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). Zyxel's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See for examples of installing and using UPnP.

Finding Out More

See for technical background information on LANs.

8.1.3 Before You Begin

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

8.2 LAN Setup

Use this screen to set the 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 69 Network Setting > Home Networking > LAN Setup

The following table describes the fields in this screen.

Table 31   Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
Interface Group	
Group Name	Select the interface group name for which you want to configure LAN settings. See Chapter 15 on page 195 for how to create a new interface group.
LAN IP Setup	
IP Address	Enter the LAN IPv4 IP address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type 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	
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 the Zyxel Device act as a DHCP server or DHCP relay agent. Select **Disable** to stop the DHCP server on the Zyxel Device. Select **DHCP Relay** to have the Zyxel Device forward DHCP request to the DHCP server.
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	This field is only available 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	Click this switch to have the Zyxel Device record DHCP IP addresses with the MAC addresses the IP addresses are assigned to. When the switch goes to the right , the function is enabled. Otherwise, it is not. The Zyxel Device assigns the same IP address to the same MAC address when the host requests an IP address again through DHCP.
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	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select **Enable** in the **DHCP** field.
DNS	Select the type of service that you are registered for from your DNS service provider (**From ISP**). Select **DNS Proxy** if you have the DNS proxy service. The Zyxel Device redirects clients' DNS queries to a DNS server for resolving domain names. Select **Static** if you have the static DNS service.

Table 31   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Server 1/2	Enter the first and second DNS (Domain Name System) server IP addresses the Zyxel Device passes to the DHCP clients.
LAN IPv6 Mode Setup	
IPv6 Active	Click this switch to enable or disable the IPv6 mode and configure IPv6 settings on the Zyxel Device. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Link Local Address Type	
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	
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	
Delegate prefix from WAN	Select this option and specify a WAN interface (connection) through which the Zyxel Device automatically obtains an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 prefix for the Zyxel Device's LAN IPv6 address.
MLD 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.
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 autoconfiguration. 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 autoconfiguration. 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 Router Advertisement**: The Zyxel Device provides DNS information through router advertisements. • **From DHCPv6 Server**: The Zyxel Device provides DNS information through DHCPv6. • **From RA & DHCPv6 Server**: The Zyxel Device provides DNS information through both router advertisements and DHCPv6.
DHCPv6 Configuration	
DHCPv6 Active	This shows the status of the DHCPv6. **DHCPv6 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 (This section is available only when you select **Stateful** in the **LAN IPv6 Address Assign Setup** field.)	

Table 31   Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
IPv6 Start Address	Enter the first of the contiguous addresses in the IPv6 address pool.
IPv6 End Address	Enter the last of the contiguous addresses in the IPv6 address pool.
IPv6 Domain Name	Enter the domain name that is assigned to the DHCPv6 clients.
IPv6 DNS Values	
IPv6 DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns IPv6 DNS server information. Select **User-Defined** if you have the IPv6 address of a DNS server. Enter the DNS server IPv6 addresses the Zyxel Device passes to the DHCP clients. Select **None** if you do not want to configure IPv6 DNS servers.
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.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

8.3 LAN Static DHCP

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.

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 70   Network Setting > Home Networking > Static DHCP

The following table describes the labels in this screen.

Table 32   Network Setting > Home Networking > Static DHCP

LABEL	DESCRIPTION
Static DHCP Configuration	Click this to add a new 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 have the IP address field editable and change it. Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

If you click **Static DHCP Configuration** in the **Static DHCP** screen or the **Edit** icon next to a static DHCP entry, the following screen displays. Using a static DHCP means a client will always have the same IP address assigned to it by the DHCP server. Assign a fixed IP address to a device by selecting the interface group of this 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 71   Static DHCP: Static DHCP Configuration/Edit

The following table describes the labels in this screen.

Table 33   Static DHCP: Static DHCP Configuration/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the connection between the client and the Zyxel Device. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Group Name	Select the interface group name for which you want to configure static DHCP settings. See Chapter 15 on page 195 for how to create a new interface group.
IP Type	This field displays **IPv4** for the type of the DHCP IP address. At the time of writing, it is not allowed to select other type.

Table 33   Static DHCP: Static DHCP Configuration/Edit (continued)

LABEL	DESCRIPTION
Select Device Info	Select a device or computer from the drop-down list or select **Manual Input** to manually enter a device's MAC address and IP address in the following fields.
MAC Address	If you select **Manual Input**, enter the MAC address of a computer on your LAN.
IP Address	If you select **Manual Input**, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Cancel	Click **Cancel** to exit this screen without saving any changes.
OK	Click **OK** to save your changes.

