Ubee DDW262.G Wireless Cable Modem and Router

Subscriber User Guide for Claro Chile

www.ubeeinteractive.com
8085 S. Chester Street, Suite 200
Englewood, CO 80112
1.888.390.8233
Sales (email): amsales@ubeeinteractive.com
Support (email) amsupport@ubeeinteractive.com

September 2011

Notices and Copyrights

Contents

1 Introduction

Welcome to the Ubee family of data networking products. This document provides instructions for anyone who uses the DDW262.G Wireless Cable Modem and Router. Ubee recommends that you read this chapter before installing and using the device. The following topics are provided in this section:

1.1 Understanding Safety and Regulatory Information

The following information provides safety and regulatory standards for anyone installing, maintaining, and using the DDW262.G.

1.2 Safety

WARNING: The following information provides safety guidelines for anyone installing and maintaining the DDW262.G. Read all safety instructions in this guide before attempting to unpack, install, operate, or connect power to this product. Follow all instruction labels on the device itself. Comply with the following safety guidelines for proper operation of the device:

Always follow basic safety precautions to reduce the risk of fire, electrical shock and injury. To prevent fire or shock hazard, do not expose the unit to rain, moisture, or install this product near water. Never spill any form of liquid on or into this product. Do not use liquid cleaners or aerosol cleaners on or close to the product. Use a soft dry cloth for cleaning.

Do not insert any sharp object into the product's module openings or empty slots. Doing so may accidentally damage its parts and/or cause electric shock.

Electrostatic discharge (ESD) can permanently damage semiconductor devices. Always follow ESD-prevention guidelines for equipment handling and storage.

Use only the power adapter supplied with the device.

- ❑ Do not place heavy objects on top of the device.
- ❑ Rest the power cable freely without any obstacle or heavy items piled on top of it. Refrain from abusing, stepping or walking on the cable. Do not place the device on an unstable stand or table; the device may drop and become damaged.
- ❑ To protect the equipment from overheating, do not block the slots and openings in the module housing that provides ventilation. Do not expose this device to direct sunlight. Do not place any hot devices close to this device, as it may degrade or cause damage to it.

Federal Communications Commission (FCC) Interference Statement

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, the device may cause harmful interference to radio communications. There is no guarantee, however, that interference will not occur in a particular installation. If this device causes harmful interference to radio or television reception, which can be determined by turning it off and on, the user can try to correct the interference by one of the following measures:

- ♦ Increase the separation between the device and the equipment with which it is interfering (for example, a television or radio).
- ♦ Connect the device into an electrical outlet on a different circuit than the interfered device is connected.
- ♦ Consult the dealer or an experienced radio/TV technician for help.

FCC Regulatory Information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

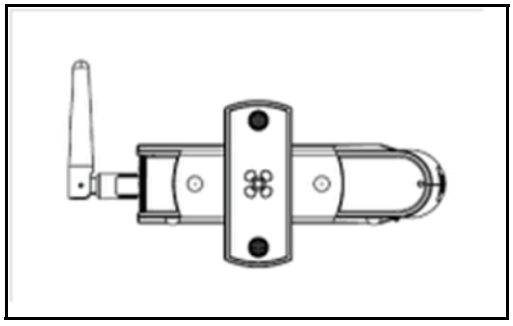
(2) This device must accept any interference received, including interference that may cause undesired operation.

(3) There are two statements for this product:

- FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this device.
- IEEE 802.11b or 802.11g or 802.11n operation of this device in the U.S.A. is firmware-limited to channels 1 through 11.

Safety Notices

1. **Grounding**: Install the device to include grounding the coaxial cable to the earth at the building entrance per ANSI/NFPA 70 and the National Electrical Code (NEC, in particular, Section 820.93, Grounding of the Outer Conductive Shield of a Coaxial Cable).
2. **Disconnecting**: If the device becomes damaged or encounters some other abnormality, disconnect the power plug from the wall outlet immediately.
3. **Installing**: Install the device in a location not to exceed the maximum temperature of 40 degrees Celsius (104 degrees Fahrenheit).
4. **Mounting**: When this device is placed upright with the aid of the stand, fix the stand at a 90-degree angle to the device. Otherwise, the device may tip over.



1.2.1 Eco-Environmental Statements

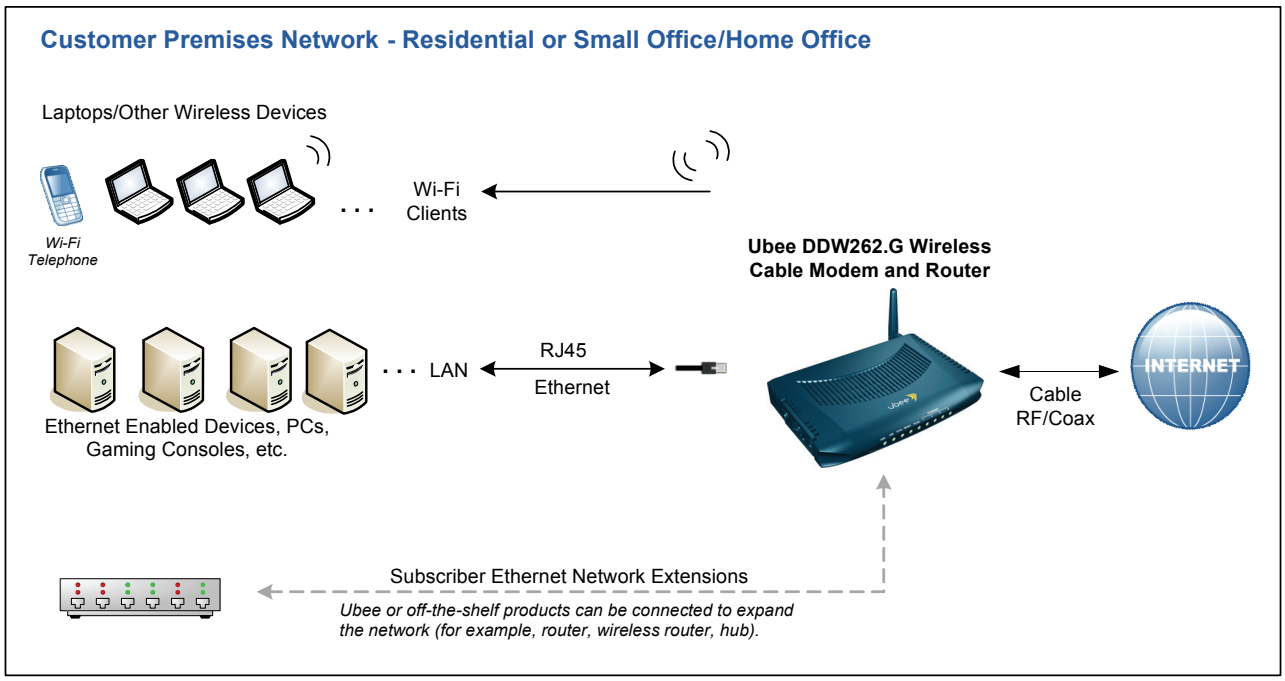
The following eco-environmental statements apply to the DDW262.G.

Packaging Collection and Recovery Requirements:

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from sewer and waste water. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste may be established. For more information regarding collection and recovery of packaging and packaging waste within specific jurisdictions, contact Ubee Interactive at www.ubeeinteractive.com.

1.3 Understanding the Customer Premises Network

The following diagram illustrates the general connection network and uses of the DDW262.G.



1.4 Contacting Support

Subscribers must contact their service provider for direct support. Device documentation support may be available at:

http://www.ubeeinteractive.com

1.5 Understanding Specifications, Standards, and Firmware

Following are the features and specifications of the DDW262.G:

Interfaces and Standards

- Cable: F-Connector, Female
- Ethernet: 4 10/100Mbps RJ45 Ports
- Antenna: 1 detachable
- DOCSIS 2.0/1.1/1.0 Compliant
- CE Certified, ENERGY STAR®-compliant power supply

Downstream

- Frequency Range: 88MHz ~ 860 MHz
- Modulation: 64/256 QAM, Channel Bandwidth: 6 MHz
- Maximum Data Rate: 30 Mbps (64QAM), 42.8 Mbps (256QAM)*
- RF Input/Output Power: -15 to +15 dBmV
- Input Impedance: 75 Ω

- Symbol Rate: 5.057/5.361/M symbols/sec

Upstream

- Frequency Range: 5 MHz ~ 42 MHz
- Modulation A-TDMA: QPSK, 8, 16, 32, 64QAM, S-CMDA: QPSK, 8, 16, 32, 64, 128QAM, TDMA: QPSK, 16QAM
- Maximum Data Rate: 0.32 ~ 10.24 Mbps (QPSK: 4QAM), 0.64 ~ 20.48 Mbps (16QAM), 0.96 ~ 30.72 Mbps (64QAM)*
- RF Output Power: TDMA/ATDMA: +8dBmV to +54dBmV (32/64 QAM), ATDMA Only: +8dBmV to +55dBmV (8/16 QAM), +8dBmV to +58dBmV (QPSK), S-CDMA: +8dBmV to +53dBmV (all modulations)
- Output Impedance: 75 Ω
- Symbol Rate: 160, 320, 640, 1280, 2560, 5120 Ksps

Security, Wireless, and Network

- VPN pass-through and VPN end-point (IPSec/L2TP/PPTP)
- NAT Firewall, MAC/IP/Port Filtering, Parental Control, Stateful Packet Inspection (SPI), DoS Attack Protection, WPS/ WPA/ WPA2/ WPA-PSK & 64/128-bit WEP Encryption
- Maximum of 4 SSIDs
- 802.11b/g/n Compliant with Wireless Link Speeds up to 65 Mbps*
- Wi-Fi Single Band (2.4GHz)
- DHCP Client/Server & Static IP Network Assignment, RIPv1/ v2, Ethernet 10/100/BaseT, Full-Duplex Auto-Negotiate Functionality, IPv4 and IPv6
- TACAS and RADIUS Authentication

*Actual speeds vary based on factors including network configuration, service tier, and network conditions.

Device Management

- WMM Power Save Technology (UAPSD) for Efficient Power Management of Wireless Devices
- Supports Local or Remote Management via Telnet, HTTP, SNMP, VSIF, and SSH

Physical and Environmental

- Dimensions: 7.75” (196.85mm) x 5.5” (139.7mm) x 1.25” (31.75mm)
- Power Consumption: Maximum 8W
- ENERGY STAR® Compliant Power Supply: 12V @ 1.0A, Input Power: 200-240VAC, 50-60 Hz
- Operating Temperature: 0°C ~ 40°C (32° F to 104° F) Humidity: 5~95% (non-condensing)

1.6 Understanding Default Values and Device Logins

This device is pre-configured with the following parameters:

Local Port Address: 192.168.0.1

Web Interface Address: http://192.168.0.1

Operation Mode: Bridge Mode

Subnet Mask: 255.255.255.0

1.6.1 Using Default Usernames and Passwords

The following usernames and passwords are available at Claro Chile.

Subscriber

Subscribers access the Web interface by opening a Web browser and going to the Web interface address **http://192.168.0.1**.

The default user name and password is:

- User name: **user**
- Password: **user**

1.6.2 Understanding Wireless Defaults

When initially connecting a wireless client to the wireless device, for example, a PC, the following wireless default values are used:

Important: The wireless radio is enabled by default.

- **System Set Identifier (SSID):** The wireless device uses the SSID to advertise itself. The SSID is equal to “CLARO_” and the last 4 characters of the Cable RF MAC address. Do not use the MTA MAC address.

  Example:

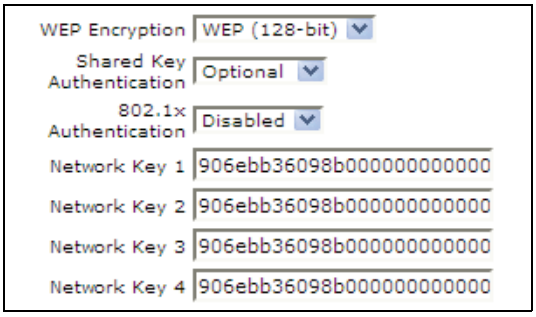
  If MAC Address is: **906EBB42FF34**

  The SSID is: **CLARO_FF34**

  Refer to Finding the MAC Address of the Device on page 7 to find the MAC address of the device.

- **Encryption Key:** The device uses 128-bit WEP encryption by default. The **WEP key** is a 26 digit HEX value. This value is equal to the device MAC address plus 14 zero’s (all lower case without the colons). Example:

  906ebb364eae00000000000000 (MAC address + 14 Zero’s)



- Broadcast Channel: The default broadcast channel is 1.

1.6.3 Finding the MAC Address of the Device

Use one of the following options to find the MAC address of the device:

- Option 1: Look on the bottom of the device for the Cable RF MAC Address.
- Option 2: Access the device Web interface and find the MAC address in the opening screen, (the Cable Modem Information screen). To access the Web interface, refer to Accessing the Web User Interface on page 15.

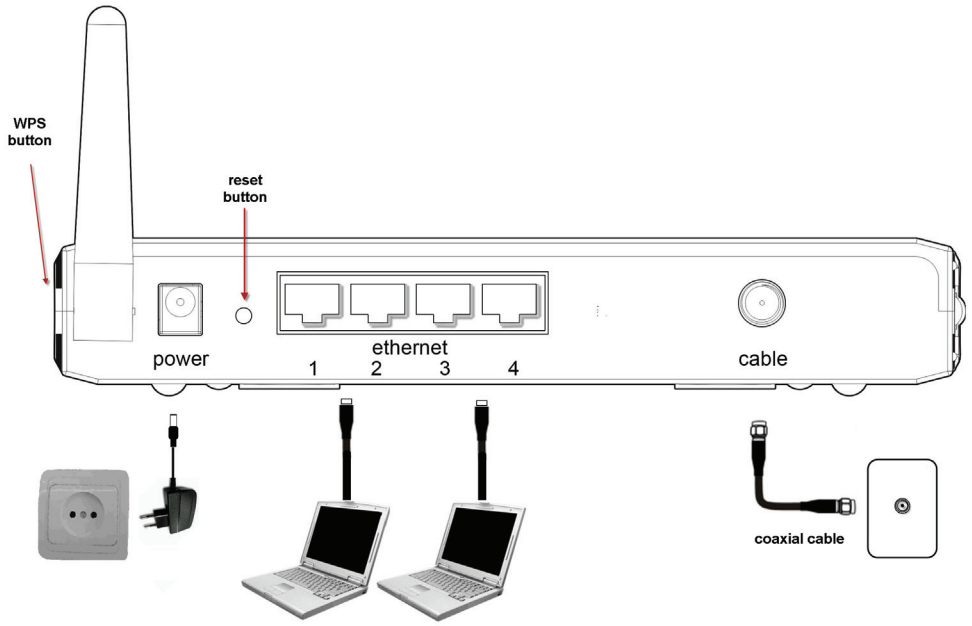
1.7 Verifying Device Package Components

The package for the DDW262.G contains the following items:

Item	Description
	1 - RJ45 Cable (Ethernet) Length ~ 6.0 ft RoHS & UL compliant *Sample image, actual appearance subject to change.*
	1 - Power Supply Input Power:200-240VAC, 50/60 Hz Output Power: 12V @1.0A *Sample image, actual appearance subject to change.*

1.8 Understanding the DDW262.G Back Panel

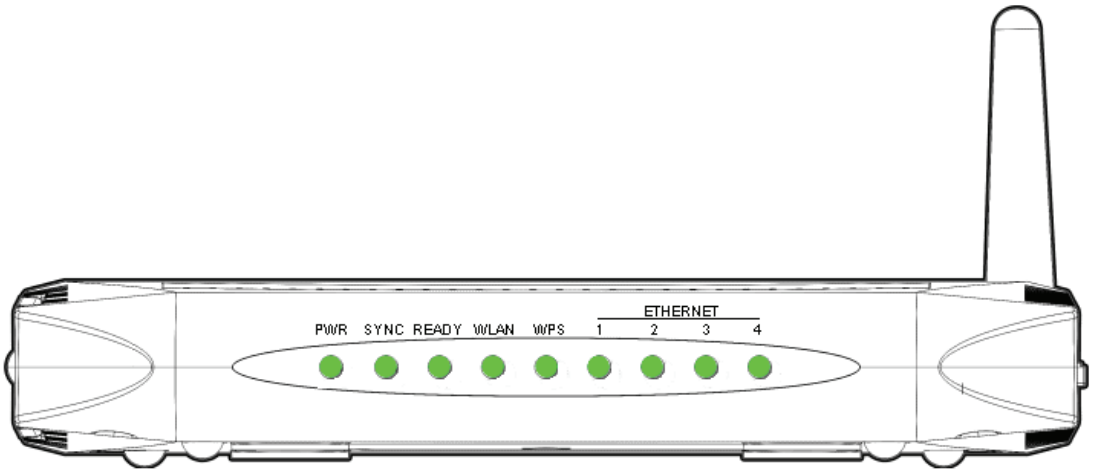
All ports to connect the device are located on the back panel. The following image and table describe the device's back panel connections.



Back Panel Label	Description
power	Connects to the power adapter. WARNING: Use only the power adapter shipped with this device. Failure to do so may cause damage to the device.
reset	Resets the device. Insert a pointed object into the opening. Press for less than10 seconds to power cycle the device. Press for more than 10 seconds to reset the device to the factory defaults.
ethernet 1 - 4	Connects an Ethernet device such as a computer, gaming console, or a router/hub to the Internet using a standard RJ45 Ethernet cable. See the Understanding the Customer Premises Network on page 3 for more information.
cable	Connects to the coaxial cable (not included) that comes from the cable wall outlet or cable splitter (not included).
WPS	Connects a PIN-protected Wi-Fi device to the cable modem when the Wi-Fi Protected Setup method is used. When the WPS button is pushed or triggered through the device's Web GUI, an LED on the top-front of the device flashes for four minutes until a PIN is entered from the wireless client, such as a laptop computer, that wants to connect. After a Wi-Fi client attaches successfully, the LED remains on for five minutes, and then turns off. Refer to Understanding the Wireless Menu on page 47 for more information.

1.9 Understanding the DDW262.G Front Panel and LED Behavior

The DDW262.G has several LEDs that provide the status of the device. The following image and the table describe LED behavior.



