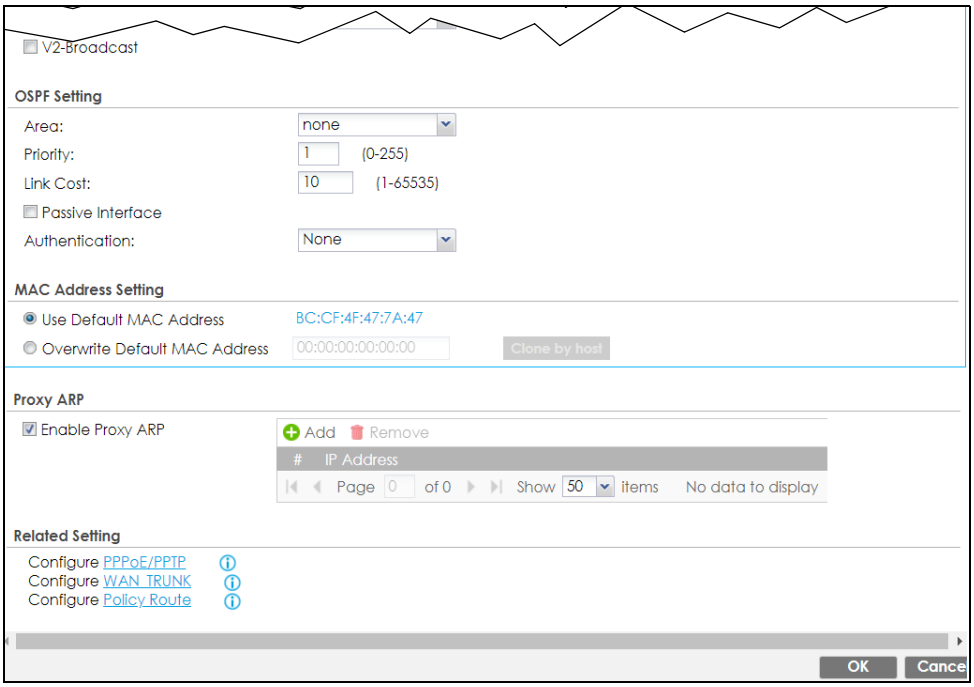


These screen's fields are described in the table below.

Table 94 Configuration > Network > Interface > Ethernet > Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	This field is configurable for the **OPT** interface only. Select to which type of network you will connect this interface. When you select **internal** or **external** the rest of the screen's options automatically adjust to correspond. The Zyxel Device automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic. **internal** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **external** is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. For **general**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Port	This is the name of the Ethernet interface's physical port.
Zone	Select the zone to which this interface is to belong. You use zones to apply security settings such as security policy, IDP, remote management, anti-malware, and application patrol. Make sure to select the correct zone as otherwise traffic may be blocked by a security policy.
MAC Address	This field is read-only. This is the MAC address that the Ethernet interface uses.
Description	Enter a description of this interface. You can use alphanumeric and `( ) +/ :=?!*#@$_%-` characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
IP Address Assignment	These IP address fields configure an IPv4 IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object.
Get Automatically	This option appears when **Interface Type** is **external** or **general**. Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server. You should not select this if the interface is assigned to a VRRP group. See Chapter 36 on page 717.
DHCP Option 60	DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Type a string using up to 64 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./ :;<=>?@\[\\\]^_`{|}~] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.
Use Fixed IP Address	This option appears when **Interface Type** is **external** or **general**. Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This option appears when **Interface Type** is **external** or **general**. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	This option appears when **Interface Type** is **external** or **general**. Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable **IGMP Upstream** on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable **IGMP Downstream** on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Link-Local Address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the interface.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 217 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to check which settings use the entry.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select **N/A** to not use DHCPv6. Select **Client** to set this interface to act as a DHCPv6 client. Select **Server** to set this interface to act as a DHCPv6 server which assigns IP addresses and provides subnet mask, gateway, and DNS server information to clients. Select **Relay** to set this interface to route DHCPv6 requests to the DHCPv6 relay server you specify. The DHCPv6 server(s) may be on another network.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 218 for more information.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 **Client**. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what additional information to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 9.4.5 on page 241 for more information.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device obtained from an uplink router (**Server** is selected) or will advertise to its clients (**Client** is selected).
Interface	When **Relay** is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When **Relay** is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 217 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the Zyxel Device. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device discards the packet and sends an error message to the sender to inform this.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the Zyxel Device to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	This table is available when the **Interface Type** is **internal**. Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The Zyxel Device will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Connectivity Check	These fields appear when **Interface Properties** is **External** or **General**. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Check these addresses	Type one or two domain names or IP addresses for the connectivity check.
Probe Succeeds When	This field applies when you specify two domain names or IP addresses for the connectivity check. Select **any one** if you want the check to pass if at least one of the domain names or IP addresses responds. Select **all** if you want the check to pass only if both domain names or IP addresses respond.
DHCP Setting	This section appears when **Interface Type** is **internal** or **general**.
DHCP	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: **None** - the Zyxel Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the Zyxel Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Zyxel Device is the DHCP server for the network.
	These fields appear if the Zyxel Device is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the Zyxel Device is a **DHCP Server**.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
IP Pool Start Address	Enter the IP address from which the Zyxel Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, use the **Static DHCP Table**. If this field is blank, the **Pool Size** must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the Zyxel Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server, Second DNS Server, Third DNS Server	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. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **Zyxel Device** - the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire. **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 9.4.6 on page 242.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the name of the DHCP option.
Code	This is the code number of the DHCP option.
Type	This is the type of the set value for the DHCP option.
Value	This is the value set for the DHCP option.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
PXE Server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system via a PXE-capable Network Interface Card (NIC). PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Zyxel Device acts as an intermediary between the PXE server and the computers that need boot software. The PXE server must have a public IPv4 address. You must enable **DHCP Server** on the Zyxel Device so that it can receive information from the PXE server.
PXE Boot Loader File	A boot loader is a computer program that loads the operating system for the computer. Type the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is typed, then the client computers cannot boot.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the Zyxel Device assigns to computers connected to the interface. Otherwise, the Zyxel Device assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
RIP Setting	See Section 10.6 on page 322 for more information about RIP.
Enable RIP	Select this to enable RIP in this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the Zyxel Device uses multicasting.
OSPF Setting	See Section 10.7 on page 324 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

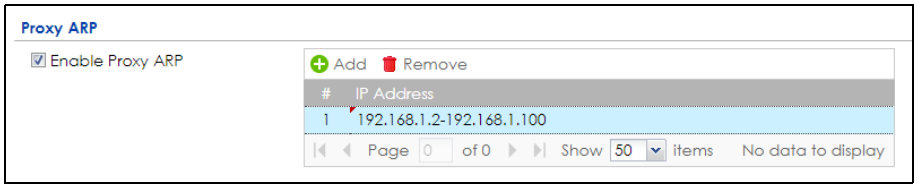
LABEL	DESCRIPTION
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MAC Address Setting	This section appears when **Interface Properties** is **External** or **General**. Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the Zyxel Device uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click **Clone by host** and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Proxy ARP	Proxy ARP is available for external or general interfaces on the Zyxel Device. See Section 9.4.2 on page 238 for more information on Proxy ARP.
Enable Proxy ARP	Select this to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are: • Ethernet • VLAN • Bridge See Section 9.4.2 on page 238 for more information.
Add	Click **Add** to create an **IPv4 Address**, an **IPv4 CIDR** (for example, 192.168.1.1/24) or an **IPv4 Range** (for example, 192.168.1.2-192.168.1.100) as the target IP address. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the **IPv4 Address** is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address. Select an existing entry and click **Remove** to delete that entry. 
Related Setting	

Table 94 Configuration > Network > Interface > Ethernet > Edit (continued)

LABEL	DESCRIPTION
Configure PPPoE/PPTP	Click **PPPoE/PPTP** if this interface's Internet connection uses PPPoE or PPTP or L2TP.
Configure VLAN	Click **VLAN** if you want to configure a VLAN interface for this Ethernet interface.
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can set this interface to be part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the policy route summary screen where you can manually associate traffic with this interface. You must manually configure a policy route to add routing and SNAT settings for an interface with the **Interface Type** set to **general**. You can also configure a policy route to override the default routing and SNAT behavior for an interface with an **Interface Type** of **internal** or **external**.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.4.2 Proxy ARP

An Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a MAC address. An ARP broadcast is sent to all devices in the same Ethernet network to request the MAC address of a target IP address.

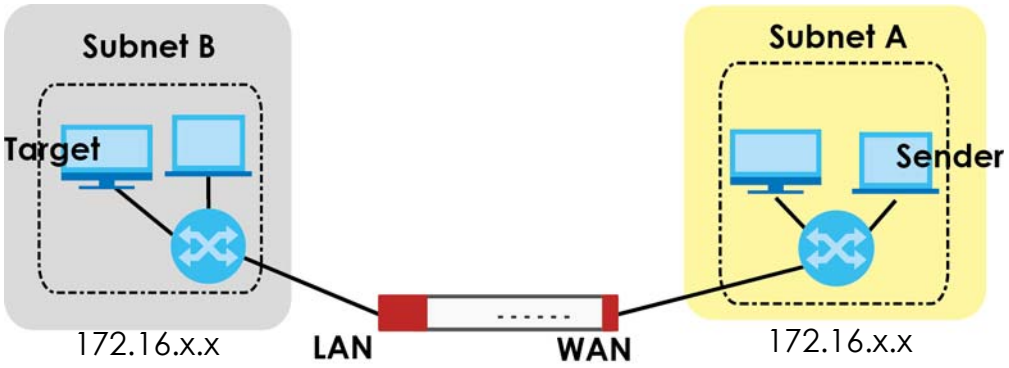
In the following figure, a host in a WAN subnet (A) broadcasts an ARP request to all devices within its network in order to find the MAC address of a target IP address (172.16.x.x). However, the target IP address may be in another subnet (B) that has the same network IP address (172.16.x.x). A router, such as the Zyxel Device, does not forward broadcasts, so the request will not reach its destination.

Enable **Proxy ARP** (RFC 1027) to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are:

- Ethernet
- VLAN
- Bridge

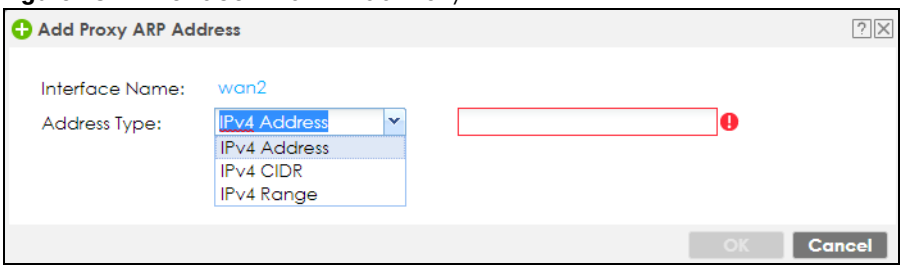
The Zyxel Device sends its external MAC address to the WAN sender as the destination for the target IP address. From then on the sender will send packets containing that target IP address directly to the external interface of the Zyxel Device. The Zyxel Device then forwards the packet to the correct target IP address in its LAN.

Figure 180 Proxy ARP



To allow the Zyxel Device to answer external interface ARP requests on behalf of a device on a supported interface, select the interface, click **Add** or **Edit**, then click **Add** in the **Proxy ARP** section of the screen.

Figure 181 Interface > Edit > Add Proxy ARP



The following table describes labels that can appear in this screen.

Table 95 Interface > Edit > Add Proxy ARP

LABEL	DESCRIPTION
Interface Name	This identifies the interface for which the configuration settings that use it are displayed.
Address Type	Choose **IPv4 Address**, or **IPv4 CIDR** (for example, 192.168.1.1/24) or an **IPv4 Range** (for example, 192.168.1.2-192.168.1.100) and then enter the target IP address information. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the **IPv4 Address** is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.4.3 Virtual Interfaces

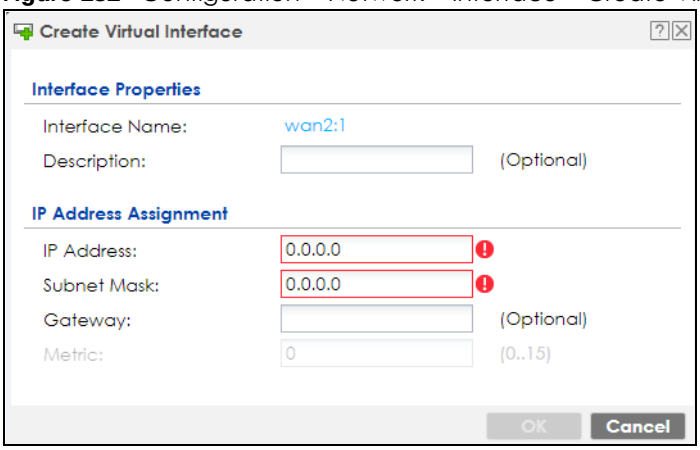
Use virtual interfaces to tell the Zyxel Device where to route packets. Virtual interfaces can also be used in VPN gateways (see Chapter 20 on page 396) and VRRP groups (see Chapter 36 on page 717).

Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, security policies) that apply to the underlying interface automatically apply to the virtual interface as well.

Like other interfaces, virtual interfaces have an IP address, subnet mask, and gateway used to make routing decisions. However, you have to manually specify the IP address and subnet mask; virtual interfaces cannot be DHCP clients. The virtual interface uses the same MTU and bandwidth settings that the underlying interface uses. Unlike other interfaces, virtual interfaces do not provide DHCP services, and they do not verify that the gateway is available.

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click the **Create Virtual Interface** icon in the Ethernet, VLAN, or bridge interface summary screen.

Figure 182 Configuration > Network > Interface > Create Virtual Interface



Each field is described in the table below.

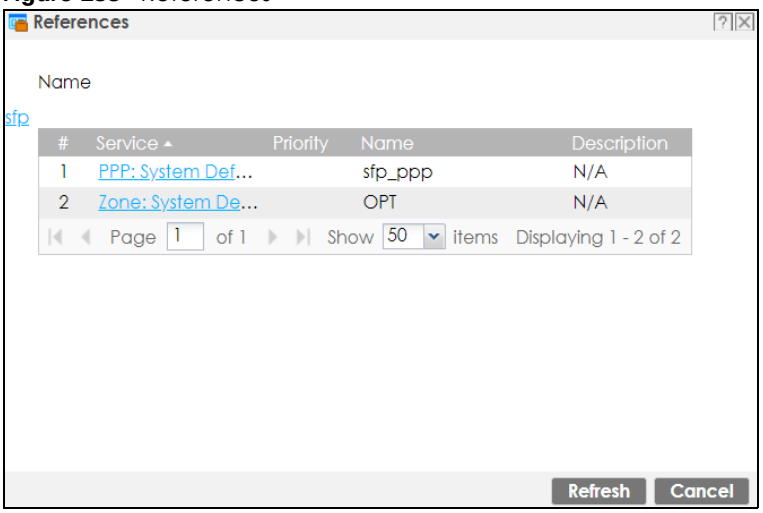
Table 96 Configuration > Network > Interface > Create Virtual Interface

LABEL	DESCRIPTION
Interface Properties	
Interface Name	This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface.
Description	Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( ) + / : = ? ! * # @ $ _ % - characters, and it can be up to 60 characters long.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.4.4 References

When a configuration screen includes an **References** icon, select a configuration object and click **References** to open the **References** screen. This screen displays which configuration settings reference the selected object. The fields shown vary with the type of object.

Figure 183 References



The following table describes labels that can appear in this screen.

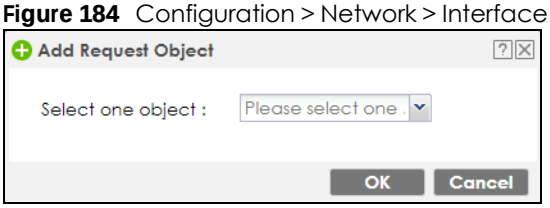
Table 97 References

LABEL	DESCRIPTION
Name	This identifies the object for which the configuration settings that use it are displayed. Click the object's name to display the object's configuration screen in the main window.
#	This field is a sequential value, and it is not associated with any entry.
Service	This is the type of setting that references the selected object. Click a service's name to display the service's configuration screen in the main window.
Priority	If it is applicable, this field lists the referencing configuration item's position in its list, otherwise **N/A** displays.
Name	This field identifies the configuration item that references the object.
Description	If the referencing configuration item has a description configured, it displays here.
Refresh	Click this to update the information in this screen.
Cancel	Click **Cancel** to close the screen.

9.4.5 Add/Edit DHCPv6 Request/Release Options

When you configure an interface as a DHCPv6 server or client, you can additionally add DHCPv6 request or lease options which have the Zyxel Device to add more information in the DHCPv6 packets. To open the screen, click **Configuration > Network > Interface > Ethernet > Edit**, select **DHCPv6 Server** or **DHCPv6 Client** in the **DHCPv6 Setting** section, and then click **Add** in the **DHCPv6 Request Options** or **DHCPv6 Lease Options** table.

Figure 184 Configuration > Network > Interface > Ethernet > Edit > Add DHCPv6 Request/Lease Options

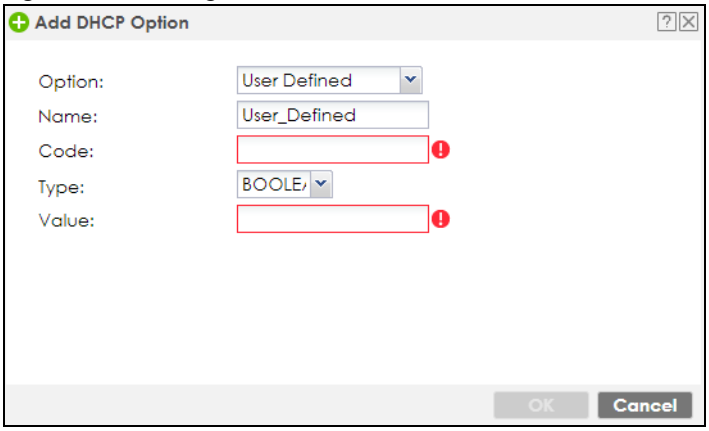


Select a DHCPv6 request or lease object in the **Select one object** field and click **OK** to save it. Click **Cancel** to exit without saving the setting.

9.4.6 Add/Edit DHCP Extended Options

When you configure an interface as a DHCPv4 server, you can additionally add DHCP extended options which have the Zyxel Device to add more information in the DHCP packets. The available fields vary depending on the DHCP option you select in this screen. To open the screen, click **Configuration > Network > Interface > Ethernet > Edit**, select **DHCP Server** in the **DHCP Setting** section, and then click **Add** or **Edit** in the **Extended Options** table.

Figure 185 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options



The following table describes labels that can appear in this screen.

Table 98 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
Option	Select which DHCP option that you want to add in the DHCP packets sent through the interface. See the next table for more information.
Name	This field displays the name of the selected DHCP option. If you selected **User Defined** in the **Option** field, enter a descriptive name to identify the DHCP option. You can enter up to 16 characters ("a-z", "A-Z, "0-9", "-", and "_") with no spaces allowed. The first character must be alphabetical (a-z, A-Z).
Code	This field displays the code number of the selected DHCP option. If you selected **User Defined** in the **Option** field, enter a number for the option. This field is mandatory.
Type	This is the type of the selected DHCP option. If you selected **User Defined** in the **Option** field, select an appropriate type for the value that you will enter in the next field. Only advanced users should configure **User Defined**. Misconfiguration could result in interface lockout.
Value	Enter the value for the selected DHCP option. For example, if you selected **TFTP Server Name (66)** and the type is **TEXT**, enter the DNS domain name of a TFTP server here. This field is mandatory.
First IP Address, Second IP Address, Third IP Address	If you selected **Time Server (4)**, **NTP Server (41)**, **SIP Server (120)**, **CAPWAP AC (138)**, or **TFTP Server (150)**, you have to enter at least one IP address of the corresponding servers in these fields. The servers should be listed in order of your preference.
First Enterprise ID, Second Enterprise ID	If you selected **VIVC (124)** or **VIVS (125)**, you have to enter at least one vendor's 32-bit enterprise number in these fields. An enterprise number is a unique number that identifies a company.
First Class, Second Class	If you selected **VIVC (124)**, enter the details of the hardware configuration of the host on which the client is running, or of industry consortium compliance.
First Information, Second Information	If you selected **VIVS (125)**, enter additional information for the corresponding enterprise number in these fields.

Table 98 Configuration > Network > Interface > Ethernet > Edit > Add/Edit Extended Options

LABEL	DESCRIPTION
OK	Click this to close this screen and update the settings to the previous Edit screen.
Cancel	Click **Cancel** to close the screen.

The following table lists the available DHCP extended options (defined in RFCs) on the Zyxel Device. See RFCs for more information.

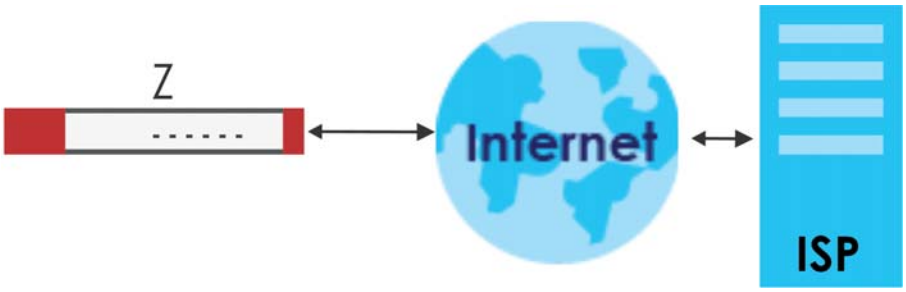
Table 99 DHCP Extended Options

OPTION NAME	CODE	DESCRIPTION
Time Offset	2	This option specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Time Server	4	This option specifies a list of Time servers available to the client.
NTP Server	42	This option specifies a list of the NTP servers available to the client by IP address.
TFTP Server Name	66	This option is used to identify a TFTP server when the "sname" field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
Bootfile	67	This option is used to identify a bootfile when the "file" field in the DHCP header has been used for DHCP options. The minimum length of the value is 1.
SIP Server	120	This option carries either an IPv4 address or a DNS domain name to be used by the SIP client to locate a SIP server.
VIVC	124	Vendor-Identifying Vendor Class option A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs.
VIVS	125	Vendor-Identifying Vendor-Specific option DHCP clients and servers may use this option to exchange vendor-specific information.
CAPWAP AC	138	CAPWAP Access Controller addresses option The Control And Provisioning of Wireless Access Points Protocol allows a Wireless Termination Point (WTP) to use DHCP to discover the Access Controllers to which it is to connect. This option carries a list of IPv4 addresses indicating one or more CAPWAP ACs available to the WTP.
TFTP Server	150	The option contains one or more IPv4 addresses that the client may use. The current use of this option is for downloading configuration from a VoIP server via TFTP; however, the option may be used for purposes other than contacting a VoIP configuration server.

9.5 PPP Interfaces

Use PPPoE/PPTP/L2TP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP/L2TP software on each computer in the network.

Figure 186 Example: PPPoE/PPTP/L2TP Interfaces



PPPoE/PPTP/L2TP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP/L2TP interfaces and other interfaces.

- You must also configure an ISP account object for the PPPoE/PPTP/L2TP interface to use.

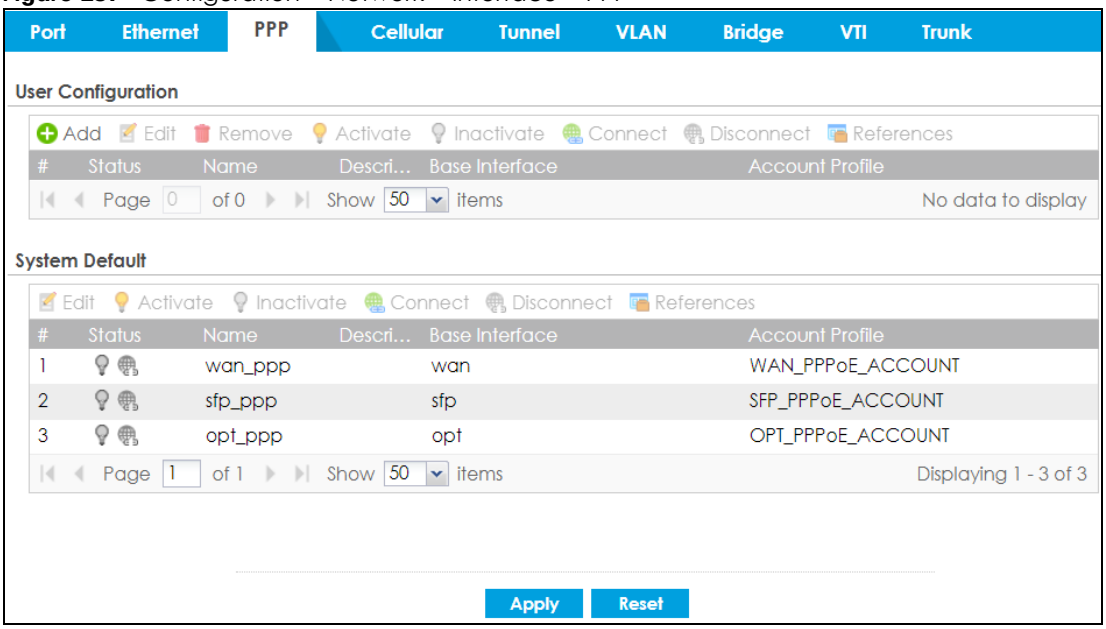
  Each ISP account specifies the protocol (PPPoE or PPTP or L2TP), as well as your ISP account information. If you change ISPs later, you only have to create a new ISP account, not a new PPPoE/PPTP/L2TP interface. You should not have to change any network policies.
- You do not set up the subnet mask or gateway.

  PPPoE/PPTP/L2TP interfaces are interfaces between the Zyxel Device and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the Zyxel Device always treats the ISP as a gateway.

9.5.1 PPP Interface Summary

This screen lists every PPPoE/PPTP/L2TP interface. To access this screen, click **Configuration > Network** > **Interface** > **PPP**.

Figure 187 Configuration > Network > Interface > PPP



Each field is described in the table below.

Table 100 Configuration > Network > Interface > PPP

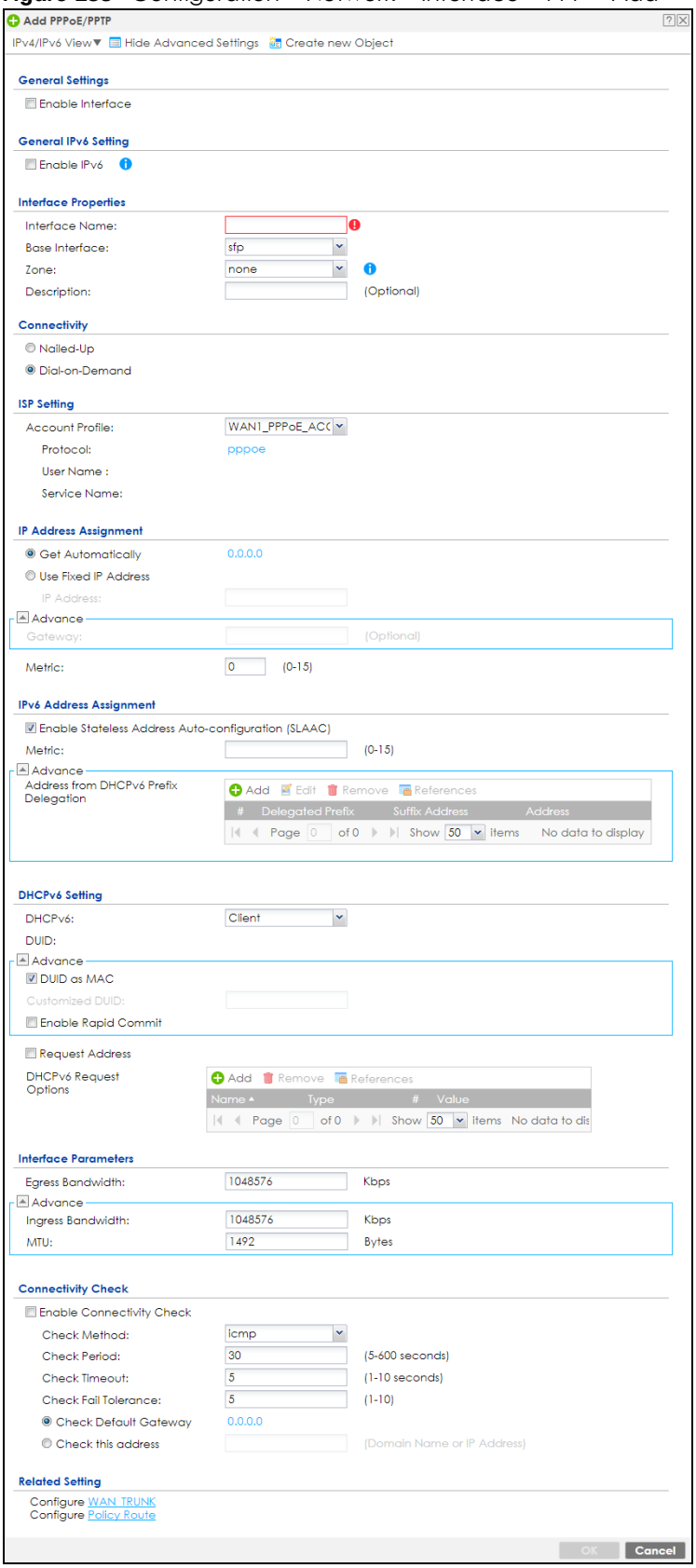
LABEL	DESCRIPTION
User Configuration / System Default	The Zyxel Device comes with the (non-removable) **System Default** PPP interfaces pre-configured. You can create (and delete) **User Configuration** PPP interfaces. **System Default** PPP interfaces vary by model.
Add	Click this to create a new user-configured PPP interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured PPP interface, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an interface, select it and click **Connect**. You might use this in testing the interface or to manually establish the connection for a **Dial-on-Demand** PPPoE/PPTP interface.
Disconnect	To disconnect an interface, select it and click **Disconnect**. You might use this in testing the interface.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Description	This field displays the description of the interface.
Base Interface	This field displays the interface on the top of which the PPPoE/PPTP/L2TP interface is.
Account Profile	This field displays the ISP account used by this PPPoE/PPTP interface.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

9.5.2 PPP Interface Add or Edit

Note: You have to set up an ISP account before you create a PPPoE/PPTP/L2TP interface.

This screen lets you configure a PPPoE or PPTP or L2TP interface. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure PPP interfaces used for your IPv6 networks on this screen. To access this screen, click the **Add** icon or an **Edit** icon in the PPP Interface screen.

Figure 188 Configuration > Network > Interface > PPP > Add



Each field is explained in the following table.

Table 101 Configuration > Network > Interface > PPP > Add

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create an ISP Account or a DHCPv6 request object that you may use for the ISP or DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Name	Specify a name for the interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.
Base Interface	Select the interface upon which this PPP interface is built. Note: Multiple PPP interfaces can use the same base interface.
Zone	Select the zone to which this PPP interface belongs. The zone determines the security settings the Zyxel Device uses for the interface.
Description	Enter a description of this interface. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
Connectivity	
Nailed-Up	Select this if the PPPoE/PPTP/L2TP connection should always be up. Clear this to have the Zyxel Device establish the PPPoE/PPTP/L2TP connection only when there is traffic. You might use this option if a lot of traffic needs to go through the interface or it does not cost extra to keep the connection up all the time.
Dial-on-Demand	Select this to have the Zyxel Device establish the PPPoE/PPTP/L2TP connection only when there is traffic. You might use this option if there is little traffic through the interface or if it costs money to keep the connection available.
ISP Setting	
Account Profile	Select the ISP account that this PPPoE/PPTP/L2TP interface uses. The drop-down box lists ISP accounts by name. Use **Create new Object** if you need to configure a new ISP account (see Chapter 35 on page 710 for details).
Protocol	This field is read-only. It displays the protocol specified in the ISP account.
User Name	This field is read-only. It displays the user name for the ISP account.
Service Name	This field is read-only. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP.
IP Address Assignment	Click **Show Advanced Settings** to display more settings. Click **Hide Advanced Settings** to display fewer settings.
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP/L2TP interfaces.
Use Fixed IP Address	Select this if you want to specify the IP address manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.

