See the tables describing the fields in the **Access Point** and **Bridge** operating modes for descriptions of the fields in this screen.

6.5 Technical Reference

This section provides technical background information about the topics covered in this chapter. Refer to Appendix E on page 153 for further readings on Wireless LAN.

6.5.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual and applications. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyXEL Device uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q or DSCP information in each packet's header. The ZyXEL Device automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency and jitter (variations in delay).

6.5.2 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

6.5.2.1 Rapid STP

The ZyXEL Device uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

6.5.2.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the following table.

Table 12 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

6.5.2.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

6.5.2.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 13 STP Port States

PORT STATES	DESCRIPTIONS
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

6.5.3 Additional Wireless Terms

Table 14 Additional Wireless Terms

TERM	DESCRIPTION
Intra-BSS Traffic	This describes direct communication (not through the ZyXEL Device) between two wireless devices within a wireless network. You might disable this kind of communication to enhance security within your wireless network.
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.
Roaming	If you have two or more ZyXEL Devices (or other wireless access points) on your wireless network, you can enable this option so that wireless devices can change locations without having to log in again. This is useful for devices, such as notebooks, that move around a lot.
Antenna	An antenna couples Radio Frequency (RF) signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air. Positioning the antennas properly increases the range and coverage area of a wireless LAN.

7

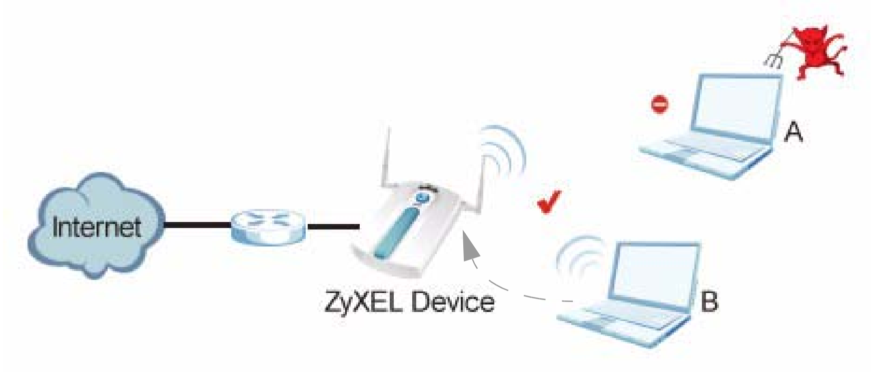
Wireless Security Screen

7.1 Overview

This chapter describes how to use the **Wireless Security** screen. This screen allows you to configure the security mode for your ZyXEL Device.

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

Figure 31 Securing the Wireless Network



In the figure above, the ZyXEL Device checks the identity of devices before giving them access to the network. In this scenario, Computer A is denied access to the network, while Computer B is granted connectivity.

The ZyXEL Device secure communications via data encryption, wireless client authentication and MAC address filtering. It can also hide its identity in the network.

7.2 What You Can Do in the Wireless Security Screen

Use the **Wireless** > **Security** screen (see Section 7.4 on page 77) to choose the security mode for your ZyXEL Device.

7.3 What You Need To Know About Wireless Security

User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

The following table shows the relative effectiveness of wireless security methods:.

Table 15 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

The available security modes in your ZyXEL Device are as follows:

- **None.** No data encryption.
- **WEP.** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.
- **802.1x-Only.** This is a standard that extends the features of IEEE 802.11 to support extended authentication. It provides additional accounting and control features. This option does not support data encryption.
- **802.1x-Static64.** This provides 802.1x-Only authentication with a static 64bit WEP key and an authentication server.
- **802.1x-Static128**. This provides 802.1x-Only authentication with a static 128bit WEP key and an authentication server.
- **WPA.** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard.
- **WPA2.** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
- **WPA2-MIX.** This commands the ZyXEL Device to use either WPA2 or WPA depending on which security mode the wireless client uses.
- **WPA2-PSK**. This adds a pre-shared key on top of WPA2 standard.

- **WPA2-PSK-MIX**. This commands the ZyXEL Device to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

In Bridge and Bridge + AP operating modes, the only available security modes are WEP and WPA2-PSK.

Passphrase

A passphrase functions like a password. In WEP security mode, it is further converted by the ZyXEL Device into a complicated string that is referred to as the “key”. This key is requested from all devices wishing to connect to a wireless network.

PSK

The Pre-Shared Key (PSK) is a password shared by a wireless access point and a client during a previous secure connection. The key can then be used to establish a connection between the two parties.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message. Encryption is the process of converting data into unreadable text. This secures information in network communications. The intended recipient of the data can “unlock” it with a pre-assigned key, making the information readable only to him. The ZyXEL Device when used as a wireless client employs Temporal Key Integrity Protocol (TKIP) data encryption.

EAP

Extensible Authentication Protocol (EAP) is a protocol used by a wireless client, an access point and an authentication server to negotiate a connection.

The EAP methods employed by the ZyXEL Device when in Wireless Client operating mode are Transport Layer Security (TLS), Protected Extensible Authentication Protocol (PEAP), Lightweight Extensible Authentication Protocol (LEAP) and Tunneled Transport Layer Security (TTLS). The authentication protocol may either be Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) or Generic Token Card (GTC).

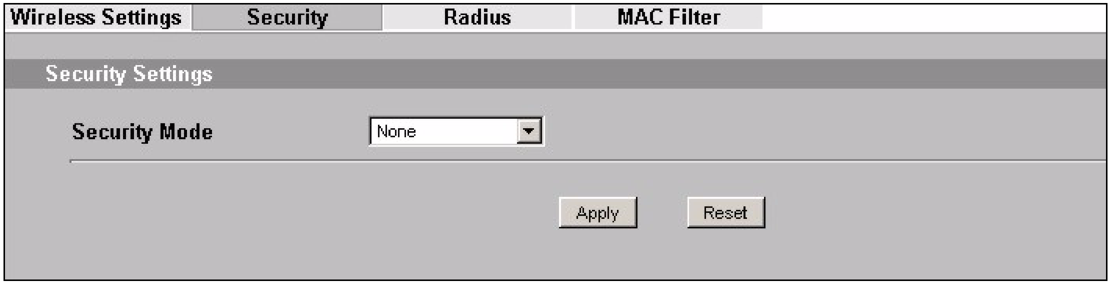
Further information on these terms can be found in Appendix E on page 153.

7.4 The Security Screen

Use this screen to choose the security mode for your ZyXEL Device.

Click **Wireless > Security**. The screen varies depending upon the security mode you select.

Figure 32 Security: None



Security Mode: None

The default security mode is set to **None**.

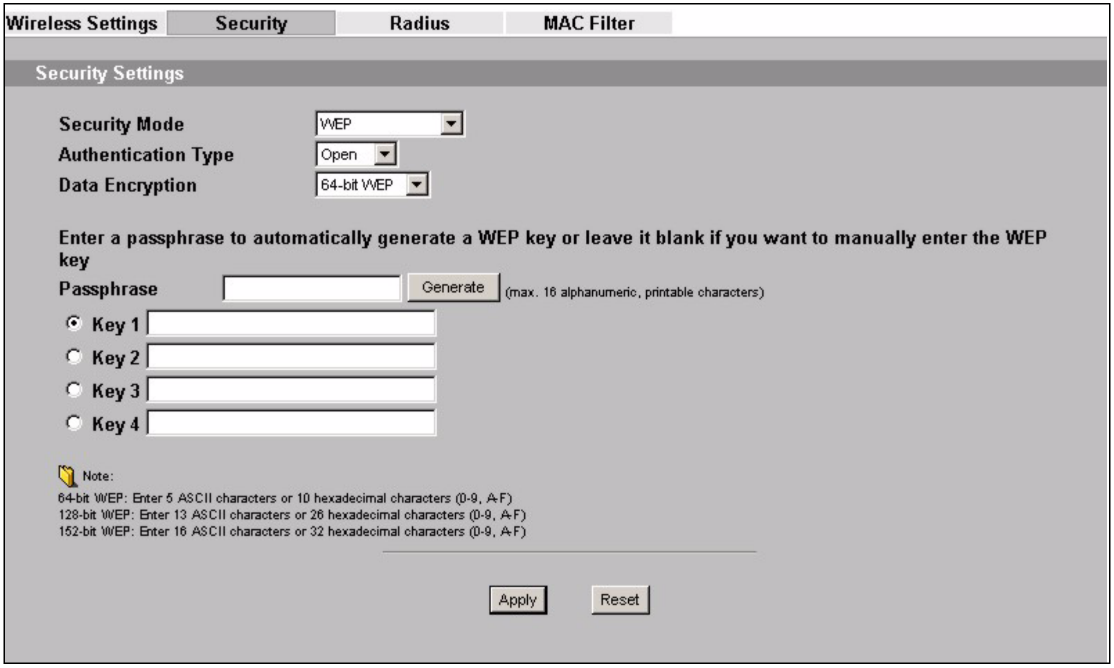
Note that some screens display differently depending on the operating mode selected in the **Wireless > Wireless Settings** screen.

You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

7.4.1 Security: WEP

Use this screen to use WEP as the security mode for your ZyXEL Device. Select **WEP** in the **Security Mode** field to display the following screen.

Figure 33 Security: WEP



Security Mode: WEP

Authentication Type: Open

Data Encryption: 64-bit WEP

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key

Passphrase [ ] Generate (max. 16 alphanumeric, printable characters)

● Key 1

○ Key 2

○ Key 3

○ Key 4

Note:

64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)

128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)

152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)

The following table describes the labels in this screen.

Table 16 Security: WEP

LABEL	DESCRIPTION
Security Mode	Choose **WEP** in this field.
Authentication Method	Select **Open** or **Shared Key** from the drop-down list box. The default setting is **Auto**.
Data Encryption	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP**, **128-bit WEP** or **152-bit WEP** to enable data encryption.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation on wireless client adapters.
Generate	Click this to get the keys from the **Passphrase** you entered.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **152-bit WEP**, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

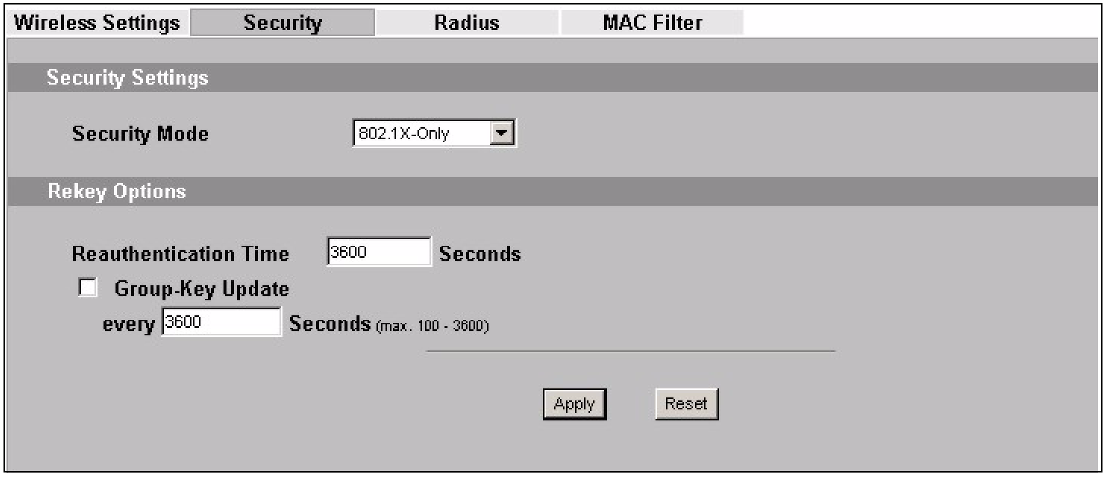
7.4.2 Security: 802.1x Only

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

7.4.2.1 Access Point

Use this screen to use 802.1x-Only security mode for your ZyXEL Device that is in Access Point operating mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 34 Security: 802.1x Only for Access Point



Security Mode 802.1X-Only

Reauthentication Time 3600 Seconds

□ Group-Key Update

every 3600 Seconds (max. 100 - 3600)

The following table describes the labels in this screen.

