4.2.7.1.4 SECURITY SET BLOCKINGLOG|INTRUSIONLOG|SESSIONLOG LEVEL

Syntax `security set {blockinglog | intrusionlog | sessionlog} <level>`

DescriptionFor each logging event it's possible set the minimum level of logging that is reported. The levels available in this command correspond to syslog levels (emergency, alert, critical, error, warning, notice, informational, debug).

The default reporting level for an enabled log activity is notice, which will report emergency, alert, critical, error, warning and notice messages but not the informational or debug messages.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
blockinglog	Configures blocking logging.	N/A
intrusionlog	Configures intrusion logging.	N/A
sessionlog	Configures session event logging.	N/A

Option	Description	Default Value
level	The level of logging reported at the event log or the console. You can choose from the following levels: emergency, alert, critical, error, warning, notice, informational, debug. These levels directly correspond to syslog levels.	Notice

Example --> security set blockinglog warning

See also `firewall set securitylevel`

4.2.7.1.5 SECURITY ADD ALG

Syntax `security add alg <algname> <algtype> [transport] [port]`

SECURITY ADD ALG <ALGNAME> <ALGTYPE> [PROT <PROTNO>]

Description This command enables a specific ALG

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
algname	A unique identifier specified by the user.	N/A
algtype	Application/Protocol ALG to be enabled. Example – sip or rtsp.	N/A
transport	Transport protocol. Example – tcp, udp. If no transport is specified, the default configured transport for the algtype will be used.	N/A
port	If the transport is neither tcp nor udp, this field is to be used to specify the transport. The actual protocol number used by ALG is to be specified.	N/A
protno	Port used by ALG. If transport is neither tcp nor udp, the port shall be 0. If no port is specified, the default configured port for the algtype will be used.	N/A

Example --> security add alg algsip sip udp 5060

--> security add alg algrsvp rsvp prot 46

See also `firewall set securitylevel`

4.2.7.1.6 SECURITY DELETE ALG

Syntax `security delete alg <algname>`

DescriptionThis command disables a specific ALG.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
algname	Unique identifier specified to delete the ALG.	N/A

Example --> security delete alg alg_sipudp

4.2.7.1.7 SECURITY LIST ALG

Syntax `security LIST alg`

DescriptionThis command will display information of all the configured ALGs in tabular format.

Example --> security list alg

```
ID | AlgType | Transport | Port |
-----------------------------------------
1  | ftp | 6 | 21
2  | ils | 6 | 389
3  | ils | 6 | 1002
4  | ike | 17 | 500
5  | aim | 6 | 5190
6  | msnmsgr | 6 | 1863
7  | pptp | 6 | 1723
8  | rsvp | 46 | 0
9  | l2tp | 17 | 1701
10 | rtsp | 6 | 554
11 |  sip | 17 |  5060
-----------------------------------------
```

4.2.7.1.8 SECURITY LIST LOGGING

Syntax `security LIST logging`

DescriptionThis command will display information of all the configured logging in tabular format. This command is not present on FIBER A,B,C devices

Example --> security list logging

```
The logging module is: true
```

```
Session event logging is: false
Blocking event logging is: false
Intrusion event logging is: false
```

4.2.7.1.9 SECURITY SHOW ALG

Syntax `security SHOW alg <algname>`

Description **Description**This command will display the following information about a specific ALG.

- AlgType - Application/Protocol ALG to be enabled. Example – sip.
- Transport - Transport protocol. Example – tcp, udp. If no transport is specified, the default configured transport for the algtype will be used.
- Port - If the transport is neither tcp nor udp, this field is to be used to specify the transport. The actual protocol number used by ALG is to be specified.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
algname	Unique identifier specified to delete the ALG.	N/A

Example --> security show alg alg_sipudp

```
Alg Type : sip
Transport: 17
Port :     5060
```

4.2.7.1.10 SECURITY STATUS

Syntax `security status`

Description This command displays the following information about the ***Security*** package:

- Security status (enabled or disabled)
- Firewall status (enabled or disabled)
- Firewall security level setting (none, high, low, or medium)
- Firewall session logging (enabled or disabled)
- Firewall blocking logging (enabled or disabled)
- Firewall intrusion logging (enabled or disabled)
- NAT status (enabled or disabled)

Example --> security status

```
Security enabled.
Firewall disabled.
Firewall security level: none.
NAT disabled.
Intrusion detection is disabled.
Security logging is enabled.
  Session logging disabled.
  Blocking logginisabled.
  Intrusion logging disabled.
Security AEM Logging Interval: 5 Sec(s).
```

See also SECURITY ENABLE | DISABLE
FIREWALL SET SECURITYLEVEL

4.2.7.1.11 SECURITY ADD INTERFACE

Syntax SECURITY ADD INTERFACE <name> {EXTERNAL | INTERNAL | DMZ}

Description This command adds an existing IP interface to the ***Security*** package to create a security interface, and specifies what type of interface it is depending on how it connects to the network.

Once you have added security interfaces, you can use them in the ***NAT*** and/or ***Firewall*** configurations.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing IP interface. To display interface names, use the ip list interfaces command.	N/A
external	An interface that connects to the external network.	N/A
internal	An interface that connects to the internal network	N/A
dmz	An interface that connects to the de-militarized zone, DMZ	N/A

Example --> security add interface ip1 internal

See also IP LIST INTERFACES

See also Firewall command reference
NAT CLI commands

4.2.7.1.12 SECURITY CLEAR INTERFACES

Syntax `security clear interfaces`

Description This command removes all security interfaces that were added to the ***Security*** package using the security add interface command.

Example --> security clear interfaces

See also `SECURITY DELETE INTERFACE`

4.2.7.1.13 SECURITY DELETE INTERFACE

Syntax `SECURITY DELETE INTERFACE <name>`

Description This command removes a single security interface that was added to the Security package using the security add interface command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing security interface. To display interface names, use the SECURITY LIST INTERFACES command.	N/A

Example --> security delete interface f1

See also `SECURITY CLEAR INTERFACES`
`SECURITY LIST INTERFACES`

4.2.7.1.14 SECURITY LIST INTERFACES

Syntax `security list interfaces`

Description This command lists the following information about security interfaces that were added to the ***Security*** package using the security add interface command:

- Interface ID number
- Interface name
- Interface type (external, internal or DMZ)

Example --> security list interfaces

```
Security Interfaces:
 ID  |   Name    | Type
-----|-----------|----------
   1 | i1        | internal
```

```
   2 | i2       | external
   3 | i3       | dmz
  --------------------------
```

See also SECURITY SHOW INTERFACE

4.2.7.1.15 SECURITY SHOW INTERFACE

Syntax SECURITY SHOW INTERFACE <name>

Description This command displays information about a single interface that was added to the Security package using the security add interface command. The following interface information is displayed:

- Interface name
- Interface type (external, internal or DMZ)

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing security interface. To display all interface names, use the security list interfaces command.	N/A

Example --> security show interface f2

```
Interface name: f2
Interface type: internal
```

See also SECURITY LIST INTERFACES

4.2.7.1.16 SECURITY ADD MGMT-STATION RANGE

Syntax SECURITY ADD MGMT-STATION <name> {RANGE <start_addr> <end_addr> | SUBNET <address> <mask> } <transport_type> <port> <idle_timeout>

Description This command creates a ***Management Station*** that allows a specific host (or range of hosts) to access your device directly, bypassing ***NAT*** and ***Firewall***. IP packets from a ***Management Station*** are sent to the external interface (WAN) using a specific transport and port number. The ***Management Station*** is not enabled until you enable it using SECURITY SET MGMT-STATION.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the management station. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
start_addr	The first remote host IP address in the range allowed.	N/A
end_addr	The last remote host IP address in the range allowed.	N/A
address	A specific IP address in the remote subnet allowed.	N/A
mask	The mask defining the remote subnet allowed.	N/A
transport_type	The number of the transport type used, e.g., TCP = 6, UDP = 17, wildcard = 255.	N/A
port	The port number used. This is only effective if the transport_type is set to 6 (TCP) or 17 (UDP). The wildcard is 65535.	N/A
idle_timeout	The idle time (in minutes). If no sessions are created by the ***Management Station*** within this setting the ***Station*** is disabled. If a session is created, that session uses the idle time set and the Station is not disabled until the session expires.	0 (no timeout)

Example --> security add mgmt-station ISP 192.168.1.1 255.255.255.0 17 26 10

See also `security set mgmt-station`

4.2.7.1.17 SECURITY DELETE MGMT-STATION

Syntax `SECURITY DELETE MGMT-STATION <name>`

Description This command deletes a single ***Management Station*** that was added to the ***Security*** module using the SECURITY ADD MGMT-STATION command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing Management Station. To display Management Station names, use the SECURITY LIST MGMT-STATION command.	N/A

Example --> security delete mgmt-station ISP

See also `SECURITY ADD MGMT-STATION`
`SECURITY LIST MGMT-STATION`

4.2.7.1.18 SECURITY SET MGMT-STATION

Syntax `SECURITY SET MGMT-STATION <name> {ENABLED|DISABLED}`

Description This command enables a ***Management Station*** that was added to the ***Security*** module using the SECURITY ADD MGMT-STATION command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing Management Station. To display Management Station names, use the SECURITY LIST MGMT-STATION command.	N/A
enabled	Enables the Management Station. Once enabled, Management Station sessions can be created.	Disabled
disabled	Disables the Management Station.	

Example --> set mgmt-station ISP enabled

See also `SECURITY ADD MGMT-STATION`
`SECURITY LIST MGMT-STATION`

4.2.7.1.19 SECURITY LIST MGMT-STATION

Syntax `security list mgmt-stations`

Description This command lists Management Stations that were added to the Security module using the security add mgmt-station command. It displays the following information about Management Stations:

- Management station id number
- Management station name
- Subnet status (true/false)
- IP address (of subnet or first address in range)
- Subnet mask or last address of range
- Transport number
- Port number
- Idle timeout (minutes)
- Enabled status (true/false)

Example --> security list mgmt-stations

```
Management Stations:

  ID |    Name    | Subnet |    IP address    | Mask/End Address |  Interface  | Transp
| Port  | Idle   | Enable
-------------------------------------------------------------------------------------
-----------------------------
   1 | new        | false  | 192.168.1.4      | 192.168.1.10     | ip1        | 17     |
26    | 10     | false
 -------------------------------------------------------------------------------------
-----------------------------
```

See also `security add mgmt-station`

4.2.7.1.20 SECURITY ADD TRIGGER TCP|UDP

Syntax `SECURITY ADD TRIGGER <name> {TCP|UDP} <startport> <endport> <maxactinterval>`

Description This command adds a trigger to the ***Security*** module. A trigger allows an application to open a secondary port in order to transport packets.

Some applications, such as FTP, need to open secondary ports - they have a control session port (21 for FTP) but also need to use a second port in order to transport data. Adding a trigger it means that you do not have to define static portfilters to open ports for each secondary session. If you did this, the ports would remain open for potential use (or misuse, see the command FIREWALL SET IDS SCANATTACKBLOCK) until the portfilters were deleted. A trigger opens a secondary port dynamically, and allows you to specify the length of time that it can remain inactive before it is closed.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the trigger. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
tcp	Adds a trigger for a TCP application to the security package.	N/A
udp	Adds a trigger for a UDP application to the security package.	N/A
startport	Sets the start of the trigger port range for the control session.	N/A
endport	Sets the end of the trigger port range for the control session.	N/A
maxactinterval	Sets the maximum interval time (in milliseconds) between the use of secondary port sessions. If a secondary port opened by a trigger has not been used for the specified time, it is closed.	3000

Example The following example creates a Netmeeting (H323) trigger:

--> security add trigger t1 tcp 1720 1720 30000

See also `SECURITY LIST TRIGGERS`
`SECURITY ADD TRIGGER NETMEETING`

4.2.7.1.21 SECURITY ADD TRIGGER NETMEETING

Syntax `SECURITY ADD TRIGGER <name> NETMEETING`

Description This command allows you to use the example trigger provided by the CLI. It allows you to add a trigger to allow ***Netmeeting*** to transport data through the ***Security*** package. This application opens a secondary port session. You do not have to set the port range or ***maxactinterval*** for a ***Netmeeting*** trigger - the CLI automatically sets this for you.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the trigger. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A

Example --> security add trigger t2 netmeeting

See also `SECURITY LIST TRIGGERS`
`SECURITY ADD TRIGGER TCP|UDP`

4.2.7.1.22 SECURITY CLEAR TRIGGERS

Syntax `security clear triggers`

Description This command deletes all triggers that were added to the ***Security*** module using the security add trigger commands.

Example --> security clear triggers

See also `security delete trigger`

4.2.7.1.23 SECURITY DELETE TRIGGER

Syntax `SECURITY DELETE TRIGGER <name>`

Description This command deletes a single trigger that was added to the ***Security*** module using the security add trigger commands.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list trigger command.	N/A

Example --> security delete trigger t2

See also `SECURITY LIST TRIGGERS`
`SECURITY CLEAR TRIGGERS`

4.2.7.1.24 SECURITY LIST TRIGGERS

Syntax `security list triggers`

Description This command lists triggers that were added to the ***Security*** module using the security add trigger command. It displays the following information about triggers:

- Trigger ID number
- Trigger name
- Trigger transport type (TCP or UDP)
- Port range
- Secondary port range
- Interval

Example --> security list triggers

```
Security Triggers:
ID| Name | Type| Port Range | Sec Port Range |Interval
--|------|-----|------------|----------------|--------
 1|  tr1 | tcp | 21   - 21  | 1720 - 1720    |3000
-----------------------------------------------------
```

See also SECURITY SHOW TRIGGER

4.2.7.1.25 SECURITY SET TRIGGER ADDRESSREPLACEMENT

Syntax SECURITY SET TRIGGER <name> ADDRESSREPLACEMENT {NONE|TCP|UDP|BOTH}

Description The settings in this command are only effective if you enable address translation using the command SECURITY SET TRIGGER BINARYADDRESSREPLACEMENT.

This command allows you to specify what type of address replacement is set on a trigger. Incoming packets are searched in order to find their embedded IP address. The address is then replaced by the correct inside host IP address, and ***NAT*** translates the packets to the correct destination.

You can specify whether you want to carry out address replacement on TCP packets, on UDP packets or on both TCP and UDP packets.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	A name that identifies a trigger. To display trigger names, use the security list triggers command.	N/A
none	Disables address replacement.	None

Option	Description	Default Value
tcp	Sets address replacement on TCP packets for an existing trigger.	
udp	Sets address replacement on UDP packets for an existing trigger.	
both	Sets address replacement on TCP and UDP packets for an existing trigger.	

Example --> security set trigger t2 addressreplacement tcp

See also SECURITY SET TRIGGER BINARYADDRESSREPLACEMENT

4.2.7.1.26 SECURITY SET TRIGGER MULTIHOST

Syntax SECURITY SET TRIGGER <name> MULTIHOST {ENABLE | DISABLE}

Description This command sets whether a secondary session can be initiated to/from different remote hosts or the same remote host on an existing trigger.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
enable	A secondary session can be initiated to/from different remote hosts.	Disable
disable	A secondary session can only be initiated to/from the same remote host.	

Example --> security set trigger t1 multihost enable

See also SECURITY LIST TRIGGERS

4.2.7.1.27 SECURITY SET TRIGGER BINARYADDRESSREPLACEMENT

Syntax SECURITY SET TRIGGER <name> BINARYADDRESSREPLACEMENT {ENABLE | DISABLE}

Description This command enables/disables binary address replacement on an existing trigger. You can then set the type of address replacement (TCP, UDP, both or none) using the command SECURITY SET TRIGGER ADDRESSREPLACEMENT.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
enable	Enables the use of binary address replacement on an existing trigger.	Disable
disable	Disables the use of binary address replacement on an existing trigger.	

Example --> security set trigger t5 binaryaddressreplacement enable

See also `SECURITY SET TRIGGER ADDRESSREPLACEMENT`
`SECURITY LIST TRIGGERS`

4.2.7.1.28 SECURITY SET TRIGGER MAXACTINTERVAL

Syntax `SECURITY SET TRIGGER <name> MAXACTINTERVAL <interval>`

Description This command sets the maximum activity interval limit on existing session entries for an existing trigger.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
interval	Sets the maximum interval time (in milliseconds) between the use of secondary port sessions. If a secondary port opened by a trigger has not been used for the specified time, it is closed.	N/A

Example --> security set trigger t2 maxactinterval 5000

See also `SECURITY LIST TRIGGERS`

4.2.7.1.29 SECURITY SET TRIGGER ENDPORT

Syntax `SECURITY SET TRIGGER <name> ENDPORT <portnumber>`

Description This command sets the end of the port number range for an existing trigger.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
portnumber	Sets the end of the trigger port range.	N/A

Example --> security set trigger t3 endport 21

See also `security set trigger startport`

4.2.7.1.30 SECURITY SET TRIGGER STARTPORT

Syntax `SECURITY POLICY <name> SET TRIGGER STARTPORT <portnumber>`

Description This command sets the start of the port number range for an existing trigger.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
port	Sets the start of the trigger port range.	N/A

Example --> security set trigger t3 startport 21

See also `security set trigger endport`

4.2.7.1.31 SECURITY SET TRIGGER SECONDARYENDPORT

Syntax `SECURITY SET TRIGGER <name> SECONDARYENDPORT <portnumber>`

Description This command sets the end of the secondary port number range for an existing trigger. It allows you to restrict the ports that a trigger will open, however, this is not usually necessary.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A

Option	Description	Default Value
portnumber	Sets the end of the trigger's secondary port range.	65535

Example --> security set trigger t3 secondaryendport 1933

See also SECURITY SET TRIGGER SECONDARYSTARTPORT

4.2.7.1.32 SECURITY SET TRIGGER SECONDARYSTARTPORT

Syntax SECURITY POLICY <name> SET TRIGGER SECONDARYSTARTPORT <portnumber>

Description This command sets the start of the secondary port number range for an existing trigger. It allows you to restrict the ports that a trigger will open, however, this is not usually necessary.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
port	Sets the start of the trigger's secondary port range.	1024

Example --> security set trigger t3 secondarystartport 1923

See also SECURITY SET TRIGGER SECONDARYENDPORT

4.2.7.1.33 SECURITY SET TRIGGER SESSIONCHAINING

Syntax SECURITY SET TRIGGER <name> SESSIONCHAINING {ENABLE | DISABLE}

Description This command determines whether a triggering protocol can be chained. If session chaining is enabled, TCP dynamic sessions also become triggering sessions, which allows multilevel session triggering.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
enable	Enables TCP session chaining on an existing trigger.	Disable

Option	Description	Default Value
disable	Disables all session chaining (TCP and UDP) on an existing trigger.	

Example --> security set trigger t4 sessionnchaining enable

See also `security set trigger UDPsessionchaining`

4.2.7.1.34 SECURITY SET TRIGGER UDPSESSIONCHAINING

Syntax `SECURITY SET TRIGGER <name> UDPSESSIONCHAINING {ENABLE | DISABLE}`

Description You must set the SECURITY SET TRIGGER SESSIONCHAINING ENABLE command in order for this command to become effective.

If UDP session chaining is enabled, both UDP and TCP dynamic sessions also become triggering sessions, which allows multi-level session triggering.

*Note: This CLI command is case-sensitive. You must type the command attributes exactly as they appear in the **Example section**. If you do not use the same case-sensitive syntax, the command fails and the CLI displays a syntax error message.*

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A
enable	Enables UDP sessionchaining on an existing trigger. TCP and UDP session chaining is allowed if the security set trigger sessionchaining command is enabled.	Disable
disable	Disables UDP session chaining on an existing trigger. TCP session chaining is allowed if the security set trigger sessionchaining command is enabled.	

Example --> security set trigger t3 UDPsessionchaining enable

See also `SECURITY SET TRIGGER SESSIONCHAINING`

4.2.7.1.35 SECURITY SHOW TRIGGER

Syntax `SECURITY SHOW TRIGGER <name>`

Description This command displays information about a single trigger that was added to the ***Security*** module using the security add trigger command. The following trigger information is displayed:

- Trigger name
- Transport type (TCP or UDP)
- Start of the port range
- End of the port range
- Multiple host permission (true/false)
- Maximum activity interval (in milliseconds)
- Session chaining permission (true/false)
- Session chaining on UDP permission (true/false)
- Binary address replacement permission (true/false)
- Address translation type (UDP, TCP, none or both)

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing trigger. To display trigger names, use the security list triggers command.	N/A

Example --> security show trigger t2

```
Security Trigger: t2
                    Transport Type: tcp
                Starting port number: 1000
                  Ending port number: 1000
                Allow multiple hosts: false
               Max activity interval: 30000
                    Session chaining: false
             Session chaining on UDP: false
          Binary address replacement: false
            Address translation type: none
```

See also SECURITY LIST TRIGGERS

4.2.7.1.36 SECURITY SET SESSIONTIMEOUT

Syntax `security set session tiemout {esp | icmp | other | tcpclose | tcpestb | tcpinit | udp} <duration>`

Description This command enables user to configure a time out period after which any session may timeout.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	Time period configured by user for session time out..	N/A

Example --> security set session timeout icmp 20

4.2.7.1.37 SECURITY ADD WAITINGSESSION

Syntax `SECURITY ADD WAITINGSESSION <name> <interface> <local_real_ip> <tranport_type> <local_mapping_port> <local_real_port> [<idle_timeout> {enabled | disabled} COMMENT <comment> REMOTEIP <remoteip>]`

Description This command adds a waitingsession to the security module. Waiting sessions are a sort of "presessions" which are created so that the security modules know about the expected traffic.

A waiting session must at least have specific local and mapping IP addresses defined. The other parameters (IP addresses, protocol, port numbers) may be specified as wildcards. However, the more parameters specified, the more secure the waiting session.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	Name of the waitingsession	N/A
interface	Specify the external/dmz interface over which traffic is expected	N/A
local_real_ip	Specify the IP address of the local host which is expecting this traffic	N/A
transport_type	Specify the transport type for the traffic eg. TCP/ UDP	N/A

Option	Description	Default Value
local_mapping_port	Specify the TCP/UDP port on local host which this traffic is to be re-directed to	N/A
local_real_port	Specify the TCP/UDP port on which the traffic reaches the router	N/A
idle_timeout	Optionally specify the time-out after which not to expect this traffic	N/A
enabled	Specify whether the waiting-session should be enabled	N/A
disabled	Specify whether the waiting-session should be disabled	N/A
comment	Optionally provide a comment for this traffic	N/A
remoteip	Optionally specify the IP address of the remote host from which the traffic is expected	N/A

Example --> security add waitingsession yahoo-video wan 192.168.0.1 17 500 5000 60 enabled comment yahoouser wants video remoteip 172.26.4.1

4.2.7.1.38 SECURITY DELETE WAITINGSESSION

Syntax `SECURITY DELETE WAITINGSESSION <name>`

Description This command deletes the waitingsession added to a security module.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	Name of the waitingsession	N/A

Example --> security delete waitingsession yahoo-video

4.2.7.1.39 SECURITY SET WAITINGSESSION

Syntax `SECURITY SET WAITINGSESSION <name> <local_real_port> <duration> (ENABLED |DISAB`

Description This command sets various attributes of the waitingsession.

'local_real_port and duration' attributes of the waitingsession cannot be set once a waitingsession has been created and enabled. To set these the waitingsession must be disabled.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	Name of the waitingsession	N/A
local_real_port	Specify the TCP/UDP port on which the traffic reaches the router	N/A
duration	Optionally specify the duration after which not to expect this traffic	N/A
Enabled	Specify whether the waiting-session should be enabled	N/A
Disabled	Specify whether the waiting-session should be disabled	N/A

Example --> security set waitingsession yahoo-video loacalrealport 4000

4.2.7.1.40 SECURITY LIST WAITINGSESSIONS

Syntax `security LIST waitingsessionS`

Description This command lists Waiting Sessions that were added to the Security module using the security add waitingsession command. It displays the following information about Waiting Sessions:

- Waiting Session Name
- Interface Name
- Local Real IP (IP-Address)
- Local Remote IP (IP-Address)
- Transport Number (prot)
- Local Real Port
- Local Map Port
- enabled status (true/false)

Example security list waitingsessions

```
Waiting Sessions:
  Local    | Local                                        | Real  | Map   |
  Name     | Interface |  Local Real IP | Remote IP | Prot | Port  | Port  | Enable
```

```
-------------------------------------------------------------------------------
 yahoo-vi.. | ip0       | 192.168.1.1   | 0.0.0.0   | 17   | 5000  | 500   | true
-------------------------------------------------------------------------------
```

4.2.7.1.41 SECURITY SHOW WAITINGSESSION

Syntax `SECURITY SHOW WAITINGSESSION <name`

Description This command displays information about a single waitingsession that was added to the Security module using the security add waitingsession command. The following informations are displayed:

- Waiting Session Name: Waiting Session Name.
- Interface Name: Specify the external/dmz interface over which traffic is expected.
- Local Real IP Address: Specify the IP address of the local host which is expecting this traffic.
- Remote IP Address: Optionally specify the IP address of the remote host from which the traffic is expected.
- Protocol: The Protocol type- TCP/ UDP.
- Local Real Port: Specify the TCP/UDP port on which the traffic reaches the router.
- Local Mapping Port: Specify the TCP/UDP port on local host which this traffic is to be redirected to.
- Remote Port: The remote port from which this traffic is expected, or wildcard.
- Duration: Optionally specify the duration after which not to expect this traffic.
- Reusable: Specify whether the waiting-session should be enabled.
- Enabled: Specify whether the waiting-session should be disabled.
- Description: Comment provided to describe this particular traffic, if any.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	Name of the waitingsession	N/A

Example --> security show waitingsession yahoo-video

```
Waiting Session Name: yahoo-video
Interface Name: wan
Local Real IP Address: 192.168.0.1
Remote IP Address: 0.0.0.0
```

```
Protocol: 17
Local Real Port: 4000
Local Mapping Port: 500
Remote Port: 65535
Duration: 300
Reusable: true
Enabled: true
Description: whatisit
```

4.2.7.1.42 SECURITY ENABLE|DISABLE IDS

Syntax `SECURITY {enable | disable} IDS`

Description This command explicitly enables/disables IDS (Intrusion Detection Service). You must enable IDS if you want to activate the settings specified in the security IDS commands.

If you disable IDS during a session, any configuration changes made when IDS was enabled are not deleted - you can re-enable them later in the session.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enable	Enables the IDS portion of the Security module.	Disable
disable	Disables the IDS portion of the Security module.	

Example --> security enable IDS

See also `SECURITY enable|disable`

4.2.7.1.43 SECURITY ENABLE|DISABLE IDS BLACKLIST

Syntax `security enable|disable IDS blacklist`

Description This command enables support for the IDS blacklist (Intrusion Detection Setting). Blacklisting denies an external host access to the system if IDS has detected an intrusion from that host. Access to the network is denied for ten minutes.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enable	Enables blacklisting of an external host if IDS has detected an intrusion from that host..	Disable

Option	Description	Default Value
disable	Disables blacklisting of an external host if IDS has detected an intrusion from that host.	

Example --> security enable IDS blacklist

4.2.7.1.44 SECURITY CLEAR IDS BLACKLIST

Syntax `SECURITY CLEAR IDS BLACKLIST`

Description This command clears blacklisting of an external host. Blacklisting denies an external host access to the system if IDS has detected an intrusion from that host. Access to the network is denied for ten minutes, unless this command is used before this duration expires.

Example --> security clear IDS blacklist

4.2.7.1.45 SECURITY ENABLE|DISABLE IDS VICTIMPROTECTION

Syntax `security enable|disable IDS victimprotection`

Description This command enables/disables the victim protection Intrusion Detection Setting (IDS). This protects your system against broadcast pings. An attacker sends out a ping with a broadcast destination address and a spoofed source address. Packets destined for the victim of a spoofing attack are blocked for a specified duration (600 minutes by default).

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enable	Enables victim protection and blocks packets destined for the victim host.	Disable
disable	Disables victim protection.	

Example --> security enable IDS victimprotection

4.2.7.1.46 SECURITY SET IDS VICTIMPROTECTION

Syntax `security set IDS victimprotection <duration>`

Description This command sets the duration of the victim protection Intrusion Detection Setting (IDS). If victim protection is enabled, packets destined for the victim host of a spoofing

style attack are blocked. The command allows you to specify the duration of the block time limit.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that packets destined for the victim of a spoofing style attack. are blocked for.	600 (10 minutes)

Example --> security set IDS victimprotection 800

4.2.7.1.47 SECURITY SET IDS DOSATTACKBLOCK

Syntax `SECURITY SET IDS DOSATTACKBLOCK <DURATION>`

Description This command sets the DOS (Denial of Service) attack block duration Intrusion Detection Setting (IDS). A DOS attack is an attempt by an attacker to prevent legitimate users from using a service. If a DOS attack is detected, all suspicious hosts are blocked for a set time limit. This command allows you to specify the duration of the block time limit.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that suspicious hosts are blocked for once a DOS attack attempt has been detected.	1800 (30 minutes)

Example --> security set IDS DOSattackblock 800

4.2.7.1.48 SECURITY SET IDS MALICIOUSATTACKBLOCK

Syntax `SECURITY SET IDS MALICIOUSATTACKBLOCK <duration>`

Description This command sets the malicious attack block duration Intrusion Detection Setting (IDS). A malicious attack happens when a bad packet is sent which causes the networking on certain systems to crash. For eg. In WinNuke attack, the attacker sends TCP packets on port NetBIOS (135) with URG bit set, which causes networking to be disabled on Win 95/NT machines. If a malicious attack is detected, all suspicious source IPs are blocked for a set time limit. This command allows you to specify the duration of the block time limit.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that suspicious hosts are blocked for once a malicious attack attempt has been detected.	1800 (30 minutes)

Example --> security set IDS MaliciousAttackBlock 3600

4.2.7.1.49 SECURITY SET IDS MAXICMP

Syntax `SECURITY SET IDS MAXICMP <MAX>`

Description This command sets the maximum number of ICMP packets per second that are allowed before an ICMP Flood is detected. An ICMP Flood is a DOS (Denial of Service) attack. An attacker tries to flood the network with ICMP packets in order to prevent transportation of legitimate network traffic. Once the maximum number of ICMP packets per second is reached, an attempted ICMP Flood is detected.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	The maximum number (per second) of ICMP packets that are allowed before an ICMP Flood attempt is detected.	100

Example --> security set IDS MaxICMP 200

4.2.7.1.50 SECURITY SET IDS MAXPING

Syntax `SECURITY SET IDS MAXPING <MAX>`

Description This command sets the maximum number of pings per second that are allowed before an Echo Storm is detected. Echo Storm is a DOS (Denial of Service) attack. An attacker sends oversized ICMP datagrams to the system using the 'ping' command. This can cause the system to crash, freeze or reboot, resulting in denial of service to legitimate users. Once the maximum number of pings per second is reached, an attempted DOS attack is detected.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	The maximum number (per second) of pings that are allowed before an Echo Storm attempt is detected.	15

Example --> security set IDS MaxPING 25

4.2.7.1.51 SECURITY SET IDS MAXTCPOPENHANDSHAKE

Syntax `SECURITY SET IDS MAXTCPOPENHANDSHAKE <MAX>`

Description This command sets the maximum number of unfinished TCP handshaking sessions per second that are allowed before a SYN Flood is detected. SYN Flood is a DOS (Denial of Service) attack. When establishing normal TCP connections, three packets are exchanged:

- 1 A SYN (synchronize) packet is sent from the host to the network server
- 2 A SYN/ACK packet is sent from the network server to the host
- 3 An ACK (acknowledge) packet is sent from the host to the network server

If the host sends unreachable source addresses in the SYN packet, the server sends the SYN/ACK packets to the unreachable addresses and keeps resending them. This creates a backlog queue of unacknowledged SYN/ACK packets. Once the queue is full, the system will ignore all incoming SYN requests and no legitimate TCP connections can be established.

Once the maximum number of unfinished TCP handshaking sessions is reached, an attempted DOS attack is detected. The suspected attacker is blocked for the time limit specified in the security set IDS DOSattackblock command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	The maximum number (per second) of unfinished TCP handshaking sessions that are allowed before a SYN Flood attempt is detected..	100

Example --> security set IDS MaxTCPopenhandshake 150

4.2.7.1.52 SECURITY SET IDS SCANATTACKBLOCK

Syntax SECURITY SET IDS SCANATTACKBLOCK <DURATION>

Description This command allows you to set the scan attack block duration Intrusion Detection Setting (IDS). If hosts are blocked for a set time limit, this command allows you to specify the duration of the block time limit.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that a suspicious host is blocked for, after scan activity has been detected.	86400 (one day)

Example --> security set IDS SCANattackblock 43200

4.2.7.1.53 SECURITY SET IDS FLOODPERIOD

Syntax SECURITY SET IDS FLOODPERIOD <DURATION>

Description This command allows you to set the time limit during which suspected SYN floods are counted. If the number of SYN floods counted within the specified duration is greater than the threshold set by either SECURITY SET IDS FLOODTHRESHOLD OR SECURITY SET IDS PORTFLOODTHRESHOLD, the suspected attacker is blocked for the time limit specified in the command SECURITY SET IDS DOSATTACKBLOCK.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that suspected SYN floods are counted for.	10

Example --> security set IDS floodperiod 60

4.2.7.1.54 SECURITY SET IDS FLOODTHRESHOLD

Syntax SECURITY SET IDS FLOODTHRESHOLD <MAX>

Description This command allows you to set the maximum number of SYN packets allowed before a flood is detected. If the number of SYN packets counted within the time duration set by the command SECURITY SET IDS FLOODPERIOD is greater than the maximum value

set here, the suspected attacker is blocked for the time limit specified in the command SECURITY SET IDS DOSATTACKBLOCK.

For example, using the default settings, if more than 20 SYN packets are received per second for a 10 second duration, the attacker is blocked.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	Maximum number of SYN packets that can be received before a flood is detected.	20 (per second)

Example --> security set IDS floodthreshold 25

4.2.7.1.55 SECURITY SET IDS PORTFLOODTHRESHOLD

Syntax `SECURITY SET IDS PORTFLOODTHRESHOLD <MAX>`

Description This command allows you to set the maximum number of SYN packets that can be sent to a single port before a port flood is detected. If the number of SYN packets counted within the time duration set by the command SECURITY SET IDS FLOODPERIOD is greater than the maximum value set here, the suspected attacker is blocked for the time limit specified in the command SECURITY SET IDS DOSATTACKBLOCK.

For example, using the default settings, if more than 10 SYN packets are received per second for a 10 second duration, the attacker is blocked.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	Maximum number of SYN packets that can be received by a single port before a flood is detected.	10 (per second)

Example --> security set IDS portfloodthreshold 15

4.2.7.1.56 SECURITY SET IDS SCANPERIOD

Syntax `SECURITY SET IDS SCANPERIOD <DURATION>`

Description This command allows you to set the time limit during which scanning type traffic (such as closed TCP port reviving SYN/ACK, FIN or RST) is counted. If the number of scanning packets counted within the specified duration is greater than the threshold set by SECURITY SET IDS SCANTHRESHOLD, the suspected attacker is blocked for the time limit specified in the command SECURITY SET IDS SCANATTACKBLOCK.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that scanning type traffic is counted for.	60 (seconds)

Example --> security set IDS scanperiod 90

4.2.7.1.57 SECURITY SET IDS SCANTHRESHOLD

Syntax `SECURITY SET IDS SCANTHRESHOLD <MAX>`

Description This command allows you to set the maximum number of scanning packets that can be received before a port scan is detected. If the number of scanning packets counted within the time duration set by the command SECURITY SET IDS SCANPERIOD is greater than the maximum value set here, the suspected attacker is blocked for the time limit specified in the command SECURITY SET IDS SCANATTACKBLOCK.

For example, using the default settings, if more than 5 scanning packets are received per second for a 60 second duration, the attacker is blocked.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	Maximum number of scanning packets that can be received before a port scan attack is detected.	5 (per second)

Example --> security set IDS scanthreshold 8

See also

4.2.7.1.58 SECURITY SET AEMLOGGINGINTERVAL

Syntax `SECURITY SET AEMLOGGINGINTERVAL <number>`

Description This command sets the alarm logging interval value

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
number	The interval between each AEM logging message.	5

Example --> security set IDS MaxPING 25

See also `security show`

4.2.7.1.59 SECURITY SHOW IDS

Syntax `SECURITY SHOW IDS`

Description This command displays the following information about IDS settings:

- IDS enabled status (true or false)
- Blacklist status (true or false)
- Use Victim Protection status (true or false)
- DOS attack block duration (in seconds)
- Scan attack block duration (in seconds)
- Victim protection block duration (in seconds)
- Maximum TCP open handshaking count allowed (per second)
- Maximum ping count allowed (per second)
- Maximum ICMP count allowed (per second)

Example --> security show IDS

```
   Firewall IDS:

                          IDS Enabled: false
                       Use Blacklist: false
                  Use Victim Protection: false
              Dos Attack Block Duration: 1800
            Scan Attack Block Duration: 86400
      Malicious Attack Block Duration: 86400
```

```
Victim Protection Block Duration: 600
       Scan Detection Threshold: 5
          Scan Detection Period: 10
  Port Flood Detection Threshold: 10
  Host Flood Detection Threshold: 20
             FloodDetectPeriod : 10
  Max TCP Open Handshaking Count: 5
                 Max PING Count: 15
                 Max ICMP Count: 100
```

4.3 Firewall

4.3.1 Overview

The AT-iMG Models security system implements a ***stateful*** Firewall providing high security by blocking certain incoming traffic based on ***stateful*** information.

Each time outbound packets are sent from an internal host to an external host, the following information is logged by the Firewall:

- source and destination addresses
- Port number
- Sequencing information
- Additional flags for each connection associated with that particular internal host

All inbound packets are compared against this logged information and only allowed through the Firewall if it can be determined that they are part of an existing connection. This makes it very difficult for hackers to break through the ***stateful*** Firewall, because they would need to know addresses, port numbers, sequencing information and individual connection flags for an existing session to an internal host.

The firewall module manages firewall behaviour. The firewall module offers the ability to:

- Control what kind of Firewall activity is logged
- Protect the internal network using ***stateful*** firewall functionality
- Create policies
- Add ***validators*** to policies
- Add ***portfilters*** to policies
- Enable/disable and configure Intrusion ***Detection Settings*** (IDS)

In order to access firewall features, the firewall module must be enabled using the firewall enable command.

Figure 9 shows the entities involved in the firewall module and their relationships.

4.3.1.1 Policy

A policy is a relationship between two security interfaces where it is possible to assign ***portfilter*** and ***validator*** rules between them.

There are three different security interface combinations that Firewall policies can be created between:

- The ***external interface*** and the ***internal interface***
- The ***external interface*** and the ***DMZ*** interface
- The ***DMZ*** interface and the ***internal interface***

To add a policy between one of the three above interface combinations use the FIREWALL ADD POLICY command.

4.3.1.2 Portfilter

A ***portfilter*** is a rule that determines how the Firewall should handle packets being transported between two security interfaces that are defined in an existing policy. The rules define:

- What protocol type is allowed
- Which TCP/UDP port numbers the packets are allowed to be transported on
- the name of the well-known protocol, service or application allowed to be transported
- source and destination addresses

Whichever type of filter rule you use, you must also determine which direction packets should be allowed to travel in:

- inbound; permitted traffic is transported from the outside interface to the inside interface
- outbound; permitted traffic is transported from the inside interface to the outside interface
- both; inbound and outbound rules apply

To add a ***portfilter*** to an existing policy use the FIREWALL ADD PORTFILTER command.

More than one ***portfilter*** object can be added to the same policy.

4.3.2 Firewall command reference

This section describes the commands available on AT-iMG Models to enable, configure and manage the ***Firewall*** module

The table below lists the ***firewall*** commands provided by the CLI:

TABLE 4-3 Firewall commands and Product Type

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
FIREWALL ENABLE|DISABLE	X	X	X	X	X	X	X	X	X
FIREWALL ENABLE|DISABLE IDS	X	X	X	X	X	X	X	X	X
FIREWALL ENABLE|DISABLE BLOCKINGLOG|INTRUSION-LOG|SESSIONLOG	X	X	X	X	X	X	X	X	X
FIREWALL SET SECURITYLEVEL	X	X	X	X	X	X	X	X	X
FIREWALL STATUS	X	X	X	X	X	X	X	X	X
FIREWALL LIST POLICIES	X	X	X	X	X	X	X	X	X
FIREWALL SHOW POLICY	X	X	X	X	X	X	X	X	X
FIREWALL LIST PROTOCOL	X	X	X	X	X	X	X	X	X
FIREWALL ADD DOMAINFILTER	X	X	X	X	X	X	X	X	X
FIREWALL SET DOMAINFILTER	X	X	X	X	X	X	X	X	X
FIREWALL DELETE DOMAINFILTER	X	X	X	X	X	X	X	X	X
FIREWALL ADD PORTFILTER	X	X	X	X	X	X	X	X	X
FIREWALL SET PORTFILTER	X	X	X	X	X	X	X	X	X
FIREWALL CLEAR PORTFILTERS	X	X	X	X	X	X	X	X	X
FIREWALL DELETE PORTFILTER	X	X	X	X	X	X	X	X	X
FIREWALL LIST PORTFILTERS	X	X	X	X	X	X	X	X	X
FIREWALL SHOW PORTFILTER	X	X	X	X	X	X	X	X	X
FIREWALL ADD VALIDATOR	X	X	X	X	X	X	X	X	X
FIREWALL DELETE VALIDATOR	X	X	X	X	X	X	X	X	X
FIREWALL LIST VALIDATORS	X	X	X	X	X	X	X	X	X
FIREWALL LIST VALIDATORS	X	X	X	X	X	X	X	X	X
FIREWALL SHOW VALIDATOR	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS VICTIMPROTECTION	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS DOSATTACKBLOCK	X	X	X	X	X	X	X	X	X

TABLE 4-3 Firewall commands (Continued)and Product Type

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
FIREWALL SET IDS MAXICMP	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS MaxPING	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS MAXTCPOPENHANDSHAKE	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS SCANATTACKBLOCK	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS FLOODPERIOD	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS FLOODTHRESHOLD	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS PORTFLOODTHRESHOLD	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS SCANPERIOD	X	X	X	X	X	X	X	X	X
FIREWALL SET IDS SCANTHRESHOLD	X	X	X	X	X	X	X	X	X
FIREWALL SHOW IDS	X	X	X	X	X	X	X	X	X

4.3.2.0.1 FIREWALL ENABLE|DISABLE

Syntax `firewall {enable | disable}`

Description This command enables/disables the entire ***Firewall*** module except for the IDS portion of the module (see the command FIREWALL ENABLE|DISABLE IDS).

When the Firewall is enabled, all IP traffic on existing security interfaces that are NOT featured in a Firewall policy is blocked. For details on setting default policy security levels on security interfaces, see the FIREWALL SET SECURITYLEVEL command.

If you disable the Firewall during a session, any configuration changes made when the Firewall was enabled remain in the Firewall, so that you can re-enable them later in the session. If you need to reboot your system but want to save the Firewall configuration between sessions, use the SYSTEM CONFIG SAVE command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enable	Enables the ***Firewall*** module.	Disable
disable	Disables the ***Firewall*** module.	

Example --> firewall enable

4.3.2.0.2 FIREWALL ENABLE|DISABLE IDS

Syntax `firewall {enable | disable}`

Description This command explicitly enables/disables IDS (Intrusion Detection Service). You must enable IDS if you want to activate the settings specified in the *security IDS* commands.

This command is nothing but an alias of the "security enable|disable IDS"

*Note: You **must** enable the Security module using the command security on in order to use IDS*

If you disable IDS during a session, any configuration changes made when IDS was enabled are not deleted - you can re-enable them later in the session.

*Note: You **must** enable the Security module using the command security on in order to use IDS*

This CLI command is **case-sensitive**. You must type the command attributes exactly as they appear in the Command Syntax section on this page. If you do not use the same case-sensitive syntax, the command fails and the CLI displays a syntax error message

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enable	Enables the IDS portion of the Security module.	Disable
disable	Disables the IDS portion of the Security module.	

Example --> firewall enable IDS

See also `security enable IDS, security disable IDS`

4.3.2.0.3 FIREWALL ENABLE|DISABLE BLOCKINGLOG|INTRUSIONLOG|SESSIONLOG

Syntax `firewall {enable | disable} {blockinglog|intrusionlog|sessionlog}`

Description This command enables/disables the entire ***Firewall*** module except for the IDS portion of the module (see the command FIREWALL ENABLE|DISABLE IDS).

When the Firewall is enabled, all IP traffic on existing security interfaces that are NOT featured in a Firewall policy is blocked. For details on setting default policy security levels on security interfaces, see the FIREWALL SET SECURITYLEVEL command.

If you disable the Firewall during a session, any configuration changes made when the Firewall was enabled remain in the Firewall, so that you can re-enable them later in the session. If you need to reboot your system but want to save the Firewall configuration between sessions, use the SYSTEM CONFIG SAVE command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
enable	Enables the ***Firewall*** module.	Disable
disable	Disables the ***Firewall*** module.	

Example --> firewall enable

4.3.2.0.4 FIREWALL SET SECURITYLEVEL

Syntax `FIREWALL SET SECURITYLEVEL {NONE | HIGH | MEDIUM | LOW}`

Description This command allows you to set which security level is used by the Firewall. There are four default security levels (none, high, medium and low) that contain different security configuration information for each interface connection.

Selecting a security level deletes the previous security level and any policies or portfilters set, and replaces them with the newly selected level.

The factory default setting none is not a security level. It is a blank firewall configuration that allows you to create your own policies and portfilters, using the commands firewall add policy and firewall add portfilter. These manually configured policies/portfilters are stored in the im.conf file.

Explicitly setting the security level to none sets a security level that does not contain any policies or portfilters. Note that if you create policies/portfilters and store them in the im.conf file, then select none (or any other security level), all of your manually configured policies/portfilters will be deleted and replaced with this level.

The userdefined option allows you to select a security configuration that you have previously created.

There are three types of interface connections:

- Between the external interface and internal interface
- Between the external interface and the de-militarized zone (DMZ)
- Between the DMZ and the internal interface

You can add your own firewall portfilters to a security level by using the FIREWALL ADD PORTFILTER command. If you then save your configuration using the SYSTEM CONFIG CREATE/SET command, these additional filters are saved with the default level and are restored on reboot.

Options The following tables describe the default policies enabled in the firewall for each of the high, medium and low security levels. The tables tell you whether a certain service can be received in or allowed out by a specific policy. (Y=yes; N=no):

TABLE 4-4 Default Policies Enabled in the Firewall - High Security

High Security Level		External< > Internal		External< >DMZ		DMZ< >Internal	
Service	**Port**	**In**	**Out**	**In**	**Out**	**In**	**Out**
http	80	N	Y	Y	Y	Y	Y
dns	53	N	Y	N	Y	N	Y
telnet	23	N	N	N	N	N	N
smtp	25	N	Y	Y	Y	Y	Y
pop3	110	N	Y	Y	Y	Y	Y
nntp	119	N	N	N	N	N	N
real audio/video	7070	N	N	N	N	N	N
icmp	N/A	N	Y	N	Y	N	Y
H.323	1720	N	N	N	N	N	N
T.120	1503	N	N	N	N	N	N
SSH	22	N	N	N		Y	N

TABLE 4-5 Default Policies Enabled in the Firewall - Medium Security

High Security Level		External< > Internal		External< >DMZ		DMZ< >Internal	
Service	**Port**	**In**	**Out**	**In**	**Out**	**In**	**Out**
http	80	N	Y	Y	Y	Y	Y
dns	53	N	Y	Y	Y	Y	Y
telnet	23	N	Y	N	Y	N	Y
smtp	25	N	Y	Y	Y	Y	Y
pop3	110	N	Y	Y	Y	Y	Y
nntp	119	N	Y	Y	Y	Y	Y
real audio/video	7070	Y	N	N	Y	N	Y
icmp	N/A	N	Y	N	Y	N	Y
H.323	1720	N	Y	N	Y	N	Y
T.120	1503	N	Y	N	Y	N	Y
SSH	22	N	Y	N	Y	N	Y

TABLE 4-6 Default Policies Enabled in the Firewall - Low Security

High Security Level		External< > Internal		External< >DMZ		DMZ< >Internal	
Service	**Port**	**In**	**Out**	**In**	**Out**	**In**	**Out**
http	80	N	Y	Y	Y	Y	Y
dns	53	Y	Y	Y	Y	Y	Y
telnet	23	N	Y	Y	Y	Y	Y
smtp	25	N	Y	Y	Y	Y	Y
pop3	110	N	Y	Y	Y	Y	Y
nntp	119	N	N	N	N	N	N
real audio/video	7070	Y	N	Y	Y	Y	Y
icmp	N/A	N	Y	Y	Y	Y	Y
H.323	1720	Y	Y	Y	Y	Y	Y
T.120	1503	Y	Y	Y	Y	Y	Y
SSH	22	Y	Y	Y	Y	Y	Y

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable):

Option	Description	Default Value
none	The factory default setting ***none*** is not a security level - it allows you to manually configure your own policies/ portfilters. Explicitly setting none sets a security level that does not contain any policies/portfilters.	None (factory default setting)
high	Your system uses the high firewall security level, providing a high level of firewall security between interfaces.	
medium	Your system uses the medium firewall security level, providing a medium level of firewall security between interfaces.	
low	Your system uses the low firewall security level, providing a low level of firewall security between interfaces.	
userdefined	Your system uses a security configuration that you have previously created.	
slevel	The name of the security configuration level that you have previously created	N/A

Example --> firewall set securitylevel medium

4.3.2.0.5 FIREWALL STATUS

Syntax `firewall status`

Description This command displays the following information about the Firewall:

- Firewall status (enabled or disabled)
- Security level setting (none, high, low or medium)
- Firewall logging status:
- session logging (enabled or disabled)
- blocking logging (enabled or disabled)
- intrusion logging (enabled or disabled)

Example --> firewall status

```
Firewall enabled.
Firewall security level: medium.
Firewall session logging enabled.
```

```
Firewall blocking logging enabled.
Firewall intrusion logging disabled.
```

See also `firewall enable|disable`
`firewall set securitylevel`

4.3.2.0.6 FIREWALL LIST POLICIES

Syntax `firewall list policies`

Description This command lists the following information about policies that were added to the firewall using the FIREWALL ADD POLICY command:

- Policy ID number
- Policy name
- Interface Type 1 and Interface Type 2 - the two interface types between which a policy exists (external - internal, external - DMZ or internal - DMZ)
- Validator Allow Only status - False, only traffic based on the direction and the IP address(es) specified by Firewall validators is blocked. All other traffic is allowed.

Example --> firewall list policies

```
Firewall Policies:
ID | Name    | Type 1   | Type 2   | Validator Allow Only
-------------------------------------------------------
1  | ext-int | external | internal | false
2  | ext-dmz | external | dmz      | false
3  | dmz-int | dmz      | internal | false
-------------------------------------------------------
```

See also `FIREWALL SHOW POLICY`
`FIREWALL ADD`
`FIREWALL ADD VALIDATOR`

4.3.2.0.7 FIREWALL SHOW POLICY

Syntax `firewall show policy {ext-int|ext-dmz|dmz-int}`

Description This command displays information about a single policy that exists between two Security interface types. Allow only Validator: false, means that only traffic based on the direction and the IP address(es) specified in the firewall add validator command is blocked. All other traffic is allowed.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall show policy ext-dmz

```
Firewall Policy: ext-dmz
Interface Type 1: external
Interface Type 2: dmz
Allow Only Validator: false
```

See also `FIREWALL LIST POLICIES`

See also `firewall set securitylevel`

4.3.2.0.8 FIREWALL LIST PROTOCOL

Syntax `firewall list protocol`

Description This command lists the. The number of a non-TCP or non-UDP protocol. Protocol numbers can be found at http://www.ietf.org/rfc/rfc1700.txt.

Example --> firewall list protocol

```
Assigned Internet Protocol Numbers
see RFC 1700 "Assigned Numbers"
section "Protocol Numbers" pages 7 - 9

 1  ICMP     Internet Control Message
 2  IGMP     Internet Group Management
 3  GGP      Gateway-to-Gateway
 4  IP       IP in IP (encapsulation)
 6  TCP      Transmission Control
 8  EGP      Exterior Gateway Protocol
 9  IGP      any private interior gateway
17  UDP      User Datagram
46  RSVP     Reservation Protocol
47  GRE      General Routing Encapsulation
89  OSPFIGP  OSPFIGP
92  MTP      Multicast Transport Protocol
94  IPIP     IP-within-IP Encapsulation Protocol
```

See also `Firewall add portfilter, firewall set portfilter`

4.3.2.0.9 FIREWALL ADD DOMAINFILTER

Syntax `FIREWALL ADD DOMAINFILTER <filtername> <policyname> <urlstring> <starttime> <endtime>`

Description This command adds a new domainfilter. Your must specify the url which is an alphanumeric string including wildcard chars("*") and ".".

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
filtername	Any alphanumeric string. This is the name of the domain filter which should be unique.	N/A
policyname	Firewall policy.	N/A
urlstring	Any alphanumeric string which represents a valid domain name. includes '*' to support wildcards.	N/A
starttime	Start time from when filter is active. Format will be in 24 hour hh:mm:ss	N/A
endtime	Time after which filter is no more active.	N/A

Example --> firewall add domainfilter all_http ext-int www.*.com 10:00:00 18:00:00

4.3.2.0.10 FIREWALL SET DOMAINFILTER

Syntax `firewall SET domainfilter RULEACTION {<ALLOW|DENY>}`

Description This command is used to change the default action required for every created domainfilter.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
allow	allows all the domainfilters created	N/A
deny	denies all the domainfilters created .	N/A

Example --> firewall add domainfilter ruleAction allow

4.3.2.0.11 FIREWALL DELETE DOMAINFILTER

Syntax `firewall delete domainfilter <filtername> <policyname>`

Description This command is used for deleting the URL filter created using the previous command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
filtername	Any alphanumeric string. This is the name of the domain filter which should be unique..	N/A
policyname	Firewall policy.	N/A

Example `-->firewall delete domainfilter all_http ext-int`

See also `firewall add portfilter, firewall list domainfilter`

4.3.2.0.12 FIREWALL ADD PORTFILTER

Syntax `FIREWALL ADD PORTFILTER <name> <policyname> {PROTOCOL <protocol>} {INBOUND|OUTBOUND|BOTH}`

FIREWALL ADD PORTFILTER <name> <policyname> {TCP|UDP} <startport> <endport> {INBOUND|OUTBOUND|BOTH}

FIREWALL ADD PORTFILTER <name> <policyname> {ICMP|SMTP|HTTP|FTP|TELNET} {INBOUND|OUTBOUND|BOTH}

Description This command adds a portfilter to an existing firewall policy. Portfilters are individual rules that determine what kind of traffic can pass between the two interfaces specified in the firewall add policy command.

There are three ways that you can add a portfilter depending on the type of protocol that you want to feature in the portfilter:

Specify the number of a non-TCP or non-UDP protocol (for more information, see http://www.ietf.org/rfc/rfc1700.txt)

Specify TCP or UDP protocol, together with an application's start/end port numbers

Specify one of the listed protocols, applications or services. These are provided by the Firewall as popular examples that you can use. You do not need to specify the portnumber - the Firewall does this for you.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the portfilter. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A
protocol		
startport		
endport		
inbound		
outbound		
both		

Example

Example 1 - specifying a protocol <number>

The following example allows IGMP (***Internet Group Management Protocol***) packets inbound from the external interface to the DMZ interface. IGMP is protocol number 2 (see http://www.ietf.org/rfc/rfc1700.txt).

First, we need to create a policy:

--> firewall add policy ext-dmz external-dmz

Then we can add the portfilter to it:

--> firewall add portfilter pf1 ext-dmz protocol 2 inbound

Example 2 - specifying a TCP/UDP protocol

The following example allows DNS (***Domain Name Service***) outbound packets from the internal interface to the external interface. DNS uses UDP port 53 (see http://www.ietf.org/rfc/rfc1700.txt).

First, we need to create a policy:

--> firewall add policy ext-int external-internal

Then we can add the portfilter to it:

--> firewall add portfilter pf2 ext-int udp 53 53 outbound

Example 3 - using a provided protocol, application or service

The following example allows SMTP (***Simple Mail Transfer Protocol***) packets inbound and outbound between the internal interface to the DMZ interface. This is a popular protocol that is provided by the Firewall. You do not need to specify the portnumber - the Firewall does this for you.

First, we need to create a policy:

--> firewall add policy dmz-int dmz-internal

Then we can add the portfilter to it:

--> firewall add portfilter pf3 dmz-int smtp both

See also `FIREWALL LIST POLICIES`

`FIREWALL LIST PROTOCOL`

See the Well Known Port Numbers section of RFC 1700 for a list of port numbers and protocols for particular services (see http://www.ietf.org/rfc/rfc1700.txt).

4.3.2.0.13 FIREWALL SET PORTFILTER

Syntax `firewall set portfilter <name> <policyname> {srcaddr <IPaddress><Mask>} {dstaddr <IPaddress><Mask>}`

firewall set portfilter <name> <policyname> {srcport <startport><endport>} {dstport <startport><endport>}

firewall set portfilter <name> <policyname> {Protocol <protocol>}

firewall set portfilter <name> <policyname> {direction <inbound | outbound | both>}

filrewall set portfilter <name> <policyname> {ENABLE | disabled}

filrewall set portfilter <name> <policyname> {ALLOW | DENY}

Description This command sets all the attributes of each portfilter object created in the system. The attributes of portfilters are:

- set the permission status of portfilter to allow or deny
- source and destination address
- source and destination port
- protocol
- direction

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the portfilter. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A
IPaddress	The source and destination IP address. The IP address is displayed in the following format: 192.168.102.3	N/A
Mask	the IP Mask address.	N/A
protocol	The number of a non-TCP or non-UDP protocol. Protocol numbers can be found at http://www.ietf.org/rfc/rfc1700.txt	N/A
startport	The start of the port range for a TCP or UDP protocol.	N/A
endport	The end of the port range for a TCP or UDP protocol.	N/A
inbound	Allows transport of packets of the specified protocol, application or service from an outside interface to an inside one. Outbound transport of the packets is not allowed.	N/A
outbound	Allows transport of packets of the specified protocol, application or service from an inside interface to an outside interface. Inbound transport of the packets is not allowed.	N/A
both	Allows inbound and outbound transport of packets of the specified protocol, application or service between inside and outside interfaces.	N/A
enable	It enables the changes done to the attributes.	N/A
disable	It disables the changes done to the attributes.	N/A
allow	set the permission status of portfilter to allow	N/A
deny	set the permission status of portfilter to deny	

4.3.2.0.14 FIREWALL CLEAR PORTFILTERS

Syntax `FIREWALL CLEAR PORTFILTERS <policyname>`

Description This command deletes all portfilters that were added to an existing firewall policy using the firewall add portfilter command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall clear portfilters ext-int

See also `FIREWALL DELETE PORTFILTER`
`FIREWALL LIST POLICIES`

4.3.2.0.15 FIREWALL DELETE PORTFILTER

Syntax `FIREWALL DELETE PORTFILTER <name> <policyname>`

Description This command deletes a single portfilter that was added to a firewall policy using the firewall add portfilter command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing portfilter. To display portfilter names, use the FIREWALL LIST PORTFILTER command.	N/A
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall delete portfilter pf3 ext-int

See also `FIREWALL LIST POLICIES`
`FIREWALL LIST PORTFILTERS`
`FIREWALL CLEAR PORTFILTERS`

4.3.2.0.16 FIREWALL LIST PORTFILTERS

Syntax `FIREWALL LIST PORTFILTERS <policyname>`

Description This command lists portfilters that were added to a firewall policy using the firewall add portfilter command. It displays the following information:

- Portfilter ID number
- Portfilter name
- Type - port number range or specified port number
- Port range used by the specified TCP or UDP protocol (e.g., 53 for DNS, 25 for SMTP). For non-TCP/UDP protocols, the port range is set to 0-0.
- In - displays the inbound permission setting (true or false)
- Out- displays the outbound permission setting (true or false)
- Raw - displays whether the portfilter uses a non-TCP/UDP protocol (true or false)
- TCP - displays whether the portfilter uses a TCP protocol (true or false)
- UDP - displays whether the portfilter uses a UDP protocol (true or false)

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall list portfilters ext-int

```
Firewall Port Filters:

 ID | Name      | Prot | Status  | allow
-----------------------------------------
  1 | pf2       | TCP  | enabled | true
  2 | pf3       | UDP  | enabled | true
  3 | pf4       | 92   | disabled| false
-----------------------------------------
```

See also FIREWALL LIST POLICIES
FIREWALL LIST PROTOCOL

See also FIREWALL SHOW PORTFILTER

See also For a list of the port numbers and/or numbers assigned to protocols, see http://www.ietf.org/rfc/rfc1700.txt.

4.3.2.0.17 FIREWALL SHOW PORTFILTER

Syntax FIREWALL SHOW PORTFILTER <name> <policyname>

Description This command displays information about a single portfilter that was added to a firewall policy using the firewall policy add portfilter command. The following portfilter information is displayed:

- Portfilter name
- Transport type used by the protocol (e.g., 6 for SMTP)
- Start of the port range
- End of the port range
- Inbound permission (true or false)
- Outbound permission (true or false)
- Raw IP - whether the portfilter uses a non-TCP/UDP protocol (true or false)
- TCP permission - whether the portfilter uses a TCP protocol (true or false)
- UDP permission - whether the portfilter uses a UDP protocol (true or false)

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing portfilter. To display portfilter names, use the FIREWALL LIST PORTFILTERS command.	N/A
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall show portfilter pf3 ext-int

```
Firewall Port Filter: pf3

          Source IP range start : 0.0.0.0
            Source IP range end : 255.255.255.255
     Destination IP range start : 0.0.0.0
       Destination IP range end : 255.255.255.255
                    IP protocol : TCP
       Source port number start : 0
         Source port number end : 65535
  Destination port number start : 25
    Destination port number end : 25
             Inbound permission : true
            Outbound permission : true
```

```
                    Status : enabled
                Permitted? : true
```

See also `FIREWALL LIST POLICIES`
`FIREWALL LIST PORTFILTERS`

4.3.2.0.18 FIREWALL ADD VALIDATOR

Syntax `FIREWALL ADD VALIDATOR <name> <policyname> {INBOUND|OUTBOUND|BOTH} <ipaddress> <hostipmask>`

Description This command adds a validator to a firewall policy. Traffic is blocked based on the source/destination IP address and netmask. This command allows you to specify:

- the IP address(es) and netmask(s) that you want to block
- the direction of traffic that you want to block

Once you have added a validator to a policy, specifying the IP address and direction values, you can reuse these values by adding the validator to other policies.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the portfilter. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A
inbound	Validator blocks incoming traffic based on IP addresses.	N/A
outbound	Validator blocks outgoing traffic based on IP addresses.	N/A
both	Validator filters inbound and outbound traffic based on IP addresses.	N/A
ipaddress	The IP address that you want to carry out IP address validation on. The IP address is displayed in the following format: 192.168.102.3	N/A
hostipmask	The IP mask address. If you want to filter a range of addresses, you can specify the mask, e.g., 255.255.255.0. If you want to filter a single IP address, you can use the specific IP mask address, e.g., 255.255.255.255.	N/A

Example In the following example, a policy is created, then a validator added to block inbound and outbound traffic from/to the IP address stated. All other traffic is allowed.

--> firewall add policy ext-int external-internal blockonly-val

--> firewall add validator v1 ext-int both 192.168.102.3 255.255.255.255

See also
```
firewall add policy
firewall list policies
firewall delete validator
firewall show validator
```

4.3.2.0.19 FIREWALL DELETE VALIDATOR

Syntax `FIREWALL DELETE VALIDATOR <name> <policyname>`

Description This command deletes a single validator from a named policy.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing validator. To display validator names, use the FIREWALL LIST VALIDATORS command.	N/A
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall delete validator v1 ext-int

See also
```
FIREWALL LIST VALIDATORS
FIREWALL LIST POLICIES
```

4.3.2.0.20 FIREWALL LIST VALIDATORS

Syntax `FIREWALL LIST VALIDATORS <policyname>`

Description This command lists the following information about validators added to a policy using the FIREWALL ADD VALIDATOR command:

- Validator ID number
- Validator name
- Direction (inbound, outbound or both)
- Host IP address

- Host mask address

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall list validators ext-int

```
Firewall Host Validators:
  ID |   Name  | Direction |    Host IP     |      Mask
-------------------------------------------------------------
   1 |  v1     | both      | 192.168.103.2  | 255.255.255.0
   2 |  v2     | inbound   | 192.168.103.1  | 255.255.255.0
-------------------------------------------------------------
```

See also FIREWALL ADD VALIDATOR
FIREWALL SHOW VALIDATOR
FIREWALL LIST POLICIES

4.3.2.0.21 FIREWALL SHOW VALIDATOR

Syntax FIREWALL SHOW VALIDATOR <name> <policyname>

Description This command displays information about a single validator that was added to firewall policy using the FIREWALL ADD VALIDATOR command. The following validator information is displayed:

- Validator name
- Direction (inbound, outbound or both)
- Host IP address
- Host mask address

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing validator. To display validator names, use the FIREWALL LIST VALIDATORS command.	N/A

Option	Description	Default Value
policyname	An existing firewall policy. To display policy names, use the FIREWALL LIST POLICIES command.	N/A

Example --> firewall show validator v1 ext-int

```
Firewall Host Validator: v1
Direction: both
  Host IP: 192.168.103.2
Host Mask: 255.255.255.0
```

See also `FIREWALL ADD VALIDATOR`
`FIREWALL LIST VALIDATORS`
`FIREWALL LIST POLICIES`

4.3.2.0.22 FIREWALL SET IDS VICTIMPROTECTION

Syntax `firewall set IDS victimprotection <duration>`

Description This command sets the duration of the victim protection Intrusion Detection Setting (IDS). If victim protection is enabled, packets destined for the victim host of a spoofing style attack are blocked. The command allows you to specify the duration of the block time limit.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that packets destined for the victim of a spoofing style attack. are blocked for.	600 (10 minutes)

Example --> firewall set IDS victimprotection 800

See also `security set ids victimprotection`

4.3.2.0.23 FIREWALL SET IDS DOSATTACKBLOCK

Syntax `firewall set IDS DOSATTACKBLOCK <DURATION>`

Description This command sets the DOS (Denial of Service) attack block duration Intrusion Detection Setting (IDS). A DOS attack is an attempt by an attacker to prevent legitimate users from using a service. If a DOS attack is detected, all suspicious hosts are blocked for a set time limit. This command allows you to specify the duration of the block time limit.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that suspicious hosts are blocked for once a DOS attack attempt has been detected.	1800 (30 minutes)

Example --> firewall set IDS DOSattackblock 800

See also `security set IdS Dosattackblock`

4.3.2.0.24 FIREWALL SET IDS MAXICMP

Syntax `FIREWALL SET IDS MAXICMP <MAX>`

Description This command sets the maximum number of ICMP packets per second that are allowed before an ICMP Flood is detected. An ICMP Flood is a DOS (Denial of Service) attack. An attacker tries to flood the network with ICMP packets in order to prevent transportation of legitimate network traffic. Once the maximum number of ICMP packets per second is reached, an attempted ICMP Flood is detected.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	The maximum number (per second) of ICMP packets that are allowed before an ICMP Flood attempt is detected.	100

Example --> firewall set IDS MaxICMP 200

See also `security set IDS MaxICMP`

4.3.2.0.25 FIREWALL SET IDS MAXPING

Syntax `FIREWALL SET IDS MAXPING <MAX>`

Description This command sets the maximum number of pings per second that are allowed before an Echo Storm is detected. Echo Storm is a DOS (Denial of Service) attack. An attacker sends oversized ICMP datagrams to the system using the 'ping' command. This can cause the system to crash, freeze or reboot, resulting in denial of service to legitimate users. Once the maximum number of pings per second is reached, an attempted DOS attack is detected.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	The maximum number (per second) of pings that are allowed before an Echo Storm attempt is detected.	15

Example --> firewall set IDS MaxPING 25

See also `security set IDS MaxPING`

4.3.2.0.26 FIREWALL SET IDS MAXTCPOPENHANDSHAKE

Syntax `FIREWALL SET IDS MAXTCPOPENHANDSHAKE <MAX>`

Description This command sets the maximum number of unfinished TCP handshaking sessions per second that are allowed before a SYN Flood is detected. SYN Flood is a DOS (Denial of Service) attack. When establishing normal TCP connections, three packets are exchanged:

- 1 A SYN (synchronize) packet is sent from the host to the network server
- 2 A SYN/ACK packet is sent from the network server to the host
- 3 An ACK (acknowledge) packet is sent from the host to the network server

If the host sends unreachable source addresses in the SYN packet, the server sends the SYN/ACK packets to the unreachable addresses and keeps resending them. This creates a backlog queue of unacknowledged SYN/ACK packets. Once the queue is full, the system will ignore all incoming SYN requests and no legitimate TCP connections can be established.

Once the maximum number of unfinished TCP handshaking sessions is reached, an attempted DOS attack is detected. The suspected attacker is blocked for the time limit specified in the FIREWALL SET IDS DOSattackblock command.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	The maximum number (per second) of unfinished TCP handshaking sessions that are allowed before a SYN Flood attempt is detected..	100

Example --> firewall set IDS MaxTCPopenhandshake 150

See also `security set IDS MaxTCPopenhandshake`

4.3.2.0.27 FIREWALL SET IDS SCANATTACKBLOCK

Syntax `FIREWALL SET IDS SCANATTACKBLOCK <DURATION>`

Description This command allows you to set the scan attack block duration Intrusion Detection Setting (IDS). If hosts are blocked for a set time limit, this command allows you to specify the duration of the block time limit.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that a suspicious host is blocked for, after scan activity has been detected.	86400 (one day)

Example --> firewall set IDS SCANattackblock 43200

See also `security set IDS SCANattackblock`

4.3.2.0.28 FIREWALL SET IDS FLOODPERIOD

Syntax `FIREWALL SET IDS FLOODPERIOD <DURATION>`

Description This command allows you to set the time limit during which suspected SYN floods are counted. If the number of SYN floods counted within the specified duration is greater than the threshold set by either FIREWALL SET IDS FLOODTHRESHOLD OR FIREWALL SET IDS PORTFLOODTHRESHOLD, the suspected attacker is blocked for the time limit specified in the command FIREWALL SET IDS DOSATTACKBLOCK.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that suspected SYN floods are counted for.	10

Example --> firewall set IDS floodperiod 60

See also `security set IDS floodperiod`

4.3.2.0.29 FIREWALL SET IDS FLOODTHRESHOLD

Syntax `FIREWALL SET IDS FLOODTHRESHOLD <MAX>`

Description This command allows you to set the maximum number of SYN packets allowed before a flood is detected. If the number of SYN packets counted within the time duration set by the command FIREWALL SET IDS FLOODPERIOD is greater than the maximum value set here, the suspected attacker is blocked for the time limit specified in the command FIREWALL SET IDS DOSATTACKBLOCK.

For example, using the default settings, if more than 20 SYN packets are received per second for a 10 second duration, the attacker is blocked.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	Maximum number of SYN packets that can be received before a flood is detected.	20 (per second)

Example --> firewall set IDS floodthreshold 25

See also `security set IDS floodthreshold`

4.3.2.0.30 FIREWALL SET IDS PORTFLOODTHRESHOLD

Syntax `FIREWALL SET IDS PORTFLOODTHRESHOLD <MAX>`

Description This command allows you to set the maximum number of SYN packets that can be sent to a single port before a port flood is detected. If the number of SYN packets counted within the time duration set by the command FIREWALL SET IDS FLOODPERIOD is greater than the maximum value set here, the suspected attacker is blocked for the time limit specified in the command FIREWALL SET IDS DOSATTACKBLOCK.

For example, using the default settings, if more than 10 SYN packets are received per second for a 10 second duration, the attacker is blocked.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	Maximum number of SYN packets that can be received by a single port before a flood is detected.	10 (per second)

Example --> firewall set IDS portfloodthreshold 15

See also `security set IDS portfloodthreshold`

4.3.2.0.31 FIREWALL SET IDS SCANPERIOD

Syntax `FIREWALL SET IDS SCANPERIOD <DURATION>`

Description This command allows you to set the time limit during which scanning type traffic (such as closed TCP port reviving SYN/ACK, FIN or RST) is counted. If the number of scanning packets counted within the specified duration is greater than the threshold set by FIREWALL SET IDS SCANTHRESHOLD, the suspected attacker is blocked for the time limit specified in the command FIREWALL SET IDS SCANATTACKBLOCK.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
duration	The length of time (in seconds) that scanning type traffic is counted for.	60 (seconds)

Example --> firewall set IDS scanperiod 90

See also `security set IDS scanperiod`

4.3.2.0.32 FIREWALL SET IDS SCANTHRESHOLD

Syntax `FIREWALL SET IDS SCANTHRESHOLD <MAX>`

Description This command allows you to set the maximum number of scanning packets that can be received before a port scan is detected. If the number of scanning packets counted within the time duration set by the command FIREWALL SET IDS SCANPERIOD is greater than the maximum value set here, the suspected attacker is blocked for the time limit specified in the command FIREWALL SET IDS SCANATTACKBLOCK.

For example, using the default settings, if more than 5 scanning packets are received per second for a 60 second duration, the attacker is blocked.

Note: This command is nothing but an alias of the corresponding "security set IDS" command

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
max	Maximum number of scanning packets that can be received before a port scan attack is detected.	5 (per second)

Example --> firewall set IDS scanthreshold 8

See also `security set IDS scanthreshold`

4.3.2.0.33 FIREWALL SHOW IDS

Syntax `FIREWALL SHOW IDS`

Description This command displays the following information about IDS settings:

- IDS enabled status (true or false)
- Blacklist status (true or false)

- Use Victim Protection status (true or false)
- DOS attack block duration (in seconds)
- Scan attack block duration (in seconds)
- Victim protection block duration (in seconds)
- Maximum TCP open handshaking count allowed (per second)
- Maximum ping count allowed (per second)
- Maximum ICMP count allowed (per second)

Example --> firewall show IDS

```
Firewall IDS:

                        IDS Enabled: false
                      Use Blacklist: false
                Use Victim Protection: false
             Dos Attack Block Duration: 1800
           Scan Attack Block Duration: 86400
     Malicious Attack Block Duration: 86400
   Victim Protection Block Duration: 600
           Scan Detection Threshold: 5
              Scan Detection Period: 10
     Port Flood Detection Threshold: 10
     Host Flood Detection Threshold: 20
                 FloodDetectPeriod : 10
     Max TCP Open Handshaking Count: 5
                    Max PING Count: 15
                    Max ICMP Count: 100
```

See also `security show IDS`

4.4 Network address translation - NAT

4.4.1 Overview

Basic NAT is a router function (described in *RFC 1631*) that determines how to translate network IP addresses. As data packets are received on the device's interfaces, data in their protocol headers is compared to criteria established in NAT rules through global pools and reserved mappings. The criteria includes ranges of source or destination addresses. If the packet meets the criteria of one of the rules, the packet header undergoes the translation specified by the mapping and the revised packet is forwarded. If the packet does not meet the criteria, it is discarded. ISOS supports both *static* and *dynamic* versions of NAT:

- *static* NAT: defines a fixed address translation from the internal network to the external network
- *dynamic* NAT: translates from a pool of local IP addresses to a pool of global IP addresses

NAT provides a mechanism for reducing the need for globally unique IP addresses. It allows you to use addresses that are not globally unique on your internal network and translate them to a single globally unique external address

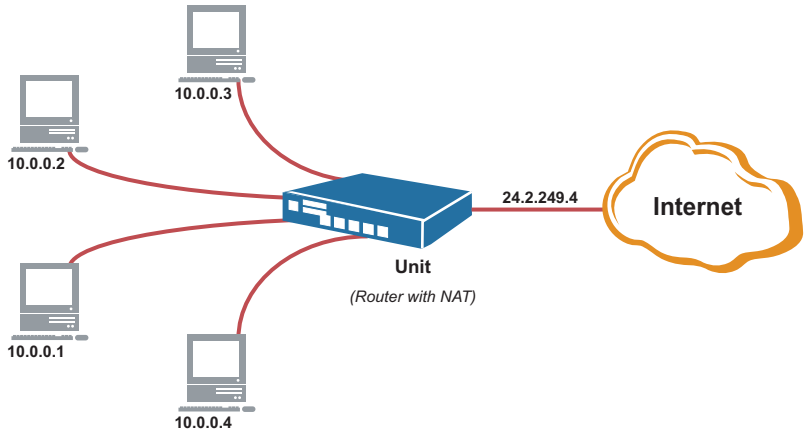


FIGURE 4-3 Address Conservation Using NAT

4.4.2 NAT support on AT-iMG Models

AT-iMG Models NAT module is designed to provide the following features:

- Global IP address pools
- Reserved mappings
- Application level gateways (algs)

NAT services are available between ***External security interface*** and ***Internal Security interfaces***.

In order to access NAT services, the NAT module must be enabled between a a pair of interfaces by using the NAT ENABLE command and assigning an arbitrary name to this relationship.

*Note: Before enabling NAT, the **Security** module must be already enabled using SECURITY ENABLE command.*

See XREF_HERE**Security** section for details regarding security interfaces.

Global IP Address Pools

A Global Address Pool is a pool of addresses seen from the external network. By default, each external interface creates a Global Address Pool with a single address – the address assigned to that interface.

For outbound sessions, an address is picked from a pool by hashing the source IP address for a pool index and then hashing again for an address index. For inbound sessions to make use of the global pool, it is necessary to create a reserved mapping. See below for more information on reserved mappings.

4.4.2.1 Reserved mappings

Reserved mapping is used to support NAT traversal.

NAT traversal is a mechanism that makes a service (listening port) on an internal computer accessible to external computers. NAT traversal operates by having the NAT listen for incoming messages on a selected port on its external interface. When the NAT receives a message, it uses its internal interface to forward the packet to the ***same port number*** on a selected internal computer (And any responses from the internal computer are forwarded to the requesting external computer).

Reserved mappings can also be used so that different internal hosts can share a global address by mapping different ports to different hosts.

For example, Host A is an FTP server and Host B is a Web server.

By choosing a particular IP address in the global address pool, and mapping the FTP port on this address to the FTP port on Host A and the HTTP port on the global address to the HTTP port on Host B, both internal hosts can share the same global address.

To add a reserved mapping rule to an existing NAT relation, use NAT ADD RESVMAP INTERFACE command.

With this command it is possible set a mapping rule based on port number or protocol number.

Setting the protocol number to 255(0xFF) means that the mapping will apply to all protocols. Setting the port number to 65535(0xFFFF) for TCP or UDP protocols means that the mapping will apply to all port numbers for that protocol.

4.4.2.2 Application level gateways (ALGs)

Some applications embed address and/or port information in the payload of the packet.

The most notorious of these is FTP. For most applications, it is sufficient to create a trigger with address replacement enabled. However, there are three applications for which a specific ALG is provided: ***FTP, NetBIOS*** and ***DNS***.

4.4.3 Interactions of NAT and other security features

4.4.3.1 Firewall filters and reserved mappings.

So far, the NAT reserved mappings have been considered independently of the firewall.

If the firewall is not enabled, then all that is required to enable NAT to allow in TCP sessions to a certain port number is to create a reserved mapping for that particular TCP port number.

However, if the firewall is enabled, there is a matter of precedence to consider if reserved mapping has been created for a particular TCP port but the firewall is not configured to allow in TCP data for that port.

In this case the blocking by the firewall will take precedence.

So, when the firewall has been enabled, care must be taken to ensure that when NAT reserved mapping are created, the firewall is also configured to allow in the traffic for which the reserve mapping is defined.

4.4.3.2 NAT and dynamic port opening

The description of ***Dynamic Port Opening*** (see Security section) discussed that feature in the context of the firewall – i.e. the ***Dynamic Port Opening*** feature was presented as being required to allow secondary sessions in through the firewall.

It should be noted that, by default, incoming sessions are not allowed through by NAT either. So, if NAT is enabled, even if the firewall is not enabled, then if you wish to be able to access services that involve incoming secondary sessions, then you will need to create ***Dynamic Port Opening*** definitions for those services.

So, for example, if you have NAT enabled on the router, and wish for users on the LAN to be able to successfully access external ***RealServers***, it will be necessary to create a ***Dynamic Port Opening*** definition.

4.4.4 NAT and secondary IP addresses

NAT services work also with secondary IP addresses.

In this case it's necessary create a secondary IP address using IP INTERFACE ADD SECONDARYIPADDRESS command and then create a security interface based on this secondary IP interface.

Then a global pool must be added and a reserved mapping configured. If using PPPoE encapsulation, secondary IP addresses in the global pool must be on a separate subnet. If the secondary IP addresses are on the same subnet as the external IP address, the addresses are not visible to the external network.

4.4.5 NAT command reference

This section describes the commands available on AT-iMG Models to enable, configure and manage NAT module.

4.4.5.1 NAT CLI commands

The table below lists the NAT commands provided by the CLI:

TABLE 4-7 NAT CLI Commands and Product Category

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
NAT ENABLE	X	X	X	X	X	X	X	X	X
NAT DISABLE	X	X	X	X	X	X	X	X	X
NAT ADD GLOBALPOOL	X	X	X	X	X	X	X	X	X
NAT ADD GLOBALPOOL	X	X	X	X	X	X	X	X	X
NAT CLEAR GLOBALPOOLS	X	X	X	X	X	X	X	X	X
NAT DELETE GLOBALPOOL	X	X	X	X	X	X	X	X	X
NAT IKETRANSLATION	X	X	X	X	X	X	X	X	X
NAT IKETRANSLATION	X	X	X	X	X	X	X	X	X
NAT LIST GLOBALPOOLS	X	X	X	X	X	X	X	X	X
NAT SHOW GLOBALPOOL	X	X	X	X	X	X	X	X	X
NAT ADD RESVMAP GLOBALIP TCP|UDP|BOTH	X	X	X	X	X	X	X	X	X
NAT ADD RESVMAP GLOBALIP	X	X	X	X	X	X	X	X	X
NAT ADD RESVMAP INTERFACENAME TCP|UDP|BOTH	X	X	X	X	X	X	X	X	X
NAT ADD RESVMAP INTERFACENAME	X	X	X	X	X	X	X	X	X
NAT CLEAR RESVMAPS	X	X	X	X	X	X	X	X	X
NAT DELETE RESVMAP	X	X	X	X	X	X	X	X	X
NAT DELETE RESVMAP	X	X	X	X	X	X	X	X	X
NAT SET RESVMAPS ENABLE|DISABLE	X	X	X	X	X	X	X	X	X
NAT SET RESVMAPS SRCIP	X	X	X	X	X	X	X	X	X
NAT SHOW RESVMAP	X	X	X	X	X	X	X	X	X
NAT STATUS	X	X	X	X	X	X	X	X	X

4.4.5.1.1 NAT ENABLE

Syntax `NAT ENABLE <name> <interfacename> {INTERNAL|DMZ}`

Description This command enables NAT between an existing security interface and a network interface type. NAT is enabled between the security interface and all the interfaces that belong to the chosen network interface type.

*Note: You must enable the **Security** package using the command SECURITY ENABLE if you want to use the **NAT** module to configure security for your system.*

An interface is either an inside or outside interface. The network attached to an inside interface needs to be protected from the network attached to an outside interface. For example, the network attached to an internal interface (inside) needs to be protected from the network attached to a DMZ (outside). Also, you can only enable ***NAT*** between two different interface types. For example, if interfacename is an external interface type, you can enable ***NAT*** between the interfacename and the internal or the DMZ interface type, but not the external interface type. The following interface combinations are the only ones that you can use:

- External (outside) and internal (inside)
- External (outside) and dmz (inside)
- Dmz (outside) and internal (inside)

The existing security interface must be an outside interface. ***NAT*** translates packets between the outside interface and the inside interface type. In this way, the IP address of a host on a network attached to an inside interface is hidden from a host on a network attached to an outside interface.

If you want to map an outside interface to an individual host on an inside interface type, you can use the command NAT ADD RESVMAP INTERFACENAME.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a NAT object enabled between a security interface and an interface type. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interface-name	The name of an existing security interface (external or DMZ) that was added to the Security package using the SECURITY ADD INTERFACE command. To display security interfaces, use the security list interfaces command.	N/A

Option	Description	Default Value
internal	Allows NAT to be enabled/disabled between the interfacename and all interfaces that belong to the internal interface type.	N/A
dmz	Allows NAT to be enabled/disabled between the interfacename and all interfaces that belong to the DMZ interface type. The interfacename must be an external interface type.	N/A

Example --> nat enable nat1 extinterface internal

See also
```
NAT DISABLE
NAT STATUS
SECURITY LIST INTERFACES
SECURITY ADD INTERFACE
NAT ADD RESVMAP INTERFACENAME
```

4.4.5.1.2 NAT DISABLE

Syntax
```
NAT DISABLE <name>
```

Description This command disables a NAT object that was previously enabled between an existing security interface and a network interface type using the nat enable command. NAT is disabled between the security interface and all the interfaces that belong to the chosen interface type.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	The name of an existing NAT object created between a security interface and an interface type using the NAT ENABLE command. To display enabled NAT objects, use the NAT STATUS command.	N/A

Example --> nat disable nat1

See also
```
nat enable
nat status
```

4.4.5.1.3 NAT ADD GLOBALPOOL

Syntax
```
NAT ADD GLOBALPOOL <name> <interfacename> {INTERNAL|DMZ}
<ipaddress> {SUBNETMASK <mask>|ENDADDRESS <address>}
```

Description The NAT ENABLE COMMAND creates an IP address for the outside security interface; however, you may want to use more than one outside IP address. For example, if your ISP provides multiple IP addresses, you might want to map an outside address to an inside interface that is your web server, and map another outside address to an inside interface that is your mail server.

*Note: Before you can add a **Global Address Pool**, you must enable a NAT object using the command NAT ENABLE*

This command creates a pool of outside network addresses. A ***Network Address Pool*** is a range of IP addresses that is visible outside your network. NAT translates packets between the outside addresses and the inside interfaces that each address is mapped to.

There are two ways to specify a range of IP addresses:

- Specify the interfacename IP address and a subnet mask address
- Specify the interfacename IP address that represents the first address in the range, then specify the last address in the range

If you want to map IP addresses to individual hosts on an inside interface type, you can use the command NAT ADD RESVMAP GLOBALIP.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a global network address or pool of addresses. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
inter-face-name	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the nat enable command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A
internal	Maps the IP addresses to the internal interface type inside the network.	N/A
dmz	Maps the global addresses to the DMZ interface type inside the network.	N/A
ipad-dress	The IP address of the interfacename that is visible outside the network.	N/A

Option	Description	Default Value
mask	The subnet mask of the network IP address.	N/A
endad-dress	The last IP address in the range of addresses that make up the global address pool.	N/A

Example Example 1

This example creates a network address pool that allows NAT to translate packets between the external interface and the DMZ interface type.

First, NAT is enabled between the external interface and the DMZ interface type:

--> nat enable n1 extinterface dmz

Then the IP address and subnet mask is created:

--> nat add globalpool gp1 extinterface dmz 192.168.102.3 subnetmask 255.255.255.0

Example 2

This example creates a network address pool that allows NAT to translate packets between the external interface and the internal interface type.

First NAT is enabled between the external interface and the internal interface type:

--> nat enable n2 extinterface internal

Then the address range is created:

--> nat add globalpool gp2 extinterface internal 192.168.103.2 endaddress 192.168.103.50

See also
```
NAT ENABLE
NAT STATUS
SECURITY LIST INTERFACES
```

Note: Once you have created an address pool, packets received on a specific IP address can be mapped to individual hosts inside the network. See NAT ADD RESVMAP GLOBALIP.

4.4.5.1.4 NAT CLEAR GLOBALPOOLS

Syntax `NAT CLEAR GLOBALPOOLS <interfacename>`

Description This command deletes all address pools that were added to a specific outside interface using the nat add globalpool command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
inter-face-name	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security inter-faces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat clear globalpools extinterface

See also `nat add globalpool`
`security list interfaces`

4.4.5.1.5 NAT DELETE GLOBALPOOL

Syntax `NAT DELETE GLOBALPOOL <name> <interfacename>`

Description This command deletes a single address pool that was added to a specific outside interface using the nat add globalpool command.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing global IP address. To display global IP addresses, use the NAT LIST GLOBALPOOLS command.	N/A
inter-face-name	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or inter-nal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat delete globalpool gp1 extinterface

See also `NAT ADD GLOBALPOOL`
`NAT LIST GLOBALPOOLS`
`SECURITY LIST INTERFACES`

4.4.5.1.6 NAT IKETRANSLATION

Syntax `NAT IKETRANSLATION {cookies | ports}`

Description This command supports NAT IPSec traversal. It allows you to specify how Internet Key Exchange (IKE) packets are translated.

IKE establishes a shared security policy and authenticates keys for services that require keys, such as IPSec. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
cookies	Source port will not be translated for IKE packets; IKE cookies are used to identify IKE sessions.	Ports
ports	Source port will be translated for IKE packets.	

Example --> nat iketranslation cookies

4.4.5.1.7 NAT LIST GLOBALPOOLS

Syntax `NAT LIST GLOBALPOOLS <interfacename>`

Description This command lists the following NAT address pool information for a specific outside interface:

- Address pool identification number
- Address pool name
- Type of inside interface (internal or DMZ)
- Subnet status (true or false)
- IP address - the outside network IP address or the first address in the range of network pool addresses
- Mask/End Address - the outside subnet mask of the outside network IP address or the last address in the range of network pool addresses

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
interface-name	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat list globalpools extinterface

```
NAT global address pool:
  ID |  Name  |   Type   | Subnet |   IP address  | Mask/End Address
-------------------------------------------------------------------------
   1 | gp1    | dmz      | true   | 192.168.102.3 | 255.255.255.0
   2 | g2     | internal | false  | 192.168.103.2 | 192.168.103.50
-------------------------------------------------------------------------
```

See also SECURITY LIST INTERFACES
NAT SHOW GLOBALPOOL

4.4.5.1.8 NAT SHOW GLOBALPOOL

Syntax `NAT SHOW GLOBALPOOL <name> <interfacename>`

Description This command displays information about a single network address pool that has been added to an outside interface:

- Type of inside interface (internal or DMZ)
- Subnet configuration status (true if the network pool was set using a subnet mask, false if it was set using a range of IP addresses)
- IP address - the outside network IP address or the first address in the range of addresses
- Subnet Mask or End Address - the subnet mask of the outside network IP address or the last address in the range of addresses

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing global IP address. To display global IP addresses, use the NAT LIST GLOBALPOOLS command.	N/A
interface-name	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat show globalpool gpl extinterface

```
NAT global address pool: gp1
            Interface type: dmz
      Subnet configuration: true
                IP address: 192.168.102.3
Subnet mask or End Address: 255.255.255.0
```

See also NAT LIST GLOBALPOOLS
SECURITY LIST INTERFACES

4.4.5.1.9 NAT ADD RESVMAP GLOBALIP TCP|UDP|BOTH

Syntax `NAT ADD RESVMAP <name> GLOBALIP <interfacename> <globalip> <internalip> {TCP|UDP|BOTH} <portno> [<2ndportno> [<localportno> [<2ndlocalportno>]]]`

Description This command maps an IP address from a global pool (created using the NAT ADD GLOBALPOOL command) to an individual IP address inside the network. NAT translates packets between the outside IP address and the individual host based on the transport information (TCP or UDP or both) given in this command.

Note: Before you can add reserved mapping, you must enable a NAT object using the command NAT ENABLE.

You can define reserved mappings for a range of ports and/or translating port numbers.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a reserved mapping configuration. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A
globalip	The IP address of an outside interface set using the NAT ADD GLOBALPOOL command.	N/A
internalip	The IP address of an individual host inside the network (internal or DMZ interface type).	N/A
portno	Either a single TCP or UDP port number that you want to use in your reserved mapping configuration, or the first port number in the range of ports.	N/A
2ndportno	The second TCP or UDP port number in the range that started with the port specified in portno.	N/A
localportno	Either a single internal TCP or UDP port number or the first port number in the range of external ports.	N/A
2ndlocalportno	The second internal TCP or UDP port number in the range of external ports to be used if you have specified a localportno.	N/A

Example --> nat add resvmap rm1 globalip extinterface 192.168.68.68 10.10.10.10 tcp 25

See also NAT ENABLE
NAT LIST GLOBALPOOLS
NAT STATUS
SECURITY LIST INTERFACES

4.4.5.1.10 NAT ADD RESVMAP GLOBALIP

Syntax `NAT ADD RESVMAP <name> GLOBALIP <interfacename> <globalip> <internalip> {ICMP|IGMP|IP|EGP|RSVP|OSPF|IPIP|ALLGRE|Protocol<number>}`

Description This command maps an IP address from a global pool (created using the nat add globalpool command) to an individual IP address inside the network. NAT translates packets

between the outside IP address and the individual host based on the transport information given in this command.

Note: Before you can add reserved mapping, you must enable a NAT object using the command NAT ENABLE

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a reserved mapping configuration. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interface-name	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use THE SECURITY LIST INTERFACES command.	N/A
globalip	The IP address of an outside interface set using the NAT ADD GLOBALPOOL command.	N/A
internalip	The IP address of an individual host inside the network (internal or DMZ interface type).	N/A
icmp	***Internet Control Message Protocol*** (ICMP) is set as the transport type. ICMP messages are used for out-of-band messages related to network operation or mis-operation. See http://www.ietf.org/rfc/rfc0792.txt.	N/A
igmp	***Internet Group Management Protocol*** (IGMP) is set as the transport type. Allows Internet hosts to participate in multicasting. See http://www.ietf.org/rfc/rfc1112.txt.	N/A
ip	***Internetwork Protocol*** (IP). Provides all of the Internet's data transport services. http://www.ietf.org/rfc/rfc791.txt and http://www.ietf.org/rfc/rfc919.txt.	N/A
egp	***Exterior Gateway Protocol*** (EGP). Protocol for exchanging routing information between autonomous systems. See http://www.ietf.org/rfc/rfc904.txt.	N/A
gre	***Generic Routing Encapsulation*** (GRE).Tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocol packet types inside IP Tunnel See http://www.ietf.org/rfc/rfc2784.txt.	N/A

Option	Description	Default Value
rsvp	***Resource Reservation Protocol*** (RSVP) is set as the transport type. Supports the reservation of resources across an IP network. See http://www.ietf.org/rfc/rfc2205.txt.	N/A
ospf	***Open Shortest Path First*** (OSPF) is set as the transport type. A link-state routing protocol. See http://www.ietf.org/rfc/rfc1583.	N/A
ipip	***IP-within-IP Encapsulation Protocol***. Encapsulates an IP datagram within a datagram. See http://www.ietf.org/rfc/rfc2896.txt.	N/A
all	All traffic is translated between the global IP address and the specified inside address that it is mapped to.	N/A
protocol <number>	Allows you to identify a protocol by its assigned number. For details of assigned numbers, see *RFC 1700*.	N/A

Example --> nat add resvmap rm1 globalip extinterface 192.168.68.68 10.10.10.10 ip

See also
```
NAT ENABLE
NAT LIST GLOBALPOOLS
NAT STATUS
SECURITY LIST INTERFACES
```

4.4.5.1.11 NAT ADD RESVMAP INTERFACENAME TCP|UDP|BOTH

Syntax
```
NAT ADD RESVMAP <name> INTERFACENAME <interfacename> <internalip> {TCP|UDP|BOTH} <portno> [<2ndportno> [<localportno> [<2ndlocalportno>]]]
```

Description This command maps an outside IP security interface (enabled as a NAT object using the nat enable command) to an individual IP address inside the network. NAT translates packets between the outside IP address and an individual host based on the transport information (TCP or UDP or both) given in this command. A range of external ports can be translated to a single local port if required.

Note: Before you can add reserved mapping, you must enable a NAT object using the command NAT ENABLE

You can define reserved mappings for a range of ports and/or translating port numbers.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a reserved mapping configuration. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interface name	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A
internalip	The IP address of an individual host inside the network (internal or DMZ interface type).	N/A
portno	Either a single TCP or UDP port number that you want to use in your reserved mapping configuration, or the first port number in the range of ports.	N/A
2ndportno	The second TCP or UDP port number in the range that started with the port specified in portno.	N/A
localportno	Either a single internal TCP or UDP port number or the first port number in the range of external ports.	N/A
2ndlocalportno	The second internal TCP or UDP port number in the range of external ports to be used if you have specified a localportno.	N/A

Example The example below forwards TCP port 25 requests on the WAN interface to 10.10.10.10 port 80:

--> nat add resvmap rm1 interfacename WAN 10.10.10.10 tcp 25

The example below forwards TCP port 80 to 90 requests on the WAN interface to 10.10.10.10 ports 8080 to 8090. Note that the first range must be the same size as the second range:

--> nat add resvmap rm2 interfacename WAN 10.10.10.10 tcp 80 90 8080 8090

See also `NAT ENABLE`
`SECURITY LIST INTERFACES`

4.4.5.1.12 NAT ADD RESVMAP INTERFACENAME

Syntax `NAT ADD RESVMAP <name> INTERFACENAME <interfacename> <internalip> {ICMP|IGMP|IP|EGP|RSVP|OSPF|IPIP|ALL|GRE|Protocol<number> }`

Description This command maps an outside IP security interface (enabled as a NAT object using the NAT ENABLE command) to an individual IP address inside the network. NAT translates packets between the outside IP address and the individual host based on the transport information given in this command.

Note: Before you can add reserved mapping, you must enable a NAT object using the command NAT ENABLE

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a reserved mapping configuration. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A
internalip	The IP address of an individual host inside the network (internal or DMZ interface type).	N/A
icmp	***Internet Control Message Protocol*** (ICMP) is set as the transport type. ICMP messages are used for out-of-band messages related to network operation or mis-operation. See http://www.ietf.org/rfc/rfc0792.txt.	N/A
igmp	***Internet Group Management Protocol*** (IGMP) is set as the transport type. Allows Internet hosts to participate in multicasting. See http://www.ietf.org/rfc/rfc1112.txt.	N/A
ip	***Internetwork Protocol*** (IP). Provides all of the Internet's data transport services. http://www.ietf.org/rfc/rfc791.txt and http://www.ietf.org/rfc/rfc919.txt.	N/A
egp	***Exterior Gateway Protocol*** (EGP). Protocol for exchanging routing information between autonomous systems. See http://www.ietf.org/rfc/rfc904.txt.	N/A

Option	Description	Default Value
gre	***Generic Routing Encapsulation*** (GRE).Tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocol packet types inside IP Tunnel See http://www.ietf.org/rfc/rfc2784.txt.	N/A
rsvp	***Resource Reservation Protocol*** (RSVP) is set as the transport type. Supports the reservation of resources across an IP network. See http://www.ietf.org/rfc/rfc2205.txt.	N/A
ospf	***Open Shortest Path First*** (OSPF) is set as the transport type. A link-state routing protocol. See http://www.ietf.org/rfc/rfc1583.	N/A
ipip	***IP-within-IP Encapsulation Protocol***. Encapsulates an IP datagram within a datagram. See http://www.ietf.org/rfc/rfc2896.txt.	N/A
all	Traffic is translated between the global IP address and the inside address that it is mapped to.	N/A
protocol <number>	Allows you to identify a protocol by its assigned number. For details of assigned numbers, see *RFC 1700*.	N/A

Example --> nat add resvmap rm1 interfacename extinterface 10.10.10.10 tcp 25

See also `NAT ENABLE`
`SECURITY LIST INTERFACES`

4.4.5.1.13 NAT CLEAR RESVMAPS

Syntax `NAT CLEAR RESVMAPS <interfacename>`

Description This command deletes all NAT reserved mappings that were added to an outside security interface using the nat add resvmap commands.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat clear resvmaps extinterface

See also NAT DELETE RESVMAP
SECURITY LIST INTERFACES

4.4.5.1.14 NAT DELETE RESVMAP

Syntax NAT DELETE RESVMAP <name> <interfacename>

Description This command deletes a single NAT reserved mapping that was added to an outside security interface using the nat add resvmap commands.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing global IP address. To display global IP addresses, use the nat list resvmaps command.	N/A
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat delete resvmap rm1 extinterface

See also nat enable
nat list resvmaps
security list interfaces

4.4.5.1.15 NAT DELETE RESVMAP

Syntax NAT DELETE RESVMAP <name> <interfacename>

Description This command deletes a single NAT reserved mapping that was added to an outside security interface using the nat add resvmap commands.