LED	COLOR	DESCRIPTION
POWER	Green	**On**—Device has successfully completed internal power-on tests. **Blinks**—Device has failed the power-on self test.
SYNC	Green	Indicates the connection status between the device and the cable network. **On**—Device has established a downstream channel connection with the MSO's cable modem termination equipment. **Blinks**—Device is registering with the network.
Ready	Green	Indicates the device has completed the ranging registration process and is ready to send and receive data. **On**—Device has completed ranging/registration process and is ready to send and receive data. **Blinks slowly**—Performing upstream ranging. **Blinks quickly**—Acquiring IP address and configuration file. **Off**—Device receives disable configuration file message.
WLAN	Green	**On**—At least one wireless client is connected to the device. **Blinks**—Device is receiving modem traffic. **Off**—Device is not connected to any wireless clients.
WPS	Green	**On**—WPS used. **Off**—WPS not used.
ETHERNET 1,2,3,4	Green or Orange	Indicates connectivity between the Ethernet port on the device and the Ethernet port of the PC or MAC. **On**—Ethernet ports are connected between the device and computer: ♦ Green - 100Mbps ♦ Orange - 10Mbps **Blinks**—Sending or receiving data.

Note: Sync and Ready LEDs blink during a firmware upgrade and remain solid when complete.

2 Installing and Connecting the DDW262.G

Use these instructions to install and connect the DDW262.G.

2.1 Installing the DDW262.G

You install the device by connecting it to a power supply, your computer, and Internet service.

Subscribers must contact the Internet service provider (ISP) to enable Internet access and wireless networking.

Typically, the service provider configures and connects the device, however, installation steps are provided here for your review. If you wish to confirm the setup, or add devices to your network, refer to Connecting Devices to Your Network on page 12.

Steps

To install the DDW262.G:

1. Verify service has been activated on the provisioning system before installing at the customer premises. Contact your Network Operations Center (NOC) or headend for instructions if service activation is not completed.
2. Remove the contents from the device packaging. Place the DDW262.G in an optimal location for connection to other devices, such as PCs or gaming consoles.
   - Keep the wireless cable modem and wireless clients in open areas or far away from transformers, heavy-duty motors, microwave ovens, refrigerators, fluorescent lights, and other manufacturing equipment. These items can impact wireless signals.
   - A wireless signal may become weaker after it has passed through metal, concrete, brick, walls, or floors.
   - Place the device in a location that has an operating temperature of 0˚C to 40˚C (32˚F to 104˚F). Refer to Understanding Safety and Regulatory Information on page 1 for more safety regulations.
3. Power on your PC. The PC must have an Ethernet network adapter/Ethernet port and an Internet browser installed, such as Netscape or Internet Explorer. The following browsers are supported:
   - For Windows 2000, XP, Vista, Windows 7: Firefox 1.07 and higher, Internet Explorer v7 and above, Netscape.
   - For MAC OS X, 10.2, and higher: Firefox 1.07 and higher, Safari 1.x and higher.
4. Using the power supply included in the product package, connect the power cord to the **POWER** outlet on the back of the modem and connect the other end into the power outlet.

Caution – Use only the power adaptor shipped with this device. Failure to do so may cause damage the device.

5. Using the Ethernet cable included in the product package, connect one end of the Ethernet cable to your computer's Ethernet port, and connect other end to the **ETHERNET** port on the cable modem.
6. Connect the coaxial cable from the cable wall outlet or a cable splitter connected to the cable wall outlet to the **CABLE** port on the device.

2.2 Connecting Devices to Your Network

Use one or more of the following sections to connect network devices and validate device functionality.

- ❑ Connecting Ethernet Devices on page 12
- ❑ Connecting Wireless Devices on page 12
- ❑ Troubleshooting the Installation on page 14

2.2.1 Connecting Ethernet Devices

You can connect an Ethernet device to your network, such as a computer, using an Ethernet cable.

Steps

To connect an Ethernet device to the network:

1. Verify an Ethernet device (for example, a PC) is connected to the device. See Installing and Connecting the DDW262.G on page 11.
2. Use the device LEDs to confirm operations. The PWR, SYNC, and READY LEDs are solidly lit in normal operations. One of the four ETHERNET LEDs is lit when a device is connected to the Ethernet port. Refer to Understanding the DDW262.G Front Panel and LED Behavior on page 9 for more information.
3. Open a Web browser and go to any Web site to validate network connectivity (for example, http://www.wikipedia.org).
4. If the connected device is a gaming console, perform an Internet connection test provided by your console. For more information please contact your console manufacturer.
5. Refer to Troubleshooting the Installation on page 14 for troubleshooting information, if needed.

2.2.2 Connecting Wireless Devices

Use these steps to connect a wireless device to the network (for example, a laptop computer). Use the device LEDs to confirm operations:

- ❑ The PWR, SYNC, and READY LEDs are solidly lit in normal operations.
- ❑ The WLAN LED must be solidly lit for wireless connections. Refer to Understanding the DDW262.G Front Panel and LED Behavior on page 9 for more information.

Steps

To connect a wireless device:

1. Access the wireless networking feature on your wireless device. For example on a Windows computer, double-click the Wireless Network Connection icon in the system tray (lower-right side of the Windows desktop).

   Note: If the icon is not present or you are using a different operating system, refer to the documentation for your computer to access wireless networking options.

2. Click **View Wireless Networks**. The screen displays a list of available SSIDs. The DDW262.G broadcasts the SSID as the name of the wireless network so that wireless clients can connect to it.

3. Double-click your SSID in the wireless networks window. The DDW262.G is shipped with a default SSID, which can be changed by the service provider if the subscriber requests. The default SSID is equal to “CLARO_” and the last 4 characters of the Cable RF MAC address printed on the bottom of the cable modem.

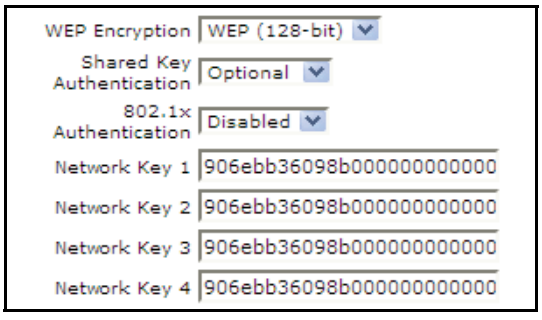
   For example: MAC Address: 906EBB42FF34
   SSID = **CLARO_FF34**

4. Enter the network key (WEP). This value is found in the Wireless Primary Network option. To find the default network key:

   a. Log in to the device using the MSO login. See Understanding Default Values and Device Logins on page 6.

   b. Click **Wireless,** and then click the **Primary Network** option.

   c. Find the WEP Encryption field. The default encryption method is WEP.



   d. Verify the encryption method. If using WPS, enter the default WPS PIN = **12345670.**

5. Confirm connectivity by opening a Web browser and going to any Web site (for example, http://www.wikipedia.org). Refer to Troubleshooting the Installation on page 14 if you are having trouble connecting to the Internet.

Note: If you cannot see or connect to the SSID, contact your service provider to enable wireless services.

2.3 Troubleshooting the Installation

Use the following tips for troubleshooting the installation.

- ❑ None of the LEDs are on when I power on the DDW262.G.
  - ♦ Verify the power outlet is energized and the power adaptor is connected to the power outlet.
  - ♦ Check the connection between the power adapter and the cable modem. Power off the cable modem by removing the power cord from the back of the unit. Wait for five seconds and power on the modem again. If the problem still exists, there may be a hardware problem.
- ❑ The Ethernet LED on the cable modem is not lit.
  - ♦ Verify both ends of the Ethernet cable are properly connected.
  - ♦ Restart the computer to re-establish a connection with the cable modem.
  - ♦ Check for a resource conflict (Windows users only).
    1. Right-click **My Computer** on your desktop and choose **Properties**.
    2. Click the **Hardware** tab, and then choose **Device Manager**.
    3. Look for a yellow exclamation point or red X over the NIC in the Network Adapters field. If you see either one, you may have an IRQ conflict.
    4. Refer to the manufacturers documentation or you cable service provider for further assistance.
  - ♦ Verify TCP/IP is the default protocol for your network interface card (NIC).
  - ♦ Power cycle the DDW262.G by removing the power adapter from the electrical outlet and plugging it back in. Wait until the cable modem re-establishes communications with the cable service provider.
- ❑ General Connectivity Issues:
  - ♦ If your PC is connected to a hub or gateway, connect the PC directly into an Ethernet port on the cable modem.
  - ♦ If you are using a cable splitter, remove the splitter and connect the cable modem directly to the cable wall outlet. Wait several minutes for the cable modem to re-establish communications with the cable service provider.
  - ♦ The Ethernet cable may be damaged. Try another cable.
- ❑ If none of these suggestions work, contact your cable service provider for further assistance.

3 Accessing the Web User Interface

The Web user interface allows you to view modem settings and monitor the DDW262.G Wireless Cable Modem and Router. Users are able to access different options based on their login: user or administrator.

3.1 Accessing the Web Interface as a User

Use the following procedure to access the Web interface as a basic user.

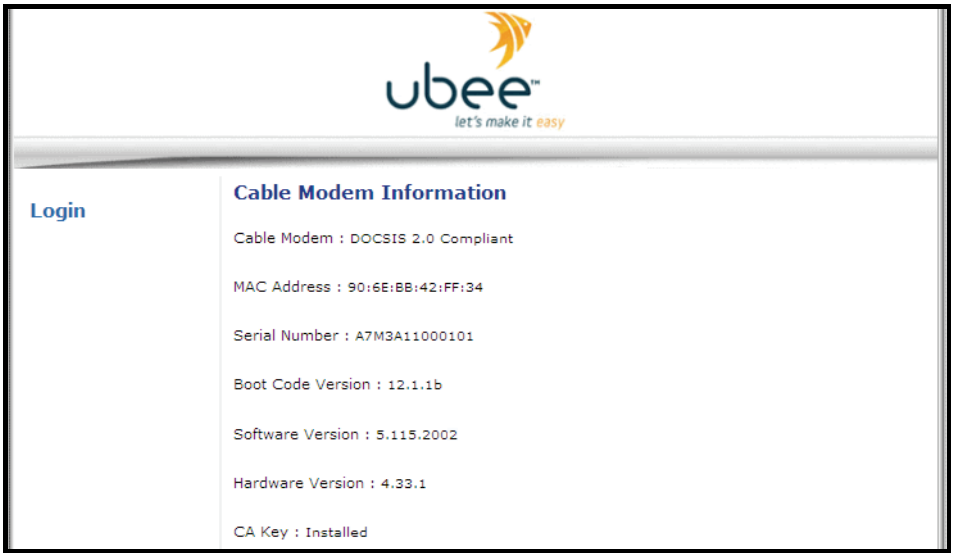
Steps

To log in to the Web interface user account:

1. Verify a PC is connected to the device as explained in Connecting Devices to Your Network on page 12.
2. From your PC, launch an Internet browser, for example, Internet Explorer.
3. In the Internet browser, enter the following address and press <**Enter**>.

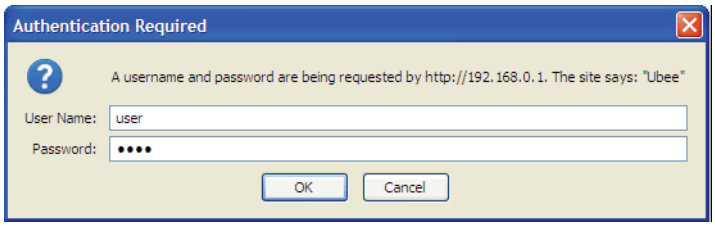
   `http://192.168.0.1`

4. On the login page, click **Login**.

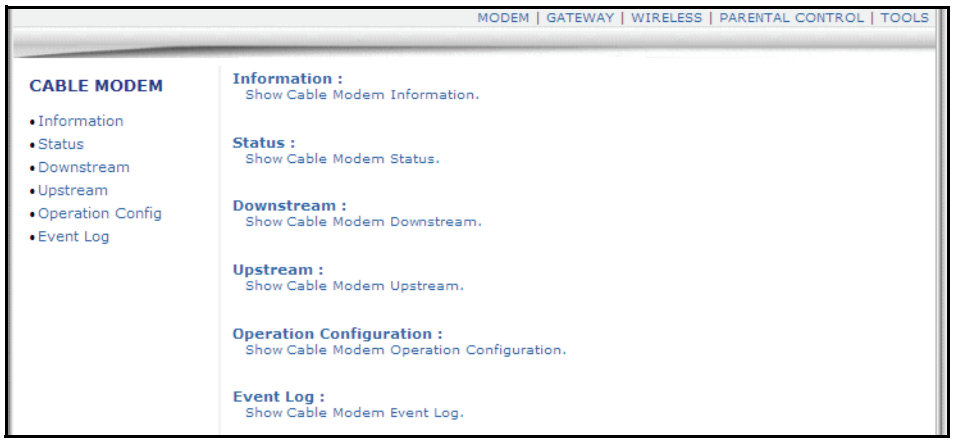


5. At the Authentication Required dialog, enter the username and password for the user

account. The default is username/password is: user/user.



The Cable Modem main menu is displayed.



3.2 Understanding Operation Modes and the Web User Interface

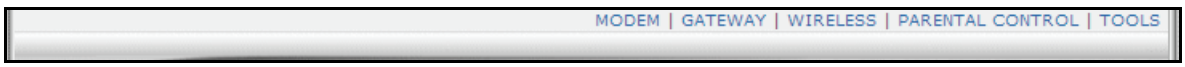
The DDW262.G Wireless Cable Modem and Router provides two operation modes:

Gateway mode—Provides a wireless access point that allows sharing a single Internet connection. Enables layer 3 protocols, including DHCP for private IP address assignment, NAT for network address and port translation, IP routing, firewall protection, and parental control features.

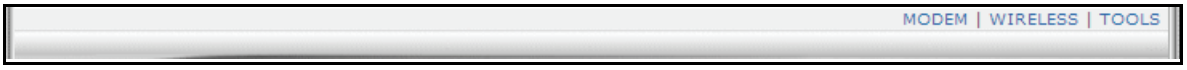
Bridge mode—Provides a wireless side for a specific access point. Enables layer 2 protocols, in which IP addresses are assigned to the subscriber from the cable company's DHCP servers. This is the default mode for Claro Chile.

Different options are available in the Web user interface depending on the mode and the type of user logged in: subscriber or administrator. The following menus show the options available in each mode.

Subscriber Web User Interface in Gateway Mode



Subscriber Web User Interface in Bridge Mode



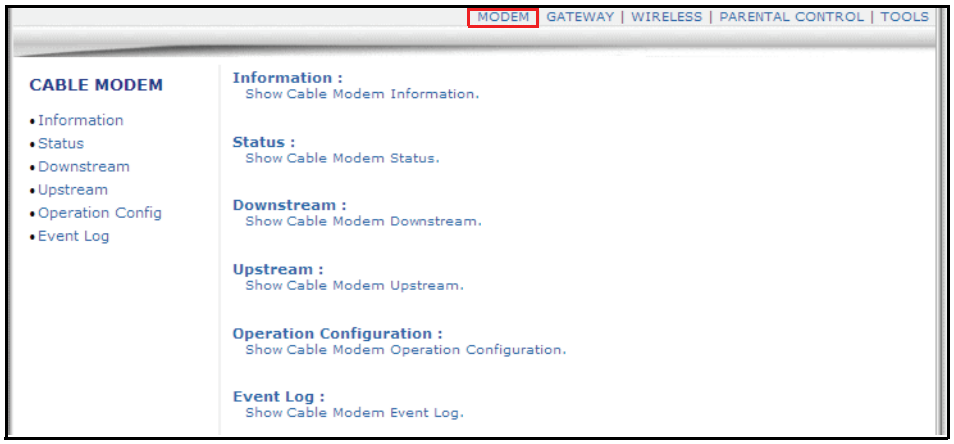
4 Understanding the Cable Modem Menu

The **Modem** menu provides access to information about the modem, such as downstream and upstream connections and event logs.

Steps

To access the Modem menu:

1. Access the Web interface. Refer to Accessing the Web User Interface on page 15.
2. Click the **Modem** link from the top menu. The Cable Modem menu is displayed.



4.1 Using the Cable Modem Information Option

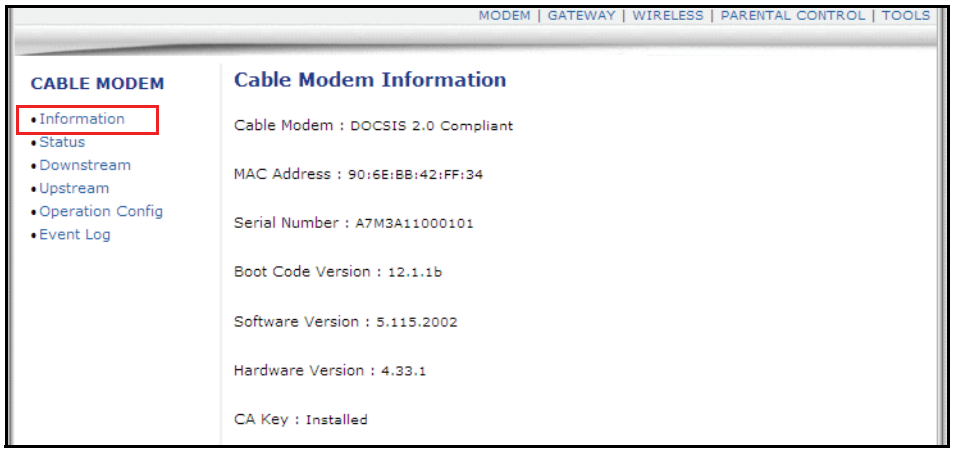
The **Cable Modem Information** screen is a read-only screen that displays the device's basic software and hardware configuration.

Steps

To view modem information:

1. Access the Web interface.
2. Click the **Modem** link from the top menu.
3. Click the **Information** link from the left side of the screen. Field explanations are listed

following the screen example.



