The following table describes the labels in this screen.

**Table 28** DHCP Setup

| LABEL | DESCRIPTION |
|---|---|
| DHCP Setup | |
| DHCP | If set to **Server**, your ZyXEL Device can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.<br>If set to **None**, the DHCP server will be disabled.<br>If set to **Relay**, the ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case.<br>When DHCP is used, the following items need to be set: |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| Remote DHCP Server | If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here. |
| DNS Server | |
| DNS Servers Assigned by DHCP Server | The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients. |
| Primary DNS Server<br>Secondary DNS Server | This field is not available when you set **DHCP** to **Relay**.<br>Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.<br>If the fields are left as **0.0.0.0**, the ZyXEL Device acts as a DNS proxy and forwards the DHCP client's DNS query to the real DNS server learned through IPCP and relays the response back to the computer. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

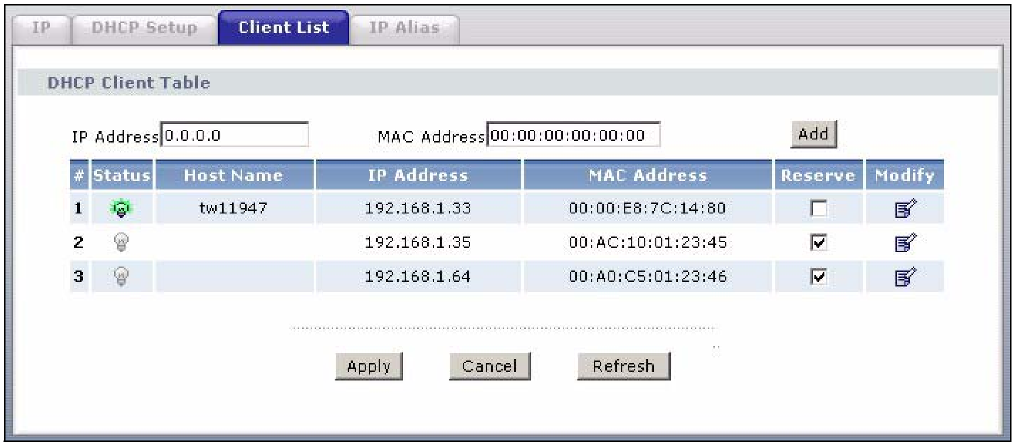
## 6.5 LAN Client List

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

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.

To change your ZyXEL Device's static DHCP settings, click **Network > LAN > Client List**. The screen appears as shown.

**Figure 57** LAN Client List



DHCP Client Table

IP Address 0.0.0.0 MAC Address 00:00:00:00:00:00

| # | Status | Host Name | IP Address | MAC Address | Reserve | Modify |
|---|---|---|---|---|---|---|
| 1 | ● | tw11947 | 192.168.1.33 | 00:00:E8:7C:14:80 | □ | ✎ |
| 2 | ○ |  | 192.168.1.35 | 00:AC:10:01:23:45 | ☑ | ✎ |
| 3 | ○ |  | 192.168.1.64 | 00:A0:C5:01:23:46 | ☑ | ✎ |

The following table describes the labels in this screen.

**Table 29** LAN Client List

| LABEL | DESCRIPTION |
|---|---|
| IP Address | Enter the IP address that you want to assign to the computer on your LAN with the MAC address specified below.<br>The IP address should be within the range of IP addresses you specified in the **DHCP Setup** for the DHCP client. |
| MAC Address | Enter the MAC address of a computer on your LAN. |
| Add | Click **Add** to add a static DHCP entry. |
| # | This is the index number of the static IP table entry (row). |
| Status | This field displays whether the client is connected to the ZyXEL Device. |
| Host Name | This field displays the computer host name. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| MAC Address | The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).<br>A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address. |
| Reserve | Select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 32 entries in this table. |
| Modify | Click the modify icon to have the **IP address** field editable and change it. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |
| Refresh | Click **Refresh** to reload the DHCP table. |

## 6.6 LAN IP Alias

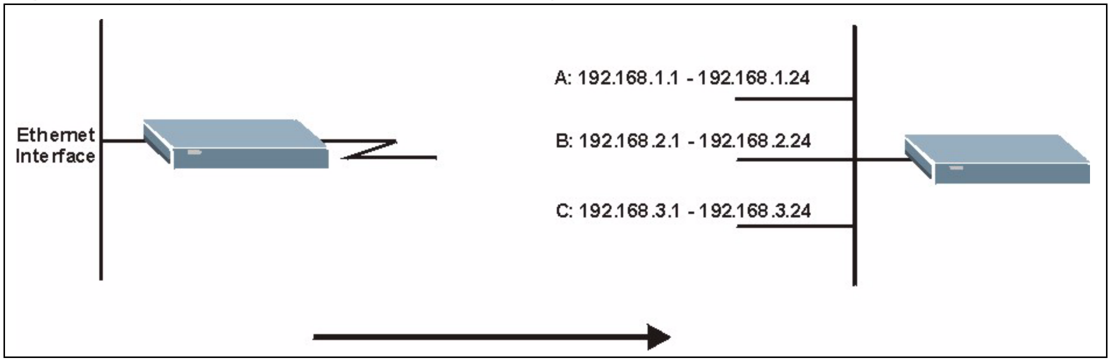
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

**Make sure that the subnets of the logical networks do not overlap.**

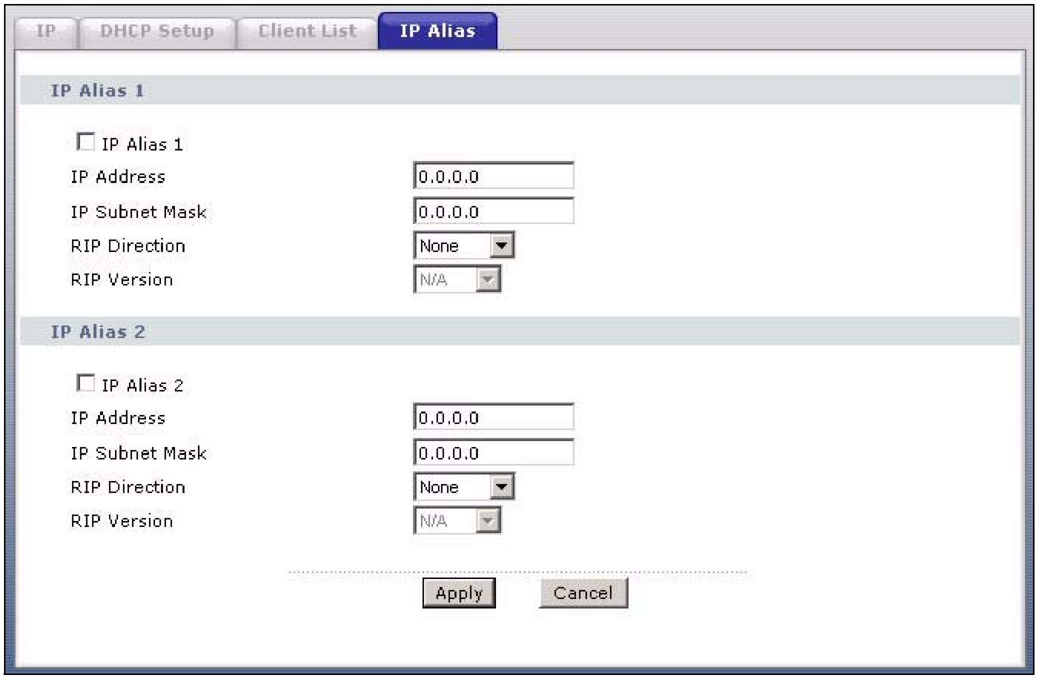
The following figure shows a LAN divided into subnets A, B, and C.

**Figure 58** Physical Network & Partitioned Logical Networks


A: 192.168.1.1 - 192.168.1.24
B: 192.168.2.1 - 192.168.2.24
C: 192.168.3.1 - 192.168.3.24
Ethernet Interface

To change your ZyXEL Device’s IP alias settings, click **Network** > **LAN** > **IP Alias**. The screen appears as shown.

**Figure 59** LAN IP Alias



IP Alias 1

☐ IP Alias 1

| | |
|---|---|
| IP Address | 0.0.0.0 |
| IP Subnet Mask | 0.0.0.0 |
| RIP Direction | None |
| RIP Version | N/A |

IP Alias 2

☐ IP Alias 2

| | |
|---|---|
| IP Address | 0.0.0.0 |
| IP Subnet Mask | 0.0.0.0 |
| RIP Direction | None |
| RIP Version | N/A |

The following table describes the labels in this screen.

**Table 30** LAN IP Alias

| LABEL | DESCRIPTION |
|---|---|
| IP Alias 1, 2 | Select the check box to configure another LAN network for the ZyXEL Device. |
| IP Address | Enter the IP address of your ZyXEL Device in dotted decimal notation.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| IP Subnet Mask | Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device. |
| RIP Direction | RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **None/ Both**/**In Only**/**Out Only**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

7

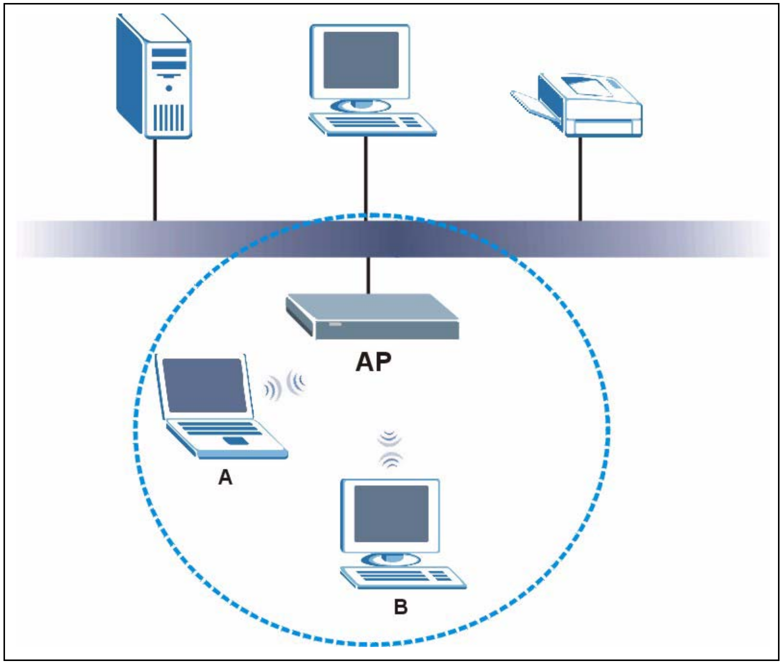
# Wireless LAN

This chapter discusses how to configure the wireless network settings on your ZyXEL Device. See the appendices for more detailed information about wireless networks.

## 7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

**Figure 60** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.
  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## 7.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

### 7.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

### 7.2.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

### 7.2.3 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. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized 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.

Local user databases also have an additional limitation that is explained in the next section.

## 7.2.4 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.

The types of encryption you can choose depend on the type of user authentication. (See Section 7.2.3 on page 106 for information about this.)

**Table 31** Types of Encryption for Each Type of Authentication

| | NO AUTHENTICATION | RADIUS SERVER |
|---|---|---|
| **Weakest** | No Security | WPA |
| ↕ | Static WEP | |
| | WPA-PSK | |
| **Strongest** | WPA2-PSK | WPA2 |

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

**It is recommended that wireless networks use WPA-PSK, WPA, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.**

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

### 7.2.5 One-Touch Intelligent Security Technology (OTIST)

With ZyXEL's OTIST, you set up the SSID and WPA-PSK on the ZyXEL Device. Then, the ZyXEL Device transfers them to the devices in the wireless networks. As a result, you do not have to set up the SSID and encryption on every device in the wireless network.

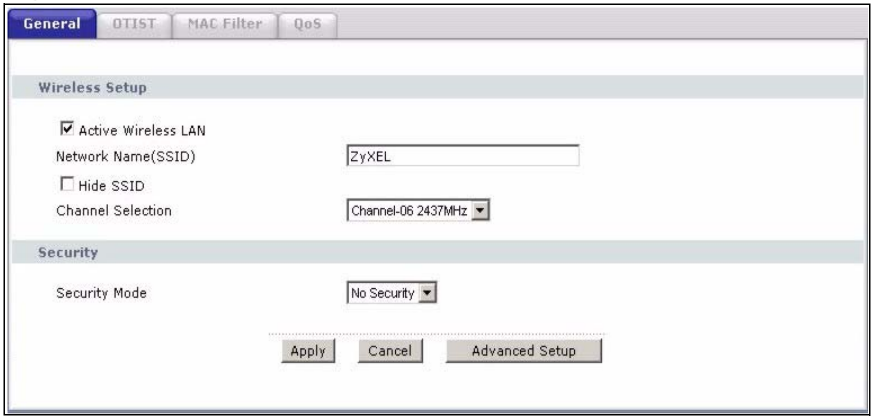
The devices in the wireless network have to support OTIST, and they have to be in range of the ZyXEL Device when you activate it. See Section 7.4 on page 117 for more details.

## 7.3 General Wireless LAN Screen

**If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.**

Click **Network** > **Wireless LAN** to open the **General** screen.

**Figure 61** Wireless LAN: General



Wireless Setup

☑ Active Wireless LAN

Network Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Security

Security Mode: No Security

The following table describes the general wireless LAN labels in this screen.

**Table 32** Wireless LAN: General

| LABEL | DESCRIPTION |
|---|---|
| Wireless Setup | |
| Active Wireless LAN | Click the check box to activate wireless LAN. |
| Network Name (SSID) | (Service Set IDentity) The SSID identifies the Service Set with which a wireless client is associated. Wireless clients associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.<br>**Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.** |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| Channel Selection | Set the operating frequency/channel depending on your particular region.<br>Select a channel from the drop-down list box. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |
| Advanced Setup | Click **Advanced Setup** to display the **Wireless Advanced Setup** screen and edit more details of your WLAN setup. |

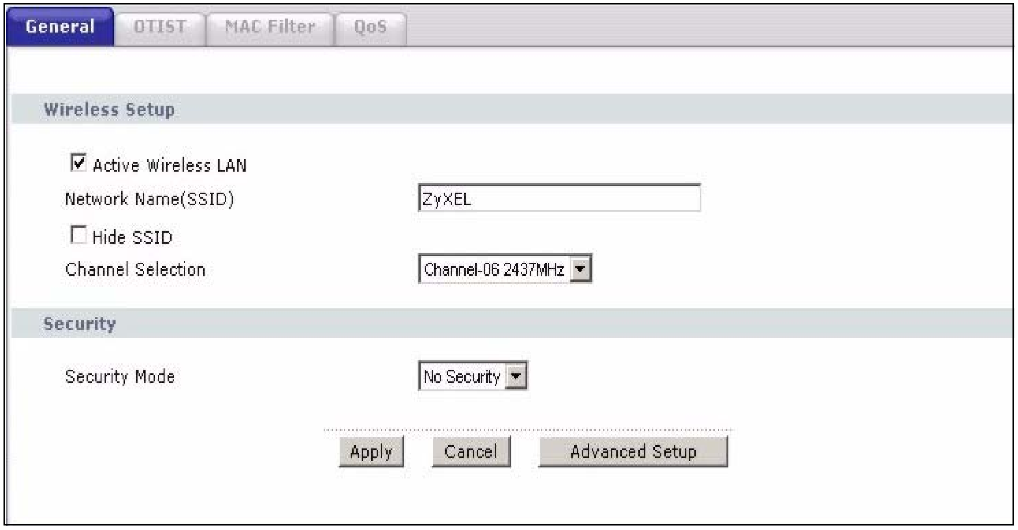
See the rest of this chapter for information on the other labels in this screen.

### 7.3.1 No Security

Select **No Security** to allow wireless clients to communicate with the access points without any data encryption.

**If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.**

**Figure 62** Wireless: No Security



☑ Active Wireless LAN

Network Name(SSID) ZyXEL

□ Hide SSID

Channel Selection Channel-06 2437MHz

Security Mode No Security

The following table describes the labels in this screen.

**Table 33** Wireless No Security

| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Choose **No Security** from the drop-down list box. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |
| Advanced Setup | Click **Advanced Setup** to display the **Wireless Advanced Setup** screen and edit more details of your WLAN setup. |

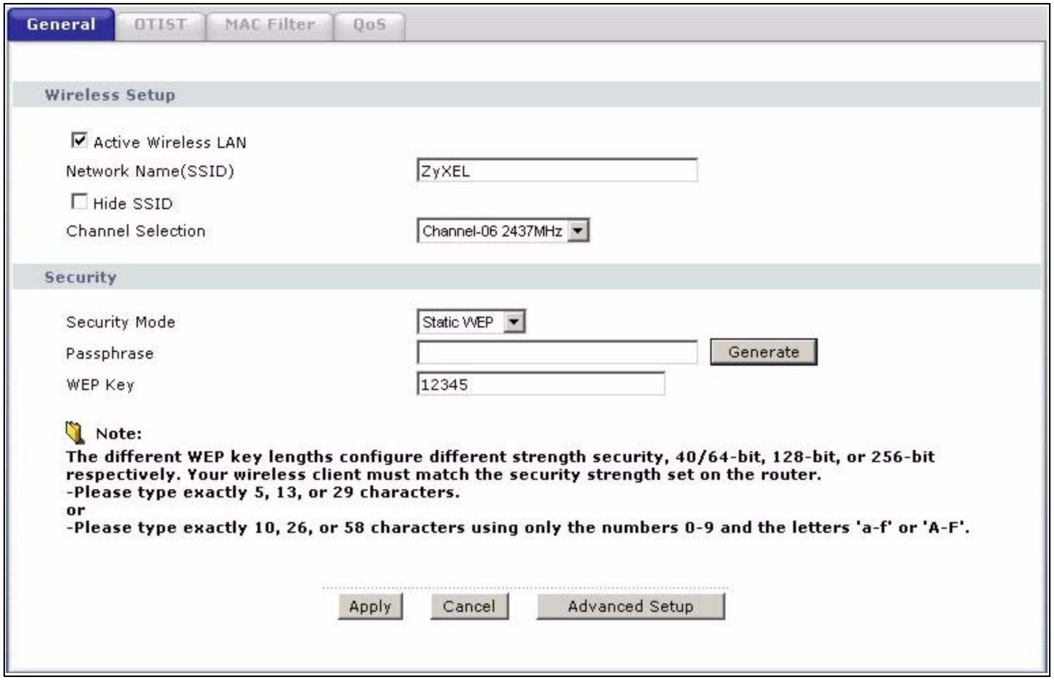
## 7.3.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless clients and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless clients and the access points must use the same WEP key.

Your ZyXEL Device allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Network** > **Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

**Figure 63** Wireless: Static WEP Encryption



☑ Active Wireless LAN
Network Name(SSID): ZyXEL
□ Hide SSID
Channel Selection: Channel-06 2437MHz
Security Mode: Static WEP
Passphrase:
WEP Key: 12345

**Note:**
**The different WEP key lengths configure different strength security, 40/64-bit, 128-bit, or 256-bit respectively. Your wireless client must match the security strength set on the router.**
**-Please type exactly 5, 13, or 29 characters.**
**or**
**-Please type exactly 10, 26, or 58 characters using only the numbers 0-9 and the letters 'a-f' or 'A-F'.**

The following table describes the wireless LAN security labels in this screen.

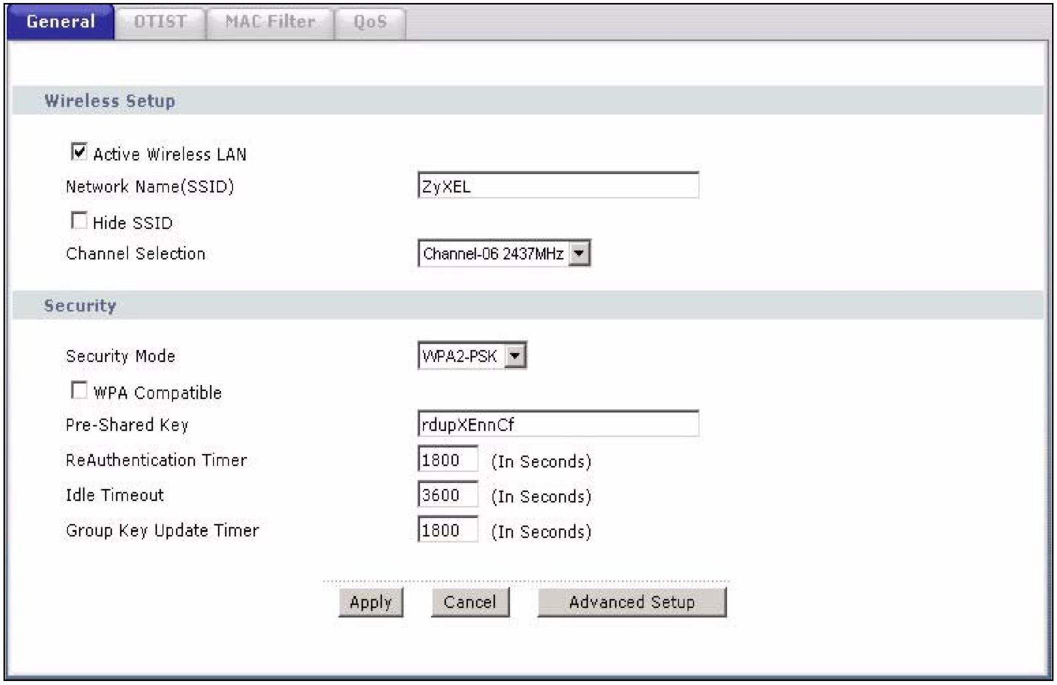
**Table 34** Wireless: Static WEP Encryption

| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Choose **Static WEP** from the drop-down list box. |
| Passphrase | Enter a Passphrase (up to 32 printable characters) and clicking **Generate**. The ZyXEL Device automatically generates a WEP key. |
| WEP Key | The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless clients must use the same WEP key for data transmission.<br>If you want to manually set the WEP key, enter any 5, 13 or 29 characters (ASCII string) or 10, 26 or 58 hexadecimal characters ("0-9", "A-F") for a 64-bit, 128-bit or 256-bit WEP key respectively. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |
| Advanced Setup | Click **Advanced Setup** to display the **Wireless Advanced Setup** screen and edit more details of your WLAN setup. |

## 7.3.3 WPA-PSK/WPA2-PSK

In order to configure and enable WPA(2)-PSK authentication; click **Network > Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

**Figure 64** Wireless: WPA-PSK/WPA2-PSK



Wireless Setup

☑ Active Wireless LAN

Network Name(SSID): ZyXEL

☐ Hide SSID

Channel Selection: Channel-06 2437MHz

Security

Security Mode: WPA2-PSK

☐ WPA Compatible

Pre-Shared Key: rdupXEnnCf

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Group Key Update Timer: 1800 (In Seconds)

The following table describes the wireless LAN security labels in this screen.

