CHAPTER 9
Wireless

9.1 Wireless Overview

This chapter describes the Zyxel Device's **Network Setting > Wireless** screens. Use these screens to set up your Zyxel Device's WiFi network and security settings.

9.1.1 What You Can Do in this Chapter

This section describes the Zyxel Device's **Wireless** screens. Use these screens to set up your Zyxel Device's WiFi connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the WiFi security mode (Section 9.2 on page 255)
- Use the **Guest/More AP** screen to set up multiple WiFi networks on your Zyxel Device (Section 9.3 on page 261).
- Use the **MAC Authentication** screen to allow or deny WiFi clients based on their MAC addresses from connecting to the Zyxel Device (Section 9.4 on page 265).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 9.5 on page 267).
- Use the **WMM** screen to enable WiFi MultiMedia (WMM) to ensure quality of service in WiFi networks for multimedia applications (Section 9.6 on page 269).
- Use the **Others** screen to configure WiFi advanced features, such as the RTS/CTS Threshold (Section 9.7 on page 270).
- Use the **Channel Status** screen to scan the number of accessing points and view the results (Section 9.8 on page 272).
- Use the **MESH** screen to enable or disable MPro Mesh on your Zyxel Device (Section 9.9 on page 274).

9.1.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there are a number of wireless networking standards available with different methods of data encryption.

WiFi6 / IEEE 802.11ax

WiFi6 is backwards compatible with IEEE 802.11a/b/g/n/ac and is most suitable in areas with a high concentration of users. WiFi6 devices support Target Wake up Time (TWT) allowing them to automatically power down when they are inactive.

The following table displays the comparison of the different WiFi standards.

Table 61 WiFI Standards Comparison

WIFI STANDARD	MAXIMUM LINK RATE*	BAND	SIMULTANEOUS CONNECTIONS
802.11b	11 Mbps	2.4 GHz	1
802.11a/g	54 Mbps	2.4 GHz and 5 GHz	1
802.11n	600 Mbps	2.4 GHz and 5 GHz	1
802.11ac	6.93 Gbps	5 GHz	4
802.11ax	2.4 Gbps	2.4 GHz	128
	9.61 Gbps	5 GHz and 6 GHz	

* The maximum link rate is for reference under ideal conditions only.

WiFi 6E (IEEE802.11ax – Extended Standard)

WiFi 6E is an extended standard of WiFi 6 (IEEE 802.11ax). WiFi 6E inherits all the WiFi 6 features and brings with an additional 6 GHz band. The 6 GHz band allows you to avoid possible congested traffic in the lower 2.4 GHz and 5 GHz bands. WiFi clients must support WiFi 6E to connect to the device using the 6 GHz band.

You must use WPA3 for security with WiFi 6E.

Note: Check your client device's product specification to see if your client device supports the 6 GHz band (WiFi 6E). If not, you should still use the 2.4/5 GHz bands for connection.

Finding Out More

See Section 9.10 on page 274 for advanced technical information on WiFi networks.

9.2 Wireless General Settings

Use this screen to enable the WiFi, enter the SSID and select the WiFi security mode. We recommend that you select **More Secure** to enable **WPA3-SAE** data encryption.

Note: If you are configuring the Zyxel Device from a computer connected by WiFi and you change the Zyxel Device's SSID, channel or security settings, you will lose your WiFi connection when you press **Apply**. You must change the WiFi settings of your computer to match the new settings on the Zyxel Device.

Note: If upstream or downstream bandwidth is empty, the Zyxel Device sets the value automatically.

Note: Setting a maximum upstream or downstream bandwidth will significantly decrease wireless performance.

Note: **Keep the same settings for 2.4G, 5G wireless networks** is enabled and cannot be disabled when you enable **MPro Mesh** in the **Network > Wireless > MESH** screen.

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

Figure 119 Network Setting > Wireless > General

The following table describes the general WiFi labels in this screen.

Table 62 Network Setting > Wireless > General

LABEL	DESCRIPTION
Wireless	
Wireless	Select **Keep the same settings for 2.4G, 5G and 6G wireless networks** and the 2.4 GHz, 5 GHz and 6 GHz WiFi networks will use the same SSID and wireless security settings.
MLO	Select **MLO** to allow a WiFi 7 client to connect to the AP using multiple frequency bands simultaneously. This increases speed and improves reliability of the WiFi connection. MLO makes WiFi 7 ideal for streaming 4K/ 8K videos, using augmented reality (AR), virtual reality (VR) applications and playing online games. Note: To use MLO, both the AP and the WiFi client have to support MLO.
Wireless/WiFi Network Setup	
Band	This shows the WiFi band which this radio profile is using. **2.4GHz** is the frequency used by IEEE 802.11b/g/n/ax WiFi clients, **5GHz** is used by IEEE 802.11a/n/ac/ax WiFi clients while **6GHz** is used by IEEE 802.11a/n/ac/ax WiFi clients.
Wireless/WiFi	Click this switch to enable or disable WiFi in this field. When the switch turns blue, the function is enabled. Otherwise, it is not.
Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Use **Auto** to have the Zyxel Device automatically determine a channel to use.
Bandwidth	A standard 20 MHz channel offers transfer speeds of up to 150 Mbps whereas a 40 MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The WiFi clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the WiFi signal. An 80 MHz channel groups adjacent 40 MHz channels into pairs to increase bandwidth even higher. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the WiFi clients do not support channel bonding. Not all Zyxel Devices support all channels. The Zyxel Device will choose the best bandwidth available automatically depending on the radio you chose and network conditions.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz** or **20/40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless/WiFi Network Settings	
Wireless/WiFi Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for this WiFi network. You can use up to 32 printable characters, including spaces.
Max Clients	Specify the maximum number of clients that can connect to this network at the same time.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. This checkbox is grayed out if the WPS function is enabled in the **Network Setting > Wireless > WPS** screen.
Blocking BSSID LAN Access	Select this checkbox so that the WiFi client's access to all devices on the LAN will be blocked.
Multicast Forwarding	Select this checkbox to allow the Zyxel Device to convert wireless Multicast traffic into wireless unicast traffic.

Table 62 Network Setting > Wireless > General (continued)

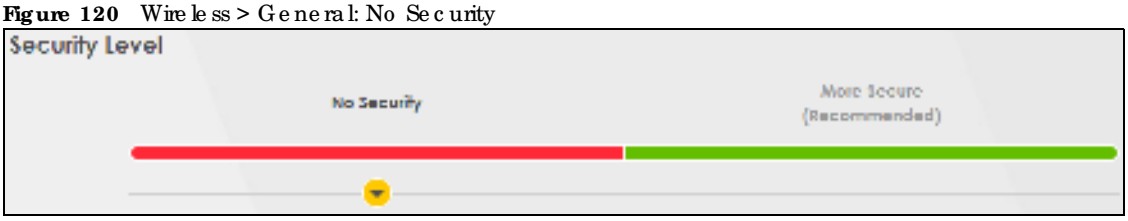
LABEL	DESCRIPTION
Max. Upstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for upstream wireless traffic to the WAN from this wireless LAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Max. Upstream Bandwidth allows you to specify the maximum rate for downstream wireless traffic to this wireless LAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the wireless interface on the Zyxel Device when WiFi is enabled.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have same WiFi security settings as the Zyxel Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

9.2.1 No Security

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

Note: If you do not enable any WiFi security on your Zyxel Device, your network is accessible to any wireless networking device that is within range.

Figure 120 Wireless > General: No Security



The following table describes the labels in this screen.

Table 63 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** to allow all WiFi connections without data encryption or authentication.

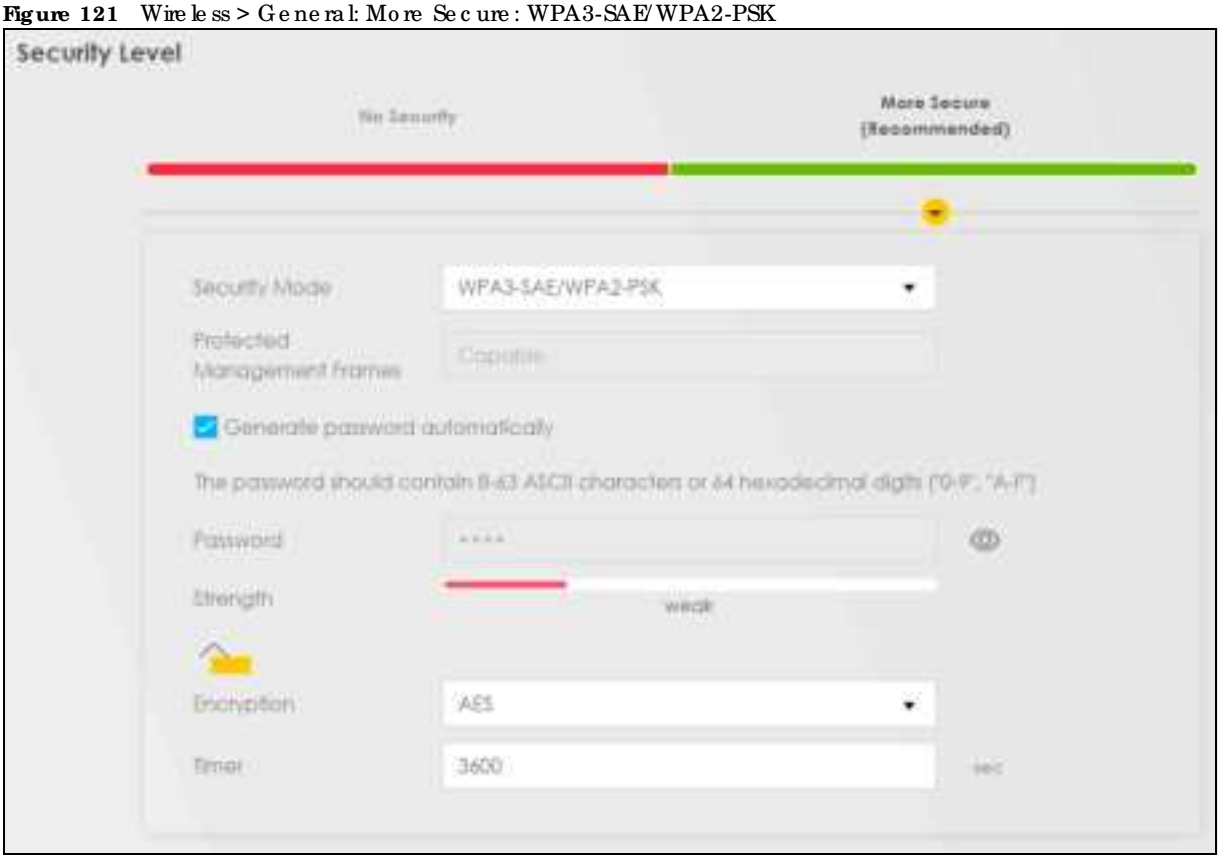
9.2.2 More Secure (Recommended)

The WPA-PSK (WiFi Protected Access-Pre-Shared Key) security mode provides both improved data encryption and user authentication over WEP. Using a pre-shared key, both the Zyxel Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a more robust version of the WPA encryption standard. It offers better security, although the use of PSK makes it less robust than it could be.

The WPA3-SAE (Simultaneous Authentication of Equals handshake) security mode protects against dictionary attacks (password guessing attempts). It improves security by requiring a new encryption key every time a WPA3 connection is made. A handshake is the communication between the Zyxel Device and a connecting client at the beginning of a WiFi session.

Click **Network Setting > Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA3-SAE** from the **Security Mode** list if your WiFi client supports it. If you are not sure, select **WPA3-SAE/WPA2-PSK** or **WPA2-PSK**.

Figure 121 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK



The following table describes the labels in this screen.

Table 64 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable data encryption.
Security Mode	Select a security mode from the drop-down list box.
Protected Management Frames	This option is only available when using **WPA2-PSK** as the **Security Mode** and **AES Encryption** in **Network Setting > Wireless > General**. Management frame protection (MFP) helps present WiFi DoS (Denial of Service) attacks. Select **Disable** if you do not want to use MFP. Select **Capable** to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select **Required** to allow only clients that support MFP to join the WiFi network. When Mesh is enabled, the settings of **Protected Management Frames** of 5G will follow 2.4G.

Table 64 Wireless > General: More Secure: WPA3-SAE/WPA2-PSK (continued)

LABEL	DESCRIPTION
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	Select **Generate password automatically** or enter a **Password**. The password has two uses. 1. Manual. Manually enter the same password on the Zyxel Device and the client. You can use 8 – 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces. 2. WPS. When using WPS, the Zyxel Device sends this password to the client. Note: More than 63 hexadecimal characters are not accepted for WPS. Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed, you will see the password in plain text. Otherwise, it is hidden.
Strength	This displays the current password strength – **weak**, **medium**, **strong**.
Click this to show more fields in this section. Click this to hide them.	
Encryption	**AES** is the default data encryption type, which uses a 128-bit key. Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your WiFi clients can all use AES. Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. Note: Not all models support **TKIP+AES** encryption.
Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.

9.3 Guest/More AP Screen

Use this screen to configure a guest WiFi network that allows access to the Internet through the Zyxel Device. You can use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. WiFi clients can use different SSIDs to associate with the same access point.

Click **Network Setting > Wireless > Guest/More AP**.

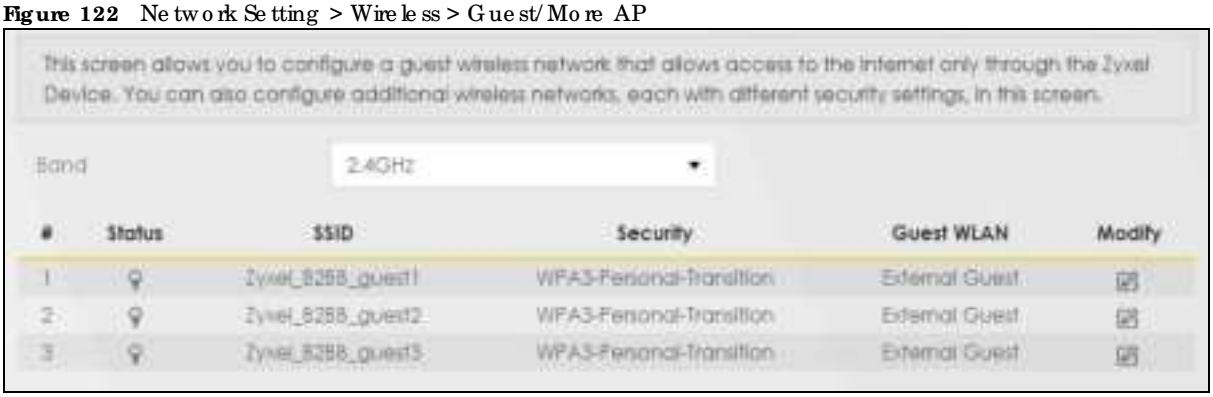
The following table introduces the supported WiFi networks.

Table 65 Supported WiFi Networks

WIFI NETWORKS	WHERE TO CONFIGURE
Main/1	Network Setting > Wireless > General screen
Guest/3	Network Setting > Wireless > Guest/More AP screen

The following screen displays.

Figure 122 Network Setting > Wireless > Guest/More AP



The following table describes the labels in this screen.

Table 66 Network Setting > Wireless > Guest/More AP

LABEL	DESCRIPTION
Band	Select a **2.4GHz** or **5GHz** frequency band to display the SSID profile of the selected band.
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active, while a gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the Zyxel Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a WiFi client scans for an AP to associate with, this is the name that is broadcast and seen in the WiFi client utility. Note: The SSID profiles displayed differ by the frequency band you select in the **Band** field.
Security	This field indicates the security mode of the SSID profile.
Guest WLAN	This displays if the guest WLAN function has been enabled for this WLAN. If **Home Guest** displays, clients can connect to each other directly. If **External Guest** displays, clients are blocked from connecting to each other directly. **N/A** displays if guest WLAN is disabled.
Modify	Click the **Edit** icon of an SSID profile to configure the SSID profile.

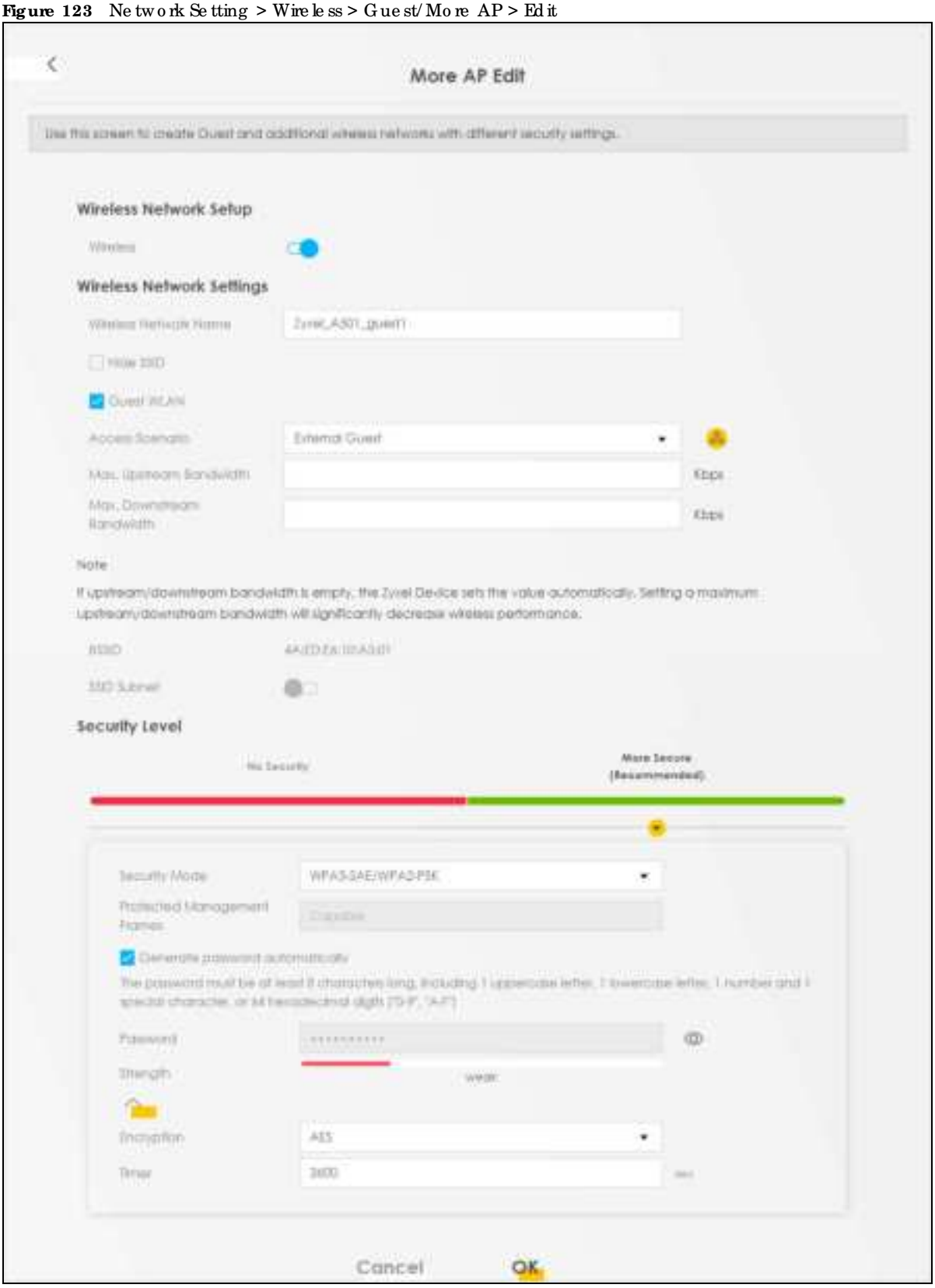
9.3.1 The Edit Guest/More AP Screen

Use this screen to create Guest and additional WiFi networks with different security settings.

Note: If upstream/downstream bandwidth is empty, the Zyxel Device sets the value automatically. Setting a maximum upstream/downstream bandwidth will significantly decrease WiFi performance.

Click the **Edit** icon next to an SSID in the **Guest/More AP** screen. The following screen displays.

Figure 123 Network Setting > Wireless > Guest/More AP > Edit



The following table describes the fields in this screen.

Table 67 Network Setting > Wireless > Guest/More AP > Edit

LABEL	DESCRIPTION
WiFi/Wireless Network Setup	
WiFi/Wireless	Click this switch to enable or disable the WiFi in this field. When the switch turns blue, the function is enabled; otherwise, it is not.
WiFi/Wireless Network Settings	
WiFi/Wireless Network Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name for the WiFi. You can use up to 32 printable characters, including spaces.
Hide SSID	Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Guest WLAN	Select this to create Guest WLANs for home and external clients. Select the WLAN type in the **Access Scenario** field.
Access Scenario	If you select **Home Guest**, clients can connect to each other directly. If you select **External Guest**, clients are blocked from connecting to each other directly.
Max. Upstream Bandwidth	Specify the maximum rate for upstream wireless traffic to the WAN from this WLAN in kilobits per second (Kbps).
Max. Downstream Bandwidth	Specify the maximum rate for downstream wireless traffic to this WLAN from the WAN in kilobits per second (Kbps).
BSSID	This shows the MAC address of the WiFi interface on the Zyxel Device when WiFi is enabled.
SSID Subnet	Click on this switch to **Enable** this function if you want the wireless network interface to assign DHCP IP addresses to the associated WiFi clients. This option cannot be used if **Keep 2.4G and 5G wireless network name the same** is enabled in **Network > Wireless > General**.
DHCP Start Address	Specify the first of the contiguous addresses in the DHCP IP address pool. The Zyxel Device assigns IP addresses from this DHCP pool to WiFi clients connecting to the SSID.
DHCP End Address	Specify the last of the contiguous addresses in the DHCP IP address pool.
SSID Subnet Mask	Specify the subnet mask of the Zyxel Device for the SSID subnet.
LAN IP Address	Specify the IP address of the Zyxel Device for the SSID subnet.
Security Level	
Security Mode	Select **More Secure (Recommended)** to add security on this WiFi network. The WiFi clients which want to associate to this network must have the same WiFi security settings as the Zyxel Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 9.2.1 on page 259 for more details about this field.

Table 67 Network Setting > Wireless > Guest/More AP > Edit (continued)

LABEL	DESCRIPTION
Protected Management Frames	This option is only available when using **WPA2-PSK** as the **Security Mode** and **AES Encryption** in **Network Setting > Wireless > General**. Management frame protection (MFP) helps present WiFi DoS (Denial of Service) attacks. Select **Disable** if you do not want to use MFP. Select **Capable** to encrypt management frames of WiFi clients that support MFP. Clients that do not support MFP will still be allowed to join the WiFi network, but remain unprotected. Select **Required** to allow only clients that support MFP to join the WiFi network. When Mesh is enabled, the settings of **Protected Management Frames** of 5G will follow 2.4G.
Generate password automatically	Select this option to have the Zyxel Device automatically generate a password. The password field will not be configurable when you select this option.
Password	WPA2-PSK uses a simple common password, instead of user-specific credentials. If you did not select **Generate password automatically**, you can manually enter a pre-shared key from 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters. Spaces are allowed. Click the Eye icon to show or hide the password of your WiFi network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it is hidden.
Strength	This displays the current password strength – **weak**, **medium**, **strong**.
Click this  to show more fields in this section. Click again to hide them.	
Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your WiFi clients can all use AES. Select **TKIP+AES** to allow the WiFi clients to use either TKIP or AES. Not all models support the **TKIP+AES** option.
Timer	The **Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

9.4 MAC Authentication

Use this screen to give exclusive access to specific connected devices **(Allow)** or exclude specific devices from accessing the Zyxel Device **(Deny)**, based on the MAC address of each connected device. Every Ethernet device has a unique factory-assigned MAC (Media Access Control) address, which consists of six pairs of hexadecimal characters, for example: 00:A0:C5:00:00:02. You need to know the MAC addresses of the connected device you want to allow/deny to configure this screen.

Note: You can have up to 25 MAC authentication rules.

Note: This screen is not available when MPro Mesh is enabled in the **Network Setting > Wireless > MESH** screen.

Use this screen to view your Zyxel Device's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless > MAC Authentication**. The screen appears as shown.

Figure 124 Network Setting > Wireless > MAC Authentication

The following table describes the labels in this screen.

Table 68 Network Setting > Wireless > MAC Authentication

LABEL	DESCRIPTION
General	
Band	Select a **2.4GHz** or **5GHz** frequency band to display associated WiFi devices in the selected band, identified by MAC address.
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the Zyxel Device. MAC addresses not listed will be allowed to access the Zyxel Device. Select **Allow** to permit access to the Zyxel Device. MAC addresses not listed will be denied access to the Zyxel Device.
MAC address List	

Table 68 Network Setting > Wireless > MAC Authentication (continued)

LABEL	DESCRIPTION
Add new MAC address	This field is available when you select **Deny** or **Allow** in the **MAC Restrict Mode** field. Click this if you want to add a new MAC address entry to the MAC filter list below. Select an existing WiFi client from the list to add as a new entry. Select **Custom** if you want to manually enter the **Host Name** and **MAC Address**. Enter the MAC addresses of the WiFi devices 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. 
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the WiFi devices that are allowed or denied access to the Zyxel Device.
Modify	Click the **Edit** icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the **Delete** icon to delete the entry.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

9.5 WPS

Use this screen to configure WiFi Protected Setup (WPS) on your Zyxel Device.

WiFi Protected Setup (WPS) allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Select one of the WPS methods and follow the instructions to establish a WPS connection. Your WiFi devices must support WPS to use this feature. We recommend using Push Button Configuration (**PBC**) if your WiFi device supports it.

Note: The Zyxel Device applies the security settings of the main SSID (**SSID1**) profile to the WPS wireless connection (see Section 9.2.2 on page 259). Some models support more than one SSID profile, check the supported number on the **Network Setting > Wireless > General** screen.

Note: The WPS switch is unavailable if the WiFi is disabled.
If WPS is enabled, UPnP will automatically be turned on.

Click **Network Setting > Wireless > WPS**. The following screen displays. Click this switch and it will turn blue. Click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 125 Network Setting > Wireless > WPS

The following table describes the labels in this screen.

Table 69 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
General	
Band	Select a **2.4GHz** and **5GHz** frequency band to enable WPS for all WiFi networks in the selected band. If you use the WPS button on the Zyxel Device ports panel, WPS is automatically enabled on both 2.4 GHz and 5 GHz bands. See Section 2.3 on page 58 for more information about the WPS button.
WPS	Slide this to the right to enable and have the Zyxel Device activate WPS. Otherwise, it is disabled.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS WiFi network using Push Button Configuration (PBC). Click this switch to make it turn blue. Click **Apply** to activate WPS method 1 on the Zyxel Device.
WPS	Click this button to add another WPS-enabled WiFi device (within WiFi range of the Zyxel Device) to your WiFi network. This button may either be a physical button on the outside of a WiFi device, or a menu button similar to the **WPS button** on this screen. Note: You must press the other WiFi device's WPS button within 2 minutes of pressing this button.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

9.6 WMM

Use this screen to enable WiFi MultiMedia (**WMM**) and **WMM Automatic Power Save Delivery** (**APSD**) in WiFi networks for multimedia applications. **WMM** enhances data transmission quality, while **APSD** improves power management of WiFi clients. This allows time-sensitive applications, such as voice and videos, to run more smoothly.

Click **Network Setting > Wireless > WMM** to display the following screen.

Figure 126 Network Setting > Wireless > WMM

Note: **WMM** cannot be disabled if 802.11 mode includes 802.11n or 802.11ac.

Note: APSD only affects SSID1. For SSID2-SSID4, APSD is always enabled.

Note: This screen is not available when MPro Mesh is enabled in the **Network Setting > Wireless > MESH** screen.

The following table describes the labels in this screen.

Table 70 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Band	Select a **2.4GHz** and **5GHz** frequency band to enable or disable the **WMM of SSID** of the selected band.
WMM of SSID	Select **On** to have the Zyxel Device automatically give the WiFi network (SSIDx) a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (WiFi MultiMedia Quality of Service) gives high priority to video, which makes them run more smoothly. SSID1 is the **General** WiFi SSID; SSID2-SSID4 are the **Guest** WiFi SSIDs. If the **802.11 Mode** in **Network Setting > Wireless > Others** is set to include 802.11n or 802.11ac, WMM cannot be disabled.

Table 70 Network Setting > Wireless > WMM (continued)

LABEL	DESCRIPTION
WMM Automatic Power Save Delivery (APSD)	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The Zyxel Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the Zyxel Device until the Zyxel Device "wakes up." The Zyxel Device wakes up periodically to check for incoming data. Note: This works only if the WiFi device to which the Zyxel Device is connected also supports this feature.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

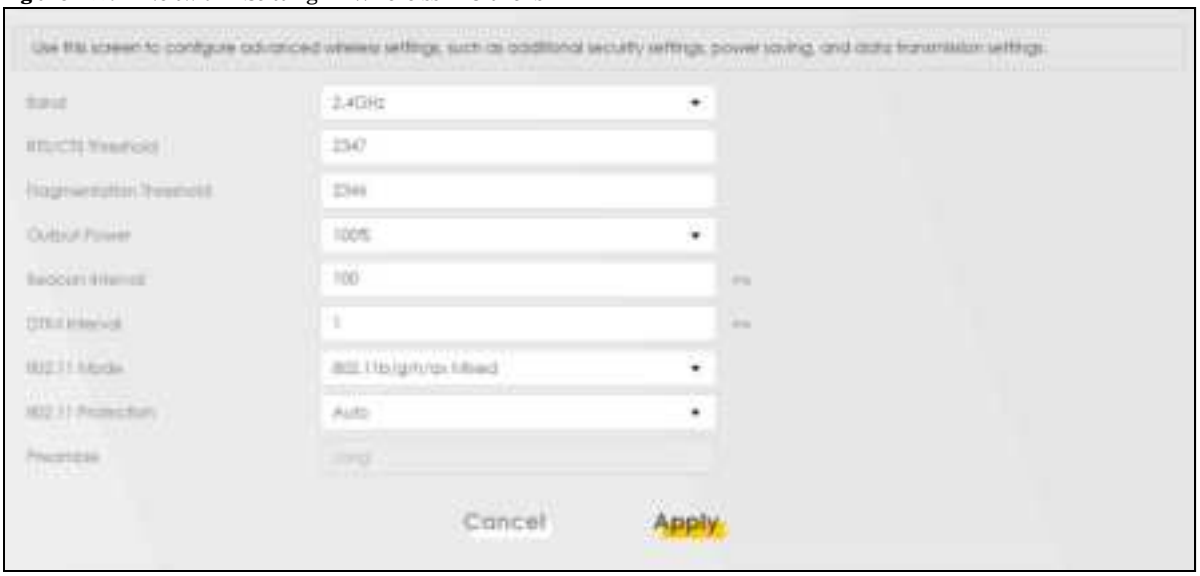
9.7 Others Screen

Use this screen to configure advanced WiFi settings, such as additional security settings, power saving, and data transmission settings. Click **Network Setting > Wireless > Others**. The screen appears as shown.

Note: This screen is not available when MPro Mesh is enabled in the **Network Setting > Wireless > MESH** screen.

See Section 9.10.2 on page 276 for detailed definitions of the terms listed here.

Figure 127 Network Setting > Wireless > Others



The following table describes the labels in this screen.

Table 71 Network Setting > Wireless > Others

LABEL	DESCRIPTION
Band	Select a **2.4GHz** or **5GHz** frequency band to display the following wireless settings for the selected band.
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Output Power	Set the output power of the Zyxel Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 50 ms to 1000 ms. A high value helps save current consumption of the access point.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and Multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
802.11 Mode	For 2.4 GHz frequency WiFi devices: • Select **802.11b Only** to allow only IEEE 802.11b compliant WiFi devices to associate with the Zyxel Device. • Select **802.11g Only** to allow only IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11b/g/n/ax Mixed** to allow IEEE 802.11b, IEEE 802.11g, IEEE 802.11n or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. For 5 GHz / 6GHz frequency WiFi devices: • Select **802.11a Only** to allow only IEEE 802.11a compliant WiFi devices to associate with the Zyxel Device. • Select **802.11n Only** to allow only IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. • Select **802.11ac Only** to allow only IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. • Select **802.11a/n Mixed** to allow either IEEE 802.11a or IEEE 802.11n compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11n/ac Mixed** to allow either IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac Mixed** to allow IEEE 802.11a, IEEE 802.11n or IEEE 802.11ac compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced. • Select **802.11a/n/ac/ax Mixed** to allow IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax compliant WiFi devices to associate with the Zyxel Device. The transmission rate of your Zyxel Device might be reduced.

Table 71 Network Setting > Wireless > Others (continued)

LABEL	DESCRIPTION
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your Zyxel Device might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See Section 9.10.7 on page 279 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

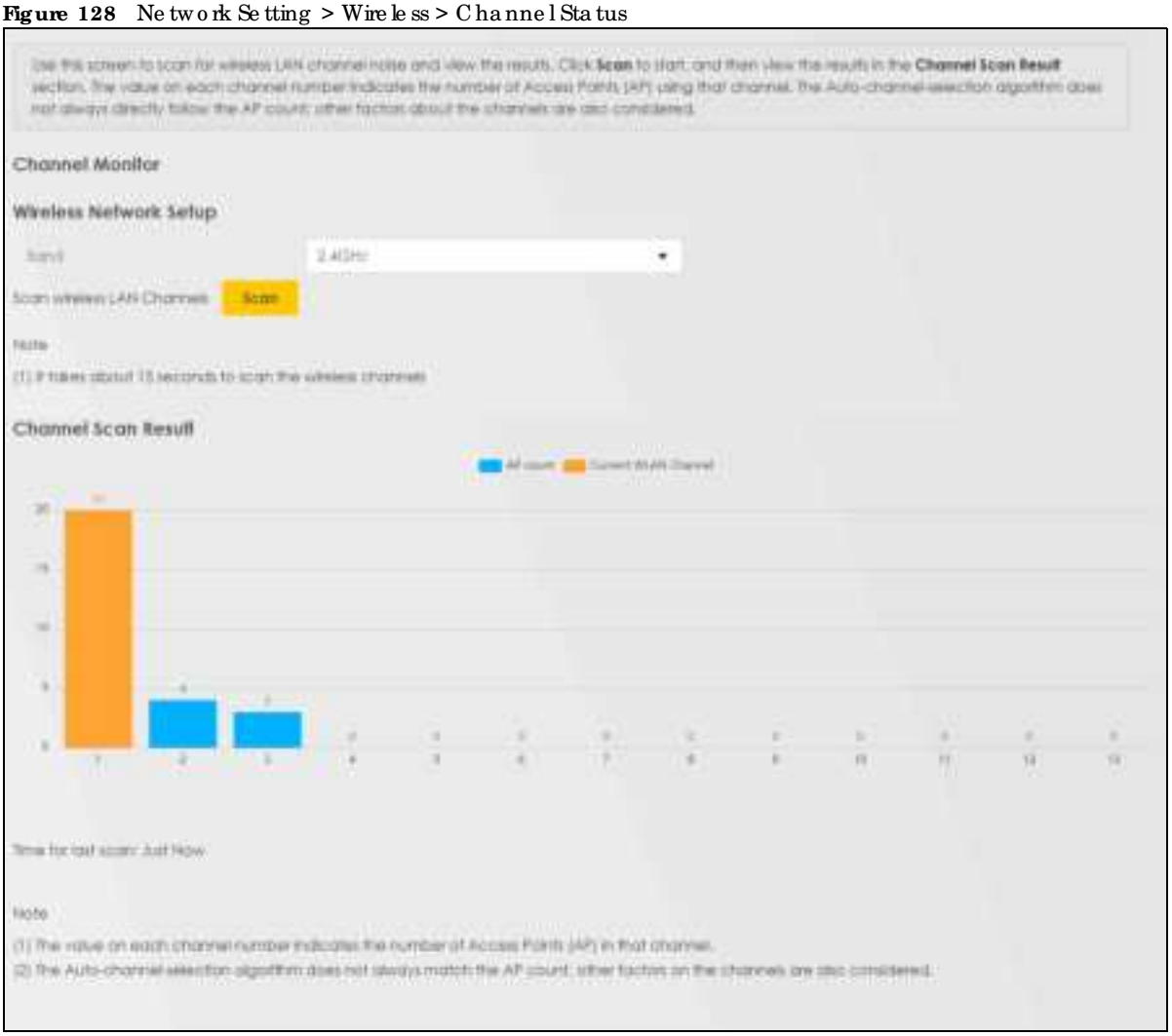
9.8 Channel Status

Use this screen to scan for WiFi channel noise and view the results. Click **Scan** to start, and then view the results in the **Channel Scan Result** section. The value on each channel number indicates the number of Access Points (AP) using that channel. The Auto-channel-selection algorithm does not always directly follow the AP count; other factors about the channels are also considered. Click **Network Setting > Wireless > Channel Status**. The screen appears as shown.