Label	Description
Cable Modem Information	
Cable Modem	Displays the current DOCSIS standard of the device.
MAC Address	Displays the unique Media Access Control (MAC) hardware address of cable modem RF interface.
Serial Number	Displays the unique manufacturer serial number of the device.
Boot Code Version	Displays the boot software code version of the device.
Software Version	Displays the general software version of the device.
Hardware Version	Displays the internal version number that identifies the hardware design.
CA Key	Displays the device Certificate Authority (CA) key that is transferred from the service provider's server after the cable modem is authenticated. The key is used to secure communication between the service provider and the cable modem.

4.2 Using the Cable Modem Status Option

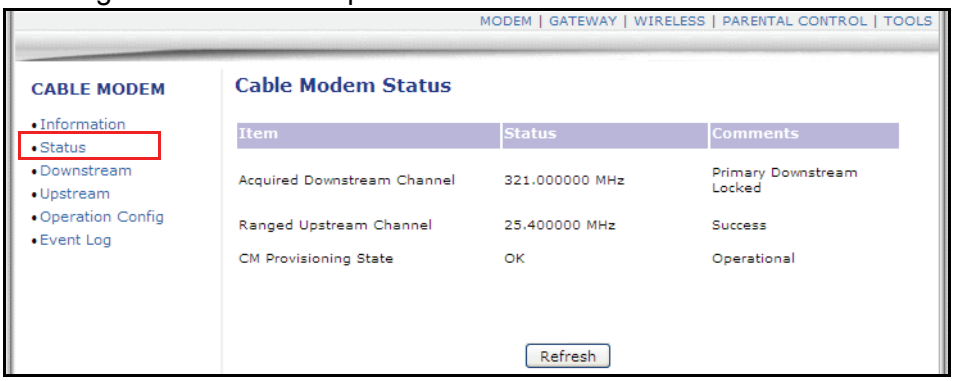
The **Status** screen of the Web interface is a read-only screen that displays the device's general connection information.

Steps

To view modem status:

1. Access the Web interface.
2. Click the **Modem** link from the top menu.
3. Click the **Status** link from the left side of the screen. Field explanations are listed

following the screen example.



Label	Description
Acquired Downstream Channel	Displays a Downstream channel that the cable modem is trying to lock to and the progress.
Ranged Upstream Channel	Displays an Upstream channel that the cable modem is trying to lock to and the progress.
CM Provisioning State	Indicates the state of the device, Operational or otherwise (for example, Disabled).

4.3 Using the Cable Modem Downstream Option

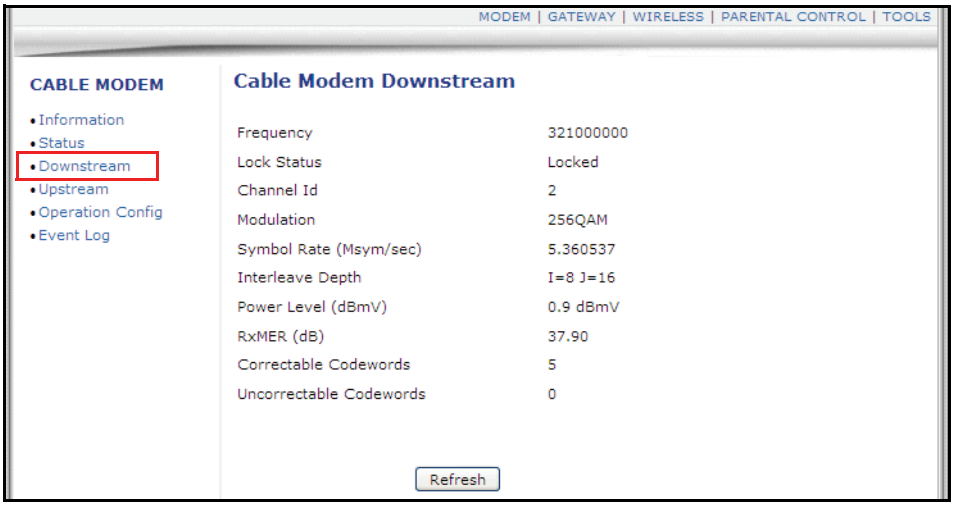
The **Downstream** screen displays detailed information on the device's connection to downstream channels from the service provider.

Steps

To view downstream information:

1. Access the Web interface.
2. Click the **Modem** link from the top menu.
3. Click the **Downstream** link from the left side of the screen. Field explanations are

listed following the screen example.



Label	Description
Frequency	Displays the downstream channel frequency on which the cable modem is scanning.
Lock Status	Displays if the cable modem succeeded in locking to a downstream channel.
Channel ID	Displays the downstream channel ID.
Modulation	Displays the modulation method that's required for the downstream channel to lock on to by the cable modem. This method is determined by the service provider.
Symbol Rate (Msym/sec)	Displays the symbol rate. The current cable modem downstream symbol rates are: QAM64 is 5056941 sym/sec, QAM256 is 5360537 sym/sec.
Interleave Depth	Displays the current cable modem downstream Interleave depth (4/8/16/32/64/128/other).
Power Level (dBmV)	Displays the receiver power level after ranging process.
RxMER (dB)	Displays the Receiver Modulation Error Ratio. The RxMER is used to quantify the performance of a digital radio receiver in a communications system using digital modulation.
Correctable Codewords	Displays the quantity of codewords which are correctable.
Uncorrectable Codewords	Displays the quantity of codewords which are not correctable.
Refresh	Recaptures and displays screen values.

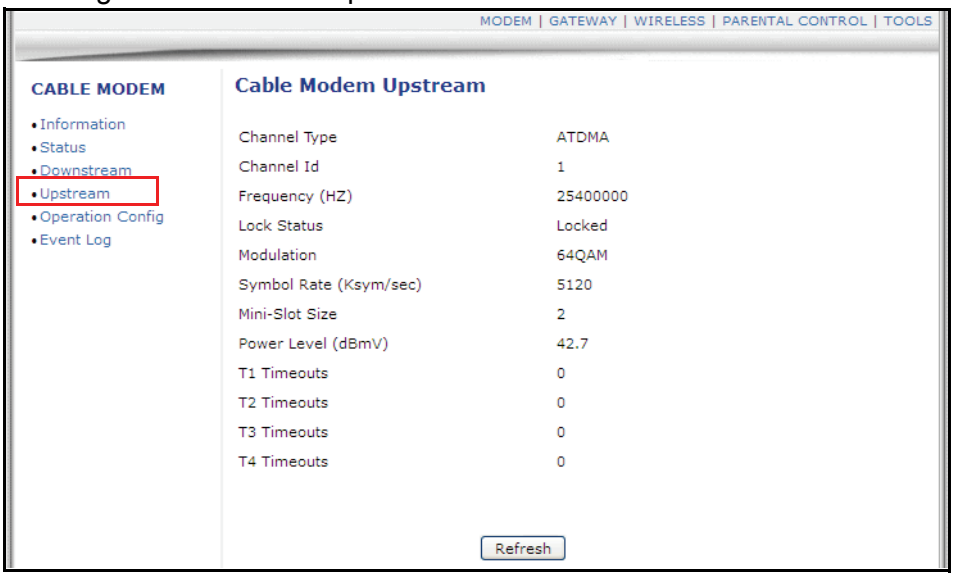
4.4 Using the Cable Modem Upstream Option

The **Upstream** screen displays detailed information on the device's connection to upstream channels to the service provider.

Steps

To view upstream information:

1. Access the Web interface.
2. Click the **Modem** link from the top menu.
3. Click the **Upstream** link from the left side of the screen. Field explanations are listed following the screen example.



Label	Description
Channel Type	Displays the channel type.
Channel ID	Displays the current cable modem upstream channel ID.
Frequency (HZ)	Displays the current cable modem upstream frequency in hertz.
Lock Status	Displays the upstream lock status.
Modulation	Displays the current cable modem upstream modulation type (QPSK/ QAM8 /QAM16/ QAM32/ QAM64/ QAM128/ QAM256).
Symbol Rate (Ksym/sec)	Displays the symbol rate in kilosymbols per second.
Upstream Mini-Slot Size	Displays the current cable modem upstream mini-slot size in Timebase Ticks of 6.25.
Power Level (dBmV)	Displays the current cable modem upstream transmit power.
T-1 through T-4 Timeouts	T-1-Displays DHCP time expiration, T-2-Displays DHCP time expiration, T-3-Displays RNG-RSP time expiration, T-4-Displays RNG time expiration.
Refresh	Recaptures and displays screen values.

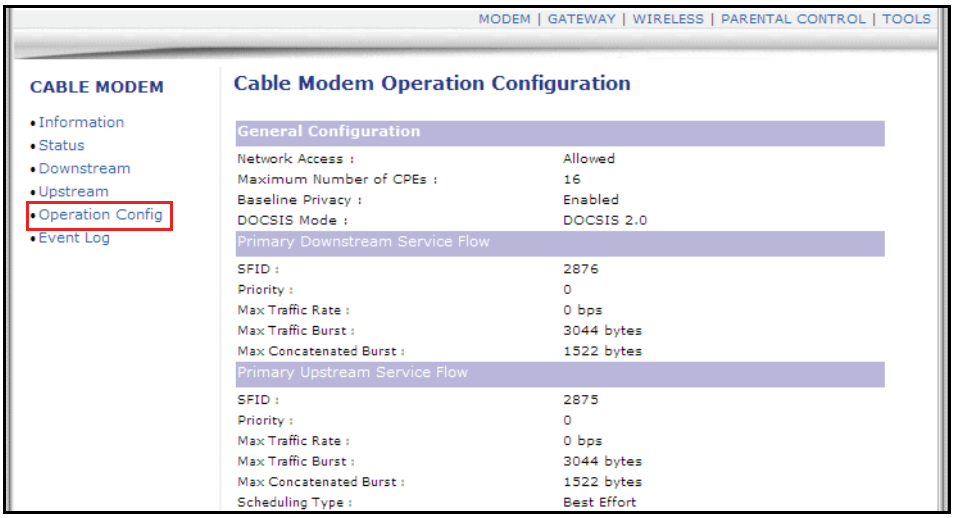
4.5 Using the Modem Operation Config Option

The **Operation Config** screen displays general information on the device's active operational capabilities.

Steps

To view operation configuration information:

1. Access the Web interface.
2. Click the **Modem** link from the top menu.
3. Click the **Operation Config** link from the left side of the screen. Field explanations are listed following the screen example.



4.6 Using the Cable Modem Event Log Option

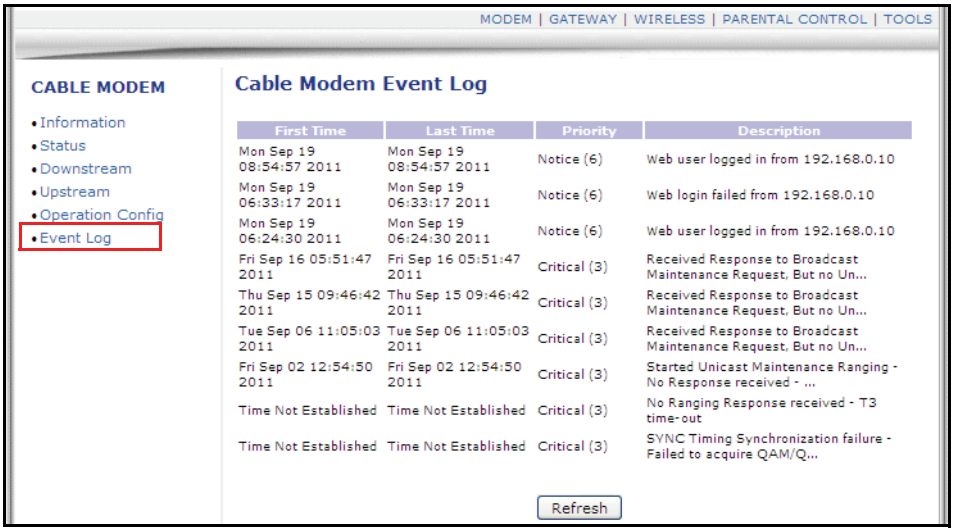
The **Event Log** screen displays log information that may be useful to diagnose operational issues with the device. It also displays all logins to this Web interface.

Steps

To view event log information:

1. Access the Web interface.
2. Click the **Modem** link from the top menu.
3. Click the **Event Log** link from the left side of the screen. Field explanations are listed

following screen example.



Label	Description
First Time	Displays the time of the event.
Last Time	Displays the last time of the event.
Priority	Displays the event log severity.
Description	Displays a detailed DESCRIPTIONof the event log.
Refresh	Refreshes the event log record.

5 Understanding the Gateway Menu

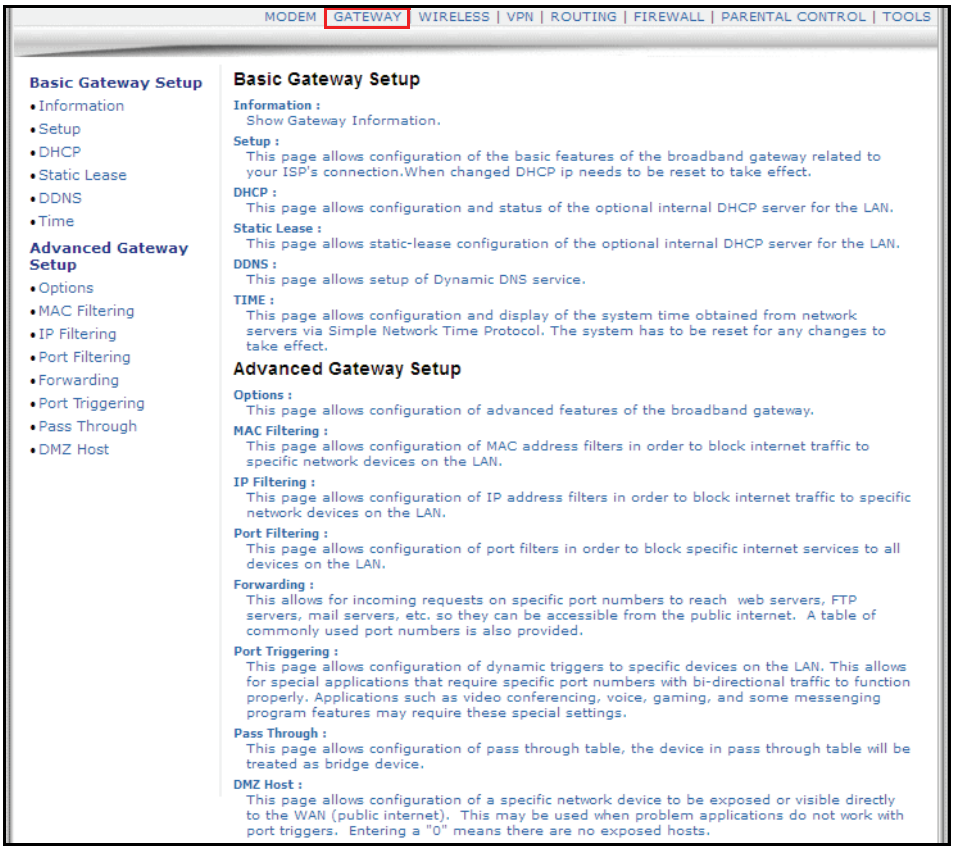
Gateway functions provide the majority of configuration for the device including WAN IP addresses, LAN IP addresses, and DHCP. Advanced settings like DMZ, MAC filtering, and port forwarding are also provided.

Note: Gateway options are not available when in Bridge mode.

Steps

To access the gateway menu:

1. Access the Web interface. Refer to Accessing the Web User Interface on page 15.
2. Click the **Gateway** link from the top of the screen.



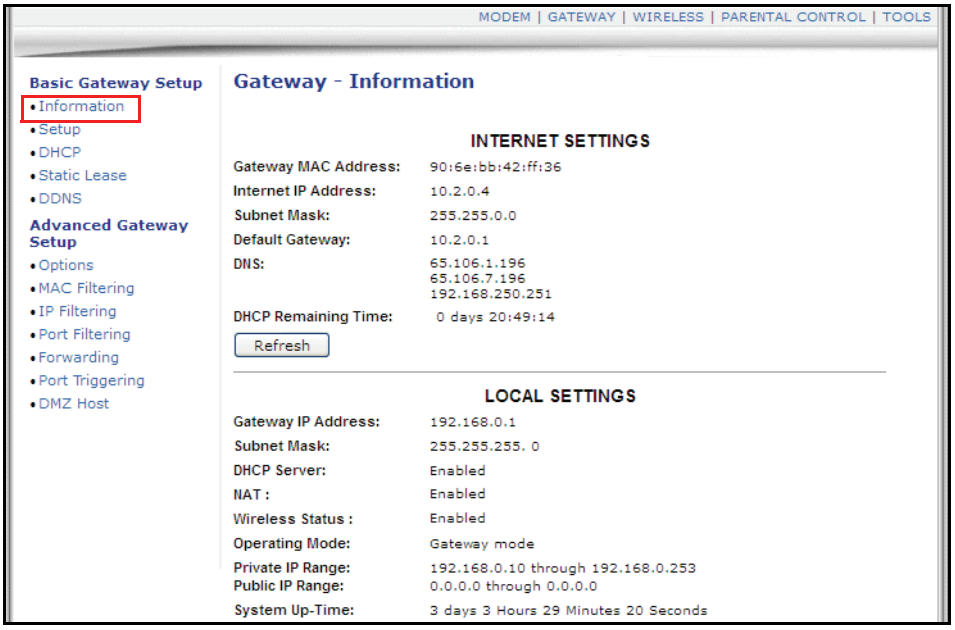
5.1 Using the Gateway Information Option

You can view Internet and local settings for your device.

Steps

To view gateway information:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click the **Information** link.The **Information** fields are defined following this screen example.



Label	Description
Internet Settings	
Gateway MAC Address	Displays the Media Access Control (MAC) address of the cable modem RF interface.
Internet IP Address	Displays the Internet IP address obtained from the service provider.
Subnet Mask	Displays the subnet mask of the Internet IP address.
Default Gateway	Displays the default gateway IP address.
DNS	Displays the DNS server IP address.
DHCP Remaining Time	Displays the remaining DHCP lease time before expiration
Refresh	Refreshes the information.
Local Settings	
Gateway IP Address	Displays the local IP address of the LAN interface.
Subnet Mask	Displays the subnet mask value.