8.4 UPnP Settings

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. A device can then leave a network smoothly and automatically when it is no longer in use.

See for more information on UPnP.

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.

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

Figure 72   Network Setting > Home Networking > UPnP

The following table describes the labels in this screen.

Table 34   Network Setting > Home Networking > UPnP

| LABEL	DESCRIPTION
UPnP State	
UPnP	Click this switch to enable or disable UPnP. When the switch goes to the right , the function is enabled. Otherwise, it is not. 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	Click this switch to allow UPnP-enabled applications to automatically configure the Zyxel Device so that they can communicate through the Zyxel Device by using NAT traversal. When the switch goes to the right , the function is enabled. Otherwise, it is not. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. The table below displays the NAT port forwarding rules added automatically by UPnP NAT-T.
#	This is the index number of the UPnP NAT-T connection.
Description	This is the description of the UPnP NAT-T connection.
Destination IP Address	This is the IP address of the other connected UPnP-enabled device.
External Port	This is the external port number that identifies the service.
Internal Port	This is the internal port number that identifies the service.
Protocol	This is the transport layer protocol used for the service.
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

8.4.1 Turning on UPnP in Windows 7 Example

This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device in **Network Setting** > **Home Networking** > **UPnP**.
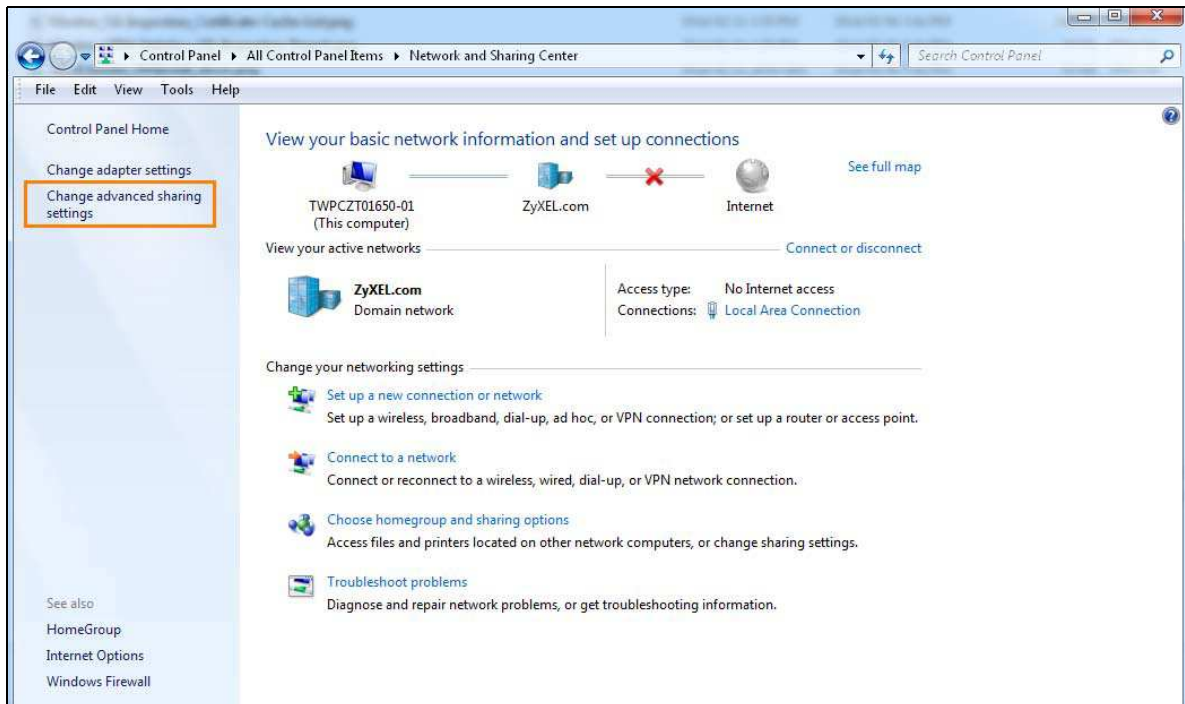
Make sure the computer is connected to a LAN port of the Zyxel Device. Turn on your computer and the Zyxel Device.