Note: If the current channel is a DFS channel, the warning 'Channel scan process is denied because current channel is a DFS channel (Channel: 52 – 140). If you want to run channel scan, please select a non-DFS channel and try again.' appears.

Note: The AP count may not be a real-time value.

Figure 128 Network Setting > Wireless > Channel Status



The following table describes the labels in this screen.

Table 72 Network Setting > Wireless > Channel Status

LABEL	DESCRIPTION
Channel Monitor	
Wireless Network Setup	
Band	Select a **2.4GHz** or **5GHz** frequency band on which you want to conduct a channel scan.
Scan WiFi LAN Channels	Click the **Scan** button to scan WiFi channels.
Channel Scan Result	This displays the results of the channel scan. The blue bar displays the number of access points (**AP count**) in the WiFi channel. The orange bar displays the WiFi channel that the Zyxel Device is now using.

9.9 MESH

The Zyxel Device supports MPro Mesh along with the MPro Mesh app to manage your WiFi network. MPro Mesh is the Zyxel implantation of WiFi-Alliance Easy Mesh. It supports AP steering, band steering, auto-configuration and other advances for your WiFi network.

The Zyxel Device can function as a controller to automatically configure WiFi settings on extenders in the network as well as optimize bandwidth usage.

The Zyxel Device optimizes bandwidth usage by directing WiFi clients to an extender (AP steering) or a 2.4GHz/ 5GHz band (band steering) that is less busy.

See Section 6.1 on page 143 for the complete MPro Mesh feature introduction and the following tutorials with the MPro Mesh app.

- Setting up your MPro Mesh network with the Zyxel Device and an MPro Mesh extender,
- setting up your general/guest WiFi,
- basic configurations.

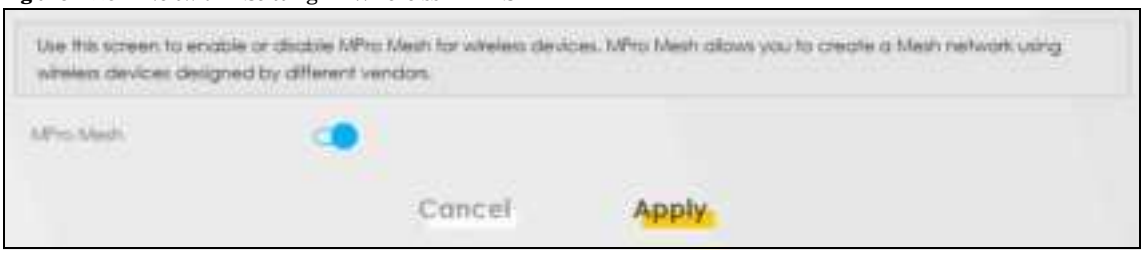
9.9.1 MPro Mesh

Use this screen to enable or disable MPro Mesh on the Zyxel Device.

Click **Network Setting > Wireless > MESH**. The following screen displays.

Note: When MPro Mesh is enabled, the SSID and WiFi password of the main 2.4 GHz WiFi network will be copied to the main 5 GHz WiFi network.

Figure 129 Network Setting > Wireless > MESH



The following table describes the labels in this screen.

Table 73 Network Setting > Wireless > MESH

LABEL	DESCRIPTION
MPro Mesh	Click the button (to the right) to enable the MPro Mesh feature on the Zyxel Device and set up your MPro Mesh network.

9.10 Technical Reference

This section discusses WiFi in depth.

9.10.1 WiFi Network Overview

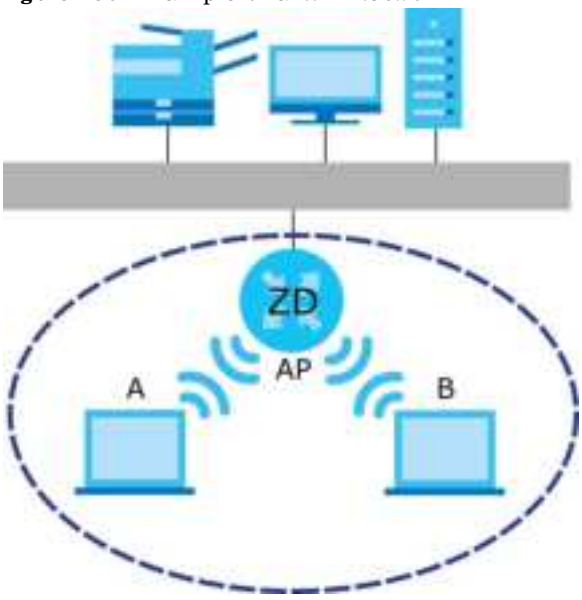
WiFi networks consist of WiFi clients, access points and bridges.

- A WiFi client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous WiFi clients and let them access the network.
- A bridge is a radio that relays communications between access points and WiFi clients, extending a network's range.

Normally, a WiFi network operates in an "infrastructure" type of network. An "infrastructure" type of network has one or more access points and one or more WiFi clients. The WiFi clients connect to the access points.

The following figure provides an example of a WiFi network.

Figure 130 Example of a WiFi Network



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

Every WiFi network must follow these basic guidelines.

- Every WiFi device in the same WiFi network must use the same SSID.

  The SSID is the name of the WiFi network. It stands for Service Set IDentifier.
- If two WiFi networks overlap, they should use a different channel.

  Like radio stations or television channels, each WiFi network uses a specific channel, or frequency, to send and receive information.
- Every WiFi device in the same WiFi network must use security compatible with the AP.

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

9.10.2 Additional WiFi Terms

The following table describes some WiFi network terms and acronyms used in the Zyxel Device's Web Configurator.

Table 74 Additional WiFi Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a WiFi network which covers a large area, WiFi devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the WiFi devices must sometimes get permission to send information to the Zyxel Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then WiFi devices never have to get permission to send information to the Zyxel Device.
Preamble	A preamble affects the timing in your WiFi network. There are two preamble modes: long and short. If a WiFi device uses a different preamble mode than the Zyxel Device does, it cannot communicate with the Zyxel Device.
Authentication	The process of verifying whether a WiFi device is allowed to use the WiFi network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

9.10.3 WiFi Security Overview

By their nature, radio communications are simple to intercept. For WiFi data networks, this means that anyone within range of a WiFi network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a WiFi data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess – for example, a twenty-letter long string of apparently random numbers and letters – but it is not very secure if you use a short key which is very easy to guess – for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it is not just people who have sensitive information on their network who should use security. Everybody who uses any WiFi network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is

Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

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

9.10.3.1 SSID

Normally, the Zyxel Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the Zyxel Device 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 WiFi devices to get the SSID. In addition, unauthorized WiFi devices can still see the information that is sent in the WiFi network.

9.10.3.2 MAC Address Filter

Every device that can use a WiFi network 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 WiFi device in the WiFi network, see the WiFi device's User's Guide or other documentation.

You can use the MAC address filter to tell the Zyxel Device which devices are allowed or not allowed to use the WiFi network. If a WiFi device is allowed to use the WiFi network, it still has to have the correct information (SSID, channel, and security). If a WiFi device is not allowed to use the WiFi network, it does not matter if it has the correct information.

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

9.10.3.3 Encryption

WiFi networks can use encryption to protect the information that is sent in the WiFi 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 authentication. (See Section 9.10.3.3 on page 277 for information about this.)

Table 75 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
	WPA-PSK	
	WPA2	WPA2
Strongest	WPA3-SAE	WPA3 (server certificate validation)

1. Some wireless devices, such as scanners, can detect WiFi networks but cannot use WiFi 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.

For example, if the WiFi network has a RADIUS server, you can choose **WPA**, **WPA2**, or **WPA3**. If users do not log in to the WiFi network, you can choose no encryption, **WPA2-PSK**, or **WPA3-SAE**.

Note: It is recommended that WiFi networks use **WPA3-SAE**, **WPA2-PSK**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized WiFi devices to figure out the original information pretty quickly.

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

9.10.4 Signal Problems

Because WiFi networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

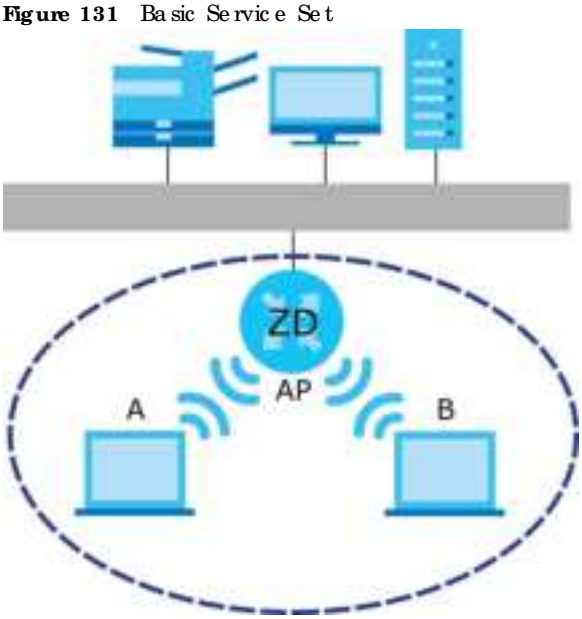
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

9.10.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 131 Basic Service Set



9.10.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The Zyxel Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

9.10.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

9.10.7 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant WiFi adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other WiFi devices on the network support, and to provide more reliable communications in busy WiFi networks.

Use short preamble if you are sure all WiFi devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all WiFi devices on the network support it, otherwise the Zyxel Device uses long preamble.

Note: The WiFi devices MUST use the same preamble mode in order to communicate.

9.10.8 WiFi Protected Setup (WPS)

Your Zyxel Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure WiFi network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has 2 minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

9.10.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within WiFi range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this – for the Zyxel Device).
3. Press the button on one of the devices (it does not matter which). For the Zyxel Device you must press the **WiFi** button for more than 5 seconds.
4. Within 2 minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through a secure connection to the enrollee.

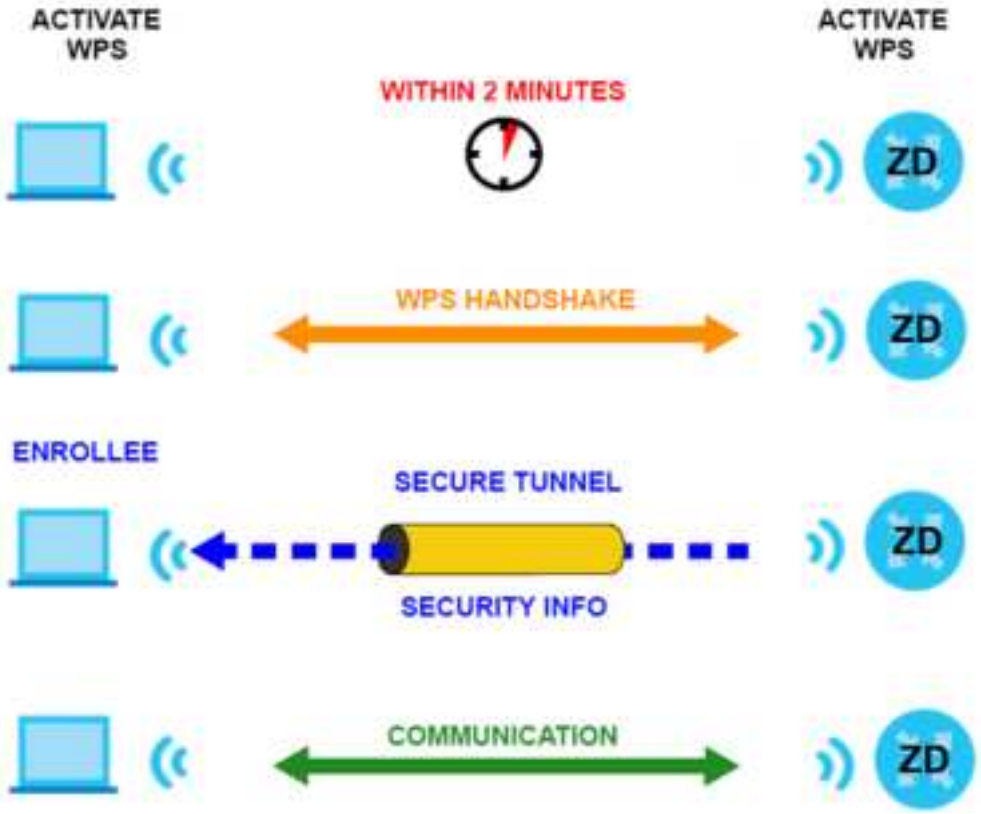
   If you need to make sure that WPS worked, check the list of associated WiFi clients in the AP's configuration utility. If you see the WiFi client in the list, WPS was successful.

9.10.8.2 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA2-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 132 How WPS Works



The roles of registrar and enrollee last only as long as the WPS setup process is active (2 minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the WiFi client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled WiFi clients.

By default, a WPS device is 'un-configured'. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is un-configured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes 'configured'. A configured WiFi client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

9.10.8.3 Example WPS Network Setup

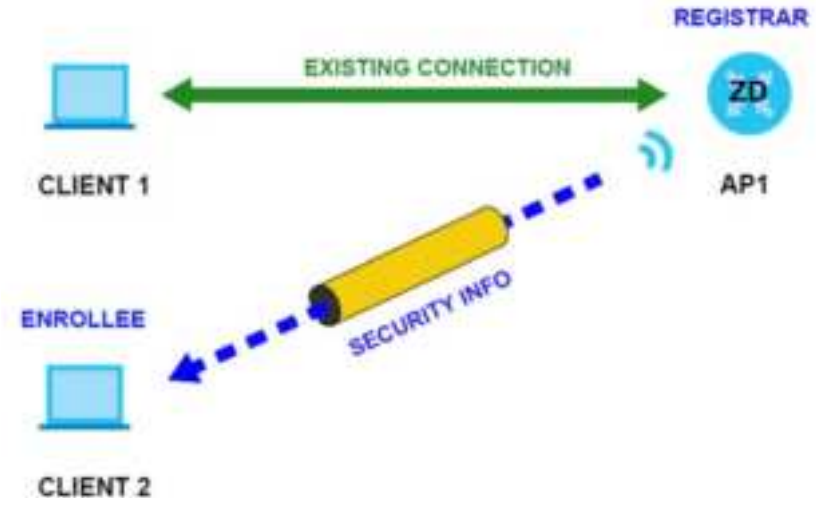
This section shows how security settings are distributed in a sample WPS setup.

The following figure shows a sample network. In step 1, both **AP1** and **Client 1** are un-configured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is un-configured and has no existing information.

Figure 133 WPS: Example Network Step 1

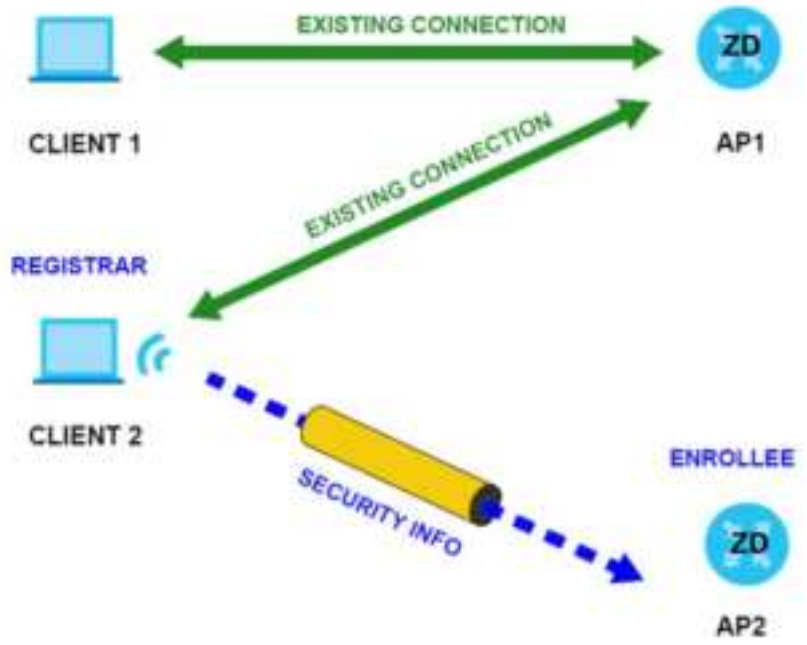
In step **2**, you add another WiFi client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 134 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 135 WPS: Example Network Step 3



9.10.8.4 Limitations of WPS

WPS has some limitations of which you should be aware.

- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it was successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the 'correct' enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS only works simultaneously between two devices, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your WiFi clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

CHAPTER 10
Home Networking

10.1 Home Networking Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

Figure 136 Home Networking Example

10.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 10.2 on page 286).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC addresses (Section 10.3 on page 292).
- Use the **UPnP** screen to enable UPnP (Section 10.4 on page 294).
- Use the **Additional Subnet** screen to configure IP alias and public static IP (Section 10.5 on page 295).
- Use the **STB Vendor ID** screen to configure the Vendor IDs of the connected Set Top Box (STB) devices, which have the Zyxel Device automatically create static DHCP entries for the STB devices when they request IP addresses (Section 10.6 on page 297).
- Use the **Wake on LAN** screen to remotely turn on a device on the network. (Section 10.7 on page 298).
- Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. (Section 10.8 on page 298).

10.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

10.1.2.1 About LAN

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your Zyxel Device will compute the subnet mask automatically based on the IP address that you entered. You do not need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This Zyxel Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

RADVD (Router Advertisement Daemon)

When an IPv6 host sends a Router Solicitation (RS) request to discover the available routers, RADVD with Router Advertisement (RA) messages in response to the request. It specifies the minimum and maximum intervals of RA broadcasts. RA messages containing the address prefix. IPv6 hosts can be generated with the IPv6 prefix an IPv6 address.

10.1.2.2 About UPnP

How do I know if I am using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows 7). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a Multicast message. For security reasons, the Zyxel Device allows Multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and Zyxel

Zyxel has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC).

See Section 10.10 on page 304 for examples on installing and using UPnP.

10.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

10.2 LAN Setup

A LAN IP address is the IP address of a networking device in the LAN. You can use the Zyxel Device's LAN IP address to access its Web Configurator from the LAN. The DHCP server settings define the rules on assigning IP addresses to LAN clients on your network.

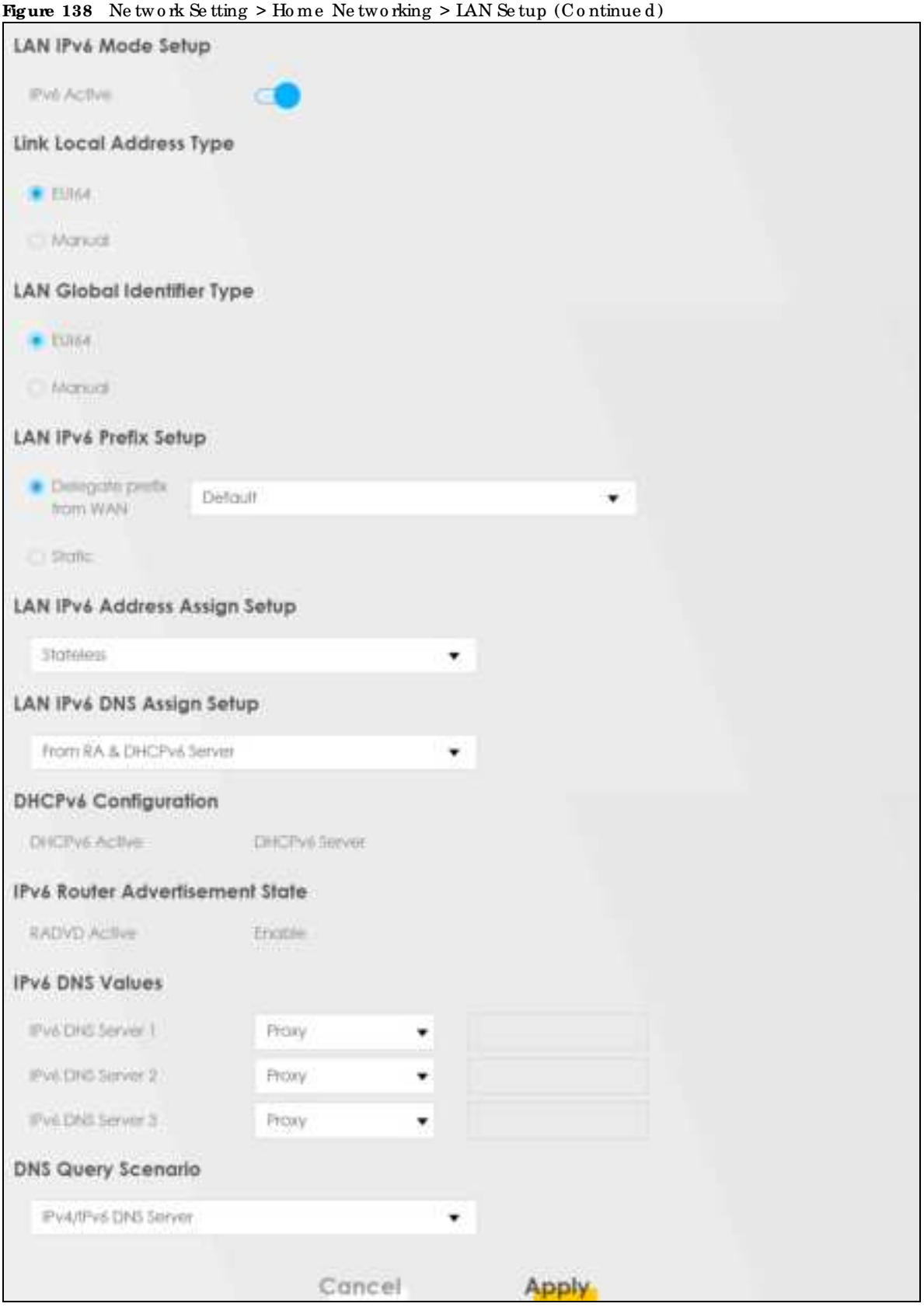
Use this screen to set the Local Area Network IP address and subnet mask of your Zyxel Device. Configure DHCP settings to have the Zyxel Device or a DHCP server assign IP addresses to devices. Click **Network Setting > Home Networking** to open the **LAN Setup** screen.

Follow these steps to configure your LAN settings.

1. Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your Zyxel Device.
2. Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
3. Click **Apply** to save your settings.

Figure 137 Network Setting > Home Networking > LAN Setup

Figure 138 Network Setting > Home Networking > LAN Setup (Continued)



The following table describes the fields in this screen.

Table 76 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group that you want to configure its LAN settings.
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Enter the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
IGMP Snooping See Section 15.1 on page 369 for more information on IGMP snooping.	
Active	Select **Enable** to allow the Zyxel Device to passively learn multicast group.
IGMP Mode	Select **Standard Mode** to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
DHCP Server State	
DHCP	Select **Enable** to have your Zyxel Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. If you select **DHCP Relay**, the Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.
DHCP Relay Server Address This field is only available when you select **DHCP Relay** in the **DHCP** field.	
IP Address	Enter the IPv4 IP address of the actual remote DHCP server in this field.
IP Addressing Values The **IP Addressing Values** fields appear only when you select **Enable** in the **DHCP** field.	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Auto reserve IP for the same host	Enable this if you want to reserve the IP address for the same host.
DHCP Server Lease Time This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.	
Days/Hours/Minutes	DHCP server leases an address to a new client device for a period of time, called the DHCP lease time. When the lease expires, the DHCP server might assign the IP address to a different client device.
DNS Values This field appears only when you select **Enable** in the **DHCP** field.	

Table 76 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS	The Zyxel Device supports DNS proxy by default. The Zyxel Device sends out its own LAN IP address to the DHCP clients as the first DNS server address. DHCP clients use this first DNS server to send domain-name queries to the Zyxel Device. The Zyxel Device sends a response directly if it has a record of the domain-name to IP address mapping. If it does not, the Zyxel Device queries an outside DNS server and relays the response to the DHCP client. Select **DNS Proxy** to have the DHCP clients use the Zyxel Device's own LAN IP address. The Zyxel Device works as a DNS relay. Select **Static** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **From ISP** if your ISP dynamically assigns DNS server information (and the Zyxel Device's WAN IP address).
LAN IPv6 Mode Setup	
IPv6 Active	Use this to enable or disable IPv6 on the Zyxel Device. When IPv6 is used, the following fields need to be set.
Link Local Address Type	A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv6. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows. Select **EUI64** to allow the Zyxel Device to generate an interface ID for the LAN interface's link-local address using the EUI-64 format. Otherwise, enter an interface ID for the LAN interface's link-local address if you select **Manual**. Link-local Unicast Address Format 1111 1110 10 | 0 | Interface ID 10 bits | 54 bits | 64 bits
EUI64	Select this to have the Zyxel Device generate an interface ID for the LAN interface's link-local address using the EUI-64 format.
Manual	Select this to manually enter an interface ID for the LAN interface's link-local address.
LAN Global Identifier Type	Select **EUI64** to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address. Select **Manual** to manually enter an interface ID for the LAN interface's global IPv6 address.
EUI64	Select this to have the Zyxel Device generate an interface ID using the EUI-64 format for its global address.
Manual	Select this to manually enter an interface ID for the LAN interface's global IPv6 address.
LAN IPv6 Prefix Setup	Select **Delegate prefix from WAN** to automatically obtain an IPv6 network prefix from the service provider or an uplink router. Select **Static** to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the Zyxel Device's LAN IPv6 address.
MLD Snooping / Multicast Snooping	Multicast Listener Discovery (MLD) allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
Active	Click this switch to enable or disable MLD Snooping on the Zyxel Device. When the switch goes to the right the function is enabled. Otherwise, it is not. This allows the Zyxel Device to check MLD packets passing through it and learn the multicast group membership. It helps reduce multicast traffic.

Table 76 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
MLD Mode	Select **Standard Mode** to forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to block all unknown multicast packets from the WAN.
LAN IPv6 Address Assign Setup	Select how you want to obtain an IPv6 address: **Stateless**: The Zyxel Device uses IPv6 stateless auto-configuration. RADVD (Router Advertisement Daemon) is enabled to have the Zyxel Device send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. **Stateful**: The Zyxel Device uses IPv6 stateful auto-configuration. The DHCPv6 server is enabled to have the Zyxel Device act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients.
LAN IPv6 DNS Assign Setup	Select how the Zyxel Device provide DNS server and domain name information to the clients: **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6. **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. **From Router Advertisement**: The Zyxel Device provides DNS information through router advertisements.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. **DHCP Server** displays if you configured the Zyxel Device to act as a DHCPv6 server which assigns IPv6 addresses and/or DNS information to clients.
IPv6 Router Advertisement State	
RADVD Active	This shows whether RADVD is enabled or not.
IPv6 Address Values	
IPv6 Start Address	This field specifies the first of the contiguous addresses in the IPv6 address pool.
IPv6 End Address	This field specifies the last of the contiguous addresses in the IPv6 address pool.
IPv6 Domain Name	The field specifies the domain name of the IPv6 address.
IPv6 DNS Values	
IPv6 DNS Server 1 – 3	Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses. **User Defined** – Select this if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. **From ISP** – Select this if your ISP dynamically assigns IPv6 DNS server information. **Proxy** – Select this if the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay. Otherwise, select **None** if you do not want to configure IPv6 DNS servers.

Table 76 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Query Scenario	Select how the Zyxel Device handles clients' DNS information requests. **IPv4/IPv6 DNS Server**: The Zyxel Device forwards the requests to both the IPv4 and IPv6 DNS servers and sends clients the first DNS information it receives. **IPv6 DNS Server Only**: The Zyxel Device forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives. **IPv4 DNS Server Only**: The Zyxel Device forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. **IPv6 DNS Server First**: The Zyxel Device forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. **IPv4 DNS Server First**: The Zyxel Device forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.3 Static DHCP

When any of the LAN clients in your network want an assigned fixed IP address, add a static lease for each LAN client. Knowing the LAN client's MAC addresses is necessary. This table allows you to assign IP addresses on the LAN to individual computers based on their MAC addresses.

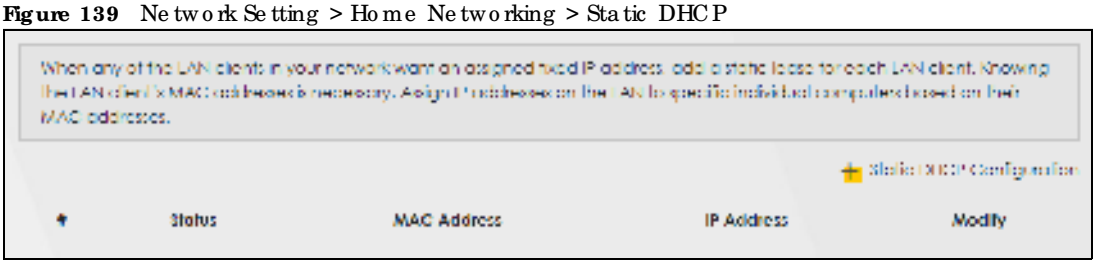
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

10.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your Zyxel Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 139 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

Table 77 Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to configure a static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the Zyxel Device.
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). 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.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to remove the connection.

If you click **Static DHCP Configuration** in the **Static DHCP** screen, the following screen displays. Using a static DHCP means a LAN client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a client device by selecting the interface group of this client device and its IP address type and selecting the device/computer from a list or manually entering its MAC address and assigned IP address.

Figure 140 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

The following table describes the labels in this screen.

Table 78 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration

LABEL	DESCRIPTION
Active	Select **Enable** to activate static DHCP in your Zyxel Device.
Group Name	Select the interface group for which you want to configure the static DHCP settings.
IP Type	The **IP Type** is normally **IPv4** (non-configurable).
Select Device Info	Select between **Manual Input** which allows you to enter the next two fields (**MAC Address** and **IP Address**); or select an existing LAN device to show its MAC address and IP address.

Table 78 Network Setting > Home Networking > Static DHCP: Static DHCP Configuration (continued)

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN if you select **Manual Input** in the previous field.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify if you select **Manual Input** in the previous field.
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.4 UPnP

Universal Plug and Play (UPnP) is an open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between networking devices or software applications which have UPnP enabled. A UPnP device can dynamically join a network, obtain an IP address, advertise its services, and learn about other devices on the network. A device can also leave a network automatically when it is no longer in use.

See Section 10.10 on page 304 for more information on UPnP.

Note: To use **UPnP NAT-T**, enable **NAT** in the **Network Setting > Broadband > Edit** or **Add New WAN Interface** screen.

Use the following screen to configure the UPnP settings on your Zyxel Device. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

Figure 141 Network Setting > Home Networking > UPnP

The following table describes the labels in this screen.

Table 79 Network Settings > Home Networking > UPnP

LABEL	DESCRIPTION
UPnP State	
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the Zyxel Device's IP address (although you must still enter the password to access the Web Configurator).
UPnP NAT-T State	
UPnP NAT-T	Select **Enable** to activate UPnP with NAT enabled. UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions.
#	This field displays the index number of the entry.
Description	This field displays the description of the UPnP NAT-T connection.
Destination IP Address	This field displays the IP address of the other connected UPnP-enabled device.
External Port	This field displays the external port number that identifies the service.
Internal Port	This field displays the internal port number that identifies the service.
Protocol	This field displays the protocol of the NAT mapping rule. Choices are **TCP** or **UDP**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.5 LAN Additional Subnet

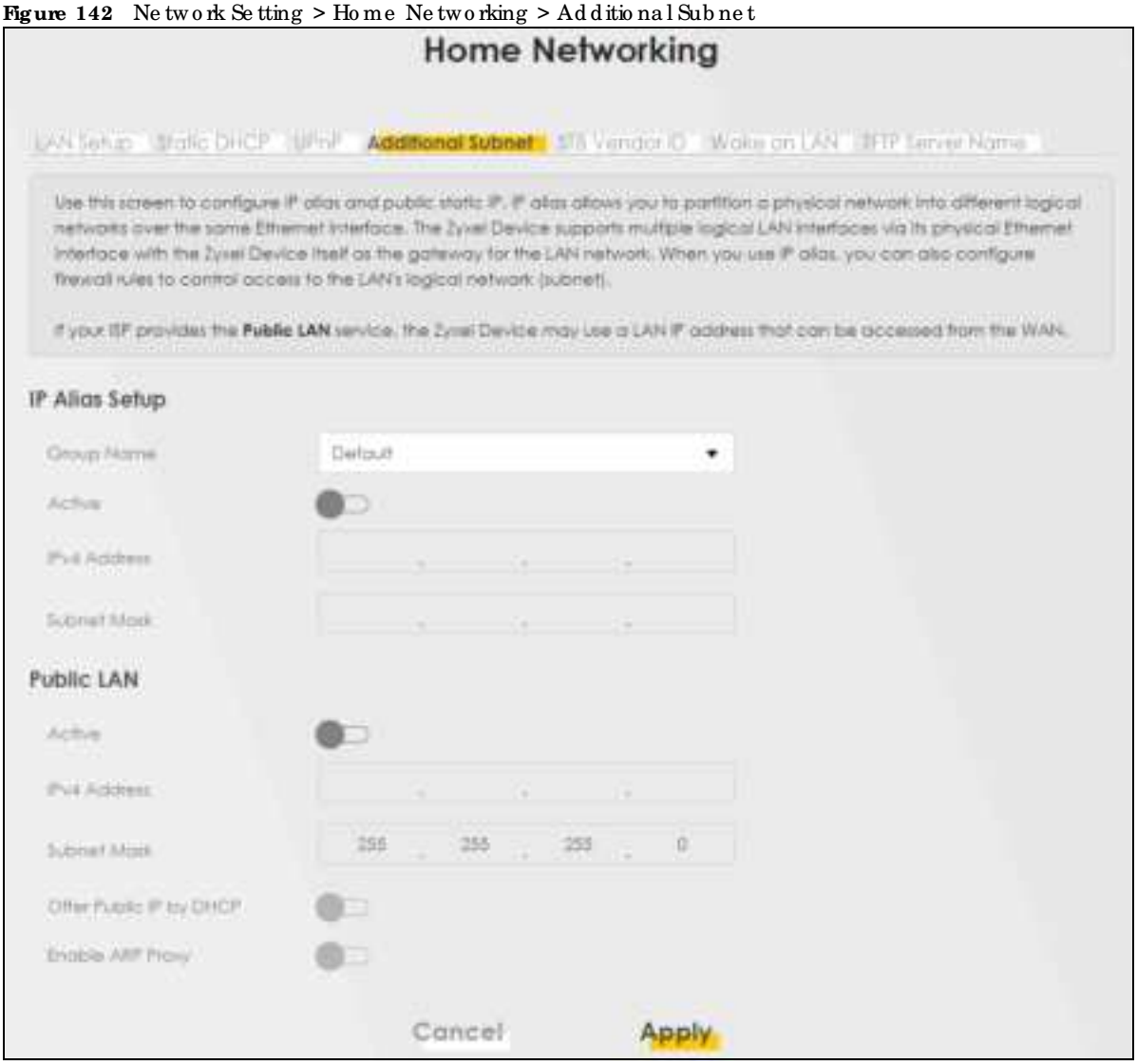
Use this screen to configure IP alias and public static IP.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Zyxel Device supports multiple logical LAN interfaces through its physical Ethernet interface with the Zyxel Device itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

If your ISP provides the **Public LAN** service, the Zyxel Device may use a LAN IP address that can be accessed from the WAN.