Label	Description
DHCP Server	Displays the status of the DHCP server feature (Enabled/Disabled).
NAT	Displays the status of the NAT feature (Enabled/Disabled).
Wireless Status	Displays the status of the wireless feature (Enabled/Disabled).
Operating Mode	Displays what mode the router is working in (Bridge, Gateway, NAT, Router, or NAT Router). **Note**: Firewall menu options are not available when the device is in Bridge mode. Firewall options are available only when the device is in NAT, NATRoute, or Route modes.
Private IP Range	Displays the private IP address assigned to DHCP client.
Public IP DHCP Server Range	Displays the Public IP DHCP Server Range.
Public IP Total Range	Displays the Public IP total range.
System Up-Time	Displays the accumulated time since the last power cycle.

5.2 Using the Gateway Setup Option

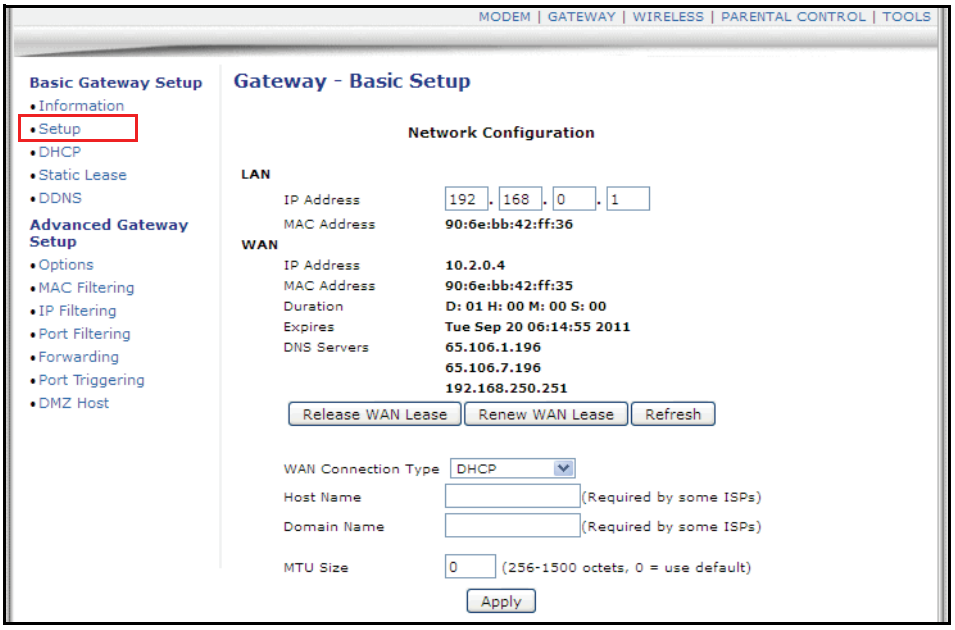
The **Setup** option allows you to configure the network settings of the device.

Steps

To configure gateway settings:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **Setup** from the left side of the screen. The **Setup** fields are explained following

this screen example.



Label	Description
LAN	
LAN IP Address	Defines the local IP address, which will be the default gateway address for all wired LAN hosts that connect to the cable modem.
MAC Address	Displays the LAN interface's hardware address.
WAN	
WAN IP Address	Displays the current WAN public IP address that is obtained from the service provider.
WAN MAC Address	Displays the WAN interface's hardware address.
Duration	Displays the accumulated time since successfully acquiring a WAN public IP address.
Expires	Displays the remaining time before the expiration of the WAN IP address, if applicable.
DNS Servers	Lists the DNS servers available on the network.
Release WAN Lease	Releases the WAN public IP address.
Renew WAN Lease	Renews the WAN IP address.
Refresh	Refreshes the status of this page.

Label	Description
WAN Connection Type	Defines the WAN connection type. For each type, different data entry is required, as explained below: ♦ DHCP: The WAN interface is set to be a DHCP client, and the IP address is assigned by the service provider's DHCP server. For more detailed configuration of the DHCP server on the device, refer to Using the Gateway DHCP Option on page 31. ♦ Static IP: For Static IP, you must manually enter the IP address for the WAN interface. ♦ PPTP (dhcp): For Point to Point Tunneling Protocol DHCP, you must enter a username, password, the PPTP server's host name or IP address, and the MTU size. ♦ PPTP (static): For Point to Point Tunneling Protocol Static, you must enter the static IP address, IP mask, default gateway, username, password, and the PPTP server's hostname or IP address, and the MTU size. ♦ L2TP (dhcp): For layer 2 tunneling protocol (dhcp), you must enter a username, password, the L2TP server's host name or IP address, and the MTU size. ♦ L2TP (static): For layer 2 tunneling protocol (static), you must enter the static IP address, IP mask, default gateway, username, password, the L2TP server's host name or IP address, and the MTU size.
Host Name	Defines the host name for the router. This may be required by some service providers.
Domain Name	Defines the domain for the router. This may be required by some service providers.
MTU Size	Defines the Maximum Transmission Unit size, which defines the largest size of the packet or frame that the device can transfer (256-1500).
Apply	Saves all changes made in the screen.

5.3 Using the Gateway DHCP Option

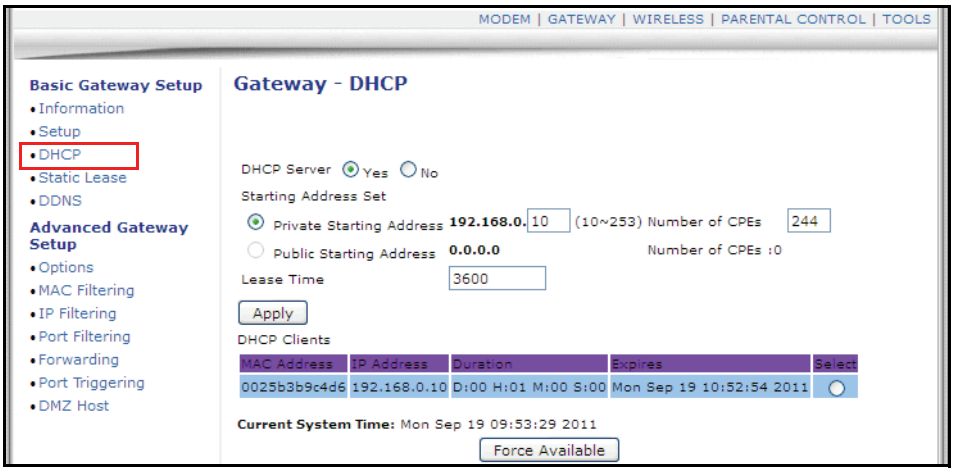
The **DHCP** option allows you to configure DHCP server-specific behavior on the device.

Steps

To configure DHCP settings:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **DHCP** from the left side of the screen. The **DHCP** fields are explained following

this screen example.



Label	Description
DHCP Server	Enables (Yes) or disables (No) the DHCP server on the device. If No is selected, all the static DHCP rules in this screen are ignored.
Private Starting Address	Defines the starting address for the pool of private IP addresses that may be used by connecting clients. Private addresses are translated to public IPs in order to be used on the network.
Number of CPEs	Defines the maximum number of Customer Premises Equipment (CPE) that can connect to the network, via the cable modem using private IP addresses. This number determines the end of the private IP address range started above.
Public Starting Address	Defines the starting public IP address. Public addresses can be recognized on the network.
Number of CPEs	Defines the maximum number of Customer Premises equipment (CPE) that can connect to the network, via the cable modem. This number determines the end of the public IP address range started above.
Lease Time	Defines the time in minutes between 1 and 71582788 for the DHCP lease time duration. A DHCP user's PC gets an IP address with a lease time. When the lease time expires, the PC must connect to the DHCP server and be reissued another, unused IP address.

Label	Description
Apply	Click Apply to save all changes.
DHCP Clients	Lists all DHCP clients currently connected to the cable modem, either via Ethernet link, or via wireless connection. Each client is also listed with the following information: ♦ MAC Address / IP Address / Subnet Mask ♦ Duration displays the accumulated time since the client acquired the IP address. ♦ Expires is the time until the IP lease time ends and must be recycled. If the IP address is reserved to a certain host, it shows “STATIC IP ADDRESS.” ♦ Select reserves the current private IP address to be assigned to this host statically when the radio button is selected.
Force Available	Activates a selected rule in the DHCP Clients List, and assigns the displayed private IP address statically to the connected network client. The Select button must be selected.

5.4 Using the Gateway DHCP Static Lease Option

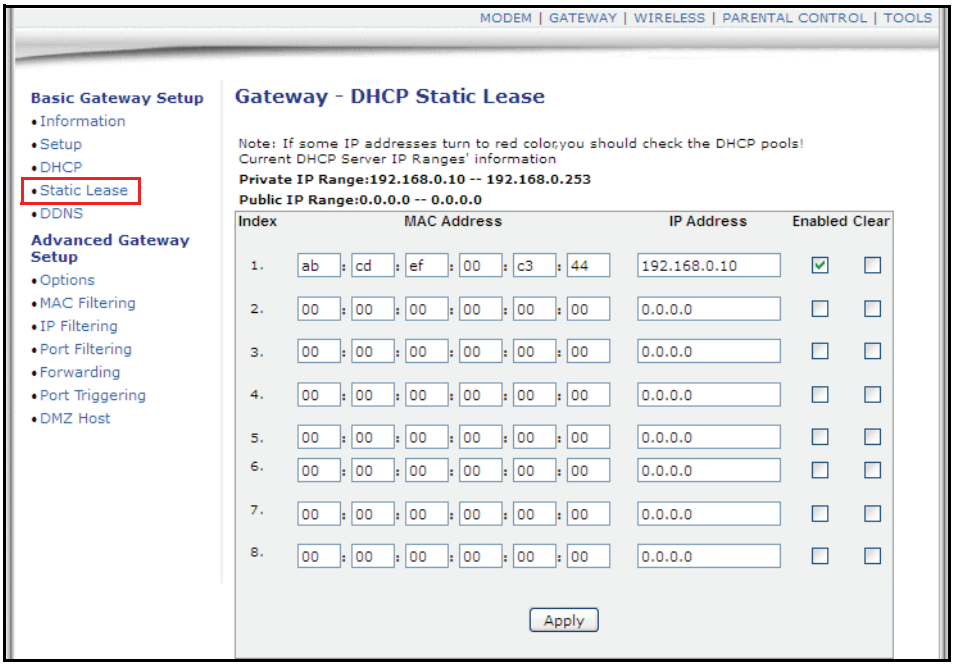
The **Static Lease** option allows you to assign static IP addresses to clients on your network using the IP addresses acquired through the DHCP server on the cable modem.The IP address must be part of the active DHCP IP pool configured on this device.

Steps

To assign static IP addresses:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **Static Lease** from the left side of the screen. The **Static Lease** fields are

explained following this screen example.



Label	DESCRIPTION
Index	Provides an index number to each client that connects to your network. Each entry reflects a direct correlation from the MAC address to the static IP address.
MAC Address	Displays the MAC address of the client to which you want to assign the static IP address. You can assign only one private IP address per MAC address.
IP Address	Defines a specific IP address to assign to the specific client/host. The IP address is reserved and not assigned to any other devices that may be connected and setup to use DHCP.
Enabled	Activates this rule.
Clear	Deletes the rule.
Apply	Saves all screen changes.

5.5 Using the DDNS Option

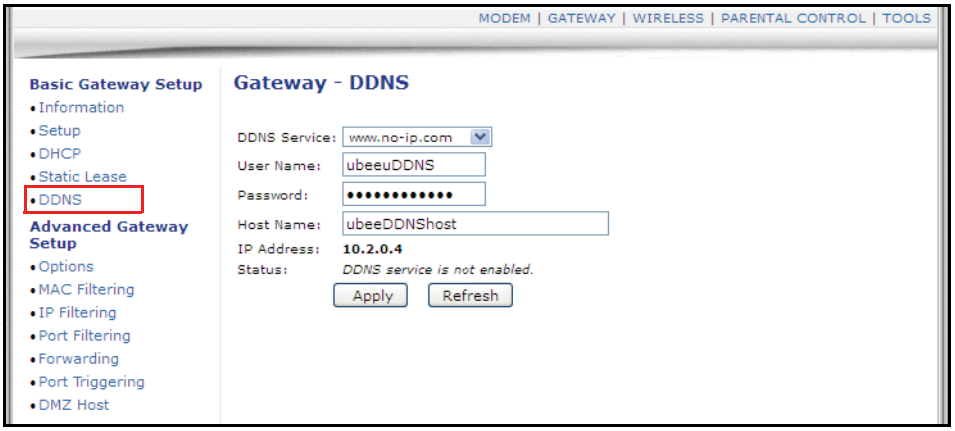
The dynamic domain name system (DDNS) allows a changing IP address to be assigned to a constant pre-defined host name. This allows the host to be contacted by other hosts on the Internet even if its IP address changes.

The DDNS service for the DDW262.G is provided through a third-party and can be purchased from Dynamic Network Services Inc. at www.dynDNS.com or No-IP at www.no-ip.com.

Steps

To use the DDNS option:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **DDNS** from the left side of the screen. The **DDNS** fields are explained following this screen example.



Label	DESCRIPTION
DDNS Service	Enables or disables the DDNS service. When enabled, this service is available from www.dynDNS.org or www.no-ip.com.
User Name	Defines the user name for the DDNS account.
Password	Defines the password for the DDNS account.
Host Name	Defines the host name for the DDNS account.
IP Address	Displays the IP address for the DDNS account.
Status	Displays if the DDNS service is enabled or disabled.
Apply	Saves all screen changes when clicked.
Refresh	Renews the screen with the latest information.

5.6 Using the Advanced Gateway Setup Options Option

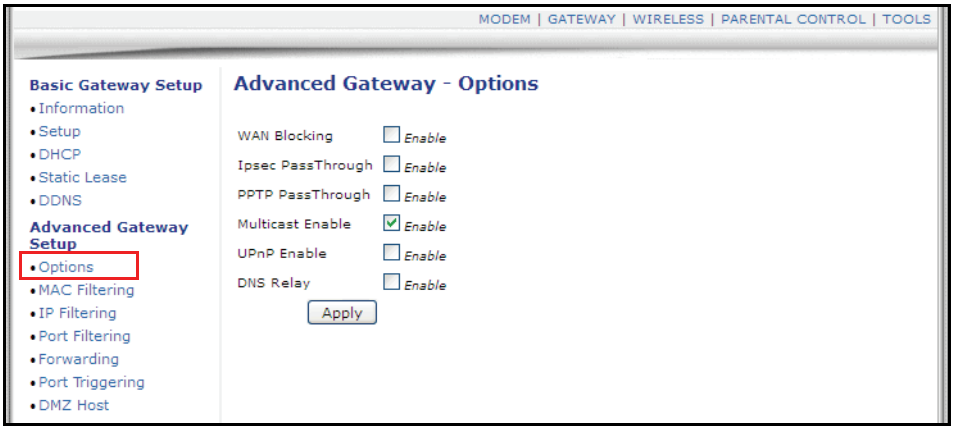
The **Options** selection allows you to define what networking protocols are enabled or disabled on the device.

Steps

To enable or disable network protocols:

1. Access the Web interface.

2. Click the **Gateway** link from the top of the screen.
3. Click **Options** from the left side of the screen. The **Options** fields are explained following this screen example.



Label	Description
WAN Blocking	Blocks connection requests initialized from Internet users when enabled.
Ipsec PassThrough	Forces the router to redirect the IPSec request to the local host when enabled. If Internet users initialize an IPSec VPN request to a host located behind the router, NAT fails this attempt.
PPTP PassThrough	Forces the router to redirect the PPTP request to the local host when enabled. If Internet users initialize a PPTP VPN request to a host located behind the router, NAT fails this attempt.
Multicast Enable	Activates multicast when enabled. Multicast optimizes the bandwidth utilization compared with unicast, especially video streaming applications.
UPnP Enable	Activates Universal Plug and Play (UPnP) when enabled. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.
DNS Relay	Activates Domain Service Relay when enabled.
Apply	Saves all screen changes.

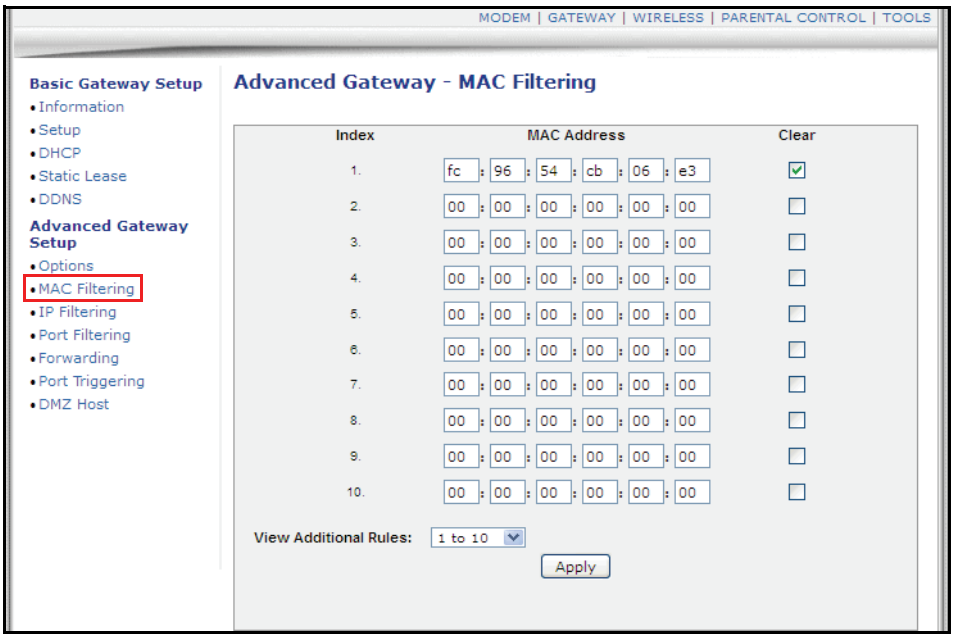
5.7 Using the Advanced Gateway Setup Mac Filtering Option

The **MAC Filtering** option filters MAC addresses to block Internet traffic from specific network devices on the LAN. Any host on this list will not be able to access the network/Internet through the cable modem.

Steps

To filter MAC addresses:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **MAC Filtering** from the left side of the screen. The **MAC Filtering** fields are explained following this screen example.