Table 101 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (the ISP) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 217 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select **Client** to obtain an IP address and DNS information from the service provider for the interface. Otherwise, select **N/A** to disable the function.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 218 for more information.

Table 101 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Request Address	Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options	Use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server.
Add	Click this to create an entry in this table. See Section 9.4.6 on page 242 for more information.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
Name	This field displays the name of the DHCPv6 request object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device will advertise to its clients.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.

Table 101 Configuration > Network > Interface > PPP > Add (continued)

LABEL	DESCRIPTION
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.6 Cellular Configuration Screen

Mobile broadband is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

Note: The actual data rate you obtain varies depending on the mobile broadband device you use, the signal strength to the service provider's base station, and so on.

You can configure how the Zyxel Device's mobile broadband device connects to a network (refer to Section 9.6.1 on page 253):

- You can set the mobile broadband device to connect only to the home network, which is the network to which you are originally subscribed.
- You can set the mobile broadband device to connect to other networks if the signal strength of the home network is too low or it is unavailable.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

4G

4G is the fourth generation of the mobile telecommunications technology and a successor of 3G. Both the WiMAX and Long Term Evolution (LTE) standards are the 4G candidate systems. 4G only supports all-IP-based packet-switched telephony services and is required to offer Gigabit speed access.

Note: The actual data rate you obtain varies depending on your mobile environment. The environmental factors may include the number of mobile devices which are currently connected to the mobile network, the signal strength to the mobile network, and so on.

See the following table for a comparison between 2G, 2.5G, 2.75G, 3G and 4G wireless technologies.

Table 102 2G, 2.5G, 2.75G, 3G, 3.5G and 4G Wireless Technologies

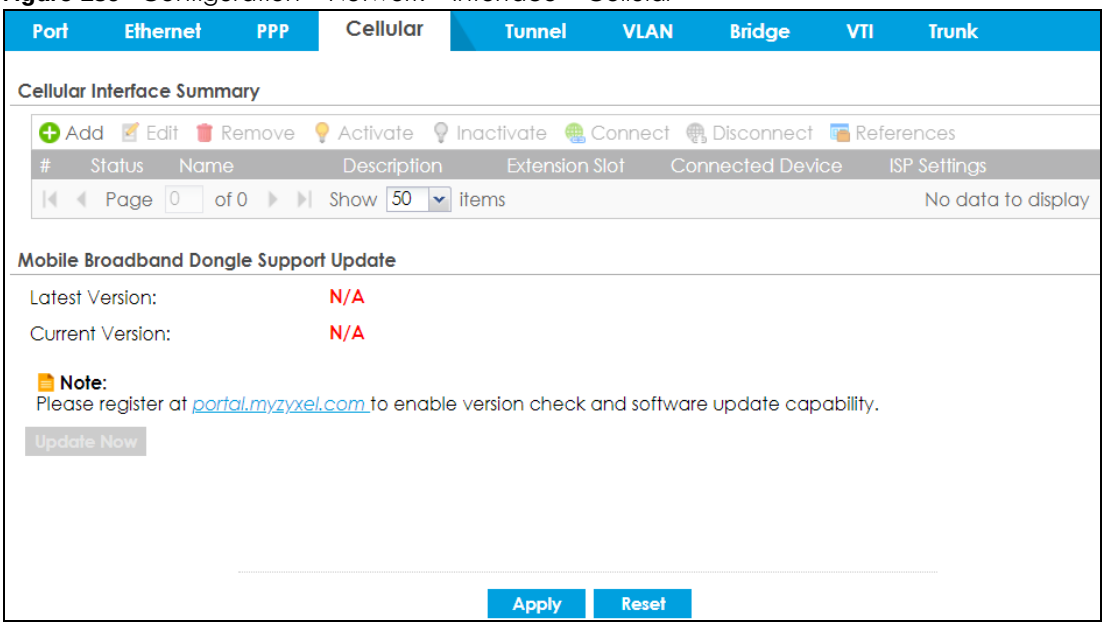
NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.	CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		
4G/LTE	Packet-switched	The LTE (Long Term Evolution) standard is based on the GSM and UMTS network technologies.		Fast

To change your mobile broadband WAN settings, click **Configuration > Network > Interface** > **Cellular**.

Note: Install (or connect) a compatible mobile broadband USB device to use a cellular connection.

Note: The WAN IP addresses of a Zyxel Device with multiple WAN interfaces must be on different subnets.

Figure 189 Configuration > Network > Interface > Cellular



The following table describes the labels in this screen.

Table 103 Configuration > Network > Interface > Cellular

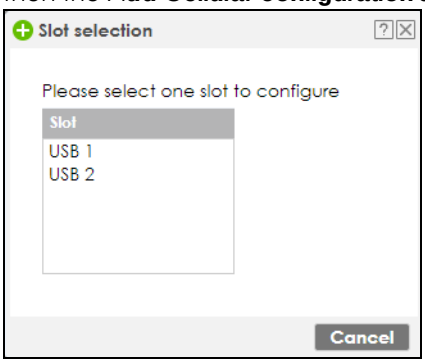
LABEL	DESCRIPTION
Add	Click this to create a new cellular interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an interface, select it and click **Connect**. You might use this in testing the interface or to manually establish the connection.
Disconnect	To disconnect an interface, select it and click **Disconnect**. You might use this in testing the interface.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the interface.
Description	This field displays the description of the interface.
Extension Slot	This field displays where the entry's cellular card is located.
Connected Device	This field displays the name of the cellular card.
ISP Settings	This field displays the profile of ISP settings that this cellular interface is set to use.
Mobile Broadband Dongle Support	You should have registered your Zyxel Device at myZyxel. myZyxel hosts a list of supported mobile broadband dongle devices. You should have an Internet connection to access this website.

Table 103 Configuration > Network > Interface > Cellular (continued)

LABEL	DESCRIPTION
Latest Version	This displays the latest supported mobile broadband dongle list version number.
Current Version	This displays the currently supported (by the Zyxel Device) mobile broadband dongle list version number.
Update Now	If the latest version number is greater than the current version number, then click this button to download the latest list of supported mobile broadband dongle devices to the Zyxel Device.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

9.6.1 Cellular Choose Slot

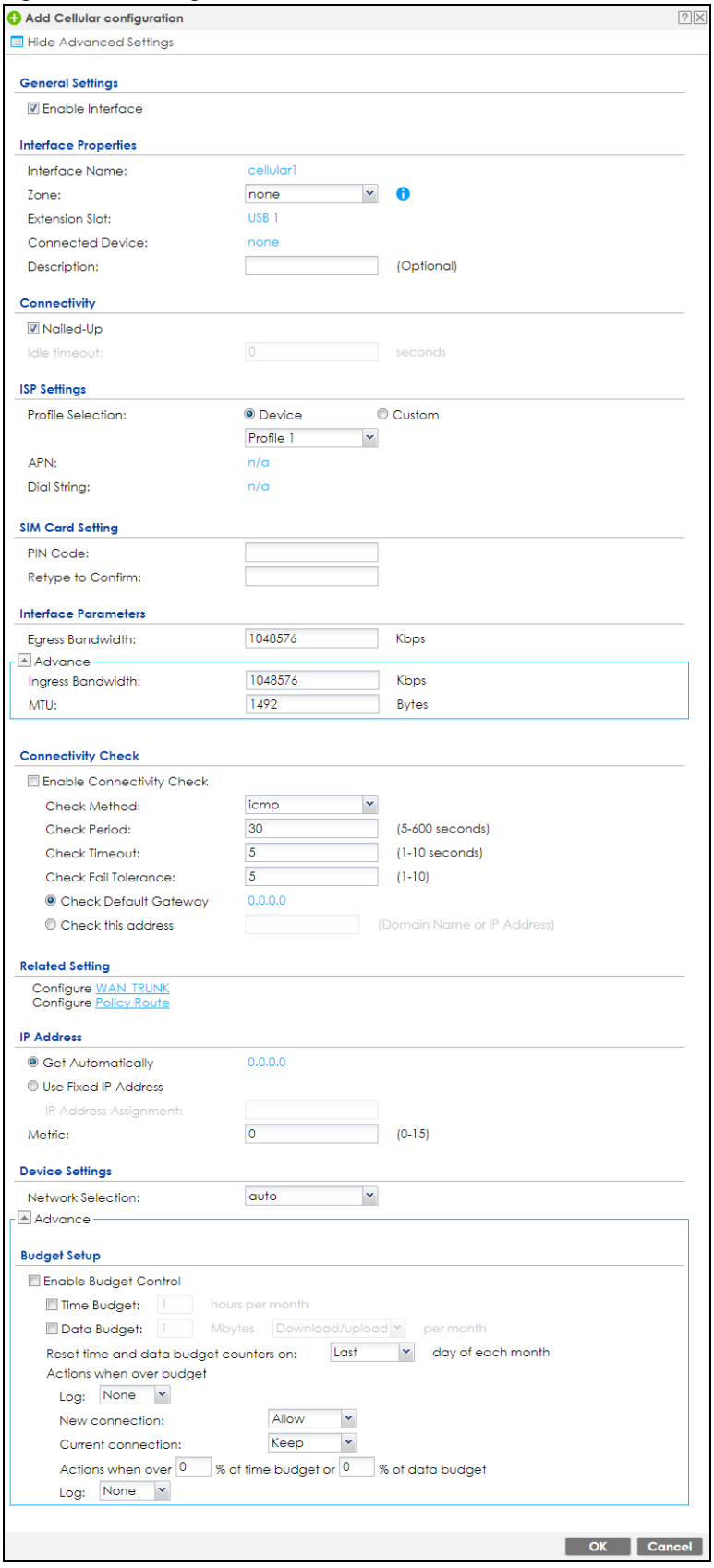
To change your mobile broadband settings, click **Configuration > Network > Interface** > **Cellular > Add** (or **Edit**). In the pop-up window that displays, select the slot that contains the mobile broadband device, then the A**dd Cellular configuration** screen displays.



9.6.2 Add / Edit Cellular Configuration

This screen displays after you select the slot that contains the mobile broadband device in the previous pop-up window.

Figure 190 Configuration > Network > Interface > Cellular > Add / Edit



The following table describes the labels in this screen.

Table 104 Configuration > Network > Interface > Cellular > Add / Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable Interface	Select this option to turn on this interface.
Interface Properties	
Interface Name	Select a name for the interface.
Zone	Select the zone to which you want the cellular interface to belong. The zone determines the security settings the Zyxel Device uses for the interface.
Extension Slot	This is the USB slot that you are configuring for use with a mobile broadband card.
Connected Device	This displays the manufacturer and model name of your mobile broadband card if you inserted one in the Zyxel Device. Otherwise, it displays **none**.
Description	Enter a description of this interface. You can use alphanumeric and `( ) + / : = ? ! * # @ $ _ % -` characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
Connectivity	
Nailed-Up	Select this if the connection should always be up. Clear this to have the Zyxel Device to establish the connection only when there is traffic. You might not nail up the connection if there is little traffic through the interface or if it costs money to keep the connection available.
Idle timeout	This value specifies the time in seconds (0~360) that elapses before the Zyxel Device automatically disconnects from the ISP's server. Zero disables the idle timeout.
ISP Settings	
Profile Selection	Select **Device** to use one of the mobile broadband device's profiles of device settings. Then select the profile (use **Profile 1** unless your ISP instructed you to do otherwise). Select **Custom** to configure your device settings yourself.
APN	This field is read-only if you selected **Device** in the profile selection. Select **Custom** in the profile selection to be able to manually input the APN (Access Point Name) provided by your service provider. This field applies with a GSM or HSDPA mobile broadband card. Enter the APN from your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method. You can enter up to 63 ASCII printable characters. Spaces are allowed.
Dial String	Enter the dial string if your ISP provides a string, which would include the APN, to initialize the mobile broadband card. You can enter up to 63 ASCII printable characters. Spaces are allowed. This field is available only when you insert a GSM mobile broadband card.
Authentication Type	The Zyxel Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **None:** No authentication for outgoing calls. **CHAP** - Your Zyxel Device accepts CHAP requests only. **PAP** - Your Zyxel Device accepts PAP requests only.

Table 104 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
User Name	This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection. If this field is configurable, enter the user name for this mobile broadband card exactly as the service provider gave it to you. You can use 1 ~ 64 alphanumeric and `#:%-_@$./` characters. The first character must be alphanumeric or `-_@$./`. Spaces are not allowed.
Password	This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection and the password is included in the mobile broadband card's profile. If this field is configurable, enter the password for this SIM card exactly as the service provider gave it to you. You can use 0 ~ 63 alphanumeric and `` `~!@#$%^&*()_-+={}|;:'<,>./ `` characters. Spaces are not allowed.
Retype to Confirm	This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection and the password is included in the mobile broadband card's profile. If this field is configurable, re-enter the password for this SIM card exactly as the service provider gave it to you.
SIM Card Setting	
PIN Code	This field displays with a GSM or HSDPA mobile broadband card. A PIN (Personal Identification Number) code is a key to a mobile broadband card. Without the PIN code, you cannot use the mobile broadband card. Enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the mobile broadband card may be blocked by your ISP and you cannot use the account to access the Internet. If your ISP disabled PIN code authentication, enter an arbitrary number.
Retype to Confirm	Type the PIN code again to confirm it.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492.
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.

Table 104 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the policy route summary screen where you can configure a policy route to override the default routing and SNAT behavior for the interface.
IP Address Assignment	
Get Automatically	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address Assignment	Enter the cellular interface's WAN IP address in this field if you selected **Use Fixed IP Address**.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Device Settings	
Band Selection	This field appears if you selected a mobile broadband device that allows you to select the type of network to use. Select the type of mobile broadband service for your mobile broadband connection. If you are unsure what to select, check with your mobile broadband service provider to find the mobile broadband service available to you in your region. Select **auto** to have the card connect to an available network. Choose this option if you do not know what networks are available. You may want to manually specify the type of network to use if you are charged differently for different types of network or you only have one type of network available to you. Select **GPRS / EDGE (GSM) only** to have this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to select this so the Zyxel Device does not spend time looking for a WCDMA network. Select **UMTS / HSDPA (WCDMA) only** to have this interface only use a 3G or 3.5G network (respectively). You may want to do this if you want to make sure the interface does not use the GSM network. Select **LTE only** to have this interface only use a 4G LTE network. This option only appears when a USG dongle for 4G technology is inserted.

Table 104 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Network Selection	Home network is the network to which you are originally subscribed. Select **Home** to have the mobile broadband device connect only to the home network. If the home network is down, the Zyxel Device's mobile broadband Internet connection is also unavailable. Select **Auto** (Default) to allow the mobile broadband device to connect to a network to which you are not subscribed when necessary, for example when the home network is down or another mobile broadband base station's signal is stronger. This is recommended if you need continuous Internet connectivity. If you select this, you may be charged using the rate of a different network.
Budget Setup	
Enable Budget Control	Select this to set a monthly limit for the user account of the installed mobile broadband card. You can set a limit on the total traffic and/or call time. The Zyxel Device takes the actions you specified when a limit is exceeded during the month.
Time Budget	Select this and specify the amount of time (in hours) that the mobile broadband connection can be used within one month. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Data Budget	Select this and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the mobile broadband connection within one month. Select **Download** to set a limit on the downstream traffic (from the ISP to the Zyxel Device). Select **Upload** to set a limit on the upstream traffic (from the Zyxel Device to the ISP). Select **Download/Upload** to set a limit on the total traffic in both directions. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.
Reset time and data budget counters on	Select the date on which the Zyxel Device resets the budget every month. If the date you selected is not available in a month, such as 30th or 31st, the Zyxel Device resets the budget on the last day of the month.
Reset time and data budget counters	This button is available only when you enable budget control in this screen. Click this button to reset the time and data budgets immediately. The count starts over with the mobile broadband connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart; so if you configured the time and data budget counters to reset on the second day of the month and you use this button on the first, the time and data budget counters will still reset on the second.
Actions when over budget	Specify the actions the Zyxel Device takes when the time or data limit is exceeded.
Log	Select **None** to not create a log, **Log** to create a log, or **Log-alert** to create an alert log. If you select **Log** or **Log-alert** you can also select **recurring every** to have the Zyxel Device send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
New connection	Select **Allow** to permit new mobile broadband connections or **Disallow** to drop/block new mobile broadband connections.
Current connection	Select **Keep** to maintain an existing mobile broadband connection or **Drop** to disconnect it. You cannot set **New connection** to **Allow** and **Current connection** to **Drop** at the same time. If you set **New connection** to **Disallow** and **Current connection** to **Keep**, the Zyxel Device allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected.
Actions when over % of time budget or % of data budget	Specify the actions the Zyxel Device takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the Zyxel Device resets the statistics.

Table 104 Configuration > Network > Interface > Cellular > Add / Edit (continued)

LABEL	DESCRIPTION
Log	Select **None** to not create a log when the Zyxel Device takes this action, **Log** to create a log, or **Log-alert** to create an alert log. If you select **Log** or **Log-alert** you can also select **recurring every** to have the Zyxel Device send a log or alert for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log or alert.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

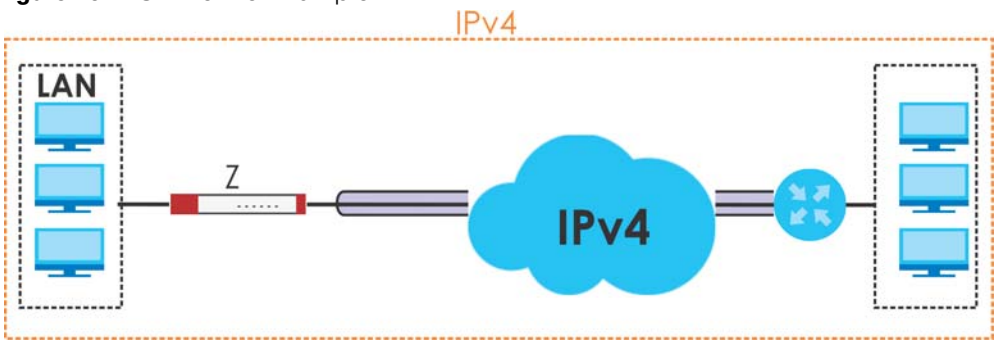
9.7 Tunnel Interfaces

The Zyxel Device uses tunnel interfaces in Generic Routing Encapsulation (GRE), IPv6 in IPv4, and 6to4 tunnels.

GRE Tunneling

GRE tunnels encapsulate a wide variety of network layer protocol packet types inside IP tunnels. A GRE tunnel serves as a virtual point-to-point link between the Zyxel Device and another router over an IPv4 network. At the time of writing, the Zyxel Device only supports GRE tunneling in IPv4 networks.

Figure 191 GRE Tunnel Example



IPv6 Over IPv4 Tunnels

To route traffic between two IPv6 networks over an IPv4 network, an IPv6 over IPv4 tunnel has to be used.

Figure 192 IPv6 over IPv4 Network

On the Zyxel Device, you can either set up a manual IPv6-in-IPv4 tunnel or an automatic 6to4 tunnel. The following describes each method:

IPv6-in-IPv4 Tunneling

Use this mode on the WAN of the Zyxel Device if

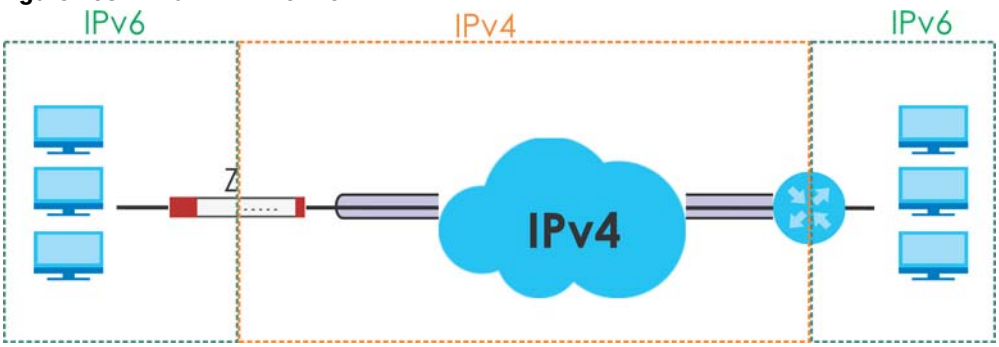
- your Zyxel Device has a public IPv4 IP address given from your ISP,

and

- you want to transmit your IPv6 packets to one and only one remote site whose LAN network is also an IPv6 network.

With this mode, the Zyxel Device encapsulates IPv6 packets within IPv4 packets across the Internet. You must know the WAN IP address of the remote gateway device. This mode is normally used for a site-to-site application such as two branch offices.

Figure 193 IPv6-in-IPv4 Tunnel



In the Zyxel Device, you must also manually configure a policy route for an IPv6-in-IPv4 tunnel to make the tunnel work.

6to4 Tunneling

This mode also enables IPv6 packets to cross IPv4 networks. Unlike IPv6-in-IPv4 tunneling, you do not need to configure a policy route for a 6to4 tunnel. Through your properly pre-configuring the destination router's IP address in the IP address assignments to hosts, the Zyxel Device can automatically forward 6to4 packets to the destination they want to go. A 6to4 relay router is required to route 6to4 packets to a native IPv6 network if the packet's destination do not match your specified criteria.

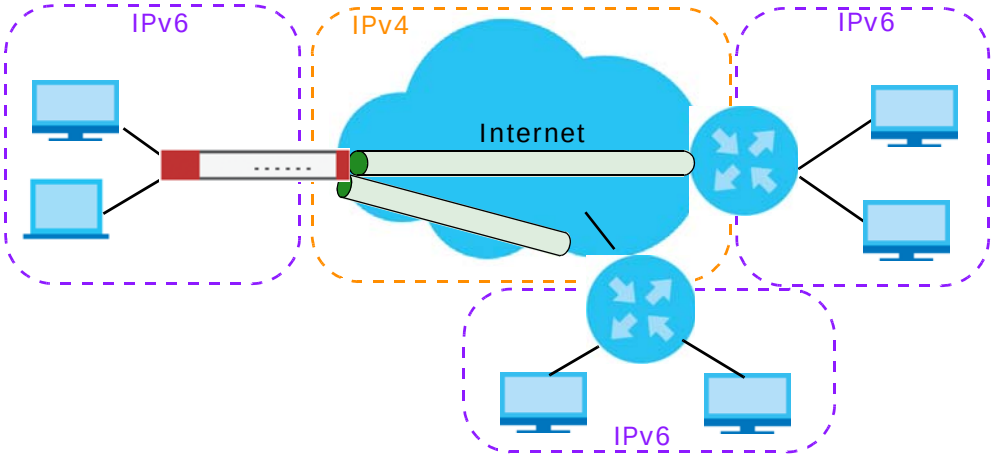
In this mode, the Zyxel Device should get a public IPv4 address for the WAN. The Zyxel Device adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the Zyxel Device removes the IPv4 header from an IPv6 packet when receiving it from the Internet.

An IPv6 address using the 6to4 mode consists of an IPv4 address, the format is as the following:

2002:[a public IPv4 address in hexadecimal]::/48

For example, a public IPv4 address is 202.156.30.41. The converted hexadecimal IP string is ca.9c.1Ee.29. The IPv6 address prefix becomes 2002:ca9c:1e29::/48.

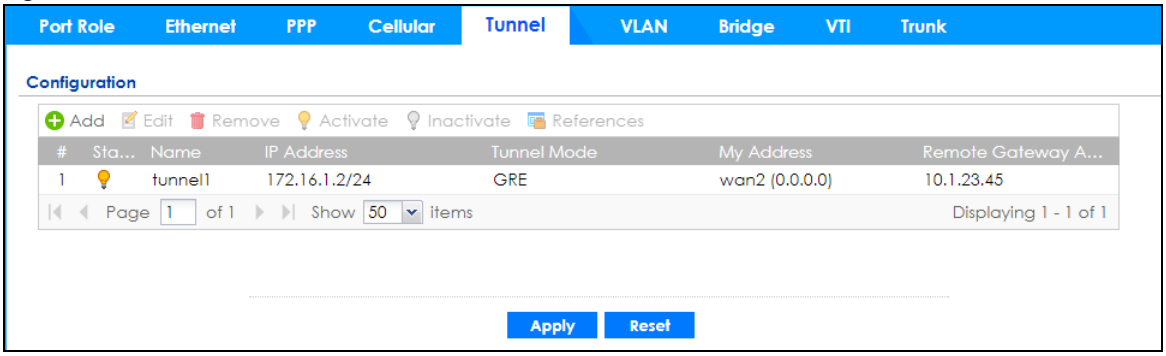
Figure 194 6to4 Tunnel



9.7.1 Configuring a Tunnel

This screen lists the Zyxel Device's configured tunnel interfaces. To access this screen, click **Network** > **Interface** > **Tunnel**.

Figure 195 Network > Interface > Tunnel



Each field is explained in the following table.

Table 105 Network > Interface > Tunnel

LABEL	DESCRIPTION
Add	Click this to create a new GRE tunnel interface.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.

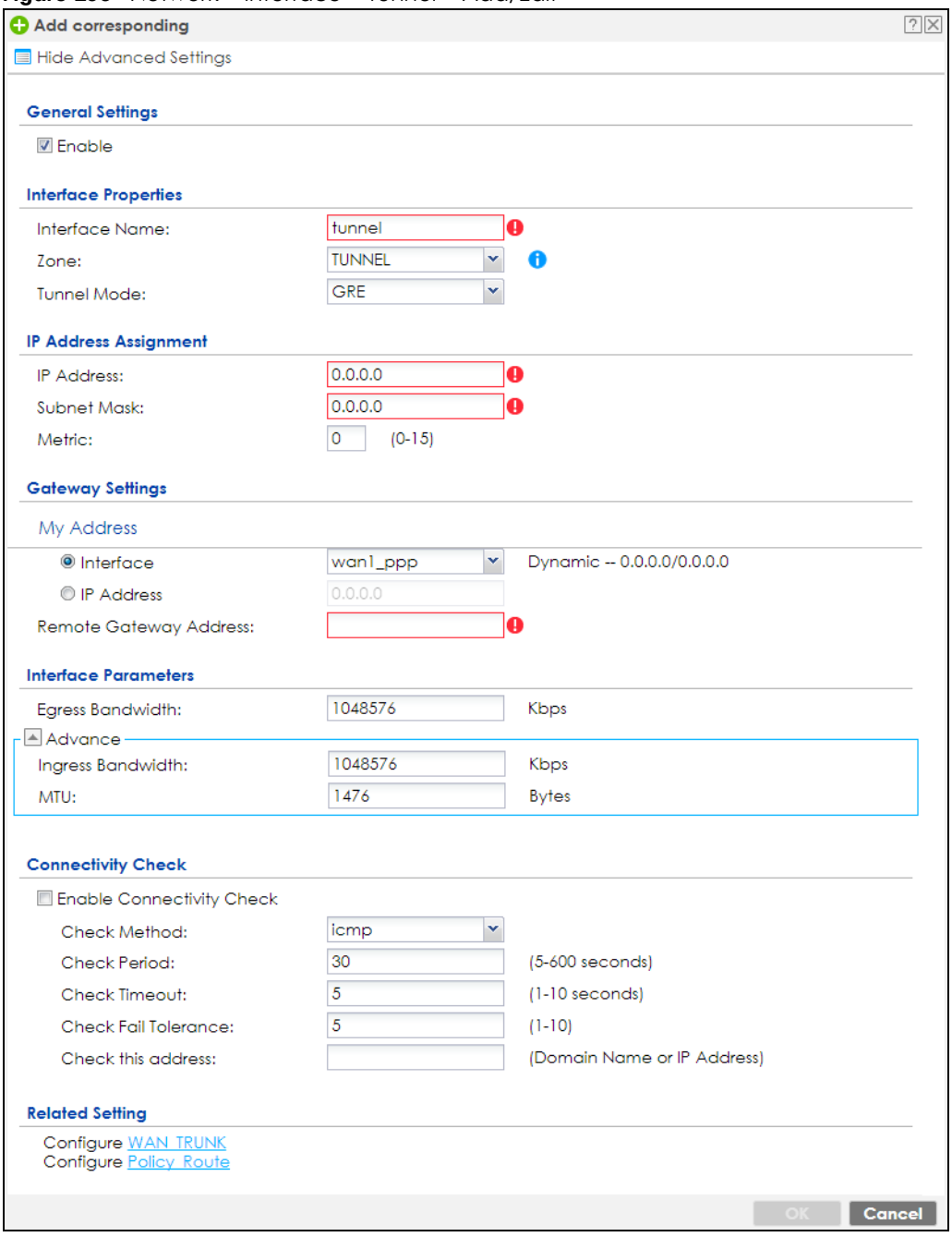
Table 105 Network > Interface > Tunnel (continued)

LABEL	DESCRIPTION
IP Address	This is the IP address of the interface. If the interface is active (and connected), the Zyxel Device tunnels local traffic sent to this IP address to the **Remote Gateway Address**.
Tunnel Mode	This is the tunnel mode of the interface (**GRE**, **IPv6-in-IPv4** or **6to4**). This field also displays the interface's IPv4 IP address and subnet mask if it is a GRE tunnel. Otherwise, it displays the interface's IPv6 IP address and prefix length.
My Address	This is the interface or IP address uses to identify itself to the remote gateway. The Zyxel Device uses this as the source for the packets it tunnels to the remote gateway.
Remote Gateway Address	This is the IP address or domain name of the remote gateway to which this interface tunnels traffic.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to begin configuring this screen afresh.

9.7.2 Tunnel Add or Edit Screen

This screen lets you configure a tunnel interface. Click **Configuration > Network > Interface > Tunnel > Add** (or **Edit**) to open the following screen.

Figure 196 Network > Interface > Tunnel > Add/Edit



Each field is explained in the following table.

Table 106 Network > Interface > Tunnel > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
General Settings	
Enable	Select this to enable this interface. Clear this to disable this interface.
Interface Properties	

Table 106 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Interface Name	This field is read-only if you are editing an existing tunnel interface. Enter the name of the tunnel interface. The format is tunnel*x*, where *x* is 0 - 3. For example, tunnel0.
Zone	Use this field to select the zone to which this interface belongs. This controls what security settings the Zyxel Device applies to this interface.
Tunnel Mode	Select the tunneling protocol of the interface (**GRE**, **IPv6-in-IPv4** or **6to4**). See Section 9.7 on page 259 for more information.
IP Address Assignment	This section is available if you are configuring a GRE tunnel.
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
IPv6 Address Assignment	This section is available if you are configuring an IPv6-in-IPv4 or a 6to4 tunnel.
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
6to4 Tunnel Parameter	This section is available if you are configuring a 6to4 tunnel which encapsulates IPv6 to IPv4 packets.
6to4 Prefix	Enter the IPv6 prefix of a destination network. The Zyxel Device forwards IPv6 packets to the hosts in the matched network. If you enter a prefix starting with 2002, the Zyxel Device will forward the matched packets to the IPv4 IP address converted from the packets' destination address. The IPv4 IP address can be converted from the next 32 bits after the prefix you specified in this field. See 6to4 Tunneling on page 260 for an example. The Zyxel Device forwards the unmatched packets to the specified **Relay Router**.
Relay Router	Enter the IPv4 address of a 6to4 relay router which helps forward packets between 6to4 networks and native IPv6 networks.
Remote Gateway Prefix	Enter the IPv4 network address and network bits of a remote 6to4 gateway, for example, 14.15.0.0/16. This field works if you enter a **6to4 Prefix** not starting with 2002 (2003 for example). The Zyxel Device forwards the matched packets to a remote gateway with the network address you specify here, and the bits converted after the **6to4 Prefix** in the packets. For example, you configure the 6to4 prefix to 2003:A0B::/32 and the remote gateway prefix to 14.15.0.0/16. If a packet's destination is 2003:A0B:1011:5::8, the Zyxel Device forwards the packet to 14.15.16.17, where the network address is 14.15.0.0 and the host address is the remain bits converted from 1011 after the packet's 6to4 prefix (2003:A0B).
Gateway Settings	
My Address	Specify the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. The remote gateway sends traffic to this interface or IP address.