**Table 35** Wireless: WPA-PSK/WPA2-PSK

| LABEL | DESCRIPTION |
|---|---|
| Security Mode | Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box. |
| WPA Compatible | This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field.<br>Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2. |
| Pre-Shared Key | The encryption mechanisms used for **WPA/WPA2** and **WPA-PSK/WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK/WPA2-PSK** uses a simple common password, instead of user-specific credentials.<br>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| ReAuthentication Timer (In Seconds) | Specify how often wireless clients 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).<br>**Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.** |

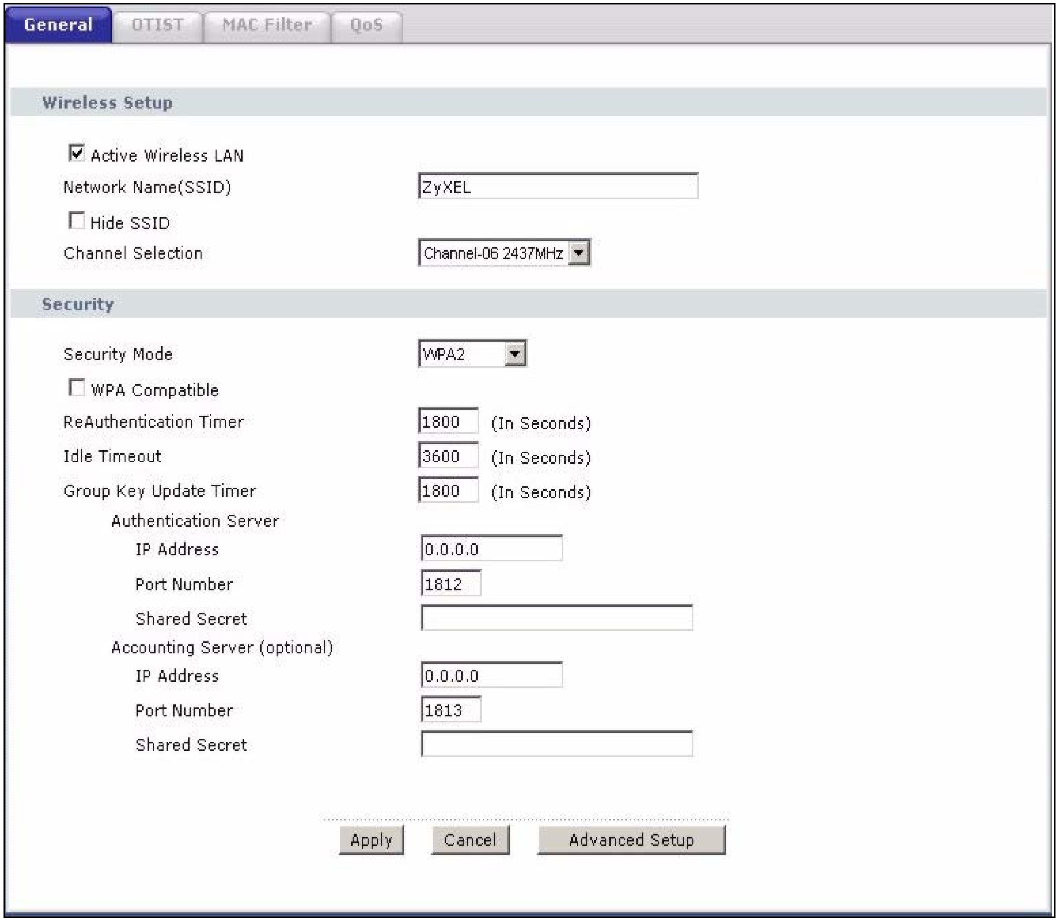
**Table 35** Wireless: WPA-PSK/WPA2-PSK

| LABEL | DESCRIPTION |
|---|---|
| Idle Timeout (In Seconds) | The ZyXEL Device automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Group Key Update Timer (In Seconds) | The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or RADIUS server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP 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/WPA2-PSK** mode. The default is **1800** seconds (30 minutes). |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |
| Advanced Setup | Click **Advanced Setup** to display the **Wireless Advanced Setup** screen and edit more details of your WLAN setup. |

### 7.3.4 WPA/WPA2

In order to configure and enable WPA/WPA2; click the **Wireless LAN** link under **Network** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

**Figure 65** Wireless: WPA/WPA2



Wireless Setup

☑ Active Wireless LAN

Network Name(SSID): ZyXEL

□ Hide SSID

Channel Selection: Channel-06 2437MHz

Security

Security Mode: WPA2

□ WPA Compatible

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Group Key Update Timer: 1800 (In Seconds)

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret:

Accounting Server (optional)

IP Address: 0.0.0.0

Port Number: 1813

Shared Secret:

The following table describes the wireless LAN security labels in this screen.

**Table 36** Wireless: WPA/WPA2

| LABEL | DESCRIPTION |
|---|---|
| WPA Compatible | This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field.<br>Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the ZyXEL Device even when the ZyXEL Device is using WPA2-PSK or WPA2. |
| ReAuthentication Timer (In Seconds) | Specify how often wireless clients 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).<br>**Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.** |
| Idle Timeout (In Seconds) | The ZyXEL Device automatically disconnects a wireless client from the wired network after a period of inactivity. The wireless client needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour). |

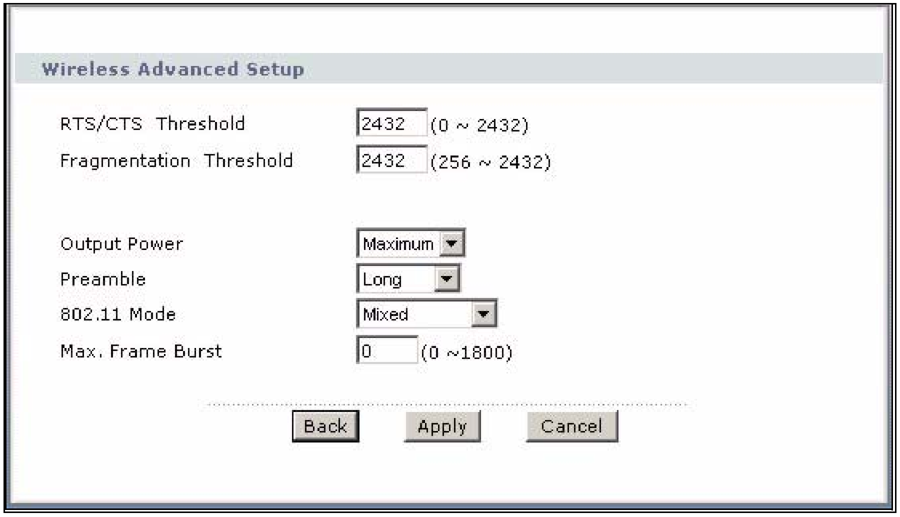
**Table 36** Wireless: WPA/WPA2 (continued)

| LABEL | DESCRIPTION |
|---|---|
| Group Key Update Timer (In Seconds) | The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP 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/WPA2-PSK** mode. The default is **1800** seconds (30 minutes). |
| Authentication Server | |
| IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port Number | Enter the port number of the external authentication server. The default port number is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device.<br>The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network. |
| Accounting Server (optional) | |
| IP Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port Number | Enter the port number of the external accounting server. The default port number is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device.<br>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 to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |
| Advanced Setup | Click **Advanced Setup** to display the **Wireless Advanced Setup** screen and edit more details of your WLAN setup. |

## 7.3.5 Wireless LAN Advanced Setup

To configure advanced wireless settings, click the **Advanced Setup** button in the **General** screen. The screen appears as shown.

**Figure 66** Advanced



Wireless Advanced Setup

RTS/CTS Threshold: 2432 (0 ~ 2432)

Fragmentation Threshold: 2432 (256 ~ 2432)

Output Power: Maximum

Preamble: Long

802.11 Mode: Mixed

Max. Frame Burst: 0 (0 ~1800)

The following table describes the labels in this screen.

**Table 37** Wireless LAN: Advanced

| LABEL | DESCRIPTION |
|---|---|
| Wireless Advanced Setup | |
| RTS/CTS Threshold | Enter a value between 0 and 2432. |
| Fragmentation Threshold | This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432. |
| Output Power | Set the output power of the ZyXEL Device in this field. This control changes the strength of the ZyXEL Device's antenna gain or transmission power. Antenna gain is the increase in coverage. Higher antenna gain improves the range of the signal for better communications. If there is a high density of APs within an area, decrease the output power of the ZyXEL Device to reduce interference with other APs.<br>The options are **Maximum**, **Middle** and **Minimum**. |
| Preamble | Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.<br>Select **Short** preamble if you are sure the wireless adapters support it, and to provide more efficient communications.<br>Select **Dynamic** to have the ZyXEL Device automatically use short preamble when wireless adapters support it, otherwise the ZyXEL Device uses long preamble. |
| 802.11 Mode | Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device.<br>Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device.<br>Select **Mixed** to allow either IEEE802.11b or IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. |
| Max. Frame Burst | Enable **Maximum Frame Burst** to help eliminate collisions in mixed-mode networks (networks with both IEEE 802.11g and IEEE 802.11b traffic) and enhance the performance of both pure IEEE 802.11g and mixed IEEE 802.11b/g networks. **Maximum Frame Burst** sets the maximum time, in micro-seconds, that the ZZyXEL Device transmits IEEE 802.11g wireless traffic only.<br>Type the maximum frame burst between 0 and 1800 (650, 1000 or 1800 recommended). Enter 0 to disable this feature. |
| Back | Click **Back** to return to the previous screen. |

**Table 37** Wireless LAN: Advanced (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

# 7.4 OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as "AP" here) in order to associate with it. Traditionally this meant that you had to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP's SSID and WPA-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA-PSK key for you if you didn't configure one manually.

**OTIST replaces the pre-configured wireless settings on the wireless clients.**

## 7.4.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

**The AP and wireless client(s) MUST use the same Setup key.**

### 7.4.1.1 AP

You can enable OTIST using the **RESET** button or the web configurator.

*7.4.1.1.1 Reset button*

If you use the **RESET** button, the default (01234567) or previous saved (through the web configurator) **Setup key** is used to encrypt the settings that you want to transfer.

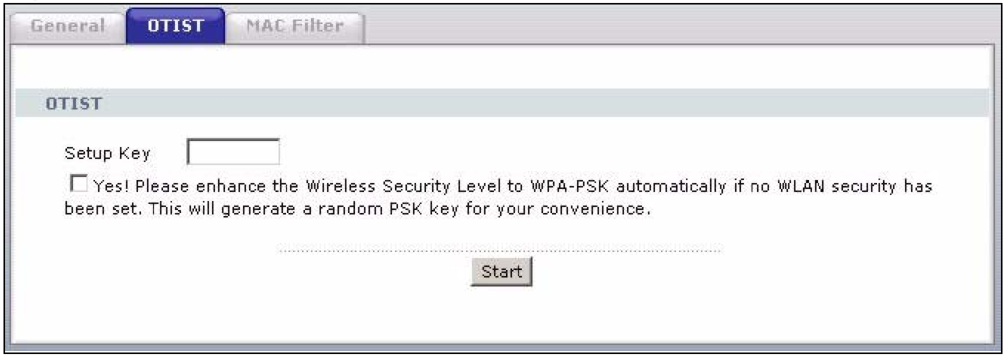
Hold in the **RESET** button for three to eight seconds.

**If you hold in the RESET button too long, the device will reset to the factory defaults!**

### *7.4.1.1.2 Web Configurator*

Click the **Network > Wireless LAN** > **OTIST**. The following screen displays.

**Figure 67** OTIST



□ Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no WLAN security has been set. This will generate a random PSK key for your convenience.

The following table describes the labels in this screen.

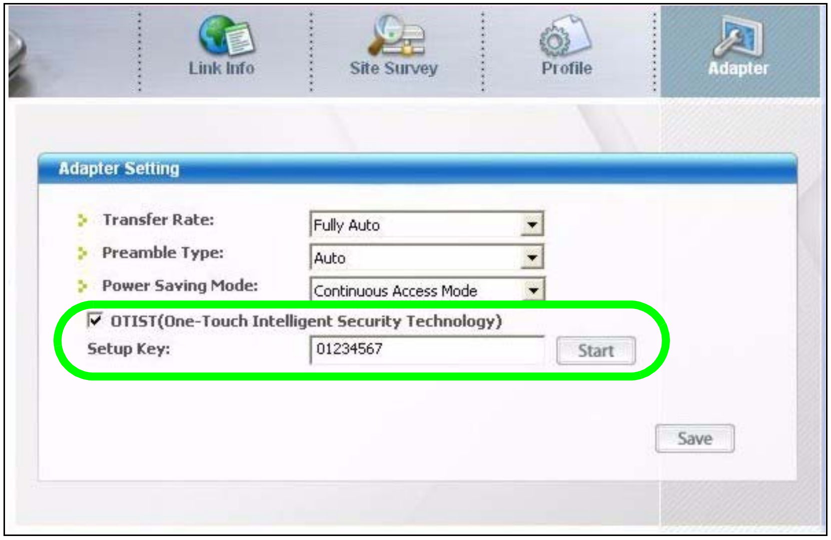
**Table 38** OTIST

| LABEL | DESCRIPTION |
|---|---|
| Setup Key | Type an OTIST **Setup Key** of exactly eight ASCII characters in length.<br>The default OTIST setup key is "01234567".<br>**Note: If you change the OTIST setup key here, you must also make the same change on the wireless client(s).** |
| Yes! | If you want OTIST to automatically generate a WPA-PSK, you must:<br>• Change your security to any security other than **WPA-PSK** in the **Wireless LAN > General** screen.<br>• Select the **Yes!** checkbox in the **OTIST** screen and click **Start**.<br>• The wireless screen displays an auto generated WPA-PSK and is now in WPA-PSK security mode.<br>The WPA-PSK security settings are assigned to the wireless client when you start OTIST.<br>**Note: If you already have a WPA-PSK configured in the Wireless LAN > General screen, and you run OTIST with Yes! selected, OTIST will use the existing WPA-PSK.** |
| Start | Click **Start** to encrypt the wireless security data using the setup key and have the ZyXEL Device set the wireless client(s) to use the same wireless settings as the ZyXEL Device. You must also activate and start OTIST on the wireless client(s) all within three minutes. |

### 7.4.1.2 Wireless Client

Start the ZyXEL utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP’s and click **Save**.

**Figure 68** Example Wireless Client OTIST Screen



Adapter Setting

- Transfer Rate: Fully Auto
- Preamble Type: Auto
- Power Saving Mode: Continuous Access Mode

☑ OTIST(One-Touch Intelligent Security Technology)

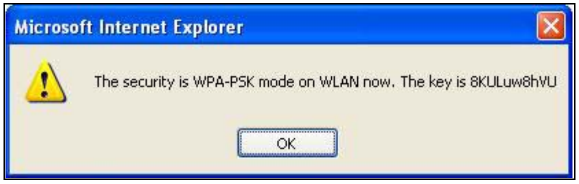
Setup Key: 01234567

## 7.4.2 Starting OTIST

**You must click Start in the AP OTIST web configurator screen and in the wireless client(s) Adapter screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.**

**1** In the AP, a web configurator screen pops up showing you the security settings to transfer. You can use the key in this screen to set up WPA-PSK encryption manually for non-OTIST devices in the wireless network. After reviewing the settings, click **OK**.

**Figure 69** Security Key

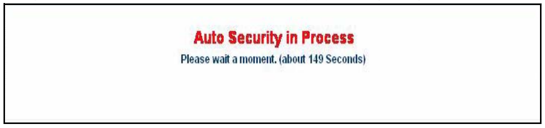


Microsoft Internet Explorer

The security is WPA-PSK mode on WLAN now. The key is 8KULuw8hVU

**2** This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.

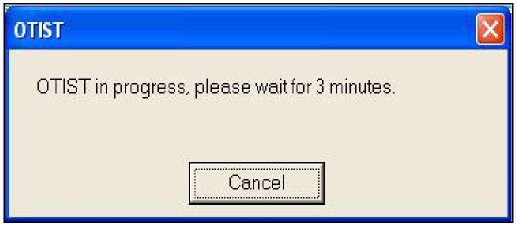
**Figure 70** OTIST in Progress (AP)



Auto Security in Process

Please wait a moment. (about 149 Seconds)

**Figure 71** OTIST in progress (Client)

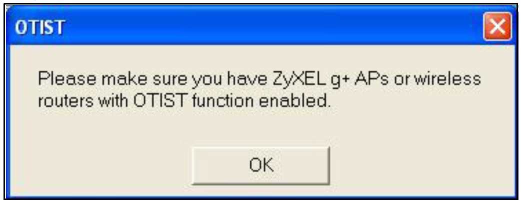


OTIST

OTIST in progress, please wait for 3 minutes.

In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same **Setup key**). Click **OK** to go back to the ZyXEL utility main screen.

**Figure 72** No AP with OTIST Found



OTIST

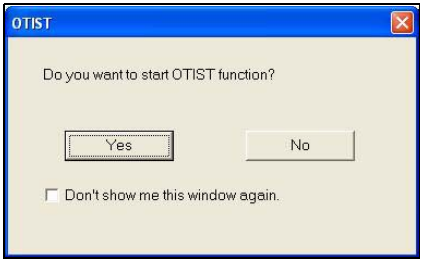
Please make sure you have ZyXEL g+ APs or wireless routers with OTIST function enabled.

- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

## 7.4.3 Notes on OTIST

1 If you enabled OTIST in the wireless client, you see this screen each time you start the utility. Click **Yes** for it to search for an OTIST-enabled AP.

**Figure 73** Start OTIST?



OTIST

Do you want to start OTIST function?

□ Don't show me this window again.

2 If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)

3 When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP **OTIST** web configurator screen or hold in the **RESET** button (for one to five seconds) for the AP to transfer settings.

4 If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).

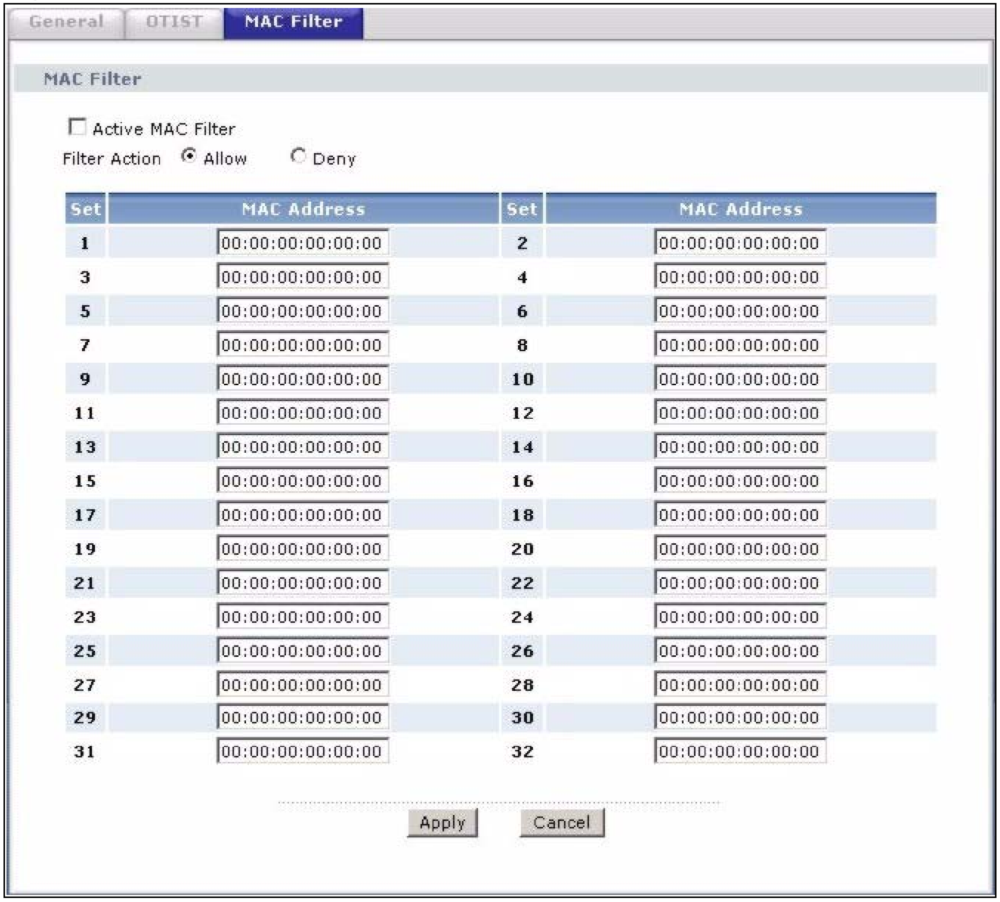
5 If you configure OTIST to generate a WPA-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL wireless clients again.

## 7.5 MAC Filter

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 devices (**Allow**) or exclude up to 32 devices from accessing the ZyXEL Device (**Deny**). 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 the devices to configure this screen.

To change your ZyXEL Device's MAC filter settings, click **Network > Wireless LAN** > **MAC Filter**. The screen appears as shown.

**Figure 74** MAC Address Filter



☐ Active MAC Filter

Filter Action ● Allow ○ Deny

| Set | MAC Address | Set | MAC Address |
|---|---|---|---|
| 1 | 00:00:00:00:00:00 | 2 | 00:00:00:00:00:00 |
| 3 | 00:00:00:00:00:00 | 4 | 00:00:00:00:00:00 |
| 5 | 00:00:00:00:00:00 | 6 | 00:00:00:00:00:00 |
| 7 | 00:00:00:00:00:00 | 8 | 00:00:00:00:00:00 |
| 9 | 00:00:00:00:00:00 | 10 | 00:00:00:00:00:00 |
| 11 | 00:00:00:00:00:00 | 12 | 00:00:00:00:00:00 |
| 13 | 00:00:00:00:00:00 | 14 | 00:00:00:00:00:00 |
| 15 | 00:00:00:00:00:00 | 16 | 00:00:00:00:00:00 |
| 17 | 00:00:00:00:00:00 | 18 | 00:00:00:00:00:00 |
| 19 | 00:00:00:00:00:00 | 20 | 00:00:00:00:00:00 |
| 21 | 00:00:00:00:00:00 | 22 | 00:00:00:00:00:00 |
| 23 | 00:00:00:00:00:00 | 24 | 00:00:00:00:00:00 |
| 25 | 00:00:00:00:00:00 | 26 | 00:00:00:00:00:00 |
| 27 | 00:00:00:00:00:00 | 28 | 00:00:00:00:00:00 |
| 29 | 00:00:00:00:00:00 | 30 | 00:00:00:00:00:00 |
| 31 | 00:00:00:00:00:00 | 32 | 00:00:00:00:00:00 |

The following table describes the labels in this menu.