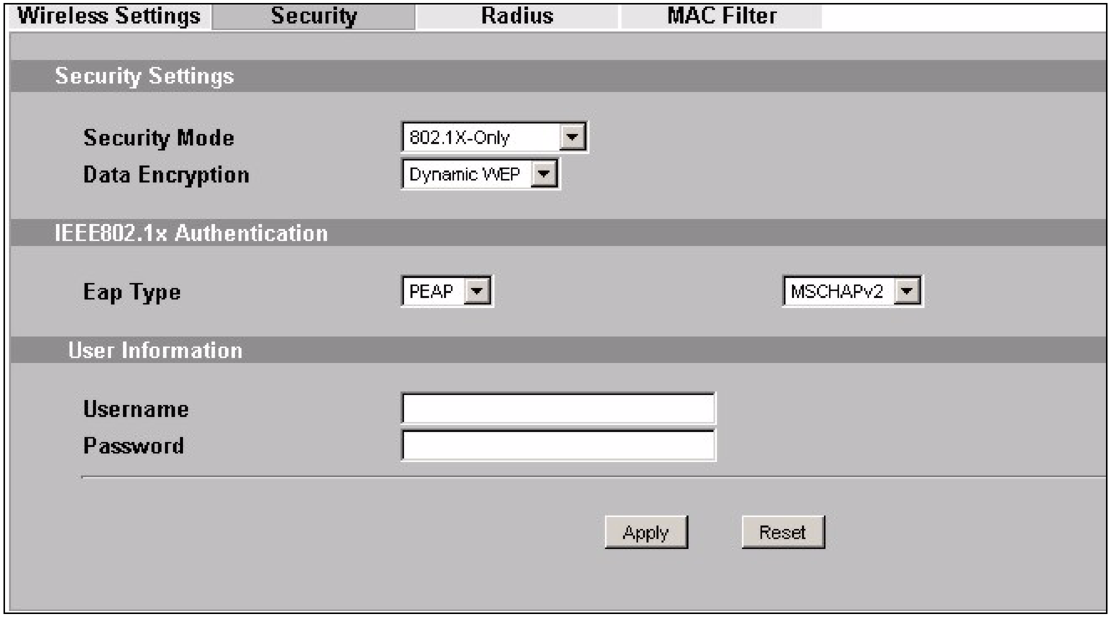
Table 17 Security: 802.1x Only for Access Point

LABEL	DESCRIPTION
Security Mode	Choose **802.1x Only** in this field.
ReAuthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off. **Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.**
Group-Key Update	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.2.2 Wireless Client

Use this screen to use 802.1x-Only security mode for your ZyXEL Device that is in Wireless Client operating mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 35 Security: 802.1x Only for Wireless Client



Security Mode: 802.1X-Only
Data Encryption: Dynamic WEP
Eap Type: PEAP, MSCHAPv2
Username:
Password:

The following table describes the labels in this screen.

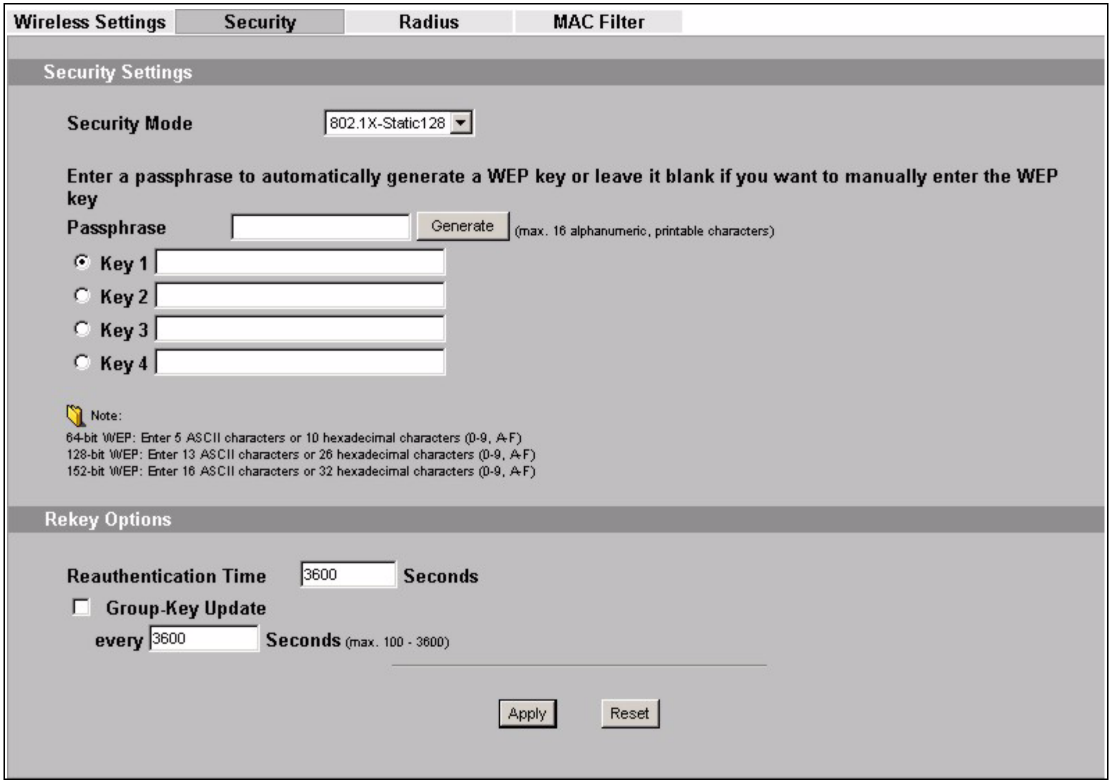
Table 18 Security: 802.1x Only for Wireless Client

LABEL	DESCRIPTION
Security Mode	Choose the same security mode used by the AP.
Data Encryption	Select between **None** and **Dynamic WEP**. Refer to Section on page 161 for information on using Dynamic WEP.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The default value is PEAP. The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.The default value is MSCHAPv2.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

Use this screen to use 802.1x Static 64 or 802.1x Static 128 security mode for your ZyXEL Device. Select **802.1x Static 64** or **802.1x Static 128** in the **Security Mode** field to display the following screen.

Figure 36 Security: 802.1x Static 64-bit, 802.1x Static 128-bit (AP mode)



Security Settings

Security Mode: 802.1X-Static128

Enter a passphrase to automatically generate a WEP key or leave it blank if you want to manually enter the WEP key

Passphrase [ ] Generate (max. 16 alphanumeric, printable characters)

● Key 1 [ ]
○ Key 2 [ ]
○ Key 3 [ ]
○ Key 4 [ ]

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters (0-9, A-F)
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters (0-9, A-F)
152-bit WEP: Enter 16 ASCII characters or 32 hexadecimal characters (0-9, A-F)

Rekey Options

Reauthentication Time: 3600 Seconds

□ Group-Key Update
every 3600 Seconds (max. 100 - 3600)

The following table describes the labels in this screen.

Table 19 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Security Mode	Choose **802.1x Static 64 or 802.1x Static 128** in this field.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation on wireless client adapters (AP mode).
Generate	Click this to get the keys from the **Passphrase** you entered (AP mode).
Key 1 to Key 4	If you chose **802.1x Static 64**, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **802.1x Static 128-bit**, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off. **Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.**

Table 19 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Group-Key Update	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

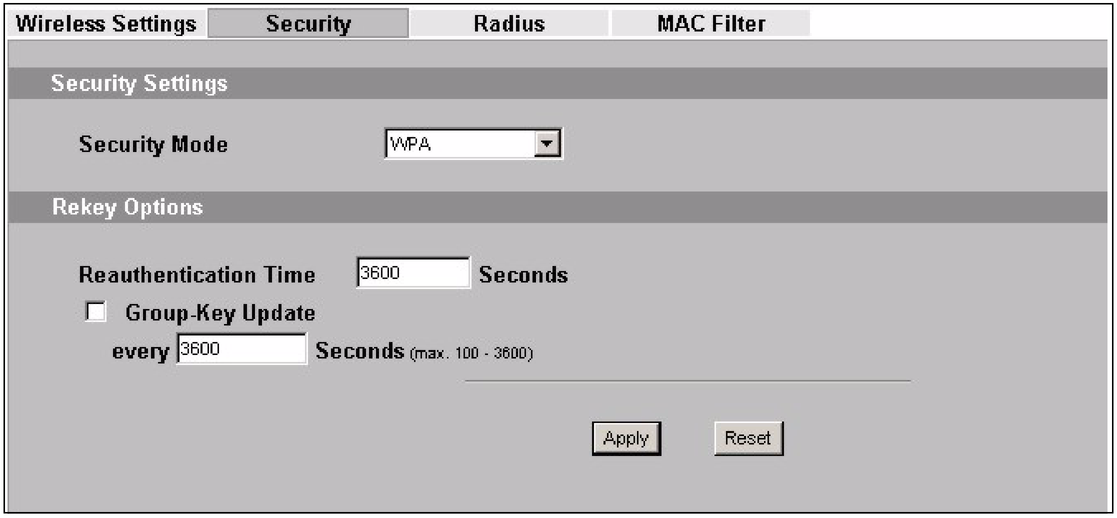
7.4.4 Security: WPA

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

7.4.4.1 Access Point

Use this screen to employ WPA as the security mode for your ZyXEL Device that is in Access Point operating mode. Select **WPA** in the **Security Mode** field to display the following screen.

Figure 37 Security: WPA for Access Point



Security Mode: WPA

Reauthentication Time: 3600 Seconds

□ Group-Key Update every 3600 Seconds (max. 100 - 3600)

The following table describes the labels in this screen.

Table 20 Security: WPA for Access Point

LABEL	DESCRIPTION
Security Mode	Choose **WPA** in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter “0” to turn reauthentication off. **Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.**

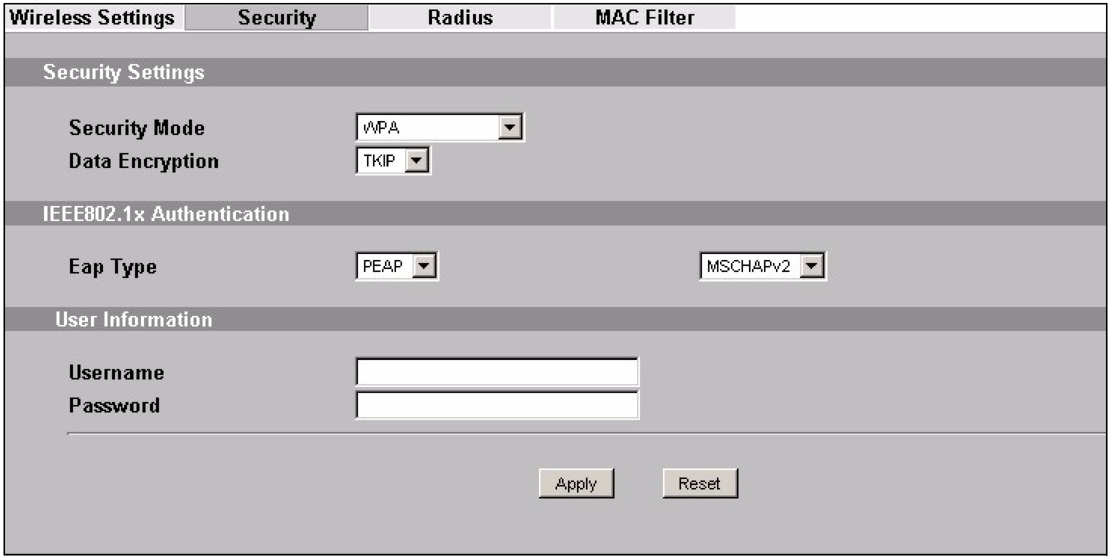
Table 20 Security: WPA for Access Point

LABEL	DESCRIPTION
Group Key Update	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device default is 3800 seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.4.2 Wireless Client

Use this screen to employ WPA as the security mode for your ZyXEL Device that is in Wireless Client operating mode. Select **WPA** in the **Security Mode** field to display the following screen.

Figure 38 Security: WPA for Wireless Client



Security Settings

Security Mode: WPA

Data Encryption: TKIP

IEEE802.1x Authentication

Eap Type: PEAP MSCHAPv2

User Information

Username

Password

The following table describes the labels in this screen.

Table 21 Security: WPA for Wireless Client

LABEL	DESCRIPTION
Security Mode	Choose the same security mode used by the AP.
Data Encryption	Select between **None** and **TKIP**.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The default value is PEAP. The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.The default value is MSCHAPv2.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.