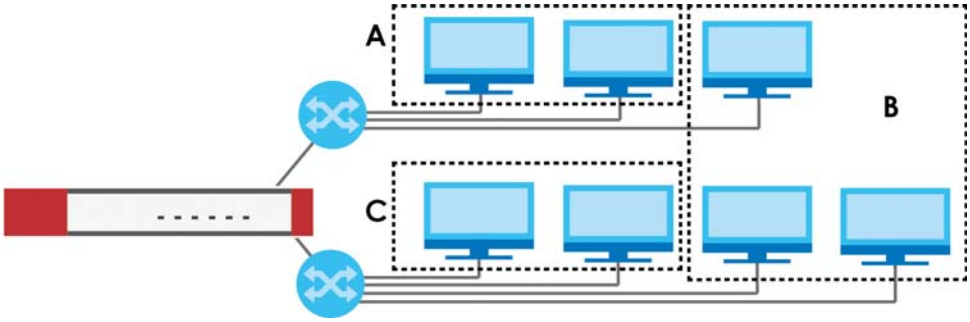
Table 106 Network > Interface > Tunnel > Add/Edit (continued)

LABEL	DESCRIPTION
Remote Gateway Address	Enter the IP address or domain name of the remote gateway to which this interface tunnels traffic. **Automatic** displays in this field if you are configuring a **6to4** tunnel. It means the 6to4 tunnel will help forward packets to the corresponding remote gateway automatically by looking at the packet's destination address.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
Connectivity Check	This section is available if you are configuring a GRE tunnel. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Related Setting	
WAN TRUNK	Click this link to go to a screen where you can configure WAN trunk load balancing.
Policy Route	Click this link to go to the screen where you can manually configure a policy route to associate traffic with this interface.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.8 VLAN Interfaces

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

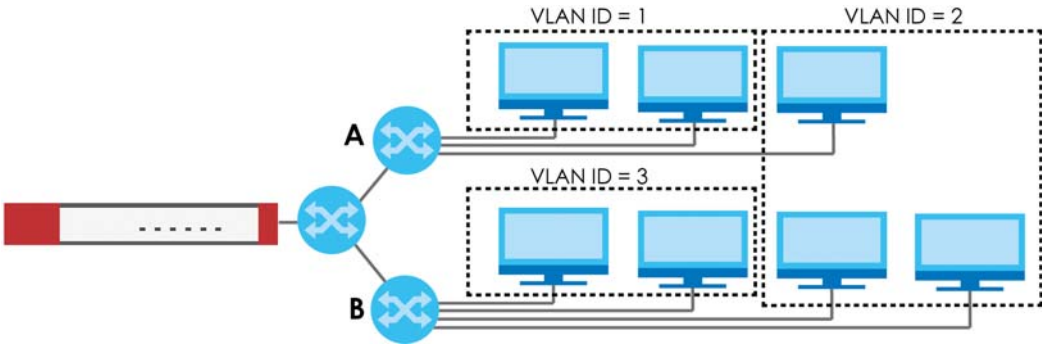
Figure 197 Example: Before VLAN



In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

Alternatively, you can divide the physical networks into three VLANs.

Figure 198 Example: After VLAN



Each VLAN is a separate network with separate IP addresses, subnet masks, and gateways. Each VLAN also has a unique identification number (ID). The ID is a 12-bit value that is stored in the MAC header. The VLANs are connected to switches, and the switches are connected to the router. (If one switch has enough connections for the entire network, the network does not need switches **A** and **B**.)

- Traffic inside each VLAN is layer-2 communication (data link layer, MAC addresses). It is handled by the switches. As a result, the new switch is required to handle traffic inside VLAN 2. Traffic is only broadcast inside each VLAN, not each physical network.
- Traffic between VLANs (or between a VLAN and another type of network) is layer-3 communication (network layer, IP addresses). It is handled by the router.

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.

- Better manageability - You can align network policies more appropriately for users. For example, you can create different content filtering rules for each VLAN (each department in the example above), and you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

In this example, the new switch handles the following types of traffic:

- Inside VLAN 2.
- Between the router and VLAN 1.
- Between the router and VLAN 2.
- Between the router and VLAN 3.

VLAN Interfaces Overview

In the Zyxel Device, each VLAN is called a VLAN interface. As a router, the Zyxel Device routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface. All traffic for each VLAN interface can go through only one Ethernet interface, though each Ethernet interface can have one or more VLAN interfaces.

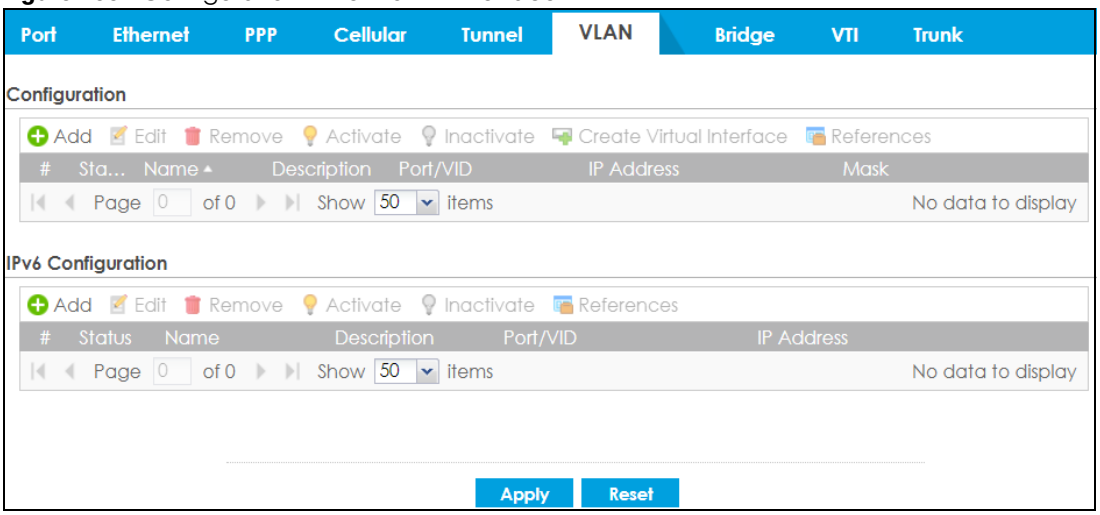
Note: Each VLAN interface is created on top of only one Ethernet interface.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

9.8.1 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure VLAN interfaces used for your IPv6 networks on this screen. To access this screen, click **Configuration > Network > Interface** > **VLAN**.

Figure 199 Configuration > Network > Interface > VLAN



Each field is explained in the following table.

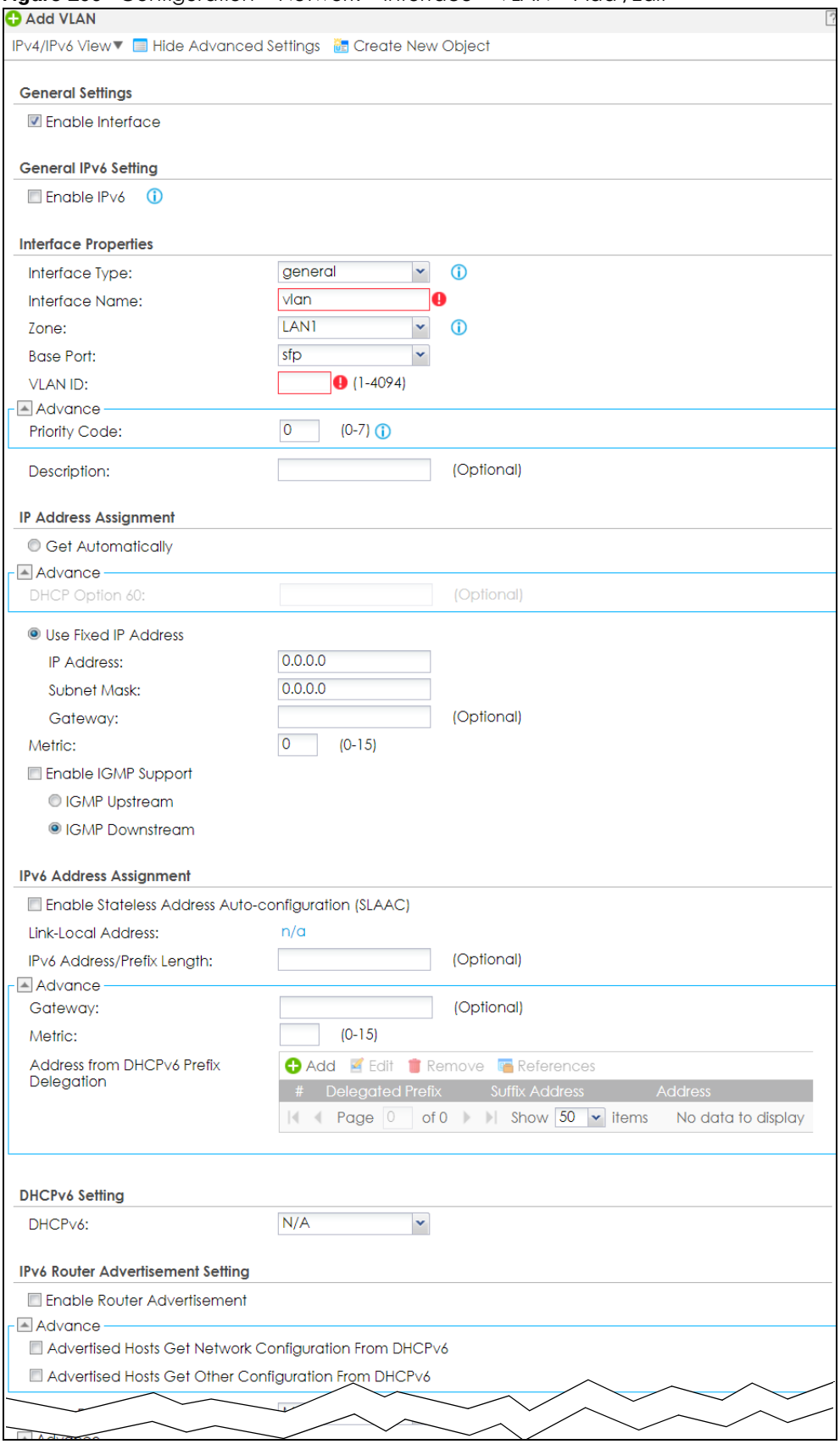
Table 107 Configuration > Network > Interface > VLAN

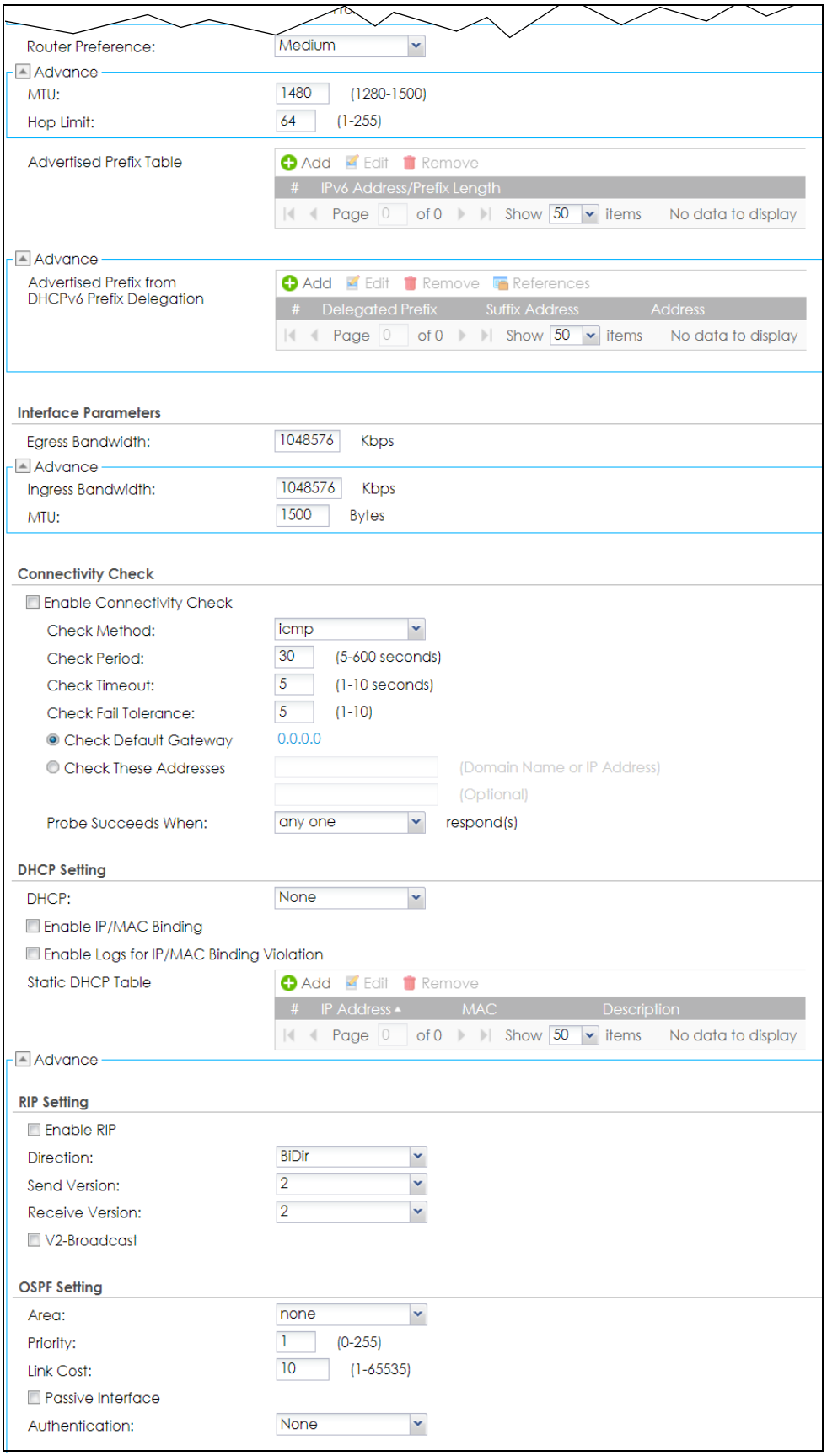
LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the **Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click **Create Virtual Interface**.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
Description	This field displays the description of the interface.
Port/VID	For VLAN interfaces, this field displays • the Ethernet interface on which the VLAN interface is created • the VLAN ID For virtual interfaces, this field is blank.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Mask	This field displays the interface's subnet mask in dot decimal notation.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

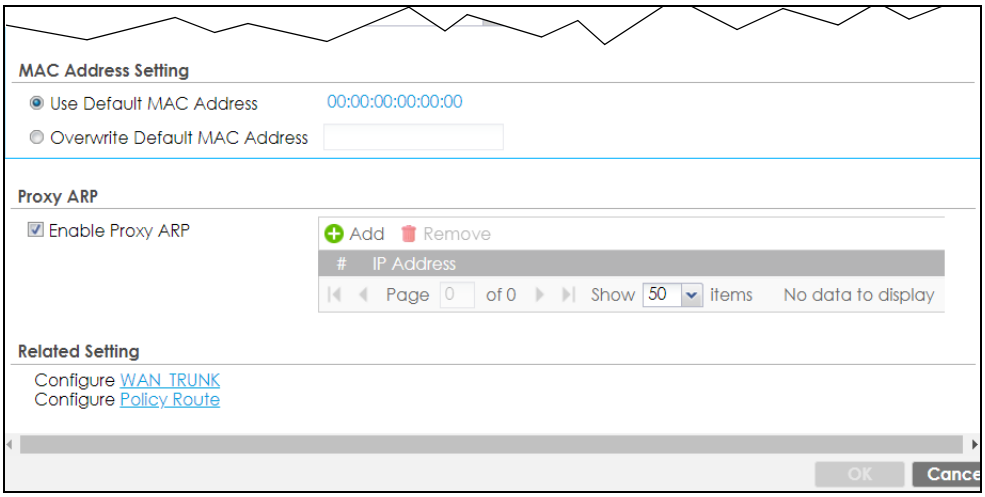
9.8.2 VLAN Add/Edit

Select an existing entry in the previous screen and click **Edit** or click **Add** to create a new entry. The following screen appears.

Figure 200 Configuration > Network > Interface > VLAN > Add /Edit




Router Preference: Medium
Advance
MTU: 1480 (1280-1500)
Hop Limit: 64 (1-255)
Advertised Prefix Table
Add Edit Remove
IPv6 Address/Prefix Length
Page 0 of 0 Show 50 items No data to display
Advance
Advertised Prefix from DHCPv6 Prefix Delegation
Add Edit Remove References
Delegated Prefix Suffix Address Address
Page 0 of 0 Show 50 items No data to display
Interface Parameters
Egress Bandwidth: 1048576 Kbps
Advance
Ingress Bandwidth: 1048576 Kbps
MTU: 1500 Bytes
Connectivity Check
Enable Connectivity Check
Check Method: icmp
Check Period: 30 (5-600 seconds)
Check Timeout: 5 (1-10 seconds)
Check Fail Tolerance: 5 (1-10)
Check Default Gateway 0.0.0.0
Check These Addresses (Domain Name or IP Address)
(Optional)
Probe Succeeds When: any one respond(s)
DHCP Setting
DHCP: None
Enable IP/MAC Binding
Enable Logs for IP/MAC Binding Violation
Static DHCP Table
Add Edit Remove
IP Address MAC Description
Page 0 of 0 Show 50 items No data to display
Advance
RIP Setting
Enable RIP
Direction: BiDir
Send Version: 2
Receive Version: 2
V2-Broadcast
OSPF Setting
Area: none
Priority: 1 (0-255)
Link Cost: 10 (1-65535)
Passive Interface
Authentication: None



Each field is explained in the following table.

Table 108 Configuration > Network > Interface > VLAN > Add / Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to turn this interface on. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the Zyxel Device is connected or if you want to additionally manually configure some related settings. **internal** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **external** is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. For **general**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing an existing VLAN interface. Enter the number of the VLAN interface. You can use a number from 0~4094. For example, use vlan0, vlan8, and so on. The total number of VLANs you can configure on the Zyxel Device depends on the model.
Zone	Select the zone to which the VLAN interface belongs.
Base Port	Select the Ethernet interface on which the VLAN interface runs.
VLAN ID	Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.)

Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Priority Code	This is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest. See Table 179 on page 451. The setting configured in **Configuration > BWM** overwrites the priority setting here.
Description	Enter a description of this interface. You can use alphanumeric and ( ) +/ : = ? ! * # @ $ _ % - characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. You should not select this if the interface is assigned to a VRRP group.
DHCP Option 60	DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Type a string using up to 64 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./ ::<=>?@\[\\\]^_`{|}~] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable **IGMP Upstream** on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable **IGMP Downstream** on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the interface.

Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to configure a static IP address for this interface. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 217 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111::1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select **N/A** to not use DHCPv6. Select **Client** to set this interface to act as a DHCPv6 client. Select **Server** to set this interface to act as a DHCPv6 server which assigns IP addresses and provides subnet mask, gateway, and DNS server information to clients. Select **Relay** to set this interface to route DHCPv6 requests to the DHCPv6 relay server you specify. The DHCPv6 server(s) may be on another network.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 218 for more information.
DUID as MAC	Select this to have the DUID generated from the interface's default MAC address.

Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 **Client**. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If this interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 9.4.5 on page 241 for more information.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device obtained from an uplink router (**Server** is selected) or will advertise to its clients (**Client** is selected).
Interface	When **Relay** is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When **Relay** is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 217 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DNS information is not available in this network.
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the Zyxel Device. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.

Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the Zyxel Device to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The Zyxel Device will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.

Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Connectivity Check	The Zyxel Device can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often to check the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Check these addresses	Type one or two domain names or IP addresses for the connectivity check.
Probe Succeeds When	This field applies when you specify two domain names or IP addresses for the connectivity check. Select **any one** if you want the check to pass if at least one of the domain names or IP addresses responds. Select **all** if you want the check to pass only if both domain names or IP addresses respond.
DHCP Setting	The DHCP settings are available for the OPT, LAN and DMZ interfaces.
DHCP	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: **None** - the Zyxel Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the Zyxel Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Zyxel Device is the DHCP server for the network.
	These fields appear if the Zyxel Device is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the Zyxel Device is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the Zyxel Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.

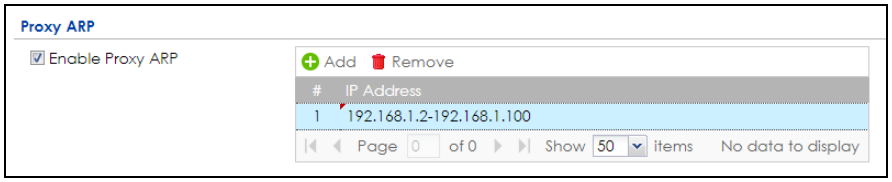
Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the Zyxel Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	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. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **Zyxel Device** - the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid. The default is 2 days.
Extended Options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 9.4.6 on page 242.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
Enable IP/MAC Binding	Select this option to have the Zyxel Device enforce links between specific IP addresses and specific MAC addresses for this VLAN. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this VLAN attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the Zyxel Device assigns to computers connected to the interface. Otherwise, the Zyxel Device assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.

Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
RIP Setting	See Section 10.6 on page 322 for more information about RIP.
Enable RIP	Select this to enable RIP on this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the Zyxel Device uses multicasting.
OSPF Setting	See Section 10.7 on page 324 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.

Table 108 Configuration > Network > Interface > VLAN > Add / Edit (continued)

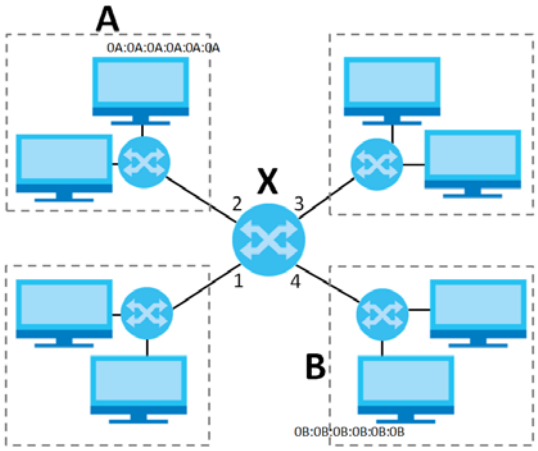
LABEL	DESCRIPTION
MAC Address Setting	This section appears when **Interface Properties** is **External** or **General**. Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer.
Use Default MAC Address	Select this option to have the interface use the factory assigned default MAC address. By default, the Zyxel Device uses the factory assigned MAC address to identify itself.
Overwrite Default MAC Address	Select this option to have the interface use a different MAC address. Either the MAC address in the field. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.
Proxy ARP	Proxy ARP is available for external or general interfaces on the Zyxel Device. See Section on page 229 for more information on Proxy ARP.
Enable Proxy ARP	Select this to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are: • Ethernet • VLAN • Bridge See Section 9.4.2 on page 238 for more information.
Add	Click **Add** to create an **IPv4 Address**, an **IPv4 CIDR** (for example, 192.168.1.1/24) or an **IPv4 Range** (for example, 192.168.1.2-192.168.1.100) as the target IP address. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the **IPv4 Address** is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address. Select an existing entry and click **Remove** to delete that entry. 
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can set this VLAN to be part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this VLAN.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.9 Bridge Interfaces

This section introduces bridges and bridge interfaces and then explains the screens for bridge interfaces.

Bridge Overview

A bridge creates a connection between two or more network segments at the layer-2 (MAC address) level. In the following example, bridge X connects four network segments.



When the bridge receives a packet, the bridge records the source MAC address and the port on which it was received in a table. It also looks up the destination MAC address in the table. If the bridge knows on which port the destination MAC address is located, it sends the packet to that port. If the destination MAC address is not in the table, the bridge broadcasts the packet on every port (except the one on which it was received).

In the example above, computer A sends a packet to computer B. Bridge X records the source address 0A:0A:0A:0A:0A:0A and port 2 in the table. It also looks up 0B:0B:0B:0B:0B:0B in the table. There is no entry yet, so the bridge broadcasts the packet on ports 1, 3, and 4.

Table 109 Example: Bridge Table After Computer A Sends a Packet to Computer B

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2

If computer B responds to computer A, bridge X records the source address 0B:0B:0B:0B:0B:0B and port 4 in the table. It also looks up 0A:0A:0A:0A:0A:0A in the table and sends the packet to port 2 accordingly.

Table 110 Example: Bridge Table After Computer B Responds to Computer A

MAC ADDRESS	PORT
0A:0A:0A:0A:0A:0A	2
0B:0B:0B:0B:0B:0B	4

Bridge Interface Overview

A bridge interface creates a software bridge between the members of the bridge interface. It also becomes the Zyxel Device's interface for the resulting network.

Unlike the device-wide bridge mode in ZyNOS-based Zyxel Devices, this Zyxel Device can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support more functions, like interface bandwidth parameters, DHCP settings, and connectivity check. To use the whole Zyxel Device as a transparent bridge, add all of the Zyxel Device's interfaces to a bridge interface.

A bridge interface may consist of the following members:

- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the Zyxel Device removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between lan1 and vlan1.

Table 111 Example: Routing Table Before and After Bridge Interface br0 Is Created

IP ADDRESS(ES)	DESTINATION
210.210.210.0/24	lan1
210.211.1.0/24	lan1:1
221.221.221.0/24	vlan0
222.222.222.0/24	vlan1
230.230.230.192/26	wan2
241.241.241.241/32	dmz
242.242.242.242/32	dmz

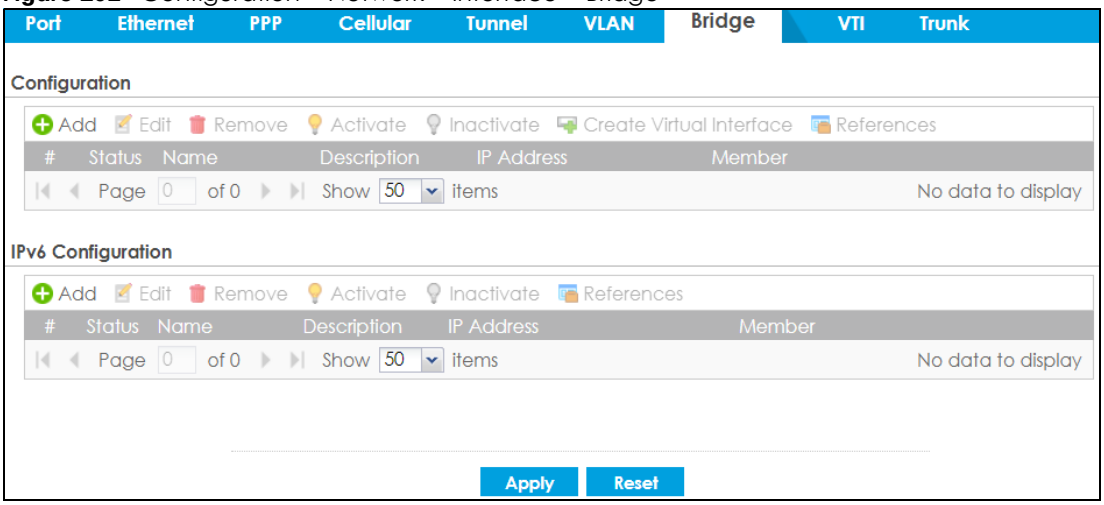
IP ADDRESS(ES)	DESTINATION
221.221.221.0/24	vlan0
230.230.230.192/26	wan2
241.241.241.241/32	dmz
242.242.242.242/32	dmz
250.250.250.0/23	br0

In this example, virtual Ethernet interface lan1:1 is also removed from the routing table when lan1 is added to br0. Virtual interfaces are automatically added to or remove from a bridge interface when the underlying interface is added or removed.

9.9.1 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure bridge interfaces used for your IPv6 network on this screen. To access this screen, click **Configuration** > **Network** > **Interface** > **Bridge**.

Figure 201 Configuration > Network > Interface > Bridge



Each field is described in the following table.