Click **Network Setting > Home Networking > Additional Subnet** to display the screen shown next.

Figure 142 Network Setting > Home Networking > Additional Subnet



The following table describes the labels in this screen.

Table 80 Network Setting > Home Networking > Additional Subnet

LABEL	DESCRIPTION
IP Alias Setup	
Group Name	Select the interface group name for which you want to configure the IP alias settings.
Active	Click this switch to enable a logical LAN for the Zyxel Device. When this is enabled, the following fields will be configurable.
IPv4 Address	Enter the IP address of your Zyxel Device in dotted decimal notation.
Subnet Mask	Your Zyxel Device will automatically calculate the subnet mask based on the IPv4 address that you assign. Unless you are implementing subnetting, use this value computed by the Zyxel Device.
Public LAN	
Active	Click this switch to enable or disable the Public LAN feature. Your ISP must support Public LAN and static IP.
IPv4 Address	Enter the public IP address provided by your ISP.

Table 80 Network Setting > Home Networking > Additional Subnet (continued)

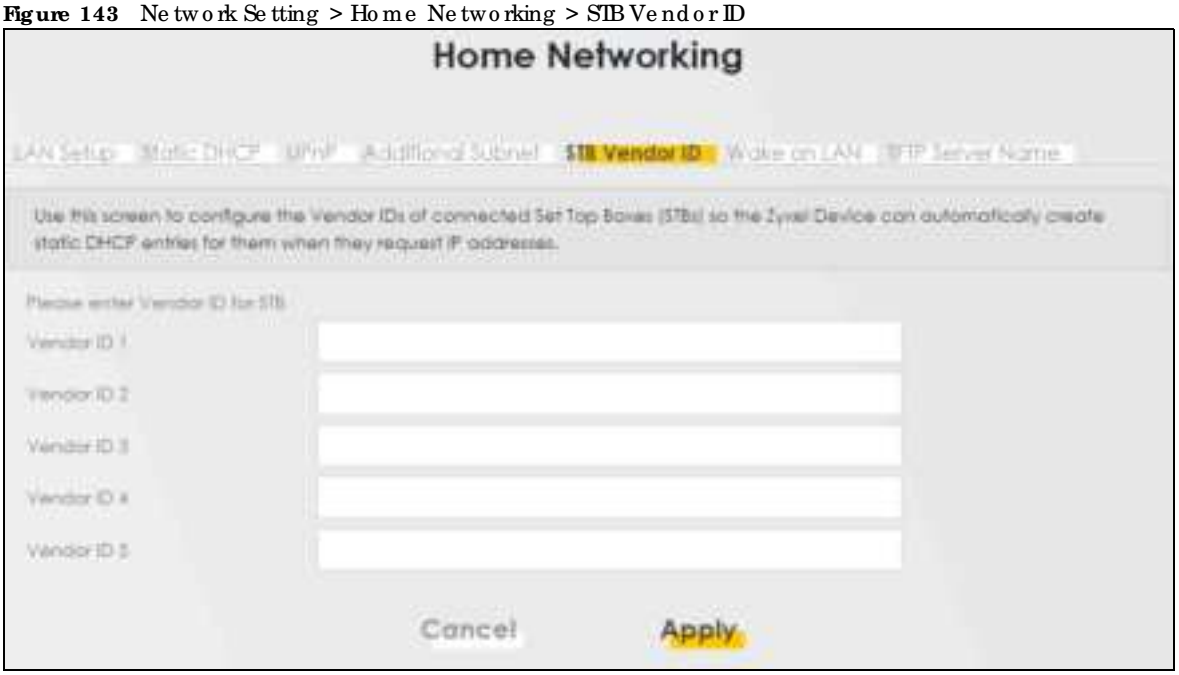
LABEL	DESCRIPTION
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.
Offer Public IP by DHCP	Click this switch to enable the Zyxel Device to provide public IP addresses by DHCP server. Otherwise, click to disable.
Enable ARP Proxy	Click this switch to enable the Address Resolution Protocol (ARP) proxy. Otherwise, click to disable.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

10.6 STB Vendor ID

Use this screen to configure the Vendor IDs of connected Set Top Boxes (STBs) so the Zyxel Device can automatically create static DHCP entries for them when they request IP addresses.

Click **Network Setting > Home Networking > STB Vendor ID** to open this screen.

Figure 143 Network Setting > Home Networking > STB Vendor ID



The following table describes the labels in this screen.

Table 81 Network Setting > Home Networking > STB Vendor ID

LABEL	DESCRIPTION
Vendor ID 1 – 5	These are STB's Vendor Class Identifiers (DHCP option 60). A Vendor Class Identifier is usually used to inform the DHCP server a DHCP client's vendor and functionality.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

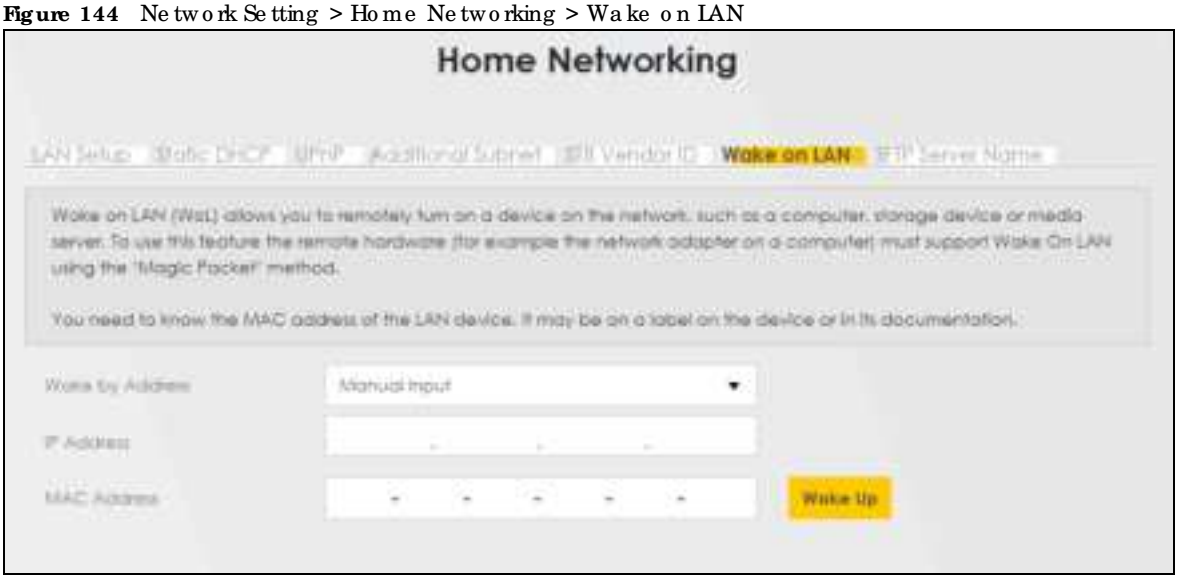
10.7 Wake on LAN

Wake on LAN (WoL) allows you to remotely turn on a device on the network, such as a computer, storage device or media server. To use this feature, the remote hardware (for example the network adapter on a computer) must support Wake on LAN using the 'Magic Packet' method.

You need to know the MAC address of the LAN device. It may be on a label on the LAN device.

Click **Network Setting > Home Networking > Wake on LAN** to open this screen.

Figure 144 Network Setting > Home Networking > Wake on LAN



The following table describes the labels in this screen.

Table 82 Network Setting > Home Networking > Wake on LAN

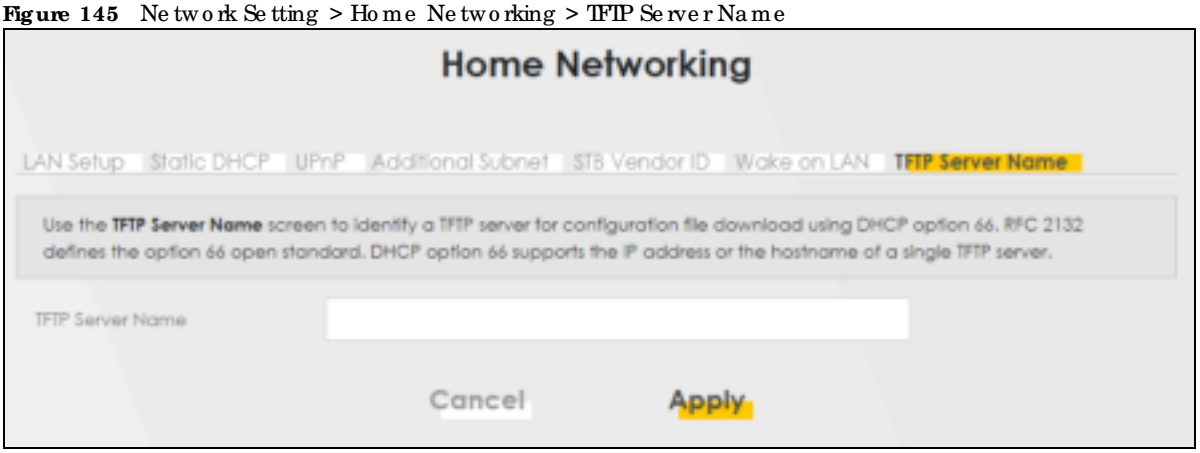
LABEL	DESCRIPTION
Wake by Address	Select **Manual** and enter the IP address or MAC address of the LAN device to turn it on remotely. The drop-down list also lists the IP addresses that can be found in the Zyxel Device's ARP table. If you select an IP address, the MAC address of the LAN device with the selected IP address then displays in the **MAC Address** field.
IP Address	Enter the IPv4 IP address of the LAN device to turn it on. This field is not available if you select an IP address in the **Wake by Address** field.
MAC Address	Enter the MAC address of the LAN device to turn it on. A MAC address consists of six hexadecimal character pairs.
Wake Up	Click this to send a WoL magic packet to wake up the specified LAN device.

10.8 TFTP Server Name

Use the **TFTP Server Name** screen to identify a TFTP server for configuration file download using DHCP option 66. RFC 2132 defines the option 66 open standard. DHCP option 66 supports the IP address or the host name of a single TFTP server.

Click **Network Setting > Home Networking > TFTP Server Name** to open this screen.

Figure 145 Network Setting > Home Networking > TFTP Server Name



The following table describes the labels in this screen.

Table 83 Network Setting > Home Networking > TFTP Server Name

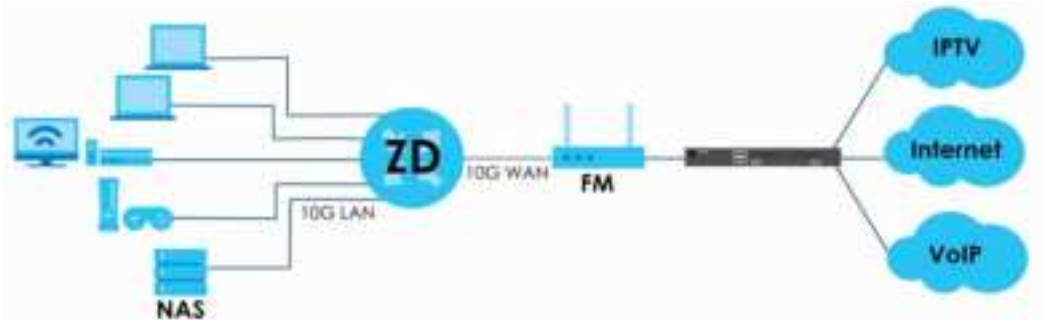
LABEL	DESCRIPTION
TFTP Server Name	Enter the IP address or the host name of a single TFTP server.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

Any Port Any Service (APAS) allows a LAN device to use any available port to access any available service from a remote WAN device. Typically, a LAN device, such as a Set Top Box (STB), would have to use a specific port to access video streams from a video server. With APAS, the video streams only need to be received through the specified Bridge WAN interface for the LAN device specified in the APAS rule. You can connect the LAN device to any LAN port. Other LAN devices can access the Internet using the default gateway.

Unlike **Port Forwarding**, which forwards traffic based on port numbers, you do not need to know the port number for the video traffic from the IPTV server. You just select the LAN device host name or enter its MAC address and select a Bridge WAN interface.

Use the wildcard '*' for a range of MAC addresses for multiple LAN devices. For example, enter 00:13:49:*:*:* for all LAN devices from a vendor with the MAC OUI 00:13:49. (range). Any device with that MAC OUI aa:bb:cc connected to any LAN port on the Zyxel Device can access services or can be accessed for services through the specified Bridge WAN interface. For example, the LAN device could be an STB receiving video streams from a video server, or it could be a server, allowing access to it through the specified Bridge WAN interface.

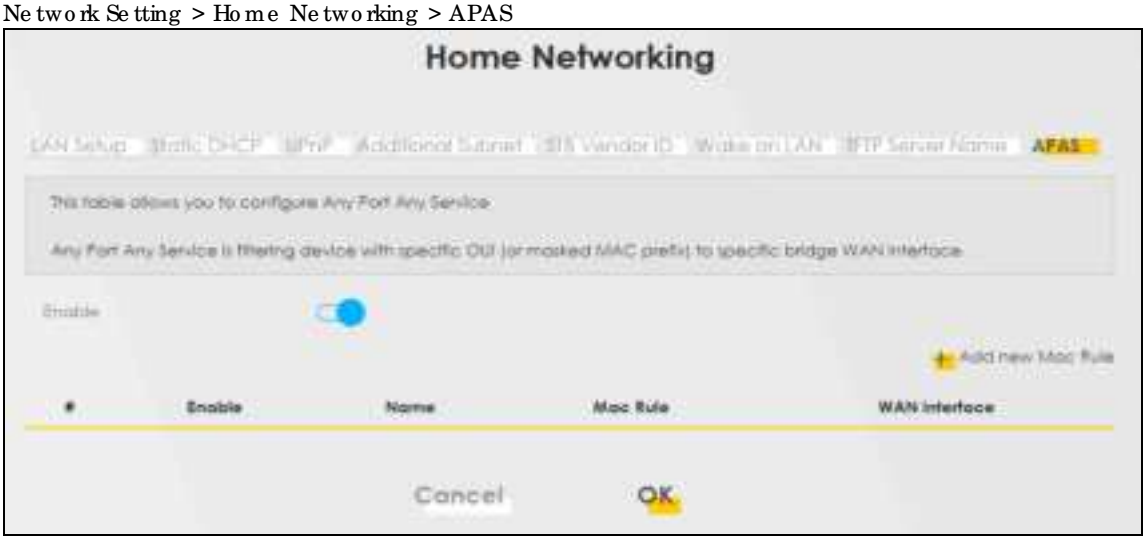
Note: You must configure a Bridge WAN interface in advance.



As APAS allows incoming traffic from any port to access any service on a configured LAN device, it may be difficult to distinguish between appropriate and malicious traffic going to the LAN device. Make sure to properly configure firewall rules to protect the LAN device, and monitor network traffic for suspicious activity.

Click **Network Setting > Home Networking > APAS** to open this screen.

Network Setting > Home Networking > APAS



The following table describes the labels in this screen.

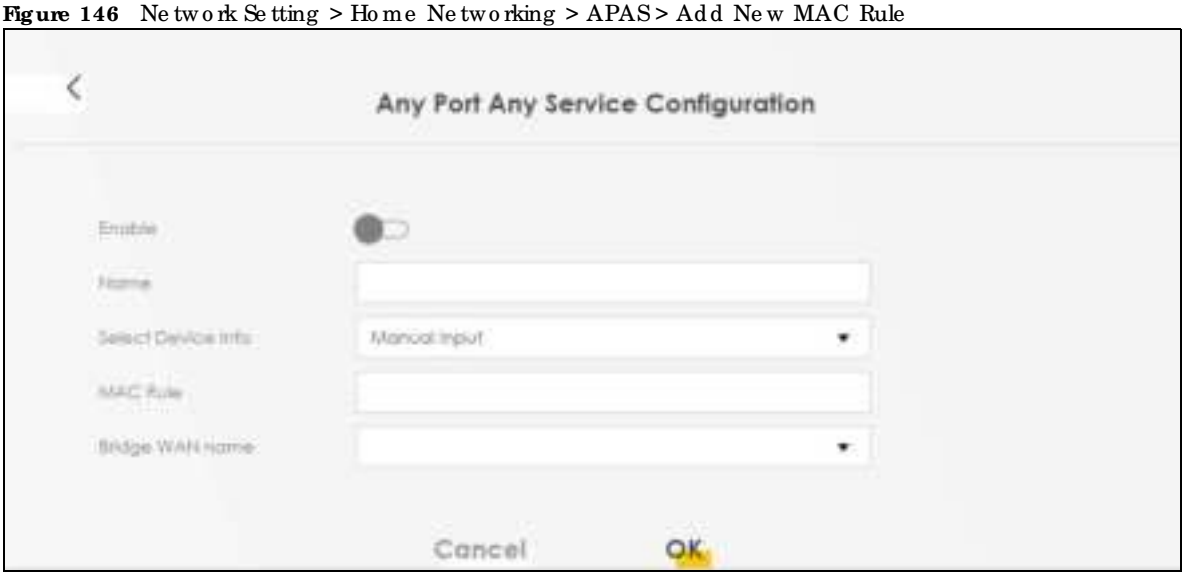
Table 84 Network Setting > Home Networking > APAS

LABEL	DESCRIPTION
Enable	Click **Enable** to activate APAS.
Add new MAC Rule	Click this button to add a new MAC rule. You can create up to eight MAC rules.
#	This is the index number.
Name	This is the name of the rule.
MAC Rule	This is the LAN host MAC address that is applied to the rule.
WAN Interface	This is the bridge WAN interface for incoming traffic.
Cancel	Click **Cancel** to restore your previously saved changes.
OK	Click **OK** to save your changes.

10.8.1 Add APAS

Use this screen to create a new MAC rule. Click **Network Setting > Home Networking > APAS > Add New MAC Rule** to open the following screen.

Figure 146 Network Setting > Home Networking > APAS > Add New MAC Rule



The following table describes the labels in this screen.

Table 85 Network Setting > Home Networking > APAS > Add New MAC Rule

LABEL	DESCRIPTION
Enable	Click this to enable APAS on the Zyxel Device.
Name	Enter a name of up to 64 characters for the **APAS** rule to this host(s). Allowed characters for **Name** include the following within quotes: "!#%()*+,-./ 0123456789:=?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]_abcdefghijklmnopqrstuvwxyz{}~"
Select Device Info	Select a connected LAN host or select **Manual Input** to enter the MAC address of a client that is not yet connected and does not display in **Connection Status > Connectivity**.
MAC Rule	If you selected **Manual Input** for **Select Device Info**, then enter the LAN host MAC address here. You can use the wildcard '*' for a MAC address range. For example, enter 00:13:49:*:*:* for all LAN devices from a vendor with the MAC OUI 00:13:49.
Bridge WAN Name	Select a Bridge WAN interface for incoming traffic to apply the rule. You must have created at least one Bridge WAN interface in **Network Setting > Broadband** screen.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

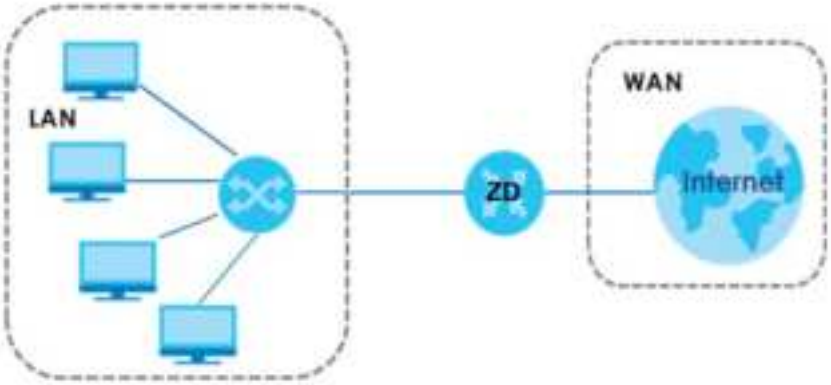
10.9 Technical Reference

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

LANs, WANs and the Zyxel Device

The actual physical connection determines whether the Zyxel Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 147 LAN and WAN IP Addresses



10.9.1 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Zyxel Device as a DHCP server or disable it. When configured as a server, the Zyxel Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The Zyxel Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

10.9.2 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Zyxel Device supports the IPCP DNS server extensions through the DNS proxy feature.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

10.9.3 LAN TCP/IP

The Zyxel Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Zyxel Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Zyxel Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Zyxel Device will compute the subnet mask automatically based on the IP address that you entered. You do not need to change the subnet mask computed by the Zyxel Device unless you are instructed to do otherwise.

Private IP Addresses

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

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

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

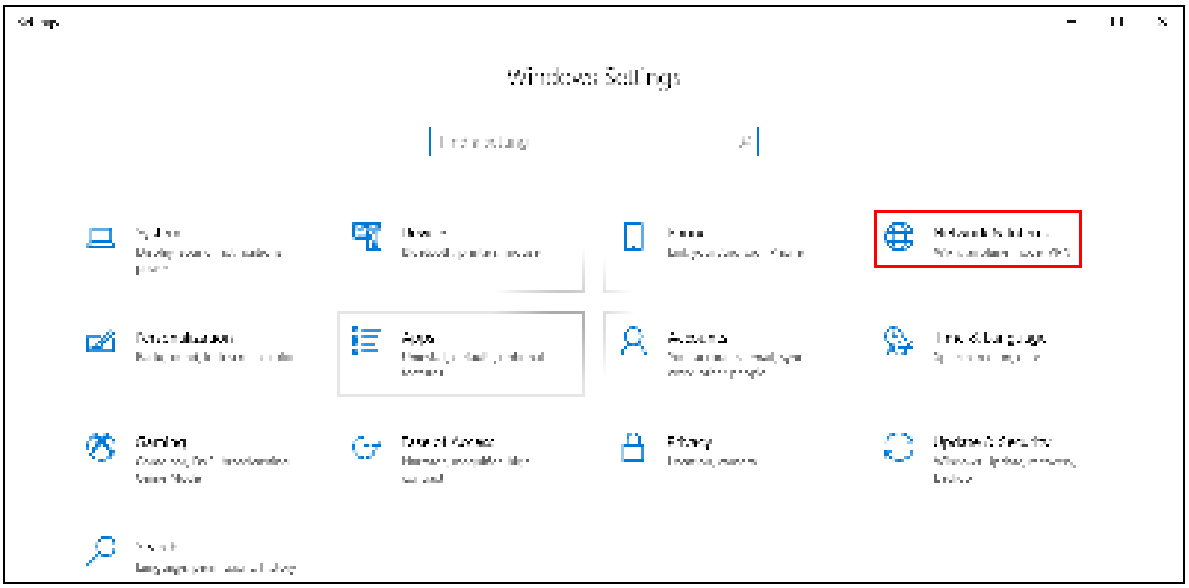
Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

10.10 Turn on UPnP in Windows 10 Example

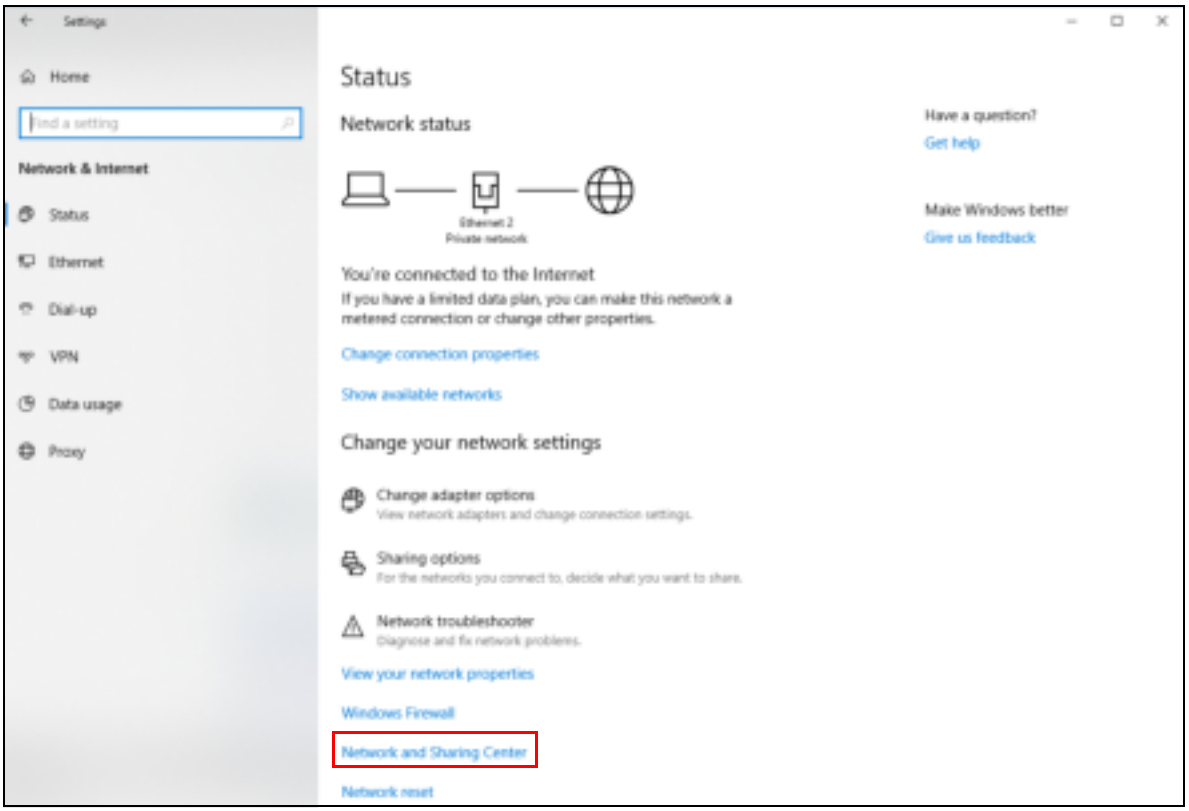
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting > Home Networking > UPnP**.

Make sure the computer is connected to the LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.

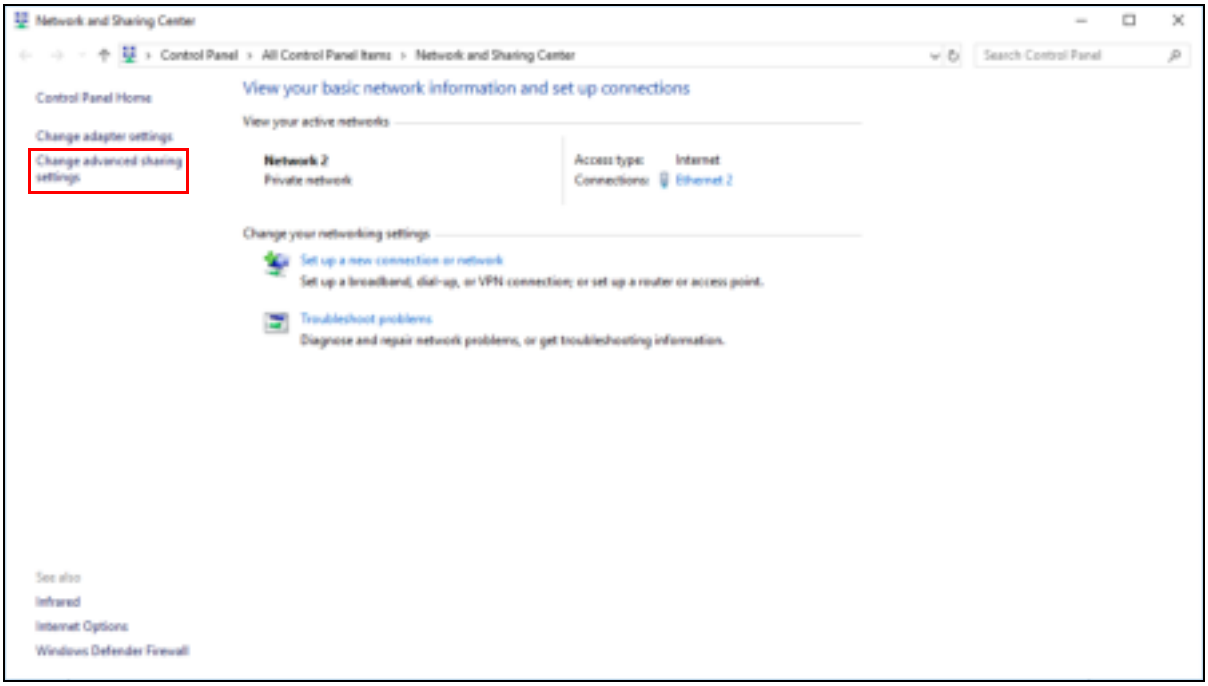
1 Click the start icon, **Settings** and then **Network & Internet**.



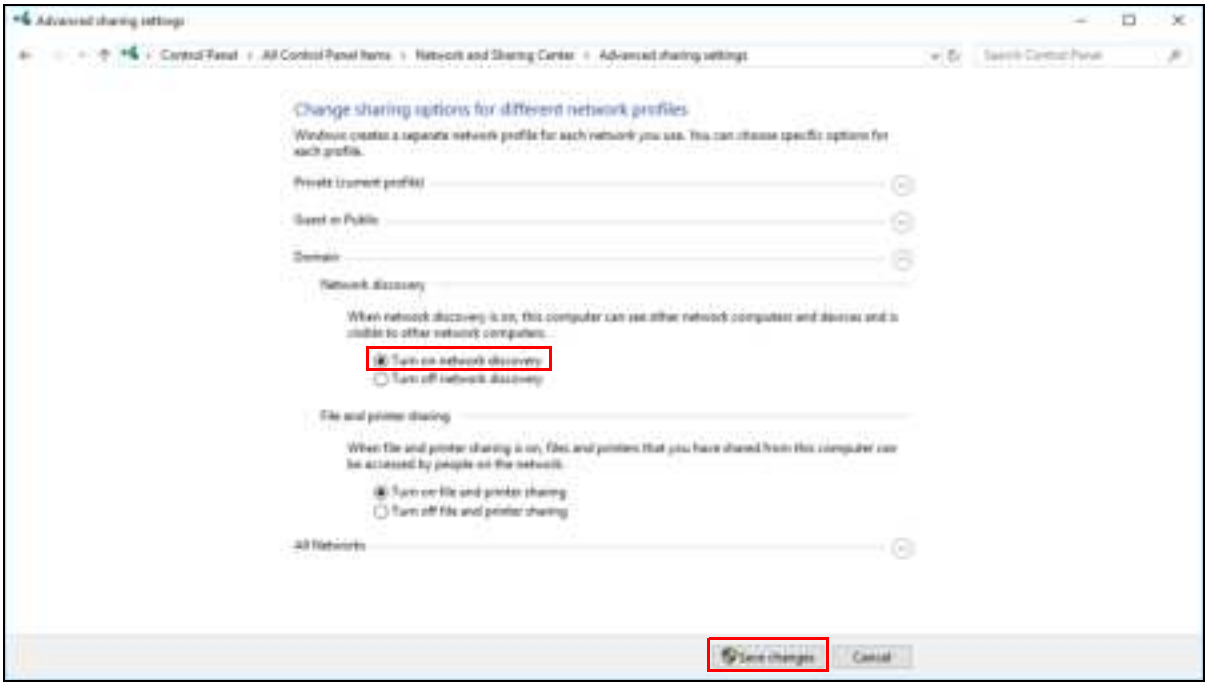
2 Click **Network and Sharing Center**.



3 Click **Change advanced sharing settings**.



4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



10.10.1 Auto-discover Your UPnP-enabled Network Device

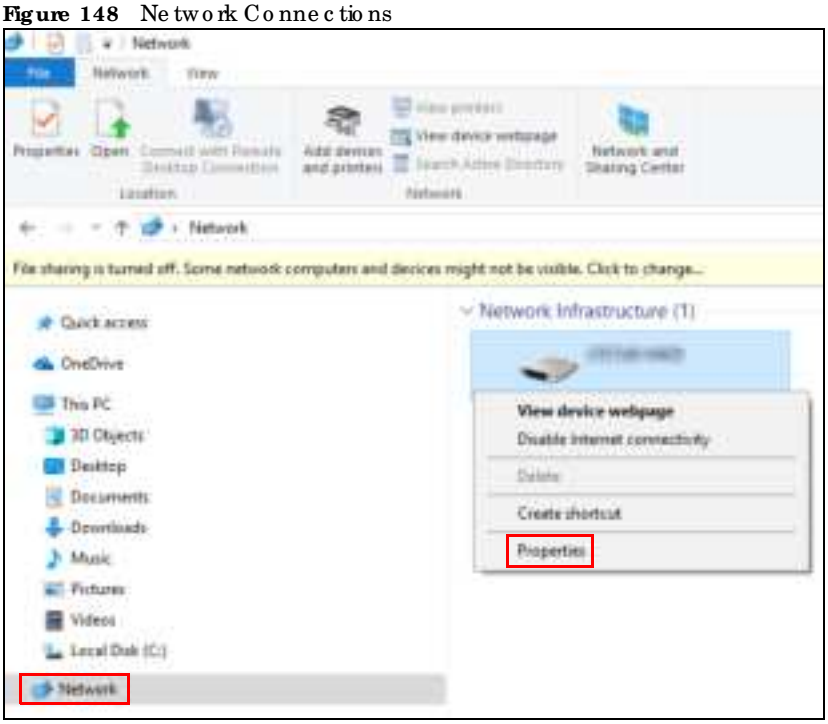
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

Make sure your computer is connected to the LAN port of the Zyxel Device.

1 Open **File Explorer** and click **Network**.

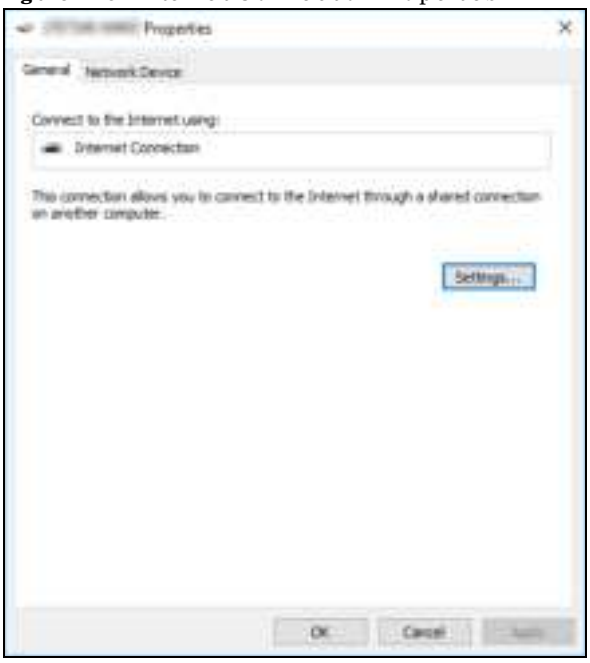
2 Right-click the Zyxel Device icon and select **Properties**.

Figure 148 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see port mappings.