Table 21 Security: WPA for Wireless Client

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

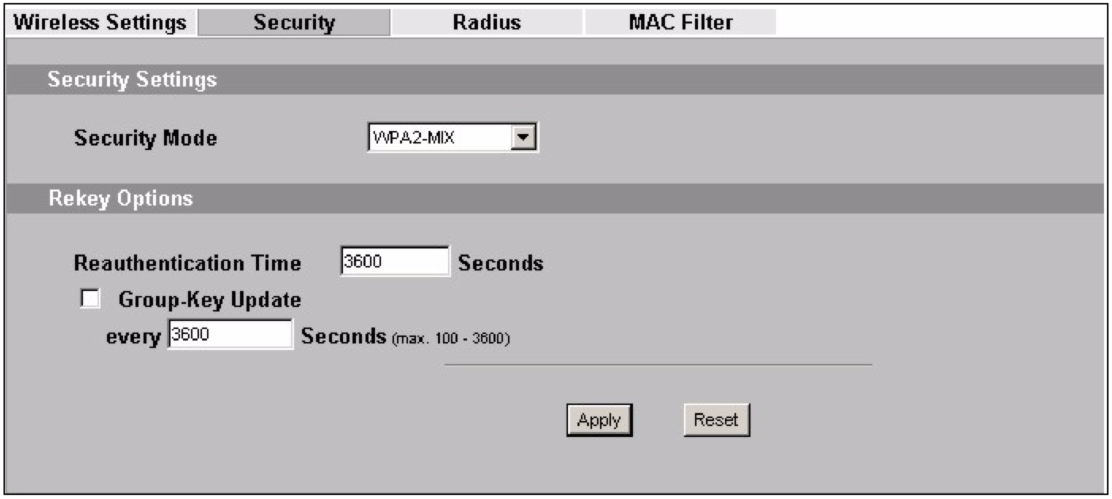
7.4.5 Security: WPA2 or WPA2-MIX

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

7.4.5.1 Access Point

Use this screen to use WAP2 or WPA2-MIX as the security mode for your ZyXEL Device that is in Access Point operating mode. Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 39 Security:WPA2 or WPA2-MIX for Access Point



Security Mode: WPA2-MIX

Reauthentication Time: 3600 Seconds

□ Group-Key Update every 3600 Seconds (max. 100 - 3600)

The following table describes the labels not previously discussed

Table 22 Security: WPA2 or WPA2-MIX for Access Point

LABEL	DESCRIPTIONS
Security Mode	Choose **WPA2** or **WPA2-MIX** in this field.
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter “0” to turn reauthentication off. **Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.**
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device‘s default is 3600 seconds (or 1 hour).

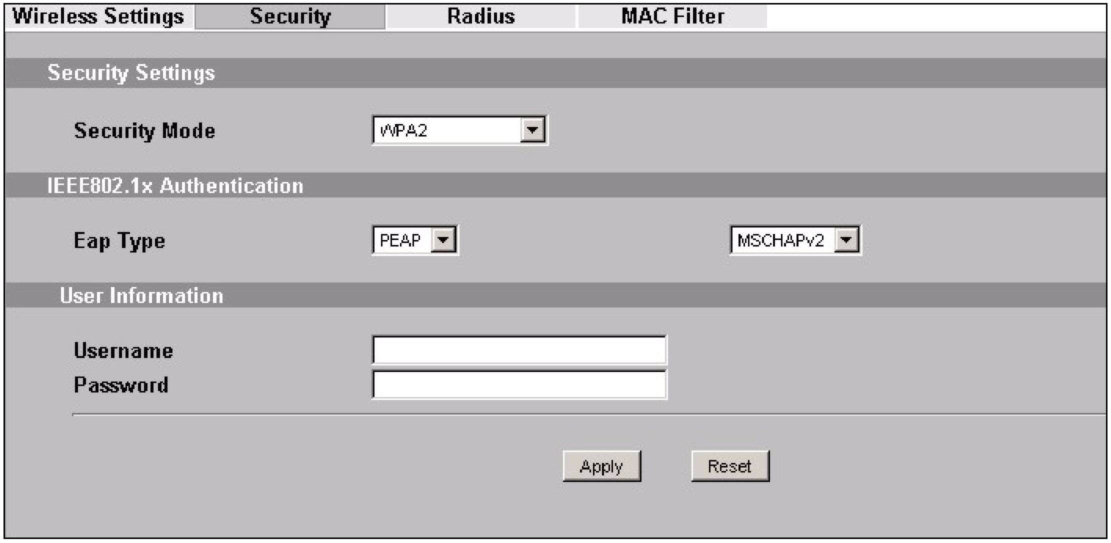
Table 22 Security: WPA2 or WPA2-MIX for Access Point

LABEL	DESCRIPTIONS
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.5.2 Wireless Client

Use this screen to employ WPA2 or WPA2-MIX as the security mode of your ZyXEL Device that is in Wireless Client operating mode. Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 40 Security: WPA2 or WPA2-MIX for Wireless Client



The following table describes the labels in this screen.

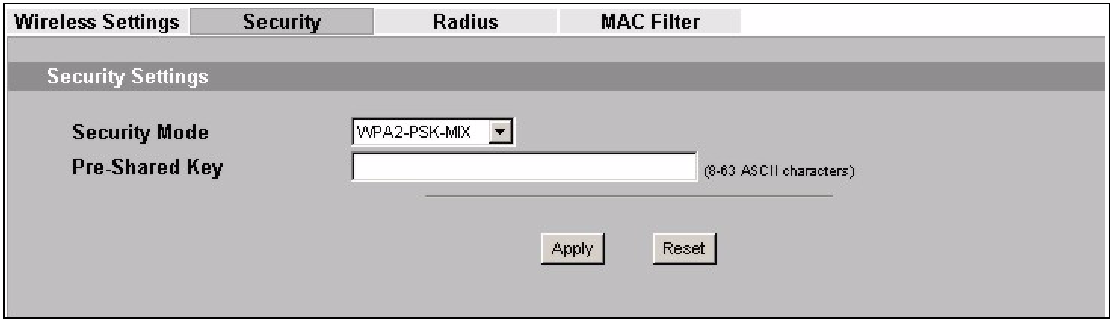
Table 23 Security: WPA2 or WPA2-MIX for Wireless Client

LABEL	DESCRIPTION
Security Mode	Choose the same security mode used by the AP.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The default value is PEAP. The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.The default value is MSCHAPv2.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Use this screen to employ WPA-PSK, WPA2-PSK or WPA2-PSK-MIX as the security mode of your ZyXEL Device. Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

Figure 41 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX



Security Mode: WPA2-PSK-MIX

Pre-Shared Key: (8-63 ASCII characters)

The following table describes the labels not previously discussed

Table 24 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.5 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

The following is a general guideline in choosing the security mode for your ZyXEL Device.

- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.Use WPA(2) security if you have WPA(2)-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.
- If you don't have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security. You can manually enter 64-bit, 128-bit or 152-bit WEP keys.

More information on Wireless Security can be found in Appendix E on page 153.

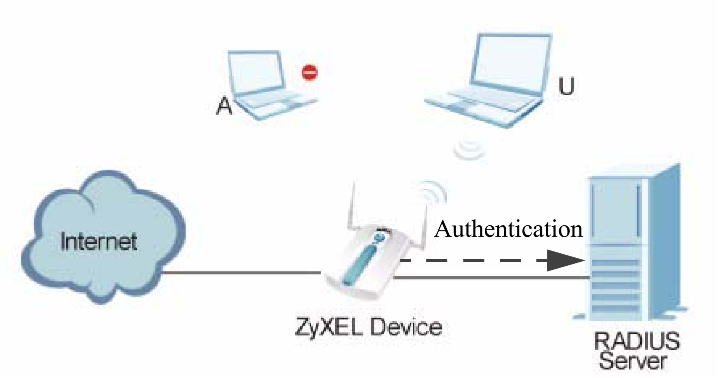
RADIUS Screen

8.1 Overview

This chapter describes how you can use the **Wireless > RADIUS** screen.

Remote Authentication Dial In User Service (RADIUS) is a protocol that can be used to manage user access to large networks. It is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server.

Figure 42 RADIUS Server Setup



In the figure above, wireless clients A and B are trying to access the Internet via the ZyXEL Device. The ZyXEL Device in turn queries the RADIUS server if the identity of clients A and U are allowed access to the Internet. In this scenario, only client U's identity is verified by the RADIUS server and allowed access to the Internet.

8.2 What You Can Do in the RADIUS Screen

Use the **Security** > **RADIUS** screen (see Section 7.4.1 on page 78) if you want to authenticate wireless users using a RADIUS Server and/or Accounting Server.

8.3 What You Need to Know About RADIUS

The RADIUS server handles the following tasks:

- **Authentication** which determines the identity of the users.
- **Authorization** which determines the network services available to authenticated users once they are connected to the network.

- **Accounting** which keeps track of the client's network activity.

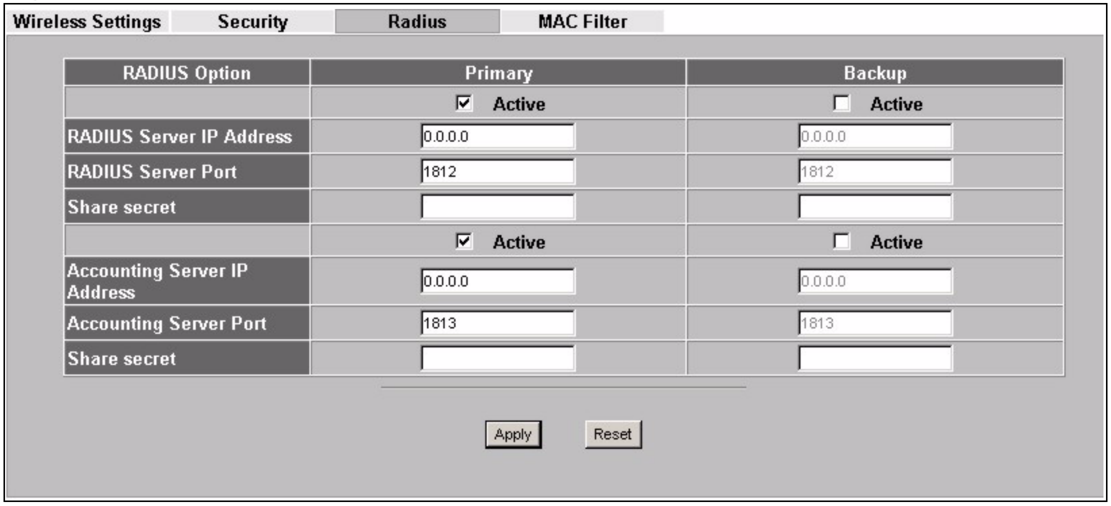
RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

You should know the IP addresses, ports and share secrets of the external RADIUS server and/or the external RADIUS accounting server you want to use with your ZyXEL Device. You can configure a primary and backup RADIUS and RADIUS accounting server for your ZyXEL Device.

8.4 The RADIUS Screen

Use this screen to set up your ZyXEL Device's RADIUS server settings. Click **Wireless** > **RADIUS**. The screen appears as shown.

Figure 43 Wireless > RADIUS



RADIUS Option	Primary	Backup
	☑ Active	□ Active
RADIUS Server IP Address	0.0.0.0	0.0.0.0
RADIUS Server Port	1812	1812
Share secret		
	☑ Active	□ Active
Accounting Server IP Address	0.0.0.0	0.0.0.0
Accounting Server Port	1813	1813
Share secret		

The following table describes the labels in this screen.

Table 25 Wireless > RADIUS

LABEL	DESCRIPTION
Primary	Configure the fields below to set up user authentication and accounting.
Backup	If the ZyXEL Device cannot communicate with the **Primary** accounting server, you can have the ZyXEL Device use a **Backup** RADIUS server. Make sure the **Active** check boxes are selected if you want to use backup servers. The ZyXEL Device will attempt to communicate three times before using the **Backup** servers. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the **ReAuthentication Timer** field in the **Security Settings** screen.
RADIUS Option	
Active	Select the check box to enable user authentication through an external authentication server. This check box is not available when you select **Internal**.
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation. This field is not available when you select **Internal**.

Table 25 Wireless > RADIUS

LABEL	DESCRIPTION
RADIUS Server Port	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so. This field is not available when you select **Internal**.
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network. This field is not available when you select **Internal**.
Active	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

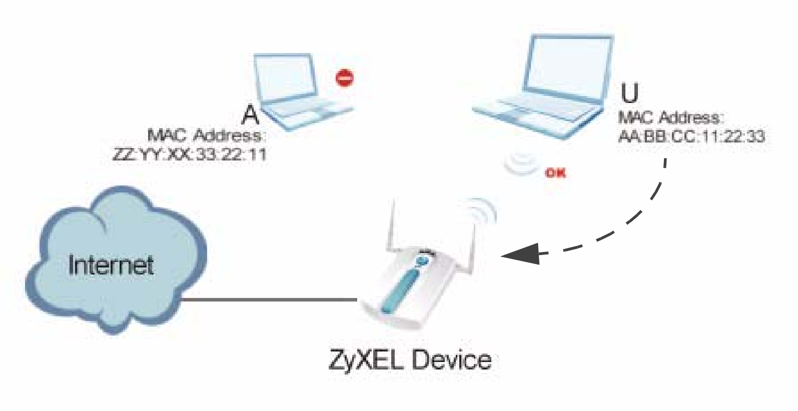
MAC Filter Screen

9.1 Overview

This chapter discusses how you can use the **Wireless > MAC Filter** screen.