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing global IP address. To display global IP addresses, use the nat list resvmaps command.	N/A
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat delete resvmap rm1 extinterface

See also
```
nat enable
nat list resvmaps
security list interfaces
```

4.4.5.1.16 NAT SET RESVMAPS ENABLE|DISABLE

Syntax `NAT SET RESVMAPS <name> <interfacename> {enable|disable}`

Description This command enables or disables an existing (created using nat add resvmap command) NAT reserve map rule

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a reserved mapping configuration. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Option	Description	Default Value
enable|disable	Enables/Disables an existing rule to be used/not to be used to match against inbound packets for translations.	N/A

Example --> nat set resvmap rm1 extinterface enable

See also `nat add resvmap interfacename`

4.4.5.1.17 NAT SET RESVMAPS SRCIP

Syntax `NAT SET RESVMAPS <name> <interfacename> srcpip {range <startaddr> <endaddr>| <subnet subnetaddr> <subnet subnetmask>}`

Description This command sets the source IP, including IP range, subnet IP, and subnet mask, of a NAT reserve map rule

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies a reserved mapping configuration. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A
startaddr	Starting IP address of the range to be configured	N/A
endaddr	End IP address of the range to be configured	N/A
subnet subnetaddr	Subnet address of the subnet to be configured	N/A
subnet mask	Subnet mask of the subnet to be configured.	N/A

Example --> `nat set resvmap rm1 WAN srcip range 172.26.1.1 172.26.1.10`

Example `--> nat set resvmap rm1 WAN srcip subnet 172.26.0.0 255.255.0.0`

See also `nat add resvmap interfacename`

4.4.5.1.18 NAT SHOW RESVMAP

Syntax `NAT SHOW RESVMAP <name> <interfacename>`

Description This command displays the following information about a single reserved mapping configuration that has been added to an outside security interface:

- Global IP address
- Internal IP address
- Transport type
- Port number

Options The following table gives the range of values for each option that can be specified with this command and a Default Value (if applicable).

Option	Description	Default Value
name	An existing global pool. To display global pool names, use the NAT LIST RESVMAPS command.	N/A
interfacename	The name of an existing security interface (external or DMZ) created and connected to an inside interface (DMZ or internal) using the NAT ENABLE command. To display security interfaces, use the SECURITY LIST INTERFACES command.	N/A

Example --> nat show resvmap rm1 extinterface

```
NAT reserved mapping: rm1
        Global IP address: 192.168.103.15
      Internal IP address: 20.20.20.20
           Transport type: tcp
              Port number: 25
```

See also `NAT LIST RESVMAPS`
`SECURITY LIST INTERFACES`

4.4.5.1.19 NAT STATUS

Syntax `nat status`

Description This command lists the outside security interfaces and inside interface types that NAT is currently enabled between. It displays the following information:

- NAT object identification number

- NAT object name
- Outside security interface name
- Inside interface type

Example --> nat status

```
NAT enabled on:
  ID |    Name    | Interface  |  Type
-----------------------------------------
   1 | n2         | ip2        | internal
   2 | n1         | if1        | internal
-----------------------------------------
```

See also `nat enable`

5. System Administration

5.1 Dynamic Host Configuration Protocol

The ***Dynamic Host Configuration Protocol*** (DHCP) is defined in RFC 1541 and provides a mechanism for passing configuration information to hosts on a TCP/IP network.

DHCP is based on the ***Bootstrap Protocol*** (BOOTP) defined in RFC 1542, but adds automatic allocation of reusable network addresses and additional configuration options.

DHCP is based on a client–server model, where the server is the host that allocates network addresses and initialization parameters, and the client is the host that requests these parameters from the server.

There are a number of parameters that a DHCP server can supply to clients in addition to assigning IP addresses. They can supply addresses of DNS server, WINS Server, Cookie server etc.… Also, they can supply the gateway address for the LAN.

DHCP supports three mechanisms for IP address allocation

- In the ***automatic allocation*** mechanism, DHCP assigns a permanent IP address to a host.
- In the ***dynamic allocation*** mechanism, DHCP assigns an IP address to a host for a limited period of time, or until the host explicitly relinquishes the address.
- In the ***manual allocation*** mechanism, the network administrator assigns a host's IP address, and DHCP is used simply to convey the assigned address to the host. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.

Dynamic allocation is the only one of the three mechanisms that allows automatic reuse of an address that is no longer needed by the host to which it was assigned. ***Dynamic allocation*** is particularly useful for assigning an address to a host that will be connected to the network only temporarily, or for sharing a limited pool of IP addresses among a group of hosts that do not need permanent IP addresses.

Dynamic allocation may also be a good choice for assigning an IP address to a new host being permanently connected to a network where IP addresses are sufficiently scarce that it is important to reclaim them when old hosts are retired.

5.1.1 DHCP support

The gateway devices are able to act both as DHCP server and as DHCP client.

Typically, DHCP server features are activated on the internal network to assign IP address to hosts connected to the internal interfaces. The DHCP client function, instead, is used on the external interface to get IP addresses from the ISP.

The devices also support DHCP relay functionality. In this case the intelligent Multiservice Gateway picks up DHCP requests sent by hosts connected to the internal interfaces, and forwards their requests to an external DHCP server and then routes back to the hosts the replies that are received from the server.

5.1.2 DHCP server

The DHCP protocol allows a host that is unknown to the network administrator to be automatically assigned a new IP address out of a pool of IP addresses for its network. In order for this to work, the network administrator allocates address pools for each available subnet and enters them into the ***dhcpd.conf*** file.

On start-up, the DHCP server software reads the ***dhcpd.conf*** file and stores a list of available addresses on each subnet. When a client requests an address using the DHCP protocol, the server allocates an address for it.

Each client is assigned a lease, which expires after an amount of time chosen by the administrator (by default, 12 hours). Some time before the leases expire, the clients to which leases are assigned are expected to renew them in order to continue to use the addresses. Once a lease has expired, the client to which that lease was assigned is no longer permitted to use the leased IP address and must resort back to the DHCPDISCOVER mechanism (see RFC 2131) to request a new lease.

In order to keep track of leases across system reboots and server restarts, the server keeps a list of leases it has assigned in the ***dhcpd.leases*** file (stored in ISFS).

Before a lease is granted to a host, it records the lease in this file. Upon start-up, after reading the ***dhcpd.conf*** file, the DHCP server reads the ***dhcpd.leases*** file to gain information about which leases had been assigned before reboot.

New leases are appended to the end of the lease file.

In order to prevent the file from becoming arbitrarily large, the server periodically creates a new ***dhcp.leases*** file from its lease database in memory.

If the system crashes in the middle of this process, only the lease file present in flash memory can be restored. This gives a window of vulnerability whereby leases may be lost.

This server also provides BOOTP support. Unlike DHCP, the BOOTP protocol does not provide a protocol for recovering dynamically assigned addresses once they are no longer needed. It is still possible to dynamically assign addresses to BOOTP clients, but some administrative process for reclaiming addresses is required. By default, leases are granted to BOOTP clients in perpetuity, although the network administrator may set an earlier cut-off date or a shorter lease length for BOOTP leases if that makes sense.

5.1.2.1 Example

This paragraph provides a guide to configuring the DHCP server using commands available on the CLI.

Let's assuming that in the system there has been defined an internal interface (where the DHCP Server module will run) with the following IP address and netmask:

```
192.168.219.1 255.255.255.
```

The following DHCP server configuration will create a range of 10 available IP addresses in the 19.168.219.0 subnet:

```
dhcpserver add subnet mysubnet 192.168.219.0 255.255.255.0
192.168.219.10 192.168.219.20
dhcpserver set subnet mysubnet defaultleasetime 1800
dhcpserver set subnet mysubnet maxleasetime 86000
dhcpserver subnet mysubnet add option domain-name-servers
192.168.220.30
dhcpserver subnet mysubnet add option routers 192.168.221.40
dhcpserver subnet mysubnet add option irc-server 10.5.7.20
dhcpserver subnet mysubnet add option auto-configure 1
```

- Default lease time and maximum lease time are set to 1800 seconds and 86000 seconds, respectively.
- Four DHCP options are configured, in addition to the usual IP address and subnet mask:
  - DNS server address of 192.168.220.30;
  - Default gateway address of 192.168.221.40;
  - IRC server address of 10.5.7.20;
  - And the ***auto-configure*** option, which will allow use of address auto-configuration by clients on the network.

Instead of specifying the ***domain-name-servers*** and ***routers*** options manually, the following commands could have been used which provide automatic values for these options:

```
dhcpserver set subnet mysubnet hostisdnsserver enabled
dhcpserver set subnet mysubnet hostisdefaultgateway enabled
```

This will result in the DHCP server taking the IP address of the IP interface it is running on, and supplying that address to DHCP clients as the DNS server and default gateway, respectively. This is especially useful in a deployment that utilizes the DNS relay on the residential gateway.

Note: Note that for DHCP clients using DHCPINFORM, the above declarations mean that the server would supply the given configuration options to any client that is on the 192.168.219.x subnet. This even includes clients that are not included in the available address ranges – this is sensible, since ideally the DHCP server should not have addresses available to give out that may already belong to hosts on the same subnet.

The CLI can also be used to define fixed host/IP address mappings. For example, the command:

```
dhcpserver add fixedhost myhost 192.168.219.5 00:20:2b:01:02:03
```

Will add a fixed mapping of the IP address 192.168.219.5 to a host whose ethernet MAC address is 00:20:2b:01:02:03.

Note: Note that fixed IP mappings cannot overlap with dynamic IP ranges on a subnet, and vice-versa (you will receive an error message if you try to do this).

Note: Note that you will still need to have a suitable subnet declaration – for example, a subnet 192.169.219.0 with netmask 255.255.255.0, as shown earlier. Any configuration options you define in this subnet will also be offered to every fixed host you have added which is also on the given subnet.

It is also possible to assign a maximum lease duration to fixed DHCP clients as follows:

```
dhcpserver set fixedhost myhost maxleasetime 7200
```

In this context, fixed lease duration would normally be used to allow DHCP clients to see changes in offered options quickly. The IP address itself is always guaranteed to be available for assignment to the specific host (unless there are other DHCP servers on the same network that are deliberately configured to conflict).

You might see the following message if you have ever turned off the DHCP server:

Note: Note the DHCP server is not currently enabled.

If you see this, issue the following command:

```
dhcpserver enable
```

The final step is to tell the system to update the DHCP server software with the new IP interface and configuration that has been defined. To do this, issue the following command:

```
dhcpserver update
```

Note: NO configuration changes that you have made on the DHCP server will take effect until you enter the DHCPSERVER UPDATE command.

5.1.3 DHCP client

A DHCP client uses the facilities of the IP stack to transmit and receive DHCP packets. This information is processed by the client and passed back to the IP stack to complete interface configuration for the lease duration.

A DHCP client is created on a given interface by using the IP SET INTERFACE command with the parameter DHCP enabled. After this, the IP settings are discovered for the interface (It's possible define one or more ***interfaceconfig*** rules to customize the option that must be requested).

This section describes how these settings are discovered.

Firstly, the interface is disabled for all non-DHCP traffic. This will reset the IP address and subnet mask of each nominated interface to 0.0.0.0.

The DHCP client learns its required configuration details via a DHCPDISCOVER request.

If configuration details are not successfully obtained using DHCP, the DHCP client will retry indefinitely in order to learn them, as described in RFC2131 (unless the interface is disabled). Retry characteristics can be defined using DHCPCLIENT SET RETRY command.

Once the DHCP client has accepted a suitable configuration for the interface, it has to configure the IP stack appropriately. This involves allocating the new IP address to the interface and configuring the subnet for the interface.

Addresses allocated by DHCP expire after the specified lease time runs out. If this happens, the DHCP client must relearn its configuration by repeating the process described above. The client will attempt to initiate renewal of a held lease well before it is due to expire (approximately half way through the total duration of the lease). This avoids the problem of an active interface being unexpectedly disabled and dropping normal IP traffic.

The DHCP client on the AT-RG624/634 DHCP conforms to most of the specification given in RFC2131. A subset of the DHCP options described in RFC2132 is supported.

The residential Gateway DHCP client accepts and makes use of the following information:

- IP address
- Subnet mask
- Default route (one only)
- Domain name servers (up to two can be usefully supported by DNS relay)
- Host name or DHCP-client-identifier. This option can be used to specify a client identifier in a host declaration, so that a DHCP server can find the host record by matching against the client identifier. This option can be useful when attempting to operate the DHCP client with a Microsoft DHCP server.

*Note: When attempting to use a DHCP client with a Microsoft DHCP server, then **send dhcpclient-identifier** is mandatory, and must be specifically set to the MAC address of the device upon which the client is running; otherwise DHCP will not work at all.*

5.1.3.1 Lease requirements and requests

The DHCP protocol allows the client to request that the server send it specific information, and not send it other information that it is not prepared to accept. The protocol also allows the client to reject offers from servers if they do not contain information the client needs, or if the information provided is not satisfactory.

Using the DHCPCLIENT INTERFACE CONFIG ADD REQUESTED OPTION command causes the client to request that any server responding to the client send the client its values for the specified options. Only the option names should be specified in the request statement - not option parameters.

Using the DHCPCLIENT INTERFACE CONFIG ADD REQUIRED OPTION command configures a list of options that must be sent in order for an offer to be accepted. Offers that do not contain ***all*** the listed options will be ignored.

Using the DHCPCLIENT INTERFACE CONFIG ADD SENT OPTION command causes the client to send the specified options to the server with the specified values. Options that are always sent in the DHCP protocol should not be specified here, except that the client can specify a ***requested-lease-time*** option other than the default requested lease time, which is two hours. The other obvious use for this statement is to send information to the server that will allow it to differentiate between this client and other clients or kinds of clients.

5.1.3.2 Support for AutoIP

The DHCP client supports also IP address auto-configuration, to be referred to as ***AutoIP*** in this manual. This includes support for RFC2563, which allows network administrators to configure DHCP servers to deny this auto-configuration capability to clients.

In summary, ***AutoIP*** will be engaged after a DHCP client fails to contact a DHCP server and cannot obtain a lease. A pseudo-random algorithm invents an IP address on the 169.254 subnet. Collisions are avoided by issuing ARP requests for the suggested IP address, abandoning the address if it is already active on the network.

Additionally, the suggested address will be abandoned if any other host on the network issues an ARP probe (i.e. the host issuing the ARP has source address 0.0.0.0) for that IP address.

Having auto-configured an IP address, the DHCP client will periodically check that it still cannot contact a DHCP server. If the client finds it can now obtain a legitimate lease from a DHCP server, this lease will supersede any auto-configured IP address.

To turn on the ***AutoIP*** feature use DHCPCLIENT SET INTERFACECONFIG AUTOIP ENABLED command

To prevent the DHCP client from using ***AutoIP***, USE DHCPCLIENT SET INTERFACECONFIG AUTOIP DISABLED command.

5.1.3.3 Additional DHCP client modes

There are two additional DHCP client modes for more fine control of how configuration parameters are accepted and propagated. The first mode allows you to choose how DNS servers are to be used; the second mode allows you to use parameters received on a DHCP client interface to automatically set up a DHCP server on another interface in the system.

5.1.3.4 Propagating DNS server information

You can tell the DHCP client what to do with received DNS server addresses. The pertinent attributes are ***giveDnsToRelay*** and ***giveDnsToClient***. As is evident from the parameter names, the effect of these settings is to cause the DHCP process to pass to the DNS relay and client processes the DNS server address(es) it has learnt, which they are then able to use for DNS queries.

By default, DNS server addresses are only given to the DNS relay, if present.

For example, to set this up via the CLI, the following command sequence can be used:

```
dhcpclient add interfaceconfig client1 ip0
dhcpclient interfaceconfig 1 add requested option domain-name-servers
dhcpclient set interfaceconfig client1 givednstorelay enabled
dhcpclient set interfaceconfig client1 givednstoclient enabled
```

5.1.3.5 Automatically setting up a DHCP server

It is possible to tell the DHCP client to use parameters it has obtained to automatically set up a DHCP server.

If you choose this mode, you must tell DHCP client how large an IP address lease pool you would like the new server to have, and which IP interface you want the new DHCP server to bind to.

If you do not supply any interface information, the DHCP client will try to place the DHCP server on the first LAN interface it finds (the DHCP client will regard an IP interface as being a LAN interface)

The new DHCP server's address pool will start one IP address after the IP address of the interface upon which the DHCP server has been set up. That is, if the DHCP client is configured to set up the DHCP server on an IP interface named ***uplink***, with address 192.168.219.2, the address range will commence from address 192.168.219.3.

At present, the new DHCP server will give out any DNS server addresses received by the DHCP client. It will then advertise its own host IP address as being the default gateway.

To set this up via the CLI, the following command sequence can be used:

```
dhcpclient add interfaceconfig client1 ip0
dhcpclient interfaceconfig 1 add requested option domain-name-servers
dhcpclient set interfaceconfig client dhcpserverpoolsize 30
dhcpclient set interfaceconfig client1 dhcpserverinterface uplink
```

5.1.3.6 Example

This paragraph provides a guide to setting up a DHCP client using commands available in the CLI.

Let's assume that the system has been configured with an interface named eth0. The first step is to enable the DHCP flag on this interface:

```
ip set interface eth0 dhcp enabled
```

DHCP client configuration is optional. You do not need to perform these steps unless you have special requirements, such as specifying whether the use of AutoIP is allowed, specific requirements for which options are to be negotiated from a DHCP server, or specific requirements about what to do with option values when they are received.

```
dhcpclient add interfaceconfig mycfg ip0
dhcpclient set interfaceconfig mycfg requestedleasetime 3600
dhcpclient set interfaceconfig mycfg clientid 00:20:2b:01:02:03
dhcpclient set interfaceconfig mycfg autoip enabled
dhcpclient set interfaceconfig mycfg givednstorelay enabled
dhcpclient interfaceconfig mycfg add requested option domain-name-
servers
dhcpclient interfaceconfig mycfg add required option routers
dhcpclient interfaceconfig mycfg add sent option host-name '"galapa-
gos"'
```

These commands create a new DHCP client interface configuration related to the IP interface you defined earlier. Let us consider, line by line, what the above configuration does:

- A lease time of one hour is requested.
- A client identifier of 00:20:2b:01:02:03 is specified.
- In the event of a DHCP server being unavailable, the DHCP client will automatically assign an address using ***AutoIP***.
- Any DNS server addresses received from a server will be passed to the DNS relay. (There is also an analogous option to pass the addresses to the DNS client).
- For this to occur, the DHCP client must request DNS server addresses from a server (maps onto the ***request*** directive).
- The DHCP client will insist that a default gateway parameter is present in any lease offer (maps onto the ***require*** directive).
- Finally, the DHCP client will send out ***galapagos*** as the value of the host name option – this can be used by some ISPs as part of a simple authentication process (maps onto the ***send*** directive).

The final step is to tell the Residential Gateway to update the DHCP client software with the new IP interface and configuration that has been defined. To do this, issue the following command:

```
dhcpclient update
```

Note: NO configuration changes that you have made on the DHCP client will take effect until you enter the DHCPCLIENT UPDATE command.

5.1.4 DHCP Relay

A DHCP relay uses the facilities of the IP stack to transmit and receive DHCP packets.

From a DHCP client's point of view, the relay acts as a de-facto DHCP server, and this operation is transparent. This is useful where a network administrator only wishes to have one DHCP server across several physical and logical sub-networks.

The relay works by forwarding all broadcasted client requests to one or more known DHCP servers.

Server replies are then either broadcast or unicast back to the client via the DHCP relay.

Note: Note DHCP Server and DHCP relay cannot coexist simultaneously

5.1.5 DHCP Server command reference

This section describes the commands available on gateway to enable, configure and manage DHCP Server module.

5.1.5.1 DHCP server CLI commands

The table below lists the ***DHCP server*** commands provided by the CLI:

TABLE 5-1 DHCP server CLI commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DHCPSERVER ADD USERS CLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER ADD VENDOR CLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER CLEAR CLASSES	X	X	X	X	X	X	X	X	X
DHCPSERVER DELETE CLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST CLASSES	X	X	X	X	X	X	X	X	X
DHCPSERVER SET USERS CLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SET VENDOR CLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SHOW CLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER CLASS ADD OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER CLASS CLEAR OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER CLASS DELETE OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER CLASS LIST OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER ADD EXCLUDE	X	X	X	X	X	X	X	X	X
DHCPSERVER CLEAR EXCLUDES	X	X	X	X	X	X	X	X	X
DHCPSERVER DELETE EXCLUDE	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST EXCLUDES	X	X	X	X	X	X	X	X	X
DHCPSERVER ADD INTERFACE	X	X	X	X	X	X	X	X	X
DHCPSERVER CLEAR INTERFACES	X	X	X	X	X	X	X	X	X
DHCPSERVER DELETE INTERFACE	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST INTERFACES	X	X	X	X	X	X	X	X	X
DHCPSERVER ADD FIXEDHOST	X	X	X	X	X	X	X	X	X
DHCPSERVER CLEAR FIXEDHOSTS	X	X	X	X	X	X	X	X	X
DHCPSERVER DELETE FIXEDHOST	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST FIXEDHOSTS	X	X	X	X	X	X	X	X	X

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DHCPSERVER SET FIXEDHOST IPADDRESS	X	X	X	X	X	X	X	X	X
DHCPSERVER SET FIXEDHOST DEFAULTLEASETIME	X	X	X	X	X	X	X	X	X
DHCPSERVER SET FIXEDHOST MACADDRESS	X	X	X	X	X	X	X	X	X
DHCPSERVER SET FIXEDHOST MAXLEASETIME	X	X	X	X	X	X	X	X	X
DHCPSERVER ADD SHAREDNETWORK	X	X	X	X	X	X	X	X	X
DHCPSERVER CLEAR SHAREDNETWORKS	X	X	X	X	X	X	X	X	X
DHCPSERVER DELETE SHAREDNETWORK	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST SHAREDNETWORKS	X	X	X	X	X	X	X	X	X
DHCPSERVER SHAREDNETOWOR ADD SHAREDSUBNET	X	X	X	X	X	X	X	X	X
DHCPSERVER SHAREDNEWORK CLEAR SHAREDSUBNETS	X	X	X	X	X	X	X	X	X
DHCPSERVER SHAREDNETWORKS LIST SHAREDSUBNET	X	X	X	X	X	X	X	X	X
DHCPSERVER ADD SUBNET	X	X	X	X	X	X	X	X	X
DHCPSERVER CLEAR SUBNETS	X	X	X	X	X	X	X	X	X
DHCPSERVER DELETE SUBNET	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST SUBNETS	X	X	X	X	X	X	X	X	X
DHCPSERVER SHOW SUBNET	X	X	X	X	X	X	X	X	X
DHCPSERVER SET SUBNET ASSIGNAUTODOMAIN	X	X	X	X	X	X	X	X	X
DHCPSERVER SET SUBNET DEFAULTLEASETIME	X	X	X	X	X	X	X	X	X
DHCPSERVER SET SUBNET HOSTISDEFAULTGATEWAY	X	X	X	X	X	X	X	X	X
DHCPSERVER SET SUBNET HOSTISDNSSERVER	X	X	X	X	X	X	X	X	X
DHCPSERVER SET SUBNET MAXLEASETIME	X	X	X	X	X	X	X	X	X
DHCPSERVER SET SUBNET SUBNET	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET ADD IPRANGE	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET ADD OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET ADD POOL	X	X	X	X	X	X	X	X	X

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DHCPSERVER SUBNET CLEAR IPRANGES	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET CLEAR OPTIONS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET CLEAR POOLS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET DELETE IPRANGE	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET DELETE OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET DELETE POOL	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET LIST IPRANGES	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET LIST OPTIONS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET LIST POOLS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL ADD ALLOWCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL ADD DENYCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL ADD OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL ADD POOLRANGE	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL CLEAR ALLOWCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL CLEAR DENYCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL CLEAR OPTIONS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL CLEAR POOLRANGE	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL DELETE ALLOWCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL DELETE DENYCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL DELETE OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL DELETE POOLRANGE	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL LIST ALLOWCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL LIST DENYCLASS	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL LIST OPTION	X	X	X	X	X	X	X	X	X
DHCPSERVER SUBNET POOL LIST POOLRANGE	X	X	X	X	X	X	X	X	X

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DHCPSERVER ENABLE|DISABLE	X	X	X	X	X	X	X	X	X
DHCPSERVER FORCERENEW	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST OPTIONS	X	X	X	X	X	X	X	X	X
DHCPSERVER LIST HOST	X	X	X	X	X	X	X	X	X
DHCPSERVER SET ALLOWUNKNOWNCLIENTS	X	X	X	X	X	X	X	X	X
DHCPSERVER SET BOOTP	X	X	X	X	X	X	X	X	X
DHCPSERVER SET DEFAULTLEASETIME	X	X	X	X	X	X	X	X	X
DHCPSERVER SET MAXLEASETIME	X	X	X	X	X	X	X	X	X
DHCPSERVER SHOW	X	X	X	X	X	X	X	X	X
DHCPSERVER UPDATE	X	X	X	X	X	X	X	X	X

5.1.5.1.1 DHCPSERVER ADD USERS CLASS

Syntax `DHCPSERVER ADD CLASS <name> USER-CLASS <userclassdata>`

Description This command sets DHCP server to refuse requests form users without a specific user-class ID.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the class	N/A
userclassdata	User class identifier string to be matched	N/A

Example --> dhcpserver add class cmyclass user-class myuserclass

5.1.5.1.2 DHCPSERVER ADD VENDOR CLASS

Syntax `DHCPSERVER ADD CLASS <name> VENDOR-CLASS <vendorclassdata>`

Description This command sets DHCP server to refuse requests form users without a specific vendor class ID.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the class	N/A
vendorclassdata	Vendo calls identifier string to be matched	N/A

Example --> dhcpserver add class myclass vendor-class myvendorclass

5.1.5.1.3 DHCPSERVER CLEAR CLASSES

Syntax `DHCPSERVER CLEAR CLASSES`

Description This command deletes all DHCP server classes.

Example dhcpserver clear classes

5.1.5.1.4 DHCPSERVER DELETE CLASS

Syntax `DHCPSERVER DELETE CLASS <name>`

Description This command deletes a single DHCP server class.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The existing class that DHCP server is set to operate on.	N/A

Example --> dhcpserver delete class myclass

5.1.5.1.5 DHCPSERVER LIST CLASSES

Syntax `DHCPSERVER LIST CLASSES`

Description This command lists the existing DHCP server classes It displays the following information:

- DHCP server interface ID number
- Class name

- User class data
- cVendor class data

Example --> dhcpserver list classes

```
DHCP Server Classes:
ID  |    Class Name    |     UserClassData    |   VendorClassData
----|------------------|----------------------|-------------------
  1 | myclass          | myuserclass          |
-------------------------------------------------------------------
```

5.1.5.1.6 DHCPSERVER SET USERS CLASS

Syntax `DHCPSERVER SET CLASS <name> USER-CLASS <userclassdata>`

Description This command sets DHCP server to refuse requests form users without a specific user-class ID.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the class	N/A
userclassdata	User class identifier string to be matched	N/A

Example --> dhcpserver set class cmyclass user-class myuserclass

5.1.5.1.7 DHCPSERVER SET VENDOR CLASS

Syntax `DHCPSERVER SET CLASS <name> VENDOR-CLASS <vendorclassdata>`

Description This command sets DHCP server to refuse requests form users without a specific vendor class ID.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the class	N/A
uvendorclassdata	Vendo calls identifier string to be matched	N/A

Example --> dhcpserver set class myclass vendor-class myvendorclass

5.1.5.1.8 DHCPSERVER SHOW CLASS

Syntax `DHCPSERVER SHOW CLASS <name>`

Description This command shwo DHCP server class informations.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the class	N/A

Example --> dhcpserver shwo class myclass

```
DHCP Server Class: myclass
  Class          : myclass
  UserClassData  : myuserclass
  VendorClassData:
```

5.1.5.1.9 DHCPSERVER CLASS ADD OPTION

Syntax `DHCPSERVER CLASS <name> ADD OPTION <identifier> <value>`

Description This command add option on DHCP server class.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the class	N/A
identifier	The identifier of the option available from command dhcpserver list options	N/A
value	The value of the option	N/A

Example --> dhcpserver class myclass add option subnet-mask 255.255.255.0

5.1.5.1.10 DHCPSERVER CLASS CLEAR OPTION

Syntax `DHCPSERVER CLASS <NAME> CLEAR OPTIONS`

Description This command deletes all DHCP server class options.

Example --> dhcpserver class myclass clear options

5.1.5.1.11 DHCPSERVER CLASS DELETE OPTION

Syntax `DHCPSERVER CLASS <name> DELETE OPTION <id>`

Description This command deletes a single DHCP server class option.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The existing class that DHCP server is set to operate on..	N/A
id	The id of the option as reported from the command dhcpserver class list options	N/A

Example --> dhcpserver class myclass delete option 1

5.1.5.1.12 DHCPSERVER CLASS LIST OPTION

Syntax `DHCPSERVER CLASS <NAME> LIST OPTIONS`

Description This command lists the existing DHCP server classes It displays the following information:

- DHCP server interface ID number
- Option identifier
- Option value

Example --> dhcpserver class myclass list options

```
DHCP Server Classes:
ID  |    Identifier    |     Value            |
----|------------------|----------------------|
  1 | subnet-mask      | 255.255.2555.0       |
-----------------------------------------------
```

5.1.5.1.13 DHCPSERVER ADD EXCLUDE

Syntax `DHCPSERVER ADD <name> EXLUDE IPADDRESS <ipaddress>`

Description This command sets DHCP server to exclude a specific IP address from the lease.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the excluded address	N/A
ipaddress	The IP address that need to be excluded	N/A

Example --> dhcpserver add exclude onepc ipaddress 10.10.10.4

5.1.5.1.14 DHCPSERVER CLEAR EXCLUDES

Syntax `DHCPSERVER CLEAR EXLUDES`

Description This command deletes all DHCP server excluded IP address.

Example --> dhcpserver clear excludes

5.1.5.1.15 DHCPSERVER DELETE EXCLUDE

Syntax `DHCPSERVER DELETE EXCLUDE <name>`

Description This command deletes a single DHCP server excluded address.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The existing name of excluded IP address obtained from the command dhcpserver list excluded	N/A

Example --> dhcpserver delete exclude onepc

5.1.5.1.16 DHCPSERVER LIST EXCLUDES

Syntax `DHCPSERVER LISTEXCLUDES`

Description This command lists the existing DHCP server excluded IP address. It displays the following information:

- DHCP server interface ID number
- Excluded name
- Excluded IP address

Example --> dhcpserver lise excluded

```
DHCP server Excluded IP Addresses:
 ID  |    Name    |    IP address
-----|------------|------------------
   1 | onepc      | 10.10.10.4
-----------------------------------
```

5.1.5.1.17 DHCPSERVER ADD INTERFACE

Syntax `DHCPSERVER ADD INTERFACE <ipinterface>`

Description This command sets DHCP server to operate on a specific IP interface. The IP interface is defined as a DHCP server IP interface. By setting DHCP relay to operate on other interfaces, you can simultaneously use DHCP server and relay in your configuration.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ipinterface	The name of the existing interface that you want DHCP server to operate on. To display interface names, use the `IP LIST INTERFACES` command.	N/A

Example --> dhcpserver add interface lan

See also `DHCPRELAY ADD INTERFACE`
`IP LIST INTERFACES`

5.1.5.1.18 DHCPSERVER CLEAR INTERFACES

Syntax `DHCPSERVER CLEAR INTERFACES`

Description This command deletes all DHCP server IP interfaces previously defined using the `DHCPSERVER ADD INTERFACE` command.

Note: This command does not delete the IP interfaces from the router. See `IP CLEAR INTERFACES`

Example --> dhcpserver clear interfaces

See also `DHCPSERVER ADD INTERFACE`
`IP LIST INTERFACES`

5.1.5.1.19 DHCPSERVER DELETE INTERFACE

Syntax `DHCPSERVER DELETE INTERFACE <ipinterface>`

Description This command deletes a single DHCP server IP interface previously defined using the dhcpserver add interface command.

Note: This command does not delete the IP interfaces from the router. See `IP CLEAR INTERFACES`

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ipinterface	The existing IP interface that DHCP server is set to operate on. To display interface names, use the `DHCPSERVER LIST INTERFACES` command.	N/A

Example --> dhcpserver delete interface lan

See also DHCPSERVER ADD INTERFACE
DHCPSERVER LIST INTERFACES

5.1.5.1.20 DHCPSERVER LIST INTERFACES

Syntax DHCPSERVER LIST INTERFACES

Description This command lists the existing DHCP server IP interfaces previously defined using the dhcpserver add interface command. It displays the following information:

- DHCP server interface ID number
- IP interface name

Example --> dhcpserver list interfaces

```
DHCP Server Interfaces:
ID  |   Name
----|----------
 1  |   lan
----|----------
 2  |   wan
---------------
```

See also DHCPSERVER ADD INTERFACE

5.1.5.1.21 DHCPSERVER ADD FIXEDHOST

Syntax DHCPSERVER ADD FIXEDHOST <name> <ipaddress> <macaddress>

Description This command creates a new fixed host mapping in the DHCP server. This allows you to configure the DHCP server to assign a specific IP address to a specific DHCP client based on the client's MAC address. If a DHCPDISCOVER or DHCPREQUEST is received from a DHCP client with a matching MAC address, it will have the specified fixed IP address assigned to it. You must also create a suitable DHCP subnet definition in order for fixed host mapping to work.

Note: If you create a fixed host mapping with an IP address that is already present inside a configured, dynamic IP range, the fixed host IP address will override the address in the dynamic range.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Name	An arbitrary name that identifies the fixed host mapping. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
IPaddress	The IP address that is assigned to a DHCP client based on the client's MAC address, in the format: 192.168.102.3	N/A
macaddress	A MAC address in the format: ##:##:##:##:##:##	N/A

Example The example below creates a fixed host mapping:

--> dhcpserver add fixedhost myhost 192.168.219.1 00:20:2b:01:02:03

The example below creates a suitable subnet for the above fixed host mapping. Note that the IP address used above is not present in the following IP range:

--> dhcpserver add subnet mysubnet 192.168.219.0 255.255.255.0 192.168.219.10 192.168.219.20

See also `DHCPSERVER DELETE FIXEDHOST`
`DHCPSERVER LIST FIXEDHOSTS`

5.1.5.1.22 DHCPSERVER CLEAR FIXEDHOSTS

Syntax `DHCPSERVER CLEAR FIXEDHOSTS`

Description This command deletes all DHCP server fixedhosts that were created using the `DHCPSERVER ADD FIXEDHOST` command.

Example --> dhcpserver clear fixedhosts

5.1.5.1.23 DHCPSERVER DELETE FIXEDHOST

Syntax `DHCPSERVER DELETE FIXEDHOST <name>`

Description This command deletes a single fixed host mapping in the DHCP server that was created using the `DHCPSERVER ADD FIXEDHOST` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing fixed host. To display fixed host names, use the DHCPSERVER LIST FIXEDHOSTS command.	N/A

Example --> dhcpserver delete fixedhost myhost

See also DHCPSERVER ADD FIXEDHOST
DHCPSERVER CLEAR FIXEDHOSTS
DHCPSERVER LIST FIXEDHOST

5.1.5.1.24 DHCPSERVER LIST FIXEDHOSTS

Syntax DHCPSERVER LIST FIXEDHOSTS

Description This command lists the following information about existing DHCP fixed host mappings:

- Fixed host ID number
- Fixed host name
- IP address
- MAC address
- Max lease time

Example --> dhcpserver list fixedhosts

```
DHCP server fixed host mappings:
 ID  |  Name |    IP address   |    MAC address     | Max Lease Time
-----|-------|-----------------|--------------------|---------------
   1 | myhost| 192.168.219.0   | 00:20:2b:01:02:03  | 86400
-------------------------------------------------------------------
```

See also DHCPSERVER ADD FIXEDHOST
DHCPSERVER SET FIXEDHOST IPADDRESS
DHCPSERVER SET FIXEDHOST MACADDRESS
DHCPSERVER SET FIXEDHOST MAXLEASETIME

5.1.5.1.25 DHCPSERVER SET FIXEDHOST IPADDRESS

Syntax DHCPSERVER SET FIXEDHOST <host name> IPADDRESS <ipaddress>

Description This command sets the IP address that will be allocated to a DHCP client by the fixed host mapping.

Note: You are not allowed to create a fixed host mapping with an IP address that is already present inside a configured, dynamic IP range on a subnet. The reverse is also forbidden; you cannot add addresses into a dynamic IP range that are already configured as fixed host addresses. The CLI will display a warning if you attempt to do this.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
host name	An existing fixedhost. To display fixedhost names, use the DHCPSERVER LIST FIXEDHOSTS command.	N/A
ip address	The IP address assigned to a DHCP client based on the client's MAC address, in the format: 192.168.102.3	N/A

Example --> dhcpserver set fixedhost myhost ipaddress 192.168.219.2

See also DHCPSERVER LIST FIXEDHOSTS
DHCPSERVER SET FIXEDHOST MACADDRESS

5.1.5.1.26 DHCPSERVER SET FIXEDHOST DEFAULTLEASETIME

Syntax DHCPSERVER SET FIXEDHOST <host name> DEFAULTLEASETIME <defaultleasetime>

Description This command sets the default leas time that will be allocated to a DHCP client by the fixed host mapping.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
host name	An existing fixedhost. To display fixedhost names, use the DHCPSERVER LIST FIXEDHOSTS command.	N/A
defaultleasetime	The default time for the lease of a specific fixed host	N/A

Example --> dhcpserver set fixedhost myhost defaultleasetime 3600

See also DHCPSERVER LIST FIXEDHOSTS
DHCPSERVER SET FIXEDHOST MACADDRESS

5.1.5.1.27 DHCPSERVER SET FIXEDHOST MACADDRESS

Syntax DHCPSERVER SET FIXEDHOST <host name> MACADDRESS <macaddress>

Description This command sets the MAC address for an existing fixed host mapping.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
host name	An existing fixedhost. To display fixedhost names, use the DHCPSERVER LIST FIXEDHOSTS command.	N/A
macaddress	A MAC address in the format: ##:##:##:##:##:##	N/A

Example --> dhcpserver set fixedhost myhost macaddress 00:20:2b:01:02:03

See also DHCPSERVER LIST FIXEDHOSTS
DHCPSERVER SET FIXEDHOST IPADDRESS

5.1.5.1.28 DHCPSERVER SET FIXEDHOST MAXLEASETIME

Syntax DHCPSERVER SET FIXEDHOST <host name> MAXLEASETIME <maxlease-time>

Description This command sets the maximum lease time for an existing fixed host mapping.

Options The following table gives the range of values for each option than can be specified with this command and a default value (if applicable).

Option	Description	Default Value
maxleasetime	The maximum time (in seconds) for a lease when the client requesting the lease does not ask for a specific expiry time.	86400

Example --> dhcpserver set fixedhost myhost maxleasetime 90000

See also DHCPSERVER LIST FIXEDHOSTS

5.1.5.1.29 DHCPSERVER ADD SHAREDNETWORK

Syntax `DHCPSERVER ADD SHAREDNETWORK <name>`

Description This command creates a shared network. All the subnets part of the same physical network should be included in a shared network.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Name	An arbitrary name that identifies the shared network	N/A

Example The example below creates a fixed host mapping:

--> dhcpserver add sharednetwork myshare

5.1.5.1.30 DHCPSERVER CLEAR SHAREDNETWORKS

Syntax `DHCPSERVER CLEAR SHAREDNETWORKS`

Description This command deletes all DHCP server share networks

Example --> dhcpserver clear sharednetworks

5.1.5.1.31 DHCPSERVER DELETE SHAREDNETWORK

Syntax `DHCPSERVER DELETE SHAREDNETWORK <name>`

Description This command deletes a single shard network.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the shared network.	N/A

Example --> dhcpserver delete sharednetwork myshared

5.1.5.1.32 DHCPSERVER LIST SHAREDNETWORKS

Syntax `DHCPSERVER LIST SHAREDNETWORKS`

Description This command lists the following information about existing DHCP fixed host mappings:

- Sahred Nnetwork ID
- Sharednetwork name

Example --> dhcpserver list sharednetorks

DHCP server fixed host mappings:

```
 DHCP Server Shared-Networks:
ID  |   Shared-Network Name
----|-------------------------
  1 | myshared
------------------------------
```

5.1.5.1.33 DHCPSERVER SHAREDNETOWOR ADD SHAREDSUBNET

Syntax `DHCPSERVER SHAREDNETWORK <name> ADD SHAREDSUBNET <subnet-name>`

Description This command add a shared subnet without IP Ranges in the Shared Network.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	Sharedsubnet name	N/A
subnetname	Subnet name	N/A

Example --> dhcpserver sharednetwork myshare add sharedsubnet first subnet

5.1.5.1.34 DHCPSERVER SHAREDNEWORK CLEAR SHAREDSUBNETS

Syntax `DHCPSERVER SHAREDNETWORK <name> CLEAR SHAREDSUBNETS`

Description This command deletes all DHCP server share subnets of a specific sharednetwrok

Example --> dhcpserver sharednetwork myshare clear sharedsubnets

5.1.5.1.35 DHCPSERVER SHAREDNETWORK DELETE SHAREDSUBNET

Syntax `DHCPSERVER SHAREDNETWORK <name> DELETE SHAREDSUBNET <subnetname>`

Description This command deletes a single shard subnet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the shared network.	N/A
subnetname	Subnet name	N/A

Example --> dhcpserver sharednetwork myshared delete sharedsubnet mysubnet

5.1.5.1.36 DHCPSERVER SHAREDNETWORKS LIST SHAREDSUBNET

Syntax `DHCPSERVER SHAREDNETWORKS <NAME> LIST SHAREDSUBNET`

Description This command lists the information about existing DHCP shared subnet in ashared network

Example --> dhcpserver sharednetorks myshare list sharedsubnet

5.1.5.1.37 DHCPSERVER ADD SUBNET

Syntax `DHCPSERVER ADD SUBNET <name> <ipaddress> <netmask> [<startaddr> <endaddr>]`

Description This command creates a subnet that stores a pool of IP addresses. The DHCP server can allocate IP addresses from this pool to clients on request.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the subnet. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
ipaddress	The IP address of the subnet in the format: 192.168.102.3	N/A

netmask	The netmask address of the subnet, for example: 255.255.255.0	N/A
startaddr	The first IP address in the pool of addresses. The IP address is displayed in the following format: 192.168.102.3	N/A
endaddr	The last IP address in the pool of addresses. The IP address is displayed in the following format: 192.168.102.3	N/A

Example --> dhcpserver add subnet sub1 239.252.197.0 255.255.255.0 239.252.197.10 239.252.197.107

See also `DHCPSERVER LIST SUBNETS`

5.1.5.1.38 DHCPSERVER CLEAR SUBNETS

Syntax `DHCPSERVER CLEAR SUBNETS`

Description This command deletes all DHCP server subnets that were created using the `DHCPSERVER ADD SUBNET` command.

Example --> dhcpserver clear subnets

See also `DHCPSERVER DELETE SUBNET`

5.1.5.1.39 DHCPSERVER DELETE SUBNET

Syntax `DHCPSERVER DELETE SUBNET {<name>|<number>}`

Description This command deletes a single DHCP server subnet. The pool of IP addresses in the subnet is also deleted.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the `DHCPSERVER LIST SUBNETS` command.	N/A
number	An existing subnet. To display subnet numbers, use the `DHCPSERVER LIST SUBNETS` command.	N/A

Example --> dhcpserver delete subnet sub1

See also DHCPSERVER CLEAR SUBNETS

5.1.5.1.40 DHCPSERVER LIST SUBNETS

Syntax DHCPSERVER LIST SUBNETS

Description This command lists the following information about existing DHCP server subnets:

- Subnet number
- Subnet name
- Subnet ip address
- Subnet netmask address
- Default lease time (in seconds)
- Maximum lease time (in seconds)
- Whether the host is a dns server (true or false)

Example --> dhcpserver list subnets

```
DHCP Server subnets:
Default       Max      Host is
 ID |   IP Address  |   Netmask     |Lease time| Lease time |DNS svr
----|---------------|---------------|----------|------------|-------
  1 | 192.168.102.0 | 255.255.255.0 | 43200    | 86400      | false
-------------------------------------------------------------------
```

See also DHCPSERVER SHOW SUBNET

5.1.5.1.41 DHCPSERVER SHOW SUBNET

Syntax DHCPSERVER SHOW SUBNET {<name>|<number>}

Description This command displays the following information about a subnet:

- Subnet name
- Subnet ip address
- Subnet netmask
- Subnet maximum lease time
- Subnet default lease time

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A

Example --> dhcpserver show subnet sub1

```
DHCP Server Subnet: sub1
            Subnet: 192.168.103.0
           Netmask: 255.255.255.0
   Max. lease time: 70000 seconds
Default lease time: 30000 seconds
```

See also DHCPSERVER SHOW

5.1.5.1.42 DHCPSERVER SET SUBNET ASSIGNAUTODOMAIN

Syntax DHCPSERVER SET SUBNET {<name>|<number>} ASSIGNAUTODOMAIN {ENABLED|DISABLED}

Description This command sets DHCP server to automatically pick up the domain name configured in DNS relay and hand it out to DHCP clients on one or more of the subnets being administered by DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
enabled	DHCP server passes the local device's domain name (set up in DNS relay) to all DHCP clients on the LAN.	disabled
disabled	DHCP server does not pass the local device's domain name (set up in DNS relay) to all DHCP clients on the LAN.	

Example --> dhcpserver set subnet sub1 assignautodomain enabled

5.1.5.1.43 DHCPSERVER SET SUBNET DEFAULTLEASETIME

Syntax `DHCPSERVER SET SUBNET {<name>|<number>} DEFAULTLEASETIME <defaultleasetime>`

Description This command sets the default lease time for an existing subnet. This command setting overrides the global default lease time setting for this particular subnet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the `DHCPSERVER LIST SUBNETS` command.	N/A
number	An existing subnet. To display subnet numbers, use the `DHCPSERVER LIST SUBNETS` command.	N/A
defaultleasetime	The default time (in seconds) a subnet assigns to a lease if the client requesting the lease does not ask for a specific expiry time.	43200

Example --> dhcpserver set subnet sub1 defaultleasetime 30000

See also `DHCPSERVER SHOW SUBNET`

5.1.5.1.44 DHCPSERVER SET SUBNET HOSTISDEFAULTGATEWAY

Syntax `DHCPSERVER SET SUBNET <{<name>|<number>} HOSTISDEFAULTGATEWAY {ENABLED | DISABLED}`

Description This command tells the DHCP server to give out its own host IP address as the default gateway address. This is useful when combined with DNS Relay.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
enabled	Allows DHCP server to give out its own host IP address as the default gateway address.	disabled
disabled	Disallows DHCP server from giving out its own host IP address as the default gateway address.	

Example --> dhcpserver set subnet sub1 hostisdefaultgateway enabled

See also DHCPSERVER SET SUBNET HOSTISDNSSERVER

5.1.5.1.45 DHCPSERVER SET SUBNET HOSTISDNSSERVER

Syntax DHCPSERVER SET SUBNET {<name>|<number>} HOSTISDNSSERVER {ENABLED | DISABLED}

Description This command tells the DHCP server to give out its own host IP address as the DNS server address. This is useful when combined with DNS Relay.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
enabled	Allows DHCP server to give out its own host IP address as the DNS server address.	disabled
disabled	Disallows DHCP server from giving out its own host IP address as the DNS server address.	

Example --> dhcpserver set subnet sub1 hostisdnsserver enabled

See also DHCPSERVER LIST SUBNETS

5.1.5.1.46 DHCPSERVER SET SUBNET MAXLEASETIME

Syntax DHCPSERVER SET SUBNET {<name>|<number>} MAXLEASETIME <max-leasetime>

Description This command sets the maximum lease time for an existing subnet. This command setting overrides the global maximum lease time setting for this particular subnet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
maxleasetime	The maximum time (in seconds) that a subnet assigns to a lease if the client requesting the lease does not ask for a specific expiry time.	86400

Example --> dhcpserver set subnet sub1 maxleasetime 70000

See also DHCPSERVER SHOW SUBNET

5.1.5.1.47 DHCPSERVER SET SUBNET SUBNET

Syntax DHCPSERVER SET SUBNET {<name>|<number>} SUBNET <ip address> <netmask>

Description This command allows you to change the IP address and netmask used by an existing DHCP server subnet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
ip address	The new IP address for the subnet (format: 192.168.102.3)	N/A
netmask	The new netmask address for the subnet, for example: 255.255.255.0	N/A

Example --> dhcpserver set subnet sub1 subnet 239.252.197.0 255.255.255.0

See also DHCPSERVER LIST SUBNETS

5.1.5.1.48 DHCPSERVER SUBNET ADD IPRANGE

Syntax DHCPSERVER SUBNET {<name>|<number>} ADD IPRANGE <startaddr> <endaddr>

Description This command adds a pool of IP addresses to an existing subnet. DHCP server can allocate IP addresses from this pool to clients on request.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
startaddr	The first IP address in the pool of addresses. The IP address is displayed in the following format: 192.168.102.3	N/A
endaddr	The last IP address in the pool of addresses. The IP address is displayed in the following format: 192.168.102.3	N/A

Example --> dhcpserver subnet sub1 add iprange 239.252.197.0 239.252.197.107

See also DHCPSERVER ADD SUBNET
DHCPSERVER LIST SUBNETS
DHCPSERVER SUBNET LIST IPRANGES

5.1.5.1.49 DHCPSERVER SUBNET ADD OPTION

Syntax DHCPSERVER SUBNET {<name>|<number>} ADD OPTION <identifier> <value>

Description This command allows you to configure the DHCP server using the options detailed in RFC2132. To display a list of available options, use the command DHCPSERVER LIST OPTIONS.

The heading of each option in the list contains the option identifier and the required value (in italics) for that specific option. The following is an extract from the option list:

- option auto-configure flag;

This option, based on RFC2563, controls whether clients on this subnet are allowed to perform the IP address auto configuration.

It only applies in cases where the DHCP server is unwilling or unable to supply an IP address lease. In this case, if this option is set to 1, then the DHCP server will not intervene to prevent clients from using auto-configuration to determine an IP address. If this option is set to 0, the DHCP server will explicitly forbid the use of IP address auto-configuration on the network.

If this option is not explicitly configured, then it will be assumed that auto-configuration is allowed on the network.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A

number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
identifier	A text string that identifies a DHCP server configuration option.	N/A
value	The value associated with the option identifier.	N/A

Example --> dhcpserver subnet sub1 add option auto-configure 1

See also DHCPCLIENT SET INTERFACECONFIG AUTOIP ENABLED|DISABLED

Note: For a list of options that you can choose from, see DHCPSERVER LIST OPTIONS

For information on RFC 2132, see http://www.ietf.org/rfc/rfc2132.txt

5.1.5.1.50 DHCPSERVER SUBNET ADD POOL

Syntax DHCPSERVER SUBNET <name> ADD POOL <poolname> <startaddr> <endaddr>

Description This command allows you to configure the DHCP server adding a pool to the specified subnet

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	the name of the subnet	N/A
poolname	Name of the pool to be added	N/A
startaddr	Starting IP address for the Pool IP range	N/A
endaddr	Ending IP address for the Pool IP range	N/A

Example --> dhcpserver subnet sub1 add pool mypool 10.17.90.1 10.17.90.128

5.1.5.1.51 DHCPSERVER SUBNET CLEAR IPRANGES

Syntax DHCPSERVER SUBNET {<name>|<number>} CLEAR IPRANGES

Description This command deletes all of the IP ranges set for an existing subnet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A

Example --> dhcpserver subnet sub1 clear ipranges

See also DHCPSERVER SUBNET LIST IPRANGES
DHCPSERVER SUBNET DELETE IPRANGE

5.1.5.1.52 DHCPSERVER SUBNET CLEAR OPTIONS

Syntax DHCPSERVER SUBNET {<name>|<number>} CLEAR OPTIONS

Description This command deletes the options set for an existing subnet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A

Example --> dhcpserver subnet sub1 clear options

See also DHCPSERVER ADD SUBNET
DHCPSERVER LIST SUBNETS
DHCPSERVER SUBNET DELETE OPTION

5.1.5.1.53 DHCPSERVER SUBNET CLEAR POOLS

Syntax DHCPSERVER SUBNET <name> CLEAR POOLS

Description This command delete all the pools of the specified subnet

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A

Example --> dhcpserver subnet sub1 clear pools

5.1.5.1.54 DHCPSERVER SUBNET DELETE IPRANGE

Syntax `DHCPSERVER SUBNET {<name>|<number>} DELETE IPRANGE <range-id>`

Description This command deletes a single IP range from an existing subnet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS COMMAND.	N/A
range-id	A number that identifies an IP range. To list the existing range-ids for a subnet, use the DHCPSERVER SUBNET LIST IPRANGES command.	N/A

Example --> dhcpserver subnet sub1 delete iprange 1

See also `DHCPSERVER LIST SUBNETS`
`DHCPSERVER SUBNET LIST IPRANGES`

5.1.5.1.55 DHCPSERVER SUBNET DELETE OPTION

Syntax `DHCPSERVER SUBNET {<name>|<number>} DELETE OPTION <option number>`

Description This command deletes a single option that was created using the DHCPSERVER SUBNET ADD OPTION command. Once deleted, the option will no longer be given out by the DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A
option number	An existing option. To list all existing options, use the DHCPSERVER SUBNET LIST OPTIONS command.	N/A

Example --> dhcpserver subnet sub1 delete option 2

See also DHCPSERVER ADD SUBNET
DHCPSERVER CLEAR SUBNETS
DHCPSERVER LIST SUBNETS
DHCPSERVER SUBNET LIST OPTIONS

5.1.5.1.56 DHCPSERVER SUBNET DELETE POOL

Syntax DHCPSERVER SUBNET <name> DELETE POOL <poolname>

Description This command deletes a single pool that was created using the DHCPSERVER SUBNET ADD POOL command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool to be deleted from the subnet.	N/A

Example --> dhcpserver subnet sub1 delete pool mypool

5.1.5.1.57 DHCPSERVER SUBNET LIST IPRANGES

Syntax `DHCPSERVER SUBNET {<name>|<number>} LIST IPRANGES`

Description This command lists the IP range(s) for an existing subnet that has been added using the dhcpserver add subnet command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the `DHCPSERVER LIST SUBNETS` command.	N/A
number	An existing subnet. To display subnet numbers, use THE `DHCPSERVER LIST SUBNETS` command.	N/A

Example --> dhcpserver subnet sub1 list ipranges

```
IP Ranges for subnet: sub1
ID  |  Start Address   |    End Address
-----|------------------|-----------------
   1 | 192.168.102.0    | 192.168.102.100
   2 | 192.168.102.200  | 192.168.102.300
-----------------------------------------
```

See also `DHCPSERVER LIST SUBNETS`
`DHCPSERVER ADD SUBNET`

5.1.5.1.58 DHCPSERVER SUBNET LIST OPTIONS

Syntax `DHCPSERVER SUBNET {<name>|<number>} LIST OPTIONS`

Description This command lists the options for an existing subnet that has been added using the dhcpserver add subnet command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
number	An existing subnet. To display subnet numbers, use the DHCPSERVER LIST SUBNETS command.	N/A

Example --> dhcpserver subnet sub1 list options

```
Options for subnet: sub1
 ID  |    Identifier    |       Value
-----|------------------|------------------
   1 | ip-forwarding    | false
   2 | subnet-mask      | 255.255.255.0
-----------------------------------------
```

See also DHCPSERVER ADD
DHCPSERVER LIST SUBNETS

5.1.5.1.59 DHCPSERVER SUBNET LIST POOLS

Syntax DHCPSERVER SUBNET <name> LIST POOLS

Description This command lists the pools for an existing subnet that has been added using the dhcpserver subnet add pool command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A

Example --> dhcpserver subnet sub1 list pools

5.1.5.1.60 DHCPSERVER SUBNET POOL ADD ALLOWCLASS

Syntax DHCPSERVER SUBNET <name> POOL <poolname> ADD ALLOWCLASS <CLASSNAME>

Description This command adds a class to be allowed by the pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A
classname	Name of the class to be allowed by the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool add allowclass myclass

5.1.5.1.61 DHCPSERVER SUBNET POOL ADD DENYCLASS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> ADD DENYCLASS <CLASSNAME>`

Description This command adds a class to be denied by the Pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A
classname	Name of the class to be denied by the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool add denyclass myclass

5.1.5.1.62 DHCPSERVER SUBNET POOL ADD OPTION

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> ADD OPTION <identifier> <value>`

Description This command add an option to the specified pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A
identifier	The identifier of the option available from command dhcpserver list options	identifier
value	The value of the option	value

Example --> dhcpserver subnet sub1 pool mypool add option auto-configure 1

5.1.5.1.63 DHCPSERVER SUBNET POOL ADD POOLRANGE

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> ADD POOLRANGE <startaddr> <endaddr>`

Description This command allows you to configure the DHCP server adding a poolrange to the specified pool

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	the name of the subnet	N/A
poolname	Name of the pool to be added	N/A
startaddr	Starting IP address for the poolrange IP range	N/A
endaddr	Ending IP address for the poolrange IP range	N/A

Example --> dhcpserver subnet sub1 add pool mypool poolrange 10.17.90.1 10.17.90.128

5.1.5.1.64 DHCPSERVER SUBNET POOL CLEAR ALLOWCLASS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> CLEAR ALLOWCLASS`

Description This command clear all the allowed class fro a pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the `DHCPSERVER LIST SUBNETS` command.	N/A
poolname	Name/Id of the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool clear allowclass

5.1.5.1.65 DHCPSERVER SUBNET POOL CLEAR DENYCLASS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> CLEAR DENYCLASS <CLASSNAME>`

Description This command clear all the class denied by the Pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the `DHCPSERVER LIST SUBNETS` command.	N/A
poolname	Name/Id of the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool clear denyclass

5.1.5.1.66 DHCPSERVER SUBNET POOL CLEAR OPTIONS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> CLEAR OPTIONS`

Description This command deletes all options from a specified pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool clear options

5.1.5.1.67 DHCPSERVER SUBNET POOL CLEAR POOLRANGE

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> CLEAR POOLRANGE`

Description This command clear all the poolranges on the poolname

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	the name of the subnet	N/A
poolname	Name of the pool to be added	N/A

Example --> dhcpserver subnet sub1 pool mypool clear poolrange

5.1.5.1.68 DHCPSERVER SUBNET POOL DELETE ALLOWCLASS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> DELETE ALLOWCLASS <CLASSNAME>`

Description This command delete a class allowed by the pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A
classname	Name of the class to be allowed by the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool delete allowclass myclass

5.1.5.1.69 DHCPSERVER SUBNET POOL DELETE DENYCLASS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> DELETE DENYCLASS <CLASSNAME>`

Description This command delete a class to be denied by the Pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A
classname	Name of the class to be denied by the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool delete denyclass myclass

5.1.5.1.70 DHCPSERVER SUBNET POOL DELETE OPTION

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> ADD OPTION <identifier>`

Description This command delete an option form the specified pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A
identifier	The identifier of the option available from command dhcpserver list options	identifier

Example --> dhcpserver subnet sub1 pool mypool delete option auto-configure

5.1.5.1.71 DHCPSERVER SUBNET POOL DELETE POOLRANGE

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> DELETE POOLRANGE <id>`

Description This command allows you to configure the DHCP server adding a poolrange to the specified pool

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	the name of the subnet	N/A
poolname	Name of the pool to be added	N/A
id	iprange Id. to be deleted from the pool	N/A

Example --> dhcpserver subnet sub1 delete pool mypool poolrange 1

5.1.5.1.72 DHCPSERVER SUBNET POOL LIST ALLOWCLASS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> LIST ALLOWCLASS`

Description This command list class allowed by the pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool list allowclass

5.1.5.1.73 DHCPSERVER SUBNET POOL LIST DENYCLASS

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> LIST DENYCLASS`

Description This command list class to be denied by the Pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool list denyclass

5.1.5.1.74 DHCPSERVER SUBNET POOL LIST OPTION

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> LIST OPTION`

Description This command list options form the specified pool.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing subnet. To display subnet names, use the DHCPSERVER LIST SUBNETS command.	N/A
poolname	Name/Id of the pool	N/A

Example --> dhcpserver subnet sub1 pool mypool list options

5.1.5.1.75 DHCPSERVER SUBNET POOL LIST POOLRANGE

Syntax `DHCPSERVER SUBNET <name> POOL <poolname> LIST POOLRANGE`

Description This command allows you to list the poolrange of a pool

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	the name of the subnet	N/A
poolname	Name of the pool to be added	N/A

Example --> dhcpserver subnet sub1 delete pool mypool poolrange 1

5.1.5.1.76 DHCPSERVER ENABLE|DISABLE

Syntax `DHCPSERVER {ENABLE|DISABLE}`

Description This command enables/disables the DHCP server. You must have the DHCP server enabled in order to carry out any DHCP server configuration. If you try configuring DHCP server when `DHCPSERVER DISABLE` is set, the CLI issues a warning message.

You can enable both DHCP server and DHCP relay simultaneously by specifying individual interfaces for the server and relay to bind to. You cannot bind the same interface to both server and relay - you must use different interfaces for each.

If you have set DHCP server to operate on an existing IP interface and you want to make configuration changes to that IP interface, you must first disable DHCP server, then re-enable it once your IP configuration is complete.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enable	Enables configuration of the DHCP server.	enable
disable	Disables configuration of the DHCP server.	

Example --> dhcpserver enable

See also DHCPRELAY ENABLE|DISABLE
DHCPSERVER ADD INTERFACE

5.1.5.1.77 DHCPSERVER FORCERENEW

Syntax DHCPSERVER FORCERENEW <ipaddress>

Description This command prompts the DHCP server to issue a DHCPFORCERENEW message to the DHCP client at the given IP address.

Note that the server will only do this if the DHCP client is on one of the subnets the DHCP server has been configured to serve. The client must also be configured to accept DHCPFORCERENEW messages using the DHCPCLIENT SET INTERFACECONFIG FORCERENEW ENABLED command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ipaddress	The IP address that the DHCP server issues the DHCPFORCERENEW message to.	N/A

Example --> dhcpserver forcerenew 192.168.1.1

See also DHCPCLIENT SET INTERFACECONFIG FORCERENEW

5.1.5.1.78 DHCPSERVER LIST OPTIONS

Syntax DHCPSERVER LIST OPTIONS

Description This command lists the option data types available for DHCP server. These options are detailed in RFC2132.

You can configure the DHCP server using any of the options listed.

Example --> dhcpserver list options

```
subnet-mask
time-offset
routers
time-servers
ien116-name-servers
domain-name-servers
log-servers
cookie-servers
lpr-servers
impress-servers
resource-location-servers
host-name
boot-size
merit-dump
domain-name
swap-server
root-path
extensions-path
ip-forwarding
non-local-source-routing
policy-filter
max-dgram-reassembly
default-ip-ttl
path-mtu-aging-timeout
path-mtu-plateau-table
interface-mtu
all-subnets-local
broadcast-address
perform-mask-discovery
mask-supplier
router-discovery
router-solicitation-address
static-routes
trailer-encapsulation
arp-cache-timeout
ieee802-3-encapsulation
default-tcp-ttl
tcp-keepalive-interval
tcp-keepalive-garbage
nis-domain
nis-servers
ntp-servers
vendor-encapsulated-options
netbios-name-servers
netbios-dd-server
netbios-node-type
netbios-scope
font-servers
x-display-manager
dhcp-requested-address
dhcp-lease-time
dhcp-option-overload
dhcp-message-type
dhcp-server-identifier
dhcp-parameter-request-list
dhcp-message
dhcp-max-message-size
dhcp-renewal-time
dhcp-rebinding-time
dhcp-class-identifier
dhcp-client-identifier
option-62
option-63
nisplus-domain
nisplus-servers
tftp-server-name
bootfile-name
mobile-ip-home-agent
smtp-server
pop-server
nntp-server
www-server
finger-server
irc-server
streettalk-server
streettalk-directory-assis-
tance-server
user-class
option-78
option-79
option-80
option-81
option-82
option-83
option-84
nds-servers
nds-tree-name
nds-context
option-88
option-89
option-115
auto-configure
option-117
option-254
option-end
```

See also DHCPSERVER SUBNET ADD OPTION

For info DHCPSERVER SET ALLOWUNKNOWNCLIENTS

Syntax DHCPSERVER SET ALLOWUNKNOWNCLIENTS {ENABLED|DISABLED}

Description This command enables/disables the dynamic assignment of addresses to unknown clients.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enabled	IP addresses are dynamically assigned to unknown clients	Enabled
disabled	IP addresses are not dynamically assigned to unknown clients	

Example --> dhcpserver set allowunknownclients disabled

See also `DHCPCLIENT SET INTERFACECONFIG CLIENTID`

5.1.5.1.79 DHCPSERVER LIST HOST

Syntax `DHCPSERVER LIST HOSTS`

Description This command lists the hosts assigned from the server.

Example --> dhcpserver list hosts

5.1.5.1.80 DHCPSERVER SET ALLOWUNKNOWNCLIENTS

Syntax `DHCPSERVER SET ALLOWUNKNOWNCLIENTS {ENABLED|DISABLED}`

Description This command enables/disables the dynamic assignment of addresses to unknown clients.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enabled	IP addresses are dynamically assigned to unknown clients	Enabled
disabled	IP addresses are not dynamically assigned to unknown clients	

Example --> dhcpserver set allowunknownclients disabled

See also `DHCPCLIENT SET INTERFACECONFIG CLIENTID`

5.1.5.1.81 DHCPSERVER SET BOOTP

Syntax `DHCPSERVER SET BOOTP {ENABLED|DISABLED}`

Description This command determines whether DHCP server can respond to BOOTP requests.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enabled	DHCP server responds to BOOTP queries.	Enabled
disabled	DHCP server does not respond to BOOTP queries.	

Example --> dhcpserver set bootp disabled

5.1.5.1.82 DHCPSERVER SET DEFAULTLEASETIME

Syntax `DHCPSERVER SET DEFAULTLEASETIME <defaultleasetime>`

Description This command sets the global default lease time for DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
defaultleasetime	The default time (in seconds) assigned to a lease if the client requesting the lease does not ask for a specific expiry time.	43200

Example --> dhcpserver set defaultleasetime 50000

See also `DHCPSERVER SET SUBNET MAXLEASETIME`

5.1.5.1.83 DHCPSERVER SET MAXLEASETIME

Syntax `DHCPSERVER SET MAXLEASETIME <maxleasetime>`

Description This command sets the global maximum lease time for DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
maxleasetime	The maximum time (in seconds) for a lease when the client requesting the lease does not ask for a specific expiry time	86400

Example --> dhcpserver set maxleasetime 90000

See also DHCPSERVER SET DEFAULTLEASETIME

5.1.5.1.84 DHCPSERVER SHOW

Syntax DHCPSERVER SHOW

Description This command displays the following global configuration information about the DHCP server:

- Status of the server (enabled/disabled)
- Global default lease time
- Global maximum lease time
- Bootp requests setting (enable/disable)
- Allow unknown clients setting (enable/disable)

Example --> dhcpserver show

```
Global DHCP Server Configuration:
                 Status: ENABLED
     Default lease time: 43200 seconds
        Max. lease time: 86400 seconds
   Allow BOOTP requests: true
  Allow unknown clients: true
```

See also DHCPSERVER SHOW SUBNET

5.1.5.1.85 DHCPSERVER UPDATE

Syntax DHCPSERVER UPDATE

Description This command updates the DHCP server configuration. Changes made to the server configuration will not take effect until this command has been entered.

Example --> dhcpserver update

```
dhcpserver: Reset request acknowledged. Reset imminent.
```

5.1.6 DHCP Client command reference

This section describes the commands available on the AT-RG624/634 Residential Gateway to enable, configure and manage the ***DHCP Client*** module.

5.1.6.1 DHCP client CLI commands

The table below lists the ***DHCP client*** commands provided by the CLI:**DHCP client CLI commands**

TABLE 5-2 DHCP client CLI commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DHCPCLIENT ADD INTERFACECONFIG	X	X	X	X	X	X	X	X	X
DHCPCLIENT CLEAR INTERFACECONFIGS	X	X	X	X	X	X	X	X	X
DHCPCLIENT DELETE INTERFACECONFIG	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG ADD REQUESTED OPTION	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG ADD REQUIRED OPTION	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG ADD SENT OPTION	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG CLEAR SENT OPTIONS	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG CLEAR REQUESTED OPTIONS	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG DELETE REQUESTED OPTION	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG DELETE SENT OPTION	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG LIST REQUESTED OPTIONS	X	X	X	X	X	X	X	X	X
DHCPCLIENT INTERFACECONFIG LIST SENT OPTIONS	X	X	X	X	X	X	X	X	X
DHCPCLIENT LIST INTERFACECONFIGS	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET BACKOFF	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG AUTOIP ENABLED|DISABLED	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG CLIENTID	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG DEFAULTROUTE ENABLED|DISABLED	X	X	X	X	X	X	X	X	X

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DHCPCLIENT SET INTERFACECONFIG DHCPINFORM ENABLED|DISABLED	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG DHCPSERVERPOOLSIZE	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG DHCPSERVERINTERFACE	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG FORCERENEW	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG GIVEDNSTOCLIENT ENABLED|DISABLED	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG GIVEDNSTORELAY ENABLED|DISABLED	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG INTERFACE	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG NOCLIENTID	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG REQUESTEDLEASETIME	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INTERFACECONFIG SERVER	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET BROADCAST-FLAG	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INITIALINTERVAL	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET INITIALINTERVAL	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET REBOOT	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET RETRY	X	X	X	X	X	X	X	X	X
DHCPCLIENT SET FORCE-BROADCAST-RENEW	X	X	X	X	X	X	X	X	X
DHCPCLIENT SHOW	X	X	X	X	X	X	X	X	X

5.1.6.1.1 DHCPCLIENT ADD INTERFACECONFIG

Syntax `DHCPCLIENT ADD INTERFACECONFIG <name> <ipinterface>`

Description This command configures DHCP client parameters for negotiation over an existing IP interface. The client interface can only set the IP configuration if the IP interface has DHCP enabled.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the client interface. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
ip interface	An IP address or An existing IP interface. The interface must have DHCP enabled. To display interface names, use the `IP LIST INTERFACES` command.	N/A

Example --> dhcpclient add interfaceconfig config1 ip1

See also
```
DHCPCLIENT LIST INTERFACECONFIGS
IP LIST INTERFACES
IP SET INTERFACE DHCP
```

5.1.6.1.2 DHCPCLIENT CLEAR INTERFACECONFIGS

Syntax `DHCPCLIENT CLEAR INTERFACECONFIGS`

Description This command deletes all existing DHCP client interface configurations.

Example --> dhcpclient clear interfaceconfigs

See also `DHCPCLIENT LIST INTERFACECONFIGS`

5.1.6.1.3 DHCPCLIENT DELETE INTERFACECONFIG

Syntax `DHCPCLIENT DELETE INTERFACECONFIG {<name>|<number>}`

Description This command deletes a single DHCP client interface configuration.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A

Example --> dhcpclient delete interfaceconfig config1

See also DHCPCLIENT LIST INTERFACECONFIGS

5.1.6.1.4 DHCPCLIENT INTERFACECONFIG ADD REQUESTED OPTION

Syntax DHCPCLIENT INTERFACECONFIG {<name>|<number>} ADD REQUESTED OPTION <option>

Description This command tells the DHCP client to request a specified option from a DHCP server. The requested option is not compulsory - if the option was not included in a lease offered by DHCP server, the DHCP client would still accept the offer.

Options are detailed in RFC 2132.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
option	A text string that identifies a DHCP server configuration option.	N/A

Example --> dhcpclient interfaceconfig client1 add requested option irc-server

See also DHCPCLIENT INTERFACECONFIG ADD REQUESTED OPTION
DHCPCLIENT INTERFACECONFIG ADD REQUIRED OPTION

For information on RFC 2132, see http://www.ietf.org/rfc/rfc2132.txt

5.1.6.1.5 DHCPCLIENT INTERFACECONFIG ADD REQUIRED OPTION

Syntax DHCPCLIENT INTERFACECONFIG {<name>|<number>} ADD REQUIRED OPTION <option>

Description This command tells DHCP client that it requires a specified option from DHCP server. The required option is compulsory - if the option was not included in a lease offered by DHCP server, the DHCP client would ignore the offer.

Options are detailed in RFC 2132.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
option	A text string that identifies a DHCP server configuration option.	N/A

Example --> dhcpclient interfaceconfig client1 add required option domain-name

See also DHCPCLIENT INTERFACECONFIG ADD REQUESTED OPTION
DHCPCLIENT INTERFACECONFIG ADD REQUIRED OPTION

5.1.6.1.6 DHCPCLIENT INTERFACECONFIG ADD SENT OPTION

Syntax DHCPCLIENT INTERFACECONFIG {<NAME>|<NUMBER>} ADD SENT OPTION {SUBNET-MASK|DHCPLEASE-TIME|DHCP-CLIENT-IDENTIFIER|ROUTERS|DOMAIN-NAME-SERVERS} <VALUE>

Description This command tells the DHCP client to send a value for the given DHCP configuration option to a DHCP server. The DHCP server's response depends on the type of option being sent out.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
subnet-mask	A text string that identifies a DHCP server configuration option.	N/A
dhcp-leasetime	An option that can be used to request a specific lease duration by the client.	N/A
dhcp-clientidentifier	An option that can be used to specify the client identifier in a host declaration so that a DHCP server can find the host record by matching against the client identifier.	N/A
Routers	An option that provides IP address of a known router to the ARTMOS DHCP configuration when DHCP server configuration is given.	N/A
Domainnameservers	An option that requests the IP address of any DNS server.	N/A
value	The value associated with the option identifier.	N/A

Example --> dhcpclient interfaceconfig client1 add sent option host-name "'vancouver'"

This command example tells the DHCP client to send the DHCP host-name option to the DHCP server with the value "vancouver". Note that for options with string-type values associated with them, the option value must be in double-quotes (" "). Also, the entire string including the double quotes must be inside single quotes (') to ensure that the CLI treats the double quotes literally.

See also DHCPCLIENT LIST INTERFACECONFIGS
DHCPCLIENT INTERFACECONFIG LIST SENT OPTIONS

5.1.6.1.7 DHCPCLIENT INTERFACECONFIG CLEAR SENT OPTIONS

Syntax DHCPCLIENT INTERFACECONFIG {<name>|<number>} CLEAR SENT OPTIONS

Description This command deletes all options that were previously added to an interfaceconfig using the DHCPCLIENT INTERFACECONFIG ADD SENT OPTION command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A

Example --> dhcpclient interfaceconfig client1 clear sent options

See also DHCPCLIENT LIST INTERFACECONFIGS
DHCPCLIENT INTERFACECONFIG LIST SENT OPTIONS
DHCPCLIENT INTERFACECONFIG ADD SENT OPTION
DHCPCLIENT INTERFACECONFIG DELETE SENT OPTION

5.1.6.1.8 DHCPCLIENT INTERFACECONFIG CLEAR REQUESTED OPTIONS

Syntax DHCPCLIENT INTERFACECONFIG {<name>|<number>} CLEAR REQUESTED OPTIONS

Description This command deletes all options that were previously added to an interfaceconfig using the DHCPCLIENT INTERFACECONFIG ADD REQUESTED/REQUIRED OPTION commands.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A

Example --> dhcpclient interfaceconfig client1 clear requested options

See also
```
DHCPCLIENT LIST INTERFACECONFIGS
DHCPCLIENT INTERFACECONFIG ADD REQUESTED OPTION
DHCPCLIENT INTERFACECONFIG ADD REQUIRED OPTION
DHCPCLIENT INTERFACECONFIG DELETE REQUESTED OPTION
```

5.1.6.1.9 DHCPCLIENT INTERFACECONFIG DELETE REQUESTED OPTION

Syntax
```
DHCPCLIENT INTERFACECONFIG {<name>|<number>} DELETE
REQUESTED OPTION <option number>
```

Description This command deletes a single option that was previously added to an interfaceconfig using the dhcpclient interfaceconfig add requested/required option commands.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
option number	A number that identifies an option that is requested from the DHCP server by the DHCP client. To display option numbers, use the DHCPCLIENT INTERFACECONFIG LIST REQUESTED OPTIONS command.	N/A

Example --> dhcpclient interfaceconfig client1 delete requested option 1

See also DHCPCLIENT LIST INTERFACECONFIGS
DHCPCLIENT INTERFACECONFIG ADD REQUESTED OPTION
DHCPCLIENT INTERFACECONFIG ADD REQUIRED OPTION
DHCPCLIENT INTERFACECONFIG CLEAR REQUESTED OPTIONS

5.1.6.1.10 DHCPCLIENT INTERFACECONFIG DELETE SENT OPTION

Syntax DHCPCLIENT INTERFACECONFIG {<name>|<number>} DELETE SENT OPTION <option number>

Description This command deletes a single option that was previously added to an interfaceconfig using the DHCPCLIENT INTERFACECONFIG ADD SENT OPTION command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
option number	A number that identifies an option that is sent from the DHCP client to the DHCP server. To display option numbers, use the DHCPCLIENT INTERFACE-CONFIG LIST SENT OPTIONS command.	N/A

Example --> dhcpclient interfaceconfig client1 delete sent option 5

See also DHCPCLIENT LIST INTERFACECONFIGS
DHCPCLIENT INTERFACECONFIG LIST SENT OPTIONS
DHCPCLIENT INTERFACECONFIG ADD SENT OPTION
DHCPCLIENT INTERFACECONFIG CLEAR SENT OPTIONS

5.1.6.1.11 DHCPCLIENT INTERFACECONFIG LIST REQUESTED OPTIONS

Syntax DHCPCLIENT INTERFACECONFIG {<name>|<number>} LIST REQUESTED OPTIONS

Description This command lists the options that the DHCP client requests and/or requires from the DHCP server. These options were set using the dhcpclient interfaceconfig add requested/required option commands. The following information is displayed:

- Option identification number
- Option identifier (name)
- Requirement status - true for options that were added using the dhcpclient interfaceconfig add required option command, false for options added using the dhcpclient interfaceconfig add requested option command.

Options and their values are detailed in RFC2132.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A

Example --> dhcpclient interfaceconfig client1 list requested options

```
 ID  |       Identifier    | Is option required?
-----|---------------------|---------------------
   1 | host-name           | true
   2 | domain-name         | false
-------------------------------------------------
```

See also DHCPCLIENT INTERFACECONFIG ADD REQUESTED OPTION
DHCPCLIENT INTERFACECONFIG ADD REQUIRED OPTION
DHCPSERVER SUBNET ADD OPTION

For information on RFC 2132, see http://www.ietf.org/rfc/rfc2132.txt

5.1.6.1.12 DHCPCLIENT INTERFACECONFIG LIST SENT OPTIONS

Syntax DHCPCLIENT INTERFACECONFIG {<name>|<number>} LIST SENT OPTIONS

Description This command displays a list of the options that the DHCP client sends to the DHCP server. These options were set using the dhcpclient interfaceconfig add sent option command. The following information is displayed:

- Option identification number
- Option identifier (name)
- Suggested value

Options and their values are detailed in RFC2132.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A

Example --> dhcpclient interfaceconfig client1 list sent options

```
DHCP client options to be sent to server for client1:
 ID  |       Identifier   | Suggested Value
-----|--------------------|---------------------
   1 | host-name          | vancouver
   2 | domain-name        | alliedtelesyn
-------------------------------------------------
```

See also DHCPCLIENT INTERFACECONFIG ADD SENT OPTION
DHCPCLIENT INTERFACECONFIG CLEAR SENT OPTIONS
DHCPCLIENT INTERFACECONFIG DELETE SENT OPTION
DHCPSERVER SUBNET ADD OPTION

For information on RFC 2132, see http://www.ietf.org/rfc/rfc2132.txt

5.1.6.1.13 DHCPCLIENT LIST INTERFACECONFIGS

Syntax DHCPCLIENT LIST INTERFACECONFIGS

Description This command lists the following information about existing DHCP client interfaces:

- Interface identification number
- Interface name
- IP interface configured by the client interface
- Requested lease time (in seconds)
- Client identifier (if set)
- Status of ip address auto-configuration (true or false)

Example --> dhcpclient list interfaceconfigs

```
DHCP Client Declarations:
      Requested
 ID  |   Name  | Interface | Lease Time | Client ID         | AutoIP
-----|---------|-----------|------------|-------------------|-------
   1 | client1 | ip1       | 9000       | 00:11:22:33:44:5a | true
-------------------------------------------------------------------
```

See also DHCPCLIENT SHOW
DHCPCLIENT SET INTERFACECONFIG REQUESTEDLEASETIME
DHCPCLIENT SET INTERFACECONFIG CLIENTID
DHCPCLIENT SET INTERFACECONFIG AUTOIP ENABLED|DISABLED

5.1.6.1.14 DHCPCLIENT SET BACKOFF

Syntax DHCPCLIENT SET BACKOFF <backofftime>

Description This command sets the global maximum time (in seconds) that a DHCP client interface will 'back off' between issuing individual DHCP requests. This prevents many clients trying to configure themselves at the same time, and sending too many requests at once.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
backofftime	The maximum number of seconds that the DHCP client can pause for between unsuccessful DHCP negotiations.	120

Example --> dhcpclient set backoff 200

See also DHCPCLIENT SHOW

5.1.6.1.15 DHCPCLIENT SET INTERFACECONFIG AUTOIP ENABLED|DISABLED

Syntax `DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} AUTOIP {ENABLED | DISABLED}`

Description This command enables/disables IP address auto-configuration (Auto-IP).

Auto-IP automatically configures an IP address when a DHCP client fails to contact a DHCP server and cannot obtain a lease. An IP address on the 169.254 subnet is automatically created, and ARP requests are issued for the suggested IP address. The address is abandoned if it already exists on the network or if any other host on the network issues an ARP probe for that IP address.

Once an IP address has been automatically configured, the DHCP client continues to check whether it can contact a DHCP server. If the client can contact a DHCP server and obtain a legitimate lease, the legitimate lease will supersede the auto-configured IP address.

Note: Even if you have enabled Auto-IP using this command, you will not be able to use IP address auto-configuration if a DHCP server on the same network does not allow it. See the dhcpserver subnet add option command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the `DHCPCLIENT LIST INTERFACECONFIGS` command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the `DHCPCLIENT LIST INTERFACECONFIGS` command.	N/A
enabled	Enables Auto-IP on a specified dhcp client.	enabled
disabled	Disables Auto-IP on a specified dhcp client.	

Example --> dhcpclient set interfaceconfig mycfg autoip enabled

See also `DHCPSERVER SUBNET ADD OPTION`

For further information on the RFC standard for DHCP IP address auto-configuration, see http://www.ietf.org/rfc/rfc2563.txt

5.1.6.1.16 DHCPCLIENT SET INTERFACECONFIG CLIENTID

Syntax `DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} CLIENTID <clientid>`

Description This command sets a unique client identifier that DHCP server uses to identify the client.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the `DHCPCLIENT LIST INTERFACECONFIGS` command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the `DHCPCLIENT LIST INTERFACECONFIGS` command.	N/A
client id	A unique identifier that DHCP server can use to identify the client. By default it is the MAC address of the CPE. The client ID can be a MAC address or a text string such as the hostname. The string must be entered as hexadecimal values separated by colon.	N/A

Example --> dhcpclient set interfaceconfig client1 clientid 00:11.22.33.44.5a

See also `DHCPCLIENT LIST INTERFACECONFIGS`

5.1.6.1.17 DHCPCLIENT SET INTERFACECONFIG DEFAULTROUTE ENABLED|DISABLED

Syntax `DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} DEFAULTROUTE {ENABLED|DISABLED}`

Description This command enables/disables whether DHCP client makes use of default gateway information received from a DHCP server. If no DHCP interfaceconfigs have been added to the system, by default DHCP client will use default gateway information received from DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
enabled	DHCP client uses default gateway information it receives from DHCP server.	enabled
disabled	DHCP client does not use default gateway information it receives from DHCP server.	

Example --> dhcpclient set interfaceconfig client1 defaultroute disabled

See also DHCPCLIENT LIST INTERFACECONFIGS

5.1.6.1.18 DHCPCLIENT SET INTERFACECONFIG DHCPINFORM ENABLED|DISABLED

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} DHCPINFORM {ENABLED|DISABLED}

Description This command enables/disables whether DHCP client uses the ***dhcpinform*** message type. This DHCP message type is used whenever a client has obtained an IP address or subnet mask (for example, the address has been manually configured or obtained through PPP/IPCP), but wishes to obtain extra configuration parameters (such as DNS servers or default gateway) from a DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A

number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
enabled	Enables the dhcpinform message type. IP address and subnet mask will not be negotiated if this mode is selected.	disabled
disabled	Disables the dhcpinform message type.	

Example --> dhcpclient set interfaceconfig client1 dhcpinform disabled

See also DHCPCLIENT LIST INTERFACECONFIGS
DHCPCLIENT SET INTERFACECONFIG SERVER

5.1.6.1.19 DHCPCLIENT SET INTERFACECONFIG DHCPSERVERPOOLSIZE

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} DHCPSERVER-POOLSIZE <pool size>

Description This command tells DHCP client to configure a DHCP server on the LAN if the given address pool size is set to a number greater than 0. The LAN DHCP server is configured using parameters received by a DHCP client interface on the WAN. Information such as DNS server addresses can then be distributed to LAN clients. The new DHCP server gives out the default gateway address as its LAN IP address.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
pool size	The number of DHCP client addresses in a pool. The first address in the pool is the address immediately after the LAN DHCP address. For example, if the LAN DHCP address is 192.168.102.3, the first address in the pool will be 192.168.102.4.	N/A

Example --> dhcpclient set interfaceconfig client1 dhcpserverpoolsize 5

See also DHCPCLIENT LIST INTERFACECONFIGS

5.1.6.1.20 DHCPCLIENT SET INTERFACECONFIG DHCPSERVERINTERFACE

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} DHCPSERVER-INTERFACE <interface name>

Description This command allows the user to specify an existing IP interface on which the automatically configured DHCP server can be created. If the interface name does not correspond with an existing IP interface, or no interface name is given, the DHCP server will be placed on the first LAN interface that it finds.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
interface name	The name that identifies an existing IP interface. To display IP interface names, use the IP LIST INTERFACES command.	N/A

Example --> dhcpclient set interfaceconfig client1 dhcpserverinterface ip2

See also DHCPCLIENT LIST INTERFACECONFIG
DHCPCLIENT SET INTERFACECONFIG DHCPSERVERPOOLSIZE
IP LIST INTERFACES

5.1.6.1.21 DHCPCLIENT SET INTERFACECONFIG FORCERENEW

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} FORCERENEW {ENABLED | DISABLED}

Description This command sets whether the DHCP client is allowed to respond to DHCPFORCERENEW requests received on the appropriate interface. If such a request is accepted, the

DHCP client will attempt to renew its lease early or, if using DHCPINFORM, will attempt to obtain a new set of configuration parameters from the DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
enabled	DHCP client responds to DHCPFORCERENEW requests	disabled
disabled	DHCP client does not respond to DHCPFORCERENEW requests	

Example --> dhcpclient set interfaceconfig forcerenew enabled

See also DHCPCLIENT SET INTERFACECONFIG DHCPINFORM ENABLED|DISABLED
DHCPSERVER FORCERENEW

5.1.6.1.22 DHCPCLIENT SET INTERFACECONFIG GIVEDNSTOCLIENT ENABLED|DISABLED

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} GIVEDNSTOCLIENT {ENABLED|DISABLED}

Description This command enables/disables whether DHCP client passes received DNS server addresses to DNS client. If no DHCP interfaceconfigs have been added to the system, by default DHCP client will not pass DNS server addresses to DNS client.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
enabled	DHCP client passes DNS server addresses to DNS client.	disabled
disabled	DHCP client does not pass DNS server addresses to DNS client.	

Example --> dhcpclient set interfaceconfig client1 givednstoclient disabled

See also DHCPCLIENT LIST INTERFACECONFIGS

5.1.6.1.23 DHCPCLIENT SET INTERFACECONFIG GIVEDNSTORELAY ENABLED|DISABLED

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} GIVEDNSTORELAY {ENABLED|DISABLED}

Description This command enables/disables whether DHCP client passes received DNS server addresses to DNS relay. If no DHCP interfaceconfigs have been added to the system, by default DHCP client will pass DNS server addresses to DNS relay.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A

number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
enabled	DHCP client passes DNS server addresses to DNS relay.	enabled
disabled	DHCP client does not pass DNS server addresses to DNS relay.	

Example --> dhcpclient set interfaceconfig client1 givednstorelay disabled

See also DHCPCLIENT LIST INTERFACECONFIGS

5.1.6.1.24 DHCPCLIENT SET INTERFACECONFIG INTERFACE

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} INTERFACE <ipinterface>

Description This command sets the IP interface that will have its configuration set by the DHCP client interface. The client interface can only set the IP configuration if the IP interface has DHCP enabled, using the ip set interface dhcp command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
ipinterface	An existing IP interface **with DHCP enabled**. To display interface names, use the IP LIST INTERFACES command.	N/A

Example --> dhcpclient set interfaceconfig client1 interface ip2

See also DHCPCLIENT LIST INTERFACECONFIGS
IP LIST INTERFACES
IP SET INTERFACE DHCP

5.1.6.1.25 DHCPCLIENT SET INTERFACECONFIG NOCLIENTID

Syntax `DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} NOCLIENTID`

Description This command deletes a client identifier from a DHCP client. The DHCP server must have 'allowunknownclients' enabled in order to work with DHCP clients that are not specifically named in DHCP server configuration or its lease database.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the `DHCPCLIENT LIST INTERFACECONFIGS` command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the `DHCPCLIENT LIST INTERFACECONFIGS` command.	N/A

Example --> dhcpclient set interfaceconfig client1 noclientid

See also `DHCPCLIENT SET INTERFACECONFIG CLIENTID`
`DHCPSERVER SET ALLOWUNKNOWNCLIENTS`

5.1.6.1.26 DHCPCLIENT SET INTERFACECONFIG REQUESTEDLEASETIME

Syntax `DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} REQUESTEDLEASETIME <requestedleasetime>`

Description The DHCP client requests a specific lease time from the DHCP server for the allocated IP addresses. This command determines the length of lease time requested. The DHCP server will 'cap' a requested lease time if it is too large.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
requested lease time	The lease time (in seconds) that a DHCP client requests from the DHCP server.	86400

Example --> dhcpclient set interfaceconfig client1 requestedleasetime 70000

See also DHCPCLIENT LIST INTERFACECONFIGS
DHCPSERVER SET MAXLEASETIME
DHCPSERVER SET DEFAULTLEASETIME

5.1.6.1.27 DHCPCLIENT SET INTERFACECONFIG SERVER

Syntax DHCPCLIENT SET INTERFACECONFIG {<name>|<number>} SERVER <ipaddress>

Description If dhcpclient set dhcpinform has been set to enabled, this command will unicast the first DHCPINFORM message to the specific DHCP server at the specified IP address. If the first unicast fails, the DHCPINFORM will default to broadcasting its messages.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing DHCP client interface. To display client interface names, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
number	An existing DHCP client interface. To display client interface numbers, use the DHCPCLIENT LIST INTERFACECONFIGS command.	N/A
ipaddress	The IP address of a DHCP server that DHCP client can use to obtain configuration parameters. The IP address is displayed in the following format: 192.168.102.3	N/A

Example --> dhcpclient set interfaceconfig client1 server 192.168.101.2

See also DHCPCLIENT SET INTERFACECONFIG DHCPINFORM ENABLED|DISABLED

5.1.6.1.28 DHCPCLIENT SET BROADCAST-FLAG

Syntax DHCPCLIENT SET BROADCAST-FLAG ENABLE|DISBALE

Description This command set the broadcast flag in the dhcpclient request. The default value is enable

Example --> dhcpclient set broadcast-flag disable

5.1.6.1.29 DHCPCLIENT SET INITIALINTERVAL

Syntax DHCPCLIENT SET INITIALINTERVAL <initialinterval>

Description This command sets the first polling interval for the DHCP client

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
initialintervall	The time (in seconds) between the first and the second DHCP request.	10

Example --> dhcpclient set initialintervall 3600

5.1.6.1.30 DHCPCLIENT SET REBOOT

Syntax `DHCPCLIENT SET REBOOT <reboottime>`

Description When the DHCP client is restarted, it tries to reacquire the last address that it had. This command sets the time between the client trying to reacquire its last address and giving up then trying to discover a new address.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
reboottime	The time (in seconds) between a client attempt to reacquire its previous IP address and its giving up to find a new one.	10

Example --> dhcpclient set reboot 5

5.1.6.1.31 DHCPCLIENT SET RETRY

Syntax `DHCPCLIENT SET RETRY <RETRYTIME>`

Description This command sets the time that must pass after the client has determined that no DHCP server is present before it tries again to contact a DHCP server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
retrytime	The time (in seconds) that must pass after the client has determined that no DHCP server is present before it tries again to contact a DHCP server.	300

Example --> dhcpclient set retry 150

5.1.6.1.32 DHCPCLIENT SET FORCE-BROADCAST-RENEW

Syntax `DHCPCLIENT SET FORCE-BROADCAST-RENEW {ENABLED|DISABLED}`

Description This command force the dhcpclient to renew the ip address always in broadcast mode. DHCPREQUEST are sent to a broadcast address instead to be sent in unicast mode to the DHCP server.

The command does not have effect until the DHCPCLIENT UPDATE command is entered.

To retrieve the current settings, use the DHCPCLIENT SHOW command.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enabled	Force the dhcpclient to renew the ip address always in broadcast mode	
disabled	Do not force the dhcpclient to renew the ip address always in broadcast mode,	disabled

Example --> dhcpclient set force-broadcast-renew enabled

5.1.6.1.33 DHCPCLIENT SHOW

Syntax `DHCPCLIENT SHOW`

Description This command displays the following global configuration information about DHCP client:

- reboot time
- retry time
- maximum backoff time
- ip renewal mode

Example --> dhcpclient show

```
Global DHCP Client Configuration:
        Reboot time: 10
         Retry time: 300
  Max. backoff time: 120
    Broadcast Renew: false
```

See also `DHCPCLIENT SET REBOOT`
`DHCPCLIENT SET RETRY`
`DHCPCLIENT SET BACKOFF`

5.1.7 DHCP Relay Command Reference

This section describes the commands available on AT-RG624/634/644 Residential Gateway to enable, configure and manage DHCP Relay module.

5.1.7.1 DHCP relay CLI commands

The table below lists the DHCP relay commands provided by the CLI:

TABLE 5-3 DHCP Relay Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DHCPRELAY ADD SERVER	X	X	X	X	X	X	X	X	X
DHCPRELAY CLEAR SERVERS	X	X	X	X	X	X	X	X	X
DHCPRELAY DELETE SERVER	X	X	X	X	X	X	X	X	X
DHCPRELAY ENABLE|DISABLE	X	X	X	X	X	X	X	X	X
DHCPRELAY LIST SERVERS	X	X	X	X	X	X	X	X	X
DHCPRELAY SHOW	X	X	X	X	X	X	X	X	X
DHCPRELAY UPDATE	X	X	X	X	X	X	X	X	X

5.1.7.1.1 DHCPRELAY ADD SERVER

Syntax `DHCPRELAY ADD SERVER <IPADDRESS>`

Description This command adds the IP address of a DHCP server to the DHCP relay's list of server IP addresses. The relay can store a maximum of 10 DHCP server addresses. Any new server IP addresses added are not actually used until the DHCPRELAY UPDATE command has been entered.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ipaddress	The IP address of a DHCP server that DHCP relay can use. The IP address is displayed in the IPv4 format (e.g 192.168.102.3)	N/A

Example --> dhcprelay add server 239.252.197.0

See also
```
dhcpserver list subnets
dhcprelay update
```

5.1.7.1.2 DHCPRELAY CLEAR SERVERS

Syntax `dhcprelay clear servers`

Description This command deletes all DHCP server IP addresses stored in DHCP relay's list of server IP addresses.

Example --> dhcprelay clear servers

See also `dhcprelay delete server`

5.1.7.1.3 DHCPRELAY DELETE SERVER

Syntax `DHCPRELAY DELETE SERVER <NUMBER>`

Description This command deletes a single DHCP server address stored in the DHCP relay's list of server IP addresses.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
number	A number that identifies the DHCP server in the DHCP relay's list of servers. To display server numbers, use the dhcprelay list servers command.	N/A

Example --> dhcprelay delete server 3

See also `dhcprelay list servers`
`dhcprelay clear servers`

5.1.7.1.4 DHCPRELAY ENABLE|DISABLE

Syntax `DHCPRELAY {ENABLE|DISABLE}`

Description This command enables/disables DHCP relay.

DHCP relay must be enabled in order to carry out any DHCP relay configuration.

Note: DHCP relay and DHCP server cannot be enabled at the same time. Trying to configure DHCP relay when DHCP server is enabled results in CLI warning message.

Options The following table gives the range of values for each option which can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enable	Enables configuration of DHCP relay.	enable
disable	Disables configuration of DHCP relay.	enable

Example --> dhcprelay enable

See also `dhcpserver enable|disable`

5.1.7.1.5 DHCPRELAY LIST SERVERS

Syntax `DHCPRELAY LIST SERVERS`

Description This command displays the DHCP relay's list of DHCP server IP addresses with their identification numbers.

Example --> dhcprelay list servers

```
DHCP Servers:

 ID  | IP Address
-----|-----------------
   1 | 192.168.102.3
   2 | 239.252.197.0
------------------------
```

See also `dhcpserver list subnets`

5.1.7.1.6 DHCPRELAY SHOW

Syntax `DHCPRELAY SHOW`

Description This command tells you whether DHCP relay is enabled or disabled.

Example --> dhcprelay show server

```
Global DHCP Relay Configuration:

                  Status: ENABLED
```

See also `DHCPRELAY ENABLE|DISABLE`

5.1.7.1.7 DHCPRELAY UPDATE

Syntax `DHCPRELAY UPDATE`

Description This command updates the DHCP relay configuration. Changes made to the relay configuration will not take effect until this command has been entered.

Example --> dhcprelay update

```
dhcprelay: Reset request acknowledged. Reset imminent.
```

5.2 Domain name system - DNS

DNS is an abbreviation for Domain Name System, a system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in TCP/IP networks, such as the Internet, to locate computers and services through user-friendly names. When a user enters a DNS name in an application, DNS services can resolve the name to other information associated with the name, such as an IP address.

For example, most users prefer a friendly name such as ***alliedtelesyn.com*** to locate a computer such as a mail or Web server on a network. A friendly name can be easier to learn and remember. However, computers communicate over a network by using numeric addresses. To make use of network resources easier, name services such as DNS provide a way to map the user-friendly name for a computer or service to its numeric address. If you have ever used a Web browser, you have used DNS.

The following graphic shows a basic use of DNS, which is finding the IP address of a computer based on its name.

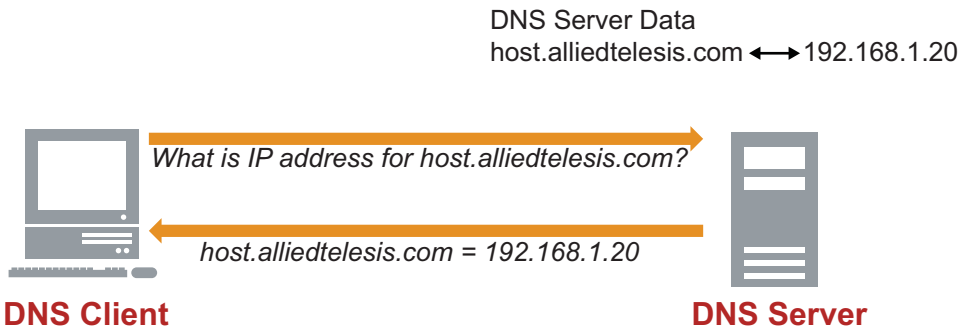


FIGURE 5-1 Domain Name System

In this example, a client computer queries a server, asking for the IP address of a computer configured to use host.alliedtelesyn.com as its DNS domain name. Because the server is able to answer the query based on its local database, it replies with an answer containing the requested information, which is a host (A) resource record that contains the IP address information for ***host.alliedtelesyn.com***. The example shows a simple DNS query between a single client and server. In practice, DNS queries can be more involved than this and include additional steps not shown here.