Figure 149 Internet Connection Properties



4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 150 Internet Connection Properties: Advanced Settings

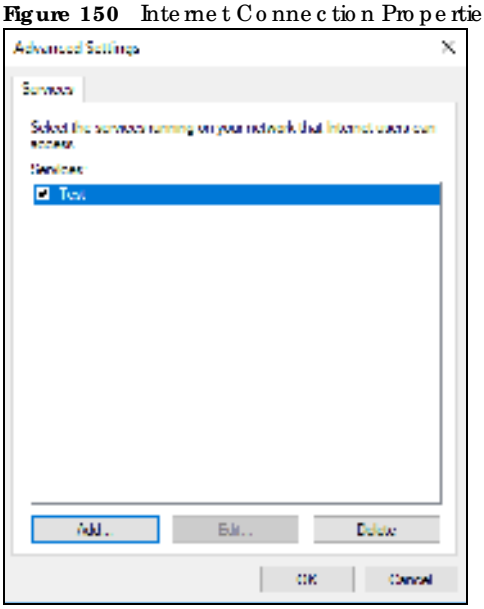
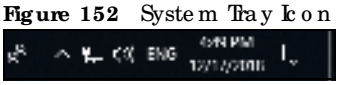


Figure 151 Internet Connection Properties: Advanced Settings: Add

Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

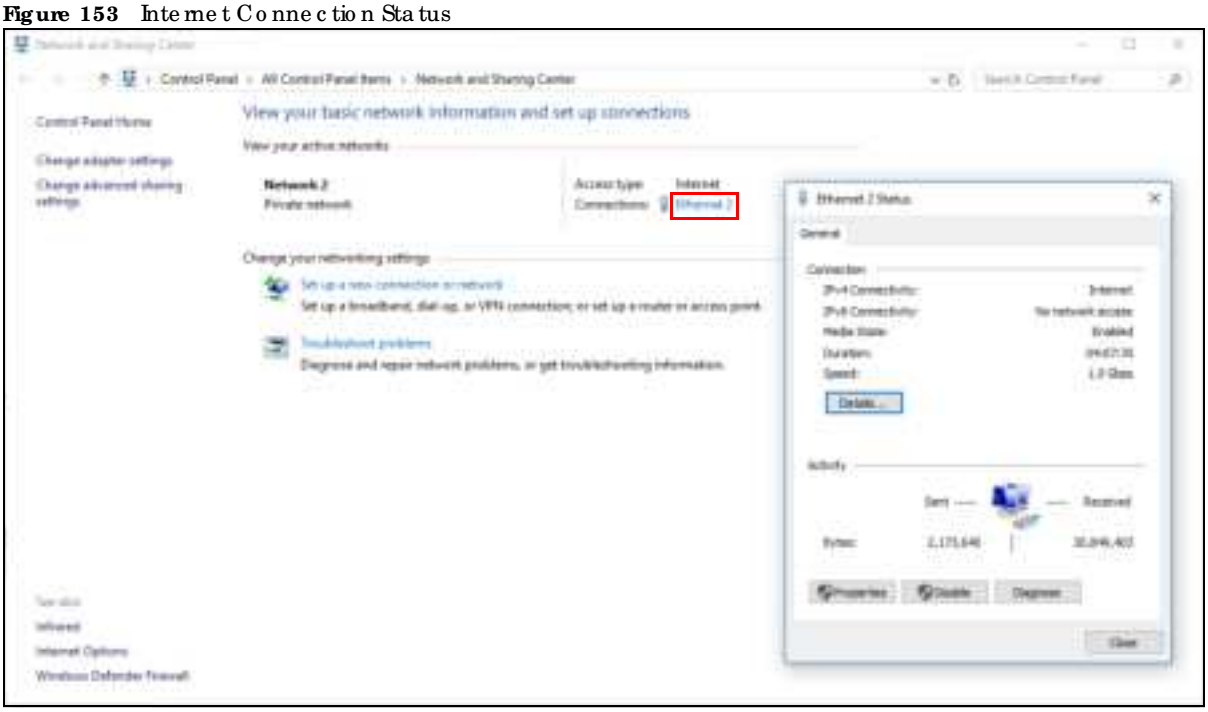
5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 152 System Tray Icon



6 To see more details about your current Internet connection status, right click the network icon in the system tray and click **Open Network & Internet settings**. Click **Network and Sharing Center** and click the **Connections**.

Figure 153 Internet Connection Status



10.11 Web Configurator Access with UPnP in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

Figure 154 Network Connections

3 An icon with the description for each UPnP-enabled device displays under **Network Infrastructure**.

4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

Figure 155 Network Connections: Network Infrastructure

5 Right-click the icon for your Zyxel Device and select **Properties**. Click the **Network Device** tab. A window displays information about the Zyxel Device.

Figure 156 Network Connections: Network Infrastructure: Properties: Example

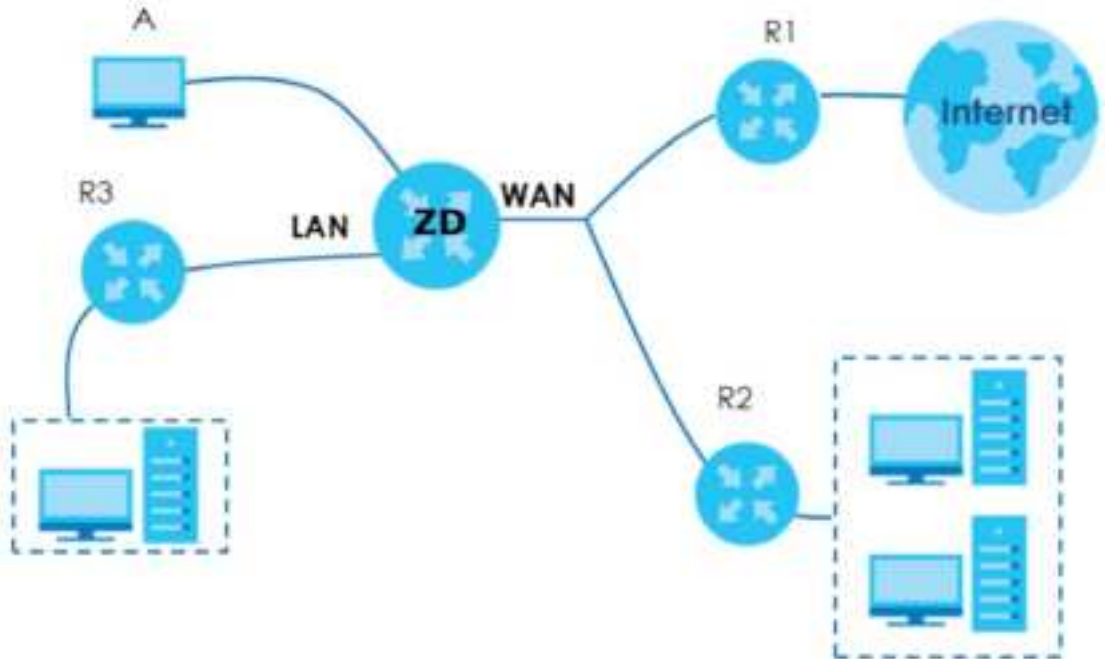
CHAPTER 11
Routing

11.1 Routing Overview

The Zyxel Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Zyxel Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Zyxel Device's LAN interface. The Zyxel Device routes most traffic from **A** to the Internet through the Zyxel Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

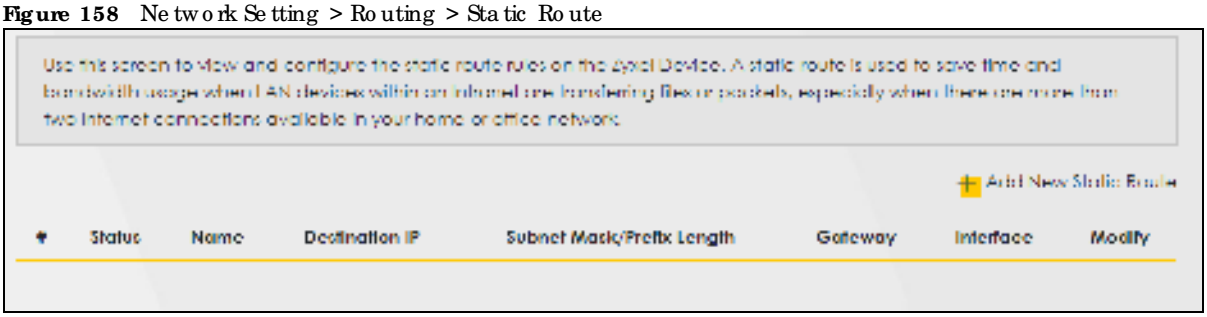
Figure 157 Example of Static Routing Topology



11.2 Configure Static Route

Use this screen to view and configure static route rules on the Zyxel Device. A static route is used to save time and bandwidth usage when LAN devices within an Intranet are transferring files or packets, especially when there are more than two Internet connections in your home or office network. Click **Network Setting > Routing** to open the **Static Route** screen.

Figure 158 Network Setting > Routing > Static Route



The following table describes the labels in this screen.

Table 86 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Zyxel Device.
#	This is the number of an individual static route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Name	This is the name of the static route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask/ Prefix Length	This parameter specifies the IP network subnet mask of the final destination.
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.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the Zyxel Device. Click the **Delete** icon to remove a static route from the Zyxel Device.

11.2.1 Add or Edit Static Route

Use this screen to add or edit a static route. Click **Add New Static Route** in the **Static Route** screen, the following screen appears. Configure the required information for a static route.

Note: The **Gateway IP Address** must be within the range of the selected interface in **Use Interface**.

Figure 159 Network Setting > Routing > Static Route > Add New Static Route

The following table describes the labels in this screen.

Table 87 Network Setting > Routing > Static Route > Add New Static Route

LABEL	DESCRIPTION
Active	Click this switch to activate static route. Otherwise, click to disable.
Route Name	Enter a name for your static route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
IP Type	Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4**/**IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD).
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.
Subnet Mask	If you are using IPv4 and 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. Enter the IP subnet mask here. Note: This field appears only when you select **IPv4** in the **IP Type** field.
Prefix Length	If you are using IPv6, enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address. Note: This field appears only when you select **IPv6** in the **IP Type** field.
Use Gateway IP Address	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. Click this switch to enable or disable the gateway IP address. When the switch goes to the right, the function is enabled. Otherwise, it is not.

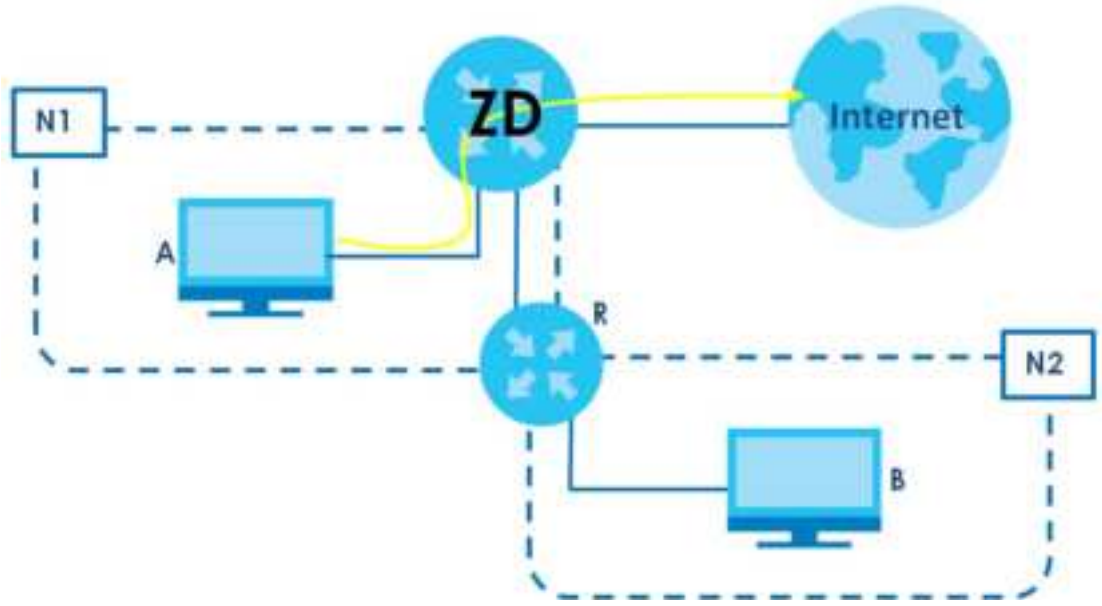
Table 87 (continued) Network Setting > Routing > Static Route > Add New Static Route

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway.
User Interface	Select the WAN interface you want to use for this static route.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

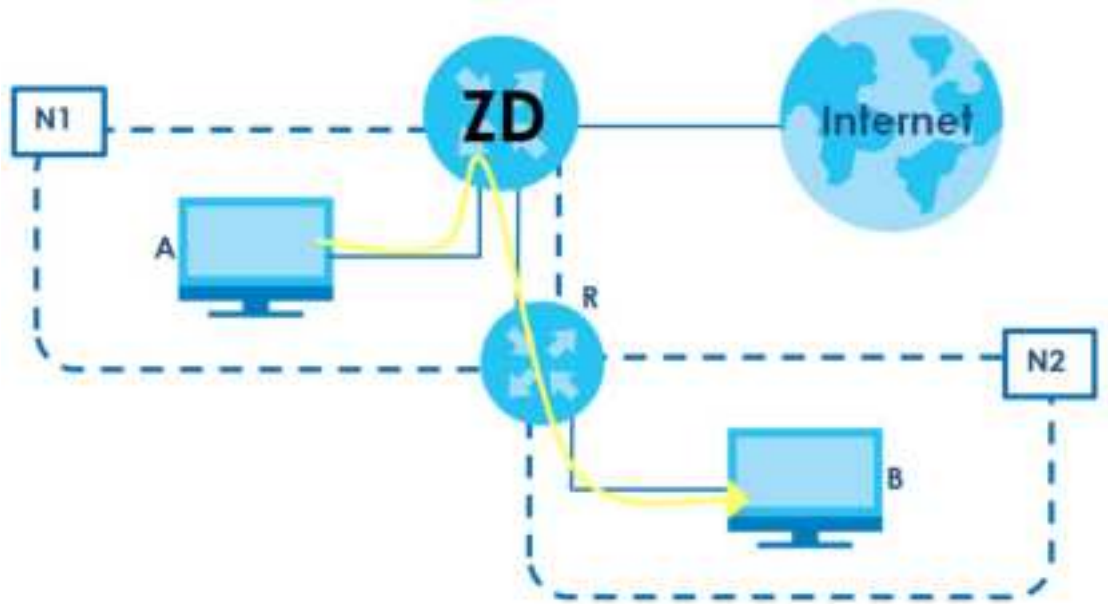
11.2.1.1 An Example of Adding a Static Route

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the Zyxel Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the Zyxel Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the Zyxel Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the Zyxel Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the Zyxel Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 88 IP Settings in this Tutorial

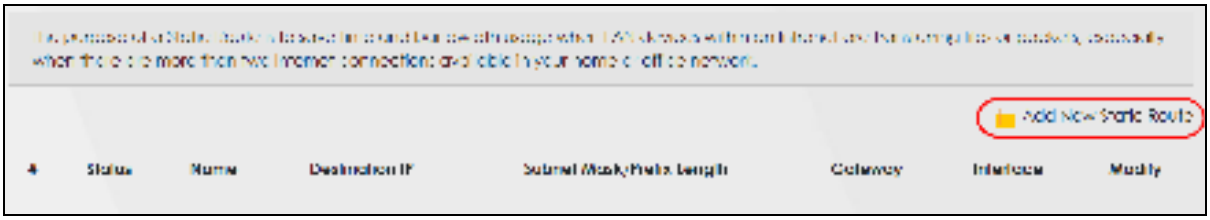
DEVICE / COMPUTER	IP ADDRESS
The Zyxel Device's WAN	172.16.1.1
The Zyxel Device's LAN	192.168.1.1
IP Type	IPv4
Use Interface	Default
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Log into the Zyxel Device's Web Configurator.

2 Click **Network Setting** > **Routing**.

3 Click **Add new Static Route** in the **Static Route** screen.



4 Configure the **Static Route Setup** screen using the following settings:

- Click the **Active** button to enable this static route. When the switch goes to the right, the function is enabled. Enter the **Route Name** as **R**.

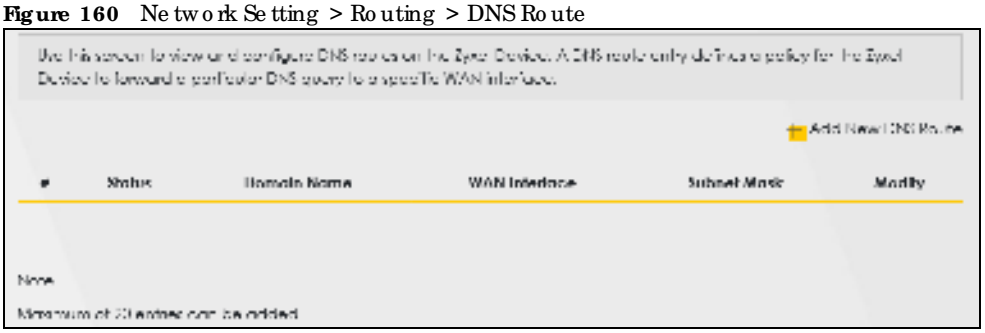
- Set **IP Type** to **IPv4**.
- Enter the **Destination IP Address 192.168.10.1** and **IP Subnet Mask 255.255.255.0** for the destination, **N2**.
- Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right, the function is enabled. Enter **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
- Select **Default** as the **Use Interface**.
- Click **OK**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

11.3 DNS Route

Use this screen to view and configure DNS routes on the Zyxel Device. A DNS route entry defines a policy for the Zyxel Device to forward a particular DNS query to a specific WAN interface. Click **Network Setting > Routing > DNS Route** to open the **DNS Route** screen.

Figure 160 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

Table 89 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to create a new entry.
#	This is the number of an individual DNS route.
Status	This field indicates whether the rule is active (yellow bulb) or not (gray bulb).
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Subnet Mask	This parameter specifies the IP network subnet mask.
Modify	Click the **Edit** icon to configure a DNS route on the Zyxel Device. Click the **Delete** icon to remove a DNS route from the Zyxel Device.

11.3.1 Add or Edit DNS Route

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **DNS Route** screen, use this screen to configure the required information for a DNS route.

Figure 161 Network Setting > Routing > DNS Route > Add New DNS Route

The following table describes the labels in this screen.

Table 90 Network Setting > Routing > DNS Route > Add New DNS Route

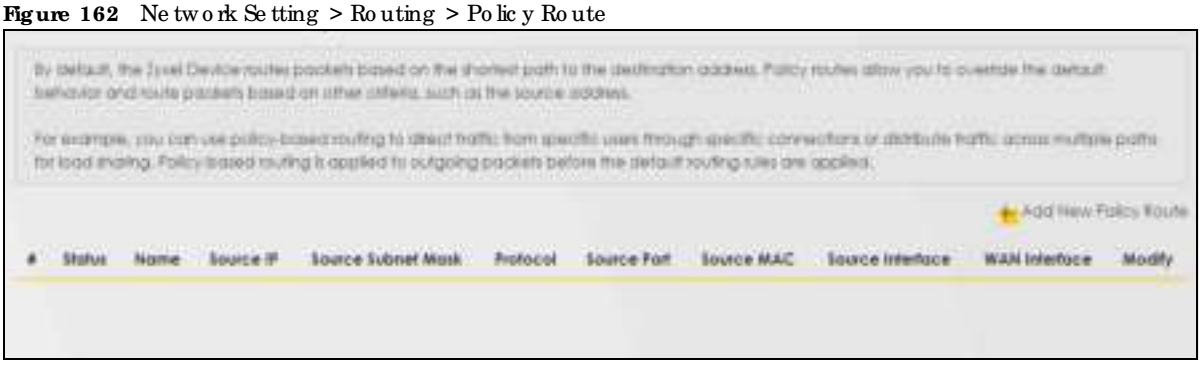
LABEL	DESCRIPTION
Active	Enable DNS route in your Zyxel Device.
Domain Name	Enter the domain name you want to resolve. You can use up to 64 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Zyxel Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
Subnet Mask	Enter the subnet mask of the network for which to use the DNS route in dotted decimal notation, for example 255.255.255.255.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interfaces already configured in the **Broadband** screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

11.4 Policy Route

By default, the Zyxel Device routes packets based on the shortest path to the destination address. Policy routes allow you to override the default behavior and route packets based on other criteria, such as the source address. For example, you can use policy-based routing to direct traffic from specific users through specific connections or distribute traffic across multiple paths for load sharing. Policy-based routing is applied to outgoing packets before the default routing rules are applied.

The **Policy Route** screen let you view and configure routing policies on the Zyxel Device. Click **Network Setting > Routing > Policy Route** to open the following screen.

Figure 162 Network Setting > Routing > Policy Route



The following table describes the labels in this screen.

Table 91 Network Setting > Routing > Policy Route

LABEL	DESCRIPTION
Add New Policy Route	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Status	This field displays whether the DNS route is active or not. A yellow bulb signifies that this DNS route is active. A gray bulb signifies that this DNS route is not active.

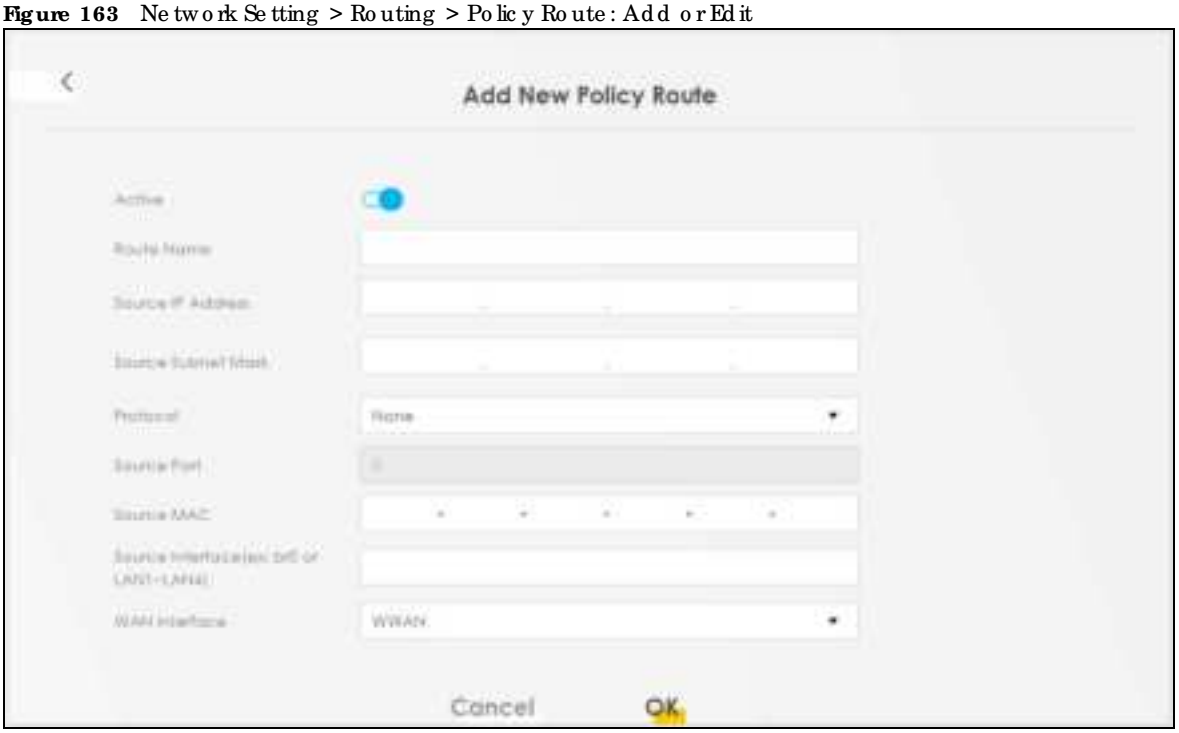
Table 91 Network Setting > Routing > Policy Route (continued)

LABEL	DESCRIPTION
Name	This is the name of the rule.
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
Source Port	This is the source port number.
Source MAC	This is the source MAC address.
Source Interface	This is the interface from which the matched traffic is sent.
WAN Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to edit this policy. Click the **Delete** icon to remove a policy from the Zyxel Device. A window displays asking you to confirm that you want to delete the policy.

11.4.1 Add or Edit Policy Route

Click **Add New Policy Route** in the **Policy Route** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 163 Network Setting > Routing > Policy Route: Add or Edit



The following table describes the labels in this screen.

Table 92 Network Setting > Routing > Policy Route: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this policy route. Otherwise, click to disable.
Route Name	Enter a descriptive name of this policy route. You can use up to 15 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP**, **UDP**, or **None**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (example: br0 or LAN1 – LAN4)	Enter the name of the interface from which the matched traffic is sent.
WAN Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interfaces already configured in the **Broadband** screens.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

11.5 RIP Overview

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows the ZyxelDevice to exchange routing information with other routers. To activate RIP for the WAN interface, select the supported RIP version and operation.

11.5.1 RIP

Click **Network Setting** > **Routing** > **RIP** to open the **RIP** screen. Select the desired RIP version and operation by clicking the checkbox. To stop RIP on the WAN interface, clear the checkbox. Click the **Apply** button to start or stop RIP and save the configuration.

Figure 164 Network Setting > Routing > RIP

The following table describes the labels in this screen.

Table 93 Network Setting > Routing > RIP

LABEL	DESCRIPTION
#	This is the index of the interface in which the RIP setting is used.
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Zyxel Device sends (it recognizes both formats when receiving). **RIPv1** is universally supported but **RIPv2** carries more information. **RIPv1** is probably adequate for most networks, unless you have an unusual network topology. When set to **Both**, the Zyxel Device will broadcast its routing table periodically and incorporate the RIP information that it receives
Operation	Select **Passive** to have the Zyxel Device update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the Zyxel Device advertise its route information and also listen for routing updates from neighboring routers.
Enable	Select the checkbox to activate the settings.
Disable Default Gateway	Select the checkbox to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 12
Quality of Service (QoS)

12.1 QoS Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

Configure QoS on the Zyxel Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1 Configure classifiers to sort traffic into different flows.

2 Assign priority and define actions to be performed for a classified traffic flow.

The Zyxel Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video. There are eight priority levels, with 1 having the highest priority.

This chapter contains information about configuring QoS and editing classifiers.

12.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 12.3 on page 325).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 12.9 on page 340).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers (Section 12.5 on page 329).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface (Section 12.6 on page 334).
- The **Policer Setup** screen lets you control incoming traffic transmission rate and bursts (Section 12.7 on page 336).
- The **Monitor** screen lets you use any available port to access any available service from a remote WAN device (Section 12.8 on page 339).

12.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus CoS

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

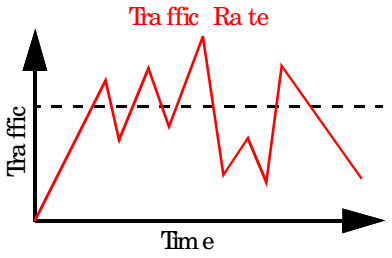
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of 3 bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

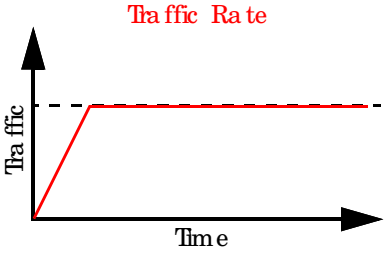
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your Zyxel Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



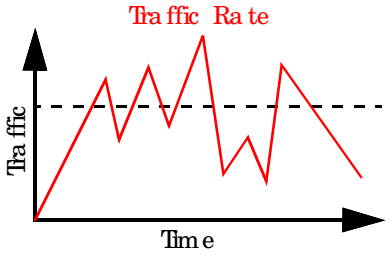
(Before Traffic Shaping)



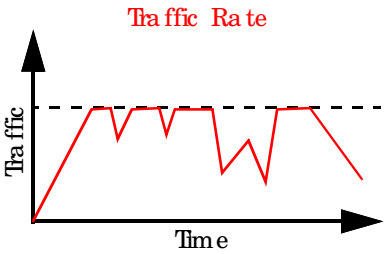
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

The Zyxel Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 12.9 on page 340 for more information on each metering algorithm.

Strictly Priority

Strictly Priority (SP) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

Weighted Round Robin Schedule (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

12.3 Quality of Service General Settings

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See Section 12.1 on page 323 for more information.

When one of the following situations happens, the current WAN linkup rate will be used instead:

1. **WAN Managed Upstream Bandwidth** is set to 0
2. **WAN Managed Upstream Bandwidth** is empty
3. **WAN Managed Upstream Bandwidth** is higher than the current WAN interface linkup rate

Note: Manually defined QoS is ignored when **Upstream Traffic Priority** is selected.

Note: **Upstream Traffic Priority** automatically assigns a traffic priority level based on the selected criteria.

Note: To have your QoS settings configured in other **QoS** screens take effect, select **None** in the **Upstream Traffic Priority Assigned by** field.

Click **Network Setting > QoS > General** to open the screen as shown next.

Figure 165 Network > QoS > General

The following table describes the labels in this screen.

Table 94 Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Click this switch to enable QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can also set this number lower than the interfaces' actual transmission speed. This will cause the Zyxel Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the Zyxel Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.
Upstream Traffic Priority Assigned by	Select how the Zyxel Device assigns priorities to various upstream traffic flows. • **None:** Disables auto priority mapping and has the Zyxel Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • **Ethernet Priority:** Automatically assign priority based on the IEEE 802.1p priority level. • **IP Precedence:** Automatically assign priority based on the first three bits of the TOS field in the IP header. • **Packet Length:** Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, Internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

12.4 Queue Setup

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment to decide the priority on WAN or LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

Note: Configure the priority level for a QoS queue from 1 to 8. The smaller the number in the **Priority** column, the higher the priority.

Note: The corresponding classifiers will be removed automatically if a queue is deleted.

Note: Rate limit 0 means there is no rate limit on a queue.

Figure 166 Network Setting > QoS > Queue Setup

The following table describes the labels in this screen.

Table 95 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Queue Setting	Select between **SP** (Strict Priority), **SP+WRR**, or **WRR** (Weighted Round Robin). **SP** scheduling singles out the highest priority queue and ensures all queued traffic in this queue is transmitted before servicing the lower priority queues. WRR scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field. Queues with larger weights get more service than queues with smaller weights. If you choose **SP+WRR**, the first and second queue will be **SP**, and the third and fourth queue will be **WRR**.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this queue passes.

Table 95 Network Setting > QoS > Queue Setup (continued)

LABEL	DESCRIPTION
Discipline	This shows the discipline of the queue. The discipline is changed according to the option chosen in **Queue Setting**. If you choose **SP**, the discipline will be SP. If you choose **SP+WRR**, the discipline of the first and second queue will be SP, and the third and fourth queue will be WRR. If you choose **WRR**, the discipline will be WRR. Strict Priority scheduling services the remaining queues using WRR. WRR scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights. Note: Queue weights can only be changed when Weighted Round Robin is selected.
Priority	This shows the priority of this queue. The lower the number, the higher the priority level.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Zyxel Device should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

12.4.1 Add a QoS Queue

Click **Add New Queue** or the **Edit** icon in the **Queue Setup** screen to configure a queue.

Figure 167 Network Setting > QoS > Queue Setup > Add New Queue/Edit

The following table describes the labels in this screen.

Table 96 Network Setting > QoS > Queue Setup > Add New Queue/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable the queue.
Name	Enter a descriptive name for this queue. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 8) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Zyxel Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the Zyxel Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue. If you enter 0 here, this means there's no rate limit on this queue.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

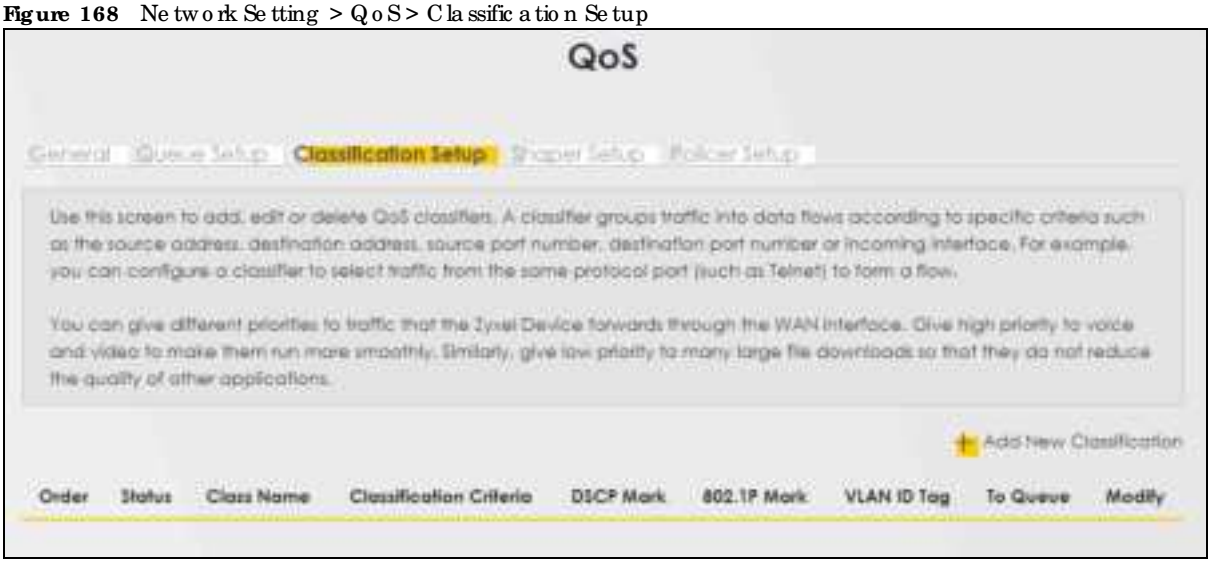
12.5 QoS Classification Setup

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Zyxel Device forwards through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Classification Setup** to open the following screen.

Figure 168 Network Setting > QoS > Classification Setup



The following table describes the labels in this screen.