The MAC filter function allows you to configure the ZyXEL Device to grant access to the ZyxEL Device from other wireless devices (Allow Association) or exclude devices from accessing the ZyXEL Device (Deny Association).

Figure 44 MAC Filtering



In the figure above, wireless client U is able to connect to the Internet because its MAC address is in the allowed association list specified in the ZyXEL Device. The MAC address of client A is either denied association or is not in the list of allowed wireless clients specified in the ZyXEL Device.

9.2 What You Can Do in the MAC Filter

Use the **Wireless > MAC Filter** screen (see Section 9.4 on page 94) to specify which wireless station is allowed or denied access to the ZyXEL Device.

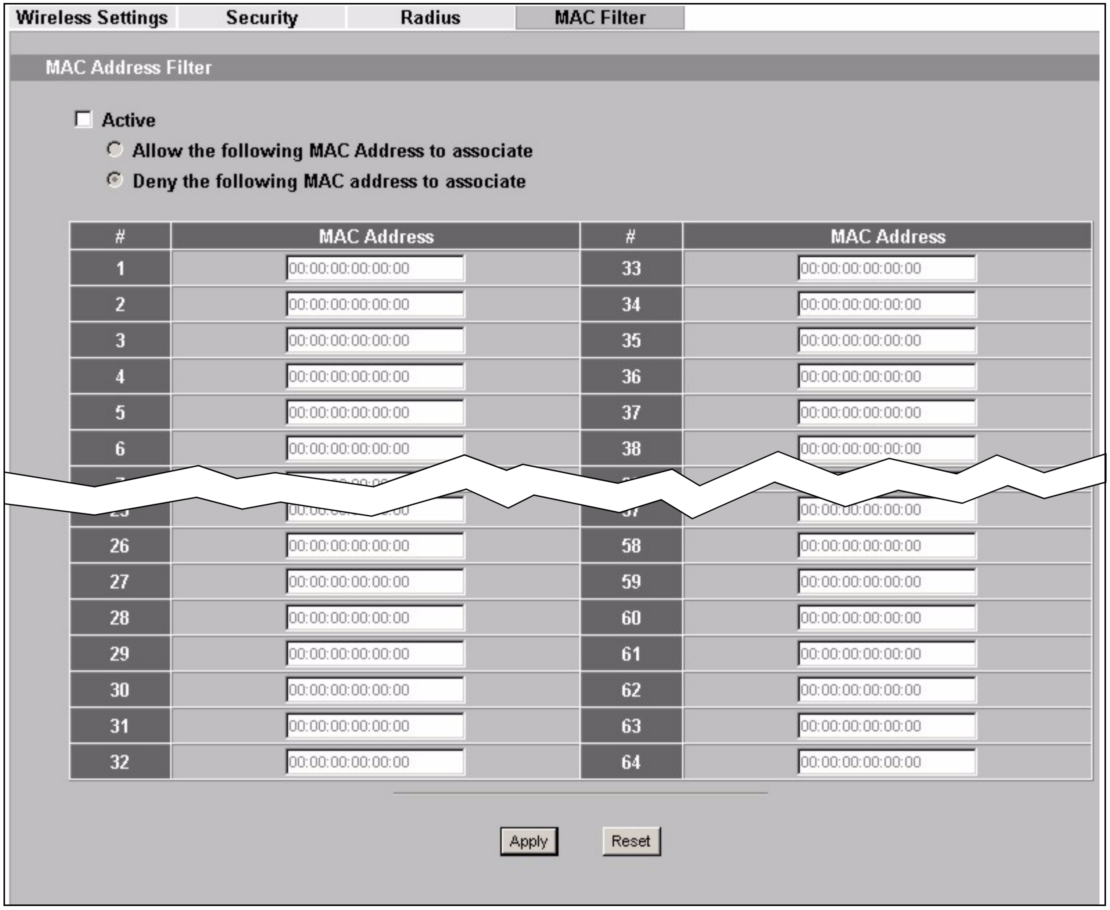
9.3 What You Need To Know About MAC Filter

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of each device to configure MAC filtering on the ZyXEL Device.

9.4 MAC Filter Screen

Use this screen to enable MAC address filtering in your ZyXEL Device.You can specify up to 64 MAC addresses to either allow or deny association with your ZyXEL Device. Click **Wireless > MAC Filter**. The screen displays as shown.

Figure 45 Wireless > MAC Filter



□ Active

○ Allow the following MAC Address to associate

● Deny the following MAC address to associate

#	MAC Address	#	MAC Address
1	00:00:00:00:00:00	33	00:00:00:00:00:00
2	00:00:00:00:00:00	34	00:00:00:00:00:00
3	00:00:00:00:00:00	35	00:00:00:00:00:00
4	00:00:00:00:00:00	36	00:00:00:00:00:00
5	00:00:00:00:00:00	37	00:00:00:00:00:00
6	00:00:00:00:00:00	38	00:00:00:00:00:00
25	00:00:00:00:00:00	57	00:00:00:00:00:00
26	00:00:00:00:00:00	58	00:00:00:00:00:00
27	00:00:00:00:00:00	59	00:00:00:00:00:00
28	00:00:00:00:00:00	60	00:00:00:00:00:00
29	00:00:00:00:00:00	61	00:00:00:00:00:00
30	00:00:00:00:00:00	62	00:00:00:00:00:00
31	00:00:00:00:00:00	63	00:00:00:00:00:00
32	00:00:00:00:00:00	64	00:00:00:00:00:00

The following table describes the labels in this screen.

Table 26 Wireless > MAC Filter

LABEL	DESCRIPTION
Active	Click this to enable this feature.
Allow the following MAC Address to associate	Define the filter action for the list of MAC addresses in the MAC address filter table. Select this to permit access to the ZyXEL Device. MAC addresses not listed will be denied access to the ZyXEL Device.
Deny the following MAC Address to associate	Select this to block access to theZyXEL Device. MAC addresses not listed will be allowed to access the ZyXEL Device.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station to be allowed or denied access to the ZyXEL Device.
Description	Type a name to identify this wireless station.

Table 26 Wireless > MAC Filter

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

10

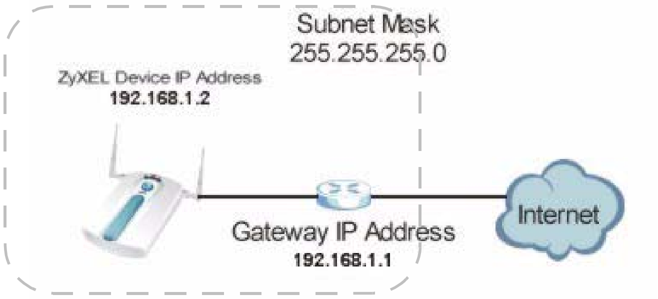
IP Screen

10.1 Overview

This chapter describes how you can configure the IP address of your ZyXEL Device.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Figure 46 IP Setup



The figure above illustrates one possible setup of your ZyXEL Device. The gateway IP address is 192.168.1.2 and the IP address of the ZyXEL Device is 192.168.1.2 (default). The gateway and the device must belong in the same subnet mask to be able to communicate with each other.

10.2 What You Can Do in the IP Screen

Use the **IP** screen (see Section 10.4 on page 98) to configure the IP address of your ZyXEL Device.

10.3 What You Need to Know About IP

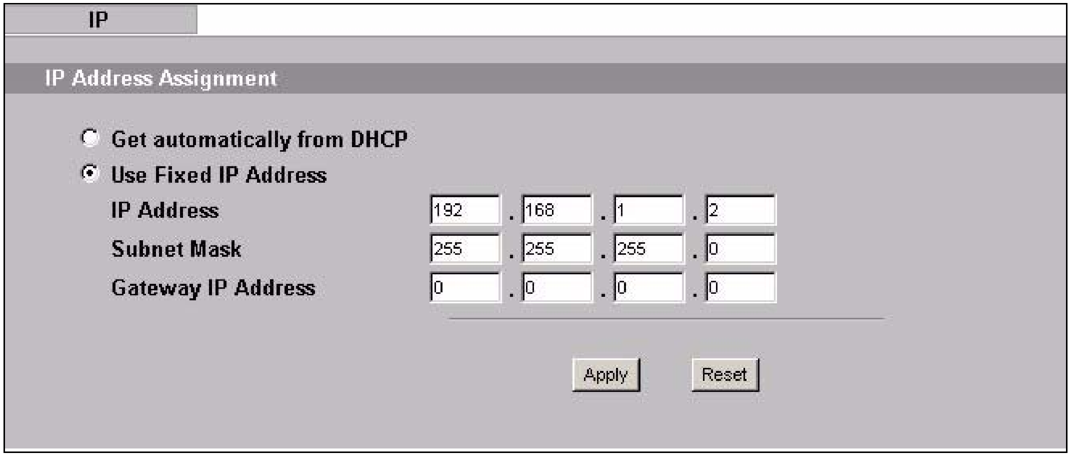
The Ethernet parameters of the ZyXEL Device are preset in the factory with the following values:

1. IP address of 192.168.1.2
2. Subnet mask of 255.255.255.0 (24 bits)

10.4 IP Screen

Use this screen to configure the IP address for your ZyXEL Device. Click **IP** to display the following screen.

Figure 47 IP Setup



○ Get automatically from DHCP
● Use Fixed IP Address
IP Address 192 . 168 . 1 . 2
Subnet Mask 255 . 255 . 255 . 0
Gateway IP Address 0 . 0 . 0 . 0

The following table describes the labels in this screen.

Table 27 IP Setup

LABEL	DESCRIPTION
IP Address Assignment	
Get automatically from DHCP	Select this option if your ZyXEL Device is using a dynamically assigned IP address from a DHCP server each time. **Note: You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again.**
Use fixed IP address	Select this option if your ZyXEL Device is using a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. **Note: If you change the ZyXEL Device's IP address, you must use the new IP address if you want to access the web configurator again.**
Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

10.5 Technical Reference

This section provides the technical background information about the topics covered in this chapter.

10.5.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet (only between your two branch offices, for instance) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 28 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

11

Remote Management

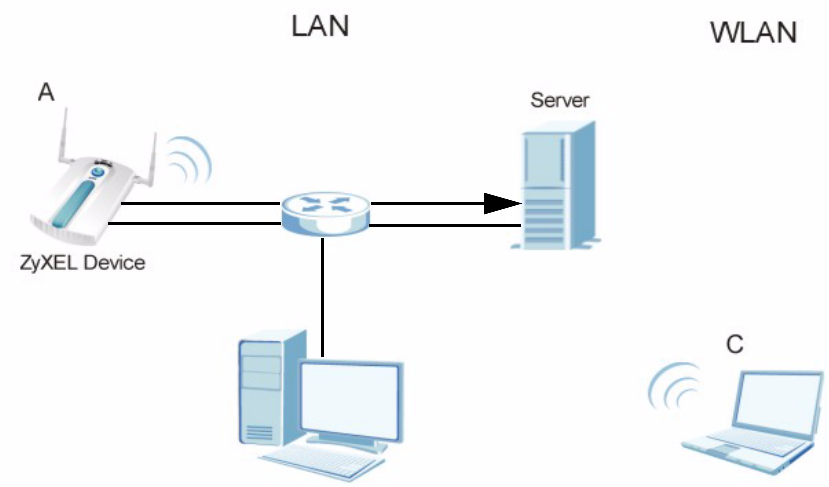
11.1 Overview

This chapter shows you how to enable remote management of your ZyXEL Device. It provides information on determining which services or protocols can access which of the ZyXEL Device's interfaces.

Remote Management allows a user to administrate the device over the network. You can manage your ZyXEL Device from a remote location via the following interfaces:

- WLAN
- LAN
- Both WLAN and LAN
- Neither (Disable)

Figure 48 Remote Management Example



In the figure above, the ZyXEL Device (A) is being managed by a desktop computer (B) connected via LAN (Land Area Network). It is also being accessed by a notebook (C) connected via WLAN (Wireless LAN).

11.2 What You Can Do in the Remote Management Screens

- Use the **Telnet** screen (see Section 11.4 on page 104) to configure through which interface(s) and from which IP address(es) you can use Telnet to manage the ZyXEL Device. A Telnet connection is prioritized by the ZyXEL Device over other remote management sessions.
- Use the **FTP** screen (see Section 11.5 on page 104) to configure through which interface(s) and from which IP address(es) you can use File Transfer Protocol (FTP) to manage the ZyXEL Device. You can use FTP to upload the latest firmware for example.
- Use the **WWW** screen (see Section 11.6 on page 105) to configure through which interface(s) and from which IP address(es) you can use the Web Browser to manage the ZyXEL Device.
- Use the **SNMP** screen (see Section 11.7 on page 106) to configure through which interface(s) and from which IP address(es) a network systems manager can access the ZyXEL Device.