1   Click the start icon, **Control Panel** and then the **Network and Sharing Center.**
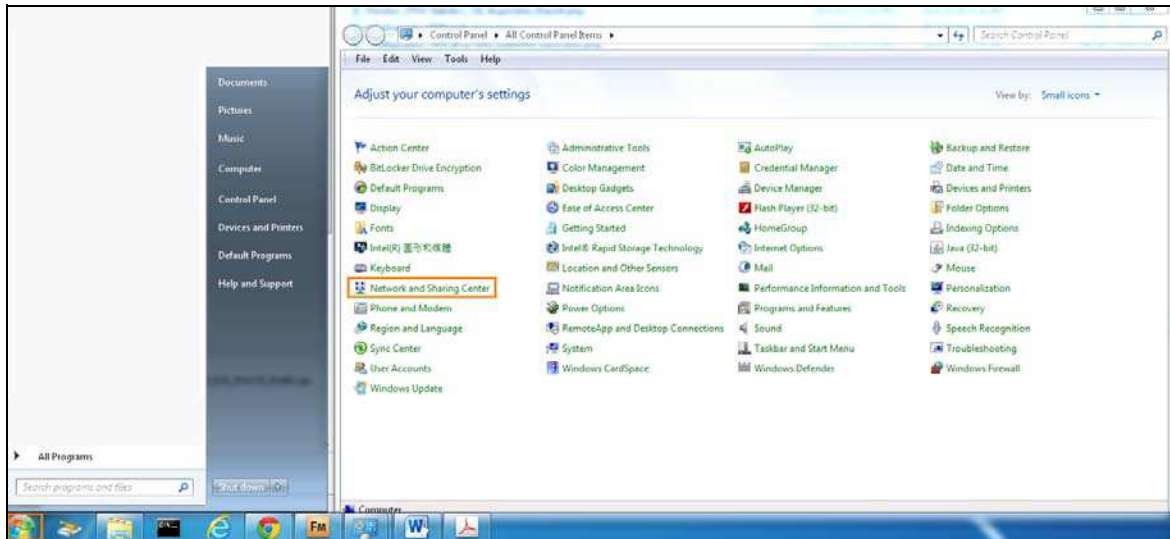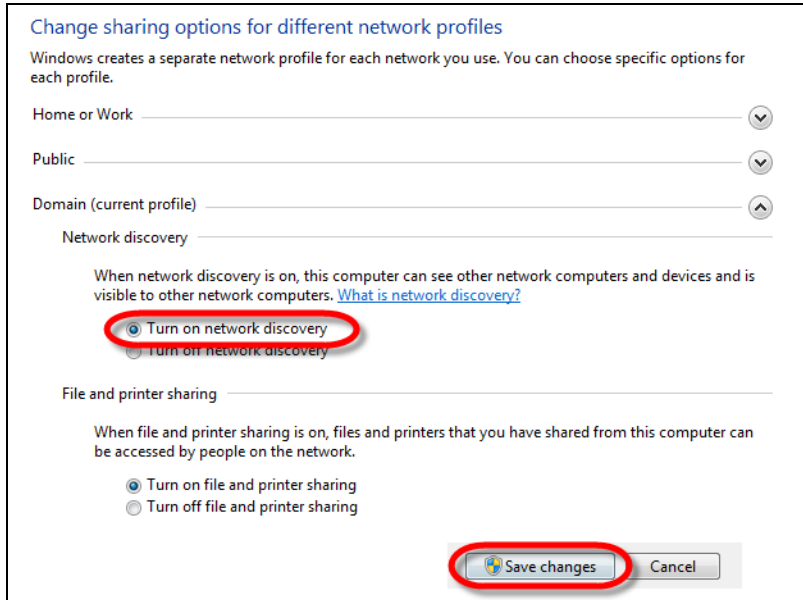
2 Click **Change Advanced Sharing Settings**.

3 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.