Label	Description
Index	Defines an index number for the rule.
MAC Address	Blocks the MAC address entered here.
Clear	Deletes the filtering rule.
View Additional Rules:	Displays the remaining ten rules by selecting the pull-down menu, if they exist. Twenty rules are supported.
Apply	Saves all screen changes.

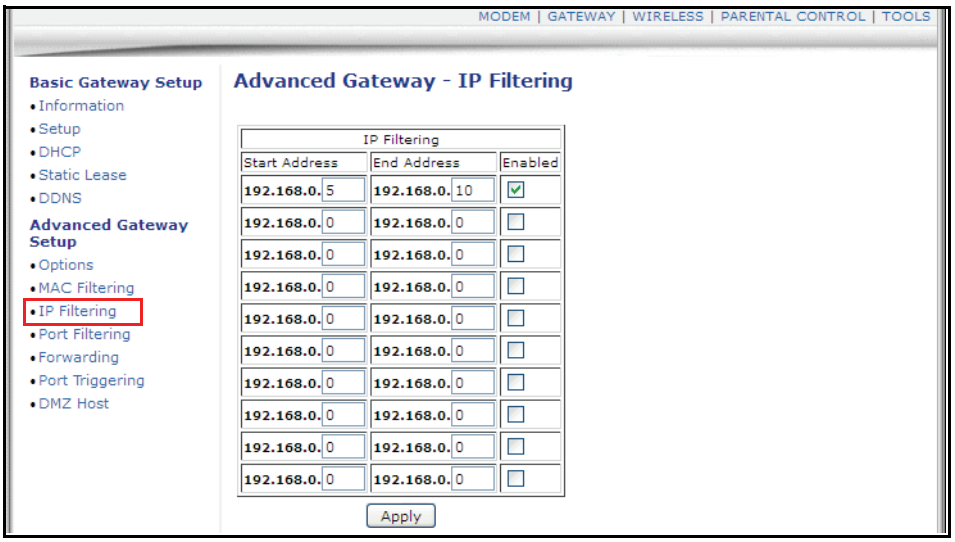
5.8 Using the Advanced Gateway Setup IP Filtering Option

The **IP Filtering** option allows you to filter IP addresses to block Internet traffic to specific network devices on the LAN. Any host on this list will not be accessible to Internet traffic.

Steps

To filter IP addresses:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **IP Filtering** from the left side of the screen. The **IP Filtering** fields are explained following this screen example.



Label	Description
Start Address	Defines the starting IP address.
End Address	Defines the ending IP address.
Enabled	Activates the rule when checked.
Apply	Saves all screen changes.

5.9 Using the Advanced Gateway Setup Port Filtering Option

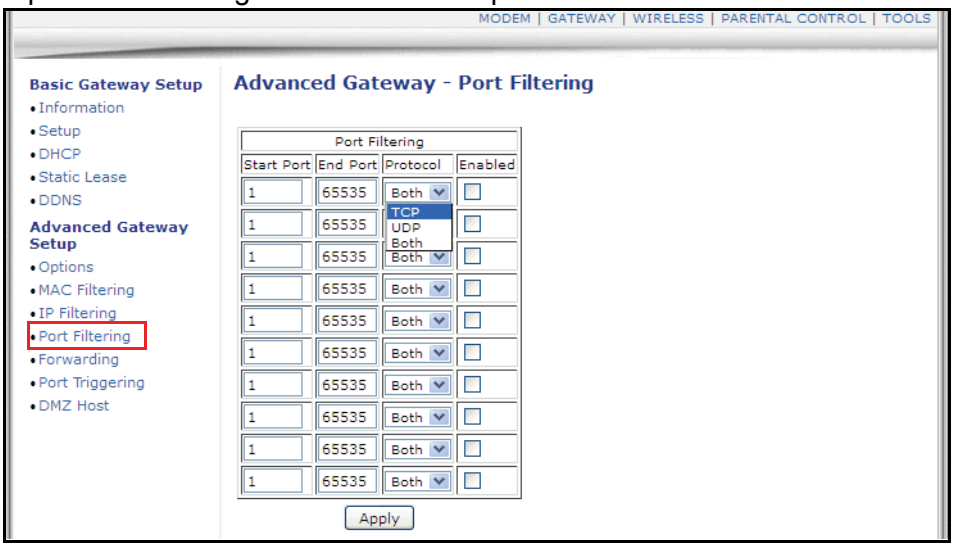
The **Port Filtering** option allows you to configure port filters to block specific Internet services on specific ports to all devices on the LAN.

Steps

To configure port filters:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **Port Filtering** from the left side of the screen. The **Port Filtering** fields are

explained following this screen example.



Label	Description
Start Port	Defines the starting port.
End Port	Defines the ending port.
Protocol	Defines the protocol type: UDP, TCP or Both for UDP and TCP.
Enabled	Activates the rule and filters out all traffic on the specified ports when enabled.
Apply	Saves all screen changes.

5.10 Using the Advanced Gateway Setup Forwarding Option

Port forwarding settings can be used to resolve issues when data is sent from a local host to the Internet, but the return path of expected data is not received by your local host.

Or, you have an application or service running on your local network (the local host) that cannot be accessed from the Internet directly (for example, a request to a local audio server). Port forwarding tells the cable modem to which computer on the local area network to send the data. Here are some examples:

- **Xbox/PlayStation**—Games/applications may require port forwarding.
- **Home Security Systems**—Security systems that use the Internet may require port forwarding.
- **Audio Servers/VoIP**—Audio and VoIP applications and services may require port forwarding to be fully enabled.

  Note: If your host systems/applications do **not** have communications issues with the Internet, forwarding is **not** needed.

You need two major items of information to setup forwarding:

- ❑ The **IP address** of each local host system (for example, Xbox) for which you need to set up a port forwarding rule. See the discussion below for how to obtain IP addresses.
- ❑ The **port numbers** that a local host's application listens to for incoming requests/data (for example, a game or other service). It is preferable to find the port number in the application's documentation, or you may refer to http://portforward.com for more information.

5.10.1 Understanding Forwarding Best Practices

The following tasks are recommended as best practices for setting up forwarding rules:

- ❑ Enable UPNP (Universal Plug and Play). This may resolve the issue you have without the need to set forwarding rules.
    1. Access the web interface of the cable modem. See Accessing the Web User Interface on page 15.
    2. Select **Gateway** from the top menu, then **Options** from the left menu.
    3. Select the option to enable UPNP.
    4. Test your local host/application (for example, Xbox) to determine correct functionality. If it is still not properly communicating, continue with forwarding.
- ❑ Using the Tools Client List Option on page 67—Use this option to obtain the MAC and IP address of the internal host for which you are setting up a forwarding rule. You also need these for the following task.
- ❑ Using the Gateway DHCP Static Lease Option on page 33—Before setting up forwarding, we recommend that you assign a Static IP lease to the client/host to which you are setting up forwarding. This way, the IP does not change and disrupt your forwarding rules. For example, if you are hosting a Web server in your internal network and you wish to setup a forwarding rule for it, you should assign a static IP lease to that system to keep the IP from renewing and disrupting the forwarding rule.

5.10.2 Setting Up Port Forwarding for an Xbox Example:

Use the following procedure to set up port forwarding for an Xbox. See the following page for screen field definitions.

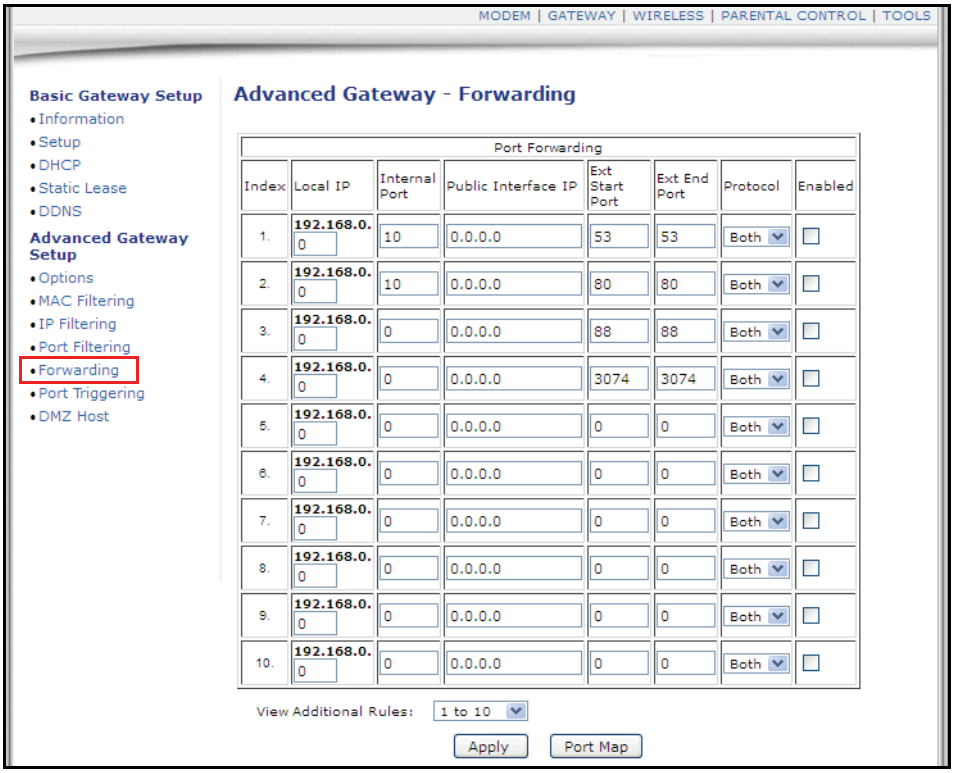
Steps

To set up port forwarding for an Xbox:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **Forwarding** from the left side of the screen.

The following example shows how to setup a single Xbox running Modern Warfare 2. Since multiple ports are used for the Xbox and the Modern Warfare 2 game, a separate forwarding rule is set up for each port. (Multiple ports and forwarding rules may not be required for other applications.) Note the following:

- The **Xbox IP address** is entered in the Local IP field. Notice how the same IP is entered in 4 rows, one row for each port used by the Xbox.
- The **ports** used by the Xbox are defined in the Internal Port field. The same ports used by the Xbox are also defined in the External Port Start and End fields.
- You may want to setup applications/services to listen on one **internal** port. External Internet users who want to access that application address it using an **external** port, such as an Audio server. Using the screen example below, **Internal Ports** are the ports that local servers listen to. **External Ports** are the ports that the cable modem listens to from the WAN.
- Port Forwarding rules are created per port. Therefore, a rule set up for port 53 only works for port 53. A port can be used only by one program at a time.
- For detailed information on port forwarding, including how to set it up for specific applications using specific network devices (for example, cable modems), refer to: http://portforward.com or consult your host device or application user manual.



Label	Description
Index	Displays the Index number of the rule.
Local IP	Defines the last digits of the IP address of the server for which to setup the forwarding rule.
Internal Port	Defines the port number listened to by the server host located in your LAN.

Public Interface IP	Designates another router on the network through which to forward data. Normally, this field is not modified.
Ext. Start Port	Defines the port number to start the range of ports to publish to the Internet.
Ext. End Port	Defines the port number to end the range of ports published to Internet. Note: Be very careful with ranges. Ports within a range are not usable by other applications that may require them. It is common and safer to enter the same port number as the start and end of the range.
Protocol	Selects the protocol type, Options are UDP, TCPIP, or Both.
Enabled	Enables this rule when checked.
Apply	Saves all screen changes when clicked.
Port Map	Shows a list of common applications and their ports.

5.11 Using the Advanced Gateway Setup Port Triggering Option

The **Port Triggering** option lets you assign dynamic triggers to specific devices on the LAN. When outgoing data is detected on an IP port set in the trigger range, the ports set in the target range are opened to accept incoming data. If no outgoing data is detected within ten minutes, the ports close. Therefore, port triggering does not keep the ports open all the time like in port forwarding. This method is safer in that specific ports are opened only for special applications, such as interactive gaming and video conferencing.

5.11.1 Understanding Port Triggering

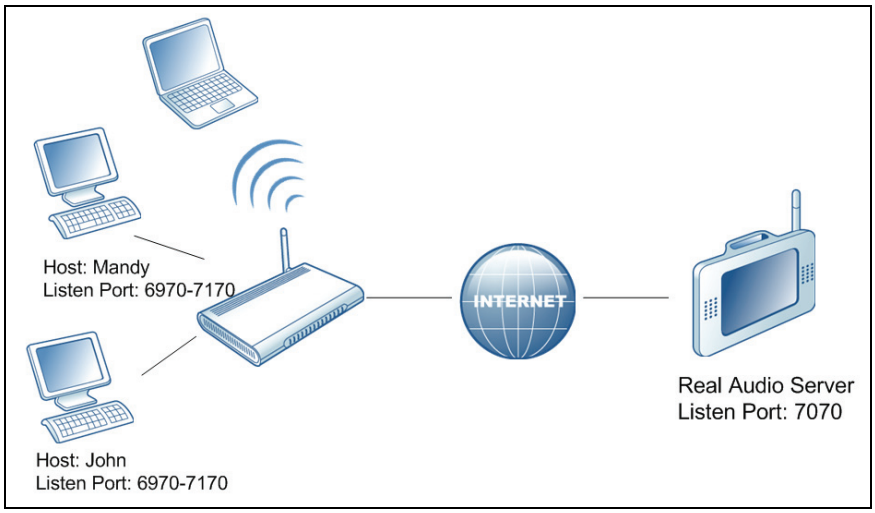
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. Port forwarding sets a forwarding rule to send a service to the IP address of a LAN side host, and sends a service to a **single** LAN IP address.

With port triggering, you can define two kinds of ports: a trigger port and a target port. A trigger port is the service request with a specific destination port number sent from a LAN side host. A target port is the port this specific application requires a LAN host to listen to. Therefore, the server returns responses to these ports.

For example:

1. John requests a file from the Real Audio server (port 7070). Port 7070 is a “trigger” port and causes the device to record John’s computer IP address. The DDW262.G associates John's computer IP address with the “target” port range of 6970-7170.
2. The Real Audio server responds to a port number ranging between 6970-7170.
3. The DDW262.G forwards the traffic to John’s computer IP address.

4. Only John can connect to the Real Audio server until the connection is closed or times out.

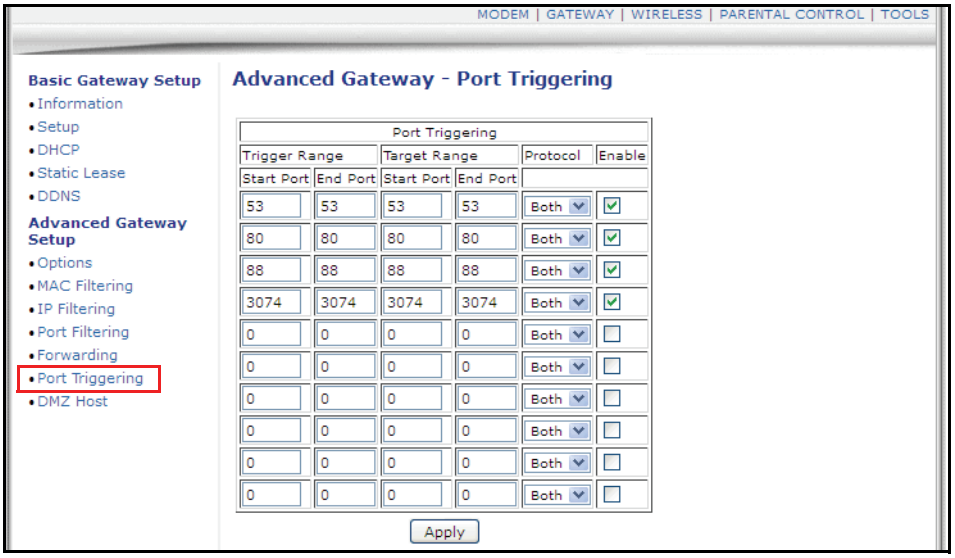


Steps

To set up port triggering:

1. Access the Web interface.
2. Click the **Gateway** link from the top of the screen.
3. Click **Port Triggering** from the left side of the screen. The **Port Triggering** fields are explained following this screen example.

   Note: The following example shows the Port Triggering option set up for a dual Xbox configuration.



Label	Description
Trigger Range	Defines the trigger port or a range of ports that triggers the router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Defines a port number or the starting port number in a range of port numbers.
End Port	Defines a port number or the ending port number in a range of port numbers.
Target Range	Defines the Target Range port or a range of ports that a server on the WAN uses when it responds to service requests. The router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service
Start Port	Defines a port number or the starting port number in a range of port numbers.
End Port	Defines a port number or the ending port number in a range of port numbers.
Protocol	Defines the protocol type for this rule, UDP, TCP, or Both.
Enable	Activates this rule when checked.
Apply	Saves all screen changes when clicked.

5.12 Using the Advanced Gateway Setup DMZ Host Option

The **DMZ** (demilitarized zone) **Host** option allows you configure a network device as a host visible to the Internet. The DMZ host receives the WAN traffic that NAT is unable to translate. This can be used when applications do not work with port triggers.

Note: Because DMZ host IP addresses are exposed to the Internet, it is strongly advised a protection mechanism is used to avoid external attacks.

5.12.1 Understanding DMZ Host Best Practices

The following instructions are best practices when adding a device into a DMZ.

1. Connect a PC to an Ethernet port on the DDW262.G Wireless Cable Modem and Router. Make sure both devices are powered on and functioning.
2. Connect a Home Gateway (or other device you wish to be in the DMZ) to an Ethernet port on the DDW262.G Wireless Cable Modem and Router.
3. Log in to the DDW262.G Web GUI.
4. Go to **Tools**>>**Client List**. Your PC and other devices are listed. Note the MAC address and IP address of the Home Gateway, VoIP Phone, or other device to put in DMZ. Refer to Using the Tools Client List Option on page 67.
5. Go to **Gateway**>>**Static Lease**. Enter the MAC address and IP address of a Home Gateway (or other device you wish to be in the DMZ).

6. Click **Apply**.

   For more information, refer to Using the Gateway DHCP Static Lease Option on page 33. A static lease ensures that the device is assigned the same IP address so it is always available on the network, especially if devices are powered on/off or disconnected and reconnected.