11.3 What You Need To Know About Remote Management

Telnet

Telnet is short for Telecommunications Network, which is a client-side protocol that enables you to access a device over the network.

FTP

File Transfer Protocol (FTP) allows you to upload or download a file or several files to and from a remote location using a client or the command console.

WWW

The World Wide Web allows you to access files hosted in a remote server. For example, you can view text files (usually referred to as ‘pages’) using your web browser via HyperText Transfer Protocol (HTTP).

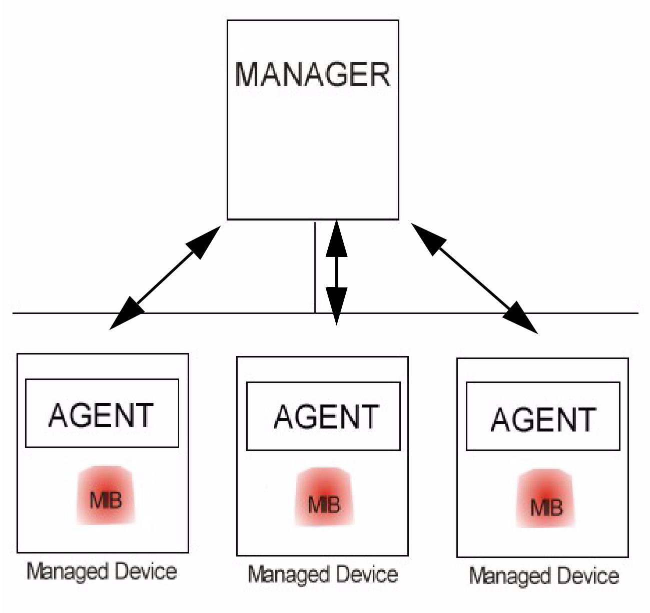
SNMP

Simple Network Management Protocol (SNMP) is a member of the TCP/IP protocol suite used for exchanging management information between network devices.

Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation. .

SNMP is only available if TCP/IP is configured.

Figure 49 SNMP Management Mode



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

SNMP allows a manager and agents to communicate for the purpose of accessing information such as packets received, node port status, etc.

Remote Management Limitations

Remote management over LAN or WLAN will not work when:

- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- You may only have one remote management session running at one time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows:
  1. Telnet
  2. HTTP

System Timeout

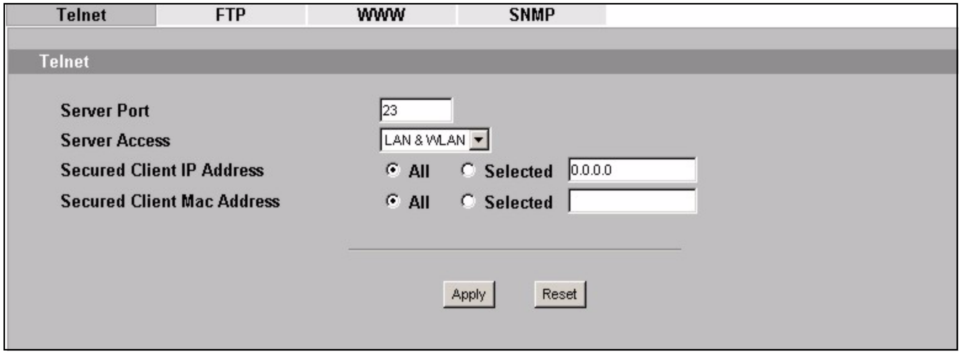
There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **SYSTEM** screen.

11.4 The Telnet Screen

Use this screen to configure your ZyXEL Device for remote Telnet access. You can use Telnet to access the ZyXEL Device's Command Line Interface (CLI).

Click **REMOTE MGNT** > **TELNET**. The following screen displays.

Figure 50 Remote Management: Telnet



Server Port: 23

Server Access: LAN & WLAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Secured Client Mac Address: ● All ○ Selected

The following table describes the labels in this screen.

Table 29 Remote Management: Telnet

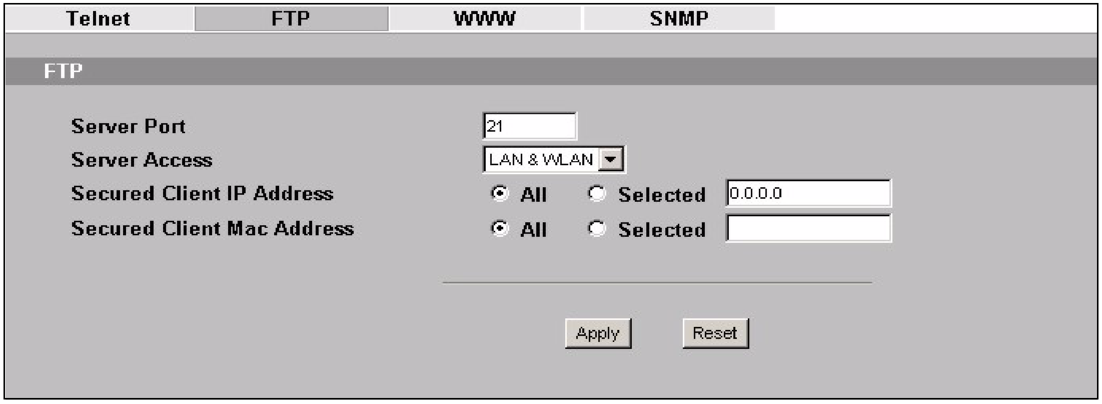
LABEL	DESCRIPTION
TELNET	
Server Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using Telnet.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 The FTP Screen

Use this screen to upload and download the ZyXEL Device's firmware using FTP. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device's FTP settings, click **REMOTE MGMT** > **FTP**. The following screen displays.

Figure 51 Remote Management: FTP



FTP

Server Port 21

Server Access LAN & WLAN

Secured Client IP Address ● All ○ Selected 0.0.0.0

Secured Client Mac Address ● All ○ Selected

The following table describes the labels in this screen.

Table 30 Remote Management: FTP

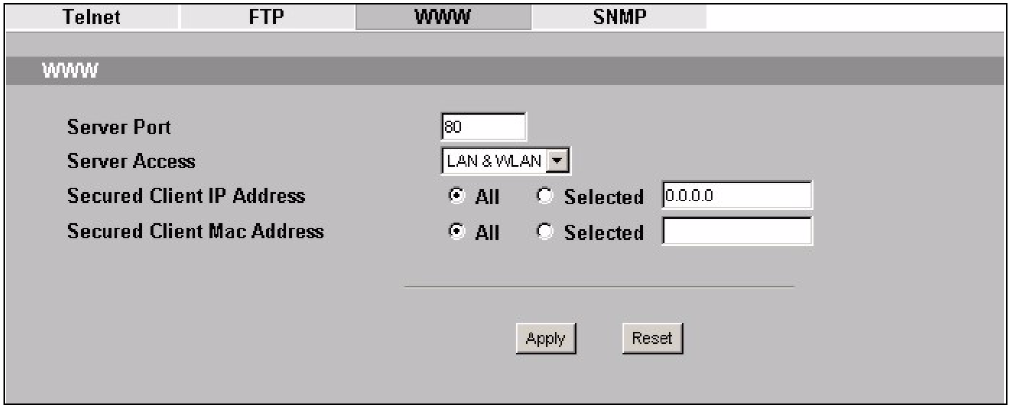
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.6 The WWW Screen

Use this screen to configure your ZyXEL Device via the World Wide Web **(WWW)** using a Web browser. This lets you specify which IP addresses or computers are able to communicate with and access the ZyXEL Device.

To change your ZyXEL Device’s **WWW** settings, click **REMOTE MGNT** > **WWW**. The following screen shows.

Figure 52 Remote Management: WWW



WWW

Server Port: 80

Server Access: LAN & WLAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Secured Client Mac Address: ● All ○ Selected

The following table describes the labels in this screen.

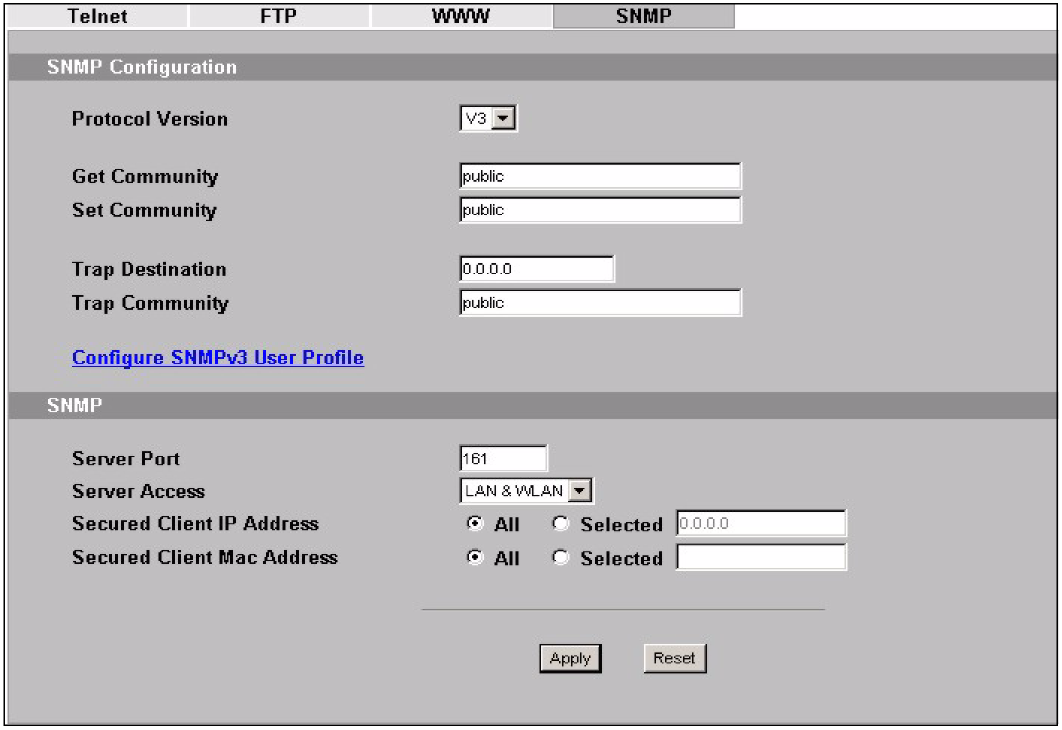
Table 31 Remote Management: WWW

LABEL	DESCRIPTION
WWW	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.7 The SNMP Screen

Use this screen to have a manager station administrate your ZyXEL Device over the network. To change your ZyXEL Device’s SNMP settings, click **REMOTE MGMT** > **SNMP**. The following screen displays.

Figure 53 Remote Management: SNMP



SNMP Configuration

Protocol Version: V3

Get Community: public

Set Community: public

Trap Destination: 0.0.0.0

Trap Community: public

Configure SNMPv3 User Profile

SNMP

Server Port: 161

Server Access: LAN & WLAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Secured Client Mac Address: ● All ○ Selected

The following table describes the labels in this screen.

Table 32 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is “public” and allows all requests. This field is available only when **SNMPv1** or **SNMPv2** is selected in the **SNMP Version** field.
Configure SNMPv3 User Profile	Click this to go to the **SNMPv3 User Profile** screen, where you can configure administration and user login details.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.

Table 32 Remote Management: SNMP

LABEL	DESCRIPTION
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.8 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

11.8.1 MIB

Managed devices in an SMNP managed network contain object variables or managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects.SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

11.8.2 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215 as well as the proprietary ZyXEL private MIB. The purpose of the MIBs is to let administrators collect statistical data and monitor status and performance.

11.8.3 SNMP Traps

SNMP traps are messages sent by the agents of each managed device to the SNMP manager. These messages inform the administrator of events in data networks handled by the device. The ZyXEL Device can send the following traps to the SNMP manager.

Table 33 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.

Table 33 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure (defined in *RFC-1215*)	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password). Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.
pwTFTPStatus	1.3.6.1.4.1.890.1.9.2.3.3.1	This trap is sent to indicate the status and result of a TFTP client session that has ended.

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ZyXEL Device's physical and virtual ports.