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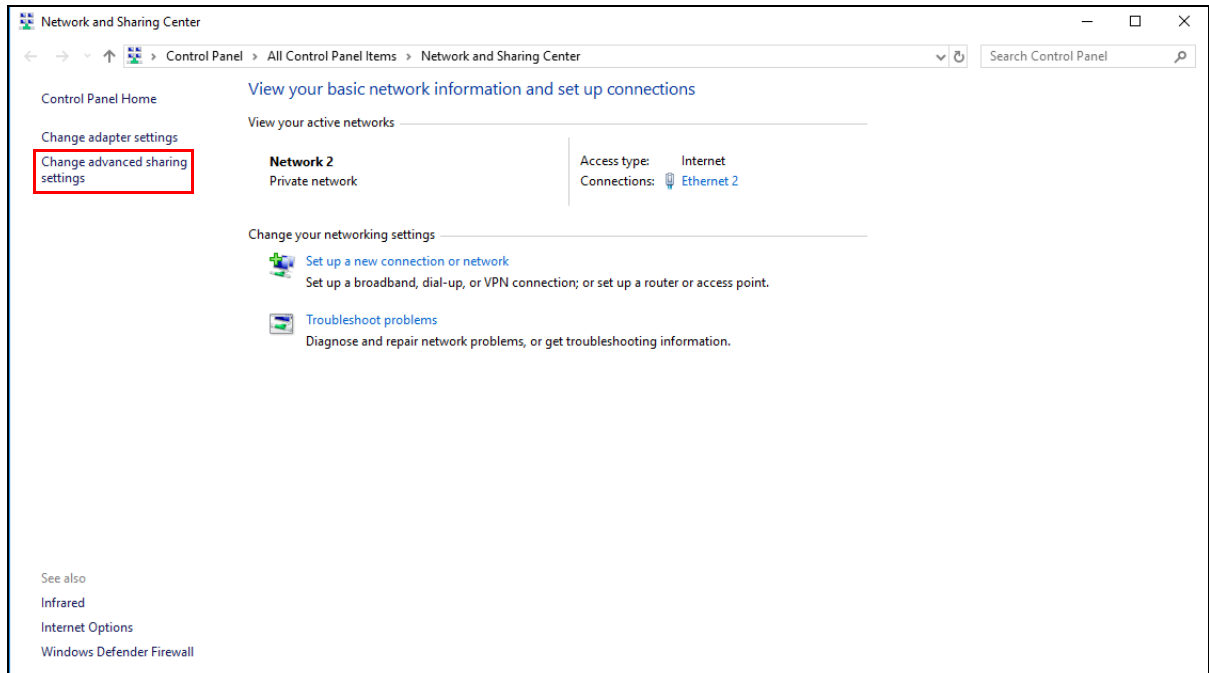
4   Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.