Table 97 Network Setting > QoS > Classification Setup

LABEL	DESCRIPTION
Add New Classification	Click this to create a new classifier.
Order	This is the index number of the entry. The classifiers are applied in order of their numbering.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

12.5.1 Add or Edit QoS Class

Click **Add New Classification** in the **Classification Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 169 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step 1

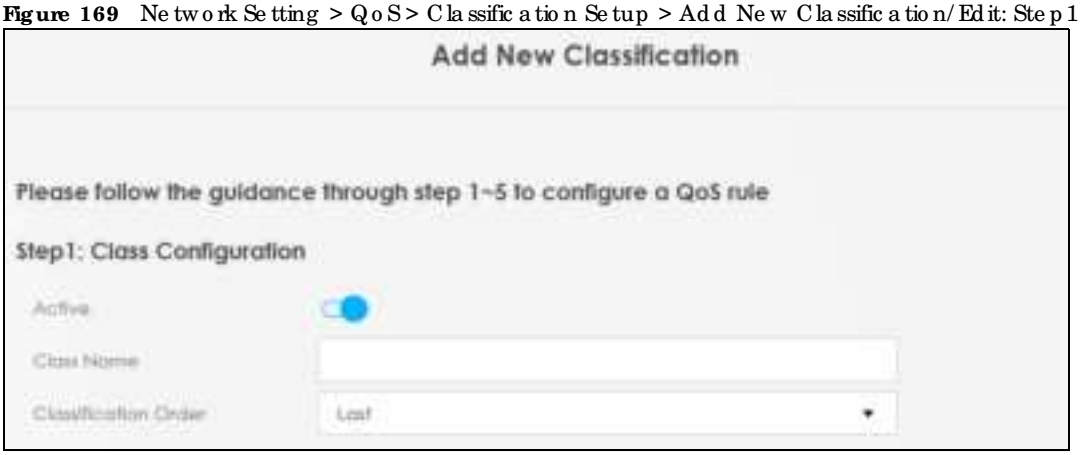


Figure 170 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step 2

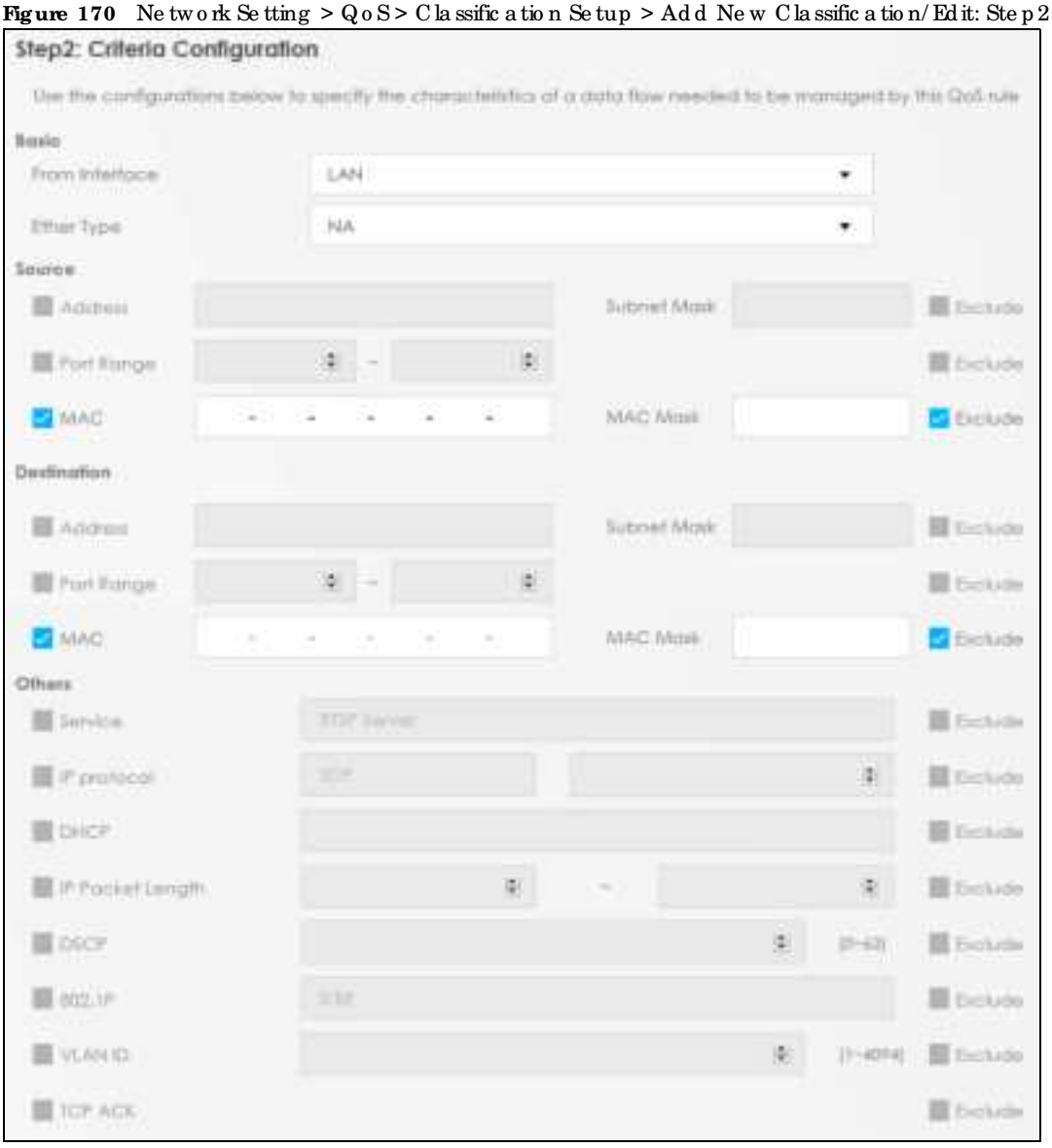


Figure 171 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step 3

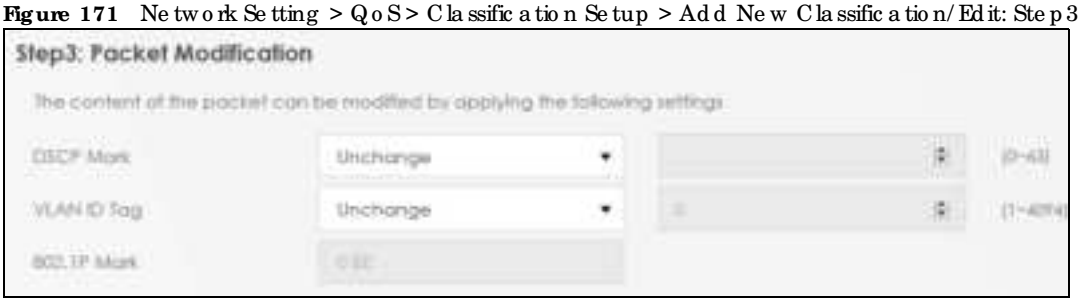


Figure 172 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step 4

Figure 173 Network Setting > QoS > Classification Setup > Add New Classification/Edit: Step 5

The following table describes the labels in this screen.

Table 98 Network Setting > QoS > Classification Setup > Add New Classification/Edit

LABEL	DESCRIPTION
Step 1: Class Configuration	
Active	Click this switch to enable the classifier.
Class Name	Enter a descriptive name for this class. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Step 2: Criteria Configuration	
Basic	
Source	
Address	Select the checkbox and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the checkbox and enter the port numbers of the source.
MAC	Select the checkbox and enter the source MAC address of the packet.
MAC Mask	Enter the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.

Table 98 Network Setting > QoS > Classification Setup > Add New Classification/Edit (continued)

LABEL	DESCRIPTION
Destination	
Address	Select the checkbox and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the checkbox and enter the port numbers of the source.
MAC	Select the checkbox and enter the source MAC address of the packet.
MAC Mask	Enter the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **Client ID (DHCP Option 61)**, enter the Identity Association IDentifier (IAD Option 61) of the matched traffic, such as the MAC address of the device. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets. If you select **Vendor Specific Info (DHCP Option 125)**, enter the vendor specific information of the matched traffic, such as the product class, model name, and serial number of the device.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Step 3: Packet Modification	
DSCP Mark	This field is available only when you select **IP** in the **Ether Type** field. If you select **Remark**, enter a DSCP value with which the Zyxel Device replaces the DSCP field in the packets. If you select **Unchange**, the Zyxel Device keep the DSCP field in the packets.

Table 98 Network Setting > QoS > Classification Setup > Add New Classification/Edit (continued)

LABEL	DESCRIPTION
VLAN ID Tag	If you select **Remark**, enter a VLAN ID number with which the Zyxel Device replaces the VLAN ID of the frames. If you select **Remove**, the Zyxel Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the Zyxel Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the Zyxel Device keep the VLAN ID in the packets.
802.1P Mark	Select a priority level with which the Zyxel Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the Zyxel Device keep the 802.1p priority field in the packets.
Step 4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the Zyxel Device forward traffic of this class according to the default routing table.
Step 5: Outgoing Queue Selection	
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

12.6 QoS Shaper Setup

This screen lets you use the token bucket algorithm to allow a certain amount of large bursts of traffic while keeping most outgoing traffic at the average rate. Click **Network Setting > QoS > Shaper Setup**. The screen appears as shown.

Figure 174 Network Setting > QoS > Shaper Setup

The following table describes the labels in this screen.

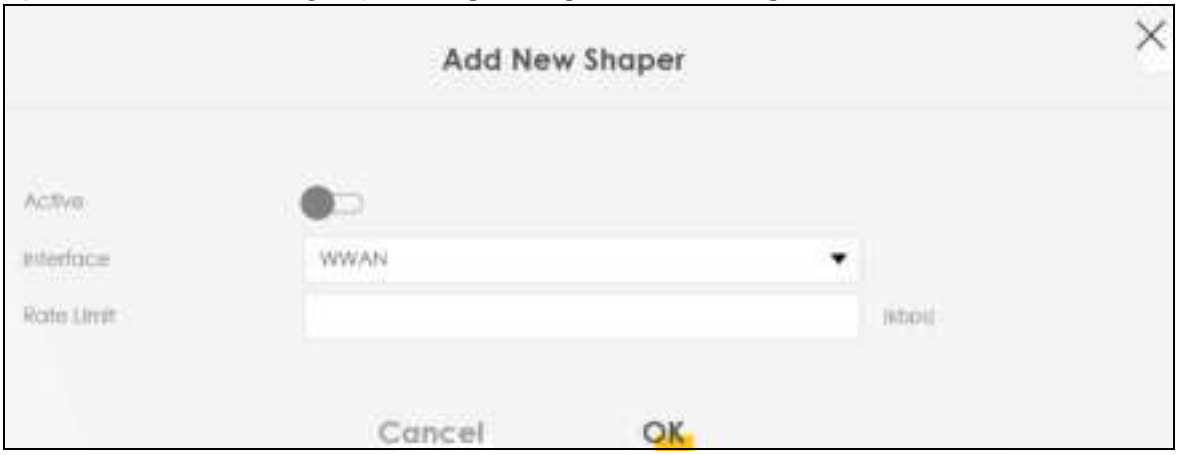
Table 99 Network Setting > QoS > Shaper Setup

LABEL	DESCRIPTION
Add New Shaper	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the shaper is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this shaper is not active.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	This shows the average rate limit of traffic bursts for this shaper.
Modify	Click the **Edit** icon to edit the shaper. Click the **Delete** icon to delete an existing shaper. Note that subsequent rules move up by one when you take this action.

12.6.1 Add or Edit a QoS Shaper

Click **Add New Shaper** in the **Shaper Setup** screen or the **Edit** icon next to a shaper to show the following screen.

Figure 175 Network Setting > QoS > Shaper Setup > Add New Shaper/Edit



The following table describes the labels in this screen.

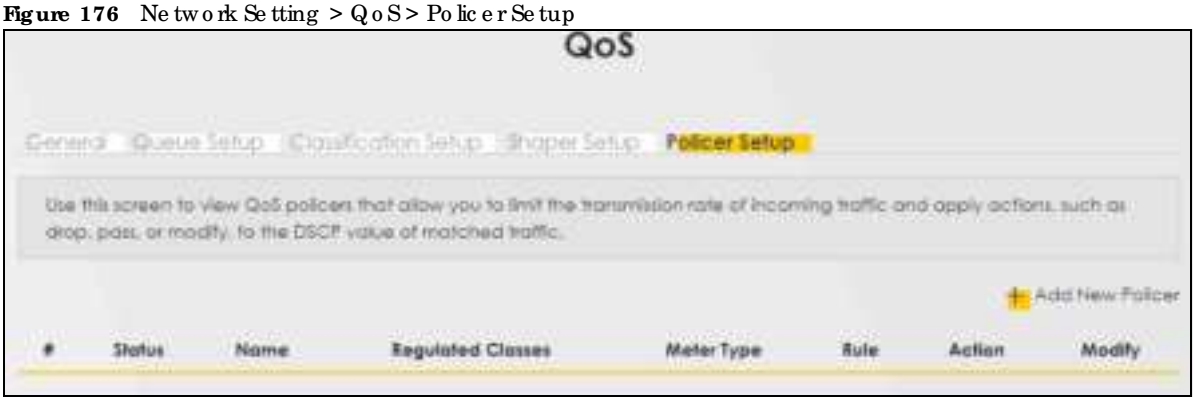
Table 100 Network Setting > QoS > Shaper Setup > Add New Shaper/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable the shaper.
Interface	Select a Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

12.7 QoS Policer Setup

Use this screen to view QoS policers that allow you to limit the transmission rate of incoming traffic and apply actions, such as drop, pass, or modify, to the DSCP value of matched traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

Figure 176 Network Setting > QoS > Policer Setup



The following table describes the labels in this screen.

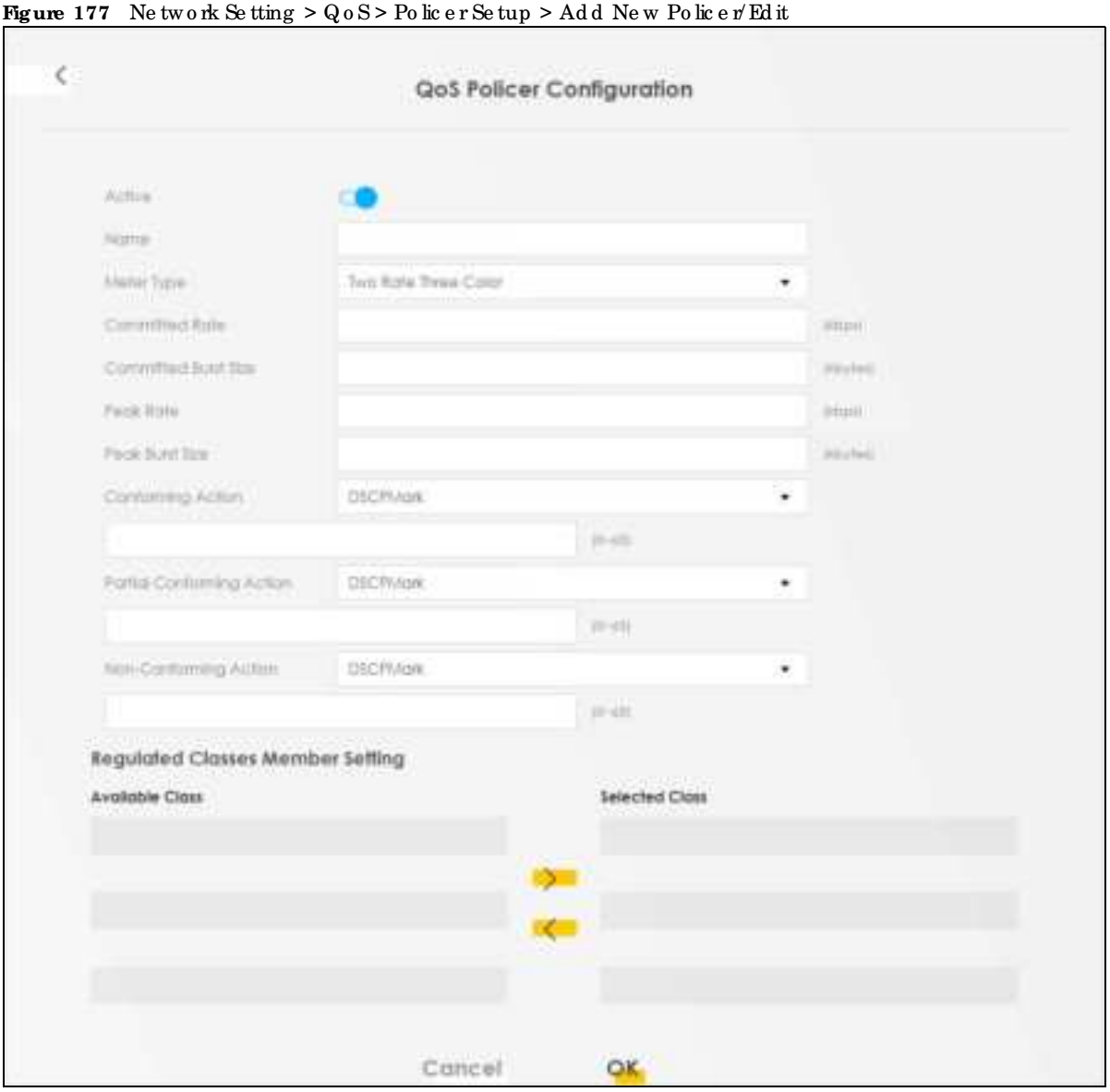
Table 101 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add New Policer	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows how the policer has the Zyxel Device treat different types of traffic belonging to the policer's member QoS classes.
Modify	Click the **Edit** icon to edit the policer. Click the **Delete** icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

12.7.1 Add or Edit a QoS Policer

Click **Add New Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 177 Network Setting > QoS > Policer Setup > Add New Policer/Edit



The following table describes the labels in this screen.

Table 102 Network Setting > QoS > Policer Setup > Add New Policer/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable the policer.
Name	Enter a descriptive name for this policer. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.

Table 102 Network Setting > QoS > Policer Setup > Add New Policer/Edit (continued)

LABEL	DESCRIPTION
Meter Type	This shows the traffic metering algorithm used in this policer. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size. The **Single Rate Three Color** Marker (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The **Two Rate Three Color** Marker (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Excess Burst Size	Specify the additional amount of bytes that are admitted at the committed rate besides the committed burst size. This is the maximum size of the second token bucket in the srTCM. This field is only available when you select **Single Rate Three Color** in the **Meter Type** field.
Peak Rate	Specify the maximum rate at which packets are admitted to the network. The peak rate should be greater than or equal to the committed rate. This is to specify how many bytes of tokens are added to the second bucket every second in the trTCM. This field is only available when you select **Two Rate Three Color** in the **Meter Type** field.
Peak Burst Size	Specify the maximum amount of bytes that are admitted at the committed rate. This is the maximum size of the second token bucket in the trTCM. This field is only available when you select **Two Rate Three Color** in the **Meter Type** field.
Conforming Action	Specify what the Zyxel Device does for packets within the committed rate and burst size (green-marked packets). • **Pass:** Send the packets without modification. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Partial Conforming Action	Specify the action that the Zyxel Device takes on yellow-marked packets. Select **Pass** to forward the packets. Select **Drop** to discard the packets. Select **DSCP Mark** to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network. This field is only available when you select **Single/Two Rate Three Color** in the **Meter Type** field.
Non-Conforming Action	Specify what the Zyxel Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). • **Drop:** Discard the packets. • **DSCP Mark:** Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Regulated Classes Member Setting	

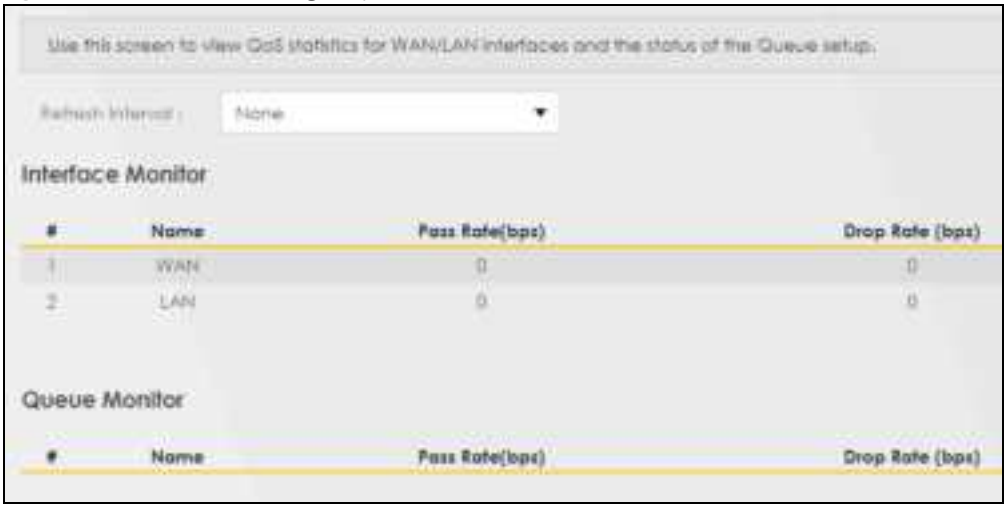
Table 102 Network Setting > QoS > Policer Setup > Add New Policer/Edit (continued)

LABEL	DESCRIPTION
Available Class Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

12.8 QoS Monitor

To view the Zyxel Device's QoS packet statistics, click **Network Setting** > **QoS** > **Monitor**. The screen appears as shown.

Figure 178 Network Setting > QoS > Monitor



The following table describes the labels in this screen.

Table 103 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen. Select **None** to stop refreshing
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the interface on the Zyxel Device.
Pass Rate (bps)	This shows how many packets forwarded to this interface are transmitted successfully.
Drop Rate (bps)	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.

Table 103 Network Setting > QoS > Monitor (continued)

LABEL	DESCRIPTION
Pass Rate (bps)	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how many packets assigned to this queue are dropped.

12.9 Technical Reference

The following section contains additional technical information about the Zyxel Device features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 104 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	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.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) 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.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) 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.

DSCP (6 bits)	Unused (2 bits)

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 kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the Zyxel Device, the Zyxel Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the Zyxel Device. On the Zyxel Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 105 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250 – 1100
4	4	2	010110 010100 010010 010000	

Table 105 Internal Layer2 and Layer3 QoS Mapping (continued)

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Zyxel Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Zyxel Device treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The Zyxel Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the ZyxelDevice checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.

- If the PBS bucket has enough tokens, the Zyxel Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 13
Network Address Translation (NAT)

13.1 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.

13.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the servers on your local network (Section 13.2 on page 346).
- Use the **Port Triggering** screen to add and configure the ZyxelDevice's trigger port settings (Section 13.3 on page 349).
- Use the **DMZ** screen to configure a default server (Section 13.4 on page 353).
- Use the **ALG** screen to enable or disable the SIP ALG (Section 13.5 on page 353).
- Use the **Address Mapping** screen to enable and disable the NAT Address Mapping in the ZyxelDevice (Section 13.6 on page 355).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section 13.7 on page 357).
- Use the **Port Control Protocol** screen to configure incoming traffic for devices behind the ZyxelDevice (Section 13.8 on page 357).

13.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the ZyxelDevice, 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.

NAT

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.

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.

13.2 Port Forwarding

Use **Port Forwarding** to forward incoming service requests from the Internet to the servers on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

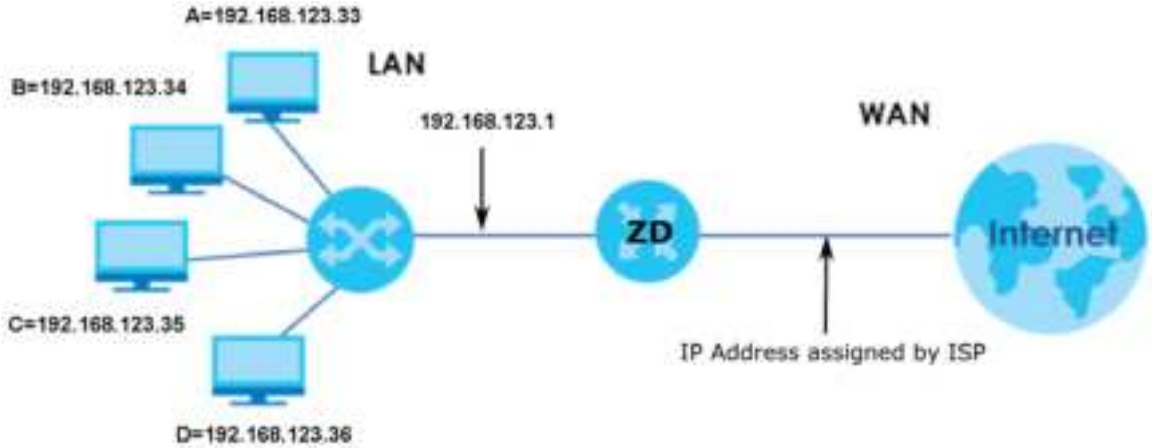
You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more 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. Please refer to RFC 1700 for further information about port numbers.

Note: 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.

Configure 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), a default server IP address of 192.168.1.35 to a third (**C** in the example), and a default server IP address of 192.168.1.36 to a fourth (**D** 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 179 Multiple Servers Behind NAT Example

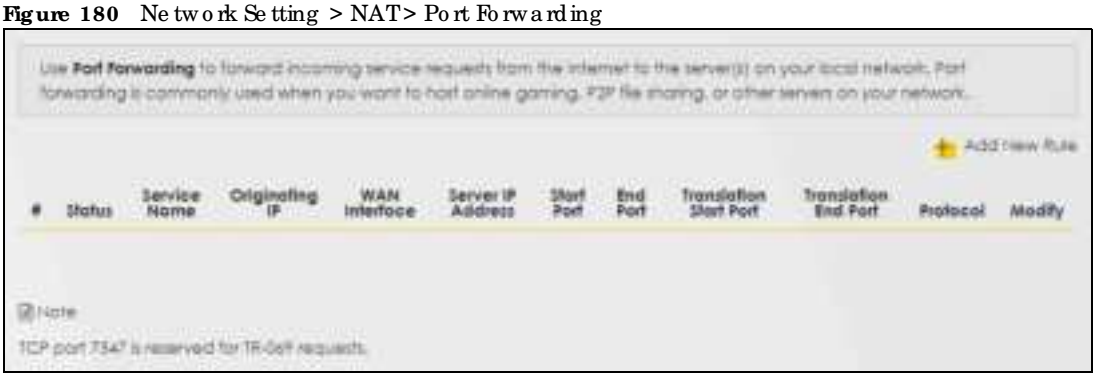


13.2.1 Port Forwarding

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

Note: TCP port 7547 is reserved for system use.

Figure 180 Network Setting > NAT> Port Forwarding



The following table describes the fields in this screen.

Table 106 Network Setting > NAT> Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
Originating IP	This is the source's IP address.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This field displays the protocol (TCP, UDP, TCP+UDP) used to transport the packets for which you want to apply the rule.
Modify	Click the **Edit** icon to edit the port forwarding rule. Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

13.2.2 Add or Edit Port Forwarding

Create or edit a port forwarding rule. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule. Click **Add New Rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 181 Network Setting > NAT> Port Forwarding: Add or Edit

Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.
Here is an example to configure port translation. Configure **Start Port** to 100, **End Port** to 120, **Translation Start Port** to 200, and **Translation End Port** to 220.

Note: TCP port 7547 is reserved for system use.

The following table describes the labels in this screen.

Table 107 Network Setting > NAT> Port Forwarding: Add or Edit

LABEL	DESCRIPTION
Active	Click to turn the port forwarding rule on or off.
Service Name	Enter a name for the service to forward. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.

Table 107 Network Setting > NAT> Port Forwarding: Add or Edit (continued)

LABEL	DESCRIPTION
Start Port	Configure this for a user-defined entry. Enter the original destination port for the packets. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Configure this for a user-defined entry. Enter the last port of the original destination port range. To forward only one port, enter the port number in the **Start Port** field above and then enter it again in this field. 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.
Translation Start Port	Configure this for a user-defined entry. This shows the port number to which you want the Zyxel Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	Configure this for a user-defined entry. This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Configure Originating IP	Click the **Enable** checkbox to enter the source IP in the next field.
Originating IP	Enter the source IP address here.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

13.3 Port Triggering

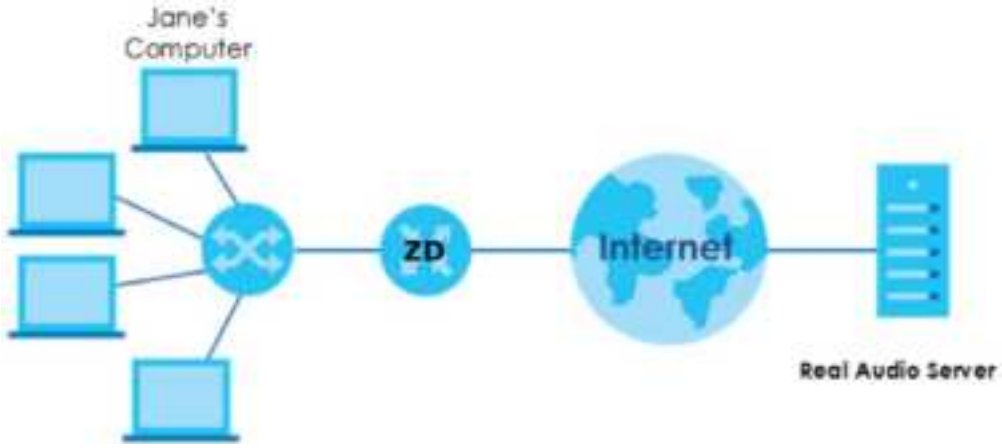
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding allows computers on the LAN to dynamically take turns using the service.

The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a \"trigger\" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol (\"open\" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 182 Trigger Port Forwarding Process: Example



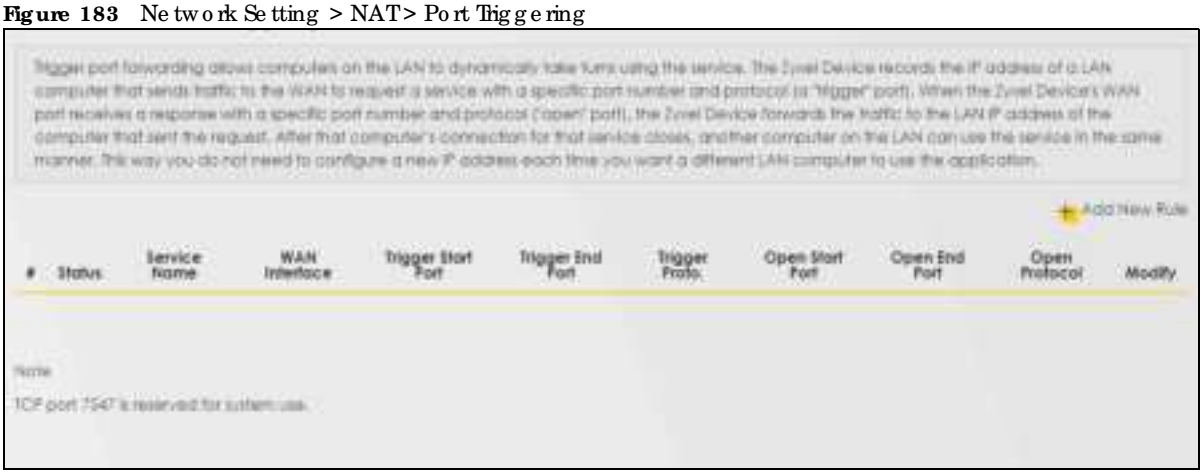
1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970 – 7170.
3. The Real Audio server responds using a port number ranging between 6970 – 7170.
4. The Zyxel Device forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in 3 minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT> Port Triggering** to open the following screen. Use this screen to view your Zyxel Device's trigger port settings.

Note: TCP port 7547 is reserved for system use.

Note: The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.

Figure 183 Network Setting > NAT> Port Triggering



The following table describes the labels in this screen.

Table 108 Network Setting > NAT> Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Protocol	This is the open transport layer protocol.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

13.3.1 Add or Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add New Rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen. Use this screen to configure a port or range of ports and protocols for sending out requests and for receiving responses.

Figure 184 Network Setting > NAT> Port Triggering: Add or Edit

The following table describes the labels in this screen.

Table 109 Network Setting > NAT> Port Triggering: Add or Edit

LABEL	DESCRIPTION
Active	Click this switch to activate this rule.
Service Name	Enter a name to identify this rule. You can use up to 256 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter a port number or the starting port number in a range of port numbers.
Trigger End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Enter a port number or the starting port number in a range of port numbers.
Open End Port	Enter a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

13.4 DMZ

Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Triggering** screen. The DMZ (De Militarized Zone) is a network between the WAN and the LAN that is accessible to devices on both the WAN and LAN with firewall protection. Devices on the WAN can initiate connections to devices on the DMZ but not to those on the LAN.

You can put public servers, such as email, web, and FTP servers, on the DMZ to provide services on both the WAN and LAN. To use this feature, you first need to assign a DMZ host. Click **Network Setting > NAT> DMZ** to open the **DMZ** screen.

Note: Use an IPv4 address for the DMZ server.

Note: Enter the IP address of the default server in the **Default Server Address** field, and click **Apply** to activate the DMZ host. Otherwise, clear the IP address in the **Default Server Address** field, and click **Apply** to deactivate the DMZ host.

Figure 185 Network Setting > NAT> DMZ

The following table describes the fields in this screen.

Table 110 Network Setting > NAT> DMZ

LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **Port Forwarding** screen. Note: If you do not assign a default server, the Zyxel Device discards all packets received for ports not specified in the virtual server configuration.
Apply	Click this to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

13.5 ALG

Application Layer Gateway (ALG) allows customized NAT traversal filters to support address and port translation for certain applications such as File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications. It allows SIP calls to pass through the Zyxel Device.

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.

Click **Network Setting > NAT> ALG** to open the **ALG** screen. Use this screen to enable and disable the NAT Application Layer Gateway (ALG) in the Zyxel Device.

Application Layer Gateway (ALG) allows certain applications such as File Transfer Protocol (FTP), Session Initiation Protocol (SIP), or file transfer in Instant Messaging (IM) applications to pass through the Zyxel Device.

Figure 186 Network Setting > NAT> ALG

The following table describes the fields in this screen.

Table 111 Network Setting > NAT> ALG

LABEL	DESCRIPTION
NAT ALG	Enable this to make sure applications such as FTP and file transfer in IM applications work correctly with port-forwarding and address-mapping rules.
SIP ALG	Click this switch to enable SIP ALG to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
RTSP ALG	Click this switch to enable RTSP ALG to have the Zyxel Device detect RTSP traffic and help build RTSP sessions through its NAT. The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
PPTP ALG	Click this switch to enable the PPTP ALG on the Zyxel Device to detect PPTP traffic and help build PPTP sessions through the Zyxel Device's NAT.
IPSEC ALG	Click this switch to enable IPsec ALG on the Zyxel Device to detect IPsec traffic and help build IPsec sessions through the Zyxel Device's NAT.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

13.6 Address Mapping

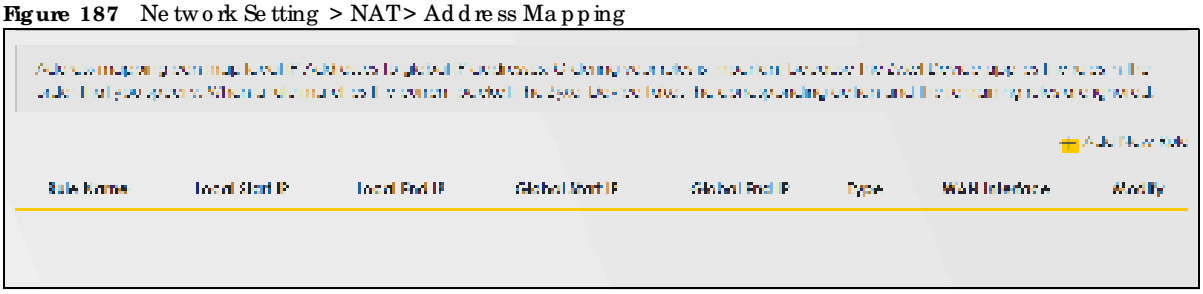
Address mapping can map local IP Addresses to global IP addresses. Ordering your rules is important because the Zyxel Device applies the rules in the order that you specify. When a rule matches the current packet, the Zyxel Device takes the corresponding action and the remaining rules are ignored.

Use this screen to enable or disable the NAT Address Mapping in the Zyxel Device.

13.6.1 Address Mapping Screen

Click **Network Setting** > **NAT**> **Address Mapping** to open the **Address Mapping** screen.

Figure 187 Network Setting > NAT> Address Mapping



The following table describes the fields in this screen.

Table 112 Network Setting > NAT> Address Mapping

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
Rule Name	This is the name of the rule.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the ending 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 blank for **One-to-One** 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 the **Many-to-One** mapping type.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
Type	This is the address mapping type. **One-to-One**: This 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. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), the Device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
WAN Interface	This is the WAN interface to which the address mapping rule applies.
Modify	Click the **Edit** icon to go to the screen where you can edit the address mapping rule. 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.