5.2.1 DNS Relay

gateway can act as a DNS relay. So, DNS packets that arrive at the Residential Gateway, addressed to the Residential Gateway, will be relayed on to a known DNS Server.

In this way, devices on the LAN can treat the Residential Gateway as though it were the DNS Server. Only the Residential Gateway needs to know the address of the real DNS Server looking into it is internal DNS Relay servers list.

It's possible configure the DHCP server running on the internal Residential Gateway's IP interface in order to offer the IP address of it's internal IP interface as DNS server's IP address for the internal hosts DNS requests.

It's also possible write a file named ***dnsrelaylandb*** with information about host attributes and a domain name and IP address mask. When DNS relay will receive a DNS request it will check if the answer to this request is in this file and in this case it will answer to the question; if it hasn't enough information it will forward the request to a DNS server.

It is possible to nominate both a primary and a secondary DNS server to contact. DNS responses received from the server are then forwarded back to the original host making the DHCP request.

Both UDP and TCP DNS requests are supported.

The DNS relay does not bind itself to any one specific interface or interface type, but rather will listen for traffic on all available IP interfaces. It relies on the well known UDP and TCP port number for a DNS server (port number 53) for receiving DNS traffic.

5.2.2 DNS Client

The ggatewayateway is provided with an internal DNS client, to use this function you must add DNS server addresses that will be used by the Residential Gateway ONLY for its own lookups.

5.2.3 DNS Relay command reference

This section describes the commands available on the gateway to enable, configure and manage the DNS Relay module.

5.2.3.1 DNS Relay CLI commands

The table below lists the ***DNSrelay*** commands provided by the CLI:

TABLE 5-4 DNS Relay Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DNSRELAY ADD LOCALDATABASE	X	X	X	X	X	X	X	X	X
DNSRELAY ADD SERVER	X	X	X	X	X	X	X	X	X
DNSRELAY CLEAR SERVERS	X	X	X	X	X	X	X	X	X
DNSRELAY DELETE SERVER	X	X	X	X	X	X	X	X	X
DNSRELAY ENABLE|DISABLE	X	X	X	X	X	X	X	X	X
DNSRELAY ENABLE|DISABLE	X	X	X	X	X	X	X	X	X
DNSRELAY SHOW	X	X	X	X	X	X	X	X	X
DNSRELAY LIST SERVERS	X	X	X	X	X	X	X	X	X
DNSRELAY SET HOSTNAME	X	X	X	X	X	X	X	X	X
DNSRELAY SET DYNAMICSERVERPRIORITY	X	X	X	X	X	X	X	X	X
DNSRELAY SET LANDOMAINNAME	X	X	X	X	X	X	X	X	X
DNSRELAY SHOW LANDOMAINNAME	X	X	X	X	X	X	X	X	X

5.2.3.1.1 DNSRELAY ADD LOCALDATABASE

Syntax `DNSRELAY ADD LOCALDATABASE <database> HOSTNAME <name> IPADDRSESS <ipaddress>`

Description This command create a local database specifying hostname and IP address.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
database	The name of the database	N/A
name	The name of the host	N/A
ip-address	The IP address of a the host	0.0.0.0

5.2.3.1.2 DNSRELAY ADD SERVER

Syntax `DNSRELAY ADD SERVER <ip-address>`

Description This command adds the IP address of a DNS server to DNS relay's list of server IP addresses. The relay can store a maximum of 10 DNS server addresses.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ip-address	The IP address of a DNS server that DNS relay can use, in the format: 192.168.102.3	0.0.0.0

Example --> dnsrelay add server 239.252.197.0

```
DNS server set to 0.0.0.0
DNS server set to 239.252.197.0
```

See also `DNSRELAY LIST SERVERS`

5.2.3.1.3 DNSRELAY CLEAR SERVERS

Syntax `DNSRELAY CLEAR SERVERS`

Description This command deletes all DNS server IP addresses stored in DNS relay's list of server IP addresses.

Example --> dnsrelay clear servers

See also `DNSRELAY DELETE SERVER`

5.2.3.1.4 DNSRELAY DELETE SERVER

Syntax `DNSRELAY DELETE SERVER <id-number>`

Description This command deletes a single DNS server address stored in DNS relay's list of server IP addresses.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ID number	A number that identifies the DNS server in the DNS relay list. To display server numbers, use the DNSRELAY LIST SERVERS command.	N/A

Example --> dnsrelay delete server 3

See also DNSRELAY LIST SERVERS

5.2.3.1.5 DNSRELAY ENABLE|DISABLE

Syntax DNSRELAY {ENABLE | DISABLE}

Description This command enables/disables DNS relay on your device. You must have DNS relay enabled in order to carry out any DNS relay configuration. If you try configuring DNS relay before you have entered the dnsrelay enable command, the CLI issues a warning message.

To display the current state of DNS relay, use the DNSRELAY SHOW command

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enable	Enables dnsrelay.	enable
disable	Disables dnsrelay.	

Example --> dnsrelay disable

See also DNSRELAY LIST SERVERS

5.2.3.1.6 DNSRELAY SHOW

Syntax DNSRELAY SHOW

Description This command indicates the status of DNS relay, enabled or disabled.

Example --> dnsrelay show

```
Global DNS Relay Configuration:
Status: ENABLED
```

See also DNSRELAY LIST SERVERS

5.2.3.1.7 DNSRELAY LIST SERVERS

Syntax DNSRELAY LIST SERVERS

Description This command displays the DNS relay's list of DNS server IP addresses with their identification numbers.

Example --> dnsrelay list servers

```
DNS Relay Servers:
 ID  | IP Address
-----|-----------------
   1 | 239.252.197.0
-----------------------
```

5.2.3.1.8 DNSRELAY SET HOSTNAME

Syntax DNSRELAY SET HOSTNAME <name>

Description This command sets the host name of your device.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The hostname that identifies your device.	N/A

Example --> dnsrelay set hostname myhost

See also DNSRELAY SET LANDOMAINNAME
DHCPSERVER SET SUBNET ASSIGNAUTODOMAIN

5.2.3.1.9 DNSRELAY SET DYNAMICSERVERPRIORITY

Syntax DNSRELAY SET DYNAMICSERVERPRIORITY ENABLE|DISABLE

Description This command enable or disable the dynamic server priority when more than one server is available.

5.2.3.1.10 DNSRELAY SET LANDOMAINNAME

Syntax DNSRELAY SET LANDOMAINNAME <name>

Description This command sets the LAN domain name of your device. DHCP server can then be configured to give out this address to DHCP clients.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The LAN domain name that identifies your device.	N/A

Example --> dnsrelay set landomainname alliedtelesyn.com

See also `DNSRELAY SET LANDOMAINNAME`
`DHCPSERVER SET SUBNET ASSIGNAUTODOMAIN`

5.2.3.1.11 DNSRELAY SHOW LANDOMAINNAME

Syntax `dnsrelay show landomainname`

Description This command displays the domain name used by the DNS relay to determine if a host name request is for the local database.

Example --> dnsrelay show landomainname

```
LAN Domain Name: alliedtelesyn.com
```

See also `DNSRELAY SET LANDOMAINNAME`

5.2.4 DNS Client command reference

This section describes the commands available on the gateway to enable, configure and manage the ***DNS Client*** module.

5.2.4.1 DNS Client CLI commands

The table below lists the ***DNSclient*** commands provided by the CLI:

TABLE 5-5 DNS Client Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
DNSCLIENT ADD SEARCHDOMAIN	X	X	X	X	X	X	X	X	X
DNSCLIENT ADD SERVER	X	X	X	X	X	X	X	X	X
DNSCLIENT CLEAR SEARCHDOMAINS	X	X	X	X	X	X	X	X	X
DNSCLIENT CLEAR SERVERS	X	X	X	X	X	X	X	X	X
DNSCLIENT DELETE SEARCHDOMAIN	X	X	X	X	X	X	X	X	X
DNSCLIENT DELETE SERVER	X	X	X	X	X	X	X	X	X
DNSCLIENT DELETE SERVER	X	X	X	X	X	X	X	X	X
DNSCLIENT LIST SEARCHDOMAINS	X	X	X	X	X	X	X	X	X
DNSCLIENT LIST SERVERS	X	X	X	X	X	X	X	X	X

5.2.4.1.1 DNSCLIENT ADD SEARCHDOMAIN

Syntax `DNSCLIENT ADD SEARCHDOMAIN <searchstring>`

Description This command creates a domain search list. The DNS client uses this list when a user asks for the IP address list for an incomplete domain name. The search string specified replaces any previous search strings added previously using this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
searchstring	A search string used to find the IP address for an incomplete domain name. You can have a maximum of 6 incomplete domain names in the search string.	N/A

Example --> dnsclient add searchdomain alliedtelesyn.com

See also `DNSCLIENT LIST SEARCHDOMAINS`

5.2.4.1.2 DNSCLIENT ADD SERVER

Syntax `DNSCLIENT ADD SERVER <ipaddress>`

Description This command adds a server IP address to the server list. This enables you to retrieve a domain name for a given IP address.

Options The following table gives the range of values for each that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ipaddress	The IP address of the server that has an unknown domain name. You can add a maximum of 3 addresses to the server list, in the format: 192.168.102.3	N/A

Example --> dnsclient add server 192.168.219.196

See also `DNSCLIENT LIST SERVERS`

5.2.4.1.3 DNSCLIENT CLEAR SEARCHDOMAINS

Syntax `DNSCLIENT CLEAR SEARCHDOMAINS`

Description This command deletes all domain names from the domain search list.

Example --> dnsclient clear searchdomains

See also `DNSCLIENT ADD SEARCHDOMAIN`
`DNSCLIENT DELETE SEARCHDOMAIN`

5.2.4.1.4 DNSCLIENT CLEAR SERVERS

Syntax `DNSCLIENT CLEAR SERVERS`

Description This command deletes all the server IP addresses to the server list.

Example --> dnsclient clear servers

See also `DNSCLIENT ADD SEARCHDOMAIN`
`DNSCLIENT DELETE SERVER`

5.2.4.1.5 DNSCLIENT DELETE SEARCHDOMAIN

Syntax `DNSCLIENT DELETE SEARCHDOMAIN <searchstring>`

Description This command deletes a single domain name from the domain search list.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
searchstring	A number that identifies a search string used to find the IP address for an incomplete domain name. To list domain search strings, use the DNSCLIENT LIST SEARCHDOMAINS command.	N/A

Example --> dnsclient delete searchdomain 1

See also DNSCLIENT CLEAR SEARCHDOMAINS
DNSCLIENT LIST SEARCHDOMAINS

5.2.4.1.6 DNSCLIENT DELETE SERVER

Syntax DNSCLIENT DELETE SERVER <number>

Description This command deletes a single server IP addresses from the server list.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
number	The server number that identifies an IP address of the server that has an unknown domain name. To display server numbers, use the DNSCLIENT LIST SERVERS command.	N/A

Example --> dnsclient delete server 1

See also DNSCLIENT CLEAR SERVERS
DNSCLIENT LIST SERVERS

5.2.4.1.7 DNSCLIENT LIST SEARCHDOMAINS

Syntax DNSCLIENT LIST SEARCHDOMAINS

Description This command lists the domain search strings that you have added to DNS client using the DNSCLIENT ADD SEARCHDOMAIN command. DNS client uses this list when a user asks for the IP address list for an incomplete domain name.

Example --> dnsclient list searchdomains

```
ID    | Domain
------|--------------------
```

```
   1 | alliedtelesyn.com
-------------------------
```

5.2.4.1.8 DNSCLIENT LIST SERVERS

Syntax `DNSCLIENT LIST SERVERS`

Description This command lists the server IP addresses that you have added to DNS client using the `DNSCLIENT ADD SERVER` command. DNS client uses this list to retrieve a domain name for a given IP address.

Example --> dnsclient list servers

```
DNS Client Servers:

 ID  | IP Address
 ----|-----------------
   1 | 192.168.100.7
    2 | 192.168.100.1
-----------------------
```

5.3 SNTP

The SNTP Version 4 client is an OSI Layer 7 application that allows the synchronization of gateway system clock to global sources of time-based information using UDP.

Its detailed implementation, which is described in RFC 2030, provides a complete and simplified method to access international time servers to receive, organize and adjust the time-synchronization of the local system.

The SNTP client described herein is a scaled down version of the Network Time Protocol (NTP) which is specified in RFC 1305. The main difference between an SNTP and an NTP client is the fact that most SNTP clients will interact with, at most, a single (S)NTP server. Also, SNTP Version 4 clients include an 'anycast' mode in addition to unicast and broadcast access modes not available in past versions of NTP/SNTP clients

5.3.1 SNTP features

The following features are available on the gateway:

- Boot time and runtime synchronization of the system clock can both be configured
- SNTP in the gateway system can function in one of three transfer modes:
  - **Unicast Mode**
    The SNTP client sends to a server, located at a specific previously configured address, a request for time synchronization and expects a reply only from that particular server
  - **Broadcast /Multicast Mode**
    A multicast NTP server periodically transmits a message to the local subnet broadcast address. The cli-

ent is configured to listen, and receives the synchronized time-based information. The client then configures itself based on this information, but sends no reply

- **Anycast Mode**
  When the client is configured in anycast mode, it sends out a sync request to a local subnet broadcast address. One or several anycast SNTP servers can respond with an individual timestamp and a unicast address. The client subsequently binds to the first response it receives and continues its operations in a unicast mode with that particular server. Any other server responses that are received by the client afterwards are ignored

- 64 local time zones (which include summertime /daylight savings time) configurations are supported (see Table 6).
- Automatic periodic timeserver polling is configurable
- Configuration of packet time-outs and retry transmissions is supported
- Getting NTP Time Server IP Addresses via DNS lookup can be used

The SNTP client mode session uses the standard remote UDP port 123 for all data transfers. Port 123 will be used in both the Source Port and Destination Port fields of the UDP header.

5.3.2 Time zones and daylight savings (summer time) conversion

Daylight Savings (a.k.a. Summer Time) time zones are configurable using the SNTP client. There is also a built-in firm ware mechanism for the automatic change to/from a standard time/daylight savings time. All the major world time zone changes are supported.

5.3.3 SNTP command reference

This section describes the commands available on gateway tgatewayo enable, configure and manage ***SNTP*** module.

5.3.3.1 SNTP CLI commands

The table below lists the ***SNTPclient*** commands provided by the CLI:

TABLE 5-6 DNS Client Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SNTPCLIENT ADD SERVER	X	X	X	X	X	X	X	X	X
SNTPCLIENT CLEAR SERVERS	X	X	X	X	X	X	X	X	X
SNTPCLIENT DELETE SERVER	X	X	X	X	X	X	X	X	X
SNTPCLIENT LIST SERVERS	X	X	X	X	X	X	X	X	X
SNTPCLIENT SET DAYLIGHTSAVINGTIME	X	X	X	X	X	X	X	X	X
SNTPCLIENT SET TIMEZONE	X	X	X	X	X	X	X	X	X
SNTPCLIENT SET MODE	X	X	X	X	X	X	X	X	X
SNTPCLIENT SET POLLINTV	X	X	X	X	X	X	X	X	X
SNTPCLIENT SYNC	X	X	X	X	X	X	X	X	X
SNTPCLIENT SET TIMEOUT	X	X	X	X	X	X	X	X	X
SNTPCLIENT SET RETRIES	X	X	X	X	X	X	X	X	X
SNTP SHOW STATUS	X	X	X	X	X	X	X	X	X
SNTPCLIENT SET CLOCK	X	X	X	X	X	X	X	X	X

5.3.3.1.1 SNTPCLIENT ADD SERVER

Syntax `SNTPCLIENT ADD SERVER {IPADDRESS <sntpipaddress> | HOSTNAME <sntphostname>}`

Description This command creates the dedicated unicast server for which the SNTP client can synchronize its time. You can add a server either by specifying the IP address or the hostname.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
sntpipaddress	The IP address of the dedicated unicast server that SNTP can use to synchronize its time.	N/A
sntphostname	The hostname of the dedicated unicast server that SNTP can use to synchronize its time.	N/A

Example Example 1 - IP address

--> sntpclient add server ipaddress 129.6.15.28

Example 2 - hostname

--> sntpclient add server hostname time-a.nist.gov

5.3.3.1.2 SNTPCLIENT CLEAR SERVERS

Syntax `SNTPCLIENT CLEAR SERVERS`

Description This command deletes the servers added using the sntpclient add server command.

Example --> sntpclient clear servers

See also `SNTPCLIENT ADD SERVER`

5.3.3.1.3 SNTPCLIENT DELETE SERVER

Syntax `SNTPCLIENT DELETE SERVER <serverid>`

Description This command deletes a single server previously added using the sntpclient add server command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
serverid	The server ID displayed by the `SNTPCLIENT LIST SERVERS` command.	N/A

Example --> sntpclient delete server 1

See also `SNTPCLIENT ADD SERVER`
`SNTPCLIENT LIST SERVERS`

5.3.3.1.4 SNTPCLIENT LIST SERVERS

Syntax `SNTPCLIENT LIST SERVERS`

Description This command lists the servers added using the `SNTPCLIENT ADD SERVER` command.

Example --> sntpclient list servers

```
SNTPClient Servers:
 ID  | IP Address
-----|-----------------
   1 | 239.252.197.0
-----------------------
```

See also `SNTPCLIENT ADD SERVER`

5.3.3.1.5 SNTPCLIENT SET DAYLIGHTSAVINGTIME

Syntax `SNTPCLIENT SET DAYLIGHTSAVINGTIME ENABLE|DISABLE`

Description This command sets the SNTP client to automatically switch between the standard time and the daylight saving time according to the time zone.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
enable	Enables the selected time synchronous access mode.	N/A
disable	Disables the selected time synchronous access mode.	N/A

Example --> sntpclient set daylightsavigntime enable

5.3.3.1.6 SNTPCLIENT SET TIMEZONE

Syntax `SNTPCLIENT SET TIMEZONE <timezone>`

Description This command sets the local time zone abbreviation as a parameter and configures the local system to be up to + 13 hours of the ***Universal Time Coordinate*** (UTC). Sixty-four of the world's most prominent time zones are represented (including those using standard time and summer/daylight savings time).

Options The following table gives the 64 time zone abbreviations that you can use in this command to set the timezone difference for the system timer. The table also contains the dif-

ference in time (in hours and minutes) from the UTC, and a description of the area of the world (from west to east) where the time difference is calculated:

TABLE 5-7 Time Abbreviations when Setting Timezone Difference

Time Zone	+ UTC	World Area of Time Zone
IDLW	-1200	International Date Line West
NT	-1100	Nome
HST	-1000	Hawaii Standard
AKST	-0900	Alaska Standard
YST	-0900	Yukon Standard
YDT	-0800	Yukon Daylight
PST	-0800	US Pacific Standard
MST	-0700	US Mountain Standard
MDT	-0600	US Mountain Daylight
CST	-0600	US Central Standard
EST	-0500	US Eastern Standard
AST	-0400	Atlantic Standard
NFST	-0330	Newfoundland Standard
NFT	-0330	Newfoundland
BRA	-0300	Brazil Standard
ADT	-0300	Atlantic Daylight
NDT	-0230	Newfoundland Daylight
AT	-0200	Azores
WAT	-0100	West Africa
GMT	+0000	Greenwich Mean
UTC	+0000	Universal (Coordinated)
WET	+0000	Western European
CET	+0100	Central European
FWT	+0100	French Winter

TABLE 5-7 Time Abbreviations when Setting Timezone Difference (Continued)

MET	+0100	Middle European
MEWT	+0100	Middle European Winter
SWT	+0100	Swedish Winter
BST	+0100	British Summer
EET	+0200	Eastern Europe
FST	+0200	French Summer
MEST	+0200	Middle European Summer
SST	+0200	Swedish Summer
IST	+0200	Israeli Standard
IDT	+0300	Israeli Daylight
BT	+0300	Baghdad
IT	+0330	Iran
USZ3	+0400	Russian Volga
USZ4	+0500	Russian Ural
INST	+0530	Indian Standard
USZ5	+0600	Russian West-Siberian
NST	+0630	North Sumatra
WAST	+0700	West Australian Standard
USZ6	+0700	Russian Yenisei
JT	+0730	Java
CCT	+0800	China Coast
WADT	+0800	West Australian Daylight
ROK	+0900	Korean Standard
KST	+0900	Korean Standard
JST	+0900	Japan Standard
CAST	+0930	Central Australian Standard
KDT	+1000	Korean Daylight

TABLE 5-7 Time Abbreviations when Setting Timezone Difference (Continued)

EAST	+1000	Eastern Australian Standard
GST	+1000	Guam Standard
CADT	+1030	Central Australian Daylight
EADT	+1100	Eastern Australian Daylight
IDLE	+1200	International Date Line East
NZST	+1200	New Zealand Standard
NZT	+1200	New Zealand
NZDT	+1300	New Zealand Daylight

Example In the example below, the time zone is set to Unites States Eastern Standard Time, which is five hours earlier than UTC (-0500):

--> sntpclient set timezone EST

5.3.3.1.7 SNTPCLIENT SET MODE

Syntax `SNTPCLIENT SET MODE {UNICAST|BROADCAST|ANYCAST} {ENABLE|DISABLE}`

Description This command enables/disables the STNP client in a particular time synchronous access mode. There are three modes to choose from, and each mode has enable and disable options:

Unicast mode

- **Enable**
  the mode uses a unicast server and the IP address or hostname in the SNTP server association list is used to synchronize the client time with the server. The SNTP client attempts to contact the specific server in the association in order to receive a timestamp when the `SNTPCLIENT SYNC COMMAND` is issued.
- **Disable**
  the unicast server is removed from the association list.

Broadcast mode

- **Enable**
  allows the SNTP client to accept time synchronization broadcast packets from an SNTP server located on the network, and updated the local system time accordingly.
- **Disable**
  stops synchronization via broadcast mode

Anycast mode

- **Enable**
  the SNTP client sends time synchronized broadcast packets to the network and subsequently expects a reply from a valid timeserver. The client then uses the first reply it receives to establish a link for future sync operations in unicast mode. This server will then be added to the server association list. The client ignores any later replies from servers after the first one is received.
  The enabled anycast mode takes precedence over any entries currently in the associations list when the SNTPCLIENT SYNC command is issued. The entry will then be substituted for any existing entry in the unicast association list.
- **Disable**
  stops synchronization via anycast mode.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
unicast	Sets the time synchronous access mode to use the unicast server.	N/A
broadcast	Sets the time synchronous access mode to use the broadcast server.	N/A
anycast	Sets the time synchronous access mode to use the anycast server.	N/A
enable	Enables the selected time synchronous access mode.	N/A
disable	Enables the selected time synchronous access mode.	N/A

Example --> sntpclient set mode anycast enable

See also SNTPCLIENT ADD SERVER
SNTP SHOW STATUS

5.3.3.1.8 SNTPCLIENT SET POLLINTV

Syntax SNTPCLIENT SET POLLINTV <pollintv>

Description This command sets the SNTP client to automatically send a time synchronization request (specific to the mode) to the network at a specific interval. If the poll-interval is set to 0, the polling mechanism will be disabled.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
pollintv	Sets the polling interval (in minutes) that SNTP client will sync with a designated server. This can be any value between 0 and 30.	0 (disabled)

Example --> sntpclient set pollintv 10

5.3.3.1.9 SNTPCLIENT SYNC

Syntax `SNTPCLIENT SYNC`

Description This command forces the SNTP client to immediately synchronize the local time with the server located in the association list (if unicast) or, if anycast is enabled, initiate an anycast sequence to the network.

Example --> sntpclient sync

See also `SNTPCLIENT ADD SERVER`

5.3.3.1.10 SNTPCLIENT SET TIMEOUT

Syntax `SNTPCLIENT SET TIMEOUT <timeout>`

Description This command sets the received packet response timeout value (in seconds) upon sync request initiation. After timeout, if the `SNTPCLIENT RETRY` command value is set, an attempt will be retried.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
timeout	Sets the received packet response timeout value (in seconds). This can be any value between 0 and 30.	5 seconds

Example --> sntpclient set timeout 10

See also `SNTPCLIENT SET RETRIES`

5.3.3.1.11 SNTPCLIENT SET RETRIES

Syntax `SNTPCLIENT SET RETRIES <retries>`

Description This command sets the number of packet retry attempts when no response is received from a timeserver. The SNTP client will send another packet for synchronization after a timeout.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
retries	Sets the number (between 0-10) of packet retry attempts made when no response is received from a timeserver.	2

Example --> sntpclient set retries 4

See also `SNTPCLIENT SET TIMEOUT`

5.3.3.1.12 SNTP SHOW STATUS

Syntax `SNTPCLIENT SHOW STATUS`

Description This command displays the SNTP client status information.

Example --> sntpclient show status

```
- SNTP CLIENT STATUS -
----------------------
Clock Synchronized:           TRUE
SNTP Standard Version Number: 4
SNTP Mode(s) Configured:      Unicast
Local Time:                   Mon, 14 Sep 2009 - 05:36:26
Local Timezone:               EST, US Eastern Standard Time
Time Difference +- UTC:       -4:00
Server Stratum:               3
Precision:                    1/1048576 of a second
Root Delay:                   +0.618 second(s)
Dispersion:                   0.5578 second(s)
Server Reference ID:          10.17.90.68
Round Trip Delay:             0 second(s)
Local Clock Offset:           -17999 second(s)
Resync Poll Interval:         20 minute(s)
Packet Retry Timeout:         5 second(s)
```

```
Packet Retry Attempts:        2
Daylight Saving :          Enabled
Daylight Saving Done :     True
sntpclient list servers
```

See also SNTPCLIENT LIST SERVERS

5.3.3.1.13 SNTPCLIENT SET CLOCK

Syntax SNTPCLIENT SET CLOCK <sntpclock>

Description This command sets the system clock to a specific time and date. This command can be used as an alternative to synchronizing the local system clock via internal or external timeservers.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
sntpclock	Sets the time and date of the system clock in the following format: yyyy:mm:dd:hh:mm:ss	N/A

Example The following command sets the system clock to 11:10:13pm, 29th December 2003:

--> sntpclient set clock 2003:12:29:23:10:13

6. Voice Service

6.1 VoIP MGCP

The MGCP (Media Gateway Control Protocol) is a protocol that assumes a call control architecture where the call control 'intelligence' is outside the gateways and is handled by external call control elements, the call agent. MGCP assumes that the gateways have limited storage and functionality.

So, there are two MGCP entities: Call Agent (Media Gateway Controller, MGC) which handles the call control 'intelligence', that means the call signaling and the call processing functions and the Media Gateway (MG) that provides conversion between the audio signals carried on telephone circuits and data packets carried over Internet or packets networks and expects to execute command sent by the Call Agent.

iMG/RG/iBG devices implement the Media gateway side.

MGCP is a master/slave protocol, while the call agent is mandatory and manages the calls and conferences and supports the services provided, the endpoint is unaware of the calls and conferences and does not maintain call states, it is simply expected to execute commands sent by the call agent.

6.1.1 MGCP Functional Description

6.1.1.1 Endpoints

iMG/RG/iBG devices support the configuration of each FXS (Foreign Exchange Station) voice port as a separate MGCP analogue endpoint allowing a different level of services (number of phone lines) to be delivered.

Each voice port is identified univocal through an endpoint identifier that, by default, takes the following syntax:

Syntax `aaln/<slot>@[$IP]`

where:

AALN -Analog Access Line eNdpoint. This name indicates that the endpoint is analog type (only FXS voice interfaces are supported).

<slot> - indicates the index of the voice port. Physical voice ports start with index 0, the second physical voice port uses index 1 and so on.

$IP - it's the ip address of the ip interface where the MGCP protocol is enabled. It is typically used in a multi host configuration where more than one IP interface is configured in the system or when the ip interface is dynamic and therefore the value is dynamically assigned by the network.

6.1.1.2 Custom endpoints syntax

iMG/RG/iBG devices allow analog endpoint MGCP identifiers to be customized to meet VoIP network configuration requirements.

The syntax of each endpoint identifier can be set to any string but must include at least a local name description in the format:

```
aaln/<slot>
```

The local and domain name part of an endpoint identifier can use also special keywords identified by the "$" sign that are automatically replaced by the value of the attribute that they represent.

The following two special keywords are supported:

$IP - when used, this keyword is automatically replaced by the ip address value (in IPv4 dotted format) of the ip interface where MGCP protocol has been enabled.

$MAC - when used, this keyword is automatically replaced by the MAC address of the iMG/RG/iBG device.

It's therefore possible create complex endpoint identifiers like the following:

aaln/0@[$IP] that will be translated at runtime for example in: aaln/0@[172.30.1.1]

aaln/0@$IP that will be translated at runtime for example in: aaln/0@172.30.1.1

aaln/0@$MAC that will be translated at runtime for example in: aaln/0@00:0d:da:01:fe:ac

$MAC:aaln/0@[$IP] that will be translated at runtime for example in: 00:0d:da:01:fe:ac:aaln/0@[172.30.1.1]

aaln/0@any-string-here

To specify a new endpoint syntax for an existing voice port the following command is used:

```
voip mgcp protocol set endpoint-syntax <ep-syntax> port <voice-port>
```

where

<ep-syntax> is the endpoint identifier string as described above

<voice-port> is the name of the physical voice port (tel1, tel2,...)

6.1.2 Piggyback

iMG/RG/iBG devices support piggy-back MGCP message handling.

As reported in RFC 2705, piggy-back refers to the support for a Call Agent to send several messages at the same time to the same gateway using the same UDP packet and separating each MGCP message by a line of text that contain a single dot.

Support for piggy-back is enabled by default on MG/RG/iBG devices and can be disabled/enabled via the following command:

```
voip mgcp protocol set piggyback disable|enable
```

6.1.3 Wildcard

MG/RG/iBG support wild card endpoint identifiers.

By default wild card support is disabled.

It can be enabled/disabled via the following CLI command:

```
voip mgcp protocol set wildcard enable|disable
```

When wild card support is enabled, MG/RG/iBG replace the local name description part of the endpoint identifier with the "*" char on RSIP messages.

In this case only one RSIP message is sent in order to notify to the call agent that all the endpoints have been taken out-of-service and are being replaced in service.

6.1.4 Heartbeat

iMG/RG/iBG support the heartbeat mechanism to detect whether User Agents are still active.

Each iMG/RG/iBG voice port has a unique User Agent permanently associated to it.

Heartbeat mechanism is typically requested on deployments that use Network Address Translation (NAT).

The reason for this requirement is that if a NAT binding expires, there is no way for a Call Agent to send an incoming call to the User Agent as NAT bindings are generated via outgoing UDP packets.

Using a heartbeat mechanism allows the User Agent to detect loss of the NAT binding (due for example to DSL uplink fails) and recreate it if required.

The heartbeat mechanism is implemented through the use of Audit commands as AuditConnection and AuditEndpoint

iMG/RG/iBG User Agents support a configurable heartbeat timer. The User Agent then waits for either the end of this timer, the reception of a command for the endpoint from the Call Agent, or the detection of a local user activity for the endpoint, such as for example an off-hook transition.

If the heartbeat timer expires the User Agent enters the "disconnected" procedure.The User Agents run a further disconnect timer and if they do not receive a command from the Call Agent or detect local activity before the timer expires, the User Agent sends an RSIP disconnected command to the Call Agent.

If it does not receive a response it continues to periodically retry to contact the provisioned Call Agents.

If the Call Agent is using the above heartbeat mechanism, the heartbeat timer should be set to a value that allows the Call Agent to send an audit command sufficiently often that the User Agent will see at least 3 audit commands in the heartbeat time interval. This is to prevent a single packet loss causing the User Agent to become "disconnected".

By default heartbeat is disabled and can be enabled via the following command:

```
voip mgcp protocol set heartbeat enable|disable
```

When heartbeat is enabled, each endpoint (or User Agent) supervises the operative status of Call Agent independently on the status of the other endpoints.

It's possible force a specific User Agent to check for Call Agent activity and to be master also for the other User Agents. If the specific endpoint does not receive a command from the Call Agent within the heartbeat timer time-out it forces all the User Agents to enter into the disconnected procedure.

To activate this behavior is necessary enable the heartbeat and then enter the following command:

By default heartbeat is disabled and can be enabled via the following command:

```
voip mgcp protocol set heartbeat port <endpoint-name>
```

To return to the default behavior is necessary disable the heartbeat and then re-enabling it.

6.1.5 Call Agent Failover

iMG/RG/iBG support dual Call Agents failover mechanism to switch between inactive to active call agents in order to support high availability services.

The failover mechanism is triggered any time a request sent by the User Agents does not get any answer from the Call Agent within the round-trip time-out.

In this case if more than one call agent is configured, the User Agent will re-send the same command toward the second call agent. As soon the User Agent get an answer from the second call agent, the second call agent becomes the active call agent and will be used for all the subsequent requests.

The process repeats any time a call agent is not reachable switching in this way the communications between primary call agent to secondary call agent and vice versa.

It's possible display the current active call agent checking the marker "*" character on the call agent list.

The active call agent is the call agent marked with the "*" char.

By default the first call agent in the call agents list is the call agent that iMG/RG/iBG will attempt to contact firstly.

It's possible changing the call agent order of preference specifying the attribute master:

```
voip mgcp callagent set <call-agent-name> master
```

Only one call agent at time can be master.

6.1.6 Functional Differences for VoIP MGCP in Product Categories

The table below is intended to identify what is common amongst the product families - as well as where there are differences - to highlight those differences. To determine which family your device belongs to - please refer to the preface.

TABLE 6-1 **Functional Mapping for VoIP MGCP**

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
Endpoints	X	X	X	X	X	X	X	X	X
Piggyback	X	X	X	X	X	X	X	X	X
Wildcard	X	X	X	X	X	X	X	X	X
Heartbeat	X	X	X	X	X	X	X	X	X
Call Agent Failover	X	X	X	X	X	X	X	X	X

6.1.7 VOIP MGCP command reference

This section describes the commands available on iMG/RG/iBG to configure and manage the MGCP protocol module.

6.1.7.1 VoIP MGCP CLI commands

The table below lists the ***voip mgcp*** commands provided by the CLI:

TABLE 6-2 ***VoIP MGCP*** commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP MGCP PROTOCOL DISABLE	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL ENABLE	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL RESTART	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SET DEFAULTPORT	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SET HEARTBEAT	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SET NAT	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SET NETINTERFACE	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SET PIGGYBACK	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SET PROFILE	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SET REFRESH-TIME	X	X	X	X	X	X	X	X	X

TABLE 6-2 *VoIP MGCP* commands **(Continued)**

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP MGCP PROTOCOL SET ROUNDTRIPTIME	X	X	X	X	X	X	X	X	X
VOIP MGCP PROTOCOL SHOW	X	X	X	X	X	X	X	X	X
VOIP MGCP CALLAGENT CREATE	X	X	X	X	X	X	X	X	X
VOIP MGCP CALLAGENT SET MASTER	X	X	X	X	X	X	X	X	X
VOIP MGCP CALLAGENT DELETE	X	X	X	X	X	X	X	X	X
VOIP MGCP CALLAGENT LIST	X	X	X	X	X	X	X	X	X

6.1.7.1.1 VOIP MGCP PROTOCOL DISABLE

Syntax `VOIP MGCP PROTOCOL DISABLE`

Description This command stops the VoIP MGCP signalling protocol and releases all the resources associated to it.

This command is typically used when it's necessary to change the VoIP signalling protocol, i.e. from MGCP to SIP.

To simply restart the MGCP module, use the VOIP MGCP PROTOCOL RESTART command. It doesn't remove any resources defined for the protocol.

To enable the MGCP module, use the VOIP MGCP PROTOCOL ENABLE command.

Example --> voip mgcp protocol disable

See also `VOIP MGCP PROTOCOL RESTART`
`VOIP MGCP PROTOCOL ENABLE`

6.1.7.1.2 VOIP MGCP PROTOCOL ENABLE

Syntax `VOIP MGCP PROTOCOL ENABLE`

Description This command turns on the MGCP signaling module.

To bind the MGCP module to a specific IP interface use the VOIP MGCP PROTOCOL SET NETINTERFACE command.

Binding the MGCP module to a specific IP interface defines the value of the source IP address for signalling and voice packets.

Description --> voip mgcp protocol enable

See also `VOIP MGCP PROTOCOL SHOW`
`VOIP MGCP PROTOCOL DISABLE`

6.1.7.1.3 VOIP MGCP PROTOCOL RESTART

Syntax `VOIP MGCP PROTOCOL RESTART`

Description This command restarts the VoIP MGCP signaling protocol module.

Any pending and active calls are released.

This command doesn't release any resources previously created during module configuration.

Example --> voip mgcp protocol restart

See also `VOIP MGCP PROTOCOL ENABLE`

6.1.7.1.4 VOIP MGCP PROTOCOL SET DEFAULTPORT

Syntax `VOIP MGCP PROTOCOL SET DEFAULTPORT <ipport>`

Description This command sets the default listening/sending port used for MGCP signaling messages. By default, when the MGCP module is attached to an IP interface using the VOIP MGCP PROTOCOL SET NETINTERFACE command, the following default value is used:

defaultport:2427

Changing the signaling port causes the MGCP module to restart.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ipport	UDP/TCP port number used for signalling messages. Available values are in the range 1026 to 65534. Only even values can be accepted	2427

Example --> voip mgcp protocol set defaultport 2427

See also `VOIP MGCP PROTOCOL ENABLE`

6.1.7.2 VOIP MGCP PROTOCOL SET ENDPOINT-SYNTAX

Syntax `VOIP MGCP PROTOCOL SET ENDPOINT-SYNTAX <ep-syntax> port <portname>`

Description This command allows to customize the endpoint identifier (EPID) used inside MGCP messages. The endpoint identifier syntax can be created using some variables listed in the following table:

TBD	TBD
$IP	It will be replaced with the gateway's IP Address
$MAC	It will be replaced with the gateway's MAC Address
$HOST	It will be replaced with the gateway's System name (If the system name is not configured the IP address will be used).

The endpoint identifier syntax default value depends on the used MGCP profile. The following table lists all the combinations.

TABLE 6-3 Possible Combinations for MGCP Profile

TBD	TBD
NONE, AGS, GB and SIEMENS	aaln/0@[$IP] for endpoint tel1 aaln/1@[$IP] for endpoint tel2 aaln/2@[$IP] for endpoint tel3 aaln/3@[$IP] for endpoint tel4
MARCONI	aaln/1@[$IP] for endpoint tel1 aaln/2@[$IP] for endpoint tel2 aaln/3@[$IP] for endpoint tel3 aaln/4@[$IP] for endpoint tel4
SPHERE	$MAC:aaln/0@[$IP] for endpoint tel1 $MAC:aaln/1@[$IP] for endpoint tel2 $MAC:aaln/2@[$IP] for endpoint tel3 $MAC:aaln/3@[$IP] for endpoint tel4
CISCOBTS	aaln/0@$IP for endpoint tel1 aaln/1@$IP for endpoint tel2 aaln/2@$IP for endpoint tel3 aaln/3@$IP for endpoint tel4

If system name is not set and/or it is not configured by DHCP, $HOST variable must be replaced by the IP address.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ep-syntax	It is the endpoint identifier used by the gateway and by the Call Agent in the command messages.	-

Example Suppose to have a device with the following parameter values:
IP Address=10.17.90.135
MAC Address=10:20:30:40:50:61
System name=gatewat-90-135

Example `--> voip mgcp prot set endpoint-syntax aaln/0@[$IP] port tel1`

The endpoint identifier is: aaln/0@[10.17.90.135]

Example `--> voip mgcp prot set endpoint-syntax $MAC:aaln/0@[$IP] port tel1`

The endpoint identifier is: 102030405061:aaln/0@[10.17.90.135]

Example `--> voip mgcp prot set endpoint-syntax $MAC:aaln/1@[$HOST] port tel2`

The endpoint identifier is: 102030405061:aaln/1@[gatewat-90-135]

Example `--> voip mgcp prot set endpoint-syntax tel3@[$HOST] port tel3`

The endpoint identifier is: tel3@[gatewat-90-135]

Example `--> voip mgcp prot set endpoint-syntax aaln/0@$IP port tel1`

The endpoint identifier is: aaln/0@10.17.90.135

6.1.7.2.1 VOIP MGCP PROTOCOL SET HEARTBEAT

Syntax `VOIP MGCP PROTOCOL SET HEARTBEAT {ENABLE|DISABLE}`

Description This command enables/disables the heartbeat feature. The heartbeat consists on a MGCP message periodically sent by the gateway to inform the callagent that the end points are up and running. The heartbeat is implemented only under some specific MGCP profiles and the sent heartbeat message is different for each profile. The following table lists the profiles and heartbeat messages.

TBD	TBD
sphere	NTFY 48 000dda010203:aaln/0[192.168.1.10] MGCP 1.0 X: 1234567 N: hb
nuera	RSIP 48 aaln/0[192.168.1.10] MGCP 1.0 NCS 1.0 RM: x-refresh
siemens	RSIP 48 aaln/0[192.168.1.10] MGCP 1.0 RM: x-keepalive

Example `--> voip mgcp protocol set heartbeat enable`

See also `VOIP MGCP PROTOCOL SET PROFILE`
`VOIP MGCP PROTOCOL SET REFRESH-TIME`

6.1.7.2.2 VOIP MGCP PROTOCOL SET NAT

Syntax `VOIP MGCP PROTOCOL SET NAT {NONE | <host>}`

Description This command sets the NAT host reference. Any MGCP message with local reference is hidden by the NAT address value.

Changing the NAT reference causes the MGCP module to restart.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Example `--> voip mgcp protocol set nat 10.17.90.110`

Option	Description	Default Value
host	The address that must displayed in the MGCP messages. It can be expressed in hostname format or IPv4 format. A Hostname can be a maximum of 255 characters long.	None

Example --> voip mgcp protocol set nat at-img600.voip.atkk.com

See also `VOIP MGCP PROTOCOL ENABLE`

6.1.7.2.3 VOIP MGCP PROTOCOL SET NETINTERFACE

Syntax `VOIP MGCP PROTOCOL SET NETINTERFACE <interface_name>`

Description This command sets the IP interface used to access the VoIP network.
Signaling and voice packets will use the Source IP address defined for the selected interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
interface_name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A

Example `--> voip MGCP protocol set netinterface ip0`

See also `VOIP MGCP PROTOCOL ENABLE`

6.1.7.2.4 VOIP MGCP PROTOCOL SET PIGGYBACK

Syntax `VOIP MGCP PROTOCOL SET PIGGYBACK {ENABLE|DISABLE}`

Description This command enables/disables the MGCP piggy-back feature as described in RFC3435 (3.5.5 Piggy backing). This feature is enabled by default. This command allow the user to disable it.

Example `--> voip mgcp protocol set piggyback disable`

6.1.7.2.5 VOIP MGCP PROTOCOL SET PROFILE

Syntax `VOIP MGCP PROTOCOL SET PROFILE <profile>`

Description This command sets specific customer MGCP call agent profile. This command is used to fix inter operability constraints when the MGCP module has to work with call agent that could differ from a standard implementation.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
profile	The specific customer call-agent type. Possible values are: ags, audiocodes, ciscobts, gb, huawei, marconi, metaswitch, ncs, netcentrex, nuera, siemens, sphere, sttnortel and none.	none

Example `--> voip mgcp protocol set profile ags`

6.1.7.2.6 VOIP MGCP PROTOCOL SET REFRESH-TIME

Syntax `VOIP MGCP PROTOCOL SET REFRESH-TIME <sec>`

Description This command sets the refresh time used by the heartbeat feature. In other words, this command sets the seconds between two successive heartbeat messages. In some profiles the heartbeat messages is sent if there are not activity (no other MGCP messages) sent/ received by the endpoint.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
sec	Number of seconds between two heartbeat message.	none

Example `--> voip mgcp protocol set refresh-time 30`

6.1.7.2.7 VOIP MGCP PROTOCOL SET ROUNDTRIPTIME

Syntax `VOIP MGCP PROTOCOL SET ROUNDTRIPTIME <msec>`

Description This command sets the maximum time out that an MGCP message needs to be acknowledged by the call agent before the same message is retrasmitted.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
msec	Maximum number of milliseconds that the system wait for an answer from the call agent.	1000

Example
```
--> voip mgcp protocol set roundtriptime 1500
```

6.1.7.2.8 VOIP MGCP PROTOCOL SHOW

Syntax `VOIP MGCP PROTOCOL SHOW [<name>]`

Description This command displays basic MGCP module configuration parameters set by the VOIP MGCP PROTOCOL ENABLE command.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP LIST command.	N/A

Example
```
--> voip mgcp protocol show

    Gateway base protocol: MGCP
    ------------------------------------------------------
       Profile:                          sphere
       Supported packages:               Basic, Generic Media, DTMF, Line
       Piggy-Back:                       Enable
       Network interface:                ip0
       Default port:                     2427
       NAT:                              None
       HeartBeat:                        Enable
```

```
HeartBeat Refresh Time:          15
Round-trip time:                 10000 msecs.
Maximum re-transmition time:     30 secs.
Network loss rate:               0 %
TEL1 Syntax Name:                aaln/0@[$IP]
TEL2 Syntax Name:                aaln/1@[$IP]
```

Example `-> voip mgcp protocol show tel1`

Gateway base protocol: MGCP end-point tel1

Operational state: Normal

Notified call-agent: None

Digit-map: (default) x.T

(current) x

See also `VOIP MGCP PROTOCOL ENABLE`

6.1.7.2.9 VOIP MGCP CALLAGENT CREATE

Syntax `OIP MGCP CALLAGENT CREATE <name> CONTACT <host>`

Description This command set the call agent address. More than one call agent can be defined to increase system robustness in case of server failure.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the call agent. The name must not be present already. The name can be a maximum of 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A
host	The hostname or IPv4 address of the call agent. Host can be a maximum of 256 chars long (when using hostname format).	N/A

Example `--> voip mgcp callagent create default contact 192.168.102.3`

See also `VOIP MGCP CALLAGENT LIST`
`VOIP MGCP CALLAGENT DELETE`

6.1.7.2.10 VOIP MGCP CALLAGENT SET MASTER

Syntax `VOIP MGCP CALLAGENT SET <name> MASTER`

Description This command set an existing call agent as Master. The Master call agent is the call agent that is attempted to be used firstly. In case of failure of the communication with it, the other call agent in the list will be used.

Example `--> voip mgcp callagent set default master`

See also `VOIP MGCP CALLAGENT LIST`
`VOIP MGCP CALLAGENT DELETE`

6.1.7.2.11 VOIP MGCP CALLAGENT DELETE

Syntax `VOIP MGCP CALLAGENT DELETE <name>`

Description This command deletes a previously defined call agent created using the VOIP MGCP CALLAGENT CREATE command.

To show the list of existing CALLAGENT entries, use the VOIP MGCP CALLAGENT LIST command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	A name (or the ID value) that identifies an existing call agent. To display the existing calla agent entries, use the VOIP MGCP CALLAGENT LIST command.	N/A

Example `--> voip mgcp callagent delete default`

See also `VOIP MGCP CALLAGENT CREATE`
`VOIP MGCP CALLAGENT LIST`

6.1.7.2.12 VOIP MGCP CALLAGENT LIST

Syntax `VOIP MGCP CALLAGENT LIST`

Description This command lists information about CALLAGENT entries added using the VOIP MGCP CALLAGENT CREATE command.

The following information is displayed:

Call agent ID numbers

Call agent names

Note: If a call agent name is longer than 32 chars, the name is shown in a short format (only the initial part of the name is displayed).

Example

```
--> voip sip fdb list

    Gateway call-agents:

 ID  |    Name    |  Master  |       Contact
-----|------------|----------|---------------------
   1 | default    | true  *  | 172.39.1.201
-------------------------------------------------
```

See also

```
VOIP MGCP CALLAGENT CREATE
VOIP MGCP CALLAGENT SHOW
```

6.2 VoIP SIP

This chapter describes how to configure the iMG for connection to a VoIP network using the SIP protocol.

6.2.1 iMG SIP Overview

6.2.1.1 iMG call processes

The iMG can communicate with the following devices:

- Another VoIP terminal on the IP network, such as another iMG.
- Any LAN SIP endpoint on the IP network, for instance:
- A Soft Phone
- An IP phone directly connected to the IP network

6.2.1.2 Calls involving another terminal

The following example shown in Figure 6-1 illustrates how to reach a phone or fax on another iMG terminal.

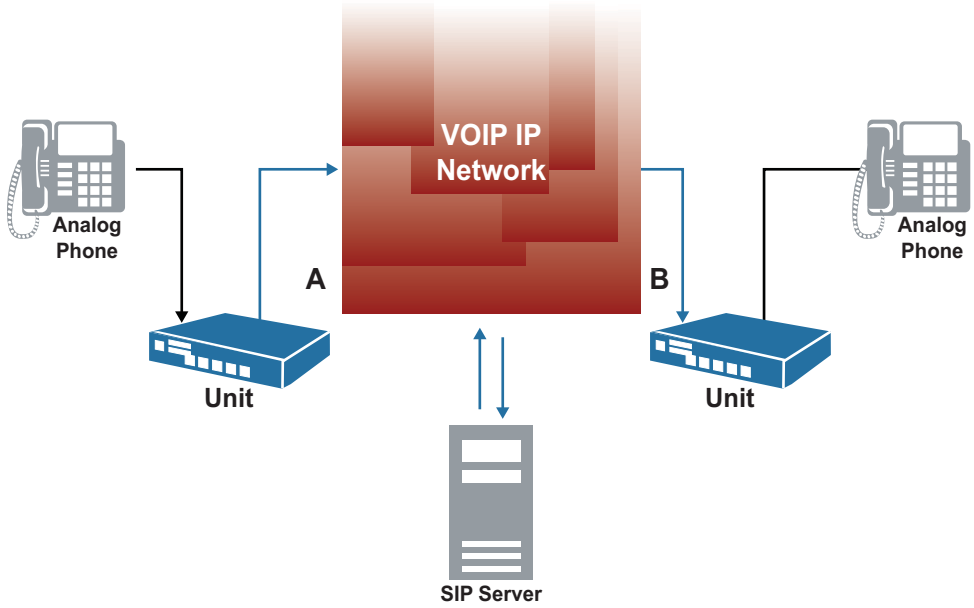


FIGURE 6-1 **Phone --> iMG(A) --> iMG(B) --> Phone**

A user makes a call with the phone connected to an iMG, which in turn contacts another iMG, which completes the connection to the phone that is attached to it.

6.2.1.3 Calls Involving a Terminal and a SIP Endpoint

The following examples illustrate how a phone connected to an iMG terminal can communicate with a LAN SIP endpoint on the IP network. Such endpoints could be:

- A Soft Phone
- An IP phone directly connected to the IP network

A user makes a call with the phone connected to an iMG, which reaches the corresponding LAN SIP endpoint on the IP network (Figure 6-2).

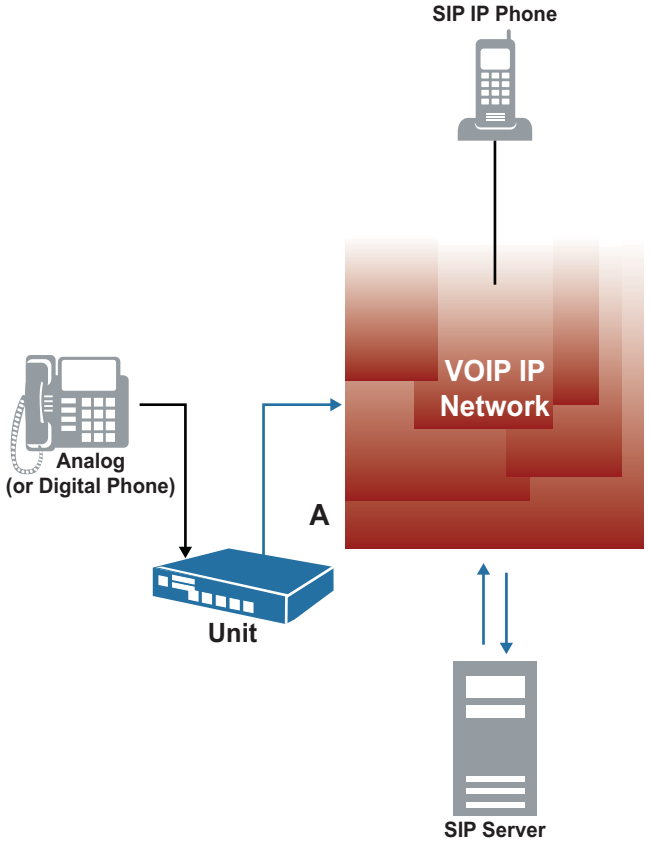


FIGURE 6-2 **Phone --> iMG(A) --> SIP IP Phone**

6.2.2 VoIP SIP Servers, Users & the Forwarding Database

The VoIP SIP subsystem on iMG residential gateways is based on the concept of SIP servers, local users, call forwarding rules and access ports.

The following section describes SIP servers, local users and forwarding database.

- SIP servers are servers where local users register themselves (Location Servers) and where calls are routed (Proxy Servers) when an outgoing call is going to be set up.
- Users are entities uniquely identified in the system by a name with an associated phone number. The User's phone number represents the user's address on the local system.
- Forwarding rules are local call routing rules used to forward an incoming call from a local user to a remote system or to a remote user. Forwarding rules are also used for locally originated calls when the called party

is not a local user and the call must be routed to a specific contact that typically is different from the proxy server.

Definition of SIP servers, users and optionally forwarding database rules, are three basic steps in correctly configuring the VoIP SIP subsystem (see Figure 8).

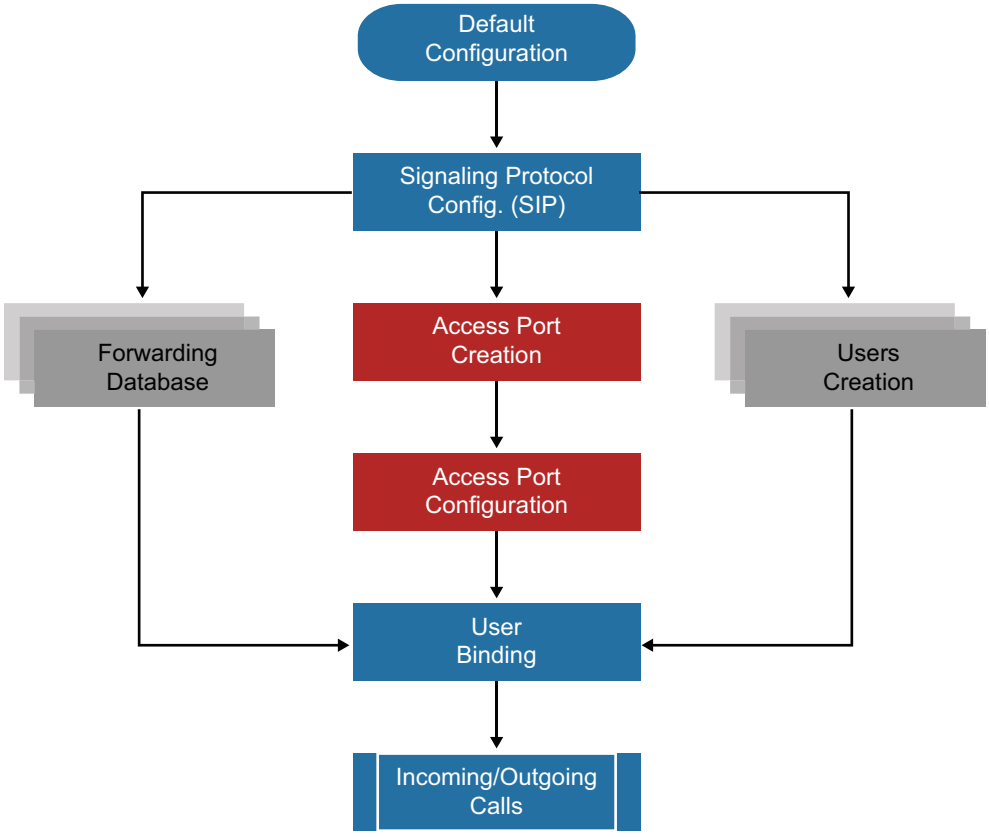


FIGURE 6-3 VoIP subsystem configuration - basic steps

6.2.2.1 SIP servers

6.2.2.1.1 Location servers

The SIP module needs to know where locally defined users attempt to register their contact in the network.

The VOIP SIP LOCATIONSERVER CREATE command is used to set the location servers used to register users.

It is possible to define more that one location server in order to increase system reliability in case the first location server cannot be reached.

The system will attempt to register the local users on all the location servers available in the location server list (see VOIP SIP LOCATIONSERVER LIST command) until the first registration phase achieves a positive result. Once a successful registration with a server has been achieved no further registration requests will be performed even if other location servers are defined.

In the case that more than one location server is defined in the system, it's possible to set a location server as Master: all registration requests will start with the master location server, independently of the position of that server in the location servers list. In the case where registration with the master location server fails, the Location Server list will be used examined to find alternative location server(s) to which registration requests will then be sent.

*Note: If no location servers are defined, the iMG uses the server addresses defined in the **Proxy Server list** instead.*

Note: If users are defined without specifying a user domain (see VOIP SIP USER CREATE command), the user domain will automatically be associated with the location server address where the user is registered.

6.2.2.1.2 Proxy servers

When an outgoing call cannot be handled by a local number or a well defined forwarding rule it must resolved by an external proxy server. In this case the SIP module needs to know which proxy server should be used.

The VOIP SIP PROXYSERVER CREATE command is used to inform the system of the proxy servers that can be contacted when an outgoing call is to be established.

Similarly to location servers, it is possible to define more that one proxy server in order to increase system reliability.

The system will attempt to contact all the proxy servers available in the proxy server list (see VOIP SIP PROXYSERVER LIST command) until the first server answers to the INVITE request. In that case no further INVITE requests are sent to the other proxy servers even if the called user cannot be reached.

In the case that more than one proxy server is defined in the system, it is possible to set a proxy server as Master. All INVITE requests will start with the master proxy server, independently of its position in the proxy servers list. In the situation where the Master proxy server cannot be reached, the Proxy Server list will be examined to find alternative proxy server(s) to which INVITE requests will be sent.

*Note: The **Proxy Server** is also used as registration server if no location servers are defined.*

*Note: If users are defined without specifying a user domain (see VOIP SIP USER CREATE command) and no **Location Servers** are defined, the user domain will automatically be associated with the proxy server upon which the user is registered.*

6.2.2.2 Users

The system is designed to support up to 100 entries, shared between users and forwarding rules.

Users are defined by the VOIP SIP USER CREATE command.

Each user must have an associated user number, composed of a address number and, optionally, an area code number if a complete E.164 number must be defined. Users may also have a pseudonym associated with their numeric address (see the VOIP SIP USER CREATE command).

Note: In any given system, there cannot be more than one user with the same area code and address. In other words: The combination of area code and address number uniquely identifies a user within a system.

Note: In any given system it is allowable to have two or more users with the same address but different area code or no area code at all.

Users may inform the VoIP network about the location (IP address) where they can be contacted by registering themselves on the location server defined in the VOIP SIP LOCATIONSERVER CREATE command. In this way other endpoints on the VoIP network can contact each user by simply using the user address.

The domain where users are members is the domain defined in the VOIP SIP USER CREATE command. If the DOMAIN is not defined, users will be implicitly associated with the address of the Location Server (or Proxy Server if no location servers are defined) where they are registered.

To establish a user's registration status use the VOIP SIP USER SHOW command.

The user number used in registration messages is the complete user number: area code + address number.

6.2.2.2.1 Users and access ports

A user needs to be 'attached' to at least one physical telephone port in order to receive or to make calls. To attach a user to a physical port use the VOIP SIP USER ADD command. When a user receives a call, only the access port(s) where the user is attached are engaged by the communication. The same user may be attached to more than one access port. In this case when a call is made to that user, all the ports to which the user is attached will be used to signal the incoming call.

To list all physical ports where a user is attached, use the VOIP SIP USER SHOW command

Note: Note that physical access ports don't have their own fixed phone number. They inherit the phone numbers from the user numbers of attached users.

More than one user may be attached to the same physical access port and therefore more than one phone number can be associated to the same physical access port.

If a user receives a call but the physical port where the user is attached is already involved in another communication (because it is used by another user), the call is rejected.

When an outgoing call is made to the VoIP network and more than one user is attached on the access port being used to make the call, the identity of calling user is deemed to be the first user defined in the list of users attached to that port.

To which which users are attached to a particular physical port, use the VOIP EP SHOW command.

When an access port is deleted from the system, all attached users are automatically detached from the port.

Detaching a user from a port by means of the VOIP SIP USER REMOVE command, or, by deletion of the port itself will result in a SIP de-registration transaction with the location server (assuming the user is registered with the location server).

6.2.2.3 Forwarding database (FDB)

The forwarding database is a component of the iMG that is used to redirect calls to a different destination address based on the called party number.

The signalling end-point layer uses the Forwarding DataBase every time the called end-point cannot be found among the local users. It is used both for incoming calls from the VoIP network or for outgoing calls generated locally and directed to a remote end-point.

The forwarding database may contain up to 100 entries (including users).

Forwarding entries are defined by the VOIP SIP FDB CREATE command.

Each FDB entry is uniquely identified by a name and defines the conditions that calls must satisfy in order to be routed to the end point specified by FDB entry parameters.

- When the signalling end-point layer receives a call it retrieves the called end-point address (called number).
  - Typically the called number is defined in the call signalling messages received from the network (in the SIP *To* header).
  - If the call is locally originated the called number address is equal the dialled number (unless the analogue/digital endpoint has the dialmask set to a value different from 0).
- The Called end-point address is searched for among the local user addresses to establish whether the called party is a user on the local system.
- If the called end-point matches the address of a local user, the access port(s) associated with the called user start ringing (if the port(s) are available).
- If the called number cannot be found among the local users, the forwarding database is scanned to look for entries matching the called number.

Note that the forwarding algorithm acts differently depending on whether the call is locally originated, or, is an incoming call:

6.2.2.3.1 Locally originated calls

If a match is found, the INVITE message is routed to the IP address defined in the CONTACT field of the matched FDB entry. The called user domain will be set to the DOMAIN value (optional) or to the CONTACT value (if no DOMAIN is specified) defined by the DOMAIN and CONTACT fields in the FDB entry respectively.
If the FDB entry has defined the FWADDRESS field, the called number is changed from the dialed number to the number defined in the FDB entry FWADDRESS field. In this way it's possible to dial short numbers that will be replaced by full-qualified numbers in outgoing calls.

If no match is found in the forwarding database, the INVITE message is routed to the first available proxy server (starting with the Master proxy server if defined) using the calling user domain as called endpoint domain.

6.2.2.3.2 Incoming calls

If a match is found, a MOVED TEMPORARY SIP message is sent back to the call originator reporting the contact address defined by the CONTACT field in the matched FDB entry.

If the FDB entry defines the FWADDRESS field, the called number is changed from the dialed number to the number defined in the FDB entry FWADDRESS field.

If no match is found in the forwarding database, the call is rejected.

6.2.2.3.3 Address and digit-map

The address field specified in FDB entries can be defined using digit map expressions.

Digit map expressions are used to increase system flexibility when defining forwarding rules that must mach multiple addresses (digit maps are used also in the VoIP access port module).

A digit map is defined either by a case insensitive 'string', or by a list of strings. Each string in the list is an alternative numbering scheme, specified either as a set of digits or as an expression to which the called address is compared by the *signalling* end-point layer to find the shortest possible match. The following constructs can be used in each digit map:

- ***Digit***
  A digit from '0' to '9'
- ***Wildcard***
  The symbol 'x' that matches any digit ('0' to '9').
- ***Range***
  One or more digit symbols enclosed between square brackets ('[' and ']').
- ***Subrange***
  Two digits separated by hyphen ('-') that matches any digit between and including the two. The subrange construct can only be used inside a range construct, i.e. between '[' and ']'.
- ***Position***
  A period ('.') that matches an arbitrary number, including zero, of occurrences of the preceding construct.

Digit map expressions are typically used when managing locally originated calls.

Using digit map expressions in this situation, it is possible to define a generic rule in such a way that all calls are routed to a specific contact (e.g. the proxy server) which will then perform call routing.

Digit map expressions are also useful for designing small networks without need to make use of any location servers, proxy servers or gatekeepers.

6.2.3 VoIP SIP Embedded Proxy Server

All gateway models with the exception of RG600E and RG6x6E variants include support for the embedded SIP proxy server. See table 1 (RG/iMG Models) for further details.

Refer to section 6.2.7 for the Embedded Proxy Server (EPS) CLI commands.

Also, note the following rules and guidelines for SIP:

- The maximum number of sip fdb users is 128, except for the iMG616E (64).
- The media port limit depends on the cpu type, and so the following number of ports are available:
  - iMG616E (Helium-210) - up to 48
  - iMG634A/B, iMG634WA/B, iBG910A/B (Argon-4x2) - up to 48
  - iBG915FX, iMG6x6MOD, iMG7x6MOD (Helium-520) - up to 128
  - iMG634A/B-R2, iMG634WA/B-R2, iMG616W (Solos) - up to 128

  The default value is always 32.

Note: Do not use the SECURITY ADD ALG command with the SIP option when configuring EPS, as this will cause issues with managing NAT sessions.

Note: When configuring EPS, note that EPS allows a maximum of three calls per line, although some IP-phones can support more than three.

6.2.4 VoIP SIP command reference

This section describes the commands available on the iMG to configure and manage the SIP protocol-signalling module.

6.2.4.1 VoIP SIP protocol CLI commands

The table below lists the VOIP SIP protocol commands provided by the CLI:

TABLE 6-4 VoIP SIP Protocol CLI Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SIP PROTOCOL DISABLE	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL ENABLE	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL RESTART	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET AUTHENTICATION	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET CONTACT-ON-1XX-RESPONSE	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET DEFAULTPORT	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET EXTENSION	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET INFO	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET INTERNAL-CALL-ROUTING	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET INVITETIMEOUT	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET KEEP-ALIVE	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET NAT	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET NETINTERFACE	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET PATH-HEADER	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET REGISTRATION-RETRY-TIME	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET REGISTRATION-RING-SPLASH	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET REMOTE-PARTY-ID-REPLACEMENT-ON-CFWD	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET ROUNDTRIPTIME	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET SERVER-REDUNDANCY	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET SERVER-SWITCHING	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET SESSIONEXPIRE	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET SUBSCRIBE-EVENT-MESSAGE-SUMMARY	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET UNRESERVED-CHAR-EXTENSION	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SET URIHOST	X	X	X	X	X	X	X	X	X
VOIP SIP PROTOCOL SHOW	X	X	X	X	X	X	X	X	X

6.2.4.1.1 VOIP SIP PROTOCOL DISABLE

Syntax `VOIP SIP PROTOCOL DISABLE`

Description This command stops the VoIP SIP signalling protocol and releases all the resources associated to it:

- Any analogue or digital port defined in the system is removed
- Any user defined in the system is deleted
- Any forwarding entry in the FDB is deleted
- Any sip server reference (location and proxy) is removed

To simply restart the SIP module, use the VOIP SIP PROTOCOL RESTART command. It doesn't remove any resources defined under the VoIP main module.

To enable the SIP module, use the VOIP SIP PROTOCOL ENABLE command.

Example --> voip sip protocol disable

See also `VOIP SIP PROTOCOL RESTART`
`VOIP SIP PROTOCOL ENABLE`

6.2.4.1.2 VOIP SIP PROTOCOL ENABLE

Syntax `VOIP SIP PROTOCOL ENABLE`

Description This command turns on the SIP *signalling* module.

To bind the SIP module to a specific IP interface use the VOIP SIP PROTOCOL SET INTERFACE command.

Note: Binding the SIP module to a specific IP interface defines the value of the source IP address for signalling and voice packets. SIP URLs with local reference offer the hostname and the IP address belonging the provisioned interface.

Note: The SIP module MUST be enabled in order to create/set analog/digital ports, users, call forwarding rules and SIP servers.

Example --> voip sip protocol enable

See also `VOIP SIP PROTOCOL SHOW`
`VOIP SIP PROTOCOL DISABLE`

6.2.4.1.3 VOIP SIP PROTOCOL RESTART

Syntax `VOIP SIP PROTOCOL RESTART`

Description This command restarts the VoIP SIP *signalling* protocol module.

Any pending and active calls are released.

Users previously registered to location servers start to unregister themselves and then re-register on the same location servers.

This command doesn't release any resources (users, physical ports and FDB entries) previously created during module configuration.

Example --> voip sip protocol restart

See also VOIP SIP PROTOCOL ENABLE

6.2.4.1.4 VOIP SIP PROTOCOL SET AUTHENTICATION

Syntax VOIP SIP PROTOCOL SET AUTHENTICATION {PROXY | PROXY,WWW | WWW}

Description This command sets the SIP dialog authentication method. By default, this is set to PROXY.

Example --> voip sip protocol set authentication proxy

See also VOIP SIP PROTOCOL SHOW
VOIP SIP PROTOCOL ENABLE

6.2.4.1.5 VOIP SIP PROTOCOL SET CONTACT-ON-1XX-RESPONSE

Syntax VOIP SIP PROTOCOL SET CONTACT-ON-1XX-RESPONSE {ENABLE | DISABLE}

Description This command sets enables and disables the inclusion of a Contact header in SIP 1xx responses. By default, this is set to disabled.

Example --> voip sip protocol set contact-on-1xx-response enable

See also VOIP SIP PROTOCOL SHOW

6.2.4.1.6 VOIP SIP PROTOCOL SET DEFAULTPORT

Syntax VOIP SIP PROTOCOL SET DEFAULTPORT <ipport>

Description This command sets the default listening/sending port used for SIP *signalling* messages.

By default, when the SIP module is attached to an IP interface using theVOIP SIP PROTOCOL SET NETINTERFACE command, the following default value is used:

- defaultport:5060

Note: Changing the signalling port causes the SIP module to restart.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Example --> voip sip protocol set defaultport 5060

Option	Description	Default Value
ipport	UDP/TCP port number used for signalling messages. Available values are in the range 1026 to 65534.Only even values can be accepted	5060

See also `VOIP SIP PROTOCOL ENABLE`

6.2.4.1.7 VOIP SIP PROTOCOL SET EXTENSION

Syntax `VOIP SIP PROTOCOL SET EXTENSION <extension>`

Description This command sets extended protocol features.

Note: 100rel and Session Timer are always supported when requested; setting "session-timer" the user agent explicitly requires this keep-alive mechanism. Info method overlaps the event transfer supported by RTP sessions.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
extension	Extension is comma separated list of values defining the protocol extension. Available values are: info session-timer keep-18x-session none	none

Example --> voip sip protocol set extension session-timer

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.8 VOIP SIP PROTOCOL SET INFO

Syntax `VOIP SIP PROTOCOL SET INFO {DTMF_0 | DTMF_1 | DTMF_2 | DTMF_3 | DTMF_4 | DTMF_5 | DTMF_6 | DTMF_7 | DTMF_8 | DTMF_9 | DTMF_Star | DTMF_Gate | DTMF_A | DTMF_B | DTMF_C | DTMF_D | Flash} <token>`

Description This command sets mappings for out of band DTMF digits and flash-hook signals within SIP INFO methods using the application/dtmf-relay content type.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
token	Signal element to be used for the DTMF digit of flash-hook event. These should take the form 'Signal=*x*', where *x* is one of the digits 0-9, *, #, A, B, C, or D.	N/A

Example --> voip sip protocol set info DTMF_0 Signal=0

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.9 VOIP SIP PROTOCOL SET INTERNAL-CALL-ROUTING

Syntax `VOIP SIP PROTOCOL SET INTERNAL-CALL-ROUTING {ENABLE | DISABLE}`

Description This command enables/disables the internal-call-routing feature. By default, if more than one SIP user has been created on the iMG device, a call between two of them does not contact the configured SIP proxy server. By setting internal-call-routing to disable, the device always contacts the SIP proxy server.

Example --> voip sip protocol set internal-call-routing disable

See also `VOIP SIP PROTOCOL ENABLE`

6.2.4.1.10 VOIP SIP PROTOCOL SET INVITETIMEOUT

Syntax `VOIP SIP PROTOCOL SET INVITETIMEOUT <sec>`

Description This command sets the number of seconds an INVITE that does not receive any answer must be sent. During an outgoing call, the INVITE sent by iMG must be received an answer within ROUNDTRIPTIME msec. If the answer is not received, the same INVITE is re-transmitted and the ROUNDTRIPTIME's value is doubled. This process ends INVITE-TIMEOUT seconds after the first INVITE.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
sec	Number of seconds that an INVITE with no answer must be sent.	32

Example --> voip sip protocol set invitetimeout 10

See also VOIP SIP PROTOCOL SET ROUNDTRIPTIME

6.2.4.1.11 VOIP SIP PROTOCOL SET KEEP-ALIVE

Syntax

```
VOIP SIP PROTOCOL SET KEEP-ALIVE {ENABLE|DISABLE}
VOIP SIP PROTOCOL SET KEEP-ALIVE TIME <sec>
```

Description This command sets a keep-alive mechanism based on the REGISTER message. When the feature is enabled, iMG sends a REGISTER message every KEEP-ALIVE TIME seconds.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
sec	Interval between two REGISTER messages.	300

Example -> voip sip protocol set keep-alive 150

See also VOIP SIP PROTOCOL SET ENABLE

6.2.4.1.12 VOIP SIP PROTOCOL SET NAT

Syntax

```
VOIP SIP PROTOCOL SET NAT ADDRESS {<host> | NONE}
VOIP SIP PROTOCOL SET NAT INTERFACE <interface>
```

Description This command sets the NAT host reference. Any SIP URLs with local references are hidden by the NAT address value. It also specifies the external interface for NAT to use.

Note: Changing the NAT reference causes the SIP module to restart.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
host	The address that will be displayed in the local SIP URL references. It can be expressed in hostname format or IPv4 format. A Hostname can be at most 255 characters long.	None
interface	The iMG interface that NAT is to use as the external interface.	None

Example --> voip sip protocol set nat address iMG.voip.atkk.com
--> voip sip protocol set nat interface ip0

See also `IP LIST INTERFACES`
`VOIP SIP PROTOCOL ENABLE`
`VOIP SIP PROTOCOL SHOW`

6.2.4.1.13 VOIP SIP PROTOCOL SET NETINTERFACE

Syntax `VOIP SIP PROTOCOL SET NETINTERFACE <interface_name>`

Description This command sets the IP interface used to access the VoIP network.

Signalling and voice packets will use the Source IP address defined for the selected interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
interface_name	An existing IP interface. To display interface names, use the IP LIST INTERFACES command.	N/A

Example --> voip sip protocol set netinterface ip0

See also `VOIP SIP PROTOCOL ENABLE`

6.2.4.1.14 VOIP SIP PROTOCOL SET PATH-HEADER

Syntax `VOIP SIP PROTOCOL SET PATH-HEADER {ENABLE|DISABLE|PROFILE}`

Description This command includes the PATH-HEADER support on REGISTER messages as detailed by RFC 3327 to discovering intermediate proxies during SIP registration.

By default the path-header support is tied to the SIP profile defined at admin level. If the SIP profile requests the path-header support, then the support is automatically turned on, otherwise it is left off.

It's also possible to force the path-header to be always turned off or on independently from the profile selected.

When path-header support is enabled and the iMG receives a valid path-header value a response to the REGISTER request, all the subsequent outgoing calls will use the address specified by the path-header value as outgoing proxy.

When registration timer expires, the iMG will reattempt a registration to the default (configured) location server. If the the iMG receives a valid path-header value in the response, it will use it for all the subsequent calls untli the registration phase restarts again. Otherwise the iMG will use the default outgoing proxy as configured in the proxy servers list.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description
ENABLE	Add always the path-header support on REGISTRATION requests.
DISABLE	Never add the path-header support on REGISTRATION requests.
PROFILE	Includes the path-header support on REGISTRATION requests depending on the selected SIP profile.

Example -> voip sip protocol set path-header enable

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.15 VOIP SIP PROTOCOL SET REGISTRATION-RETRY-TIME

Syntax `VOIP SIP PROTOCOL SET REGISTRATION-RETRY-TIME <secs>`

Description This command sets the interval between two failed registrations. If a REGISTER sent by iMG fails, the next attempt will be executed after REGISTRATION-RETRY-TIME seconds.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
secs	Seconds must elapse after a failed registration before exec another attempt. Available values are in the range 10 to 3600 sec (24 hours).	20

Example --> voip sip protocol set registration-retry-time 30

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.16 VOIP SIP PROTOCOL SET REGISTRATION-RING-SPLASH

Syntax `VOIP SIP PROTOCOL SET REGISTRATION-RING-SPLASH {ENABLED|DISABLED}`

Description This command enables/disables the ring-splash after the user has been registered. If the feature is enabled, as soon as the user is registered the phone connected to the relevant phone port plays a ring-splash. The default value is disabled.

Example --> voip sip protocol set registration-ring-splash enable

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.17 VOIP SIP PROTOCOL SET REMOTE-PARTY-ID-REPLACEMENT-ON-CFWD

Syntax `VOIP SIP PROTOCOL SET REMOTE-PARTY-ID-REPLACEMENT-ON-CFWD {ENABLE|DISABLE}`

Description This command enables/disables substitution of the remote party identity on call forwarding. The default value is disabled.

Example --> voip sip protocol set remote-party-id-replacement-on-cfwd enable

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.18 VOIP SIP PROTOCOL SET ROUNDTRIPTIME

Syntax `VOIP SIP PROTOCOL SET ROUNDTRIPTIME <msecs>`

Description This command sets the maximum time between the transmission of a packet and the reception of the response. If the time expires, protocol primitives are retransmitted.

Retransmission of protocol primitives is useful in case of unreliable transports like UDP to recover errors in transactions.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
msecs	The round trip time in milliseconds. Acceptable values are from 500 to 4000 msecs.	500

Example --> voip sip protocol set roundtriptime 1000

See also `VOIP SIP PROTOCOL ENABLE`

6.2.4.1.19 VOIP SIP PROTOCOL SET SERVER-REDUNDANCY

Syntax `VOIP SIP PROTOCOL SET SERVER-REDUNDANCY {DNS-BASED|PERMANENT}`

Description This command sets how switching between primary & secondary SIP servers is managed by the gateway.

- If PERMANENT is set, then once the current server is noted as failed, all subsequent server requests will be routed to the alternate server. The alternate server will continue to be used until such time as it fails, at which point all subsequent server requests will be routed to the original server.
- If DNS-BASED is set, then upon primary server failure all future server requests for this particular dialog will be routed to the secondary server. Any subsequent new dialogs created on the gateway will always try to contact the primary server first.

The default value is permanent.

Example --> voip sip protocol set server-redundancy dns-based

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.20 VOIP SIP PROTOCOL SET SERVER-SWITCHING

Syntax `VOIP SIP PROTOCOL SET SERVER-SWITCHING {AUTHENTICATION-FAILURE | LINK-FAILURE-ONLY}`

Description This command sets the switching mode between two or more location or proxy servers. When more than one location-server or proxy-server are configured, iMG can switch between them if the communication fails. The following table lists the two available switching modes.

Option	Description
AUTHENTICATION-FAILURE	Switching between the provisioned servers happens when authentication fails, or when no responses are received from the server (link fails).
LINK-FAILURE-ONLY	Switching between the provisioned servers happens only when no responses are received from the current server (link fails). A failed authentication does not cause a server switch.

Example --> voip sip protocol set server-switching authentication-failure

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.21 VOIP SIP PROTOCOL SET SESSIONEXPIRE

Syntax `VOIP SIP PROTOCOL SET SESSIONEXPIRE <secs>`

Description This command sets the largest amount of time that can occur between session refresh in dialog before the session will be considered timed out.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
secs	The session expire time in seconds. Available values are in the range 30 to 86400 sec (24 hours).	1800

Example --> voip sip protocol set sessionexpire 180

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.22 VOIP SIP PROTOCOL SET SUBSCRIBE-EVENT-MESSAGE-SUMMARY

Syntax `VOIP SIP PROTOCOL SET SUBSCRIBE-EVENT-MESSAGE-SUMMARY {ENABLED | DISABLED}`

Description This command enables and disables subscription to SIP message summary events.

Note: This command can only be used prior to creating any SIP users on the gateway.

The default value is disabled.

Example --> voip sip protocol set subscribe-event-message-summary enabled

See also `VOIP SIP PROTOCOL SHOW`
`VOIP SIP USER CREATE`

6.2.4.1.23 VOIP SIP PROTOCOL SET UNRESERVED-CHAR-EXTENSION

Syntax `VOIP SIP PROTOCOL SET UNRESERVED-CHAR-EXTENTION {NONE | #}`

Description SIP protocol states the char "#" must not be present in SIP messages and it must be replaced with "%23" (23 is the ASCII value for "#"). This command allows leaving the char # in the SIP message to accommodate some SIP implementation and easy fix possible interoperability issues.

Example --> voip sip protocol set unreserved-char-extension #

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.24 VOIP SIP PROTOCOL SET URIHOST

Syntax `VOIP SIP PROTOCOL SET URIHOST {DNS-HOSTNAME | LOCAL-IP | SYSTEM-NAME}`

Description By default iMG use his IP address Uri host part of the sent SIP messages. This command allows to configure the URI host part. The possible choices are listed in the following table.

Option	Description
LOCAL-IP	The URI host is the IP address of the IP interface where the SIP is attached.
DNS-HOSTNAME	iMG resolves its DNS-HOSTNAME and uses it as URI host. If the address resolution fails, the LOCAL-IP is used.
SYSTEM-NAME	iMG uses the SYSTEM-NAME configured on the device via CLI command SYSTEM NAME as URI host. If the SYSTEM NAME is not configured, the LOCAL-IP is used as URI host.

Example --> voip sip protocol set URIhost system-name

See also `VOIP SIP PROTOCOL SHOW`

6.2.4.1.25 VOIP SIP PROTOCOL SHOW

Syntax `VOIP SIP PROTOCOL SHOW`

Description This command displays basic SIP module configuration parameters set by the VOIP SIP PROTOCOL SET commands.

Example --> voip sip protocol show

```
--> voip sip protocol show
Gateway base protocol: SIP
------------------------------------------------------------------------
   Network interface:                    ip0
   Default port:                         5060
   NAT:
   Extension features:                   none
   Unreserved chars:                     none
   Dialog authentication method:         proxy
   SIP URI host scheme:                  local-ip
   Keep alive                            disabled (300 secs.)
   Round-trip time:                      500 msecs.
   Registration/Subscription retry time:  20 secs.
   Registration ring splash:             disabled
   Invite transaction timeout:           32 secs. (6 retransmition
times)
   Session expire time:                  1800 secs.
   Internal call routing:                enabled
```

```
        Server redundancy:                      permanent
        Server switching:                       on link failure only
        Remote Party ID replacement
           on call-forwarding:                  disabled
        Contact header on 1xx response:         disabled
        Event Subscription message-summary:     disabled

        INFO signal mapping:
           DTMF_0                               Signal=0
           DTMF_1                               Signal=1
           DTMF_2                               Signal=2
           DTMF_3                               Signal=3
           DTMF_4                               Signal=4
           DTMF_5                               Signal=5
           DTMF_6                               Signal=6
           DTMF_7                               Signal=7
           DTMF_8                               Signal=8
           DTMF_9                               Signal=9
           DTMF_Star                            Signal=*
           DTMF_Gate                            Signal=#
           DTMF_A                               Signal=A
           DTMF_B                               Signal=B
           DTMF_C                               Signal=C
           DTMF_D                               Signal=D
           Flash
    -->
```

See also VOIP SIP PROTOCOL ENABLE
VOIP SIP PROTOCOL SET MEDIAPORT
VOIP SIP PROTOCOL SET EXTENSION

6.2.5 VoIP SIP Locationserver command reference

This section describes the commands available on the iMG intelligent Multiservice Gateway to enable, configure and manage the ***VoIP SIP Locationserver*** module.

6.2.5.1 VoIP SIP Locationserver CLI commands

The table below lists the ***VOIP SIP Locationserver*** commands provided by the CLI:

TABLE 6-5 VoIP SIP Location Server CLI Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SIP LOCATIONSERVER CREATE	X	X	X	X	X	X	X	X	X
VOIP SIP LOCATIONSERVER DELETE	X	X	X	X	X	X	X	X	X
VOIP SIP LOCATIONSERVER LIST	X	X	X	X	X	X	X	X	X
VOIP SIP LOCATIONSERVER SET MASTER	X	X	X	X	X	X	X	X	X

6.2.5.1.1 VOIP SIP LOCATIONSERVER CREATE

Syntax `VOIP SIP LOCATIONSERVER CREATE <name> CONTACT <host:port/transport>`

Description This command creates a new entry in the ***location server*** list. Each ***location server*** must have a different <name>. If the ***location server*** already exists, an error message is raised.

This command is accepted only if the SIP module is already running. See the VOIP SIP PROTOCOL ENABLE command to turn on the SIP module.

This command doesn't set the master location server. To define a location server as master use the VOIP SIP LOCATIONSERVER SET MASTER command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the location server. The name must not be present already. The name can be at most 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A
host	The hostname or IPv4 address of the location server where registrations are sent. ***host*** can be at most 256 chars long (when using hostname format).	N/A
port	The UDP/TCP port on the location server to which signalling messages are sent.	5060

transport	The protocol used to transport the signalling messages to the location server. Possible values are: • udp • tcp	udp

Example --> voip sip locationserver create default contact 192.168.102.3

See also `VOIP SIP LOCATIONSERVER LIST`
`VOIP SIP LOCATIONSERVER SHOW`

6.2.5.1.2 VOIP SIP LOCATIONSERVER DELETE

Syntax `VOIP SIP LOCATIONSERVER DELETE <name>`

Description This command deletes a single location server created using the VOIP SIP LOCATIONSERVER CREATE command.

To show the list of existing location servers, use the VOIP SIP LOCATIONSERVER LIST command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing location server (it can also be the ID value associated with the location server). To display the existing location servers, use the VOIP SIP LOCATIONSERVER LIST command.	N/A

Example --> voip sip locationserver delete backuplocserv

See also `VOIP SIP LOCATIONSERVER CREATE`
`VOIP SIP LOCATIONSERVER LIST`
`VOIP SIP LOCATIONSERVER SHOW`

6.2.5.1.3 VOIP SIP LOCATIONSERVER LIST

Syntax `VOIP SIP LOCATIONSERVER LIST`

Description This command lists information about location servers that were added using the VOIP SIP LOCATIONSERVERS CREATE command. The following information is displayed:

- *Server ID numbers*
- *Server names*

- ***Master***
  whether the server has been set as Master or not. A star symbol in the field identifies the server as the current location server where local users are registered.
- ***Contact***
  the IP address (IPv4 or hostname format) of the location server

Note: If a name is longer than 32 chars, the name is shown in a short format (only the initial part of the name is displayed). To show the full name use the VOIP SIP LOCATIONSERVER SHOW command, specifying the server ID instead of server name.

Example --> voip sip location list

```
 ID  |    Name    |  Master  |              Contact
-----|------------|----------|-------------------------------------
   1 | default    | false *  | 192.168.1.2
-------------------------------------------------------------------
```

See also VOIP SIP LOCATIONSERVER CREATE
VOIP SIP LOCATIONSERVER SHOW

6.2.5.1.4 VOIP SIP LOCATIONSERVER SET MASTER

Syntax VOIP SIP LOCATIONSERVER SET <name> MASTER

Description This command sets a location server as Master. If another location server was set Master previously, the flag Master is removed from the old one.

To show the list of existing location servers, use the VOIP SIP LOCATIONSERVER LIST command.

Option	Description	Default Value
name	An arbitrary name that identifies the proxy server. The name must not be present already.The name can be at most 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A

Example --> voip sip locationserver set backuplocserv master

See also VOIP SIP LOCATIONSERVER CREATE
VOIP SIP LOCATIONSERVER LIST
VOIP SIP LOCATIONSERVER SHOW

6.2.6 VoIP SIP Proxyserver command reference

This section describes the commands available on the iMG intelligent Multiservice Gateway to enable, configure and manage the ***VoIP SIP Proxyserver*** module.

6.2.6.1 VoIP SIP Proxyserver CLI commands

The table below lists the ***VOIP SIP Proxyserver*** commands provided by the CLI:

TABLE 6-6 Commands for VoIP Proxy Server

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SIP PROXYSERVER CREATE	X	X	X	X	X	X	X	X	X
VOIP SIP PROXYSERVER DELETE	X	X	X	X	X	X	X	X	X
VOIP SIP PROXYSERVER LIST	X	X	X	X	X	X	X	X	X
VOIP SIP PROXYSERVER SET MASTER	X	X	X	X	X	X	X	X	X

6.2.6.1.1 VOIP SIP PROXYSERVER CREATE

Syntax `VOIP SIP PROXYSERVER CREATE <name> CONTACT <host:port/transport >`

Description This command creates a new entry in the proxy servers' list. Each proxy server must have a different <name>. If the proxy server already exists, an error message is raised.

This command is accepted only if the SIP module is already running. See the VOIP SIP PROTOCOL ENABLE command to turn on the SIP module.

This command doesn't set the master proxy server. To define a proxy server as master use the VOIP SIP PROXYSERVER SET MASTER command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the proxy server. The name must not be present already.The name can be at most 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A
host	The hostname or IPv4 address of the proxy server where *signalling* messages are senthost can be at most 256 chars long (when using hostname format).	N/A

port	The UDP/TCP port on the proxy server to which signalling messages are sent.	5060
transport	The protocol used to transport the signalling messages to the proxy server. Possible values are:udptcp	udp

Example --> voip sip proxy create default contact 192.168.102.3

See also `VOIP SIP PROXYSERVER LIST`
`VOIP SIP PROXYSERVER SHOW`

6.2.6.1.2 VOIP SIP PROXYSERVER DELETE

Syntax `VOIP SIP PROXYSERVER DELETE <name>`

Description This command deletes a single proxy server created using the VOIP SIP PROXYSERVER CREATE command.

To show the list of existing proxy servers, use the VOIP SIP PROXYSERVER LIST command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing proxy server (it can also be the ID value associated with the proxy server). To display the existing proxy servers, use the VOIP SIP PROXYSERVER LIST command.	N/A

Example --> voip sip proxyserver delete backuplocserv

See also `VOIP SIP PROXYSERVER CREATE`
`VOIP SIP PROXYSERVER LIST`
`VOIP SIP PROXYSERVER SHOW`

6.2.6.1.3 VOIP SIP PROXYSERVER LIST

Syntax `VOIP SIP PROXY LIST`

Description This command lists information about proxy servers that were added using the VOIP SIP PROXYSERVER CREATE command. The following information is displayed:

- server ID numbers
- server names

- ***Master***
  whether the server has been set as Master or not. A star symbol in the field identifies the server as the current proxy server used by outgoing calls.
- ***Contact***
  the IP address (IPv4 or hostname format) of the proxy server

Note: If a name is longer than 32 chars, the name is shown in a short format (only the initial part of the name is displayed). To show the full name use the VOIP SIP PROXYSERVER SHOW command, specifying the server ID instead of server name.

Example--> voip sip proxyserver list

```
 ID  |    Name    |  Master  |              Contact
-----|------------|----------|-------------------------------------
   1 | default    | false *  | 192.168.1.2
-------------------------------------------------------------------
```

See also VOIP SIP PROXYSERVER CREATE
VOIP SIP PROXYSERVER SHOW

6.2.6.1.4 VOIP SIP PROXYSERVER SET MASTER

Syntax VOIP SIP PROXYSERVER SET <name> MASTER

Description This command sets a proxy server as Master. If another proxy server was set Master previously, the flag Master is removed from the old one.

To show the list of existing proxy servers, use the VOIP SIP PROXYSERVER LIST command.

Option	Description	Default Value
name	An arbitrary name that identifies the proxy server. The name must not be present already.The name can be at most 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A

Example --> voip sip proxyserver set backuplocserv master

See also VOIP SIP PROXYSERVER CREATE
VOIP SIP PROXYSERVER LIST
VOIP SIP PROXYSERVER SHOW

6.2.7 VoIP SIP Embeddedserver command reference

This section describes the commands available on the AT-iBG900 intelligent Multiservice Gateway to enable, configure and manage the ***VoIP SIP Embeddedserver*** module.

6.2.7.1 VoIP SIP Embeddedserver CLI commands

The table below lists the ***VOIP SIP Embeddedserver*** commands provided by the CLI:

TABLE 6-7 Commands for VoIP Embeddedserver

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SIP EMBEDDEDSERVER CREATE			X	X	X	X	X	X	X
VOIP SIP EMBEDDEDSERVER DELETE			X	X	X	X	X	X	X
VOIP SIP EMBEDDEDSERVER LIST			X	X	X	X	X	X	X
VOIP SIP EMBEDDEDSERVER SET EMERGENCY-SERVICE			X	X	X	X	X	X	X
VOIP SIP EMBEDDEDSERVER SET PERMANENT-STORAGE			X	X	X	X	X	X	X
VOIP SIP EMBEDDEDSERVER SHOW			X	X	X	X	X	X	X

6.2.7.1.1 VOIP SIP EMBEDDEDSERVER CREATE

Syntax `VOIP SIP EMBEDDEDSERVER CREATE <name> [DOMAIN <domain>] CONTACT <host:port/transport >`

Description This command creates a new entry in the embedded servers' list. If the embedded server already exists, an error message is raised. Currently only one embedded server can be configured

This command is accepted only if the SIP module is already running. See the VOIP SIP PROTOCOL ENABLE command to turn on the SIP module.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the embedded server. The name must not be present already. The name can be at most 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A

domain	The domain name or IPv4 address of the embedded server where *signalling* messages are sent.	N/A
host	The hostname or IPv4 address of the embedded server where *signalling* messages are sent. Host can be at most 256 chars long (when using hostname format).	N/A
port	The UDP/TCP port on the embedded server to which signalling messages are sent.	5060
transport	The protocol used to transport the signalling messages to the embedded server. Possible values are: udp or tcp	udp

Example --> voip sip embedded create default contact 192.168.102.3

See also `VOIP SIP EMBEDDEDSERVER LIST`
`VOIP SIP EMBEDDEDSERVER SHOW`

6.2.7.1.2 VOIP SIP EMBEDDEDSERVER DELETE

Syntax `VOIP SIP PROXYSERVER DELETE <name>`

Description This command deletes a single embedded server created using the VOIP SIP EMBEDDEDSERVER CREATE command.

To show the list of existing embedded servers, use the VOIP SIP EMBEDDED LIST command. Currently only one embedded server can be configured.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing embedded server (it can also be the ID value associated with the embedded server).	N/A

Example --> voip sip embeddedserver delete backuplocserv

See also `VOIP SIP EMBEDDEDSERVER CREATE`
`VOIP SIP EMBEDDEDSERVER LIST`
`VOIP SIP EMBEDDEDSERVER SHOW`

6.2.7.1.3 VOIP SIP EMBEDDEDSERVER LIST

Syntax `VOIP SIP EMBEDDEDSERVER LIST`

Description This command lists information about embedded servers that were added using the VOIP SIP EMBEDDEDSERVER CREATE command. The following information is displayed:

- server ID numbers
- server names
- *NVS (not used)*
- *Contact*
  the IP address (IPv4 or hostname format) of the proxy server

Note: If a name is longer than 32 chars, the name is shown in a short format (only the initial part of the name is displayed). To show the full name use the VOIP SIP EMBEDDEDSERVER SHOW command, specifying the server ID instead of server name.

Example --> voip sip embeddedserver list

```
Gateway - Embedded Proxy Servers:
 ID  |    Name    |  NVS   |              Contact
-----|------------|--------|--------------------------------------
   1 | def-server | false  | 192.168.1.2
-------------------------------------------------------------------
```

See also VOIP SIP EMBEDDEDSERVER CREATE
VOIP SIP EMBEDDEDSERVER SHOW

6.2.7.1.4 VOIP SIP EMBEDDEDSERVER SET EMERGENCY-SERVICE

Syntax `VOIP SIP EMBEDDEDSERVER SET <name> EMERGENCY-SERVICE <service>`

Description This command sets the way the embedded server works when the external server is unreachable.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing embedded server (it can also be the ID value associated with the embedded server).	N/A
service	Service provided by the embedded server when the public sip proxy is unreachable. Possible values are: redirect-server or stateless-proxy	redirect-server

Example --> voip sip embedded set def-server emergency-service redirect-server

See also VOIP SIP EMBEDDEDSERVER CREATE
VOIP SIP EMBEDDEDSERVER LIST
VOIP SIP EMBEDDEDSERVER SHOW

6.2.7.1.5 VOIP SIP EMBEDDEDSERVER SET PERMANENT-STORAGE

Syntax VOIP SIP EMBEDDEDSERVER SET <name> PERMANENT-STORAGE <ENABLED|DISABLED>

Description This command enables or disables the permanent storage feature in the embedded-server module.

Option	Description	Default Value
name	An arbitrary name that identifies the proxy server. The name must not be present already.The name can be at most 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A

Example --> voip sip embedded set def-server permanent-storage enabled

See also VOIP SIP EMBEDDEDSERVER CREATE
VOIP SIP EMBEDDEDSERVER LIST
VOIP SIP EMBEDDEDSERVER SHOW

6.2.7.1.6 VOIP SIP EMBEDDEDSERVER SHOW

Syntax VOIP SIP EMBEDDEDSERVER SHOW

Description This command shows the setting of the embedded-server module.

Example --> voip sip embeddedserver show def-server

```
Gateway - Embedded Proxy Servers:
------------------------------------------------------------------
   Operational Status:       in service
   Emergency proxy mode:     redirect server
   Domain:
```

See also VOIP SIP EMBEDDEDSERVER CREATE
VOIP SIP EMBEDDEDSERVER LIST
VOIP SIP EMBEDDEDSERVER SET

6.2.8 VoIP SIP User command reference

This section describes the commands available on the iMG intelligent Multiservice Gateway to enable, configure and manage the ***VoIP SIP User*** module.

6.2.8.1 VoIP SIP User CLI commands

The table below lists the ***VoIP SIP User*** commands provided by the CLI:

TABLE 6-8 Commands for VoIP SIP User

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SIP USER ADD	X	X	X	X	X	X	X	X	X
VOIP SIP USER CREATE	X	X	X	X	X	X	X	X	X
VOIP SIP USER DELETE	X	X	X	X	X	X	X	X	X
VOIP SIP USER LIST	X	X	X	X	X	X	X	X	X
VOIP SIP USER REMOVE	X	X	X	X	X	X	X	X	X
VOIP SIP USER SHOW	X	X	X	X	X	X	X	X	X

6.2.8.1.1 VOIP SIP USER ADD

Syntax `VOIP SIP USER ADD <username> PORT <portname> [MASTER]`

Description This command attaches a user created with the command VOIP SIP USER CREATE to a named port created with the command VOIP EP ANALOGUE CREATE.

As soon as this command is entered, the registration phase starts.

Note: The system tries to register the user with the location server specified by the VOIP SIP LOCATIONSERVER CREATE command. If no location servers are defined, the system tries to register the user with the proxy server specified by the VOIP SIP PROXYSERVER CREATE command. If no proxy servers are defined, registration phase is not performed until a location server or proxy server is added to the SIP module.

To display the user's registration status and port association use the VOIP SIP USER SHOW command.