**Table 39** MAC Address Filter

| LABEL | DESCRIPTION |
|---|---|
| Active MAC Filter | Select the check box to enable MAC address filtering. |
| Filter Action | Define the filter action for the list of MAC addresses in the **MAC Address** table.<br>Select **Deny** to block access to the ZyXEL Device, MAC addresses not listed will be allowed to access the ZyXEL Device<br>Select **Allow** to permit access to the ZyXEL Device, MAC addresses not listed will be denied access to the ZyXEL Device. |
| Set | This is the index number of the MAC address. |

**Table 39** MAC Address Filter

| LABEL | DESCRIPTION |
|---|---|
| MAC Address | Enter the MAC addresses of the wireless client that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

## 7.6 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services.

WMM is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

### 7.6.1 WMM QoS Example

When WMM QoS is not enabled, all traffic streams are given the same access throughput 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.

When WMM QoS is enabled, the streams are prioritized according to the needs of the application. You can assign different priorities to different applications. This prevents reductions in data transmission for applications that are sensitive.

### 7.6.2 WMM QoS Priorities

The following table describes the priorities that you can apply to traffic that the ZyXEL Device sends to the wireless network.

**Table 40** WMM QoS Priorities

| PRIORITY LEVELS: | |
|---|---|
| Highest | Typically used for voice traffic or video that is especially sensitive to jitter (variations in delay). Use the highest priority to reduce latency for improved voice quality. |
| High | Typically used for video traffic which has some tolerance for jitter but needs to be prioritized over other data traffic. |
| Mid | Typically used for traffic from applications or devices that lack QoS capabilities. Use mid priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing. |
| Low | This is typically used for non-critical “background” traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use low priority for applications that do not have strict latency and throughput requirements. |

## 7.6.3 Services

The commonly used services and port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the DNS service. (UDP/TCP:53) means UDP port 53 and TCP port 53.

**Table 41** Commonly Used Services

| SERVICE | DESCRIPTION |
|---|---|
| AIM/New-ICQ(TCP:5190) | AOL’s Internet Messenger service, used as a listening port by ICQ. |
| AUTH(TCP:113) | Authentication protocol used by some servers. |
| BGP(TCP:179) | Border Gateway Protocol. |
| BOOTP_CLIENT(UDP:68) | DHCP Client. |
| BOOTP_SERVER(UDP:67) | DHCP Server. |
| CU-SEEME(TCP/UDP:7648, 24032) | A popular videoconferencing solution from White Pines Software. |
| DNS(UDP/TCP:53) | Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers. |
| FINGER(TCP:79) | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP(TCP:20.21) | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323(TCP:1720) | NetMeeting uses this protocol. |
| HTTP(TCP:80) | Hyper Text Transfer Protocol - a client/server protocol for the world wide web. |
| HTTPS(TCP:443) | HTTPS is a secured http session often used in e-commerce. |
| ICQ(UDP:4000) | This is a popular Internet chat program. |
| IKE(UDP:500) | The Internet Key Exchange algorithm is used for key distribution and management. |
| IPSEC_TUNNEL(AH:0) | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| IPSEC_TUNNEL(ESP:0) | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| IRC(TCP/UDP:6667) | This is another popular Internet chat program. |
| MSN Messenger(TCP:1863) | Microsoft Networks’ messenger service uses this protocol. |
| MULTICAST(IGMP:0) | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| NEW-ICQ(TCP:5190) | An Internet chat program. |
| NEWS(TCP:144) | A protocol for news groups. |
| NFS(UDP:2049) | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP(TCP:119) | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |

**Table 41** Commonly Used Services (continued)

| SERVICE | DESCRIPTION |
|---|---|
| PING(ICMP:0) | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3(TCP:110) | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP(TCP:1723) | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL(GRE:0) | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel. |
| RCMD(TCP:512) | Remote Command Service. |
| REAL_AUDIO(TCP:7070) | A streaming audio service that enables real time sound over the web. |
| REXEC(TCP:514) | Remote Execution Daemon. |
| RLOGIN(TCP:513) | Remote Login. |
| RTELNET(TCP:107) | Remote Telnet. |
| RTSP(TCP/UDP:554) | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP(TCP:115) | Simple File Transfer Protocol. |
| SMTP(TCP:25) | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP(TCP/UDP:161) | Simple Network Management Program. |
| SNMP-TRAPS(TCP/UDP:162) | Traps for use with the SNMP (RFC:1215). |
| SQL-NET(TCP:1521) | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSH(TCP/UDP:22) | Secure Shell Remote Login Program. |
| STRM WORKS(UDP:1558) | Stream Works Protocol. |
| SYSLOG(UDP:514) | Syslog allows you to send system logs to a UNIX server. |
| TACACS(UDP:49) | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET(TCP:23) | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| TFTP(UDP:69) | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE(TCP:7000) | Another videoconferencing solution. |

## 7.7 QoS Screen

The QoS screen by default allows you to automatically give a service a priority level according to the ToS value in the IP header of the packets it sends.

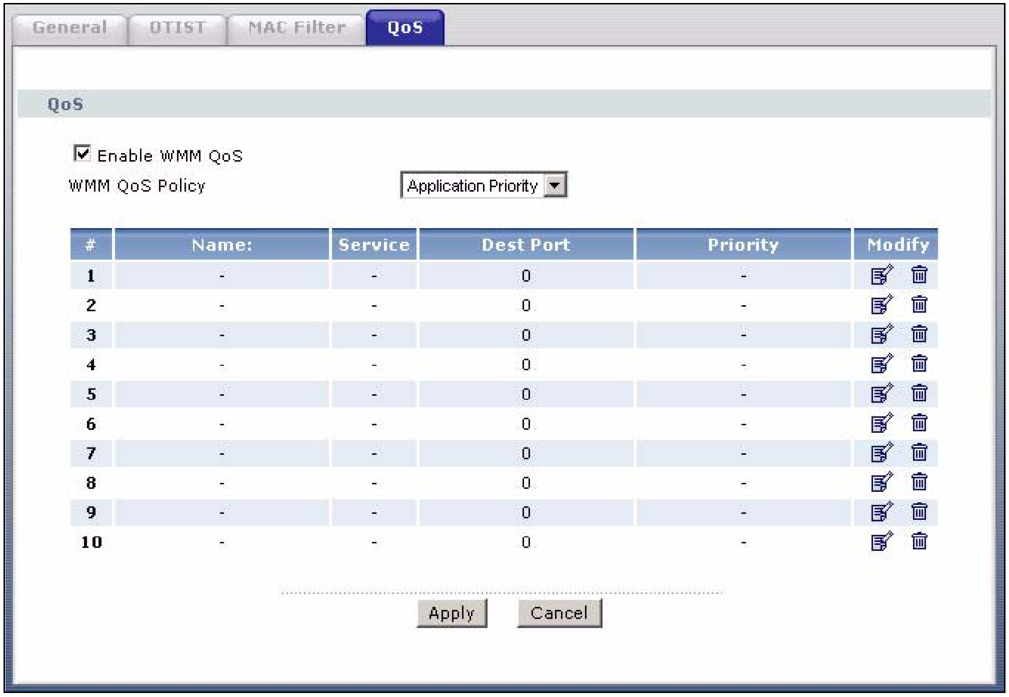
### 7.7.1 ToS (Type of Service) and WMM QoS

ToS defines the DS (Differentiated Service) field in the IP packet header. The ToS value of outgoing packets is between 0 and 255. 0 is the lowest priority.

WMM QoS checks the ToS in the header of transmitted data packets. It gives the application a priority according to this number. If the ToS is not specified, then transmitted data is treated as normal or best-effort traffic.

Click **Network > Wireless LAN** > **QoS**. The following screen displays.

**Figure 75** Wireless LAN: QoS



QoS

☑ Enable WMM QoS

WMM QoS Policy: Application Priority

| # | Name: | Service | Dest Port | Priority | Modify |
|---|---|---|---|---|---|
| 1 | - | - | 0 | - | ✎ 🗑 |
| 2 | - | - | 0 | - | ✎ 🗑 |
| 3 | - | - | 0 | - | ✎ 🗑 |
| 4 | - | - | 0 | - | ✎ 🗑 |
| 5 | - | - | 0 | - | ✎ 🗑 |
| 6 | - | - | 0 | - | ✎ 🗑 |
| 7 | - | - | 0 | - | ✎ 🗑 |
| 8 | - | - | 0 | - | ✎ 🗑 |
| 9 | - | - | 0 | - | ✎ 🗑 |
| 10 | - | - | 0 | - | ✎ 🗑 |

The following table describes the fields in this screen.

**Table 42** Wireless Lan: QoS

| LABEL | DESCRIPTION |
|---|---|
| QoS | |
| Enable WMM QoS | Select the check box to enable WMM QoS on the ZyXEL Device. |
| WMM QoS Policy | Select **Default** to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends.<br>Select **Application Priority** from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS. |
| # | This is the number of an individual application entry. |
| Name | This field displays a description given to an application entry. |
| Service | This field displays either **FTP**, **WWW**, **E-mail** or a **User Defined** service to which you want to apply WMM QoS. |

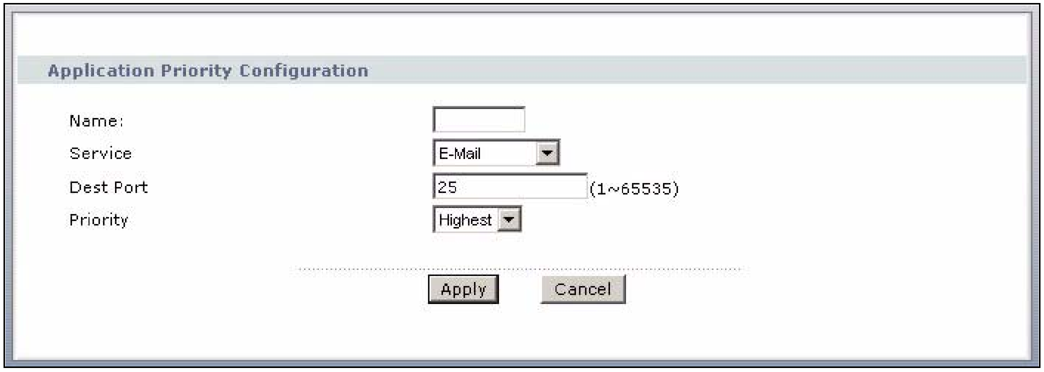
**Table 42** Wireless Lan: QoS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Dest Port | This field displays the destination port number to which the application sends traffic. |
| Priority | This field displays the WMM QoS priority for traffic bandwidth. |
| Modify | Click the to open the **Application Priority Configuration** screen. Modify an existing application entry or create a application entry in the **Application Priority Configuration** screen.<br>Click the **Remove** icon to delete an application entry. |
| Apply | Click **Apply** to save your changes back to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

## 7.7.2 Application Priority Configuration

To edit a WMM QoS application entry, click the edit icon (✎) under **Modify**. The following screen displays.

**Figure 76** Application Priority Configuration



Application Priority Configuration

| | |
|---|---|
| Name: | |
| Service | E-Mail |
| Dest Port | 25 (1~65535) |
| Priority | Highest |

The following table describes the fields in this screen.

**Table 43** Application Priority Configuration

| LABEL | DESCRIPTION |
|---|---|
| Application Priority Configuration | |
| Name | Type a description of the application priority. |

**Table 43** Application Priority Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service | The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box.<br>• **FTP**<br>File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.<br>• **E-Mail**<br>Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail:<br>POP3 - port 110<br>IMAP - port 143<br>SMTP - port 25<br>HTTP - port 80<br>• **WWW**<br>The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.<br>• **User-Defined**<br>User-defined services are user specific services configured using known ports and applications. |
| Dest Port | This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port. See table Table 41 on page 123 for information on port numbers. |
| Priority | Select a priority from the drop-down list box. |
| Apply | Click **Apply** to save your changes back to the ZyXEL Device. |
| Cancel | Click **Cancel** to return to the previous screen without saving your changes. |

8

# Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyXEL Device.

## 8.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

### 8.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 44** NAT Definitions

| ITEM | DESCRIPTION |
|---|---|
| Inside | This refers to the host on the LAN. |
| Outside | This refers to the host on the WAN. |
| Local | This refers to the packet address (source or destination) as the packet travels on the LAN. |
| Global | This refers to the packet address (source or destination) as the packet travels on the WAN. |

NAT never changes the IP address (either local or global) of an outside host.

## 8.1.2 What NAT Does

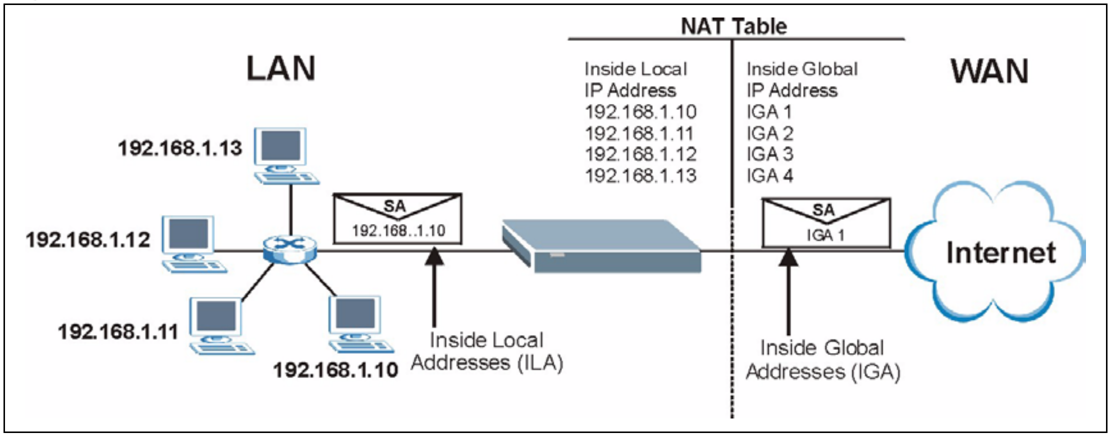
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see Table 45 on page 132), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

## 8.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

**Figure 77** How NAT Works



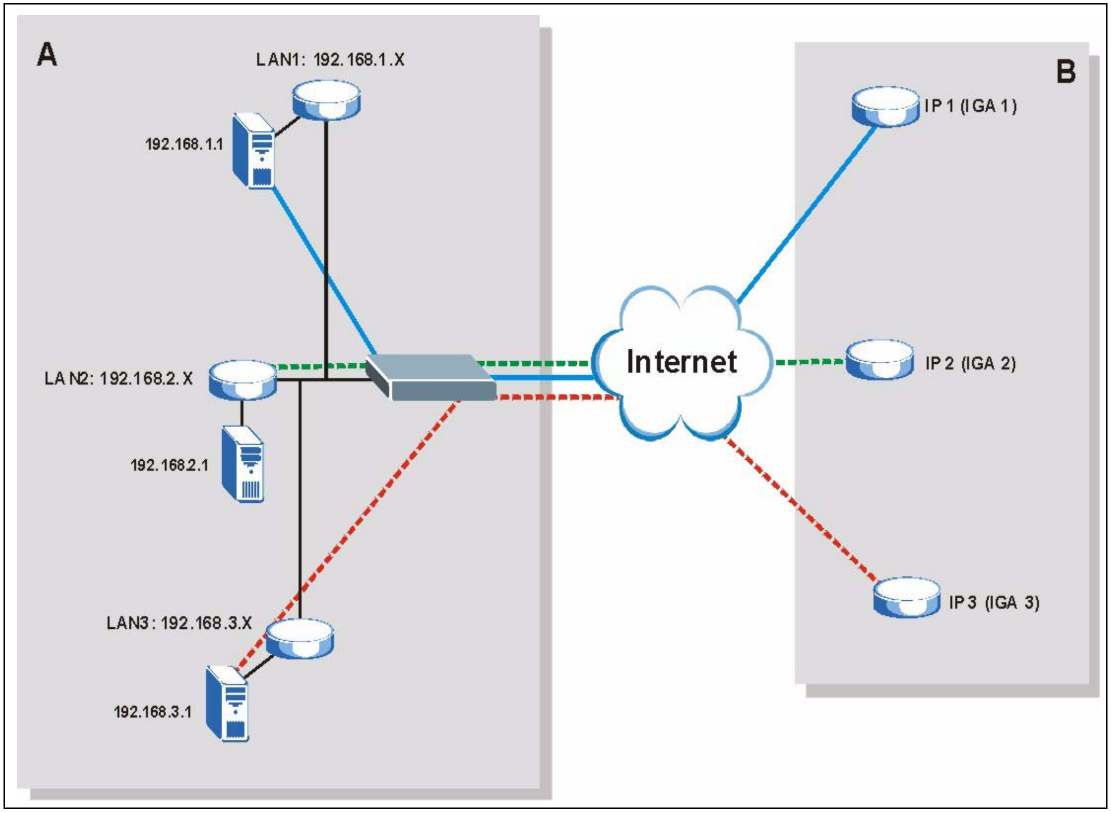
NAT Table

| Inside Local IP Address | Inside Global IP Address |
|---|---|
| 192.168.1.10 | IGA 1 |
| 192.168.1.11 | IGA 2 |
| 192.168.1.12 | IGA 3 |
| 192.168.1.13 | IGA 4 |

## 8.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyXEL Device can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

**Figure 78** NAT Application With IP Alias



## 8.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

**Table 45** NAT Mapping Types

| TYPE | IP MAPPING |
|---|---|
| One-to-One | ILA1←→ IGA1 |
| Many-to-One (SUA/PAT) | ILA1←→ IGA1<br>ILA2←→ IGA1<br>… |
| Many-to-Many Overload | ILA1←→ IGA1<br>ILA2←→ IGA2<br>ILA3←→ IGA1<br>ILA4←→ IGA2<br>… |
| Many-to-Many No Overload | ILA1←→ IGA1<br>ILA2←→ IGA2<br>ILA3←→ IGA3<br>… |
| Server | Server 1 IP←→ IGA1<br>Server 2 IP←→ IGA1<br>Server 3 IP←→ IGA1 |

## 8.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 45 on page 132.

- Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

## 8.3 SIP ALG

Some applications, such as SIP, cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload.

Some NAT routers may include a SIP Application Layer Gateway (ALG). An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer.

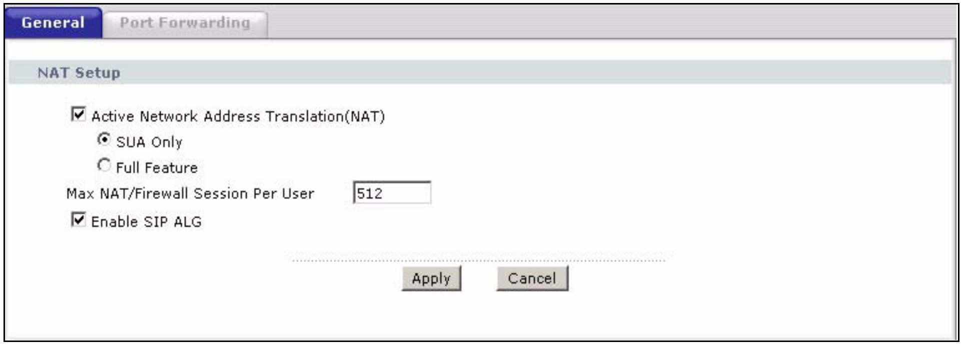
A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream.

When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

## 8.4 NAT General Setup

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device. Click **Network > NAT** to open the following screen.

**Figure 79** NAT General



NAT Setup

☑ Active Network Address Translation(NAT)

● SUA Only

○ Full Feature

Max NAT/Firewall Session Per User 512

☑ Enable SIP ALG

The following table describes the labels in this screen.

**Table 46** NAT General

| LABEL | DESCRIPTION |
|---|---|
| Active Network Address Translation (NAT) | Select this check box to enable NAT. |
| SUA Only | Select this radio button if you have just one public WAN IP address for your ZyXEL Device. |
| Full Feature | Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device. |
| Max NAT/ Firewall Session Per User | When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet.<br>Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the ZyXEL Device.<br>If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions. |
| Enable SIP ALG | Select this option if you want to enable SIP ALG, for example, to use an IP phone through your NAT enabled ZyXEL Device. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to reload the previous configuration for this screen. |

## 8.5 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

### 8.5.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

**If you do not assign a Default Server IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.**

### 8.5.2 Port Forwarding: Services and Port Numbers

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

**Table 47** Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|---|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer protocol or WWW, Web) | 80 |
| POP3 (Post Office Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| SNMP (Simple Network Management Protocol) | 161 |

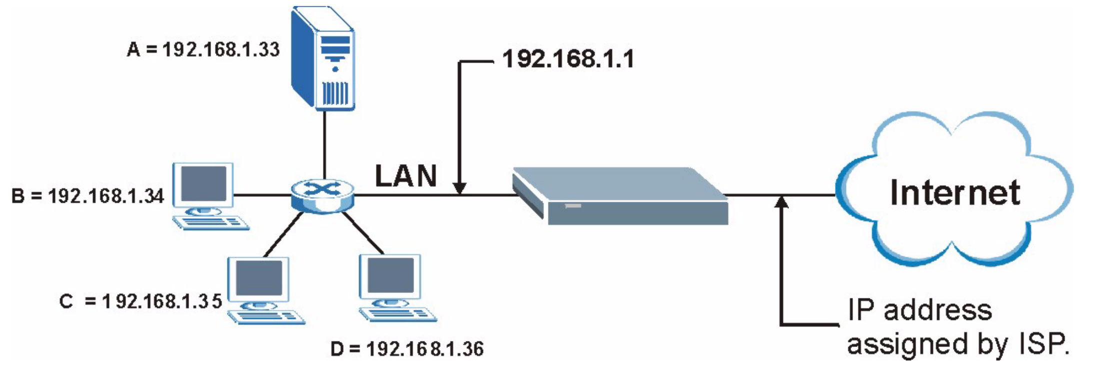
**Table 47** Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|---|
| SNMP trap | 162 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

### 8.5.3 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 80** Multiple Servers Behind NAT Example



## 8.6 Configuring Port Forwarding

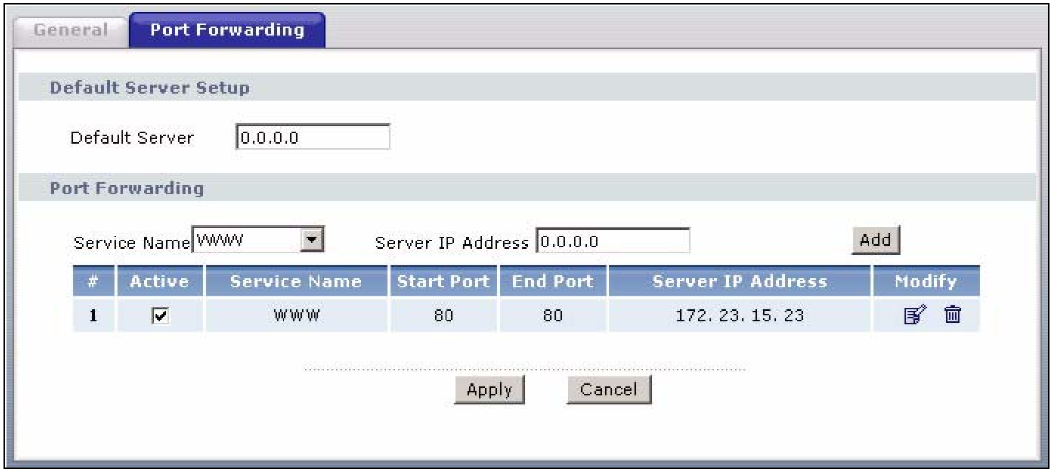
**The Port Forwarding screen is available only when you select SUA Only in the NAT > General screen.**

**If you do not assign a Default Server IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.**

Click **Network** > **NAT** > **Port Forwarding** to open the following screen.