13.6.2 Add New Rule Screen

To add or edit an address mapping rule, click **Add New Rule** or the **Modify** icon in the **Address Mapping** screen to display the screen shown next.

Figure 188 Network Setting > NAT> Address Mapping > Add New Rule

The following table describes the fields in this screen.

Table 113 Network Setting > NAT> Address Mapping > Add New Rule

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name for this rule. You can use up to 20 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Type	Choose the IP or port mapping type from one of the following. **One-to-One**: This 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. **Many-to-One**: This mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the device's Single User Account feature that previous routers supported only. **Many-to-Many**: This mode maps multiple local IP addresses to shared global IP addresses.
Local Start IP	Enter the starting Inside Local IP Address (ILA).
Local End IP	Enter the ending 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 blank for **One-to-One** mapping types.
Global Start IP	Enter 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 the Many-to-One mapping type.
Global End IP	Enter the ending Inside Global IP Address (IGA). This field is blank for **One-to-One** and **Many-to-One** mapping types.
WAN Interface	Select a WAN interface to which the address mapping rule applies.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

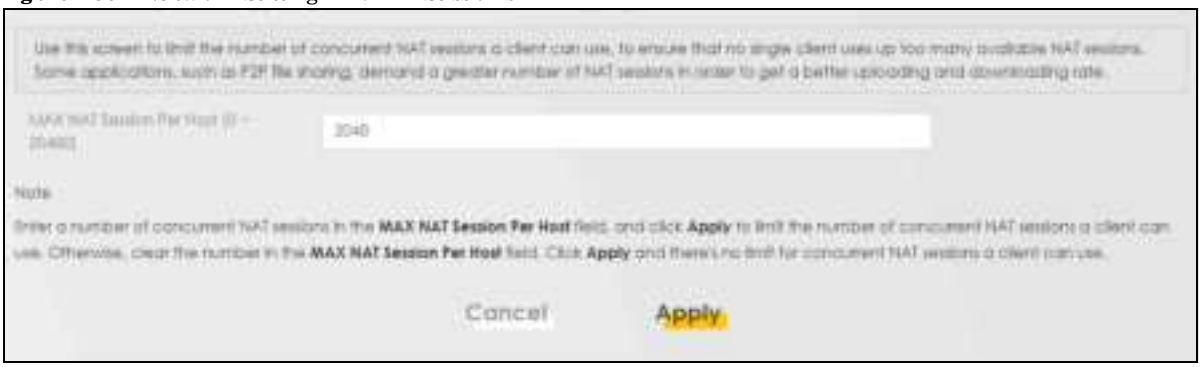
13.7 Sessions

Use this screen to limit the number of concurrent NAT sessions a client can use, to ensure that no single client uses up too many available NAT sessions. Some applications, such as P2P file sharing, demand a greater number of NAT sessions in order to get a better uploading and downloading rate. Click **Network Setting > NAT> Sessions** to display the following screen.

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use. Click **Network Setting > NAT> Sessions** to open the **Sessions** screen.

Note: Enter a number of concurrent NAT sessions in the **MAX NAT Session Per Host** field, and click **Apply** to limit the number of concurrent NAT sessions a client can use. Otherwise, clear the number in the **MAX NAT Session Per Host** field. Click **Apply** and there is no limit for concurrent NAT sessions a client can use.

Figure 189 Network Setting > NAT> Sessions



The following table describes the fields in this screen.

Table 114 Network Setting > NAT> Sessions

LABEL	DESCRIPTION
MAX NAT Session Per Host	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

13.8 Port Control Protocol (PCP)

Use this screen to view, add, or delete PCP rules. Port Control Protocol (PCP) allows devices such as web or file sharing servers behind the Zyxel Device to receive incoming traffic.

Example Applications

- Some remote access applications, such as remote desktop or SSH, require incoming traffic to be routed to the user's device in order to establish a remote connection. Use PCP to dynamically map incoming traffic to the user's device, allowing them to establish remote connections.

The PCP server allows dynamic mapping of external ports to internal IP addresses and ports. PCP allows devices to request and release mappings for specific ports, and to specify the lifetime of those mappings. This allows devices to dynamically open and close ports just as needed, and does not need keepalive packets that can drain battery life of home devices such as smartphones.

In the following figure, the Zyxel Device is the PCP client. DS-Lite tunnels IPv4 packets over an IPv6 network to an AFTR (Address Family Transition Router) and Carrier-Grade NAT (CGNAT) which includes the PCP server, then sends traffic to its external IPv4 network. The Port Control Protocol with DS Lite allows you to create PCP mapping rules with the PCP server.

Requirement

You must enable DS Lite (Dual-Stack Lite) in **Network Setting > Broadband > Edit WAN Interface** to use PCP.

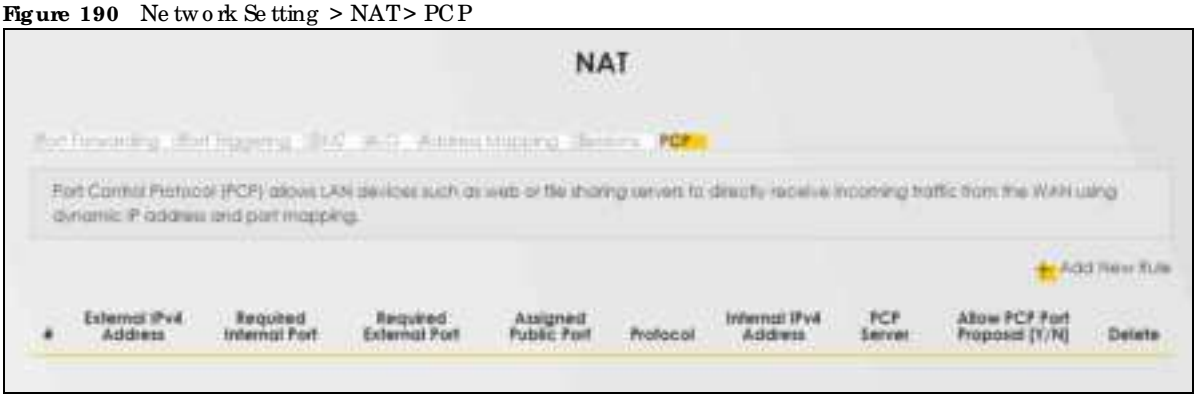
- If you select **Automatically configured by DHCPC**, then the IP address of the PCP server is in assigned to the Zyxel Device using DCHP Option 64.

- If you select **Manually Configured**, then you must enter the IPv6 address of the PCP server in the **DS-Lite Relay server IP** field.

Configuring PCP

Click **Network Setting > NAT> PCP** to display the following screen.

Figure 190 Network Setting > NAT> PCP



The following table describes the fields in this screen.

Table 115 Network Setting > NAT> PCP

LABEL	DESCRIPTION
Add New Rule	Click this to add a new PCP rule.
#	This is the index number of the rule.
External IPv4 Address	This displays the external IP address assigned by the PCP server. PCP maps from this IP address to the LAN device IP address.
Required Internal Port	This displays the internal port number that the PCP server maps to, from the external port.
Required External Port	This displays the proposed external port number that the PCP server maps from, to the internal port.
Assigned Public Port	This displays the allocated external port number assigned by the PCP server for the service on the WAN if Allow PCP Port Proposal is enabled. PCP maps from this port number to the internal port number.
Protocol	This is the protocol (**TCP** or **UDP**) for port number that identifies a service.
Internal IPv4 Address	This is the LAN device IP address. PCP maps the external IP address to this IP address.
PCP Server	This field displays the status of the PCP mapping request to the PCP server. • **Succeeded** - The PCP server successfully mapped the external IP address and port to the internal IP address and port. • **Failed** - The PCP server failed to map the external IP address and port to the internal IP address and port. Make sure to select Allow PCP Port Proposal to allow the PCP server to assign an external IP address and port if the configured ones are not available.
Allow PCP Port Proposal (Y/N)	This displays **Y** if the PCP server can assign a different external IP address and port to the required ones you configured.
Delete	Select a rule, then click this icon to remove the rule from the Zyxel Device.

13.8.1 Add New Rule Screen

To add a new PCP rule, click **Add New Rule**. To edit an existing rule, select the rule, then click the **Modify** icon. The following screen displays.

Note: Be careful not to configure conflicting mapping between PCP and NAT port forwarding for incoming traffic.

Figure 191 Network Setting > NAT> PCP > Add New Rule

The following table describes the fields in this screen.

Table 116 Network Setting > NAT> PCP > Add New Rule

LABEL	DESCRIPTION
Required Internal Port	Enter an internal port number that the PCP server maps to, from the external port.
Required External Port	Enter a proposed external port number that the PCP server maps from, to the internal port.
Protocol	Select the transport layer protocol. Choices are **TCP** and **UDP**. See the Service Appendix to see what services require what protocol and port number.
Internal IPv4 Address	Enter the IP address of the LAN device. PCP maps the external IP address to this IP address.
Allow PCP Port Proposal	Select this to allow the PCP server to assign an external IP address and port. If you clear this, PCP mapping will fail if the required ones configured are not available on the PCP server.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

13.9 Technical Reference

This part contains more information regarding NAT.

13.9.1 NAT Definitions

Inside or 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 or 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 or 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 117 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.

13.9.2 What NAT Does

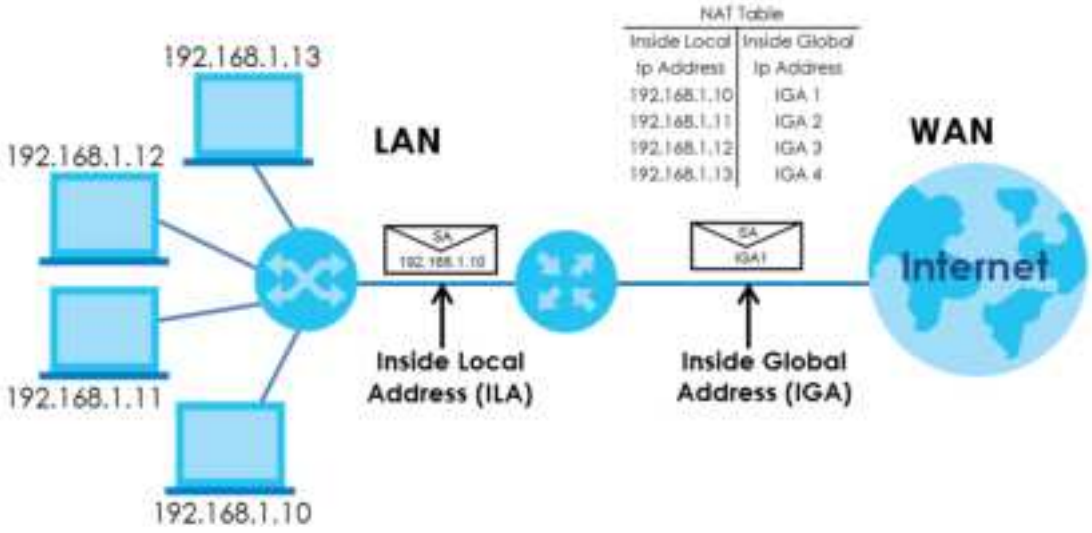
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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), 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)*.

13.9.3 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.

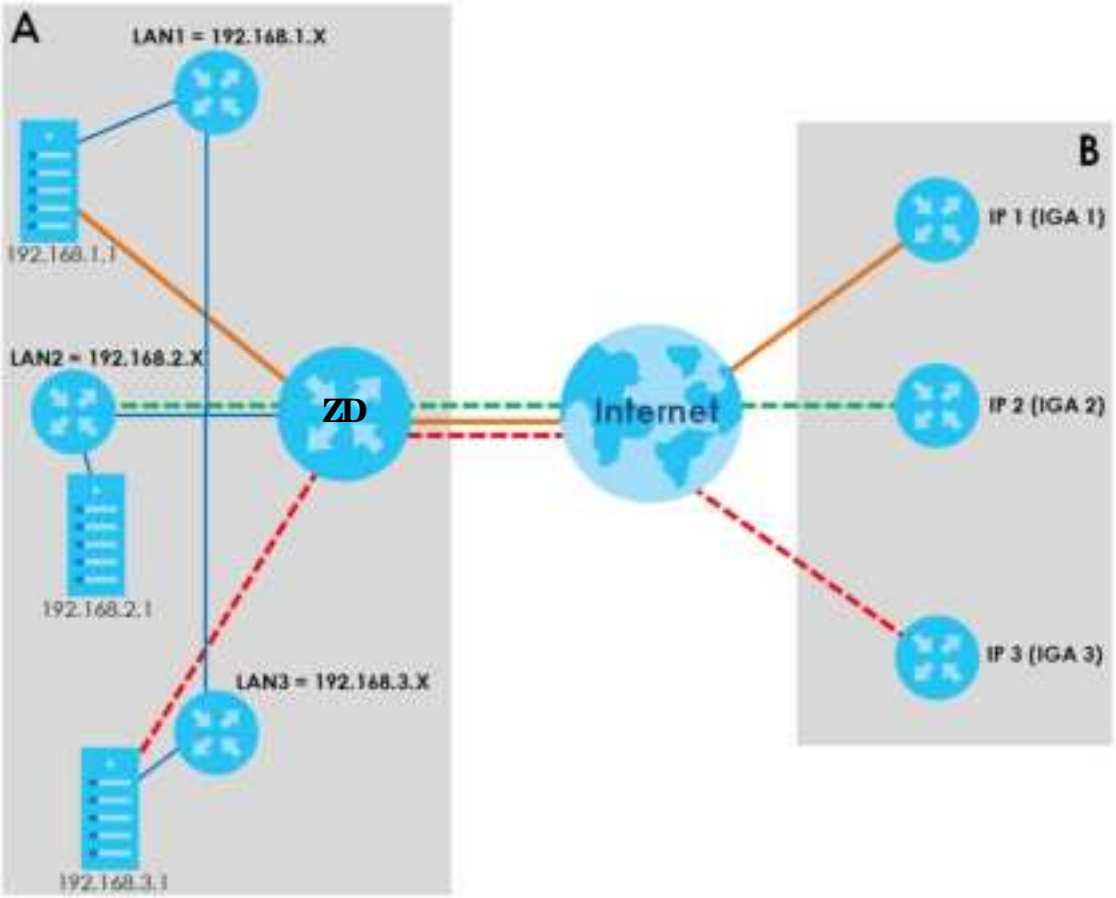
Figure 192 How NAT Works



13.9.4 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.

Figure 193 NAT Application With IP Alias



Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

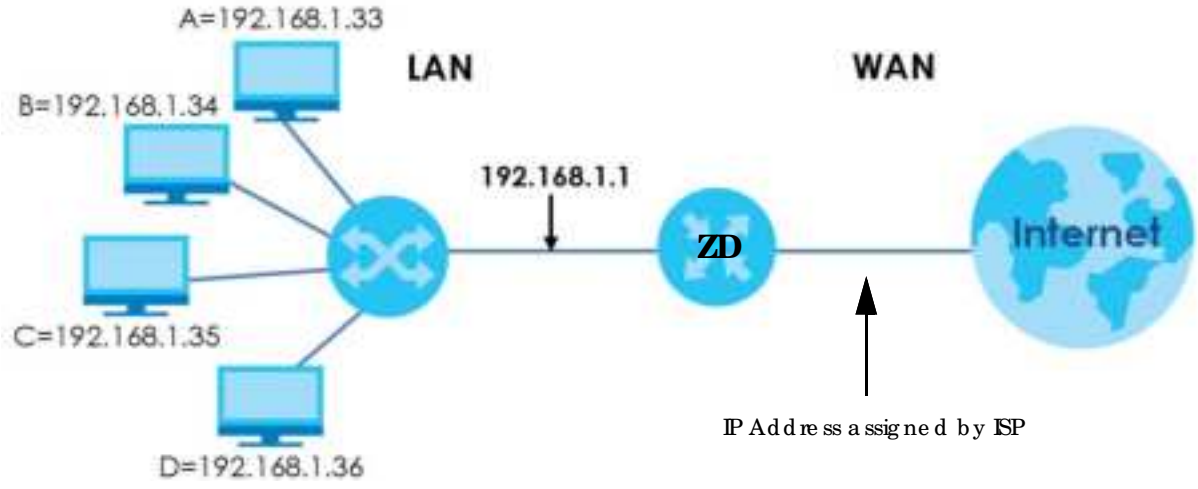
Table 118 Services and Port Numbers

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

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 194 Multiple Servers Behind NAT Example



CHAPTER 14
DNS

14.1 DNS Overview

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS servers, each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. The Zyxel Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Zyxel Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

Dynamic DNS

Dynamic DNS allows you to use a dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, and so on). 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 do not know your IP address.

You first 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 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 14.2 on page 365).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Zyxel Device (Section 14.3 on page 366).

14.1.2 What You Need To Know

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.

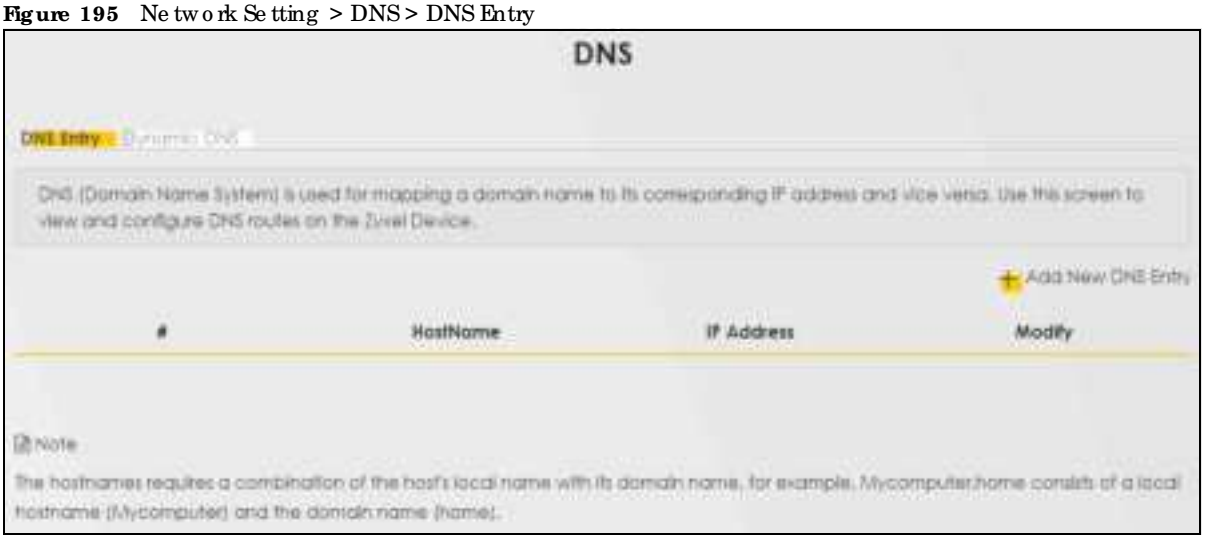
If you have a private WAN IP address, then you cannot use Dynamic DNS.

14.2 DNS Entry

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP address and vice versa. Use this screen to view and configure manual DNS entires on the Zyxel Device. Click **Network Setting** > **DNS** to open the **DNS Entry** screen.

Note: The host name should consist of the host's local name and the domain name. For example, Mycomputer.home is a host name where Mycomputer is the host's local name, and .home is the domain name.

Figure 195 Network Setting > DNS > DNS Entry



The following table describes the fields in this screen.

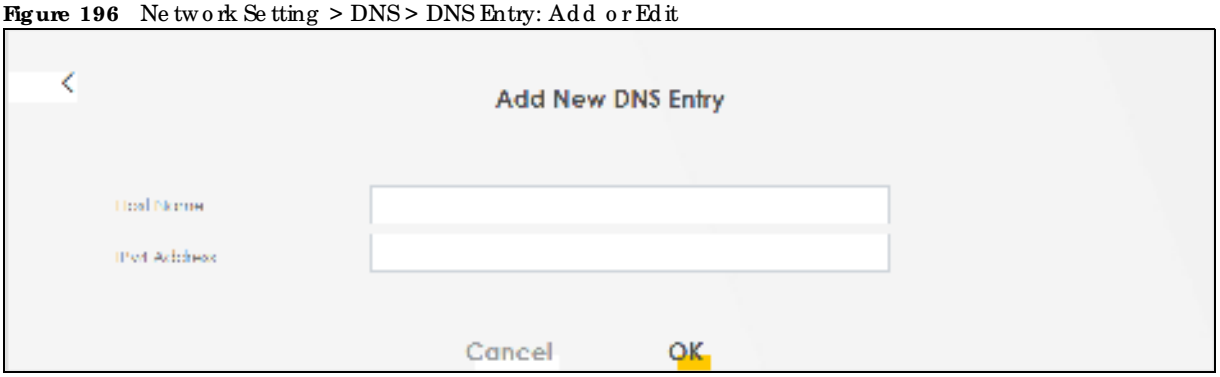
Table 119 Network Setting > DNS > DNS Entry

LABEL	DESCRIPTION
Add New DNS Entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
HostName	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule.

14.2.1 Add or Edit DNS Entry

You can manually add or edit the Zyxel Device's DNS name and IP address entry. Click **Add New DNS Entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 196 Network Setting > DNS > DNS Entry: Add or Edit



The following table describes the labels in this screen.

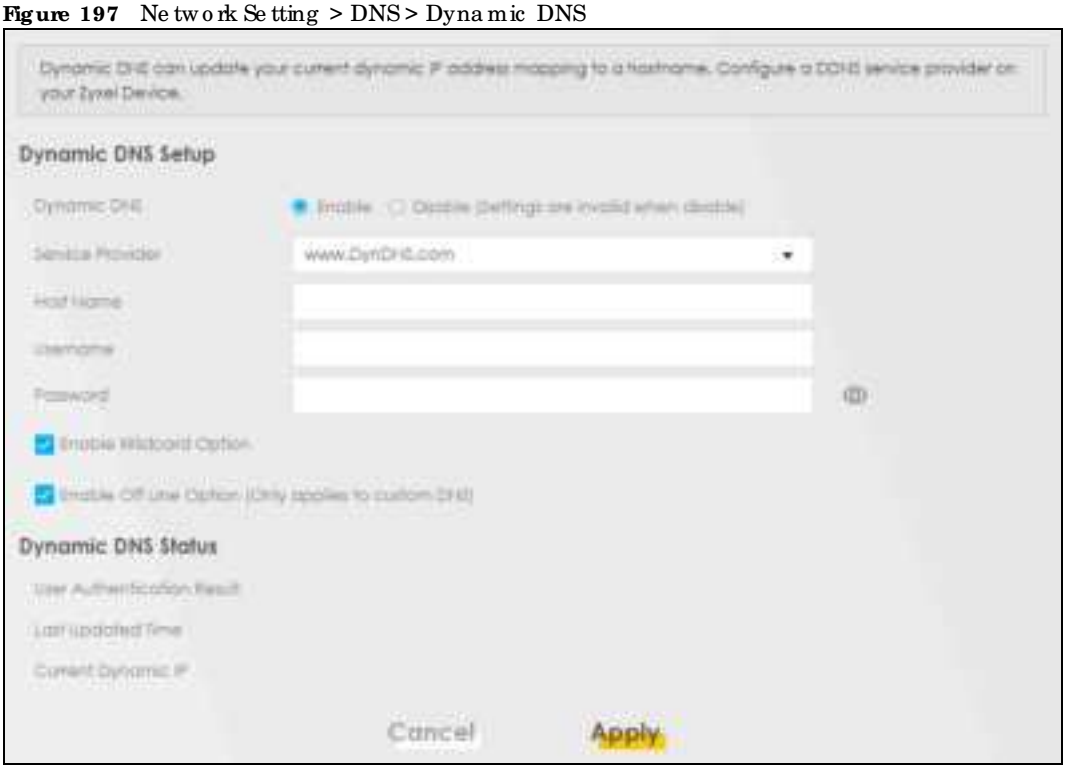
Table 120 Network Setting > DNS > DNS Entry: Add or Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com.
IPv4 Address	Enter the IPv4 address of the DNS entry.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

14.3 Dynamic DNS

Dynamic DNS can update your current dynamic IP address mapping to a hostname. Configure a DDNS service provider on your Zyxel Device. Click **Network Setting > DNS > Dynamic DNS**. The screen appears as shown.

Figure 197 Network Setting > DNS > Dynamic DNS



The following table describes the fields in this screen.

Table 121 Network Setting > DNS > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Host Name	Enter the domain name assigned to your Zyxel Device by your Dynamic DNS provider. You can use up to 256 alphanumeric (0-9, a-z, A-Z) characters with hyphens [-] and periods [.]. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the checkbox to enable DynDNS Wildcard.
Enable Off Line Option (Only applies to custom DNS)	Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Dynamic DNS Status	
User Authentication Result	This shows **Success** if the account is correctly set up with the Dynamic DNS provider account.
Last Updated Time	This shows the last time the IP address the Dynamic DNS provider has associated with the hostname was updated.
Current Dynamic IP	This shows the IP address your Dynamic DNS provider has currently associated with the hostname.

Table 121 Network Setting > DNS > Dynamic DNS (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 15
IGMP/MLD

15.1 IGMP/MLD Overview

Multicast delivers IP packets to a group of hosts on the network defined by multicast groups. Membership to these multicast groups are established using IGMP/MLD.

Use the **IGMP/MLD** screen to configure IGMP/MLD group settings.

15.1.1 What You Need To Know

Multicast and IGMP

See Multicast on page 252 for more information.

Multicast Listener Discovery (MLD)

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

- MLD allows an IPv6 switch or router to discover the presence of MLD hosts who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.
- MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.
- MLD filtering controls which multicast groups a port can join.
- An MLD Report message is equivalent to an IGMP Report message, and an MLD Done message is equivalent to an IGMP Leave message.

IGMP Fast Leave

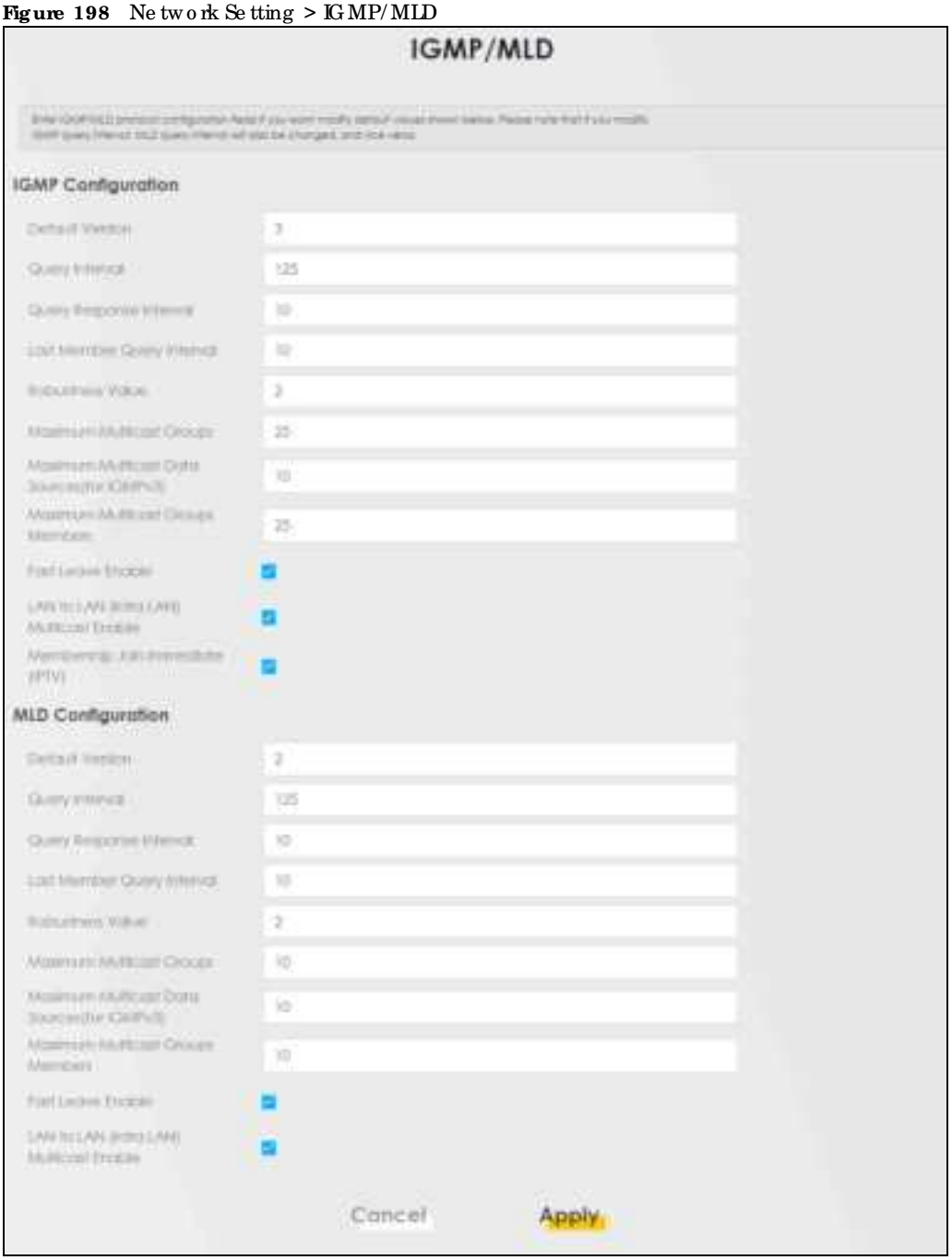
When a host leaves a multicast group (224.1.1.1), it sends an IGMP leave message to inform all routers (224.0.0.2) in the multicast group. When a router receives the leave message, it sends a specific query message to all multicast group (224.1.1.1) members to check if any other hosts are still in the group. Then the router deletes the host's information.
With the IGMP fast leave feature enabled, the router removes the host's information from the group member list once it receives a leave message from a host and the fast leave timer expires.

15.2 The IGMP/MLD Screen

Use this screen to configure multicast groups that the Zyxel Device manages through IGMP/MLD settings. To open this screen, click **Network Setting > IGMP/MLD**.

Note: Some models might only support IGMP/MLD **Default Version** configuration.

Figure 198 Network Setting > IGMP/MLD



The following table describes the labels in this screen.

Table 122 Network Setting > IGMP/MLD

LABEL	DESCRIPTION
IGMP/MLD Configuration	
Default Version	Enter the version of IGMP (1~3) and MLD (1~2) that you want the Zyxel Device to use on the WAN.

Table 122 Network Setting > IGMP/MLD (continued)

LABEL	DESCRIPTION
Query Interval	Enter the number of seconds the Zyxel Device sends a query message to hosts to get the group membership information.
Query Response Interval	Enter the maximum number of seconds the Zyxel Device can wait for receiving a General Query message. Multicast routers use general queries to learn which multicast groups have members.
Last Member Query Interval	Enter the maximum number of seconds the Zyxel Device can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group.
Robustness Value	Enter the number of times (1~7) the Zyxel Device can resend a packet if packet loss occurs due to network congestion.
Maximum Multicast Groups	Enter a number to limit the number of multicast groups an interface on the Zyxel Device is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface.
Maximum Multicast Data Sources(for IGMPv3)	Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2.
Maximum Multicast Group Members	Enter a number to limit the number of multicast members a multicast group can have.
Fast Leave Enable	Select this option to set the Zyxel Device to remove a port from the multicast tree immediately (without sending an IGMP or MLD membership query message) once it receives an IGMP or MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications.
LAN to LAN (Intra LAN) Multicast Enable	Select this to enable LAN to LAN IGMP snooping capability.
Membership Join Immediate (IPTV)	Select this to have the Zyxel Device add a host to a multicast group immediately once the Zyxel Device receives an IGMP or MLD join message.
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 16
VLAN Group

16.1 VLAN Group Overview

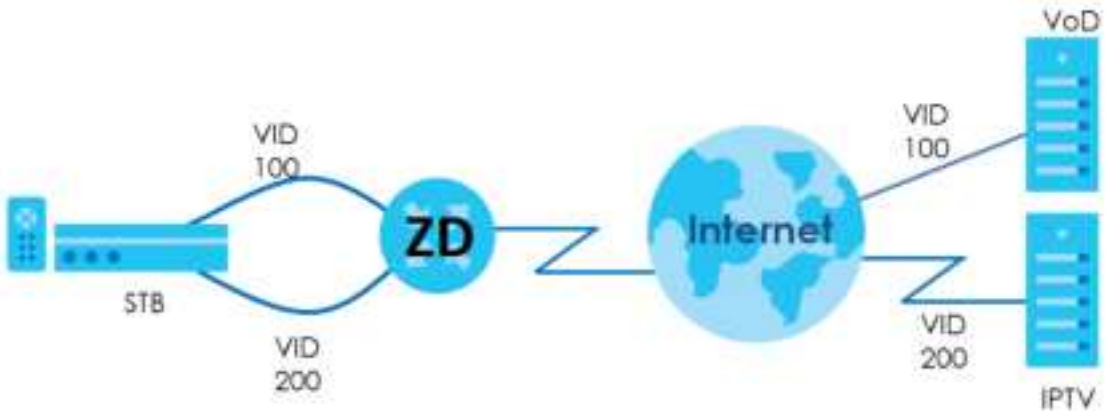
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same groups; the traffic must first go through a router.

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. Shared resources such as a server can be used by all ports in the same VLAN as the server. Ports can belong to other VLAN groups too. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges. The VLAN ID associates a frame with a specific VLAN and provides the information that switches the need to process the frame across the network.

In the following example, VLAN IDs (VIDs) 100 and 200 are added to identify Video-on-Demand and IPTV traffic respectively coming from the VoD and IPTV multicast servers. The Zyxel Device can also tag outgoing requests to the servers with these VLAN IDs.

Figure 199 VLAN Group Example



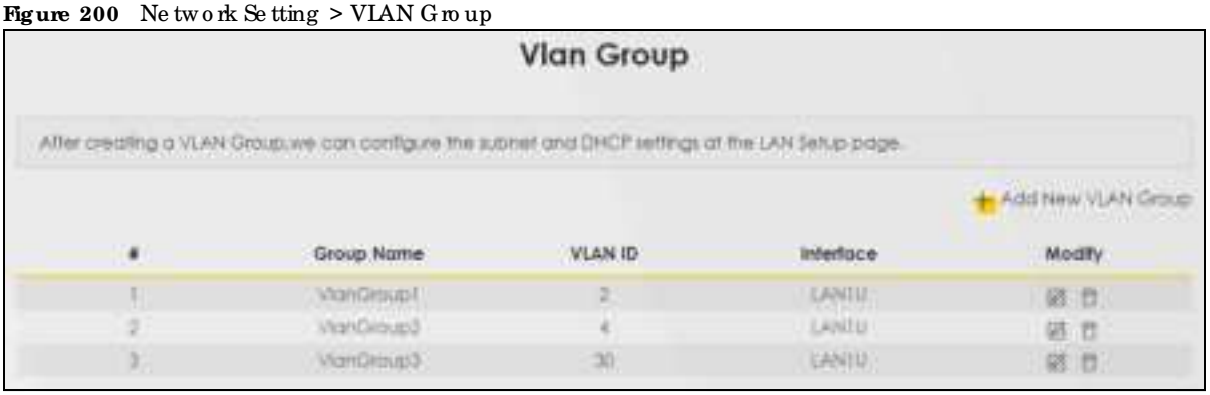
16.1.1 What You Can Do in this Chapter

Use these screens to manage VLAN groups on the Zyxel Device.

16.2 VLAN Group Settings

This screen shows the VLAN groups created on the Zyxel Device. Click **Network Setting > VLAN Group** to open the following screen.

Figure 200 Network Setting > VLAN Group



The following table describes the fields in this screen.