The optional ‘master’ token may be used when multiple users are added to a single port. Marking a user as ‘master’ indicates that this user should be specified in the From header of outgoing SIP INVITE requests. Note that is no user is marked as ‘master’, then the address of last user added to the port will be used in the From header of outgoing SIP INVITE requests.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
username	An existing user (it can be also the ID value associated with the user name). To display the existing users, use the VOIP SIP USER LIST command.	N/A
portname	An existing port. To display the existing ports, use the VOIP EP LIST command.	N/A

Example --> voip sip user add MrBrown port fxs0

See also
```
VOIP SIP USER ADD
VOIP SIP USER CREATE
VOIP SIP USER DELETE
VOIP SIP USER LIST
VOIP SIP USER REMOVE
VOIP SIP USER SHOW
VOIP EP LIST
```

6.2.8.1.2 VOIP SIP USER CREATE

Syntax
```
VOIP SIP USER CREATE <username> ADDRESS <digit-map> [AREA-
CODE <area-number>] [AUTHENTICATION <login:password>]
[DOMAIN <host >] [TRANSPORT <transport>] [PSEUDONYM <pseud-
onym>]
```

Description This command creates a new entry in the users list. Each user must have a different <username>. If the user already exists, an error message is raised.

This command is accepted only if the SIP module is already running. See the VOIP SIP PROTOCOL ENABLE command to turn on the SIP module.

This command doesn't bind the user to a physical access port. In order to inform the system that the user is attached to a specific physical port, the VOIP SIP USER ADD command must be used.

Note: If the DOMAIN parameter is not specified, the user domain is set equal to the location server address (if defined) or proxy server address (if location server is not defined).

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
username	An arbitrary name that identifies the user. The name must not be present already. The username can be at most 16 characters long; cannot start with a digit and cannot contain dots '.' or slash symbols '/'.	N/A
digit-map	The phone number (E.164) used to reach the user. The address can be 32 characters long.	N/A
area-number	The prefix number to be dialed before the destination number. Valid characters are only numerical characters. The area number can be at most 10 digits long.	empty
login	The user name used during the authentication phase. The login can be at most 32 characters long. The same rules defined for the username field also apply here, except the login can start with a digit.	empty
password	The password used during the authentication phase. The password can be at most 16 characters long. The same rules defined for the username field also apply here, except the password can start with a digit.	empty
host	The domain address in hostname format or IPv4 format. The domain can be at most 255 characters long.	empty
transport	The transport protocol used to contact the user. Possible values are: • udp • tcp	udp
pseudonym	The pseudonym allows iMG SIP users to register with a pseudonym (instead of their numeric address). A user registered by pseudonym can then be addressed either by pseudonym or numeric address.	empty

Example --> voip sip user create MrBrown address 12345 domain 192.168.102.3 pseudonym Charlie

See also
```
VOIP SIP USER ADD
VOIP SIP USER CREATE
VOIP SIP USER DELETE
VOIP SIP USER LIST
```

```
VOIP SIP USER REMOVE
VOIP SIP USER SHOW
```

6.2.8.1.3 VOIP SIP USER DELETE

Syntax `VOIP SIP USER DELETE <username>`

Description This command deletes a single user created using the VOIP SIP USER CREATE command.

To show the list of existing users, use the VOIP SIP USER LIST command.

As soon this command is entered, the de-registration phase starts (REGISTER request) to the location server (registrar) removing the user from the user list on the server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
username	An existing user (it can also be the ID value associated with the user name). To display the existing users, use the VOIP SIP USER LIST command.	N/A

Example --> voip sip user delete MrBrown

See also

```
VOIP SIP USER ADD
VOIP SIP USER CREATE
VOIP SIP USER DELETE
VOIP SIP USER LIST
VOIP SIP USER REMOVE
VOIP SIP USER SHOW
```

6.2.8.1.4 VOIP SIP USER LIST

Syntax `VOIP SIP USER LIST`

Description This command lists information about users that were added using the VOIP SIP USER CREATE command. The following information is displayed:

- user ID numbers
- user names
- Area Codes
- Addresses

Note: If a user name is longer than 32 chars, the name is shown in a short format (only the initial part of the name is displayed). To show the full name use the VOIP SIP USER SHOW command, specifying the user ID instead of user name.

Example --> voip sip user list

```
ID   | Name       | Global Address                | Pseudonym
-----|------------|-------------------------------|------------------
   1 | MrBrown    | 12345                         | Charlie
   2 | Puck       | +6422221112                   | RobinGoodfellow
   3 | Topolino   | 54321                         |
-------------------------------------------------------------------
```

See also
```
VOIP SIP USER ADD
VOIP SIP USER CREATE
VOIP SIP USER DELETE
VOIP SIP USER LIST
VOIP SIP USER REMOVE
VOIP SIP USER SHOW
```

6.2.8.1.5 VOIP SIP USER REMOVE

Syntax `VOIP SIP USER REMOVE <username> PORT <portname>`

Description This command removes a single user from the port where it was added with the VOIP SIP USER ADD command.

Removing a user from a port results in an un-registration request to the location server.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
username	An existing user (it can also be the ID value associated with the user name). To display the existing users, use the VOIP SIP USER LIST command.	N/A
portname	An existing port. To know the ports where the user is added, use the VOIP SIP USER SHOW command.	N/A

Example --> voip sip user remove MrBrown port fxs0

See also
```
VOIP SIP USER ADD
VOIP SIP USER CREATE
VOIP SIP USER DELETE
VOIP SIP USER LIST
VOIP SIP USER REMOVE
VOIP SIP USER SHOW
```

6.2.8.1.6 VOIP SIP USER SHOW

Syntax `VOIP SIP USER SHOW <username>`

Description This command displays the following information about a named user:

- Country code
- Area Code
- Address
- Pseudonym
- Business-group ID
- Domain
- Authetication (login:password)
- Transport
- SIP registration state
- Attached ports
- Call forwarding settings

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
username	An existing user. To display the existing users, use the VOIP SIP USER LIST command.	N/A

Example --> voip sip user show MrBrown

```
Gateway user: MrBrown
------------------------------------------------------------------------
   Country Code:
   Area Code:
   Address:                    12345
   Pseudonym:                  Charlie
   Business group ID:
   Domain:                     192.168.102.3
   Authentication:             charlie:123charlie
   Transport:
   State:                      registered (expire time: 2864 Sec.)
```

```
Attached ports:             port0
Call Forwarding:
   on all calls:            not active
   on busy:                 not active
   on not answer:           not active
   not answer time-out:     30 Sec.
```

See also VOIP SIP USER ADD
VOIP SIP USER CREATE
VOIP SIP USER DELETE
VOIP SIP USER LIST
VOIP SIP USER REMOVE
VOIP SIP USER SHOW
VOIP SIP USER SET

6.2.9 VoIP SIP FDB command reference

This section describes the commands available on the iMG intelligent Multiservice Gateway to configure and manage the FDB module.

6.2.9.1 VoIP SIP FDB CLI commands

The table below lists the ***VoIP SIP FDB*** commands provided by the CLI:

TABLE 6-9 VoIP SIP SDB CLI Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SIP FDB CREATE	X	X	X	X	X	X	X	X	X
VOIP SIP FDB DELETE	X	X	X	X	X	X	X	X	X
VOIP SIP FDB LIST	X	X	X	X	X	X	X	X	X
VOIP SIP FDB SHOW	X	X	X	X	X	X	X	X	X

6.2.9.1.1 VOIP SIP FDB CREATE

Syntax `VOIP SIP FDB CREATE <name> ADDRESS <digit-map> CONTACT <contact-host:port/transport;proxy> [DOMAIN <host>] [FWADDRESS <tel-number>]`

Description This command creates a new entry in the forwarding database (FDB).

ADDRESS is the called address expected for receiving by the calling end-point in order to forward the call to the CONTACT.

CONTACT is the host reference where the call is forwarded. The contact-host part is the default to form the URL domain (Request-URI, From and To fields).

The flag proxy modifies the rule to make the Request-URI: if it is present then the Request-URI domain gets the value from the contact-host part of CONTACT parameter otherwise the current call domain will be used.

The DOMAIN assigns the call domain and it is used to format the "To" and "From" headers. It is optional and the contact host part is used if it is not set.

The FWADDRESS replaces the destination address of the call. It is optional and it is used to make a short selection rule (e.g. dialled number 01 corresponds to 0039022414112l)

Options

The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies this specific FDB rule. The name must not be present already. The FDB name can be at most 16 characters long.	N/A
digit-map	The called user address (i.e. phone number) expected to be received. It can be a digit map expression as described in section 0.The digit-map can be at most 32 chars long.	N/A
contact-host	The hostname or IPv4 address of the remote end-point where call must be routed. Contact-host can be at most 256 chars long (when using hostname format).	N/A
port	The UDP/TCP port on the contact host to which signalling messages are sent.	5060
transport	The protocol used to transport the signalling messages to the contact host. Possible values are: udp tcp	udp
proxy	If proxy is specified, the contact host is considered to be a proxy server, otherwise the contact-host is considered to be another SIP end-point (e.g. another iMG unit)	none
host	The domain assigned to the redirected call. It can be a host-name or IPv4 address. ***Host*** can be at most 256 chars long (when using hostname format).	N/A

tel-number	It is the new number to which the call is redirected.	N/A

Example --> voip sip fdb create default address 9x. contact 192.168.1.10 domain voip.atkk.com

See also
```
VOIP SIP FDB LIST
VOIP SIP FDB SHOW
```

6.2.9.1.2 VOIP SIP FDB DELETE

Syntax `VOIP SIP FDB DELETE <name>`

Description This command deletes a single FDB entry created using the VOIP SIP FDB CREATE command. To show the list of existing FDB entries, use the VOIP SIP FDB LIST command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	A name (or the ID value) that identifies an existing user in the forwarding database. To display the existing FDB entries, use the VOIP SIP FDB LIST command.	N/A

Example --> voip sip fdb delete default

See also
```
VOIP SIP FDB CREATE
VOIP SIP FDB LIST
```

6.2.9.1.3 VOIP SIP FDB LIST

Syntax `VOIP SIP FDB LIST`

Description This command lists information about FDB entries added using the VOIP SIP FDB CREATE command.

The following information is displayed:

- FDB entry ID numbers
- FDB entry names
- FDB entry Address

Note: If an FDB name is longer than 32 chars, the name is shown in a short format (only the initial part of the name is displayed). To show the full name use the VOIP SIP FDB SHOW command, specifying the user ID instead of user name.

Example --> voip sip fdb list

```
Gateway Forwarding DataBase:
ID  |    Name    |    Address
```

```
----|------------|---------------------
  1 |   pstn     |    9x.
-------------------------------------
```

See also VOIP SIP FDB CREATE
VOIP SIP FDB SHOW

6.2.9.1.4 VOIP SIP FDB SHOW

Syntax VOIP SIP FDB SHOW <name>

Description This command lists information about a named FDB entry added to the forwarding database using the VOIP SIP FDB CREATE command. The following information is displayed:

- Address
- Domain
- Contact

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	A name (or the ID value) that identifies an existing user in the forwarding database. To display the existing FDB entries, use the VOIP SIP FDB LIST command.	N/A

Example --> voip sip fdb show MrJohn

Gateway forwarding database entry: MrJohn

```
-------------------------------------------
   Address:              2010
   Area Code (AC):
   Domain:               192.168.0.5
   Contact:              10.17.90.51
```

See also VOIP SIP FDB LIST

6.2.10 VoIP SIP ALERTINFO command reference

This section describes the commands available on the iMG intelligent Multiservice Gateway to configure and manage ringing cadence mapping.

6.2.10.1 VoIP SIP ALERTINFO CLI commands

The table below lists the ***VoIP SIP ALERTINFO*** commands provided by the CLI:

TABLE 6-10 VoIP SIP Alertinfo CLI commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SIP ALERTINFO CREATE	X	X	X	X	X	X	X	X	X
VOIP SIP ALERTINFO DELETE	X	X	X	X	X	X	X	X	X
VOIP SIP ALERTINFO LIST	X	X	X	X	X	X	X	X	X

6.2.10.1.1 VOIP SIP ALERTINFO CREATE

Syntax `VOIP SIP ALERTINFO CREATE <name> CADENCE-TYPE <ring-cadence >`

Description This command creates an alert-info name to represent a ring-cadence

NAME is the text string assigned to the incoming SIP message's alert-info header.

RING-CADENCE is the ringing pattern announcing for collie.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the ringing-cadence presentation. The name must not be present already. The name can be at most 16 characters long.	N/A
cadence-type	The supported cadence type.	N/A

Example --> voip sip alertinfo create short-short-short cadence-type distinctive-ring-2

See also `VOIP SIP ALERTINFO LIST`

6.2.10.1.2 VOIP SIP ALERTINFO DELETE

Syntax `VOIP SIP ALERTINFO DELETE <name>`

Description This command deletes an existing alert-info name.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	A name (or the ID value) that identifies the ringing cadence and the alert-info (in SIP message) mapping.	N/A

Example --> voip sip alertinfo delete distinctive-ring-1

See also VOIP SIP ALERTINFO CREATE
VOIP SIP ALERTINFO LIST

6.2.10.1.3 VOIP SIP ALERTINFO LIST

Syntax VOIP SIP ALERTINFO LIST

Description This command lists information about ALERTINFO entries added using the VOIP SIP ALERTINFO CREATE command.

The following information is displayed:

- ALERTINFO entry ID numbers
- ALERTINFO entry names
- CADENCE-TYPE

Example --> voip sip alerrinfo list

```
 ID  |        AlertInfo        |  Cadence |
-----|-------------------------|----------|
   1 | ping-ring               | pingring
   2 | distinctive-ring-1      | cadence1
   3 | distinctive-ring-2      | cadence2
   4 | distinctive-ring-3      | cadence3
   5 | distinctive-ring-4      | cadence4
   6 | distinctive-ring-5      | cadence5
   7 | distinctive-ring-6      | cadence6
   8 | distinctive-ring-7      | cadence7
   9 | distinctive-ring-8      | cadence8
-----------------------------------------
```

See also VOIP SIP ALERTINFO CREATE

6.3 VoIP phone ports

This chapter describes the telephony services available on the iMG and the support for analogue (FXS) voice ports.

The analogue endpoint module (AEP) is the module in charge to control analogue ports. This module detects hardware events like off-hook and DTMF key press and controls hardware functions such as tone generation and ringing.

The analogue endpoint module also performs the voiceband processing required to interface analog or PCM voice, fax with data networks incorporating packet-based protocols such as Internet protocol (IP).

This system incorporates a voiceband processor (VoIP DSP) that operates in conjunction with analogue interface circuitry and with the unit main processor (CPU).

The unit main processor implements packet network protocol stacks and system control, while the voice-band processor primarily performs mathematically intensive DSP algorithms.

The following are the features available on the ***Voice system***:

Voice encoding/decoding

- G.711 A-/μ-law 64 Kbps PCM Speech CODEC
- G.729A/B CS-ACELP Speech CODEC with VAD
- G.726-32Kbps
- T.38 support for transmission of T.30 fax signals into T.30 Internet Fax Protocol (IFP) packets.

Voice quality management

- Fixed Gain Control configurable independently on TX and RX transmission
- G.168 Line Echo Cancellation management (disabled or 16 ms – on analogue ports only)
- Voice Activity Detection (VAD)
- Comfort Noise Generation (CNG)

Telecom tone management

- Tone Generation
- DTMF Detection

6.3.1 Port configuration

Port creation and configuration (if necessary) are part of the VoIP system configuration steps required in order to receive or make calls, as illustrated in Figure 6-4.

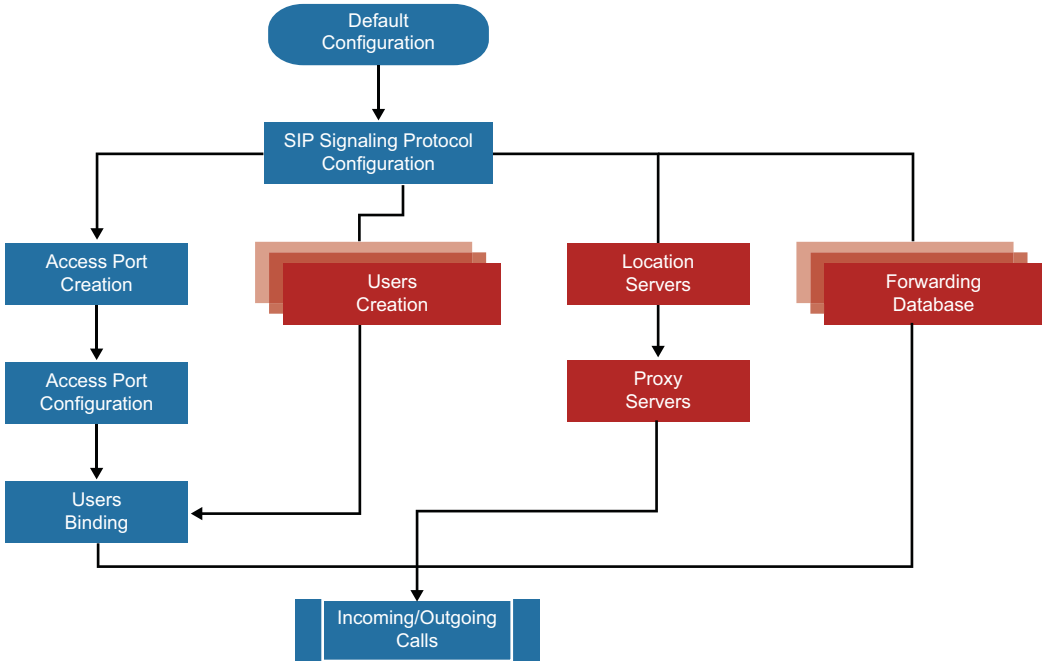


FIGURE 6-4 VoIP subsystem configuration - basic steps

By default, analogue access ports are not configured in the system when the unit starts from a factory default configuration. If a port is not defined, no users can be added to the port and therefore no incoming calls can be received and no outgoing calls can be made.

On the iMG, attempting to make a call through an undefined analogue port will result in absence of any tone provided by the unit.

To create a port, use the command VOIP EP ANALOGUE CREATE and to enable a port use the command VOIP EP ANALOGUE ENABLE.

Each access port has a unique identifier used during the VOIP EP ANALOGUE CREATE command. Depending on the model, the following ports and port identifiers can be used:

- iBG series gateways have their analogue ports named ep1-1, ep1-2, ep2-1, ep2-2, etc.
- RG & iMG series gateways have their analogue ports named tel1, tel2, etc.

Table 1 (RG/iMG Models) lists the number of FXS ports available on each gateway.

To disable a port use the VOIP EP ANALOGUE DISABLE command.

Port configuration is managed through the VOIP EP ANALOGUE SET command. It is used to configure the following subsections:

- Digit Map/Dial Mask
- Voice Coder/Decoder
- Voice Quality Management
- Telecom Tone Management

6.3.1.1 Digit map

The ***Digit Map*** is a rule used by the access port to understand when dialling is to be considered completed and the dialled number is ready to be processed by the call control layer. It works for outgoing calls (in the direction from user to VoIP network).A digit map is defined either by a (case insensitive) ***string*** or by a list of strings. Each string in the list is an alternative numbering scheme, specified either as a set of digits or timers, or as an expression over which the port will attempt to find a shortest possible match. The following constructs can be used in each digit map:

- ***DTMF***
  A digit from '0' to '9' or one of the symbols 'A', 'B', 'C', 'D'. Symbols '#' or '*', if necessary, have to be added separately.
- ***Timer***
  The symbol 'T' matching the timer expiry. The symbol 'T' at the end of Digit Map indicates that if user has not dialled a digit for a time longer than the value of the inter-digit time, the dialled number shall be considered complete. If the symbol T appears in the middle of digit map expression is not considered and skipped during expression evaluation.
- ***Wildcard***
  The symbol 'x', which matches any digit (' 0' to '9').
- ***Range***
  One or more DTMF symbols enclosed between square brackets (' [' and ']').
- ***Subrange***
  Two digits separated by a hyphen (' -') that matches any digit between and including the two. The subrange construct can only be used inside a range construct, i.e., between '[' and ']'.
- ***Position***
  A period ('.'), which matches an arbitrary number, including zero, of occurrences of the preceding construct.

Also, note that the whole ***Digit Map*** shall not exceed 128 characters.

Let's consider an example where the user in an office wants to call a co-worker's 3-digit extension. The ***Digit Map*** is defined in such a way that the called number is processed after the user has entered 3 digits.

The command to set the ***Digit Map*** could look as follows:

```
voip ep analogue set prt0 digitmap xxx
```

This ***Digit Map*** specifies that after the user has entered any three digits, the call is placed. It's possible to refine this Digit Map by including a range of digits. For example, if all extensions in the user company begin with 2, 3, or 4, the corresponding ***Digit Map*** command could look as:

```
voip ep analogue set prt0 digitmap [2-4]xx
```

If the number dialled begins with anything other than 2, 3, or 4, the call is rejected and a busy tone is generated. Another way to achieve the same result would be:

```
voip ep analogue set prt0 digitmap [234]xx
```

It is possible to combine two or more expressions in the same Digit Map by using the '|' operator, which is equivalent to OR. The left-most expression has precedence over the other expressions

Let's consider the case of a choice: the Digit Map must check if the number is internal (an extension), or external (a local call). Assuming that dialling '9' makes an external call, the Digit Map could be defined with the command:

```
voip ep analogue set prt0 digitmap ([2-4]xx|9[2-9]xxxxxx)
```

In this case the ***Digit Map*** checks if the number begins with 2, 3, or 4 and the number has 3 digits

If not, it checks if the number begins with 9 and the second digit is any digit between 2 and 9 and the number has 7 digits

It may sometimes be required that users dial the '#' or '*' to make calls.

This can be easily incorporated in a Digit Map with the command:

```
voip ep analogue set prt0 digitmap xxxxxxx#|xxxxxxx*
```

The '#' or '*' character could indicate that users must dial the '#' or '*' character at the end of their number to indicate it is complete.

When the outgoing call is in process, the call control layer removes any '#'', '*' and 'T' symbols from the dialled number.

6.3.1.2 Dial mask

The Dial Mask specifies the number of digits that must be removed from the dialled number ***before*** checking the dialled number against the ***Digit Map***.

6.3.1.3 Voice coder/decoder

The Voice system makes use of a specific DSP with an embedded sigma-delta Coder/Decoder to process voice and data from/to access ports.

Different codec types are available in order to satisfy the requirements of different environments.

It's possible to specify more than one codec type for each port using the command VOIP EP ANALOGUE SET CODECS.

The codec specified at the leftmost ends of the codec list has precedence over the other codecs.

The signalling protocol (SIP) will negotiate the active codec based on the capabilities supported by the other peer involved in the VoIP connection. In the case of local calls, the call control layer performs codec negotiation locally.

The following table lists the codecs available on the iMG units.

TABLE 6-11 Codecs Available for iMGs

Codec	Notes
g711a	G.711 A law
g711u	G.711 μ law
g729ab	G.729 Annex A and Annex B
g726-32	G.726 32kbps
T38	Media/codec negotiation for transmission of ITU-T T.30 fax signals via internet. This is not an actual codec, but when specified in the codecs list indicates to the iMG that ITU-T T.38 negotiation of media sessions & fall-back codecs should be enabled.

6.3.1.3.1 T.38 support

The iMG is designed to support the transmission of T.30 fax signals using T.38 Internet Fax Protocol (IFP) packets.

Although T38 is listed the as a supported codec for the iMG family, T.38 is not in itself a codec, but rather a technical solution to map FAX signals into a dedicated IP protocol - overriding the limitations (e.g. signal distortion) that are present when faxes are sent using codecs designed for speech applications.

When T.38 support is enabled and a fax must be sent or received, the intelligent Multiservice Gateway tries firstly to negotiate T.38 support with the called or calling end-point respectively. If this fails, the iMG automatically falls-back to a non-compressed codec such as G711 A-law or μ-law.

6.3.1.4 Voice quality management

To increase the voice/data quality additional parameters can be set on the voice system DSP. The following settings are available on iMG models:

- A fixed jitter buffer. Set to 120 ms with a jitter delay of 60 ms.
- Separate TX and RX direction volume gain control. Adjustable between -48dB and +24dB.
- ITU-T G.168 Line Echo Cancellation. Adjustable between 0 and 32 msec (a value of 0 disabled Line Echo Cancellation).
- Voice activity detection (VAD)/comfort noise generation (CNG).

- Telecom tone management and DTMF relay.
- This is a SIP protocol dependent solution used to transfer DTMF tones out-of-band either using SIP INFO messages, or by means of RFC2833 'Named DTMF Events' within the RTP stream. The underlying logic is as follows:
  - When the iMG attempts to establish a call, it adds RFC2833 'Named Telephone Event' to the capabilities listed for RTP packets, but only if a compressed codec (g726 or g729ab) has been configured for the Voice access port involved in the call.
  - If a call is then established using an uncompressed codec (i.e. g711u or g711a), the iMG will send DTMF tones in-band - irrespective of whether or not the called endpoint supports RFC2833 Named Telephone Events.
  - If however a the call is established using a compressed codec, the iMG will send DTMF tones using RFC2833 Named Telephone Events, but only if the called end-point supports this mechanism - otherwise it switches to the same path used for voice (accepting DTMF distortion).

When the intelligent Multiservice Gateway is going to accept a call, it adds to the capabilities list the RTP packet Named Telephone Event only if a compressed codec (g726 or g729ab) has been configured for the Voice access port involved in the call.

- Then if the call is established using an uncompressed codec (i.e. g711u or g711a), the intelligent Multiservice Gateway will send DTMF tone in-band (independently of whether the caller endpoint supports RTP packet Named Telephone Event) on the same path used for voice.
- If the call is established using a compressed codec, the intelligent Multiservice Gateway will send DTMF tones using RTP packet Named Telephone Event only if the caller end-point supports it, otherwise it switches to the same path used for voice (accepting DTMF distortion).
- Inter-digit time/Inter-digit critical time.
  Inter-digit time is the maximum acceptable time between the dialling of one digit and the next. If a time longer than the ***Inter-digit time*** elapses after the dialling of a digit, dialling is considered complete. The timer 'T' in the digit map expression uses the ***Inter-digit time*** value. To change the value of the ***Inter-digit time*** use the VOIP EP ANALOGUE SET IDT-PARTIAL command.
  Inter-digit critical time is the maximum acceptable time between the off-hook event and the dialling of the first digit. If a time longer than this has elapsed since off-hook and dialling has not yet started, then the connection is closed and a busy tone is generated. To change the value of the ***Inter-digit critical ti***me use the VOIP EP ANALOGUE SET IDT-CRITICAL command.
- Off-hook time / On-hook time / Flash-Hook time.
  - Off-hook time is the minimum time (msec) that the analogue line must stay in off-hook before the system detects the off-hook state.
  - On-hook time is the minimum time (msec) that the analogue line must stay in on-hook before the system detects the on-hook state.
  - Flash-hook. The flash-hool period may vary between countries, and the iMG flash-hook time parameter allows the iMG user to allow for this. Note that flash-hook time can not be greater that on-hook time.

The iMG detects a flash-hook event when the on-hook period falls within a a time window. The lower bound of this window is one third of the configured flash-hook time, and the upper bound is the lesser of on-hook time and double the configured flash-hook time.

6.3.1.5 Country-specific telecom tones

The iMG is able to reproduce the same country-specific telecom tones used by Central Offices or Foreign Exchanges simply by selecting the preferred country via the VOIP EP ANALOGUE SET COUNTRY command.

Dial Tone, Busy Tone and ***Ring Back T***one refer to ITU-T E.180 specifications as reported in the following table:

TABLE 6-12 Country-specific Telecom tones

Country	Dial Tone		Busy Tone		Ring Back Tone	
	Frequency (Hz)	Cadence (msec)	Frequency (Hz)	Cadence (msec)	Frequency (Hz)	Cadence (msec)
Australia	425x25	Continuous	400	375 - 375	400x17	400 - 200 - 400 - 2000
Austria	450	Continuous	450	300 - 300	450	1000 - 5000
Belgium	425	Continuous	425	500 - 500	425	1000 - 3000
Canada	350+440	Continuous	480+620	500 - 500	440+480	2000 - 4000
China	450	Continuous	450	350 - 350	450	1000 - 4000
France	440	Continuous	440	500 - 500	440	1500 - 3500
Germany	425	Continuous	425	480 - 480	425	250 - 4000 - 1000 - 4000 - 1000 - 4000
Israel	400	Continuous	400	500 - 500	400	1000 - 3000
Italy	425	600 - 1000 - 200 - 200	425	200 - 200	425	1000 - 4000
Japan	400	Continuous	400	500 - 500	400x16	1000 - 2000
New Zealand	400	Continuous	400	500 - 500	400 + 450	400 - 200 - 400 - 2000
Norway	no tone	//	425	1000 - 4000	425	500 - 500
Russia	no tone	//	425	400 - 400	425	800 - 3200

TABLE 6-12 Country-specific Telecom tones (Continued)

Singapore	425	Continuous	425	750 - 750	425x24	400 - 200 - 400 - 2000
Spain	425	Continuous	425	200 - 200	425	1500 - 3000
Sweden	425	Continuous	425	250 - 250	425	1000 - 5000
Turkey	450	Continuous	450	500 - 500	450	2000 - 4000
United Kingdom	350+440	Continuous	400	375 - 375	400+450	400 - 200 - 400 - 2000
United States	350+440	Continuous	480+620	500 - 500	440+480	2000 - 4000

Note: Frequency in Hz:f1xf2 means f1 is modulated by f2

Note: f1+f2 is the juxtaposition of two frequencies f1 and f2 without modulation.

Note: Cadence in seconds:ON – OFF

6.3.1.6 Port enable/disable

It's possible to temporarily disable a port by using the VOIP EP ANALOGUE DISABLE command.

Any call originated from, or sent to, a user attached to a disabled access port is discharged.

When a port is disabled, each user added to the port starts to un-register from the Location Server (SIP *signalling* protocol).

To change the port status from disabled to enabled use the VOIP EP ANALOGUE ENABLE command.

As soon the port is enabled all the users attached to the port automatically restart the process of registration with the location server or gatekeeper.

To show the users attached to a port (and their SIP registration status), use the VOIP EP ANALOGUE SHOW command.

6.3.2 VoIP ADMIN Command Reference

6.3.2.1 VoIP ADMIN commands

VoIP ADMIN commands set the service profile to be compliant with specific customer requirement and assign main parameter concerning network administration.

TABLE 6-13 Commands for VoIP Admin

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP SHOW	X	X	X	X	X	X	X	X	X
VOIP ADMIN ENABLE PROFILE	X	X	X	X	X	X	X	X	X
VOIP ADMIN ENABLE RFC3660-DIGIT-INPUT-TIMER	X	X	X	X	X	X	X	X	X
VOIP ADMIN DISABLE PROFILE	X	X	X	X	X	X	X	X	X
VOIP ADMIN DISABLE RFC3660-DIGIT-INPUT-TIMER	X	X	X	X	X	X	X	X	X
VOIP ADMIN PREFIX-REPLACEMENT ADD	X	X	X	X	X	X	X	X	X
VOIP ADMIN PREFIX-REPLACEMENT CREATE	X	X	X	X	X	X	X	X	X
VOIP ADMIN PREFIX-REPLACEMENT DELETE	X	X	X	X	X	X	X	X	X
VOIP ADMIN PREFIX-REPLACEMENT LIST	X	X	X	X	X	X	X	X	X
VOIP ADMIN PREFIX-REPLACEMENT REMOVE	X	X	X	X	X	X	X	X	X
VOIP ADMIN PREFIX-REPLACEMENT SHOW	X	X	X	X	X	X	X	X	X
VOIP ADMIN SET E164-COUNTRY-CODE	X	X	X	X	X	X	X	X	X
VOIP ADMIN SET INTERNATIONAL-CALL-PREFIX	X	X	X	X	X	X	X	X	X
VOIP ADMIN SHOW	X	X	X	X	X	X	X	X	X

6.3.2.1.1 VOIP SHOW

Syntax `VOIP SHOW`

Description This command shows the configured VoIP protocol.

Example --> voip show

Gateway base protocol: SIP

Endpoints: 1

Users: 1

FDB items: -

6.3.2.1.2 VOIP ADMIN ENABLE PROFILE

Syntax `VOIP ADMIN ENABLE PROFILE <profilename>`

Description It enables a specific customer profile.

*Note: The command is available only for the **SIP protocol***

Note: The command MUST be executed before users are provisioned.

Note: Enabling a specific profile re-sets the numbering plan parameters to default.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
profilename	The profile identifies a specific behaviour At the moment, the following profile have been developed: • ntt-cw NTT-Comware profile • sonus Sonus solution for Voice over IP service provided by AT&T • lucent Lucent SIP proxy profile • Broadsoft. When activated, the broadsoft profile has only one effect: If a SIP Info request is encoded to send a flash-hook event, the content-type header will be set to 'application/broadsoft' instead of 'application/dtmf-relay' No profile is enabled by default.	N/A

Example --> voip admin enable profile sonus

6.3.2.1.3 VOIP ADMIN ENABLE RFC3660-DIGIT-INPUT-TIMER

Syntax `VOIP ADMIN ENABLE RFC3660-DIGIT-INPUT-TIMER`

Description This command enables the management of critical and partial inter-digit times as specified in RFC3660.

Example --> voip admin enable rfc3660-digit-input-timer

See also `VOIP EP SET IDT-CRITICAL`
`VOIP EP SET IDT-PARTIAL`

6.3.2.1.4 VOIP ADMIN DISABLE PROFILE

Syntax `VOIP ADMIN DISABLE PROFILE`

Description This command disables the specific customer profile that was in use; standard behaviour is then assumed.

Note: This command is not available once users have been provisioned.

Note: Disabling a specific profile re-sets the numbering plan parameters to default.

Example --> voip admin disable profile

6.3.2.1.5 VOIP ADMIN DISABLE RFC3660-DIGIT-INPUT-TIMER

Syntax `VOIP ADMIN DISABLE RFC3660-DIGIT-INPUT-TIMER`

Description This command disables the management of critical and partial inter-digit times as specified in RFC3660.

Example --> voip admin disable rfc3660-digit-input-timer

6.3.2.1.6 VOIP ADMIN PREFIX-REPLACEMENT ADD

Syntax `VOIP ADMIN PREFIX-REPLACEMENT ADD <name> PORT <ep-name>`

Description This command adds the prefix-replacement rule to an already provisioned endpoint. The prefix replacement rule must already have been created with the VOIP ADMIN PREFIX-REPLACEMENT CREATE" command.

Options The following table gives the range of values for each option which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing prefix replacement rule created with the command "VOIP ADMIN PREFIX-REPLACEMENT CREATE". To display existing access port names, use the VOIP ADMIN PREFIX-REPLACEMENT LIST command.	N/A
ep-name	An existing access port. To display existing access port names, use the VOIP EP LIST command.	N/A

Example --> voip admin prefix-replacement add pref001 port prt0

See also
```
VOIP ADMIN PREFIX-REPLACEMENT CREATE
VOIP ADMIN PREFIX-REPLACEMENT DELETE
VOIP ADMIN PREFIX-REPLACEMENT LIST
VOIP ADMIN PREFIX-REPLACEMENT REMOVE
VOIP ADMIN PREFIX-REPLACEMENT SHOW
```

6.3.2.1.7 VOIP ADMIN PREFIX-REPLACEMENT CREATE

Syntax `VOIP ADMIN PREFIX-REPLACEMENT CREATE <name> PREFIX <digit-map> REPLACEMENT <digit>`

Description This command creates a prefix-replacement rule. When the rule is added to an endpoint, if the PREFIX digit-map is matched, it is replaced by the REPLACEMENT digit(s).

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A string identifies the item, 1 to 16 characters in length. Valid characters are any printable characters, except code 0x2E and 0x2F; digits cannot be used as first character and if the space character is present, the string must be quoted..	N/A
digit-map	An expression string 1 to 16 characters in length. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-'. The service is disabled by default.	N/A
digits	A telephone number; 1 to 16 characters in length. Valid characters are only numerical characters accepts the first one that may assume the '+' letter.	N/A

Example --> voip admin prefix-replacement create prefix001 prefix *001 replacement 04411

See also
```
VOIP ADMIN PREFIX-REPLACEMENT ADD
VOIP ADMIN PREFIX-REPLACEMENT DELETE
VOIP ADMIN PREFIX-REPLACEMENT LIST
VOIP ADMIN PREFIX-REPLACEMENT REMOVE
VOIP ADMIN PREFIX-REPLACEMENT SHOW
```

6.3.2.1.8 VOIP ADMIN PREFIX-REPLACEMENT DELETE

Syntax `VOIP ADMIN PREFIX-REPLACEMENT DELETE <name>`

Description This command deletes a prefix-replacement rule.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing prefix replacement rule created with the command "VOIP ADMIN PREFIX-REPLACEMENT CREATE". To display existing access port names, use the VOIP ADMIN PREFIX-REPLACEMENT LIST command.	N/A

Example --> voip admin prefix-replacement delete prefix001

See also
```
VOIP ADMIN PREFIX-REPLACEMENT ADD
VOIP ADMIN PREFIX-REPLACEMENT CREATE
VOIP ADMIN PREFIX-REPLACEMENT LIST
VOIP ADMIN PREFIX-REPLACEMENT REMOVE
VOIP ADMIN PREFIX-REPLACEMENT SHOW
```

6.3.2.1.9 VOIP ADMIN PREFIX-REPLACEMENT LIST

Syntax `VOIP ADMIN PREFIX-REPLACEMENT LIST`

Description This command lists all defined prefix-replacement rules.

Example --> voip admin prefix-replacement list

```
Gateway prefix replacements:
 ID  |    Name    |      Prefix      |              Replacement
-----|------------|------------------|------------------------------
   1 | mobile     | *001             | 712
   2 | internal   | *002             | 713
   3 | extern     | *003             | 714
-------------------------------------------------------------------
-->
```

See also
```
VOIP ADMIN PREFIX-REPLACEMENT ADD
VOIP ADMIN PREFIX-REPLACEMENT CREATE
VOIP ADMIN PREFIX-REPLACEMENT DELETE
VOIP ADMIN PREFIX-REPLACEMENT REMOVE
VOIP ADMIN PREFIX-REPLACEMENT SHOW
```

6.3.2.1.10 VOIP ADMIN PREFIX-REPLACEMENT REMOVE

Syntax `VOIP ADMIN PREFIX-REPLACEMENT REMOVE <name> PORT <ep-name>`

Description This command removes a prefix-replacement rule from an existing endpoint.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing prefix replacement rule created with the command "VOIP ADMIN PREFIX-REPLACEMENT CREATE". To display existing access port names, use the VOIP ADMIN PREFIX-REPLACEMENT LIST command.	N/A

ep-name	An existing access port. To display existing access port names, use the VOIP EP LIST command.	N/A

Example --> voip admin prefix-replacement remove prefix001 port prt0

See also
```
VOIP ADMIN PREFIX-REPLACEMENT ADD
VOIP ADMIN PREFIX-REPLACEMENT CREATE
VOIP ADMIN PREFIX-REPLACEMENT DELETE
VOIP ADMIN PREFIX-REPLACEMENT LIST
VOIP ADMIN PREFIX-REPLACEMENT SHOW
```

6.3.2.1.11 VOIP ADMIN PREFIX-REPLACEMENT SHOW

Syntax `VOIP ADMIN PREFIX-REPLACEMENT SHOW <name>`

Description This command shows a prefix-replacement rule.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing prefix replacement rule created with the command "VOIP ADMIN PREFIX-REPLACEMENT CREATE". To display existing access port names, use the VOIP ADMIN PREFIX-REPLACEMENT LIST command.	N/A

Example --> voip admin prefix-replacement show prefix001

```
Gateway prefix replacement: prefix001
------------------------------------------------------------------
   Prefix:                          *001
   Replacement:                     712
   Attached ports:                  prt0
-->
```

See also
```
VOIP ADMIN PREFIX-REPLACEMENT ADD
VOIP ADMIN PREFIX-REPLACEMENT CREATE
VOIP ADMIN PREFIX-REPLACEMENT DELETE
VOIP ADMIN PREFIX-REPLACEMENT LIST
VOIP ADMIN PREFIX-REPLACEMENT REMOVE
```

6.3.2.1.12 VOIP ADMIN SET E164-COUNTRY-CODE

Syntax `VOIP ADMIN SET E164-COUNTRY-CODE <code>`

Description This command set the E.164 country code. The E.164 country code accepts only digits (not digit-maps), that are 1 to 3 characters in length. No code is provisioned by default. Assignment is only allowed if no users have yet been created. If the E.164 country code is configured, the "userinfo" field of "From" headers in all SIP requests adopts the E.164 global address format <+><country-code><area-code><subscriber-address>. Example: From: "+390241412533" <sip:+390241412533@10.17.90.165;user=phone>;tag=AQBGCRAgMEBAQAxx

If the E.164 country code is NOT configured, existing rules are followed and the "userinfo" field of "From" headers in all SIP requests has the address format <area-code><subscriber-address>; see the following example where the area code is "02": From: "02414112533" <sip:02414112533@10.17.90.165;user=phone>;tag=AQBGCRAgMEBAQAxx.

Example voip admin set e164-country-code 64

See also `VOIP ADMIN SET INTERNATIONAL-CALL-PREFIX`

6.3.2.1.13 VOIP ADMIN SET INTERNATIONAL-CALL-PREFIX

Syntax `VOIP ADMIN SET INTERNATIONAL-CALL-PREFIX <prefix>`

Description If the gateway has been provisioned with an E.164 country code (see VOIP ADMIN SET E164-COUNTRY-CODE), then incoming calls will be recognised if addressed to either '<user address>' or '+<country code><user address>. This command allows definition of an alternate international call prefix (typically 00), extending the set of recognised numbers to also include '<prefix><country code><user address>'.

No prefix is provisioned by default. Assignment is allowed only if no users have yet been created.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
prefix	A digit string (not digit-map), from 1 to 8 characters in length.	none

Example
```
voip admin set e164-country-code 64
voip admin set international-call-prefix 00
...
voip sip user create user1 address 1017901291
```

The gateway will now recognise the follow in-dialled numbers:
1017901291, +641017901291 and 00641017901291.

See also VOIP ADMIN SET E164-COUNTRY-CODE

6.3.2.1.14 VOIP ADMIN SHOW

Syntax `VOIP ADMIN SHOW`

Description This command shows the VoIP admin settings.

Example `--> voip admin show`

```
Gateway Admin:
------------------------------------------------------------------------
   Profile:                              none
   E.164 country code:                   none
   International call prefix:           none
   Extended call prefix:                 disabled
   Input digit timer:                    proprietary handling
   Hotline mode:                         endpoint
-->
```

6.3.3 VoIP EP command reference

This section describes the commands available on iMG to create, configure and manage access ports (also called ***end points - EP***).

6.3.3.1 VoIP EP CLI commands

The table below lists the ***VOIP EP*** commands provided by the CLI:

TABLE 6-14 Commands for VoIP EP

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP EP CREATE	X	X	X	X	X	X	X	X	X
VOIP EP DELETE	X	X	X	X	X	X	X	X	X
VOIP EP DIAGNOSE						X			
VOIP EP DISABLE	X	X	X	X	X	X	X	X	X
VOIP EP ENABLE	X	X	X	X	X	X	X	X	X
VOIP EP LIST	X	X	X	X	X	X	X	X	X
VOIP EP SET ALERTING-TIMEOUT	X	X	X	X	X	X	X	X	X
VOIP EP SET ATTENDED-CALL-TRANSFER	X	X	X	X	X	X	X	X	X
VOIP EP SET BLIND-CALL-TRANSFER	X	X	X	X	X	X	X	X	X
VOIP EP SET CALL-ON-HOLD-SERVICE	X	X	X	X	X	X	X	X	X
VOIP EP SET CALL-WAITING-SERVICE	X	X	X	X	X	X	X	X	X
VOIP EP SET CFWD ALL-CALLS	X	X	X	X	X	X	X	X	X
VOIP EP SET CFWD ON-BUSY	X	X	X	X	X	X	X	X	X
VOIP EP SET CFWD ON-NO-ANSWER	X	X	X	X	X	X	X	X	X
VOIP EP SET CFWD-EXT	X	X	X	X	X	X	X	X	X
VOIP EP SET CLIP	X	X	X	X	X	X	X	X	X
VOIP EP SET CLIP-REDUCTION	X	X	X	X	X	X	X	X	X
VOIP EP SET CLIR	X	X	X	X	X	X	X	X	X
VOIP EP SET CNG	X	X	X	X	X	X	X	X	X
VOIP EP SET CODECS	2	2	2	1	2	1	2	1	1
VOIP EP SET CONFERENCE-SERVICE	X	X	X	X	X	X	X	X	X
VOIP EP SET COUNTRY	X	X	X	X	X	X	X	X	X
VOIP EP SET DIALMASK	X	X	X	X	X	X	X	X	X
VOIP EP SET DIALMODE	X	X	X	X	X	X	X	X	X
VOIP EP SET DIGITMAP	X	X	X	X	X	X	X	X	X
VOIP EP SET EMERGENCY-SERVICE-NUMBER	X	X	X	X	X	X	X	X	X
VOIP EP SET FAX-MODEM-DETECTION	X	X	X	X	X	X	X	X	X

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP EP SET FLASHHOOK-TIME	X	X	X	X	X	X	X	X	X
VOIP EP SET HOLD-LOCAL-TONE-SERVICE	X	X	X	X	X	X	X	X	X
VOIP EP SET HOTLINE TIME-OUT	X	X	X	X	X	X	X	X	X
VOIP EP SET HOTLINE DISABLE	X	X	X	X	X	X	X	X	X
VOIP EP SET HOTLINE ENABLE	X	X	X	X	X	X	X	X	X
VOIP EP SET IDT-PARTIAL	X	X	X	X	X	X	X	X	X
VOIP EP SET INTERNAL-3-WAY-CALL	X	X	X	X	X	X	X	X	X
VOIP EP SET JITTERDELAY	X	X	X	X	X	X	X	X	X
VOIP EP SET JITTERMODE	X	X	X	X	X	X	X	X	X
VOIP EP SET LEC	4	4	4	3	4	3	4	3	3
VOIP EP SET OFFHOOK-TIME	X	X	X	X	X	X	X	X	X
VOIP EP SET ONHOOK-TIME	X	X	X	X	X	X	X	X	X
VOIP EP SET RXGAIN	X	X	X	X	X	X	X	X	X
VOIP EP SET STUTTER-DIAL-TONE	X	X	X	X	X	X	X	X	X
VOIP EP SET SUPPLEMENTARY-SERVICE-PREFIX	X	X	X	X	X	X	X	X	X
VOIP EP SET TXGAIN	X	X	X	X	X	X	X	X	X
VOIP EP SET UNREGISTERED-TONE	X	X	X	X	X	X	X	X	X
VOIP EP SET VAD	X	X	X	X	X	X	X	X	X
VOIP EP SHOW	X	X	X	X	X	X	X	X	X

6.3.3.1.1 VOIP EP CREATE

Syntax `VOIP EP ANALOGUE CREATE <name> TYPE <port-type> PHYSICAL-PORT <phy-port-id>`

Description This command adds a named access port and binds it to a physical access port.

If the physical resource is already assigned to another named port, an error is raised and the command fails.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the access port. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit. The maximum length is fixed to 16 characters.	N/A
port-type	This is the user access typology served by the physical port; the possible values depend on the model (analog access or digital access).Valid values are al-fxs-del, al-fxs-lc and al-fxo-del	N/A
phy-port-id	This is the physical port providing the access to VoIP network. "Port configuration"	N/A

Example --> voip ep analogue create prt0 type al-fxs-del physical-port tel1

See also
```
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SET
VOIP EP ANALOGUE SHOW
```

6.3.3.1.2 VOIP EP DELETE

Syntax `VOIP EP ANALOGUE DELETE <name>`

Description This command deletes the named access port created previously using the VOIP EP CREATE command.

Note: Deleting an access port where one or more users are attached, causes a deregistration procedure to be invoked for the users attached to the removed port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display existing access port names, use the VOIP EP LIST command.	N/A

Example --> voip ep analogue delete prt0

See also

```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SET
VOIP EP ANALOGUE SHOW
```

6.3.3.1.3 VOIP EP DIAGNOSE

Syntax `VOIP EP ANALOGUE DIAGNOSE <name> {INTERNAL|EXTERNAL}`

Description This command starts GR.909 metallic loop tests on the selected analogue endpoint.

The support for metallic loop tests (internal and/or external) is available only on specific iMG families.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display existing access port names, use the VOIP EP LIST command.	N/A
internal	In this case diagnostic tests apply only to internal iMG circuitry.	N/A
external	In this case diagnostic tests apply only to the external metallic loop and resistive loads connected to the subscriber side.	N/A

Example --> voip ep analogue diagnose tel1 internal

```
End point:tel1, PHY tel1 is slic port #0

Calibration:
 TG 1.1865V
 RG 1.1865V
 TR 2.7319V

      :                                    :  Pass       :
Status :             Test                   :  Criteria   :  Results
-------------------------------------------------------------------------
PASS   : Battery input SWY                  :    >=45V    : 52.718V
PASS   : Tip/Ground Voltage                 :  abs <= 10V : -5.1268V
```

```
PASS   : Ring/Ground Voltage                  :  abs >= 38V : -46.888V
PASS   : Tip/Ring Voltage                     : abs >= 38V  : -41.454V
PASS   : Tip/Ring Current                     : abs <= 10mA : .12993mA
-------------------------------------------------------------------
PASS   : AC Ringing Voltage                 :    >=53V    : 56.492Vrms
PASS   : AC Ringing Frequency                : 23Hz to 27Hz: 25Hz
-------------------------------------------------------------------
PASS   : Off Hook Sense                    :     N/A     : No Problems
Found
```

Example --> voip ep analogue diagnose tel1 external

```
End point:tel1, PHY tel1 is slic port #0

      :                                       :  Pass       :
Status :              Test                    :  Criteria   :  Results
-------------------------------------------------------------------
PASS   : Off Hook Sense                    :     N/A     : No Problems
Found
-------------------------------------------------------------------
PASS   : HEMF    Tip/Ground  DC Voltage      : abs <= 135V : .43944V
PASS   : HEMF    Ring/Ground DC Voltage      : abs <= 135V : .43212V
PASS   : HEMF    Tip/Ring    DC Voltage     : abs <= 135V : -.014648V

PASS   : HEMF    Tip/Ground  AC Voltage      : abs <= 50V  : 0Vrms @
0Hz
PASS   : HEMF    Ring/Ground AC Voltage      : abs <= 50V  : 0Vrms @
0Hz
PASS   : HEMF    Tip/Ring    AC Voltage      : abs <= 50V  : 0Vrms @
0Hz
-------------------------------------------------------------------
PASS   : FEMF    Tip/Ground  DC Voltage      : abs <= 6V   : .43944V
PASS   : FEMF    Ring/Ground DC Voltage      : abs <= 6V   : .43212V
PASS   : FEMF    Tip/Ring    DC Voltage     : abs <= 6V   : -.014648V

PASS   : FEMF    Tip/Ground  AC Voltage      : abs <= 10V  : 0Vrms @
0Hz
PASS   : FEMF    Ring/Ground AC Voltage      : abs <= 10V  : 0Vrms @
0Hz
PASS   : FEMF    Tip/Ring    AC Voltage      : abs <= 10V  : 0Vrms @
0Hz
-------------------------------------------------------------------
```

```
PASS   : FEMF    Tip/Ring Current            :  Info Only  : .37332mA
-------------------------------------------------------------------------
PASS   : Ringer Equivalance                  :     N/A     : No Problems
Found
-------------------------------------------------------------------------
PASS   : Resistive Fault (Tip/Ring)          :  R >= 150k  : 19969k
PASS   : Resistive Fault (Tip/Ground)        :  R >= 150k  :  2372k
PASS   : Resistive Fault (Ring/Ground)       :  R >= 150k  :  2553k
```

6.3.3.1.4 VOIP EP DISABLE

Syntax `VOIP EP ANALOGUE DISABLE <name>`

Description This command disables the physical port referred to by the named access port.

Use the VOIP EP SHOW command to retrieve the Operational Status of a specific port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display existing access port names, use the VOIP EP LIST command.	N/A

Example --> voip ep analogue disable prt0

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SET
VOIP EP ANALOGUE SHOW
```

6.3.3.1.5 VOIP EP ENABLE

Syntax `VOIP EP ANALOGUE ENABLE <name>`

Description This command enables the physical port referred to by the named access port.

Use the VOIP EP SHOW command to retrieve the Operational Status of a specific port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display existing access port names, use the VOIP EP LIST command.	N/A

Example --> voip ep analogue enable prt0

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SET
VOIP EP ANALOGUE SHOW
```

6.3.3.1.6 VOIP EP LIST

Syntax `VOIP EP ANALOGUE LIST`

Description This command lists the named access port defined in the system using the VOIP EP CREATE command.

The following information is displayed:

- End-point ID value
- End-point name
- Physical port index
- Physical port typology

Example --> voip ep analogue list

```
Gateway access ports:
ID   |    Name    |  Physical Port   |    Typology
-----|------------|------------------|------------------
1    | prt0       | tel1             | al-fxs-del
-------------------------------------------------------
```

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE SET
VOIP EP ANALOGUE SHOW
```

6.3.3.1.7 VOIP EP SET ALERTING-TIMEOUT

Syntax `VOIP EP ANALOGUE SET <name> ALERTING TIME-OUT <sec>`

Description This command sets the number of seconds the analogue port rings for before releasing the call if the user doesn't answer.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing analogue endpoint name.	-
sec	The number of seconds the port rings before the call is cancelled by the called peer. Valid values are from 0 to 600. Setting the values to 0 restore to the default.	0 (default)

Table 6 – voip ep analogue set alerting-timeout command parameters

Example --> voip ep analogue set tel1 alerting-timeout 60

6.3.3.1.8 VOIP EP SET ATTENDED-CALL-TRANSFER

Syntax
```
VOIP EP ANALOGUE SET <name> ATTENDED-CALL-TRANSFER ENABLE
PREFIX <attended_prefix>
VOIP EP ANALOGUE SET <name> ATTENDED-CALL-TRANSFER DISABLE
```

Description This command set the prefix used to activate the attended call transfer feature. The caller is in conversation with "A", it puts "A" on hold and calls "B" using this prefix. The caller and "B" are in conversation. When the caller on-hooks, "B" will be in conversation with "A".

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing analogue endpoint name.	-
attended-prefix	The prefix used to enable the attended call transfer feature only on the endpoint where it is configured. It is a digit-map and is the expression string in use to recognize the prefix. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-', 1 to 10 characters long. It can be configured to none	none

Table 7 – voip ep analogue set alerting-timeout command parameters

Example --> voip ep analogue set tel1 attended-call-transfer enable prefix #98

6.3.3.1.9 VOIP EP SET BLIND-CALL-TRANSFER

Syntax `VOIP EP ANALOGUE SET <name> BLIND-CALL-TRANSFER ENABLE PREFIX <attended_prefix>`

VOIP EP ANALOGUE SET <name> BLIND-CALL-TRANSFER DISABLE

Description This command set the prefix used to activate the blind call transfer feature. The caller is in conversation with "A", it puts "A" on hold and calls "B" using this prefix. When "B" answers will be in conversation with "A".

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing analogue endpoint name.	-
attended-prefix	The prefix used to enable the blind call transfer feature only on the endpoint where it is configured. It is a digit-map and is the expression string in use to recognize the prefix. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-', 1 to 10 characters long. It can be configured to none	none

Example --> voip ep analogue set tel1 blind-call-transfer enable prefix #98

6.3.3.1.10 VOIP EP SET CALL-ON-HOLD-SERVICE

Syntax `VOIP EP ANALOGUE SET <name> CALL-ON-HOLD-SERVICE {ENABLED|DISABLED}`

Description This command enables/disables the call on hold supplementary service. When enabled, the user can put the current call on hold using the flash-hook button and make a new outgoing call. Then the user can switch between each call simply pressing the flash-hook button.

Note: The call-on-hold service is available only if the active VoIP protocol is SIP.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing analogue endpoint name.	-
enabled	Enable the call-on-hold service.	Disabled
disabled	Disable the call-on-hold service	

Example --> voip ep analogue set tel1 call-on-hold service enabled

6.3.3.1.11 VOIP EP SET CALL-WAITING-SERVICE

Syntax `VOIP EP ANALOGUE SET <name> CALL-WAITING-SERVICE {ENABLED|DISABLED}`

Description This command enables/disables the call waiting supplementary service. When enabled, a user already busy in a call is notified of a new incoming call via a special waiting tone and then the user can put the current call on hold using the flash-hook button and answer the new call. Then the user can switch between each call simply pressing the flash-hook button.

Note: The call-waiting service is available only if the active VoIP protocol is SIP.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing analogue endpoint name.	-
enable	Enable the call-waiting service.	Disabled
disable	Disable the call-waiting service	

6.3.3.1.12 VOIP EP SET CFWD ALL-CALLS

Syntax `VOIP EP ANALOGUE SET <name> CFWD ENABLE ALL-CALLS ON-PREFIX <on-prefix> ON-SUFFIX <on-suffix> OFF-PREFIX <off-prefix>`

VOIP EP ANALOGUE SET <name> CFWD DISABLE ALL-CALLS

VOIP EP DIGITAL SET <name> CFWD ENABLE ALL-CALLS ON-PREFIX <on-prefix> ON-SUFFIX <on-suffix> OFF-PREFIX <off-prefix>

VOIP EP ANALOGUE SET <name> CFWD DISABLE ALL-CALLS

Description This command enables/disables the call forwarding on all calls supplementary service. When enabled, an incoming call is automatically redirected to the forwarded number the user as specified via the phone dialpad.

To enable the service the user has to enter a special code, the on-prefix code, to inform the intelligent Multiservice Gateway that the remaining digits constitute the forwarded numer. The selection of the forwarded number terminates as soon the user enter the on-suffix code.

To temporary disable the service, the user has to enter a special code, the off-prefix code.

Note: The call-forwarding service is available only if the active voip protocol is SIP.

To display the current call forwarding settings enter the VOIP EP ANALOGUE SHOW CFWD command.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
on-prefix	The digits to dial before entering the forwarded number.	N/A
on-suffix	The digit (one digit only) to enter after the forwarded number has been entered via phone dialpad.	N/A
off-prefix	The digits to enter after via phone dialpad to temporary disable the service.	N/A

Example --> voip ep analogue set tel1 cfwd enable all-calls on-prefix *21* on-suffix # off-prefix #21#

--> voip ep analogue set tel1 cfwd disable all-calls

6.3.3.1.13 VOIP EP SET CFWD ON-BUSY

Syntax

```
VOIP EP ANALOGUE SET <name> CFWD ENABLE ON-BUSY ON-PREFIX
<on-prefix> ON-SUFFIX <on-suffix> OFF-PREFIX <off-prefix>
VOIP EP ANALOGUE SET <name> CFWD DISABLE ON-BUSY
```

Description This command enables/disables the call forwarding on busy supplementary service. When enabled, an incoming call is automatically redirected to the forwarded number if the called user is busy.

To enable the service the user has to enter a special code, the on-prefix code, to inform the intelligent Multiservice Gateway that the remaining digits constitute the forwarded number. The selection of the forwarded number terminates as soon the user enter the on-suffix code.

To temporary disable the service, the user has to enter a special code, the off-prefix code.

Note: The call-forwarding service is available only if the active VoIP protocol is SIP.

To display the current call forwarding settings enter the VOIP EP ANALOGUE SHOW CFWD command.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
on-prefix	The digits to dial before entering the forwarded number.	N/A
on-suffix	The digit (one digit only) to enter after the forwarded number has been entered via phone dialpad.	N/A
off-prefix	The digits to enter after via phone dialpad to temporary disable the service.	N/A

Example --> voip ep analogue set tel1 cfwd enable on-busy on-prefix *22* on-suffix # off-prefix #22#

--> voip ep analogue set tel1 cfwd disable on-busy

6.3.3.1.14 VOIP EP SET CFWD ON-NO-ANSWER

Syntax

```
VOIP EP ANALOGUE SET <name> CFWD ENABLE ON-NO-ANSWER ON-PRE-
FIX <on-prefix> ON-SUFFIX <on-suffix> OFF-PREFIX <off-pre-
fix>
VOIP EP ANALOGUE SET <name> CFWD DISABLE ON-NO-ANSWER
VOIP EP ANALOGUE SET <name> CFWD ON-NO-ANSWER TIMEOUT <TIME-
OUT>
```

Description This command enables/disables the call forwarding on no-answer supplementary service. When enabled, an incoming call is automatically redirected to the forwarded number if the called user doesn't answer with the timeout value.

To enable the service the user has to enter a special code, the on-prefix code, to inform the intelligent Multiservice Gateway that the remaining digits constitute the forwarded number. The selection of the forwarded number terminates as soon the user enter the on-suffix code.

To temporary disable the service, the user has to enter a special code, the off-prefix code.

Note: The call-farwarding service is available only if the active voip protocol is SIP.

To display the current call forwarding settings enter the VOIP EP ANALOGUE SHOW CFWD command.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
on-prefix	The digits to dial before entering the forwarded number.	N/A
on-suffix	The digit (one digit only) to enter after the forwarded number has been entered via phone dialpad.	N/A
off-prefix	The digits to enter after via phone dialpad to temporary disable the service.	N/A
timeout	The timeout in seconds the CPE waits for user answer before routing the incoming call to the forwarded number. Setting the timeout to the zero, reset the value to the default (30secs).	0

Example --> voip ep analogue set tel1 cfwd enable on-no-answer on-prefix *23* on-suffix # off-prefix #23#

--> voip ep an set tel1 cfwd on-no-answer timeout 10

--> voip ep analogue set tel1 cfwd disable on-no-answer

6.3.3.1.15 VOIP EP SET CFWD-EXT

Syntax

```
VOIP EP ANALOGUE SET <name> CFWD-EXT ENABLE ACTIVATE-PREFIX <digit-map> | DEACTIVATE-PREFIX <digit-map> | REACTIVATE-PREFIX <digit-map>
VOIP EP ANALOGUE SET <name> CFWD-EXT DISABLE
```

Description This command enables/disabled the call-forwarding feature managed by an external server and sets the prefixes used by the server. The feature is available only on SIP protocol and must be supported by the SIP server.

The command comes with three optional prefix settings:

Activate-prefix is the prefix used to activate the call forwarding. When the user dials this prefix iMG plays the “stutter dial”, the user must then dial the number to which calls are to be forwarded. When the dialing is finished iMG sends and INVITE containing the activate-prefix and the new number to inform the server that successive calls must be forwarded to this new number. The forwarding policy (call forward on busy, call forward on no answer, etc.) is provisioned on the server.

Deactivate-prefix is the prefix used to activate the call forwarding. When it is dialed, iMG sends an INVITE containing this prefix to inform the server that the call forwarding feature has been disabled. The server must keep stored the number where the calls must be forwarded configured with the activate-prefix.

Reactivate-prefix is the prefix used to reactivate the call forwarding feature. When it is dialed, iMG sends and INVITE containing this prefix to inform the server that the call forwarding feature has been enabled using the same previously provisioned forward number. The server must forwards the calls to the number previously configured with the activate-prefix. The forwarding policy (call forward on busy, call forward on no answer, etc.) is provisioned on the server.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	Identifies an analogue endpoint name previously created with the command "voip ep analogue create".	
digit-map	is the expression string in use to recognize the feature. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-'. The service is disabled by default.	

Example --> voip ep analogue set tel1 enable activate-prefix *71 deactivate-prefix *72 reactivate-prefix *73

6.3.3.1.16 VOIP EP SET CLIP

Syntax

```
VOIP EP ANALOGUE SET <name> CLIP {NONE | BELL | ETSI | NTT | DTMFTDK
}
VOIP EP ANALOGUE SET <name> CLIP ETSI [DTMF [DURING-RINGING |
PRIOR-TO-RINGING] | FSK [DURING-RINGING | PRIOR-TO-RINGING] ]
```

Description This command sets the type of caller ID that is generated during an incoming call.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing access port. To display access port names, use the VOIP EP ANALOG LIST command.	N/A

BELL	Generate a caller ID accordingly to BELL standard.	None
ETSI	Generate a caller ID accordingly to ETSI standard. The ETSI caller ID can be of two type: DTMF: the DTMF tones can be sent before the first ring (prior-to-ring) or after the first ring (during-ringing). FSK: the FSK signals can be sent before the first ring (prior-to-ring) or after the first ring (during-ringing). If not differently specified the default value is ETSI FSK during-ringing.	
NTT	Generate a caller ID accordingly to NTT standard.	
DTMFTDK	Generate a caller ID accordingly to Denmark DTMF standard. This setting is equal to ETSI DTMF DURING-RINGING. The value is maintained for backward compatibility.	
NONE	Do not generate any caller-id	

Example --> voip ep analogue set tel1 clip etsi

--> voip ep digital set tel clip on

See also
```
voip ep analogue create
voip ep analogue disable
voip ep analogue delete
voip ep analogue enable
voip ep analogue list
voip ep analogue show
```

6.3.3.1.17 VOIP EP SET CLIP-REDUCTION

Syntax
```
VOIP EP ANALOGUE SET <name> CLIP-REDUCTION {NONE | CC |
CC+AC}
VOIP EP ANALOGUE SET <name> CLIP-REDUCTION REPLACE <prefix-
digit> REPLACEMENT <digit>
```

Description This command sets the CLIP address prefix handling to be used on a previously defined endpoint. It allows the CLIP number to be manipulated by the gateway prior to being sent to the user handset, and is typically used to remove prefixed country-code information so the user handset can match the delivered CLIP number with it's internal phone book entries.

There are four possible options:

- NONE: No CLIP prefix reduction will be performed. This is the default setting.

- CC: The country code will be omitted from the CLIP address delivered to the handset.
- CC+AC: Both the country code and area code will be omitted from the CLIP address delivered to the handset.
- REPLACE: The specified prefix 'prefix-digit' will be replaced with 'digit'.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
prefix-digits	A digit string of 1 - 8 digits in length.	none
digit	A digit string of 1 - 8 digits in length.	none

Example --> voip ep analogue set prt1 clip-reduction replace 0064 replacement 0

See also `VOIP EP ANALOG SHOW`

6.3.3.1.18 VOIP EP SET CLIR

Syntax `VOIP EP ANALOGUE SET <name> CLIR { ON OFF-PREFIX <off-prefix> | OFF ON-PREFIX <on-prefix>}`

Description This command enables or disables the caller identifier restriction.

There are four different situations:

- CLIR ON: The Caller ID Restriction is always ON.
- CLIR OFF: The Caller ID Restriction is always OFF.
- CLIR ON OFF_PREFIX <off-prefix>: The Caller ID Restriction is always ON but it can be disabled for the next call dialing the off-prefix.
- CLIR OFF ON_PREFIX <on-prefix>: The Caller ID Restriction is always OFF but it can be enabled for the next call dialing the on-prefix.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing access port. To display access port names, use the voip ep list command.	N/A

on-prefix	The digitmap to be used to enable the caller identifier for the successive call.	N/A
off-prefix	The digitmap to be used to disable the caller identifier for the successive call.	N/A

Example --> voip ep analogue set prt0 clir on off-prefix *1

See also
```
voip ep analogue create
voip ep analogue disable
voip ep analogue delete
voip ep analogue enable
voip ep analogue list
voip ep analogue show
```

6.3.3.1.19 VOIP EP SET CNG

Syntax `VOIP EP ANALOGUE SET <name> CNG <status>`

Description This command enables or disables the comfort noise generation feature.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display access port names, use the VOIP EP ANALOGUE LIST command.	N/A
status	The status of the comfort noise generation feature. Valid values are: **Off**: CNG disabled **On**: CNG enabled	

Example --> voip ep analogue set prt0 cng off

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.20 VOIP EP SET CODECS

Syntax `VOIP EP ANALOGUE SET <name> CODECS <codec-list>`

Description This command sets the codec capability list for an existing access port.

Note: T.38 support must always be selected together with another speech codec (G711a/u or G726 or G729ab).

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display access port names, use the VOIP EP ANALOGUE LIST command.	N/A
codec-list	The value or a comma separated list of values defining the compression algorithm on codec. Valid values are: g711a: referring to G.711 a-law PCM g711u: referring to G.711 µ-law PCM g729ab: referring to G.729A/B 8 kbps ACELP A/B g726-16: referring to G.726 16 kbps g726-24: referring to G.726 24 kbps g726-32: referring to G.726 32 kbps g726-40: referring to G.726 40 kbps T38	N/A

Example --> voip ep analogue set prt0 codecs g711a,g711u,g729ab

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.21 VOIP EP SET CONFERENCE-SERVICE

Syntax `VOIP EP ANALOGUE SET <name> CONFERENCE-SERVICE <conf-type>`

Description This command sets conference-service feature. It is possible allow N-way conference or limit the feature to a 3-way conference. The feature is available only for the SIP protocol and requires the “SONUS” profile.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing access port. To display access port names, use the voip ep list command.	N/A
conf-type	Valid values are: • 3-way • N-way	3-way

Example --> voip ep analogue set prt0 conference-service N-way

See also
```
voip ep analogue create
voip ep analogue disable
voip ep analogue delete
voip ep analogue enable
voip ep analogue list
voip ep analogue show
```

6.3.3.1.22 VOIP EP SET COUNTRY

Syntax `VOIP EP ANALOGUE SET <name> COUNTRY <country>`

Description This command sets dial tone, busy tone and ring back tone frequencies and cadences on the physical port referred to by the named access port, appropriately for the selected country.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display access port names, use the VOIP EP ANALOGUE LIST command.	N/A

country	The national signalling system and defines the analogue signalling criteria in use. Valid values are: • australia • austria • belgium • canada • china • france • germany • irael • ialy • japan • newzealand • norway • russia • singapore • spain • sweden • turkey • uk • usa	N/A

Example --> voip ep analogue set prt0 country usa

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.23 VOIP EP SET DIALMASK

Syntax `VOIP EP ANALOGUE SET <name> DIALMASK <digit-number>`

Description This command sets the dial mask value (number of chars to be removed from the dialled number) on the physical port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
digit-number	The number of digits to be removed from the dialled number. Acceptable values are from 0 to 3.	

Example --> voip ep analogue set prt0 dialmask 2

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.24 VOIP EP SET DIALMODE

Syntax `VOIP EP ANALOGUE SET <name> DIALMODE {AUTO | DTMF | PULSE 10PPS|20PPS}`

Description This command sets the dial mode used by analogue ports. On the ***fxo*** port, if DIALMODE is set to AUTO, the iMG examines the type of signalling mode supported on the PSTN line and set the port signalling to the same mode automatically. On ***fxs*** ports, if DIALMODE is set to AUTO, the iMG uses the same signalling mode selected for ***fxo*** port.

If PULSE mode is selected, it's also necessary select the pulse rate: 10pps or 20pps.

Option	Description	Default Value
name	An existing access port. To display access port names, use the VOIP EP ANALOGUE LIST command.	N/A
country	The national signalling system and defines the analogue signalling criteria in use. Valid values are: • australia • austria • belgium • canada • china • france • germany • irael • ialy • japan • newzealand • norway • russia • singapore • spain • sweden • turkey • uk • usa	N/A

Example --> voip ep analogue set prt0 dialmode auto

See also

```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.25 VOIP EP SET DIGITMAP

Syntax `VOIP EP ANALOGUE SET <name> DIGITMAP <digit-map>`

Description This command sets the digit map rule on the physical port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
digit-map	The digit map expression. A Digit map may have up to 32 chars. The following symbols can be used: • **DTMF**: A digit from '0' to '9' or one of the symbols 'A', 'B', 'C', 'D'. Symbols '#' and '*', if needed, must be added separately. • **Timer**: The symbol 'T' • **Wildcard**: The symbol 'x' • **Range**: The symbols '[' and ']' • **Subrange**: The symbol '-' • **Position**: The symbol '.'	N/A

Example --> voip ep analogue set prt0 digitmap x.T

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.26 VOIP EP SET EMERGENCY-SERVICE-NUMBER

Syntax `VOIP EP ANALOGUE SET <name> EMERGENCY-SERVICE-NUMBER <digit-map>`

Description This command sets the rule used to understand when the dialed number is an emergency call. When a number matching the digit-map is dialed the invite with this number is

immediately sent and this call can not be interrupted by other incoming calls using the flash-hook key. The feature is available only on SIP protocol and must be supported by the SIP server.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	Identifies an analogue endpoint name previously created with the command "voip ep analogue create".	
digit-map	Is the expression string in use to know the end of dialling phase. Valid value is either the string is "none" or characters like digit and symbols '#', '*', '.', '|', '[', ']', '-'.	"none"

Example --> voip ep analogue set tel1 emergency-service-number 911

6.3.3.1.27 VOIP EP SET FAX-MODEM-DETECTION

Syntax `VOIP EP ANALOGUE SET <name> FAX-MODEM-DETECTION {ENABLE | DISABLE}`

Description Disables or enables detection modem and fax tones. This is enabled by default.

Option	Description	Default Value
name	A name that identifies an existing access port. To display the existing access port names, use the voip ep list command.	N/A

Example --> voip ep analogue set tel1 fax-modem-detection disable

See also `VOIP EP ANALOGUE SHOW`

6.3.3.1.28 VOIP EP SET FLASHHOOK-TIME

Syntax `VOIP EP ANALOGUE SET <name> FLASHHOOK-TIME <msec>`

Description This command set the flash-hook time on the port referred to by the named access port. Flash-hook time cannot be less then the on-hook time. Flash-hook event is detected by iMG when its length in msec is within a valid window. The lower limit of the window is msec/3. The higher limit of the window is the lesser of msec*2 and the on-hook time.

For example: If the on-hook time is 900 msec and flash-hook time is 600msec a valid flash-hook event must be higher than 200 msec and lower than 900 msec. If the on-hook time is 800 msec and flash-hook time is 300msec a valid flash-hook event must be higher than 100 msec and lower than 600 msec.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing access port. To display the existing access port names, use the voip ep list command.	N/A
msec	The flash-hook time in millisecond. Valid values are from 80 to 600msec. Flash-hook time can not be less then the on-hook time. Flash-hook validation window is the narrower between msec/3 and msec*2 or msec/3 and on-hook time.	N/A

Example --> voip ep analogue set prt0 flashhook-time 350

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.29 VOIP EP SET HOLD-LOCAL-TONE-SERVICE

Syntax `VOIP EP ANALOGUE SET <name> HOLD-LOCAL-TONE-SERVICE {ENABLED|DISABLED}`

VOIP EP DIGITAL SET <name> HOLD-LOCAL-TONE-SERVICE {ENABLED|DISABLED}

Description This command enables/disables a comfort tone generated when a user is put on hold. The generated tone has a proprietary frequency and cadence common for all countries.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing endpoint name.	-

Example --> voip ep analogue set tel1 hold-local-tone-service enabled

6.3.3.1.30 VOIP EP SET HOTLINE TIME-OUT

Syntax `voip ep analogue set <name> hotline time-out <sec>`

Description This command set the number of seconds between the off hook and the beginning of the digit collection when the feature is enabled.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing endpoint name.	-
sec	The number of seconds between the off-hook and the beginning of the digit collection Valid values are from 0 to 30.	2

Table 15 – voip ep set hotl-timeout command parameters

Example --> voip ep analogue set tel1 hotline time-out 4

--> voip ep digital set tel hotline time-out 4

6.3.3.1.31 VOIP EP SET HOTLINE DISABLE

Syntax `VOIP EP ANALOGUE SET <name> HOTLINE DISABLE`

Description This command disables the hotline feature on the selected analogue port.

Option	Description	Default Value
name	An existing endpoint name.	-

6.3.3.1.32 VOIP EP SET HOTLINE ENABLE

Syntax `VOIP EP ANALOGUE SET <name> HOTLINE ENABLE ACTI-PREFIX <act-prefix> DEACT-PREFIX <deact-prefix> REACT-PREFIX <react-prefix> [ADDRESS <address>]`

VOIP EP DIGITAL SET <name> HOTLINE ENABLE ACTI-PREFIX <act-prefix> ACT-ALL-PREFIX <act-all-prefix> DEACT-PREFIX <deact-prefix> REACT-PREFIX <react-prefix>

Description

This command enables the hotline feature. When enabled, as soon the user pick-up the phone, a call is made automatically to the forwarded number without requiring the user to dial the number on the phone keypad.

Act-prefix is the prefix must be dialed to enable the feature; upon receipt of the prefix, you hear the stutter-dial tone and the subsequent dialed digits will populate the provisioned hotline address. The hotline address MUST match the current digit-map to be confirmed. Upon confirmation, the device issues one sequence of stutter tone. On error condition, when the dialed digits do not match the current digit map, the device issues the reorder tone.

ACT-PREFIX acts only on the used endpoint. Each endpoint has its own configuration.

DEACT-PREFIX is the prefix must be dialed to disable the feature; previous hotline provisioned address is preserved. Upon confirmation, the device issues one sequence of stutter tone.

REACT-PREFIX is the prefix must be dialed to re-activate the feature. Upon confirmation, the device issues one sequence of stutter tone. If no hotline provisioned address has been previously defined, the device issues the reorder tone.

Options

The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Name	An existing endpoint name.	-
act-prefix	The prefix used to enable the hot line feature only on the endpoint where it is configured. It is a digit-map and is the expression string in use to recognize the prefix. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-', 1 to 10 characters long. It can be configured to none	none
act-all-prefix	The prefix used to enable the hot line feature on all the device's endpoint It is a digit-map and is the expression string in use to recognize the prefix. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-', 1 to 10 characters long. It can be configured to none	none

deact-prefix	The suffix used to disable the hot line feature. It is a digit-map and is the expression string in use to recognize the prefix. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-', 1 to 10 characters long	none
react-prefix	The prefix used to re-activate the hot line feature. It is a digit-map and is the expression string in use to recognize the prefix. Valid characters are digit and symbols '#', '*', '.', '|', '[', ']', '-', 1 to 10 characters long	none

Example --> voip ep analogue set tel1 hotline act-prefix *12 deact-prefix *73 react-prefix *72

--> voip ep digital set tel1 hotline act-prefix *12 deact-prefix *73 react-prefix *72

The user will dial *12 and, upon receipt the stutter dial tone, the hotline address. When the phone is off hooked, the user hears the stutter dial tone for an interval time defined by time-out and after time-out elapsing a call will be done towards the provisioned hotline address.

6.3.3.1.33 VOIP EP SET IDT-PARTIAL

Syntax `VOIP EP ANALOGUE SET <name> IDT-PARTIAL <secs>`

Description This command sets the Inter-digit time on the physical port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
secs	The time duration in seconds of the inter-digit time. Acceptable values are in the range 2 sec to 10sec.	N/A

Example --> voip ep analogue set prt0 idt-partial 10

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.34 VOIP EP SET INTERNAL-3-WAY-CALL

Syntax `VOIP EP ANALOGUE SET <name> INTERNAL-3-WAY-CALL {ENABLE | DISABLE}`

Description This command disables or enables internal 3-way calls. It is disabled by default.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A

Example --> voip ep analogue set prt0 internal-3-way-call enable

VOIP EP ANALOGUE SHOW
VOIP EP ANALOGUE LIST

6.3.3.1.35 VOIP EP SET JITTERDELAY

Syntax `VOIP EP ANALOGUE SET <name> JITTERDELAY <msecs>`

Description This command sets the jitter delay value on the port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
msecs	The delay in milliseconds that the jitter buffer waits before it transmits the data samples that are collected from the VoIP network.Valid values are from 0.16 to 0.32 msec:	N/A

Example --> voip ep analogue set prt0 jitterdelay 6

See also `VOIP EP ANALOGUE CREATE`
`VOIP EP ANALOGUE DISABLE`
`VOIP EP ANALOGUE DELETE`
`VOIP EP ANALOGUE ENABLE`

```
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.36 VOIP EP SET JITTERMODE

Syntax `VOIP EP ANALOGUE SET <name> JITTERMODE {ADAPTIVE | FIXED | SEQUENTIAL}`

Description This command sets the type of jitter buffering that will be used by the gateway.

The default mode is 'fixed'.

Note: Some gateway products support only fixed jitter buffering. Attempting to change the jitter buffer mode on these devices will result in a 'webserver: Not available Parameter' error.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A

Example --> voip ep analogue set prt0 jittermode adaptive

VOIP EP ANALOGUE SHOW

6.3.3.1.37 VOIP EP SET LEC

Syntax `VOIP EP ANALOGUE SET <name> LEC <msecs>`

Description This command sets the line echo cancellation length on the port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A

msecs	The length in milliseconds of the buffer used for echo cancellation. Valid values are 0, 8, 16, 32 msec depending on iMG family.	8 msec

Example --> voip ep analogue set prt0 lec 16

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.38 VOIP EP SET OFFHOOK-TIME

Syntax `VOIP EP ANALOGUE SET <name> OFFHOOK-TIME <msecs>`

Description This command set the off-hook time on the port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
msecs	The off-hook time in millisecond. Valid values are from 100 to 500msec.	N/A

Example --> voip ep analogue set prt0 offhook-time 350

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.39 VOIP EP SET ONHOOK-TIME

Syntax `VOIP EP ANALOGUE SET <name> ONHOOK-TIME <msecs>`

Description This command set the on-hook time on the port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
msecs	The on-hook time in milliseconds. Valid values are in the range 100 to 500msec.	N/A

Example --> voip ep analogue set prt0 onhook-time 250

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.40 VOIP EP SET RXGAIN

Syntax `VOIP EP ANALOGUE SET <name> RXGAIN <gain>`

Description This command sets the input gain (in the direction from iMG/VoIP network to phone/user) of the port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
gain	The value of rx gain in dB. Valid values are from –48dB to +28dB.	N/A

Example --> voip ep analogue set prt0 rxgain –3.0

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
```

```
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.41 VOIP EP SET STUTTER-DIAL-TONE

Syntax `VOIP EP ANALOGUE SET <name> STUTTER-DIAL-TONE {PERIODIC|SINGLE-REPETITION}`

Description This command sets the mode to play the stutter dial tone usually used to signal a waiting message is available. The tone can be played periodically or only once (single repetition).

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A

Example --> voip ep analogue set tel1 stutter-dial-tone periodic

6.3.3.1.42 VOIP EP SET SUPPLEMENTARY-SERVICE-PREFIX

Syntax `VOIP EP ANALOGUE SET <name> SUPPLEMENTARY-SERVICE-PREFIX <digit-map>`

Description This command sets a prefix used by iMG to switch the status of the supplementary services. When the user dials this prefix iMG plays the “stutter dial”, the user must dial a phone number. iMG sends an INVITE containing the prefix and dialed number. The server recognizes the prefix and used the dialed number to enable or disable some supplementary services. The effects on this INVITE on the server depend on the server provisioning. The feature is available only on SIP protocol and must be supported by the SIP server.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	Identifies the access port, 1 to 16 characters in length. Valid characters are any printable characters, except code 0x2E and 0x2F; digits cannot be used as first character and if the space character is present, the string must be quoted.	N/A
<digit-map>	is the expression string in use to know the end of dialling phase. Valid value is either the string is "none" or characters like digit and symbols '#', '*', '.', '|', '[', ']', '-'.	"none"

Example --> voip ep analogue set tel1 supplementary-service-prefix *222

6.3.3.1.43 VOIP EP SET TXGAIN

Syntax `VOIP EP ANALOGUE SET <name> TXGAIN <gain>`

Description This command sets the output gain (in the direction from phone/user to iMG/VoIP network) of the port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
gain	The value of rx gain in dB. Valid values are from –48dB to +28dB.	N/A

Example --> voip ep analogue set prt0 txgain –3.0

See also
```
VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SHOW
```

6.3.3.1.44 VOIP EP SET UNREGISTERED-TONE

Syntax `VOIP EP ANALOGUE SET <name> UNREGISTERED-TONE {ENABLE|DISABLE}`

Description This command enables/disables a tone generated when the user is not registered. By default, if the user is not registered and no FDB entries exist a reorder tone is generated. If the unregistered-tone is disabled, no tones are generated.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A

Example --> voip ep analogue set tel1 unregistered-tone disabled

6.3.3.1.45 VOIP EP SET VAD

Syntax `VOIP EP ANALOGUE SET <name> VAD <status>`

Description This command enables or disables the voice activity detection feature on the port referred to by the named access port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A
status	The status of the VAD feature. Valid values are: • **on** VAD enabled • **off** VAD disabled	N/A

Example --> voip ep analogue set prt0 vad off

See also
`VOIP EP ANALOGUE CREATE`
`VOIP EP ANALOGUE DISABLE`
`VOIP EP ANALOGUE DELETE`
`VOIP EP ANALOGUE ENABLE`
`VOIP EP ANALOGUE LIST`
`VOIP EP ANALOGUE SHOW`

6.3.3.1.46 VOIP EP SHOW

Syntax `VOIP EP ANALOGUE SHOW <name>`

Description This command displays the following information about a named access port:

- Physical Port
- Typology
- Operational status
- Comfort Noise Generation (CNG)
- Codec Capabilities
- Country
- Critical-digit time
- Inter-digit time
- Dialing Mode
- Digit map
- Dial mask
- Line Echo Cancellation
- Jitter Delay
- Voice Activity Detection (VAD)
- Off-hook time
- On-hook time
- Rx gain
- Tx gain
- Attached users

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A

Example --> voip ep analogue show prt0

```
--> voip ep analogue show tel1
```

```
Gateway access port: tel1
------------------------------------------------------------------------
   Physical port:                    ep1-1
   Typology:                         AL-FXS-DEL
   Operational status:               Activated
   Disconnect procedure:             immediate-release
   Suppl. service prefixes:
   Call on Hold service:             disabled
   Hold Local Tone service:          disabled
   Call Waiting service:             disabled
      active-prefix:
      deactive-prefix:
      deactivetion-on-prefix:
      reactivetion-on-prefix:
   Conference service:               unavailable
   Call forward (provided by external server):
     activation prefix:
     re-activation prefix:
     de-activation prefix:
   Blind Call Transfer:              disabled
     activation prefix:
   Attended Call Transfer:           disabled
     activation prefix:
   Internal 3-Way Call:              enabled
     activation prefix:              none
   CLI Presentation (CLIP):          none
   CLIP Reduction:                   none
     Digit prefix:                   none
     Replacement digit:              none
   CLI Restriction (CLIR):           OFF
     prefix disabling restriction:
     prefix enabling restriction:
   Comfort Noise Generation (CNG):   OFF
   Codec Capabilities:               G711U,G711A,T38
   Country:                          usa
   Stutter-dial Tone type:           single-repetition
   Un-Registered Tone:               enable
   Alerting time-out:                default
   Critical-digit time:
      min:                           0 msecs.
      max:                           16 secs.
   Inter-digit time:
      min:                           0 msecs.
```

```
      max:                          4 secs.
   Dialling mode:                   DTMF
   Digit map:                       x.T
   Dial mask:                       0
   Emergency service number:        none
   Line Echo Cancellation (LEC):    16
   Fax/Modem detection:             enabled
   Jitter Delay:                    60 msecs.
   Jitter Mode:                     fixed
   Voice Activity Detection (VAD):  ON
   Hotline:
      service state:                Not provisioned service
   Recognition time:
      Off-hook:                     250 msecs.
      On-hook:                      1000 msecs.
      Flash-hook:                   950 msecs.
   Rx gain:                         -6.0 dB.
   Tx gain:                         +0.0 dB.



   Prefix replacement:

   Custom Signaling Protocol items:

   Attached users:                  user1
-->
```

See also VOIP EP ANALOGUE CREATE
VOIP EP ANALOGUE DISABLE
VOIP EP ANALOGUE DELETE
VOIP EP ANALOGUE ENABLE
VOIP EP ANALOGUE LIST
VOIP EP ANALOGUE SET

6.3.3.1.47 VOIP EP SHOW CFWD

Syntax VOIP EP ANALOGUE SHOW <name> cfwd

Description This command displays the call forwarding rules defined for the specified port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An existing access port. To display the existing access port names, use the VOIP EP ANALOGUE LIST command.	N/A

Example --> voip ep analogue show prt0 cfwd

```
Gateway access port - Call Forwarding rules
-------------------------------------------------------------------
all-calls:
   active               false
   forwarding number
   on-prefix            *72
   on-suffix            #
   off-prefix           *73


on-busy:
   active               false
   forwarding number
   on-prefix            *222
   on-suffix            #
   off-prefix           *223


on-no-answer:
   active               false
   forwarding number
   on-prefix            *333
   on-suffix            #
   off-prefix           *334
   timeout              10 secs.
```

See also VOIP EP ANALOGUE SET CFWD

6.3.3.1.48 VOIP EP SIGNALING ADD

Syntax VOIP EP SIGNALING ADD <name> PORT <port>

Description This command adds a previously created custom signal to an existing endpoint.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing customized signalling created with the VOIP EP SIGNALING CREATE command. To display the existing access port names, use the voip ep list command.	N/A
port	A name that identifies an existing access port. To display the existing customized signalling use the voip ep SIGNALING list command.	N/A

Example --> voip ep signaling add myring port prt0

See also
```
voip ep SIGNALING CREATE
voip ep SIGNALING DELETE
voip ep SIGNALING LIST
voip ep SIGNALING REMOVE
voip ep SIGNALING SHOW
```

6.3.3.1.49 VOIP EP SIGNALING CREATE

Syntax
```
VOIP EP SIGNALING CREATE <name> TYPE <type> TIME-OUT <secs>
FREQUENCY <frequency> CADENCE <cadence>
```

Description This command creates a new entry in the custom signaling list. Each customized signal must have a different <name>. If the customized signaling already exists, an error message is raised.

The type of the signaling, the used frequency and the cadence must be provided. The setting of a time-out is optional and is available only for the ring type.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the customized signaling port. It can be made up of one or more letters, digit or a combination of letters and digits. To display the existing access port names, use the voip ep list command.	N/A

type	The class of the customized signalling. Valid values are: busy-tone dial-tone ring ringback-tone.	N/A
secs	Time interval expressed in seconds. Valid values are from 1 to 3600 seconds.	N/A
frequency	One or more (up to three) tones separated by a "/" char. Each tones can be composed by one of the following combination of frequency: f1 - Single frequency f1xf2 - f1 is modulated by f2 f1+f2 - f1 is a juxtaposition of f2 Only one frequency can be set on a signalling with a type set to ring. Values are in Hz.	N/A
cadence	A sequence of time intervals to specify if the signale must be present or not. Each time interval is prefixed by "+" or "-" indicating, respectively, the signal issue or a pause. Sub-sequences may by provisioned specifying the number of cycles followed by the cadence inside brackets. The item "continuous" is available for infinite repetition or time. Values are in seconds.	N/A

Example A customized dial tone with a single frequency of 440 Hz always present (with no pause).

```
--> voip ep signaling create create dial1 type dial-tone frequency
440 cadence +continuous
```

A customized dial tone with a modulated tone (240 Hz modulated by 450 Hz) with a cadence of +0.4 sec. on, 0.2 sec. off, 0.4 sec. on and 2..6 sec. off.

```
--> voip ep signaling create create dial2 type dial-tone frequency
240x450 cadence +0.4-0.2+0.4-2.6
```

A customized ringback tone with a sequence of three tones followed by a pause. The three tones are executed in order for 0.4 sec, 0.5 sec and 0.6 sec. The pause is 2.5 sec.

```
--> voip ep signaling create create rbt type ringback-tone frequency
225x325/424x525/320+480 cadence +0.4+0.5+0.6-2..5
```

A customized ring signal with a complext cadence. The ring is executed three times with a cadence of 0.5 sec. on and 0.5 sec. off followed by an infinite cadence of 1 sec on and 2 sec off. The timeout is set to 180 sec.