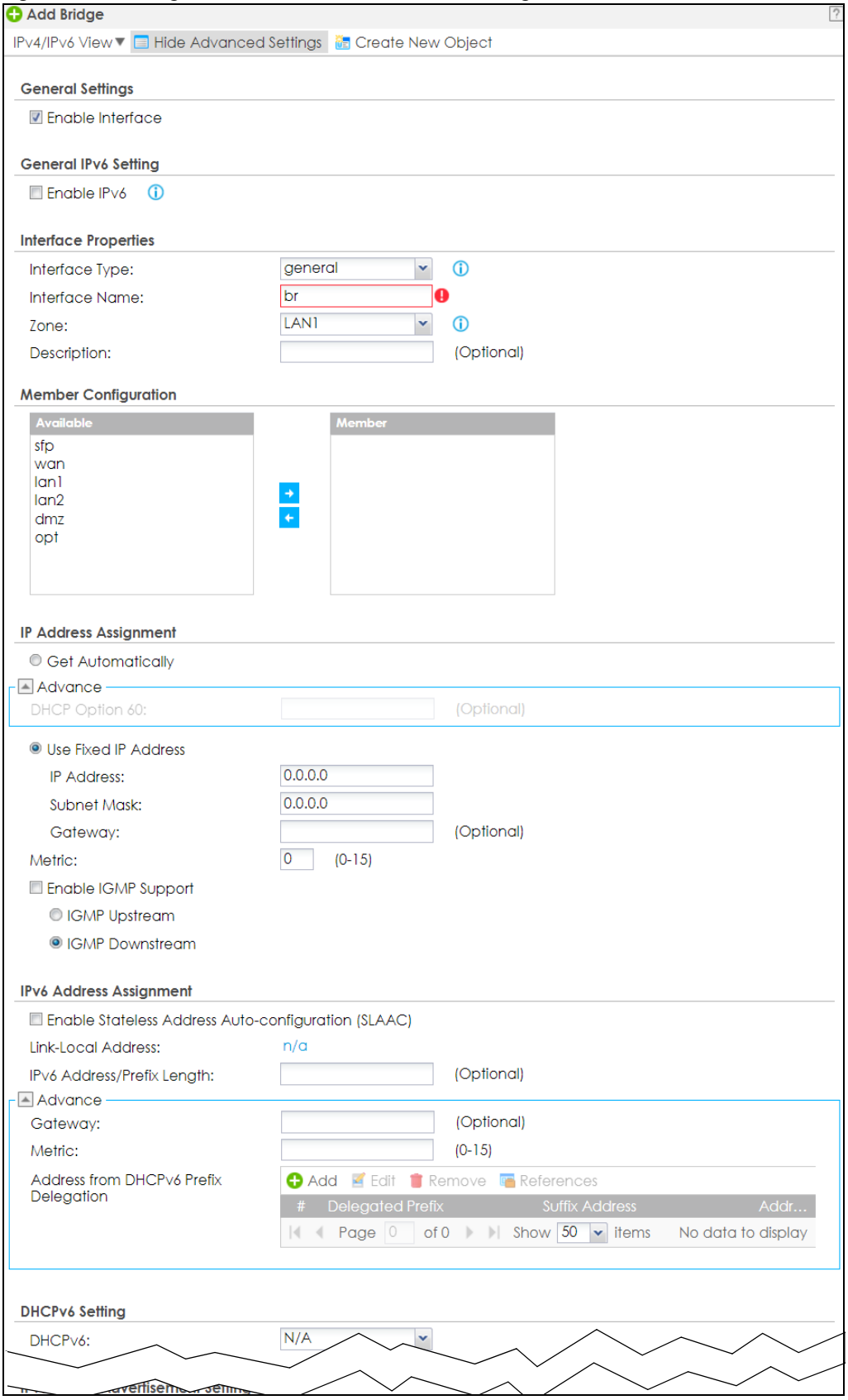
Table 112 Configuration > Network > Interface > Bridge

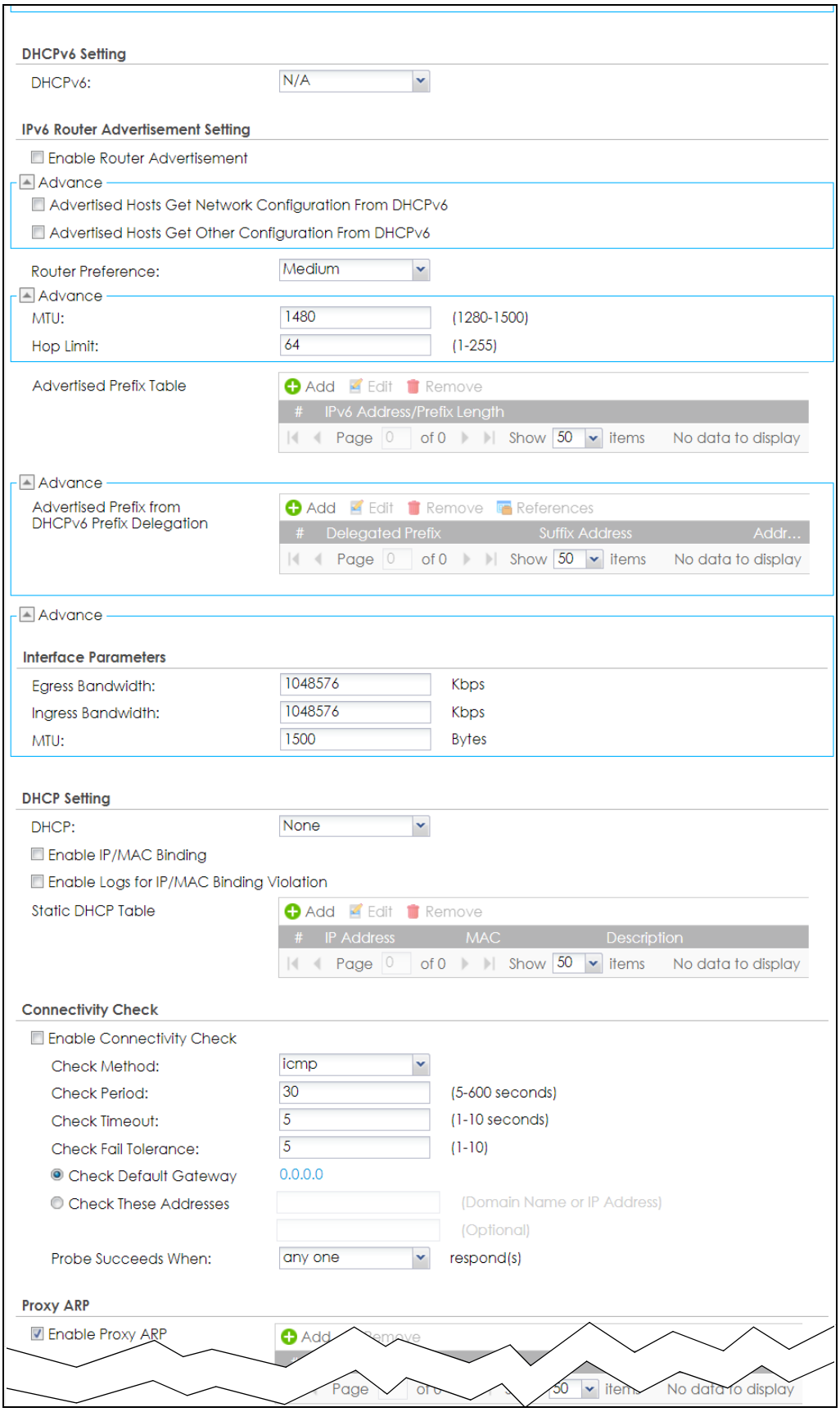
LABEL	DESCRIPTION
Configuration / IPv6 Configuration	Use the **Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Create Virtual Interface	To open the screen where you can create a virtual interface, select an interface and click **Create Virtual Interface**.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the interface.
Description	This field displays the description of the interface.
IP Address	This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet. This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces.
Member	This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

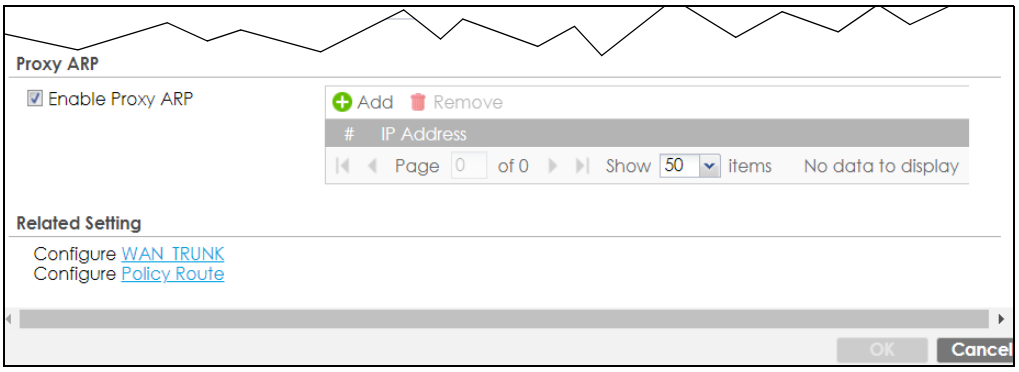
9.9.2 Bridge Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each bridge interface. To access this screen, click the **Add** or **Edit** icon in the **Bridge Summary** screen. The following screen appears.

Figure 202 Configuration > Network > Interface > Bridge > Add / Edit




DHCPv6 Setting
DHCPv6:
N/A
IPv6 Router Advertisement Setting
Enable Router Advertisement
Advance
Advertised Hosts Get Network Configuration From DHCPv6
Advertised Hosts Get Other Configuration From DHCPv6
Router Preference:
Medium
Advance
MTU:
1480
(1280-1500)
Hop Limit:
64
(1-255)
Advertised Prefix Table
Add
Edit
Remove
IPv6 Address/Prefix Length
Page 0 of 0 Show 50 items No data to display
Advance
Advertised Prefix from DHCPv6 Prefix Delegation
Add
Edit
Remove
References
Delegated Prefix Suffix Address Addr...
Page 0 of 0 Show 50 items No data to display
Advance
Interface Parameters
Egress Bandwidth:
1048576
Kbps
Ingress Bandwidth:
1048576
Kbps
MTU:
1500
Bytes
DHCP Setting
DHCP:
None
Enable IP/MAC Binding
Enable Logs for IP/MAC Binding Violation
Static DHCP Table
Add
Edit
Remove
IP Address MAC Description
Page 0 of 0 Show 50 items No data to display
Connectivity Check
Enable Connectivity Check
Check Method:
icmp
Check Period:
30
(5-600 seconds)
Check Timeout:
5
(1-10 seconds)
Check Fail Tolerance:
5
(1-10)
Check Default Gateway
0.0.0.0
Check These Addresses
(Domain Name or IP Address)
(Optional)
Probe Succeeds When:
any one
respond(s)
Proxy ARP
Enable Proxy ARP
Add
Page of 0 50 items No data to display



Each field is described in the table below.

Table 113 Configuration > Network > Interface > Bridge > Add / Edit

LABEL	DESCRIPTION
IPv4/IPv6 View / IPv4 View / IPv6 View	Use this button to display both IPv4 and IPv6, IPv4-only, or IPv6-only configuration fields.
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Click this button to create a DHCPv6 lease or DHCPv6 request object that you may use for the DHCPv6 settings in this screen.
General Settings	
Enable Interface	Select this to enable this interface. Clear this to disable this interface.
General IPv6 Setting	
Enable IPv6	Select this to enable IPv6 on this interface. Otherwise, clear this to disable it.
Interface Properties	
Interface Type	Select one of the following option depending on the type of network to which the Zyxel Device is connected or if you want to additionally manually configure some related settings. **internal** is for connecting to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The Zyxel Device automatically adds default SNAT settings for traffic flowing from this interface to an external interface. **external** is for connecting to an external network (like the Internet). The Zyxel Device automatically adds this interface to the default WAN trunk. For **general**, the rest of the screen's options do not automatically adjust and you must manually configure a policy route to add routing and SNAT settings for the interface.
Interface Name	This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is br*x*, where *x* is 0 - 11. For example, br0, br3, and so on.
Zone	Select the zone to which the interface is to belong. You use zones to apply security settings such as security policy, IDP, remote management, anti-malware, and application patrol.
Description	Enter a description of this interface. You can use alphanumeric and ( ) +/ : =?!*#@$_%- characters, and it can be up to 60 characters long. Spaces are allowed, but the string can't start with a space.
Member Configuration	

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Available	This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations: • There is a virtual interface on top of it • It is already used in a different bridge interface Select one, and click the **>>** arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface.
Member	This field displays the interfaces that are part of the bridge interface. Select one, and click the **<<** arrow to remove it from the bridge interface.
IP Address Assignment	
Get Automatically	Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.
DHCP Option 60	DHCP Option 60 is used by the Zyxel Device for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Zyxel Device adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Type a string using up to 64 of these characters [a-zA-Z0-9!\"#$%&\'()*+,-./ :;<=>?@\[\\\]^_`{|}~] to identify this Zyxel Device to the DHCP server. For example, Zyxel-TW.
Use Fixed IP Address	Select this if you want to specify the IP address, subnet mask, and gateway manually.
IP Address	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address for this interface.
Subnet Mask	This field is enabled if you select **Use Fixed IP Address**. Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Gateway	This field is enabled if you select **Use Fixed IP Address**. Enter the IP address of the gateway. The Zyxel Device sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable **IGMP Upstream** on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable **IGMP Downstream** on the interface which connects to the multicast hosts.
IPv6 Address Assignment	These IP address fields configure an IPv6 IP address on the interface itself.
Enable Stateless Address Auto-configuration (SLAAC)	Select this to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network.
Link-Local address	This displays the IPv6 link-local address and the network prefix that the Zyxel Device generates itself for the interface.

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
IPv6 Address/ Prefix Length	Enter the IPv6 address and the prefix length for this interface if you want to use a static IP address. This field is optional. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Gateway	Enter the IPv6 address of the default outgoing gateway using colon (:) hexadecimal notation.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Address from DHCPv6 Prefix Delegation	Use this table to have the Zyxel Device obtain an IPv6 prefix from the ISP or a connected uplink router for an internal network, such as the LAN or DMZ. You have to also enter a suffix address which is appended to the delegated prefix to form an address for this interface. See Prefix Delegation on page 217 for more information. To use prefix delegation, you must: • Create at least one DHCPv6 request object before configuring this table. • The external interface must be a DHCPv6 client. You must configure the DHCPv6 request options using a DHCPv6 request object with the type of prefix-delegation. • Assign the prefix delegation to an internal interface and enable router advertisement on that interface.
Add	Click this to create an entry.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use from the drop-down list.
Suffix Address	Enter the ending part of the IPv6 address, a slash (/), and the prefix length. The Zyxel Device will append it to the delegated prefix. For example, you got a delegated prefix of 2003:1234:5678/48. You want to configure an IP address of 2003:1234:5678:1111:1/128 for this interface, then enter ::1111:0:0:0:1/128 in this field.
Address	This field displays the combined IPv6 IP address for this interface. Note: This field displays the combined address after you click **OK** and reopen this screen.
DHCPv6 Setting	
DHCPv6	Select **N/A** to not use DHCPv6. Select **Client** to set this interface to act as a DHCPv6 client. Select **Server** to set this interface to act as a DHCPv6 server which assigns IP addresses and provides subnet mask, gateway, and DNS server information to clients. Select **Relay** to set this interface to route DHCPv6 requests to the DHCPv6 relay server you specify. The DHCPv6 server(s) may be on another network.
DUID	This field displays the DHCP Unique IDentifier (DUID) of the interface, which is unique and used for identification purposes when the interface is exchanging DHCPv6 messages with others. See DHCPv6 on page 218 for more information.
DUID as MAC	Select this if you want the DUID is generated from the interface's default MAC address.

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Customized DUID	If you want to use a customized DUID, enter it here for the interface.
Enable Rapid Commit	Select this to shorten the DHCPv6 message exchange process from four to two steps. This function helps reduce heavy network traffic load. Note: Make sure you also enable this option in the DHCPv6 clients to make rapid commit work.
Information Refresh Time	Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.
Request Address	This field is available if you set this interface to DHCPv6 **Client**. Select this to get an IPv6 IP address for this interface from the DHCP server. Clear this to not get any IP address information through DHCPv6.
DHCPv6 Request Options / DHCPv6 Lease Options	If this interface is a DHCPv6 client, use this section to configure DHCPv6 request settings that determine what additional information to get from the DHCPv6 server. If the interface is a DHCPv6 server, use this section to configure DHCPv6 lease settings that determine what to offer to the DHCPv6 clients.
Add	Click this to create an entry in this table. See Section 9.4.5 on page 241 for more information.
Edit	Select an entry and click this to change the settings.
Remove	Select an entry and click this to delete it from this table.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Name	This field displays the name of the DHCPv6 request or lease object.
Type	This field displays the type of the object.
Value	This field displays the IPv6 prefix that the Zyxel Device obtained from an uplink router (**Server** is selected) or will advertise to its clients (**Client** is selected).
Interface	When **Relay** is selected, select this check box and an interface from the drop-down list if you want to use it as the relay server.
Relay Server	When **Relay** is selected, select this check box and enter the IP address of a DHCPv6 server as the relay server.
IPv6 Router Advertisement Setting	
Enable Router Advertisement	Select this to enable this interface to send router advertisement messages periodically. See IPv6 Router Advertisement on page 217 for more information.
Advertised Hosts Get Network Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain network settings (such as prefix and DNS settings) through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DHCPv6 is not available and they should use the prefix in the router advertisement message.
Advertised Hosts Get Other Configuration From DHCPv6	Select this to have the Zyxel Device indicate to hosts to obtain DNS information through DHCPv6. Clear this to have the Zyxel Device indicate to hosts that DNS information is not available in this network.

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Router Preference	Select the router preference (**Low**, **Medium** or **High**) for the interface. The interface sends this preference in the router advertisements to tell hosts what preference they should use for the Zyxel Device. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network. Note: Make sure the hosts also support router preference to make this function work.
MTU	The Maximum Transmission Unit. Type the maximum size of each IPv6 data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments.
Hop Limit	Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.
Advertised Prefix Table	Configure this table only if you want the Zyxel Device to advertise a fixed prefix to the network.
Add	Click this to create an IPv6 prefix address.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
IPv6 Address/ Prefix Length	Enter the IPv6 network prefix address and the prefix length. The prefix length indicates what the left-most part of the IP address is the same for all computers in the network, that is, the network address.
Advertised Prefix from DHCPv6 Prefix Delegation	Use this table to configure the network prefix if you want to use a delegated prefix as the beginning part of the network prefix.
Add	Click this to create an entry in this table.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any entry.
Delegated Prefix	Select the DHCPv6 request object to use for generating the network prefix for the network.
Suffix Address	Enter the ending part of the IPv6 network address plus a slash (/) and the prefix length. The Zyxel Device will append it to the selected delegated prefix. The combined address is the network prefix for the network. For example, you got a delegated prefix of 2003:1234:5678/48. You want to divide it into 2003:1234:5678:1111/64 for this interface and 2003:1234:5678:2222/64 for another interface. You can use ::1111/64 and ::2222/64 for the suffix address respectively. But if you do not want to divide the delegated prefix into subnetworks, enter ::0/48 here, which keeps the same prefix length (/48) as the delegated prefix.
Address	This is the final network prefix combined by the selected delegated prefix and the suffix. Note: This field displays the combined address after you click **OK** and reopen this screen.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
MTU	Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the Zyxel Device divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500.
DHCP Setting	
DHCP	Select what type of DHCP service the Zyxel Device provides to the network. Choices are: **None** - the Zyxel Device does not provide any DHCP services. There is already a DHCP server on the network. **DHCP Relay** - the Zyxel Device routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network. **DHCP Server** - the Zyxel Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The Zyxel Device is the DHCP server for the network.
	These fields appear if the Zyxel Device is a **DHCP Relay**.
Relay Server 1	Enter the IP address of a DHCP server for the network.
Relay Server 2	This field is optional. Enter the IP address of another DHCP server for the network.
	These fields appear if the Zyxel Device is a **DHCP Server**.
IP Pool Start Address	Enter the IP address from which the Zyxel Device begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**. If this field is blank, the **Pool Size** must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
Pool Size	Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the Zyxel Device can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses. If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the Zyxel Device can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address.
First DNS Server Second DNS Server Third DNS Server	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. **Custom Defined** - enter a static IP address. **From ISP** - select the DNS server that another interface received from its DHCP server. **Zyxel Device** - the DHCP clients use the IP address of this interface and the Zyxel Device works as a DNS relay.
First WINS Server, Second WINS Server	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Default Router	If you set this interface to **DHCP Server**, you can select to use either the interface's IP address or another IP address as the default router. This default router will become the DHCP clients' default gateway. To use another IP address as the default router, select **Custom Defined** and enter the IP address.

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Lease time	Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are: **infinite** - select this if IP addresses never expire **days, hours, and minutes** - select this to enter how long IP addresses are valid.
Extended Options	This table is available if you selected **DHCP server**. Configure this table if you want to send more information to DHCP clients through DHCP packets.
Add	Click this to create an entry in this table. See Section 9.4.6 on page 242.
Edit	Select an entry in this table and click this to modify it.
Remove	Select an entry in this table and click this to delete it.
#	This field is a sequential value, and it is not associated with any entry.
Name	This is the option's name.
Code	This is the option's code number.
Type	This is the option's type.
Value	This is the option's value.
PXE Server	PXE (Preboot eXecution Environment) allows a client computer to use the network to boot up and install an operating system via a PXE-capable Network Interface Card (NIC). PXE is available for computers on internal interfaces to allow them to boot up using boot software on a PXE server. The Zyxel Device acts as an intermediary between the PXE server and the computers that need boot software. The PXE server must have a public IPv4 address. You must enable **DHCP Server** on the Zyxel Device so that it can receive information from the PXE server.
PXE Boot Loader File	A boot loader is a computer program that loads the operating system for the computer. Type the exact file name of the boot loader software file, including filename extension, that is on the PXE server. If the wrong filename is typed, then the client computers cannot boot.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address.
Static DHCP Table	Configure a list of static IP addresses the Zyxel Device assigns to computers connected to the interface. Otherwise, the Zyxel Device assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific entry.
IP Address	Enter the IP address to assign to a device with this entry's MAC address.
MAC Address	Enter the MAC address to which to assign this entry's IP address.
Description	Enter a description to help identify this static DHCP entry. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

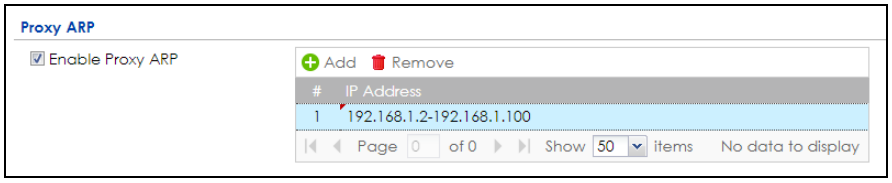
LABEL	DESCRIPTION
Connectivity Check	The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check Default Gateway	Select this to use the default gateway for the connectivity check.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Check these addresses	Type one or two domain names or IP addresses for the connectivity check.
Probe Succeeds When	This field applies when you specify two domain names or IP addresses for the connectivity check. Select **any one** if you want the check to pass if at least one of the domain names or IP addresses responds. Select **all** if you want the check to pass only if both domain names or IP addresses respond.
Proxy ARP	Proxy ARP is available for external or general interfaces on the Zyxel Device. See Section on page 229 for more information on Proxy ARP.
Enable Proxy ARP	Select this to allow the Zyxel Device to answer external interface ARP requests on behalf of a device on its internal interface. Interfaces supported are: • Ethernet • VLAN • Bridge See Section 9.4.2 on page 238 for more information.
Add	Click **Add** to create an **IPv4 Address**, an **IPv4 CIDR** (for example, 192.168.1.1/24) or an **IPv4 Range** (for example, 192.168.1.2-192.168.1.100) as the target IP address. The Zyxel Device answers external ARP requests only if they match one of these inputted target IP addresses. For example, if the **IPv4 Address** is 192.168.1.5, then the Zyxel Device will answer ARP requests coming from the WAN only if it contains 192.168.1.5 as the target IP address. Select an existing entry and click **Remove** to delete that entry. 

Table 113 Configuration > Network > Interface > Bridge > Add / Edit (continued)

LABEL	DESCRIPTION
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

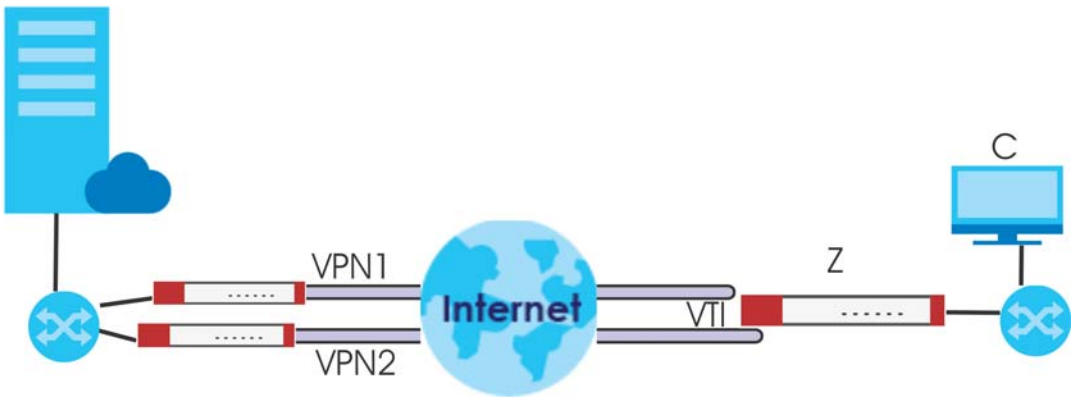
9.10 VTI

IPSec VPN Tunnel Interface (VTI) encrypts or decrypts IPv4 traffic from or to the interface according to the IP routing table.

VTI allows static routes to send traffic over the VPN. The IPSec tunnel endpoint is associated with an actual (virtual) interface. Therefore many interface capabilities such as Policy Route, Static Route, Trunk, and BWM can be applied to the IPSec tunnel as soon as the tunnel is active

IPSec VTI simplifies network management and load balancing. Create a trunk using VPN tunnel interfaces for load balancing. In the following example configure VPN tunnels with static IP addresses or DNS on both Zyxel Devices (or IPSec routers at the end of the tunnel). Also configure VTI and a trunk on both Zyxel Devices.

Figure 203 VTI and Trunk for VPN Load Balancing



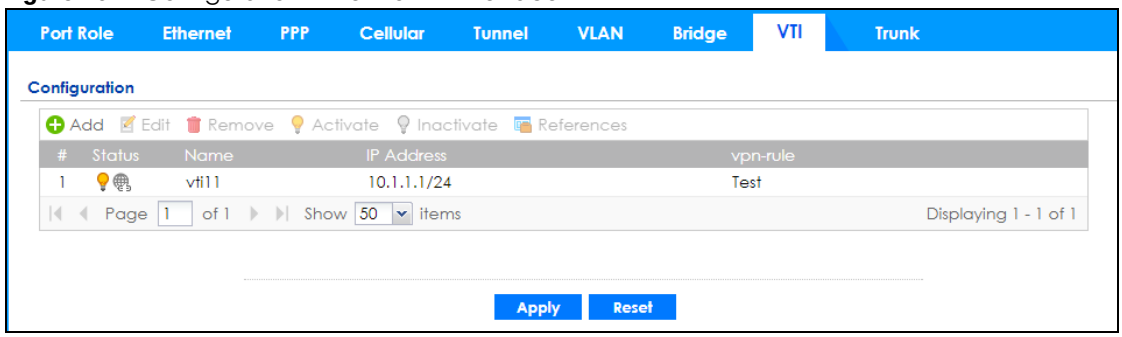
9.10.1 Restrictions for IPSec Virtual Tunnel Interface

- IPv4 traffic only
- IPSec tunnel mode only. A shared keyword must not be configured when using tunnel mode.
- With a VTI VPN you do not add local or remote LANs to your VPN configuration.
- For a VTI VPN you should only have one local and one remote WAN.
- A dynamic peer is not supported
- The IPSec VTI is limited to IP unicast and multicast traffic only.

9.10.2 VTI Screen

To access this screen, click **Configuration > Network > Interface > VTI**.

Figure 204 Configuration > Network > Interface > VTI



The following table describes the fields in this screen.

Table 114 Configuration > Network > Interface > VTI

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
References	Select an entry and click **References** to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with any interface.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the VTI interface.
IP Address	This field displays the current IP address of the virtual interface and subnet mask in bits. If the IP address is 0.0.0.0, the interface does not have an IP address yet.
vpn-rule	This shows the name of the associated IPSec VPN rule with **VPN Tunnel Interface** application scenario.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

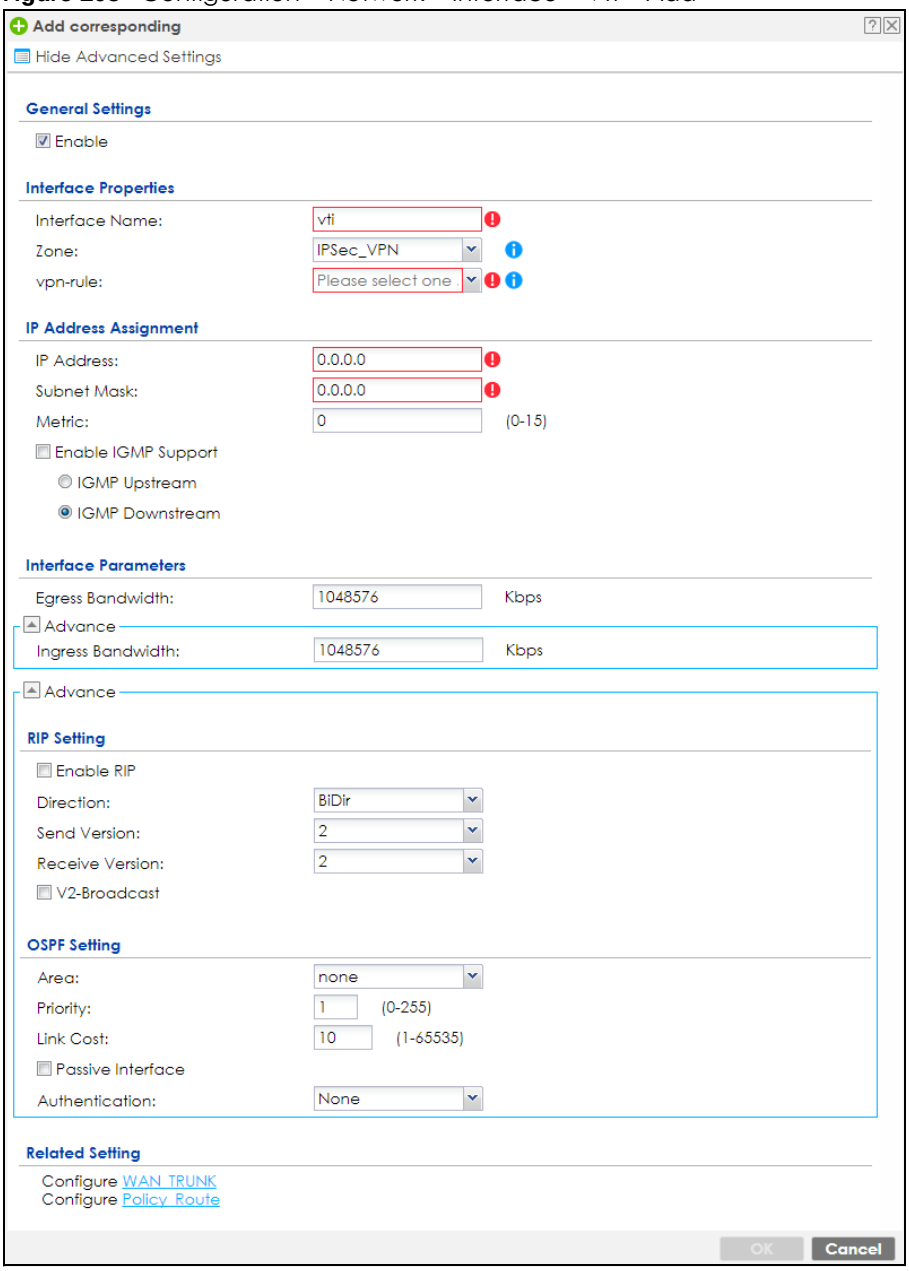
9.10.3 VTI Add/Edit

This screen lets you configure IP address assignment and interface parameters for VTI.

Note: You should have created a VPN tunnel for a **VPN Tunnel Interface** scenario first.

To access this screen, click the **Add** or **Edit** icon in **Network > Interface > VTI**. The following screen appears.

Figure 205 Configuration > Network > Interface > VTI > Add



Each field is described in the table below.

Table 115 Configuration > Network > Interface > VTI > Add

LABEL	DESCRIPTION
General Settings	
Enable	Select this to enable VTI. Clear this to disable it.
Interface Properties	
Interface Name	This field is read-only if you are editing an existing VPN tunnel interface. For a new VPN tunnel interface, enter the name of the VPN tunnel interface in vtix format, where x is a number from 0 to the maximum number of VPN connections allowed for this model. For example, enter vti10.

Table 115 Configuration > Network > Interface > VTI > Add (continued)

LABEL	DESCRIPTION
Zone	Select a zone. Make sure that the zone you select does not have traffic blocked by a security feature such as a security policy.
vpn-rule	You should have created a VPN tunnel first for a **VPN Tunnel Interface** scenario. Select one of the **VPN Tunnel Interface** scenario rules that you created.
IP Address Assignment	
IP Address	Enter the IP address for this interface.
Subnet Mask	Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network.
Metric	Enter the priority of the gateway (if any) on this interface. The Zyxel Device decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the Zyxel Device uses the one that was configured first.
Enable IGMP Support	Select this to allow the Zyxel Device to act as an IGMP proxy for hosts connected on the IGMP downstream interface.
IGMP Upstream	Enable **IGMP Upstream** on the interface which connects to a router running IGMP that is closer to the multicast server.
IGMP Downstream	Enable **IGMP Downstream** on the interface which connects to the multicast hosts.
Interface Parameters	
Egress Bandwidth	Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can send through the interface to the network. Allowed values are 0 - 1048576.
Ingress Bandwidth	This is reserved for future use. Enter the maximum amount of traffic, in kilobits per second, the Zyxel Device can receive from the network through the interface. Allowed values are 0 - 1048576.
Connectivity Check	These fields appear when you select a **vpn-rule**. The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the Zyxel Device stops routing to the gateway. The Zyxel Device resumes routing to the gateway the first time the gateway passes the connectivity check.
Enable Connectivity Check	Select this to turn on the connection check.
Check Method	Select the method that the gateway allows. Select **icmp** to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures before the Zyxel Device stops routing through the gateway.
Check this address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check Port	This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
RIP Setting	See Section 10.6 on page 322 for more information about RIP.

Table 115 Configuration > Network > Interface > VTI > Add (continued)

LABEL	DESCRIPTION
Enable RIP	Select this to enable RIP in this interface.
Direction	This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box. **BiDir** - This interface sends and receives routing information. **In-Only** - This interface receives routing information. **Out-Only** - This interface sends routing information.
Send Version	This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**.
Receive Version	This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**.
V2-Broadcast	This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the Zyxel Device uses multicasting.
OSPF Setting	See Section 10.7 on page 324 for more information about OSPF.
Area	Select the area in which this interface belongs. Select **None** to disable OSPF in this interface.
Priority	Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR.
Link Cost	Enter the cost (between 1 and 65,535) to route packets through this interface.
Passive Interface	Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information.
Authentication	Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are: **Same-as-Area** - use the default authentication method in the area **None** - disable authentication **Text** - authenticate OSPF routing information using a plain-text password **MD5** - authenticate OSPF routing information using MD5 encryption
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Related Setting	
Configure WAN TRUNK	Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing.
Configure Policy Route	Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this bridge interface.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.11 Trunk Overview

Use trunks for WAN traffic load balancing to increase overall network throughput and reliability. Load balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

Maybe you have two Internet connections with different bandwidths. You could set up a trunk that uses spillover or weighted round robin load balancing so time-sensitive traffic (like video) usually goes through the higher-bandwidth interface. For other traffic, you might want to use least load first load balancing to even out the distribution of the traffic load.

Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routes and trunks to have traffic for your European branch office primarily use ISP A and traffic for your Australian branch office primarily use ISP B.

Or maybe one of the Zyxel Device's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You can use policy routing to send the VoIP traffic through a trunk with the interface connected to the VoIP service provider set to active and another interface (connected to another ISP) set to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

- Use the **Trunk** summary screen (Section 9.12 on page 301) to view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the **Add Trunk** screen (Section 9.12.1 on page 302) to configure the member interfaces for a trunk and the load balancing algorithm the trunk uses.
- Use the **Add System Default** screen (Section 9.12.2 on page 304) to configure the load balancing algorithm for the system default trunk.