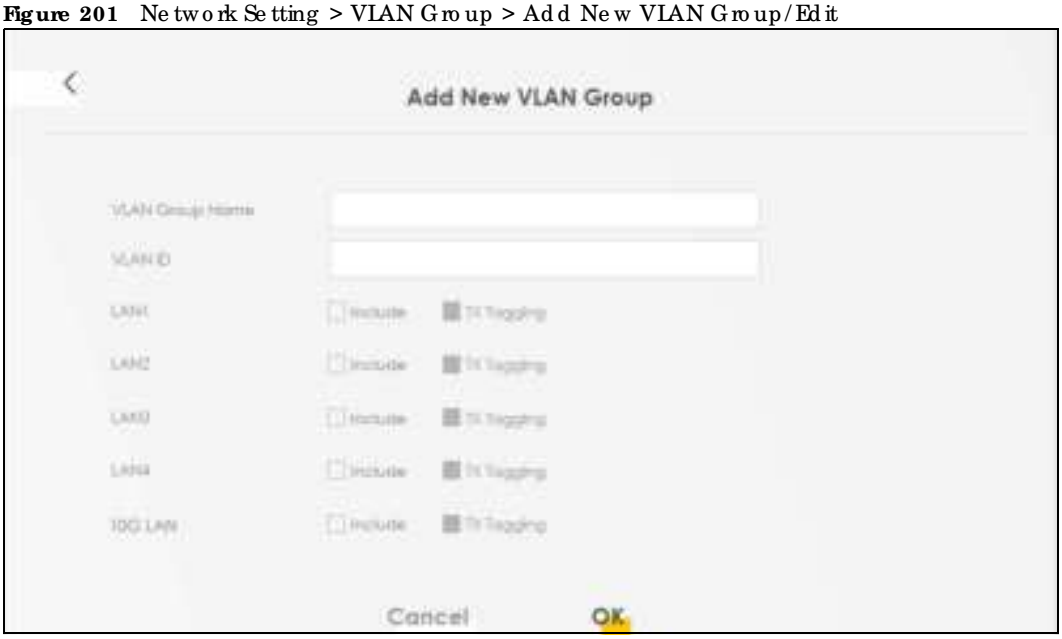
Table 123 Network Setting > VLAN Group

LABEL	DESCRIPTION
Add New VLAN Group	Click this button to create a new VLAN group.
#	This is the index number of the VLAN group.
Group Name	This shows the descriptive name of the VLAN group.
VLAN ID	This shows the unique ID number that identifies the VLAN group.
Interface	This shows the LAN ports included in the VLAN group and if traffic leaving the port will be tagged with the VLAN ID.
Modify	Click the **Edit** icon to change an existing VLAN group setting or click the **Delete** icon to remove the VLAN group.

16.2.1 Add or Edit a VLAN Group

Click the **Add New VLAN Group** button in the **VLAN Group** screen to open the following screen. Use this screen to create a new VLAN group.

Figure 201 Network Setting > VLAN Group > Add New VLAN Group/Edit



The following table describes the fields in this screen.

Table 124 Network Setting > VLAN Group > Add New VLAN Group/Edit

LABEL	DESCRIPTION
VLAN ID	Enter a unique ID number, from 1 to 4,094, to identify this VLAN group. Outgoing traffic is tagged with this ID if **TX Tagging** is selected below.
LAN	Select **Include** to add the associated LAN interface to this VLAN group. Note: Select **TX Tagging** to tag outgoing traffic from the associated LAN port with the **VLAN ID** number entered above.
	Select **Include** to add the associated LAN interface to this VLAN group. Note: Select **TX Tagging** to tag outgoing traffic from the associated LAN port with the **VLAN ID** number entered above.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

CHAPTER 17
Interface Grouping

17.1 Interface Grouping Overview

By default, all LAN and WAN interfaces on the Zyxel Device are in the same group and can communicate with each other. Create interface groups to have the Zyxel Device assign IP addresses in different domains to different groups. Each group acts as an independent network on the Zyxel Device. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

17.1.1 What You Can Do in this Chapter

The **Interface Grouping** screen lets you create multiple networks on the Zyxel Device (Section 17.2 on page 375).

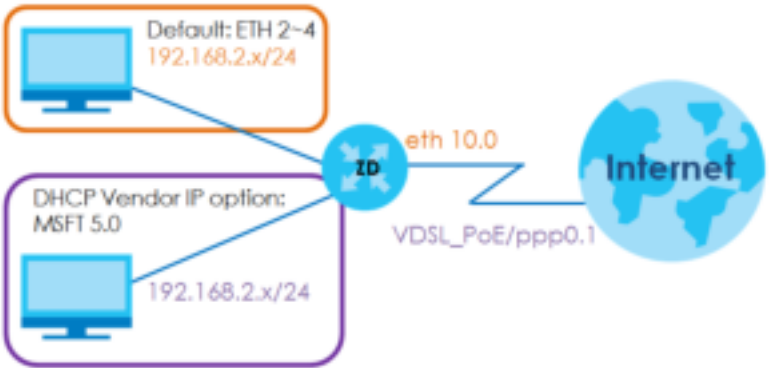
17.2 Interface Grouping

You can manually add a LAN interface to a new group. Alternatively, you can have the Zyxel Device automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN Setup** screen to configure the private IP addresses the DHCP server on the Zyxel Device assigns to the clients in the default and/or user-defined groups. If you set the Zyxel Device to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. See Chapter 10 on page 284 for more information.

In the following example, the client that sends packets with the DHCP Vendor ID option set to MSFT 5.0 (meaning it is a Windows 2000 DHCP client) is assigned the IP address 192.168.2.2 and uses the WAN VDSL_PoE/ppp0.1 interface.

Figure 202 Interface Grouping Application



You can use this screen to create new user-defined interface groups or modify existing ones. Interfaces that do not belong to any user-defined group always belong to the default group.

Click **Network Setting > Interface Grouping** to open the following screen.

Figure 203 Network Setting > Interface Grouping

The following table describes the fields in this screen.

Table 125 Network Setting > Interface Grouping

LABEL	DESCRIPTION
Add New Interface Group	Click this button to create a new interface group.
Group Name	This shows the descriptive name of the group.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
Criteria	This shows the filtering criteria for the group.
Modify	Click the **Edit** icon to modify an existing Interface group setting or click the **Delete** icon to remove the Interface group.

17.2.1 Interface Group Configuration

Click the **Add New Interface Group** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group. If you want to automatically add LAN clients to a new group, use filtering criteria.

Note: An interface can belong to only one group at a time.

Note: After configuring a vendor ID, reboot the client device attached to the Zyxel Device to obtain an appropriate IP address.

Note: You can have up to 15 filter criteria.

Figure 204 Network Setting > Interface Grouping > Add New Interface Group (for DSL routers)

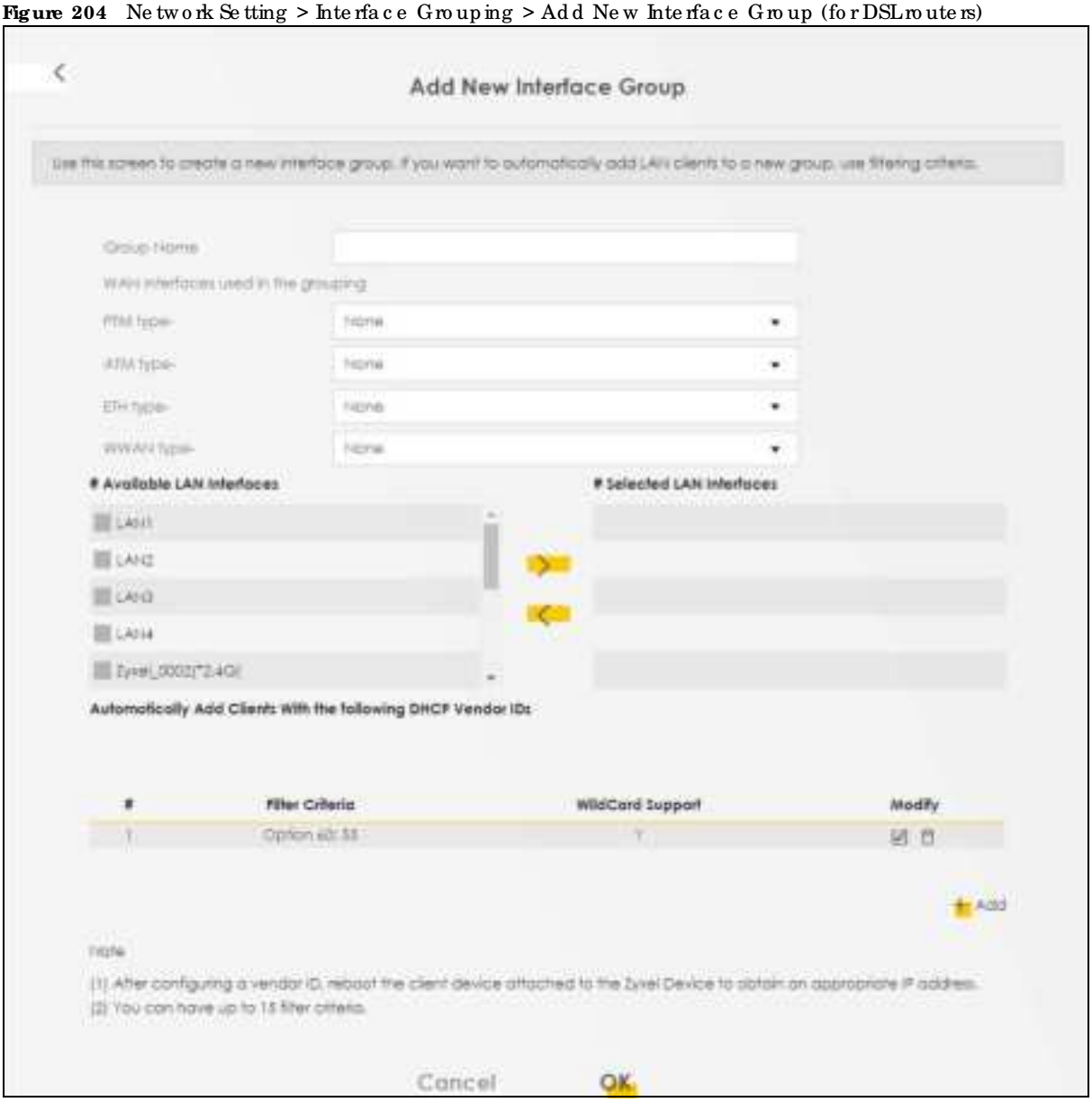


Figure 205 Network Setting > Interface Grouping > Add New Interface Group (for Ethernet routers)

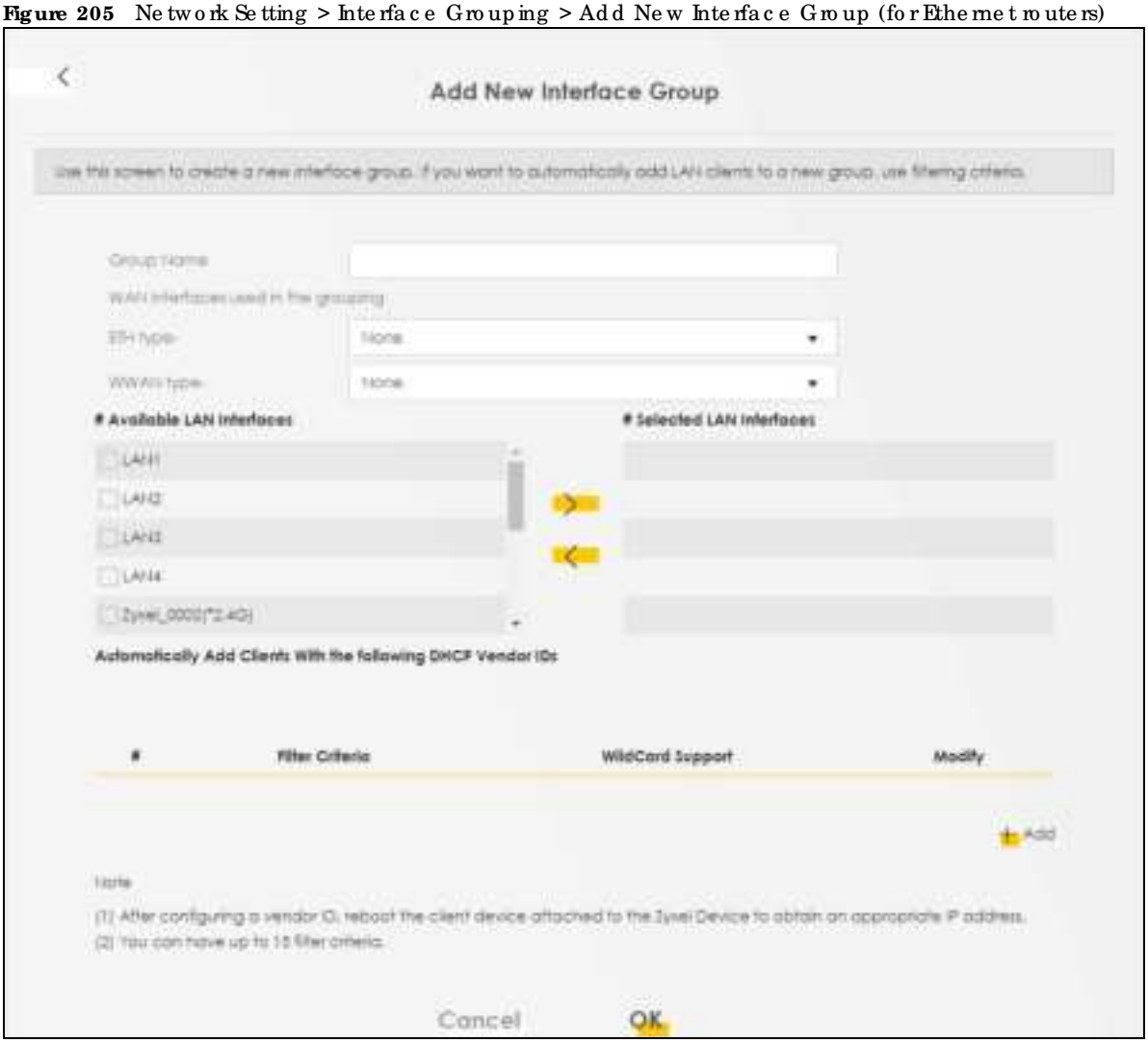
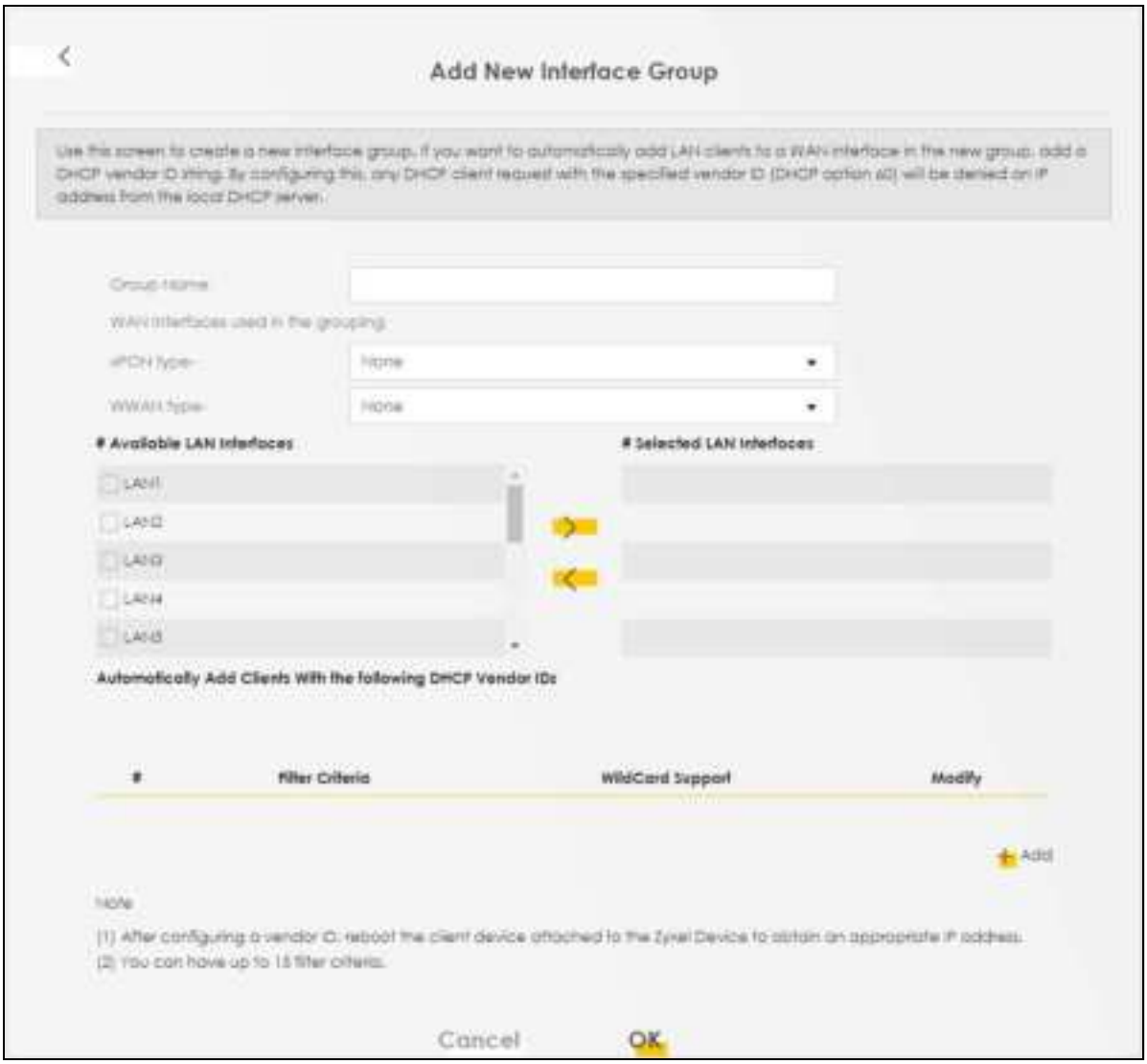


Figure 206 Network Setting > Interface Grouping > Add New Interface Group (for AON and PON routers)



The following table describes the fields in this screen.

Table 126 Network Setting > Interface Grouping > Add New Interface Group/Edit

LABEL	DESCRIPTION
Group Name	Enter a descriptive name for this interface group. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface, up to one ATM interface, up to one ETH interface, and up to one WWAN interface. Select **None** to not add a WAN interface to this group.
Selected LAN Interfaces Available LAN Interfaces	Select one or more interfaces (Ethernet LAN, wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Selected LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Selected LAN Interfaces**, use the right-facing arrow.

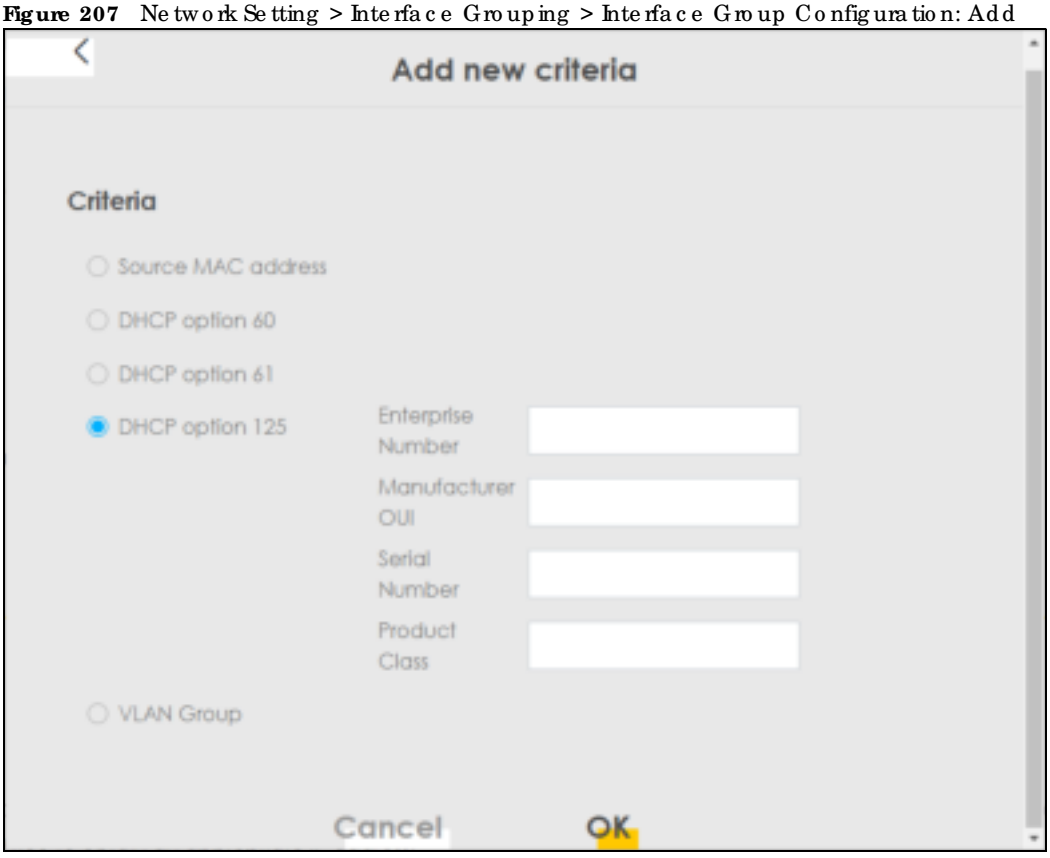
Table 126 Network Setting > Interface Grouping > Add New Interface Group/Edit (continued)

LABEL	DESCRIPTION
Automatically Add Clients With the following DHCP Vendor IDs	Click **Add** to identify LAN hosts to add to the interface group by criteria such as the type of the hardware or firmware. See Section 17.2.2 on page 380 for more information.
#	This shows the index number of the rule.
Filter Criteria	This shows the filtering criteria. The LAN interface on which the matched traffic is received will belong to this group automatically.
Wild Card Support	This shows if wildcard on DHCP option 60 is enabled.
Modify	Click the **Edit** icon to change the group setting. Click the **Delete** icon to delete this group from the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click OK to save your changes.

17.2.2 Interface Grouping Criteria

Click the **Add** button in the **Interface Grouping Configuration** screen to open the following screen. Use this screen to automatically add clients to an interface group based on specified criteria. You can choose to define a group based on a MAC address, a vendor ID (DHCP option 60), an Identity Association Identifier (DHCP option 61), vendor specific information (DHCP option 125), or a VLAN group.

Figure 207 Network Setting > Interface Grouping > Interface Group Configuration: Add



The following table describes the fields in this screen.

Table 127 Network Setting > Interface Grouping > Interface Group Configuration: Add

LABEL	DESCRIPTION
Source MAC Address	Enter the source MAC address of the packet.
APAS MAC Filter	Select this option and enter the MAC address of the matched LAN host.
DHCP Option 60	Select this option and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
Enable wildcard	Select this option to be able to use wildcards in the Vendor Class Identifier configured for DHCP option 60.
DHCP Option 61	Select this and enter the device identity of the matched traffic.
	Enter the Identity Association Identifier (IAID) of the device, for example, the WAN connection index number.
DHCP Option 125	Select this and enter vendor specific information of the matched traffic.
Enterprise Number	Enter the vendor's 32-bit enterprise number registered with the IANA (Internet Assigned Numbers Authority).
Manufacturer OUI	Specify the vendor's OUI (Organization Unique Identifier). It is usually the first 3 bytes of the MAC address.
Serial Number	Enter the serial number of the device.
Product Class	Enter the product class of the device.
VLAN Group	Select this and the VLAN group of the matched traffic from the drop-down list box. A VLAN group can be configured in **Network Setting > VLAN Group**.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

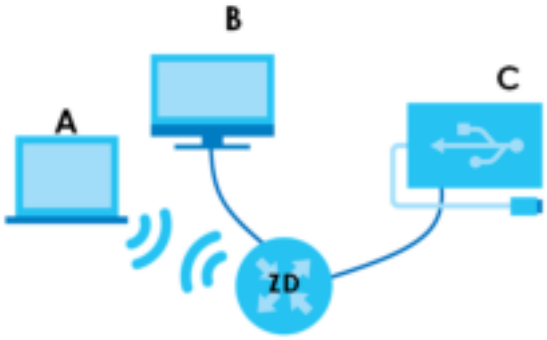
CHAPTER 18
USB Service

18.1 USB Service Overview

You can share files on a USB memory stick or hard drive connected to your Zyxel Device with users on your network.

The following figure is an overview of the Zyxel Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the Zyxel Device.

Figure 208 File Sharing Overview



The Zyxel Device will not be able to join a workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

18.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to enable file-sharing server (Section 18.2 on page 383).
- Use the **Media Server** screen to enable or disable the sharing of media files (Section 18.3 on page 386).

18.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

18.1.2.1 About File Sharing

Workgroup Name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the Zyxel Device is given a folder, called a "share". If a USB hard drive connected to the Zyxel Device has more than one partition, then each partition will be allocated a share. You can also configure a "share" to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your Zyxel Device supports File Allocation Table (FAT) and FAT32.

Common Internet File System

The Zyxel Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the Zyxel Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

18.1.3 Before You Begin

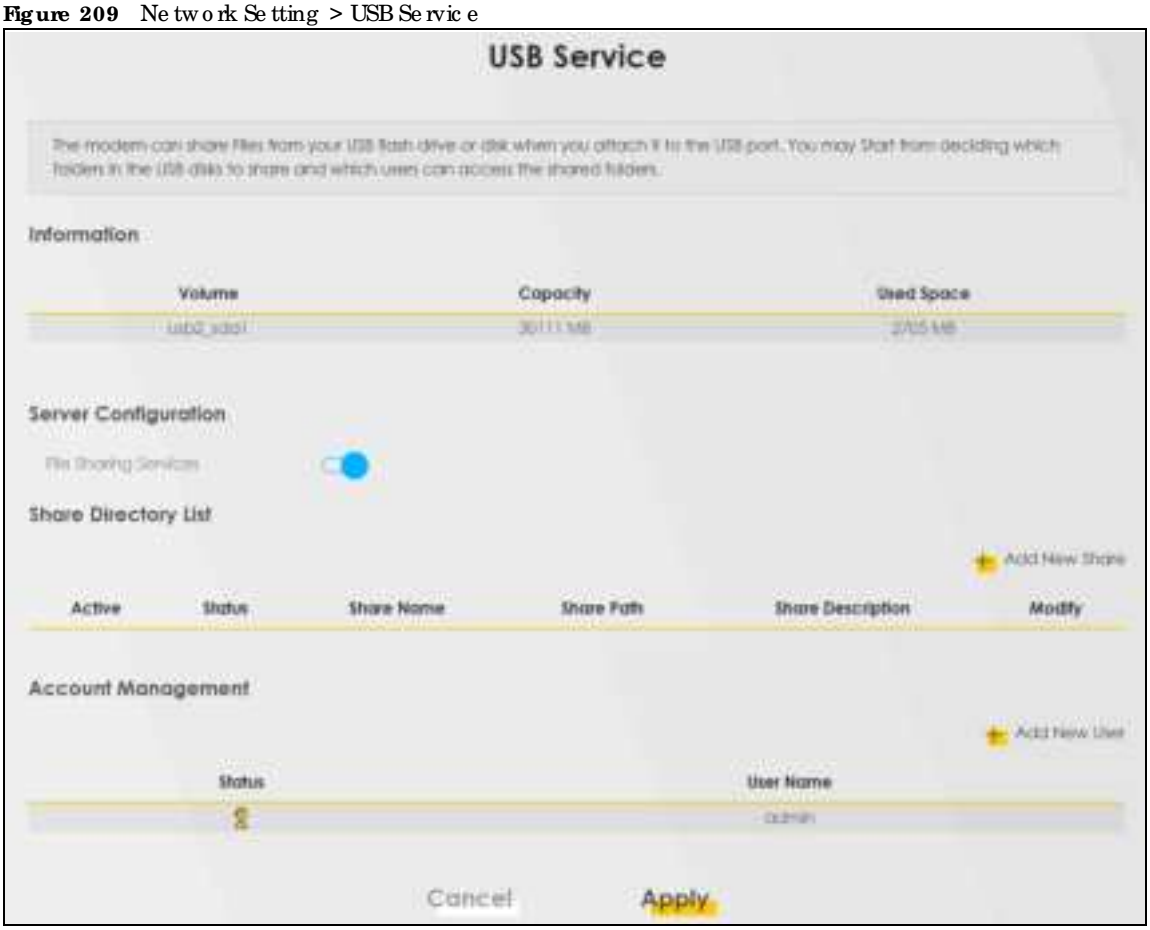
1. Make sure the Zyxel Device is connected to your network and turned on.
2. Connect the USB device to one of the Zyxel Device's USB port. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source.
3. The Zyxel Device detects the USB device and makes its contents available for browsing.

Note: If your USB device cannot be detected by the Zyxel Device, see the troubleshooting for suggestions.

18.2 USB Service

Use this screen to set up file sharing through the Zyxel Device. The Zyxel Device's LAN users can access the shared folder (or share) from the USB device inserted in the Zyxel Device. To access this screen, click **Network Setting > USB Service**.

Figure 209 Network Setting > USB Service



Note: The **Share Directory List** is only visible when you connect a USB device.

Each field is described in the following table.

Table 128 Network Setting > USB Service

LABEL	DESCRIPTION
Information	
Volume	This is the volume name the Zyxel Device gives to an inserted USB device.
Capacity	This is the total available memory size (in megabytes) on the USB device.
Used Space	This is the memory size (in megabytes) already used on the USB device.
Server Configuration	
File Sharing Services	Click this switch to enable file sharing through the Zyxel Device.
Share Directory List This only appears when you have inserted a USB device.	
Add New Share	Click this to set up a new share on the Zyxel Device.
Active	Select this to allow the share to be accessed.
Status	This field shows the status of the share : The share is not activated. : The share is activated.

Table 128 Network Setting > USB Service (continued)

LABEL	DESCRIPTION
Share Name	This field displays the name of the file you shared.
Share Path	This field displays the location in the USB of the file you shared.
Share Description	This field displays a description of the file you shared.
Modify	Click the **Edit** icon to change the settings of an existing share. Click the **Delete** icon to delete this share in the list.
Account Management	
Add New User	Click this button to create a user account to access the secured shares. This button redirects you to **Maintenance > User Account.**
Status	This field shows the status of the user. : The user account is not activated for the share. : The user account is activated for the share.
User Name	This is the name of a user who is allowed to access the secured shares on the USB device.
Cancel	Click this to restore your previously saved settings.
Apply	Click this to save your changes to the Zyxel Device.

18.2.1 Add New Share

Use this screen to set up a new share or edit an existing share on the Zyxel Device. Click **Add New Share** in the **File Sharing** screen or click the **Edit** or **Modify** icon next to an existing share.

Please note that you need to set up shared folders on the USB device before enabling file sharing in the Zyxel Device. Spaces and the following special characters, ["], [`], ['], [<], [>], [^], [$], [|], [&], [;], are not allowed for the USB share name.

Figure 210 Network Setting > USB Service > Add New Share

The following table describes the labels in this menu.

Table 129 Network Setting > USB Service > Add New Share

LABEL	DESCRIPTION
Volume	Select the volume in the USB storage device that you want to add as a share in the Zyxel Device. This field is read-only when you are editing the share.
Share Path	Manually enter the file path for the share, or click the **Browse** button and select the folder that you want to add as a share. This field is read-only when you are editing the share.
Description	You can either enter a short description of the share, or leave this field blank. You can use up to 128 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Access Level	Select **Public** if you want the share to be accessed by users connecting to the Zyxel Device. Otherwise, select **Security**.
Allowed	If **Security** is selected in the **Access Level** field, select this check box to allow/prohibit access to the share.
User Name	This field specifies the user for which the **Allowed** setting applies. Users can be added or modified in **Maintenance > User Account.**
Cancel	Click **Cancel** to return to the previous screen.
OK	Click **OK** to save your changes.

18.2.2 Add New User Screen

Once you click the **Add New User** button, you will be directed to the **User Account** screen. To create a user account that can access the secured shares on the USB device, click the **Add New Account** button in the **Network Setting > USB Service > User Account screen**.

Please see Chapter 36 on page 475, for detailed information about **User Account** screen.

18.3 Media Server

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your Zyxel Device without having to copy them to another computer. The Zyxel Device can function as a DLNA-compliant media server, where the Zyxel Device streams files to DLNA-compliant media clients like Windows Media Player. The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

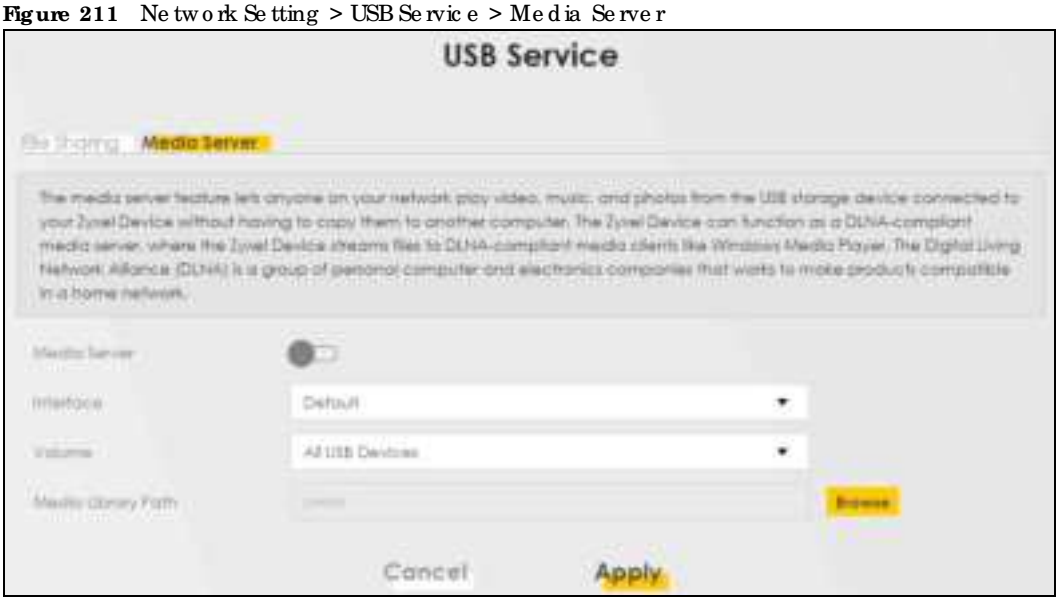
The Zyxel Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the Zyxel Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

To change your Zyxel Device's media server settings, click **Network Setting > USB Service > Media Server**. The screen appears as shown.

Figure 211 Network Setting > USB Service > Media Server



The following table describes the labels in this menu.