```
--> voip ep signaling create create myring type ring time-out 180 fre-
quency 25 cadence -3(+0.5-0.5)+continuous(+1.0-2.0)
```

See also

```
voip ep SIGNALING ADD
voip ep SIGNALING DELETE
voip ep SIGNALING LIST
voip ep SIGNALING REMOVE
voip ep SIGNALING SHOW
```

6.3.3.1.50 VOIP EP SIGNALING DELETE

Syntax `VOIP EP SIGNALING DELETE <name>`

Description This command deletes an entry in the customized signaling list.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing customized signalling created with the VOIP EP SIGNALING CREATE command. To display the existing access port names, use the voip ep list command.	N/A

Example --> voip ep signaling create delete dial1

See also

```
voip ep SIGNALING ADD
voip ep SIGNALING CREATE
voip ep SIGNALING LIST
voip ep SIGNALING REMOVE
voip ep SIGNALING SHOW
```

6.3.3.1.51 VOIP EP SIGNALING LIST

Syntax `VOIP EP SIGNALING LIST`

Description This command lists all the entries in the customized signaling list defined in the system using the VOIP EP SIGNALING CREATE command.

The following information is displayed:

- signaling entry ID value
- signaling entry name
- signaling entry type

Example --> voip ep signaling list

```
Custom Signaling Protocol items:
 ID  |    Name    |                        Type
-----|------------|---------------------------------------
   1 | mydial     | dial-tone
   2 | mybusy     | busy-tone
   3 | myring     | cai
-----|------------|---------------------------------------
```

See also VOIP EP SIGNALING ADD
VOIP EP SIGNALING CREATE
VOIP EP SIGNAaLING DELETE
VOIP EP SIGNAaLING REMOVE
VOIP EP SIGNALING SHOW

6.3.3.1.52 VOIP EP SIGNALING REMOVE

Syntax VOIP EP SIGNALING REMOVE <name> PORT <port>

Description This command removes a previously added customized signaling from an existing endpoint.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing customized signalling created with the VOIP EP SIGNALING CREATE command. To display the existing access port names, use the voip ep list command.	N/A
port	A name that identifies an existing access port. To display the existing customized signalling use the voip ep SINALING list command.	N/A

Example --> voip ep signaling remove myring port prt0

See also voip ep SIGNALING ADD
voip ep SIGNALING CREATE

```
voip ep SIGNALING DELETE
voip ep SIGNALING LIST
voip ep SIGNALING SHOW
```

6.3.3.1.53 VOIP EP SIGNALING SHOW

Syntax `VOIP EP SIGNALING SHOW <name>`

Description This command shows a previously created customized signaling.

The following information is displayed:

- signaling entry type
- signaling entry time out
- signaling entry frequency
- signaling entry cadence
- signaling entry attached endpoints

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing customized signalling created with the VOIP EP SIGNALING CREATE command. To display the existing access port names, use the voip ep list command.	N/A

Example --> voip ep signaling show mydial

```
Custom Signaling Protocol item: mydial
------------------------------------------------------------
   Type:             dial-tone
   Time-Out:
   Frequency:        240x340/425x525/340+480 Hz.
   Cadence:          -3(+0.5-0.5)+continuous(+1-1)
   Attached ports:   tel1
```

See also

```
voip ep SIGNALING ADD
voip ep SIGNALING CREATE
voip ep SIGNALING DELETE
```

```
voip ep SIGNALING LIST
voip ep SIGNALING REMOVE
```

6.4 Common VoIP attributes: QoS, Media and DTMF-Relay

The following section details voip attributes that are typically used to handle voice quality and that are common for both the two main VoIP protocols (SIP and MGCP).

In some specific cases some commands are effective only when a specific voip protocol is selected (see the comand details).

All the following commands can be entered only after the voip protocol has been enabled.

6.4.1 QoS

iMG/RG/iBG devices allow to specify a specific DSCP/TOS priority value to the originated VoIP traffic.

DSCP and TOS are mutually exclusive because they refers to the same IP Header field using only a different number of bits (3 bits in case of TOS, 6 bits in case of DSCP) and assigning different packet classification accordingly to the TOS or DSCP value.

The command VOIP QOS SET DSCP is used to set the DSCP value while the VOIP QOS SET TOS command is used to set the TOS value. The two commands are mutually exclusive: only DSCP or TOS can be configured.

Attempting to configure the TOS attributes after having configured the DSCP attributes (or viceversa) will result in a conflict failure. It's necessary reset the DSCP attributes (or TOS) befor setting the TOS attributes (or DSCP).

It's possible differentiate DSCP/TOS values for VoIP signalling packets from the DSCP/TOS values for the media streams.

The command voip qos set dscp/tos signaling-protocol specify the DSCP/TOS values only for VoIP signaling packets originated by iMG/RG/iBG devices.

The command voip qos set dscp/tos media-protocol specify the DSCP/TOS values only for VoIP media packets originated by iMG/RG/iBG devices.

If signalling-protocol or media-protocol is not specified, the DSCP/TOS values are set to the same value for both signaling and media packets.

6.4.2 Media

iMG/RG/iBG devices allow to specify a specific pool of IP UDP ports to be used for media (RTP) transport.

Each even media port is paired with the subsequent odd portand assigned to RTP or RTCP streams respectively.

Then maximum number of simultaneously streams is therefore half of the size of the media range.

When VoIP MGCP protocol is used, the lowest ports pair is assigned to the first configured end-point, the subsequent pair is assigned to the second configured end-point and so on.

When SIP protocol is used, ports pair are used in a round robin fashion.

iMG/RG/iBG devices allow to specify a specific the RTP packetization time as timeframe between to consecutive RTP packets.

Packetization time could be negotiated at runtime during the call establishment phase.

The value specified via CLI is the value that is normally advertized by the VoIP protocol (via VoIP signalling messages) and that it's used when is not negotiated during the call setup.

6.4.2.1 Media Timeout

Only when VoIP SIPprotocol is used, it's also possible set iMG/RG/iBG devices to detect if an incoming RTP flow is still present or not (e.g. the other end-point was abruptly disconnected or network has critical problems) forcing the call release if no RTP packet flow has been detected for the current call for a time longer than the specified observation period.

6.4.3 DTMF-RELAY

iMG/RG/iBG devices support DTMF relay for the transmission of DTMF dialpad tones.

DTMF tones can be transmitted in-band through the RTP media stream as normal voice or can be transmitted via RTP stream accordingly to RFC2833 or can even being transmitted via VoIP specific messages.

Using DTMF in-band transmission is reliable only when the media stream uses uncompressed codec like G.711u or G.711a. When compressed codecs like G.729 or G.726 are used, the distortion produced by the codec compression algorithm does not allow a clear transmission of the DTMF tones that could be not intelligible on the far end.

In this case iMG/RG/iBG devices allow to use RFC2833 Telephone events or SIP NOTIFY or MGCP NTFY messages for DTMF transmission.

In case of SIP protocol, it's possible force the system to automatically select the proper DTMF relay mode depending on the negotiated codec.

In case of MGCP protocol, because call properties are controlled by the call agent, the selection of the proper DTMF relay mode is demanded to the call agent logic.

6.4.4 Functional Differences for Common VoIP attributes in Product Categories

The table below is intended to identify what is common amongst the product families - as well as where there are differences - to highlight those differences. To determine which family your device belongs to - please refer to the preface.

TABLE 6-15 Functional Mapping for Common VoIP attributes

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP QOS CLI COMMANDS	X	X	X	X	X	X	X	X	X
VOIP MEDIA CLI COMMANDS	X	X	X	X	X	X	X	X	X
VOIP DTMF-RELAY CLI COMMANDS	X	X	X	X	X	X	X	X	X

6.4.5 VOIP QOS command reference

This section describes the commands available on iMG/RG/iBG to configure and manage the VoIP QoS attributes.

6.4.5.1 VoIP QoS CLI commands

The table below lists the ***voip qos*** commands provided by the CLI:

TABLE 6-16 ***VoIP QoS*** commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP QOS SET DSCP	X	X	X	X	X	X	X	X	X
VOIP QOS SET DSCP SIGNALING-PROTOCOL	X	X	X	X	X	X	X	X	X
VOIP QOS SET DSCP MEDIA-PROTOCOL	X	X	X	X	X	X	X	X	X
VOIP QOS SET TOS	X	X	X	X	X	X	X	X	X
VOIP QOS SET TOS SIGNALING-PROTOCOL	X	X	X	X	X	X	X	X	X
VOIP QOS SET TOS MEDIA-PROTOCOL	X	X	X	X	X	X	X	X	X
VOIP QOS SHOW	X	X	X	X	X	X	X	X	X

6.4.5.1.1 VOIP QOS SET DSCP

Syntax `VOIP QOS SET {DSCP <dscp-code> | NONE}`

Description This command sets the value of the *dsc*p field in the IP header for both VoIP signaling and media (RTP) originated packets.

Note: To disable DSCP support (i.e. remove any previous configuration performed on DSCP field on signalling and speech packets) use the VOIP QOS SET NONE command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
dscp-code	The value of ***dscp*** field. Acceptable value are from 0 to 63	none

Example --> voip qos set dscp 24

See also `VOIP QOS SHOW`

6.4.5.1.2 VOIP QOS SET DSCP SIGNALING-PROTOCOL

Syntax `VOIP QOS SET {DSCP <dscp-code> | NONE} SIGNALING-PROTOCOL`

Description This command sets the value of the *dsc*p field in the IP header only for VoIP signaling originated packets.

Note: To disable DSCP support (i.e. remove any previous configuration performed on DSCP field on signalling and speech packets) use the VOIP QOS SET NONE SIGNALING-PROTOCOL command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
dscp-code	The value of ***dscp*** field. Acceptable value are from 0 to 63	none

Example --> voip qos set dscp 34 signaling-protocol

See also `VOIP QOS SET DSCP`
`VOIP QOS SHOW`

6.4.5.1.3 VOIP QOS SET DSCP MEDIA-PROTOCOL

Syntax `VOIP QOS SET {DSCP <dscp-code> | NONE} MEDIA-PROTOCOL`

Description This command sets the value of the *dscp* field in the IP header only for VoIP media (RTP) originated packets.

Note: To disable DSCP support (i.e. remove any previous configuration performed on DSCP field on signalling and speech packets) use the VOIP QOS SET NONE MEDIA-PROTOCOL command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
dscp-code	The value of *dscp* field. Acceptable value are from 0 to 63	none

Example --> voip qos set dscp 63 media-protocol

See also `VOIP QOS SET DSCP`
`VOIP QOS SHOW`

6.4.5.1.4 VOIP QOS SET TOS

Syntax `VOIP QOS SET {TOS <tos-code> | NONE}`

Description This command sets the value of the ***tos*** field in the IP header for both VoIP signaling and media (RTP) originated packets.

Note: To disable TOS support (i.e. remove any previous configuration performed on TOS field on signalling and speech packets) use the VOIP QOS SET NONE command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
tos-code	The value of ***tos*** field. Acceptable value are in the range 0 to 7	none

Example --> voip qos set tos 4

See also `VOIP QOS SHOW`

6.4.5.1.5 VOIP QOS SET TOS SIGNALING-PROTOCOL

Syntax `VOIP QOS SET {TOS <tos-code> | NONE} SIGNALING-PROTOCOL`

Description This command sets the value of the ***tos*** field in the IP header only for VoIP signaling originated packets.

Note: To disable TOS support (i.e. remove any previous configuration performed on TOS field on signalling and speech packets) use the VOIP QOS SET NONE SIGNALING-PROTOCOL command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
tos-code	The value of ***tos*** field. Acceptable value are in the range 0 to 7	none

Example --> voip qos set tos 4 signaling-protocol

See also `VOIP QOS SET TOS`
`VOIP QOS SHOW`

6.4.5.1.6 VOIP QOS SET TOS MEDIA-PROTOCOL

Syntax `VOIP QOS SET {TOS <tos-code> | NONE} MEDIA-PROTOCOL`

Description This command sets the value of the ***tos*** field in the IP header only for VoIP media (RTP) originated packets.

Note: To disable TOS support (i.e. remove any previous configuration performed on TOS field on signalling and speech packets) use the VOIP QOS SET NONE MEDIA-PROTOCOL command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
tos-code	The value of ***tos*** field. Acceptable value are in the range 0 to 7	none

Example --> voip qos set tos 7 media-protocol

See also `VOIP QOS SET TOS`
`VOIP QOS SHOW`

6.4.5.1.7 VOIP QOS SHOW

Syntax `VOIP QOS SHOW`

Description This command shows the value of DSCP or TOS fields used in the IP header of RTP voice packets.

Example --> voip qos show

```
Gateway Quality of Service:
-----------------------------------------------------------------
   QoS media:                          63 (DSCP)
   Qos signaling:                      34 (DSCP)
```

Example --> voip qos show

```
Gateway Quality of Service:
-----------------------------------------------------------------
   QoS media:                           7 (TOS)
   Qos signaling:                       4 (TOS)
```

6.4.6 VoIP Media command reference

This section describes the commands available on iMG/RG/iBG to configure and manage the VoIP Media attributes.

6.4.6.1 VoIP Media CLI commands

The table below lists the ***VOIP Media*** commands provided by the CLI:

TABLE 6-17 ***VoIP Media*** commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP MEDIA SET PACKETLENGTH	X	X	X	X	X	X	X	X	X
VOIP MEDIA SET PORTRANGE	X	X	X	X	X	X	X	X	X
VOIP MEDIA SET RTCP	X	X	X	X	X	X	X	X	X
VOIP MEDIA SET SESSIONTIMEOUT	X	X	X	X	X	X	X	X	X
VOIP MEDIA SHOW	X	X	X	X	X	X	X	X	X

6.4.6.1.1 VOIP MEDIA SET PACKETLENGTH

Syntax `VOIP MEDIA SET PACKETLENGTH <packet-length>`

Description This command set the size of each local generated voice RTP packets. The packetlength specifies the voice time period that is carried by each voice RTP packet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
packet-length	The length (in msecs) of voice period carried by each RTP packet. Allowed values are from 10 to 100msec.	20

Example --> voip media set packetlength 10

6.4.6.1.2 VOIP MEDIA SET PORTRANGE

Syntax `VOIP MEDIA SET PORTRANGE {ANY | <ipport/n-ports>}`

Description This command sets the port pool available for media transport. Ports are dynamically allocated in pairs to support new connections; the odd-numbered port is reserved for RTCP. If the port pool is sold out, new sessions will be refused for lack of available resource.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
ANY	any sets the default port range	
ipport	ipport is theUDP/TCP port number being set. The range is 1026 to 65534. The value specified must be an even number	50600
n-ports	n-ports are the number of ports. The range is 2 to 32; The value specified has to be an even number.	32

Example --> voip media set portrange 50500/12

See also `VOIP MEDIA SET RTCP`

6.4.6.1.3 VOIP MEDIA SET RTCP

Syntax `VOIP MEDIA SET RTCP {OFF | ON}`

Description This command enables RTCP.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
OFF	Turn off the RTCP support.	off
ON	Enable the RTCP support.	

Example --> voip media set rtcp on

See also `VOIP MEDIA SET DSCP`

6.4.6.1.4 VOIP MEDIA SET SESSIONTIMEOUT

Syntax `VOIP MEDIA SET SESSIONTIMEOUT <mins>`

Description This command sets the maximum timeout interval used to detect a fail in the incoming RTP speech packets. If no RTP packet is received on the UDP port used by the active call for a time longer than the SESSIONTIMEOUT value, the other endpoint is considered disconnected and the active call is released.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
mins	The SESSIONTIMEOUT value expressed in minutes. Available values are form 0 mins to 1440 mins (24 hours).0 mins is equivalent to disable the SessionTimeOut feature.	0

Example --> voip media set sessiontimeout 1

See also `VOIP MEDIA SHOW`

6.4.6.1.5 VOIP MEDIA SHOW

Syntax `VOIP MEDIA SHOW`

Description This command shows the media values defined by the VOIP MEDIA SET commands.

Example --> voip media show

```
Gateway Media:
------------------------------------------------------
   Port range:                      50600/32
   Packet length:                   10 msecs.
   RTCP enable:                     off
   RTP session time-out:            0 mins.
```

See also VOIP MEDIA SET PORTRANGE
VOIP MEDIA SET RTCP
VOIP MEDIA SET SESSIONTIMEOUT

6.4.7 VoIP DTMF-RELAY command reference

This section describes the commands available on to configure and manage the VoIP DTMF-RELAY attributes.

6.4.7.1 VoIP DTMF-RELAY CLI commands

The table below lists the ***VOIP DTMF*** commands provided by the CLI:

TABLE 6-18 Commands for VoIP DTMF

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
VOIP DTMF-RELAY SET MODE	X	X	X	X	X	X	X	X	X
VOIP DTMF-RELAY SET TELEPHONE-EVENT-FINAL-PACKETS	X	X	X	X	X	X	X	X	X
VOIP DTMF-RELAY SET TELEPHONE-EVENT-TIME	X	X	X	X	X	X	X	X	X
VOIP DTMF-RELAY SET TELEPHONE-EVENT-PAYLOADTYPE	X	X	X	X	X	X	X	X	X
VOIP DTMF-RELAY SHOW	X	X	X	X	X	X	X	X	X

6.4.7.1.1 VOIP DTMF-RELAY SET MODE

Syntax VOIP DTMF-RELAY SET MODE <mode>

Description This command sets the value of the ***DTMF-RELAY mode*** used to decide if to send DTMF tones in band or out of band. Note the protocol used to send the DTMF tones out-of-band can be configured on the used signalling protocol (SIP).

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
mode	DTMF-Relay mode can be set with the following values: **auto**: DTMF tones are transported in band when the call is set up with g711u (PCMU), g711A (PCMA), g726-32 and g726-40. Out of band in all the other cases. **none**: DTMF tones are transported always in band. **auto-of-band**: DTMF tones are transported always out of band.	auto

Example --> voip dtmf-relay set mode out-of-band

See also `VOIP DTMF-RELAY SHOW`

6.4.7.1.2 VOIP DTMF-RELAY SET TELEPHONE-EVENT-FINAL-PACKETS

Syntax `VOIP DTMF-RELAY SET TELEPHONE-EVENT-FINAL-PACKETS <number>`

Description This command sets the number of final packets must be sent when DTMF tones are sent out-of-band using telephone event (RFC2833). For redundancy reasons the user can decide to send the final packet more than one time.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
number	The number of telephone event final packet. Acceptable values are from 1 to 3.	1

Example --> voip dtmf-relay set telephone-event-final-packet 3

See also `VOIP DTMF-RELAY SHOW`

6.4.7.1.3 VOIP DTMF-RELAY SET TELEPHONE-EVENT-TIME

Syntax `VOIP DTMF-RELAY SET TELEPHONE-EVENT-TIME <msecs>`

Description This command sets the number of milliseconds that a tone is locally played when a telephone event rtp message is received.

The value rfc2833 is shown when telephone-event time is set 0 for communicating that the duration is managed in the standard way as described in rfc2833.

Description ***Options*** The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
msecs	The number of milliseconds that the tome is played when receiving a telephone event message	0

Example --> voip dtmf-relay set telephone-event-time 100

See also `VOIP DTMF-RELAY SHOW`

See also `VOIP DTMF-RELAY SHOW`

6.4.7.1.4 VOIP DTMF-RELAY SET TELEPHONE-EVENT-PAYLOADTYPE

Syntax `VOIP DTMF-RELAY SET TELEPHONE-PAYLOADTYPE <number>`

Description This command sets the payload type advertized by iMG/RG/iBG during the call setup when telephone-event support has been enabled.

Note: This command works only when VoIP SIP protocol is selected.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
number	The payload type used inside the telephone-event RTP message to notify DTMF tones.	default

Example --> voip dtmf-relay set telephone-event-payloadtype 101

See also `VOIP DTMF-RELAY SHOW`

6.4.7.1.5 VOIP DTMF-RELAY SHOW

Syntax `VOIP DTMF-RELAY SHOW`

Description This command shows the DTMF-Releay setting.

Example --> voip dtmf-relay show

```
Gateway DTMF-Relay:
-------------------------------------------------------
   Mode:                            out-of-band
   Telephone-event final packets:   2
   Telephone-event time:            rfc2833
   Telephone-event Payload Type:    default
```

7. Quality of Service

7.1 QOS

7.1.1 Introduction

The Quality of Service (QoS) support within gateway units allows different classes of traffic, such as specific applications or users of a network, to be offered different levels of service. The key features offered are:

- Quality of service for traffic managed by the ADSL module.
- Quality of service for local applications such as Voice over IP (VoIP) traffic.
- Architecture compatible with *RFC 2475 An Architecture for Differentiated Services* and *RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

7.1.2 QoS architecture overview

The basic building blocks of *DIFFSERV* functionality are various traffic conditioning functions, such as:

- Classification
- Policing
- Marking
- Shaping

The gateway provide a set of software tools that implement these traffic-conditioning functions. Hence, these tools can configure *DIFFSERV* or any other QoS behaviour. These software tools are:

- The Classifier; it classifies incoming packets to ensure that important packets are marked as high priority. It will also communicate the scheduling priority and drop priority to the Scheduler and communicate the meter-id to the Meter
- The Meter; it measures the temporal properties of the incoming stream against configured parameters and communicates the drop priority to the Scheduler.
- The Scheduler; it is used for scheduling packets for transmission on an outgoing interface based on information received from the Meter and the Classifier. It can be configured to provide Priority Scheduling or WF2Q+ Scheduling behavior.

Priority Scheduling is used to send out one class of packets with absolute priority over other classes. *WF2Q+ Scheduling* is used to provide a fair sharing of a single outgoing link between multiple classes (*Assured forwarding*) or to send out one class of packets with priority over other classes while ensuring that lower priority traffic is not completely starved (*Expedited Forwarding*).

Taking into account the QoS related software tools described above, a more detailed view of the gateway architecture is shown below.

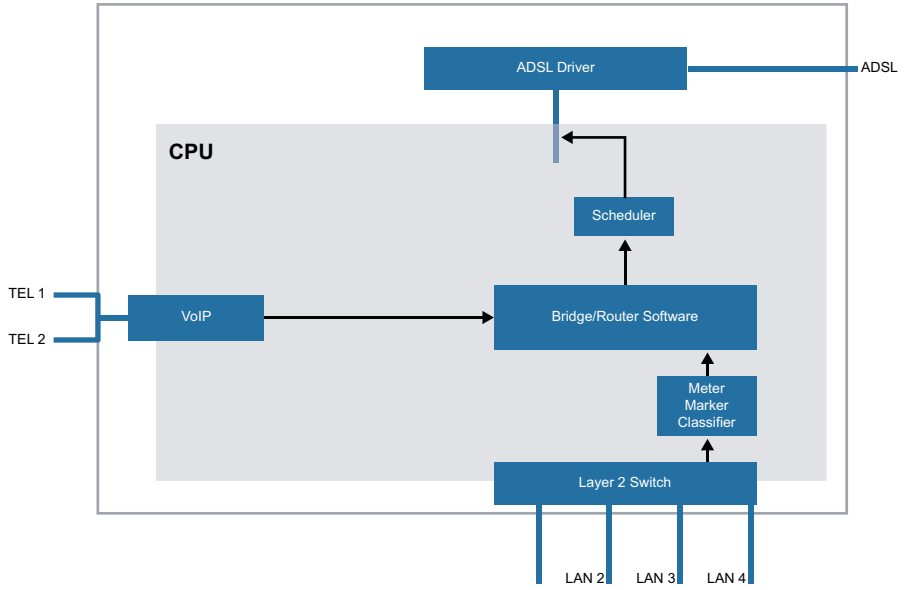


FIGURE 7-1 Gateway Architecture

Note: Note that QoS support is available only for the upstream direction, i.e. in for Ethernet packets that coming from internal hosts (connected to the Layer2 switch VLANs) need to be routed or bridged to the ADSL port.

Note: If two-level priority scheduling is required per ATM VC then ATM packet prioritization provides a lower latency alternative to the Scheduler.

Note: If more than two levels of priority scheduling (or WF2Q+ scheduling) is required then the Scheduler should be used instead of ATM Packet prioritization.

7.1.3 QoS implementation for DIFFSERV

7.1.3.1 The Classifier

When packet classification is enabled on a transport (only the Ethernet transport named *default*) every incoming packet is examined by the Classifier. The Classifier never examines outgoing packets.

The Classifier examines incoming packets and assigns a traffic class to them based on user-configured rules that are stored in a profile. These rules can depend on various IP header fields, or can simply be a function of which interface the packet arrived on.

Without the packet classifier, every packet arriving on any interface would be treated with the same priority. The same profile can be added to more than one transport, so that the same set of rules are used by multiple transports.

Each rule can test any of the following fields in the packet:

- IP header DIFFSERV Codepoint (DSCP).
- Source and/or destination IP address.
- IP protocol (incorporating TCP/UDP/ICMP/GRE protocols).
- For TCP and UDP packets, the source and/or destination port number.

This means that the Classifier device can be used in two ways (see *RFC 2475)*:

- Multi-field (MF) Classifier
- Behavior Aggregate (BA) Classifier

When used as a *Multi-Field (MF)* classifier, the Classifier device examines a combination of fields in the IP header and payload, and, if configured to do so, may also act as a Marker to set the DS field of the IP header.

When used as a *Behaviour Aggregate (BA)* classifier, the Classifier device examines the DSCP value written into the DS field of the IP header by the Ingress node of the DiffServ network.

7.1.3.2 Classifying packets

An incoming packet is tested against each rule in order of configuration. If all of the tests on the packet succeed, the rule is 'matched' and the packet is assigned the traffic class, or Quality of Service Class (QoSC) associated with that rule. The QoSC value in the packet comprises three fields and Classifier rules can be configured to set these fields independently. The three fields that can be set for each packet are:

- *Scheduling Priority.* This value is used by the Scheduler, the Monitored Pools, the Priority Queue, to identify different priority streams and to provide appropriate scheduling behavior. The Classifier device sets configured scheduling priority for a traffic stream matching a classification rule. Multiple traffic streams may map to the same scheduling priority. At present, 8 levels (values 0 to 7) of scheduling priority are defined. The value 7 is the highest priority and 0 is the lowest priority.
- *Meter Id.* A number of meter instances can be configured on a Meter device channel. Each meter instance measures the temporal properties of a single traffic stream and is identified by a unique meter-id (number) on a channel. The Classifier device sets the configured meter-id for a traffic stream matching a classification rule. Note that there is no correlation between scheduling priority and meter-id. Different traffic streams may be configured with different meter-ids but still have the same scheduling priority.
- *Drop Priority.* The drop priority can take three values: 0, 1 or 2. The values are described below:
  - 0 lowest drop priority (green),
  - 1 medium drop priority (yellow)
  - 2 highest drop priority (red).

The Drop priority is used by the Algorithmic dropper component of the Schedule, which when configured drops packets selectively during a congestion condition in Scheduler queues. The packets with a higher drop priority have a higher probability of getting dropped than lower priority packets.

The Classifier initially sets the drop priority, and then the drop priority may optionally be modified by the Meter device if the packet is out of profile. The Meter will then communicate the drop priority to the Scheduler device.

Both the Classifier and Meter devices can set the drop priority. The Classifier device sets the drop priority configured in the classification rule while the Meter device sets the drop priority depending upon the metering result.

Note: If both the Classifier and the Meter are configured, then the Meter overwrites the drop priority value that the Classifier has set.

7.1.3.2.1 Configuring the Classifier

This section explains the basic steps to follow in order to configure the Classifier. It *does not* include details about the function of each command. See the section at the end of the currect section for a detailed description of each classifier command. To configure the Classifier, use the following CLI commands:

1. Create a profile using the command `CLASSIFIER ADD PROFILE`.
2. Add one or more rules to the profile using the command `CLASSIFIER PROFILE ADD RULE`
3. Configure the rule, using one the following commands:

```
CLASSIFIER PROFILE SET RULE DROPPRIO
CLASSIFIER PROFILE SET RULE DSCP
CLASSIFIER PROFILE SET RULE DSTADDR
CLASSIFIER PROFILE SET RULE DSTPORT
CLASSIFIER PROFILE SET RULE MARK DSCP
CLASSIFIER PROFILE SET RULE METERID
CLASSIFIER PROFILE SET RULE PRIORITY
CLASSIFIER PROFILE SET RULE PROTOCOL
CLASSIFIER PROFILE SET RULE SRCADDR
CLASSIFIER PROFILE SET RULE SRCPORT
CLASSIFIER PROFILE SET RULE TOS
```

Note: Note that the classifier can be assigned only on the ethernet transport named default

The rule value or values will vary, depending on which packet fields you want to test. For example, to configure a rule to test the source IP address of incoming packets, use the command:

```
classifier profile cp1 set rule rule1 srcaddr 20.20.20.1
255.255.255.255
```

To configure a rule to assign priority value 1, use the command:

```
classifier profile cp1 set rule rule1 priority 1
```

To configure a rule to assign a meter Id to a packet matching the rule use the command:

```
classifier profile MF set rule Gold meterid 1
```

Add the profile to an existing transport using the command:

```
transport set default classifier profile <profile>
```

Typically, you would use the Classifier with the Meter to provide a full policing QoS implementation.

7.1.3.2.2 Marking packets

The Classifier incorporates the functionality of a DIFFSERV Marker. It can be configured to mark packets with a specific DSCP. You can set a classifier rule to configure marking using the CLI command `CLASSIFIER PROFILE SET RULE MARK DSCP`

This command allows you to set a particular DSCP for a specific rule.

If the rule is matched, the DSCP will be written into the DS (or ToS) field in the header of the IP packet and the checksum for the IP header will also be updated.

For example, a router at the edge of a network might classify packets according to their source and destination address and port number, and then mark the packet with a specific DSCP. A router in the core of the network would only need to examine the DSCP field to determine the traffic class of the packet.

The Classifier is not used to mark packets originated by applications running on the device itself. For locally originated traffic, local applications such as VoIP allow to set the value of the IP header DS field, instead of using the default value of 0.

7.1.3.3 Meter

The Meter is used to measure and police the rate of incoming traffic streams. The Meter does not examine outgoing packets and is placed after the Classifier in the receive data path.

The Meter is layered on top of the Classifier. The Classifier classifies (or segregates) incoming traffic stream on the interface to which it is attached, into multiple traffic streams according to configured rules. Each traffic stream then gets metered by the Meter device (provided a meter instance has been configured for the stream).

Metering is done against the meter profile configured by the user to measure that stream.

7.1.3.3.1 How metering works

The Meter device compares temporal properties of the incoming traffic stream against configured parameters. There are two types of meter:

- Two-level meter

  This meter informs whether a packet is in profile (Green) or out of profile (Red).

- Three-level meter

  This informs whether a packet is completely in profile (Green), partially in profile (Yellow) or out of profile (Red).

The meter profile consists of a collection of parameters that define how the metering of packets is to be performed. There are three different meter profiles that can be used with the above meter types.

- *Token bucket* meter profile (used with two-level meter).
- *srTCM (single rate three color marker)* meter profile (used with three-level meter).
- *trTCM (two rate three color marker)* meter profile (used with three-level meter).

These meter profiles differ in the algorithms that they use to decide if a packet is in or out of profile. The following sections describe the above profiles.

7.1.3.3.2 Token bucket meter profile

A two-level meter profile called the Token bucket meter profile consists of two parameters:

- Committed information rate (CIR)
- Committed burst size (CBS)

If the packet stream's average rate is within CIR and the burst size is within CBS then the packet is marked Green, otherwise the packet is marked Red.

7.1.3.3.3 srTCM (single rate three color marker) meter profile

A three-level meter profile named as srTCM (single rate three color marker) meter profile consists of three parameters:

- Committed information rate (CIR)
- Committed Burst Size (CBS)
- Excess Burst Size (EBS)

If the packet stream's average rate is within CIR and the burst size is within CBS then the packet is marked Green. If the packet stream's average rate is within CIR and the burst size is not within CBS but within "CBS+EBS" then the packet is marked Yellow. Otherwise, the packet is marked Red.

7.1.3.3.4 trTCM (two rate three color marker) meter profile

Another three-level meter profile named as trTCM (two rate three color marker) meter profile consists of four parameters:

- Committed information rate (CIR)
- Committed burst size (CBS)
- Peak Information rate (PIR)
- Peak burst size (PBS)

If the packet stream's average rate is within CIR and the burst size is within CBS then the packet is marked Green. If the packet stream's average rate is within PIR and the burst size is within PBS then the packet is marked Yellow. Otherwise the packet is marked Red.

7.1.3.3.5 Metering packets

The Meter device will take one of the following actions for each packet which has been metered:

- Drop (default action for Red packets): Drop the packet buffer.
- Set DSCP value in IP header: Set the DSCP value in the DS field in the header of the IP packet. The Meter will overwrite the DSCP value the packet had before metering. The checksum for the IP packet is also updated following an update to the DSCP value.
- Pass (Default Action for green and yellow packets): Does not set any DSCP value in the IP header. The packet has the same DSCP value it had before metering.

The above actions can be configured by the user.

For every metering result, the Meter will also set a drop priority value in the buffer.

This drop priority value is used by the Algorithmic dropper (if configured) that is used by the *Scheduler* in order to select a packet to drop if the system detects congestion in queues.

The following drop priority values can be set in the buffer:

- If the packet is completely in profile (Green) then a low drop priority value '0' is set in the buffer.
- If the packet if partially in profile (Yellow) then a medium drop priority value '1' is set in the buffer.
- If the packet is out of profile (Red) then a high drop priority value '2' is set in the buffer.

The following diagram illustrates the complete metering process:

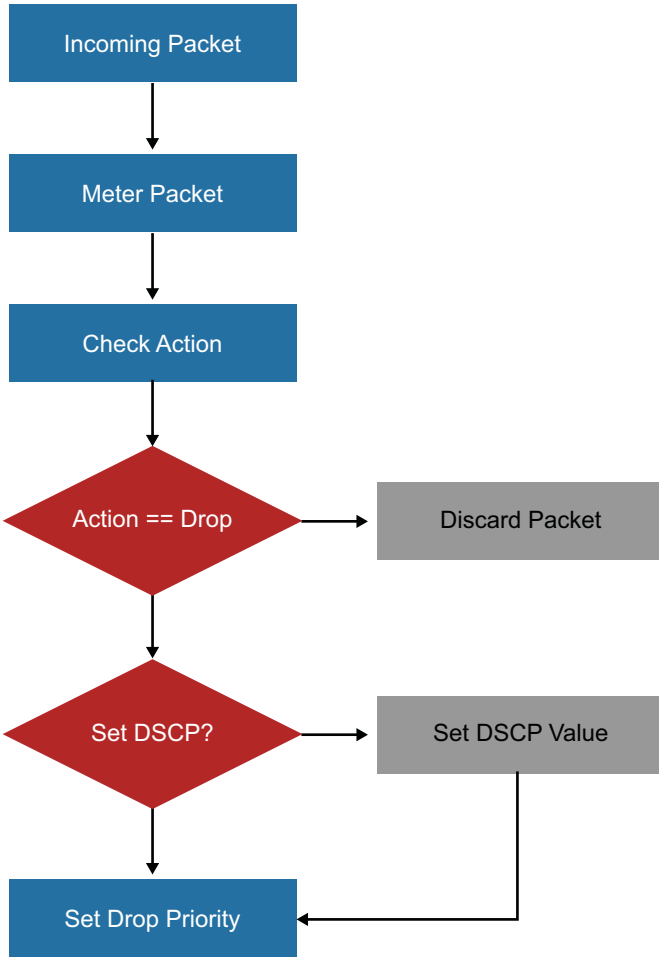


FIGURE 7-2 Metering for Traffic Control

Note that the *Meter* uses the TRUE size of the IP packet for metering. For example, if the Meter receives an Ethernet packet with the following structure:

- 14 bytes Ethernet header.
- 100 bytes of IP packet (20 bytes IP header + 80 bytes payload).
- 4 bytes of Ethernet padding & FCS.

For these types of packets, the Meter will uses 100 bytes for metering calculations. Therefore, don't be surprised if the Meter is configured at 100kbps and you send an Ethernet packet stream of 118 kbps (Ethernet packet size 118bytes) which is unaffected by the Meter process.

7.1.3.3.6 Configuring the meter

To configure the Meter, use the following CLI commands:

1. Create a profile using one of the commands:

```
METER ADD PROFILESRTCM
METER ADD PROFILETOKENBUCKET
METER ADD PROFILETRTCM
```

The metering algorithm type and associated parameters are specified in the command options.

2. By default, green and yellow packets are passed and red packets are dropped. But, you can override these default settings and configure the profile to drop, mark or pass packets for a specific result, using the following commands:

```
METER SET PROFILE {GREEN | RED | YELLOW} ACTION DROP
METER SET PROFILE {GREEN | RED | YELLOW} ACTION MARK DSCP
METER SET PROFILE {GREEN | RED | YELLOW} ACTION PASS
```

3. Add the profile to an existing transport using the command:

```
TRANSPORTS SET DEFAULT METER INSTANCE PROFILE
```

Multiple meter instances can be added to the same transport.

Note: Note that the meter can be assigned only on the ethernet transport named default

7.1.3.4 Scheduler

On the gateways, the Scheduler is used to schedule outgoing packets, belonging to different priority streams, for transmission on an outgoing interface as per the configured service discipline.

Note: If the Scheduler is configured on a network interface (actually it's only supported on ADSL interface), all packets transmitted through that network interface driver are first processed by the Scheduler Device.

The Scheduler device provides the following functions:

- Algorithmic dropper
- Queuing
- Scheduling
- Shaping

These components can be configured in the Scheduler to provide all the above functions or a subset of the above functions, depending on the network requirements. The possible combinations are:

- Shaping only.

- Priority Queuing.
- WFQ2+ Queuing.
- Priority Queuing and Shaping.
- WFQ2+ Queuing and Shaping.
- Shaping and Algorithmic Dropper.
- Priority Queuing and Algorithmic Dropper.
- WFQ2+ Queuing and Algorithmic Dropper.
- Priority Queuing and Shaping and Algorithmic Dropper.
- WFQ2+ Queuing and Shaping and Algorithmic Dropper.

The task of qualifying packets arriving on the incoming interfaces to different priority streams is handled by the Classifier device. The Classifier and Meter devices associate a *scheduling priority* and a *drop priority* value respectively, with the incoming buffer. The service provided by the *Scheduler* to a packet is determined by these values.

- *Scheduling Priority*: This value is used by the Scheduler to identify different priority streams to provide appropriate scheduling behavior. The Classifier sets the configured scheduling priority for a traffic stream matching a classification rule. Multiple traffic streams may map to the same scheduling priority. At present 8 levels (values 0 to 7) of scheduling priority are defined. The value 7 is the highest priority and 0 is the lowest priority.
- *Drop Priority*: The Scheduler implements Algorithmic Dropper functionality, which when configured drops packets selectively during congestion conditions in Scheduler queues.

The packets with higher drop priority have a higher probability of getting dropped than lower priority ones. The Drop priority value is *set by the Meter.* The Classifier is used to set the Drop priority if the Meter has not been configured.

The following diagram provides an overview of the functionality provided by the Scheduler:

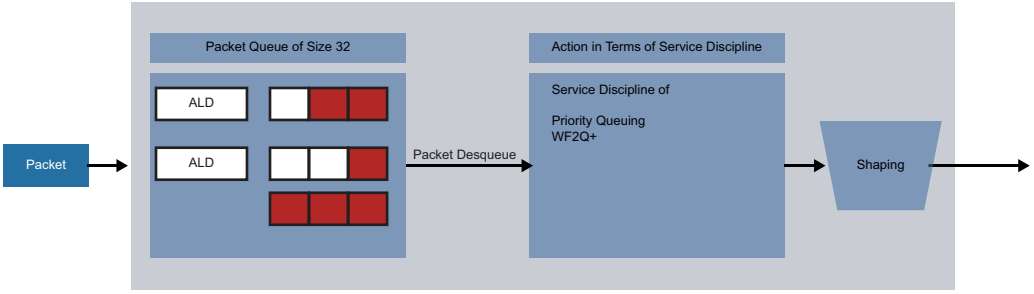


FIGURE 7-3 Overview of Scheduler Functionality

7.1.3.4.1 Service discipline

The Scheduler Service discipline determines the service provided to packets belonging to distinct scheduling priority streams. The incoming packets are buffered in multiple queues based on the Scheduling Priority value (contained in the buffer) associated with the respective packet buffers. These packets are then selected for transmission, based on the configured Service Discipline (the packet selection algorithm).

There are two types of service disciplines that can be used for transmission.

- Priority Queuing

Priority queuing aims at providing better treatment to higher priority traffic as compared to lower priority traffic. The Scheduler supports 8 queues, corresponding to the scheduling priority values (0-7), with 7 being the highest priority and 0 the lowest.

A lower priority queue is only served if the queues having higher priority are not backlogged. This scheme may cause starvation to low priority traffic packets if there is a continuous flow of high priority packets.

- WF2Q+ (WF2Qplus)

WF2Q+ is a version of WF2Q (Worst case weighted fair queuing) algorithm. The WF2Q+ algorithm requires participating queues to have an associated weight value. It distributes the link bandwidth among these queues in the ratio of their respective configured weights.

A single default queue with a weight of 100 percent is created by default. Packets with scheduling priority 0 are always enqueued in the default queue. Weight values may be configured for the other scheduling priority levels 1-7.

As weight values are configured for a scheduling priority level, the weight allocation for the default queue is decremented by the same amount. That is, the total weight allocation for all priority levels is not allowed to exceed 100.

Packets belonging to the scheduling priority level for which a weight was configured, are enqueued in a separate queue and the bandwidth is allocated for all participating queues as per the configured weights.

Packets with scheduling priority for which no weight allocation is configured are enqueued in the default queue.

7.1.3.4.2 Shaping

The Scheduler device may also be configured in a *Shaping mode* to limit the aggregate outgoing traffic to a certain rate using a Token Bucket. Rate limiting for individual traffic streams is not supported.

Note: The Scheduler considers the complete length of a packet for shaping calculations. However, the extra bytes added by lower layer devices than the Scheduler may not be considered. For example, if the Scheduler is applied over an Ethernet interface, the padding and FCS are NOT considered. Also, if the Scheduler is configured over an ATM interface (e.g. PPPoE over RFC1483 over Utopia) the LLC header and the AAL-5 header and trailer are not considered.

7.1.3.4.3 Algorithmic dropper

The Scheduler also supports an active queuing mechanism called the *Algorithmic Dropper (ALD)*. ALD uses RED (Random Early Detection) and WRED (Weighted RED) algorithms for congestion avoidance.

The user can configure the Algorithmic Dropper on any created queue by setting their relevant attributes. This will lead to the association of an Algorithmic Dropper with that particular queue.

The Dropper will decide at the time of packet enqueuing whether the packet should be enqueued in the queue or dropped. When there is no congestion, all packets are queued for transmission on the outgoing interface. When there is congestion or when congestion is about to occur the ALD is used to determine which packets to drop.

The RED algorithm uses a single set of parameters (ALD profiles) to all packets being enqueued, to decide whether to drop a packet.

The WRED algorithm uses three sets of parameters (ALD Profiles). A Drop Priority value associated with each packet is used to determine the ALD profile to use. Based on the profile parameters it is decided whether or not to drop the packet.

The drop priority value is set by the Meter or the Classifier device (if configured).

7.1.3.4.4 Scheduler Profiles

There are two types of profiles used by the Scheduler:

1. Scheduler profiles
2. Algorithmic Dropper Profiles

Scheduler profiles are used to define the following parameters:

- Type of Service Discipline (WF2Q+ or Priority Queuing)
- Parameters for configuring the Scheduler for Shaping
- Values of queue parameters (Algorithmic Dropper profile and queue weights) for WF2Q+ algorithm.

It is possible to create and store multiple profiles. Any one of these profiles can then be used to create multiple Schedulers, each of which can be applied on a different channel.

- Algorithmic Dropper configurations are stored as Algorithmic Dropper Profiles. It is possible to create and store multiple profiles. These profiles can then be associated with a configured queue in a Scheduler profile.

To configure the RED algorithm on a created Scheduler queue, only one ALD profile needs to be set for that queue; the ALD Green profile attribute needs to be set to an existing ALD profile.

To configure WRED on a created Scheduler queue, three ALD profiles need to be created; one profile needs to be set for each drop priority corresponding to the Green, Yellow and Red drop priorities.

For the WRED algorithm, ALD profiles should be configured and applied to Scheduler queues in such a way that packets with a higher drop priority are more likely to be dropped than packets with lower drop priority value.

7.1.3.4.5 Scheduling packets

Packets forwarded to the Scheduler are buffered internally in multiple queues based on the scheduling priority value associated with each packet. If the Algorithmic Dropper is associated with that particular queue then the Dropper will be invoked, at the time of enqueuing, to decide whether the packet should be enqueued in the queue or dropped.

The flow chart below summarises the scheduling process for packet enqueuing.

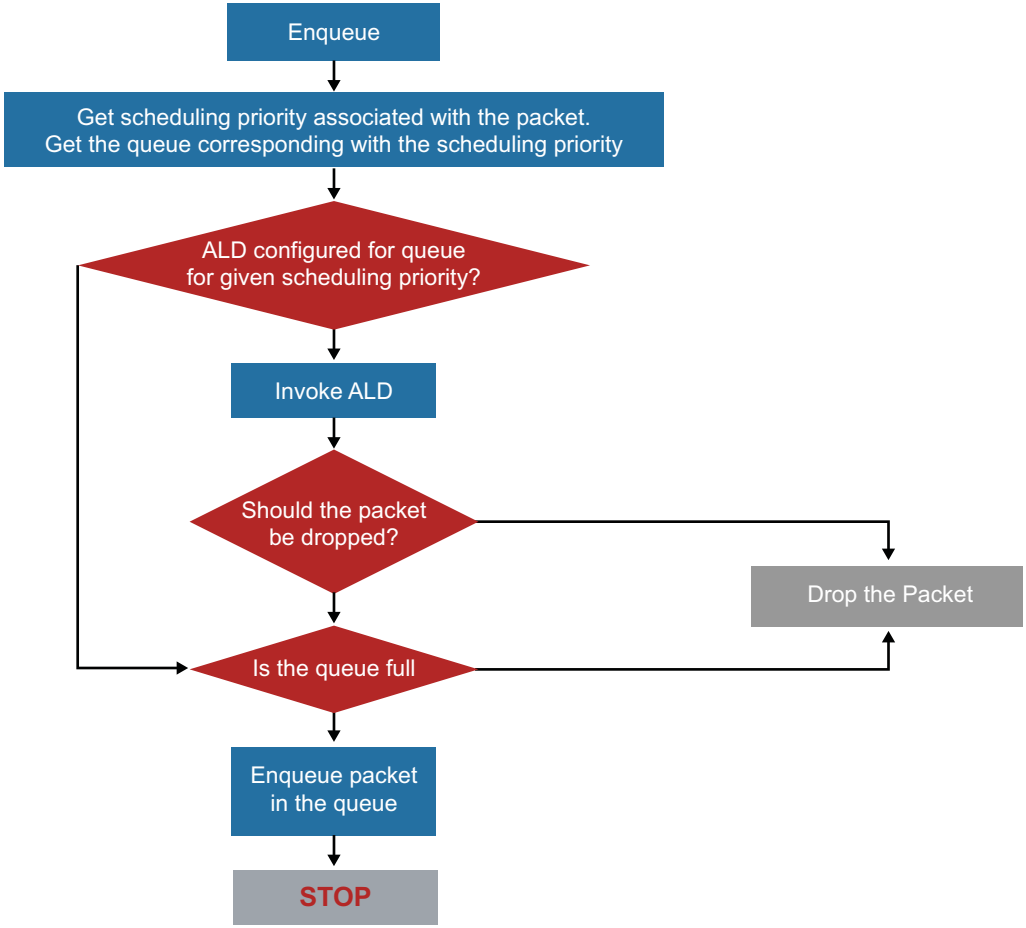


FIGURE 7-4 Scheduling Process for Packet Enqueuing

7.1.3.4.6 Packet Dequeue

The packets present in various queues are selected based on the configured service discipline and transmitted to the driver below. As an optimization measure, the Scheduler tries to utilize a low level driver queue fully by pushing as many packets as possible (limited by the driver queue size) to the driver. The flow chart below summarises the scheduling process for packet dequeuing.

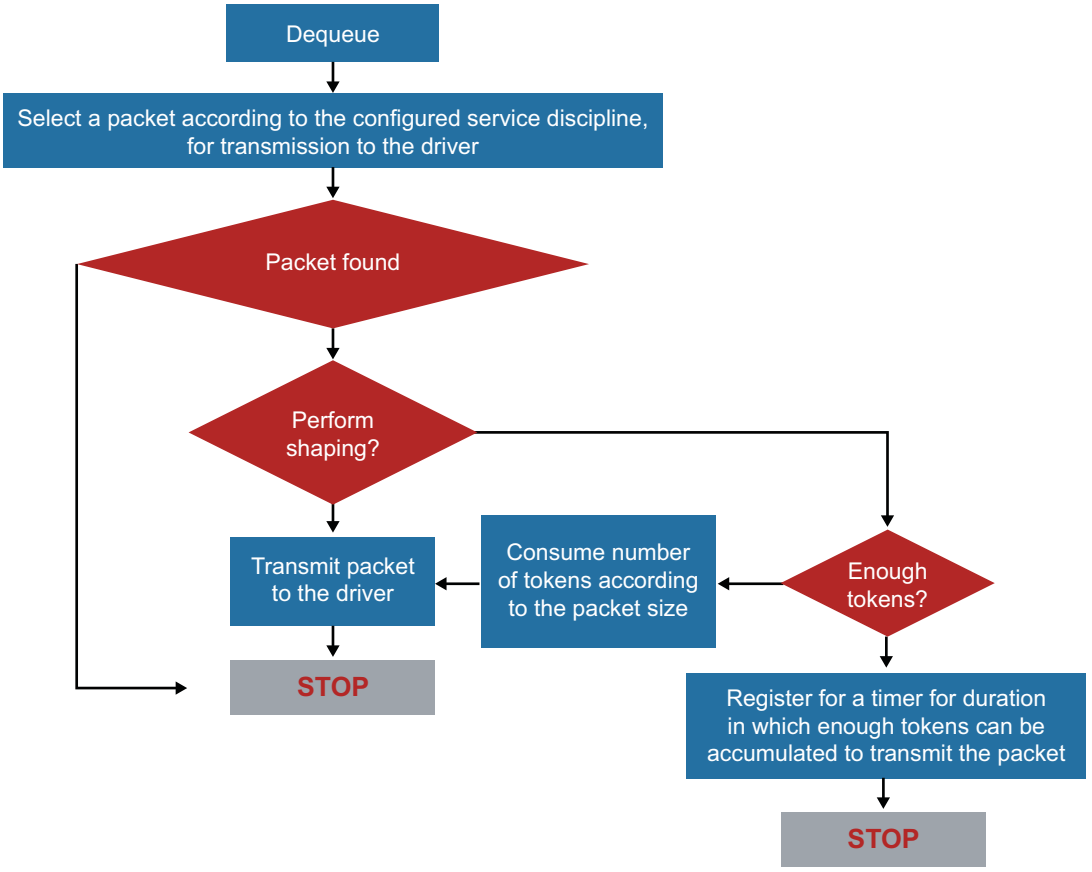


FIGURE 7-5 Scheduling Process for Packet Dequeuing

7.1.3.4.7 Configuring the Scheduler

This section explains the basic steps to follow in order to configure the Scheduler.

To configure the Scheduler, use the following CLI commands:

1. Create a Scheduler profile using the command scheduler add profile {wf2qplus | priority}

The scheduling algorithm type is specified in the command. If the scheduling algorithm is WF2Qplus, then all traffic gets enqueued to a default queue (queue 0) with a weight allocation of 100% by default. To enable enqueuing to the other queues (1-7), assign a weight to the queues using the command SCHEDULER PROFILE SET QUEUE [1-7] WEIGHT

2. The Algorithmic Dropper (ALD) can be applied to a queue using the following command SCHEDULER PROFILE SET QUEUE {DEFAULT | [1-7]} ALD PROFILE <GREENPROFILE> [<YELLOWPROFILE> <REDPROFILE>]

Note that GreenProfile, YellowProfile and RedProfile are the names of ALD profiles that are different from Scheduler profiles. An ALD profile can be created using the command ALD ADD PROFILE [<MINTH> <MAXTH> <MAXDROPPROB> <WEIGHTFACTOR>]

3. Shaping can be configured to throttle the aggregate output rate of the Scheduler to the specified maximum rate and burst size using the COMMAND SCHEDULER SET PROFILE SHAPING <MAXRATE> <MAXBURST>
4. Apply the Scheduler profile to an existing transport using the command TRANSPORTS SET SCHEDULER PROFILE

Note: Note that the classifier can be assigned only for transports attached to the adsl interface like RFC1483, PPPoA and PPPoE(oA).

7.1.4 ATM QoS Feature

The following ATM QoS features are provided by the gateway.

7.1.4.1 ATM Packet Prioritization

After packets have been routed or bridged, the ADSL driver provides transmit prioritisation when packets with different priorities are sent on the same ATM VC.

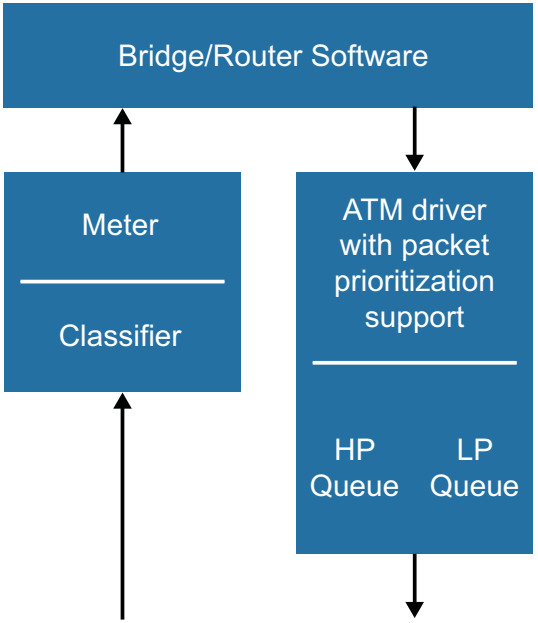


FIGURE 7-6 **The ADSL Driver**

7.1.4.2 How ATM packet prioritization works

The ADSL device driver is responsible for transmit scheduling when packets of different priorities are sent on the same channel.

Note: ADSL driver prioritization support provides a pure prioritization approach, useful for providing Expedited Forwarding for voice packets, as opposed to the Scheduler/Algorithmic Dropper that can provide fair sharing of bandwidth for Assured Forwarding.

The driver discovers the priority of the packet by examining the traffic class field of the buffer that was written by the Classifier.

If a local application, such as the VoIP, originates packets, the IP stack will set the priority of the packet as appropriate. The data stream from the Classifier can also be policed using the Meter to control the data rate for each stream defined by the Classifier. If the data rate of a stream exceeds the rate set in the Meter profile being used to police the data stream, then the Meter will drop packets from that stream.

Therefore, using the Classifier and the Meter can help to lessen the impact of forwarding incoming packets from a high-speed interface such as Ethernet to a low-speed interface such as DSL.

But, without prioritization support in the device driver used for transmitting outgoing packets, the following problems would also occur when packets are forwarded from a high speed interface to a low speed interface:

- high priority packets would suffer latency because they are queued behind a number of low priority packets awaiting transmission

- high priority packets would be dropped, because such a large number of buffers are queued from transmission that system buffering resources are exhausted.

The ADSL driver provides the following features to prevent this:

- Transmit scheduling
- Queue depth limiting

7.1.4.2.1 Transmit scheduling

The ADSL driver can be configured to support two transmit queues per VC; a high priority queue, and a low priority queue. Packets are placed on a queue indicated by the traffic class field of the buffer.

Note: Whenever a transmit slot becomes available, a packet is sent from the high priority queue. If there are no high priority packets available, a packet from the low priority queue is sent instead.

7.1.4.3 Configuring priority handling support

To enable support for different priorities on an existing ATM transport, use the following CLI commands:

```
pppoe set transport mypppoe prilevels 2
pppoa set transport mypppoa prilevels 2
rfc1483 set transport myrfc prilevels 2
```

These commands set two priority levels, as supported by the adsl driver.

Note: Note that packets classified as priority 0 will be placed on the default queue, packets classified as priority 1 or higher will all be placed on the high priority queue.

7.1.5 Classifier command reference

7.1.5.1 Classifier CLI commands

The table below lists the ***classifier*** commands provided by the CLI:

TABLE 7-1 ***Classifier*** commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
CLASSIFIER ADD PROFILE	X	X	X	X	X	X	X	X	X
CLASSIFIER CLEAR PROFILES	X	X	X	X	X	X	X	X	X
CLASSIFIER DELETE PROFILE	X	X	X	X	X	X	X	X	X
CLASSIFIER LIST PROFILES	X	X	X	X	X	X	X	X	X

TABLE 7-1 *Classifier* commands **(Continued)**

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
CLASSIFIER PROFILE ADD RULE	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE CLEAR RULES	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE DELETE RULE	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE LIST RULES	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE DATALENGTH	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE DROPPRI	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE DSCP	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE DSTADDR	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE DSTPORT	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE IFDOMAIN	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE MARK DSCP	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE MARK TOS	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE MARK VPRI	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE METERID	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE OFFSET	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE PHYPORT	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE PRIORITY	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE PROTOCOL	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE SRCADDR	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE SRCPORT	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE TOS	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE TRAFFICTYPE	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE VLANID	X	X	X	X	X	X	X	X	X
CLASSIFIER PROFILE SET RULE VLANPRI	X	X	X	X	X	X	X	X	X
CLASSIFIER SHOW PROFILE	X	X	X	X	X	X	X	X	X

7.1.5.1.1 CLASSIFIER ADD PROFILE

Syntax `CLASSIFIER ADD PROFILE <name>`

Description This command creates a classifier profile. You can add rules to the profile using the classifier profile add rule command. You can then set the profile to work on an ATM transport or transports, using the `TRANSPORT SET CLASSIFIER PROFILE` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Syntax

Option	Description	Default Value
name	An arbitrary name that identifies the profile. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A

Example classifier add profile pr1

See also `CLASSIFIER PROFILE ADD RULE`
`TRANSPORTS SET CLASSIFIER PROFILE`

7.1.5.1.2 CLASSIFIER CLEAR PROFILES

Syntax `classifier clear profiles`

Description This command deletes all classifier profiles that were created using the classifier add profile command. Any rules associated with the profiles are also deleted by this command.

Example --> classifier clear profiles

See also `CLASSIFIER ADD PROFILE`

7.1.5.1.3 CLASSIFIER DELETE PROFILE

Syntax `CLASSIFIER DELETE PROFILE {<name>|<number>}`

Description This command deletes a single profile that was created using the `CLASSIFIER ADD PROFILE` command. Any rules associated with the profile are also deleted by this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A

Example --> classifier delete profile pr1

See also CLASSIFIER ADD PROFILE

7.1.5.1.4 CLASSIFIER LIST PROFILES

Syntax CLASSIFIER LIST PROFILES

Description This command lists all classifier profiles that have been created using the CLASSIFIER ADD PROFILE command. It displays the following information about classifier profiles:

- Profile ID number
- Profile name

Example --> classifier list profiles

```
Classifier Profiles:
 ID |   Name
----|---------------
 1  | pr1
 2  | pr2
 3  | pr3
---------------------
```

See also CLASSIFIER ADD PROFILE

7.1.5.1.5 CLASSIFIER PROFILE ADD RULE

Syntax CLASSIFIER PROFILE {<name>|<number>} ADD RULE <rule name>

Description This command adds a rule to an existing profile. Once you have created a rule, you can configure it using the CLASSIFIER PROFILE SET RULE commands.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An arbitrary name that identifies the rule. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A

Example --> classifier profile pr1 add rule r1

See also CLASSIFIER LIST PROFILES

7.1.5.1.6 CLASSIFIER PROFILE CLEAR RULES

Syntax CLASSIFIER PROFILE {<name>|<number>} CLEAR RULES

Description This command deletes all of the rules that were added to an existing profile using the CLASSIFIER PROFILE ADD RULE command.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A

Example --> classifier profile pr1 clear rules

See also CLASSIFIER PROFILE ADD RULE
CLASSIFIER LIST PROFILES

7.1.5.1.7 CLASSIFIER PROFILE DELETE RULE

Syntax CLASSIFIER PROFILE {<name>|<number>} DELETE RULE {<rule name>|<rule number>}

Description This command deletes a single rule that was added to an existing profile using the CLASSIFIER PROFILE ADD RULE command.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A

Example --> classifier profile pr1 delete rule r1

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE ADD RULE

7.1.5.1.8 CLASSIFIER PROFILE LIST RULES

Syntax CLASSIFIER PROFILE LIST RULES

Description This command displays the following information about the rules previously added to an existing profile:

- Rule ID number
- Rule name
- Test details; each packet is tested against the following configurable fields:
- The source IP address and netmask
- The destination IP address and netmask
- The *Differentiated Services Code Point* (DSCP)
- The protocol name or number
- The source port range
- The destination port range

If a packet matches the configured fields, the packet is assigned a specific QoSC. If a DSCP is specified by the classifier profile set rule mark command, a DSCP is also assigned. The assigned fields are also displayed in the ***Test details*** column.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the `CLASSIFIER LIST PROFILES` command.	N/A
number	An existing profile. To display profile numbers, use the `CLASSIFIER LIST PROFILES` command.	N/A

Example --> classifier profile pr1 list rules

```
Classifier profile: pr1
 ID | Name | Test details
----|-------------------------------------------------------
 1  | r1   | Set QOSC 1         Mark DSCP none
    |      | Src Addr 1.1.1.1   Src Mask  255.255.255.0
    |      | Dst Addr 2.2.2.2   Dst Mask  255.255.255.255
    |      | DSCP     any       Protocol  UDP
    |      | Src Port 2727-2727 Dst Port  0  -  0
-------------------------------------------------------------
```

See also `CLASSIFIER LIST PROFILES`

7.1.5.1.9 CLASSIFIER PROFILE SET RULE DATALENGTH

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} DATALENGTH <min> <max>`

Description This command configures a classifier rule to check the size of the payload data carried by packets.

If the <protocol> value of the classifier profile set rule protocol command is set to TCP, this rule compares the payload data length of the TCP packet (i.e., IP total length - IP header length - TCP header length) to the <min> and <max> values specified here.

If the <protocol> value of the classifier profile set rule protocol command is set to UDP, this rule compares the payload data length of the UCP packet (i.e., IP total length - IP header length - UDP header length) to the <min> and <max> values specified here.

If the <protocol> value of the classifier profile set rule protocol command is set to any or to a valueother than TCP or UDP, this rule compares the payload data length of the IP packet (i.e., IP total length - IP header length) to the <min> and <max> values specified here.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	A name that identifies an existing profile. To display profile names, use the classifier list profiles command.	N/A
number	A number that identifies an existing profile. To display profile numbers, use the classifier list profiles command.	N/A
rule number	A number that identifies an existing rule. To display rule numbers, use the classifier profile list rules command.	N/A
min/max	Minimum and maximum payload values.	N/A

Example --> classifier profile pr1 set rule r1 datalength 0 0

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`

7.1.5.1.10 CLASSIFIER PROFILE SET RULE DROPPRI

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} DROPPRI <droppri>`

Description This command configures the specified drop priority to be assigned to packets when the rule is matched. The algorithmic dropper module reads the drop priority of the packet.

If the algorithmic dropper is not in use (for example, the scheduler device is not included in the build), this setting has no effect.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
droppri	The drop priority set as either 0, 1 or 2: 0 = the lowest drop priority (green) 1 = the medium drop priority (yellow) 2 = the highest drop priority (red)	N/A

Example --> classifier profile pr1 set rule r1 droppri 0

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES

7.1.5.1.11 CLASSIFIER PROFILE SET RULE DSCP

Syntax CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} DSCP <dscp>

Description This command configures a classifier rule to test the ***Differentiated Services Code Point*** (DSCP) field in the IP header of incoming packets.

The DSCP field is also known as the ***Type of Service*** (TOS) field. See the CLASSIFIER PROFILE SET RULE TOS command, which provides an alternative method of testing the same IP header field.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable)

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
dscp	The ***Differentiated Service Code Point*** (DSCP). This value is specified as 6 binary digits (NNNNNN). Set to any to cancel the DSCP setting.	any

Example --> classifier profile pr1 set rule r1 dscp 101110

See also
```
CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES
CLASSIFIER PROFILE SET RULE TOS
```

7.1.5.1.12 CLASSIFIER PROFILE SET RULE DSTADDR

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} DSTADDR <addr> <mask>`

Description This command configures a classifier rule to test the destination IP address of incoming packets. The netmask address is compulsory and allows you to match either a whole subnet or just one host using the mask 255.255.255.255.

Set the DSTADDR values to 0.0.0.0 if you want to cancel this test and set the rule to match any destination IP address.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A

Option	Description	Default Value
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
addr	The destination IP address, displayed in the following format: 192.168.102.3	0.0.0.0
mask	The destination subnet mask address, displayed in the following format: 255.255.255.0	0.0.0.0

Example --> classifier profile pr2 set rule r1 dstaddr 192.168.86.93 255.255.255.255

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES

7.1.5.1.13 CLASSIFIER PROFILE SET RULE DSTPORT

Syntax CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} DSTPORT <min> <max>

Description This command configures a classifier rule to test the destination port of incoming packets. You can specify a range of ports by configuring different minimum and maximum port numbers, or specify a single port by configuring the same port number for both port values.

Set the DSTPORT min and max values to 0 if you want to cancel this test and set the rule to match any destination port.

Note: This rule is only meaningful for TCP and UDP protocols. If you have set a destination port rule, you must also specify which protocol (TCP or UDP) should be tested by the rule. See CLASSIFIER PROFILE SET RULE PROTOCOL

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable)

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
min	The start of the destination port range for a TCP or UDP protocol.	0
max	The end of the destination port range for a TCP or UDP protocol.	0

Example --> classifier profile pr1 set rule r1 dstport 2727 2727

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES
CLASSIFIER PROFILE SET RULE PROTOCOL

7.1.5.1.14 CLASSIFIER PROFILE SET RULE IFDOMAIN

Syntax CLASSIFIER PROFILE <name> SET RULE <rule_name> IFDOMAIN <ifdomain> ACTION <action>

Description The purpose of this command is to create a rule that matches the interface domain of the incoming packet.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	The name of the profile under which the rule exists	N/A
rule_name	The name of the rule in the profile to alter.	N/A

Option	Description	Default Value
ifdomain	The name of the domain on which to match	N/A
action	The action to be carried out in the event of a match	N/A

Example --> classifier profile TestProfile set rule TestRule ifdomain example.com action drop

See also `CLASSIFIER PROFILE LIST RULES`
`CLASSIFIER PROFILE ADD RULE`

7.1.5.1.15 CLASSIFIER PROFILE SET RULE MARK DSCP

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} MARK DSCP <dscp>`

Description **T**his command determines what happens if a rule is matched. You can configure the classifier to mark packets with a specific ***Differentiated Services Code Point*** (DSCP). If set, the DSCP field in the IP header will be changed to the value set here.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the `CLASSIFIER LIST PROFILES` command.	N/A
number	An existing profile. To display profile numbers, use the `CLASSIFIER LIST PROFILES` command.	N/A
rule name	An existing rule. To display rule names, use the `CLASSIFIER PROFILE LIST RULES` command.	N/A
rule number	An existing rule. To display rule numbers, use the `CLASSIFIER PROFILE LIST RULES` command.	N/A
dscp	The ***Differentiated Service Code Point*** that marked matched packets. It can be either an hexadecimal (0xNN) or 6 binary digits (NNNNNN). "none" deletes the DSCP setting.	none

Example --> classifier profile pr1 set rule r1 mark dscp 101110

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`

7.1.5.1.16 CLASSIFIER PROFILE SET RULE MARK TOS

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} MARK TOS <tos>`

Description This command determines what happens if a rule is matched. You can configure the classifier to mark packets with a specific Type of Service (ToS). If set, the TOS field in the IP header will be changed to the value set here.

The ToS field is also known as the DSCP field. See also the classifier profile set rule mark dscp command which provides an alternative method of marking the same IP header field.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	A name that identifies an existing profile. To display profile names, use the classifier list profiles command.	N/A
number	A number that identifies an existing profile. To display profile numbers, use the classifier list profiles command.	N/A
rule name	A name that identifies an existing rule. To display rule names, use the classifier profile list rules command.	N/A
rule number	A number that identifies an existing rule. To display rule numbers, use the classifier profile list rules command.	N/A
tos	The Type of Service (ToS). This value is specified in hexadecimal format (0xNN) between the ranges 0x00 and 0xfc. The 2 least significant bits are ignored. Set to any to cancel the tos setting.	none

Example --> classifier profile pr1 set rule r1 mark tos 0x04

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES

7.1.5.1.17 CLASSIFIER PROFILE SET RULE MARK VPRI

Syntax CLASSIFIER PROFILE <profilename> SET RULE <rulename> MARK VLANPRI <vlanpri>

Description This rule marks 802.1p priority in the packet. This rule works on both 802.1q tagged and untagged packets, if the packet is untagged and rule is configured a 4byte field (802.1q field) is added in the packet and 802.1p priority is set.

If packet is already tagged then the value of 802.1p priority is reset to the value provided in the rule.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
profilename	A name that identifies an existing profile. To display profile names, use the classifier list profiles command.	N/A
rule name	A name that identifies an existing rule. To display rule names, use the classifier profile list rules command.	N/A
vlanpri	The vlan priority to be matched ,valid values 0 to 7	N/A

Example --> classifier profile pr1 set rule r1 mark vlanpri 3

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES

7.1.5.1.18 CLASSIFIER PROFILE SET RULE METERID

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} METERID <meterid>`

Description This command determines what happens if a rule is matched. You can configure the classifier to assign a ***meter Id*** to the packet matching a rule.

Once you have set which ***meter Id*** to assign, you need to create an association between the classified stream and the meter instance using the `TRANSPORTS SET METER INSTANCE` command.

If the meter device is not in use, this setting has no effect.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the `CLASSIFIER LIST PROFILES` command.	N/A
number	An existing profile. To display profile numbers, use the `CLASSIFIER LIST PROFILES` command.	N/A
rule name	An existing rule. To display rule names, use the `CLASSIFIER PROFILE LIST RULES` command.	N/A
meterid	A number that represents a meter instance. The meter instance and profile is set on a specific transport using the `TRANSPORTS SET METER INSTANCE` command.	N/A

Example --> classifier profile pr1 set rule r1 meterid 1

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`
`TRANSPORTS SET METER INSTANCE PROFILE`

7.1.5.1.19 CLASSIFIER PROFILE SET RULE OFFSET

Syntax `CLASSIFIER PROFILE <profilename> SET RULE <rule name> OFFSET <offset> MASK <mask> VALUE <value>`

Description This command tries to match all bytes in the packet starting at a valid offset from the Ethernet header.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
profilename	A name that identifies an existing profile. To display profile names, use the classifier list profiles command.	N/A
rule name	A name that identifies an existing rule. To display rule names, use the classifier profile list rules command.	N/A
offset	Offset from the ethernet header ,valid values 0 to 1500	N/A
mask	Mask to be taken , valid values 0x000000000000 to 0xffffffffffff	N/A
value	It is the value to match against	N/A

Example --> classifier profile pr1 set rule r1 offset 0 mask ffffffffffff value 000000000001

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`

7.1.5.1.20 CLASSIFIER PROFILE SET RULE PHYPORT

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} PHYPORT <portnum>`

Description This command configures a classifier rule to test the physical port on which a packet arrived. This test is used when multiple Ethernet ports are connected to the same transport (and therefore share the same classifier profile), but packets must be classified differently depending on which port they arrive on. The physical port numbers are positive, non-zero integers.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	A name that identifies an existing profile. To display profile names, use the classifier list profiles command.	N/A
number	A number that identifies an existing profile. To display profile numbers, use the classifier list profiles command.	N/A
rule name	A name that identifies an existing rule. To display rule names, use the classifier profile list rules command.	N/A
portnum	A physical port number which must be a positive, non-zero integer.	N/A

Example --> classifier profile pr1 set rule r1 phyport 1

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`

7.1.5.1.21 CLASSIFIER PROFILE SET RULE PRIORITY

Syntax `CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} PRIORITY <priority>`

Description **T**his command determines what happens if a rule is matched. You can configure the classifier to assign a priority to the packet matching a rule. The priority is mapped to a scheduling priority value or queue ID (configured using the `SCHEDULER PROFILE SET QUEUE WEIGHT` command) in order for the scheduler to identify different priority streams and provide appropriate scheduling behavior.

Multiple traffic streams may map to the same scheduling priority.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
priority	The scheduling priority value or queue ID value, that is any number between 1 and 7 (included). To display scheduling priority values, use the SCHEDULER SHOW PROFILE QUEUES command.	N/A

Example --> classifier profile pr1 set rule r1 priority 1

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES
SCHEDULER PROFILE SET QUEUE WEIGHT

7.1.5.1.22 CLASSIFIER PROFILE SET RULE PROTOCOL

Syntax CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} PROTOCOL <protocol>

Description **T**his command configures a classifier rule to test the protocol of incoming packets. You can specify the following protocols by name or decimal protocol number:

- TCP (6)
- UDP (17)
- ICMP (1)
- GRE (47)

All other protocols can only be specified by their decimal protocol number.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the classifier list profiles command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
protocol	The name/decimal number for the supported protocol. Set to 'any' to cancel the test and let the rule match any protocol	any

Example --> classifier profile pr1 set rule r1 protocol udp

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES

7.1.5.1.23 CLASSIFIER PROFILE SET RULE SRCADDR

Syntax CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} SRCADDR <addr> <mask>

Description This command configures a classifier rule to test the source IP address of incoming packets. The netmask address is compulsory and allows you to match either a whole subnet or just one host using the mask 255.255.255.255.

Set the srcaddr values to 0.0.0.0 if you want to cancel this test and set the rule to match any source IP address.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A

Option	Description	Default Value
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
addr	The source IP address, in the format 192.168.102.3	0.0.0.0
mask	The source subnet mask address in the format 255.255.255.0	0.0.0.0

Example --> classifier profile pr2 set rule r1 srcaddr 192.168.101.1 255.255.255.255

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES

7.1.5.1.24 CLASSIFIER PROFILE SET RULE SRCPORT

Syntax CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} SRCPORT <min> <max>

Description This command configures a classifier rule to test the source port of incoming packets. You can specify a range of ports by configuring different minimum and maximum port numbers, or specify a single port by configuring the same port number for both port values.

Set the srcport value to 0.0.0.0 if you want to cancel this test and set the rule to match any source port.

Note: This rule is only meaningful for TCP and UDP protocols. If you have set a source port rule, you must also specify which protocol (TCP or UDP) should be tested by the rule. See CLASSIFIER PROFILE SET RULE PROTOCOL

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable)

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A

Option	Description	Default Value
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
min	The start of the source port range for a TCP or UDP protocol.	0
max	The end of the source port range for a TCP or UDP protocol.	0

Example --> classifier profile pr1 set rule r1 srcport 2727 2727

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES
CLASSIFIER PROFILE SET RULE PROTOCOL

7.1.5.1.25 CLASSIFIER PROFILE SET RULE TOS

Syntax CLASSIFIER PROFILE {<name>|<number>} SET RULE {<rule name>|<rule number>} TOS <tos>

Description This command configures a classifier rule to test the ***Type of Service*** (ToS) field in the IP header of incoming packets.

The ToS field is also known as the DSCP field. See also the CLASSIFIER PROFILE SET RULE DSCP command that provides an alternative method of testing the same IP header field.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display profile names, use the CLASSIFIER LIST PROFILES command.	N/A
number	An existing profile. To display profile numbers, use the CLASSIFIER LIST PROFILES command.	N/A

Option	Description	Default Value
rule name	An existing rule. To display rule names, use the CLASSIFIER PROFILE LIST RULES command.	N/A
rule number	An existing rule. To display rule numbers, use the CLASSIFIER PROFILE LIST RULES command.	N/A
tos	The ***Type of Service***, specified as a hexadecimal (0xNN) in the range 0x00 and 0xfc. The 2 least significant bits are ignored. Set to 'any' to cancel the ToS setting.	any

Example --> classifier profile pr1 set rule r1 tos 0x04

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES
CLASSIFIER PROFILE SET RULE DSCP

7.1.5.1.26 CLASSIFIER PROFILE SET RULE TRAFFICTYPE

Syntax CLASSIFIER PROFILE <name> SET RULE <rule_name> TRAFFICTYPE <type>

Description The purpose of this command is to match the rule based on the traffic type specified in the ethernet header.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	The name of the profile in which to alter the rule	N/A
rule name	The name of the rule in the profile to alter	N/A
type	The value of the traffic type on which to match the rule.	N/A

Example --> classifier profile TestProfile set rule TestRule traffictype 0x800

See also CLASSIFIER LIST PROFILES
CLASSIFIER PROFILE LIST RULES

7.1.5.1.27 CLASSIFIER PROFILE SET RULE VLANID

Syntax `CLASSIFIER PROFILE <profilename> SET RULE <rule name> VLANID <vlanidmin> <vlanidmax>`

Description This command classifies packet based on the vlanid range specified.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
profilename	A name that identifies an existing profile. To display profile names, use the classifier list profiles command.	N/A
rule name	A name that identifies an existing rule. To display rule names, use the classifier profile list rules command.	N/A
vlanidmin	Lower range to be matched, valid values 1 to 4094	N/A
vlanidmax	Upper range to be matched, valid values 1 to 4094	N/A

Example --> classifier profile pr1 set rule r1 vlanid 2 4091

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`

7.1.5.1.28 CLASSIFIER PROFILE SET RULE VLANPRI

Syntax `CLASSIFIER PROFILE <profilename> SET RULE <rule name> VLAN-PRI <vlanpri>`

Description This command classifies packet based on the 802.1p priority.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
profilename	A name that identifies an existing profile. To display profile names, use the classifier list profiles command.	N/A
rule name	A name that identifies an existing rule. To display rule names, use the classifier profile list rules command.	N/A
vlanpri	The vlan priority to be matched , valid values 0 to 7	N/A

Example --> classifier profile pr1 set rule r1 vlanpri 2

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`

7.1.5.1.29 CLASSIFIER SHOW PROFILE

Syntax `CLASSIFIER SHOW PROFILE {<name>|<number>}`

Description This command displays the following information about the rules previously added to an existing profile:

- Rule ID number
- Rule name
- Test details; each packet is tested against the following configurable fields:
- The source IP address and netmask
- The destination IP address and netmask
- The Differentiated Services Code Point (DSCP)
- The protocol name or number
- The source port range
- The destination port range

If a packet matches the configured fields, the packet is assigned a specific QoSC. If a DSCP is specified by the classifier profile set rule mark command, a DSCP is also assigned. The assigned fields are also displayed in the ***Test details*** column.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable)

Option	Description	Default Value
name	An existing profile. To display profile names, use the `CLASSIFIER LIST PROFILES` command.	N/A
number	An existing profile. To display profile numbers, use the `CLASSIFIER LIST PROFILES` command.	N/A

Example --> classifier show profile pr1

```
Classifier profile: pr1
 ID | Name | Test details
----|-----------------------------------------------------
 1  | r1   | Set QOSC 1         Mark DSCP none
    |      | Src Addr 1.1.1.1    Src Mask  255.255.255.0
    |      | Dst Addr 2.2.2.2   Dst Mask  255.255.255.255
    |      | DSCP     any       Protocol  UDP
    |      | Src Port 2727-2727 Dst Port  0  -  0
-------------------------------------------------------------
```

See also `CLASSIFIER LIST PROFILES`
`CLASSIFIER PROFILE LIST RULES`
`CLASSIFIER PROFILE SET RULE PROTOCOL`

7.1.6 Meter command reference

7.1.6.1 Meter CLI commands

The table below lists the ***meter*** commands provided by the CLI:

TABLE 7-2 Meter commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
METER ADD PROFILE SRTCM	X	X	X	X	X	X	X	X	X
METER ADD PROFILE TOKENBUCKET	X	X	X	X	X	X	X	X	X

TABLE 7-2 **Meter** commands **(Continued)**

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
METER ADD PROFILE TRTCM	X	X	X	X	X	X	X	X	X
METER CLEAR PROFILES	X	X	X	X	X	X	X	X	X
METER DELETE PROFILE	X	X	X	X	X	X	X	X	X
METER LIST PROFILES	X	X	X	X	X	X	X	X	X
METER SET PROFILE ACTION DROP	X	X	X	X	X	X	X	X	X
METER SET PROFILE ACTION MARK DSCP	X	X	X	X	X	X	X	X	X
METER SET PROFILE ACTION PASS	X	X	X	X	X	X	X	X	X
METER SHOW PROFILE	X	X	X	X	X	X	X	X	X

7.1.6.1.1 METER ADD PROFILE SRTCM

Syntax `METER ADD PROFILe <name> SRTCM <cir> <cbs> <ebs>`

Description This command creates a meter profile that uses srTCM algorithm for metering.

If a packet stream's average rate is within CIR and the burst size is within CBS, then that packet is in-profile (green).

If a packet stream's average rate is within CIR and the burst size is not within CBS but is within CBS+EBS, then that packet is partially in profile (yellow).

All other packets are out of profile (red).

Note that only IP packet size (IP header and payload) is considered for calculations.

You can specify the treatment or actions for green, yellow and red packets using the meter set profile action commands. You can then set the profile to create meter instance on a transport using the `TRANSPORTS SET METER INSTANCE PROFILE` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the profile. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
cir	***Committed Information Rate*** in kbps.	N/A
cbs	***Committed Burst Size*** in bytes.	N/A
ebs	***Excess Burst Size*** in bytes.	N/A

Example --> meter add profile mp1 srtcm 80 10000 25000

See also
```
METER ADD PROFILE TOKENBUCKET
METER ADD PROFILE TRTCM
METER LIST PROFILES
```

7.1.6.1.2 METER ADD PROFILE TOKENBUCKET

Syntax
```
METER ADD PROFILE <name> TOKENBUCKET <cir> <cbs>
<scalar>
```

Description This command creates a meter profile that uses the token-bucket algorithm for metering.

Allows for a larger <cbs> while retaining the committed <cir> – this is especially helpful managing packet loss with bursty TCP/IP traffic. Possible values are from 1 to 15, with 1 resulting in no change to the cbs and 15 resulting in a cbs that is 15 times the configured value.

If a packet stream's average rate is within CIR and the burst size is within CBS, then the packet is in profile (green).

All other packets are out of profile (red).

Note that only IP packet size (IP header and payload) is considered for calculations.

You can specify the treatment or actions for green, yellow and red packets using the meter set profile action commands. You can then set the profile to create meter instance on a transport using the `TRANSPORTS SET METER INSTANCE PROFILE` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the profile. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
cir	***Committed Information Rate*** in kbps.	N/A
cbs	***Committed Burst Size*** in bytes.	N/A

Example --> meter add profile mp1 tokenbucket 80 10000

See also `METER ADD PROFILE SRTCM`
`METER ADD PROFILE TRTCM`

7.1.6.1.3 METER ADD PROFILE TRTCM

Syntax `METER ADD PROFILE <name> TRTCM <cir> <cbs> <pir> <pbs>`

Description This command creates a meter profile that uses the trTCM algorithm for metering.

If a packet stream's average rate is within CIR and the burst size is within CBS, then the packet is in profile (green).

If a packet stream's average rate is within PIR and the burst size is within PBS, then the packet is partially in profile (yellow).

All other packets are out of profile (red).

Note that only IP packet size (IP header and payload) is considered for calculations.

You can specify the treatment or actions for green, yellow and red packets using the meter set profile action commands. You can then set the profile to create meter instance on a transport using the `TRANSPORTS SET METER INSTANCE PROFILE` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the profile. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A

Option	Description	Default Value
cir	***Committed Information Rate*** in kbps.	N/A
cbs	***Committed Burst Size*** in bytes.	N/A
pir	***Peak Information Rate*** in kbps.	N/A
pbs	***Peak Burst Size*** in bytes.	N/A

Example --> meter add profile mp1 trtcm 80 10000 120 15000

See also
```
METER ADD PROFILE SRTCM
METER ADD PROFILE TOKENBUCKET
METER LIST PROFILES
```

7.1.6.1.4 METER CLEAR PROFILES

Syntax `METER CLEAR PROFILES`

Description This command allows you to delete all meter profiles that were previously created using the meter add profile commands.

Note that this command does not delete the profiles that are associated with meter instances created using the `TRANSPORTS SET METER INSTANCE PROFILE` command.

Example --> meter clear profiles

See also
```
METER ADD PROFILE SRTCM
METER ADD PROFILE TOKENBUCKET
METER ADD PROFILE TRTCM
```

7.1.6.1.5 METER DELETE PROFILE

Syntax `METER DELETE PROFILE <name>`

Description This command deletes a single meter profile that was previously created using one of the meter add profile commands.

Note: Note that this command does not delete the profiles that are associated with meter instances created using the `TRANSPORTS SET METER INSTANCE PROFILE` *command.*

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the METER LIST PROFILES command.	N/A

Example --> meter delete profile mp1

See also METER ADD PROFILE SRTCM
METER ADD PROFILE TOKENBUCKET
METER ADD PROFILE TRTCM

7.1.6.1.6 METER LIST PROFILES

Syntax METER LIST PROFILES

Description This command lists all of the meter profiles that were created using the METER ADD PROFILE commands. It displays the following information about meter profiles:

- Name
- Type of algorithm used
- CIR value (in kbps)
- CBS value (in bytes)
- EBS value (for algorithm type srtcm only)
- PIR value (for algorithm type trtcm only)
- PBS value (for algorithm type trtcm only)
- Green action
- Yellow action (for algorithm types trtcm and srtcm only)
- Red action

Example --> meter list profiles

```
Meter Profiles:
Name|    Type    | CIR | CBS | PIR | PBS | EBS |Green | Yellow| Red
    |            |kbps |bytes|kbps |bytes|bytes|      |       |
----|------------|-----|-----|-----|-----|-----|------|-------|-----
 mp1| tokenbucket| 80  |10000|     |     |     | Pass |       | Drop
 mp2| srtcm      | 80  |10000|     |     |25000| Pass | Pass  | Drop
 mp3| trtcm      | 80  |10000| 120 |15000|     | Pass | Pass  | Drop
-------------------------------------------------------------------
```

See also METER ADD PROFILE SRTCM
METER ADD PROFILE TOKENBUCKET
METER ADD PROFILE TRTCM

7.1.6.1.7 METER SET PROFILE ACTION DROP

Syntax METER SET PROFILE <name> {GREEN|RED|YELLOW} ACTION DROP

Description This command configures an existing profile to drop packets depending on their metering result. Note that if this command is not applied, by default the green and yellow packets are passed and red packets are dropped.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the METER LIST PROFILES command.	N/A
green	Sets packets with green (in profile) metering results to be dropped.	pass
red	Sets packets with red (out of profile) metering results to be dropped.	drop
yellow	Sets packets with yellow (partially in profile) metering results to be dropped.	pass

Example --> meter set profile mp1 green action drop

See also METER LIST PROFILES

7.1.6.1.8 METER SET PROFILE ACTION MARK DSCP

Syntax METER SET PROFILE <name> {GREEN|RED|YELLOW} ACTION MARK DSCP <dscp>

Description This command configures a profile to set the DSCP value in the IP header of packets depending on their metering result (green, yellow or red). The DSCP value is written into the DS field in the header of the IP packet.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the METER LIST PROFILES command.	N/A
green	Sets the DSCP value in packets with green (in profile) metering results.	N/A
red	Sets the DSCP value in packets with red (out of profile) metering results.	N/A
yellow	Sets the DSCP value in packets with yellow (partially in profile) metering results to be dropped.	N/A
dscp	The ***Differentiated Service Code Point*** (DSCP). This can be either a hexadecimal (0xNN) or a 6 binary digits (NNNNNN), in which case the six most significant bits indicate the DSCP value while the two least significant ones are ignored.	N/A

Example --> meter set profile mp1 yellow action mark dscp 011001

See also METER LIST PROFILES

7.1.6.1.9 METER SET PROFILE ACTION PASS

Syntax METER SET PROFILE <name> {GREEN|RED|YELLOW} ACTION PASS

Description This command configures an existing profile to pass packets depending on their metering result. The DSCP value in the IP header of packets is not set.

Note that if this command is not applied, by default the green and yellow packets are passed and red packets are dropped.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the METER LIST PROFILES command.	N/A
green	Sets packets with green (in profile) metering results to pass.	pass

Option	Description	Default Value
red	Sets packets with red (out of profile) metering results to pass.	drop
yellow	Sets packets with yellow (partially in profile) metering results to pass.	pass

Example --> meter set profile mp1 green action pass

See also `METER LIST PROFILES`

7.1.6.1.10 METER SHOW PROFILE

Syntax `METER SHOW PROFILE <name>`

Description This command displays information about a meter profile that was created using one of the `METER ADD PROFILE` commands. It displays the following information about the specified profile:

- Name
- Type of algorithm used
- CIR value (in kbps)
- CBS value (in bytes)
- EBS value (for algorithm type srtcm only)
- PIR value (for algorithm type trtcm only)
- PBS value (for algorithm type trtcm only)
- Green action
- Yellow action (for algorithm types trtcm and srtcm only)
- Red action

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the `METER LIST PROFILES` command.	N/A

Example --> meter show profile mp3

```
Meter Profile : mp3
Type            : trtcm
CIR (kbps)    : 80
CBS (bytes)   : 10000
PIR (kbps)    : 120
PBS (bytes)   : 15000
EBS (bytes)   :
Green Action  : Pass
Yellow Action : Pass
Red Action    : Drop
```

See also METER LIST PROFILES

7.1.6.2 Scheduler CLI commands

The table below lists the commands provided by the CLI:

TABLE 7-3 ***Scheduler*** commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
SCHEDULER ADD PROFILE	X	X	X	X	X	X	X	X	X
SCHEDULER CLEAR PROFILES	X	X	X	X	X	X	X	X	X
SCHEDULER DELETE PROFILE	X	X	X	X	X	X	X	X	X
SCHEDULER LIST PROFILES	X	X	X	X	X	X	X	X	X
SCHEDULER SET PROFILE SHAPING	X	X	X	X	X	X	X	X	X
SCHEDULER PROFILE SET QUEUE WEIGHT	X	X	X	X	X	X	X	X	X
SCHEDULER PROFILE SET QUEUE ALD PROFILE	X	X	X	X	X	X	X	X	X
SCHEDULER PROFILE SET QUEUE ALD DISABLED	X	X	X	X	X	X	X	X	X
SCHEDULER SHOW PROFILE	X	X	X	X	X	X	X	X	X
SCHEDULER SHOW PROFILE QUEUES	X	X	X	X	X	X	X	X	X

7.1.6.2.1 SCHEDULER ADD PROFILE

Syntax SCHEDULER ADD PROFILE <name> {WF2QPLUS | PRIORITY}

Description This command creates a scheduler profile with either WF2Q+ or Priority Queuing set as the type of service discipline. Classifier assigns scheduling priority to a packet (configured

by the classifier profile set rule priority command). This value determines the scheduling behavior received by a packet. If a packet is not classified, scheduling priority 0 is assigned to the packet by default.

If you select the priority service discipline, the profile supports 8 queues, each corresponding to a scheduling priority from 0-7. Each queue can hold a maximum of 32 packets at any instant. Scheduling priority value 0 assigns the lowest priority while 7 assigns the highest priority.

If you select the WF2QPlus service discipline, the weight value (percentage) configured for a scheduling priority determines the share of bandwidth received by packets belonging to the scheduling priority level. A single default queue with a weight of 100% is created by default. Packets with scheduling priority 0 are always enqueued in the default queue. You may configure weights for scheduling priority levels (1-7) using the scheduler profile set queue weight command.

If you do configure weight for a scheduling priority level, the corresponding packets are enqueued in a separate queue and the bandwidth is allocated in accordance with the configured weights. Otherwise, packets are enqueued in the default queue.

Each queue can hold a maximum of 32 packets at any instance.

In addition, this created scheduler profile may be configured with shaping and algorithmic dropper (RED/WRED):

- *Shaping*: you can configure the scheduler profile for shaping by using the scheduler set profile shaping command. Shaping is disabled by default.
- *Algorithmic Dropper*: you can configure Algorithmic Dropper (RED/WRED) for a queue by using the scheduler profile set queue ald profile command.

You can set the profile to work on a transport by using the transport set scheduler profile command.

Options

The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the profile. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
wf2qplus	WF2Q+ (***Worst Case Weighted Fair Queueing Plus***) service discipline. This service discipline distributes the link bandwidth among participating queues in ratio of their respective configured weights.	N/A

Option	Description	Default Value
priority	Priority Queueing provides prioritized treatment to higher priority traffic.	N/A

Example --> scheduler add profile prioschlr priority

See also SCHEDULER SHOW PROFILE

7.1.6.2.2 SCHEDULER CLEAR PROFILES

Syntax SCHEDULER CLEAR PROFILES

Description This command deletes all scheduler profiles that were previously created using the SCHEDULER ADD PROFILE command.

Example --> scheduler clear profiles

See also SCHEDULER ADD PROFILE

7.1.6.2.3 SCHEDULER DELETE PROFILE

Syntax SCHEDULER DELETE PROFILE <name>

Description This command deletes a single scheduler profile that was previously created using the SCHEDULER ADD PROFILE command.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the SCHEDULER LIST PROFILES command.	N/A

Example --> scheduler delete profile prioschlr

See also SCHEDULER ADD PROFILE
SCHEDULER LIST PROFILES

7.1.6.2.4 SCHEDULER LIST PROFILES

Syntax SCHEDULER LIST PROFILES

Description This command lists information about profiles previously created using THE SCHEDULER ADD PROFILE command. The following information is displayed:

- Profile ID number
- Profile name

Example --> scheduler list profiles

```
Scheduler Profiles:
 ID | Name
----|--------------
 1  | sch1
 2  | sch2
-------------------
```

See also SCHEDULER ADD PROFILE

7.1.6.2.5 SCHEDULER SET PROFILE SHAPING

Syntax SCHEDULER SET PROFILE <name> SHAPING <MaxRate> <MaxBurst>

Description This command configures the specified scheduler profile to shape aggregate traffic to the specified maximum rate and burst size.

To disable shaping, set <***MaxRate***> and <***MaxBurst***> values to 0 and apply the profile to the transport using the TRANSPORT SET SCHEDULER PROFILE command.

If scheduler is applied over an Ethernet interface, the padding and FCS are not taken into account. When applied over other types of interfaces, the extra bytes added by devices lower than scheduler may not be taken into account. For example, when configured over an ATM interface, the padding and trailer added by AAL5 are not taken into account.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the SCHEDULER LIST PROFILES command.	N/A
MaxRate	Maximum rate for outgoing traffic in kilobits per second (kbps).	N/A
MaxBurst	Maximum burst size value in bytes. This value should be greater than the MTU, otherwise the packets of greater size shall be dropped.	N/A

Example --> scheduler set profile prioschlr shaping 2000 10000

See also SCHEDULER LIST PROFILES
SCHEDULER SHOW PROFILE

7.1.6.2.6 SCHEDULER PROFILE SET QUEUE WEIGHT

Syntax SCHEDULER PROFILE <name> SET QUEUE [1-7] WEIGHT <weight>

Description This command configures a scheduler profile of WF2QPlus service discipline to configure a separate queue for a scheduling priority level with the specified weight value. The weight value is set as a percentage. The configured queue is identified by a ***queueid*** that is the same value as the scheduling priority value.

The weight value configured for a scheduling priority level determines the share of bandwidth received by packets belonging to the scheduling priority. A single queue with the weight set to 100% is configured by default when the profile is created using the scheduler add profile command. Packets with scheduling priority 0 are always enqueued in the default queue. You may configure weights for scheduling priority (1-7) using this command. If the weight for a scheduling priority level is configured, the corresponding packets are enqueued in a separate queue and the bandwidth is allocated in accordance with the configured weight. Otherwise, packets are enqueued in the default queue.

You cannot set the weight for the default queue directly. As you assign values to the other queues (1-7), the default queue weight is decreased by that amount. The sum total of weights of other queues cannot exceed 99%.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the SCHEDULER LIST PROFILES command.	N/A
1-7	The scheduling priority value or queue ID value. This can be any number between 1 and 7 (included).	N/A
weight	Weight value in percentage. You cannot set weight to more than 99 for a queue. In addition, the sum total of all weight values you configure cannot be more than 99. To display weight value for scheduler profile queues, use the SCHEDULER PROFILE SHOW QUEUES command.	N/A

Example --> scheduler profile prioschlr set shaping 2000 10000

See also SCHEDULER LIST PROFILES
SCHEDULER SHOW PROFILE

7.1.6.2.7 SCHEDULER PROFILE SET QUEUE ALD PROFILE

Syntax SCHEDULER PROFILE <name> SET QUEUE {DEFAULT | [1-7]} ALD PROFILE <GreenProfile> [<YellowProfile> <Red Profile>]

Description This command associates a scheduler profile queue with an ***Algorithmic Dropper*** (ALD) profile. ALD is a congestion control mechanism. The dropper associated with a particular scheduler profile decided at the time of packet enqueuing whether the packet should be enqueued in the queue or dropped. The ALD profile is created using the ald add profile command.

Each configured queue can have one of the following ALD algorithms associated with it:

- RED (***Random Early Detection***); applied if only one (green) ALD profile is configured.
- WRED (***Weighted RED***); treats packets differently depending on the drop priorities assigned to packets by the classifier profile set rule droppri command, or assigned by meter on the basis of metering results. Note that meter always sets the drop priority in the packet. Green is the lowest drop priority (0), yellow is the medium drop priority (1) and red is the highest drop priority (2). The WRED algorithm is applied if three ALD profiles (green, yellow and red; one for each drop priority) are configured.

Note: If the scheduler profile uses the WF2Q+ service discipline, the weight of the queue must be set to a non-zero value before you can associate an ALD profile. See SCHEDULER PROFILE SET QUEUE WEIGHT

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the SCHEDULER LIST PROFILES command.	N/A
default	The default priority value. See the SCHEDULER ADD PROFILE command description.	N/A

Option	Description	Default Value
1-7	The scheduling priority value or queue ID value (created using the SCHEDULER PROFILE SET QUEUE WEIGHT command) that you want to associate the ALD profile with. This can be any number between 1 and 7 (included).	N/A
GreenProfile	An existing ALD profile. This is the only profile required if the RED algorithm is used. If you are using the WRED algorithm, this ALD profile is applied to packets with green drop priority. To display ALD profiles, use the ALD LIST PROFILES command.	N/A
YellowProfile	An existing ALD profile. If you are using the WRED algorithm, this ALD profile is applied to packets with yellow drop priority. To display ALD profiles, use the ALD LIST PROFILES command.	N/A
RedProfile	An existing ALD profile. If you are using the WRED algorithm, this ALD profile is applied to packets with red drop priority. To display ALD profiles, use the ALD LIST PROFILES command.	N/A

Example --> scheduler profile prioschlr set queue 1 ald profile ald1

--> scheduler profile prioschlr set queue 1 ald profile ald1 ald2 ald3

See also SCHEDULER LIST PROFILES
SCHEDULER PROFILE SET QUEUE WEIGHT
METER SET PROFILE ACTION DROP

7.1.6.2.8 SCHEDULER PROFILE SET QUEUE ALD DISABLED

Syntax SCHEDULER PROFILE <name> SET QUEUE {DEFAULT | [1-7]} ALD DISABLED

Description This command disables the ***Algorithmic Dropper*** (ALD) on a specified scheduler profile queue.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the SCHEDULER LIST PROFILES command.	N/A
default	The default priority value. See the SCHEDULER ADD PROFILE command description.	N/A
1-7	The scheduling priority value or queue ID value (created using the SCHEDULER PROFILE SET QUEUE WEIGHT command) that the ALD profile is associated with. This can be any number between 1 and 7 (included).	N/A

Example --> scheduler profile prioschlr set queue 1 disabled

See also
```
SCHEDULER LIST PROFILES
SCHEDULER PROFILE SET QUEUE WEIGHT
SCHEDULER PROFILE SET QUEUE ALD PROFILE
METER SET PROFILE ACTION DROP
```

7.1.6.2.9 SCHEDULER SHOW PROFILE

Syntax `SCHEDULER SHOW PROFILE <name>`

Description This command displays the following information about an existing scheduler profile.

- Type of service discipline set
- Maximum Rate of traffic
- Maximum Burst Size (MBS) of traffic

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the SCHEDULER LIST PROFILES command.	N/A

Example --> scheduler show profile prioschlr

```
Type             : priority
MaxRate (kbps)   : 2000
MaxBurst (bytes) : 10000
```

See also SCHEDULER LIST PROFILES
SCHEDULER ADD PROFILE
SCHEDULER SET PROFILE SHAPING

7.1.6.2.10 SCHEDULER SHOW PROFILE QUEUES

Syntax SCHEDULER SHOW PROFILE <name> QUEUES

Description This command displays the following information about the queues of an existing scheduler profile.

- Queue ID number (0-7)
- Weight value (percentage)
- ALD Green Profile name
- ALD Yellow Profile name
- ALD Red Profile name

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing profile. To display names, use the SCHEDULER LIST PROFILES command.	N/A

Example --> scheduler show profile prioschlr show queues

```
Queues:
QueueId | Weight | ALD Green Profile | ALD Yellow Profile | ALD Red Profile
--------|--------|-------------------|--------------------|---------
 0      | 0      | ald1              |                    |
 1      | 0      | ald1              | ald2               | ald3
 2      | 0      |                   |                    |
 3      | 0      |                   |                    |
 4      | 0      |                   |                    |
 5      | 0      |                   |                    |
 6      | 0      |                   |                    |
 7      | 0      |                   |                    |
-----------------------------------------------------------------------
```

See also SCHEDULER LIST PROFILES
SCHEDULER ADD PROFILE
SCHEDULER PROFILE SET QUEUE WEIGHT
SCHEDULER PROFILE SET QUEUE ALD PROFILE

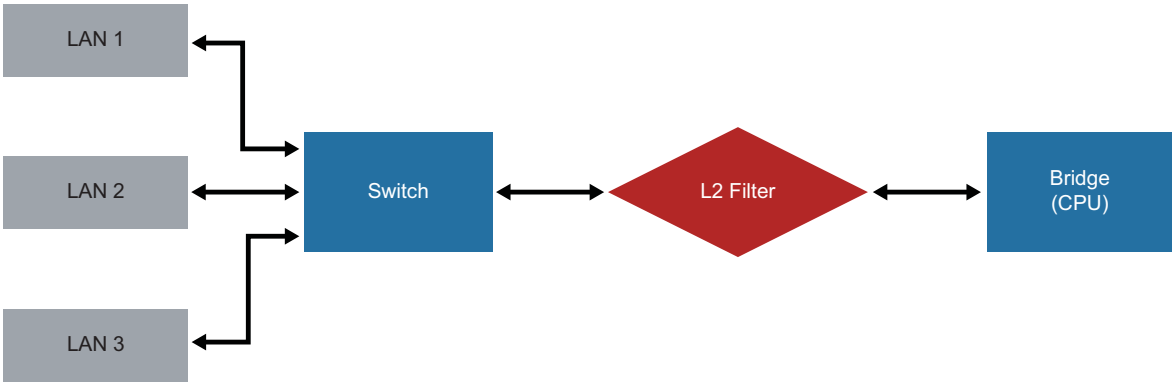
7.2 L2Filter

7.2.1 Overview

The purpose of the L2 Filter module is to provide a mechanism by which inbound traffic can be classified and acted upon based on its contents. The module is configured by defining a set of profiles which themselves contain a set of rules. Each rule defines a packet classification and the appropriate action to take in the event of a match. The actions vary from basic operations, such as DROP, to more complex actions such as packet rewriting. This mechanism provides a powerful and flexible framework for filtering of traffic in the system.

7.2.1.1 Packet Flow

In order to properly utilize the L2 Filter system, it is important to understand where this module falls in the general flow of a packet through the system.



The important item to note in the above diagram is that packets are only run through the L2 Filter module in the event they leave the layer 2 switch bound for the bridge. This occurs when the CPU requires access to the packet in order to read it, alter it or route it to another device in the system. Some examples of these scenarios are the following: NAT, VLAN translation, usage of the ADSL module, etc.

7.2.1.1.1 Profiles

The profile is the high level container of the L2 Filter system. The user creates a profile, assigns a series of rules to that profile and then attaches it to the bridge transport. Once the L2 Filter system is activated the packet flow, in the system, is run through the profiles and the appropriate rules are applied. Multiple profiles can be configured however only two can be applied to the bridge at any given time. You can assign one profile to each direction of packet flow from the bridge (Rx and Tx).

7.2.1.1.2 Rules

The rule is the workhorse of the L2 Filter system. A user defines a set of rules which contain one packet classifier and its associated action. The packet classifier is an offset / value pair that the filter uses to identify packets on which to apply a rule. Several of the basic classifier fields have been pre-defined for use however the user has the ability to define their own.

7.2.1.1.3 Example

The following is an example of how the L2 Filter module can be used to filter incoming and outgoing DHCP requests for VLAN 402 on the bridge.

Example