See Table 47 on page 134 for port numbers commonly used for particular services.

**Figure 81** NAT Port Forwarding



Default Server Setup

Default Server: 0.0.0.0

Port Forwarding

Service Name: WWW
Server IP Address: 0.0.0.0

| # | Active | Service Name | Start Port | End Port | Server IP Address | Modify |
|---|---|---|---|---|---|---|
| 1 | ☑ | WWW | 80 | 80 | 172.23.15.23 | ✎ 🗑 |

The following table describes the fields in this screen.

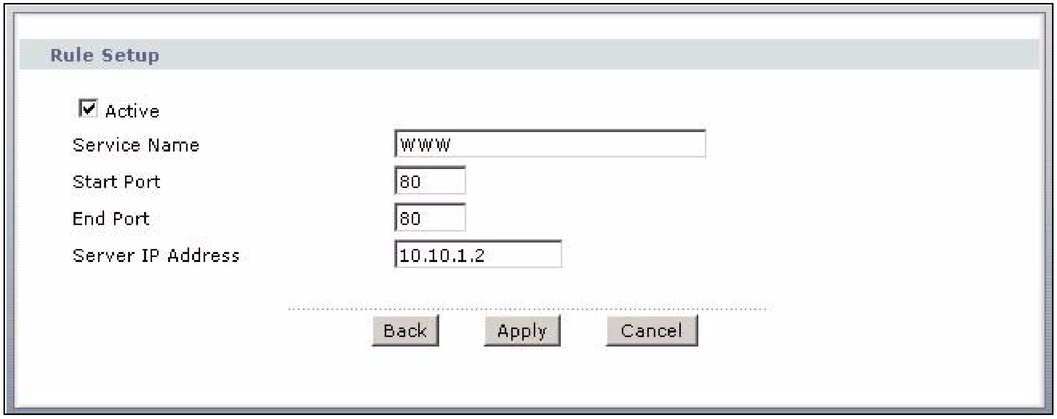
**Table 48** NAT Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Default Server Setup | |
| Default Server | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup. |
| Port Forwarding | |
| Service Name | Select a service from the drop-down list box. |
| Server IP Address | Enter the IP address of the server for the specified service. |
| Add | Click this button to add a rule to the table below. |
| # | This is the rule index number (read-only). |
| Active | Click this check box to enable the rule. |
| Service Name | This is a service's name. |
| Start Port | This is the first port number that identifies a service. |
| End Port | This is the last port number that identifies a service. |
| Server IP Address | This is the server's IP address. |
| Modify | Click the edit icon to go to the screen where you can edit the port forwarding rule.<br>Click the delete icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to return to the previous configuration. |

## 8.6.1 Port Forwarding Rule Edit

To edit a port forwarding rule, click the rule's edit icon (✎) in the **Port Forwarding** screen to display the screen shown next.

**Figure 82** Port Forwarding Rule Setup



Rule Setup

☑ Active

Service Name: WWW

Start Port: 80

End Port: 80

Server IP Address: 10.10.1.2

The following table describes the fields in this screen.

**Table 49** Port Forwarding Rule Setup

| LABEL | DESCRIPTION |
|---|---|
| Active | Click this check box to enable the rule. |
| Service Name | Enter a name to identify this port-forwarding rule. |
| Start Port | Enter a port number in this field.<br>To forward only one port, enter the port number again in the **End Port** field.<br>To forward a series of ports, enter the start port number here and the end port number in the **End Port** field. |
| End Port | Enter a port number in this field.<br>To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field.<br>To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above. |
| Server IP Address | Enter the inside IP address of the server here. |
| Back | Click **Back** to return to the previous screen. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

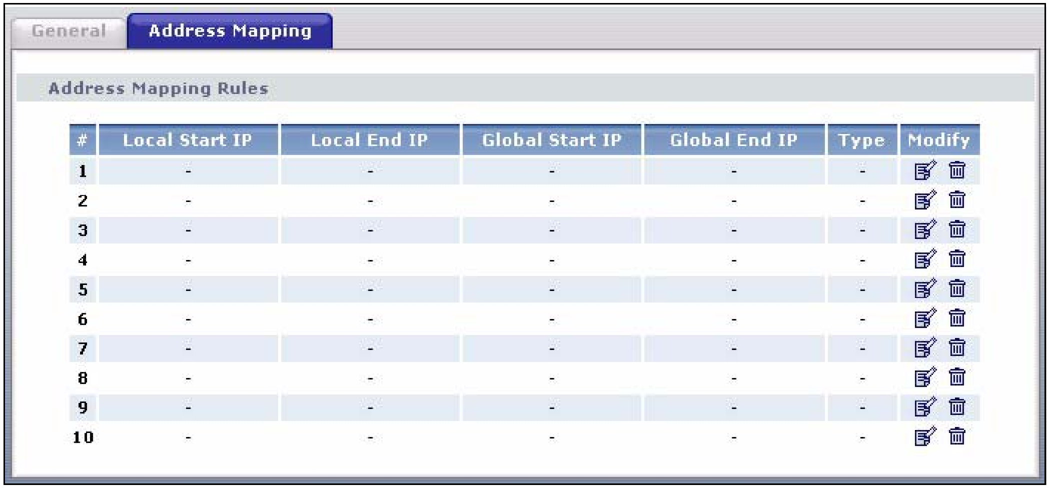
## 8.7 Address Mapping

**The Address Mapping screen is available only when you select Full Feature in the NAT > General screen.**

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyXEL Device's address mapping settings, click **Network** > **NAT** > **Address Mapping** to open the following screen.

**Figure 83** Address Mapping Rules



| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type | Modify |
|---|---|---|---|---|---|---|
| 1 | - | - | - | - | - | ✎ 🗑 |
| 2 | - | - | - | - | - | ✎ 🗑 |
| 3 | - | - | - | - | - | ✎ 🗑 |
| 4 | - | - | - | - | - | ✎ 🗑 |
| 5 | - | - | - | - | - | ✎ 🗑 |
| 6 | - | - | - | - | - | ✎ 🗑 |
| 7 | - | - | - | - | - | ✎ 🗑 |
| 8 | - | - | - | - | - | ✎ 🗑 |
| 9 | - | - | - | - | - | ✎ 🗑 |
| 10 | - | - | - | - | - | ✎ 🗑 |

The following table describes the fields in this screen.

**Table 50** Address Mapping Rules

| LABEL | DESCRIPTION |
|---|---|
| # | This is the rule index number. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types. |

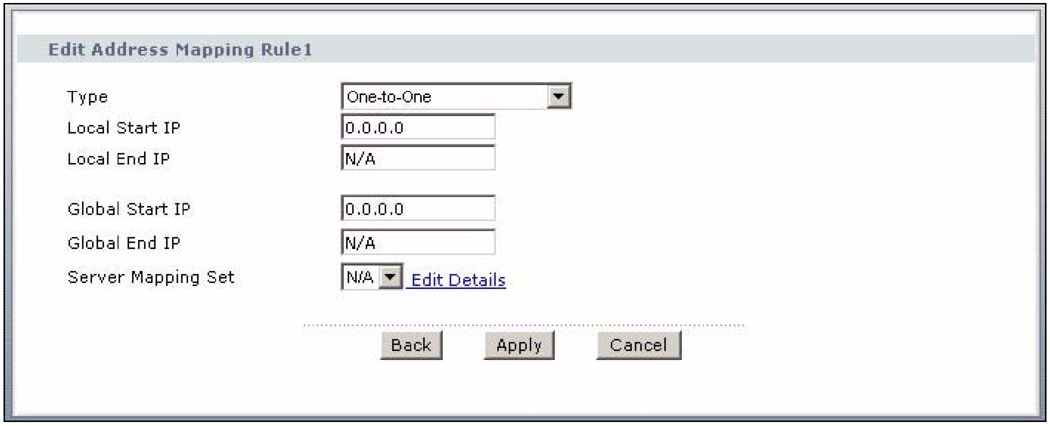
**Table 50** Address Mapping Rules (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | **1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.<br>**M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.<br>**M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br>**MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.<br>**Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Modify | Click the edit icon to go to the screen where you can edit the address mapping rule.<br>Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action. |

## 8.7.1 Address Mapping Rule Edit

To edit an address mapping rule, click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

**Figure 84** Edit Address Mapping Rule



Edit Address Mapping Rule1

| | |
|---|---|
| Type | One-to-One |
| Local Start IP | 0.0.0.0 |
| Local End IP | N/A |
| Global Start IP | 0.0.0.0 |
| Global End IP | N/A |
| Server Mapping Set | N/A |

The following table describes the fields in this screen.

**Table 51** Edit Address Mapping Rule

| LABEL | DESCRIPTION |
|---|---|
| Type | Choose the port mapping type from one of the following.<br>• **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type.<br>• **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.<br>• **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br>• **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.<br>• **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Local Start IP | This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address.<br>This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. |
| Global End IP | This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |
| Server Mapping Set | Only available when **Type** is set to **Server**.<br>Select a number from the drop-down menu to choose a server mapping set. |
| Edit Details | Click this link to go to the **Port Forwarding** screen to edit a server mapping set that you have selected in the **Server Mapping Set** field. |
| Back | Click **Back** to return to the previous screen. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# PART IV
# Security

9

# Firewalls

This chapter gives some background information on firewalls and introduces the ZyXEL Device firewall.

## 9.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

Refer to Section 10.5 on page 158 to configure default firewall settings.

Refer to Section 10.6 on page 159 to view firewall rules.

Refer to Section 10.6.1 on page 161 to configure firewall rules.

Refer to Section 10.6.2 on page 164 to configure a custom service.

Refer to Section 10.10.3 on page 173 to configure firewall thresholds.

## 9.2 Types of Firewalls

There are three main types of firewalls:

- Packet Filtering Firewalls
- Application-level Firewalls
- Stateful Inspection Firewalls

### 9.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

### 9.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

### 9.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See Section 9.5 on page 148 for more information on stateful inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

## 9.3 Introduction to ZyXEL’s Firewall

The ZyXEL Device firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The ZyXEL Device’s purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyXEL Device also has packet filtering capabilities.

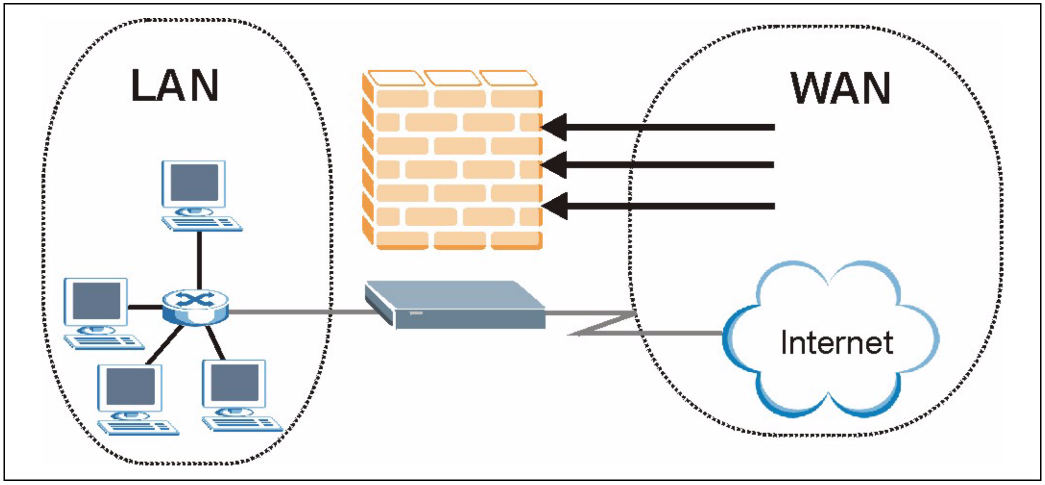
The ZyXEL Device is installed between the LAN and the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyXEL Device has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- The DSL/ISDN port connects to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, “inbound access” will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

### 9.3.1 Denial of Service Attacks

**Figure 85** Firewall Application



## 9.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

### 9.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An "extension number", called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

**Table 52** Common IP Ports

| | | | |
|---|---|---|---|
| 21 | FTP | 53 | DNS |
| 23 | Telnet | 80 | HTTP |
| 25 | SMTP | 110 | POP3 |

### 9.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1 Those that exploit bugs in a TCP/IP implementation.

2 Those that exploit weaknesses in the TCP/IP specification.

3 Brute-force attacks that flood a network with useless data.

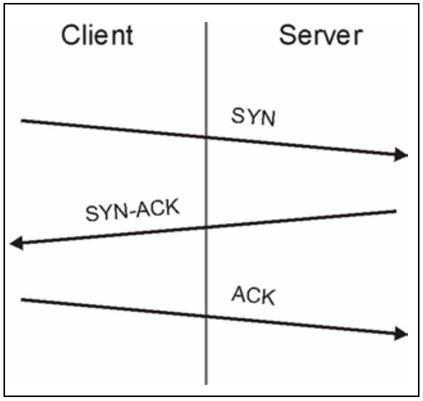
4 IP Spoofing.

5 "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

- Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
- Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

6 Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

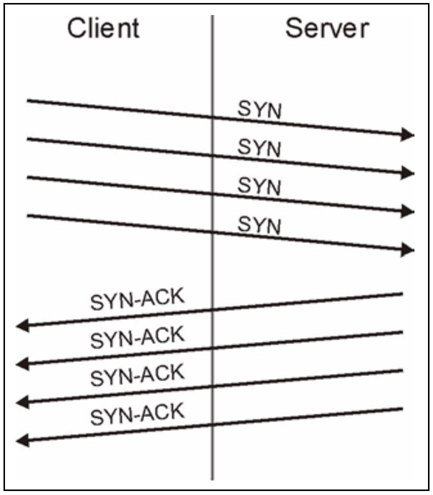
**Figure 86** Three-Way Handshake



Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

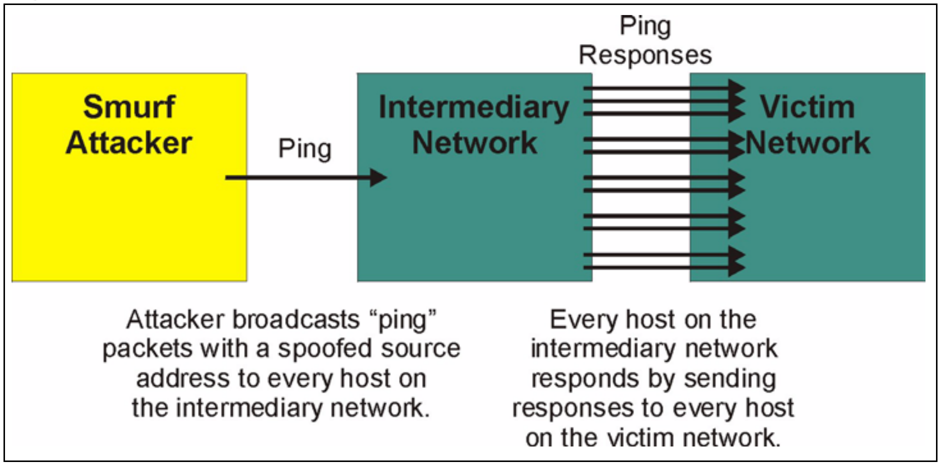
**Figure 87** SYN Flood



- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

**7** A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

**Figure 88** Smurf Attack


Ping
Responses
Smurf
Attacker
Ping
Intermediary
Network
Victim
Network
Attacker broadcasts “ping” packets with a spoofed source address to every host on the intermediary network.
Every host on the intermediary network responds by sending responses to every host on the victim network.

#### 9.4.2.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

**Table 53** ICMP Commands That Trigger Alerts

| | |
|---|---|
| 5 | REDIRECT |
| 13 | TIMESTAMP_REQUEST |
| 14 | TIMESTAMP_REPLY |
| 17 | ADDRESS_MASK_REQUEST |
| 18 | ADDRESS_MASK_REPLY |

#### 9.4.2.2 Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

**Table 54** Legal NetBIOS Commands

| |
|---|
| MESSAGE: |
| REQUEST: |
| POSITIVE: |
| VE: |
| RETARGET: |
| KEEPALIVE: |

All SMTP commands are illegal except for those displayed in the following tables.

**Table 55** Legal SMTP Commands

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| AUTH | DATA | EHLO | ETRN | EXPN | HELO | HELP | MAIL | NOOP |
| QUIT | RCPT | RSET | SAML | SEND | SOML | TURN | VRFY | |

#### 9.4.2.3 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

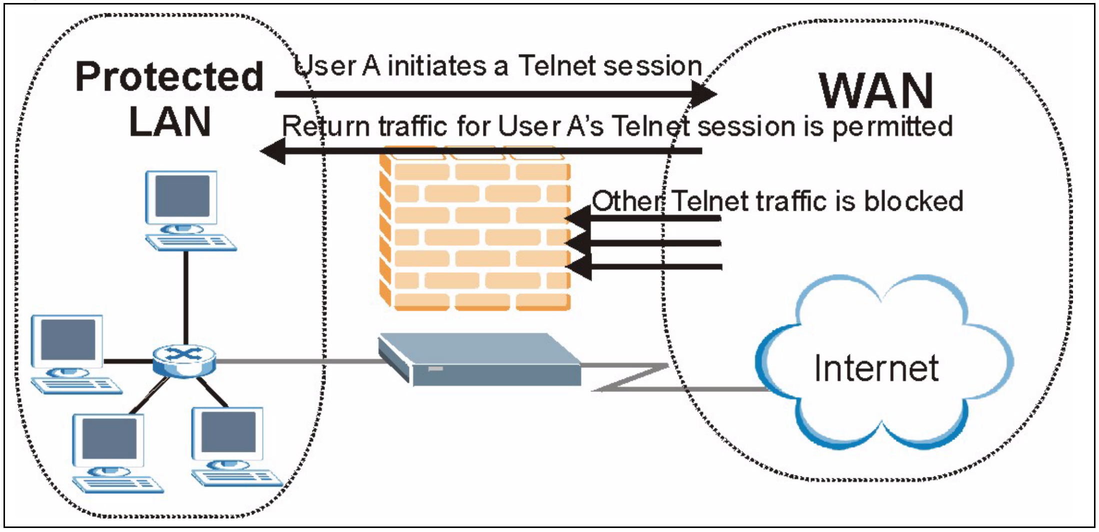
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyXEL Device blocks all IP Spoofing attempts.

## 9.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This “remembering” is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyXEL Device uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyXEL Device's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

**Figure 89** Stateful Inspection


Protected LAN
User A initiates a Telnet session
WAN
Return traffic for User A's Telnet session is permitted
Other Telnet traffic is blocked
Internet

The previous figure shows the ZyXEL Device's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

## 9.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then the settings in the **Firewall General** screen determine the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.

6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.

7 The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.

8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.

9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

### 9.5.2 Stateful Inspection and the ZyXEL Device

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic’s Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

**The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.**

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyXEL Device itself (as with the "virtual connections" created for UDP and ICMP).

### 9.5.3 TCP Security

The ZyXEL Device uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyXEL Device receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

### 9.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyXEL Device is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

### 9.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyXEL Device inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator’s Custom Ports feature to do this.

## 9.6 Guidelines for Enhancing Security with Your Firewall

- Change the default password via CLI (Command Line Interpreter) or web configurator.
- Limit who can telnet into your router.
- Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- Protect against IP spoofing by making sure the firewall is active.
- Keep the firewall in a secured (locked) room.

### 9.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

- Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
- DSL or cable modem connections are "always-on" connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
- Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
- If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.

- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

## 9.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyXEL Device's filtering and firewall functions.

### 9.7.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

#### 9.7.1.1 When To Use Filtering

- To block/allow LAN packets by their MAC addresses.
- To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- To block/allow IP trace route.

### 9.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

#### 9.7.2.1 When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.
- A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.

- To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- The firewall performs better than filtering if you need to check many rules.
- Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

# 10

# Firewall Configuration

This chapter shows you how to enable and configure the ZyXEL Device firewall.

## 10.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyXEL Device has to offer. For this reason, it is recommended that you configure your firewall using the web configurator.CLI (Command Line Interpreter) commands provide limited configuration options and are only recommended for advanced users.

## 10.2 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ Router
- LAN to WAN
- WAN to LAN
- WAN to WAN/ Router

By default, the ZyXEL Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router

  This allows computers on the LAN to manage the ZyXEL Device and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN

By default, the ZyXEL Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ Router

  This prevents computers on the WAN from using the ZyXEL Device as a gateway to communicate with other computers on the WAN and/or managing the ZyXEL Device.

  You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

✍ **If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.**

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyXEL Device’s default rules.

## 10.3 Rule Logic Overview

✍ **Study these points carefully before configuring rules.**

### 10.3.1 Rule Checklist

State the intent of the rule. For example, “This restricts all IRC access from the LAN to the Internet.” Or, “This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.”

1. Is the intent of the rule to forward or block traffic?
2. What direction of traffic does the rule apply to?
3. What IP services will be affected?
4. What computers on the LAN are to be affected (if any)?
5. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

### 10.3.2 Security Ramifications

1. Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:
2. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?

3 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

4 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

5 Does this rule conflict with any existing rules?

6 Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

## 10.3.3 Key Fields For Configuring Rules

### 10.3.3.1 Action

Should the action be to **Drop**, **Reject** or **Permit**?

**"Drop" means the firewall silently discards the packet. "Reject" means the firewall discards packets and sends an ICMP destination-unreachable message to the sender.**

### 10.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See Section 10.8 on page 169 for more information on predefined services.

### 10.3.3.3 Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

### 10.3.3.4 Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

## 10.4 Connection Direction

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ Router and WAN to WAN/ Router rules apply to packets coming in on the associated interface (LAN or WAN respectively). LAN to LAN/ Router means policies for LAN-to-ZyXEL Device (the policies for managing the ZyXEL Device through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/ Router polices apply in the same way to the WAN port.