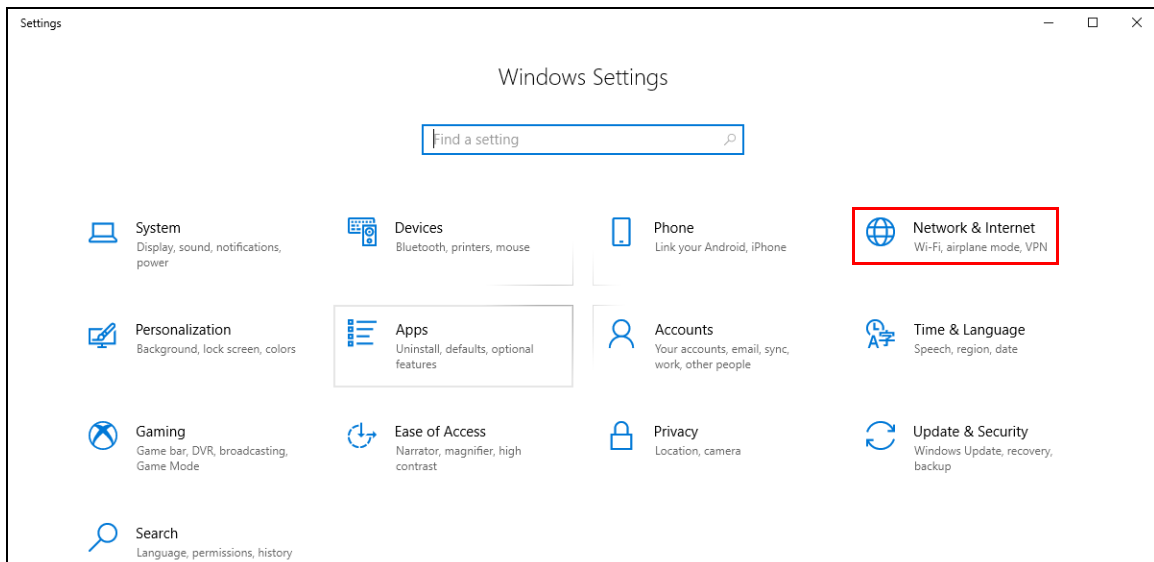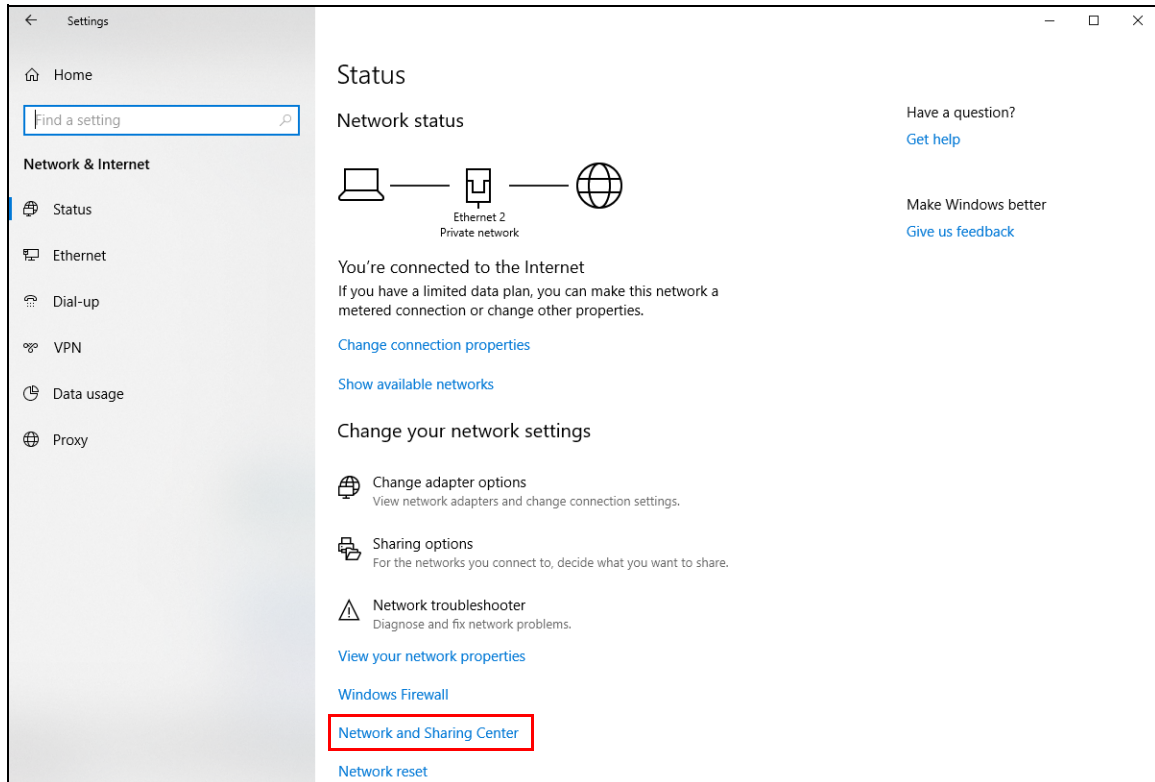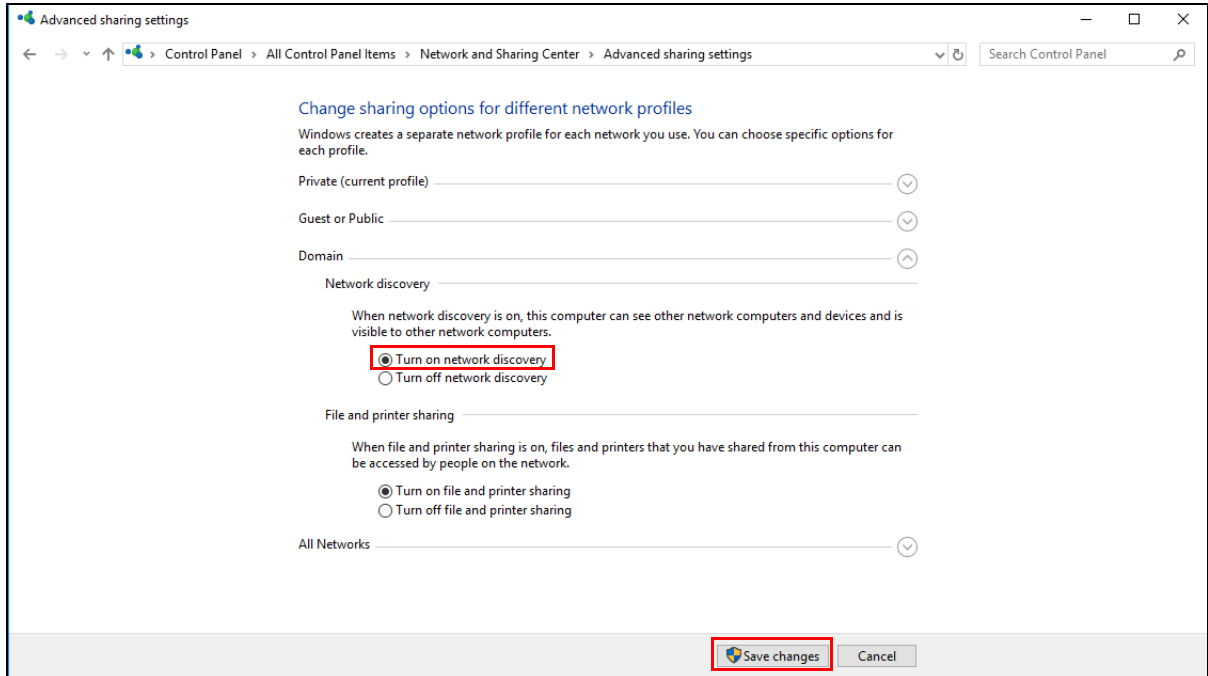
8.5 LAN Additional Subnet