```
l2filter add fieldType udpDstPort base udp_header offset 2 mask 0xffff
l2filter add fieldType ipProtocol base ip_header offset 9 mask 0xff
l2filter add profile bridge_rx
l2filter add profile bridge_tx
l2filter add rule Vlan402DhcpServerRx
l2filter rule Vlan402DhcpServerRx add action drop
l2filter rule Vlan402DhcpServerRx add field udpDstPort EQ 67
l2filter rule Vlan402DhcpServerRx add field packetvid EQ 402
l2filter add rule Vlan402DhcpServerTx
l2filter rule Vlan402DhcpServerTx add action drop
l2filter rule Vlan402DhcpServerTx add field udpDstPort EQ 67
l2filter rule Vlan402DhcpServerTx add field packetvid EQ 402
l2filter profile bridge_rx attach rule Vlan402DhcpServerRx
l2filter profile bridge_tx attach rule Vlan402DhcpServerTx
transport attach default l2filter profile bridge_rx Rx
transport attach default l2filter profile bridge_tx Tx
transport set default l2filter state enabled
```

7.2.2 L2Filter Command Reference

7.2.2.1 L2 Filter CLI commands

The table below lists the ***l2filter*** commands provided by the CLI:

TABLE 7-4 L2filter commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
L2FILTER ADD FIELDTYPE		X		X	X	X	X	X	X

TABLE 7-4 L2filter commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
L2FILTER ADD PROFILE		X		X	X	X	X	X	X
L2FILTER ADD RULE		X		X	X	X	X	X	X
L2FILTER CLEAR FIELDTYPES		X		X	X	X	X	X	X
L2FILTER CLEAR PROFILES		X		X	X	X	X	X	X
L2FILTER CLEAR RULES		X		X	X	X	X	X	X
L2FILTER DELETE FIELDTYPE		X		X	X	X	X	X	X
L2FILTER DELETE RULE		X		X	X	X	X	X	X
L2FILTER DELETE PROFILE		X		X	X	X	X	X	X
L2FILTER LIST FIELDTYPES		X		X	X	X	X	X	X
L2FILTER LIST PROFILES		X		X	X	X	X	X	X
L2FILTER LIST RULES		X		X	X	X	X	X	X
L2FILTER SHOW PROFILE		X		X	X	X	X	X	X
L2FILTER SHOW RULE		X		X	X	X	X	X	X
L2FILTER SHOW FIELDTYPE		X		X	X	X	X	X	X
L2FILTER PROFILE ATTACH RULE		X		X	X	X	X	X	X
L2FILTER PROFILE DETACH RULE		X		X	X	X	X	X	X
L2FILTER RULE ADD ACTION		X		X	X	X	X	X	X
L2FILTER RULE ADD FIELD		X		X	X	X	X	X	X
L2FILTER RULE LIST ACTIONS		X		X	X	X	X	X	X
L2FILTER RULE LIST FIELDS		X		X	X	X	X	X	X
L2FILTER RULE DELETE ACTION		X		X	X	X	X	X	X
L2FILTER RULE DELETE FIELD		X		X	X	X	X	X	X
L2FILTER SET RULE ENABLE		X		X	X	X	X	X	X
L2FILTER SET RULE DISABLE		X		X	X	X	X	X	X

7.2.2.1.1 L2FILTER ADD FIELDTYPE

Syntax `L2FILTER ADD FIELDTYPE <name> BASE <base_value> OFFSET <offset_value> MASK <mask_value>`

Description This command allows the user to create their own filter field types.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the new field type	n/a
base_value	The location in the packet to offset from	n/a
offset_value	The offset distance from the base to compare	n/a
mask_value	The mask to apply at the offset	n/a

Example --> l2filter add fieldType test_field base ethernet_header offset 10 mask 0xf

See also `L2FILTER SHOW FIELDTYPE`

7.2.2.1.2 L2FILTER ADD PROFILE

Syntax `L2FILTER ADD PROFILE <name>`

Description This command adds a profile to the L2 filter module.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the rule	n/a

Example --> l2filter add profile InboundTraffic

See also `L2FILTER SHOW PROFILE`

7.2.2.1.3 L2FILTER ADD RULE

Syntax `L2FILTER ADD RULE <name> STAGE <stage> ORDER <order>`

Description This command adds a rule to the module that can be attached to a profile.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the rule	n/a
stage	The stage of processing in which this rule will be applied	1
order	The order in the stage when this rule will be applied	1

Example --> l2filter add rule TestRule stage 1 order 2

See also `L2FILTER SHOW RULE`

7.2.2.1.4 L2FILTER CLEAR FIELDTYPES

Syntax `L2FILTER CLEAR FIELDTYPES`

Description This command will clear all the available field types from the system.

Example --> l2filter clear fieldtypes

See also `L2FILTER LIST FIELDTYPES`

7.2.2.1.5 L2FILTER CLEAR PROFILES

Syntax `L2FILTER CLEAR PROFILES`

Description This command will clear all the available profiles from the system.

Example --> l2filter clear profiles

See also `L2FILTER LIST PROFILES`

7.2.2.1.6 L2FILTER CLEAR RULES

Syntax `L2FILTER CLEAR RULES`

Description This command will clear the available rules from the system.

Example --> l2filter clear rules

See also `L2FILTER LIST RULES`

7.2.2.1.7 L2FILTER DELETE FIELDTYPE

Syntax `L2FILTER DELETE FIELDTYPE <name>`

Description This command deletes the specified fieldtype from the system.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the field to be deleted	n/a

Example --> l2filter delete fieldtype TestFieldType

See also `L2FILTER LIST FIELDTYPES`
`L2FILTER ADD FIELDTYPE`

7.2.2.1.8 L2FILTER DELETE RULE

Syntax `L2FILTER DELETE RULE <name>`

Description This command deletes the specified rule from the system.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the rule to be deleted	n/a

Example --> l2filter delete rule TestRule

See also `L2FILTER LIST RULES`
`L2FILTER ADD RULE`

7.2.2.1.9 L2FILTER DELETE PROFILE

Syntax `L2FILTER DELETE PROFILE <name>`

Description This command deletes the specified profile from the system.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the profile to be deleted	n/a

Example --> l2filter delete profile TestProfile

See also `L2FILTER LIST PROFILES`
`L2FILTER ADD PROFILE`

7.2.2.1.10 L2FILTER LIST FIELDTYPES

Syntax `L2FILTER LIST FIELDTYPES`

Description This command lists the available field types in the system. The system creates a default set of fields at boot time.

Example --> l2filter list fieldtypes

See also `L2FILTER SHOW FIELDTYPE`
`L2FILTER ADD FIELDTYPE`
`L2FILTER DELETE FIELDTYPE`

7.2.2.1.11 L2FILTER LIST PROFILES

Syntax `L2FILTER LIST PROFILES`

Description This command lists the available profiles in the system.

Example --> l2filter list profiles

See also `L2FILTER SHOW PROFILE`
`L2FILTER ADD PROFILE`
`L2FILTER DELETE PROFILE`

7.2.2.1.12 L2FILTER LIST RULES

Syntax `L2FILTER LIST RULES`

Description This command lists the available rules in the system and basic information about each one.

Example --> l2filter list rules

See also `L2FILTER SHOW RULE`
`L2FILTER ADD RULE`
`L2FILTER DELETE RULE`

7.2.2.1.13 L2FILTER SHOW PROFILE

Syntax `L2FILTER SHOW PROFILE <name>`

Description This command displays information about the specified profile. This information includes which rules the profile will attempt to match.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the field to display	n/a

Example --> l2filter show profile TestProfile

See also `L2FILTER ADD PROFILE`
`L2FILTER DELETE PROFILE`

7.2.2.1.14 L2FILTER SHOW RULE

Syntax `L2FILTER SHOW RULE <name>`

Description This command displays information about the specified rule. This information includes the rule's ordering and its enabled state.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the rule to display	n/a

Example --> l2filter show rule TestRule

See also `L2FILTER ADD RULE`
`L2FILTER DELETE RULE`

7.2.2.1.15 L2FILTER SHOW FIELDTYPE

Syntax `L2FILTER SHOW FIELDTYPE <name>`

Description This command displays information about the specified field type. This information includes the base, offset and mask values.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the field to display	n/a

Example --> l2filter show fieldtype TestFieldType

See also `L2FILTER ADD FIELDTYPE`
`L2FITLER DELETE FIELDTYPE`

7.2.2.1.16 L2FILTER PROFILE ATTACH RULE

Syntax `L2FILTER PROFILE <profile_name> ATTACH RULE <rule_name>`

Description This command associates a given rule with a specified profile.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
profile_name	The name of the profile in which to associate the rule	n/a
rule_name	The name of the rule to associate with the profile	n/a

Example --> l2filter profile TestProfile attach rule TestRule

See also `L2FILTER ADD RULE`
`L2FILTER ADD PROFILE`

7.2.2.1.17 L2FILTER PROFILE DETACH RULE

Syntax `L2FILTER PROFILE <profile_name> DETACH RULE <rule_name>`

Description This command removes a given rule from the specified profile.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
profile_name	The name of the profile from which we want to remove the rule	n/a
rule_name	The name of the rule to remove from the profile	n/a

Example --> l2filter profile TestProfile detach rule TestRule

See also `L2FILTER DELETE RULE`
`L2FILTER DELETE PROFILE`

7.2.2.1.18 L2FILTER RULE ADD ACTION

Syntax `L2FILTER RULE <rule_name> ADD ACTION <action_type> VALUE <action_data>`

Description This command adds an action to the specified rule.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
rule_name	The name of the in which to add the action	n/a

Option	Description	Default Value
action_type	The action that should be performed. The available actions are the following: drop allow_packet dump_packet mark_dscp mark_8021p mark_vlan untag_packet jump_stage mark_sch mark_meter mark_drop	n/a
action_data	Additional data that may be required to perform the function specified by the action	0

Example --> l2filter rule TestRule add action mark_vlan value 1234

See also `L2FILTER ADD RULE`

7.2.2.1.19 L2FILTER RULE ADD FIELD

Syntax `L2FILTER RULE <rule_name> ADD FIELD <field_name> <operation> <val1> VALUE2 <val2>`

Description This command adds the specified field to the rule. The arguments for the field specifiy the conditions of how the field should be tested.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
rule_name	The name of the to which the field should be added	n/a
field_name	The name of the field type to be added	n/a

Option	Description	Default Value
operation	The type of operation that should be used for the test. The available tests are the following: • GT • LT • GTEQ • LTEQ • EQ • NEQ • INRANGE • EXRANGE	0
val1	The first argument to be used in the test	0
val2	The second argument to be used in the test	0

Example --> l2filter rule TestRule add field TestField INRANGE 1 value2 10

See also `L2FILTER ADD RULE`
`L2FILTER ADD FIELDTYPE`

7.2.2.1.20 L2FILTER RULE LIST ACTIONS

Syntax `L2FILTER RULE <name> LIST ACTIONS`

Description This command lists the actions associated with the specified rule.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the rule to display actions	n/a

Example --> l2filter rule TestRule list actions

See also `L2FILTER ADD RULE`
`L2FILTER RULE ADD ACTION`
`L2FILTER RULE DELETE ACTION`

7.2.2.1.21 L2FILTER RULE LIST FIELDS

Syntax `L2FILTER RULE <name> LIST FIELDS`

Description This command lists all the fields associated with the specified rule.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	The name of the rule to display the fields	n/a

Example --> l2filter rule TestRule list fields

See also
`L2FILTER ADD RULE`
`L2FILTER RULE ADD FIELD`
`L2FILTER RULE DELETE FIELD`

7.2.2.1.22 L2FILTER RULE DELETE ACTION

Syntax `L2FILTER RULE <rule_name> DELETE ACTION <action_type>`

Description This command deletes the specified action from the given rule.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
rule_name	The name of the rule from which to delete the action	n/a
action_type	The action that should be deleted. The available actions are the following: drop allow_packet dump_packet mark_dscp mark_8021p mark_vlan untag_packet jump_stage mark_sch mark_meter mark_drop	n/a

Example --> l2filter rule TestRule delete action drop

See also `L2FILTER ADD RULE`
`L2FILTER RULE ADD ACTION`

7.2.2.1.23 L2FILTER RULE DELETE FIELD

Syntax `L2FILTER RULE <rule_name> DELETE FIELD <field_name>`

Description This command deletes the specified field from the given rule.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
rule_name	The rule from which to delete the field	n/a
field_name	The name of the field to delete from the rule	n/a

Example --> l2filter rule TestRule delete field destMAC

See also `L2FILTER ADD RULE`
`L2FILTER RULE ADD FIELD`

7.2.2.1.24 L2FILTER SET RULE ENABLE

Syntax `L2FILTER SET RULE <rule_name> ENABLE`

Description This command enables a rule in the system.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
field_name	The name of the rule to enable	n/a

Example --> l2filter set rule TestRule enable

See also `L2FILTER ADD RULE`

7.2.2.1.25 L2FILTER SET RULE DISABLE

Syntax `L2FILTER SET RULE <rule_name> DISABLE`

Description This command disables a rule in the system.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
rule_name	The name of the rule to disable	n/a

Example --> l2filter set rule TestRule disable

See also `L2FILTER ADD RULE`

8. ADSL Port

8.1 Overview

8.1.1 ADSL upload interface

The Allied Telesis Gateway product provide an ADSL access to WAN Network, this interface is commonly called upload interface. This chapter will describe the interaction between the ADSL physical port **a1** and the TCP/IP stack of the system using different kind of transport layer.

8.1.2 Documentation Structure

After a brief description of the ADSL module and its interaction with other modules of the system all the CLI (command line interface) commands will be described to allow a correct configuration of all the parameters available configuring an ADSL Allied Media Gateway product.

We will start from a description of the physical ADSL port a1 and its parameters and all possible setting in accord with any DSLAM access device. Then, following the main indication of network topology after some example of configuration there will be a complete and exhaustive description of all CLI command available on Allied Telesis Media Gateway.

8.2 ADSL System description

8.2.1 Overview

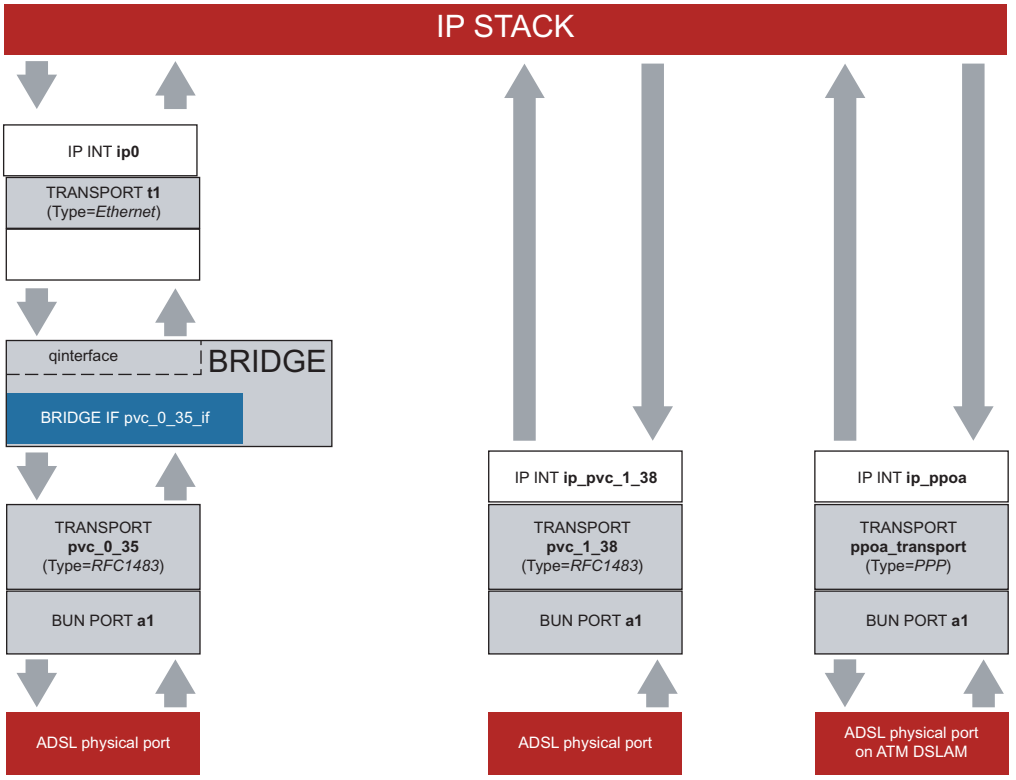


FIGURE 8-1 ADSL upload interface module

The ADSL port of a Media Gateway can be connected both to an Ethernet DSLAM or to an ATM DSLAM, observing the figure the connection between the ADSL port and the TCP/IP stack would be done via rfc1483 encapsulation transport in case of an Ethernet DSLAM while will be done using a Point to Point Protocol transport in case of a connection to an ATM DSLAM.

8.2.2 ADSL connection via RFC1483 bridged mode

In order to allow the management of the VLAN directly from the Allied Media Gateway using only one ADSL PVC (permanent virtual circuit) it is possible to set up an RFC1483 transport attached to the ATI Bridge module; ATI Bridge module provides support for virtual VLAN creating a domain, one for each VLAN, in which RFC1483 bridged transport can carry on frames tagged for each different domain on the Bridge that will correspond to different VLAN the Bridge module provide also standard interfaces for attachment to the system

TCP/IP Stack allowing the termination of IP frames belonging to a specific VLAN to a well defined IP interface (see proper chapter of this manual for further information about ATI Bridge module).

Example

#Typical set up for ADSL B and ADSL C group of devices
#Create a vlan with vid 666 and name vlan666
-->vlan create vlan666 666
#Create rfc1483 transport with VPI/VCI: 1/34
-->rfc1483 add transport pvc_1_34 a1 1 34
#Create a bridge interface
-->bridge add interface pvc_1_34_if
#Attach the bridge interface to the bridge
-->bridge attach pvc_1_34_if pvc_1_34
#Put the interface in the correct vlan on the bridge
-->bridge add vlaninterface vlan666 untagged pvc_1_34_if
#Create IP interface
-->ip add interface ip666
#Attach rfc1483 transport to the defined IP interface
-->ip attach ip666 vlan666
#Set a static IP address on the IP interface
-->ip set interface ip666 ipaddress 192.168.99.1 255.255.255.0

See also

`vlan (chapter 2-Layer 2 functions)`
`rfc1483 (chapter 7-ADSL Port)`
`bridge (chapter 7-ADSL Port)`
`ip (chapter 2-Layer 2 functions)`

Example

#Typical set up for ADSL A group of devices
#Create a vlan with vid 666 and name vlan666
-->vlan add vlan666 vid 666
#Add ethernet transport type named vlan666
-->ethernet add transport vlan666
#Create rfc1483 transport with VPI/VCI: 1/34
-->rfc1483 add transport pvc_1_34 a1 1 34
set transport to manage frame untagged on vlan666
-->rfc1483 set transport pvc_1_34 vlan vlan666 frame untagged
#Create BRIDGE interface and attach to the transport
bridge add interface pvc_1_34_if
bridge attach pvc_1_34_if pvc_1_34
#Create IP interface
-->ip add interface ip666
#Attach rfc1483 transport to the defined IP interface
-->ip attach ip666 vlan666

```
#Set a static IP address on the IP interface
-->ip set interface ip666 ipaddress 192.168.99.1 255.255.255.0
```

See also `vlan (chapter 2-Layer 2 functions)`
`ethernet (chapter 7-ADSL Port)`
`rfc1483 (chapter 7-ADSL Port)`
`bridge (chapter 7-ADSL Port)`
`ip (chapter 2-Layer 2 functions)`

8.2.3 ADSL connection via RFC1483 routed mode

When it is not necessary to make ATI media gateway manage virtual vlans but it is preferable to leave the Ethernet DSLAM manages directly one or more IP interfaces on different ADSL permanent virtual circuit then the connection between the physical adsl port and the TCP/IP stack will be done using directly a transport of type RFC1483 since not using ATI Bridge it will be routed directly to the ADSL port

This approach let the Ethernet DSLAM to manage a multiple ADSL PVC connection and multiple vlan network.

Example

```
#Typical set up for all ADSL group of devices
#Create rfc1483 transport with VPI/VCI: 1/34
-->rfc1483 add transport pvc_1_34 a1 1 34
#Create IP interface
-->ip add interface ip666
#Attach rfc1483 transport to the defined IP interface
-->ip attach ip666 pvc_1_34
#Set a static IP address on the IP interface
-->ip set interface ip666 ipaddress 192.168.99.1 255.255.255.0
```

See also `rfc1483 (chapter 7-ADSL Port)`
`ip (chapter 2-Layer 2 functions)`

8.2.4 ADSL connection via Point to Point Protocol over ATM (PPPOA)

To maintain the compatibility with old type of network topography it is possible to set up a connection between Allied Telesis media gateway TCP/IP stack and an ATM DSLAM using a Point to Point Protocol connection transport over ATM cells.

Example

```
#Typical set up for all ADSL group of devices
#Create PPPoA transport with VPI/VCI: 8/35
-->pppoa add transport trpppoa dialout pvc 2 a1 8 35
#Create IP interface
-->ip add interface ip_pppoa
#Attach PPPoA transport to the defined IP interface
-->ip attach ip_pppoa trpppoa
# Set PPPoA account parameters
-->pppoa set transport trpppoa username <username>
```

```
-->pppoa set transport trpppoa password <password>
-->pppoa set transport trpppoa welogin auto
-->pppoa set transport trpppoa headers llc enabled
-->pppoa set transport trpppoa enable
```

See also `rfc1483 (chapter 7-ADSL Port)`
`pppoa (chapter 7-ADSL Port)`
`ip (chapter 2-Layer 2 functions)`

8.3 Port a1

The following chapter describes all the ADSL port available parameters. Note the ADSL port is physically identified in the system with the name *a1*.

Under the Port command section it's also possible display other ports (ethernet0, bunbridge, tel1 tel2, etc). Some of these ports are real physical ports while others are virtual ports used by software modules as logical ports.

Only ADSL a1 port is described in this section.

8.3.1 Port a1 command reference

8.3.1.1 Port a1 CLI commands

This chapter describes the ***Port a1*** commands provided by the CLI:

TABLE 8-1 Port a1 Commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PORT LIST							X	X	X
PORT A1 SET							X	X	X
PORT A1 SHOW							X	X	X
PORT A1 STATUS							X	X	X

8.3.1.1.1 PORT LIST

Syntax `PORT LIST ? | <port class>`

Description The `PORT LIST ?` command lists all possible types of port and their port classes. THE `PORT LIST <port class>` command allows you to display the port names that belong to a specific class.

Options The following table gives the range of values for each option <port class> that can be specified with this command and a default value (if applicable).

Example --> port list ?

Option	Description	Default Value
all	all port classes available, classes meaning a grouping of software device driver to manage different media type of protocols, i.s. atm for ADSL ethernet for 802.1x frames or wireless for wireless connection	N/A
atm	class which contains port a1, software device driver elected to manage ATM cells.	N/A
ethernet	class which contain any port that manages 802.x frames	N/A
802_1x	for wireless devices this class contain the port to manage wireless frames on Bridge layer	N/A
802_11	for wireless devices this class contain the port to manage wireless frames on switch layer	
vca	not supported	N/A

See also
```
all              Port class
atm              Port class
ethernet         Port class
vca             Port class
```

Example --> port list atm

Valid port names in class 'atm':
a1

See also
```
PORT A1 SET
PORT A1 SHOW
PORT A1 STATUS
```

8.3.1.1.2 PORT A1 SET

Syntax `PORT A1 SET <option> <value>`

Description This command allows you to modify attributes on the ADSL port. Any modifications override existing attribute values specified in the device. Typically it's necessary to save the changes with the `SYSTEM CONFIG CREATE` command and restart the Allied Telesis Media Gateway in order to activate the changes.

To display a list of valid attributes for the ADSL port, use the `PORT A1 SHOW` or `PORT A1 STATUS` command.

Options

The following table gives the range of values for each attribute option that can be specified with this command and a default value (if applicable).

TABLE 8-2 Options for ADSL Port Attributes

Option	Description	Default Value
Action	Startup Possible values are: Startup DELT L3REQ SpectrumReverb SpectrumMedely SpectrumPilot MtsRequest	Startup
ActivateLine	Force the ADSL port to close or restart the link. Possible values are: abort: turn off the ADSL port none: no action start: turn on the ADSL port	none
AnnexABitSwap AnnexBBitSwap	ONLY Group B devices. Downstream BitSwap for AnnexA/AnnexB. Possible values are: enable disable	Enable
AnnexABitSwapUp AnnexBBitSwapUp	ONLY Group B devices. Downsteam BitSwap Upstream for AnnexA/ annexB. Possible values are: enable disable	Enable

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
AnnexACapability AnnexBCapability	ONLY Group B devices. Supported AnnexA/annexB capabilities. Possible values are: AnnexA/AnnexB T1413/T1413B {AnnexA/T1413}{AnnexB/T1413B} disable: line will not try to come in AnnexA/ AnnexB	AnnexA/T1413 AnnexB/T1413B
AnnexACodingGain AnnexBCodingGain	ONLY Group B devices Configures the Coding Gain in AnnexA/B Possible values are: auto, 0, 1, 2, 3, 4, 5, 6, 7	auto
AnnexAEcFdm-Mode AnnexBEcFdmMode	ONLY Group B devices Configures Ec/Fdm Mode for AnnexA/B Possible values are: EC, FDM	FDM
AnnexAFastRetrain AnnexBFastRetrain	ONLY Group B devices Configures Fast Retrain on the Line for AnnexA/ B. Possible values are: Enable, Disable	Enable
AnnexAForceSNR-MarginDn	Group B devices ONLY AnnexA Parameter to set downstream SNR margin force-fully at the CPE for AnnexA. Possible values are: [0, 0x136] or 0xFFFF	0xFFFF

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
AnnexAFramerType AnnexBFramerType	ONLY Group B devices Configures the Framer Type for AnnexA/B. There are five different types of framing structures: Type0: Full overhead framing with asynchronous bit-to-modem timing. Type1: Full overhead framing with synchronous bit-to-modem timing. Type2: Reduced overhead framing with separate fast and sync byte in fast and interleaved latency buffer respectively. Type3: Reduced overhead framing with merged fast and sync byte, using either the fast or the interleaved latency buffer. Type3ET: It refers to Databoost(CNXT proprietary, b/w CNXT CO & CNXT CPE) enabled on top Possible values are: Type0, Type1, Type2, Type3, Type3ET	Type3
AnnexAMax-BitsPerBin AnnexBMax-BitsPerBin	ONLY Group B devices Configures Maximum Bits per Bin for AnnexA/B Possible values are: [0, 15]	15
AnnexAMaxDown-Rate AnnexBMaxDown-Rate	ONLY Group B devices Configures the Maximum Down Rate for AnnexA/B	255 (AnnexA) 4095 (AnnexB)
AnnexAMaxMargin AnnexBMaxMargin	ONLY Group B devices Configures Maximum SNR Margin for AnnexA/B Possible values are: PerCO, Disable	PerCO
AnnexANTRMode AnnexBNTRMode	ONLY Group B devices Possible values are: Enable, Disable	Disable

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
AnnexAQualificationMode AnnexBQualificationMode	ONLY Group B devices Configures Qualification mode for AnnexA/B. This parameter is mainly used for Qualifications and internal test/debugging. Possible values are: Mode0, Mode1, Mode2,Mode3, Mode4, Mode5	mode1
AnnexARxAutoBinAdjust AnnexBRxAutoBinAdjust	ONLY Group B devices Possible values are: Enable, Disable	Disable
AnnexARxEndBin AnnexBRxEndBin	ONLY Group B devices Configures Rx End Bin for AnnexA/B Possible values are:	255
AnnexARxStartBin AnnexBRxStartBin	ONLY Group B devices Configures Rx StartBin for AnnexA/B	32 (AnnexA) 64 (AnnexB)
AnnexAStandard AnnexBStandard	ONLY Group B devices No longer considered.	
AnnexATxAttenuation AnnexBTxAttenuation	ONLY Group B devices Configures Tx Attenuation for AnnexA/B	0
AnnexATxEndBin AnnexBTxEndBin	ONLY Group B devices Configures Tx End Bin for AnnexA/B	31 (AnnexA) 63 (AnnexB)
AnnexATxStartBin AnnexBTxStartBin	ONLY Group B devices Configures Tx StartBin for AnnexA/B	6 (AnnexA) 33 (AnnexB)
AutoSRA	Group A, B and C devices ONLY AnnexB Possible values are: Enable, Disable	Disable
AutoSRADnShiftPeriod	Group A and group C devices ONLY AnnexB	
AutoSRAMaxTimeCRC	Group A and group C devices ONLY AnnexB	

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
AutoSRAMaxTime-FEC	Group A and group C devices ONLY AnnexB	
AutoSRAUpShiftPe-riod	Group A and group C devices ONLY AnnexB	
AutoStart	Flag indicating whether the Line should be auto started or not when the system comes up. Possible values are: true: a connection will be established at power up false: ADSL port a1 will remain in *idle* mode at power up	true
BisABitSwap BisBBitSwap BisMBitSwap	ONLY Group B devices To Enable/Disable Downsteam BitSwap for Bis/Bis+ Possible values are: Disable, Enable	Enable
BisABitSwapUp BisBBitSwapUp BisMBitSwapUp	ONLY Group B devices To Enable/Disable Upsteam BitSwap for Bis/Bis+ Possible values are: Disable, Enable	Enable
BisACabinetMode BisBCabinetMode BisMCabinetMode	ONLY Group B devices Sets the Cabinet Mode for Bis/Bis+ Possible values are: Disable, Enable	Enable (BisA/B) Disable (BisM)
BisACapability BisBCapability BisMCapability	ONLY Group B devices Supported A2/A2 capabilities for A2/A2+.. If Disabled line will not try to come in Bis/Bis+ Possible values are: {A2, A2L, A2+, A2/A2+} (BisA) OR {M2, M2+, M2+/M2} (BisM) OR {B2, B2+, B2+/B2} (BisB) AND Disable	A2/A2+ (BisA) M2+/M2 (BisM) B2/B2+ (BisB)

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
BisACodingGain BisBCodingGain BisMCodingGain	ONLY Group B devices Configures the Coding Gain in Bis/Bis Possible values are: auto, 0, 1, 2, 3, 4, 5, 6, 7	auto
BisADsInp BisBDsInp BisMDsInp	ONLY Group B devices Possible values are: MinPossible, NextPossible,MaxPossible	MinPossible
BisAEcFdmMode BisBEcFdmMode BisMEcFdmMode	ONLY Group B devices Configures Ec/Fdm Mode for Bis/Bis+ Possible values are: EC, FDM	EC (BisA/M) FDM (BisB)
BisAFastRetrain BisBFastRetrain BisMFastRetrain	ONLY Group B devices Configures Fast Retrain on the Line for Bis/Bis+ Possible values are: Disable, Enable	Disable (BisA/B) Enable (BisM)
BisAForceSNRMarginDn BisBForceSNRMarginDn BisMForceSNRMarginDn	ONLY Group B devices Parameter to set downstream SNR margin forcefully at the CPE for Bis/Bis+ Possible values are: [0, 0x136] or 0xFFFF	0xFFFF

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
BisAFramerType BisBFramerType BisMFramerType	ONLY Group B devices Configures the Framer Type for Bis/Bis+. There are five different types of framing structures: Type0: Full overhead framing with asynchronous bit-to-modem timing. Type1: Full overhead framing with synchronous bit-to-modem timing. Type2: Reduced overhead framing with separate fast and sync byte in fast and interleaved latency buffer respectively. Type3: Reduced overhead framing with merged fast and sync byte, using either the fast or the interleaved latency buffer. Type3ET: It refers to Databoost (CNXT proprietary, b/w CNXT CO & CNXT CPE) enabled on top of framing mode - 3. Possible values are: Type0, Type1, Type2, Type3,Type3ET	Type3ET
BisAMaxBitsPerBin BisBMaxBitsPerBin BisMMaxBitsPerBin	ONLY Group B devices Configures Maximum Bit per Bin for Bis/Bis+	15
BisAMaxDownRate BisBMaxDownRate BisMMaxDownRate	ONLY Group B devices Configures the Maximum Down Rate for Bis/Bis+	511
BisAMaxInterleaveD BisBMaxInterleaveD BisMMaxInterleaveD	ONLY Group B devices Sets the Max interleaved Depth for Bis/Bis+. Possible values are: 64, 128, 256, 512	511

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
BisAMaxMargin BisBMaxMargin BisMMaxMargin	ONLY Group B devices Configures Maximum SNR Margin for Bis/Bis+ Possible values are: PerCO, Disable	PerCO
BisAMaxSInverse BisBMaxSInverse BisMMaxSInverse	ONLY Group B devices Limits the number of Code words in a DMT Symbol, configured for Bis/Bis+ Possible values are: 0x02, 0x03, 0x04, 0x05, 0x06,0x07, 0x08, 0x09, 0x0A,0x0B, 0x0C, 0x0D, 0x0E,0x0F, 0x10	0x10
BisANTRMode BisBNTRMode BisMNTRMode	ONLY Group B devices Possible values are: Disable, Enable	Disable
BisAPSDMask BisBPSDMask BisMPSDMask	ONLY Group B devices PSD Mask for Bis/Bis+ Possible values are: Standard, NonOvlp-M1,NonOvlp-M2, NonOvlp-M1M2,NonOvlp-Flat, ALL	NonOvlp-M1 (BisA/B) ALL (BisM)
BisAPrecedence BisBPrecedence BisMPrecedence	ONLY Group B devices Sets the Precedence to DSInp/RSDelay for Bis/Bis+. DSInp: This setting will maximize the rates, i.e. during calculation the delay is minimized to achieve better rates. RSDelay: This setting gives precedence to the delay value, i.e. it will result in a relatively larger delay as compared to the above setting, thus resulting in a slightly better INP value and may be slightly lowerrates. Possible values are: DSInp, RSDelay	DSInp

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
BisAQualification-Mode BisBQualification-Mode BisMQualification-Mode	ONLY Group B devices Configures Qualification mode for Bis/Bis+ Possible values are: Mode0, Mode1, Mode2, Mode3, Mode4, Mode5	Mode1
BisARxAutoBinAd-just BisBRxAutoBinAd-just BisMRxAutoBinAd-just	ONLY Group B devices Possible values are: Disable, Enable	Disable
BisARxEndBin BisBRxEndBin BisMRxEndBin	ONLY Group B devices Configures Rx End Bin for Bis/Bis+	511
BisARxStartBin BisBRxStartBin BisMRxStartBin	ONLY Group B devices Configures Rx Start Bin for Bis/Bis+	6 (BisA/M) 64 (BisB)
BisASHalf BisBSHalf BisMSHalf	ONLY Group B devices Enable/Disable SHalf Feature on Bis/Bis+. Possible values are: Disable, Enable	Disable
BisAStandard BisBStandard BisMStandard	ONLY Group B devices No longer considered in Solos family.	
BisATxAttenuation BisBTxAttenuation BisMTxAttenuation	ONLY Group B devices Configures Tx Attenuation for Bis/Bis+ Possible values are: Dmt_0DB,Dmt_0.1DB to Dmt_0.9DB to Dmt_1DB to Dmt_12DB, Bis_0DB, Bis_0.1DB to Bis_0.9DB, Bis_13DB to Bis_40DB	Bis_0DB

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
BisATxEndBin BisBTxEndBin BisMTxEndBin	ONLY Group B devices Configures Tx End Bin for Bis/Bis+	31 (BisA) 63 (BisM/B)
BisATxStartBin BisBTxStartBin BisMTxStartBin	ONLY Group B devices Configures Rx Start Bin for Bis/Bis+	6 (BisA/M) 64 (BisB)
BisA_PMmode BisB_PMmode BisM_PMmode	ONLY Group B devices Parameter controls which Power Management modes are to be supported on Bis/Bis+ Possible values are: L2L3NotAllowed, L3NotAllowed, L2L3Allowed	L2L3Allowed
BisA_REIN BisB_REIN BisM_REIN	ONLY Group B devices Possible values are: Per_CO_Request, 60pps,120pps	60pps
BisA_SRA BisB_SRA BisM_SRA	ONLY Group B devices Enables/Disables the Downstream SRA feature on Bis/Bis+ Possible values are: Disable, Enable	Enable
BitSwap	Group A and Group C devices Enable/Disable downstream bit swapping. Possible values are: enable, disable	Enable
BitSwapUp	Group A and Group C devices To Enable/Disable Downstream BitSwap for AnnexA/B	Enable

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
Capability	Group A and Group C devices This parameter controls if the CPE will attempt to startup using alternate standards, dependent upon CO capability. Possible values are for AnnexA: GDMT, BIS, BIS+, BIS+/GDMT, BIS+/T1413, BIS+/BIS, BIS+/BIS/T1413, BIS+/BIS/GDMT, A-ALL, MBIS, MBIS+, MBIS+/MBIS, MA-ALL, BIS+/BIS/A/MULTIMODE, Disable. Possible values are for AnnexB: BIS+/BIS/B, Disable	MA-ALL (AnnexA)
ClockType	Configures the Clock Type to Crystal/Oscillator	Crystal
CodeType	Group A and Group C devices	
CodingGain	Group A and Group C devices Coding gain is the reduction in transmit power realized by implementing trellis/RS coding techniques. Automatic coding gain selection is recommended for automatic bit allocation depending upon line conditions. Otherwise, requested coding gain is selectable from 0 dB to 7 dB in 1 dB increments.	N/A
CabinetMode	Group A and Group C devices	
DSPTrace	ONLY Group B devices This option allows to start logging of the DSP Trace to a file. Possible values are: StopLogging, StartLogging	StopLogging

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
Defaults	Group B devices: Option to assign defaults to all the parameters. Possible values are: None, All Group A and C devices: Set default parameters based on the standard selected. Possible values are: None, ADSL2, ADSL2PlusAuto, ADSL2PlusOnly, AnnexA, AnnexM2, AnnexM2PlusAutoAnnexM2PlusOnly, AnnexB, AnnexB2, AnnexB2PlusAuto, AnnexB2PlusOnly	None
DetectNoise	Enables and Disables Detect Noise	Disable
DyingGasp	Enable or Disable the DyingGasp support	Disable
EcFdmMode	Group A and Group C devices Depending upon which mode is required by your service provider, overlap of bins (Echo Cancellation) may be selected by the value EC. Likewise, if you should deploy no overlap (Frequency Division Multiplexing) the value FDM may be selected. Possible values are: EC,FDM	FDM
FastRetrain	Group A and Group C devices Configures Fast Retrain on the Line for AnnexA/B. Possible values are: Enable, Disable	Disable

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
FramerType	Group A and Group C devices There are two types of framing defined per T1.413: full overhead and reduced overhead. Each type has 2 versions thus resulting in four framing structures referred to as 0, 1, 2, and 3. These framing structures are described in Table 4 of T1.413. Framing type 3 should be used for single latency applications. When using dual latency, framing type 2 should be selected. Possible values are: Type0, Type1, Type2, Type3,Type3ET for Data boost	Type3ET
GenericTrace	ONLY Group B devices Configure the GenX trace(SAS/DSP). Possible values are: Disable, EnableAll, DSP, SAS	DSP
HappyMode	Group A and Group C devices Possible values are: Disable, Enable	Enable
HostControl	Enable/Disable Flag to control host. Possible values are: Disable, Enable	Enable
LoopbackTest	ONLY Group B devices Parameter to set and test the Loopback assigned. Possible values are: DAC/ADC Lpbk MTS, TX/RX Baseline MTS, Hybrid Resp Lpbk MTS, TX Filter Lpbk MTS, RX Filter Lpbk MTS, MTPR Lpbk MTS, Quiet Line PSD MTS	
MaxBitsPerBin	Group A and Group C devices Set the maximum number of receive bits per bin can be selected. Possible values are: 0 to 15	15

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
MaxDownRate	Group A and Group C devices Set the maximum downstream rate in bits per seconds	511
MaxInterleaveD	Group A and Group C devices Sets the Max interleaved Depth Possible values are: 64, 128, 256, 511	511
MaxRSMemory	ONLY Group B devices Configures the Size of RS Memory Possible values are: 16, 24, 32, 48	32
MaxSNRMargin	Group A and Group C devices SNR Margin Possible values are: Enable, Disable	Disable
MemorizedConnec-tion	Group A and Group C devices Possible values are: Enable, Disable	Disable
NTRMode	Group A and Group C devices	
PMmode	Possible values are: L2L3NotAllowed, L3NotAllowed, L2L3Allowed	L2L3Allowed
PSDMask	Group A and Group C devices	
PhysicalPort	Physical port of the PCU that is to be used for Data transfer.	0
Profile	Configures the Profile to be used Possible values are: MAIN, BT, SPAIN, SBC, COVAD, BRAZIL, MII, KT, TELSTRA, XR, HAN, FRANCE, FINLANDa, FASTWEB, RESERVED	MAIN

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
Retrain	Enable/disable the automatic full retrain Capability. If enabled, the unit will automatically monitor the following statistics and attempt a full retrain when the following conditions occur: OverallFailure status has a non-zero value. This indicates that one or more failures have occurred for 2.25 seconds or more. CRC error rate exceeds 40 per second for 10 consecutive second Possible values are: EnableAll, EnableOverallOnly, EnableCrcMinuteOnly, Disable	EnableOverallOnly
RxAutoBinAdjust	Group A and Group C devices Automatic bin adjustment can be enabled or disabled Possible values are: enable: automatically adjusts bin numbers - bin limitations specified by RxStartBin and RxEndBin options are ignored disable: limitations specified by RxStartBin and RxEndBin options are used.	Disable
RxEndBin	Group A and Group C devices The highest bin number allowed for the receive signal can be selected. This allows the customer to limit bins used for special configurations. For ADSL2plus, 512downstream bins are utilized.	511
RxStartBin	Group A and Group C devices The lowest bin number allowed for the receive signal can be selected. This allows the customer to limit bins used for special configurations.	6 (AnnexA) 64 (AnnexB)
SHalf	Group A and Group C devices Enable/Disable SHalf Feature	Enable

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
SRA	Group A and Group C devices Enables/Disables the Downstream SRA feature on Bis/Bis+ Possible values are: Disable, Enable	Disable
ShowtimeLed	To specify which LED is to be used to display State. Possible values are: 0, 1, 2, 3, 4, None	0
Standard	This parameter selects the preferred standard compliance. ADSL StandardCompliance to either T1.413, G992.1 (G.dmt), or G992.2 (G.lite) Multimodewhere one unit detects the other end as T1.413, G.lite, G.dmt, G.SPAN. G.SpanThe following option is to enable High Speed ADSL DMT applications ADSL2The following option allows the CPE to automatically connect in either ADSL Annex A or ADSL2 mode, depending upon the standard support of the CO. ADSL2plusThe following option allows the CPE to automatically connect in eitherADSL Annex A, ADSL2 or ADSL2plus mode, depending upon the standard support of the CO. Possible values for AnnexA are: G.Dmt, Bis, BisPlusAuto, BisPlusOnly, G.Span, G.Span+, G.Span++, t1.413, g.lite, Multimode, ALCTL_14, ALCATEL_T1413_B, ALCTL, ADI, G.Dmt.Bis, G.Dmt.BisPlusAuto, G.Dmt.BisPlusOnly. Possible values for AnnexB are: G.Dmt, Bis, BisPlusAuto, BisPlusOnly, G.Span, G.Span+, G.Span++, t1.413, g.lite, Multimode, ALCTL_14, ALCATEL_T1413_B, ALCTL, ADI	BisPlusAuto

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
StatusFailCount	ONLY Annex A devices group ADSL A and group ADSL C	0
TxAttenuation	Group A and Group C devices The user can specify transmit power attenuation. Possible values are: Dmt_0DB, Dmt_0.1DB, Dmt_0.2DB, Dmt_0.3DB, Dmt_0.4DB, Dmt_0.5DB, Dmt_0.6DB, Dmt_0.7DB, Dmt_0.8DB, Dmt_0.9DB, Dmt_1DB, Dmt_2DB, Dmt_3DB, Dmt_4DB, Dmt_5DB, Dmt_6DB, Dmt_7DB, Dmt_8DB, Dmt_9DB, Dmt_10DB, Dmt_11DB, Dmt_12DB, Bis_0DB, Bis_0.1DB, Bis_0.2DB, Bis_0.3DB, Bis_0.4DB, Bis_0.5DB, Bis_0.6DB, Bis_0.7DB, Bis_0.8DB, Bis_0.9DB	Bis_0DB
TxEndBin	Group A and Group C devices The highest bin number allowed for the transmit signal can be selected. This allows the customer to limit bins used for special configurations	63
TxStartBin	Group A and Group C devices The lowest bin number allowed for the transmit signal can be selected. This allows the customer to limit bins used for special configurations.	6 annexA 33 AnnexB
UtopiaInterface	It specifies the Utopia interface type Possible values are: Level1, Level2	Level1
Whip	Parameter to configure the WHIP mode to TCP or Serial Possible values are: Disable, TCP	Disable

TABLE 8-2 Options for ADSL Port Attributes (Continued)

Option	Description	Default Value
WhipMode	ONLY Group B devices This parameter can be used to set the WHIP Possible values are: WhipOnly (runs only Whip and no APIs), Standalone(disable whip) or Concurrent (run along with APIs)	Standalone
WriteMemory	ONLY Group B devices This Parameter acts as a CLI which allows to write into any DSP memory. Possible values are: "0xMemType 0xOffset 0xData"	"\0"
debug	ONLY Group B devices This parameter enables the debugging of Read/Write requests to DSP memory. Possible values are: disable, readen, writen, rwen	disable
resetDefaults	Possible values are: true, false	false

Example --> port a1 set AutoStart true

See also `PORT A1 LIST`
`PORT A1 SHOW`

8.3.1.1.3 PORT A1 SHOW

Syntax `PORT A1 SHOW`

Description This command displays the current attributes and values of ADSL port a1.

Example AT-iMG634A-R2 device port a1 show

--> port a1 show

```
DriverVersion                                   = 1.75
APIVersion                                      = GS_API_634
FirmwareVersion                                  = E.25.41.41    A
DspVersion                                      = 0x00000000
```

```
CommonHandshake                                 = Enable
Connected                                       = true
OperationalMode                                 = ADSL2+
State                                           = Showtime
Watchdog                                        = 0x00000053
OperationProgress                               = 0x00000000
LastFailed                                      = 0x00000044
TxBitRate                                       = 1020100
RxBitRate                                       = 20476100
DeltACTATPds                                    = +0.0 dB
DeltACTATPus                                    = +0.0 dB
DeltHLINscds                                    = 0
ACTPSDDs                                        = -46.00 dB
ACTPSDUs                                        = -50.00 dB
BisTEQError                                     = -38.40 dB
RxATTNDR                                        = 21992000
TxATTNDR                                        = 1100000
AnnexType                                       = AnnexA
TxCellRate                                      = 2405
RxCellRate                                      = 48292
PhyTXCellCount                                  = 30530
PhyRXCellCount                                  = 1154939
PhyCellDropCount                                = 0
OverallFailure                                  = 0
InterleaveDpDn                                  = 64
InterleaveDpUp                                  = 8
RSCorrectedErrorsDn                             = 127
RSUnCorrectedErrorsDn                           = 1
RSCorrectedErrorsUp                             = 2
RSUnCorrectedErrorsUp                           = 1
SuperFramesDn                                   = 10270882
SuperFramesUp                                   = 10270882
InterleaveRDn                                   = 0
InterleaveRUp                                   = 0
InterleaveSDn                                   = 0
InterleaveSUp                                   = 0
FastRDn                                         = 0
FastRUp                                         = 0
BisMDn                                          = 1
BisMUp                                          = 8
BisBDn                                          = 242
BisBUp                                          = 28
BisTDn                                          = 7
```

```
BisTUp                                  = 4
BisLDn                                  = 5375
BisLUp                                  = 275
BisRDn                                  = 12
BisRUp                                  = 16
BisSDn                                  = 0.37
BisSUp                                  = 7.21
BisDelayDn                              = 6.25
BisDelayUp                              = 14.50
ShowtimeStart                           = 174605
ATURVendor                              = CNXT
ATUCCountry                             = 46591
ATURANSIRev                             = 5632
ATURANSISTD                             = 0
ATUCANSIRev                             = 4096
ATUCANSIId                              = CNXT
ATUCANSISTD                             = 0
DataBoost                               = Disable
LocalITUCountryCode                     = 46591
LocalSEF                                = 0
LocalEndLOS                             = 0
LocalSNRMargin                          = 9.75 dB
LocalLineAttn                           = 3.0 dB
INPup                                   = 1.86
INPdown                                 = 0.57
PMstatus                                = L0
RawAttn                                 = 0.0 dB
LocalTxPower                            = 0.4 dB
LocalFastChannelRxRate                  = 0
LocalFastChannelTxRate                  = 0
LocalFastChannelFEC                     = 0
LocalFastChannelCRC                     = 0
LocalFastChannelHEC                     = 0
LocalFastChannelNCD                     = 0
LocalFastChannelOCD                     = 0
LocalFastChannelLCD                     = 0
LocalInterleavedChannelRxRate           = 20476100
LocalInterleavedChannelTxRate           = 1020100
LocalInterleavedChannelFEC              = 0
LocalInterleavedChannelCRC              = 0
LocalInterleavedChannelHEC              = 0
LocalInterleavedChannelNCD              = 0
LocalInterleavedChannelOCD              = 0
```

```
LocalInterleavedChannelLCD                    = 0
RemoteTxPower                                 = 14.3 dB
RemoteSEF                                     = 0
RemoteLOS                                     = 0
RemoteLineAttn                                = 0.0 dB
RemoteSNRMargin                               = 9.0 dB
RemoteFastChannelFEC                          = 0
RemoteFastChannelCRC                          = 0
RemoteFastChannelHEC                          = 0
RemoteFastChannelNCD                          = 0
RemoteFastChannelLCD                          = 0
RemoteInterleavedChannelFEC                   = 0
RemoteInterleavedChannelCRC                   = 0
RemoteInterleavedChannelHEC                   = 0
RemoteInterleavedChannelNCD                   = 0
RemoteInterleavedChannelLCD                   = 0
LocalMgmtFEC0                                 = 127
LocalMgmtCRC0                                 = 1
LocalMgmtFECErroredSec                        = 6
LocalMgmtErroredSec                           = 1
LocalMgmtSeverelyErroredSec                   = 0
LocalMgmtLOSErroredSec                        = 0
LocalMgmtUnavailErroredSec                    = 0
LocalMgmtHEC0                                 = 0
RemoteMgmtFEC0                                = 2
RemoteMgmtCRC0                                = 1
RemoteMgmtFECErroredSec                       = 2
RemoteMgmtErroredSec                          = 1
RemoteMgmtSeverelyErroredSec                  = 0
RemoteMgmtLOSErroredSec                       = 0
RemoteMgmtUnavailErroredSec                   = 0
RemoteMgmtHEC0                                = 0
LocalTPSTCCell0                               = 4135809766
LocalTPSTCCell0UpperLayer                     = 1154939
LocalTPSTCBitError                            = 0
RemoteTPSTCCell0                              = 420082063
RemoteTPSTCCell0UpperLayer                    = 161594
RemoteTPSTCBitError                           = 0
PSDMaskStatus                                 = Standard
StatusFailCount                               = 981
LineUpCount                                   = 2
SRACnt                                        = 19
DSBitSwapCnt                                  = 46908
```

```
USBitSwapCnt                                = 256
ProfileStatus                               = MAIN
Action                                      = Startup
ActivateLine                                = None
LineStatus                                  = true
HostControl                                 = Enable
AutoStart                                   = true
failsafe                                    = false
ShowtimeLed                                 = 3
Retrain                                     = EnableOverallOnly
Defaults                                    = None
ReadMemory                                  =
WriteMemory                                 =
DSPTrace                                    = StopLogging
LoopbackTest                                = Unknown (0)
LineMode                                    = None
Whip                                        = Disable
WhipActive                                  = Inactive
WhipMode                                    = Standalone
DyingGasp                                   = Enable
UtopiaInterface                             = Level1
PhysicalPort                                = 0
ClockType                                   = Crystal
GenericTrace                                = DSP
debug                                       = disable
MaxRSMemory                                 = 32
Profile                                     = MAIN
DetectNoise                                 = Disable
AnnexAStandard                              = Multimode
AnnexAEcFdmMode                             = FDM
AnnexAMaxBitsPerBin                         = 15
AnnexATxStartBin                            = 6
AnnexATxEndBin                              = 31
AnnexARxStartBin                            = 32
AnnexARxEndBin                              = 255
AnnexARxAutoBinAdjust                       = Disable
AnnexATxAttenuation                         = 0
AnnexABitSwap                               = Enable
AnnexABitSwapUp                             = Enable
AnnexANTRMode                               = Disable
AnnexAMaxDownRate                           = 255
AnnexACapability                            = AnnexA/T1413
AnnexACodingGain                            = auto
```

```
AnnexAFramerType                        = Type3
AnnexAFastRetrain                       = Enable
AnnexAQualificationMode                 = Mode1
AnnexAMaxMargin                         = PerCO
AnnexAForceSNRMarginDn                  = 0x0000ffff
BisAMaxInterleaveD                      = 511
BisASHalf                               = Disable
BisACabinetMode                         = Enable
BisAPSDMask                             = NonOvlp-M1
BisAStandard                            = BisPlusAuto
BisAEcFdmMode                           = EC
BisAMaxBitsPerBin                       = 15
BisATxStartBin                          = 6
BisATxEndBin                            = 31
BisARxStartBin                          = 6
BisARxEndBin                            = 511
BisARxAutoBinAdjust                     = Disable
BisATxAttenuation                       = Bis_0DB
BisABitSwap                             = Enable
BisABitSwapUp                           = Enable
BisANTRMode                             = Disable
BisAMaxDownRate                         = 511
BisACapability                          = A2/A2+
BisACodingGain                          = auto
BisAFramerType                          = Type3ET
BisAFastRetrain                         = Disable
BisAMaxSInverse                         = 0x10
BisA_REIN                               = 60pps
BisA_SRA                                = Enable
BisA_PMmode                             = L2L3Allowed
BisAQualificationMode                   = Mode1
BisAPrecedence                          = DSInp
BisAMaxMargin                           = PerCO
BisADsInp                               = MinPossible
BisAForceSNRMarginDn                    = 0x0000ffff
BisMMaxInterleaveD                      = 511
BisMSHalf                               = Disable
BisMCabinetMode                         = Disable
BisMPSDMask                             = ALL
BisMStandard                            = BisPlusAuto
BisMEcFdmMode                           = EC
BisMMaxBitsPerBin                       = 15
BisMTxStartBin                          = 6
```

```
BisMTxEndBin                                = 63
BisMRxStartBin                              = 6
BisMRxEndBin                                = 511
BisMRxAutoBinAdjust                         = Disable
BisMTxAttenuation                           = Bis_0DB
BisMBitSwap                                 = Enable
BisMBitSwapUp                               = Enable
BisMNTRMode                                 = Disable
BisMMaxDownRate                             = 511
BisMCapability                              = M2+/M2
BisMCodingGain                              = auto
BisMFramerType                              = Type3ET
BisMFastRetrain                             = Enable
BisMMaxSInverse                             = 0x10
BisM_REIN                                   = 60pps
BisM_SRA                                    = Enable
BisM_PMmode                                 = L2L3Allowed
BisMQualificationMode                       = Mode1
BisMPrecedence                              = DSInp
BisMMaxMargin                               = PerCO
BisMDsInp                                   = MinPossible
BisMForceSNRMarginDn                        = 0x0000ffff
BisBMaxInterleaveD                          = 511
BisBSHalf                                   = Disable
BisBCabinetMode                             = Enable
BisBPSDMask                                 = NonOvlp-M1
BisBStandard                                = BisPlusAuto
BisBEcFdmMode                               = FDM
BisBMaxBitsPerBin                           = 15
BisBTxStartBin                              = 33
BisBTxEndBin                                = 63
BisBRxStartBin                              = 64
BisBRxEndBin                                = 511
BisBRxAutoBinAdjust                         = Disable
BisBTxAttenuation                           = Bis_0DB
BisBBitSwap                                 = Enable
BisBBitSwapUp                               = Enable
BisBNTRMode                                 = Disable
BisBMaxDownRate                             = 511
BisBCapability                              = Disable
BisBCodingGain                              = auto
BisBFramerType                              = Type3ET
BisBFastRetrain                             = Disable
```

```
BisBMaxSInverse                                 = 0x10
BisB_REIN                                       = 60pps
BisB_SRA                                        = Enable
BisB_PMmode                                     = L2L3Allowed
BisBQualificationMode                           = Mode1
BisBPrecedence                                  = DSInp
BisBMaxMargin                                   = PerCO
BisBDsInp                                       = MinPossible
BisBForceSNRMarginDn                            = 0x0000ffff
SupportedAnnexes                               = BisA/BisM/AnnexA/
T1413A
LineCoding                                      = 2
LineType                                        = 5
AtucInvSerialNumber                             = 0x00baad9c
AtucInvVendorId                                 = 0x00baadbc
AtucInvVersionNumber                            = 0x00baad7c
AtucCurrSnrMgn                                  = 0
AtucCurrAtn                                     = 452460574
AtucCurrStatus                                  = 0x0103f59c
AtucCurrOutputPwr                               = 0
AtucCurrAttainableRate                          = 20476100
AturInvSerialNumber                             = 0x00baad3c
AturInvVendorId                                 = 0x00baad5c
AturInvVersionNumber                            = 0x00baad1c
AturCurrSnrMgn                                  = 90
AturCurrAtn                                     = 452460544
AturCurrStatus                                  = 0x0103f59c
AturCurrOutputPwr                               = 4
AturCurrAttainableRate                          = 1020100
AtucChanReceivedBlks                            = 0
AtucChanTransmittedBlks                         = 0
AtucChanCorrectedBlks                           = 0
AtucChanUncorrectBlks                           = 0
AtucChanPerfValidIntervals                      = 86
AtucChanPerfInvalidIntervals                    = 86
AtucChanPerfCurr15MinTimeElapsed                = 619
AtucChanPerfCurr15MinReceivedBlks               = 0
AtucChanPerfCurr15MinTransmittedBlks            = 0
AtucChanPerfCurr15MinCorrectedBlks              = 0
AtucChanPerfCurr15MinUncorrectBlks              = 0
AtucChanPerfCurr1DayTimeElapsed                 = 77119
AtucChanPerfCurr1DayReceivedBlks                = 0
AtucChanPerfCurr1DayTransmittedBlks             = 0
```

```
AtucChanPerfCurr1DayCorrectedBlks                = 0
AtucChanPerfCurr1DayUncorrectBlks                = 0
AtucChanPerfPrev1DayMoniSecs                     = 86400
AtucChanPerfPrev1DayReceivedBlks                 = 0
AtucChanPerfPrev1DayTransmittedBlks              = 0
AtucChanPerfPrev1DayCorrectedBlks                = 0
AtucChanPerfPrev1DayUncorrectBlks                = 0
AturChanReceivedBlks                             = 0
AturChanTransmittedBlks                          = 0
AturChanCorrectedBlks                            = 0
AturChanUncorrectBlks                            = 0
AturChanPerfValidIntervals                       = 86
AturChanPerfInvalidIntervals                     = 86
AturChanPerfCurr15MinTimeElapsed                 = 619
AturChanPerfCurr15MinReceivedBlks                = 0
AturChanPerfCurr15MinTransmittedBlks             = 0
AturChanPerfCurr15MinCorrectedBlks               = 0
AturChanPerfCurr15MinUncorrectBlks               = 0
AturChanPerfCurr1DayTimeElapsed                  = 77119
AturChanPerfCurr1DayReceivedBlks                 = 0
AturChanPerfCurr1DayTransmittedBlks              = 0
AturChanPerfCurr1DayCorrectedBlks                = 0
AturChanPerfCurr1DayUncorrectBlks                = 0
AturChanPerfPrev1DayMoniSecs                     = 86400
AturChanPerfPrev1DayReceivedBlks                 = 0
AturChanPerfPrev1DayTransmittedBlks              = 0
AturChanPerfPrev1DayCorrectedBlks                = 0
AturChanPerfPrev1DayUncorrectBlks                = 0
AtucPerfLofs                                     = 0
AtucPerfLoss                                     = 0
AtucPerfLprs                                     = 0
AtucPerfESs                                      = 0
AtucPerfValidIntervals                           = 86
AtucPerfInvalidIntervals                         = 0
AtucPerfCurr15MinTimeElapsed                     = 619
AtucPerfCurr15MinLofs                            = 0
AtucPerfCurr15MinLoss                            = 0
AtucPerfCurr15MinLprs                            = 0
AtucPerfCurr15MinESs                             = 0
AtucPerfCurr1DayTimeElapsed                      = 77119
AtucPerfCurr1DayLofs                             = 0
AtucPerfCurr1DayLoss                             = 0
AtucPerfCurr1DayLprs                             = 0
```

```
AtucPerfCurr1DayESs                          = 0
AtucPerfPrev1DayMoniSecs                     = 86400
AtucPerfPrev1DayLofs                         = 0
AtucPerfPrev1DayLoss                         = 0
AtucPerfPrev1DayLprs                         = 0
AtucPerfPrev1DayESs                          = 0
AturPerfLofs                                 = 0
AturPerfLoss                                 = 0
AturPerfLprs                                 = 0
AturPerfESs                                  = 5
AturPerfValidIntervals                       = 86
AturPerfInvalidIntervals                     = 0
AturPerfCurr15MinTimeElapsed                 = 619
AturPerfCurr15MinLofs                        = 0
AturPerfCurr15MinLoss                        = 0
AturPerfCurr15MinLprs                        = 0
AturPerfCurr15MinESs                         = 5
AturPerfCurr1DayTimeElapsed                  = 77119
AturPerfCurr1DayLofs                         = 0
AturPerfCurr1DayLoss                         = 0
AturPerfCurr1DayLprs                         = 0
AturPerfCurr1DayESs                          = 0
AturPerfPrev1DayMoniSecs                     = 86400
AturPerfPrev1DayLofs                         = 0
AturPerfPrev1DayLoss                         = 0
AturPerfPrev1DayLprs                         = 0
AturPerfPrev1DayESs                          = 0
AtucChanInterleaveDelay                      = 6.25
AtucChanCurrTxRate                           = 20476100
AtucChanPrevTxRate                           = 20476100
AtucChanCrcBlockLength                       = 0
AturChanInterleaveDelay                      = 14.50
AturChanCurrTxRate                           = 1020100
AturChanPrevTxRate                           = 1020100
AturChanCrcBlockLength                       = 8
Version                                      = 2.10
PortClassATM                                 = true
PortSpeed                                    = 2405
TxBurstSize                                  = 1
CACMode                                      = None
CACFunction                                  = 0x00000000
UPSAddr                                      = 0x0103e6cc
cbr_CPS                                      = 0
```

```
rvbrPCR_CPS                                    = 0
rvbrSCR_CPS                                    = 0
vbrPCR_CPS                                     = 0
vbrSCR_CPS                                     = 0
ubr_CPS                                        = 12000
RingLength                                     = 1000
VPIRange                                       = 12
VCIRange                                       = 16
MaxVcs                                         = 12
DefaultPCR                                     = 2000
DefaultMaxQueue                                = 16
TrafficShaping                                 = false
NiType                                         = nni
SnmpIfIndex                                    = 3
SnmpIfType                                     = 37
SnmpVcListHead                                 = 0x01066f3c
resetDefaults                                  = false
portSnmpIfIndex                                = 3
portSnmpIfType                                 = 37
```

See also `PORT A1 SET`
`PORT A1 STATUS`

8.3.1.1.4 PORT A1 STATUS

Syntax `PORT A1 STATUS`

Description This command displays basic connection parameters for ADSL port.

Some of the information reported are:

- The connection status (idle, training, showtime)
- The ADSL connection mode negotiated (G.DMT, T1.413, G.SPAN, ADSL2, ADSL2+)
- The maximum negotiated uplink bit rate
- The maximum negotiated downlink bit rate
- The administrative port status (none, activate, abort)
- The administrative connection mode.

Example AT-iMG634A-R2 device port a1 status

--> port a1 status

```
DriverVersion                                   = 1.75
APIVersion                                      = GS_API_634
FirmwareVersion                                 = E.25.41.41   A
DspVersion                                      = 0x00000000
CommonHandshake                                 = Enable
Connected                                       = true
OperationalMode                                 = ADSL2+
State                                           = Showtime
Watchdog                                        = 0x00000053
OperationProgress                               = 0x00000000
LastFailed                                      = 0x00000044
TxBitRate                                       = 1020100
RxBitRate                                       = 20476100
RxATTNDR                                        = 21992000
TxATTNDR                                        = 1100000
AnnexType                                       = AnnexA
TxCellRate                                      = 2405
RxCellRate                                      = 48292
OverallFailure                                  = 0
DataBoost                                       = Disable
LocalITUCountryCode                             = 46591
INPup                                           = 1.86
INPdown                                         = 0.57
PMstatus                                        = L0
PSDMaskStatus                                   = Standard
StatusFailCount                                 = 982
ProfileStatus                                   = MAIN
Action                                          = Startup
ActivateLine                                    = None
HostControl                                     = Enable
AutoStart                                       = true
failsafe                                        = false
ShowtimeLed                                     = 3
Retrain                                        = EnableOverallOnly
Defaults                                        = None
Whip                                            = Disable
WhipActive                                      = Inactive
WhipMode                                        = Standalone
DyingGasp                                       = Enable
UtopiaInterface                                 = Level1
PhysicalPort                                    = 0
ClockType                                       = Crystal
```

```
GenericTrace                                    = DSP
debug                                           = disable
MaxRSMemory                                     = 32
Profile                                         = MAIN
DetectNoise                                     = Disable
PortSpeed                                       = 2405
resetDefaults                                   = false
```

8.4 Bridge

The transparent bridge on the Allied Telesis Media Gateway main application software provides MAC level bridging for Ethernet-like networks. The transparent bridge may be configured to interconnect different type of interfaces in order to forward packets that arrive from a specific physical media to another different physical media.

The transparent bridge plays a fundamental rule in the Allied Telesis Media Gateway architecture because it is used not only for pure bridging functionality but it's also used when routing is performed between ip interfaces attached to Ethernet ports to ipinterfaces attached to ADSL port (only when RFC1483 encapsulation type is used).

8.4.1 Basic bridge configuration

The following picture reports the basic bridge configuration that is always present in any Allied Telesis Media Gateway system configuration, note that group ADSL C devices have a 6 ethernet switch ports on board but the basic principles operation are the same.

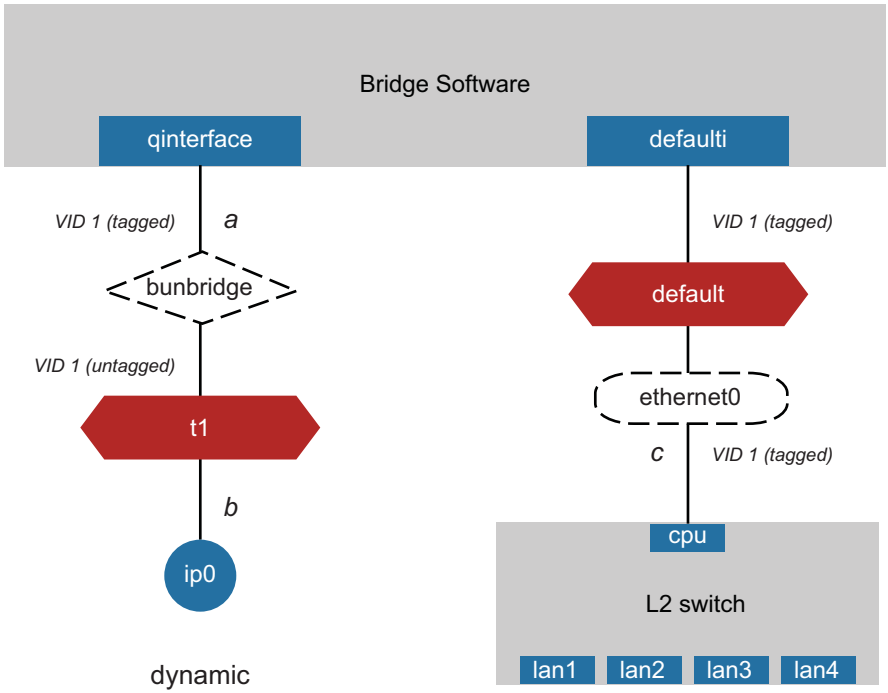


FIGURE 8-2 Basic software bridge configuration

The bridge software and the overall system architecture has been designed in order to have frames forwarded by the bridge always being tagged frames. All the bridge interfaces must therefore be able to manage tagged frames.

The bridge software has two interfaces named *defaulti* and *qinterface* respectively.

The *defaulti* interface receives always tagged frames from the switch chipset that is configured to support multiple vlan on the Ethernet ports and manage tagged/untagged frames. The *defaulti* interface forwards tagged frames either to the bridge ***qinterface*** or to other configured bridge interfaces based on the destination MAC address (see below).

The Allied Telesis Media Gateway is always configured with one ip interface ip0 attached (connection *b*) on an Ethernet transport named *t1*.

The transport *t1* add a tag header with VID = 1 to all the outgoing packets routed or generated by ip0 interface. These packets arriving on the bridge interface *qinterface* will be forwarded to the other bridge interfaces depending on the destination MAC address registered in the bridge database: if the bridge has previously registered the destination MAC address as belong to a specific interface, the packet will be forwarded only to this interface, otherwise the packet is forwarded to all the existing interfaces.

In the opposite direction, packets arriving from *qinterface* (connection *a*) are filtered by the *bunbridge* module and only tagged packets having VID = 1 are sent to ip0 interface.

8.4.2 Multiple VLAN support

Bunbridge port is an intermediate layer between the bridge *qinterface* and the ethernet transport *t1*. This intermediate layer is used to separate tagged frames received from ***qinterface*** based on the VID value:

- It remove the tag header from tagged framed with VID=1 and then forward them to ip0 interface;
- it forward any other tagged frames with VID ≠1 to an additional intermediate port, named *ethernet1* (see example below).

Ethernet1 port looks like an additional system port that receives tagged frames (from the bridge) and forward them to Ethernet transports modules depending on the VID value. Each Ethernet transport will then remove the tag header from the frames and will forward such untagged frames to the IP interface attached to it.

Once frames are arrived to the IP layer, routing functions as well as any other functionality that operates at layer 3/4 can be performed.

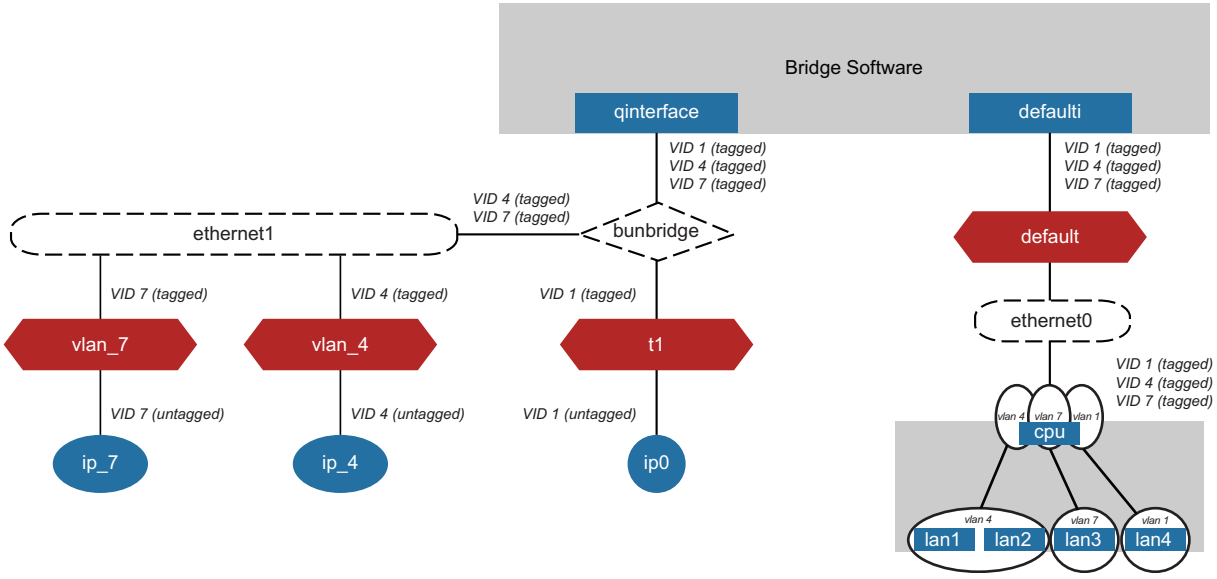


FIGURE 8-3 Example of system architecture to support multiple vlan management

8.4.3 Bridge command reference

8.4.3.1 Bridge CLI commands

This chapter describes the ***Bridge*** commands provided by the CLI:

TABLE 8-3 Bridge commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
BRIDGE ADD INTERFACE							X	X	X
BRIDGE ADD VLANINTERFACE								X	X
BRIDGE ATTACH							X	X	X
BRIDGE CLEAR INTERFACES							X	X	X
BRIDGE DELETE INTERFACE							X	X	X
BRIDGE DETACH							X	X	X
BRIDGE LIST INTERFACES							X	X	X
BRIDGE LIST VLANS								X	X
BRIDGE SET FILTERAGE							X	X	X
BRIDGE SET INTERFACE FILTERTYPE							X	X	X
BRIDGE SET INTERFACE PORTFILTER									
BRIDGE SHOW							X	X	X
BRIDGE SHOW INTERFACE							X	X	X

8.4.3.1.1 BRIDGE ADD INTERFACE

Syntax `BRIDGE ADD INTERFACE <name>`

Description This command adds a named interface to the bridge.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the interface. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A

Example --> bridge add interface pvc_1_32_if

See also BRIDGE ATTACH
BRIDGE LIST INTERFACES
BRIDGE LIST VLAN

8.4.3.1.2 BRIDGE ADD VLANINTERFACE

Description BRIDGE ADD VLANINTERFACE {<name>|number} {tagged|untagged} <interfacename>

This command adds an interface in the egress interface list of the named VLAN. The egress interface list for a VLAN is the union of tagged interfaces and the untagged interfaces. For the default VLAN, all the bridge interfaces, are automatically configured as its untagged egress interfaces. The user need not explicitly add untagged interfaces for the DefaultVlan.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	A name that identifies an existing VLAN. To display the list of statically configured VLANs, use *bridge list static vlans*.	N/A
number	A number that identifies an existing VLAN.	
tagged	To add a port in the tagged port list of the named VLAN.	
untagged	To add a port in the untagged port list of the named VLAN.	

Example --> bridge add vlainterface vlan666 tagged pvc_0_35_if

See also BRIDGE LIST VLAN
BRIDGE LIST INTERFACES

8.4.3.1.3 BRIDGE ATTACH

Syntax BRIDGE ATTACH {<name>|<number>} <transport>

Description This command attaches an existing transport to an existing bridge interface to allow data to be bridged via the transport.

Only one transport can be attached to an interface. If you use this command when there is already a transport attached to the interface; the new transport replaces the previous one.

This command implicitly enables the transport being attached.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing bridge interface. To display interface names, use the BRIDGE LIST INTERFACES command.	N/A
number	An existing bridge interface. To display interface numbers, use the BRIDGE LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
transport	An existing transport. To display transport names, use the <***transport type***>TRANSPORTS LIST command.	N/A

Example --> bridge attach bridge1 my1483

See also BRIDGE ADD INTERFACE
BRIDGE LIST INTERFACES
TRANSPORTS LIST

8.4.3.1.4 BRIDGE CLEAR INTERFACES

Syntax BRIDGE CLEAR INTERFACES

Description This command deletes **ALL** bridge interfaces that were created using the bridge add interface command. Any source MAC forwarding rules associated with the interfaces are also deleted by this command.

Example --> bridge clear interfaces

See also BRIDGE DELETE INTERFACE

8.4.3.1.5 BRIDGE DELETE INTERFACE

Syntax BRIDGE DELETE INTERFACE {<name>|<number>}

Description This command deletes a **SINGLE** interface from the bridge configuration. All source MAC forwarding rules associated with the interface that you want to delete are also deleted by this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing bridge interface. To display interface names, use the BRIDGE LIST INTERFACES command.	N/A
number	An existing bridge interface. To display interface numbers, use the BRIDGE LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> bridge delete interface 1

See also BRIDGE LIST INTERFACES

8.4.3.1.6 BRIDGE DETACH

Syntax BRIDGE DETACH {<name>|<number>}

Description This command detaches the transport that was attached to the bridge interface using the bridge attach interface command. All source MAC forwarding rules associated with the interface that you want to detach are deleted by this command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing bridge interface. To display interface names, use the BRIDGE LIST INTERFACES command.	N/A
number	An existing bridge interface. To display interface numbers, use the BRIDGE LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example --> bridge detach interface 2

See also BRIDGE LIST INTERFACES

8.4.3.1.7 BRIDGE LIST INTERFACES

Syntax BRIDGE LIST INTERFACES

Description This command lists all bridge interfaces that have been created using the bridge add interface command. It displays the following information about bridge interfaces:

- Interface ID number
- Interface name
- Filter type
- Name of attached transport (if applicable)

Example 1) Group ADSL A devices

--> bridge list interfaces

```
Bridge Interfaces:
 ID  |      Name        | Filter Type  |    Transport
-----|------------------|--------------|----------------
   1 | defaulti         | All          | default
   2 | pvc_0_35_if      | All          | pvc_0_35
-------------------------------------------------------
```

Example 2) Group ADSL B and ADSL C devices

--> bridge list interfaces
ID: 1

```
Name: defaulti

Filter| PVID  | Accept    | Ingress   | User  | Transport
Type  |       | FrameType | Filtering | Prio  |
------|-------|-----------|-----------|-------|-----------------
All   | 1     | ALL       | disabled  | 0     | default

ID:      2
Name: pvc_0_35_if

Filter| PVID  | Accept    | Ingress   | User  | Transport
Type  |       | FrameType | Filtering | Prio  |
------|-------|-----------|-----------|-------|-----------------
All   | 1     | ALL       | disabled  | 0     | pvc_0_35
```

See also BRIDGE SET FILTERAGE
BRIDGE SET INTERFACE FILTERTYPE
BRIDGE SET INTERFACE PORTFILTER

8.4.3.1.8 BRIDGE LIST VLANS

Syntax `bridge list VLANS`

Description This command lists all bridge vlans created on the bridge

Example bridge list vlans

VLANs:

```
  ID | VLAN ID | VLAN Name     | FDB Name   | Type
-------------------------------------------------------------
   1 | 1       | DefaultVlan   | DefaultFdb | static
Tagged Interfaces:   defaulti
Untagged Interfaces:
-------------------------------------------------------------
   2 | 2020     | vlan2020     | vlan2020  | static

Tagged Interfaces:   defaulti   pvc_0_35_if
Untagged Interfaces:
-----------------------------------------------------------
   3 | 2030     | vlan2030     | vlan2030  | static

Tagged Interfaces:   defaulti
Untagged Interfaces: pvc_0_35_if
-------------------------------------------------------------
```

8.4.3.1.9 BRIDGE SET FILTERAGE

Syntax `BRIDGE SET FILTERAGE <filter age>`

Description This command specifies the maximum age of filter table entries for the bridge. The filter age for the bridge is displayed by the `BRIDGE SHOW` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
filter age	The filter age is the time (in seconds) after which MAC addresses are removed from the filter table when there has been no activity. The time may be an integer value between 10 and 100,000 seconds.	300 seconds

Example --> bridge set filterage 2000

See also BRIDGE SHOW

8.4.3.1.10 BRIDGE SET INTERFACE FILTERTYPE

Syntax BRIDGE SET INTERFACE {<name>|<number>} FILTERTYPE {ALL|IP|PPPOE}

Description This command specifies the type of Ethernet filtering performed by the named bridge interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing bridge interface. To display interface names, use the BRIDGE LIST INTERFACES command.	N/A
number	An existing bridge interface. To display interface numbers, use THE BRIDGE LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A
all	Allows all types of Ethernet packets through the port.	All
ip	Allows only IP/ARP Ethernet packets through the port.	
pppoe	Allows only PPPoE Ethernet packets through the port.	

Example --> bridge set interface bridge2 filtertype ip

See also BRIDGE LIST INTERFACES

8.4.3.1.11 BRIDGE SET INTERFACE PORTFILTER

Syntax `BRIDGE SET INTERFACE {<name>|<number>} PORTFILTER {ALL|<port>}`

Description This command controls the bridge's forwarding and broadcasting behavior. It allows you to set a portfilter on a bridge interface to determine which port or ports multicast and unknown packets should be forwarded to.

This command sets one destination port at a time. If you want to forward packets to several ports, enter a bridge set interface portfilter <port> command for each port. If you want to forward packets to all ports, enter the command and specify the all value.

Note: If a unicast packet is received by an interface with a portfilter set to all, the portfilter rule is ignored. The unicast packet is still only sent to one port.

Note: If the bridge itself is attached to the router, the bridge itself will always forward to all ports and will always be forwarded to by all ports.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing bridge interface. To display interface names, use the `BRIDGE LIST INTERFACES` command.	N/A
number	An existing bridge interface. To display interface numbers, use the `BRIDGE LIST INTERFACES` command. The number appears in the first column under the heading ID.	N/A
port	The name of the existing port that you want packets, received on a specified bridge interface, to be forwarded to. To display port names, use the `PORT ?` command.	all
all	Forwards packets, received on a specified bridge interface, to all existing bridge ports.	

Example --> bridge set interface bridge1 portfilter ethernet

See also `BRIDGE SHOW INTERFACE`

8.4.3.1.12 BRIDGE SHOW

Syntax `BRIDGE SHOW`

Description This command shows the global configuration settings for the bridge. The following bridge information is displayed:

- Filter age

Example 1) Group ADSL A devices

--> bridge show

```
Global bridge configuration:

    MAC Address:            0:d:da:7:36:d3
        Number of Interfaces:   3
        Type:                   TRANSPARENT
        Filter Age:             300 seconds
        LAN-LAN Forwarding:     true
        WAN-WAN Forwarding:     true
```

Example 2) Group ADSL B and ADSL C devices

--> bridge show

```
Global bridge configuration:

        MAC Address:            0:d:da:16:f4:9b
        Number of Interfaces:   2
        Type:                   TRANSPARENT
        Filter Age:             300 seconds
        LAN-LAN Forwarding:     true
        WAN-WAN Forwarding:     true
        Unicast-Learning:       HYBRID
        Multicast-Learning:     HVM
        Interface VLAN ID:      ENABLED
        Traffic Classes:        DISABLED
        Tagging:                ENABLED
        Acceptable Frame Type:  ENABLED
        Ingress Filtering:      ENABLED

VLAN bridge Configuration:

        VLAN Version Number:        1
        Maximum VLAN ID:            4095
        Maximum Number of VLANS:    16
        Current Number of VLANS:    6

IGMP Snoop Configuration:
```

```
IGMP Snoop:                 Enable
IGMP Net Interface:           ip_static_video
IGMP Enabled Vlan:            205
Default Fast Leave            Enable
Last Member Query Interval:   0
Query Interval:               41
Robustness Variable:          2
Query Response Interval:      3
V1 Timer Value:               133
Multicast Intf Aging Time:    133
IGMP Snoop Mode:              proxy
IGMP MAC Security:            Disable
IGMP MAC Security Learning:   Disable
IGMP MAC Security Max Number: 5
     MAC Address 1:           Empty
     MAC Address 2:           Empty
     MAC Address 3:           Empty
     MAC Address 4:           Empty
     MAC Address 5:           Empty
     MAC Address 6:           Empty
     MAC Address 7:           Empty
     MAC Address 8:           Empty
     MAC Address 9:           Empty
     MAC Address 10:          Empty
```

See also `BRIDGE SET FILTERAGE`

8.4.3.1.13 BRIDGE SHOW INTERFACE

Syntax `BRIDGE SHOW INTERFACE {<name>|<number>}`

Description This command displays the filter type value and portfilter setting of a named bridge interface.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing bridge interface. To display interface names, use the `BRIDGE LIST INTERFACES` command.	N/A

Option	Description	Default Value
number	An existing bridge interface. To display interface numbers, use THE BRIDGE LIST INTERFACES command. The number appears in the first column under the heading ID.	N/A

Example 1) Group ADSL A devices

```
--> bridge show interface pvc_0_35_if
Bridge Interface:  pvc_0_35_if
Filter Type:       All
Port Filter:       All
Transport:         pvc_0_35
```

Example 2) Group ADSL B and ADSL C device

```
--> bridge show interface pvc_0_35_if
Bridge Interface: pvc_0_35_if
Name:                       pvc_0_35_if
Filter Type:                All
Port Filter:                All
PVID:                       1
Acceptable Frame Type:      ALL
Ingress Filtering:          disabled
User Priority:              0
Transport:                  pvc_0_35
Leave Mode:                 Normal
IGMP Port State:            Enable
```

See also `bridge set interface filtertype`
`bridge set interface portfilter`

8.5 Transports

This section describes the commands available on the AT-iMG/AT-iBG to manage the ***Transport*** module.

Note: Throughout this section, the syntax <TRANSPORT_MODULE> is used to generically represent a transport module like PPPOE or Ethernet.

This module allows you to clear, delete, list and display information about existing transports that were created using the <TRANSPORT_MODULE> add transport commands. To carry out more detailed configuration of transports, see the corresponding transport module chapter:

For PPPoE commands, see PPPoE CLI commands.

For Ethernet commands, see Ethernet CLI commands.

8.5.1 Transports command reference

This section describes the commands available on the AT-iMG/AT-iBG to configure and manage the ***Transports*** module.

8.5.1.1 Transports CLI commands

The table below lists the Transports commands provided by the CLI:

TABLE 8-4 Transport commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
TRANSPORTS CLEAR							X	X	X
TRANSPORTS DELETE							X	X	X
TRANSPORTS LIST							X	X	X
TRANSPORTS SET CLASSIFIER DISABLED							X	X	X
TRANSPORTS SET CLASSIFIER PROFILE							X	X	X
TRANSPORTS SET METER INSTANCE DISABLED							X	X	X
TRANSPORTS SET METER INSTANCE PROFILE							X	X	X
TRANSPORTS SET SCHEDULER PROFILE							X	X	X
TRANSPORTS SET SCHEDULER DISABLED							X	X	X
TRANSPORTS SHOW							X	X	X

8.5.1.1.1 TRANSPORTS CLEAR

Syntax `TRANSPORTS CLEAR`

Description This command deletes all transports present on the device.

Example --> transports clear

See also `TRANSPORTS DELETE`
`TRANSPORTS LIST`

8.5.1.1.2 TRANSPORTS DELETE

Syntax `TRANSPORTS DELETE {<name>|<number>}`

Description This command deletes a single transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the transports list command.	N/A
number	An existing transport. To display transport numbers, use the transports list command.	N/A

Example --> transports delete eth1

See also TRANSPORTS CLEAR
TRANSPORTS LIST

8.5.1.1.3 TRANSPORTS LIST

Syntax TRANSPORTS LIST

Description This command lists all transports created during a session. It displays the following information about the transports:

- Transport identification number
- Transport name
- Transport type (rfc1483, PPP, Ethernet, frame relay or IPoA)
- Number of transmitted/received packets for each transport
- VPI/VCI setting (rfc1483, PPP and IPoA transports only)

Example --> transports list

```
Services:
ID | Name    | Type
---|---------|-------------------------------------------------
 1 | rfc1483 | RFC1483 | TxPkts:0/0  RxPkts:0/0  VPI/VCI:0/100
 2 | pppoh2  | PPP     | TxPkts:0/0  RxPkts:0/0  VPI/VCI:0/101
 3 | pppoh1  | PPP     | TxPkts:0/0  RxPkts:0/0  VPI/VCI:0/102
 4 | pppoa2  | PPP     | TxPkts:0/0  RxPkts:0/0  VPI/VCI:0/103
 5 | eth0    | Ethernet| TxPkts:0/0  RxPkts:0/0
-----------------------------------------------------------------
```

See also TRANSPORTS SHOW

8.5.1.1.4 TRANSPORTS SET CLASSIFIER DISABLED

Syntax `TRANSPORTS SET {<name>|<number>} CLASSIFIER DISABLED`

Description This command disables packet classification previously set on a specified transport using the transports set classifier profile command. The classifier is removed from the data path.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the transports list command.	N/A
number	An existing transport. To display transport numbers, use the transports list command.	N/A

Example --> transports set pvc_0_35 classifier disabled

See also `TRANSPORTS SET CLASSIFIER PROFILE`
`TRANSPORTS LIST CLASSIFIER CLI COMMANDS`

8.5.1.1.5 TRANSPORTS SET CLASSIFIER PROFILE

Syntax `TRANSPORTS SET {<name>|<number>} CLASSIFIER PROFILE {<profile name>|<profile number>}`

Description This command sets an existing classifier profile on an existing transport. All rules that exist in this profile will test incoming packets on the specified transport.

The same profile can be added to more than one transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the transports list command.	N/A
number	An existing transport. To display transport numbers, use the transports list command.	N/A

Option	Description	Default Value
profile name	An existing profile. To display transport names, use the classifier list profiles command.	N/A
profile number	An existing profile. To display profile numbers, use the classifier list profiles command.	N/A

Example --> transports set myrfc classifier profile p1

See also
```
TRANSPORTS SET CLASSIFIER DISABLED
TRANSPORTS LIST
QOS (chapter X-QOS)
CLASSIFIER ADD PROFILE
CLASSIFIER LIST PROFILES
```

8.5.1.1.6 TRANSPORTS SET METER INSTANCE DISABLED

Syntax
```
TRANSPORTS SET {<name>|<number>} METER INSTANCE <meterid>
DISABLED
```

Description This command disables a meter instance previously set on a transport using the transport set meter instance profile command.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the transports list command.	N/A
number	An existing transport. To display transport numbers, use the transports list command.	N/A
meterid	A number that represents a meter instance. The meter instance is set on a specific classifier profile using the classifier profile set rule meterid command.	N/A

Example --> transports set myrfc meter instance 1 disabled

See also
```
TRANSPORTS LIST
TRANSPORTS SET METER INSTANCE PROFILE
QOS (chapter X-QOS)
CLASSIFIER PROFILE SET RULE METERID
METER LIST PROFILES
```

8.5.1.1.7 TRANSPORTS SET METER INSTANCE PROFILE

Syntax `TRANSPORTS SET {<name>|<number>} METER INSTANCE <meterid> PROFILE <ProfileName>`

Description This command sets a meter profile on a transport for a specific meter instance. The meter instance matches a meter Id configured using the `CLASSIFIER PROFILE SET RULE METERID` command. This creates an association between the classified stream and the meter instance.

You can set multiple meter instances on an existing transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the `TRANSPORTS LIST` command.	N/A
number	An existing transport. To display transport numbers, use the `TRANSPORTS LIST` command.	N/A
meterid	A number that represents a meter instance. The meter instance is set on a specific classifier profile using the `CLASSIFIER PROFILE SET RULE METERID` command.	N/A
ProfileName	An existing meter profile. To display profile names, use the `METER LIST PROFILES` command.	N/A

Example --> transports set myrfc meter instance 1 mp1

See also `TRANSPORTS LIST`
`TRANSPORTS SET METER INSTANCE DISABLED`
`QOS (chapter X-QOS)`
`CLASSIFIER PROFILE SET RULE METERID`
`METER LIST PROFILES`

8.5.1.1.8 TRANSPORTS SET SCHEDULER PROFILE

Syntax `TRANSPORTS SET {<name>|<number>} SCHEDULER PROFILE <profile name>`

Description This command sets an existing scheduler profile on an existing transport. The outgoing traffic on the transport will be scheduled according to the configuration of the scheduler profile. Shaping and algorithmic dropping are also performed if configured in the scheduler profile.

The same profile can be added to more than one transport.

Note: If a scheduler profile is modified after setting on this transport, the new scheduler configuration is not applied to the transport automatically. You must enter this transport set scheduler profile command again with the correct profile specified in order to apply changes.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the TRANSPORTS LIST command.	N/A
number	An existing transport. To display transport numbers, use the TRANSPORTS LIST command.	N/A
profile name	An existing profile. To display profile names, use the SCHEDULER LIST PROFILES command.	N/A

Example --> transports set eth scheduler profile p1

See also TRANSPORTS LIST
TRANSPORTS SET SCHEDULER DISABLED
QOS (chapter X-QOS)
SCHEDULER ADD PROFILE
SCHEDULER LIST PROFILES
Scheduler CLI commands

8.5.1.1.9 TRANSPORTS SET SCHEDULER DISABLED

Syntax TRANSPORTS SET {<name>|<number>} SCHEDULER DISABLED

Description This command disables packet scheduling previously set on the specified transport using the transports set scheduler profile command. The scheduler is removed from the data path.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the TRANSPORTS LIST command.	N/A

Option	Description	Default Value
number	An existing transport. To display transport numbers, use the TRANSPORTS LIST command.	N/A

Example --> transports set eth scheduler disabled

See also
```
TRANSPORTS LIST
TRANSPORTS SET SCHEDULER PROFILE
SCHEDULER ADD PROFILE
SCHEDULER LIST PROFILES
```

8.5.1.1.10 TRANSPORTS SHOW

Syntax `TRANSPORTS SHOW {<name>|<number>}`

Description This command displays detailed information about an existing transport. The information displayed depends on the transport type selected. See below for examples of PPP and RFC1483 transport information.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing transport. To display transport names, use the TRANSPORTS LIST command.	N/A
number	An existing transport. To display transport numbers, use the TRANSPORTS LIST command.	N/A

Example Example 1- PPP transport

--> transports show pppoa1

```
PPP Status
PPP
Summary                : disabled
Server                 : true
Create Route           : true
Specific Route         : false
Subnet Mask            : 0.0.0.0
Route Mask             : 0.0.0.0
```

```
Hdlc                  : false
LLC                   : false
Lcp Max Configure     : 10
Lcp Max Failure       : 5
Lcp Max Terminate     : 2
Dialin Auth           : none
Dialout Username      :
Dialout Password      :
Dialout Auth          : none
Interface ID          : 2
Magic Number          : 0
MRU                   : 0
SVC                   : false
Remote Atm            :
IP Addr From IPCP     : true
Give DNSto Relay      : true
Give DNSto Client     : true
Lcp Echo Every        : 10
If In Octets          : 0
If Out Octets         : 0
If In Errors          : 0
If Out Errors         : 0
Packets Sent          : 0
Good Packets Received : 0
Enabled               : false
Termination           :
Hdlc Channel
Port                  : hdlc
Classifier
Clsfr Profile         : p1
Clsfr Encap           : PPPoA
```

Example 2 - RFC1483 transport

```
--> transports show myrfc1483
RFC1483 Status
RFC1483
Mode                : LlcBridged
If In Octets        : 0
If Out Octets       : 0
If In Errors        : 0
If Out Errors       : 0
Packets Sent        : 0
Good Packets Received : 0
```

```
Enabled              : true
Atm Channel
Tx Vci               : 600
Rx Vci               : 600
Peak Cell Rate       : 2000
Class                : UBR
Port                 : a1
Classifier
Clsfr Profile        : p1
Clsfr Encap          : Ethernet
```

See also TRANSPORTS LIST

8.6 Ethernet

Ethernet module it's an intermediate software layer used to interconnect an IP interface to a physical or virtual port where 802.3 frame type traffic is exchanged.

The Ethernet module is called every time an IP interface must be attached to a VLAN in order to be able to receive or send frames on this VLAN.

In this case it's necessary create an Ethernet module instance, named Ethernet transport, with the command ETHERNET ADD TRANSPORT VLAN. This command informs the system that this Ethernet module instance will manage only tagged frames with the 802.1Q VID value equals to the VLAN identifier defined when the VLAN has been created. All the other tagged frames that arrive to this module with 802.1Q VID value different from the VLAN identifier, will be considered invalid and discharged.

When an IP interface is attached to the Ethernet transport with the IP ATTACH command, the Ethernet transport object will remove the 802.1Q header from the incoming valid tagged frames and then it will pass these frames to the upper IP layer to be processed.

Note: Note that, inside the system, all frames are tagged. It's a responsibility of the external interfaces remove, if necessary, the 802.1Q header for outgoing frames and add the 802.1Q header for incoming untagged frames.

8.6.1 Ethernet command reference

This section describes the commands available on the AT-iMG/AT-iBG to manage the ***Ethernet*** module

8.6.1.1 Ethernet CLI commands

The table below lists the Ethernet commands provided by the CLI:

TABLE 8-5 Ethernet commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
ETHERNET ADD TRANSPORT							X	X	X
ETHERNET CLEAR TRANSPORTS							X	X	X
ETHERNET DELETE TRANSPORT							X	X	X
ETHERNET LIST PORTS							X	X	X
ETHERNET LIST TRANSPORTS							X	X	X
ETHERNET SET TRANSPORT PORT							X	X	X
ETHERNET SHOW TRANSPORT							X	X	X

8.6.1.1.1 ETHERNET ADD TRANSPORT

Syntax `ETHERNET ADD TRANSPORT <vlan_name | port>`

Description This command adds a named Ethernet transport and specify on which VLAN the module is listening for incoming frames or it is sending tagged frames.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
port	For ADSL B and ADSL C devices. It is the name of the port that identifies the ethernet transport class	ethernet0
vlan_name	For ADSL A devices The name of an existing vlan created with the VLAN ADD command. To display the list of existing vlans, use the VLAN SHOW command.	N/A

Example --> ethernet add transport vlan_2

See also ETHERNET LIST TRANSPORTS
ETHERNET LIST PORTS
PORT LIST

8.6.1.1.2 ETHERNET CLEAR TRANSPORTS

Syntax ETHERNET CLEAR TRANSPORTS

Description This command deletes all Ethernet transports that were created using the ETHERNET ADD TRANSPORT command.

Example --> ethernet clear transports

See also ETHERNET DELETE TRANSPORT

8.6.1.1.3 ETHERNET DELETE TRANSPORT

Syntax ETHERNET DELETE TRANSPORT {<name>|<number>}

Description This command deletes a single Ethernet transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing Ethernet transport. To display transport names, use the ETHERNET LIST TRANSPORTS command.	N/A
number	An existing Ethernet transport. To display transport numbers, use the ETHERNET LIST TRANSPORTS command.	N/A

Example --> ethernet delete transport eth1

See also ETHERNET LIST TRANSPORTS

8.6.1.1.4 ETHERNET LIST PORTS

Syntax ETHERNET LIST PORTS

Description This command lists the valid physical or virtual ports that can be used to transport Ethernet data.

Example --> ethernet list ports

```
Valid ethernet port names:
      ethernet1
      bunbridge
```

8.6.1.1.5 ETHERNET LIST TRANSPORTS

Syntax `ETHERNET LIST TRANSPORTS`

Description This command lists all Ethernet transports that have been created using the `ETHERNET ADD TRANSPORT` command. It displays the transport identification number and name, and the name of the port that it uses to transport Ethernet data.

Example --> ethernet list transports

```
Ethernet transports:
 ID  |    Name     |    Port
-----|-------------|------------
   1 | default     | ethernet0
   2 | t1          | bunbridge
   3 | vlan_2      | ethernet1
------------------------------
```

See also `ETHERNET LIST PORTS`

8.6.1.1.6 ETHERNET SET TRANSPORT PORT

Syntax `ETHERNET SET TRANSPORT {<name>|<number>} PORT <port>`

Description This command sets the port that an existing Ethernet transport uses to transport Ethernet data.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing Ethernet transport. To display transport names, use the `ETHERNET LIST TRANSPORTS` command.	N/A
number	An existing Ethernet transport. To display transport numbers, use the `ETHERNET LIST TRANSPORTS` command.	N/A
port	The system port that is used to transport Ethernet data. The same port cannot be used for more than one Ethernet transport at a time.	Ethernet

Example --> ethernet set transport eth1 port hdlc

See also `ETHERNET ADD TRANSPORT`
`ETHERNET LIST TRANSPORTS`
`PORT LIST`

8.6.1.1.7 ETHERNET SHOW TRANSPORT

Syntax `ETHERNET SHOW TRANSPORT {<name>|<number>}`

Description This command displays the name and port used by an existing Ethernet transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing Ethernet transport. To display transport names, use the `ETHERNET LIST TRANSPORTS` command.	N/A
number	An existing Ethernet transport. To display transport numbers, use the `ETHERNET LIST TRANSPORTS` command.	N/A

Example --> ethernet show transport eth1

```
Ethernet transport: vlan_2
Description: vlan_2
      Port: ethernet1
```

See also `ETHERNET LIST TRANSPORTS`

8.7 PPPoE

8.7.1 PPPoE Overview

The PPPoE (Point to Point Protocol over Ethernet) protocol provides user and network management, and accounting benefits to ISPs and network administrators as ISPs can easily control client connections for xDSL and cable modems as well as plain Ethernet networks. PPPoE is an extension of the standard Point to Point Protocol (PPP). The difference between them is expressed in transport method: PPPoE employs Ethernet instead of serial line connection.

Generally speaking, PPPoE is used to assign IP addresses to clients based on the user authentication as opposed to open connections where static IP addresses or DHCP are used.

PPPoE has two distinct stages. There is a Discovery stage and a PPP Session stage. When a Host wishes to initiate a PPPoE session, it must first perform Discovery to identify the Ethernet MAC address of the peer and establish a PPPoE SESSION_ID.

The PPPoE Discovery Stage is made up of four steps: initiation, offer, request, and session confirmation:

The PPPoE Active Discovery Initiation (PADI) packet:

The PPPoE client sends out a PADI packet to the broadcast address. This packet can also populate the "service-name" field if a service name has been entered on the dial-up networking properties of the PPPoE broadband connection. If a service name has not been entered, this field cannot be populated.

The PPPoE Active Discovery Offer (PADO) packet:

The PPPoE server, or Access Concentrator, should respond to the PADI with a PADO if the Access Concentrator is able to service the "service-name" field that had been listed in the PADI packet. If no "service-name" field had been listed, the Access Concentrator should respond with a PADO packet that has the "service-name" field populated with the service names that the Access Concentrator can service. The PADO packet is sent to the unicast address of the PPPoE client.

The PPPoE Active Discovery Request (PADR) packet:

When a PADO packet is received, the PPPoE client responds with a PADR packet. This packet is sent to the unicast address of the Access Concentrator. The client may receive multiple PADO packets, but the client responds to the first valid PADO that the client received. If the initial PADI packet had a blank "service-name" field filed, the client populates the "service-name" field of the PADR packet with the first service name that had been returned in the PADO packet.

The PPPoE Active Discovery Session-confirmation (PADS) packet:

When the PADR is received, the Access Concentrator generates unique session identification (ID) for the Point-to-Point Protocol (PPP) session and returns this ID to the PPPoE client in the PADS packet. This packet is sent to the unicast address of the client.

When this process has completed, the client is aware of the address of the Access Concentrator and a session ID has been established. At this point, a normal PPP session begins. This session can remain established until a PPPoE Active Discovery Terminate (PADT) packet is sent. The PADT may be sent by either the Access Concentrator or the PPPoE client.

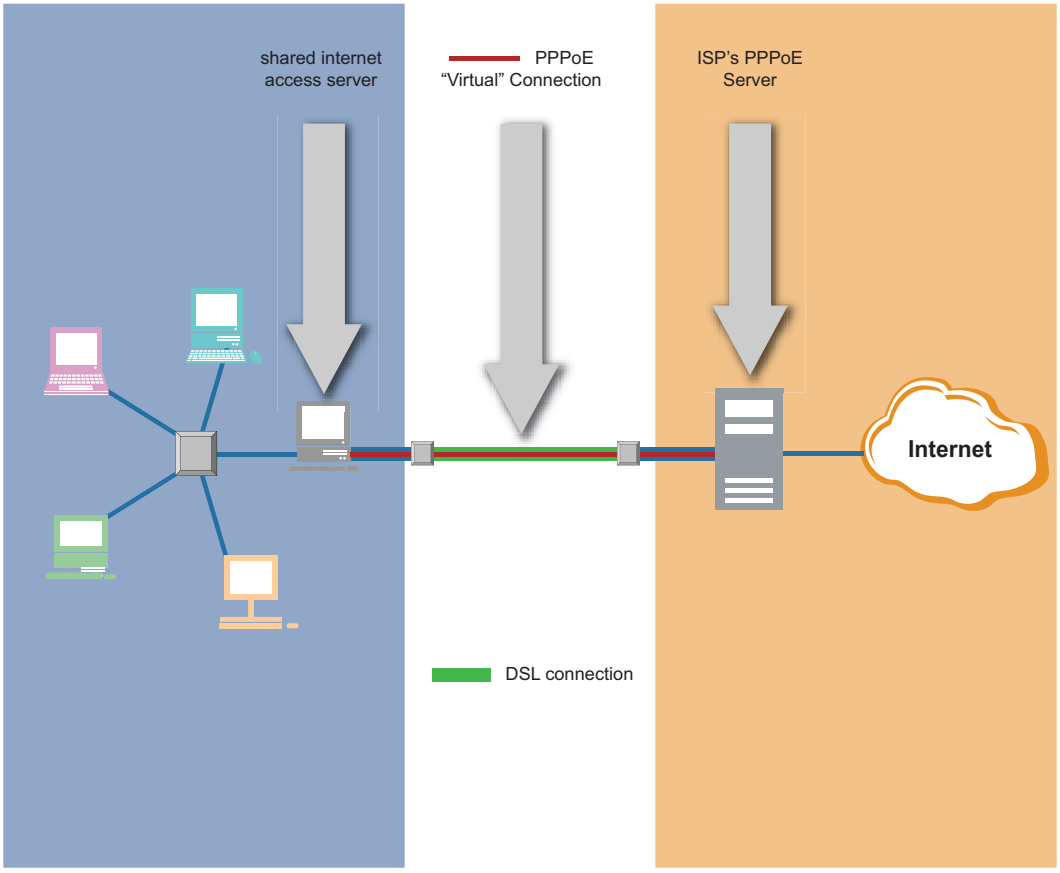


FIGURE 8-4 **Example of PPPoE connection**

8.7.2 PPPoE Functional Overview

8.7.2.1 PPPoE Connections

The system is designed to implement more than one embedded PPPoE clients able to connect to external Access Concentrators. It can support up to 8 PPP simultaneous connections (shared between PPPoE or PPPoA types).

8.7.2.2 PPPoE connections over ATM - VLAN Unaware

PPPoE connections can be established over a specific ATM channel without or without knowledge of VLANs.

If without, all PPPoE frames are untagged and are terminated directly on the IP layer without passing to the internal CPE bridging process. This limits this PPPoE application to those solutions where the sharing of the same ATM channel (VPI/VCI) between local PPP interfaces and internal user network traffic is not requiested. Such a solution implies a strict routed CPE configuration where internal user network traffic can be transported over an ATM channel already used by a PPP connection only if routed at the IP level.

The configuration of a PPPoE connection over ATM (PPPoEoA) it's performed in a three stage process:

- First, an un-numbered IP interface (all zeros ip address) must be created:
  ```
  ip add interface <ip_name>
  ```
- Second, a PPPoE transport object responsible for the PPPoE session management and PPPoE frames transmission must be created and the ATM channel specified:
  ```
  pppoe add transport <pppoe_name> dialout pvc <iface> a1 <vpi> <vci>
  ```
  This command must specify the ATM channel coordinates (VPI/VCI) where PPPoE frames will be exchanged (always as untagged frames only).
- Third, the un-numbered IP interface must be attached to the previously created PPPoE transport object.
  ```
  ip attach transport <ip_name> <pppoe_name>
  ```

8.7.2.3 PPPoE connections - VLAN Aware

PPPoE connections can also be established with knowledge of VLANs.

In this case the PPPoE transport is associated with the VLAN - and PPPoE traffic passes through the bridge - and flows out the ADSL interface - or an Ethernet interface - depending on the VLAN configuration.

The configuration of a PPPoE connection over ATM (PPPoEoA) is performed in a three stage process:

- First, an un-numbered IP interface (all zeros ip address) must be created:
  ```
  vlan create <pppoe_vlan> 512
  ip add interface <ip_name>
  ```
- Second, a PPPoE transport object responsible for the PPPoE session management and PPPoE frames transmission must be created and the VLAN specified: Note that the name of the pppoe transport must be **different** from the name used for the pppoe vlan.