### 10.4.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

### 10.4.2 Alerts

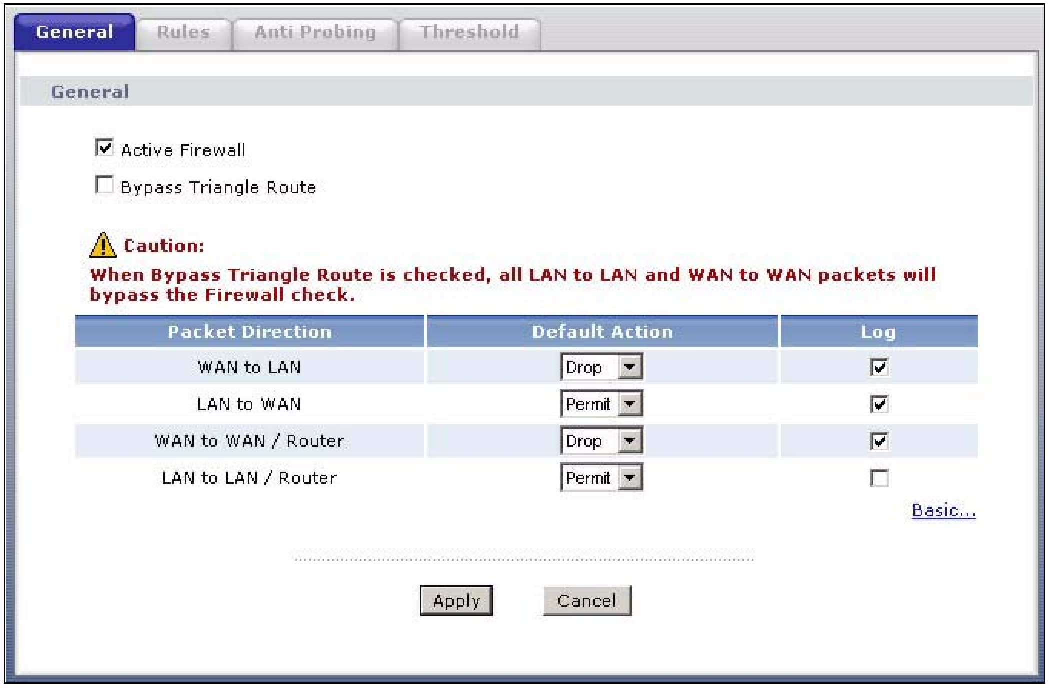
Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when a rule is matched in the **Edit Rule** screen (see Figure 92 on page 162). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen. Refer to the chapter on logs for details

## 10.5 General Firewall Policy

Click **Security > Firewall** to display the following screen. Activate the firewall by selecting the **Active Firewall** check box as seen in the following screen.

Refer to Section 9.1 on page 143 for more information.

**Figure 90** Firewall: General



General

☑ Active Firewall

☐ Bypass Triangle Route

Caution:
When Bypass Triangle Route is checked, all LAN to LAN and WAN to WAN packets will bypass the Firewall check.

| Packet Direction | Default Action | Log |
|---|---|---|
| WAN to LAN | Drop | ☑ |
| LAN to WAN | Permit | ☑ |
| WAN to WAN / Router | Drop | ☑ |
| LAN to LAN / Router | Permit | ☐ |

The following table describes the labels in this screen.

**Table 56** Firewall: General

| LABEL | DESCRIPTION |
|---|---|
| Active Firewall | Select this check box to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. |
| Bypass Triangle Route | Select this check box to have the ZyXEL Device firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology.<br>**Note: Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the router. See Appendix I on page 341 for more on triangle route topology and how to deal with this problem.** |
| Packet Direction | This is the direction of travel of packets (**LAN to LAN / Router**, **LAN to WAN**, **WAN to WAN / Router**, **WAN to LAN)**.<br>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, **LAN to LAN / Router** means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyXEL Device or the ZyXEL Device itself. |
| Default Action | Use the drop-down list boxes to select the default action that the firewall is take on packets that are traveling in the selected direction and do not match any of the firewall rules.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets. |
| Log | Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules. |
| Expand... | Click this button to display more information. |
| Basic... | Click this button to display less information. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

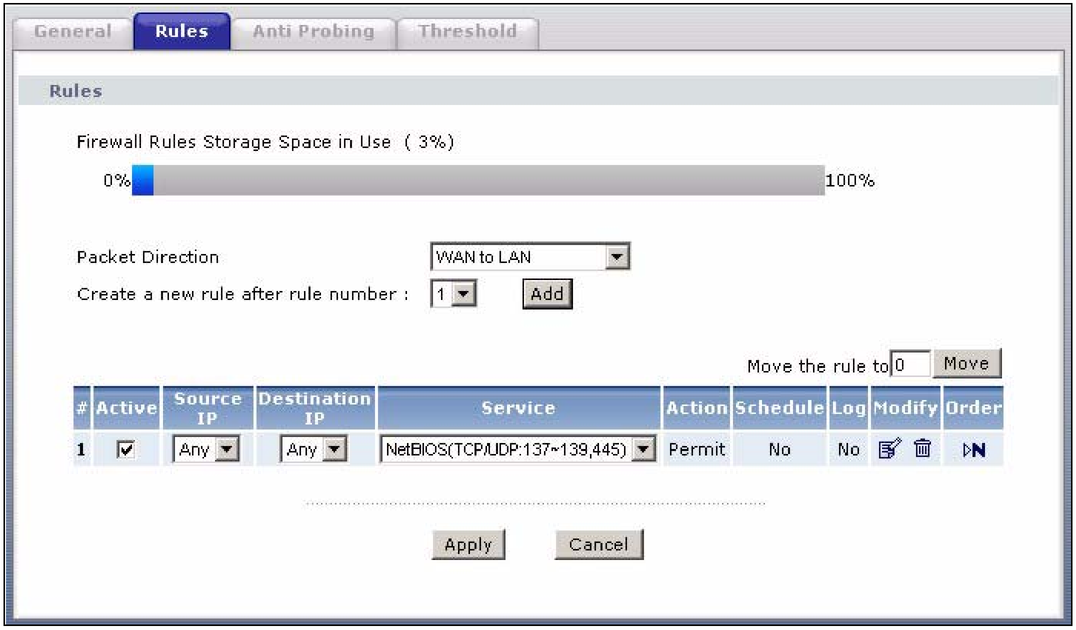
## 10.6 Firewall Rules Summary

**The ordering of your rules is very important as rules are applied in turn.**

Refer to Section 9.1 on page 143 for more information.

Click **Security** > **Firewall** > **Rules** to bring up the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

**Figure 91** Firewall Rules



Firewall Rules Storage Space in Use ( 3%)

0% 100%

Packet Direction: WAN to LAN

Create a new rule after rule number : 1 Add

Move the rule to 0 Move

| # | Active | Source IP | Destination IP | Service | Action | Schedule | Log | Modify | Order |
|---|---|---|---|---|---|---|---|---|---|
| 1 | ☑ | Any | Any | NetBIOS(TCP/UDP:137~139,445) | Permit | No | No | | |

The following table describes the labels in this screen.

**Table 57** Firewall Rules

| LABEL | DESCRIPTION |
|---|---|
| Firewall Rules Storage Space in Use | This read-only bar shows how much of the ZyXEL Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. |
| Packet Direction | Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules. |
| Create a new rule after rule number | Select an index number and click **Add** to add a new firewall rule after the selected index number. For example, if you select “6”, your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8. |
| | The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the **General** screen. |
| # | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. |
| Active | This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule. |
| Source IP | This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Destination IP | This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Service | This drop-down list box displays the services to which this firewall rule applies. See Section 10.8 on page 169 for more information. |
| Action | This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**) |
| Schedule | This field tells you whether a schedule is specified (**Yes**) or not (**No**). |

**Table 57** Firewall Rules (continued)

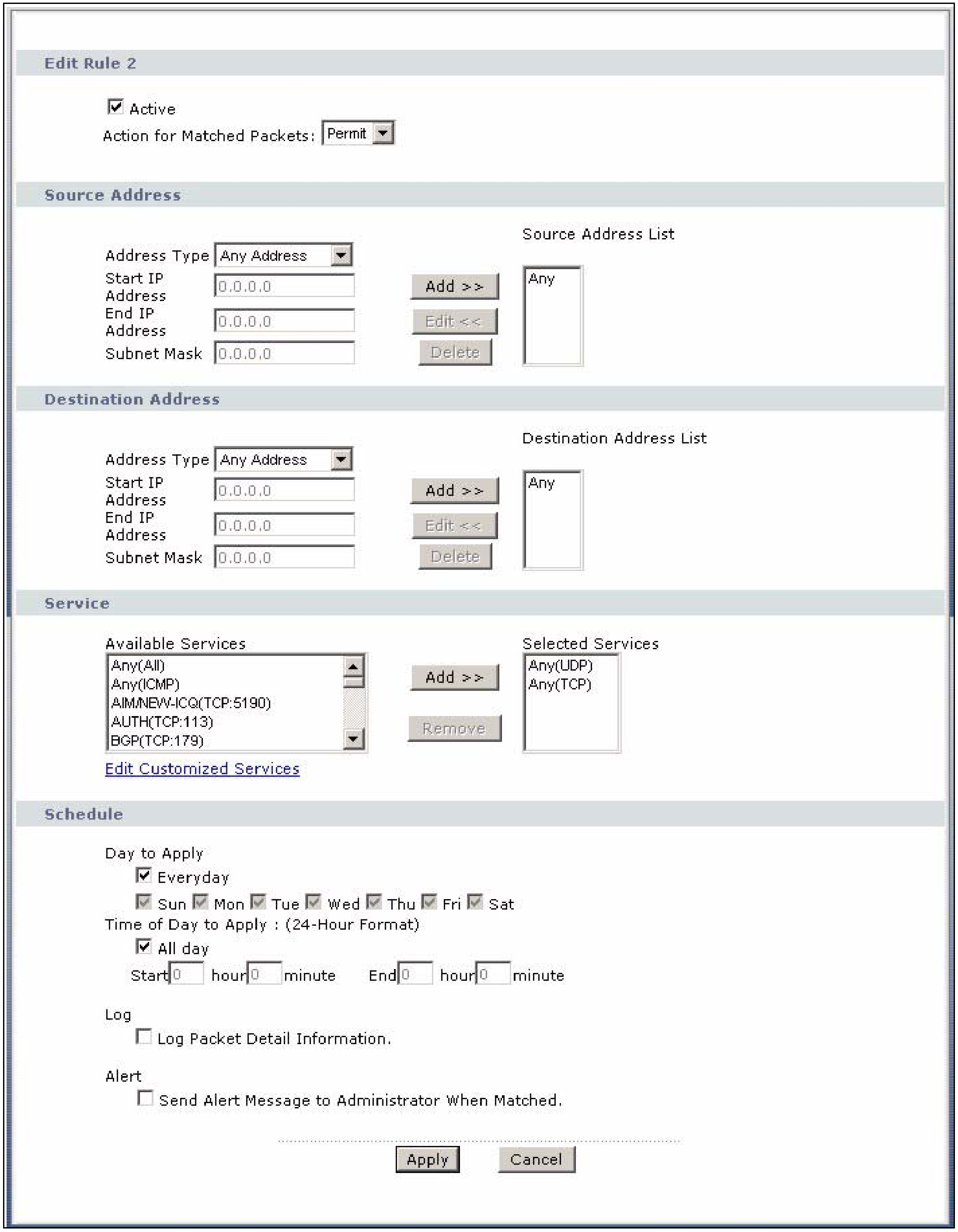
| LABEL | DESCRIPTION |
|---|---|
| Log | This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**). |
| Modify | Click the Edit icon to go to the screen where you can edit the rule.<br>Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action. |
| Order | Click the Move icon to display the **Move the rule to** field. Type a number in the **Move the rule to** field and click the **Move** button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

## 10.6.1 Configuring Firewall Rules

Refer to Section 9.1 on page 143 for more information.

In the **Rules** screen, select an index number and click **Add** or click a rule’s Edit icon to display this screen and refer to the following table for information on the labels.

**Figure 92** Firewall: Edit Rule



Edit Rule 2

☑ Active

Action for Matched Packets: Permit

Source Address

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Source Address List: Any

Destination Address

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Destination Address List: Any

Service

Available Services:
Any(All)
Any(ICMP)
AIM/NEW-ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)

Selected Services:
Any(UDP)
Any(TCP)

Edit Customized Services

Schedule

Day to Apply

☑ Everyday

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Apply : (24-Hour Format)

☑ All day

Start 0 hour 0 minute End 0 hour 0 minute

Log

☐ Log Packet Detail Information.

Alert

☐ Send Alert Message to Administrator When Matched.

The following table describes the labels in this screen.

**Table 58** Firewall: Edit Rule

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this option to enable this firewall rule. |
| Action for Matched Packet | Use the drop-down list box to select what the firewall is to do with packets that match this rule.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets. |
| Source/Destination Address | |
| Address Type | Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**. |
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Add >> | Click **Add >>** to add a new address to the **Source** or **Destination Address** box. You can add multiple addresses, ranges of addresses, and/or subnets. |
| Edit << | To edit an existing source or destination address, select it from the box and click **Edit <<**. |
| Delete | Highlight an existing source or destination address from the **Source** or **Destination Address** box above and click **Delete** to remove it. |
| Services | |
| Available/ Selected Services | Please see Section 10.8 on page 169 for more information on services available. Highlight a service from the **Available Services** box on the left, then click **Add >>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **Remove**. |
| Edit Customized Service | Click the **Edit Customized Services** link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services. |
| Schedule | |
| Day to Apply | Select everyday or the day(s) of the week to apply the rule. |
| Time of Day to Apply (24-Hour Format) | Select **All Day** or enter the start and end times in the hour-minute format to apply the rule. |
| Log | |
| Log Packet Detail Information | This field determines if a log for packets that match the rule is created or not. Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyXEL Device record these logs. |
| Alert | |
| Send Alert Message to Administrator When Matched | Select the check box to have the ZyXEL Device generate an alert when the rule is matched. |

**Table 58** Firewall: Edit Rule (continued)

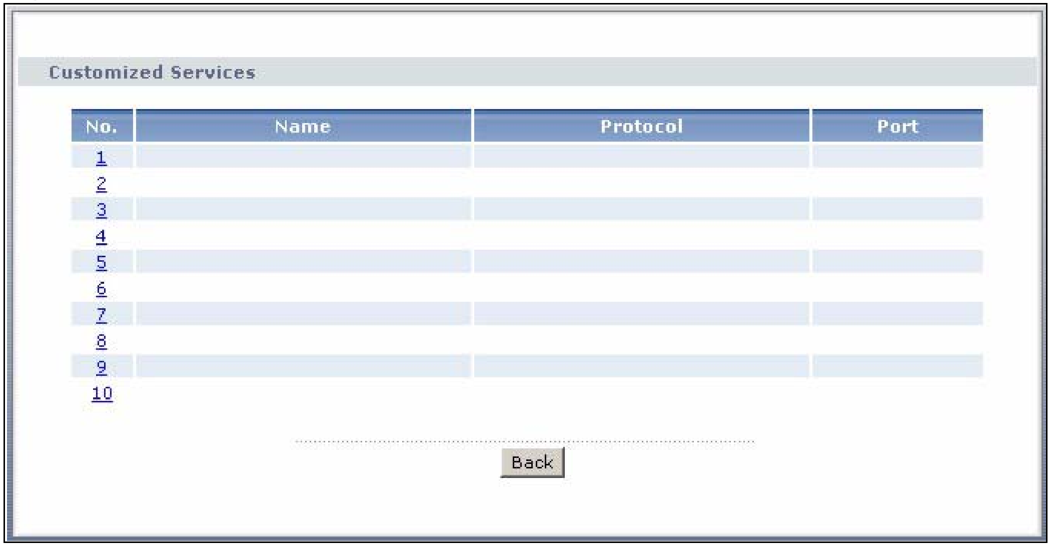
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 10.6.2 Customized Services

Configure customized services and port numbers not predefined by the ZyXEL Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read Section 10.8 on page 169. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Refer to Section 9.1 on page 143 for more information.

**Figure 93** Firewall: Customized Services



Customized Services

| No. | Name | Protocol | Port |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

The following table describes the labels in this screen.

**Table 59** Customized Services

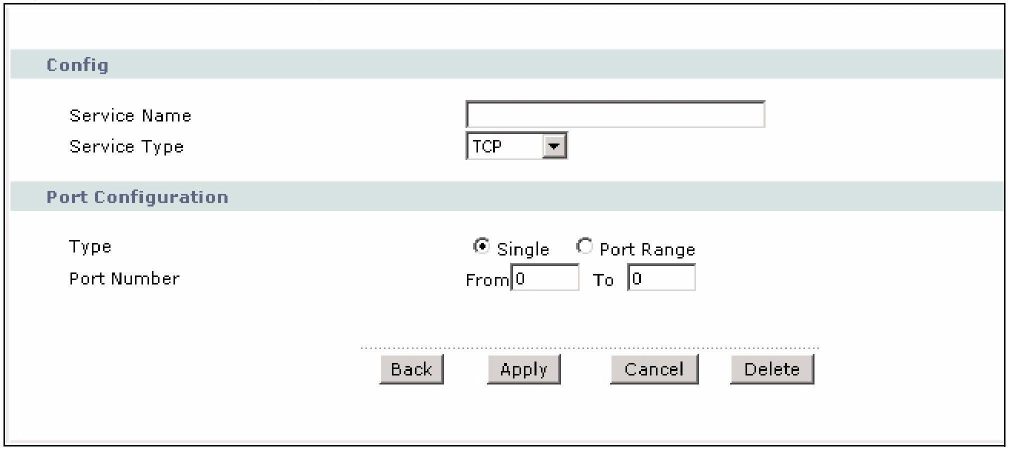
| LABEL | DESCRIPTION |
|---|---|
| No. | This is the number of your customized port. Click a rule's number of a service to go to a screen where you can configure or edit a customized service. See Section 10.6.3 on page 164 for more information. |
| Name | This is the name of your customized service. |
| Protocol | This shows the IP protocol (**TCP**, **UDP** or **TCP/UDP**) that defines your customized service. |
| Port | This is the port number or range that defines your customized service. |
| Back | Click **Back** to return the **Firewall Edit Rule** screen. |

## 10.6.3 Configuring a Customized Service

Click a rule number in the **Firewall Customized Services** screen to create a new custom port or edit an existing one. This action displays the following screen.

Refer to Section 9.1 on page 143 for more information.

**Figure 94** Firewall: Configure Customized Services



Config

Service Name

Service Type: TCP

Port Configuration

Type: ● Single ○ Port Range

Port Number: From 0 To 0

The following table describes the labels in this screen.

**Table 60** Firewall: Configure Customized Services

| LABEL | DESCRIPTION |
|---|---|
| Service Name | Type a unique name for your custom port. |
| Service Type | Choose the IP port (**TCP**, **UDP** or **TCP/UDP**) that defines your customized port from the drop down list box. |
| Port Configuration | |
| Type | Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. |
| Port Number | Type a single port number or the range of port numbers that define your customized service. |
| Back | Click **Back** to return to the previous screen. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to return to the previous screen. |
| Delete | Click **Delete** to delete the current rule and return to the previous screen. |

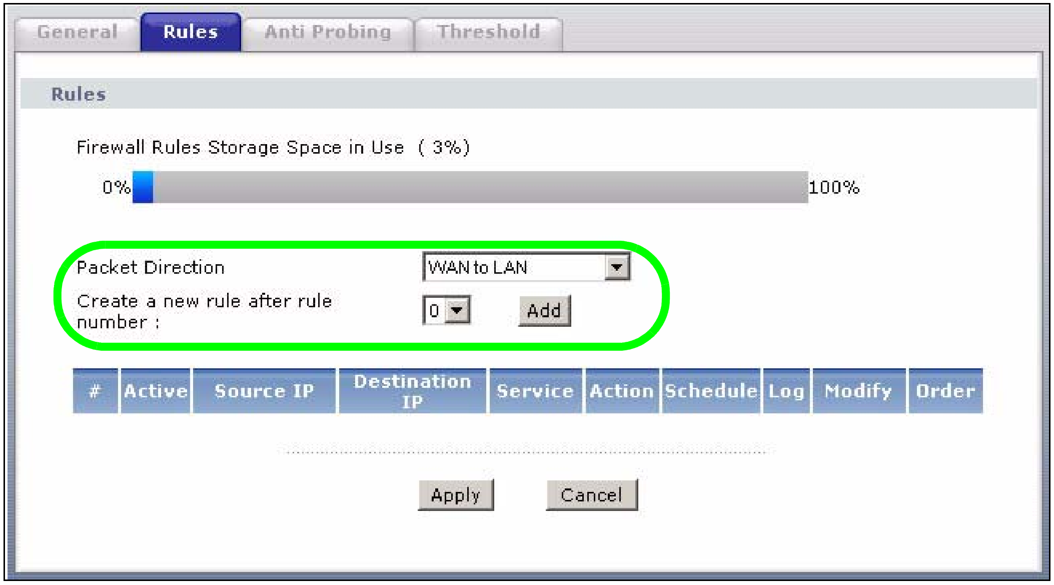
## 10.7 Example Firewall Rule

The following Internet firewall rule example allows a hypothetical “MyService” connection from the Internet.

1 Click **Security** > **Firewall** > **Rules**.

2 Select **WAN to LAN** in the **Packet Direction** field.

Figure 95   Firewall Example: Rules



Rules

Firewall Rules Storage Space in Use ( 3%)

0% 100%

Packet Direction: WAN to LAN

Create a new rule after rule number : 0

| # | Active | Source IP | Destination IP | Service | Action | Schedule | Log | Modify | Order |
|---|---|---|---|---|---|---|---|---|---|

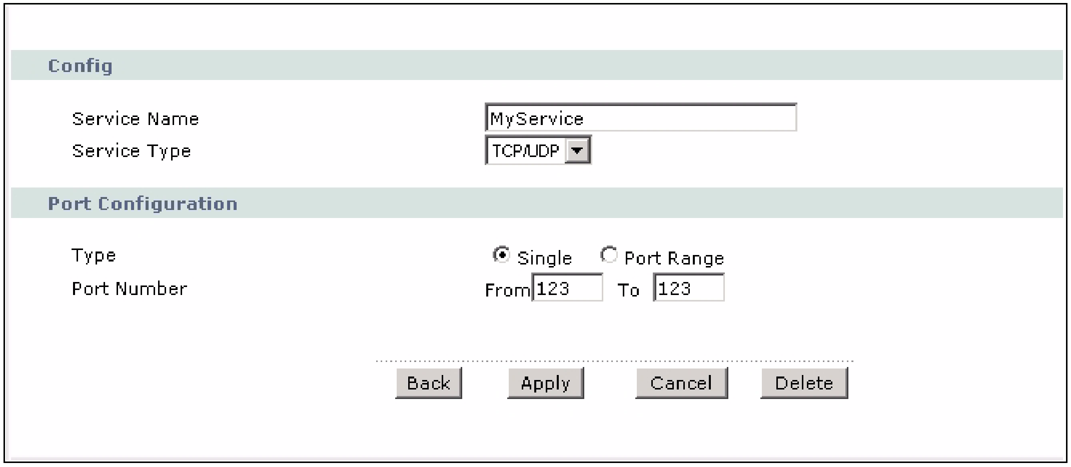
3 In the **Rules** screen, select the index number after that you want to add the rule. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.