9.11.1 What You Need to Know

- Add WAN interfaces to trunks to have multiple connections share the traffic load.
- If one WAN interface's connection goes down, the Zyxel Device sends traffic through another member of the trunk.
- For example, you connect one WAN interface to one ISP and connect a second WAN interface to a second ISP. The Zyxel Device balances the WAN traffic load between the connections. If one interface's connection goes down, the Zyxel Device can automatically send its traffic through another interface.

You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

- If that interface's connection goes down, the Zyxel Device can still send its traffic through another interface.
- You can define multiple trunks for the same physical interfaces.

1 LAN user **A** logs into server **B** on the Internet. The Zyxel Device uses wan1 to send the request to server **B**.

2 The Zyxel Device is using active/active load balancing. So when LAN user **A** tries to access something on the server, the request goes out through wan2.

3 The server finds that the request comes from wan2's IP address instead of wan1's IP address and rejects the request.

If link sticking had been configured, the Zyxel Device would have still used wan1 to send LAN user **A**'s request to the server and server would have given the user **A** access.

Load Balancing Algorithms

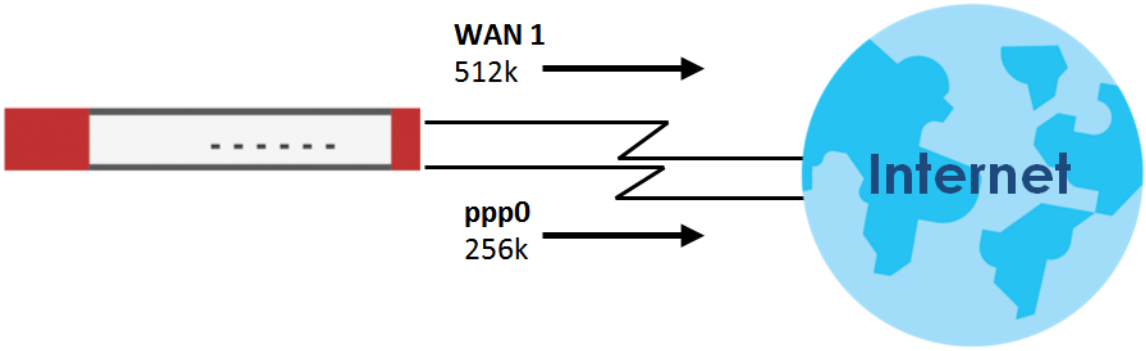
The following sections describe the load balancing algorithms the Zyxel Device can use to decide which interface the traffic (from the LAN) should use for a session. In the load balancing section, a session may refer to normal connection-oriented, UDP or SNMP2 traffic. The available bandwidth you configure on the Zyxel Device refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about to which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

Here the Zyxel Device has two WAN interfaces connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

Figure 206 Load Balancing Least Load First Example



The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and WAN 2 is 198K. The Zyxel Device calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the Zyxel Device will send the subsequent new session traffic through WAN 2.

Table 116 Least Load First Example

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

Weighted Round Robin

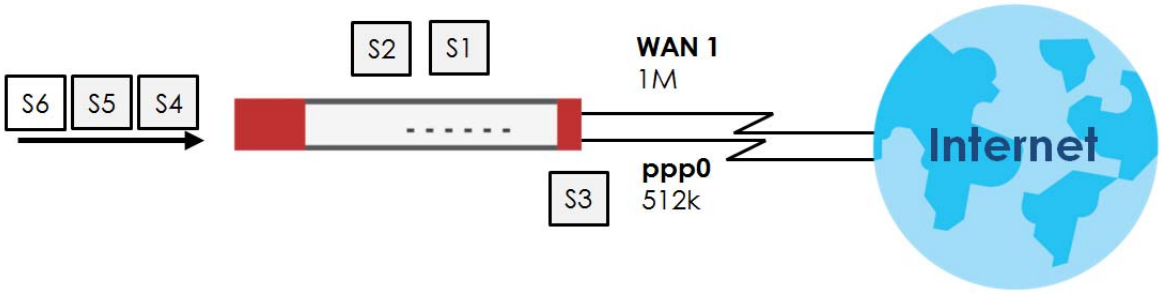
Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming

traffic on that interface. 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.

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the Zyxel Device to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the Zyxel Device to distribute the network traffic between the two interfaces by setting the weight of wan1 and wan2 to 2 and 1 respectively. The Zyxel Device assigns the traffic of two sessions to wan1 and one session's traffic to wan2 in each round of 3 new sessions.

Figure 207 Weighted Round Robin Algorithm Example



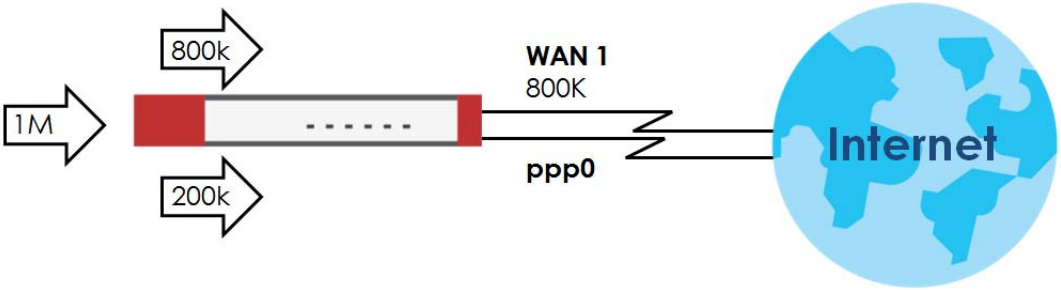
Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

In this example figure, the upper threshold of the first interface is set to 800K. The Zyxel Device sends network traffic of new sessions that exceed this limit to the secondary WAN interface.

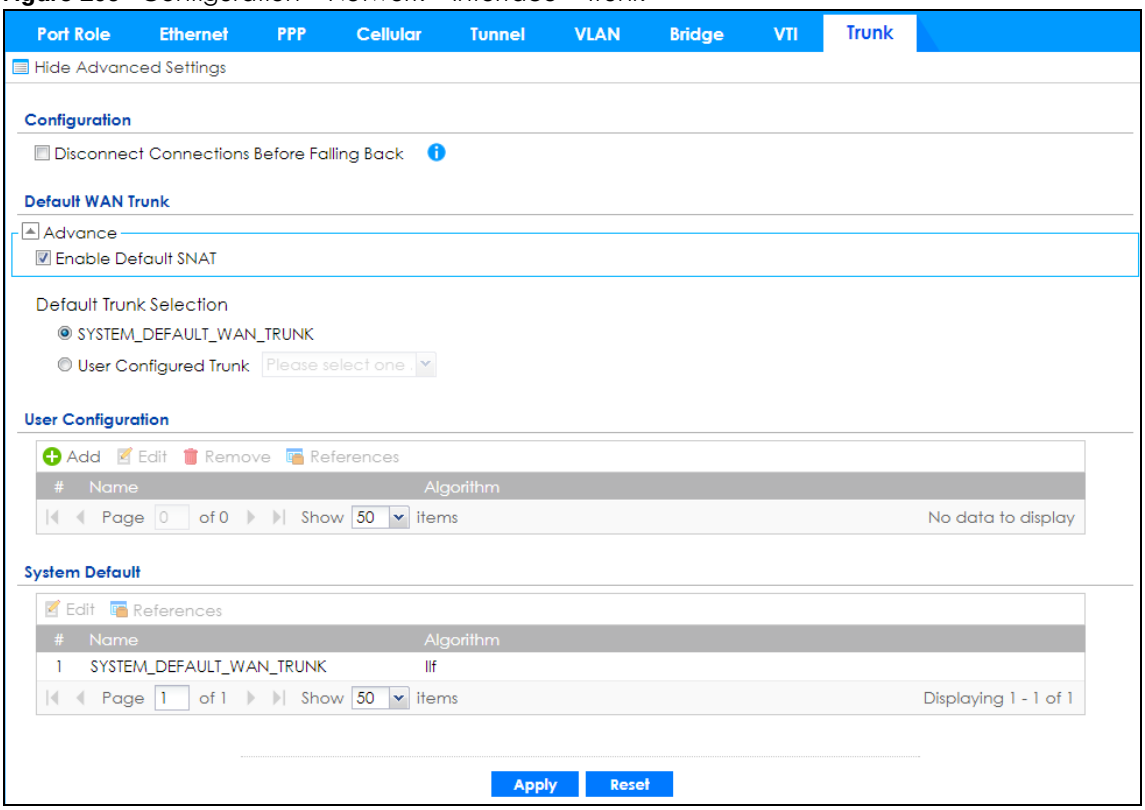
Figure 208 Spillover Algorithm Example



9.12 The Trunk Summary Screen

Click **Configuration > Network > Interface > Trunk** to open the **Trunk** screen. The Trunk Summary screen lists the configured trunks and the load balancing algorithm that each is configured to use.

Figure 209 Configuration > Network > Interface > Trunk



The following table describes the items in this screen.

Table 117 Configuration > Network > Interface > Trunk

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Configuration	Configure what to do with existing passive mode interface connections when an interface set to active mode in the same trunk comes back up.
Disconnect Connections Before Falling Back	Select this to terminate existing connections on an interface which is set to passive mode when any interface set to active mode in the same trunk comes back up.
Enable Default SNAT	Select this to have the Zyxel Device use the IP address of the outgoing interface as the source IP address of the packets it sends out through its WAN trunks. The Zyxel Device automatically adds SNAT settings for traffic it routes from internal interfaces to external interfaces.
Default Trunk Selection	Select whether the Zyxel Device is to use the default system WAN trunk or one of the user configured WAN trunks as the default trunk for routing traffic from internal interfaces to external interfaces.

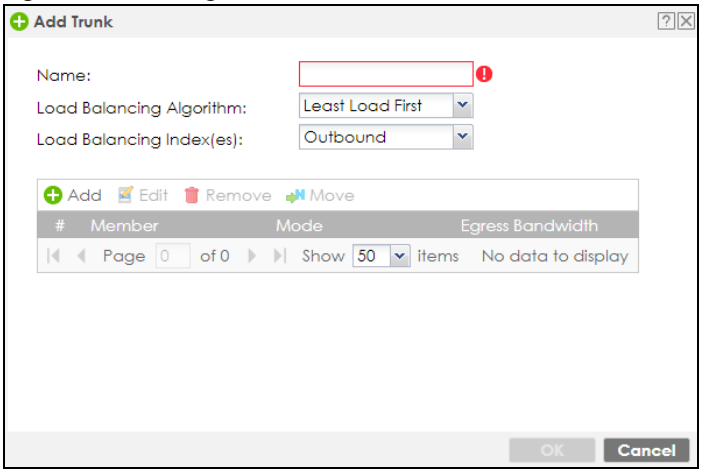
Table 117 Configuration > Network > Interface > Trunk (continued)

LABEL	DESCRIPTION
User Configuration / System Default	The Zyxel Device automatically adds all external interfaces into the pre-configured system default **SYSTEM_DEFAULT_WAN_TRUNK**. You cannot delete it. You can create your own **User Configuration** trunks and customize the algorithm, member interfaces and the active/passive mode.
Add	Click this to create a new user-configured trunk.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the label that you specified to identify the trunk.
Algorithm	This field displays the load balancing method the trunk is set to use.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

9.12.1 Configuring a User-Defined Trunk

Click **Configuration > Network > Interface > Trunk**, in the **User Configuration** table click the **Add** (or **Edit**) icon to open the **following** screen. Use this screen to create or edit a WAN trunk entry.

Figure 210 Configuration > Network > Interface > Trunk > Add (or Edit)



Each field is described in the table below.

Table 118 Configuration > Network > Interface > Trunk > Add (or Edit)

LABEL	DESCRIPTION
Name	This is read-only if you are editing an existing trunk. When adding a new trunk, enter a descriptive name for this trunk. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select **Least Load First** to send new session traffic through the least utilized trunk member. Select **Spillover** to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
Load Balancing Index(es)	This field is available if you selected to use the **Least Load First** or **Spillover** method. Select **Outbound**, **Inbound**, or **Outbound + Inbound** to set the traffic to which the Zyxel Device applies the load balancing method. Outbound means the traffic traveling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound means the opposite.
	The table lists the trunk's member interfaces. You can add, edit, remove, or move entries for user configured trunks.
Add	Click this to add a member interface to the trunk. Select an interface and click **Add** to add a new member interface after the selected member interface.
Edit	Select an entry and click **Edit** to modify the entry's settings.
Remove	To remove a member interface, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Move	To move an interface to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	Click this table cell and select an interface to be a group member. If you select an interface that is part of another Ethernet interface, the Zyxel Device does not send traffic through the interface as part of the trunk. For example, if you have physical port 5 in the ge2 representative interface, you must select interface ge2 in order to send traffic through port 5 as part of the trunk. If you select interface ge5 as a member here, the Zyxel Device will not send traffic through port 5 as part of the trunk.
Mode	Click this table cell and select **Active** to have the Zyxel Device always attempt to use this connection. Select **Passive** to have the Zyxel Device only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the Zyxel Device assigns to each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more sessions that interface should handle.

Table 118 Configuration > Network > Interface > Trunk > Add (or Edit) (continued)

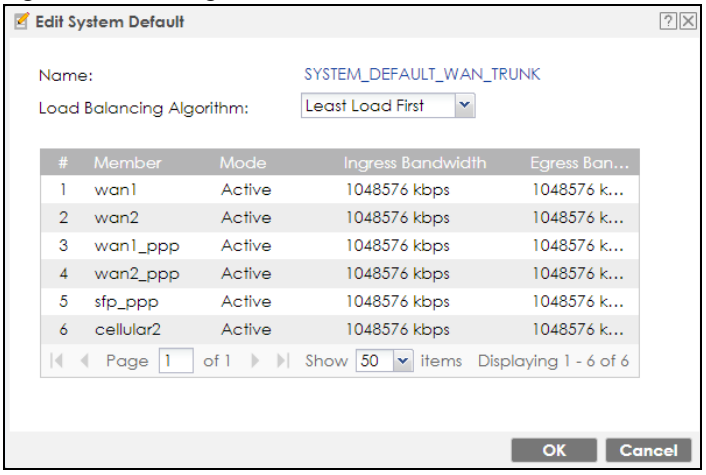
LABEL	DESCRIPTION
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the Zyxel Device is to allow to come in through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the Zyxel Device is to send out through the interface per second. Note: You can configure the bandwidth of an interface in the corresponding interface edit screen.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the Zyxel Device sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The Zyxel Device uses the group member interfaces in the order that they are listed.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.12.2 Configuring the System Default Trunk

In the **Configuration > Network > Interface > Trunk** screen and the **System Default** section, select the default trunk entry and click **Edit** to open the **following** screen. Use this screen to change the load balancing algorithm and view the bandwidth allocations for each member interface.

Note: The available bandwidth is allocated to each member interface equally and is not allowed to be changed for the default trunk.

Figure 211 Configuration > Network > Interface > Trunk > Edit (System Default)



Each field is described in the table below.

Table 119 Configuration > Network > Interface > Trunk > Edit (System Default)

LABEL	DESCRIPTION
Name	This field displays the name of the selected system default trunk.
Load Balancing Algorithm	Select the load balancing method to use for the trunk. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. Select **Least Load First** to send new session traffic through the least utilized trunk member. Select **Spillover** to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on).
	The table lists the trunk's member interfaces. This table is read-only.
#	This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed.
Member	This column displays the name of the member interfaces.
Mode	This field displays **Active** if the Zyxel Device always attempt to use this connection. This field displays **Passive** if the Zyxel Device only use this connection when all of the connections set to active are down. Only one of a group's interfaces can be set to passive mode.
Weight	This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. s
Ingress Bandwidth	This is reserved for future use. This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the Zyxel Device is to allow to come in through the interface per second.
Egress Bandwidth	This field displays with the least load first or spillover load balancing algorithm. It displays the maximum number of kilobits of data the Zyxel Device is to send out through the interface per second.
Spillover	This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the Zyxel Device sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started. The Zyxel Device uses the group member interfaces in the order that they are listed.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

9.13 Interface Technical Reference

Here is more detailed information about interfaces on the Zyxel Device.

IP Address Assignment

Most interfaces have an IP address and a subnet mask. This information is used to create an entry in the routing table.

Figure 212 Example: Entry in the Routing Table Derived from Interfaces

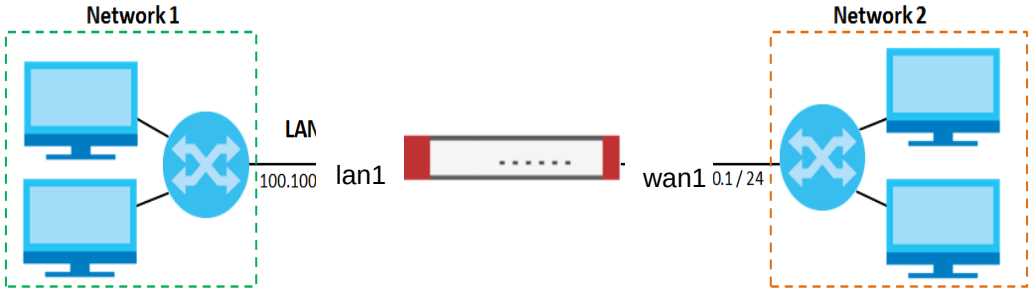


Table 120 Example: Routing Table Entries for Interfaces

IP ADDRESS(ES)	DESTINATION
100.100.1.1/16	lan1
200.200.200.1/24	wan1

For example, if the Zyxel Device gets a packet with a destination address of 100.100.25.25, it routes the packet to interface lan1. If the Zyxel Device gets a packet with a destination address of 200.200.200.200, it routes the packet to interface wan1.

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP/L2TP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

In many interfaces, you can also let the IP address and subnet mask be assigned by an external DHCP server on the network. In this case, the interface is a DHCP client. Virtual interfaces, however, cannot be DHCP clients. You have to assign the IP address and subnet mask manually.

In general, the IP address and subnet mask of each interface should not overlap, though it is possible for this to happen with DHCP clients.

In the example above, if the Zyxel Device gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the Zyxel Device should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at 200.200.200.100 on ge2. In this case, the Zyxel Device creates the following entry in the routing table.

Table 121 Example: Routing Table Entry for a Gateway

IP ADDRESS(ES)	DESTINATION
0.0.0.0/0	200.200.200.100

The gateway is an optional setting for each interface. If there is more than one gateway, the Zyxel Device uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the Zyxel Device uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP/L2TP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

If the interface gets its IP address and subnet mask from a DHCP server, the DHCP server also specifies the gateway, if any.

Interface Parameters

The Zyxel Device restricts the amount of traffic into and out of the Zyxel Device through each interface.

- Egress bandwidth sets the amount of traffic the Zyxel Device sends out through the interface to the network.
- Ingress bandwidth sets the amount of traffic the Zyxel Device allows in through the interface from the network.At the time of writing, the Zyxel Device does not support ingress bandwidth management.

If you set the bandwidth restrictions very high, you effectively remove the restrictions.

The Zyxel Device also restricts the size of each data packet. The maximum number of bytes in each packet is called the maximum transmission unit (MTU). If a packet is larger than the MTU, the Zyxel Device divides it into smaller fragments. Each fragment is sent separately, and the original packet is re-assembled later. The smaller the MTU, the more fragments sent, and the more work required to re-assemble packets correctly. On the other hand, some communication channels, such as Ethernet over ATM, might not be able to handle large data packets.

DHCP Settings

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

In the Zyxel Device, some interfaces can provide DHCP services to the network. In this case, the interface can be a DHCP relay or a DHCP server.

As a DHCP relay, the interface routes DHCP requests to DHCP servers on different networks. You can specify more than one DHCP server. If you do, the interface routes DHCP requests to all of them. It is possible for an interface to be a DHCP relay and a DHCP client simultaneously.

As a DHCP server, the interface provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the Zyxel Device's static DHCP table, the interface assigns the corresponding IP address. If not, the interface assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

Table 122 Example: Assigning IP Addresses from a Pool

START IP ADDRESS	POOL SIZE	RANGE OF ASSIGNED IP ADDRESS
50.50.50.33	5	50.50.50.33 - 50.50.50.37
75.75.75.1	200	75.75.75.1 - 75.75.75.200
99.99.1.1	1023	99.99.1.1 - 99.99.4.255
120.120.120.100	100	120.120.120.100 - 120.120.120.199

  The Zyxel Device cannot assign the first address (network address) or the last address (broadcast address) in the subnet defined by the interface's IP address and subnet mask. For example, in the first entry, if the subnet mask is 255.255.255.0, the Zyxel Device cannot assign 50.50.50.0 or 50.50.50.255. If the subnet mask is 255.255.0.0, the Zyxel Device cannot assign 50.50.0.0 or 50.50.255.255. Otherwise, it can assign every IP address in the range, except the interface's IP address.

  If you do not specify the starting address or the pool size, the interface the maximum range of IP addresses allowed by the interface's IP address and subnet mask. For example, if the interface's IP address is 9.9.9.1 and subnet mask is 255.255.255.0, the starting IP address in the pool is 9.9.9.2, and the pool size is 253.

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See IP Address Assignment on page 306.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 306.
- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

It is not possible for an interface to be the DHCP server and a DHCP client simultaneously.

WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

PPPoE/PPTP/L2TP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections. PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service
- PPPoE does not usually require any special configuration of the modem.

PPTP is used to set up virtual private networks (VPN) in unsecured TCP/IP environments. It sets up two sessions.

1. The first one runs on TCP port 1723. It is used to start and manage the second one.
2. The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

PPTP is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

Layer 2 Tunneling Protocol (L2TP) was taken from PPTP of Microsoft and Cisco's L2F (Layer 2 Forwarding technology), so LT2P combines PPTP's control and runs over a faster transport protocol, UDP, although it may be a bit more complicated to set up.

It supports up to 256 bit session keys using the IPSec protocol. When security is a priority, L2TP is a good option as it requires certificates unlike PPTP.

It uses the following ports: UDP 500, Protocol 50, UDP 1701 and UDP 4500.

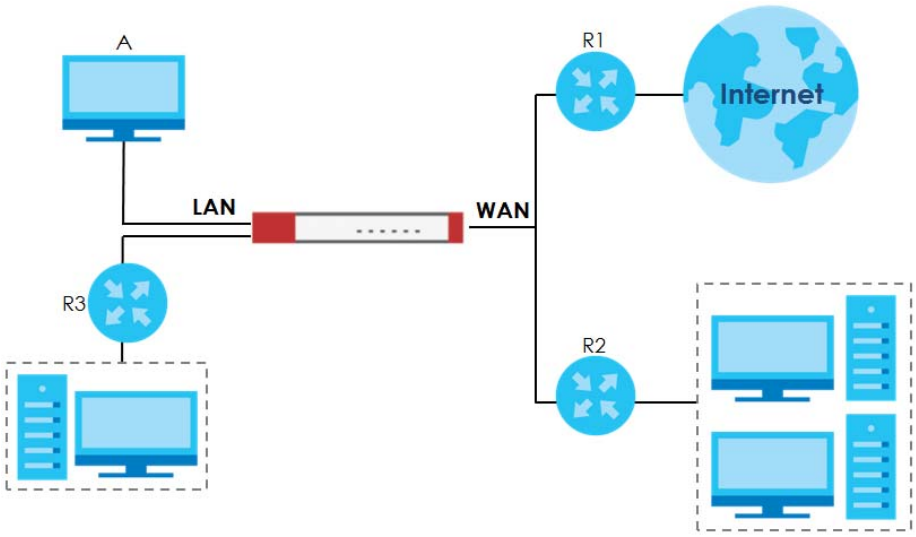
CHAPTER 10
Routing

10.1 Policy and Static Routes Overview

Use policy routes and static routes to override the Zyxel Device's default routing behavior in order to send packets through the appropriate interface or VPN tunnel.

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 policy route to connect to services offered by your ISP behind router **R2**. You create another policy route to communicate with a separate network behind another router (**R3**) connected to the LAN.

Figure 213 Example of Policy Routing Topology



Note: You can generally just use policy routes. You only need to use static routes if you have a large network with multiple routers where you use RIP or OSPF to propagate routing information to other routers.

10.1.1 What You Can Do in this Chapter

- Use the **Policy Route** screens (see Section 10.2 on page 312) to list and configure policy routes.
- Use the **Static Route** screens (see Section 10.3 on page 319) to list and configure static routes.

10.1.2 What You Need to Know

Policy Routing

Traditionally, routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism 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 incoming packets on a per interface basis, prior to the normal routing.

How You Can Use Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – You can allocate bandwidth to traffic that matches routing policies and prioritize traffic (however the application patrol's bandwidth management is more flexible and recommended for TCP and UDP traffic). You can also use policy routes to manage other types of traffic (like ICMP traffic) and send traffic through VPN tunnels.

Note: Bandwidth management in policy routes has priority over application patrol bandwidth management.

- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The Zyxel Device performs NAT by default for traffic going to or from the **WAN** interfaces. A routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

Note: The Zyxel Device automatically uses SNAT for traffic it routes from internal interfaces to external interfaces. For example LAN to WAN traffic.

Static Routes

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. Configure static routes if you need to use RIP or OSPF to propagate the routing information to other routers. See Chapter 10 on page 321 for more on RIP and OSPF.

Policy Routes Versus Static Routes

- Policy routes are more flexible than static routes. You can select more criteria for the traffic to match and can also use schedules, NAT, and bandwidth management.
- Policy routes are only used within the Zyxel Device itself. Static routes can be propagated to other routers using RIP or OSPF.
- Policy routes take priority over static routes. If you need to use a routing policy on the Zyxel Device and propagate it to other routers, you could configure a policy route and an equivalent static route.

DiffServ

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.

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 Marking and Per-Hop Behavior

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

DSCP (6 bits)	Unused (2 bits)

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.

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.

10.2 Policy Route Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

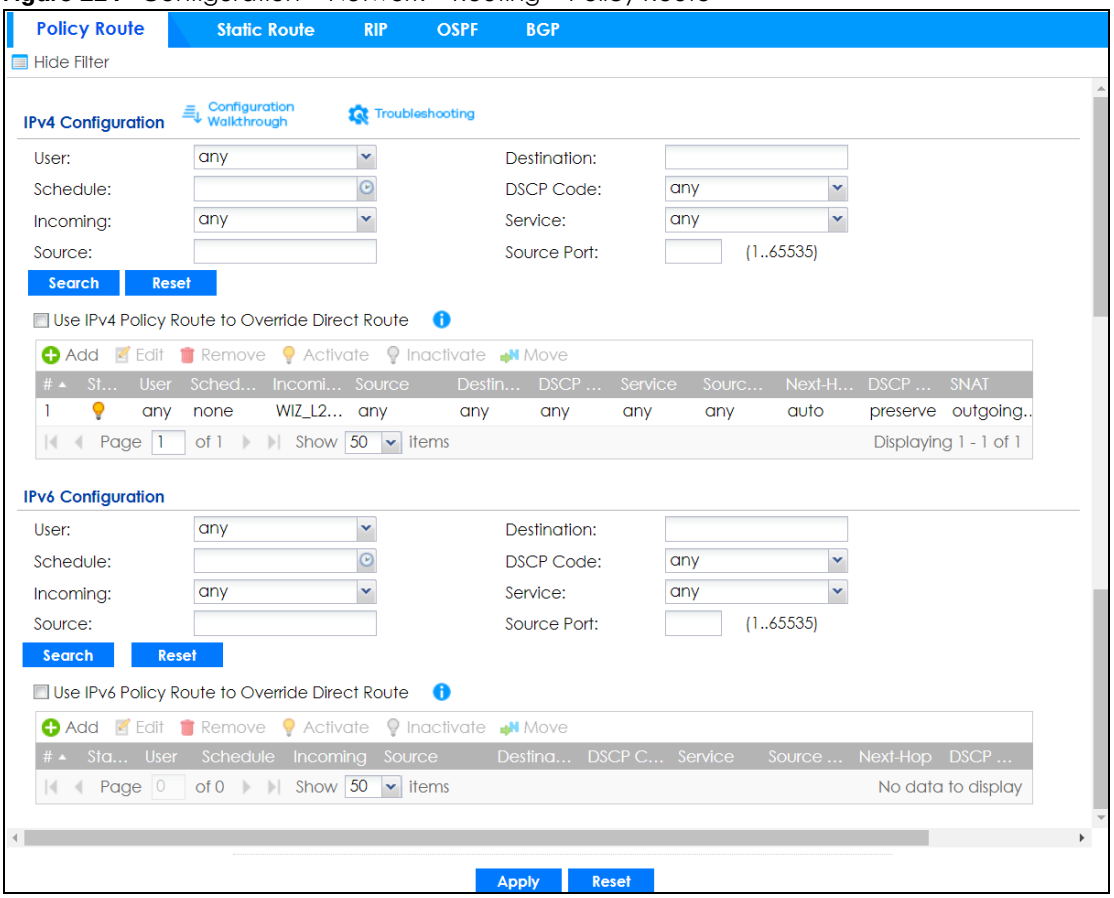
- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure policy routes used for your IPv6 networks on this screen.

Click on the icons to go to the OneSecurity website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 214 Configuration > Network > Routing > Policy Route



The following table describes the labels in this screen.

Table 123 Configuration > Network > Routing > Policy Route

LABEL	DESCRIPTION
Show Filter / Hide Filter	Click this button to display a greater or lesser number of configuration fields.
IPv4 Configuration / IPv6 Configuration	Use the **IPv4 Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below.
Use IPv4/IPv6 Policy Route to Override Direct Route	Select this to have the Zyxel Device forward packets that match a policy route according to the policy route instead of sending the packets directly to a connected network.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.

Table 123 Configuration > Network > Routing > Policy Route (continued)

LABEL	DESCRIPTION
#	This is the number of an individual policy route.
Status	This icon is lit when the entry is active, red when the next hop's connection is down, and dimmed when the entry is inactive.
User	This is the name of the user (group) object from which the packets are sent. **any** means all users.
Schedule	This is the name of the schedule object. **none** means the route is active at all times if enabled.
Incoming	This is the interface on which the packets are received.
Source	This is the name of the source IP address (group) object, including geographic address and FQDN (group) objects. **any** means all IP addresses.
Destination	This is the name of the destination IP address (group) object, including geographic and FQDN (group) address objects. **any** means all IP addresses.
DSCP Code	This is the DSCP value of incoming packets to which this policy route applies. **any** means all DSCP values or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" entries stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details.
Service	This is the name of the service object. **any** means all services.
Source Port	This is the name of a service object. The Zyxel Device applies the policy route to the packets sent from the corresponding service port. **any** means all service ports.
Next-Hop	This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk.
DSCP Marking	This is how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. If this field displays a DSCP value, the Zyxel Device applies that DSCP value to the route's outgoing packets. **preserve** means the Zyxel Device does not modify the DSCP value of the route's outgoing packets. **default** means the Zyxel Device sets the DSCP value of the route's outgoing packets to 0. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details.
SNAT	This is the source IP address that the route uses. It displays **none** if the Zyxel Device does not perform NAT for this route.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

10.2.1 Policy Route Edit Screen

Click **Configuration > Network > Routing** to open the **Policy Route** screen. Then click the **Add** or **Edit** icon in the **IPv4 Configuration** or **IPv6 Configuration** section. The **Add Policy Route** or **Policy Route Edit** screen opens. Use this screen to configure or edit a policy route. Both IPv4 and IPv6 policy route have similar settings except the **Address Translation** (SNAT) settings.