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 via 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 73   Network Setting > Home Networking > Additional Subnet

The following table describes the labels in this screen.

Table 35   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. See Chapter 15 on page 195 for how to create a new interface group.
Active	Click this switch to configure a LAN network for the Zyxel Device. When the switch goes to the right ⬤, the following fields will be configurable. Otherwise, they are not.
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. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not. Your ISP must support Public LAN and static IP.
IPv4 Address	Enter the public IP address provided by your ISP.
Subnet Mask	Enter the public IPv4 subnet mask provided by your ISP.
Offer Public IP by DHCP	Click this switch to enable or disable the Zyxel Device to provide public IP addresses by DHCP server. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Enable ARP Proxy	Click this switch to enable or disable the ARP (Address Resolution Protocol) proxy. When the switch goes to the right ⬤, the function is enabled. Otherwise, it is not.
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

8.6 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 74   Network Setting > Home Networking > STB Vendor ID

The following table describes the labels in this screen.

Table 36   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 exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

8.7 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 device or in its documentation.

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

Figure 75   Network Setting > Home Networking > Wake on LAN

The following table describes the labels in this screen.

Table 37   Network Setting > Home Networking > Wake on LAN

LABEL	DESCRIPTION
Wake by Address	Select **Manual** and enter the IP address or MAC address of the 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 device with the selected IP address then displays in the **MAC Address** field.
IP Address	Enter the IPv4 IP address of the 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 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 device.

8.8 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 76   Network Setting > Home Networking > TFTP Server Name

The following table describes the labels in this screen.

Table 38   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 exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

8.9 Technical Reference

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

8.9.1 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 77   LAN and WAN IP Addresses
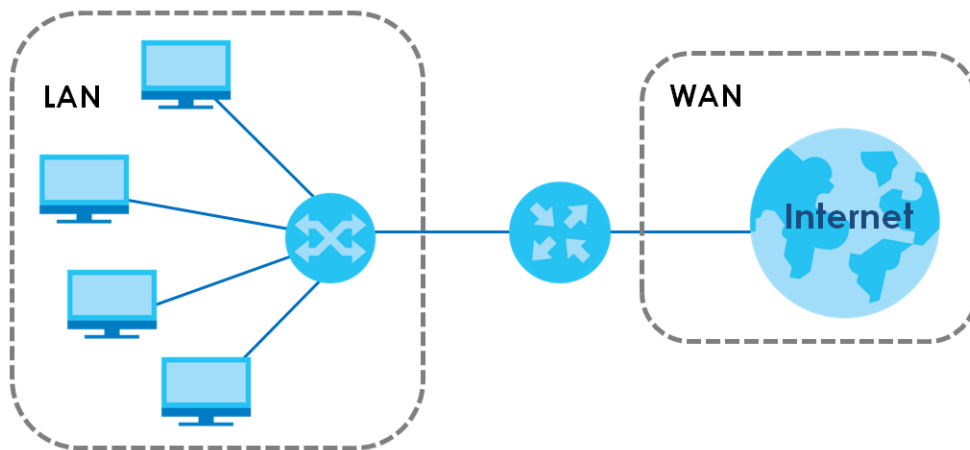
8.9.2 DHCP Setup

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.

8.9.3 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.

8.9.4 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 us 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".

CHAPTER 9
Routing

9.1 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 78   Example of Routing Topology
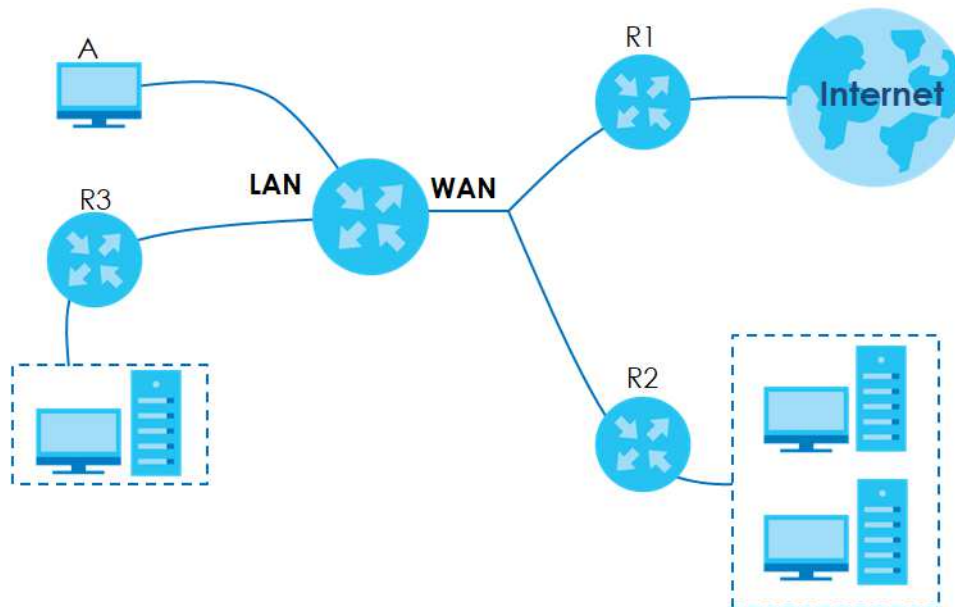
9.2 Static Route Settings