Table 34 SNMP Interface Index to Physical and Virtual Port Mapping

TYPE	INTERFACE	PORT
Physical	enet0	Wireless LAN adaptor WLAN1
	enet1	Ethernet port (LAN)
	enet2	Wireless LAN adaptor WLAN2
Virtual	enet3 ~ enet9	WLAN1 in MBSSID mode
	enet10 ~ enet16	WLAN2 in MBSSID mode
	enet17 ~ enet21	WLAN1 in WDS mode
	enet22 ~ enet26	WLAN2 in WDS mode

12

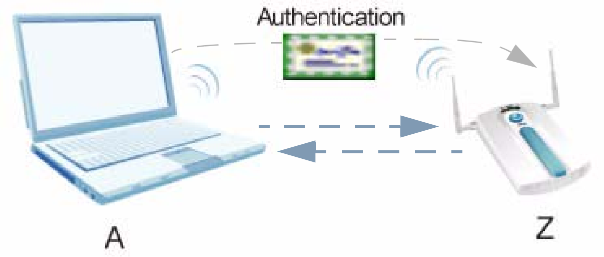
Certificate Screen

12.1 Overview

This chapter describes how your ZyXEL Device can use certificates as a means of authenticating wireless clients. It gives background information about public-key certificates and explains how to use them.

A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Figure 54 Certificates Example



In the figure above, the ZyXEL Device (Z) checks the identity of the notebook (A) using a certificate before granting access to the network.

12.2 What You Can Do in the Certificate Screen

Use the **CERTIFICATES** > **Certificate** screen (seen Section 12.4 on page 112) to view, delete and import certificates.

12.3 What You Need To Know About Certificates

The certification authority certificate that you can import to your ZyXEL Device should be in PFX PKCS#12 file format. This format referred to as the Personal Information Exchange Syntax Standard is comprised of a private key-public certificate pair that is further encrypted with a password. Before you import a certificate into the ZyXEL Device, you should verify that you have the correct certificate.

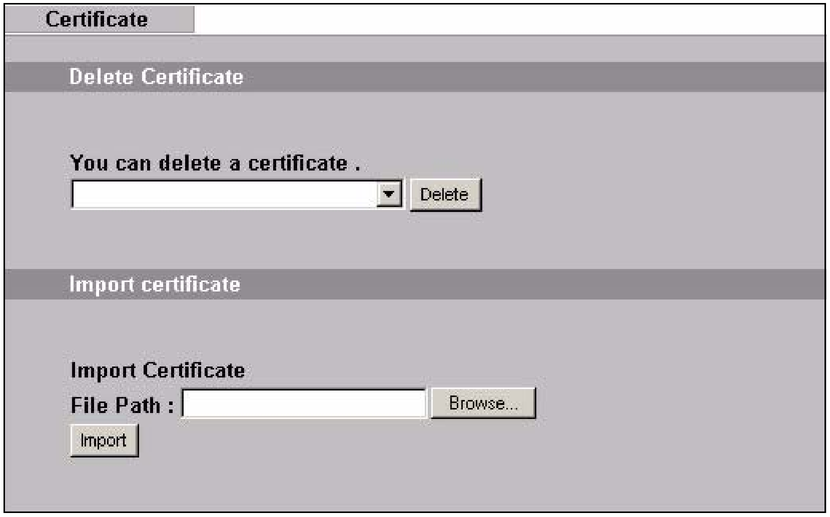
Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

12.4 Certificate Screen

Use this screen to view, delete and import certificates.

Click **CERTIFICATE** to open the ZyXEL Device's summary list of certificates and to import a new certificate. See the following figure.

Figure 55 Certificate



The following table describes the labels in this screen.

Table 35 Certificate

LABEL	DESCRIPTION
Delete Certificate	
You can delete a certificate	Select the certificate from the list that you want to delete.
Delete	Click this to delete the selected certificate.
Import Certificate	
File Path	Enter the location of a previously-saved certificate to upload to the ZyXEL Device. Alternatively, click the **Browse** button to locate a list.
Browse	Click this button to locate a previously-saved certificate to upload to the ZyXEL Device.
Import	Click this button to upload the previously-saved certificate displayed in the **File Path** field to the ZyXEL Device.

12.5 Technical Reference

This section provides technical background information about the topics covered in this chapter.

12.5.1 Private-Public Certificates

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as “digital signatures”). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key “writes” your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3 Tim uses his private key to sign the message and sends it to Jenny.
4 Jenny receives the message and uses Tim’s public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim’s private key).
5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny’s public key to verify the message.

12.5.2 Certification Authorities

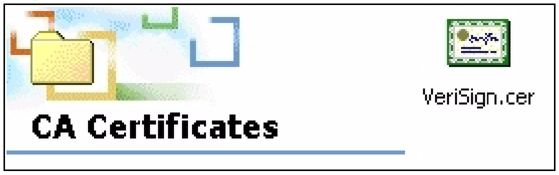
A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

12.5.3 Checking the Fingerprint of a Certificate on Your Computer

A certificate’s fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate’s fingerprint to verify that you have the actual certificate.

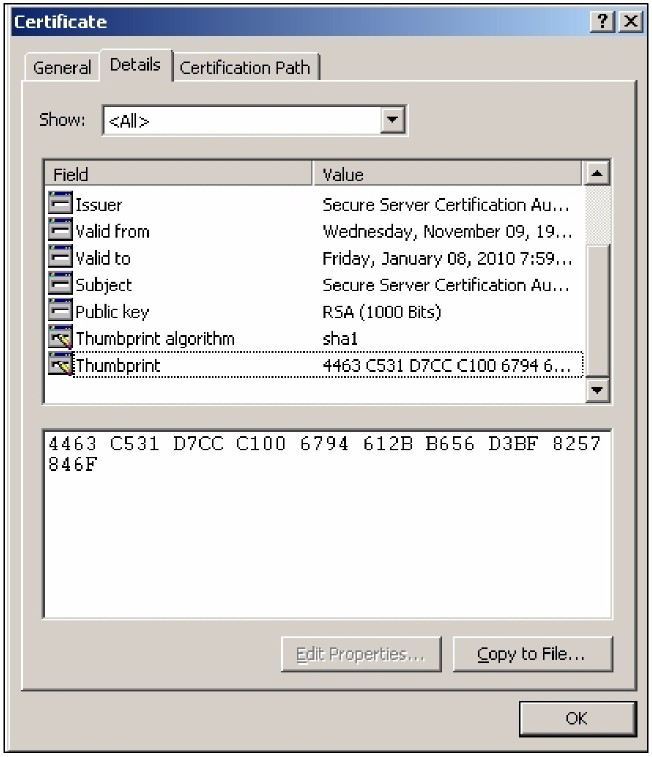
1 Browse to where you have the certificate saved on your computer.
2 Make sure that the certificate has a “.cer” or “.crt” file name extension.

Figure 56 Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 57 Certificate Details



Show: <All>

Field	Value
Issuer	Secure Server Certification Au...
Valid from	Wednesday, November 09, 19...
Valid to	Friday, January 08, 2010 7:59...
Subject	Secure Server Certification Au...
Public key	RSA (1000 Bits)
Thumbprint algorithm	sha1
Thumbprint	4463 C531 D7CC C100 6794 6...

```
4463 C531 D7CC C100 6794 612B B656 D3BF 8257
846F
```

4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary according to your situation. Possible examples would be over the telephone or through an HTTPS connection.

13

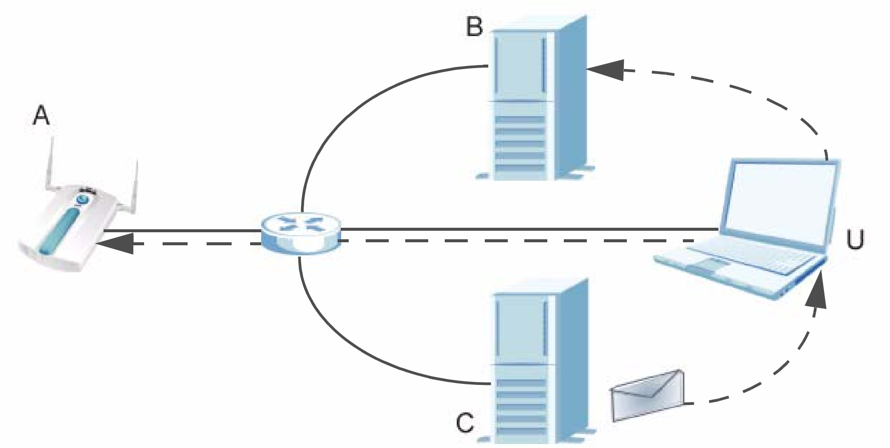
Log Screens

13.1 Overview

This chapter provides information on viewing and generating logs on your ZyXEL Device.

Logs are files that contain recorded network activity over a set period. They are used by administrators to monitor the health of the system(s) they are managing. Logs enable administrators to effectively monitor events, errors, progress, etc. so that when network problems or system failures occur, the cause or origin can be traced. Logs are also essential for auditing and keeping track of changes made by users.

Figure 58 Accessing Logs in the Network



The figure above illustrates three ways to access logs. The user **(U)** can access logs directly from the ZyXEL Device **(A)** via the Web configurator. Logs can also be located in an external log server **(B)**. An email server **(C)** can also send harvested logs to the user's email account.

13.2 What You Can Do in the Log Screens

- Use the **View Log** screen (Section 13.4 on page 116) to display all logs or logs for a certain category. You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted.
- Use the **Log Settings** screen (Section 13.5 on page 117) to configure where and when the ZyXEL Device will send the logs, and which logs and/or immediate alerts it will send.

13.3 What You Need To Know About Logs

Alerts and Logs

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You can differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

Receiving Logs via E-mail

If you want to receive logs in your e-mail account, you need to have the necessary details ready, such as the Server Name or Simple Mail Transfer Protocol (SMTP) Address of your e-mail account. Ensure that you have a valid e-mail address.

Enabling Syslog Logging

To enable Syslog Logging, obtain your Syslog server's IP address (or server name).

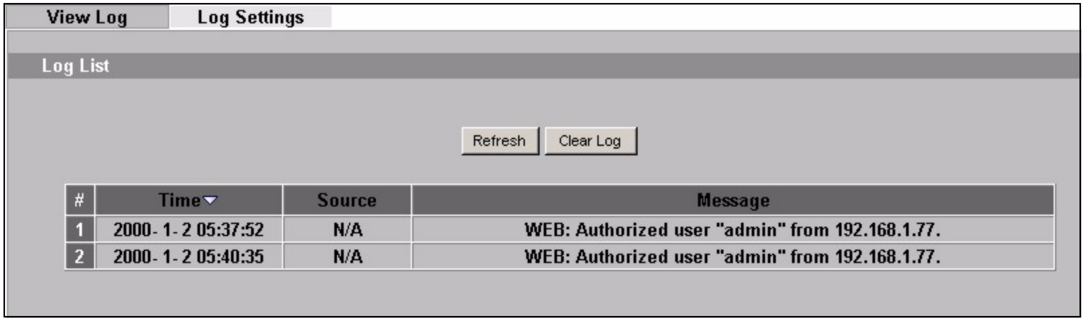
13.4 View Log Screen

Use this screen to view all the ZyXEL Device's logs in one location.

Click **Logs > View Log**. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Figure 60 on page 117). Options include logs about system maintenance, system errors and access control.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

Figure 59 View Log



#	Time▽	Source	Message
1	2000- 1- 2 05:37:52	N/A	WEB: Authorized user "admin" from 192.168.1.77.
2	2000- 1- 2 05:40:35	N/A	WEB: Authorized user "admin" from 192.168.1.77.

The following table describes the labels in this screen.

Table 36 View Log

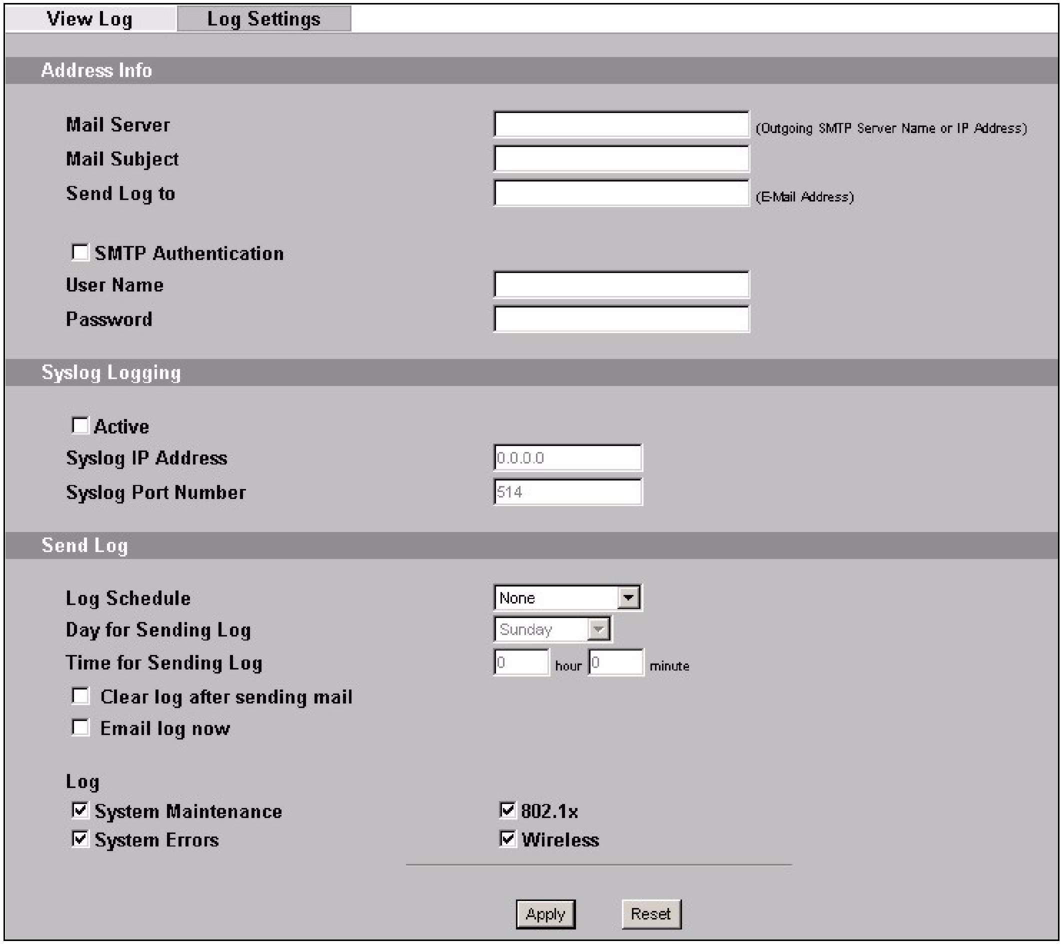
LABEL	DESCRIPTION
Time	This field displays the time the log was recorded.
Source	This field lists the source IP address and the port number of the incoming packet.
Message	This field states the reason for the log.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.