Figure 215 Configuration > Network > Routing > Policy Route > Add/Edit (IPv4 Configuration)

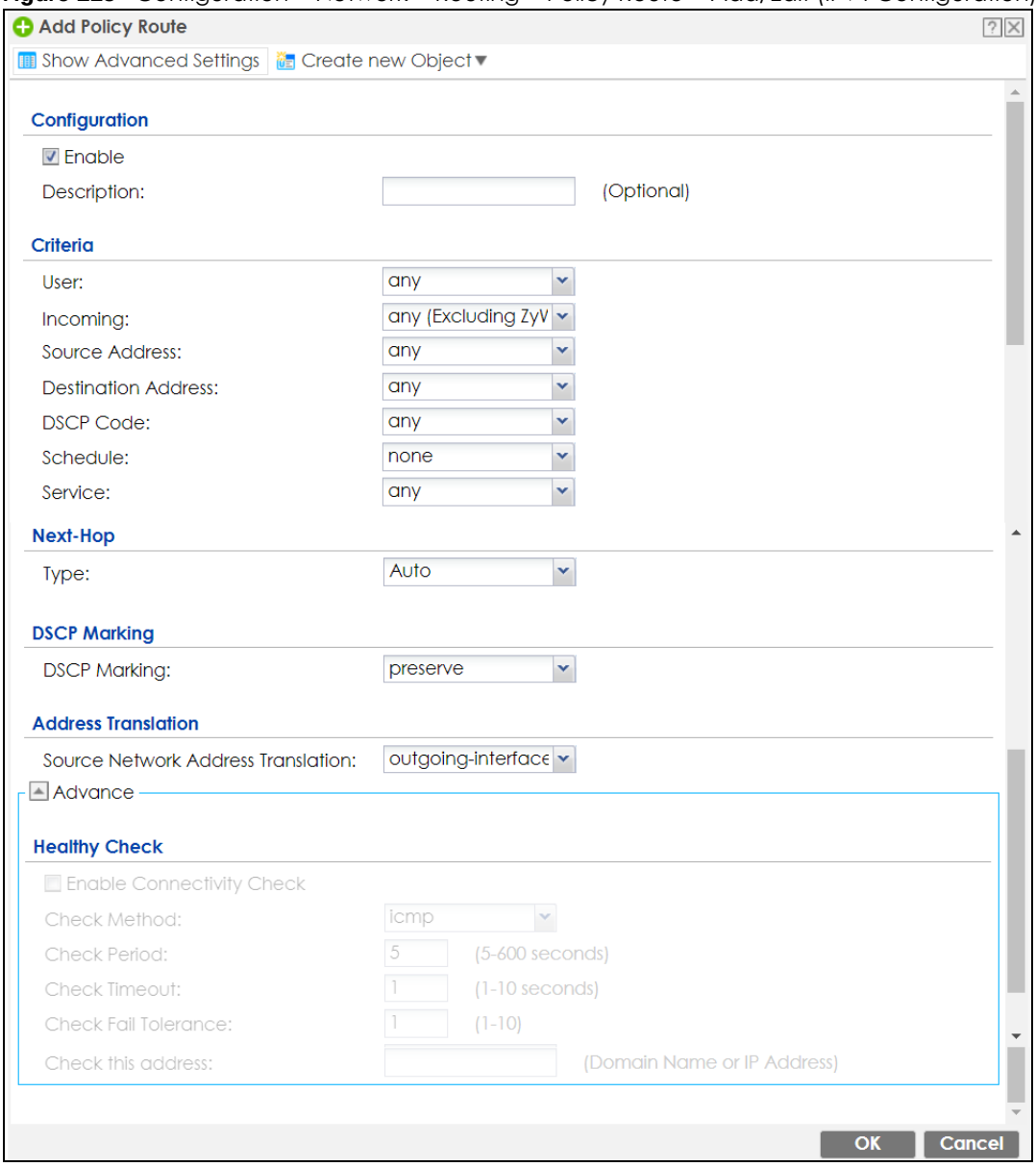
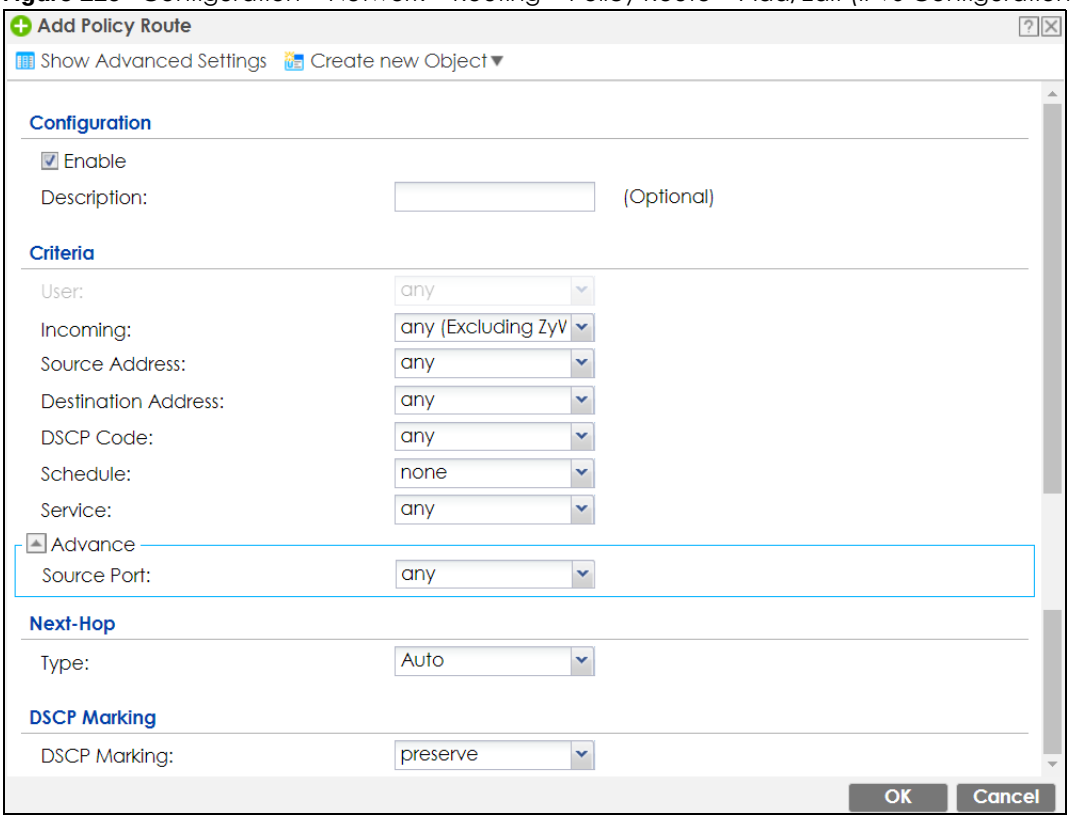


Figure 216 Configuration > Network > Routing > Policy Route > Add/Edit (IPv6 Configuration)



The following table describes the labels in this screen.

Table 124 Configuration > Network > Routing > Policy Route > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this to activate the policy.
Description	Enter a descriptive name of up to 31 printable ASCII characters for the policy.
Criteria	
User	Select a user name or user group from which the packets are sent.
Incoming	Select where the packets are coming from; any, an interface, a tunnel, an SSL VPN, or the Zyxel Device itself. For an interface, a tunnel, or an SSL VPN, you also need to select the individual interface, VPN tunnel, or SSL VPN connection.
Source Address	Select a source IP address object, including geographic address and FQDN (group) objects, from which the packets are sent.
Destination Address	Select a destination IP address object, including geographic address and FQDN (group) objects, to which the traffic is being sent. If the next hop is a dynamic VPN tunnel and you enable **Auto Destination Address**, the Zyxel Device uses the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of your configuration here.

Table 124 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select **User Define** to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. **any** means all DSCP value or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point when you select **User Define** in the previous field.
Schedule	Select a schedule to control when the policy route is active. **none** means the route is active at all times if enabled.
Service	Select a service or service group to identify the type of traffic to which this policy route applies.
Source Port	Select a service or service group to identify the source port of packets to which the policy route applies.
Next-Hop	
Type	Select **Auto** to have the Zyxel Device use the routing table to find a next-hop and forward the matched packets automatically. Select **Gateway** to route the matched packets to the next-hop router or switch you specified in the **Gateway** field. You have to set up the next-hop router or switch as a HOST address object first. Select **VPN Tunnel** to route the matched packets via the specified VPN tunnel. Select **Trunk** to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm. Select **Interface** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface).
Gateway	This field displays when you select **Gateway** in the **Type** field. Select a HOST address object. The gateway is an immediate neighbor of your Zyxel Device that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your Zyxel Device's interface(s).
VPN Tunnel	This field displays when you select **VPN Tunnel** in the **Type** field. Select a VPN tunnel through which the packets are sent to the remote network that is connected to the Zyxel Device directly.
Auto Destination Address	This field displays when you select **VPN Tunnel** in the **Type** field. Select this to have the Zyxel Device use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy. Leave this cleared if you want to manually specify the destination address.
Trunk	This field displays when you select **Trunk** in the **Type** field. Select a trunk group to have the Zyxel Device send the packets via the interfaces in the group.
Interface	This field displays when you select **Interface** in the **Type** field. Select an interface to have the Zyxel Device send traffic that matches the policy route through the specified interface.

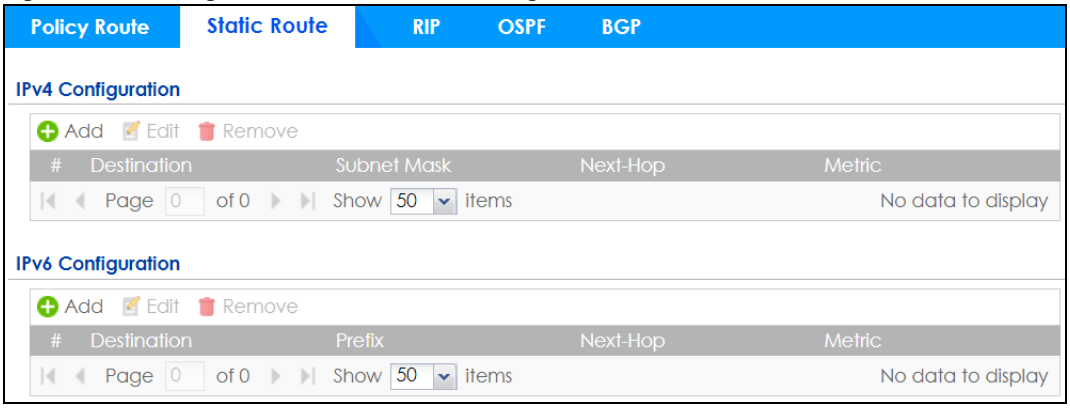
Table 124 Configuration > Network > Routing > Policy Route > Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Marking	Set how the Zyxel Device handles the DSCP value of the outgoing packets that match this route. Select one of the pre-defined DSCP values to apply or select **User Define** to specify another DSCP value. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. See Assured Forwarding (AF) PHB for DiffServ for more details. Select **preserve** to have the Zyxel Device keep the packets' original DSCP value. Select **default** to have the Zyxel Device set the DSCP value of the packets to 0.
User-Defined DSCP Marking	Use this field to specify a custom DSCP value.
Address Translation	Use this section to configure NAT for the policy route. This section does not apply to policy routes that use a VPN tunnel as the next hop.
Source Network Address Translation	Select **none** to not use NAT for the route. Select **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnets. Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route. Use **Create new Object** if you need to configure a new address (group) to use as the source IP address(es) of the packets that match this route.
Healthy Check	Use this part of the screen to configure a route connectivity check and disable the policy if the interface is down.
Disable policy route automatically while Interface link down	Select this to disable the policy if the interface is down or disabled. This is available for **Interface** and **Trunk** in the **Type** field above.
Enable Connectivity Check	Select this to turn on the connection check. This is available for **Interface** and **Gateway** in the **Type** field above.
Check Method:	Select the method that the gateway allows. Select icmp to have the Zyxel Device regularly ping the gateway you specify to make sure it is still available. Select tcp to have the Zyxel Device regularly perform a TCP handshake with the gateway you specify to make sure it is still available.
Check Period:	Enter the number of seconds between connection check attempts (5-600 seconds).
Check Timeout:	Enter the number of seconds to wait for a response before the attempt is a failure (1-10 seconds).
Check Fail Tolerance:	Enter the number of consecutive failures before the Zyxel Device stops routing using this policy (1-10).
Check Port:	This field only displays when you set the Check Method to tcp. Specify the port number to use for a TCP connectivity check (1-65535).
Check this address:	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

10.3 IP Static Route Screen

Click **Configuration > Network > Routing > Static Route** to open the **Static Route** screen. This screen displays the configured static routes. Configure static routes to be able to use RIP or OSPF to propagate the routing information to other routers. If you enabled IPv6 in the **Configuration** > **System** > **IPv6** screen, you can also configure static routes used for your IPv6 networks on this screen.

Figure 217 Configuration > Network > Routing > Static Route



The following table describes the labels in this screen.

Table 125 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
IPv4 Configuration / IPv6 Configuration	Use the **IPv4 Configuration** section for IPv4 network settings. Use the **IPv6 Configuration** section for IPv6 network settings if you connect your Zyxel Device to an IPv6 network. Both sections have similar fields as described below.
Add	Click this to create a new static route.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This is the number of an individual static route.
Destination	This is the destination IP address.
Subnet Mask	This is the IP subnet mask.
Prefix	This is the IPv6 prefix for the destination IP address.
Next-Hop	This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.
Metric	This is the route's priority among the Zyxel Device's routes. The smaller the number, the higher priority the route has.

10.3.1 Static Route Add/Edit Screen

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

Figure 218 Configuration > Network > Routing > Static Route > Add (IPv4 Configuration)

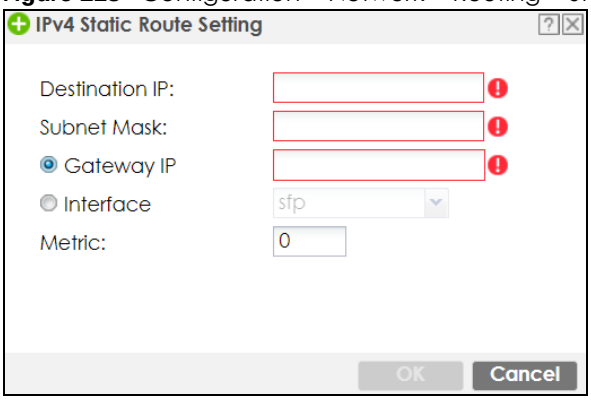
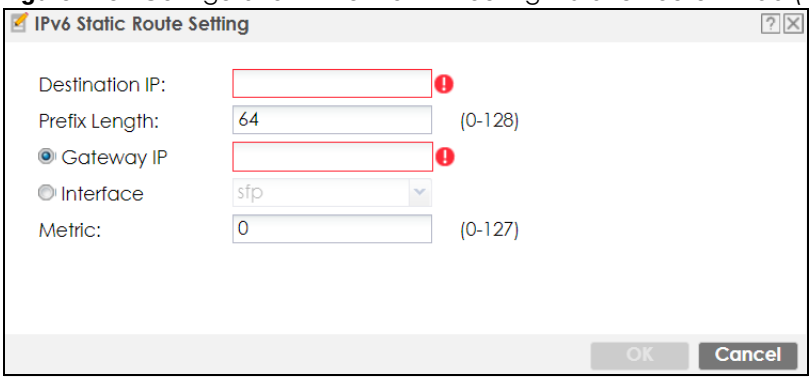


Figure 219 Configuration > Network > Routing > Static Route > Add (IPv6 Configuration)



The following table describes the labels in this screen.

Table 126 Configuration > Network > Routing > Static Route > Add

LABEL	DESCRIPTION
Destination IP	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, enter the specific IP address here and use a subnet mask of 255.255.255.255 (for IPv4) in the **Subnet Mask** field or a prefix of 128 (for IPv6) in the **Prefix Length** field to force the network number to be identical to the host ID. For IPv6, if you want to send all traffic to the gateway or interface specified in the **Gateway IP** or **Interface** field, enter :: in this field and 0 in the **Prefix Length** field.
Subnet Mask	Enter the IP subnet mask here.
Prefix Length	Enter the number of left-most digits in the destination IP address, which indicates the network prefix. Enter :: in the **Destination IP** field and 0 in this field if you want to send all traffic to the gateway or interface specified in the **Gateway IP** or **Interface** field.
Gateway IP	Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your Zyxel Device's interface(s). The gateway helps forward packets to their destinations.
Interface	Select the radio button and a predefined interface through which the traffic is sent.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0~127. In practice, 2 or 3 is usually a good number.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

10.4 Policy Routing Technical Reference

Here is more detailed information about some of the features you can configure in policy routing.

NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

Table 127 Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

Maximize Bandwidth Usage

The maximize bandwidth usage option allows the Zyxel Device to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a policy route is not using) among the policy routes that require more bandwidth.

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

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

10.5 Routing Protocols Overview

Routing protocols give the Zyxel Device routing information about the network from other routers. The Zyxel Device stores this routing information in the routing table it uses to make routing decisions. In turn, the Zyxel Device can also use routing protocols to propagate routing information to other routers.

Routing protocols are usually only used in networks using multiple routers like campuses or large enterprises.

- Use the **RIP** screen (see Section 10.6 on page 322) to configure the Zyxel Device to use RIP to receive and/or send routing information.
- Use the **OSPF** screen (see Section 10.7 on page 324) to configure general OSPF settings and manage OSPF areas.
- Use the **OSPF Area Add/Edit** screen (see Section 10.7.2 on page 328) to create or edit an OSPF area.
- Use the **BGP** screen (see Section 10.8 on page 331) to configure eBGP (exterior Border Gate Protocol).

10.5.1 What You Need to Know

The Zyxel Device supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared here and discussed further in the rest of the chapter.

Table 128 RIP vs. OSPF

	RIP	OSPF
Network Size	Small (with up to 15 routers)	Large
Metric	Hop count	Bandwidth, hop count, throughput, round trip time and reliability.
Convergence	Slow	Fast

10.6 The RIP Screen

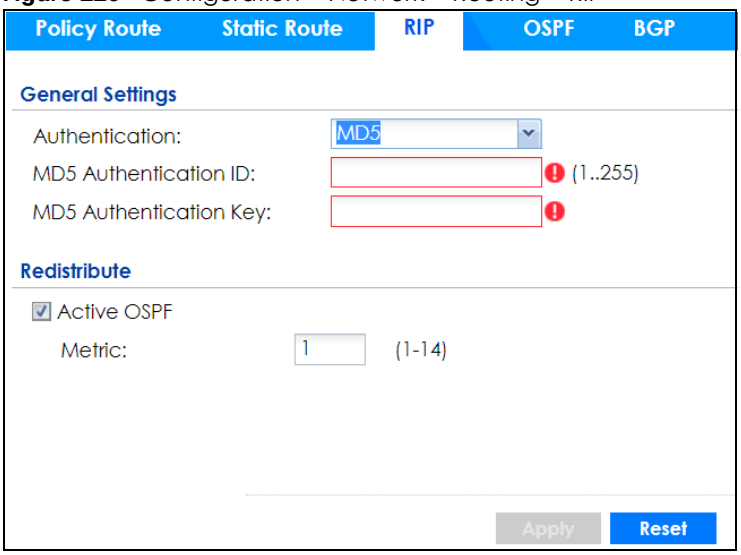
RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

- In the Zyxel Device, you can configure two sets of RIP settings before you can use it in an interface.
- First, the **Authentication** field specifies how to verify that the routing information that is received is the same routing information that is sent.
- Second, the Zyxel Device can also **redistribute** routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the **Metric** field to specify the cost in RIP terms.
- RIP uses UDP port 520.

Use the **RIP** screen to specify the authentication method and maintain the policies for redistribution.

Click **Configuration > Network** > **Routing > RIP** to open the following screen.

Figure 220 Configuration > Network > Routing > RIP



The following table describes the labels in this screen.

Table 129 Configuration > Network > Routing Protocol > RIP

LABEL	DESCRIPTION
Authentication	The transmitting and receiving routers must have the same key. For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces.
Authentication	Select the authentication method used in the RIP network. This authentication protects the integrity, but not the confidentiality, of routing updates. • **None** uses no authentication. • **Text** uses a plain text password that is sent over the network (not very secure). • **MD5** uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Redistribute	
Active OSPF	Select this to use RIP to advertise routes that were learned through OSPF.
Metric	Type the cost for routes provided by OSPF. The metric represents the "cost" of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

10.7 The OSPF Screen

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.
- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes in the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

OSPF Areas

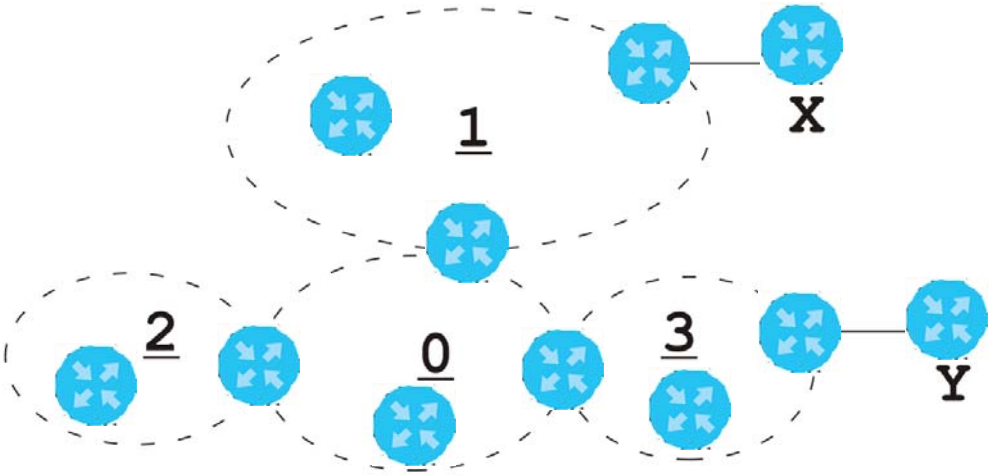
An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.
- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

Figure 221 OSPF: Types of Areas



This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.
- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.
- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

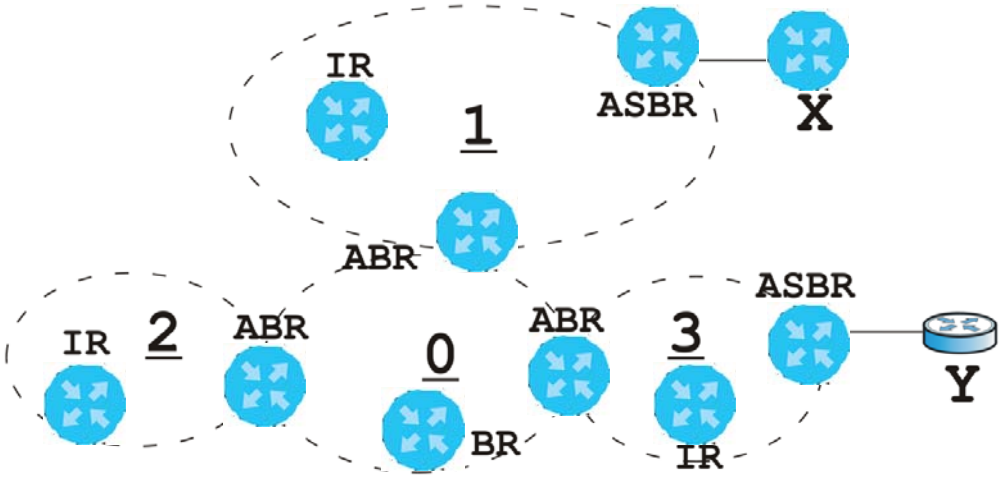
Table 130 OSPF: Redistribution from Other Sources to Each Type of Area

SOURCE \ TYPE OF AREA	NORMAL	NSSA	STUB
Static routes	Yes	Yes	No
RIP	Yes	Yes	Yes

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

Figure 222 OSPF: Types of Routers



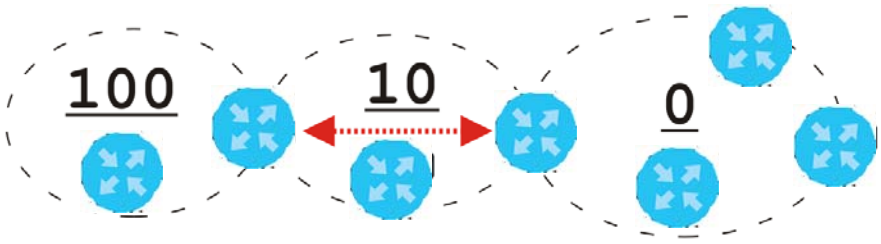
In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area to logically connect the area to the backbone. This is illustrated in the following example.

Figure 223 OSPF: Virtual Link



In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

OSPF Configuration

Follow these steps when you configure OSPF on the Zyxel Device.

1 Enable OSPF.

2 Set up the OSPF areas.

3 Configure the appropriate interfaces. See Section 9.4.1 on page 222.

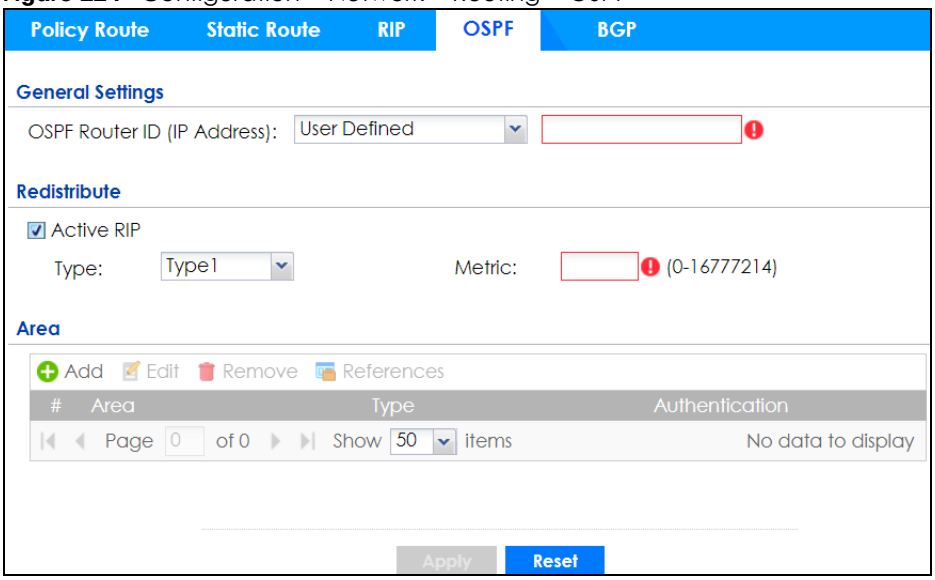
4 Set up virtual links, as needed.

10.7.1 Configuring the OSPF Screen

Use the first OSPF screen to specify the OSPF router the Zyxel Device uses in the OSPF AS and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the **OSPF Add/Edit** screen to add or edit them.

Click **Configuration > Network** > **Routing > OSPF** to open the following screen.

Figure 224 Configuration > Network > Routing > OSPF



The following table describes the labels in this screen. See Section 10.7.2 on page 328 for more information as well.

Table 131 Configuration > Network > Routing Protocol > OSPF

LABEL	DESCRIPTION
OSPF Router ID	Select the 32-bit ID the Zyxel Device uses in the OSPF AS. **Default** - the first available interface IP address is the Zyxel Device's ID. **User Defined** - enter the ID (in IP address format) in the field that appears when you select **User Define.**
Redistribute	
Active RIP	Select this to advertise routes that were learned from RIP. The Zyxel Device advertises routes learned from RIP to **Normal** and **NSSA** areas but not to **Stub** areas.
Type	Select how OSPF calculates the cost associated with routing information from RIP. Choices are: **Type 1** and **Type 2**. **Type 1** - cost = OSPF AS cost + external cost (**Metric**) **Type 2** - cost = external cost (**Metric**); the OSPF AS cost is ignored.

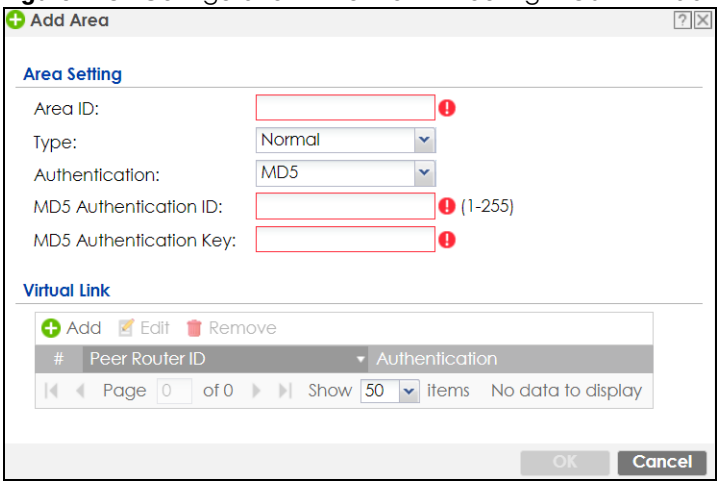
Table 131 Configuration > Network > Routing Protocol > OSPF (continued)

LABEL	DESCRIPTION
Metric	Type the external cost for routes provided by RIP. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the **Type** field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214.
Area	This section displays information about OSPF areas in the Zyxel Device.
Add	Click this to create a new OSPF area.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. Click **Refresh** to update information on this screen.
#	This field is a sequential value, and it is not associated with a specific area.
Area	This field displays the 32-bit ID for each area in IP address format.
Type	This field displays the type of area. This type is different from the **Type** field above.
Authentication	This field displays the default authentication method in the area.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

10.7.2 OSPF Area Add/Edit Screen

The **OSPF Area Add/Edit** screen allows you to create a new area or edit an existing one. To access this screen, go to the **OSPF** summary screen (see Section 10.7 on page 324), and click either the **Add** icon or an **Edit** icon.

Figure 225 Configuration > Network > Routing > OSPF > Add



The following table describes the labels in this screen.

Table 132 Configuration > Network > Routing > OSPF > Add

LABEL	DESCRIPTION
Area ID	Type the unique, 32-bit identifier for the area in IP address format.
Type	Select the type of OSPF area. **Normal** - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS. **Stub** - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS. **NSSA** - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS.
Authentication	Select the default authentication method used in the area. This authentication protects the integrity, but not the confidentiality, of routing updates. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure).
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
Virtual Link	This section is displayed if the **Type** is **Normal**. Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone.
Add	Click this to create a new virtual link.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Peer Router ID	This is the 32-bit ID (in IP address format) of the other ABR in the virtual link.

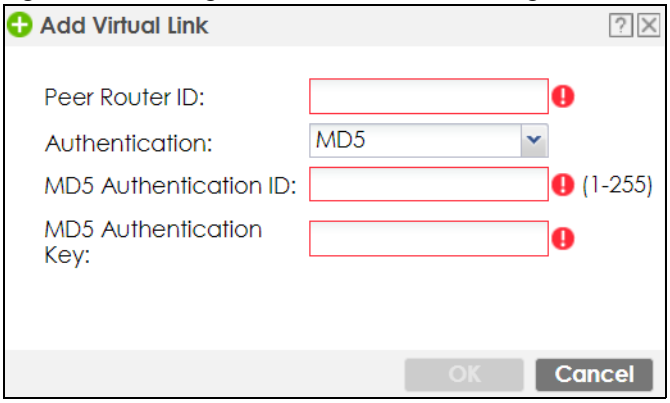
Table 132 Configuration > Network > Routing > OSPF > Add (continued)

LABEL	DESCRIPTION
Authentication	This is the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. For OSPF, the Zyxel Device supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated Authentication Type field to **Same as Area**. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). Hover your cursor over this label to display the password. **MD5** uses an MD5 password and authentication ID (most secure). Hover your cursor over this label to display the authentication ID and key. **Same as Area** has the virtual link also use the **Authentication** settings above.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

10.7.3 Virtual Link Add/Edit Screen

The **Virtual Link Add/Edit** screen allows you to create a new virtual link or edit an existing one. When the OSPF add or edit screen (see Section 10.7.2 on page 328) has the Type set to Normal, a Virtual Link table displays. Click either the **Add** icon or an entry and the **Edit** icon to display a screen like the following.

Figure 226 Configuration > Network > Routing > OSPF > Add > Add



The following table describes the labels in this screen.