Use this screen to view and configure the 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 available in your home or office network. Click **Network Setting > Routing > Static Route** to open the following screen.

Figure 79   Network Setting > Routing > Static Route

The following table describes the labels in this screen.

Table 39   Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to configure a new static route.
#	This is the index number of the entry.
Status	This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active.
Name	This is the name that describes or identifies this 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 used for this static route.
Modify	Click the **Edit** icon to edit the static route on the Zyxel Device. Click the **Delete** icon to remove a static route from the Zyxel Device. A window displays asking you to confirm that you want to delete the route.

9.2.1 Add/Edit Static Route

Use this screen to add or edit a static route. Click **Add new static route** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

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

Figure 80 Network Setting > Routing > Static Route: Add/Edit

The following table describes the labels in this screen.

Table 40   Network Setting > Routing > Static Route: Add/Edit

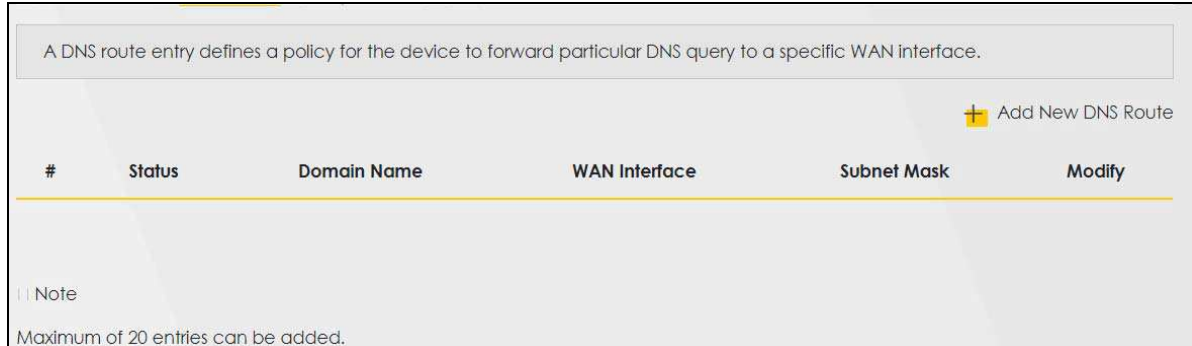| LABEL	DESCRIPTION
Active	Click this switch to enable or disable this static route. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Route Name	Enter a descriptive name for the static route.
IP Type	Select whether your IP type is **IPv4** or **IPv6**.
Destination IP Address	Enter the IPv4 or IPv6 network address of the final destination.
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.
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.
Gateway IP Address	Enter the IP address of the gateway.
Use Interface	Select the WAN interface you want to use for this static route.
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes.

9.3 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.

Note: A maximum of 20 DNS routes can be added.

Click **Network Setting > Routing > DNS Route** to open the following screen.

Figure 81   Network Setting > Routing > DNS Route

The following table describes the labels in this screen.

Table 41   Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to add a new DNS route.
#	This is the index number of a DNS route.
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.
Domain Name	This is the host name or domain name of the DNS route entry.
WAN Interface	This is the WAN connection through which the Zyxel Device forwards DNS requests for this domain name.
Subnet Mask	This is the subnet mask of the DNS route entry.
Modify	Click the **Edit** icon to modify the DNS route. Click the **Delete** icon to delete the DNS route.

9.3.1 Add DNS Route

You can manually add the Zyxel Device's DNS route entry. Click **Add New DNS Route** in the **Network Setting > Routing > DNS Route** screen. The screen shown next appears.

Figure 82   DNS Route Add

The following table describes the labels in this screen.