  ```
  pppoe add transport <pppoe_name> dialout eth 2 <pppoe_vlan>
  ```

- Third, the un-numbered IP interface must be attached to the previously created PPPoE transport object.
  ```
  ip attach transport <ip_name> <pppoe_name>
  ```

8.7.2.4 Populating automatically routing table and DNS server table

During the PPP connection establishment, the Network Control Protocol IPCP is called to negotiate the IP address of the local end of the link and to retrieve, eventually, a list of DNS server ip addresses.

The negotiated local IP address is used to assign the ip address value to the un-numbered IP interface attached to the PPPoE transport. In this case when the PPP session is established, the un-numbered IP interface changes from having a null IP address to the new negotiated IP address and every time the PPP session is closed, the IP interface will revert back to having a null IP address.

Note: Note that, even if the IP interface is attached to a PPP transport, the IP subnet mask is assumed to be the class-based subnet mask of the IP address that has been allocated.

It's possible force the PPPoE transport to assign always a 32bit subnet mask (all ones) to the IP interface via the configuration command:

```
pppoe set transport <pppoe_name> subnetmask 255.255.255.255
```

In this way, independently of the IP address value assigned by the Remote Access Server, the IP interface will be configured as a single host address.

Note: Note that if more than one PPP connection is active at the same time on the CPE, adjacent IP addresses can fall into the same subnet causing the IP addresses assignment to fail. In this case, it's strongly suggested to force each PPPoE transport to assign a 32bit subnet mask (all ones) to the IP interface.

The PPPoE transport object is also able to set automatically the CPE default route to use the IP interface to which the PPPoE object is attached. By default this functionality is turned ON and can be deactivated or re-activated via the command:

```
pppoe set transport <pppoe_name> createroute disabled|enabled
```

Note: If more than one PPP connection is active at the same time on the CPE, all those, by default, will try to configure the default route causing possible problems on the proper packets routing. To avoid this, it's strongly suggested to have only one PPP session that drives the default route configuration.

Instead to create the default route when a PPP connection is established successfully, it's possible inform the PPPoE transport object to create a specific route based on the IP address of the Remote Access Server and a subnet mask configured manually. In this case the default route cannot be created automatically because the PPPoE transport object is able to create only one route (default or specific) at the same time. To inform the PPPoE module to create a specific rule instead of the default route, the following commands are used:

```
pppoe set transport <pppoe_name> specifyroute enabled
pppoe set transport <pppoe_name> routemask <specific_route_mask>
```

The capability of the PPPoE transport object to configure automatically the properties of other modules is also extended to the DNS Client and DNS Relay modules. It's possible force, during IPCP phase, the PPP module to

requests for DNS primary and secondary IP addresses and, if received, assigns them to the DNS Client and DNS relay lists respectively. This feature can be enabled via the commands:

```
pppoe set transport <pppoe_name> givedns client enabled|disabled
pppoe set transport <pppoe_name> givedns relay enabled|disabled
pppoe set transport <pppoe_name> discoverdns enabled|disabled
```

8.7.2.5 Configuration Option to Clamp Maximum TCP MSS Value

When using the PPPoE client on the iMG, either the iMG or the PPPoE concentrator/RAS should be configured to clamp the maximum TCP MSS value. For PPPoE the maximum mss is 1452.

On the iMG the command to perform this is `IP SET INTERFACE <ip interface> tcpmssclamp enabled` (Refer to 4.1.8.2.49.)

On a device such as one by Cisco, the command would be `ip tcp adjust -mss 1452`.

Note: Without this clamp, connectivity issues could occur, and access to some websites could fail.

8.7.3 Functional Differences in Product Categories

TABLE 8-6 Functional Mapping for PPPoE

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PPPOE CONNECTIONS	X	X	X	X	X	X	X	X	X
PPPOE CONNECTIONS OVER ATM - VLAN UNAWARE							X	X	X
PPPOE CONNECTIONS - VLAN AWARE	X	X	X	X	X	X	X	X	X
POPULATING AUTOMATICALLY ROUTING TABLE AND DNS SERVER TABLE	X	X	X	X	X	X	X	X	X

8.7.4 PPPoE command reference

This section describes the commands available to enable, configure and manage the *PPPoE* module.

8.7.4.1 PPPoE CLI commands

The table below lists the *PPPoE* commands provided by the CLI:

TABLE 8-7 *PPPoE* COMMANDS PROVIDED BY THE CLI

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PPPOE ADD TRANSPORT DIALOUT ETH	X	X	X	X	X	X	X	X	X
PPPOE ADD TRANSPORT DIALOUT PVC							X	X	X
PPPOE CLEAR TRANSPORTS	X	X	X	X	X	X	X	X	X
PPPOE DELETE TRANSPORT	X	X	X	X	X	X	X	X	X
PPPOE LIST TRANSPORTS	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT ACCESSCONCENTRATOR	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT AUTOCONNECT	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT AUTOCONNECT FILTER	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT BT	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT CONNECTNOW	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT CREATEROUTE	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT DIALOUT	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT DISCOVERDNS PRIMARY	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT DISCOVERDNS SECONDARY	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT DISCOVERIPSUBNET	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT ENABLED|DISABLED	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT ETH	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT EVENTLEVEL	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT HEADERS LLC	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT HEADERS LLC_ROUTED	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT HEADERS VCMUX_BRIDGED	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT HEADERS VCMUX_ROUTED	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT IDLETIME LANTRAFFICONLY	X	X	X	X	X	X	X	X	X

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PPPOE SET TRANSPORT IDLETIMEOUT	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT INTERFACE	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT LCPECHOEVERY	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT LCPMAXCONF	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT LCPMAXFAIL	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT LCPMAXTERM	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT LOCALIP	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT MANUALCONNECT	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT MAXREAUTHATTEMPTS	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT MBS	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT MCR	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT PASSWORD	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT PCR	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT PRILEVELS	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT PVC	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT QOSCLASS	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT RANDOMIZECONNECTIONATTEMPTS	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT REAUTHTIMER TR68	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT REMOTEDNS	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT REMOTEIP	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT ROUTEMASK	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT SCR	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT SERVICENAME	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT SPECIFICROUTE	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT START/STOP TEST	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT SUBNETMASK	X	X	X	X	X	X	X	X	X

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PPPOE SET TRANSPORT THEYLOGIN	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT USERNAME	X	X	X	X	X	X	X	X	X
PPPOE SET TRANSPORT WELOGIN	X	X	X	X	X	X	X	X	X
PPPOE SHOW TRANSPORT	X	X	X	X	X	X	X	X	X

8.7.4.1.1 PPPOE ADD TRANSPORT DIALOUT ETH

Syntax `PPPOE ADD TRANSPORT <name> DIALOUT ETH <interface> <vlan_name> [ACCESSCONCENTRATOR <concentrator>] [SERVICENAME <servicename>]`

Description This command creates a PPPoE transport that performs dialout over a VLAN. It allows you to specify the following PVC information:

- The VLAN name that will transport data
- Access concentrator (optional)
- Service name (optional)

OptionsThe following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Name	An arbitrary name that identifies the transport. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
Interface	The PPP interface to a channel that transports PPPoE data. The interface value must be the ID value of the IP interface that will be attached to the PPPoE transport. The IP ID value is reported by the command *ip list interfaces*.	N/A
vlan_name	The vlan name that will be used to transport PPPoE frames.	N/A
concentrator	A PPPoE tag that identifies a remote access concentrator (or PPPoE server). PPPoE will only connect to the named access concentrator. If no concentrator tag is set, PPPoE connects to the first access concentrator that responds. It is your ISP that determines the tag name/number.	N/A

service name	A PPPoE tag that identifies a specific service that is acceptable to the PPPoE client. If set, the PPPoE transport will connect to the first access concentrator it finds that uses this service. If an access concentrator is also set, the PPPoE transport will connect to the specified service on the named concentrator. It is your ISP that determines the service name.	N/A

Example `--> pppoe add transport pppoe_t dialout eth 2 vlan_2`

See also
```
PPPOE LIST TRANSPORTS
IP LIST INTERFACES
VLAN SHOW
```

8.7.4.1.2 PPPOE ADD TRANSPORT DIALOUT PVC

Syntax `PPPOE ADD TRANSPORT <name> DIALOUT PVC <interface> <port> <vpi> <vci> [ACCESSCONCENTRATOR <concentrator>] [SERVICENAME <service-name>]`

Description This command creates a PPPoE transport that performs dialout over a PVC (*Permanent Virtual Circuit*). It allows you to specify the following PVC information:

- The PPP interface to the channel that the PVC will use
- The ATM port that will transport data
- VPI (Virtual Path Identifier)
- VCI (Virtual Circuit Identifier)
- Access concentrator (optional)
- Service name (optional)

The port/VPI/VCI combination must be unique for each transport.

OptionsThe following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the transport. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A

interface	The PPP interface to a channel that transports PPPoE data. The interface value must be the ID value of the IP interface that will be attached to the PPPoE transport. The IP ID value is reported by the command *ip list interfaces*.	N/A
port	The system port that is used to transport ATM data.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A
vci	Part of the *ATM header*. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 1 and 65535.	N/A
concentrator	A PPPoE tag that identifies a remote access concentrator (or PPPoE server). PPPoE will only connect to the named access concentrator. If no concentrator tag is set, PPPoE connects to the first access concentrator that responds. It is your ISP that determines the tag name/number.	N/A
service name	A PPPoE tag that identifies a specific service that is acceptable to the PPPoE client. If set, the PPPoE transport will connect to the first access concentrator it finds that uses this service. If an access concentrator is also set, the PPPoE transport will connect to the specified service on the named concentrator. It is your ISP that determines the service name.	N/A

Example `--> pppoe add transport pppoe1 dialout pvc 1 a1 0 800 accessconcentrator server32 servicename mercury`

See also `PPPOE LIST TRANSPORTS`
`IP LIST INTERFACES`

8.7.4.1.3 PPPOE CLEAR TRANSPORTS

Syntax `PPPOE CLEAR TRANSPORTS`

Description This command deletes all PPPoE transports that were created using the pppoe add transport commands.

Example `--> pppoe clear transports`

See also `PPPOE DELETE TRANSPORT`

8.7.4.1.4 PPPOE DELETE TRANSPORT

Syntax `PPPOE DELETE TRANSPORT {<name>|<number>}`

Description This command deletes a single PPPoE transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A

Example `--> pppoe delete transport pppoe1`

See also `PPPOE LIST TRANSPORTS`

8.7.4.1.5 PPPOE LIST TRANSPORTS

Syntax `PPPOE LIST TRANSPORTS`

Description This command lists PPPoE transports that have been created using the pppoe add transport command. It displays the following information about the transports:

- Transport identification number
- Transport name
- Name of port used
- Virtual circuit identifier (vci) used (pvc transports only)
- Virtual path identifier (vpi) used (pvc transports only)

Example **Example**`--> pppoe list transports`

```
PPPoE transports:

 ID  |    Name    | Port      | Vci       | Vpi
-----|------------|-----------|-----------|-----------
   1 | p3         | realtek   | N/A       | N/A
   2 | p2         | a1        | 800       | 0
   3 | p1         | ethernet0 | N/A       | N/A
-------------------------------------------------
```

See also PPPOE SHOW TRANSPORT

8.7.4.1.6 PPPOE SET TRANSPORT ACCESSCONCENTRATOR

Syntax PPPOE SET TRANSPORT {<name>|<number>} ACCESSCONCENTRATOR <concentrator>

Description This command specifies the access concentrator that you want PPPoE to connect to.

You can also specify a service name using the set transport servicename command so that PPPoE will only accept a specific service via a specific access concentrator.

The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
concentrator	A PPPoE tag that identifies a remote access concentrator (or PPPoE server). PPPoE will only connect to the named access concentrator. If no concentrator tag is set, PPPoE connects to the first access concentrator that responds. The tag name/number is determined by your ISP.	Empty string

Example --> pppoe set transport pppoe1 accessconcentrator server5

See also PPPOE LIST TRANSPORTS
PPPOE SET TRANSPORT SERVICENAME
PPPOE SHOW TRANSPORT

Note: For more information on PPPoE and access concentrators, see RFC2516; http://www.ietf.org/rfc/rfc2516.txt

8.7.4.1.7 PPPOE SET TRANSPORT AUTOCONNECT

Syntax PPPOE SET TRANSPORT {<name>|<number>} AUTOCONNECT {ENABLED|DISABLED}

Description This command allows you to enable/disable the *PPPoE autoconnect* function. If enabled, PPPoE automatically connects to TCP/IP whenever a user requests TCP/IP packets from a public destination.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
enabled	Enables PPPoE autoconnect.	disabled
disabled	Disables PPPoE autoconnect.	

Example `--> pppoe set transport pppoe1 autoconnect enabled`

See also `PPPOE LIST TRANSPORTS`
`PPPOE SET TRANSPORT AUTOCONNECT FILTER`

8.7.4.1.8 PPPOE SET TRANSPORT AUTOCONNECT FILTER

Syntax `PPPOE SET TRANSPORT {<name>|<number>} AUTOCONNECT FILTER {ADD|DELETE} {TCPPORT <tcpportadd>|UDPPORT <udpportadd>}`

Description This command allows you to add filters to TCP/UDP ports to prevent PPP from autoconnecting with certain IP packets.

- Certain IP packet types may force an unwanted autoconnect sequence. Setting a filter on the port used by these packets prevents them from starting PPP autoconnect.
- The delete option allows you to clear an existing autoconnect filter.

Note: This command is only effective if you have already enabled PPP autoconnection using `PPPOE SET TRANSPORT AUTOCONNECT`

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
add	Adds an autoconnect filter to the specified port.	N/A
delete	Deletes an existing autoconnect filter from the specified port.	N/A
tcpportadd	The TCP port that you want to set the autoconnect filter on.	N/A
udpportadd	The UDP port that you want to set the autoconnect filter on.	N/A

Example This example creates a filter to prevent TCP SNMPTRAP packets from starting *PPP autoconnect*:

Example --> pppoe set transport pppoe1 autoconnect filter add tcpport 162

See also `PPPOE LIST TRANSPORTS`
`PPPOE SET TRANSPORT AUTOCONNECT`

8.7.4.1.9 PPPOE SET TRANSPORT BT

Syntax `PPPOE SET TRANSPORT {<name>|<number>} BT <burst tolerance>`

Description his command sets the burst tolerance (bt) for an existing PPPoE transport. This command is only valid if you set VBR or VBR RT as the QoS Class using the pppoe set transport qosclass command.

Options he following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A

burst tolerance	Controls the duration of traffic bursts on VBR (Variable Bit Rate) and VBR RT (VBR Real Time) channels. This value overrides an existing MBS value (if set). The BT can be any value between 0 and 100.	0

Example `--> pppoe set transport pppoe1 bt 5`

See also `PPPOE SET TRANSPORT MBS`

8.7.4.1.10 PPPOE SET TRANSPORT CONNECTNOW

Syntax `PPPOE SET TRANSPORT {<name>|<number>} CONNECTNOW {ENABLED|DISABLED}`

Description This command is used to send a manual connectio request to the specified PPPoE transport through CLI. The "manualconnect" option should be "enabled" before enabling connectnow.

When disabled, this command tears down the specified PPPoE connection.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	Gives manual connection request when "manualconnect" is enabled.	enabled
disabled	Gives a manual disconnect request.	

Example `--> pppoe set transport pppoe1 connectnow enabled`

Syntax `PPPOE SHOW TRANSPORT`
`PPPOE SET TRANSPORT MANUALCONNECT`

8.7.4.1.11 PPPOE SET TRANSPORT CREATEROUTE

Syntax `PPPOE SET TRANSPORT {<name>|<number>} CREATEROUTE {ENABLED|DISABLED}`

Description This command specifies whether a route is added to the system after IPCP (*Internet Protocol Control Protocol*) negotiation is completed. If set to enabled, a route will be created which directs packets to the remote end of the PPP link.

This route can either be a default route or a specific route, depending on the value set using the pppoe set transport specificroute command.

To display the createroute setting, use the `PPPOE SHOW TRANSPORT` command. The route is removed when the PPP link is disconnected.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	Adds a route to the system after IPCP negotiation.	enabled
disabled	Does not add a route to the system after IPCP negotiation.	

Example `--> pppoe set transport pppoe1 createroute disabled`

Syntax `PPPOE SHOW TRANSPORT  PPPOE SET TRANSPORT SPECIFICROUTE IP LIST ROUTES`

8.7.4.1.12 PPPOE SET TRANSPORT DIALOUT

Syntax `PPPOE SET TRANSPORT {<name>|<number>} DIALOUT`

Description This command sets a PPPoE transport to perform dialout over a PVC (*Permanent Virtual Circuit*). This replaces the transports existing dialin/dialout setting. The transport uses the interface that was specified when the transport was created.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A

number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A

Example `--> pppoe set transport pppoe2 dialout`

See also `PPPOE LIST TRANSPORTS`

8.7.4.1.13 PPPOE SET TRANSPORT DISCOVERDNS PRIMARY

Syntax `PPPOE SET TRANSPORT {<name>|<number>} DISCOVERDNS PRIMARY {ENABLED|DISABLED}`

Description This command enables/disables whether the primary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is enabled. The default setting for the `PPPOE SET TRANSPORT GIVEDNS` command is also enabled.

Note: You must enable one of the pppoe set transport givedns commands in order for this command setting to work. See `PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED` *or* `PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED`

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	A primary DNS server IP address is requested.	enabled
disabled	A primary DNS server IP address is not requested.	

Example `--> pppoe set transport pppoe3 discoverdns primary enabled`

See also
```
PPPOE SET TRANSPORT DISCOVERDNS SECONDARY
PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED
PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED
PPPOE SET TRANSPORT REMOTEDNS
```

8.7.4.1.14 PPPOE SET TRANSPORT DISCOVERDNS SECONDARY

Syntax `PPPOE SET TRANSPORT {<name>|<number>} DISCOVERDNS SECONDARY {ENABLED|DISABLED}`

Description This command enables/disables whether the secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is enabled. The default setting for the `PPPOE SET TRANSPORT GIVEDNS` commanD is also enabled.

Note: You must enable one of the pppoe set transport givedns commands in order for this command setting to work. See `PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED` *or* `PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED`

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	A secondary DNS server IP address is requested.	enabled
disabled	A secondary DNS server IP address is not requested.	

Example `--> pppoe set transport pppoe3 discoverdns secondary enabled`

See also `PPPOE SET TRANSPORT DISCOVERDNS PRIMARY`
`PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED`
`PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED`
`PPPOE SET TRANSPORT REMOTEDNS`

8.7.4.1.15 PPPOE SET TRANSPORT DISCOVERIPSUBNET

Syntax `PPPOE SET TRANSPORT {<name>|<number>} DISCOVERIPSUBNET {ENABLED|DISABLED}`

Description This command enables/disables PPP IPCP subnet discovery. Once enabled, PPP can discover the link subnet (4 octets) from the service for the Point to Point link. The actual IPCP option is 0x90 (option 144). This is similar to discovering the primary and secondary DNS addresses with IPCP.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
enabled	Enables PPP IPCP subnet discovery.	disabled
disabled	Disables PPP IPCP subnet discovery.	

Example `--> pppoe set transport pppoe3 discoveripsubnet enabled`

See also PPPOE SHOW TRANSPORT

8.7.4.1.16 PPPOE SET TRANSPORT ENABLED|DISABLED

Syntax `PPPOE SET TRANSPORT {<name>|<number>} {ENABLED|DISABLED}`

Description This command explicitly enables/disables a PPPoE transport. Attaching a transport to an interface implicitly enables it, but for cases where no attach is performed (for example, multiple channels on an interface, a PPP session that is not attached but needed for testing purposes) the transport must be enabled explicitly.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
enabled	Enables a PPPoE transport.	disabled

disabled	Disables a PPPoE transport.	

Example `--> pppoe set transport pppoe1 enabled`

See also **See also** `PPPOE LIST TRANSPORTS`

8.7.4.1.17 PPPOE SET TRANSPORT ETH

Syntax `PPPOE SET TRANSPORT {<name>|<number>} ETH <port>`

Description This command sets the Ethernet port that an existing *PPPoE transport* uses to transport PPPoE data.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use `THE PPPOE LIST TRANSPORTS` command.	N/A
port	The system port that is used to transport Ethernet data. To display Ethernet ports, use the ethernet list ports command.	N/A

Example `--> pppoe set transport pppoe3 eth ethernet0`

See also `PPPOE LIST TRANSPORTS`
`ETHERNET LIST PORTS`

8.7.4.1.18 PPPOE SET TRANSPORT EVENTLEVEL

Syntax `PPPOE SET TRANSPORT {<name>|<number>} EVENTLEVEL <pppeventlevel>`

Description This command sets a debugging tracing event level for PPP. The <pppeventlevel> can be any level between 1 and 9.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
pppevent level	The debug tracing level from 1 to 9. 1: Only very serious errors reported 2: Definite protocol errors or very significant events are reported 3: Links going up/down reported 4: Every packet and significant state change is reported. 5: Every packet sent/received is disassembled and hex dumped 6: Levels 1-5 plus assignment of the IP addresses to the interface and extra authentication information (CHAP/PAP) reported. 7: Levels 1-6 plus tunneling reported. 8: Levels 1-7 plus minor phase changes reported. 9: Levels 1-8 plus all timer information reported.	1

Example `pppoe set transport pppoe1 pppeventlevel 6`

See also **See also** `PPPOE LIST TRANSPORTS`

8.7.4.1.19 PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED

Syntax `PPPOE SET TRANSPORT {<name>|<number>} GIVEDNS CLIENT {ENABLED | DISABLED}`

Description This command controls whether the *PPP Internet Protocol Control Protocol* (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

You must have the DNS client process included in your image build in order to use this protocol.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
enabled	IPCP can request a DNS server IP address and then give the address to DNS client.	enabled
disabled	IPCP cannot request a DNS server IP address and then give the address to DNS client.	

```
--> pppoe set transport pppoe1 givedns client enabled
```

See also
```
PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED
PPPOE SET TRANSPORT REMOTEDNS
PPPOE SET TRANSPORT DISCOVERDNS PRIMARY
PPPOE SET TRANSPORT DISCOVERDNS SECONDARY
```

8.7.4.1.20 PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED

Syntax `PPPOE SET TRANSPORT {<name>|<number>} GIVEDNS RELAY {ENABLED | DISABLED}`

Description This command controls whether the PPP *Internet Protocol Control Protocol* (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

You must have the DNS relay process included in your image build in order to use this protocol.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
enabled	IPCP can request a DNS server IP address and then give the address to DNS relay.	enabled
disabled	IPCP cannot request a DNS server IP address and then give the address to DNS relay.	

Example `--> pppoe set transport pppoe1 givedns relay enabled`

See also `PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED`
`PPPOE SET TRANSPORT DISCOVERDNS PRIMARY`
`PPPOE SET TRANSPORT DISCOVERDNS SECONDARY`
`PPPOE SET TRANSPORT REMOTEDNS`

8.7.4.1.21 PPPOE SET TRANSPORT HEADERS LLC

Syntax `PPPOE SET TRANSPORT {<name>|<number>} HEADERS LLC {ENABLED|DISABLED}`

Description This command allows you to enable/disable whether your system can transmit and receive packets containing *LLC_bridged headers*. To disable this encapsulation, you need to enable some other type of encapsulation. For example, if you want ot use llc_routed encapsulation, use the PPPOE SET TRANSPORT HEADERS LLC_ROUTED ENABLED command. Then llc_routed packets will be transmitted and received instead of llc_bridged packets.

PPP determines which format to use to transmit/receive packets by "learning" the format information from incoming packet headers.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
enabled	Packets that have LLC headers can be transmitted/received.	enabled
disabled	Packets that have LLC headers can not be transmitted/ received.	

Example `--> pppoe set transport pppoe1 headers llc enabled`

See also
```
PPPOE LIST TRANSPORTS
PPPOE SHOW TRANSPORT
PPPOE SET TRANSPORT HEADERS LLC
```

8.7.4.1.22 PPPOE SET TRANSPORT HEADERS LLC_ROUTED

Syntax `PPPOE SET TRANSPORT {<name>|<number>} HEADERS LLC_ROUTED {ENABLED|DISABLED}`

Description This command allows you to enable/disable whether your system can transmit and receive packets containing *llc_routed packets*. If you want LLC_bridged packets to be transmitted and received instead of llc_routed packets, use the PPPOE SET TRANSPORT HEADERS LLC ENABLED command.

When *llc_routed headers* are disabled, the default encapsulation method is *llc_bridged*. PPP determines which format to use to transmit/receive packets by 'learning' the format information from incoming packet headers.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A

number	An existing PPPoE transport. To display transport numbers, use THE PPPOE LIST TRANSPORTS command.	N/A
enabled	The encapsulation method to be used is llc_routed	Disabled
disabled	Packets that have llc_routed headers cannot be transmitted/received.	

Example `--> pppoe set transport pppoe1 headers llc_routed enabled`

See also
`PPPOE LIST TRANSPORTS`
`PPPOE SHOW TRANSPORT`
`PPPOE SET TRANSPORT HEADERS LLC`

8.7.4.1.23 PPPOE SET TRANSPORT HEADERS VCMUX_BRIDGED

Example `PPPOE SET TRANSPORT {<name>|<number>} HEADERS VCMUX_BRIDGED {ENABLED|DISABLED}`

Description This command allows you to enable/disable whether your system can transmit and receive packets containing *vcmux_bridged packets*. If you want vcmux_routed packets to be transmitted and received instead of vcmux_bridged packets, use the `PPPOE SET TRANSPORT HEADERS VCMUX_ROUTED` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use THE PPPOE LIST TRANSPORTS command.	N/A
enabled	The encapsulation method to be used is Vcmux Bridged	Disabled
disabled	Packets that have vcmux_bridged headers cannot be transmitted/received.	

Example `--> pppoe set transport pppoe1 headers vcmux_bridged enabled`

See also PPPOE LIST TRANSPORTS
PPPOE SHOW TRANSPORT
PPPOE SET TRANSPORT HEADERS LLC

8.7.4.1.24 PPPOE SET TRANSPORT HEADERS VCMUX_ROUTED

Syntax PPPOE SET TRANSPORT {<name>|<number>} HEADERS VCMUX_BRIDGED {ENABLED|DISABLED}

Description This command allows you to enable/disable whether your system can transmit and receive packets containing *vcmux_routed packets*. If you want vcmux_bridged packets to be transmitted and received instead of vcmux_routed packets, use the PPPOE SET TRANSPORT HEADERS VCMUX_BRIDGEDcommand.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use THE PPPOE LIST TRANSPORTS command.	N/A
enabled	The encapsulation method to be used is Vcmux Routed	Disabled
disabled	Packets that have vcmux_routed headers cannot be transmitted/received.	

Example --> pppoe set transport pppoe1 headers vcmux_bridged enabled

See also PPPOE LIST TRANSPORTS
PPPOE SHOW TRANSPORT
PPPOE SET TRANSPORT HEADERS LLC

8.7.4.1.25 PPPOE SET TRANSPORT IDLETIME LANTRAFFICONLY

Syntax PPPOE SET TRANSPORT {<name>|<number>} IDLETIME LANTRAFFICONLY {ENABLED|DISABLED}

Description This command allows you to specify that the value of ideltime which has been set, to be valid when there is no IP activity on the lan side. With the ideltime lantrafficonly set as disabled, the value of ideltime takes into account the IP traffic from the wan side also. However when set as enabled, it takes only the lan side IP traffic into account.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	Enable the ideltimeout for LAN traffic only	Disabled
disabled	Include WAN traffic for the idletimeout interval.	

Example `--> pppoe set transport pppoe1 idletime lantrafficonly enabled`

See also `PPPOE LIST TRANSPORTS`
`PPOE SET TRANSPORT LCPECHOEVERY`

8.7.4.1.26 PPPOE SET TRANSPORT IDLETIMEOUT

Syntax `PPPOE SET TRANSPORT {<name>|<number>} IDLETIMEOUT <idletimeout>`

Description This command allows you to set a 'idle' time out for your LAN connection. If you are connected to an ISP via PPPoE but fail to send a request for data within a specified time limit, the PPPoE session is disabled.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A

idletimeout	The length of time (in minutes) that a PPPoE session connected to an ISP can remain idle before the session is disabled. The time can be any value between 0 and 60. A value of 0 means that no idletimeout is set.	0

Example `--> pppoe set transport pppoe1 idletimeout 20`

See also `PPPOE LIST TRANSPORTS`
`PPOE SET TRANSPORT LCPECHOEVERY`

8.7.4.1.27 PPPOE SET TRANSPORT INTERFACE

Syntax `PPPOE SET TRANSPORT {<name>|<number>} INTERFACE <interface>`

Description This command sets the PPP interface for an existing PPPoE transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
interface	The PPP interface to a channel that transports PPPoE data. Multiple channels can use a single interface. The interface value can be any positive integer.	N/A

Example `--> pppoe set transport pppoe2 interface 4`

See also `PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`

8.7.4.1.28 PPPOE SET TRANSPORT LCPECHOEVERY

Syntax `PPPOE SET TRANSPORT {<name>|<number>} LCPECHOEVERY <interval>`

Description This command tells a specified PPP transport to send an LCP (*Link Control Protocol*) echo request frame at specified intervals (in seconds). If no reply to the request is received, the PPP connection is torn down. This functionality is also known as 'keep-alive'.

If you do not want to send LCP echo frames, specify zero (0) in the <interval> attribute.

Options The following table gives the range of values for each optionthat can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
interval	The length of time (in seconds) between LCP echo request frames being sent. If you do not want echo request frames to be sent, specify '0' as the interval.	10 seconds

Example `--> pppoe set transport pppoe2 lcpechoevery 0`

See also `PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`

8.7.4.1.29 PPPOE SET TRANSPORT LCPMAXCONF

Syntax `PPOE SET TRANSPORT {<name>|<number>} LCPMAXCONF <lcp max configure>`

Description This command sets the *Link Control Protocol* (LCP) maximum configure number for an existing PPPoE transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A

lcp max configure	*Link Control Protocol*: the maximum number of configures that can be transmitted without reply before assuming that the destination address is unable to respond. The LCPmaxconf can be any positive value.	10

Example `--> pppoe set transport pppoe1 lcpmaxconf 20`

See also `PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`

8.7.4.1.30 PPPOE SET TRANSPORT LCPMAXFAIL

Syntax `PPPOE SET TRANSPORT {<name>|<number>} LCPMAXFAIL <lcp max fail>`

Description This command sets the *Link Control Protocol* (LCP) maximum fail number for an existing PPPoE transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use `THE PPPOE LIST TRANSPORTS` command.	N/A
lcp max fail	*Link Control Protocol*: the maximum number of consecutive negative acknowledgements (indicating that the information received contains errors) that can be transmitted before assuming that parameter negotiation is not converging. The LCPmaxfail can be any positive value.	5

Example `--> pppoe set transport pppoe1 lcpmaxfail 20`

See also `PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`

8.7.4.1.31 PPPOE SET TRANSPORT LCPMAXTERM

Syntax `PPPOE SET TRANSPORT {<name>|<number>} LCPMAXTERM <lcp max terminate>`

Description This command sets the *Link Control Protocol* (LCP) maximum terminate number for an existing PPPoE transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
lcp max term	*Link Control Protocol*: the maximum number of consecutive Terminate Requests that will be sent without reply before assuming that the destination address is unable to respond. The LCPfailterm can be any positive value.	2

Example `--> pppoe set transport pppoe1 lcpmaxterm 20`

See also `PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`

8.7.4.1.32 PPPOE SET TRANSPORT LOCALIP

Syntax `PPPOE SET TRANSPORT {<name>|<number>} LOCALIP <ip-address>`

Description This command tells the PPP process the local IP address to be associated with the client-end of an interface. This enables remote users to have dialin access via the channel(s) that the interface is attached to.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A

ip-address	The IP address of the local 'client-end' of an interface displayed in the following format: 111.222.254.4	0.0.0.0

Example `--> pppoe set transport pppoe1 localip 192.168.103.2`

See also
`PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`
`PPPOE SET TRANSPORT REMOTEIP`

8.7.4.1.33 PPPOE SET TRANSPORT MANUALCONNECT

Syntax `PPPOE SET TRANSPORT {<name>|<number>} MANUALCONNECT {ENABLED|DISABLED}`

Description This command enales/disables the manual connect option for a givien PPPoE transport. In this mode, the connection to the network is initiated manually through a GUI request of a CLI command and by default, terminates only when done so explicitly by a user, dur ot power loss, or when the connection is lost.

When the manual connect option is enabled, the autoconnect feature of the device is automatically disabled.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	Enable the "manualconnect" option	Disabled
disabled	Disable the "manualconnect" option	

Example `--> pppoe set transport pppoe1 manualconnect enabled`

Description
`PPPOE LIST TRANSPORTS`
`PPOE SET TRANSPORT LCPECHOEVERY`

8.7.4.1.34 PPPOE SET TRANSPORT MAXREAUTHATTEMPTS

Syntax `PPPOE SET TRANSPORT {<name>|<number>} MAXREAUTHATTEMPTS <max reauthattempts>`

Description This command is used to specify the number of re-authentication attempts in case of authentication failure. After the specified number of re-authentication attempts fail, there would be no more configure requests from PPPoE transports until the unsername and/or password are reset.

A zero (default) value specifies inifinate connection attempts.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
maxreauthattempts	A number tht specifies the maximum re-authentication requests that can be made	0

Example `--> pppoe set transport pppoe3 maxreauthattempts 10`

See also `PPPOE SET TRANSPORT REAUTHTIMER`

8.7.4.1.35 PPPOE SET TRANSPORT MBS

Syntax `PPPOE SET TRANSPORT {<name>|<number>} MBS <max burst size>`

Description This command sets the maximum burst size (MBS) for an existing PPPoE transport that performs dialout over PVC.

Description This command is only valid if you set VBR or VBR RT as the QoS Class using the `PPPOE SET TRANSPORT QUOSCLASS` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
maximum burst size	Controls the maximum burst size for VBR (Variable Bit Rate) and VBR RT (VBR Real Time) channels. This value overrides an existing BT value (if set). The MBS can be any value between 0 and 100.	0

Example `--> pppoe set transport pppoe3 mbs 10`

See also `PPPOE SET TRANSPORT BT`
`PPPOE SET TRANSPORT QOSCLASS`

8.7.4.1.36 PPPOE SET TRANSPORT MCR

Syntax `PPPOE SET TRANSPORT {<name>|<number>} MCR <min cell rate>`

Description This command sets the minimum cell rate for an existing PPPoE transport that performs dialout over PVC.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
minimum cell rate	Determines the minimum rate at which ATM cells may be sent along the PPPoE transport.	0

Example `--> pppoe set transport pppoe2 mcr 0`

See also `PPPOE SET TRANSPORT PCR`

8.7.4.1.37 PPPOE SET TRANSPORT PASSWORD

Syntax `PPPOE SET TRANSPORT {<name>|<number>} PASSWORD <password>`

Description This command sets a dialout password on a named transport. The password is required when PPP negotiation takes place and is supplied to the remote PPP server for authentication.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
password	An arbitrary word that acts as a dialout password enabling the login to the remote end. The PPP server requires the password when remote login is performed. It can be made up of one or more characters and/or digits. To display the password, use the `PPPOE SHOW TRANSPORT` command.	N/A

Example `--> pppoe set transport pppoe2 password mercury`

See also
`PPPOE LIST TRANSPORTS`
`PPPOE SHOW TRANSPORT`
`PPPOE SET TRANSPORT USERNAME`

8.7.4.1.38 PPPOE SET TRANSPORT PCR

Syntax `PPPOE SET TRANSPORT {<name>|<number>} PCR <peak cell rate>`

Description This command sets the peak cell rate (pcr) for an existing PPPoE transport that performs dialout over PVC.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
peak cell rate	Determines the maximum rate at which ATM cells may be sent along the PPPoE transport. The PCR can be any value from 0 up to the maximum PortSpeed parameter set when the port was created (using the *initbun* file in *FlashFS* or the CLI command PORT SET).	0

Example `--> pppoe set transport pppoe2 pcr 50000`

See also `PPPOE SET TRANSPORT MCR`

8.7.4.1.39 PPPOE SET TRANSPORT PRILEVELS

Syntax `PPPOE SET TRANSPORT {<name>|<number>} PRILEVELS <prilevels>`

Description This command enables support for multiple packet priority levels on the same ATM VC.

Two prilevel values are supported:

- There are no multiple priority levels enabled so the feature is disabled.
- Packets with different priorities set (such as best effort and high priority traffic) are prioritized on the same ATM VC.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
prilevels	The number of priority levels available on an ATM transport.	1

Example `--> pppoe set transport myrfc prilevels 2`

See also `PPPOE SHOW TRANSPORT`

8.7.4.1.40 PPPOE SET TRANSPORT PVC

Syntax `PPPOE SET TRANSPORT {<name>|<number>} PVC <port> <vpi> <vci>`

Description This command sets the PVC information for an existing PPPoE transport PVC. The PVC uses the interface that was specified when the transport was created.

The command allows you to specify the following PVC information:

- The ATM port that will transport data
- VPI (*Virtual Path Identifier*)
- VCI (*Virtual Circuit Identifier*)
- The port/VPI/VCI combination must be unique for each transport

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
port	The system port that is used to transport ATM data.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 1 and 65535.	N/A

Example `--> pppoe set transport pppoe2 pvc a1 0 800`

See also `PPOE SET TRANSPORT DIALOUT`
`PPPOE LIST TRANSPORTS`
`PORT LIST`

8.7.4.1.41 PPPOE SET TRANSPORT QOSCLASS

Syntax `PPPOE SET TRANSPORT {<name>|<number>} QOSCLASS {UBR|CBR|VBR|VBRRT|ABR|QFC}`

Description This command sets the quality of service class for an existing PPPoE transport that performs dialout over PVC.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
ubr	Unspecified Bit Rate; non-constant and unpredictable data transport rate. PCR (Peak Cell Rate) is the average and maximum speed of transmission.	UBR
cbr	Constant Bit Rate; constant demand and predictable data transport rate. PCR is the average and maximum speed of transmission.	
vbr	Variable Bit Rate; non-constant but predictable data transport rate that uses Non-Real-Time (NRT). You can specify the PCR, SCR, BT and MBS for VBR traffic.	
vbrrt	Variable Bit Rate Real-Time; non-constant but predictable data transport rate that uses Real-Time (RT). You can specify the PCR, SCR, BT and MBS for VBRRT traffic.	
abr	Available Bit Rate; non-constant and unpredictable data transport rate that provides ATM-layer feedback and flow control.	
qfc	QFC; ATM flow control protocol that supports ABR.	

Example `--> pppoe set transport pppoe3 abr`

See also `PPPOE SHOW TRANSPORT`
`PPPOE SET TRANSPORT QOSCLASS`

8.7.4.1.42 PPPOE SET TRANSPORT RANDOMIZECONNECTIONATTEMPTS

Syntax `PPPOE SET TRANSPORT {<name>|<number>} RANDOMIZECONNECTIONATTEMPTS {ENABLED|DISABLED}`

Description This command is used to specify that a device should incorporate a ramdom timing delay prior to starting each IP and PPP session. This random timing delay helps to reduce connection failures when a group of users attempts to establish connections to a service provider at the same time (such as after retoration of power after an outage.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	Enable the "randomizeconnectionattempts" option	Disabled
disabled	Disable the "randomizeconnectionattempts" option	

Example `--> pppoe set transport pppoe1 randomizeconnectionattempts enabled`

See also `PPPOE LIST TRANSPORTS`

8.7.4.1.43 PPPOE SET TRANSPORT REAUTHTIMER TR68

Syntax `PPPOE SET TRANSPORT {<name>|<number>} REAUTHTIMER TR68 {ENABLED|DISABLED}`

Description This command is used to specify that a device should not attempt imediately for additional PPP session connections upon receipt of an authentication failure. A back-off mechanism limits the repeated attempts to reconnect in this situation. Three connection attempts are made with a gap of 10 seconds, followed by a delay of five minutes, then repeated by thee next sequence of connection attempts.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
enabled	Enable the "reauthtimer" option	Disabled
disabled	Disable the "reauthtimer" option	

Example `--> pppoe set transport pppoe1 randomizeconnectionattempts enabled`

See also `PPPOE LIST TRANSPORTS`

8.7.4.1.44 PPPOE SET TRANSPORT REMOTEDNS

Syntax `PPPOE SET TRANSPORT {<name>|<number>} REMOTEDNS <ipaddress> [<ipaddress2>]`

Description This command is a PPP server function.

This command sets the primary and secondary local DNS server addresses that will be given to a remote PPP peer when the peer requests a primary or secondary DNS server IP address using IPCP. Setting the secondary IP address is optional.

If you want to delete an IP address, set the IP address to 0.0.0.0.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A

ipaddress	The ip address of the primary local DNS server displayed in the following format: 192.168.102.3	0.0.0.0 (no primary address set)
ipaddress2	The ip address of the secondary local DNS server displayed in the following format: 192.168.102.3	0.0.0.0 (no secondary address set)

Example 1 - setting a primary address

```
--> pppoe set transport pppoe1 remotedns 192.168.102.3
```

Example 2 - setting primary and secondary addresses

```
--> pppoe set transport pppoe1 remotedns 192.168.102.3 192.168.105.1
```

Example 3 - deleting an address

To delete an address, set it to 0.0.0.0. The example below deletes the secondary address that was set in Example Two:

```
--> pppoe set transport pppoe1 remotedns 192.168.102.3 0.0.0.0
```

See also

```
PPPOE SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED
PPPOE SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED
PPPOE SET TRANSPORT DISCOVERDNS PRIMARY
PPPOE SET TRANSPORT DISCOVERDNS SECONDARY
```

8.7.4.1.45 PPPOE SET TRANSPORT REMOTEIP

Syntax `PPPOE SET TRANSPORT {<name>|<number>} REMOTEIP <ip-address>`

Description This command sets the IP address supplied to the remote end of the PPP connection during negotiation. This is particularly important for PPP dialin transports.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
ip-address	The IP address of the local 'server-end' of an interface displayed in the following format: 111.222.254.4	0.0.0.0

Example `--> pppoe set transport pppoe1 remoteip 192.168.103.2`

See also `PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`
`PPPOE SET TRANSPORT LOCALIP`

8.7.4.1.46 PPPOE SET TRANSPORT ROUTEMASK

Syntax `PPPOE SET TRANSPORT {<name>|<number>} ROUTEMASK <mask>`

Description This command sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to 0.0.0.0, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (*Internet Protocol Control Protocol*) negotiation.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the pppoe list transports command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the pppoe list transports command.	N/A
mask	The subnet mask that is used for the route that is created when a PPP link comes up. 0.0.0.0	0.0.0.0

Example `--> pppoe set transport pppoe1 routemask 0.0.0.0`

See also `PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`

8.7.4.1.47 PPPOE SET TRANSPORT SCR

Syntax `PPPOE SET TRANSPORT {<name>|<number>} SCR <sustainable cell rate>`

Description This command sets the sustainable cell rate for an existing PPPoE transport that performs dialout over PVC. This command is only valid if you set VBR or VBR RT as the QoS Class using the pppoe set transport qosclass command.

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
sustainable cell rate	the average cell rate for a VBR or VBR RT connection. The SCR can be any positive value that is less than the PortSpeed and the PCR for the channel.	0

Example `--> pppoe set transport pppoe2 scr 25000`

See also `PPPOE SET TRANSPORT QOSCLASS`

8.7.4.1.48 PPPOE SET TRANSPORT SERVICENAME

Syntax `PPPOE SET TRANSPORT {<name>|<number>} SERVICENAME <service-name>`

Description This command specifies the service name that is acceptable to the PPPoE client.

You can also set the access concentrator using the set transport accessconcentrator command so that PPPoE will only accept a specific service via a specific access concentrator.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
service name	A PPPoE tag that identifies a specific service that is acceptable to the PPPoE client. If set, the PPPoE transport will connect to the first access concentrator it finds that uses this service. If an access concentrator is also set, the PPPoE transport will connect to the specified service on the named concentrator. It is your ISP that determines the service name.	Empty string

Example `--> pppoe set transport pppoe1 servicename jupiter`

See also
`PPPOE LIST TRANSPORTS`
`PPPOE SET TRANSPORT ACCESSCONCENTRATOR`
`PPPOE SHOW TRANSPORT`

Note: For more information on PPPoE and service names, see RFC2516 http://www.ietf.org/rfc/rfc2516.txt

8.7.4.1.49 PPPOE SET TRANSPORT SPECIFICROUTE

Syntax `PPOE SET TRANSPORT {<name>|<number>} SPECIFICROUTE {ENABLED | DISABLED}`

Description This command specifies whether the route created when a PPP link comes up is a specific or default route. If set to enabled, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Note: This command is only valid if the PPPOE SET TRANSPORT CREATEROUTE *command is set to enabled. If the* CREATEROUTE *command is set to disabled, no route is created and therefore the* PPPOE SET TRANSPORT SPECIFICROUTE *command is ignored.*

The mask for the route is calculated from the class of the remote subnet unless an alternative has been specified using the PPPOE SET TRANSPORT ROUTEMASK command. If *specificroute* is set to 'disabled', a default route to the subnet at the remote end of the PPP link is created. Note that the current setting of this command is ignored if PPPOE SET TRANSPORT CREATEROUTE command is set to disabled.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
enabled	Allows the created route to apply to packets for the subnet at the remote end of the PPP link.	disabled
disabled	A default route to the subnet at the remote end of the PPP link is created.	

Example `--> pppoe set transport pppoe1 specificroute disabled`

See also PPPOE SET TRANSPORT ROUTEMASK
PPPOE SET TRANSPORT CREATEROUTE
PPPOE LIST TRANSPORTS

8.7.4.1.50 PPPOE SET TRANSPORT START/STOP TEST

Syntax PPPOE SET TRANSPORT {<name>|<number>} START/STOP TEST

Description This command starts and stops a PPPoE test on a transport.

Example `--> pppoe set transport START/STOP TEST`

See also `PPPOE LIST TRANSPORTS`

8.7.4.1.51 PPPOE SET TRANSPORT SUBNETMASK

Syntax `PPPOE SET TRANSPORT {<name>|<number>} SUBNETMASK <mask>`

Description This command sets the subnet mask used for the local IP interface connected to the PPP transport. If the value 0.0.0.0 is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
mask	The subnet mask used by the local IP interface connected to the PPP transport.	0.0.0.0

Example `--> pppoe set transport pppoe1 subnetmask 255.255.255.0`

See also `PPPOE LIST TRANSPORTS`

8.7.4.1.52 PPPOE SET TRANSPORT THEYLOGIN

Syntax `PPPOE SET TRANSPORT {<name>|<number>} THEYLOGIN {NONE|PAP|CHAP}`

Description This command sets the authentication method that remote PPP clients must use to dialin to the server. If authentication is used, clients must use the specified authentication method and provide the username set using the `SYSTEM ADD USER` command.

This command is only valid if the user had *maydialin* set using the `SYSTEM SET LOGIN MAYDIALIN` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
none	No authentication method was set.	None
pap	*Password Authentication Protocol*: the server sends an authentication request to the remote user dialing in. PAP passes the unencrypted username and password and identifies the remote end.	
chap	*Challenge Handshake Authentication Protocol*; the server sends an authentication request to the remote user dialing in. PAP passes the encrypted username and password and identifies the remote end.	

Example `--> pppoe set transport pppoe2 theylogin pap`

See also
```
PPPOE LIST TRANSPORTS
PPPOE SHOW TRANSPORT
SYSTEM ADD USER
SYSTEM SET USER MAYDIALIN
```

8.7.4.1.53 PPPOE SET TRANSPORT USERNAME

Syntax `PPPOE SET TRANSPORT {<name>|<number>} USERNAME <username>`

Description This command sets a (dialout) username on a named transport. The username is required when PPP negotiation takes place and is supplied to the remote PPP server for authentication.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A

number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
username	A name that identifies a user and, together with the dialout password, enables a user to login to the remote end. The PPP server will require the username when the user wants to login remotely. It can be made up of one or more characters and/or digits. To display the username, use the PPPOE SHOW TRANSPORT command.	N/A

Example `--> pppoe set transport pppoe2 username jsmith`

See also `PPPOE SET TRANSPORT PASSWORD`

8.7.4.1.54 PPPOE SET TRANSPORT WELOGIN

Syntax `PPPOE SET TRANSPORT {<name>|<number>} WELOGIN {NONE|AUTO|PAP|CHAP}`

Description This command sets the authentication protocol used to connect to external PPP servers (dialout).

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the PPPOE LIST TRANSPORTS command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the PPPOE LIST TRANSPORTS command.	N/A
none	No authentication method is used.	None
auto	The authentication protocol used by the remote PPP server is discovered and used.	
pap	*Password Authentication Protocol*; the server sends an authentication request to the remote user dialing in. PAP passes the unencrypted username and password and identifies the remote end.	

chap	*Challenge Handshake Authentication Protocol*; the server sends an authentication request to the remote user dialing in. PAP passes the encrypted username and password and identifies the remote end.	

Example `--> pppoe set transport pppoe2 theylogin pap`

See also `PPPOE SET TRANSPORT THEYLOGIN`
`PPPOE SHOW TRANSPORT`
`PPPOE LIST TRANSPORTS`

8.7.4.1.55 PPPOE SHOW TRANSPORT

Syntax `PPPOE SHOW TRANSPORT {<name>|<number>}`

Description This command displays the following information about an existing PPPoE transport:

- Description
- Interface number
- Server - dialin status
- Headers - the data format that the transport can accept or receive
- SVC status (false)
- Local IP address
- Subnet mask
- Remote IP address
- Remote DNS
- Propagate DNS to client (true or false)
- Propagate DNS to relay (true or false)
- Create route (true or false)
- Specific route (true or false)
- Route netmask
- Dialout Username
- Dialout Password
- Dialout Authentication method
- Dialin Authentication method

- LCP Max Configure
- LCP Max Failure
- LCP Max Terminate
- LCP Echo Every
- Autoconnect status (true or false)
- User Idle Timeout setting (in minutes)
- Access concentrator
- Service name
- Port name
- VPI (PVC transport only)
- VCI (PVC transport only)
- Quality of Service (QoS) class (PVC transport only)
- Peak cell rate (PVC transport only)
- Burst tolerance (PVC transport only)
- Sustainable Cell Rate (SCR) (PVC transport only)
- Maximum burst size (MBS) (PVC transport only)
- Maximum Cell Rate (MCR) (PVC transport only)
- Packet Priority Levels setting

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoE transport. To display transport names, use the `PPPOE LIST TRANSPORTS` command.	N/A
number	An existing PPPoE transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A

Example

```
--> pppoe show transport ppp-ext
PPP Transport: ppp-ext
```

```
          Description: ppp-ext
         Interface ID: 2                 Server: false

   PPPoE Admin State: true
        PPPoE Status: open for IP, sent 130901, received 143026
  PPPoE Error Status:

  Remote NCP Address: 151.99.57.156
        HDLC Headers: false
         LLC Headers: false
                 SVC:
              IPv6CP: false
            Local IP: 0.0.0.0
         Subnet Mask: 255.255.255.255
Discover IPCP Subnet: false
           Remote IP: 0.0.0.0
          Remote DNS: 0.0.0.0
    Propogate DNS to client: false  To relay: true

        Create route: true
      Specific route: false
       Route netmask: 0.0.0.0

    Dialout username: MyUsername
    Dialout password: MyPassword
       Dialout auth.: auto
        Dialin auth.: none

      LCP Max. Conf.: 10
    LCP Max. Failure: 5
   LCP Max Terminate: 2
      LCP Echo Every: 10

         Autoconnect: false
   User Idle Timeout: 0
 PPP Reconnect Timer: 0

 Access Concentrator:
        Service Name:

           VLAN name:

               ATM Port : a1
                 Tx VPI : 8
                 Rx VPI : 8
                 Tx VCI : 35
                 Rx VCI : 35
```

```
          ATM Traffic Class : UBR
             Peak Cell Rate : 7000
            Burst Tolerance : N/A
      Sustainable Cell Rate : N/A
             Max Burst Size : N/A
              Min Cell Rate : N/A
    Packet Priority Levels : N/A
```

See also PPPOE LIST TRANSPORTS

8.8 PPPoA

8.8.1 PPPoA command reference

8.8.1.1 PPPoA CLI commands

This chapter describes the ***PPPoA*** commands provided by the CLI:

TABLE 8-8 PPPOA Command

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PPPOA ADD TRANSPORT DIALIN PVC							X	X	X
PPPOA ADD TRANSPORT DIALOUT PVC								X	X
PPPOA CLEAR TRANSPORTS							X	X	X
PPPOA DELETE TRANSPORT							X	X	X
PPPOA LIST TRANSPORTS							X	X	X
PPPOA SET TRANSPORT AUTOCONNECT							X	X	X
PPPOA SET TRANSPORT BT							X	X	X
PPPOA SET TRANSPORT CREATEROUTE								X	X
PPPOA SET TRANSPORT DIALIN PVC							X	X	X
PPPOA SET TRANSPORT DIALOUT PVC							X	X	X
PPPOA SET TRANSPORT DISCOVERDNS PRIMARY							X	X	X
PPPOA SET TRANSPORT DISCOVERDNS SECONDARY							X	X	X
PPPOA SET TRANSPORT ENABLED|DISABLED							X	X	X

TABLE 8-8 PPPOA Command

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PPPOA SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED								X	X
PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED							X	X	X
PPPOA SET TRANSPORT HEADERS HDLC							X	X	X
PPPOA SET TRANSPORT HEADERS LLC								X	X
PPPOA SET TRANSPORT IDLETIMEOUT							X	X	X
PPPOA SET TRANSPORT INTERFACE							X	X	X
PPPOA SET TRANSPORT LCPECHOEVERY							X	X	X
PPPOA SET TRANSPORT LCPMAXCONF							X	X	X
PPPOA SET TRANSPORT LCPMAXFAIL							X	X	X
PPPOA SET TRANSPORT LCPMAXTERM							X	X	X
PPPOA SET TRANSPORT LOCALIP							X	X	X
PPPOA SET TRANSPORT MBS								X	X
PPPOA SET TRANSPORT MCR							X	X	X
PPPOA SET TRANSPORT PASSWORD							X	X	X
PPPOA SET TRANSPORT PCR							X	X	X
PPPOA SET TRANSPORT PORT							X	X	X
PPPOA SET TRANSPORT PRILEVELS							X	X	X
PPPOA SET TRANSPORT PVC							X	X	X
PPPOA SET TRANSPORT QOSCLASS								X	X
PPPOA SET TRANSPORT REMOTEDNS							X	X	X
PPPOA SET TRANSPORT REMOTEIP							X	X	X
PPPOA SET TRANSPORT ROUTEMASK							X	X	X
PPPOA SET TRANSPORT SCR							X	X	X
PPPOA SET TRANSPORT SPECIFICROUTE							X	X	X

TABLE 8-8 PPPOA Command

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PPPOA SET TRANSPORT SUBNETMASK								X	X
PPPOA SET TRANSPORT THEYLOGIN							X	X	X
PPPOA SET TRANSPORT USERNAME							X	X	X
PPPOA SET TRANSPORT VCI							X	X	X
PPPOA SET TRANSPORT VPI							X	X	X
PPPOA SET TRANSPORT WELOGIN							X	X	X
PPPOA SHOW TRANSPORT							X	X	X

8.8.1.1.1 PPPOA ADD TRANSPORT DIALIN PVC

Example PPPOA ADD TRANSPORT <name> DIALIN PVC <interface> <port> <vpi> <vci>

- This command creates a PPPoA transport that accepts dialling connections over a PVC (***Permanent Virtual Circuit***). It allows you to specify the following information:
- The PPP interface to the channel that the PVC will use
- The ATM port that will transport data
- VPI (***Virtual Path Identifier***)
- VCI (***Virtual Circuit Identifier***)

The port/VPI/VCI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the transport. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interface	The PPP interface to a channel that transports PPPoA data. Multiple channels can use a single interface. The interface value can be any positive integer.	N/A
port	The system port that is used to transport ATM data.	N/A

Option	Description	Default Value
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 1 and 65535.	N/A

Example --> pppoa add transport pppoa1 dialin pvc 1 a1 0 800

See also
```
PPPOA LIST TRANSPORTS
PPPOA SET TRANSPORT VCI
PPPOA SET TRANSPORT VPI
PORT LIST
```

8.8.1.1.2 PPPOA ADD TRANSPORT DIALOUT PVC

Syntax `PPPOA ADD TRANSPORT <name> DIALOUT PVC <interface> <port> <vpi> <vci>`

Description This command creates a PPPoA transport that performs dialout over a PVC (***Permanent Virtual Circuit***). It allows you to specify the following PVC information:

- The PPP interface to the channel that the PVC will use
- The ATM port that will transport data
- VPI (***Virtual Path Identifier***)
- VCI (***Virtual Circuit Identifier***)

The port/VPI/VCI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the transport. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
interface	The PPP interface to a channel that transports PPPoA data. Multiple channels can use a single interface. The interface value can be any positive integer.	N/A
port	The system port that is used to transport ATM data.	N/A

Option	Description	Default Value
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 1 and 65535.	N/A

Example --> pppoa add transport pppoa1 dialout pvc 1 a1 0 800

See also `PPPOA LIST TRANSPORTS`
`PORT LIST`

8.8.1.1.3 PPPOA CLEAR TRANSPORTS

Syntax `PPPOA CLEAR TRANSPORTS`

Description This command deletes all PPPoA transports that were created using the `PPPOA ADD TRANSPORT` commands.

Example --> pppoa clear transports

See also `PPPOA DELETE TRANSPORT`

8.8.1.1.4 PPPOA DELETE TRANSPORT

Syntax `PPPOA DELETE TRANSPORT {<name>|<number>}`

Description This command deletes a single PPPoA transport. The PVC or SVC attached to the transport is also deleted.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A

Example --> pppoa delete transport pppoa1

See also `PPPOA LIST TRANSPORTS`

8.8.1.1.5 PPPOA LIST TRANSPORTS

Syntax `PPPOA LIST TRANSPORTS`

Description This command lists PPPoA transports that have been created using the `PPPOA ADD TRANSPORT` commands. It displays the following information about the transports:

- Transport identification number
- Transport name
- ATM port used (if applicable)
- ***Virtual Circuit Identifier*** (VCI) used (if applicable)
- ***Virtual Path Identifier*** (VPI) used (if applicable)

Example --> pppoa list transports

```
PPPOA transports:
 ID  |    Name    | Port      | Vci       | Vpi
-----|------------|-----------|-----------|-----------
   1 | p2         | N/A       | N/A       | N/A
   2 | p1         | a1        | 800       | 0
-------------------------------------------------------
```

See also `PPPOA SHOW TRANSPORT`

8.8.1.1.6 PPPOA SET TRANSPORT AUTOCONNECT

Syntax `PPPOA SET TRANSPORT {<name>|<number>} AUTOCONNECT {ENABLED|DISABLED}`

Description This command allows you to enable/disable the PPPoA autoconnect function. If enabled, PPPoA automatically connects to TCP/IP whenever a user requests TCP/IP packets from a public destination.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
enabled	Enables PPPoA autoconnect.	disabled

Option	Description	Default Value
disabled	Disables PPPoA autoconnect.	

Example --> pppoa set transport pppoa1 autoconnect enabled

See also PPPOA LIST TRANSPORTS

8.8.1.1.7 PPPOA SET TRANSPORT BT

Syntax PPPOA SET TRANSPORT {<name>|<number>} BT <burst tolerance>

Description This command applies to existing PVC transports - it does not apply to SVC transports. This command sets the ***Burst Tolerance*** (BT) for an existing PPPoA transport. This command is only valid if you set VBR or VBR RT as the QoS Class using the PPPOA SET TRANSPORT QOSCLASS command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
burst tolerance	Controls the duration of traffic bursts on VBR (***Variable Bit Rate***) and VBR RT (***VBR Real Time***) channels. This value overrides an existing MBS value (if set). The BT can be any value between 0 and 100.	0

Example --> pppoa set transport pppoa1 bt 5

See also PPPOA SET TRANSPORT MBS

8.8.1.1.8 PPPOA SET TRANSPORT CREATEROUTE

Syntax PPPOA SET TRANSPORT {<name>|<number>} CREATEROUTE {ENABLED|DISABLED}

Description This command specifies whether a route is added to the system after IPCP (***Internet Protocol Control Protocol***) negotiation is completed. If set to enabled, a route will be created which directs packets to the remote end of the PPP link.

This route can either be a default route or a specific route, depending on the value set using the PPPOA SET TRANSPORT SPECIFICROUTE command.

To display the ***createroute*** setting, use the PPPOA SHOW TRANSPORT command. The route is removed when the PPP link is disconnected.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
enabled	Adds a route to the system after IPCP negotiation.	enabled
disabled	Does not add a route to the system after IPCP negotiation.	

Example --> pppoa set transport pppoa1 createroute disabled

See also PPPOA SHOW TRANSPORT
PPPOA SET TRANSPORT SPECIFICROUTE

8.8.1.1.9 PPPOA SET TRANSPORT DIALIN PVC

Syntax PPPOA SET TRANSPORT {<name>|<number>} DIALIN PVC <port> <vpi> <vci>

Description This command sets an existing PPPoA transport to accept dialin connections over a PVC (***Permanent Virtual Circuit***). This replaces the transports existing dialin/dialout setting over PVC/SVC. The PVC uses the interface that was specified when the transport was created.

The command allows you to specify the following PVC information:

- The ATM port that will transport data
- VPI (***Virtual Path Identifier***)
- VCI (***Virtual Circuit Identifier***)

The port/VPI/VCI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
port	The system port that is used to transport ATM data.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A

Example --> pppoa set transport pppoa2 dialin pvc a1 0 800

See also PPPOA LIST TRANSPORTS
PPPOA SET TRANSPORT DIALOUT PVC
PORT LIST

8.8.1.1.10 PPPOA SET TRANSPORT DIALOUT PVC

Syntax PPPOA SET TRANSPORT {<name>|<number>} DIALOUT PVC <port> <vpi> <vci>

Description This command sets a PPPoA transport to perform dialout over a PVC (***Permanent Virtual Circuit***). This replaces the transports existing dialin/dialout setting over PVC/SVC. The PVC uses the interface that was specified when the transport was created.

The command allows you to specify the following PVC information:

- The ATM port that will transport data
- VPI (***Virtual Path Identifier***)
- VCI (***Virtual Circuit Identifier***)

The port/VPI/VCI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
port	The system port that is used to transport ATM data.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 1 and 65535.	N/A

Example --> pppoa set transport pppoa2 dialout pvc a1 0 800

See also PPPOA LIST TRANSPORTS
PPPOA SET TRANSPORT DIALIN PVC
PORT LIST

8.8.1.1.11 PPPOA SET TRANSPORT DISCOVERDNS PRIMARY

Syntax PPPOA SET TRANSPORT {<name>|<number>} DISCOVERDNS PRIMARY {ENABLED|DISABLED}

Description This command enables/disables whether the primary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is enabled. The default setting for the pppoa set transport givedns commands is also enabled.

Note: You must enable one of the PPPOA SET TRANSPORT GIVEDNS *commands in order for this command setting to work. See* PPPOA SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED *or* PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
enabled	A primary DNS server IP address is requested.	enabled
disabled	A primary DNS server IP address is not requested.	

Example --> pppoa set transport pppoa3 discoverdns primary enabled

See also PPPOA SET TRANSPORT DISCOVERDNS SECONDARY
PPPOA SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED
PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED
PPPOA SET TRANSPORT REMOTEDNS

8.8.1.1.12 PPPOA SET TRANSPORT DISCOVERDNS SECONDARY

Syntax PPPOA SET TRANSPORT {<name>|<number>} DISCOVERDNS SECONDARY {ENABLED|DISABLED}

Description This command enables/disables whether the secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is enabled. The default setting for the PPPOA SET TRANSPORT GIVEDNS commands is also enabled.

Note: You must enable one of the PPPOA SET TRANSPORT GIVEDNS *commands in order for this command setting to work. See* PPPOA SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED *or* PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
enabled	A secondary DNS server IP address is requested.	enabled

Option	Description	Default Value
disabled	A secondary DNS server IP address is not requested.	

Example --> pppoa set transport pppoa3 discoverdns secondary enabled

See also
```
PPPOA SET TRANSPORT DISCOVERDNS PRIMARY
PPPOA SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED
PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED
PPPOA SET TRANSPORT REMOTEDNS
```

8.8.1.1.13 PPPOA SET TRANSPORT ENABLED|DISABLED

Syntax
```
PPPOA SET TRANSPORT {<name>|<number>} {ENABLED|DISABLED}
```

Description This command explicitly enables/disables a PPPoA transport. Attaching a transport to an interface implicitly enables it, but for cases where no attach is performed (for example, multiple channels on an interface, a PPP session that is not attached but needed for testing purposes) the transport must be enabled explicitly.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
enabled	Enables a PPPoA transport.	disabled
disabled	Disables a PPPoA transport.	

Example --> pppoa set transport pppoa1 enabled

See also `PPPOA LIST TRANSPORTS`

8.8.1.1.14 PPPOA SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED

Syntax
```
PPPOA SET TRANSPORT {<name>|<number>} GIVEDNS CLIENT
{ENABLED | DISABLED}
```

Description This command controls whether the PPP ***Internet Protocol Control Protocol*** (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

You must have the DNS client process included in your image build in order to use this protocol.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use THE PPPOA LIST TRANSPORTS command.	N/A
enabled	IPCP can request a DNS server IP address and then give the address to DNS client.	enabled
disabled	IPCP cannot request a DNS server IP address and then give the address to DNS client.	

Example --> pppoa set transport pppoa1 givedns client enabled

See also PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED
PPPOA SET TRANSPORT REMOTEDNS
PPPOA SET TRANSPORT DISCOVERDNS PRIMARY
PPPOA SET TRANSPORT DISCOVERDNS SECONDARY
DNS Client CLI commands

8.8.1.1.15 PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED

Syntax PPPOA SET TRANSPORT {<name>|<number>} GIVEDNS RELAY {ENABLED | DISABLED}

Description This command controls whether the PPP ***Internet Protocol Control Protocol*** (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

You must have the DNS relay process included in your image build in order to use this protocol.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPP0A LIST TRANSPORTS command.	N/A
number	An existing pppoa transport. To display transport numbers, use the PPP0A LIST TRANSPORTS command.	N/A
enabled	IPCP can request a DNS server IP address and then give the address to DNS relay.	enabled
disabled	IPCP cannot request a DNS server IP address and then give the address to DNS relay.	

Example --> pppoa set transport pppoa1 givedns relay enabled

See also PPP0A SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED
PPP0A SET TRANSPORT REMOTEDNS
PPP0A SET TRANSPORT DISCOVERDNS PRIMARY
PPP0A SET TRANSPORT DISCOVERDNS SECONDARY
DNS Relay CLI commands

8.8.1.1.16 PPPOA SET TRANSPORT HEADERS HDLC

Syntax PPP0A SET TRANSPORT {<name>|<number>} HEADERS HDLC {ENABLED|DISABLED}

Description This command allows you to enable/disable whether your system can transmit and receive packets containing HDLC headers. If you want LLC packets to be transmitted and received instead of/as well as HDLC packets, use the PPP0A SET TRANSPORT HEADERS LLC ENABLED command.

When both HDLC and LLC headers are disabled, the default encapsulation method is VC multiplexed (VC Mux). PPP determines which format to use to transmit/receive packets by 'learning' the format information from incoming packet headers.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
enabled	Packets that have HDLC headers can be transmitted/received.	Disabled (if LLC headers are disabled too, the default value is VC Mux)
disabled	Packets that have HDLC headers cannot be transmitted/received.	

Example --> pppoa set transport pppoa1 headers hdlc enabled

See also PPPOA LIST TRANSPORTS
PPPOA SHOW TRANSPORT
PPPOA SET TRANSPORT HEADERS LLC

8.8.1.1.17 PPPOA SET TRANSPORT HEADERS LLC

Syntax PPPOA SET TRANSPORT {<name>|<number>} HEADERS LLC {ENABLED|DISABLED}

Description This command allows you to enable/disable whether your system can transmit and receive packets containing LLC headers. If you want HDLC packets to be transmitted and received instead of/as well as LLC packets, use the PPPOA SET TRANSPORT HEADERS HDLC ENABLED command.

When both LLC and HDLC headers are disabled, the default encapsulation method is VC multiplexed (VC Mux). PPP determines which format to use to transmit/receive packets by 'learning' the format information from incoming packet headers.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOE LIST TRANSPORTS` command.	N/A
enabled	Packets that have LLC headers can be transmitted/ received.	Disabled (if HDLC headers are disabled too, the default value is VC Mux)
disabled	Packets that have LLC headers cannot be transmitted/ received.	

Example --> pppoa set transport pppoa1 headers llc enabled

Options
```
PPPOA LIST TRANSPORTS
PPPOA SHOW TRANSPORT
PPPOA SET TRANSPORT HEADERS HDLC
```

8.8.1.1.18 PPPOA SET TRANSPORT IDLETIMEOUT

Syntax `PPPOA SET TRANSPORT {<name>|<number>} IDLETIMEOUT <idletimeout>`

Description This command allows you to set some 'idle' time out for your LAN connection. If you are connected to an ISP via PPPoA but fail to send a request for data within a specified time limit, the PPPoA session is disabled.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A

Option	Description	Default Value
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
idletimeout	The length of time (in minutes) that a PPPoA session connected to an ISP can remain idle before the session is disabled. The time can be any value between 0 and 60. A value of 0 means that no idletimeout is set.	0

Example --> pppoa set transport pppoa1 idletimeout 20

See also PPPOA LIST TRANSPORTS
PPPOA SET TRANSPORT LCPECHOEVERY

8.8.1.1.19 PPPOA SET TRANSPORT INTERFACE

Syntax PPPOA SET TRANSPORT {<name>|<number>} INTERFACE <interface>

Description This command sets the PPP interface for an existing PPPoA transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
interface	The PPP interface to a channel that transports PPPoA data. Multiple channels can use a single interface. The interface value can be any positive integer.	N/A

Example --> pppoa set transport pppoa2 interface 4

See also PPPOA SHOW TRANSPORT
PPPOA LIST TRANSPORTS

8.8.1.1.20 PPPOA SET TRANSPORT LCPECHOEVERY

Syntax PPPOA SET TRANSPORT {<name>|<number>} LCPECHOEVERY <interval>

Description This command tells a specified PPP transport to send an LCP (***Link Control Protocol***) echo request frame at specified intervals (in seconds). If no reply to the request is

received, the PPP connection is torn down. This functionality is also known as 'keep-alive'.

If you do not want to send LCP echo frames, specify zero (0) in the <interval> attribute.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
interval	The length of time (in seconds) between LCP echo request frames being sent. If you do not want echo request frames to be sent, specify '0' as the interval.	10 seconds

Example --> pppoa set transport pppoa2 lcpechoevery 0

See also `PPPOA SHOW TRANSPORT`
`PPPOA LIST TRANSPORTS`

8.8.1.1.21 PPPOA SET TRANSPORT LCPMAXCONF

Syntax `PPPOA SET TRANSPORT {<name>|<number>} LCPMAXCONF <lcp max configure>`

Description This command sets the ***Link Control Protocol*** (LCP) maximum configure number for an existing PPPoA transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A

Option	Description	Default Value
lcp max configure	***Link Control Protocol***; the maximum number of configures that can be transmitted without reply before assuming that the destination address is unable to respond. The LCPmaxconf can be any positive value.	10

Example --> pppoa set transport pppoa1 lcpmaxconf 20

See also `PPPOA SHOW TRANSPORT`
`PPPOA LIST TRANSPORTS`

8.8.1.1.22 PPPOA SET TRANSPORT LCPMAXFAIL

Syntax `PPPOA SET TRANSPORT {<name>|<number>} LCPMAXFAIL <lcp max fail>`

Description This command sets the ***Link Control Protocol*** (LCP) maximum fail number for an existing PPPoA transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
lcp max fail	***Link Control Protocol***; the maximum number of consecutive negative acknowledgements (indicating that the information received contains errors) that can be transmitted before assuming that parameter negotiation is not converging. The LCPmaxfail can be any positive value.	5

Example --> pppoa set transport pppoa1 lcpmaxfail 20

See also `PPPOA SHOW TRANSPORT`
`PPPOA LIST TRANSPORTS`

8.8.1.1.23 PPPOA SET TRANSPORT LCPMAXTERM

Syntax `PPPOA SET TRANSPORT {<name>|<number>} LCPMAXTERM <lcp max terminate>`

Description This command sets the ***Link Control Protocol*** (LCP) maximum terminate number for an existing PPPoA transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
lcp max term	***Link Control Protocol***; the maximum number of consecutive Terminate Requests that will be sent without reply before assuming that the destination address is unable to respond. The LCPfailterm can be any positive value.	2

Example --> pppoa set transport pppoa1 lcpmaxterm 20

See also PPPOA SHOW TRANSPORT
PPPOA LIST TRANSPORTS

8.8.1.1.24 PPPOA SET TRANSPORT LOCALIP

Syntax PPPOA SET TRANSPORT {<name>|<number>} LOCALIP <ip-address>

Description This command is only applicable to dialin SVC or PVC transports that provide the server-end of a connection. The command tells the PPP process the local IP address to be associated with the client-end of an interface. This allows remote users to have dialin access via the channel(s) that the interface is attached to.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use THE PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A

Option	Description	Default Value
ip-address	The ip address of the local 'client-end' of an interface displayed in the following format: 111.222.254.4	0.0.0.0

Example --> pppoa set transport pppoa1 localip 192.168.103.2

See also
```
PPPOA SHOW TRANSPORT
PPPOA LIST TRANSPORTS
PPPOA SET TRANSPORT REMOTEIP
```

8.8.1.1.25 PPPOA SET TRANSPORT MBS

Syntax `PPPOA SET TRANSPORT {<name>|<number>} MBS <max burst size>`

Description This command applies to existing PVC transports - it does not apply to SVC transports. It sets the ***Maximum Burst Size*** (MBS) for the PPPoA transport.

This command is only valid if you set VBR or VBR RT as the QoS Class using the pppoa set transport quosclass command.

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
maximum burst size	Controls the maximum burst size for VBR (***Variable Bit Rate***) and VBR RT (***VBR Real Time***) channels. This value overrides an existing BT value (if set). The MBS can be any value between 0 and 100.	0

Example --> pppoa set transport pppoa3 mbs 10

See also
```
PPPOA SET TRANSPORT BT
PPPOA SET TRANSPORT QOSCLASS
```

8.8.1.1.26 PPPOA SET TRANSPORT MCR

Syntax `PPPOA SET TRANSPORT {<name>|<number>} MCR <min cell rate>`

Description This command applies to existing PVC transports - it does not apply to SVC transports. This command sets the minimum cell rate for an existing PPPoA transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
minimum cell rate	Determines the minimum rate at which ATM cells can be sent along the PPPoA transport.	0

Example --> pppoa set transport pppoa2 mcr 0

See also PPPOA SET TRANSPORT PCR

8.8.1.1.27 PPPOA SET TRANSPORT PASSWORD

Syntax PPPOA SET TRANSPORT {<name>|<number>} PASSWORD <password>

Description This command sets a dial-out password on a named transport. The password is required when PPP negotiation takes place and is supplied to the remote PPP server for authentication.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
password	An arbitrary word that acts as a dialout password enabling you to login to the remote end. The PPP server will require the password when you want to login remotely. It can be made up of one or more characters and/or digits. To display the password, use the PPPOA SHOW TRANSPORT command.	N/A

Example --> pppoa set transport pppoa2 password mercury

See also PPPOA LIST TRANSPORTS
PPPOA SHOW TRANSPORT
PPPOA SET TRANSPORT USERNAME

8.8.1.1.28 PPPOA SET TRANSPORT PCR

Syntax PPPOA SET TRANSPORT {<name>|<number>} PCR <peak cell rate>

Description This command applies to existing PVC transports - it does not apply to SVC transports. This command sets the ***Peak Cell Rate*** (PCR) for an existing PPPoA transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
peak cell rate	Determines the maximum rate at which ATM cells can be sent along the PPPoA transport. The PCR can be any value from 0 up to the maximum PortSpeed parameter set when the port was created (using the initbun file in ***FlashFS*** or the CLI command PORT LIST).	0

Example --> pppoa set transport pppoa2 pcr 50000

See also PPPOA SET TRANSPORT MCR

8.8.1.1.29 PPPOA SET TRANSPORT PORT

Syntax PPPOA SET TRANSPORT {<name>|<number>} PORT <port>

Description This command applies to existing PVC transports - it does not apply to SVC transports. This command sets the port that an existing transport uses to transport PPPoA data.

The port/VPI/VCI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A

Option	Description	Default Value
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
port	The system port that is used to transport ATM data.	N/A

Example --> pppoa set transport pppoa4 port a1

See also `pppoa list transports`
`port list`

8.8.1.1.30 PPPOA SET TRANSPORT PRILEVELS

Syntax `PPPOA SET TRANSPORT {<name>|<number>} PRILEVELS <prilevels>`

Description This command enables support for multiple packet priority levels on the same ATM VC.

Two prilevel values are supported:

- There are no multiple priority levels enabled so the feature is disabled.
- Packets with different priorities set (such as best effort and high priority traffic) are prioritized on the same ATM VC.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
prilevels	The number of priority levels available on an ATM transport.	1

Example --> pppoa set transport myrfc prilevels 2

See also `PPPOA SHOW TRANSPORT`

8.8.1.1.31 PPPOA SET TRANSPORT PVC

Syntax `PPPOA SET TRANSPORT {<name>|<number>} PVC <port> <vpi> <vci>`

Description This command sets the PVC information for an existing PPPoA transport PVC. The PVC uses the interface that was specified when the transport was created.

The command allows you to specify the following PVC information:

- The ATM port that will transport data
- VPI (Virtual Path Identifier)
- VCI (Virtual Circuit Identifier)

The port/VPI/VCI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
port	The system port that is used to transport ATM data.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 1 and 65535.	N/A

Example --> pppoa set transport pppoa2 pvc a1 0 800

See also
```
PPPOA LIST TRANSPORTS
PPPOA SET TRANSPORT DIALIN PVC
PPPOA SET TRANSPORT DIALOUT PVC
PORT LIST
```

8.8.1.1.32 PPPOA SET TRANSPORT QOSCLASS

Syntax
```
PPPOA SET TRANSPORT {<name>|<number>} QOSCLASS
{UBR|CBR|VBR|VBRRT|ABR|QFC}
```

Description This command applies to existing PVC transports - it does not apply to SVC transports. It sets the quality of service class for the transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
ubr	Unspecified Bit Rate; non-constant and unpredictable data transport rate. PCR (***Peak Cell Rate***) is the average and maximum speed of transmission.	UBR
cbr	***Constant Bit Rate***; constant demand and predictable data transport rate. PCR is the average and maximum speed of transmission.	
vbr	***Variable Bit Rate***; non-constant but predictable data transport rate that uses ***Non-Real-Time*** (NRT). You can specify the PCR, SCR, BT and MBS for VBR traffic.	
vbrrt	***Variable Bit Rate Real-Time***; non-constant but predictable data transport rate that uses ***Real-Time*** (RT). You can specify the PCR, SCR, BT and MBS for VBRRT traffic.	
abr	***Available Bit Rate***; non-constant and unpredictable data transport rate that provides ATM-layer feedback and flow control.	
qfc	QFC: ATM flow control protocol that supports ABR.	

Example --> pppoa set transport pppoa3 qosclass abr

See also PPPOA SHOW TRANSPORT
PPPOA SET TRANSPORT QOSCLASS

8.8.1.1.33 PPPOA SET TRANSPORT REMOTEDNS

Syntax PPPOA SET TRANSPORT {<name>|<number>} REMOTEDNS <ipaddress> [<ipaddress2>]

Description This command is a PPP server function.

This command sets the primary and secondary local DNS server addresses that will be given to a remote PPP peer when the peer requests a primary or secondary DNS server IP address using IPCP. Setting the secondary IP address is optional.

If you want to delete an IP address, set the IP address to 0.0.0.0.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing pppoa transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing pppoa transport. To display transport numbers, use THE PPPOA LIST TRANSPORTS command.	N/A
ipaddress	The ip address of the primary local DNS server displayed in the following format: 192.168.102.3	0.0.0.0 (no primary address set)
ipaddress2	The ip address of the secondary local DNS server displayed in the following format: 192.168.102.3	0.0.0.0 (no secondary address set)

ExamplesExample 1 - setting a primary address

--> pppoa set transport pppoa1 remotedns 192.168.102.3

Example 2 - setting primary and secondary addresses

To set primary and secondary addresses, use this command syntax:

--> pppoa set transport pppoa1 remotedns 192.168.102.3 192.168.105.1

Example 3 - deleting an address

To delete an address, set it to 0.0.0.0. The example below deletes the secondary address that was set in Example Two:

--> pppoa set transport pppoa1 remotedns 192.168.102.3 0.0.0.0

See also
```
PPPOA SET TRANSPORT GIVEDNS CLIENT ENABLED|DISABLED
PPPOA SET TRANSPORT GIVEDNS RELAY ENABLED|DISABLED
PPPOA SET TRANSPORT DISCOVERDNS PRIMARY
PPPOA SET TRANSPORT DISCOVERDNS SECONDARY
```

8.8.1.1.34 PPPOA SET TRANSPORT REMOTEIP

Syntax `PPPOA SET TRANSPORT {<name>|<number>} REMOTEIP <ip-address>`

Description This command sets the IP address supplied to the remote end of the PPP connection during negotiation. This is particularly important for PPP dialin transports.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
ip-address	The ip address of the local 'server-end' of an interface displayed in the following format: 111.222.254.4	0.0.0.0

Example --> pppoa set transport pppoa1 remoteip 192.168.103.2

See also PPPOA SHOW TRANSPORT
PPPOA LIST TRANSPORTS
PPPOA SET TRANSPORT LOCALIP

8.8.1.1.35 PPPOA SET TRANSPORT ROUTEMASK

Syntax PPPOA SET TRANSPORT {<name>|<number>} ROUTEMASK <mask>

Description This command sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to 0.0.0.0, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (***Internet Protocol Control Protocol***) negotiation.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A

Option	Description	Default Value
mask	The subnet mask that is used for the route that is created when a PPP link comes up. 0.0.0.0	0.0.0.0

Example --> pppoa set transport pppoa1 routemask 0.0.0.0

See also `PPPOA SHOW TRANSPORT`
`PPPOA LIST TRANSPORTS`

8.8.1.1.36 PPPOA SET TRANSPORT SCR

Syntax `PPPOA SET TRANSPORT {<name>|<number>} SCR <sustainable cell rate>`

Description This command applies to existing PVC transports - it does not apply to SVC transports. This command is only valid if you set VBR or VBR RT as the QoS Class using the pppoa set transport qosclass command.

The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
sustainable cell rate	Sustainable Cell Rate; the average cell rate for a VBR or VBR RT connection. The SCR can be any positive value that is less than the PortSpeed and the PCR for the channel.	0

Example --> pppoa set transport pppoa2 scr 25000

See also `PPPOA SET TRANSPORT QOSCLASS`

8.8.1.1.37 PPPOA SET TRANSPORT SPECIFICROUTE

Syntax `PPPOA SET TRANSPORT {<name>|<number>} SPECIFICROUTE {ENABLED | DISABLED}`

Description This command specifies whether the route created when a PPP link comes up is a specific or default route. If set to enabled, the route created will only apply to packets for

the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Note: This command is only valid if the PPPOA SET TRANSPORT CREATEROUTE *command is set to* ***enabled****. If the* CREATEROUTE COMMAND *is set to* ***disabled****, no route is created and therefore the* PPPOA SET TRANSPORT SPECIFICROUTE *command is ignored.*

The mask for the route is calculated from the class of the remote subnet unless an alternative has been specified using the PPPOA SET TRANSPORT ROUTEMASK command. If specificroute is set to disabled, a default route to the subnet at the remote end of the PPP link is created.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
enabled	Allows the created route to apply to packets for the subnet at the remote end of the PPP link.	disabled
disabled	A default route to the subnet at the remote end of the PPP link is created.	

Example --> pppoa set transport pppoa1 specificroute disabled

See also PPPOA SET TRANSPORT ROUTEMASK
PPPOA SET TRANSPORT CREATEROUTE
PPPOA LIST TRANSPORTS
PPPOA SHOW TRANSPORT

8.8.1.1.38 PPPOA SET TRANSPORT SUBNETMASK

Syntax PPPOA SET TRANSPORT {<name>|<number>} SUBNETMASK <mask>

Description This command sets the subnet mask used for the local IP interface connected to the PPP transport. If the value 0.0.0.0 is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
mask	The subnet mask used by the local IP interface connected to the PPP transport.	0.0.0.0

Example --> pppoa set transport pppoa1 subnetmask 255.255.255.0

See also PPPOA LIST TRANSPORTS

8.8.1.1.39 PPPOA SET TRANSPORT THEYLOGIN

Syntax PPPOA SET TRANSPORT {<name>|<number>} THEYLOGIN {NONE|PAP|CHAP}

Description This command sets the authentication method that remote PPP clients must use to dialin to the server. If authentication is used, clients must use the specified authentication method and provide the username set using the SYSTEM ADD USER command.

This command is only valid if the user has maydialin set using the SYSTEM SET LOGIN MAYDIALIN command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
none	No authentication method is set.	None
pap	***Password Authentication Protocol***; the server sends an authentication request to the remote user dialing in. PAP passes the un-encrypted username and password and identifies the remote end.	

Option	Description	Default Value
chap	***Challenge Handshake Authentication Protocol***; the server sends an authentication request to the remote user dialing in. PAP passes the encrypted username and password and identifies the remote end.	

Example --> pppoa set transport pppoa2 theylogin pap

See also
```
PPPOA LIST TRANSPORTS
PPPOA SHOW TRANSPORT
SYSTEM ADD USER
SYSTEM SET USER MAYDIALIN
```

8.8.1.1.40 PPPOA SET TRANSPORT USERNAME

Syntax `PPPOA SET TRANSPORT {<name>|<number>} USERNAME <username>`

Description This command sets a (dial-out) username on a named transport. The username is required when PPP negotiation takes place and is supplied to the remote PPP server for authentication.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A
username	A name that identifies a user and, together with the dialout password, enables a user to login to the remote end. The PPP server will require the username when the user wants to login remotely. It can be made up of one or more characters and/or digits. To display the username, use the `PPPOA SHOW TRANSPORT` command.	N/A

Example --> pppoa set transport pppoa2 username jsmith

See also `PPPOA SET TRANSPORT PASSWORD`

8.8.1.1.41 PPPOA SET TRANSPORT VCI

Syntax `PPPOA SET TRANSPORT {<name>|<number>} VCI <vci>`

Description This command applies to existing PVC transports - it does not apply to SVC transports. This command sets the ***Virtual Circuit Identifier***.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 1 and 65535.	N/A

Example --> pppoa set transport pppoa4 vci 800

See also PPPOA LIST TRANSPORTS
PPPOA SHOW TRANSPORT
PPPOA SET TRANSPORT VPI

8.8.1.1.42 PPPOA SET TRANSPORT VPI

Syntax PPPOA SET TRANSPORT {<name>|<number>} VPI <vpi>

Description This command applies to existing PVC transports - it does not apply to SVC transports.This command sets the ***Virtual Path Identifier***.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A

Example --> pppoa set transport pppoa3 vpi 0

See also PPPOA LIST TRANSPORTS
PPPOA SHOW TRANSPORT
PPPOA SET TRANSPORT VCI

8.8.1.1.43 PPPOA SET TRANSPORT WELOGIN

Syntax PPPOA SET TRANSPORT {<name>|<number>} WELOGIN {NONE|AUTO|PAP|CHAP}

Description This command sets the authentication protocol used to connect to external PPP servers (dial-out).

Options The following table gives the range of values for each option thatcan be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the PPPOA LIST TRANSPORTS command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the PPPOA LIST TRANSPORTS command.	N/A
none	No authentication method is used.	None
auto	The authentication protocol used by the remote PPP server is discovered and used.	
pap	***Password Authentication Protocol***; the server sends an authentication request to the remote user dialing in. PAP passes the unencrypted username and password and identifies the remote end.	
chap	***Challenge Handshake Authentication Protocol***; the server sends an authentication request to the remote user dialing in. PAP passes the encrypted username and password and identifies the remote end.	

Example --> pppoa set transport pppoa2 theylogin pap

See also PPPOA SET TRANSPORT THEYLOGIN
PPPOA SHOW TRANSPORT
PPPOA LIST TRANSPORTS

8.8.1.1.44 PPPOA SHOW TRANSPORT

Syntax `PPPOA SHOW TRANSPORT {<name>|<number>}`

Description This command displays the following information about an existing PPPoA transport:

- Description
- Summary - the connection state
- Server - dialin status
- Headers - the data format that the transport can accept or receive
- SVC status (true or false)
- Local IP address
- Subnet mask
- Remote IP address
- Remote DNS
- Give DNS to Client status
- Give DNS to Relay status
- Create Route status
- Specific Route status
- Route Mask
- Dialout Username
- Dialout Password
- Dialout Authentication method
- Dialin Authentication method
- LCP Max Configure
- LCP Max Failure
- LCP Echo Every
- ATM address (for SVC transports only)
- Auto-connect status
- Idletime status
- ATM port (for PVC transports only)
- Rx VPI (for PVC transports only)

- Rx VCI (for PVC transports only)
- ***Quality of Service*** (QoS) class (for PVC transports only)
- Burst tolerance (for PVC transports only)
- ***Sustainable Cell Rate*** (SCR) (for PVC transports only)
- ***Maximum Burst Size*** (MBS) (for PVC transports only)
- ***Maximum Cell Rate*** (MCR) (for PVC transports only)
- ***Packet Priority Levels*** setting

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing PPPoA transport. To display transport names, use the `PPPOA LIST TRANSPORTS` command.	N/A
number	An existing PPPoA transport. To display transport numbers, use the `PPPOA LIST TRANSPORTS` command.	N/A

Example There are two examples given below. Example one is of an SVC transport. Example two is of a PVC transport.

Example 1 - SVC

--> pppoa show transport pppoa1

```
PPP Transport: pppoa1
Description : pppoa1
                Summary : disabled
                 Server : true
          Headers: learn            SVC: true
                Local IP : 192.168.100.1
              Subnet Mask : 255.255.255.0
                Remote IP : 192.168.100.2
               Remote DNS : N/A
        Give DNSto Client : true
         Give DNSto Relay : true
            Create Route : true
          Specific Route : false
              Route Mask : 255.0.0.0
         Dialout Username :
         Dialout Password :
```

```
              Dialout Auth : none
               Dialin Auth : none
        Lcp Max Configure : 10
          Lcp Max Failure : 5
        Lcp Max Terminate : 2
           Lcp Echo Every : 10
             Auto Connect : false
             Idle Timeout : 0
ATM address:
47.00.83.10.a2.b1.00.00.00.00.00.00.00.00.20.2b.01.00.07.00
```

Example 2 - PVC

--> pppoa show transport pppoa2

```
PPP Transport: pppoa2
Summary : enabled, down
                   Server : true
           Headers: learn             SVC: false
                 Local IP : 192.168.100.1
              Subnet Mask : 255.255.255.0
                Remote IP : 192.168.100.2
               Remote DNS : N/A
        Give DNSto Client : true
         Give DNSto Relay : true
             Create Route : true
           Specific Route : false
                Route Mask : 255.0.0.0
         Dialout Username :
         Dialout Password :
             Dialout Auth : none
              Dialin Auth : none
        Lcp Max Configure : 10
          Lcp Max Failure : 5
        Lcp Max Terminate : 2
           Lcp Echo Every : 10
             Auto Connect : false
             Idle Timeout : 0
                     Port : a1
                  Rx Vpi : N/A
                  Rx Vci : 100
                   Class : UBR
          Burst Tolerance : N/A
    Sustainable Cell Rate : N/A
                      MBS : N/A
```

```
                          MCR : N/A
      Packety Priority Levels : 2
```

See also PPPOA LIST TRANSPORTS

8.9 RFC1483

8.9.1 RFC1483 command reference

8.9.1.1 RFC1483 CLI command

This chapter describes the ***RFC1483*** commands provided by the CLI:

TABLE 8-9 RFC1883 Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
RFC1483 ADD TRANSPORT							X	X	X
RFC1483 CLEAR TRANSPORTS							X	X	X
RFC1483 DELETE TRANSPORT							X	X	X
RFC1483 LIST TRANSPORTS							X	X	X
RFC1483 SET TRANSPORT BT							X	X	X
RFC1483 SET TRANSPORT MBS							X	X	X
RFC1483 SET TRANSPORT MCR							X	X	X
RFC1483 SET TRANSPORT MODE							X	X	X
RFC1483 SET TRANSPORT PCR							X	X	X
RFC1483 SET TRANSPORT PORT							X	X	X
RFC1483 SET TRANSPORT PRILEVELS							X	X	X
RFC1483 SET TRANSPORT QOSCLASS							X	X	X
RFC1483 SET TRANSPORT RXVCI							X	X	X
RFC1483 SET TRANSPORT RXVPI							X	X	X
RFC1483 SET TRANSPORT SCR							X	X	X
RFC1483 SET TRANSPORT TXVCI							X	X	X
RFC1483 SET TRANSPORT TXVPI							X	X	X

TABLE 8-9 RFC1883 Commands

Commands	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
RFC1483 SET TRANSPORT VCI							X	X	X
RFC1483 SET TRANSPORT VPI							X	X	X
RFC1483 SHOW TRANSPORT							X	X	X

8.9.1.1.1 RFC1483 ADD TRANSPORT

Syntax `RFC1483 ADD TRANSPORT <name> <port> <vpi> <vci> {LLC|VCMUX} {BRIDGED|ROUTED}`

Description This command creates a named RFC1483 transport and allows you to specify the following:

- The ATM port that will transport RFC1483 data. (ATM ports are initialized in the initbun file in flashfs, or using the bun set port console command.)
- VPI (Virtual Path Identifier)
- VCI (Virtual Circuit Identifier)
- LLC or vcmux encapsulation (optional)
- Bridged or Routed (optional)
- The port/VPI/VCI combination must be unique for each transport

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An arbitrary name that identifies the transport. It can be made up of one or more letters or a combination of letters and digits, but it cannot start with a digit.	N/A
port	The system port that is used to transport ATM data.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 4095.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 32 and 65535.	N/A

Option	Description	Default Value
llc	LLC encapsulation method.	llc
vcmux	VC Multiplexing encapsulation method.	
bridged	Traffic type that is going to be transmitted/received.	bridged
routed	Traffic type that is going to be transmitted/received.	

Example --> rfc1483 add transport my1483 myport 0 700 vcmux routed

See also `RFC1483 LIST TRANSPORTS`
`PORT ?`

8.9.1.1.2 RFC1483 CLEAR TRANSPORTS

Syntax `RFC1483 CLEAR TRANSPORTS`

Description This command deletes **ALL** RFC1483 transports that were created using the `RFC1483 ADD TRANSPORT` command.
WARNING: recommended do not use with ADSL A group of devices, otherwise restart of the Media Gateway it will be necessary. USE rf1483 delete transport (see following)

Example --> rfc1483 clear transports

See also `RFC1483 DELETE TRANSPORT`

8.9.1.1.3 RFC1483 DELETE TRANSPORT

Syntax `RFC1483 DELETE TRANSPORT {<name>|<number>}`

Description This command deletes a single RFC1483 transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A

Example --> rfc1483 delete transport my1483

See also RFC1483 LIST TRANSPORTS

8.9.1.1.4 RFC1483 LIST TRANSPORTS

Syntax RFC1483 LIST TRANSPORTS

Description This command lists all RFC1483 transports that have been created using the RFC1483 add transport command. It displays the following information about the transports:

- Transport identification number
- Transport name
- Name of the ATM port used to transport rfc1483 data
- Transmit and receive vci numbers
- Transmit and receive vpi numbers

Example --> rfc1483 list transports