Table 130 Network Setting > USB Service > Media Server

LABEL	DESCRIPTION
Media Server	Click this switch to have the Zyxel Device function as a DLNA-compliant media server. When the switch goes to the right, the function is enabled. Otherwise, it is not. Enable the media server to let (DLNA-compliant) media clients on your network play media files located in the shares.
Interface	Select an interface on which you want to enable the media server function. An interface can be added or modified in **Network Setting > Interface Grouping.**
Volume	This is the volume name the Zyxel Device gives to an inserted USB device. Select a volume in the USB storage device(s) to allow the Zyxel Device media server access. Select **All USB Devices** to enable access on all volumes.
Media Library Path	Enter the path clients use to access the media files on a USB storage device connected to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

CHAPTER 19
Firewall

19.1 Firewall Overview

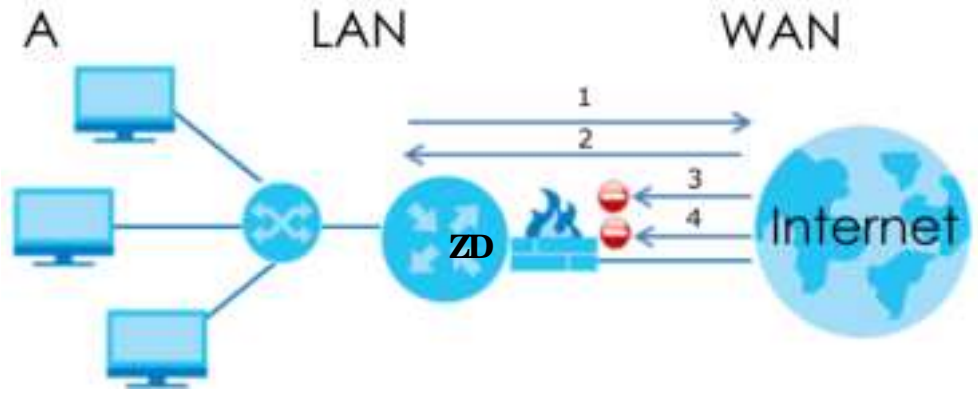
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

By default, the Zyxel Device blocks DoS attacks whether the firewall is enabled or disabled.

The following figure illustrates the firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 212 Default Firewall Action



19.1.1 What You Need to Know About Firewall

SYN Attack

A 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 a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer 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.

DoS

Denial-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.

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.

DDoS

A Distributed Denial-of-Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

ICMP

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.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target 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.

Ping of Death

Ping of Death uses a 'ping' utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

19.2 Firewall

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it.

19.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device (Section 19.3 on page 390).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 19.4 on page 391).

- Use the **Access Control** screen to view and configure incoming or outgoing filtering rules (Section 19.5 on page 392).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks (Section 19.6 on page 395).

19.3 Firewall General Settings

Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. Use this screen to set the security level of the firewall on the Zyxel Device. Firewall rules are grouped based on the direction of travel of packets. A higher firewall level means more restrictions on the Internet activities you can perform. Click **Security > Firewall > General** to display the following screen. Use the slider to select the level of firewall protection.

Figure 213 Security > Firewall > General

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.
When the security level is set to **High**, Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and/or IPv6 ICMPv6 (Ping) traffic from the LAN are still allowed.

The following table describes the labels in this screen.

Table 131 Security > Firewall > General

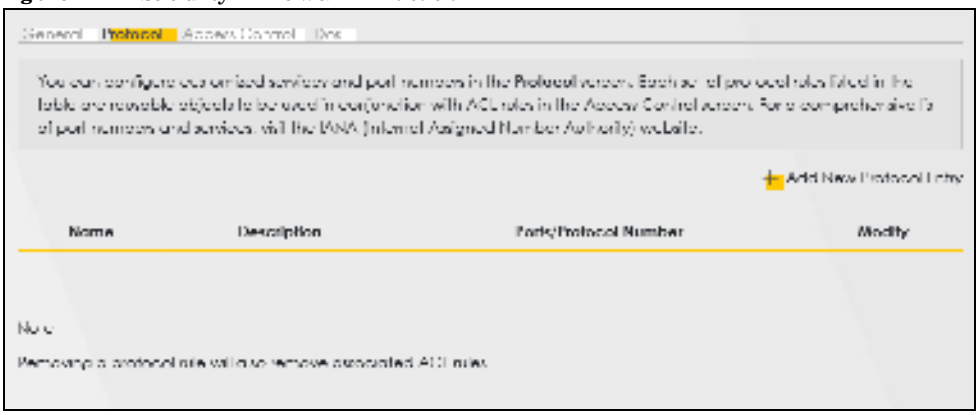
LABEL	DESCRIPTION
IPv4 Firewall	Enable firewall protection when using **IPv4** (Internet Protocol version 4).
IPv6 Firewall	Enable firewall protection when using **IPv6** (Internet Protocol version 6).
High	This setting blocks all traffic to and from the Internet. Only local network traffic and LAN to WAN service (Telnet, FTP, HTTP, HTTPS, DNS, POP3, SMTP) is permitted.
Medium	This is the recommended setting. It allows traffic to the Internet but blocks anyone from the Internet from accessing any services on your local network.
Low	This setting allows traffic to the Internet and also allows someone from the Internet to access services on your local network. This would be used with Port Forwarding, Default Server.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19.4 Protocol (Customized Services)

You can configure customized services and port numbers in the **Protocol** screen. Each set of protocol rules listed in the table are reusable objects to be used in conjunction with ACL rules in the Access Control screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security > Firewall > Protocol** to display the following screen.

Note: Removing a protocol rule will also remove associated ACL rules.

Figure 214 Security > Firewall > Protocol



The following table describes the labels in this screen.

Table 132 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to configure a customized service.
Name	This is the name of your customized service.
Description	This is a description of your customized service.

Table 132 Security > Firewall > Protocol (continued)

LABEL	DESCRIPTION
Ports/Protocol Number	This shows the port number or range and the IP protocol (**TCP** or **UDP**) that defines your customized service.
Modify	Click this to edit a customized service.

19.4.1 Add Customized Service

Add a customized rule or edit an existing rule by specifying the protocol and the port numbers. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

Figure 215 Security > Firewall > Protocol: Add New Protocol Entry

The following table describes the labels in this screen.

Table 133 Security > Firewall > Protocol: Add New Protocol Entry

LABEL	DESCRIPTION
Service Name	Enter a descriptive name for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Description	Enter a description for your customized service. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Protocol	Select the protocol (**TCP**, **UDP**, **ICMP**, **ICMPv6**, or **Other**) that defines your customized port from the drop down list box.
Protocol Number	Enter a single port number or the range of port numbers (**0 – 255**) that define your customized service.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

19.5 Access Control (Rules)

An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed. Click **Security > Firewall > Access Control** to display the following screen.

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

Figure 216 Security > Firewall > Access Control

The following table describes the labels in this screen.

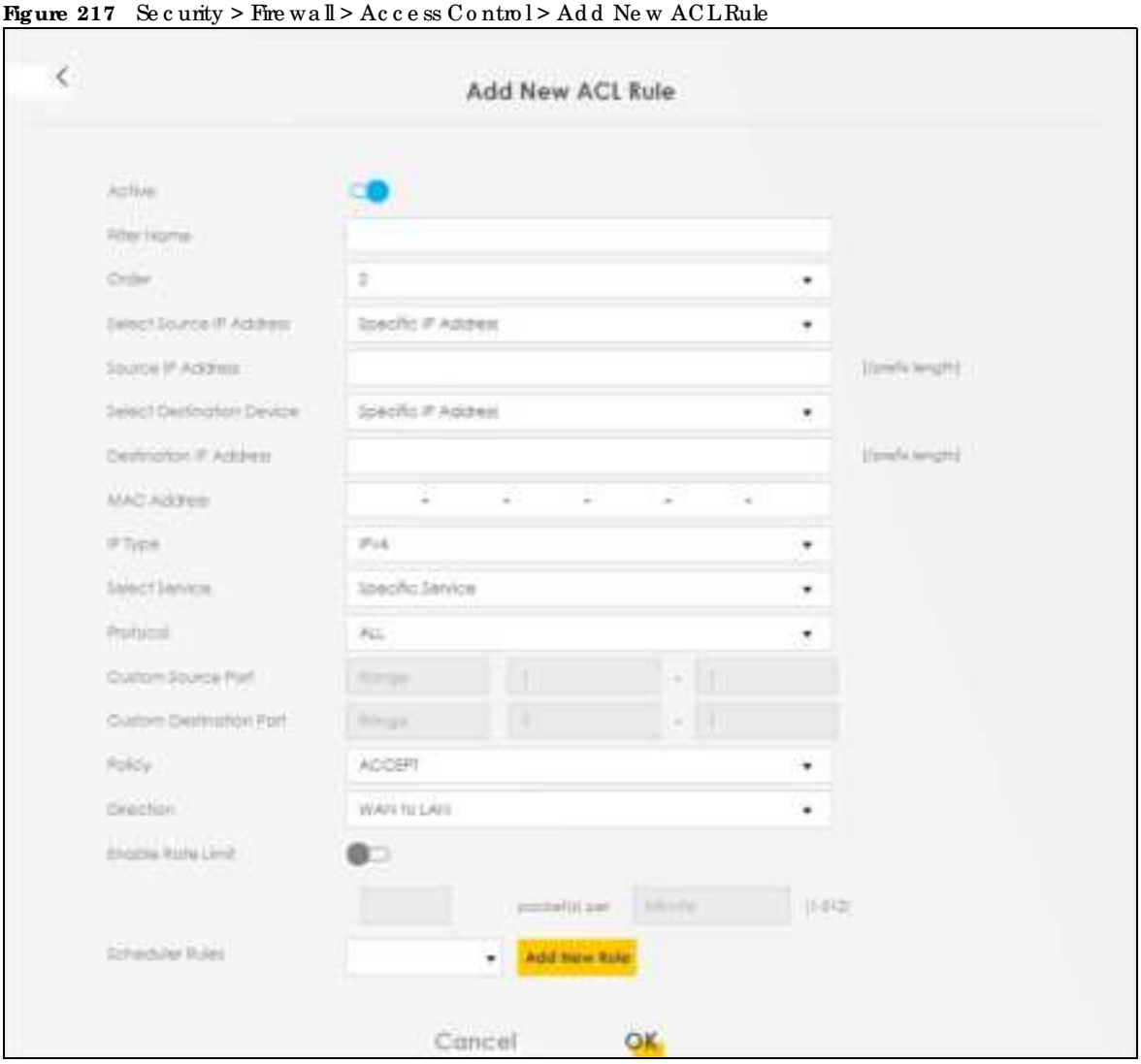
Table 134 Security > Firewall > Access Control

LABEL	DESCRIPTION
Rules Storage Space Usage	This read-only bar shows how much of the Zyxel Device's memory is in use for recording firewall rules. 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.
Add New ACL Rule	Select an index number and click **Add New ACL Rule** 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.
#	This field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Status	This field displays the status of the ACL rule. A yellow bulb signifies that this ACL rule is active, while a gray bulb signifies that this ACL rule is not active.
Name	This field displays the rule name.
Src IP	This field displays the source IP addresses to which this rule applies.
Dest IP	This field displays the destination IP addresses to which this rule applies.
Service	This field displays the protocol (All, TCP, UDP, TCP/UDP, ICMP, ICMPv6, or any) used to transport the packets for which you want to apply the rule.
Action	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 allow the passage of (**Accept**) packets that match this rule.
Modify	Click the **Edit** icon to edit the firewall rule. Click the **Delete** icon to delete an existing firewall rule.

19.5.1 Add New ACL Rule

Click **Add new ACL** rule or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays. Use this screen to accept, reject, or drop packets based on specified parameters, such as source and destination IP address, IP Type, service, and direction. You can also specify a limit as to how many packets this rule applies to at a certain period of time or specify a schedule for this rule.

Figure 217 Security > Firewall > Access Control > Add New ACL Rule



The following table describes the labels in this screen.

Table 135 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Active	Click this switch to enable this ACL rule.
Filter Name	Enter a descriptive name for your filter rule. You can use up to 16 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Order	Assign the order of your rules as rules are applied in turn.
Select Source IP Address	If you want the source to come from a particular (single) IP, select **Specific IP Address**. If not, select from a detected device.
Source IP Address	If you selected **Specific IP Address** in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select **Specific IP Address**. If not, select a detected device.
Destination IP Address	If you selected **Specific IP Address** in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.

Table 135 Security > Firewall > Access Control > Add New ACL Rule (continued)

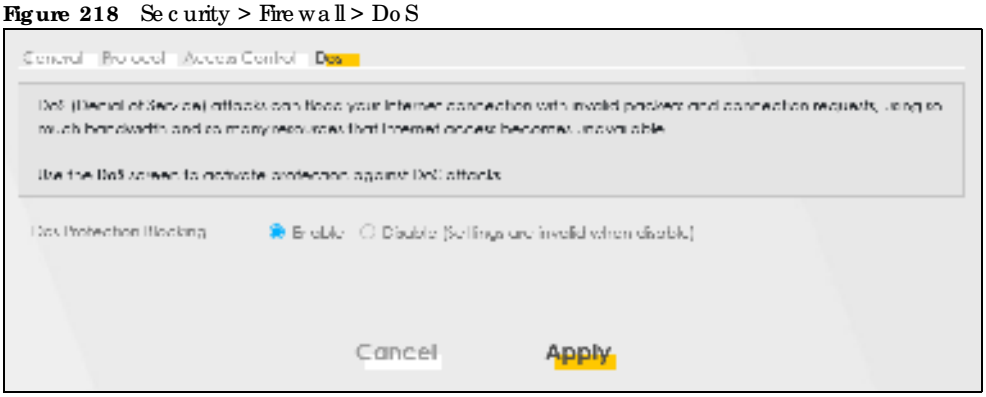
LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses of the WiFi or wired LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
IP Type	Select between **IPv4** or **IPv6**. Compared to **IPv4**, **IPv6** (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in **IPv6** address size to 128 bits (from the 32-bit **IPv4** address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use **IPv4**/**IPv6** dual stack to connect to **IPv4** and **IPv6** networks, and supports **IPv6** rapid deployment (6RD).
Select Service	Select a service from the **Select Service** box.
Protocol	Select the protocol (**ALL**, **TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **ICMPv6**) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
TCP Flag	Select the TCP Flag (SYN, ACK, URG, PSH, RST, FIN). This appears when you select **TCP/UDP** or **TCP** in the **Protocol** field.
Policy	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP destination-unreachable message to the sender (**Reject**), or allow the passage of (**Accept**) packets that match this rule.
Direction	Select **WAN to IAN** to apply the rule to traffic from WAN to IAN. Select **IAN to WAN** to apply the rule to traffic from IAN to WAN. Select **WAN to Router** to apply the rule to traffic from WAN to router. Select **IAN to Router** to apply the rule to traffic from IAN to router.
Enable Rate Limit	Click this switch to enable the setting of maximum number of packets per maximum number of minute or second to limit the throughput of traffic that matches this rule. If not, the next item will be disabled.
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by clicking **Add New Rule**. This will bring you to the **Security > Scheduler Rules** screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

19.6 DoS

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Use the **DoS** screen to activate protection against DoS attacks.

Click **Security > Firewall > DoS** to display the following screen.

Figure 218 Security > Firewall > DoS



The following table describes the labels in this screen.

Table 136 Security > Firewall > DoS

LABEL	DESCRIPTION
DoS Protection Blocking	Enable this to protect against DoS attacks. The Zyxel Device will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

19.7 Firewall Technical Reference

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

19.7.1 Firewall Rules Overview

Your customized rules take precedence and override the Zyxel Device's default settings. The Zyxel Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the Zyxel Device takes the action specified in the rule.

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

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

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

- LAN to Router

  These rules specify which computers on the LAN can manage the Zyxel Device (remote management).

Note: You can also configure the remote management settings to allow only a specific computer to manage the Zyxel Device.

- LAN to WAN

  These rules specify which computers on the LAN can access which computers or services on the WAN.

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

- WAN to LAN

  These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

- WAN to Router

  By default the Zyxel Device stops computers on the WAN from managing the Zyxel Device. You could configure one of these rules to allow a WAN computer to manage the Zyxel Device.

Note: You also need to configure the remote management settings to allow a WAN computer to manage the Zyxel Device.

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

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.

19.7.2 Guidelines For Security Enhancement With Your Firewall

1. Change the default password through the Web Configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your router.
4. Do not enable any local service (such as telnet or FTP) that you do not 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.
5. 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.

6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

19.7.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the Zyxel Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC (Internet Relay Chat) is blocked, are there users that require this service?

2 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?

3 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.

4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the Web Configurator screens.

CHAPTER 20
MAC Filter

20.1 MAC Filter Overview

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired connections. 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 addresses of wired LAN client to configure this screen.

20.2 MAC Filter

Enable **MAC Address Filter** and add the host name and MAC address of a wired LAN client to the table if you wish to allow or deny them access to your network. You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter. Select **Security > MAC Filter**. The screen appears as shown.

Figure 219 Security > MAC Filter

The following table describes the labels in this screen.

Table 137 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate the MAC filter function.
MAC Restrict Mode	Select **Allow** to only permit the listed MAC addresses access to the Zyxel Device. Select **Deny** to permit anyone access to the Zyxel Device except the listed MAC addresses.
Add New Rule	Select an existing wired LAN client from the list to add as a new entry. Select **Custom** if you want to manually enter the **Host Name** and **MAC Address**. Click the **Add** button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select **Active** to enable the MAC filter rule. The rule will not be applied if **Allow** is not selected under **MAC Restrict Mode**.
Host Name	Enter the host name of a wired LAN client that you want to allow access to the Zyxel Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC address of a wired LAN client that you want to allow access to the Zyxel Device. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the **Delete** icon to delete an existing rule.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

20.2.1 Add New Rule

You can choose to enable or disable the filters per entry; make sure that the checkbox under **Active** is selected if you want to use a filter, as shown in the example below. Select **Security > MAC Filter > Add New Rule**. The screen appears as shown.

Figure 220 Security > MAC Filter > Add New Rule

The following table describes the labels in this screen.

Table 138 Security > MAC Filter > Add New Rule

LABEL	DESCRIPTION
Set	This is the index number of the MAC address.
Active	Select **Active** to enable the MAC filter rule. The rule will not be applied if **Allow** is not selected under **MAC Restrict Mode**.
Host Name	Enter the host name of a wired LAN client that you want to allow access to the Zyxel Device. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
MAC Address	Enter the MAC addresses of a wired LAN client that you want to allow 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.

Table 138 Security > MAC Filter > Add New Rule (continued)

LABEL	DESCRIPTION
Delete	Click the **Delete** icon to delete an existing rule.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

Chapter 21 Home Security

21.1 Home Security Overview

The Zyxel Device supports URL (Uniform Resource Locator) filtering that allows you to block user access to specific websites containing inappropriate or harmful content. Users on your network will not be able to enter the websites with URL domain names, keywords or full URLs you specify. Check Section 1.1 on page 20 to see if your Zyxel Device supports the Home Security feature.

21.2 Home Security

Use this screen to configure URL filtering settings to block users on your network from accessing certain websites. To access this screen, click **Security > Home Security**.

Figure 221 Security > Home Security

The following table describes the labels in this screen.

Table 139 Security > Home Security

LABEL	DESCRIPTION
Enter Website URL	Enter the URL of a website or URL keyword to which the Zyxel Device blocks access. Click **Block** to add the website to the **Block List**. Use keywords, domain names, or full URLs to block websites. For example, if you want to block a website with the domain name "www.exampleWeb.com", you can use the following input formats: • http://exampleWeb.com • https://exampleWeb.com • exampleWeb.com • www.exampleWeb.com • example
Block List	The Zyxel Device prohibits users on your network from viewing the websites with the URLs/keywords in this block list. Click **x** to remove the entry from the list.

CHAPTER 22
Parental Control

22.1 Parental Control Overview

Parental control allows you to limit the time a user can access the Internet and prevent users from viewing inappropriate content or participating in specified online activities.

Your parental control screens may be different depending on the model you're using. Some Zyxel Devices support scheduling, some support scheduling and URL filtering.

See Section 1.1 on page 20 for more information.

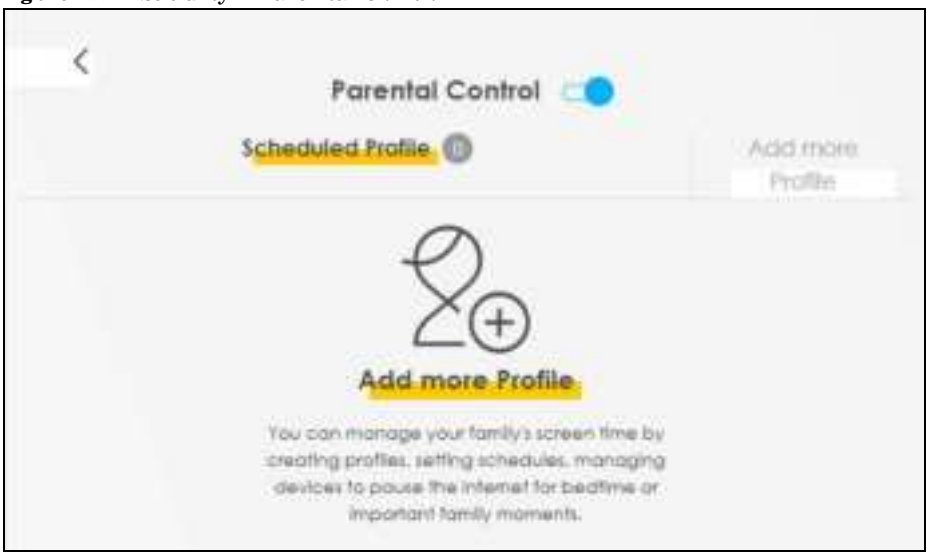
22.2 Parental Control Schedule

Use this screen to enable parental control and view parental control rules and schedules. You can limit the time a user can access the Internet. These rules are defined in a Parental Control Profile (PCP).

Click **Security > Parental Control** to open the following screen.

Note: For some Zyxel Device models, you need to disable MESH to add a new parental control profile.

Figure 222 Security > Parental Control



The following table describes the fields in this screen.

Table 140 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control.
Scheduled Profile	This screen shows all the created profiles.
Add more Profile	Click this button to create a new profile.

22.2.1 Add or Edit a Parental Control Profile

Click **Add more Profile** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule.

Figure 223 Security > Parental Control > Add more Profile: Select Device

The following table describes the fields in this screen.

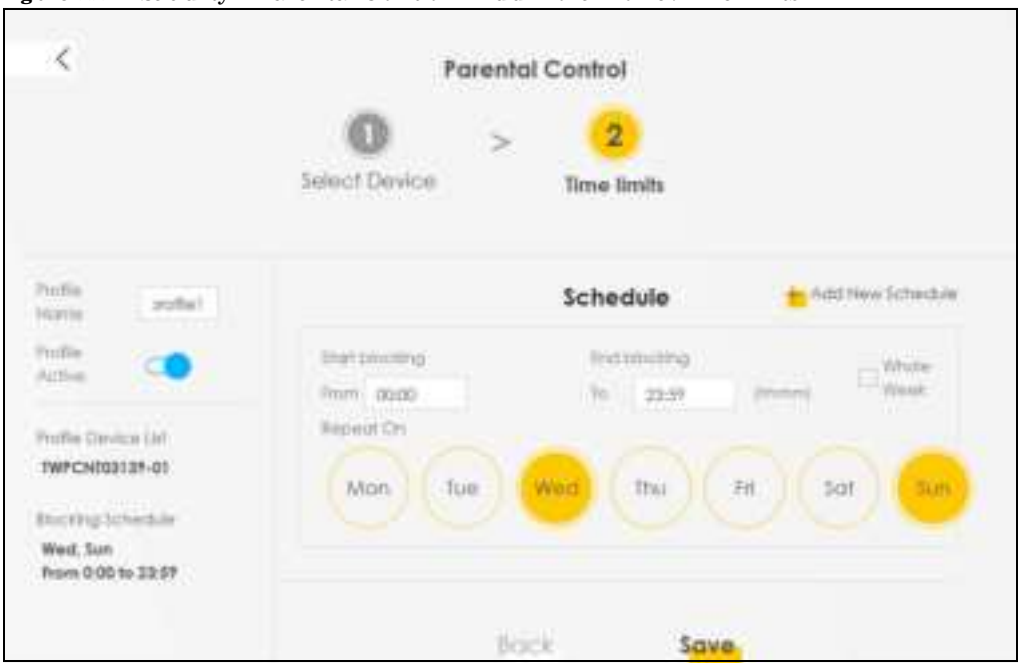
Table 141 Security > Parental Control > Add more Profile: Select Device

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile. You can use up to 17 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Profile Active	Click this switch to enable or disable this profile.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile devices.
Next	Click **Next** to go to the next step to set a schedule for this profile.

22.2.2 Define a Schedule

This screen allow you to define time periods and days during which Internet access is blocked on the profile devices. Finish the settings in the **Select Device** step and click **Next** to access this screen.

Figure 224 Security > Parental Control > Add more Profile: Time limits



The following table describes the fields in this screen.

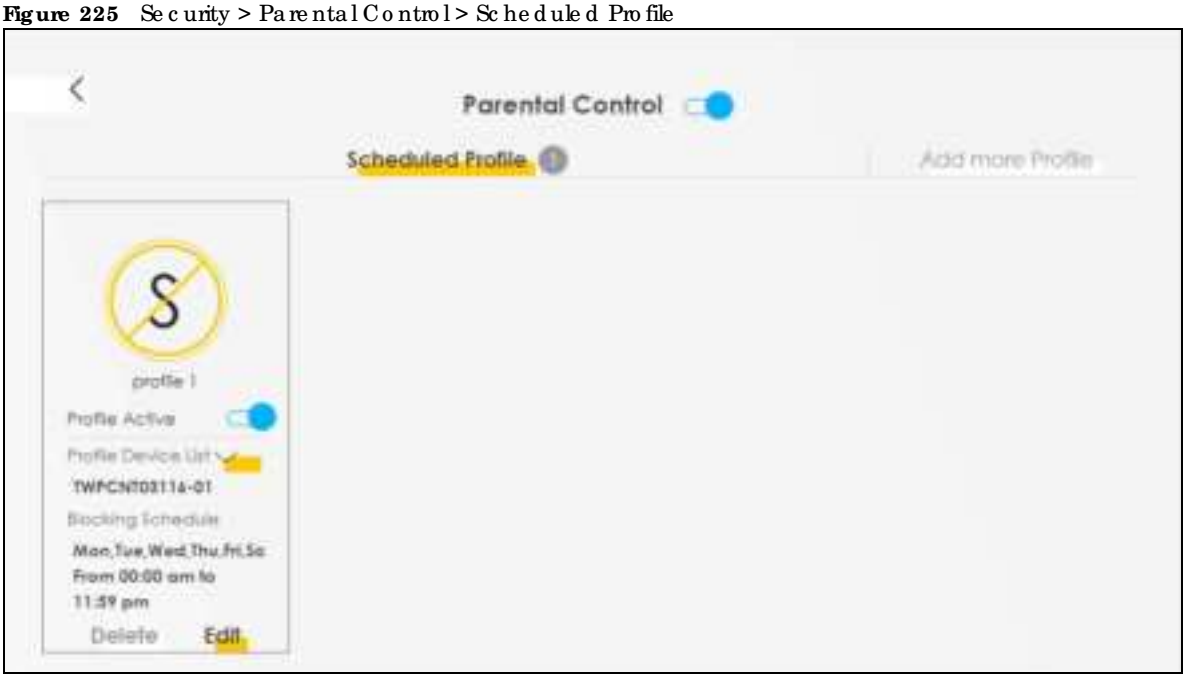
Table 142 Security > Parental Control > Add more Profile: Time limits

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable this profile. When the switch goes to the right ( ), this profile is active. Otherwise, it is not.
Profile Device List	This field shows the devices selected on the right for this profile.
Blocking Schedule	This field shows the time during which Internet access is blocked on the profile devices.
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Start/End blocking	Select the time period when Internet access is blocked on the profile devices.
Repeat On	Select the days when Internet access is blocked on the profile devices. Select **Whole Week** and the scheduler rule will be activated for the whole week.
Back	Click **Back** to return to the previous screen.
Save	Click **Save** to save your changes.

22.2.3 Parental Control Scheduled Profile

Use this screen to view and manage the created parental control profiles.

Figure 225 Security > Parental Control > Scheduled Profile



The following table describes the fields in this screen.

Table 143 Security > Parental Control > Scheduled Profile

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control. When the switch goes to the right ( ), the function is enabled. Otherwise, it is not.
Profile Active	Click this switch to enable or disable a created profile. When the switch goes to the right ( ), this profile is active. Otherwise, it is not.
Scheduled Profile	This screen shows all the created profiles. Click beside **Profile Device List** to view more information about the profile. You can click **Delete** to remove the profile or click **Edit** to change the profile settings. Only the **Add more Profile** button displays if there is no profile created.
Add more Profile	Click this button to create a new profile.

CHAPTER 23
Scheduler Rule

23.1 Scheduler Rule Overview

A Scheduler Rule allows you to define time periods and days during which the Zyxel Device allows certain actions.

23.2 Scheduler Rule Settings

Use this screen to view, add, or edit time schedule rules. A scheduler rule is a reusable object that is applied to other features, such as Firewall Access Control.

Click **Security > Scheduler Rule** to open the following screen.

Figure 226 Security > Scheduler Rule

The following table describes the fields in this screen.

Table 144 Security > Scheduler Rule

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the days on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.
Description	This shows the description of this rule.
Modify	Click the **Edit** icon to edit the schedule. Click the **Delete** icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

23.2.1 Add or Edit a Schedule Rule

Click the **Add New Rule** button in the **Scheduler Rule** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule.

Figure 227 Security > Scheduler Rule: Add or Edit

The following table describes the fields in this screen.

Table 145 Security > Scheduler Rule: Add or Edit

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name for this schedule. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Day	Select check boxes for the days that you want the Zyxel Device to perform this scheduler rule.
Time of Day Range	Enter the time period of each day, in 24-hour format, during which the rule will be enforced.
Description	Enter a description for this scheduler rule. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

CHAPTER 24
Certificates

24.1 Certificates Overview

The Zyxel Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

24.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Zyxel Device's CA-signed (Certification Authority) certificates (Section 24.3 on page 410).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer (Section 24.4 on page 414).

24.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the Zyxel Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

24.3 Local Certificates

Use this screen to view the Zyxel Device's summary list of certificates, generate certification requests, and import signed certificates. You can import the following certificates to your Zyxel Device:

- Web Server – This certificate secures HTTP connections.
- SSH – This certificate secures remote connections.

Click **Security > Certificates** to open the **Local Certificates** screen.

Figure 228 Security > Certificates > Local Certificates

The following table describes the labels in this screen.

Table 146 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Replace Private Key/Certificate file in PEM format	
Private Key is protected by password	Select the checkbox and enter the private key into the text box to store it on the Zyxel Device. You can use up to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
Choose File/ Browse	Click this button to find the certificate file you want to upload.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Zyxel Device.
Create Certificate Request	Click this button to go to the screen where you can have the Zyxel Device generate a certification request.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have a unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate. For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

24.3.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state or province name, and the default US two-letter country code (The US country code is by default and not changeable when sold in the U.S.) for the certificate.

Figure 229 Security > Certificates > Local Certificates: Create Certificate Request

The following table describes the labels in this screen.

Table 147 Security > Certificates > Local Certificates: Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Enter a descriptive name to identify this certificate. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Common Name	Select **Auto** to have the Zyxel Device configure this field automatically. Or select **Customize** to enter it manually. Enter the IP address (in dotted decimal notation), domain name or email address in the field provided. You can use up to 63 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Enter a descriptive name to identify the company or group to which the certificate owner belongs. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
State/Province Name	Enter a descriptive name to identify the state or province where the certificate owner is located. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click **Cancel** to exit this screen without saving.
OK	Click **OK** to save your changes.

24.3.2 View Certificate Request

Use this screen to view in-depth information about the certificate request. The **Certificate** is used to verify the authenticity of the certification authority. The **Private Key** serves as your digital signature for authentication and must be safely stored. The **Signing Request** contains the certificate signing request value that you will copy upon submitting the certificate request to the CA (certificate authority).

Click the **View** icon in the **Local Certificates** screen to open the following screen.

Figure 230 Security > Certificates > Local Certificates: View Certificate

The following table describes the fields in this screen.

Table 148 Security > Certificates > Local Certificates: View Certificates

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.
Private Key	This field displays the private key of this certificate.
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click **Back** to return to the previous screen.

24.4 Trusted CA

Click **Security > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the Zyxel Device to accept as trusted. The Zyxel Device accepts any valid certificate signed by a certification authority on this list as being trustworthy, which means you do not need to import any certificate that is signed by one of these certification authorities.

Note: A maximum of ten certificates can be added.

Figure 231 Security > Certificates > Trusted CA

The following table describes the labels in this screen.

Table 149 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this to open a screen where you can save the certificate of a certification authority that you trust to the Zyxel Device.
#	This is the index number of the entry.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have a unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

24.5 Import Trusted CA Certificate

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. The Zyxel Device trusts any valid certificate signed by any of the imported trusted CA certificates. Certificates should be in one of the following formats: Binary X.509, PEM (base-64) encoded, Binary PKCS# 7, or PEM (base-64) encoded PKCS# 7.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 232 Security > Certificates > Trusted CA > Import Certificate

The following table describes the labels in this screen.

Table 150 Security > Certificates > Trusted CA > Import Certificate

LABEL	DESCRIPTION
Certificate File Path	Enter the location of the file you want to upload in this field or click **Choose File/Browse** to find it.
Choose File/ Browse	Click this to find the certificate file you want to upload.
OK	Click this to save the certificate on the Zyxel Device.
Cancel	Click this to exit this screen without saving.

24.6 View Trusted CA Certificate

Use this screen to view in-depth information about the certification authority's certificate. The certificate text box is read-only and can be distributed to others.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 233 Security > Certificates > Trusted CA > View Certificate

The following table describes the labels in this screen.

Table 151 Security > Certificates > Trusted CA > View Certificate

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through USB thumb drive for example).
Back	Click this to return to the previous screen.

24.7 Certificates Technical Reference

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

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The Zyxel Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Advantages of Certificates

Certificates offer the following benefits.

- The Zyxel Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Format

The certification authority certificate that you want to import has to be in PEM (Base-64) encoded X.509 file format. This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

24.7.1 Verify a Certificate

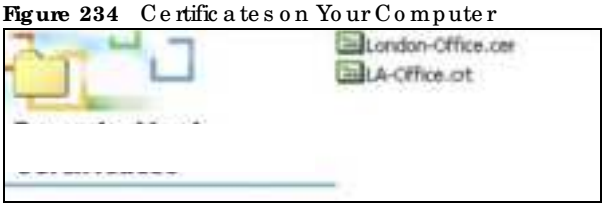
Before you import a trusted CA or trusted remote host certificate into the Zyxel Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the Zyxel Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

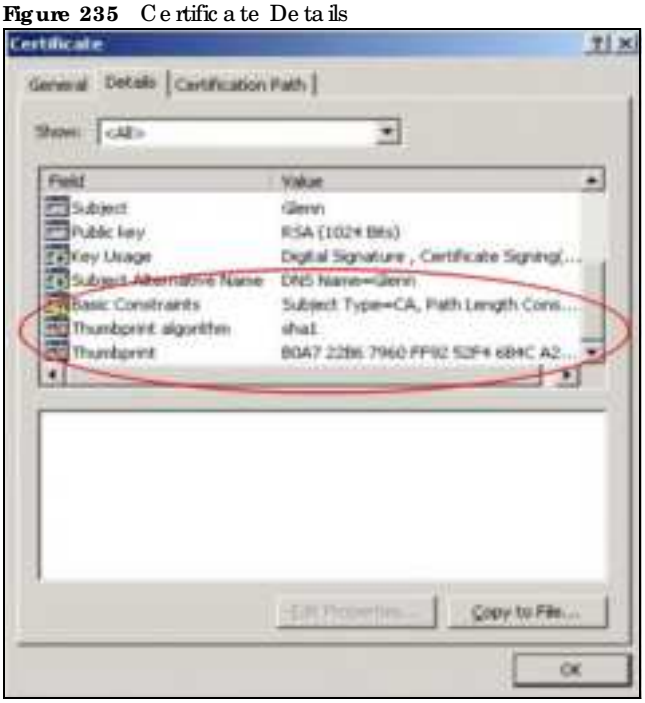
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 234 Certificates on Your Computer



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

Figure 235 Certificate Details



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