4 Click **Add** to display the firewall rule configuration screen.

5 In the **Edit Rule** screen, click the **Edit Customized Services** link to open the **Customized Service** screen.

6 Click an index number to display the **Customized Services Config** screen and configure the screen as follows and click **Apply**.

Figure 96   Edit Custom Port Example



Config

Service Name: MyService

Service Type: TCP/UDP

Port Configuration

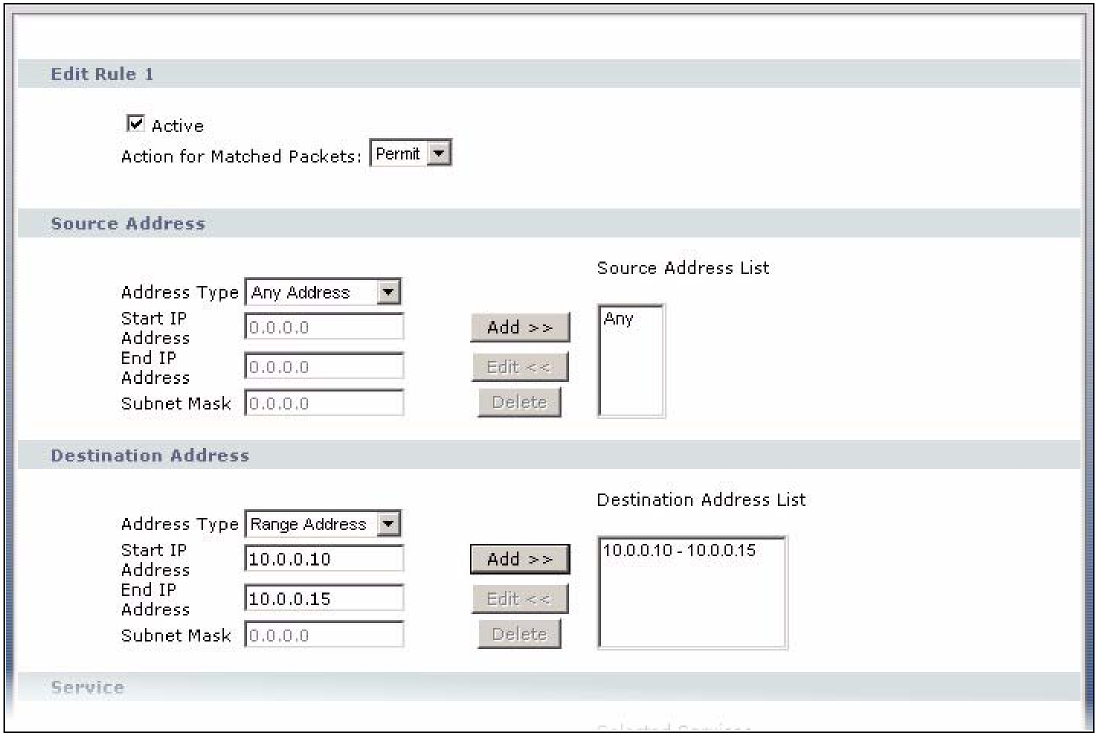
Type: ● Single ○ Port Range

Port Number: From 123 To 123

7 Select **Any** in the **Destination Address** box and then click **Delete**.

8 Configure the destination address screen as follows and click **Add**.

**Figure 97** Firewall Example: Edit Rule: Destination Address



Edit Rule 1

☑ Active

Action for Matched Packets: Permit

Source Address

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Source Address List: Any

Destination Address

Address Type: Range Address

Start IP Address: 10.0.0.10

End IP Address: 10.0.0.15

Subnet Mask: 0.0.0.0

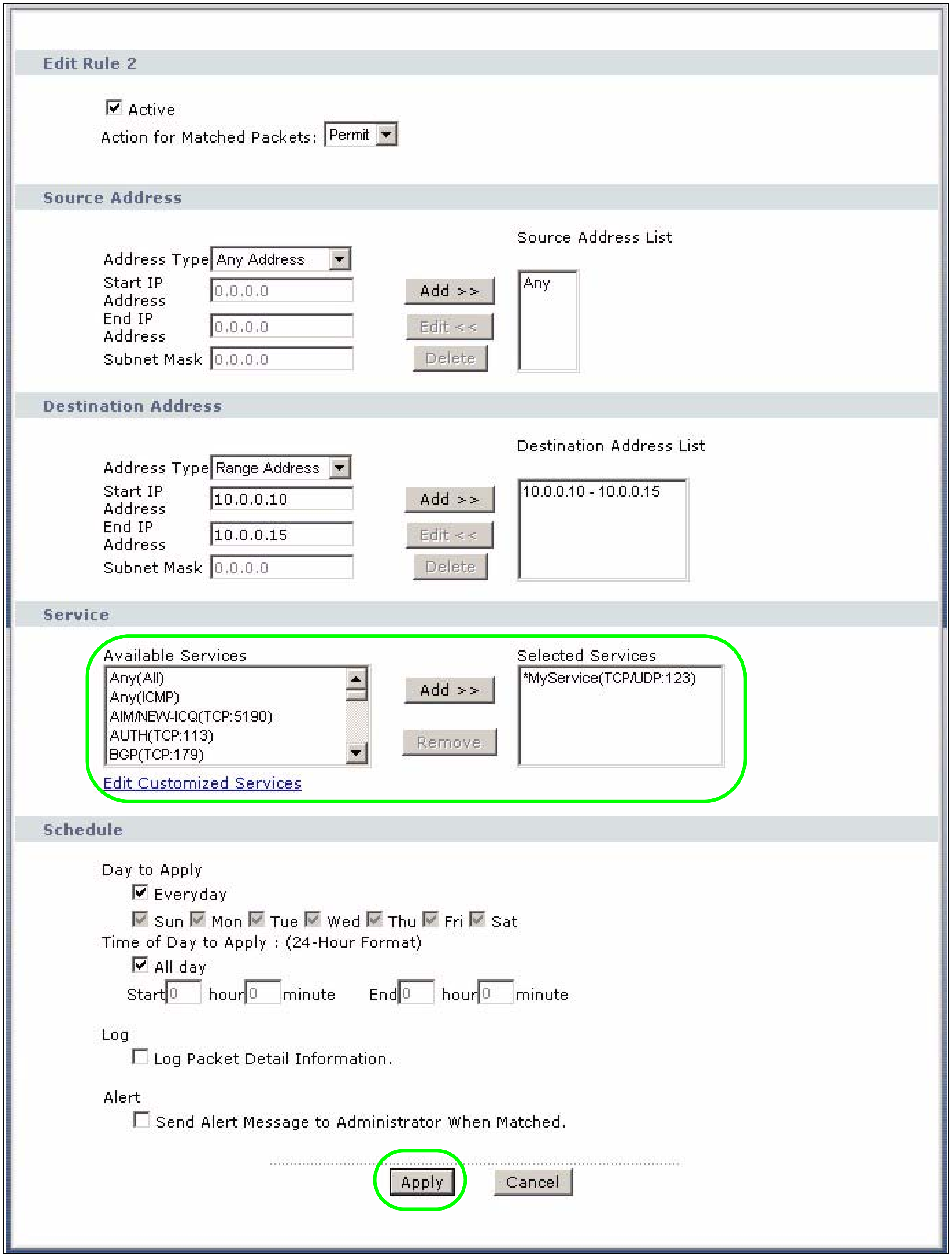
Destination Address List: 10.0.0.10 - 10.0.0.15

Service

9 Use the **Add >>** and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.

**Custom services show up with an "*" before their names in the Services list box and the Rules list box.**

**Figure 98** Firewall Example: Edit Rule: Select Customized Services



Edit Rule 2

☑ Active

Action for Matched Packets: Permit

Source Address

Address Type: Any Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Source Address List: Any

Destination Address

Address Type: Range Address

Start IP Address: 10.0.0.10

End IP Address: 10.0.0.15

Subnet Mask: 0.0.0.0

Destination Address List: 10.0.0.10 - 10.0.0.15

Service

Available Services: Any(All), Any(ICMP), AIM/NEW-ICQ(TCP:5190), AUTH(TCP:113), BGP(TCP:179)

Selected Services: *MyService(TCP/UDP:123)

Edit Customized Services

Schedule

Day to Apply

☑ Everyday

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Apply : (24-Hour Format)

☑ All day

Start 0 hour 0 minute End 0 hour 0 minute

Log

☐ Log Packet Detail Information.

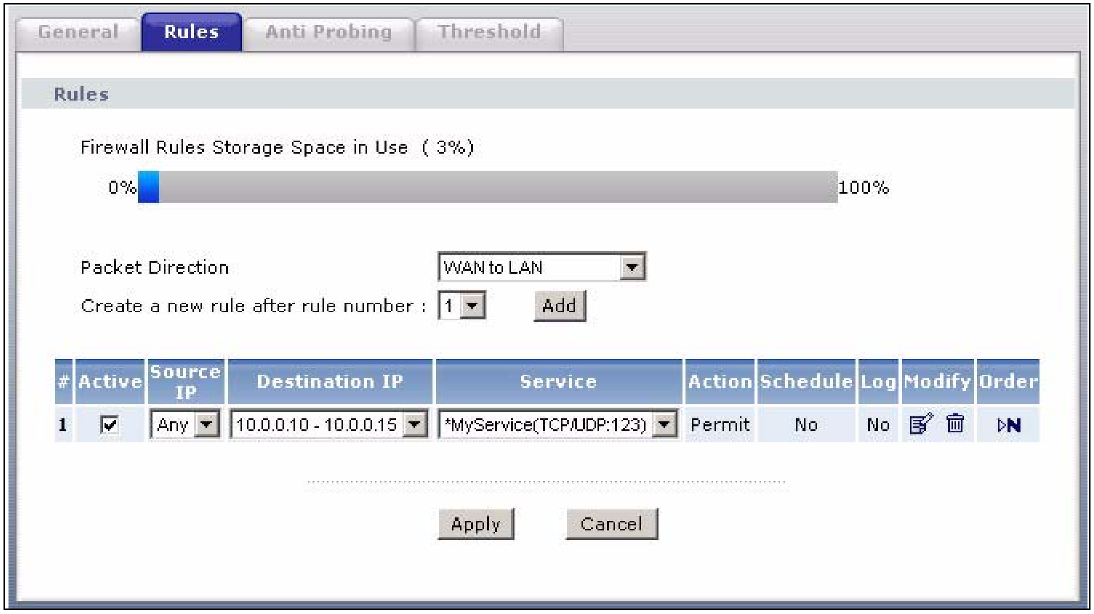
Alert

☐ Send Alert Message to Administrator When Matched.

On completing the configuration procedure for this Internet firewall rule, the **Rules** screen should look like the following.

Rule 1 allows a “MyService” connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

**Figure 99** Firewall Example: Rules: MyService



Rules

Firewall Rules Storage Space in Use ( 3%)

Packet Direction: WAN to LAN

Create a new rule after rule number : 1

| # | Active | Source IP | Destination IP | Service | Action | Schedule | Log | Modify | Order |
|---|---|---|---|---|---|---|---|---|---|
| 1 | ☑ | Any | 10.0.0.10 - 10.0.0.15 | *MyService(TCP/UDP:123) | Permit | No | No | | |

## 10.8 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see Section 10.6.1 on page 161) displays all predefined services that the ZyXEL Device already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom service ports may also be configured using the **Edit Customized Services** function discussed previously.

**Table 61** Predefined Services

| SERVICE | DESCRIPTION |
|---|---|
| AIM/NEW_ICQ(TCP:5190) | AOL's Internet Messenger service, used as a listening port by ICQ. |
| AUTH(TCP:113) | Authentication protocol used by some servers. |
| BGP(TCP:179) | Border Gateway Protocol. |
| BOOTP_CLIENT(UDP:68) | DHCP Client. |
| BOOTP_SERVER(UDP:67) | DHCP Server. |
| CU-SEEME(TCP/UDP:7648, 24032) | A popular videoconferencing solution from White Pines Software. |
| DNS(UDP/TCP:53) | Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers. |
| FINGER(TCP:79) | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP(TCP:20.21) | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323(TCP:1720) | Net Meeting uses this protocol. |

**Table 61** Predefined Services (continued)

| SERVICE | DESCRIPTION |
|---|---|
| HTTP(TCP:80) | Hyper Text Transfer Protocol - a client/server protocol for the world wide web. |
| HTTPS | HTTPS is a secured http session often used in e-commerce. |
| ICQ(UDP:4000) | This is a popular Internet chat program. |
| IPSEC_TRANSPORT/ TUNNEL(AH:0) | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| IPSEC_TUNNEL(ESP:0) | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| IRC(TCP/UDP:6667) | This is another popular Internet chat program. |
| MSN Messenger(TCP:1863) | Microsoft Networks' messenger service uses this protocol. |
| MULTICAST(IGMP:0) | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| NEWS(TCP:144) | A protocol for news groups. |
| NFS(UDP:2049) | Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments. |
| NNTP(TCP:119) | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING(ICMP:0) | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3(TCP:110) | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP(TCP:1723) | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL(GRE:0) | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel. |
| RCMD(TCP:512) | Remote Command Service. |
| REAL_AUDIO(TCP:7070) | A streaming audio service that enables real time sound over the web. |
| REXEC(TCP:514) | Remote Execution Daemon. |
| RLOGIN(TCP:513) | Remote Login. |
| RTELNET(TCP:107) | Remote Telnet. |
| RTSP(TCP/UDP:554) | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP(TCP:115) | Simple File Transfer Protocol. |
| SMTP(TCP:25) | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP(TCP/UDP:161) | Simple Network Management Program. |
| SNMP-TRAPS (TCP/ UDP:162) | Traps for use with the SNMP (RFC:1215). |
| SQL-NET(TCP:1521) | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSDP(UDP:1900) | Simole Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using DUDP port 1900. |

**Table 61** Predefined Services (continued)

| SERVICE | DESCRIPTION |
|---|---|
| SSH(TCP/UDP:22) | Secure Shell Remote Login Program. |
| STRMWORKS(UDP:1558) | Stream Works Protocol. |
| SYSLOG(UDP:514) | Syslog allows you to send system logs to a UNIX server. |
| TACACS(UDP:49) | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET(TCP:23) | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| TFTP(UDP:69) | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE(TCP:7000) | Another videoconferencing solution. |

## 10.9 Anti-Probing

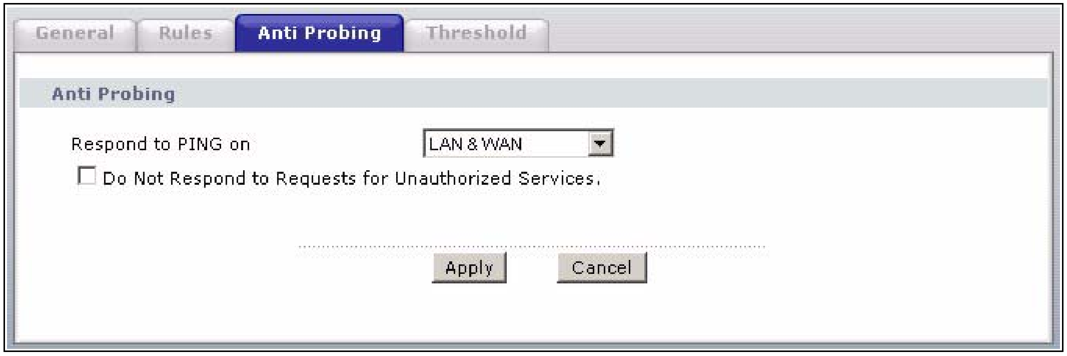
If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. The ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

Refer to Section 9.1 on page 143 for more information.

Click **Security** > **Firewall** > **Anti Probing** to display the screen as shown.

**Figure 100** Firewall: Anti Probing



Anti Probing

Respond to PING on: LAN & WAN

□ Do Not Respond to Requests for Unauthorized Services.

The following table describes the labels in this screen.

**Table 62** Firewall: Anti Probing

| LABEL | DESCRIPTION |
|---|---|
| Respond to PING on | The ZyXEL Device does not respond to any incoming Ping requests when **Disable** is selected.<br>Select **LAN** to reply to incoming LAN Ping requests.<br>Select **WAN** to reply to incoming WAN Ping requests.<br>Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests. |
| Do Not Respond to Requests for Unauthorized Services. | Select this option to prevent hackers from finding the ZyXEL Device by probing for unused ports. If you select this option, the ZyXEL Device will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyXEL Device unseen. By default this option is not selected and the ZyXEL Device will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.<br>Note that the probing packets must first traverse the ZyXEL Device's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyXEL Device reacts based on the corresponding firewall policy to send a TCP reset packet for a blocked TCP packet or an ICMP port-unreachable packet for a blocked UDP packets or just drop the packets without sending a response packet. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 10.10 DoS Thresholds

For DoS attacks, the ZyXEL Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Refer to Section 10.10.3 on page 173 to configure thresholds.

## 10.10.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for most small offices. Factors influencing choices for threshold values are:

- The maximum number of opened sessions.
- The minimum capacity of server backlog in your LAN network.
- The CPU power of servers in your LAN network.
- Network bandwidth.
- Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

## 10.10.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see Figure 86 on page 146). For UDP, "half-open" means that the firewall has detected no return traffic.

The ZyXEL Device measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the ZyXEL Device starts deleting half-open sessions as required to accommodate new connection requests. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

### 10.10.2.1 TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the ZyXEL Device starts deleting half-open sessions according to one of the following methods:

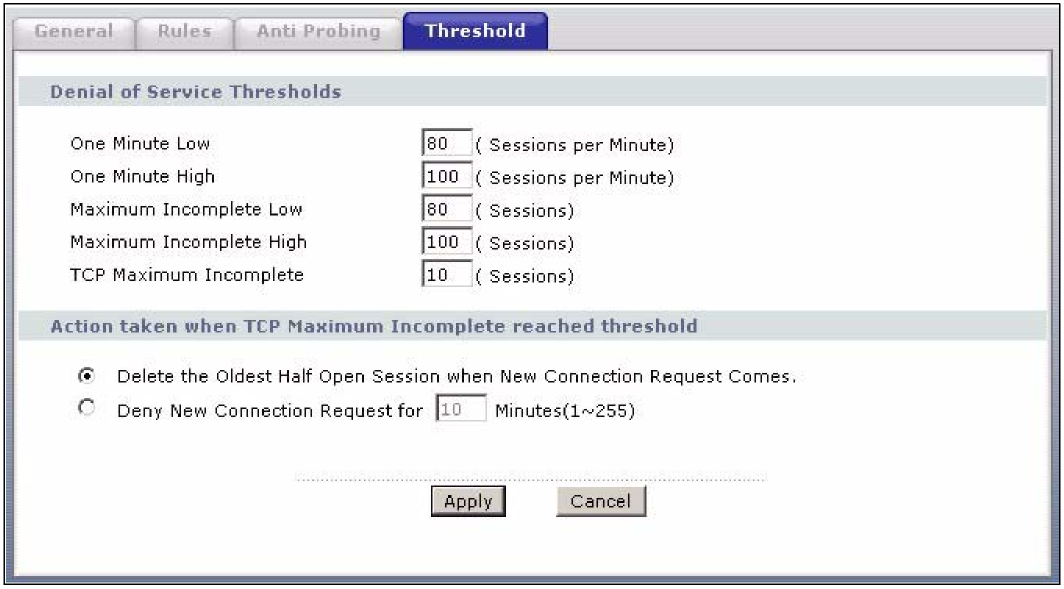
- If the **Blocking Time** timeout is 0 (the default), then the ZyXEL Device deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Time** timeout is greater than 0, then the ZyXEL Device blocks all new connection requests to the host giving the server time to handle the present connections. The ZyXEL Device continues to block all new connection requests until the **Blocking Time** expires.

## 10.10.3 Configuring Firewall Thresholds

The ZyXEL Device also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall**, and **Threshold** to bring up the next screen.

**Figure 101** Firewall: Threshold



Denial of Service Thresholds

| | |
|---|---|
| One Minute Low | 80 ( Sessions per Minute) |
| One Minute High | 100 ( Sessions per Minute) |
| Maximum Incomplete Low | 80 ( Sessions) |
| Maximum Incomplete High | 100 ( Sessions) |
| TCP Maximum Incomplete | 10 ( Sessions) |

Action taken when TCP Maximum Incomplete reached threshold

● Delete the Oldest Half Open Session when New Connection Request Comes.

○ Deny New Connection Request for 10 Minutes(1~255)

The following table describes the labels in this screen.

**Table 63** Firewall: Threshold

| LABEL | DESCRIPTION | DEFAULT VALUES |
|---|---|---|
| Denial of Service Thresholds | | |
| One Minute Low | This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number. | 80 existing half-open sessions. |
| One Minute High | This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection attempts. | 100 half-open sessions per minute. The above numbers cause the ZyXEL Device to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute. |
| Maximum Incomplete Low | This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyXEL Device continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number. | 80 existing half-open sessions. |

**Table 63** Firewall: Threshold (continued)

| LABEL | DESCRIPTION | DEFAULT VALUES |
|---|---|---|
| Maximum Incomplete High | This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyXEL Device deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum** I**ncomplete Low** number. | 100 existing half-open sessions. The above values causes the ZyXEL Device to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80. |
| TCP Maximum Incomplete | This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. | 10 existing half-open TCP sessions. |
| Action taken when the TCP Maximum Incomplete threshold is reached. | | |
| Delete the oldest half open session when new connection request comes | Select this radio button to clear the oldest half open session when a new connection request comes. | |
| Deny new connection request for | Select this radio button and specify for how long the ZyXEL Device should block new connection requests when **TCP Maximum Incomplete** is reached.<br>Enter the length of blocking time in minutes (between 1 and 256). | |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. | |
| Cancel | Click **Cancel** to begin configuring this screen afresh. | |

# 11

# Content Filtering

This chapter covers how to configure content filtering.