13.5 Log Settings Screen

Use this screen to configure to where and when the ZyXEL Device is to send the logs and which logs and/or immediate alerts it is to send.

To change your ZyXEL Device’s log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Figure 60 Log Settings



Address Info

Mail Server		(Outgoing SMTP Server Name or IP Address)
Mail Subject		
Send Log to		(E-Mail Address)
□ SMTP Authentication		
User Name		
Password		

Syslog Logging

□ Active	
Syslog IP Address	0.0.0.0
Syslog Port Number	514

Send Log

Log Schedule	None
Day for Sending Log	Sunday
Time for Sending Log	0 hour 0 minute
□ Clear log after sending mail	
□ Email log now	

Log

☑ System Maintenance	☑ 802.1x
☑ System Errors	☑ Wireless

The following table describes the labels in this screen.

Table 37 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
SMTP Authentication	If you use SMTP authentication, the mail receiver should be the owner of the SMTP account.

Table 37 Log Settings

LABEL	DESCRIPTION
User Name	If your e-mail account requires SMTP authentication, enter the username here.
Password	Enter the password associated with the above username.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the IP address of the syslog server that will log the selected categories of logs.
Syslog Port Number	Enter the port number of the syslog server that will log the selected categories of logs.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Email log now	Select the categories of alerts for which you want the ZyXEL Device to immediately send e-mail alerts.
Log	
System Maintenance	Click this to receive logs related to system maintenance.
System Errors	Click this to receive logs related to system errors.
802.1x	Click this to receive logs related to the 802.1x mode.
Wireless	Click this to receive logs related to the wireless function.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to reconfigure all the fields in this screen.

13.6 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

13.6.1 Example Log Messages

The following tables provide descriptions of some example log messages that the ZyXEL Device generates.

Table 38 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`WLAN: Radar interference 2412 MHz.`	Wireless driver receives radar pulse at center frequency 2412 MHz.
`WLAN: CW interference 2412 MHz.`	Wireless driver receives noise interference pulse at center frequency 2412 MHz.
`WLAN service started.`	Wireless port ath0 started.
`WLAN service stopped.`	Wireless port ath0 stopped.
`AP MIC failed.`	Wireless driver MIC checked failed.
`AP MIC attacked.`	Wireless driver received MIC attack packet.
`Station authenticated.`	AP received the request for authentication from station and authenticated the station successfully.
`Station authentication failed.`	AP received the request for authentication from station but the authentication failed.
`Station deauthenticated.`	AP receive the deauthenticated packet from the STA which connected with AP.
`Station associated.`	AP receive the association request packet from the STA which connected with AP.
`Station disassociated.`	AP receive the disassociation request packet from the STA, which connected with AP.
`Station refused.`	A STA wanted to connect to the AP but was refused.
`Remote Bridge AP configured.`	Remote AP MAC address was configured.
`Remote Bridge AP deleted.`	Remote AP MAC address was deleted.
`CLI: Authorized user from IP.`	A device succesfully logs into the AP via Telnet (the device’s IP address shows in the log message.)
`CLI: Unauthorized user from IP.`	A device fails to log into the AP via Telnet (the device’s IP address shows in the log message.)
`WEB: Authorized user from IP.`	A device successfully logs into the AP via WWW (the device’s IP address shows in the log message.)
`WEB: Unauthorized user from IP.`	A device fails to log into the AP via WWW (the device’s IP address shows in the log message.)

13.7 Log Commands

Go to the command interpreter interface (refer to Appendix I on page 187 for the Command Interpreter appendix explains how to access and use the commands).

13.7.1 Configuring What You Want the ZyXEL Device to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Table 39 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
error	0, 1, 2, 3
mten	0, 1
Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

13.7.2 Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.

Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

13.7.3 Command List

The following table provides the commands that can be used for your ZyXEL Device to configure the log settings.

Table 40 Log Command List

KEYWORD	DESCRIPTION
`client`	Enable SYSLOG client
`ipaddr`	SYSLOG server IP address
`port`	SYSLOG server port
`Email server`	E-mail server address
`Email subject`	E-mail subject
`Email Address`	E-mail address
`Email SmtpAuthEnable`	SMPTP auth enable when e-mail log
`Email User`	E-mail user name
`Email Password`	E-mail password
`Email Schedule`	E-mail schedule mode
`Email Day`	E-mail schedule day
`Email Hour`	E-mail schedule hour
`Email Minute`	E-mail schedule minute
`Email Clear`	Clear log after e-mail
`Email Now`	Send e-mail now

14

Maintenance

14.1 Overview

This chapter describes the maintenance screens. It discusses how you can view the association list and channel usage, upload new firmware, manage configuration and restart your ZyXEL Device without turning it off and on.

14.2 What You Can Do in the Maintenance Screens

- Use the **Association List** screen (see Section 14.4 on page 121) to view the wireless stations that are currently associated with the ZyXEL Device.
- Use the **Channel Usage** screen (see Section 14.5 on page 122) to view whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.
- Use the **F/W Upload** screen (see Section 14.6 on page 123) to upload the latest firmware for your ZyXEL Device.
- Use the **Configuration** screen (see Section 14.7 on page 124) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use **Restart** screen (see Section 14.8 on page 127) to reboot the ZyXEL Device without turning the power off.

14.3 What You Need To Know About the Maintenance Screens

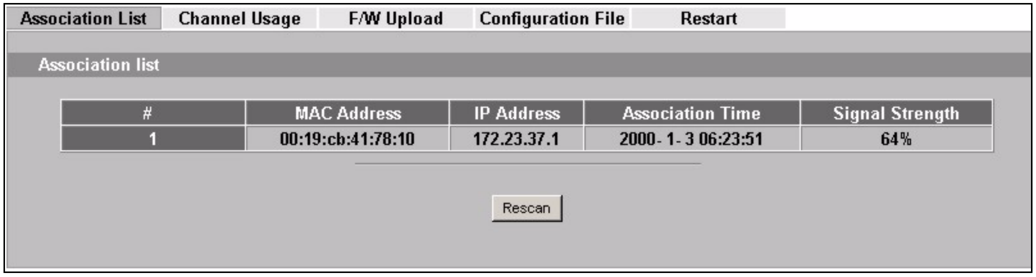
You can find the firmware for your device at www.zyxel.com. It is a file that (usually) uses the system model name with a "*.bin" extension, for example "NWA-1100.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

14.4 Association List Screen

Use this screen to view the wireless stations that are currently associated with the ZyXEL Device.

Click **Maintenance** > **Association List**. The following screen displays.

Figure 61 Association List



#	MAC Address	IP Address	Association Time	Signal Strength
1	00:19:cb:41:78:10	172.23.37.1	2000- 1- 3 06:23:51	64%

The following table describes the labels in this screen.

Table 41 Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
IP Address	This identifies the individual devices on a network.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Signal Strength	This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.
Rescan	Click **Rescan** to reload the screen.

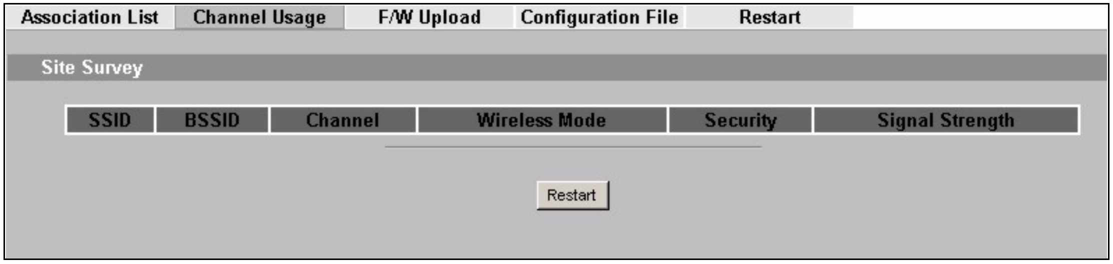
14.5 Channel Usage Screen

Use this screen to know whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **Maintenance** > **Channel Usage** to display the screen shown next.

Wait a moment while the ZyXEL Device compiles the information.

Figure 62 Channel Usage



SSID	BSSID	Channel	Wireless Mode	Security	Signal Strength

The following table describes the labels in this screen.

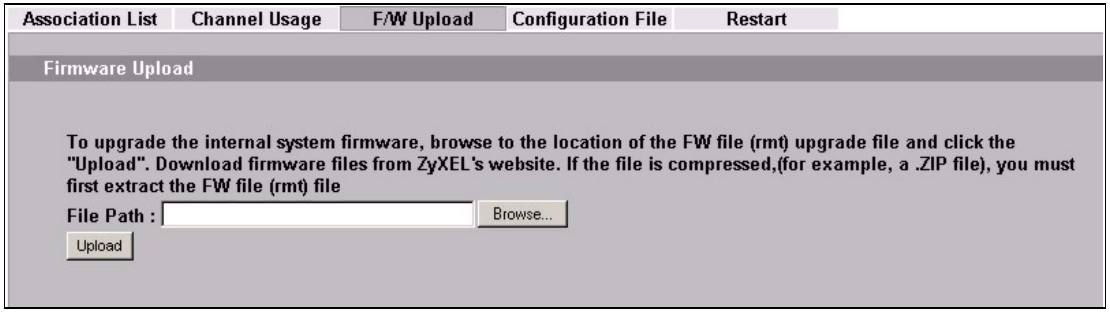
Table 42 Channel Usage

LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the chapter on wireless configuration for more information on basic service sets (BSS) and extended service sets (ESS).
BSSID	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Wireless Mode	This is the IEEE 802.1x standard used by your ZyXEL Device to apply enhanced security methods for both the authentication of wireless stations and encryption key management.
Security	This is the wireless security method used by your ZyXEL Device protect wireless communication between wireless stations, access points and the wired network.
Restart	Click **Restart** to reload the screen.

14.6 F/W Upload Screen

Use this screen to upload a firmware to your ZyXEL Device. Click **Maintenance** > **F/W Upload**. Follow the instructions in this section to upload firmware to your ZyXEL Device.

Figure 63 Firmware Upload



To upgrade the internal system firmware, browse to the location of the FW file (rmt) upgrade file and click the "Upload". Download firmware files from ZyXEL's website. If the file is compressed,(for example, a .ZIP file), you must first extract the FW file (rmt) file

File Path :

The following table describes the labels in this screen.

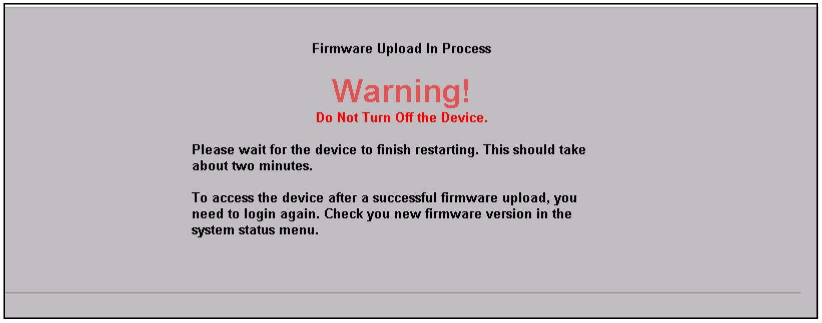
Table 43 Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Do not turn off the ZyXEL Device while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 64 Firmware Upload In Process



Firmware Upload In Process

Warning!