Table 133 Configuration > Network > Routing > OSPF > Add > Add

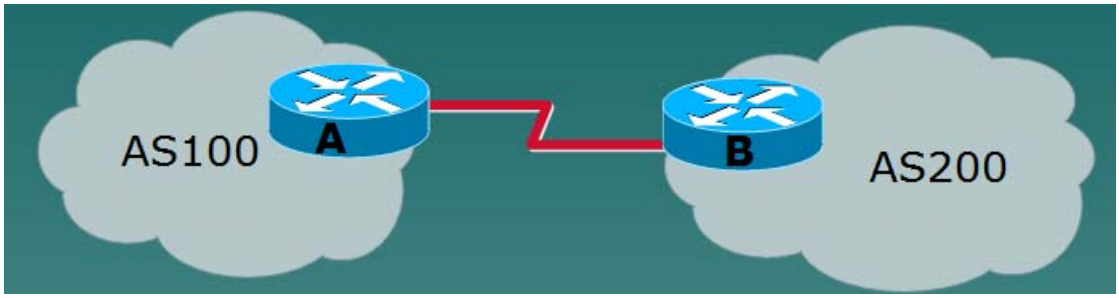
LABEL	DESCRIPTION
Peer Router ID	Enter the 32-bit ID (in IP address format) of the other ABR in the virtual link.
Authentication	Select the authentication method the virtual link uses. This authentication protects the integrity, but not the confidentiality, of routing updates. For OSPF, the Zyxel Device supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated Authentication Type field to **Same as Area**. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information. **None** uses no authentication. **Text** uses a plain text password that is sent over the network (not very secure). **MD5** uses an MD5 password and authentication ID (most secure). **Same as Area** has the virtual link also use the **Authentication** settings above.
Text Authentication Key	This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
MD5 Authentication ID	This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255.
MD5 Authentication Key	This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

10.8 BGP (Border Gateway Protocol)

The Zyxel Device supports eBGP (exterior Border Gate Protocol) to route IPv4 traffic between routers in different Autonomous Systems (AS). An AS number is a number from 1 to 4294967295), that identifies an autonomous system. 4200000000 – 4294967294 are private AS numbers.

See Section 10.7 on page 324 for more information on autonomous systems.

Figure 227 eBGP Concept



10.8.1 Allow BGP Packets to Enter the Zyxel Device

You must first allow BGP packets to enter the Zyxel Device from the WAN.

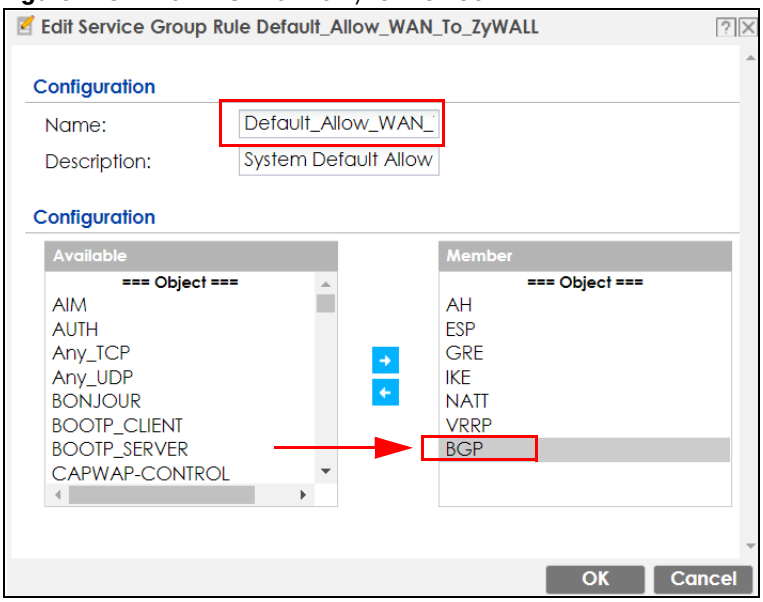
1 Go to **Configuration > Object > Service > Service Group**

2 Select the **Default_Allow_WAN_To_ZyWALL** rule and click **Edit**.

3 Move BGP from **Available** to **Member**.

4 Click **OK**.

Figure 228 Allow BGP to the Zyxel Device

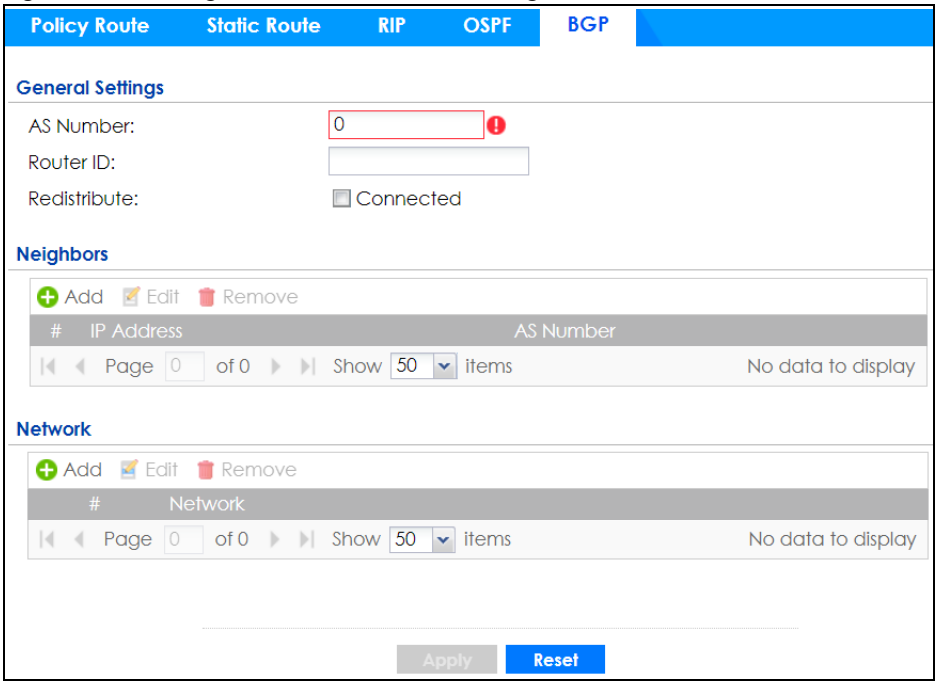


10.8.2 Configuring the BGP Screen

Use this screen to configure BGP information about the Zyxel Device and its peer BGP routers.

Click **Configuration > Network** > **Routing > BGP** to open the following screen.

Figure 229 Configuration > Network > Routing > BGP



The following table describes the labels in this screen.

Table 134 Configuration > Network > Routing Protocol > BGP

LABEL	DESCRIPTION
AS Number	Type a number from 1 to 4294967295 in this field. Note: The Zyxel Device can only belong to one AS at a time.
Router ID	Type the IP address of the interface on the Zyxel Device. This field is optional.
Redistribute	Select **Connected** to redistribute routes of directly attached devices to the Zyxel Device into the BGP Routing Information Base (RIB).
Neighbors	This section displays information about peer BGP routers in neighboring AS'. Note: The maximum number of neighboring BGP routers supported by the Zyxel Device is 5.
Add	Click this to configure BGP criteria for a new peer BGP router.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
IP Address	This displays the IPv4 address of the peer BGP router in a neighboring AS.
AS Number	This displays the AS Number of the peer BGP router in a neighboring AS.
Network	Use this section to add routes that will be announced to all BGP neighbors. Note: You may configure up to 16 network routes.
Add	Click this to configure network information for a new route.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.

Table 134 Configuration > Network > Routing Protocol > BGP (continued)

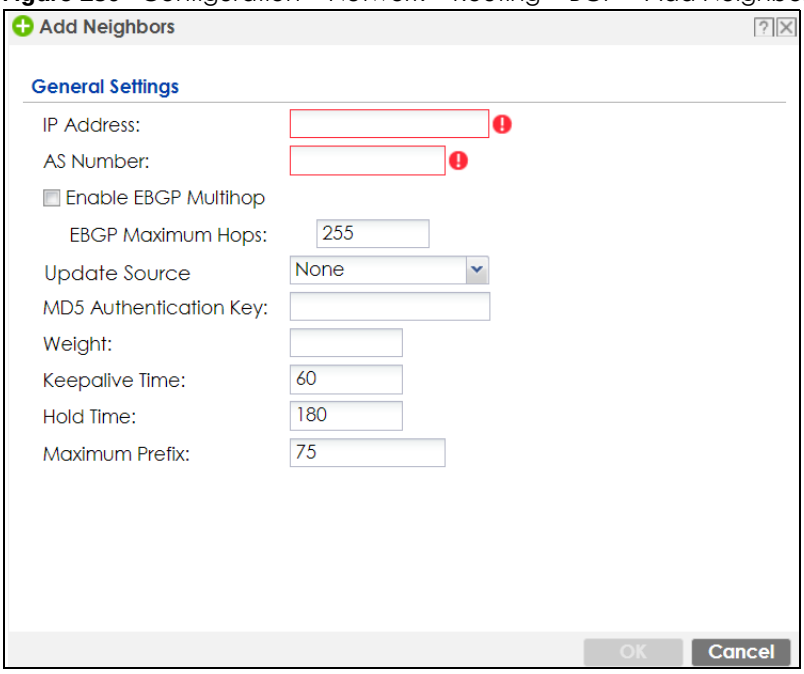
LABEL	DESCRIPTION
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This field is a sequential value, and it is not associated with a specific area.
Network	This displays the IP address and the number of subnet mask bits for the peer BGP route.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

10.8.3 The BGP Neighbors Screen

Use this screen to configure BGP information about a peer BGP router.

Click **Configuration > Network** > **Routing > BGP > Add Neighbors** to open the following screen.

Figure 230 Configuration > Network > Routing > BGP > Add Neighbors



The following table describes the labels in this screen.

Table 135 Configuration > Network > Routing Protocol > BGP

LABEL	DESCRIPTION
IP Address	Type the IP address of the interface on the peer BGP router.
AS Number	Type a number from 1 to 4294967295 in this field. Get the number from your service provider.
Enable EBGP Multihop	Select this to allow the Zyxel Device to attempt BGP connections to external peers on indirectly connected networks. eBGP neighbors must also perform multihop. Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.
EBGP Maximum Hops	Enter a maximum hop count from <1-255>. The default is 255.

Table 135 Configuration > Network > Routing Protocol > BGP (continued)

LABEL	DESCRIPTION
Update Source	Use this to allow BGP sessions use the selected interface for TCP connections. • Choose **Gateway** and then enter the gateway IP address • Choose **Interface** and then select a Zyxel Device interface. • Choose **None** to use the closest interface.
MD5 authentication key	Type the default password for MD5 authentication of communication between the Zyxel Device and the peer BGP router. The password can consist of alphanumeric characters and the underscore, and it can be up to 63 characters long.
Weight	Specify a weight value for all routes learned from this peer BGP router in the specified network. The route with the highest weight gets preference.
Keepalive Time	Keepalive messages are sent by the Zyxel Device to a peer BGP router to inform it that the BGP connection between the two is still active. The **Keepalive Time** is the interval between each Keepalive message sent by the Zyxel Device. We recommend **Keepalive Time** is 1/3 of the **Hold Time** time.
Hold Time	This is the maximum time the Zyxel Device waits to receive a Keepalive message from a peer BGP router before it declares that the peer BGP router is dead. **Hold Time** must be greater than the **Keepalive Time**.
Maximum Prefix	A prefix is a network address (IP/subnet mask) that a BGP router can reach and that it shares with its neighbors. Set the maximum number, from 1 to 4294967295, of prefixes that can be received from a neighbor. This limits the number of prefixes that the Zyxel Device is allowed to receive from a neighbor. If extra prefixes are received, the Zyxel Device ends the connection with the peer BGP router. You need to edit the peer BGP router configuration to bring the connection back.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

10.8.4 Example Scenario

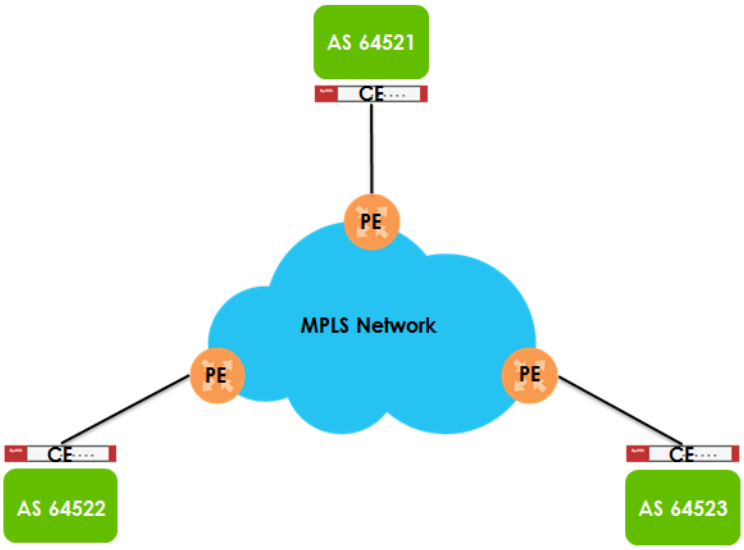
This is an example scenario for using BGP on the Zyxel Device.

10.8.4.1 Scenario: CE - PE (MLPS)

In this scenario, you want to transmit BGP packets from a **CE** router (Zyxel Device) to a peer BGP **PE** router in an **MPLS** network.

- **CE**: The Zyxel Device is the customer edge router located on the customer premises and connects to a PE router in the service provider MPLS network.
- **PE**: The provider edge router is located at the edge of the service provider MPLS network.
- **MPLS:** MultiProtocol Label Switching (MPLS) forwards data from one network node to the next based on path labels rather than network addresses.

Figure 231 Scenario 1: CE Router - to - MPLS



10.8.4.2 CE - PE Configuration Process

The process for configuring BGP in this scenario is:

1. Configure the AS number for BGP on the Zyxel Device (CE) in **Configuration > Network** > **Routing > BGP**.

   Note: The Zyxel Device can only belong to one AS at a time.

2. Configure the AS number and BGP criteria of the peer BGP routers (PE) in the neighboring AS in **Configuration > Network** > **Routing > BGP > Add Neighbors**.

   Note: The maximum number of neighboring BGP routers supported by the Zyxel Device is 5.

3. Configure the network for BGP routes in the neighboring AS.

   Note: You may configure up to 16 network routes.

CHAPTER 11
DDNS

11.1 DDNS Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

11.1.1 What You Can Do in this Chapter

- Use the **DDNS** screen (see Section 11.2 on page 338) to view a list of the configured DDNS domain names and their details.
- Use the **DDNS Add/Edit** screen (see Section 11.2.1 on page 339) to add a domain name to the Zyxel Device or to edit the configuration of an existing domain name.

11.1.2 What You Need to Know

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, Dynamic DNS (DDNS) maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current (dynamic) IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

You must set up a dynamic DNS account with a supported DNS service provider before you can use Dynamic DNS services with the Zyxel Device. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the Zyxel Device supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

Table 136 DDNS Service Providers

PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com
Dynu	Basic, Premium	www.dynu.com
No-IP	No-IP	www.no-ip.com
Peanut Hull	Peanut Hull	www.oray.cn
3322	3322 Dynamic DNS, 3322 Static DNS	www.3322.org
Selfhost	Selfhost	selfhost.de

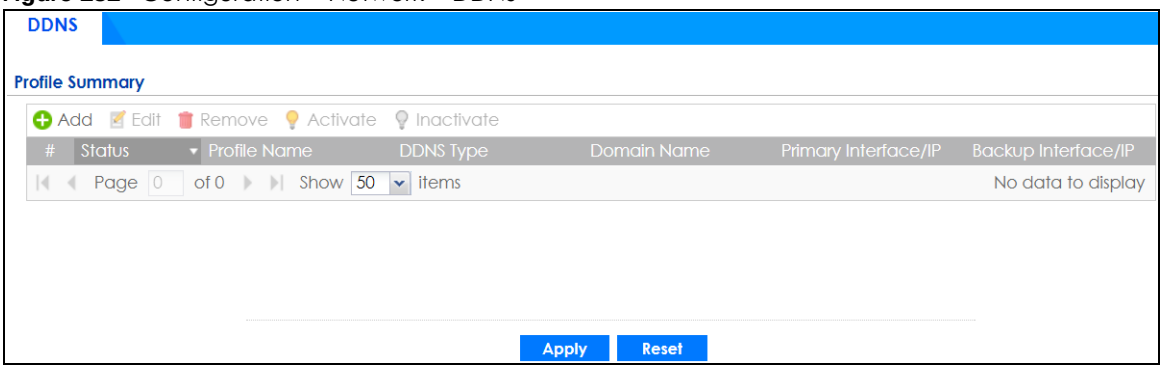
Note: Record your DDNS account's user name, password, and domain name to use to configure the Zyxel Device.

After you configure the Zyxel Device, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

11.2 The DDNS Screen

The **DDNS** screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names. Click **Configuration > Network > DDNS** to open the following screen.

Figure 232 Configuration > Network > DDNS



The following table describes the labels in this screen.

Table 137 Configuration > Network > DDNS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This is the number of an individual DDNS profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field displays the descriptive profile name for this entry.
DDNS Type	This field displays which DDNS service you are using.
Domain Name	This field displays each domain name the Zyxel Device can route.
Primary Interface/IP	This field displays the interface to use for updating the IP address mapped to the domain name followed by how the Zyxel Device determines the IP address for the domain name. **from interface** - The IP address comes from the specified interface. **auto detected** -The DDNS server checks the source IP address of the packets from the Zyxel Device for the IP address to use for the domain name. **custom** - The IP address is static.
Backup Interface/IP	This field displays the alternate interface to use for updating the IP address mapped to the domain name followed by how the Zyxel Device determines the IP address for the domain name. The Zyxel Device uses the backup interface and IP address when the primary interface is disabled, its link is down or its connectivity check fails. **from interface** - The IP address comes from the specified interface. **auto detected** -The DDNS server checks the source IP address of the packets from the Zyxel Device for the IP address to use for the domain name. **custom** - The IP address is static.

Table 137 Configuration > Network > DDNS (continued)

LABEL	DESCRIPTION
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

11.2.1 The Dynamic DNS Add/Edit Screen

The **DDNS Add/Edit** screen allows you to add a domain name to the Zyxel Device or to edit the configuration of an existing domain name. Click **Configuration > Network > DDNS** and then an **Add** or **Edit** icon to open this screen.

Figure 233 Configuration > Network > DDNS > Add

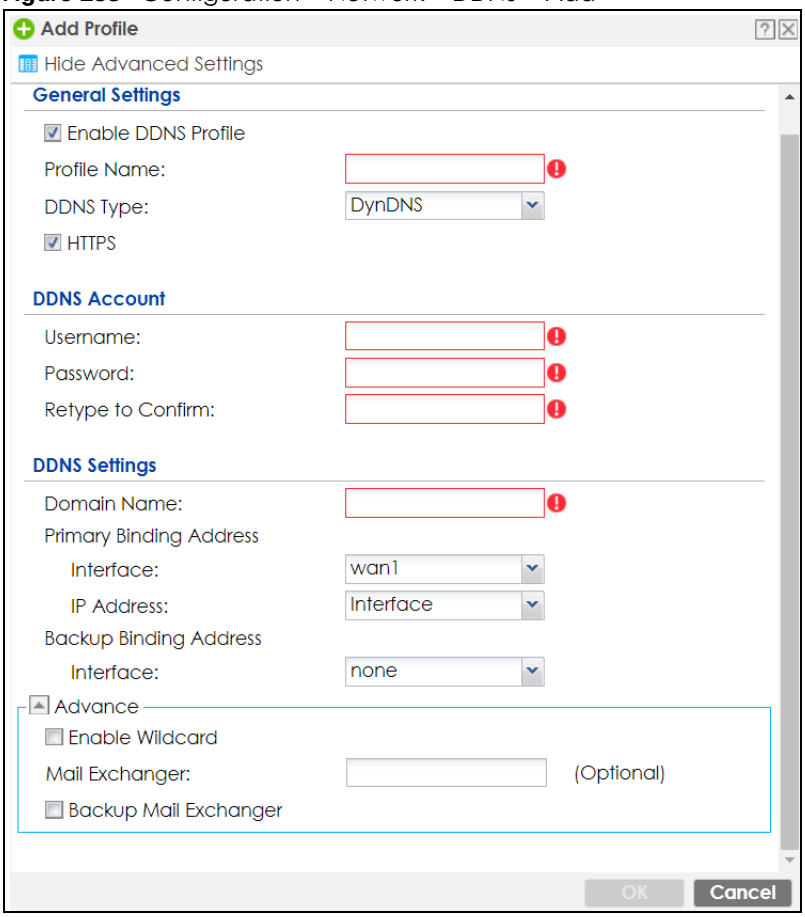
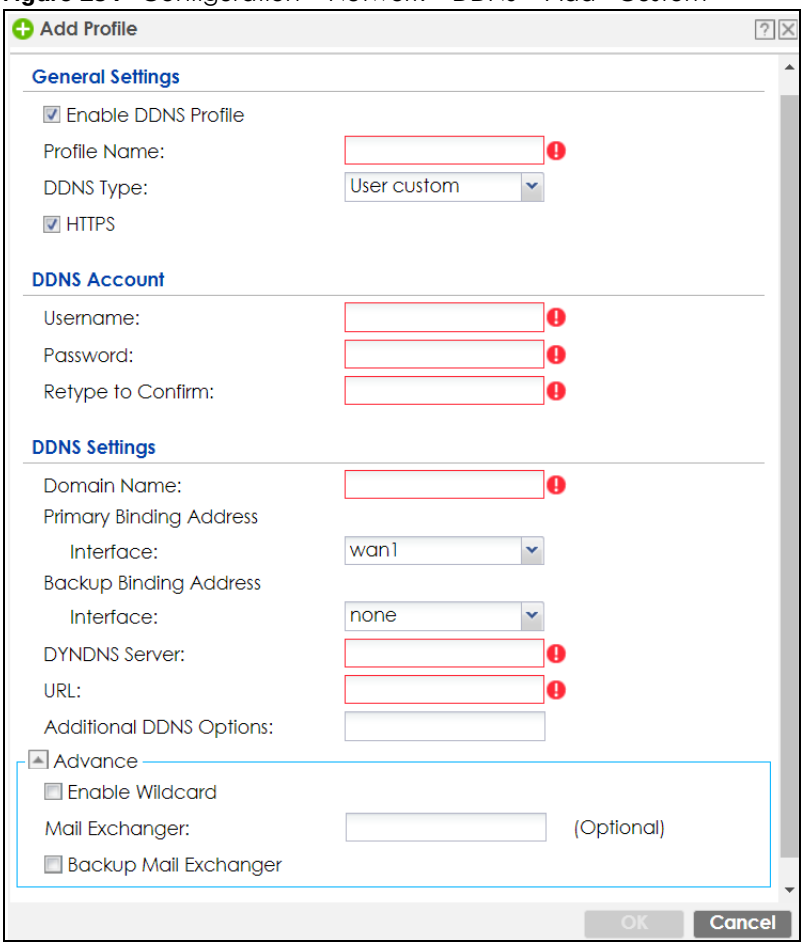


Figure 234 Configuration > Network > DDNS > Add - Custom



The following table describes the labels in this screen.

Table 138 Configuration > Network > DDNS > Add

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DDNS Profile	Select this check box to use this DDNS entry.
Profile Name	When you are adding a DDNS entry, type a descriptive name for this DDNS entry in the Zyxel Device. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is read-only when you are editing an entry.
DDNS Type	Select the type of DDNS service you are using. Select **User custom** to create your own DDNS service and configure the **DYNDNS Server**, **URL**, and **Additional DDNS Options** fields below.
HTTPS	Select this to encrypt traffic using SSL (port 443), including traffic with username and password, to the DDNS server. Not all DDNS providers support this option.
Username	Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed. For a Dynu DDNS entry, this user name is the one you use for logging into the service, not the name recorded in your personal information in the Dynu website.

Table 138 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Password	Type the password provided by the DDNS provider. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed.
Retype to Confirm	Type the password again to confirm it.
DDNS Settings	
Domain name	Type the domain name you registered. You can use up to 255 characters.
Primary Binding Address	Use these fields to set how the Zyxel Device determines the IP address that is mapped to your domain name in the DDNS server. The Zyxel Device uses the **Backup Binding Address** if the interface specified by these settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface.
IP Address	The options available in this field vary by DDNS provider. **Interface** -The Zyxel Device uses the IP address of the specified interface. This option appears when you select a specific interface in the **Primary Binding Address Interface** field. **Auto** - If the interface has a dynamic IP address, the DDNS server checks the source IP address of the packets from the Zyxel Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Zyxel Device and the DDNS server. Note: The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. **Custom** - If you have a static IP address, you can select this to use it for the domain name. The Zyxel Device still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name.
Backup Binding Address	Use these fields to set an alternate interface to map the domain name to when the interface specified by the **Primary Binding Interface** settings is not available.
Interface	Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface. Select **None** to not use a backup address.
IP Address	The options available in this field vary by DDNS provider. **Interface** -The Zyxel Device uses the IP address of the specified interface. This option appears when you select a specific interface in the **Backup Binding Address Interface** field. **Auto** -The DDNS server checks the source IP address of the packets from the Zyxel Device for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the Zyxel Device and the DDNS server. Note: The Zyxel Device may not determine the proper IP address if there is an HTTP proxy server between the Zyxel Device and the DDNS server. **Custom** - If you have a static IP address, you can select this to use it for the domain name. The Zyxel Device still sends the static IP address to the DDNS server.
Custom IP	This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name.
Enable Wildcard	This option is only available with a DynDNS account. Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Table 138 Configuration > Network > DDNS > Add (continued)

LABEL	DESCRIPTION
Mail Exchanger	This option is only available with a DynDNS account. DynDNS can route email for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes email for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger. If you are using this service, type the host record of your mail server here. Otherwise leave the field blank. See www.dyndns.org for more information about mail exchangers.
Backup Mail Exchanger	This option is only available with a DynDNS account. Select this check box if you are using DynDNS's backup service for email. With this service, DynDNS holds onto your email if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service.
DYNDNS Server	This field displays when you select **User custom** from the **DDNS Type** field above. Type the IP address of the server that will host the DDSN service.
URL	This field displays when you select **User custom** from the **DDNS Type** field above. Type the URL that can be used to access the server that will host the DDSN service.
Additional DDNS Options	This field displays when you select **User custom** from the **DDNS Type** field above. These are the options supported at the time of writing: • dyndns_system to specify the DYNDNS Server type - for example, dyndns@dyndns.org • ip_server_name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

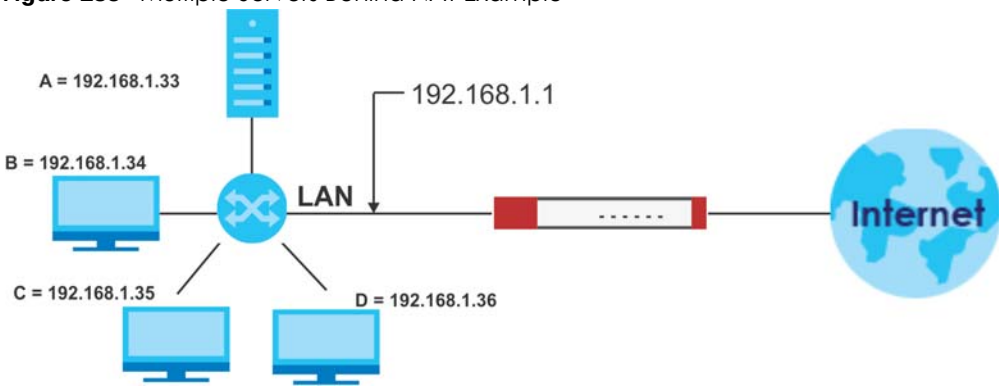
CHAPTER 12
NAT

12.1 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 is changed to a different IP address known within another network. Use Network Address Translation (NAT) to make computers on a private network behind the Zyxel Device available outside the private network. If the Zyxel Device has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

Suppose 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 235 Multiple Servers Behind NAT Example



12.1.1 What You Can Do in this Chapter

Use the **NAT** screens (see Section 12.2 on page 344) to view and manage the list of NAT rules and see their configuration details. You can also create new NAT rules and edit or delete existing ones.

12.1.2 What You Need to Know

NAT is also known as virtual server, port forwarding, or port translation.

Well-known Ports

Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and designated as well-known ports. The following list specifies the ports used by the server process as its contact ports. See Section 35.7 on page 665 (Configuration > Object > Service) for more information about service objects.

- Well-known ports range from 0 to 1023.
- Registered ports range from 1024 to 49151.
- Dynamic ports (also called private ports) range from 49152 to 65535.

Table 139 Well-known Ports

PORT	TCP/UDP	DESCRIPTION
1	TCP	TCP Port Service Multiplexer (TCPMUX)
20	TCP	FTP - Data
21	TCP	FTP - Control
22	TCP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
42	UDP	Host Name Server (Nameserv)
43	TCP	Whols
53	TCP/UDP	Domain Name System (DNS)
67	UDP	BOOTP/DHCP server
68	UDP	BOOTP/DHCP client
69	UDP	Trivial File Transfer Protocol (TFTP)
79	TCP	Finger
80	TCP	HTTP
110	TCP	POP3
119	TCP	Newsgroup (NNTP)
123	UDP	Network Time Protocol (NTP)
135	TCP/UDP	RPC Locator service
137	TCP/UDP	NetBIOS Name Service
138	UDP	NetBIOS Datagram Service
139	TCP	NetBIOS Datagram Service
143	TCP	Interim Mail Access Protocol (IMAP)
161	UDP	SNMP
179	TCP	Border Gateway Protocol (BGP)
389	TCP/UDP	Lightweight Directory Access Protocol (LDAP)
443	TCP	HTTPS
445	TCP	Microsoft - DS
636	TCP	LDAP over TLS/SSL (LDAPS)
953	TCP	BIND DNS
990	TCP	FTP over TLS/SSL (FTPS)
995	TCP	POP3 over TLS/SSL (POP3S)

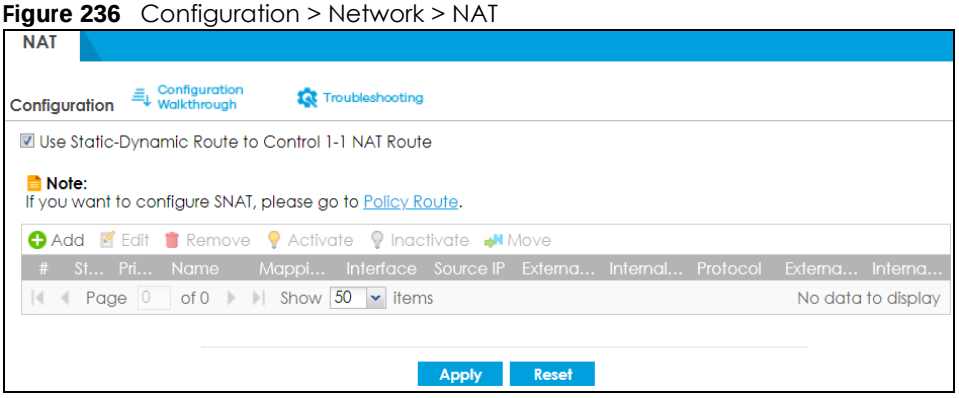
12.2 The NAT Screen

The **NAT** summary screen provides a summary of all NAT rules and their configuration. In addition, this screen allows you to create new NAT rules and edit and delete existing NAT rules. To access this screen,

login to the Web Configurator and click **Configuration > Network > NAT**. The following screen appears, providing a summary of the existing NAT rules.

Click on the icons to go to the OneSecurity website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 236 Configuration > Network > NAT



The following table describes the labels in this screen.

Table 140 Configuration > Network > NAT

LABEL	DESCRIPTION
Use Static-Dynamic Route to Control 1-1 NAT Route	If you are using **SiteToSite VPN** and **1-1 SNAT**, it's recommended that you select this check box. Otherwise, you'll need to create policy route rules for VPN and Destination NAT traffic. Note that the selection of this check box will change the priority of the routing flow **(SiteToSite VPN**, **Static-Dynamic Route**, and **1-1 SNAT)**. See Chapter 42 on page 842 for more information about the routing flow.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This field displays the priority for the entry. The smaller the number, the higher the priority.
Name	This field displays the name of the entry.
Mapping Type	This field displays what kind of NAT this entry performs: **Virtual Server**, **1:1 NAT**, or **Many 1:1 NAT**.
Interface	This field displays the interface on which packets for the NAT entry are received.
Source IP	This field displays the source IP address (or address object) of traffic that matches this NAT entry. It displays **any** if there is no restriction on the source IP address.
External IP	This field displays the original destination IP address (or address object) of traffic that matches this NAT entry. It displays **any** if there is no restriction on the original destination IP address.