7. Go to **Gateway>>Advanced>>DMZ Host**. Enter the IP address you just configured in the Static Lease section.

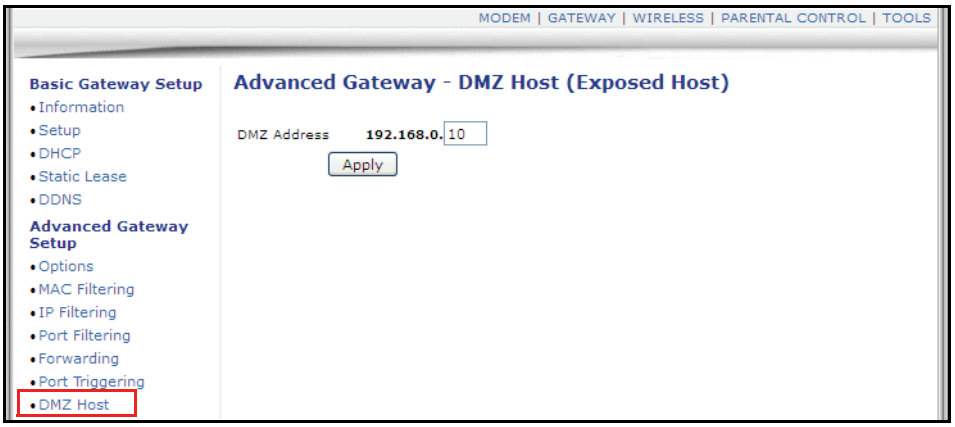
8. Test the device to ensure Internet access is available and the device is functional (for example, connect to the Internet from a PC connected to the Home Gateway, or make calls from a VoIP phone).

Steps

To setup the DMZ host option:

1. Access the Web interface
2. Click the **Gateway** link from the top of the screen.
3. Click **DMZ Host** from the left side of the screen. The **DMZ Host** fields are explained following this screen example.

   Note: The following example shows the DMZ Host set up for a dual Xbox configuration.



Label	Description
DMZ Address	Defines the DMZ host IP address. Entering 0 (zero) indicates there are no exposed hosts.
Apply	Saves all screen changes when clicked.

6 Understanding the Wireless Menu

This chapter contains instructions for all wireless configuration settings. **Note**: The Wireless radio is enabled by default.

Important: To troubleshoot wireless issues, refer to Deploying and Troubleshooting the Wireless Network on page 55.

Steps

To access the wireless menu:

1. Access the Web interface. Refer to Accessing the Web User Interface on page 15.
2. Click the **Wireless** link from the top of the screen.

6.1 Using the Wireless Radio Option

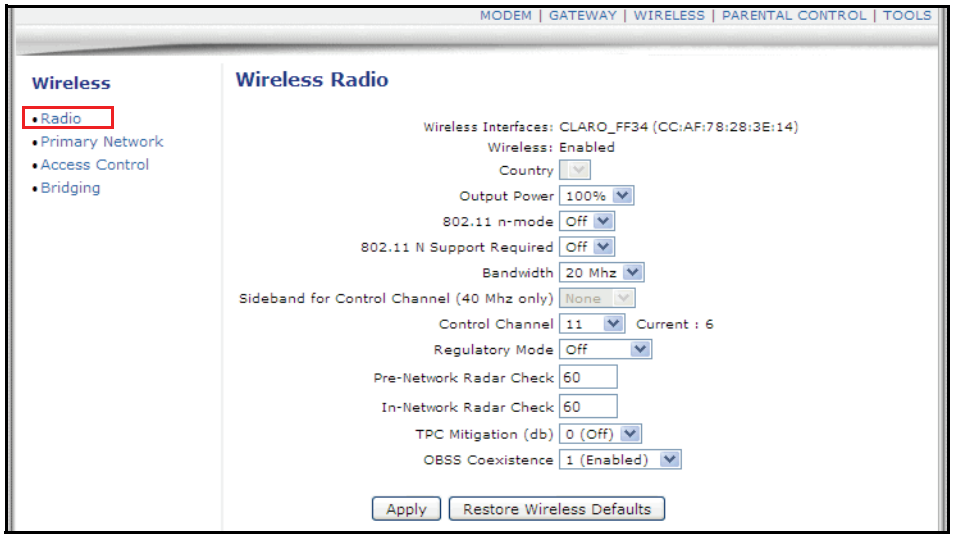
The **Radio** option allows you to configure key wireless operations including channel selection, bandwidth control, and the primary broadcast SSID.

Steps

To configure wireless operations:

1. Access the Web interface.
2. Click the **Wireless** link from the top of the screen.
3. Click **Radio** from the left side of the screen. The **Radio** fields are explained following

this screen example.



Label	Description
Wireless Interfaces	Displays the Wireless SSID and MAC address of the wireless interface.
Wireless	Displays the wireless radio's status, Enabled or Disabled.
Country	Defines the country where you use this device. When set to USA, channels 1 to 11 are available. If selecting worldwide, 13 channels are available.
Output Power	Sets a percentage of output power to use for the wireless radio transmitter.
802.11 n-Mode	Sets the wireless networking standard. Select Auto to use 802.11 n mode when possible.
Bandwidth	Sets the bandwidth to 20Mhz.
Sideband for Control Channel (40 Mhz only)	Not available for this device.
Control Channel	Selects a specific channel 1-11 to deploy the wireless network. This allows you to set the operating frequency/channel depending on your particular region. Channel selection can have an impact on wireless networking performance. For more information, refer to Selecting a Wireless Channel on page 57.
Regulatory Mode	Defines whether Regulatory Mode is set to off, 802.11d, or 802.11h.
Pre-Network Radar Check	Defines the number of seconds to check for radar on a channel before establishing a network. Current specs specify 60 seconds. Range 0-99. Zero disables checking. Designed so APs avoid channels that contain radar systems. Used for 802.11h only.

In-Network Radar Check	Defines the number of seconds to check for radar when switching to a new channel after a network has been established. Current specs specify 60 seconds. Range: 10-99. Cannot be disabled. Designed so APs avoid channels that contain radar systems. Used for 802.11h only.
TPC Mitigation (dB)	Sets TPC Mitigation to 0 (off), 2,3, or 4.
OBSS Coexistence	Enables or disables overlapping BSS coexistence.
Apply	Saves all screen changes when clicked.
Restore Wireless Defaults	Restores the factory default settings for wireless configurations. In some cases, the wireless interface/radio is turned off by default (determined by service provider).

6.2 Using the Wireless Primary Network Option

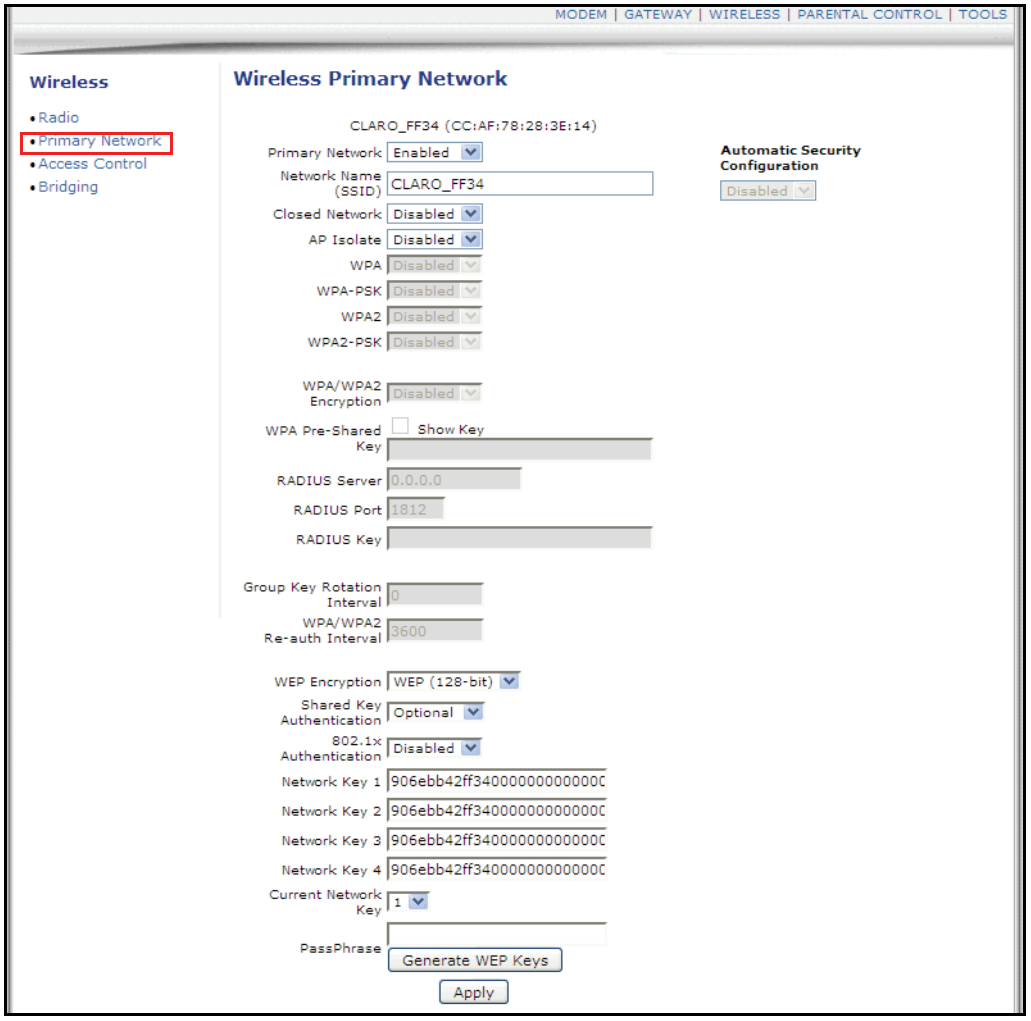
The **Primary Network** option allows you to configure a variety of wireless security settings for the **primary** wireless network. The device also supports **guest networks** that can have different SSIDs and security settings. Refer to on page 55 for more information on guest networks.

Important: To troubleshoot wireless issues, refer to Deploying and Troubleshooting the Wireless Network on page 55.

Steps

To configure wireless security options:

1. Access the Web interface.
2. Click the **Wireless** link from the top of the screen.
3. Click **Primary Network** from the left side of the screen. The **Primary Network** fields are explained following this screen example.



Label	Description
Primary Network	Enables or disables the primary network.
Network Name	Allows you to define the unique SSID of the cable modem or accept the default. Refer to Understanding Default Values and Device Logins on page 6 for more information on the SSID.
Closed Network	Hides the selected SSID when enabled so that it is undiscoverable by wireless clients unless manually setup on the client. If disabled, the SSID is discoverable.
WPA	Enables or disables the Wi-Fi Protected Access (WPA) security protocol. WPA is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA-PSK	Enables or disables WPA Pre-Shared Key (WPA-PSK). If you do not have an external RADIUS server, use WPA-PSK that requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN.

Label	Description
WPA2	Enables or disables WPA2. This advanced protocol is certified through Wi-Fi Alliance's WPA2 program and implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm (CCMP) that is considered fully secure.
WPA2-PSK	Enables or disables WPA2-PSK, If you do not have an external RADIUS server, use WPA2-PSK that requires a single (identical) password entered into wireless gateway and wireless client. As long as the passwords match, a client is granted access to the wireless LAN.
WPA/WPA2 Encryption	Sets WPA/WPA2 encryption to AES or TKIP+AES.
WPA Pre-Shared Key	Displays (checked) or hides (unchecked) the WPA key. The encryption mechanisms for WPA and WPA-PSK are the same, except that WPA-PSK uses a simple common password instead of user-specific credentials. Refer to Understanding Default Values and Device Logins on page 6 for the default value of the shared key. For MIB information about the pre-shared key, see dot11WpaPreSharedKey on page 127.
RADIUS Server	Defines the IP address of RADIUS server, if used.
RADIUS Port	Defines the port number of the RADIUS server when WPA or 802.1x network authentication is selected.
RADIUS Key	Defines the RADIUS Key when WPA or 802.1x network authentication is selected.
Group Key Rotation Interval	Allows the device to generate the best possible random group key and update all the key-management capable stations periodically.
WPA/WPA2 Re-auth Interval	For a wireless router (if using WPA-PSK key management) or RADIUS server (if using WPA key management) sends a new group key out to all clients at the specified interval. The re-keying process is the WPA equivalent of automatically changing the WEP key for a wireless access point and all stations in the WLAN on a periodic basis. Setting the WPA Group Key Update Timer (defined in seconds) is also supported in WPA-PSK mode.
WEP Encryption	Enables or disables WEP encryption. If you do not have WPA(2)-aware wireless clients, use WEP key encrypting. A higher bit key offers better security. WEP encryption scrambles the data transmitted between the wireless stations and the DDW262.G to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the DDW262.G must use the same WEP key. Data Encryption can be set to WEP **128-bit, 64-bit,** or **Disable.**
Shared Key Authentication	Defines Shared Key Authentication as optional or required. Shared Key is an authentication method used by wireless LANs, which follow the IEEE 802.11 standard. Wireless devices authenticate each other by using a secret key that is kept by both devices.

Label	Description
802.1x Authentication	Enables or disables 802.1x to authenticate wireless clients.
Network Key 1-4	Lets you pre-define up to 4 keys for 64-bit or 128-bit (64-bit keys require 10 hexadecimal digits) (128-bit key require 26 hexadecimal digits).
Current Network Key	Selects one of the four pre-defined keys as the current network key.
Passphrase	Sets the WEP encryption key by entering a word or group of printable characters in the Passphrase box and clicking Generate WEP keys. These characters are case sensitive.
Generate WEP Keys	Forces the device to generate 4 WEP keys automatically.
Apply	Saves the wireless configurations when clicked.
Automatic Security Configuration	Sets up WPS (Wi-Fi Protected Setup) for devices connecting to the wireless network.
Device Name	Defines a name for this wireless cable modem for WPS.
PIN	Defines the Personal Identification Number for this wireless cable modem.
Configure	Applies the WPS-Device Name/PIN Setup.
WPS Add Client/Push Button/PIN	Selects which method to have connecting wireless clients connect to the wireless network: Push Button or PIN. If PIN is selected, enter the PIN clients need to enter to access the DDW262.G. For push button, a client pushes a button, either on the device or in software on the device, and then on the wireless cable modem to establish secure communications.
Apply	Saves WPS configurations when clicked.

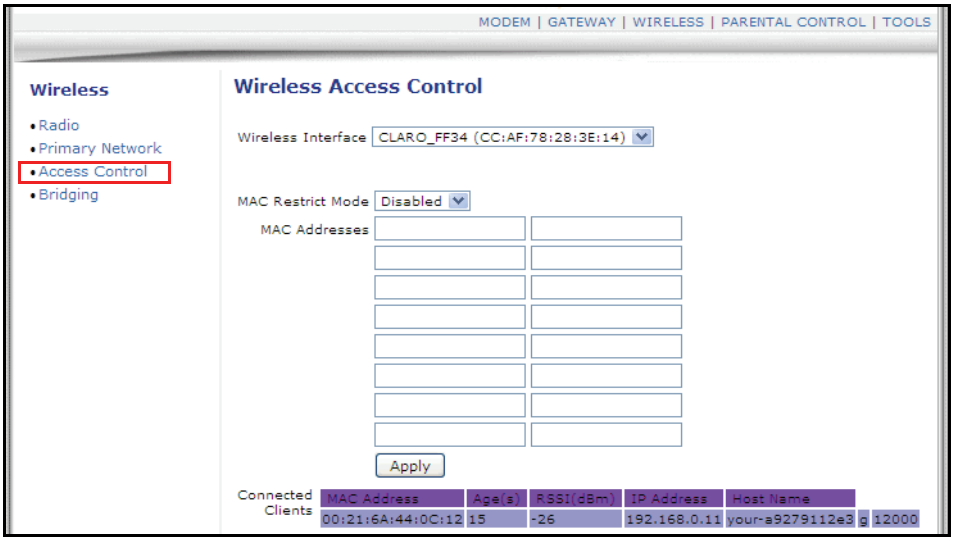
6.3 Using the Wireless Access Control Option

The **Access Control** option allows you to configure which clients can access your wireless network.

Steps

To configure client access:

1. Access the Web interface.
2. Click the **Wireless** link from the top of the screen.
3. Click **Access Control** from the left side of the screen. The **Access Control** fields are explained following this screen example.



Label	Description
Wireless Interface	Defines the wireless interface to set access control parameters.
MAC Restrict Mode	Controls wireless access to your network by MAC address. ♦ **Disable** turns off MAC Restrictions and allows any wireless client to connect to this device. However, if you use other security mechanisms for access to the wireless network, as explained in the previous section, clients must still adhere to those restrictions. ♦ **Allow** creates a list of wireless clients that can connect to the wireless network. Enter the MAC Addresses of these clients in the MAC Addresses fields. MAC addresses not on the list, are not allowed access to your wireless network. ♦ **Deny** creates a list of wireless clients that you do not want to have access to your wireless network. Enter the MAC Addresses of these clients in the MAC Addresses fields.
MAC Addresses	Defines the MAC addresses. Note: You may cut and paste MAC addresses from the connected clients list at the bottom of the screen.
Apply	Saves changes when clicked.

Connected Clients	Lists wireless clients currently connected listed by MAC address. ♦ **MAC Address**—Displays the MAC addresses entered in the MAC Addresses field (see above). ♦ **Age(s)**—Displays the duration since the wireless client's polled values were sent to the device. The values include all information shown on this screen. The lower the number, the more current its data. ♦ **RSSI(dBm)**—Displays the received signal strength from the device to the wireless cable modem. This value is commonly used to assist in troubleshooting wireless performance issues. A signal strength of -30dBm to -67dBm is considered optimal. Levels of -67dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput. Refer to Deploying and Troubleshooting the Wireless Network on page 55 for more information. ♦ **IP Address**—Displays the IP address assigned to this wireless client. ♦ **Host Name**—Displays the host name of the wireless client.

6.4 Using the Wireless Bridging Option

The **Bridging** option allows you to configure the DDW262.G to act as a wireless network bridge and establish wireless links with other wireless access points. To establish a bridge, you need to know the MAC address of the peer device, which also must be in wireless bridging mode. The DDW262.G can establish up to four wireless links with other wireless access points. When wireless devices are in wireless bridging mode, they form a wireless distribution system (WDS) allowing the computers in one LAN to connect to the computers in the other LAN.