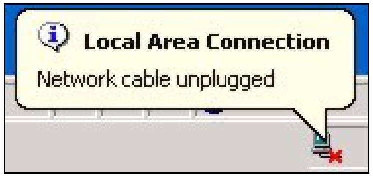
Do Not Turn Off the Device.

Please wait for the device to finish restarting. This should take about two minutes.

To access the device after a successful firmware upload, you need to login again. Check you new firmware version in the system status menu.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 65 Network Temporarily Disconnected



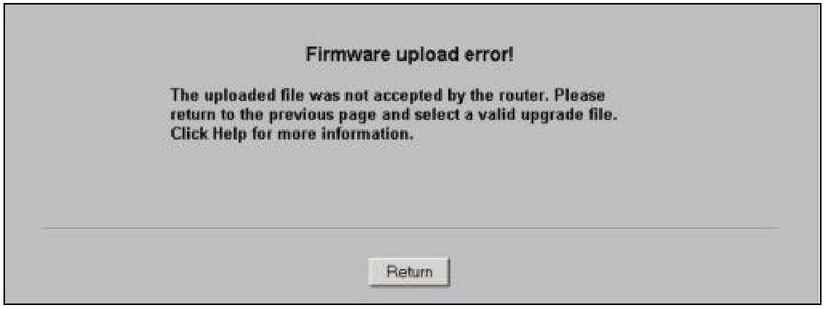
Local Area Connection

Network cable unplugged

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 66 Firmware Upload Error



Firmware upload error!

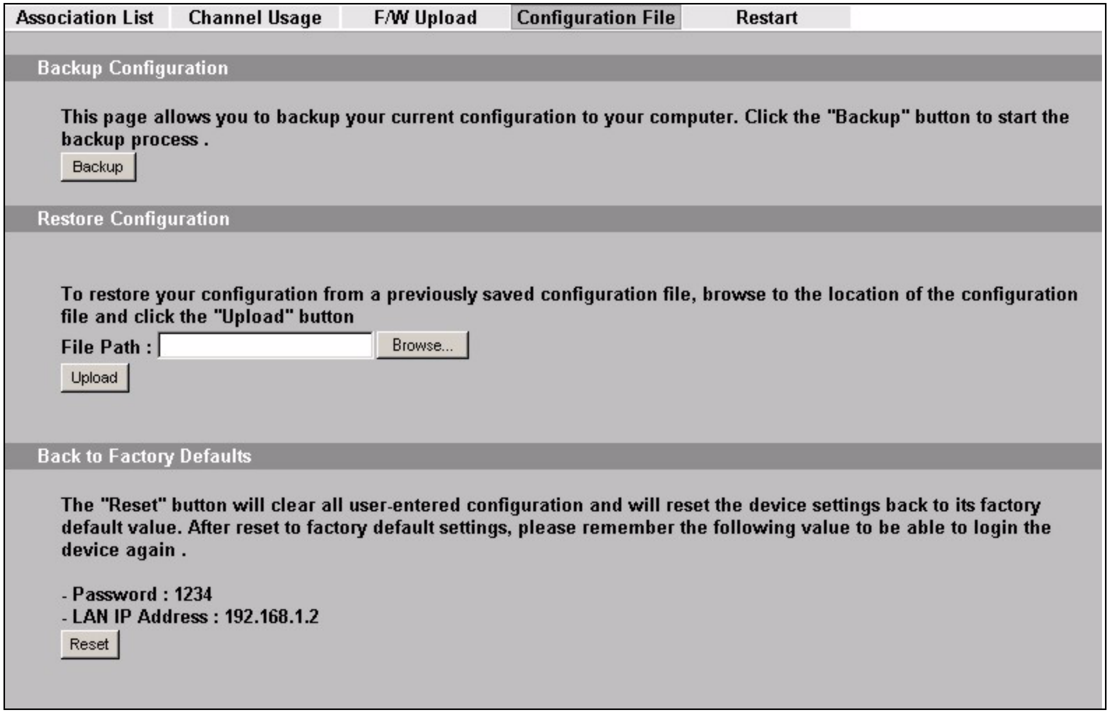
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

14.7 Configuration Screen

Use this screen to backup, restore and reset the configuration of your ZyXEL Device.

Click **Maintenance** > **Configuration**. The screen appears as shown next.

Figure 67 Configuration



Backup Configuration

This page allows you to backup your current configuration to your computer. Click the "Backup" button to start the backup process .

Restore Configuration

To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the "Upload" button

File Path :

Back to Factory Defaults

The "Reset" button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following value to be able to login the device again .

- Password : 1234
- LAN IP Address : 192.168.1.2

14.7.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyXEL Device’s current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device’s current configuration to your computer.

14.7.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

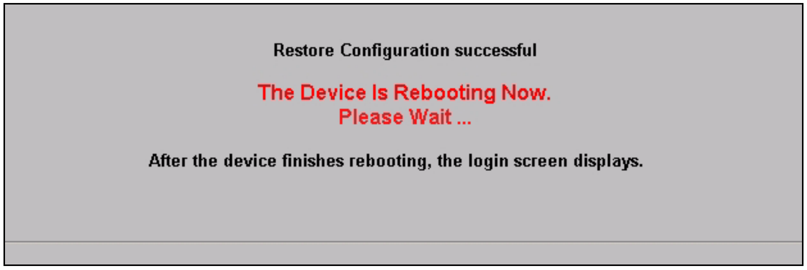
Table 44 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 68 Configuration Upload Successful



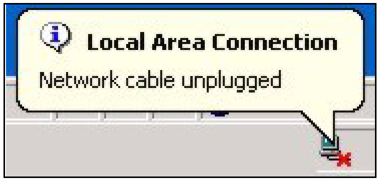
Restore Configuration successful

The Device Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 69 Network Temporarily Disconnected

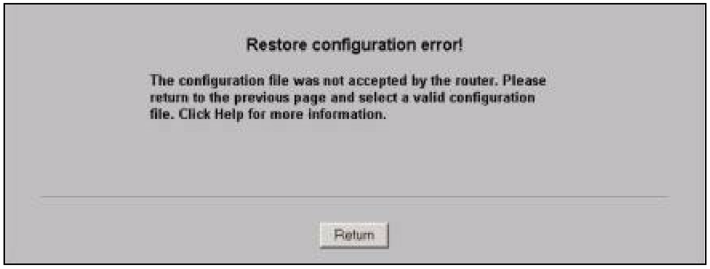


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.2). See your Quick Start Guide for details on how to set up your computer’s IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 70 Configuration Upload Error



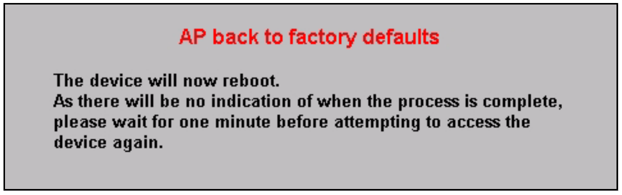
Restore configuration error!

The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.

14.7.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 71 Reset Warning Message



AP back to factory defaults

The device will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the device again.

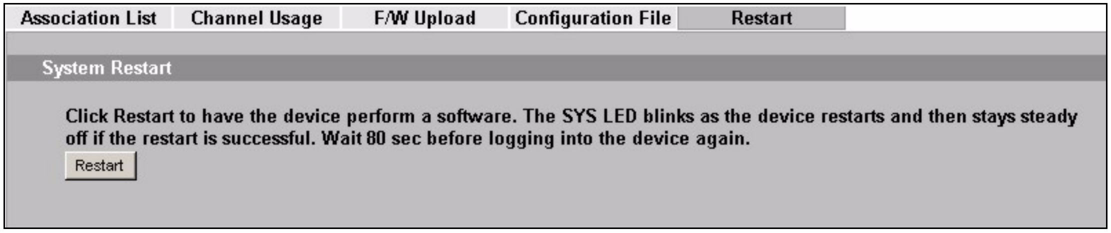
You can also press the **RESET** button to reset your ZyXEL Device to its factory default settings. Refer to Section 2.2 on page 36 for more information.

14.8 Restart Screen

Use this screen to reboot the ZyXEL Device without turning the power off.

Click **Maintenance** > **Restart**. The following screen displays.

Figure 72 Restart Screen



Click Restart to have the device perform a software. The SYS LED blinks as the device restarts and then stays steady off if the restart is successful. Wait 80 sec before logging into the device again.

Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

15

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access

15.1 Power, Hardware Connections, and LEDs

?

The ZyXEL Device does not turn on. None of the LEDs turn on.

1 Make sure you are using the power adaptor or cord included with the ZyXEL Device.
2 Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.
4 If the problem continues, contact the vendor.

?

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 1.7 on page 32.
2 Check the hardware connections. See the Quick Start Guide.
3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4 Disconnect and re-connect the power adaptor to the ZyXEL Device.
5 If the problem continues, contact the vendor.

15.2 ZyXEL Device Access and Login

?

I forgot the IP address for the ZyXEL Device.

1 The default IP address is **192.168.1.2**.
2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter "**cmd**", and then enter "**ipconfig**". The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
3 If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 36.

I forgot the password.

1 The default password is **1234**.
2 If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 36.

I cannot see or access the Login screen in the web configurator.

1 Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.2.
   - If you changed the IP address (Section 10.4 on page 98), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.
2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 32.
3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Section 15.1 on page 129.
4 Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device.
5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See your Quick Start Guide.
6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the Login screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.
2 You cannot log in to the web configurator while someone is using the Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.
3 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.
4 If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 36.

I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

15.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 15.1 on page 129.
2 2. Make sure your ZyXEL Device is connected to a networking device that provides Internet access.
3 If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the AP.
4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 32.
2 Reboot the ZyXEL Device.

3 If the problem continues, contact your ISP or network administrator.

?

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.7 on page 32. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal is weak, try moving the ZyXEL Device (in wireless client mode) closer to the AP (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).

3 Reboot the ZyXEL Device.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it.

PART III
Appendices and Index

A

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 45 Hardware Specifications

Power Specification	12 V DC, 1 A
Reset button	Returns all settings to their factory defaults.
Ethernet Port	• Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. • Auto-crossover: Use either crossover or straight-through Ethernet cables.
Power over Ethernet (PoE)	IEEE 802.3af compliant.
Antenna	SMA antenna connectors, equipped by default with 3dBi omni antenna, 60°
Operation Temperature	0 ~ 50 ° C
Storage Temperature	-30 ~ 60 ° C
Operation Humidity	20 ~ 90 % (non-condensing)
Storage Humidity	10 ~ 90 % (non-condensing)
Dimensions	152mm x 92mm x 45mm

Table 46 Firmware Specifications

Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Wireless LAN Standards	IEEE 802.11b, IEEE 802.11g
Wireless security	WEP, WPA(2), WPA(2)-PSK, 802.1x
STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network.
WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic.
Certificates	The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

Table 46 Firmware Specifications

SSL Passthrough	SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https” instead of “http”. The ZyXEL Device allows SSL connections to take place through the ZyXEL Device.
MAC Address Filter	Your ZyXEL Device checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.
Wireless Association List	With the wireless association list, you can see the list of the wireless stations that are currently using the ZyXEL Device to access your wired network.
Logging and Tracing	Built-in message logging and packet tracing.
Embedded FTP and TFTP Servers	The embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.
Auto Configuration	Administrators can use text configuration files to configure the wireless LAN settings for multiple APs. The AP can automatically get a configuration file from a TFTP server at start up or after renewing DHCP client information.
SNMP	SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manger station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

B

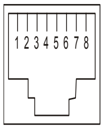
Power over Ethernet (PoE) Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.-7

Table 47 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 48 Power over Ethernet Injector RJ-45 Port Pin Assignments

	**PIN NO**	**RJ-45 SIGNAL ASSIGNMENT**
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

C

Power Adaptor Specifications

Table 49 North American Plug Standards

AC Power Adaptor Model	ADS6818-1812-W 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5A, 18W
Power Consumption	6 W Max
Safety Standards	UL, CUL (UL60950 Third Edition, CSA C22.2 No. 60950)

Table 50 European Plug Standards

AC Power Adaptor Model	ADS6818-1812-B 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS, CE (EN 60950)

Table 51 United Kingdom Plug Standards

AC Power Adaptor Model	ADS6818-1812-D 1215
Input Power	100~240 Volts AC, 50~60 Hz,0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS (BS EN 60950)

Table 52 Australia and New Zealand Plug Standards

AC Power Adaptor Model	ADS6818-1812-A 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	DOFT (AS/NZS 60950, AS/NZSB 3112:1-2)