## 11.1 Content Filtering Overview

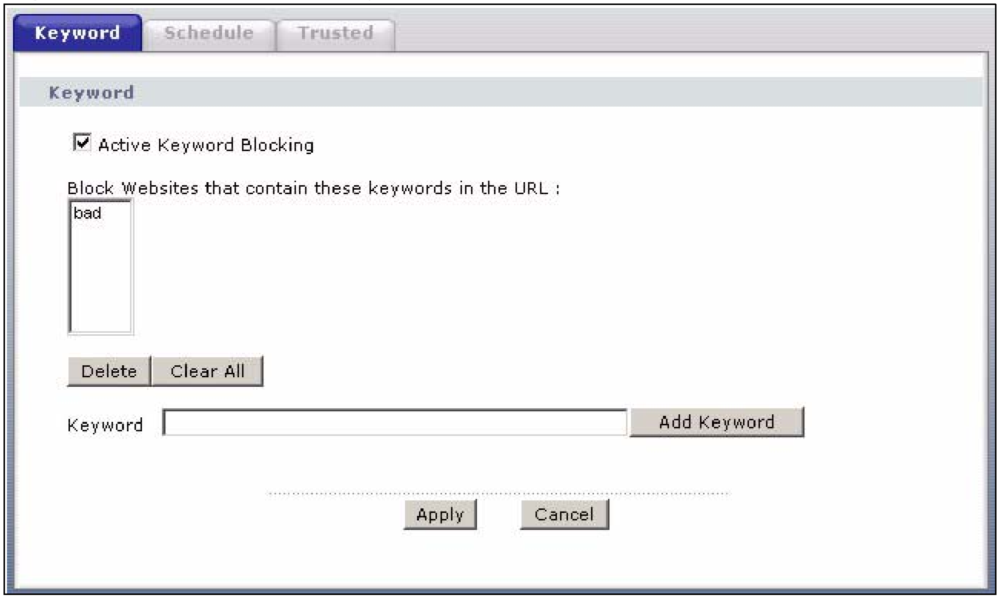
Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering gives you the ability to block web sites that contain key words (that you specify) in the URL. You can set a schedule for when the ZyXEL Device performs content filtering. You can also specify trusted IP addresses on the LAN for which the ZyXEL Device will not perform content filtering.

## 11.2 Configuring Keyword Blocking

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the ZyXEL Device blocks all sites containing this keyword including the URL http://www.website.com/bad.html, even if it is not included in the Filter List.

To have your ZyXEL Device block Web sites containing keywords in their URLs, click **Security > Content Filter**. The screen appears as shown.

**Figure 102** Content Filter: Keyword



☑ Active Keyword Blocking

Block Websites that contain these keywords in the URL :

bad

The following table describes the labels in this screen.

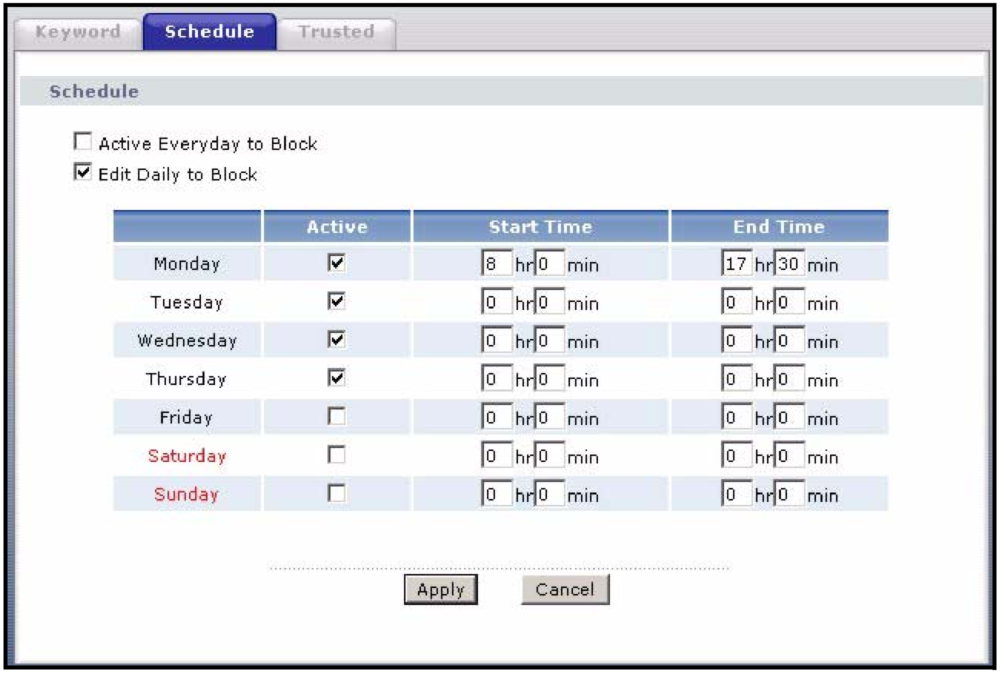
**Table 64** Content Filter: Keyword

| LABEL | DESCRIPTION |
|---|---|
| Active Keyword Blocking | Select this check box to enable this feature. |
| Block Websites that contain these keywords in the URL: | This box contains the list of all the keywords that you have configured the ZyXEL Device to block. |
| Delete | Highlight a keyword in the box and click **Delete** to remove it. |
| Clear All | Click **Clear All** to remove all of the keywords from the list. |
| Keyword | Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed. |
| Add Keyword | Click **Add Keyword** after you have typed a keyword.<br>Repeat this procedure to add other keywords. Up to 64 keywords are allowed.<br>When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to return to the previously saved settings. |

## 11.3 Configuring the Schedule

To set the days and times for the ZyXEL Device to perform content filtering, click **Security** > **Content Filter** > **Schedule**. The screen appears as shown.

**Figure 103** Content Filter: Schedule



Schedule

□ Active Everyday to Block

☑ Edit Daily to Block

| | Active | Start Time | End Time |
|---|---|---|---|
| Monday | ☑ | 8 hr 0 min | 17 hr 30 min |
| Tuesday | ☑ | 0 hr 0 min | 0 hr 0 min |
| Wednesday | ☑ | 0 hr 0 min | 0 hr 0 min |
| Thursday | ☑ | 0 hr 0 min | 0 hr 0 min |
| Friday | □ | 0 hr 0 min | 0 hr 0 min |
| Saturday | □ | 0 hr 0 min | 0 hr 0 min |
| Sunday | □ | 0 hr 0 min | 0 hr 0 min |

The following table describes the labels in this screen.

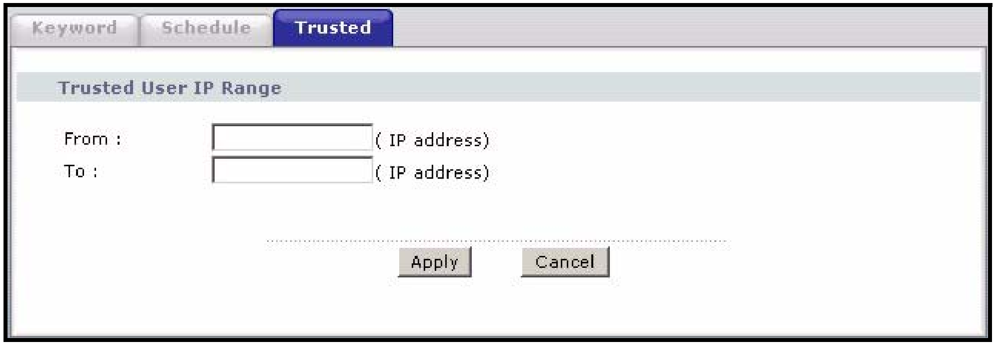
Table 65 Content Filter: Schedule

| LABEL | DESCRIPTION |
|---|---|
| Schedule | Select **Active Everyday to Block** to make the content filtering active everyday.<br>Otherwise, select **Edit Daily to Block** and configure which days of the week (or everyday) and which time of the day you want the content filtering to be active. |
| Active Everyday to Block | Select this option to allow continuous filtering of websites based on the keywords you have chosen. |
| Edit Daily to Block | Select this option to filter websites according to the day(s) and time(s) configured. |
| Active | Select the check box to have the content filtering active on the selected day. |
| Start TIme | Enter the start time when you want the content filtering to take effect in hour-minute format. |
| End Time | Enter the end time when you want the content filtering to stop in hour-minute format. |
| Apply | Click **Apply** to save your changes. |
| Cancel | Click **Cancel** to return to the previously saved settings. |

## 11.4 Configuring Trusted Computers

To exclude a range of users on the LAN from content filtering on your ZyXEL Device, click **Security > Content Filter** > **Trusted**. The screen appears as shown.

Figure 104 Content Filter: Trusted



The following table describes the labels in this screen.

Table 66 Content Filter: Trusted

| LABEL | DESCRIPTION |
|---|---|
| Trusted User IP Range | |
| From | Type the IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering. |
| To | Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to return to the previously saved settings. |

# PART V
# Advanced

# 12

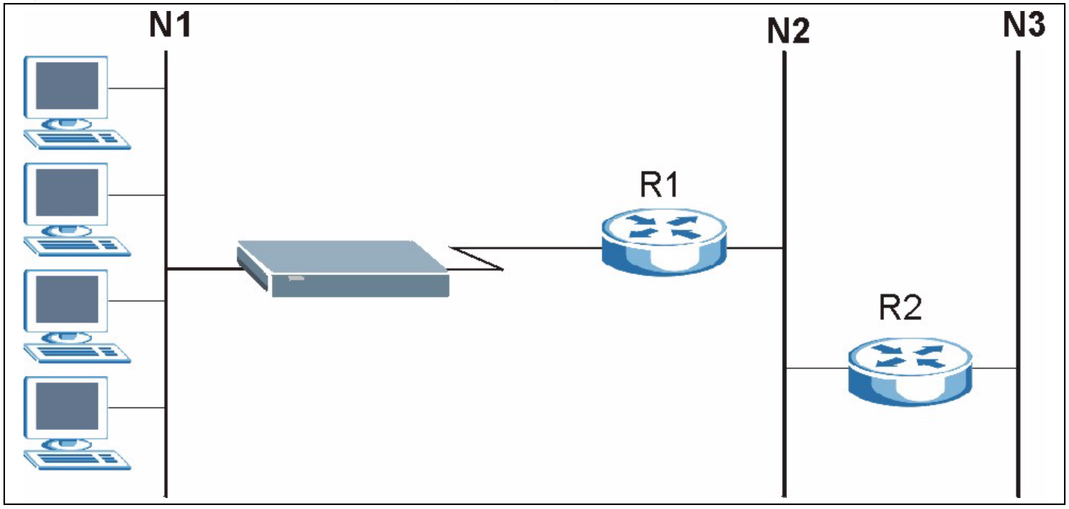
# Static Route

This chapter shows you how to configure static routes for your ZyXEL Device.

## 12.1 Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

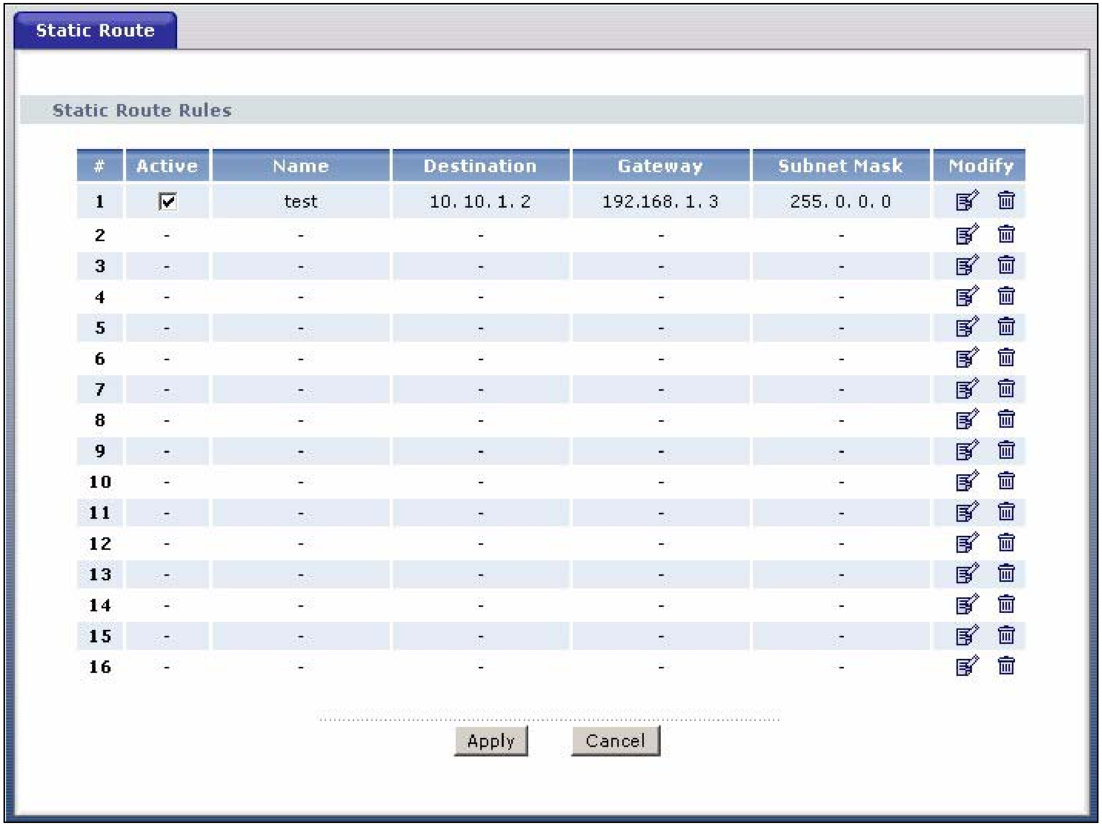
**Figure 105** Example of Static Routing Topology



## 12.2 Configuring Static Route

Click **Advanced** > **Static Route** to open the **Static Route** screen.

**Figure 106** Static Route



Static Route Rules

| # | Active | Name | Destination | Gateway | Subnet Mask | Modify |
|---|---|---|---|---|---|---|
| 1 | ☑ | test | 10.10.1.2 | 192.168.1.3 | 255.0.0.0 | ✎ 🗑 |
| 2 | - | - | - | - | - | ✎ 🗑 |
| 3 | - | - | - | - | - | ✎ 🗑 |
| 4 | - | - | - | - | - | ✎ 🗑 |
| 5 | - | - | - | - | - | ✎ 🗑 |
| 6 | - | - | - | - | - | ✎ 🗑 |
| 7 | - | - | - | - | - | ✎ 🗑 |
| 8 | - | - | - | - | - | ✎ 🗑 |
| 9 | - | - | - | - | - | ✎ 🗑 |
| 10 | - | - | - | - | - | ✎ 🗑 |
| 11 | - | - | - | - | - | ✎ 🗑 |
| 12 | - | - | - | - | - | ✎ 🗑 |
| 13 | - | - | - | - | - | ✎ 🗑 |
| 14 | - | - | - | - | - | ✎ 🗑 |
| 15 | - | - | - | - | - | ✎ 🗑 |
| 16 | - | - | - | - | - | ✎ 🗑 |

The following table describes the labels in this screen.

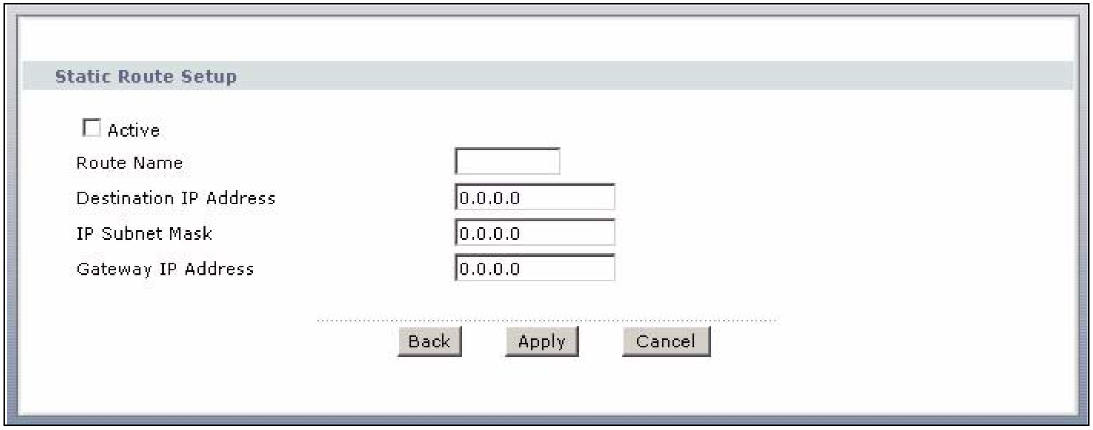
**Table 67** Static Route

| LABEL | DESCRIPTION |
|---|---|
| # | This is the number of an individual static route. |
| Active | Select the check box to activate this static route. Otherwise, clear the check box. |
| Name | This is the name that describes or identifies this route. |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Gateway | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Subnet Mask | This is the IP subnet mask. |
| Modify | Click the Edit icon to go to the screen where you can set up a static route on the ZyXEL Device.<br>Click the Delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route. |

## 12.2.1 Static Route Edit

Select a static route index number and click **Edit** (✎). The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 107** Static Route Edit



Static Route Setup

☐ Active

| | |
|---|---|
| Route Name | |
| Destination IP Address | 0.0.0.0 |
| IP Subnet Mask | 0.0.0.0 |
| Gateway IP Address | 0.0.0.0 |

The following table describes the labels in this screen.

**Table 68** Static Route Edit

| LABEL | DESCRIPTION |
|---|---|
| Active | This field allows you to activate/deactivate this static route. |
| Route Name | Enter the name of the IP static route. Leave this field blank to delete this static route. |
| Destination IP Address | This parameter specifies the IP network address of the final destination.  Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Enter the IP subnet mask here. |
| Gateway IP Address | Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Back | Click **Back** to return to the previous screen without saving. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

13

# Bandwidth Management

This chapter contains information about configuring bandwidth management, editing rules and viewing the ZyXEL Device's bandwidth management logs.

## 13.1 Bandwidth Management Overview

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The ZyXEL Device applies bandwidth management to traffic that it forwards out through an interface. The ZyXEL Device does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management.

The sum of the bandwidth allotments that apply to any interface must be less than or equal to the speed allocated to that interface in the **Bandwidth Management** > **Summary** screen.

## 13.2 Application-based Bandwidth Management

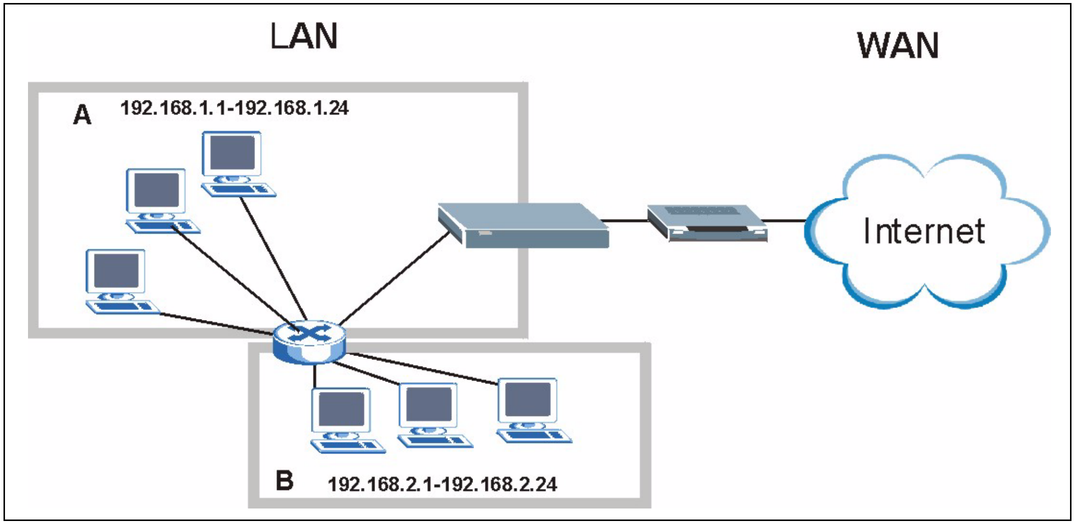
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

## 13.3 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet **A** and another for subnet **B**.

**Figure 108** Subnet-based Bandwidth Management Example



## 13.4 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

**Table 69** Application and Subnet-based Bandwidth Management Example

| TRAFFIC TYPE | FROM SUBNET A | FROM SUBNET B |
|---|---|---|
| VoIP | 64 Kbps | 64 Kbps |
| Web | 64 Kbps | 64 Kbps |
| FTP | 64 Kbps | 64 Kbps |
| E-mail | 64 Kbps | 64 Kbps |
| Video | 64 Kbps | 64 Kbps |

## 13.5 Scheduler

The scheduler divides up an interface’s bandwidth among the bandwidth classes. The ZyXEL Device has two types of scheduler: fairness-based and priority-based.

### 13.5.1 Priority-based Scheduler

With the priority-based scheduler, the ZyXEL Device forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class’s priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

### 13.5.2 Fairness-based Scheduler

The ZyXEL Device divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

## 13.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see Figure 109 on page 192) allows the ZyXEL Device to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyXEL Device first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the ZyXEL Device divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the ZyXEL Device gives extra bandwidth to that class.

When multiple classes require more bandwidth, the ZyXEL Device gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The ZyXEL Device distributes the available bandwidth equally among classes with the same priority level.

### 13.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following three steps to configure the ZyXEL Device to allow bandwidth for traffic that is not defined in a bandwidth filter.

1 Leave some of the interface's bandwidth unbudgeted.

2 Do not enable the interface's **Maximize Bandwidth Usage** option.

3 Do not enable bandwidth borrowing on the child-classes that have the root class as their parent (see Section 13.9 on page 192).

### 13.6.2 Maximize Bandwidth Usage Example

Here is an example of a ZyXEL Device that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The unbudgeted 2048 kbps allows traffic not defined in any of the bandwidth filters to go out when you do not select the maximize bandwidth option.

**Table 70** Maximize Bandwidth Usage Example

| BANDWIDTH CLASSES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: 2048 kbps |
| | Sales: 2048 kbps |
| | Marketing: 2048 kbps |
| | Research: 2048 kbps |

The ZyXEL Device divides up the unbudgeted 2048 kbps among the classes that require more bandwidth. If the administration department only uses 1024 kbps of the budgeted 2048 kbps, the ZyXEL Device also divides the remaining 1024 kbps among the classes that require more bandwidth. Therefore, the ZyXEL Device divides a total of 3072 kbps of unbudgeted and unused bandwidth among the classes that require more bandwidth.

#### 13.6.2.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the priorities of the bandwidth classes and the amount of bandwidth that each class gets.

**Table 71** Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

| BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: Priority 4, 1024 kbps |
| | Sales: Priority 6, 3584 kbps |
| | Marketing: Priority 6, 3584 kbps |
| | Research: Priority 5, 2048 kbps |

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The sales and marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1536 kbps or more of extra bandwidth, the ZyXEL Device divides the total 3072 kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1536 kbps extra to each for a total of 3584 kbps for each) because they both have the highest priority level.
- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

#### 13.6.2.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the amount of bandwidth that each class gets.

**Table 72** Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

| BANDWIDTH CLASSES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: 1024 kbps |
| | Sales: 3072 kbps |
| | Marketing: 3072 kbps |
| | Research: 3072 kbps |

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The ZyXEL Device divides the total 3072 kbps total of unbudgeted and unused bandwidth equally among the other classes. 1024 kbps extra goes to each so the other classes each get a total of 3072 kbps.

### 13.6.3 Bandwidth Management Priorities

The following table describes the priorities that you can apply to traffic that the ZyXEL Device forwards out through an interface.