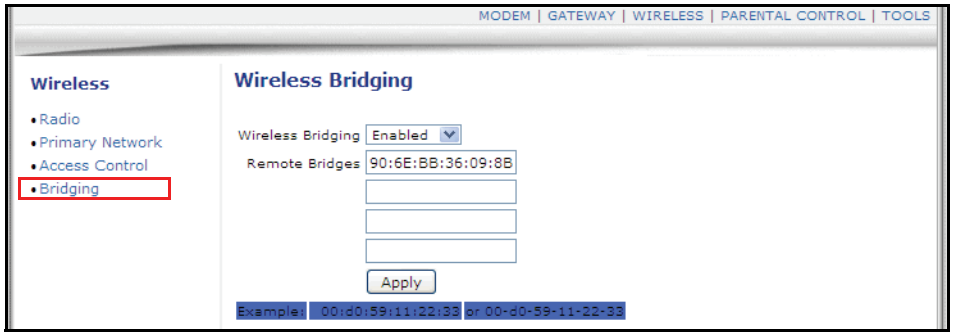
Note: Be careful to avoid bridge loops when you enable bridging devices. Bridge loops cause broadcast traffic to circle the network endlessly. This can degrade throughput and disrupt communications.

Note: Firewall menu options are not available when the device is in Bridge mode.

Steps

To configure the device as a bridge:

1. Access the Web interface.
2. Click the **Wireless** link from the top of the screen.
3. Click **Bridging** from the left side of the screen. The **Bridging** fields are explained following this screen example.



Label	Description
Wireless Bridging	Enables or disables bridging.
Remote Bridges	Defines the MAC addresses of other wireless access points that you want to establish a bridge to and from. These access points must also have bridging enabled.
Apply	Saves all changes.

6.5 Deploying and Troubleshooting the Wireless Network

This section provides the following information to help you understand, deploy, and troubleshoot your wireless environments:

- ❑ Understanding Received Signal Strength on page 55
- ❑ Estimating Wireless Cable Modem to Wireless Client Distances on page 56
- ❑ Selecting a Wireless Channel on page 57

Understanding Received Signal Strength

Received signal strength (RSSI) is measured from connected wireless client devices to the wireless cable modem. This value can significantly impact wireless speeds/performance. It is determined by:

- ❑ Materials (for example, open air, concrete, trees)
- ❑ Distance between wireless clients and the wireless cable modem
- ❑ Wireless capabilities of the client devices

To determine the received signal strength, refer to Using the Wireless Access Control Option on page 52 and review the **RSSI** value. A signal strength of -30dBm to -67dBm is considered optimal. Levels of -67dBm and lower (for example, -70, -80, etc.) have a downward impact on wireless data throughput.

Estimating Wireless Cable Modem to Wireless Client Distances

This section provides guidelines on how far a wireless cable modem can be placed from wireless client devices. Environmental variances include the capabilities of wireless clients and the types of material through which the wireless signal must pass. When the wireless cable modem and wireless clients reach the distance threshold between each other, network performance degrades.

Steps

To estimate wireless distances:

1. Connect a wireless client to the wireless cable modem. Refer to Connecting Devices to Your Network on page 12.
2. Place the wireless client at around one meter (three feet) away from the wireless cable modem.
3. Obtain the **RSSI** value for the connected client. Refer to Using the Wireless Access Control Option on page 52. This value is used in the formula further below.
4. Use the following table to determine what materials the wireless signal must travel through in order to reach the desired wireless coverage distance.

Attenuation Considerations at 2.4GHz

Material	Attenuation
Connector/Cable	3.5dB
Free Space	.24dB / foot
Interior Drywall	3dB to 4dB
Cubicle Wall	2dB to 5dB
Wood Door (Hollow/Solid)	3dB to 4dB
Brick, Concrete Wall (Note 1)	6dB to 18db
Glass Window (not tinted)	2dB to 3dB
Double Pane Coated Glass	13dB
Bullet Proof Glass	10dB
Steel / Fire Exit Door	13dB to 19dB
Human Body	3dB
Trees (Note 2)	.15dB / foot
Note 1: Different types of concrete materials are used in different parts of the world and the thickness and coating differ depending on whether it is used in floors, interior walls, or exterior walls.	**Note 2**: The attenuation caused by trees varies significantly depending upon the shape and thickness of the foliage.

5. Using the attenuation value from the materials table above, enter it in the following formula.

Formula:

(Transmit Power, **use -30dBm**) **–** (Receiver Sensitivity, **use RSSI value**) **=** Allowable Free Space Loss

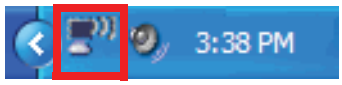
Allowable Free Space Loss **÷** Materials Attenuation Value **=** Optimal Distance in Feet Between the Cable Modem and a Wireless Client

Example:

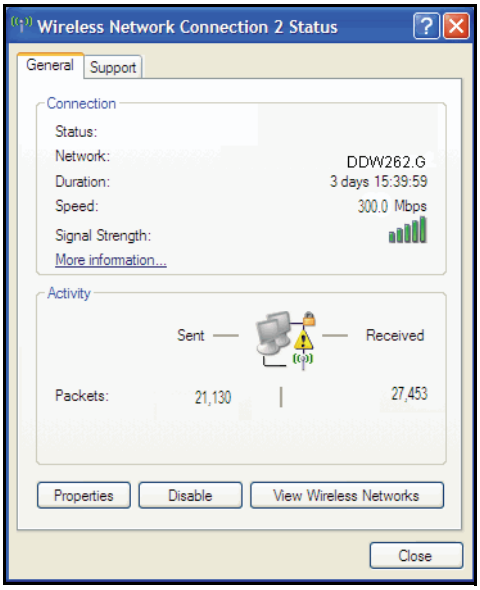
(-30dBm) **-** (-67dBm) **=** 37dBm (allowable free space loss for a 54Mbps connection)

37dBm **÷** .24db/foot (for open space) **=** 154.16 feet

6. Once you know the optimal feet distance between individual wireless clients and the wireless cable modem, you may resolve and prevent some performance issues.
7. To check the wireless signal strength and speed, use the following steps for a Windows computer connected wirelessly to the wireless cable modem. If the wireless computer is not connected, refer to Connecting Wireless Devices on page 12.
   - ❑ Double-click the Wireless networking icon in the system tray.



   - ❑ Review the speed and signal strength in the status window.

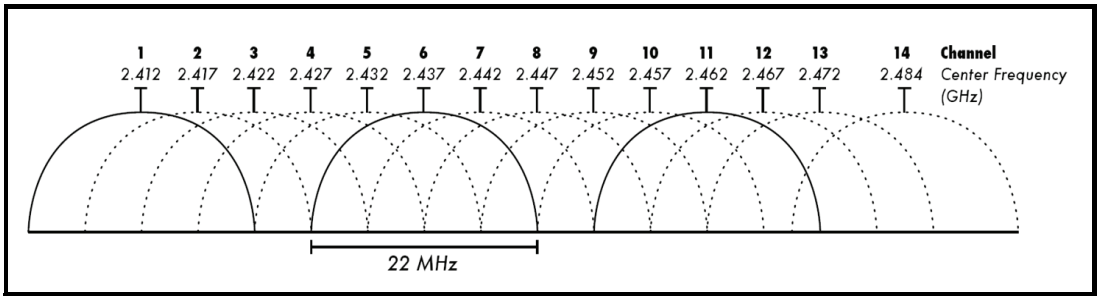


Selecting a Wireless Channel

In some environments it may be necessary to change the wireless channel on which the wireless cable modem operates, such as computing, test, and other environments where there can be several wireless access points operating in the 2.4Ghz range.

In some cases, you may want to segment your wireless traffic where a group of devices operates on one channel and another group operates on another channel. Do this by configuring the channel on each wireless access point individually (if you have multiples). If you have control over only one wireless device in an environment where several exist, you can change the wireless channel on your device to one that is not heavily used. To change the wireless broadcast channel, refer to Using the Wireless Radio Option on page 47.

The following diagram (Source: Wikipedia.org, and IEEE article IEEE 802.11n-2009) displays channels available in the Americas. Each available channel is 22Mhz wide. Since channels overlap, it is best to choose channels with the least overlap (typically 1, 6, and 11 in the Americas, and 1, 5, 9, and 13 in Europe). Overlapping channels are one possible source for wireless network performance issues.



7 Understanding the Parental Control Menu

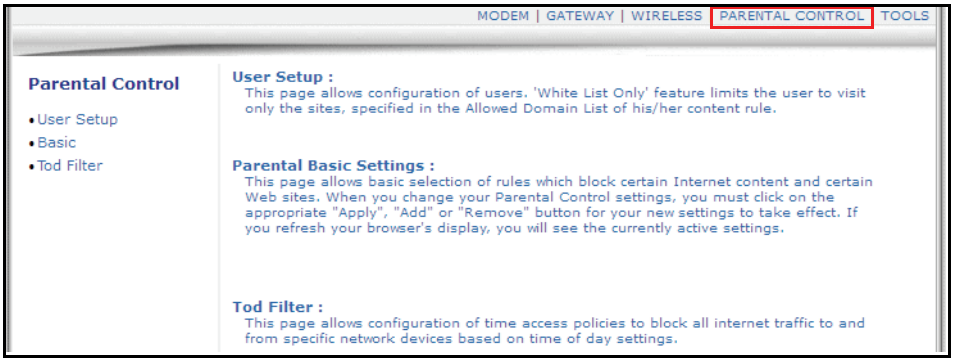
This chapter provides instructions for controlling the Internet access of users on the DDW262.G network. Parental Controls provides the following features:

- ❑ User/password access
- ❑ Block specific Web sites and Web sites based on keywords
- ❑ Times users are allowed to access the Internet

Steps

To access the parental control menu:

1. Access the Web interface. Refer to Accessing the Web User Interface on page 15.
2. Click the **Parental Control** link from the top of the screen.



7.1 Using the Parental Control User Setup Option

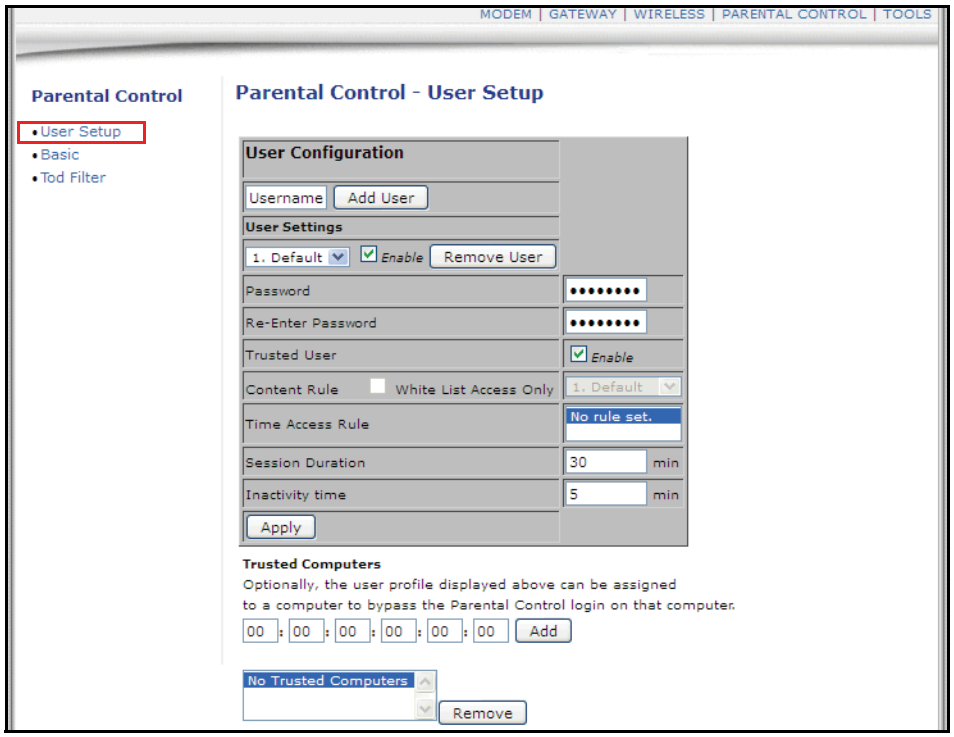
The **User Setup** option allows you to configure which user accounts can or cannot connect to your wireless or wired network and the parameters of the connection.

Steps

To configure user accounts:

1. Access the Web interface.
2. Click the **Parental Control** link from the top of the screen.
3. Click **User Setup** from the left side of the screen. The **User Setup** fields are explained following this screen example.

Note: To enable Parental Control, refer to Using the Parental Control Basic Option on page 61.



Label	Description
User Configuration	
Add User **Remove User** **Enable**	Defines user accounts. ♦ To select an existing user, choose the user from the User Settings pop-up menu. ♦ To add a new user, add the user name and click Add. ♦ To activate the user, check Enable. ♦ To remove a user, select the user from the pop-up menu and click Remove User.
Password	Defines the password for this user. It is required when this user tries to access the Internet via the device.
Re-Enter Password	Verifies the password by re-entering the password.
Trusted User	Defines the selected user as a trusted user when enabled is checked. The user is limited to timing and content when visiting the Internet, as defined in the following fields.
Content Rule	Selects from the pop-up menu an existing content rule that defines what kind of Websites the user can visit or not.
White List Access Only	Selects the White List Access option. If you have created a content rule that defines a black list and white list, select the White List Access Only checkbox to force the wireless modem to execute the policy for the selected user

Time Access Rule	Selects a defined time access rule to apply to the selected user.
Session Duration	Allows you to enter a time in minutes for the user's session expiration. Upon expiration, the user can log back in for the same session duration.
Inactivity Time	Allows you to enter the time out value when a user has no activity on the Internet. When the time expires, the user interface to the Internet is cancelled.
Apply	Saves all changes when clicked.
Trusted Computers	Defines the trusted hosts that can bypass the Parental Control Process.
Add	Adds the trusted host's MAC address entered in the given area and Add is clicked.
Remove	Removes a trusted computer from the list when it is highlighted and Remove is clicked.

7.2 Using the Parental Control Basic Option

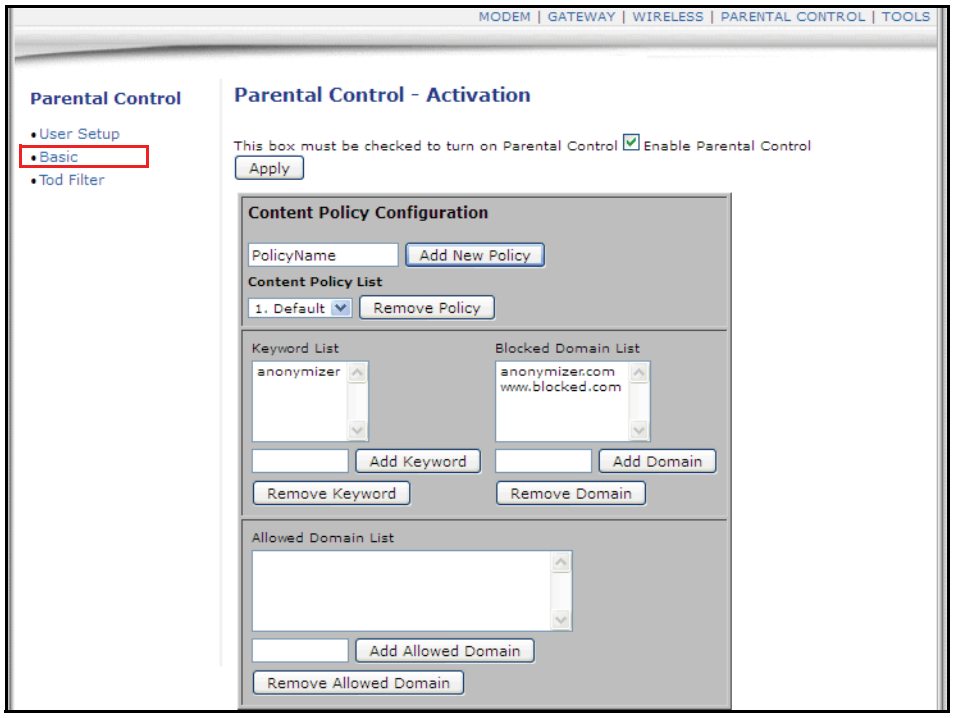
The **Basic** option allows basic selection of rules which block certain Internet content and certain Web sites. After you change your Parental Control settings, click the appropriate Apply, Add, or Remove button for your new settings to take effect. Refresh your browser's display to see the currently active settings.

Steps

To filter Internet content and Web sites:

1. Access the Web interface.
2. Click the **Parental Control** link from the top of the screen.
3. Click **Basic** from the left side of the screen. The **Basic** fields are explained following

this screen example.



Label	Description
Enable Parental Control	Activates the Parental Control feature when checked.
Apply	Saves all changes in the screen and activates Parental Control, if enabled.
Content Policy Configuration	
Add New Policy	Allows you to add a policy. ♦ To create a new policy, enter the policy name and click Add New Policy.
Content Policy List	
Select or Remove Policy	Select or remove existing policies. ♦ To select an exiting policy, click the down arrow next to the list box. Choose the policy from the list. ♦ To remove a policy, select it from the list and click Remove Policy.
Keyword List **Add Keyword** **Remove Keyword**	Allows you to enter keywords to block Web site addresses (URLs) containing those words. ♦ To add a keyword, enter the word in the field next to the Add Keyword button and click Add Keyword. The keyword is added to the list. ♦ To remove a keyword, select it from the list and click Remove Keyword.

Blocked Domain List **Add Domain** **Remove Domain**	Allows you to enter Web domains (for example, unwanted.com) to block access to those domains. ♦ To add a domain, enter a domain and click Add Domain. ♦ To remove a domain, select it from the list and click Remove Domain.
Allowed Domain List	Allows users to visit only the sites defined in this list.
Add Allowed Domain	Adds allowed domains to the list. ♦ To enter an allowed domain, enter the name and click Add Allowed Domain.
Remove Allowed Domain	Removes domain names from the list. ♦ To remove a domain, highlight it from the list and click Remove Allowed Domain.