Table 42   DNS Route Add

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the DNS route. When the switch goes to the right ⬤ , the function is enabled. Otherwise, it is not.
Domain Name	Enter the domain name of the DNS route entry.
Subnet Mask	Enter the subnet mask of the DNS route entry.
WAN Interface	Select the WAN connection through which the Zyxel Device forwards DNS requests for this domain name. **ETHWAN** means the wireless cellular interface.
Cancel	Click this to exit this screen without saving any changes.
OK	Click this to save your changes.

9.4 Policy Route

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. Policy routes allow the Zyxel Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

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 83   Network Setting > Routing > Policy Route

The purpose of a Policy Route is 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 available in your home or office network.

<div style="text-align:right">➕ Add New Policy Route</div>

#	Status	Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	Source Interface	WAN Interface	Modify

The following table describes the labels in this screen.

Table 43   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.
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.

9.4.1 Add/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 84   Policy Route: Add/Edit

The following table describes the labels in this screen.

Table 44   Policy Route: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the policy route. When the switch goes to the right , the function is enabled. Otherwise, it is not.
Route Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source MAC	Enter the source MAC address.
Source Interface (ex: br0 or LAN1~LAN4)	Type the name of the interface from which the matched traffic is sent.
WAN Interface	This field shows **ETHWAN** as the WAN interface through which the traffic is sent.

Table 44   Policy Route: Add/Edit (continued)

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

9.5 RIP Settings

Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

Click **Network Setting > Routing > RIP** to open the **RIP** screen.

Figure 85   Network Setting > Routing > RIP

The following table describes the labels in this screen.

Table 45   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). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
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 check box to activate the settings.
Disable Default Gateway	Select the check box to set the Zyxel Device to not send the route information to the default gateway.
Cancel	Click **Cancel** to exit this screen without saving any changes.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 10
Quality of Service (QoS)

10.1 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.

10.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 10.3 on page 149).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 10.4 on page 151).
- The **Classification Setup** screen lets you add, edit or delete QoS classifiers (Section 10.5 on page 153).
- The **Shaper Setup** screen limits outgoing traffic transmission rate on the selected interface (Section 10.6 on page 158).
- The **Policer Setup** screen lets you control incoming traffic transmission rate and bursts (Section 10.7 on page 159).
- The **Monitor** screen lets you view statistics of QoS on WAN/LAN interface and the status of queues (Section 10.8 on page 162).

10.2 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 three 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.
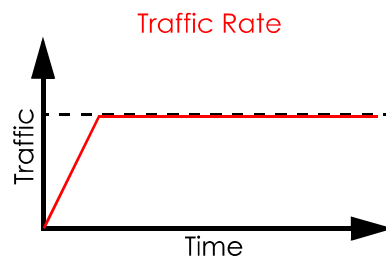
Tagging and Marking

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.
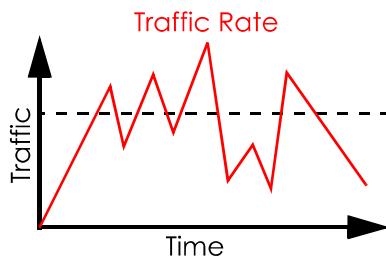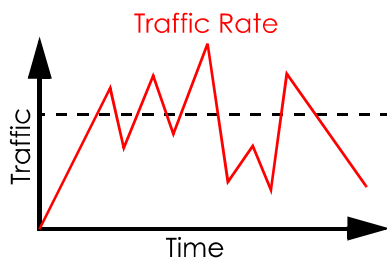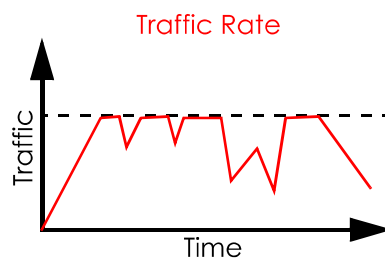

(Before Traffic Shaping)   (After Traffic Shaping)

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.

Traffic Rate   Traffic Rate

(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 10.8 on page 162 for more information on each metering algorithm.

10.3 Quality of Service General Settings

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

Use this screen to enable or disable QoS and set the upstream bandwidth or assign traffic priority. See Section 10.1 on page 147 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.

Figure 86   Network > QoS > General

The following table describes the labels in this screen.

Table 46   Network Setting > QoS > General

LABEL	DESCRIPTION
QoS	Click this switch to enable or disable QoS to improve your network performance. When the switch goes to the right , the function is enabled. Otherwise, it is not.
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 set this number higher than the interfaces' actual transmission speed. The Zyxel Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed.
	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.
LAN Managed Downstream Bandwidth	Enter the amount of downstream bandwidth for the LAN interfaces (including wireless LAN) that you want to allocate using QoS.
	The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection.
	You can also set this number lower than the WAN 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 to the LAN interfaces' maximum supported connection speed.