**Table 73** Bandwidth Management Priorities

| PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED. | |
|---|---|
| High | Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay). |
| Mid | Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay. |
| Low | This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users. |

## 13.7 Over Allotment of Bandwidth

You can set the bandwidth management speed for an interface higher than the interface’s actual transmission speed. Higher priority traffic gets to use up to its allocated bandwidth, even if it takes up all of the interface’s available bandwidth. This could stop lower priority traffic from being sent. The following is an example.

**Table 74** Over Allotment of Bandwidth Example

| BANDWIDTH CLASSES, ALLOTMENTS | | PRIORITIES |
|---|---|---|
| Actual outgoing bandwidth available on the interface: 1000 kbps | | |
| Root Class: 1500 kbps (same as Speed setting) | VoIP traffic (Service = SIP): 500 Kbps | High |
| | NetMeeting traffic (Service = H.323): 500 kbps | High |
| | FTP (Service = FTP): 500 Kbps | Medium |

If you use VoIP and NetMeeting at the same time, the device allocates up to 500 Kbps of bandwidth to each of them before it allocates any bandwidth to FTP. As a result, FTP can only use bandwidth when VoIP and NetMeeting do not use all of their allocated bandwidth.

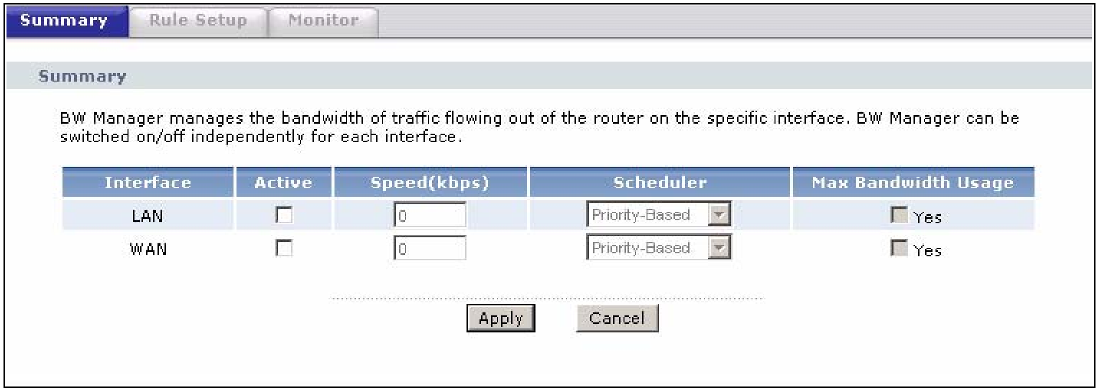
Suppose you try to browse the web too. In this case, VoIP, NetMeeting and FTP all have higher priority, so they get to use the bandwidth first. You can only browse the web when VoIP, NetMeeting, and FTP do not use all 1000 Kbps of available bandwidth.

## 13.8 Configuring Summary

Click **Advanced > Bandwidth MGMT** to open the screen as shown next.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

**Figure 109** Bandwidth Management: Summary



BW Manager manages the bandwidth of traffic flowing out of the router on the specific interface. BW Manager can be switched on/off independently for each interface.

| Interface | Active | Speed(kbps) | Scheduler | Max Bandwidth Usage |
|---|---|---|---|---|
| LAN | □ | 0 | Priority-Based | □ Yes |
| WAN | □ | 0 | Priority-Based | □ Yes |

The following table describes the labels in this screen.

**Table 75** Media Bandwidth Management: Summary

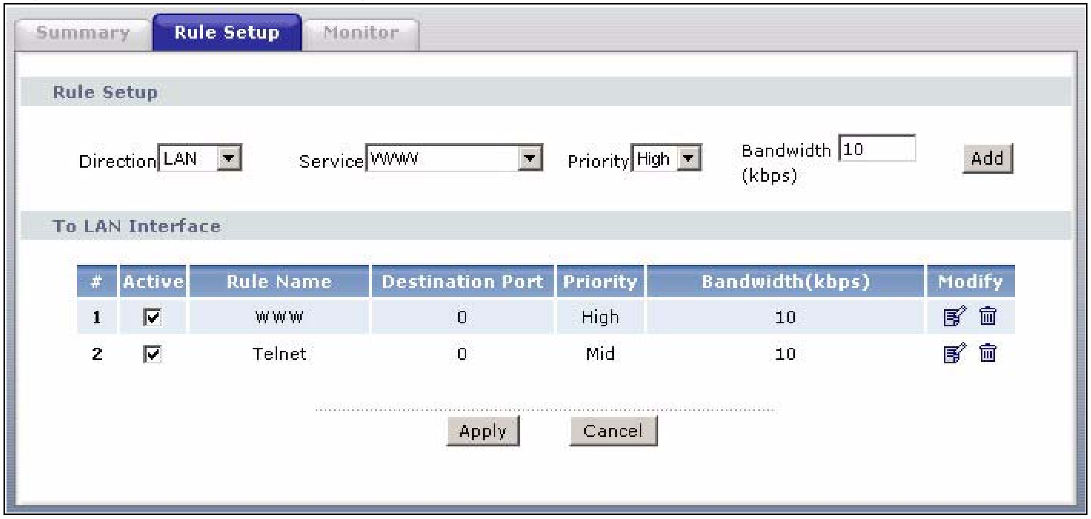
| LABEL | DESCRIPTION |
|---|---|
| Interface | These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.<br>Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the ZyXEL Device and be managed by bandwidth management. |
| Active | Select an interface's check box to enable bandwidth management on that interface. |
| Speed (kbps) | Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.<br>The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps.<br>You can set this number higher than the interface's actual transmission speed. This may stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth.<br>You can also set this number lower than the interface's actual transmission speed. If you do not enable **Max Bandwidth Usage**, this will cause the ZyXEL Device to not use some of the interface's available bandwidth. |
| Scheduler | Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow.<br>Select **Priority-Based** to give preference to bandwidth classes with higher priorities.<br>Select **Fairness-Based** to treat all bandwidth classes equally. |
| Max Bandwidth Usage | Select this check box to have the ZyXEL Device divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the speed of this interface (see the **Speed** field description). |
| Apply | Click **Apply** to save your settings to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

## 13.9 Bandwidth Management Rule Setup

You must use the **Bandwidth Management Summary** screen to enable bandwidth management on an interface before you can configure rules for that interface.

Click **Advanced** > **Bandwidth MGMT** > **Rule Setup** to open the following screen.

**Figure 110** Bandwidth Management: Rule Setup



Rule Setup

Direction: LAN
Service: WWW
Priority: High
Bandwidth (kbps): 10

To LAN Interface

| # | Active | Rule Name | Destination Port | Priority | Bandwidth(kbps) | Modify |
|---|---|---|---|---|---|---|
| 1 | ☑ | WWW | 0 | High | 10 | |
| 2 | ☑ | Telnet | 0 | Mid | 10 | |

The following table describes the labels in this screen.

**Table 76** Bandwidth Management: Rule Setup

| LABEL | DESCRIPTION |
|---|---|
| Direction | Select the direction of traffic to which you want to apply bandwidth management. |
| Service | Select a service for your rule or you can select **User Defined** to go to the screen where you can define your own. |
| Priority | Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**. |
| Bandwidth (kbps) | Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule. |
| Add | Click this button to add a rule to the following table. |
| To LAN Interface | |
| # | This is the number of an individual bandwidth management rule. |
| Active | This displays whether the rule is enabled. Select this check box to have the ZyXEL Device apply this bandwidth management rule.<br>Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule.<br>Enabling a bandwidth management rule also allows you to control the maximum amounts of bandwidth that can be used by traffic that matches the rule. |
| Rule Name | This is the name of the rule. |
| Destination Port | This is the port number of the destination. 0 means any destination port. |
| Priority | This is the priority of this rule. |
| Bandwidth (kbps) | This is the maximum bandwidth allowed for the rule in kbps. |
| Modify | Click the Edit icon to go to the screen where you can edit the rule.<br>Click the Remove icon to delete an existing rule. |
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

# 13.10 DiffServ

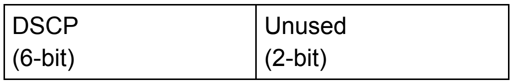
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

## 13.10.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

**Figure 111** DiffServ: Differentiated Service Field



| | |
|---|---|
| DSCP<br>(6-bit) | Unused<br>(2-bit) |

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

PHB consists of two types of services: EF (Expedited Forwarding) and AF (Assured Forwarding). EF has higher priority. EF guarantees services with minimal loss and delay. AF has four sub-classes, each with three levels of importance (drop precedence). A high drop precedence means low importance.

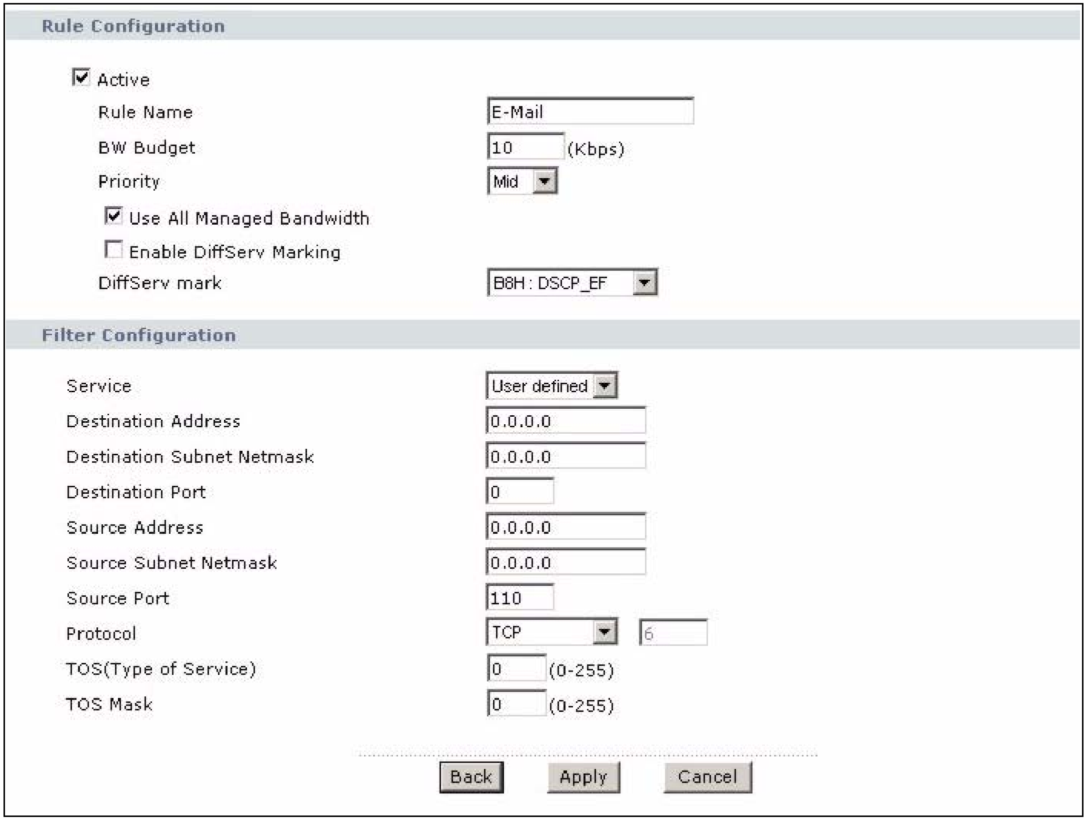
**Table 77** Sub-Classes of AF Services

| DIFFSERV PRIORITY | LOW DROP PRECEDENCE | MEDIUM DROP PRECEDENCE | HIGH DROP PRECEDENCE |
|---|---|---|---|
| SUB-CLASS4 | AF41 | AF42 | AF43 |
| SUB-CLASS3 | AF31 | AF32 | AF33 |
| SUB-CLASS2 | AF21 | AF22 | AF23 |
| SUB-CLASS1 | AF11 | AF12 | AF13 |

## 13.10.2 Rule Configuration

Click the Edit icon or select **User Defined** from the **Service** drop-down list in the **Rule Setup** screen to configure a bandwidth management rule. Use bandwidth rules to allocate specific amounts of bandwidth capacity (bandwidth budgets) to specific applications and/or subnets.

**Figure 112** Bandwidth Management Rule Configuration



Rule Configuration

☑ Active

Rule Name: E-Mail

BW Budget: 10 (Kbps)

Priority: Mid

☑ Use All Managed Bandwidth

□ Enable DiffServ Marking

DiffServ mark: B8H : DSCP_EF

Filter Configuration

Service: User defined

Destination Address: 0.0.0.0

Destination Subnet Netmask: 0.0.0.0

Destination Port: 0

Source Address: 0.0.0.0

Source Subnet Netmask: 0.0.0.0

Source Port: 110

Protocol: TCP 6

TOS(Type of Service): 0 (0-255)

TOS Mask: 0 (0-255)

The following table describes the labels in this screen.

**Table 78** Bandwidth Management Rule Configuration

| LABEL | DESCRIPTION |
|---|---|
| Rule Configuration | |
| Active | Select this check box to have the ZyXEL Device apply this bandwidth management rule.<br>Enable a bandwidth management rule to give traffic that matches the rule priority over traffic that does not match the rule.<br>Enabling a bandwidth management rule also allows you to control the maximum amounts of bandwidth that can be used by traffic that matches the rule. |
| Rule Name | Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces. |
| BW Budget | Specify the maximum bandwidth allowed for the rule in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual rule. |
| Priority | Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**. |
| Use All Managed Bandwidth | Select this option to allow a rule to borrow unused bandwidth on the interface.<br>Bandwidth borrowing is governed by the priority of the rules. That is, a rule with the highest priority is the first to borrow bandwidth. Do not select this if you want to leave bandwidth available for other traffic types or if you want to restrict the amount of bandwidth that can be used for the traffic that matches this rule. |
| Enable DiffServ Marking | Select this option to enable DiffServ marking on the ZyXEL Device. |

**Table 78** Bandwidth Management Rule Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| DiffServ mark | Select the marking rule from the drop-down list. The first three digits are the DiffServ code point. A packet with the lowest priority mark will be dropped when the line is busy. |
| Filter Configuration | |
| Service | This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).<br>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select **SIP** from the drop-down list box to configure this bandwidth filter for traffic that uses SIP.<br>File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select **FTP** from the drop-down list box to configure this bandwidth filter for FTP traffic.<br>H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select **H.323** from the drop-down list box to configure this bandwidth filter for traffic that uses H.323.<br>Select **User defined** from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select **User defined**, you need to configure at least one of the following fields (other than the **Subnet Mask** fields which you only enter if you also enter a corresponding destination or source IP address). |
| Destination Address | Enter the destination IP address in dotted decimal notation. |
| Destination Subnet Netmask | Enter the destination subnet mask. This field is N/A if you do not specify a **Destination Address**. Refer to the appendices for more information on IP subnetting. |
| Destination Port | Enter the port number of the destination. See Table 79 on page 197 for some common services and port numbers. A blank destination IP address means any destination IP address. |
| Source Address | Enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address. |
| Source Subnet Netmask | Enter the destination subnet mask. This field is N/A if you do not specify a **Source Address**. Refer to the appendices for more information on IP subnetting. A blank source port means any source port number. |
| Source Port | Enter the port number of the source. See Table 79 on page 197 for some common services and port numbers. |
| Protocol | Select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number. 0 means any protocol number. |
| TOS (Type of Service) | TOS defines the DS (Differentiated Service) field in the IP header.<br>Enter the new TOS value of the outgoing packet (between 0 and 255). 0 is the lowest priority. |
| TOS Mask | The TOS mask is used to compare the specified (or entire) bits in the TOS IP header with the value specified in this rule.<br>Enter the **TOS Mask** value between 0 (lowest priority) and 255. |
| Back | Click **Back** to go to the previous screen. |

**Table 78** Bandwidth Management Rule Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes to the ZyXEL Device. |
| Cancel | Click **Cancel** to begin configuring this screen afresh. |

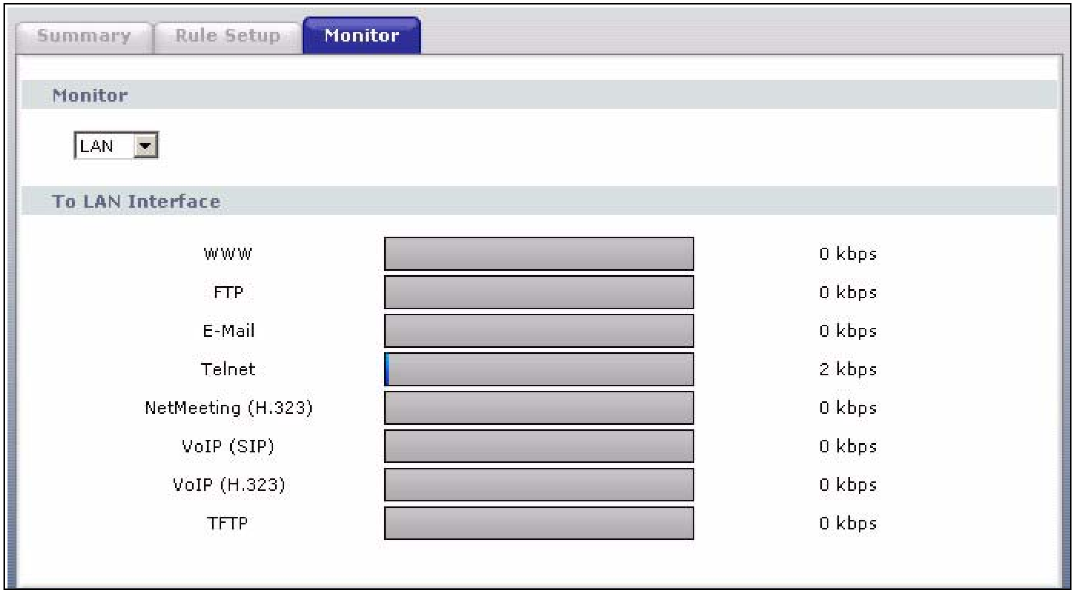
**Table 79** Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|---|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer protocol or WWW, Web) | 80 |
| POP3 (Post Office Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| SNMP (Simple Network Management Protocol) | 161 |
| SNMP trap | 162 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

## 13.11 Bandwidth Monitor

To view the ZyXEL Device's bandwidth usage and allotments, click **Advanced > Bandwidth MGMT > Monitor**. The screen appears as shown. Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth rules. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use. The screen refreshes every few seconds.

**Figure 113** Bandwidth Management: Monitor



Monitor

LAN

To LAN Interface

| | |
|---|---|
| WWW | 0 kbps |
| FTP | 0 kbps |
| E-Mail | 0 kbps |
| Telnet | 2 kbps |
| NetMeeting (H.323) | 0 kbps |
| VoIP (SIP) | 0 kbps |
| VoIP (H.323) | 0 kbps |
| TFTP | 0 kbps |

**Table 80** Bandwidth Management Monitor

| LABEL | DESCRIPTION |
|---|---|
| Monitor | This section allows you to select which network to monitor. You may select either a **LAN**, **WLAN**, or **WAN**. After selecting a network to monitor, information on active services and their bandwidth usage will appear. |

# 14

# Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

## 14.1 Dynamic DNS Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

### 14.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

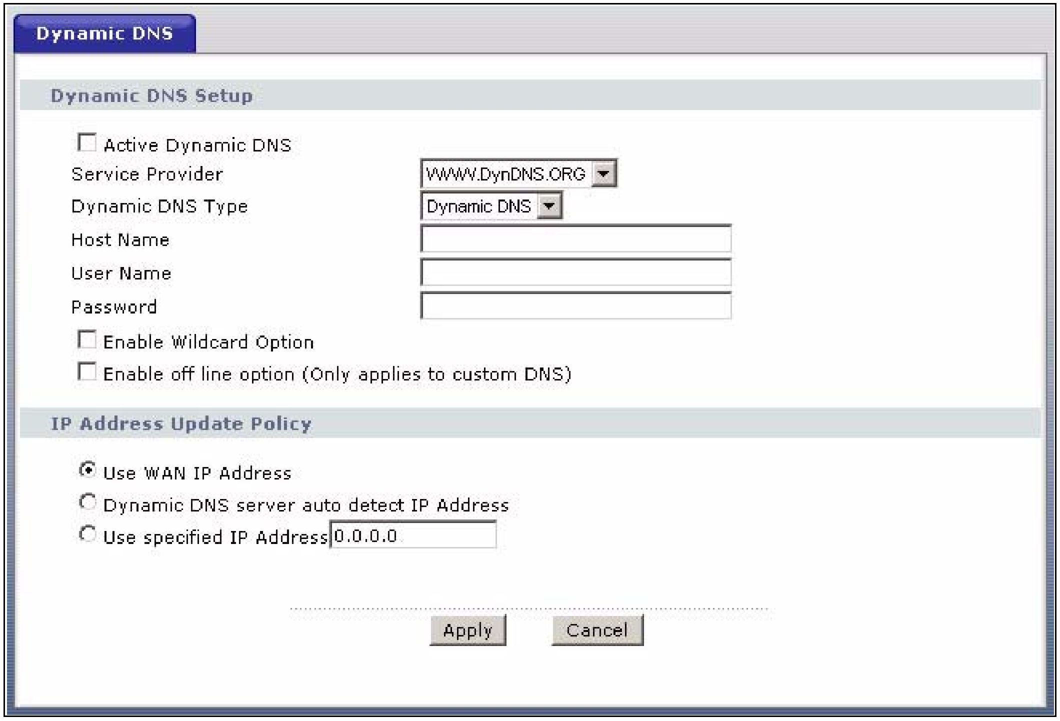
See Section 14.2 on page 199 for configuration instruction.

## 14.2 Configuring Dynamic DNS

To change your ZyXEL Device's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

See Section 14.1 on page 199 for more information.

**Figure 114** Dynamic DNS



Dynamic DNS Setup

□ Active Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Dynamic DNS Type: Dynamic DNS

Host Name:

User Name:

Password:

□ Enable Wildcard Option

□ Enable off line option (Only applies to custom DNS)

IP Address Update Policy

● Use WAN IP Address

○ Dynamic DNS server auto detect IP Address

○ Use specified IP Address 0.0.0.0

The following table describes the fields in this screen.

**Table 81** Dynamic DNS

| LABEL | DESCRIPTION |
|---|---|
| Dynamic DNS Setup | |
| Active Dynamic DNS | Select this check box to use dynamic DNS. |
| Service Provider | This is the name of your Dynamic DNS service provider. |
| Dynamic DNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider. |
| Host Name | Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider.<br>You can specify up to two host names in the field separated by a comma (","). |
| User Name | Type your user name. |
| Password | Type the password assigned to you. |
| Enable Wildcard Option | Select the check box to enable DynDNS Wildcard. |
| Enable off line option | This option is available when **Custom DNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line. |
| IP Address Update Policy | |
| Use WAN IP Address | Select this option to update the IP address of the host name(s) to the WAN IP address. |