```
RFC1483 transports:
 ID  |    Name   | Port     | TxVci    | RxVci    | TxVpi    | RxVpi
-----|-----------|----------|----------|----------|----------|------
   1 | my1483    | a1       | 700      | 700      | 0        | 0
-------------------------------------------------------------------
```

See also RFC1483 SHOW TRANSPORT

8.9.1.1.5 RFC1483 SET TRANSPORT BT

Syntax RFC1483 SET TRANSPORT {<name>|<number>} BT <burst tolerance>

Description This command sets the ***Burst Tolerance*** (BT) that an existing RFC1483 transport uses to transport data over ATM. This command is only valid if you set VBR or VBR RT as the QoS Class using the RFC1483 SET TRANSPORT QOSCLASS command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A

Option	Description	Default Value
burst tolerance	Controls the duration of traffic bursts on VBR (Variable Bit Rate) and VBR RT (VBR Real Time) channels. This value overrides an existing MBS value (if set). The BT can be any value between 0 and 100 (999999999).	N/A means "0"

Example --> rfc1483 set transport my1483 bt 5

See also `RFC1483 SET TRANSPORT MBS`
`RFC1483 SET TRANSPORT QOSCLASS`

8.9.1.1.6 RFC1483 SET TRANSPORT MBS

Syntax `RFC1483 SET TRANSPORT {<name>|<number>} MBS <maximum burst size>`

Description This command sets the maximum burst size (MBS) for the RFC1483 transport. This command is only valid if you set VBR or VBR RT as the QoS Class using the `RFC1483 SET TRANSPORT QOSCLASS` command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A
maximum burst size	Controls the maximum burst size for VBR (***Variable Bit Rate***) and VBR RT (***VBR Real Time***) channels. This value overrides an existing BT value (if set). The MBS can be any value between 0 and 100(999999999).	N/A means "0"

Example --> rfc1483 set transport my1483 mbs 10

See also `RFC1483 SET TRANSPORT BT`
`RFC1483 SET TRANSPORT QOSCLASS`

8.9.1.1.7 RFC1483 SET TRANSPORT MCR

Syntax `RFC1483 SET TRANSPORT {<name>|<number>} MCR <minimum cell rate>`

Description This command sets the ***Minimum Cell Rate*** (MCR) for an existing RFC1483 transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A
minimum cell rate	Determines the minimum rate at which ATM cells can be transported into the ATM network.	0

Example --> rfc1483 set transport my1483 mcr 0

See also `RFC1483 SET TRANSPORT PCR`

8.9.1.1.8 RFC1483 SET TRANSPORT MODE

Syntax `RFC1483 SET TRANSPORT {<name>|<number>} MODE {LLC|VCMUX}`

Description This command sets the mode of encapsulation that an existing RFC1483 transport uses.

Options The following table gives the range of values for each option that can be specified with this command and a default value for each option (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A

Option	Description	Default Value
llc	***Logical Link Control*** encapsulation method.	LLC
vcmux	VC Multiplexing encapsulation method.	

Example --> rfc1483 set transport my1483 mode vcmux

See also `RFC1483 LIST TRANSPORTS`

8.9.1.1.9 RFC1483 SET TRANSPORT PCR

Syntax `RFC1483 SET TRANSPORT {<name>|<number>} PCR <peak cell rate>`

Description This command sets the ***Peak Cell Rate*** (PCR) for an existing RFC1483 transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A
peak cell rate	Determines the maximum rate at which ATM cells can be transported into the ATM network. The PCR can be any value from 0 up to the maximum PortSpeed parameter set when the port was created (`PORT a1 SET`)	N/A means "0"

Example --> rfc1483 set transport my1483 pcr 50000

See also `RFC1483 SET TRANSPORT MCR`
`RFC1483 LIST TRANSPORTS`

8.9.1.1.10 RFC1483 SET TRANSPORT PORT

Syntax `RFC1483 SET TRANSPORT {<name>|<number>} PORT <atm-port>`

Description This command sets the port that an existing RFC1483 transport uses to transport RFC1483 data over ATM. ATM ports are initialized in the initbun file in ***FlashFS***, or using the BUN SET PORT CONSOLE command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A
atm-port	The system port that is used to transport ATM data. The port/VPI/VCI combination must be unique for each transport.	N/A

Example --> rfc1483 set transport my1483 port a1

See also RFC1483 LIST TRANSPORTS
PORT SET

8.9.1.1.11 RFC1483 SET TRANSPORT PRILEVELS

Syntax RFC1483 SET TRANSPORT {<name>|<number>} PRILEVELS <prilevels>

Description This command enables support for multiple packet priority levels on the same ATM VC.

Two prilevel values are supported:

- There are no multiple priority levels enabled so the feature is disabled.
- Packets with different priorities set (such as best effort and high priority traffic) are prioritized on the same ATM vc.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A
prilevels	The number of priority levels available on an ATM transport.	1

Example --> rfc1483 set transport myrfc prilevels 2

See also RFC1483 SHOW TRANSPORT

8.9.1.1.12 RFC1483 SET TRANSPORT QOSCLASS

Syntax RFC1483 set transport {<name>|<number>} QOSCLASS {UBR|CBR|VBR|VBRRT|ABR|QFC}

Description This command sets the ***Quality of Service*** (QoS) class for the transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A
ubr	***Unspecified Bit Rate***; non-constant and unpredictable data transport rate. PCR (***Peak Cell Rate***) is the average and maximum speed of transmission.	UBR
ubr+	***Unspecified Bit Rate*** plus; is a special ATM service class developed by Cisco Systems.	
cbr	***Constant Bit Rate***; constant demand and predictable data transport rate. PCR is the average and maximum speed of transmission.	

Option	Description	Default Value
vbr	***Variable Bit Rate***; non-constant but predictable data transport rate that uses ***Non-Real-Time*** (NRT). You can specify the PCR, SCR, BT and MBS for VBR traffic.	
vbrrt	***Variable Bit Rate Real-Time***; non-constant but predictable data transport rate that uses ***Real-Time*** (RT). You can specify the PCR, SCR, BT and MBS for VBRRT traffic.	
abr	***Available Bit Rate***; non-constant and unpredictable data transport rate that provides ATM-layer feedback and flow control.	
qfc	QFC: ATM flow control protocol that supports ABR.	

Example --> rfc1483 set transport my1483 abr

See also
```
RFC1483 SHOW TRANSPORT
RFC1483 SET TRANSPORT BT
RFC1483 SET TRANSPORT MBS
RFC1483 SET TRANSPORT PCR
RFC1483 SET TRANSPORT SCR
```

8.9.1.1.13 RFC1483 SET TRANSPORT RXVCI

Syntax `RFC1483 SET TRANSPORT {<name>|<number>} RXVCI <vci>`

Description This command sets the receive ***Virtual Circuit Identifier*** channel. If you later set the VCI using the `RFC1483 SET TRANSPORT VCI` command, the RX VCI setting will be overridden.

The port/VCI/VPI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A

Option	Description	Default Value
rxvci	Part of the ATM header. The RXVCI is a tag that identifies which channel a cell will be received over. The RXVCI can be any value between 32 and 9999999999.	VCI value set when the transport was created using the RFC1483 ADD TRANSPORT command

Example --> rfc1483 set transport my1483 rxvci 700

Options RFC1483 LIST TRANSPORTS
RFC1483 SET TRANSPORT TXVCI

8.9.1.1.14 RFC1483 SET TRANSPORT RXVPI

Syntax RFC1483 SET TRANSPORT {<name>|<number>} RXVPI <vpi>

Description This command sets the receive ***Virtual Path Identifier***. If you later set the VPI using the RFC1483 SET TRANSPORT VPI command, the rxvpi setting will be overridden.

The port/VCI/VPI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A
rxvpi	A field in the ATM header. The RXVPI is used to identify the virtual path that a circuit belongs to and receives information on. The RXVPI can be any value between 0 and 9999999999.	VPI value set when the transport was created using the rfc1483 add transport command

Example --> rfc1483 set transport my1483 rxvpi 0

See also RFC1483 LIST TRANSPORTS
RFC1483 SET TRANSPORT TXVPI

8.9.1.1.15 RFC1483 SET TRANSPORT SCR

Syntax RFC1483 SET TRANSPORT {<name>|<number>} SCR <sustainable cell rate>

Description This command sets the ***Sustainable Cell Rate***. This command is only valid if you set VBR or VBR RT as the QoS Class using the RFC1483 SET TRANSPORT QOSCLASS command.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A
sustainable cell rate	***Sustainable Cell Rate***; the average cell rate for a VBR or VBR RT connection. The SCR can be any positive value that is less than the both PORTSPEED SET (when the port was created) and the PCR SET for the channel. (The port is initialized using the initbun file in ***FlashFS*** or the CLI command PORT SET)	0

Example --> rfc1483 set transport my1483 scr 25000

See also RFC1483 SET TRANSPORT QOSCLASS
RFC1483 LIST TRANSPORTS

8.9.1.1.16 RFC1483 SET TRANSPORT TXVCI

Syntax RFC1483 SET TRANSPORT {<name>|<number>} TXVCI <vci>

Description This command sets the transmit ***Virtual Circuit Identifier*** channel. If you later set the VCI using the RFC1483 SET TRANSPORT VCI command, the TXVCI setting will be overridden.

The port/VCI/VPI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A
txvci	Part of the ATM header. The TX VCI is a tag that identifies which channel a cell will be transmitted over. The TX VCI can be any value between 1 and 65535.	VCI value set when the transport was created using the rfc1483 add transport command

Example --> rfc1483 set transport my1483 txvci 800

See also `RFC1483 LIST TRANSPORTS`
`RFC1483 SET TRANSPORT RXVCI`

8.9.1.1.17 RFC1483 SET TRANSPORT TXVPI

Syntax `RFC1483 SET TRANSPORT {<name>|<number>} TXVPI <vpi>`

Description This command sets the transmit ***Virtual Path Identifier***. If you later set the VPI using the `RFC1483 SET TRANSPORT VPI` command, the RXVPI setting will be overridden.

The port/VCI/VPI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A
txvpi	A field in the ATM header. The TX VPI is used to identify the virtual path that a circuit belongs to and transmits information on. The TX VPI can be any value between 0 and 9999999999.	VPI value set when the transport was created using the rfc1483 add transport command

Example --> rfc1483 set transport my1483 txvpi 0

See also RFC1483 LIST TRANSPORTS
RFC1483 SET TRANSPORT RXVPI

8.9.1.1.18 RFC1483 SET TRANSPORT VCI

Syntax RFC1483 SET TRANSPORT {<name>|<number>} VCI <vci>

Description This command sets the ***Virtual Circuit Identifier*** channel. It overrides existing VCI settings (including RX VCI and TX VCI).

The port/VCI/VPI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
vci	Part of the ATM header. The VCI is a tag that identifies which channel a cell will travel over. The VCI can be any value between 32 and 9999999999.	VCI value set when the transport was created using the add transport command

Example --> rfc1483 set transport my1483 vci 800

See also RFC1483 LIST TRANSPORTS
RFC1483 SET TRANSPORT TXVCI
RFC1483 SET TRANSPORT RXVCI

8.9.1.1.19 RFC1483 SET TRANSPORT VPI

Syntax RFC1483 SET TRANSPORT {<name>|<number>} VPI <vpi>

Description This command sets the ***Virtual Path Identifier***. It overrides existing VPI settings (including RX VPI and TX VPI).

The port/VPI/VCI combination must be unique for each transport.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the RFC1483 LIST TRANSPORTS command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the RFC1483 LIST TRANSPORTS command.	N/A
vpi	A field in the ATM header. The VPI is used to identify the virtual path that a circuit belongs to. The VPI can be any value between 0 and 9999999999.	VPI value set when the transport was created using the add transport command

Example --> rfc1483 set transport my1483 vpi 0

See also `RFC1483 LIST TRANSPORTS`
`RFC1483 SET TRANSPORT RXVPI`
`RFC1483 SET TRANSPORT TXVPI`

8.9.1.1.20 RFC1483 SHOW TRANSPORT

Syntax `RFC1483 SHOW TRANSPORT {<name>|<number>}`

Description This command displays the following information about an existing RFC1483 transport:

- Name
- Description
- Encapsulation method
- ATM port
- TX VPI - transmit Virtual Path Identifier
- RX VPI - receive Virtual Path Identifier
- TX VCI - transmit Virtual Circuit Identifier
- TX VCI - receive Virtual Circuit Identifier
- ATM Traffic Class
- PCR - Peak Cell Rate
- BT - Burst Tolerance
- SCR - Sustainable Cell Rate
- MBS - Maximum Burst Size
- MCR - Minimum Cell Rate
- Packet Priority Levels

Example The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

See also

Option	Description	Default Value
name	An existing RFC1483 transport. To display transport names, use the `RFC1483 LIST TRANSPORTS` command.	N/A
number	An existing RFC1483 transport. To display transport numbers, use the `RFC1483 LIST TRANSPORTS` command.	N/A

Example --> rfc1483 show transport my1483

```
RFC1483 Transport: my1483
    Description: Default LAN port
  Encapsulation: LlcBridged
                ATM port: a1
                  Tx VPI: 0
                  Rx VPI: 0
                  Tx VCI: 800
                  Rx VCI: 800
        ATM Traffic class: UBR
          Peak Cell Rate : 0
         Burst Tolerance : N/A
  Sustainable Cell Rate : 800
         Max Burst Size : N/A
          Max Cell Rate : N/A
Packety Priority Levels : 2
```

See also RFC1483 LIST TRANSPORTS

9. Wireless

9.1 Wireless Interface

This part of the Software Reference Manual provides an overview about the wireless device configuration and usage on products supporting the wireless interface ("W" models in groups: Fiber D, ADSL A, ADSL B - please refer to the preface for the complete groups table).

9.1.1 Wireless LAN module

Allied Telesis wireless products are designed to support either embedded pci wireless networking card (ADSL A group wireless products) or integrated wireless LAN chipset (FIBER D, ADSL B) with a range up to 300 m.

The following wireless main features are available on all Allied Telesis wireless products:

- Fully compliant with standards IEEE 802.11b and IEEE 802.11g.
- IEEE 802.11a is NOT supported
- High speed wireless connection, up to 54 Mbps
- Auto fallback data rate under noisy environment
- High sensitivity and output power
- 64-bit, 128-bit Wired Equivalent Privacy (WEP) encryption
- 802.1x authentication
- Wi-Fi Protected Access (WPA) encryption
- Compliant with Standard 802.11i (WPA2) with AES-CCMP encryption
- 802.1q vlan integration with layer 2 802.3u managed switch (NOTE: only untagged vlans are supported on the wireless interface)

Note: Refer to the Release Notes for guidelines on the use of these features with specific customer products.

9.1.2 Layer 2 switch on wireless port

The following scenario details a network example where the CPE wireless interface is used in a switched scenario where wireless traffic is simply bridged to the ADSL port and vice versa.

In this scenario the wireless interface is member of the data VLAN together with a switch Ethernet port and the ADSL port. Traffic originated by the wireless host can be forwarded to the host connected at the Ethernet port and then to the uplink path without requiring any packet routing at layer 3.

Please refer to chapter 2. for any information on how to configure the bridge functionality on the CPE for each different products group.

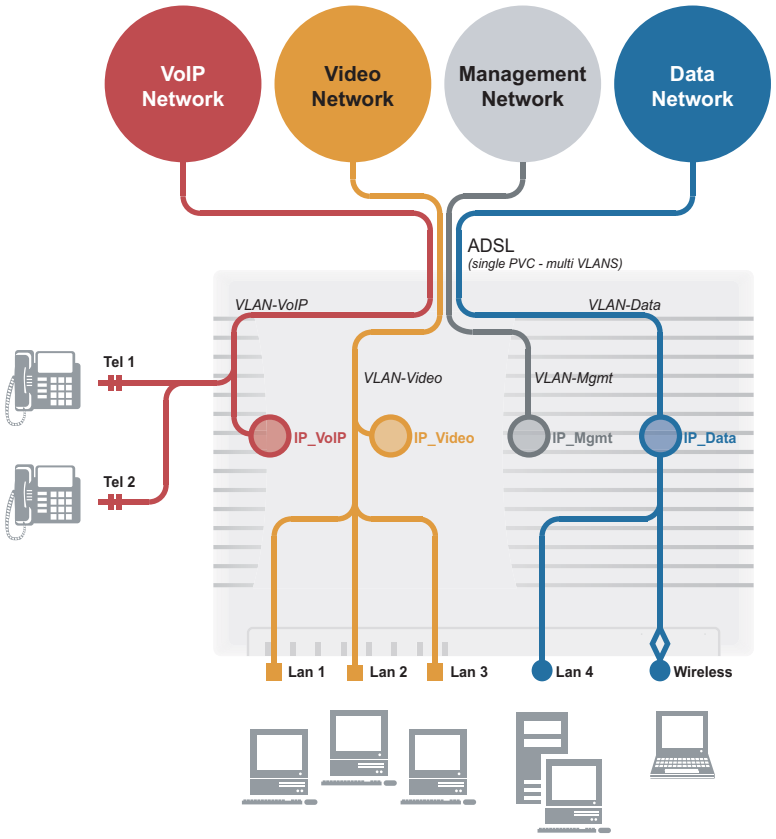


FIGURE 9-1 Wireless interface usage on a bridged scenario

9.1.2.1 Layer 2 CPE Configuration for ADSL A group wireless products

A DHCP server is used to provide addresses on this subnet. 172.32.2.1 is the default gateway for this subnet.

```
vlan add vlan_mgmt vid 202
ethernet ad transport vlan_mgmt
ip ad interface ip_mgmt
dhcpclient ad interfaceconfig ic_mgmt ip_mgmt
dhcpclient interfaceconfig ic_mgmt add requested option subnet-mask
dhcpclient interfaceconfig ic_mgmt add requested option routers
dhcpclient interfaceconfig ic_mgmt add requested option domain-name
dhcpclient interfaceconfig ic_mgmt add requested option domain-name-
servers
rfc1483 set transport pvc_0_35 vlan vlan_mgmt frame tagged
ip attach ip_mgmt vlan_mgmt
```

```
dhcpclient update
#Clean up interface ip0 (default)
ip set interface ip0 dhcp disabled
dhcpclient update
ip set interface ip0 ipaddress 0.0.0.0 0.0.0.0
rfc1483 unset transport pvc_0_35 vlan default
ip set interface ip_mgmt dhcp enabled
dhcpclient update
#Management access configuration. 172.30.1.0 and 10.17.90.0 subnets
are located on management networks.
webserver add managementsubnet mgmt1 172.30.1.0 255.255.255.0
172.30.1.1 172.30.1.254
webserver add managementsubnet mgmt2 10.17.90.0 255.255.255.0
10.17.90.1 10.17.90.254
#VoIP network configuration. A DHCP server is used to provides
addresses on this subnet. 172.32.3.1 is the default gateway for this
subnet.
vlan add vlan_voip vid 203 802.1p_priority 7
ip add interface ip_voip
ip set interface ip_voip dhcp enabled
dhcpclient add interfaceconfig ic_voip ip_voip
dhcpclient interfaceconfig ic_voip add requested option subnet-mask
dhcpclient interfaceconfig ic_voip add requested option routers
dhcpclient interfaceconfig ic_voip add requested option domain-name-
servers
dhcpclient interfaceconfig ic_voip add requested option domain-name
dhcpclient set interfaceconfig ic_voip givednstoclient enabled
dhcpclient set interfaceconfig ic_voip givednstorelay disabled
dhcpclient set interfaceconfig ic_voip defaultroute disabled
ethernet add transport vlan_voip
rfc1483 set transport pvc_0_35 vlan vlan_voip frame tagged
ip attach ip_voip vlan_voip
dhcpclient update
#Data network configuration. A DHCP server is used to provides
addresses on this subnet. 172.32.4.1 is the default gateway for this
subnet.
vlan add vlan_data vid 204 802.1p_priority 7
vlan add vlan_data port lan4 frame untagged
vlan add vlan_data port wireless frame untagged
ip add interface ip_data
ip set interface ip_data dhcp enabled
dhcpclient add interfaceconfig ic_data ip_data
dhcpclient interfaceconfig ic_data add requested option subnet-mask
```

```
dhcpclient interfaceconfig ic_data add requested option routers
dhcpclient interfaceconfig ic_data add requested option domain-name-
servers
dhcpclient interfaceconfig ic_data add requested option domain-name
dhcpclient set interfaceconfig ic_data givednstoclient disabled
dhcpclient set interfaceconfig ic_data givednstorelay disabled
dhcpclient set interfaceconfig ic_data defaultroute enabled
ethernet add transport vlan_data
rfc1483 set transport pvc_0_35 vlan vlan_data frame tagged
ip attach ip_data vlan_data
dhcpclient update
#Video network configuration. No IP addresses are assigned on this
subnet.
vlan add vlan_video vid 205 802.1p_priority 0
vlan add vlan_video port lan1 frame untagged
vlan add vlan_video port lan2 frame untagged
vlan add vlan_video port lan3 frame untagged
ip add interface ip_video
ip set interface ip_video ipaddress 0.0.0.0 0.0.0.0
ethernet add transport vlan_video
rfc1483 set transport pvc_0_35 vlan vlan_video frame tagged
ip attach ip_video vlan_video
#Routing table reconfiguration.
ip add route voice_server 172.30.1.121 255.255.255.255 gateway
172.32.3.1
ip add route voice_server2 172.30.1.123 255.255.255.255 gateway
172.32.3.1
ip add route voice_server3 172.30.1.201 255.255.255.255 gateway
172.32.3.1
ip add route mgmt-1 10.17.90.0 255.255.255.0 gateway 172.32.2.1
ip add route mgmt-2 172.30.1.202 255.255.255.255 gateway 172.32.2.1
#Local time and date configuration.
sntpclient add server ipaddress 172.30.1.202
sntpclient set pollintv 2
sntpclient set timezone MET
#Igmp snooping configuration.
igmp snooping enable vlan_video
igmp snooping set mode snooping
igmp snooping set secondary-netinterface ip_mgmt
#VoIP protocol configuration.
voip sip protocol enable
voip dtmf-relay set mode auto
voip ep analogue create tel1 type al-fxs-del physical-port tel1
```

```
voip ep analogue set tel1 country usa
voip ep analogue set tel1 clip BELL
voip ep analogue set tel1 clir off
voip ep analogue set tel1 codec g711u
voip ep analogue set tel1 vad off
voip ep analogue set tel1 cng off
voip ep analogue set tel1 lec 8
voip ep analogue create tel2 type al-fxs-del physical-port tel2
voip ep analogue set tel2 country usa
voip ep analogue set tel2 clip BELL
voip ep analogue set tel2 clir off
voip ep analogue set tel2 codec g711u
voip ep analogue set tel2 vad off
voip ep analogue set tel2 cng off
voip ep analogue set tel2 lec 8
voip sip protocol set netinterface ip_voip
voip sip locationserver create loc1 contact 172.30.1.121
voip sip proxyserver create prox1 contact 172.30.1.121
voip sip protocol set internal-call-routing enable
voip sip user create 1723231461 address 1723231461 areacode 604
voip sip user add 1723231461 port tel1
voip sip user create 1723231462 address 1723231462 areacode 604
voip sip user add 1723231462 port tel2
#MpegMon configuration.
mpeg-mon create instance1 membership 224.2.2.50 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance1
mpeg-mon create instance2 membership 224.2.2.51 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance2
mpeg-mon create instance3 membership 224.2.2.56 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance3
mpeg-mon create instance4 membership 224.2.2.57 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance4
mpeg-mon create instance5 membership 224.2.2.58 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance5
#Software update configuration
swupdate set server 172.30.1.9
swupdate set path /public/swupdate/3-4_57_02_04/alpha/iMG634B/upload
swupdate set login root
```

```
swupdate set passwd friend
swupdate stop_time none
swupdate start_time minute */2 hour * day_of_month * month *
day_of_week *
#Wireless port configuration for WPA-PSK authentication with password
“friendfriend”
port wireless set Disable false
port wireless set ESSID iMG634WA-example
802.1x authenticator set authentication local
802.1x authenticator set authentication enabled
port wireless set WPAEnableWPA1 true
port wireless set WPAEnableWPA2 false
port wireless set WPA true
port wireless set WPAEnablePSK true
port wireless set WPA2EnableTKIP false
port wireless set WPA2EnableAES_CCMP true
port wireless set WPA2EnablePreauth true
port wireless set Authentication WPA-PSK
port wireless set Encryption TKIP
port wireless set WPAEnableWPA2 false
wpa set shared passphrase friendfriend
```

9.1.2.2 Layer 2 CPE Configuration for ADSL B group wireless products

```
#Management network configuration. A DHCP server is used to provides
addresses on this subnet. 172.32.2.1 is the default gateway for this
subnet.
vlan create vlan_mgmt 202
ip ad interface ip_mgmt
dhcpclient ad interfaceconfig ic_mgmt ip_mgmt
dhcpclient interfaceconfig ic_mgmt add requested option subnet-mask
dhcpclient interfaceconfig ic_mgmt add requested option routers
dhcpclient interfaceconfig ic_mgmt add requested option domain-name
dhcpclient interfaceconfig ic_mgmt add requested option domain-name-
servers
bridge add vlaninterface vlan_mgmt tagged pvc_0_35_if
ip attach ip_mgmt vlan_mgmt
dhcpclient update
#Clean up interface ip0 (default)
ip set interface ip0 dhcp disabled
dhcpclient update
ip set interface ip0 ipaddress 0.0.0.0 0.0.0.0
bridge delete vlaninterface DefaultVlan pvc_0_35_if
ip set interface ip_mgmt dhcp enabled
```

```
dhcpclient update
#Management access configuration. 172.30.1.0 and 10.17.90.0 subnets
are located on management networks.
webserver add managementsubnet mgmt1 172.30.1.0 255.255.255.0
172.30.1.1 172.30.1.254
webserver add managementsubnet mgmt2 10.17.90.0 255.255.255.0
10.17.90.1 10.17.90.254
#VoIP network configuration. A DHCP server is used to provides
addresses on this subnet. 172.32.3.1 is the default gateway for this
subnet.
vlan create vlan_voip 203
ip add interface ip_voip
ip set interface ip_voip dhcp enabled
dhcpclient add interfaceconfig ic_voip ip_voip
dhcpclient interfaceconfig ic_voip add requested option subnet-mask
dhcpclient interfaceconfig ic_voip add requested option routers
dhcpclient interfaceconfig ic_voip add requested option domain-name-
servers
dhcpclient interfaceconfig ic_voip add requested option domain-name
dhcpclient set interfaceconfig ic_voip givednstoclient enabled
dhcpclient set interfaceconfig ic_voip givednstorelay disabled
dhcpclient set interfaceconfig ic_voip defaultroute disabled
bridge add vlaninterface vlan_voip tagged pvc_0_35_if
bridge set interface pvc_0_35_if defaultuserpriority 7
ip attach ip_voip vlan_voip
dhcpclient update
#Data network configuration. A DHCP server is used to provides
addresses on this subnet. 172.32.4.1 is the default gateway for this
subnet.
vlan create vlan_data 204
vlan add vlan_data lan4 frame untagged
switch set port lan4 802.1p Enabled
switch set port lan4 defaultpriority 7
bridge add vlaninterface vlan_data untagged wlan_filtered
bridge set interface wlan_filtered defaultuserpriority 7
ip add interface ip_data
ip set interface ip_data dhcp enabled
dhcpclient add interfaceconfig ic_data ip_data
dhcpclient interfaceconfig ic_data add requested option subnet-mask
dhcpclient interfaceconfig ic_data add requested option routers
dhcpclient interfaceconfig ic_data add requested option domain-name-
servers
dhcpclient interfaceconfig ic_data add requested option domain-name
```

```
dhcpclient set interfaceconfig ic_data givednstoclient disabled
dhcpclient set interfaceconfig ic_data givednstorelay disabled
dhcpclient set interfaceconfig ic_data defaultroute enabled
bridge add vlaninterface vlan_data tagged pvc_0_35_if
ip attach ip_data vlan_data
dhcpclient update
#Video network configuration. No IP addresses are assigned on this
subnet.
vlan create vlan_video 205
vlan add vlan_video lan1 frame untagged
switch set port lan1 802.1p Enabled
switch set port lan1 defaultpriority 0
vlan add vlan_video lan2 frame untagged
switch set port lan2 802.1p Enabled
switch set port lan2 defaultpriority 0
vlan add vlan_video lan3 frame untagged
switch set port lan3 802.1p Enabled
switch set port lan3 defaultpriority 0
ip add interface ip_video
ip set interface ip_video ipaddress 0.0.0.0 0.0.0.0
bridge add vlaninterface vlan_video tagged pvc_0_35_if
ip attach ip_video vlan_video
#Routing table reconfiguration.
ip add route voice_server 172.30.1.121 255.255.255.255 gateway
172.32.3.1
ip add route voice_server2 172.30.1.123 255.255.255.255 gateway
172.32.3.1
ip add route voice_server3 172.30.1.201 255.255.255.255 gateway
172.32.3.1
ip add route mgmt-1 10.17.90.0 255.255.255.0 gateway 172.32.2.1
ip add route mgmt-2 172.30.1.202 255.255.255.255 gateway 172.32.2.1
#Local time and date configuration.
sntpclient add server ipaddress 172.30.1.202
sntpclient set pollintv 2
sntpclient set timezone MET
#Igmp snooping configuration.
igmp snooping enable vlan_video
igmp snooping set mode snooping
igmp snooping set secondary-netinterface ip_mgmt
#VoIP protocol configuration.
voip sip protocol enable
voip dtmf-relay set mode auto
voip ep analogue create tel1 type al-fxs-del physical-port tel1
```

```
voip ep analogue set tel1 country usa
voip ep analogue set tel1 clip BELL
voip ep analogue set tel1 clir off
voip ep analogue set tel1 codec g711u
voip ep analogue set tel1 vad off
voip ep analogue set tel1 cng off
voip ep analogue set tel1 lec 8
voip ep analogue create tel2 type al-fxs-del physical-port tel2
voip ep analogue set tel2 country usa
voip ep analogue set tel2 clip BELL
voip ep analogue set tel2 clir off
voip ep analogue set tel2 codec g711u
voip ep analogue set tel2 vad off
voip ep analogue set tel2 cng off
voip ep analogue set tel2 lec 8
voip sip protocol set netinterface ip_voip
voip sip locationserver create loc1 contact 172.30.1.121
voip sip proxyserver create prox1 contact 172.30.1.121
voip sip protocol set internal-call-routing enable
voip sip user create 1723231461 address 1723231461 areacode 604
voip sip user add 1723231461 port tel1
voip sip user create 1723231462 address 1723231462 areacode 604
voip sip user add 1723231462 port tel2
#MpegMon configuration.
mpeg-mon create instance1 membership 224.2.2.50 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance1
mpeg-mon create instance2 membership 224.2.2.51 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance2
mpeg-mon create instance3 membership 224.2.2.56 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance3
mpeg-mon create instance4 membership 224.2.2.57 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance4
mpeg-mon create instance5 membership 224.2.2.58 port 1234 netinter-
face ip_mgmt
mpeg-mon disable instance5
#Software update configuration
swupdate set server 172.30.1.9
swupdate set path /public/swupdate/3-4_57_02_04/alpha/iMG634B/upload
swupdate set login root
```

```
swupdate set passwd friend
swupdate stop_time none
swupdate start_time minute */2 hour * day_of_month * month *
day_of_week *
#Wireless port configuration for WPA-PSK authentication with password
“friendfriend”
port wireless set Disable false
port wireless set ESSID iMG634WA-example
802.1x authenticator set authentication local
802.1x authenticator set authentication enabled
port wireless set WPAEnableWPA1 true
port wireless set WPAEnableWPA2 false
port wireless set WPA true
port wireless set WPAEnablePSK true
port wireless set WPA2EnableTKIP false
port wireless set WPA2EnableAES_CCMP true
port wireless set WPA2EnablePreauth true
port wireless set Authentication WPA-PSK
port wireless set Encryption TKIP
port wireless set WPAEnableWPA2 false
wpa set shared passphrase friendfriend
```

9.1.3 Layer 3 routing on wireless port

The following scenario it’s similar to the layer 2 scenario except that the traffic on CPE wireless interface is routed to a public interface attached to the ADSL port.

In this scenario the wireless interface is member of the data VLAN together with a switch Ethernet port. Traffic originated by the wireless host can be forwarded to the host connected at the Ethernet port or can be routed to the uplink path where IP masquerading is performed by NAT.

In this scenario the access to the public network (the data path) is based on a PPPoEoA connection.

Please refer to chapter 2. for any information on how to configure the bridge functionality on the CPE for each different products group.

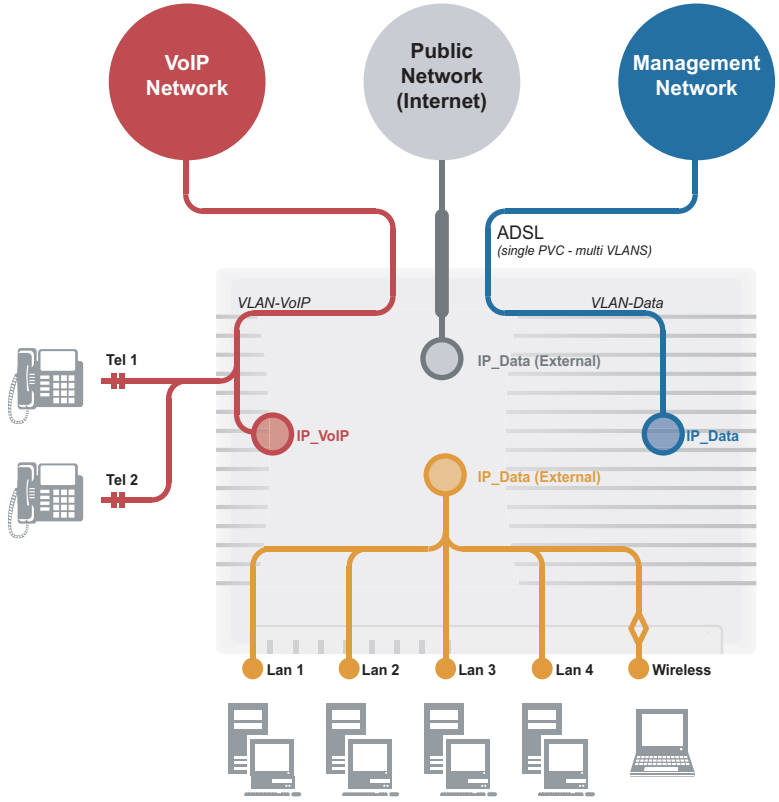


FIGURE 9-2 Wireless interface usage on a routed scenario

9.1.3.1 Layer 3 CPE Configuration for ADSL A group wireless products

A DHCP server is used to provides addresses on this subnet. 172.32.2.1 is the default gateway for this subnet.

```
vlan add vlan_mgmt vid 202
ethernet ad transport vlan_mgmt
ip ad interface ip_mgmt
dhcpclient ad interfaceconfig ic_mgmt ip_mgmt
dhcpclient interfaceconfig ic_mgmt add requested option subnet-mask
dhcpclient interfaceconfig ic_mgmt add requested option routers
dhcpclient interfaceconfig ic_mgmt add requested option domain-name
dhcpclient interfaceconfig ic_mgmt add requested option domain-name-
servers
rfc1483 set transport pvc_0_35 vlan vlan_mgmt frame tagged
ip attach ip_mgmt vlan_mgmt
dhcpclient update
```

```
#Clean up interface ip0 (default)
ip set interface ip0 dhcp disabled
dhcpclient update
ip set interface ip0 ipaddress 0.0.0.0 0.0.0.0
rfc1483 unset transport pvc_0_35 vlan default
ip set interface ip_mgmt dhcp enabled
dhcpclient update
#Management access configuration. 172.30.1.0 and 10.17.90.0 subnets
are located on management networks.
webserver add managementsubnet mgmt1 172.30.1.0 255.255.255.0
172.30.1.1 172.30.1.254
webserver add managementsubnet mgmt2 10.17.90.0 255.255.255.0
10.17.90.1 10.17.90.254
#VoIP network configuration. A DHCP server is used to provides
addresses on this subnet on PVC 8/35. 172.32.3.1 is the default gate-
way for this subnet.
ip add interface ip_voip
ip set interface ip_voip dhcp enabled
dhcpclient add interfaceconfig ic_voip ip_voip
dhcpclient interfaceconfig ic_voip add requested option subnet-mask
dhcpclient interfaceconfig ic_voip add requested option routers
dhcpclient interfaceconfig ic_voip add requested option domain-name-
servers
dhcpclient interfaceconfig ic_voip add requested option domain-name
dhcpclient set interfaceconfig ic_voip givednstoclient enabled
dhcpclient set interfaceconfig ic_voip givednstorelay disabled
dhcpclient set interfaceconfig ic_voip defaultroute disabled
rfc1483 add transport pvc_voip a1 8 35
bridge add interface if_pvc_voip
vlan add vlan_voip vid 203
ethernet add transport vlan_voip
rfc1483 set transport pvc_voip vlan vlan_voip frame untagged
bridge attach if_pvc_voip pvc_voip
ip attach ip_voip vlan_voip
dhcpclient update
#Data network configuration. A PPP connection is configured on this
interface on PVC 1/35.
ip add interface ip_data
pppoe add transport pppoe_data dialout pvc 4 a1 1 35
pppoe set transport pppoe_data welogin chap
pppoe set transport pppoe_data username manager
pppoe set transport pppoe_data password friend
pppoe set transport pppoe_data subnetmask 255.255.255.255
```

```
pppoe set transport pppoe_data givedns client disabled
pppoe set transport pppoe_data givedns relay enabled
pppoe set transport pppoe_data createroute enabled
ip attach ip_data pppoe_data
#Internal private user network. A DHCP server is configured on the CPE
to provide addresses to the hosts connected on this network.
vlan add vlan_user vid 100 802.1p_priority 0
ethernet add transport vlan_user
vlan add vlan_user port lan4 frame untagged
vlan add vlan_user port wireless frame untagged
ip add interface ip_user
ip set interface ip_user ipaddress 192.168.1.1 255.255.255.0
ip attach ip_user vlan_user
dhcpserver enable
dhcpserver add subnet dhcp_user 192.168.1.0 255.255.255.0
192.168.1.100 192.168.1.200
dhcpserver set subnet dhcp_user hostisdefaultgateway enabled
dhcpserver set subnet dhcp_user hostisdnsserver enabled
dhcpserver update
#Routing table reconfiguration.
ip add route voice_server 172.30.1.121 255.255.255.255 gateway
172.32.3.1
ip add route voice_server2 172.30.1.123 255.255.255.255 gateway
172.32.3.1
ip add route voice_server3 172.30.1.201 255.255.255.255 gateway
172.32.3.1
ip add route mgmt-1 10.17.90.0 255.255.255.0 gateway 172.32.2.1
ip add route mgmt-2 172.30.1.202 255.255.255.255 gateway 172.32.2.1
#Local time and date configuration.
sntpclient add server ipaddress 172.30.1.202
sntpclient set pollintv 2
sntpclient set timezone MET
#VoIP protocol configuration.
voip sip protocol enable
voip dtmf-relay set mode auto
voip ep analogue create tel1 type al-fxs-del physical-port tel1
voip ep analogue set tel1 country usa
voip ep analogue set tel1 clip BELL
voip ep analogue set tel1 clir off
voip ep analogue set tel1 codec g711u
voip ep analogue set tel1 vad off
voip ep analogue set tel1 cng off
voip ep analogue set tel1 lec 8
```

```
voip ep analogue create tel2 type al-fxs-del physical-port tel2
voip ep analogue set tel2 country usa
voip ep analogue set tel2 clip BELL
voip ep analogue set tel2 clir off
voip ep analogue set tel2 codec g711u
voip ep analogue set tel2 vad off
voip ep analogue set tel2 cng off
voip ep analogue set tel2 lec 8
voip sip protocol set netinterface ip_voip
voip sip locationserver create loc1 contact 172.30.1.121
voip sip proxyserver create prox1 contact 172.30.1.121
voip sip protocol set internal-call-routing enable
voip sip user create 1723231461 address 1723231461 areacode 604
voip sip user add 1723231461 port tel1
voip sip user create 1723231462 address 1723231462 areacode 604
voip sip user add 1723231462 port tel2
#IP masquerade configuration.
security enable
security add interface ip_data external
security add interface ip_user internal
nat enable data-ext_int ip_data internal
#Software update configuration
swupdate set server 172.30.1.9
swupdate set path /public/swupdate/3-4_57_02_04/alpha/iMG634B/upload
swupdate set login root
swupdate set passwd friend
swupdate stop_time none
swupdate start_time minute */2 hour * day_of_month * month *
day_of_week *
#Wireless port configuration for WPA2 AES-CCMP authentication with
password “friendfriend”
port wireless set Disable false
port wireless set ESSID iMG634WA-example
802.1x authenticator set authentication local
802.1x authenticator set authentication enable
port wireless set WPAEnableWPA1 true
port wireless set WPAEnableWPA2 true
port wireless set WPA true
port wireless set WPAEnablePSK true
port wireless set WPA2EnableTKIP false
port wireless set WPA2EnableAES_CCMP true
port wireless set WPA2EnablePreauth true
port wireless set Authentication WPA-PSK
```

```
port wireless set Encryption TKIP
wpa set shared passphrase friendfriend
```

9.1.3.2 Layer 3 CPE Configuration for ADSL B group wireless products

```
#Management network configuration. A DHCP server is used to provides
addresses on this subnet. 172.32.2.1 is the default gateway for this
subnet.
vlan create vlan_mgmt 202
ip ad interface ip_mgmt
dhcpclient ad interfaceconfig ic_mgmt ip_mgmt
dhcpclient interfaceconfig ic_mgmt add requested option subnet-mask
dhcpclient interfaceconfig ic_mgmt add requested option routers
dhcpclient interfaceconfig ic_mgmt add requested option domain-name
dhcpclient interfaceconfig ic_mgmt add requested option domain-name-
servers
bridge add vlaninterface vlan_mgmt tagged pvc_0_35_if
ip attach ip_mgmt vlan_mgmt
dhcpclient update
#Clean up interface ip0 (default)
ip set interface ip0 dhcp disabled
dhcpclient update
ip set interface ip0 ipaddress 0.0.0.0 0.0.0.0
bridge delete vlaninterface DefaultVlan pvc_0_35_if
ip set interface ip_mgmt dhcp enabled
dhcpclient update
#Management access configuration. 172.30.1.0 and 10.17.90.0 subnets
are located on management networks.
webserver add managementsubnet mgmt1 172.30.1.0 255.255.255.0
172.30.1.1 172.30.1.254
webserver add managementsubnet mgmt2 10.17.90.0 255.255.255.0
10.17.90.1 10.17.90.254
#VoIP network configuration. A DHCP server is used to provides
addresses on this subnet on PVC 8/35. 172.32.3.1 is the default gate-
way for this subnet.
ip add interface ip_voip
ip set interface ip_voip dhcp enabled
dhcpclient add interfaceconfig ic_voip ip_voip
dhcpclient interfaceconfig ic_voip add requested option subnet-mask
dhcpclient interfaceconfig ic_voip add requested option routers
dhcpclient interfaceconfig ic_voip add requested option domain-name-
servers
dhcpclient interfaceconfig ic_voip add requested option domain-name
```

```
dhcpclient set interfaceconfig ic_voip givednstoclient enabled
dhcpclient set interfaceconfig ic_voip givednstorelay disabled
dhcpclient set interfaceconfig ic_voip defaultroute disabled
rfc1483 add transport pvc_voip a1 8 35
bridge add interface if_pvc_voip
vlan create vlan_voip 203
bridge attach if_pvc_voip pvc_voip
bridge add vlaninterface vlan_voip untagged if_pvc_voip
ip attach ip_voip vlan_voip
dhcpclient update
#Data network configuration. A PPP connection is configured on this
interface on PVC 1/35.
ip add interface ip_data
pppoe add transport pppoe_data dialout pvc 4 a1 1 35
pppoe set transport pppoe_data welogin chap
pppoe set transport pppoe_data username manager
pppoe set transport pppoe_data password friend
pppoe set transport pppoe_data subnetmask 255.255.255.255
pppoe set transport pppoe_data givedns clint disabled
pppoe set transport pppoe_data givedns relay enabled
pppoe set transport pppoe_data createroute enabled
ip attach ip_data pppoe_data
#Internal private user network. A DHCP server is configured on the
CPE to provide addresses to the hosts connected on this network.
vlan create vlan_user 100
vlan add vlan_user lan4 frame untagged
switch set port lan4 802.1p Enabled
switch set port lan4 defaultpriority 0
bridge add vlaninterface vlan_user untagged wlan_filtered
bridge set interface wlan_filtered defaultuserpriority 0
ip add interface ip_user
ip set interface ip_user ipaddress 192.168.1.1 255.255.255.0
ip attach ip_user vlan_user
dhcpserver enable
dhcpserver add subnet dhcp_user 192.168.1.0 255.255.255.0
192.168.1.100 192.168.1.200
dhcpserver set subnet dhcp_user hostisdefaultgateway enabled
dhcpserver set subnet dhcp_user hostisdnsserver enabled
dhcpserver update
#Routing table reconfiguration.
ip add route voice_server 172.30.1.121 255.255.255.255 gateway
172.32.3.1
```

```
ip add route voice_server2 172.30.1.123 255.255.255.255 gateway
172.32.3.1
ip add route voice_server3 172.30.1.201 255.255.255.255 gateway
172.32.3.1
ip add route mgmt-1 10.17.90.0 255.255.255.0 gateway 172.32.2.1
ip add route mgmt-2 172.30.1.202 255.255.255.255 gateway 172.32.2.1
#Local time and date configuration.
sntpclient add server ipaddress 172.30.1.202
sntpclient set pollintv 2
sntpclient set timezone MET
#VoIP protocol configuration.
voip sip protocol enable
voip dtmf-relay set mode auto
voip ep analogue create tel1 type al-fxs-del physical-port tel1
voip ep analogue set tel1 country usa
voip ep analogue set tel1 clip BELL
voip ep analogue set tel1 clir off
voip ep analogue set tel1 codec g711u
voip ep analogue set tel1 vad off
voip ep analogue set tel1 cng off
voip ep analogue set tel1 lec 8
voip ep analogue create tel2 type al-fxs-del physical-port tel2
voip ep analogue set tel2 country usa
voip ep analogue set tel2 clip BELL
voip ep analogue set tel2 clir off
voip ep analogue set tel2 codec g711u
voip ep analogue set tel2 vad off
voip ep analogue set tel2 cng off
voip ep analogue set tel2 lec 8
voip sip protocol set netinterface ip_voip
voip sip locationserver create loc1 contact 172.30.1.121
voip sip proxyserver create prox1 contact 172.30.1.121
voip sip protocol set internal-call-routing enable
voip sip user create 1723231461 address 1723231461 areacode 604
voip sip user add 1723231461 port tel1
voip sip user create 1723231462 address 1723231462 areacode 604
voip sip user add 1723231462 port tel2
#IP masquerade configuration.
security enable
security add interface ip_data external
security add interface ip_user internal
nat enable data-ext_int ip_data internal
#Software update configuration
```

```
swupdate set server 172.30.1.9
swupdate set path /public/swupdate/3-4_57_02_04/alpha/iMG634B/upload
swupdate set login root
swupdate set passwd friend
swupdate stop_time none
swupdate start_time minute */2 hour * day_of_month * month *
day_of_week *
#Wireless port configuration for WPA2 AES-CCMP authentication with
password “friendfriend”
port wireless set Disable false
port wireless set ESSID iMG634WA-example
802.1x authenticator set authentication local
802.1x authenticator set authentication enable
port wireless set WPAEnableWPA1 true
port wireless set WPAEnableWPA2 true
port wireless set WPA true
port wireless set WPAEnablePSK true
port wireless set WPA2EnableTKIP false
port wireless set WPA2EnableAES_CCMP true
port wireless set WPA2EnablePreauth true
port wireless set Authentication WPA-PSK
port wireless set Encryption TKIP
wpa set shared passphrase friendfriend
```

9.1.4 Authentication Configuration

9.1.4.1 Open Authentication Configuration

9.1.4.1.1 Open Authentication - None Encryption

On open-system authentication no actual authentication takes place: all stations are allowed to connect to the AP without credential exchange.

On CPE side, an open wireless network can be configured through the following CLI commands list:

```
port wireless set Disable false
port wireless set ESSID iMG634WB-172.32.2.146 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication disabled
port wireless set Authentication Open
port wireless set Encryption None
```

9.1.4.1.2 Open Authentication - WEP Encryption @ 64 bit

WEP (Wired Equivalent Privacy) is the basic 802.11's encryption algorithm implemented in the Medium Access Control Layer (MAC layer) of wireless network devices. WEP has been deprecated by IEEE as it provides security that deters only unintentional use, leaving the network vulnerable to deliberate compromise.

For better security levels use WPA or WPA2.

The open network authentication system with WEP encryption doesn't pass on any information to the client in plain text, just the corresponding encrypted text.

On CPE side, a 64bit WEP encrypted wireless network can be configured through the following CLI commands list:

```
port wireless set Disable false
port wireless set ESSID iMG634WB-172.32.2.146 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication disable
port wireless set Authentication Open
port wireless set Encryption WEP64
port wireless set Mode64Key0 11-22-33-44-55 (example)
port wireless set Mode64Key1 66-77-88-99-aa (example)
port wireless set Mode64Key2 bb-cc-dd-ee-ff (example)
port wireless set Mode64Key3 10-1a-aa-a1-01 (example)
```

9.1.4.1.3 Open Authentication - WEP Encryption @ 128 bit

On CPE side, a 128bit WEP encrypted wireless network can be configured through the following CLI commands list:

```
port wireless set Disable false
port wireless set ESSID iMG634WB-172.32.2.143 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication disable
port wireless set Authentication Open
port wireless set Encryption WEP128
port wireless set Mode128Key0 11-22-33-44-55-66-77-88-99-aa-bb-cc-dd*
port wireless set Mode128Key1 66-77-88-99-aa-bb-cc-dd-ee-ff-11-22-33*
port wireless set Mode128Key2 bb-cc-dd-ee-ff-11-22-33-44-55-66-77-88*
port wireless set Mode128Key3 10-1a-aa-a1-10-1a-aa-a1-10-1a-aa-a1-77*
```

*examples

9.1.4.2 Shared Authentication Configuration

With a shared-key authentication process the AP (Access Point) sends challenge text to the client in clear text, and then the client encrypts it and sends it back to the AP for authentication.

Because on shared-key authentication the shared system passes along additional information, this authentication method exposes information that could be used by a hacker to crack the WEP key.

For better security levels use WPA or WPA2.

9.1.4.2.1 Shared Authentication and WEP Encryption @ 64bit

On CPE side, a Shared system supporting 64bit WEP encryption can be configured through the following CLI commands list:

```
port wireless set Disable false
port wireless set ESSID iMG634WA-ST-172.32.2.142 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication disable
port wireless set Authentication Shared
port wireless set Encryption WEP64
port wireless set Mode64Key0 11-22-33-44-00
port wireless set Mode64Key1 55-66-77-88-00
port wireless set Mode64Key2 aa-bb-cc-dd-00
port wireless set Mode64Key3 ab-cd-ef-98-76
```

9.1.4.2.2 Shared Authentication and WEP Encryption @ 128bit

On CPE side, a Shared system supporting 128bit WEP encryption can be configured through the following CLI commands list:

```
port wireless set Disable false
port wireless set ESSID iMG634WA-ST-172.32.2.142 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication disable
port wireless set Authentication Shared
port wireless set Encryption WEP128
port wireless set Mode128Key0 11-22-33-44-55-66-77-88-99-aa-bb-cc-dd*
port wireless set Mode128Key1 66-77-88-99-aa-bb-cc-dd-ee-ff-11-22-33*
port wireless set Mode128Key2 bb-cc-dd-ee-ff-11-22-33-44-55-66-77-88*
port wireless set Mode128Key3 10-1a-aa-a1-10-1a-aa-a1-10-1a-aa-a1-77*
```

*examples

9.1.4.3 WPA-PSK Authentication and TKIP Encryption

WPA (Wi-Fi Protected Access) authentication is a strong, standards-based interoperable Wi-Fi security specification that uses Temporal Key Integrity Protocol (TKIP) as data encryption method.

On CPE side, a WPA-PSK with TKIP encryption wireless network can be configured through the following command list:

```
port wireless set Disable false
port wireless set ESSID iMG634WA-ST-172.32.2.142 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication enabled
port wireless set Authentication WPA-PSK
port wireless set Encryption TKIP
wpa set shared passphrase friendfriend (example)
```

9.1.4.4 WPA2-PSK Authentication and AES_CCMP Encryption

WPA2 (formerly IEEE 802.11i) is an evolution of WPA and uses a new strong AES-based encryption algorithm, CCMP (Counter Mode with CBC-Message Authentication Code Protocol), which is considered fully secure.

On CPE side, a WPA2-PSK AES_CCMP encryption wireless network can be configured through the following CLI commands list:

```
port wireless set Disable false
port wireless set ESSID iMG634WA-ST-172.32.2.142 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication enabled
port wireless set Authentication WPA-PSK
port wireless set Encryption AES_CCMP
wpa set shared passphrase friendfriend (example)
```

9.1.4.5 WPA2 Mixed Mode Authentication

Using this configuration, wireless clients of both types (WPA and WPA2) can connect to the device.

On CPE side, a WPA2 Mixed Mode encryption wireless network can be configured through the following CLI commands list:

```
port wireless set Disable false
port wireless set ESSID iMG634WA-ST-172.32.2.142 (example)
802.1x authenticator set authentication local
802.1x authenticator set authentication enabled
port wireless set Authentication WPA-PSK
port wireless set Encryption WPA2_Mixed
wpa set shared passphrase friendfriend (example)
```

9.1.5 Summary of wireless attribute and configurations

The configuration commands <`port wireless set Authentication/Encryption ...`> acts directly on the wireless port attributes in order to set up the desired authentication configuration. The follow-

ing table summarizes the relationship between these commands and the related port attributes (see next chapter for a detailed description of each one).

TABLE 9-1 Summary of wireless port attributes versus wireless security schemes

Authentication type / Encryption method	Open None	Open Wep 64bit	Open Wep 128bit	Shared Wep 64bit	Shared Wep 128bit	WPA-PSK TKIP	WPA2-PSK AES_CCMP	WPA2 Mixed Mode
WepEncryption	disabled	64bit	128bit	64bit	128bit	disabled	disabled	disabled
WepAuthentication	False	False	False	True	True	False	False	False
WPAEnableWPA1	False	False	False	False	False	True	False	True
WPAEnableWPA2	False	False	False	False	False	False	True	True
WPA	False	False	False	False	False	True	True	True
WPAEnablePSK	False	False	False	False	False	True	True	True
WPAEnableTKIP	False	False	False	False	False	True	False	True
WPA2EnableAES_CCMP	False	False	False	False	False	False	True	True
802.1x authentication	disable	disable	disable	disable	disable	enable	enable	enable

9.1.6 Wireless Interface CLI commands

9.1.6.1 802.1x Authenticator commands

The table below lists the *802.1x Authenticator* commands provided by the CLI:

TABLE 9-2 802.1x Authenticator Commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
802.1X AUTHENTICATOR SET AUTHENTICATION				X			X	X	
802.1X AUTHENTICATOR SET IDENTITY				X			X	X	
802.1X AUTHENTICATOR SET KEY-TRANSMISSION				X			X	X	
802.1X AUTHENTICATOR SET REKEY-TIMEOUT				X			X	X	
802.1X AUTHENTICATOR SHOW				X			X	X	

9.1.6.1.1 802.1X AUTHENTICATOR SET AUTHENTICATION

Syntax `802.1x AUTHENTICATOR SET AUTHENTICATION <value>`

Description This command allows to enable/disable authentication methods with 802.1x standard, accordingly to 802.11 specifications.

Options The following table gives the range values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
value	Possible values are: **Local** - Set a local server as device authentication method (using MD5) **Disable** - Disable authentication on the device, mandatory for Open/Shared system wireless networks. **Enable** - Set the CPE as authenticator in the WPA/WAP2 system wireless network	Local

9.1.6.1.2 802.1X AUTHENTICATOR SET IDENTITY

Syntax `802.1x AUTHENTICATOR SET IDENTITY <string>`

Description This command allows to set a unique identity string for the device. The authenticator will use this string to identify the device.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
string	A string used for identification purposes. If not configured manually, the model name and device's MAC Address is displayed.	Model Name and MAC address (i.e.iMG634WA-R2-main 00:0d:da:05:51:8f)

9.1.6.1.3 802.1X AUTHENTICATOR SET KEY-TRANSMISSION

Syntax `802.1x AUTHENTICATOR SET KET-TRANSMISSION {ENABLED | DISABLED}`

Description This command enables/disables key-transmission according to 802.11 specifications.

9.1.6.1.4 802.1X AUTHENTICATOR SET REKEY-TIMEOUT

Syntax `802.1x AUTHENTICATOR SET REKEY-TIMEOUT <sec>`

Description This command sets the WEP rekey timeout that causes the issue of a new WEP key for the session. Once set to a suitable timeout, the keys will rotate at a rate fast enough to prevent an attacker from sniffing enough packets in order to discover the WEP key.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
sec	The time (in seconds) before a WEP key is rotated.	600

9.1.6.1.5 802.1X AUTHENTICATOR SHOW

Syntax `802.1x AUTHENTICATOR SHOW`

Description This command returns the status of 802.1x settings

Example --> 802.1x authenticator show

```
802.1x Authenticator
Auth Server          : Local
Auth Control Enabled : true
Identity String      : VoIP gateway 00:01:38:b6:3e:99
Rekey Timeout        : 600
Key Transmission Enabled : true
Vap Id               : 0
```

```
Entropy Pool          : a508abe250752d01f0aae300146ff200

Supplicants:

 None
```

9.1.6.2 Port Wireless commands

The table below lists the *port wireless* commands provided by the CLI:

TABLE 9-3 Port Wireless Commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
PORT WIRELESS COUNTERS				X			X	X	
PORT WIRELESS SET				X			X[1]	X	
PORT WIRELESS SHOW				X			X	X	
PORT WIRELESS STATUS				X			X	X	

[1)]The command Port Wireless Set IntraBSSRelay 2 is not available on ADSL A

9.1.6.2.1 PORT WIRELESS COUNTERS

Syntax `PORT WIRELESS COUNTERS`

Description This command shows the value of the attribute WPAMICFailures (WPA Message Integrity Code failures) of the wireless device.

Example --> port wireless counters

WPAMICFailures = 0

9.1.6.2.2 PORT WIRELESS SET

Syntax `PORT WIRELESS SET <option> <value>`

Description This command allows to set configuration parameters of the wireless device. Any modification overrides the existing attribute values previously set.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Authentication	Configuration command to be used in conjunction with "*Encryption*" to easily set up an authentication configuration for the network Possible values are: **Open -** Set an open authentication network **Shared** - Set a shared authentication network **WPA-PSK** - Set a WPA/WPA2 authentication network	Open
AutoChannel	Possible values are: **False -** Disable AutoChannel feature **True** - Enable AutoChannel feature: allow the AP to select the best channel on startup	True
CurrentCountry	It sets the current 802.11d country string for the wireless card. The driver will only show the possible values depending on the countries that it actually supports. The form of a country string is the two-byte ISO code for that country (from ISO 3166)	US
DefaultChannel	Default Channel to use. The default value should be the minimum allowed for this band (e.g. 1 for802.11b) unless the device is able to auto-select	n/a
DefaultTxKey	Specifies which encryption key to use by default (offset into the list of 64/128 bit keys depending on the value of "*WepEncryption*" attribute)	0
Disable	Possible values are: **False -** Wireless interface is enabled, wireless connection is allowed **True** - Wireless interface is disabled, wireless network can be seen but no connection will be allowed	False

Option	Description	Default Value
ESSID	Service Set Identifier for the access point	PRISM_xx_yy_zz where xx/yy/zz are the last 3 bytes of the wireless device MAC address
Encryption	Configuration command to be used in conjunction with "*Authentication*" to easily set up an authentication configuration for the network Possible values are: **None -** No encryption used (open authentication network) **WEP64/WEP128** - Use WEP at 64 or 128 bit encryption method (open or shared authentication network) **TKIP** - Use TKIP encryption (WPA authentication network) **AES_CCMP** - Use AES CCMP encryption (WPA2 authentication network) **WPA2_Mixed** - Use both WPA-TKIP and WPA2-AES_CCMP encryption method, to let clients of both authentication types (WPA or WPA2) connect to the device	None
FragmentationThreshold	Set a threshold over which frames will be fragmented	2346
HideSSID	Possible values are: **False** - SSID is shown inside beacon frames **True** - Prevent the CPE from advertising the SSID inside beacon frames	False
IntraBSSRelay	Possible values are: **0** - Disable IntraBSSRelay feature **1** - Enable IntraBSSRelay feature **2*** - Enable Wireless L2 Client Isolation (IntraBSSDrop) feature	1

Option	Description	Default Value
MacAddressAuth	Possible values are: **Disabled** - feauture disabled **Blacklist** - traffic is accepted from all stations except those listed in MacAddressList **Whitelist** - traffic is discarded from all stations except those listed in MacAddressList	Disabled
MacAddressList	A list of station MAC addresses that are allowed or prevented (allowing all others) to communicate with the CPE wireless device, depending on the value of the MacAddressAuth attribute.	Empty list
MaxFrameBurst	Set a threshold for Nitro frames bursting into the CPE	1500
Mode128Key0**	first 128-bit encryption key	all zeros
Mode128Key1**	second 128-bit encryption key	all zeros
Mode128Key2**	third 128-bit encryption key	all zeros
Mode128Key3**	fourth 128-bit encryption key	all zeros
Mode64Key0***	first 64-bit encryption key	all zeros
Mode64Key1***	second 64-bit encryption key	all zeros
Mode64Key2***	third 64-bit encryption key	all zeros
Mode64Key3***	fourth 64-bit encryption key	all zeros
NitroXMCompression	Possible values are: **False** - NitroXM Compression disabled **True** - NitroXM Compression will be used on packets sent to and from the device to another device which supports NitroXM Compression	False
NitroXMConcatenation	Possible values are: **False** - NitroXM Concatenation disabled **True** - NitroXM Concatenation will be used on packets sent to and from the device to another device which supports NitroXM Concatenation	True

Option	Description	Default Value
NitroXMPiggyBack	Possible values: **False** - NitroXM Piggy Back disabled **True** - NitroXM Piggy Back will be used on packets sent to and from the device to another device which supports NitroXM Piggy Back	True
Profile	This attribute is used to set a "profile" for device operation. Different profiles select different operating parameters. Cards that support 802.11g must default to MIXED_G_WIFI. Possible values are: **MIXED_G_WIFI** - 2.4 GHz 802.11g/b Dynamic Non-ERP **B_ONLY** - 2.4 GHz 802.11b **G_ONLY** - 2.4 GHz 802.11g without Non-ERP **MIXED_LONG** - 2.4 GHz 802.11g/b long preamble	MIXED_G_WIFI
RtsThreshold	Set a threshold over which frames will use RTS/CTS	2347
TransmitRate	Set the desired transmit rate. Possible values are: **Automatic** - Let the driver choose the optimal transmit rate **1,2,5.5,6,9,11,12,18,24,36,48,54 Mbps** - Manually set the corresponding rate	Automatic
WMM	Possible values are: **False -** Disable WMM support **True** - Enable WMM support	False
WMMPS	Possible values are: **False -** Disable WMMPS support **True** - Enable WMMPS support	False

Option	Description	Default Value
WPA	Possible values are: **False** - Disable WPA1 and WPA2 authentication method **True** - Enable WPA1 if WPAEnableWPA1 is enabled, WPA2 if WPAEnableWPA2 is enabled, both if either WPAEnableWPA1 and WPAEnableWPA2 are enabled	False
WPA2EnableAES_CCMP	Possible values are: **False -** Disable AES_CCMP encryption method with WPA2 **True -** Enable AES_CCMP with WPA2 authentication method, this is the normal mode of operation for WPA2	False
WPA2EnablePreauth	Possible values are: **False** - Disable Pre-authentication feature **True -** Enable Pre-authentication feature with WPA2 authentication method	True
WPA2EnableTKIP	Possible values are: **False -** Disable TKIP with WPA2 authentication **True** - Enable TKIP also for WPA2 authentication except for WPA1, for WPA2 is an optional mode of operation	False
WPAEnableAES_CCMP	Possible values are: **False -** Disable AES_CCMP encryption method with WPA1 authentication **True -** Enable AES_CCMP with WPA1 authentication method	False
WPAEnablePSK	Possible values are: **False -** Disable PSK (Pre-shared Key) **True -** Enable PSK (Pre-shared Key)	False

Option	Description	Default Value
WPAEnableTKIP	Possible values are: **False -** Disable TKIP with WPA1 authentication **True** - Enable TKIP also for WPA1 authentication, this is the normal mode of operation for WPA1	True
WPAEnableWPA1	Possible values are: **False -** Disable the WPA1 standard authentication method **True -** Enable the WPA1 support if WPA is also enabled	True
WPAEnableWPA2	Possible values are: **False** - Disable the WPA2 authentication method **True -** Enable the WPA2 (802.11i) standard support if WPA is also enabled	True
WepAuthentication	Possible values are: **False -** Disable WEP Authentication (Open system wireless network) **True** - Enable WEP Authentication (Shared system wireless network)	False
WepEncryption	Possible values are: **Disabled -** No WEP encryption **64bit** - Enable 40-bit encryption **128bit** - Enable 104-bit encryption	Disabled
resetDefaults	Mark the port in order to don't save its configuration and to acquire its default values at next reboot. Possible values are: **False -** Allow saving new port configuration and keeping it after reboot **True** - Do not save port changes when saving system configuration, letting the port acquire its default values at next reboot	False

* Feature present only on FIBER D / ADSL B group wireless products

** 26 hexadecimal characters

*** 10 hexadecimal characters

9.1.6.2.3 PORT WIRELESS SHOW

Syntax `PORT WIRELESS SHOW`

Description This command shows a complete description of the wireless device configuration set

Example --> port wireless show

```
Authentication                  = Open
Encryption                      = None
PortClassEthernet               = true
PortClass802_11                 = true
VapId                           = 0
Version                         = 1.20
BMACVersion                     = 2.1.25.0
LMACVersion                     = 2.17.27.0
UMACVersion                     = 2.20.12.0e
State                           = LinkUp
AllowedChannels                 = 1,2,3,4,5,6,7,8,9,10,11
AntennaDiversity                = 1
AuthenticateSTA                 = 00:00:00:00:00:00
AutoChannel                     = true
CollectStats                    = true
Connected                       = true
CurrentCountry                  = US
DeAuthenticateSTA               = 00:00:00:00:00:00
DefaultChannel                  = 10
DefaultMaxQueue                 = 32
DefaultTxKey                    = 0
Disable                         = false
ESSID                           = PRISM_69_ae_52
FragmentationThreshold          = 2346
HideSSID                        = false
IEEE802_11_EventSink            = /task/i802_1x
IntraBSSRelay                   = 1
WMM                              = false
WMMPS                           = false
LinkSpeed                       = 540000
MAC                             = 00:01:38:69:ae:52
MacAddressAuth                  = disabled
MacMode                         = AP
MaxAssociatedStations           = 32
```

```
MaxFrameBurst                    = 1500
Mode128Key0                        = 00-00-00-00-00-00-00-00-00-00-
00-00-00
Mode128Key1                        = 00-00-00-00-00-00-00-00-00-00-
00-00-00
Mode128Key2                        = 00-00-00-00-00-00-00-00-00-00-
00-00-00
Mode128Key3                        = 00-00-00-00-00-00-00-00-00-00-
00-00-00
Mode64Key0                       = 00-00-00-00-00
Mode64Key1                       = 00-00-00-00-00
Mode64Key2                       = 00-00-00-00-00
Mode64Key3                       = 00-00-00-00-00
EnableKey0                       = true
EnableKey1                       = true
EnableKey2                       = true
EnableKey3                       = true
NitroXMCompression               = false
NitroXMConcatenation             = true
NitroXMDirectLink                = true
NitroXMPiggyBack                 = true
PlainTextEAPOL                   = false
Profile                          = MIXED_G_WIFI
PromiscuousEnable                = true
RtsThreshold                     = 2347
SMDebugLevel                     = 1
TransmitRate                     = Automatic
WepEncryption                    = disabled
WepAuthentication                = false
WepKeyMapping                    = false
WPAEnableWPA1                    = true
WPAEnableWPA2                    = true
WPA                              = false
WPAAdvertisedIE                  = 0x00000000
RSNAdvertisedIE                  = 0x00000000
WPAMICFailures                   = 0
WPAEnablePSK                     = false
WPAEnableEAP                     = false
WPA2EnableTKIP                   = false
WPA2EnableAES_CCMP               = false
WPAEnableAES_CCMP                = false
WPAEnableTKIP                    = true
WPA2EnablePreauth                = true
```

```
WIRELESSTAG                    = 0
AssociatedClients              = 0
McMsduTx                       = 0
McMsduRx                       = 0
TxSuccessful                   = 3042
TxOneRetry                     = 665
TxMultipleRetries              = 0
TxFailed                       = 3033
RxSuccessful                   = 56248
RxDups                         = 0
RTSSuccessful                  = 0
RTSFailed                      = 0
ACKFailed                      = 6721
FrameReceives                  = 127166
FrameErrors                    = 35386
FrameAborts                    = 24585
FrameAbortsPHY                 = 128458
PrivTxRejected                 = 0
PrivRxPlain                    = 0
PrivRxFailed                   = 0
PrivRxNoKey                    = 0
AllocBufTooShort               = 0
AllocNoBuf                     = 0
AllocNoPCIMap                  = 0
ICNoRxCtrlBuf                  = 0
ICNoRxDataBuf                  = 0
Resets                         = 0
RxErrBus                       = 0
RxErrWrongMAC                  = 0
SMACServiceError               = 0
TxErrBus                       = 0
TxErrNoBuffers                 = 0
TxErrNoRemap                   = 0
TxErrQDepth                    = 0
TxErrResetOrCancel             = 0
TxErrSMAC                      = 6
TxErrTooLong                   = 0
TxNoPCIMap                     = 0
TxNoPrefix                     = 0
TxNoTrailer                    = 0
TxBeacons                      = 1
TxProbeResponses               = 6019
AssociationsRefused            = 0
```

```
AssociationsGranted                = 0
resetDefaults                      = false
portSnmpIfIndex                    = 0
portSnmpIfType                     = 0
```

9.1.6.2.4 PORT WIRELESS STATUS

Syntax `PORT WIRELESS STATUS`

Description This command shows a brief description of the wireless device configuration set

Example --> port wireless status

```
Authentication                     = Open
Encryption                         = None
AutoChannel                        = true
Connected                          = true
CurrentCountry                     = US
DefaultChannel                     = 10
DefaultTxKey                       = 0
Disable                            = false
ESSID                              = PRISM_69_ae_52
LinkSpeed                          = 540000
MAC                                = 00:01:38:69:ae:52
Mode128Key0                        = 00-00-00-00-00-00-00-00-00-000
Mode128Key1                        = 00-00-00-00-00-00-00-00-00-000
Mode128Key2                        = 00-00-00-00-00-00-00-00-00-000
Mode128Key3                        = 00-00-00-00-00-00-00-00-00-000
Mode64Key0                         = 00-00-00-00-00
Mode64Key1                         = 00-00-00-00-00
Mode64Key2                         = 00-00-00-00-00
Mode64Key3                         = 00-00-00-00-00
Profile                            = MIXED_G_WIFI
TransmitRate                       = Automatic
WPAEnableWPA1                      = true
WPAEnableWPA2                      = true
WPA                                = false
resetDefaults                      = false
```

9.1.6.3 WPA Commands

The table below lists the *wpa* commands provided by the CLI:

TABLE 9-4 Port Wireless Commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
WPA SET SHARED				X			X	X	
WPA SET PMK CACHING				X			X	X	
WPA GET PMK CACHING				X			X	X	

9.1.6.3.1 WPA SET SHARED

Syntax `WPA SET SHARED <option> <value>`

Description This command allows to set the password or network-key for the WPA/WPA2 authentication wireless method.

Options The following table gives the range of values for each option that can be specified with this command and a default value (if applicable).

Option	Description	Default Value
Passphrase	A unique network password of between 8 and 63 characters, including special characters. The password must be enclosed in double quotation marks if it contains spaces	n/a
key	Hexadecimal string of at least 32 bytes or 64 hexadecimal digits	n/a

9.1.6.3.2 WPA SET PMK CACHING

Syntax `WPA SET PMK CACHING {ENABLED | DISABLED}`

Description This command enables/disables PMK caching feature. Once this setting has been enabled, the system will start caching the PMK security association (PMKSA).

9.1.6.3.3 WPA GET PMK CACHING

Syntax `WPA GET PMK CACHING`

Description This command tells whether PMK caching feature is enable in the system or not. This would only be effective in case the system is configured n WPA2 mode.

Example --> wpa get pmk caching

```
Pmk Caching: false
```

10. LAN Module Management

The iMG Mods, including the iMG626, iMG646, iMG726, and iMG746, support multiple LAN modules. Each LAN module can be used to provide a different type of service.

10.1 System Overview

10.1.1 Default Factory Configuration

When a LAN Module is detected, a port is created that corresponds to the service on that LAN module. Specifically for the HPNA daughter-card, an HPNA ports is created and attached to the default VLAN. If the CES daughter-card is created then the ports CESD and CESC are created. The CESD port is attached to the default VLAN and is used to transport the E1/T1 data. The CESC port is for management – and is automatically managed by the software.

10.1.2 Adding/Removing & Changing LAN Modules

When a new LAN module is added or changed to a different type, it is recommended that the user set the configuration back to the factory mode and remove all current saved configurations. This ensures that the base configuration is clean and only reflects what is in the device. The iMG Mod will then need to be reconfigured with the new LAN module features as well as any non-module based configuration such as voice or internet.

WARNING: Power MUST BE REMOVED before changing the LAN module. Damage to the device can result if these directions are not followed.

10.1.3 Device and Module Compatibility

When LAN and WAN modules are added to the devices, they utilize resources within the device to prvide the service that they are offering. There are some WAN modules that require resources that are only available on Later Modular units and there are some LAN Modules that require resources that are also required by some LAN modules. In this architecture - the LAN Module always wins - so if a LAN Module is added that conflicts, then the ports associated with it will not be created, a Log will be created - and the LAN LED will go red - and stay red.

Module	iMG 626	iMG 646	iMG 726	iMG 746					
100M BIDI WAN MODULE	X	X	X	X					
GEPON WAN MODULE	X	X	X	X					

1 GIG BIDI WAN MODULE			X	X					
1 GIG BIDI WAN PLUS 1 GIG COPPER LAN			X	X					
HPNA LAN MODULE (120MBPS LOW BAND)	X	X	X	X					
CES LAN MODULE	X	X	X(a)	X(a)					

Note: a) Not compatible with 1 Gig BiDi WAN plus 1 Gig Copper LAN MOdule.

10.1.4 Functional Differences for LAN Modules Management in Product Categories

The table below is intended to identify what is common amongst the product families - as well as where there are differences - to highlite those differences. To determine which family your device belongs to - please refer to the preface.

TABLE 10-1 Functions for Modular iMGs

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
HPNA LAN MODULE						X			
CES LAN MODULE						X			

10.2 HPNA LAN Module

10.2.1 HPNA Deployment Model

Here is a typical HPNA Deploment Model

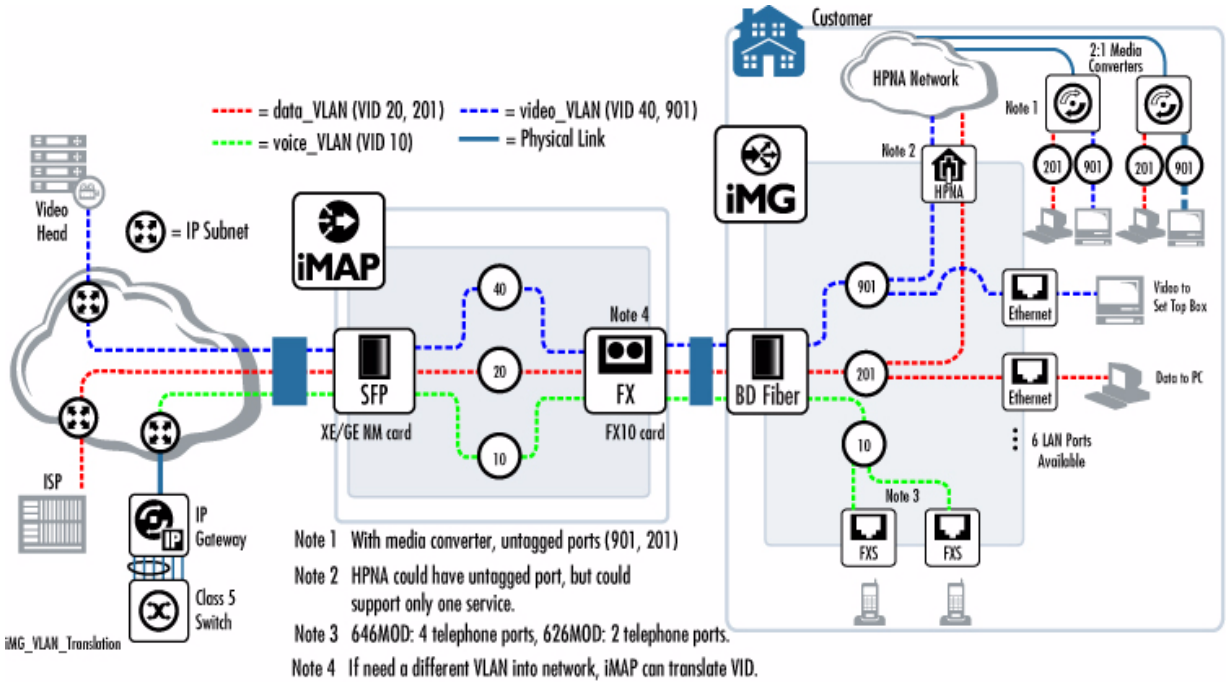


FIGURE 10-1 HPNA Section of LAN Module Diagram

- HPNA is deployed over coax in a residence – and is capabile of carrying both data and video. In order to ensure that the appropriate priority is observed for the different content sources, the recommended deployment model utilizes VLANs and the associated 802.p priority bits (with a P-bit value of 5 or greated equating to high prioirity Video). Since the end points that are recommended for use are fixed to support VLAN 201 and 901 – it is essential that the network deployment be such that the VLANs carrying the video and data align. Normally this is not the case within the carriers network – thus the recommendation to use VLAN translations in order to map the appropriate services onto the 201 and 901 VLAN ids.

Note: If there is a power outage, this card can be powered down in order to conserve electricity.

10.3 HPNA Command Reference

10.3.1 Overview

This section describes the commands available on the Gateway to configure and manage the HPNA module.

0.0.1 System CLI commands

The table below lists all HPNA commands provided by the CLI:

TABLE 10-2 HPNA Commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
HPNA SHOW MASTER						X			
HPNA SHOW COUNTERS						X			
HPNA RESET COUNTERS						X			
HPNA SHOW STATIONS						X			
HPNA SHOW STATIONS ALL						X			
HPNA SHOW PERFORMANCE						X			
HPNA UPGRADE ENDPOINT						X			

10.3.1.0.1 HPNA SHOW MASTER

Syntax HPNA SHOW MASTER

Description This command displays the status of the iMG HPNA device which is in actual fact the Master node in the HPNA network. This includes whether the node is enabled and whether an endpoint is connected.

Example hpna show master

```
HPNA Port hpna
   ConfigState                  :  Enabled
   DeviceState                  :  InService
   Connected                    :  true
   HpnaMode                     :  V3
   HpnaNetworkMode              :  Managed
   MacAddress                   :  00:01:02:03:00:03
   FirmwareVersion              :  1.7.4

 HPNA Physical Layer Utilization
   HpnaPerCyclePercentTx        :    2%
   HpnaPerCyclePercentIdle      :   98%
   HpnaAccumulatedPercentTx     :    1%
   HpnaAccumulatedPercentIdle   :   99%
```

10.3.1.0.2 HPNA SHOW COUNTERS

Syntax HPNA SHOW COUNTERS [<TargetMac|All>]

Description This command displays the packet counters for the master node of the HPNA Network. Note that it is possible to get related switch counters via the appropriate switch command

Option	Description	Default Value
TargetMac | All	Mac address of the target device for which to show counters. All will display counter for all attached stations and the Master.	All

Example hpna show counters All

```
Device  MAC                Link  Sync   Mode  SW
  0     00:0c:25:13:90:1b  Down  True   V3    1.7.5
 HPNA Network to Port Interface Counters
   HpnaTxPkt                  : 54920
   HpnaTxBcastPkt             : 23944
   HpnaTxMcastPkt             : 16511
   HpnaTxByte                 : 6020335
   HpnaTxShort                : 0
   HpnaTxDropped              : 2
   HpnaRxPkt                  : 285
   HpnaRxBcastPkt             : 0
   HpnaRxMcastPkt             : 0
   HpnaRxByte                 : 20032
   HpnaRxShort                : 0
   HpnaRxDropped              : 0
   HpnaRxCrc                  : 0
 HPNA Control Packet Counters
   HpnaControlReqPkt          : 286
   HpnaControlReplyPkt        : 286
   HpnaRemControlReqPkt       : 0
   HpnaRemControlReplyPkt     : 0
 HPNA Physical Layer Utilization
   HpnaPerCyclePercentTx      : (  1%)
   HpnaPerCyclePercentIdle    : ( 99%)
   HpnaAccumulatedPercentTx   : (  1%)
   HpnaAccumulatedPercentIdle : ( 99%)
```

10.3.1.0.3 HPNA RESET COUNTERS

Syntax `HPNA RESET COUNTERS <TargtMac|All>`

Description Command zeros out the counters for the associated HPNA device or all devices if the string "All" is entered

Option	Description	Default Value
TargetMac | All	Mac address of the target device for which to reset counters. All will display counter for all attached stations and the Master.	-

Example `hpna reset counters All`

10.3.1.0.4 HPNA SHOW STATIONS

Syntax `HPNA SHOW STATIONS`

Description This command shows the MAC Addresses of all the HPNA devices on the HPNA network plus a little info about them.

Example `hpna show stations`

```
HPNA Stations Attached to Host...
HPNA                                    HPNA
Device  MAC                Link    Sync   Mode  SW
  0     00:01:02:03:00:03  Up    True   V3      1.7.4
  1     00:13:ba:00:01:56  Up    False  V2     1.7.1

Number of HPNA stations=2
Total number of devices=4
```

10.3.1.0.5 HPNA SHOW STATIONS ALL

Syntax `HPNA SHOW STATIONS ALL`

Description This command provides the same information as above, but also displays all the MAC addresses that originated from behind each HPNA endpoint.

Example hpna show stations All

```
HPNA Stations Attached to Host...

 HPNA                                      HPNA
Device  MAC                Link  Sync    Mode  SW
```

```
  0     00:0c:25:13:90:1b  Down  True   V3    1.7.5
                Host 001 Behind Device 0   00:02:b3:98:56:6b
                Host 002 Behind Device 0   00:30:b6:35:68:80
                Host 003 Behind Device 0   00:18:8b:a7:f3:e8

Number of HPNA stations=1
Total number of devices=4
```

10.3.1.0.6 HPNA SHOW PERFORMANCE

Syntax `HPNA SHOW PERFORMANCE [<sourcemac> <destmac>]`

Description This command is Service Affecting and will take on the order of a minute or more

Optional parameters sourcemac and destmac allow the user to limit the diagnostic run to a particular pair of HPNA endpoints – rather than running the diagnostics on all possible pairings. The sourcemac and destmac are the MAC Addresses of the HPNA Endpoints. Execute the HPNA SHOW STATIONS command to find the possible MAX addresses.

Option	Description	Default Value
sourcemac	Source mac address for targeted performance testing	-
destmac	Destination mac address for targeted performance testing	-

Example `hpna show performance`

```
warning: This command is service affecting

CERT Test Results...

Source MAC       -->Destination MAC

00:01:02:03:00:03-->00:13:ba:00:01:56: pkts: 1000/1000 per: 0
snr 41.08 db, rate: 128Mbps 16/8 Rx power: -6.967 dBm

00:13:ba:00:01:56-->00:01:02:03:00:03: pkts: 1000/1000 per: 0
snr 43.17 db, rate: 128Mbps 16/8 Rx power: -.4288 dBm
```

10.3.1.0.7 HPNA UPGRADE ENDPOINT

Syntax `HPNA UPGRADE ENDPOINT < targetMac|All >`

Description This command will force an upgrade of the firmware level of the HPNA Endpoint that is identified – or all if all is specified. The upgrade is to the firmware level equivalent to that loaded on the local Master node. In order to minimize the likelihood of corrupting devices, this command will only work with certified Allied Telesis certified endpoints. At this time only Readylinks endpoints can be upgraded. Other HPNA endpoint manufactures will be added as certified via iMG Mod firmware updates.

In all the above cases – targetMac is the MAC address of the HPNA Endpoint. To determine the MAC Address – execute the HPNA SHOW STATIONS command. In addition there is the option to enter the string "All" which implies all the endpoints on the HPNA network.

Options	Description	Default Value
TargetMac | All	Mac address of the target device for which to upgrade the firmware. 'All' will upgrade the firmware for all stations.	-

10.4 CES LAN Module

10.4.1 CES Deployment Model

Here is a typical CES Deployment Model:

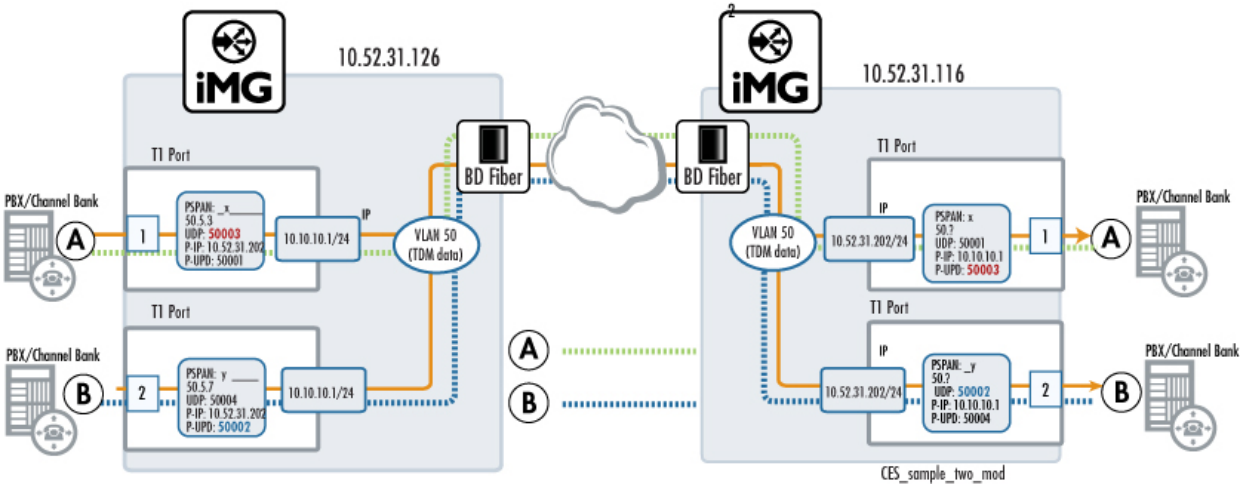


FIGURE 10-2 Typical CES Deployment Model:

Note that it is possible to connect a PSPAN between a CES daughter-card on an iMG Mod and an iMAP CES8 card.

- Key points here are that the PSPANs are all contained in the same VLAN – and have fixed IP addresses assigned. This is required in order to ensure that the pspans remain configured. Note that due to the expected use of this daughter-card – it is never powered down in order to conserve power.

Note: The CES module will create two new ports on the switch, cesc and cesd. These switch ports are the Ethernet transports for control and T1/E1 data communications to the CES module.

10.5 Circuit Emulation Command Reference

10.5.1 Overview

This section describes the commands available on the Gateway to configure and manage the CES module.

10.5.1.1 CES CLI commands

The table below lists all CES commands provided by the CLI:

TABLE 10-3 *CES* commands

Functions	Fiber A	Fiber B	Fiber C	Fiber D	Fiber E	Modular	ADSL A	ADSL B	ADSL C
CES SET DEVICE IPINT						X			
CES SET DEVICE PORTTYPE						X			
CES SET PORT DISABLED						X			
CES SET PORT LINEBUILDOUT						X			
CES SET PORT LINEENCODING						X			
CES SET PORT LOOPBACK						X			
CES SET PORT TIMINGREFERENCE						X			
CES SET PSPAN DISABLED						X			
CES SET PSPAN IPDSCP						X			
CES SET PSPAN JITTERDEPTH						X			
CES SET PSPAN LOCALUDP						X			
CES SET PSPAN PAYLOADBYTES						X			
CES SET PSPAN PEERIP						X			
CES SET PSPAN PEERUDP						X			
CES SET PSPAN RTPENABLED						X			
CES SHOW DEVICE						X			
CES LIST ALARMS						X			
CES SHOW ALARMS						X			
CES LIST PORTS						X			
CES SHOW PORT						X			
CES SHOW PORT COUNTERS						X			
CES RESET PORT COUNTERS						X			
CES LIST PSPANS						X			
CES SHOW PSPAN						X			
CES SHOW PSPAN COUNTERS						X			
CES RESET PSPAN COUNTERS						X			

10.5.1.1.1 CES SET DEVICE IPINT

Syntax `CES SET DEVICE IPINT <ip_name>`

Description This command associates an IP interface with the CES service – thus providing it with an IP address.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
IP_name	An existing ip interface with an IP address assigned. This IP is used to terminate communication for PSPANs terminated on this device.	-

Example `ces set device ipint cesip`

10.5.1.1.2 CES SET DEVICE PORTTYPE

Syntax `CES SET DEVICE PORTTYPE <port_type>`

Description This command allows the user to specify the type of TDM port that is to be used.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Port_type	The TDM port configuration – DS1 or E1.	DS1

Example `ces set device porttype DS1`

10.5.1.1.3 CES SET PORT DISABLED

Syntax `CES SET PORT <TDM_PORT> DISABLED <STATE>`

Description This command is used to enable or disable the TDM side of the circuit.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-
state	True for disabling – False for enabling	false

Example `ces set port tdm-1 disabled true`

10.5.1.1.4 CES SET PORT LINEBUILDOUT

Syntax `CES SET PORT <tdm_port> LINEBUILDOUT <buildout>`

Description This command adjusts the power output of the TDM port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-
buildout	The attenuation to place on the line neg75db neg150db neg225db neg133 neg266 neg399 neg533 neg655 NA	00db

Example `ces set port tdm-1 linebuildout 00db`

10.5.1.1.5 CES SET PORT LINEENCODING

Syntax `CES SET PORT <tdm_port> LINEENCODING <encoding>`

Description This command allows the user to specify the encoding method to be used.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-
encoding	The line encoding to use on the line ami b8zs hdb3	B8zs

Example `ces set port tdm-1 lineencoding ami`

10.5.1.1.6 CES SET PORT LOOPBACK

Syntax `CES SET PORT <tdm_port> LOOPBACK <loopback_mode>`

Description This command allows the user configure a loopback on the tdm port to facilitate fault diagnosis.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-
Loopback_mode	The direction of the loopback to be used none inward: towards the pspan line: toward the connected circuit	none

Example `ces set port tdm-1 loopback line`

10.5.1.1.7 CES SET PORT TIMINGREFERENCE

Syntax `CES SET PORT <tdm_port> TIMINGREFERENCE <timing_reference>`

Description This command allows the user specify the timeing reference to be used. It is important that the timing reference be correctly selected so that there is only one source on the link.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-
Timing_reference	The source of the timing reference to be used internal: from an internal oscillator self: from the TDM circuit connection: from the pspan	connection

Example `ces set port tdm-1 timingreference self`

10.5.1.1.8 CES SET PSPAN DISABLED

Syntax `CES SET PSPAN <PSPAN_PORT> DISABLED <STATE>`

Description This command is used to enable or disable the Ethernet side of the circuit.

The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
state	True for disabling – False for enabling	false

Example `ces set pspan pspan-1 disabled true`

10.5.1.1.9 CES SET PSPAN IPDSCP

Syntax `CES SET PSPAN <pspan_port> IPDSCP <priority_level>`

Description This command allows the user to configure a priority level for all the RTP packets that are being sent over the PSPAN.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
Priority_level	The DSCP priority level to be used.	46

Example `ces set pspan pspan-1 ipdscp 33`

10.5.1.1.10 CES SET PSPAN JITTERDEPTH

Syntax `CES SET PSPAN <pspan_port> JUTTERDEPTH <msecs>`

Description This command allows the user to configure a jitter depth for the pspan. For voice applications – 1000 is a good value.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
msecs	The depth in milli-seconds of the Jitter Buffer – ranges from 164 to 74272	6000

Example `ces set pspan pspan-1 jitterdepth 1000`

10.5.1.1.11 CES SET PSPAN LOCALUDP

Syntax `CES SET PSPAN <pspan_port> LOCALUDP <port_number>`

Description This command allows the user to source udp port number to be used in when transmitting packets over the network.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
Port_number	The udp port number to be used when creating packets for transmission	-none-

Example `ces set pspan pspan-1 localudp 50001`

10.5.1.1.12 CES SET PSPAN PAYLOADBYTES

Syntax `CES SET PSPAN <pspan_port> PAYLOADBYTES <numbytes>`

Description This command allows the user to determine how much data is sent in each packet. It is a trade-off between latency and the number of packets sent. For voice applications, 48 is preferred.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
Num_bytes	The number of bytes of source data in each packet. It can range from 16 to 1023.	1023

Example `ces set pspan pspan-1 payloadbytes 48`

10.5.1.1.13 CES SET PSPAN PEERIP

Syntax `CES SET PSPAN <pspan_port> PEERIP <ip_address>`

Description This command allows the user to specify the peer PSPAN endpoint address.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
IP_address	The ip address of the device at the other end of the pspan	-none-

Example `ces set pspan pspan-1 peerip 10.10.10.1`

10.5.1.1.14 CES SET PSPAN PEERUDP

Syntax `CES SET PSPAN <pspan_port> PEERUDP <port_number>`

Description This command allows the user to specify the peer PSPAN udp port number that all traffic should be received from.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
Port_number	The udp port number to be used when filtering for the incoming stream of data	-none-

Example `ces set pspan pspan-1 peerudp 50003`

10.5.1.1.15 CES SET PSPAN RTPENABLED

Syntax `CES SET PSPAN <pspan_port> RTPENABLED <state>`

Description This command allows the user to specify whether or not rtp packets are to be used for transmission.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-
state	True for sending RTP packets	true

Example `ces set pspan pspan-1 rtpenabled false`

10.5.1.1.16 CES SHOW DEVICE

Syntax `CES SHOW DEVICE`

Description This command allows the user to display the status of the CES daughter card.

Example
```
ces show device
CES Device level settings
--------------------------
Port Type          DS1
Local IP Interface   ces (8.8.8.1)
```

10.5.1.1.17 CES LIST ALARMS

Syntax `CES LIST ALARMS`

Description This command shows all the alarms that have been raised on the CES daughter-card and when.

Example
```
ces list alarms
1970/01/01 00:00:19.55: Raised Communication Failed on pspan-1
1970/01/01 00:00:24.84: Raised Loss of Signal on tdm-1
```

10.5.1.1.18 CES SHOW ALARMS

Syntax `CES SHOW ALARMS`

Description This command shows all the current alarms on the CES daughter-card.

Example
```
ces show alarms
 Entity   | Raised                  | Alarm Name
```

```
----------|------------------------|----------------------
 tdm-1    | 1970/01/01 00:00:24.84 | Loss of Signal
 pspan-1  | 1970/01/01 00:00:19.55 | Communication Failed
```

10.5.1.1.19 CES LIST PORTS

Syntax `CES LIST PORTS`

Description This command allows the user to display the status of the both the individual tdm ports on the card.

Example

```
ces list ports
  Name | Type | Disabled | Operational | Alarms
-------|------|----------|-------------|-----------
 tdm-1 | DS1  | false    | down        | LOS
 tdm-2 | DS1  | true     | down        | <none>
-------------------------------------------------
```

10.5.1.1.20 CES SHOW PORT

Syntax `CES SHOW PORT <tdm_port>`

Description This command allows the user to display the status of a particular TDM port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-

Example

```
ces show port tdm-1
DS1 Port Attributes
-----------------------------------
Name                tdm-1
Disabled            false
Operational State   down
Alarms              LOS
Timing Reference    connection
Line Encoding       b8zs
Line Build-out      00db
Loopback State      none
Receiving AIS       no
```

10.5.1.1.21 CES SHOW PORT COUNTERS

Syntax `CES SHOW PORT <tdm_port>  COUNTERS`

Description This command allows the user to display the counters associated with a particular TDM Port.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-

Example

```
ces show pspan pspan-2 counters
DS1 Port Statistics
----------------------------------------
Name                        tdm-1
Line Code Violations        0
Errored Seconds             0
Severely Errored Seconds    0
LOS Seconds                 124167
Unavailable Seconds         124167
```

10.5.1.1.22 CES RESET PORT COUNTERS

Syntax `CES RESET PORT <tdm_port>  COUNTERS`

Description This command resets the counters associated with a physical TDM interface.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
Tdm_port	The Physical port on the card (TDM-1 or TDM-2)	-none-

Example

```
ces reset port tdm-1 counters
```

10.5.1.1.23 CES LIST PSPANS

Syntax `CES LIST PSPANS`

Description This command allows the user to display the status of the both the individual tdm ports on the card.

Example

```
ces list pspans
   Name   | Disabled | Operational | Alarms
----------|----------|-------------|-----------
 pspan-1  | false    | down        | COMM
 pspan-2  | true     | down        | <none>
-----------------------------------------------
```

10.5.1.1.24 CES SHOW PSPAN

Syntax `CES SHOW PSPAN <pspan_port>`

Description This command allows the user to display the status of a particular PSPAN.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-

Example

```
ces show pspan pspan-1
PSPAN Attributes
------------------------------------------------------------
Name                                pspan-2
Disabled                            true
Operational state                   down
Alarms                              <none>
Encapsulation                       SAToP over IPv4
Local IP Interface                  ces (8.8.8.1)
Local UDP Port                      60001
Peer IP Address                     0.0.0.0
Peer UDP Port                       60001
Bytes per packet                    1023
RTP                                 true
Requested Jitter Buffer (+/- us) 6000
IP DiffServ code Point              46
```

```
Actual Received Indication(s)
Actual Transmitted Indication(s) Local Loss of Carrier
Actual Jitter Buffer Size (us)   0
```

10.5.1.1.25 CES SHOW PSPAN COUNTERS

Syntax `CES SHOW PSPAN <pspan_port>  COUNTERS`

Description This command allows the user to display the counters associated with a particular PSPAN.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-

Example ces show pspan pspan-2 counters
PSPAN

Example

```
ces show pspan pspan-2 counters
PSPAN Statistics
------------------------------------------------------------
Name                                pspan-2
Errored Seconds                      0
LOPS Seconds                         0
Early Packets                        0
Late Packets                         0
Lost Packets                         0
Received Packets                     0
Transmitted Packets                  0
Maximum Jitter                       0
Minimum Jitter                       0
Average Jitter                       0
```

10.5.1.1.26 CES RESET PSPAN COUNTERS

Syntax `CES RESET PSPAN <pspan_port>  COUNTERS`

Description This command resets the counters associated with a pspan.

Options The following table gives the range of values for each option, which can be specified with this command, and a default value (if applicable).

Option	Description	Default Value
pspan_port	The network based connection associated with the TDM port on the card (TDM-1 and PSPAN-1 or TDM-2 and PSPAN-2)	-none-

Example `ces reset pspan pspan-2 counters`