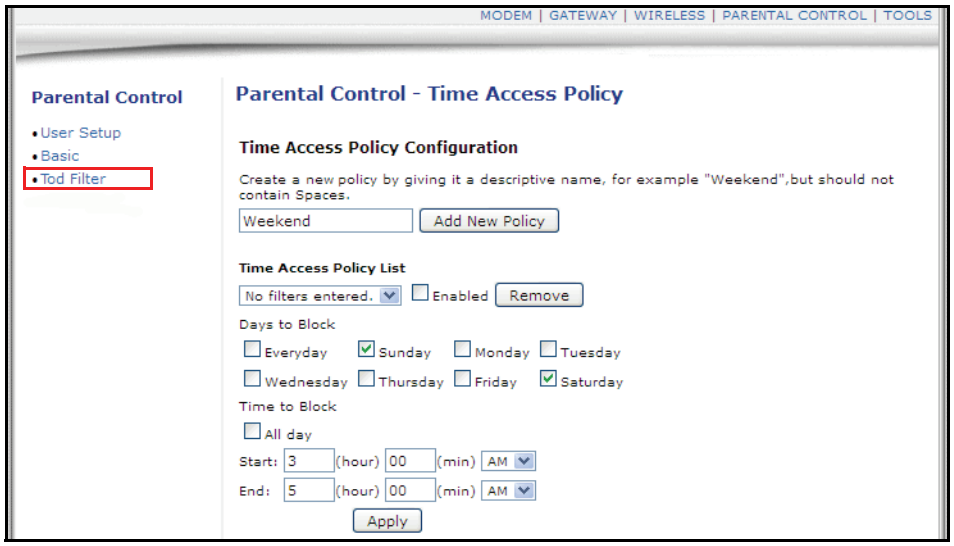
7.3 Using the Parental Control Tod Filter Option

The **Tod Filter** option allows the configuration of time-based access policies to block all Internet traffic at specified times of the day.

Steps

To configure time-of-day filters:

1. Access the Web interface.
2. Click the **Parental Control** link from the top of the screen.
3. Click **Tod Filter** from the left side of the screen. The **Tod Filter** fields are explained following this screen example.



Label	Description
Time Access Policy Configuration	
Add New Policy	Adds a new policy. ♦ To add a new policy, enter a policy name and click the Add New Policy button.
Time Access Policy List	
Select **Enable** **Remove**	Allows you to select, enable, or remove a time access policy. If the checkbox is unchecked, the policy is not active. ♦ To select an existing policy, click the down arrow next to the list box. Choose the policy from the list. ♦ To enable a policy, select the policy from the drop-down list and check Enable. ♦ To remove a policy, select the policy from the drop-down list and click Remove.
Days to Block	Selects the days to block Internet access. The Internet access times for the days selected to block are defined in the following fields.
Time to Block	Defines the time to block. ♦ To block all day, check All Day to eliminate all access during the days selected to block. ♦ To block specific times, enter the time range in the Start and End fields.
All Day	Saves all changes when clicked.
Apply	Adds a new policy. ♦ To add a new policy, enter a policy name and click the Add New Policy button.

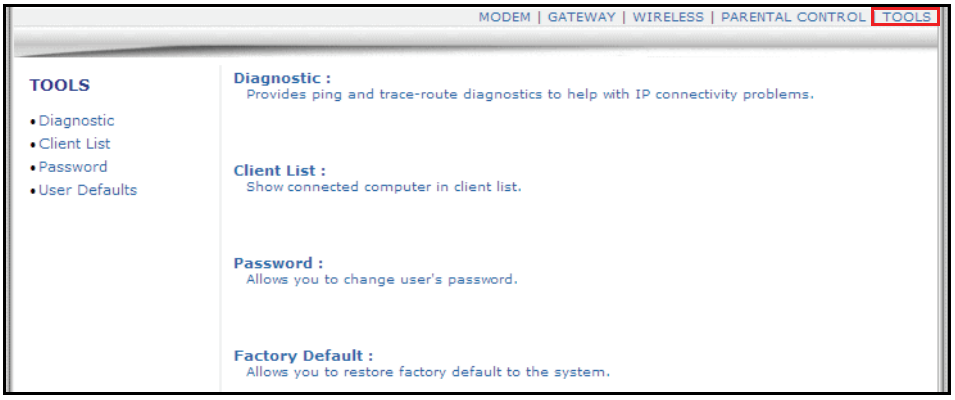
8 Understanding the Tools Menu

This chapter contains instructions for using a variety of tools to evaluate, diagnose, and configure the operation of DDW262.G Wireless Cable Modem and Router.

Steps

To access the tools menu:

1. Access the Web interface. Refer to Accessing the Web User Interface on page 15.
2. Click the **Tools** link from the top of the screen.



8.1 Using the Tools Diagnostics Option

The diagnostics tool provides the Ping utility.

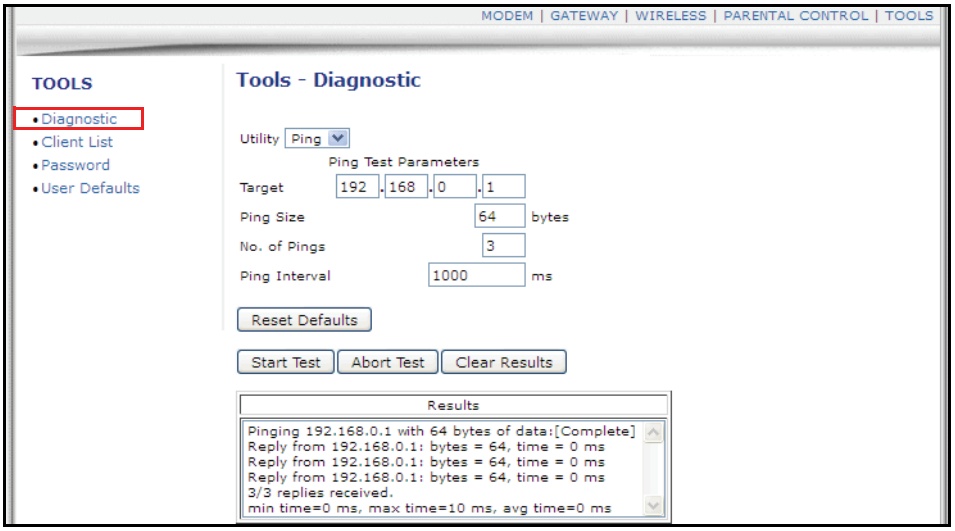
8.1.1 Using the Ping Utility

The **Ping** utility tests the network connectivity between devices by sending a test message to a specific device. You can also confirm the size of data sent is the same as the size of data received.

Steps

To test connectivity between devices:

1. Access the Web interface.
2. Click the **Tools** link from the top of the screen.
3. Click **Ping** from the left side of the screen. The **Ping** fields are explained following this screen example.



Label	Description
Ping	
Ping Target	Defines the IP address to which you want to send a ping.
Ping Size	Defines the packet size to send for the ping operation.
No. of Pings	Defines the number of ping commands to send to the ping target.
Ping Interval	Defines the interval between ping operations in milliseconds.
Start Test/Abort Test/Clear Results	Defines what you want to do. ♦ To start the test, click Start. Test ♦ To cancel the test, click Abort Test. ♦ To clear the displayed results, click Clear Results.
Results	Displays the results of the ping test.
Refresh	Updates the results in the Results window. You must click the Refresh button to get the latest results.

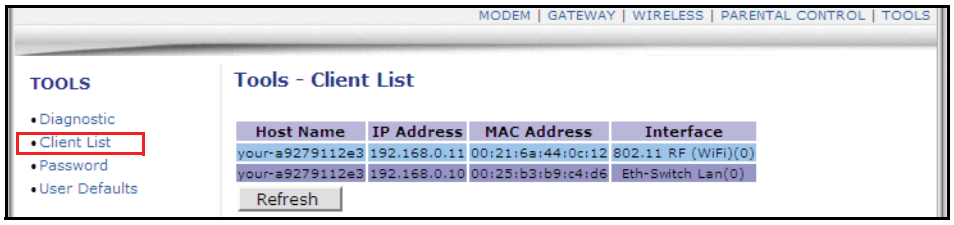
8.2 Using the Tools Client List Option

The **Client List** option displays computers connected to the DDW262.G.

Steps

To view a list of computers connected to this device:

1. Access the Web interface.
2. Click the **Tools** link from the top of the screen.
3. Click **Client List** from the left side of the screen. The **Client List** fields are explained following this screen example.



Label	Description
Hostname	DIsplays the hostnames of the DHCP clients currently connected to the device.
IP Address	Displays the IP Address of the DHCP clients currently connected to the device.
MAC Address	Displays the MAC Address of the DHCP clients currently connected to the device.
Interface	Displays the how clients are connected to the device. For example: Ethernet LAN, Wireless.
Refresh	Refreshes the client list. Useful when testing network connectivity between connecting clients and the DDW262.G.

8.3 Using the Tools Password Option

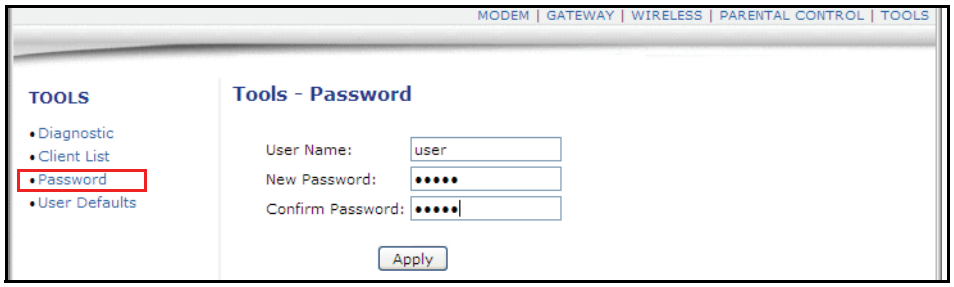
The **Password** option allows you to change the passwords for user login. This login is used to access this Web interface. For information on the default logins, see.

Steps

To change user passwords:

1. Access the Web interface.
2. Click the **Tools** link from the top of the screen.

3. Click **Password** from the left side of the screen. The **Password** fields are explained following this screen example.



Label	Description
User Name	Defines a new user name for the **user** account to access the web interface of the DDW262.G.
New Password	Defines a new password for the user account to access the web interface of the DDW262.G.
Confirm Password	Confirms the password when re-entered.

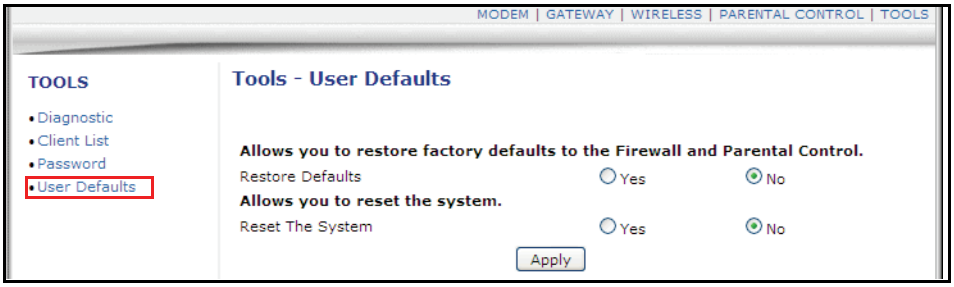
8.4 Using the Tools User Defaults Option

The **User Defaults** option allows you to restore Firewall and Parental Control factory defaults to the device. You can also reset the device from this screen.

Steps

To reset firewall and parental controls to factory defaults or reset the system:

1. Access the web interface.
2. Click the **Tools** link from the top of the screen.
3. Click **User Defaults** from the left side of the screen. The **User Defaults** fields are explained following this screen example.



Label	Description
Restore Defaults	Restore the firewall and parental control settings to the defaults set at the factory. ♦ **Yes**—Resets firewall and parental control to factory defaults. ♦ **No**—Leaves settings as configured by the user.
Reset The system	♦ **Yes**—Power-cycles the device. ♦ **No**—Does not power-cycle the device.
Apply	Applies the options selected in this screen.

9 Glossary

This chapter defines terms used in this guide and in the industry.

Broadcast
A packet sent to all devices on a network.

Cable Modem Termination System (CMTS)
Typically located in the cable company's headend, the CMTS is equipment that provides high-speed data services to subscribers, such as cable Internet and VoIP.

Channel Bonding
A computer networking configuration where two or more network interfaces are combined on a host computer for redundancy or increased throughput. Data is transmitted over these channels as if they are one channel.

Customer Premises Equipment (CPE)
Equipment such as telephones, routers, and modems located at a subscribers location to enable customers access to communication services.

Default Gateway
The routing device used to forward all traffic that is not addressed to a computer on the local subnet.

Demilitarized Zone (DMZ)
Allows one IP address (or computer) to be placed in between the firewall and the Internet (usually for gaming and video conferencing). This allows risky, open access to the Internet.

Domain
A subnetwork comprised of a group of clients and servers under the control of one security database.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are in the form of a registered entity name plus one of a number of predefined top-level suffixes, such as .com, .edu, .org.

Domain Name System (DNS)
An Internet service that locates and translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. The DNS system is actually its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Downstream
A term to describe the direction of data from the network service provider to the customer.

Dynamic Host Configuration Protocol (DHCP)
A protocol that centrally automates the assignment of IP addresses (see IP Address) in a network. Using the Internet's set of protocols (TCP/IP) (see Transmission Control Protocol/Internet Protocol (TCP/IP)) , each machine that can connect to the Internet needs a unique IP address. For example, when the service provider sets up computer users with a connection to the Internet, an IP address is assigned to each machine. DHCP lets the service provider distribute IP addresses and automatically sends a new IP address when a computer is plugged in to the high-speed Internet network. DHCP uses the concept of a "lease" or amount of time an IP address is valid for a computer. Lease times can vary.

Ethernet
A standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. It forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS (see Xerox Network Services (XNS)) .

Firewall
A highly effective method to block unsolicited traffic from outside the connected computers in your gateway.

Gateway
A local device, usually a router, that connects hosts on a local network to other networks – sometimes with different incompatible communication protocols.

Headend
A main facility to process and distribute Internet communication signals. Headend may also refer to cable television signals and power line communication facilities.

Internet Protocol (IP)
The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to understand each other. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address
In the most widely installed level of the IP today, an IP address is a 32-bit binary digit number that identifies each sender or receiver of information that is sent in packet form across the Internet. When you request a Web page or send an e-mail, the IP part of TCP/IP includes your IP address. IP sends your IP address to the IP address obtained by looking up the domain name in the URL (see Uniform Resource Locator (URL)) you requested or in the e-mail address to which you are sending a note. A dynamic IP address is an IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

Internet Service Provider (ISP)
A company that provides individuals and companies access to the Internet and other related services.

Interval Usage Code (IUC)
Interval usage codes define different profiles for upstream burst profiles to use for the data. IUCs are sent to the cable modem from the CMTS to tell the device important characteristics to use for the burst, such as modulation type, preamble length, and so on.

Local Area Network (LAN)
A group of computers and associated devices such as printers and servers that share a common communication line and other resources within a small geographic area.

Media Access Control (MAC) Address
A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. Usually written in the form 01:23:45:67:89:ab.

Megabits per Second (Mbps)
A unit of measurement for data transmission that represents one million bits per second.

Maximum Transmission Unit (MTU)
The size in bytes of the largest packet that can be sent or received.

Network Address Translation (NAT)
A technique by which several hosts or computers share a single IP address for access to the Internet. NAT enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic, and provides a type of firewall by hiding internal IP addresses.

Network Basic Input Output System (NetBIOS)
An application programming interface (API) that augments the DOS BIOS by adding special functions for LANs. Almost all Windows-based LANs for PCs are based on the NetBIOS.

Network Operations Center (NOC)
A location that controls computer, television, or telecommunications networks. Large organizations usually have more than one network operations center to manage multiple networks.

Packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Ranging
A process in which a cable modem sends a range request at a power of 8 dBmV (very low power). If it does not rec i eve a range response from the CMTS, the cable modem re-transmits the range request at a 3 dB higher power level and continues the process until a range response is received.

Routing Information Protocol (RIP)
A protocol in which routers periodically exchange information with one another to determine minimum-distance paths between sources and destinations.

Router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Subnet
A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 10.1.10 would be part of the same subnet. IP networks are divided using a subnet mask.

Subnet Mask
Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network.

Telnet
A network protocol used on the Internet or a local area network. Provides bi-directional interactive text-oriented communications using a virtual terminal connection.

Terminal Access Controller Access-Control System (TACACS)
A remote authentication protocol used to communicate with an authentication server to determine if the user is allowed to access the network.

Time Division Multiple Access (TDMA)
A method in which cable modems must time-share the upstream channel because there are many cable modems and only one upstream channel frequency.

Transmission Control Protocol (TCP)
A method (protocol) used with the IP to send data in the form of message units (datagrams) between network devices over a LAN or WAN. While IP handles the actual delivery of the data (routing), TCP keeps track of the individual units of data (packets) that a message is divided into for efficient delivery over the network. TCP requires the receiver of a packet to return an acknowledgment of receipt to the sender of the packet.

Transmission Control Protocol/Internet Protocol (TCP/IP)
The basic communication language or set of protocols to communicate over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols.

Trivial File Transfer Protocol
A file transfer protocol used to transfer automatically configuration or boot files.

Uniform Resource Identifier (URI)
A string of characters used to identify a name or a resource on the Internet.

Upstream
A term to describe the direction of data from the customer to the network service provider.

Uniform Resource Locator (URL)
A URI that specifies where a known resource is available and how to retrieve it.

Wide Area Network (WAN)
A long-distance link or computer network that spans a relatively large geographical area that connects remotely located LANs. Typically, a WAN consists of two or more LANs. The Internet is a large WAN.

Wi-Fi Protected Setup (WPS)
A security protocol for wireless home networks. Created by the Wi-Fi Alliance, this protocol allows home users to easily set up wireless security and add new devices without needing to enter long passwords.

Wireless Local Area Network (WLAN)
A method that links two or more devices to provide a connection through an access point the wider Internet. Users can move within the local coverage area and stay connect to the network.

Xerox Network Services (XNS)
A protocol suite developed by Xerox that provides general purpose network communications, Internet routing, and packet delivery.