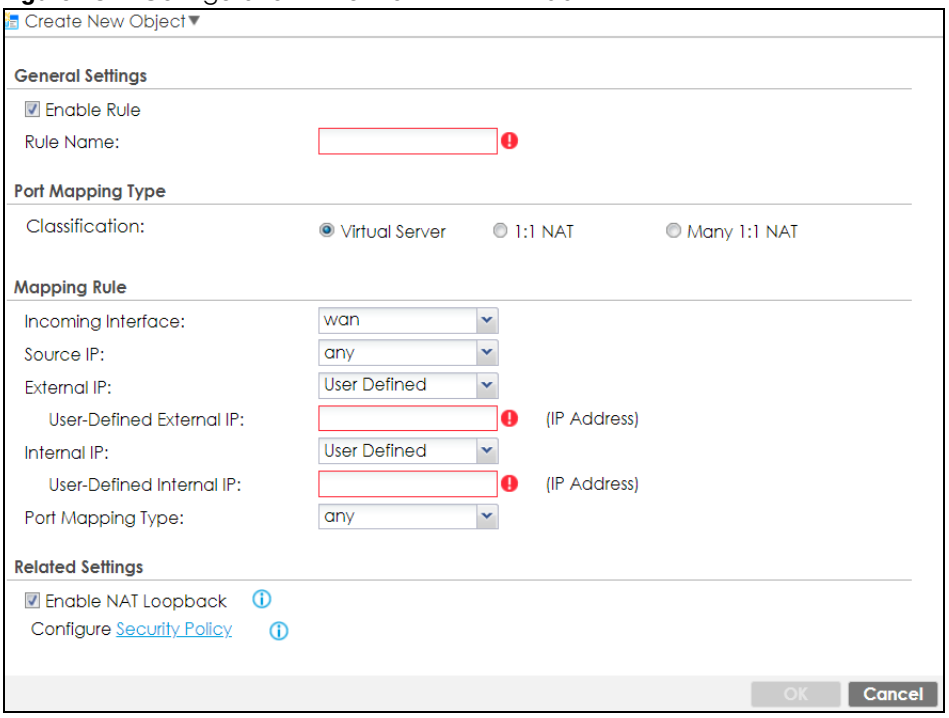
Table 140 Configuration > Network > NAT (continued)

LABEL	DESCRIPTION
Internal IP	This field displays the new destination IP address for the packet.
Protocol	This field displays the service used by the packets for this NAT entry. It displays **any** if there is no restriction on the services.
External Port	This field displays the original destination port(s) of packets for the NAT entry. This field is blank if there is no restriction on the original destination port.
Internal Port	This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

12.2.1 The NAT Add/Edit Screen

The **NAT Add/Edit** screen lets you create new NAT rules and edit existing ones. To open this window, open the **NAT** summary screen. (See Section 12.2 on page 344.) Then, click on an **Add** icon or **Edit** icon to open the following screen.

Figure 237 Configuration > Network > NAT > Add



The following table describes the labels in this screen.

Table 141 Configuration > Network > NAT > Add

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable Rule	Use this option to turn the NAT rule on or off.
Rule Name	Type in the name of the NAT rule. The name is used to refer to the NAT rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

Table 141 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Classification	Select what kind of NAT this rule is to perform. **Virtual Server** - This makes computers on a private network behind the Zyxel Device available to a public network outside the Zyxel Device (like the Internet). **1:1 NAT** - If the private network server will initiate sessions to the outside clients, select this to have the Zyxel Device translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server. **Many 1:1 NAT -** If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, select this to have the Zyxel Device translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses. One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases configuration effort since you only create one rule.
Incoming Interface	Select the interface on which packets for the NAT rule must be received. It can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface.
Source IP	Specify the source IP address of the packets received by this NAT rule's specified incoming interface. **any** - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface. **User Defined** - Select this to manually enter an IP address in the **User Defined** field. For example, you could enter a static IP address. Host address - select a address object to use the IP address it specifies.
External IP	Specify the destination IP address of the packets received by this NAT rule's specified incoming interface. The specified IP address will be translated to the **Internal IP** address. **any** - Select this to use all of the incoming interface's IP addresses including dynamic addresses or those of any virtual interfaces built upon the selected incoming interface. **User Defined** - Select this to manually enter an IP address in the **User Defined** field. For example, you could enter a static public IP assigned by the ISP without having to create a virtual interface for it. Host address - select a host address object to use the IP address it specifies. The list also includes address objects based on interface IPs. So for example you could select an address object based on a WAN interface even if it has a dynamic IP address.
User Defined External IP	This field is available if **External IP** is **User Defined**. Type the destination IP address that this NAT rule supports.
External IP Subnet/ Range	This field displays for **Many 1:1 NAT**. Select the destination IP address subnet or IP address range that this NAT rule supports. The original and mapped IP address subnets or ranges must have the same number of IP addresses.
Internal IP	Select to which translated destination IP address this NAT rule forwards packets. **User Defined** - this NAT rule supports a specific IP address, specified in the **User Defined** field. HOST address - the drop-down box lists all the HOST address objects in the Zyxel Device. If you select one of them, this NAT rule supports the IP address specified by the address object.
User Defined Internal IP	This field is available if **Internal IP** is **User Defined**. Type the translated destination IP address that this NAT rule supports.
Internal IP Subnet/ Range	This field displays for **Many 1:1 NAT**. Select to which translated destination IP address subnet or IP address range this NAT rule forwards packets. The original and mapped IP address subnets or ranges must have the same number of IP addresses.

Table 141 Configuration > Network > NAT > Add (continued)

LABEL	DESCRIPTION
Port Mapping Type	Use the drop-down list box to select how many original destination ports this NAT rule supports for the selected destination IP address (**Original IP**). Choices are: **Any** - this NAT rule supports all the destination ports. **Port** - this NAT rule supports one destination port. **Ports** - this NAT rule supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service. **Service** - this NAT rule supports a service such as FTP (see **Object > Service > Service**) **Service-Group** - this NAT rule supports a group of services such as all service objects related to DNS (see **Object > Service > Service Group**)
Protocol Type	This field is available if **Mapping Type** is **Port** or **Ports**. Select the protocol (**TCP**, **UDP**, or **Any**) used by the service requesting the connection.
External Port	This field is available if **Mapping Type** is **Port**. Enter the external destination port this NAT rule supports.
Internal Port	This field is available if **Mapping Type** is **Port**. Enter the translated destination port if this NAT rule forwards the packet.
External Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of original destination ports this NAT rule supports.
External End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of original destination ports this NAT rule supports.
Internal Start Port	This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of translated destination ports if this NAT rule forwards the packet.
Internal End Port	This field is available if **Mapping Type** is **Ports**. Enter the end of the range of translated destination ports if this NAT rule forwards the packet. The original port range and the mapped port range must be the same size.
Enable NAT Loopback	Enable NAT loopback to allow users connected to any interface (instead of just the specified **Incoming Interface**) to use the NAT rule's specified **External IP** address to access the **Internal IP** device. For users connected to the same interface as the **Internal IP** device, the Zyxel Device uses that interface's IP address as the source address for the traffic it sends from the users to the **Internal IP** device. For example, if you configure a NAT rule to forward traffic from the WAN to a LAN server, enabling NAT loopback allows users connected to other interfaces to also access the server. For LAN users, the Zyxel Device uses the LAN interface's IP address as the source address for the traffic it sends to the LAN server. See NAT Loopback on page 349 for more details. If you do not enable NAT loopback, this NAT rule only applies to packets received on the rule's specified incoming interface.
Security Policy	By default the security policy blocks incoming connections from external addresses. After you configure your NAT rule settings, click the **Security Policy** link to configure a security policy to allow the NAT rule's traffic to come in. The Zyxel Device checks NAT rules before it applies To-Zyxel Device security policies, so To-Zyxel Device security policies, do not apply to traffic that is forwarded by NAT rules. The Zyxel Device still checks other security policies, according to the source IP address and mapped IP address.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to return to the **NAT** summary screen without creating the NAT rule (if it is new) or saving any changes (if it already exists).

12.3 NAT Technical Reference

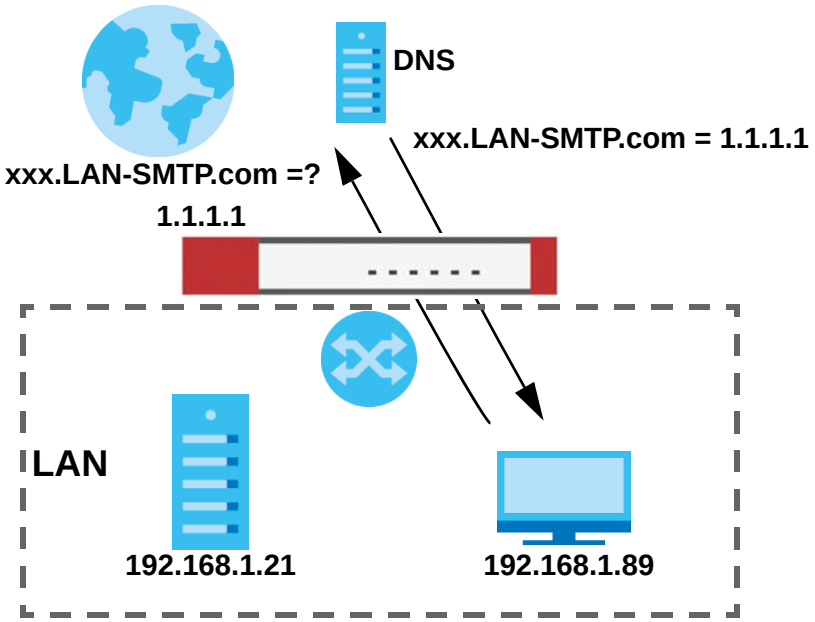
Here is more detailed information about NAT on the Zyxel Device.

NAT Loopback

Suppose an NAT 1:1 rule maps a public IP address to the private IP address of a LAN SMTP email server to give WAN users access. NAT loopback allows other users to also use the rule's original IP to access the mail server.

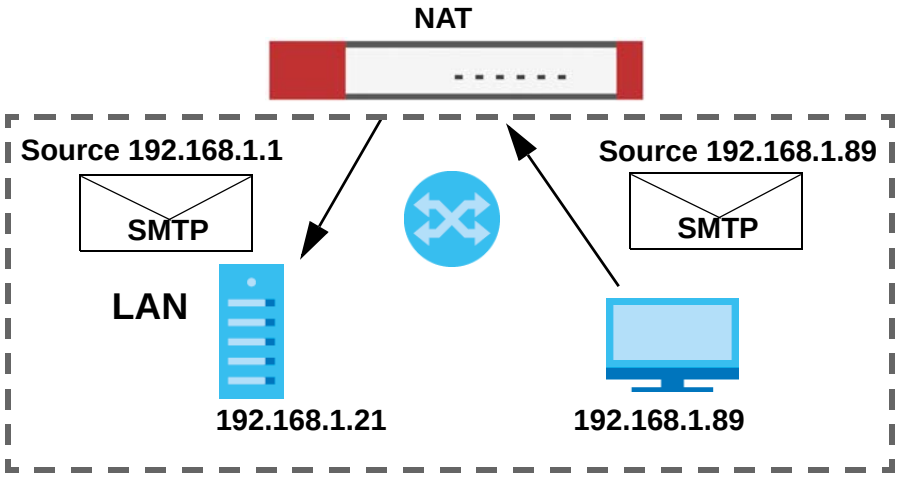
For example, a LAN user's computer at IP address 192.168.1.89 queries a public DNS server to resolve the SMTP server's domain name (xxx.LAN-SMTP.com in this example) and gets the SMTP server's mapped public IP address of 1.1.1.1.

Figure 238 LAN Computer Queries a Public DNS Server



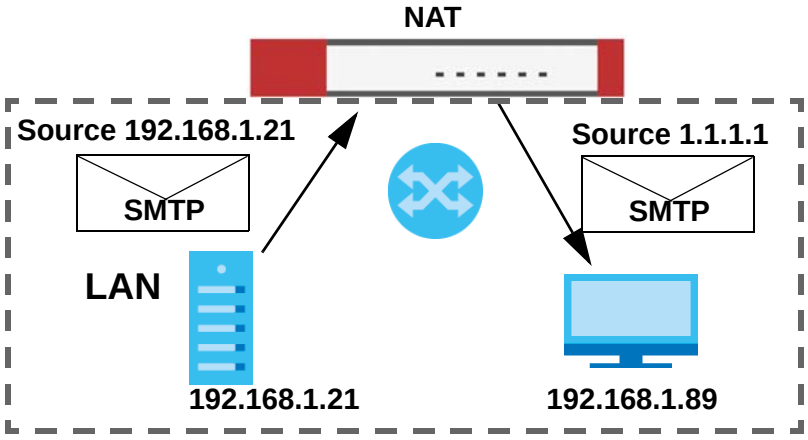
The LAN user's computer then sends traffic to IP address 1.1.1.1. NAT loopback uses the IP address of the Zyxel Device's LAN interface (192.168.1.1) as the source address of the traffic going from the LAN users to the LAN SMTP server.

Figure 239 LAN to LAN Traffic



The LAN SMTP server replies to the Zyxel Device's LAN IP address and the Zyxel Device changes the source address to 1.1.1.1 before sending it to the LAN user. The return traffic's source matches the original destination address (1.1.1.1). If the SMTP server replied directly to the LAN user without the traffic going through NAT, the source would not match the original destination address which would cause the LAN user's computer to shut down the session.

Figure 240 LAN to LAN Return Traffic



CHAPTER 13
Redirect Service

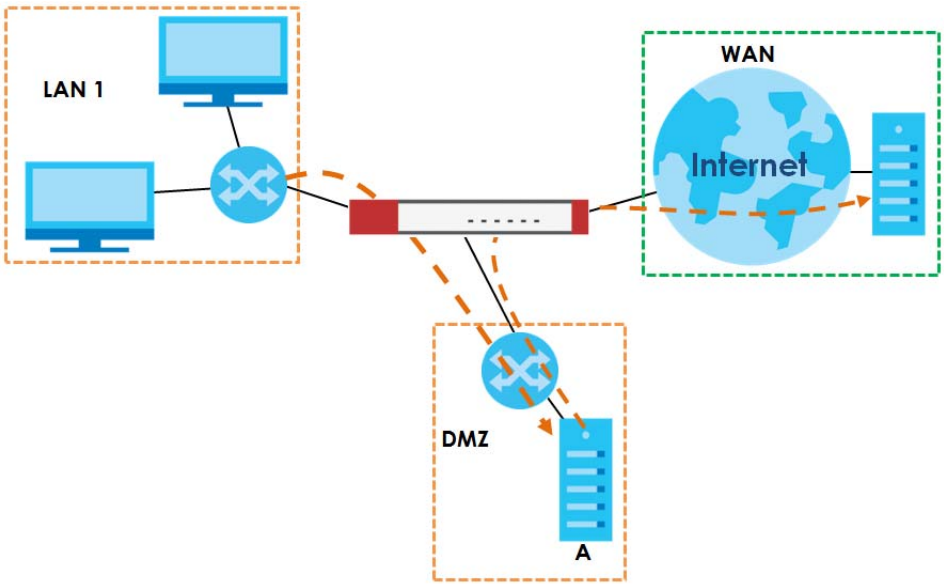
13.1 Overview

Redirect Service redirects HTTP and SMTP traffic.

13.1.1 HTTP Redirect

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the Zyxel Device) to a web proxy server. In the following example, proxy server **A** is connected to the **DMZ** interface. When a client connected to the **LAN1** zone wants to open a web page, its HTTP request is redirected to proxy server **A** first. If proxy server **A** cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server **A** then forwards the response to the client.

Figure 241 HTTP Redirect Example

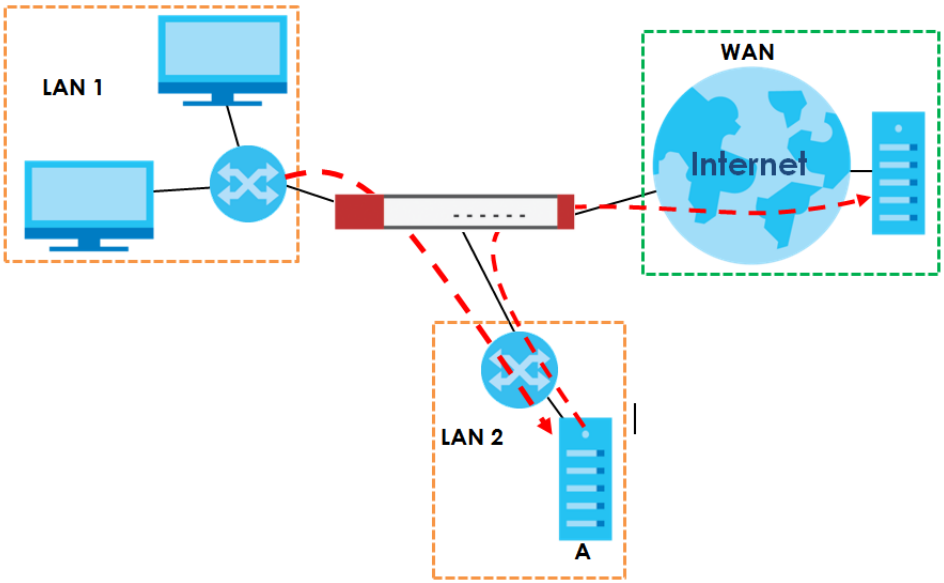


13.1.2 SMTP Redirect

SMTP redirect forwards the authenticated client's SMTP message to a SMTP server, that handles all outgoing email messages. In the following example, SMTP server **A** is connected to the **lan2** interface in the **LAN2** zone. When a client connected to the **lan1** interface in the **LAN1** zone logs into the Zyxel Device and wants to send an email, its SMTP message is redirected to SMTP server **A**. SMTP server **A** then sends it to a mail server, where the message will be delivered to the recipient.

The Zyxel Device forwards SMTP traffic using TCP port 25.

Figure 242 SMTP Redirect Example



13.1.3 What You Can Do in this Chapter

Use the **Redirect Service** screens (see Section 13.2 on page 354) to display and edit the HTTP and SMTP redirect rules.

13.1.4 What You Need to Know

Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a security policy or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

HTTP Redirect, Security Policy and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

1. Security Policy
2. Application Patrol
3. HTTP Redirect
4. Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the Zyxel Device checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no security policy blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet. To make the example in Figure 241 on page 351 work, make sure you have the following settings.

For HTTP traffic between **lan1** and **dmz**:

- a from LAN1 to DMZ security policy (default) to allow HTTP requests from **lan1** to **dmz**. Responses to this request are allowed automatically.
- a application patrol rule to allow HTTP traffic between **lan1** and **dmz**.
- a HTTP redirect rule to forward HTTP traffic from **lan1** to proxy server **A**.

For HTTP traffic between **dmz** and **wan1**:

- a from DMZ to WAN security policy (default) to allow HTTP requests from **dmz** to **wan1**. Responses to these requests are allowed automatically.
- a application patrol rule to allow HTTP traffic between **dmz** and **wan1**.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

SMTP

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of email messages between servers. Email clients (also called email applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve email. Email clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many email applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

SMTP Redirect, Firewall and Policy Route

With SMTP redirect, the relevant packet flow for SMTP traffic is:

1. Firewall
2. SMTP Redirect
3. Policy Route

Even if you set a policy route to the same incoming interface and service as a SMTP redirect rule, the Zyxel Device checks the SMTP redirect rules first and forwards SMTP traffic to a SMTP server if matched. You need to make sure there is no firewall rule(s) blocking the SMTP traffic from the client to the SMTP server.

You also need to manually configure a policy route to forward the SMTP traffic from the SMTP server to the Internet. To make the example in Figure 242 on page 352 work, make sure you have the following settings.

For SMTP traffic between **lan1** and **lan2**:

- a from LAN1 to LAN2 firewall rule to allow SMTP messages from **lan1** to **lan2**. Responses to this request are allowed automatically.
- a SMTP redirect rule to forward SMTP traffic from **lan1** to SMTP server **A**.

For SMTP traffic between **lan2** and **wan1**:

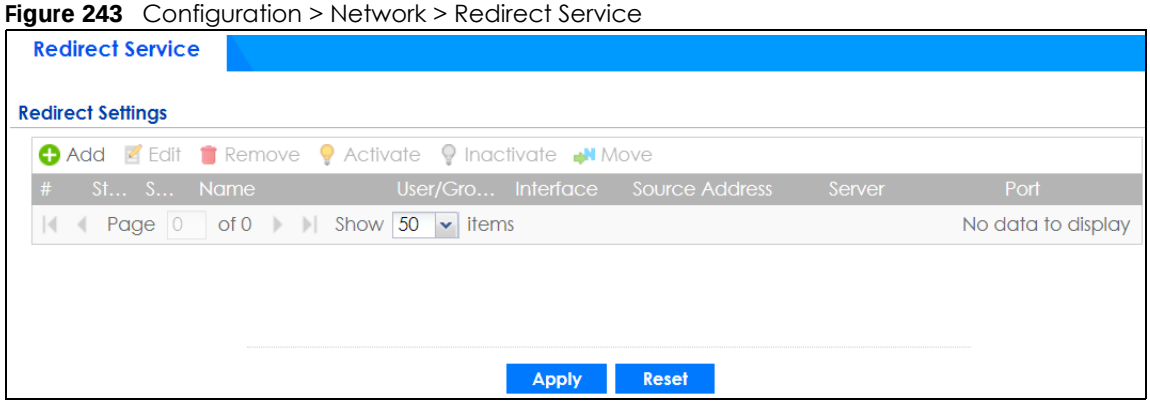
- a from LAN2 to WAN firewall rule (default) to allow SMTP messages from **lan2** to **wan1**. Responses to these requests are allowed automatically.
- a policy route to forward SMTP messages from SMTP server **A** to the Internet.

13.2 The Redirect Service Screen

To configure redirection of a HTTP or SMTP request, click **Configuration > Network > HTTP Redirect**. This screen displays the summary of the redirect rules.

Note: You can configure up to one HTTP redirect rule and one SMTP redirect rule for each (incoming) interface.

Figure 243 Configuration > Network > Redirect Service



The following table describes the labels in this screen.

Table 142 Configuration > Network > Redirect Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change a rule's position in the numbered list, select the rule and click **Move** to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
#	This field is a sequential value, and it is not associated with a specific entry.

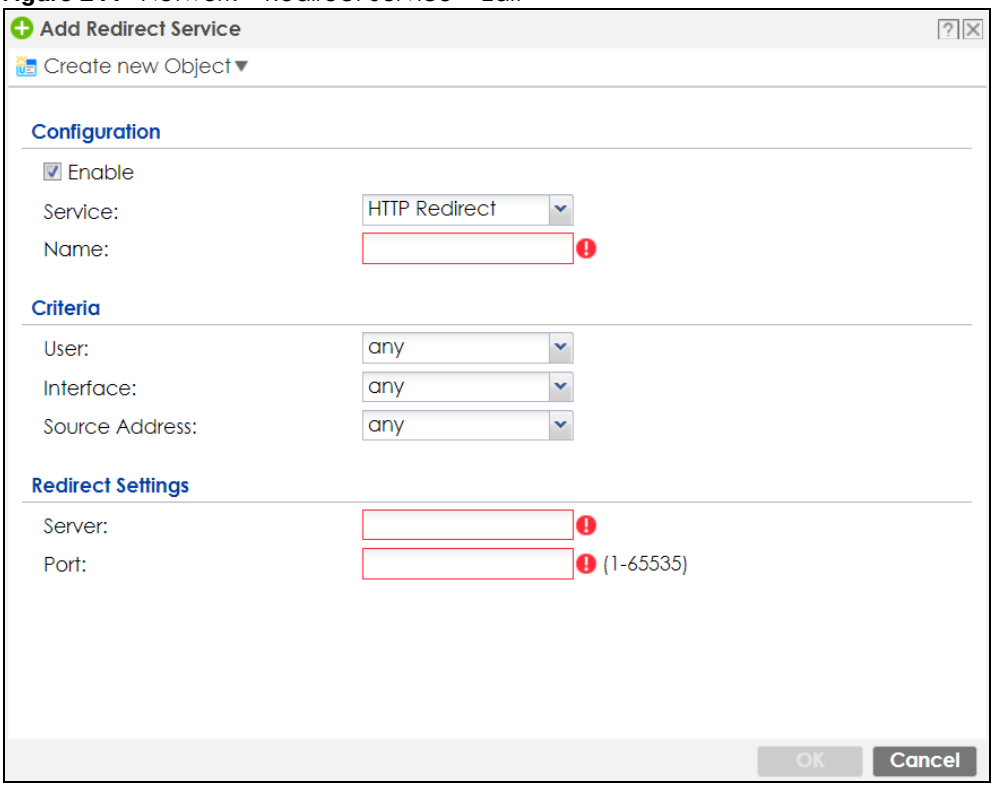
Table 142 Configuration > Network > Redirect Service (continued)

LABEL	DESCRIPTION
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Service	This is the name of the service: HTTP or SMTP.
Name	This is the descriptive name of a rule.
User/Group	This is the user account or user group name to which this rule is applied.
Interface	This is the interface on which the request must be received.
Source Address	This is the name of the source IP address object from which the traffic should be sent. If **any** displays, the rule is effective for every source.
Server	This is the IP address of the HTTP proxy server or the SMTP server to which the matched traffic is forwarded.
Port	This is the service port number used by the HTTP proxy server or SMTP server.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

13.2.1 The Redirect Service Edit Screen

Click **Network > Redirect Service** to open the **Redirect Service** screen. Then click the **Add** or **Edit** icon to open the **Redirect Service Edit** screen where you can configure the rule.

Figure 244 Network > Redirect Service > Edit



The following table describes the labels in this screen.

Table 143 Network > Redirect Service > Edit

LABEL	DESCRIPTION
Enable	Use this option to turn the Redirect Service rule on or off.
Service	Select the service to be redirected: **HTTP Redirect** or **SMTP redirect.**
Name	Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Criteria	
User	Select the user account or user group name to which this rule is applied.
Interface	Select the interface on which the request must be received for the Zyxel Device to forward it to the specified server.
Source Address	Select the name of the source IP address object from which the traffic should be sent. Select **any** for the rule to be effective for every source.
Redirect Settings	
Server	Enter the IP address of the HTTP proxy or SMTP server.
Port	Enter the port number that the HTTP proxy or SMTP server uses.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 14
ALG

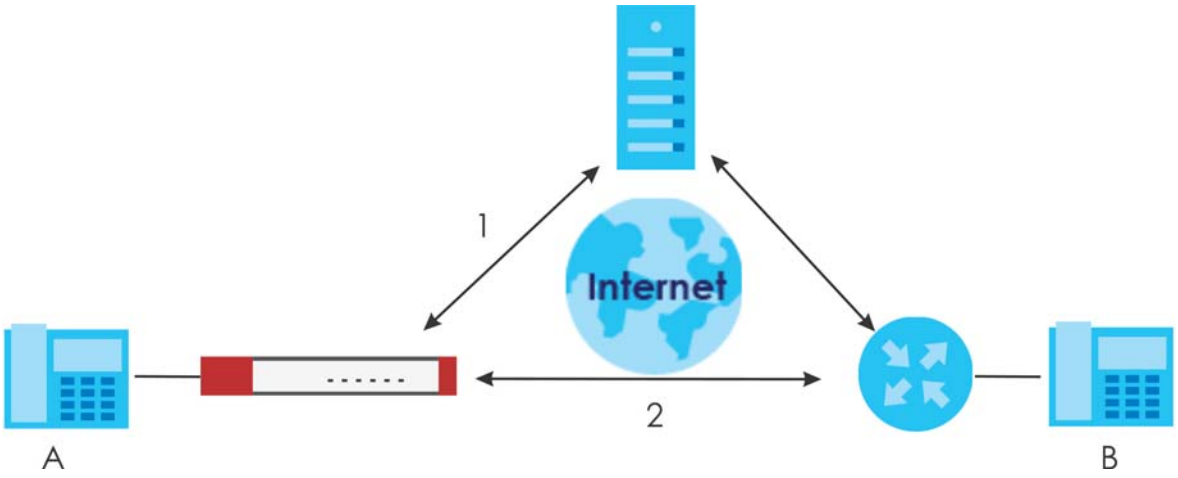
14.1 ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the Zyxel Device's NAT.

- SIP - Session Initiation Protocol (SIP) - An application-layer protocol that can be used to create voice and multimedia sessions over Internet.
- H.323 - A teleconferencing protocol suite that provides audio, data and video conferencing.
- FTP - File Transfer Protocol - an Internet file transfer service.

The following example shows SIP signaling (**1**) and audio (**2**) sessions between SIP clients **A** and **B** and the SIP server.

Figure 245 SIP ALG Example



The ALG feature is only needed for traffic that goes through the Zyxel Device's NAT.

14.1.1 What You Need to Know

Application Layer Gateway (ALG), NAT and Security Policy

The Zyxel Device can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the Zyxel Device's NAT and security policy. The Zyxel Device dynamically creates an implicit NAT session and security policy session for the application's traffic from the WAN to the LAN. The ALG on the Zyxel Device supports all of the Zyxel Device's NAT mapping types.

FTP ALG

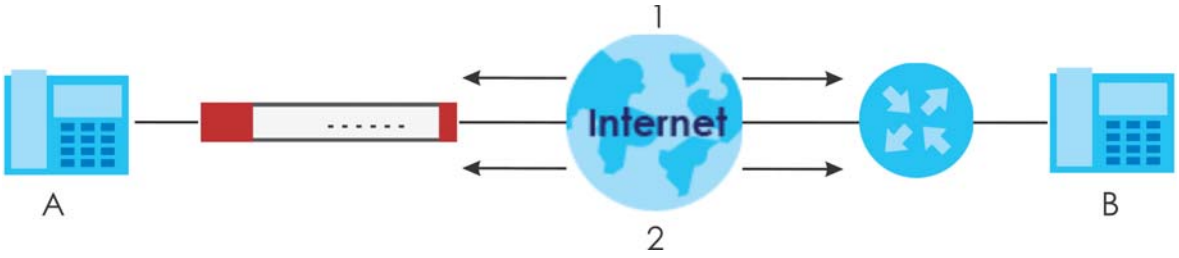
The FTP ALG allows TCP packets with a specified port destination to pass through. If the FTP server is located on the LAN, you must also configure NAT (port forwarding) and security policies if you want to allow access to the server from the WAN. Bandwidth management can be applied to FTP ALG traffic.

H.323 ALG

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the Zyxel Device routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- The H.323 ALG operates on TCP packets with a specified port destination.
- Bandwidth management can be applied to H.323 ALG traffic.
- The Zyxel Device allows H.323 audio connections.
- The Zyxel Device can also apply bandwidth management to traffic that goes through the H.323 ALG.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

Figure 246 H.323 ALG Example



SIP ALG

- SIP phones can be in any zone (including LAN, DMZ, WAN), and the SIP server and SIP clients can be in the same network or different networks. The SIP server cannot be on the LAN. It must be on the WAN or the DMZ.
- There should be only one SIP server (total) on the Zyxel Device's private networks. Any other SIP servers must be on the WAN. So for example you could have a Back-to-Back User Agent such as the IPPBX x6004 or an asterisk PBX on the DMZ or on the LAN but not on both.
- Using the SIP ALG allows you to use bandwidth management on SIP traffic. Bandwidth management can be applied to FTP ALG traffic. Use the option in the **Configuration > BWM** screen to configure the highest bandwidth available for SIP traffic.
- The SIP ALG handles SIP calls that go through NAT or that the Zyxel Device routes. You can also make other SIP calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The SIP ALG supports peer-to-peer SIP calls. The security policy (by default) allows peer to peer calls from the LAN zone to go to the WAN zone and blocks peer to peer calls from the WAN zone to the LAN zone.
- The SIP ALG allows UDP packets with a specified port destination to pass through.
- The Zyxel Device allows SIP audio connections.

- You do not need to use TURN (Traversal Using Relay NAT) for VoIP devices behind the Zyxel Device when you enable the SIP ALG.
- Configuring the SIP ALG to use custom port numbers for SIP traffic also configures the application patrol (see Chapter 26 on page 515) to use the same port numbers for SIP traffic. Likewise, configuring the application patrol to use custom port numbers for SIP traffic also configures SIP ALG to use the same port numbers for SIP traffic.

Peer-to-Peer Calls and the Zyxel Device

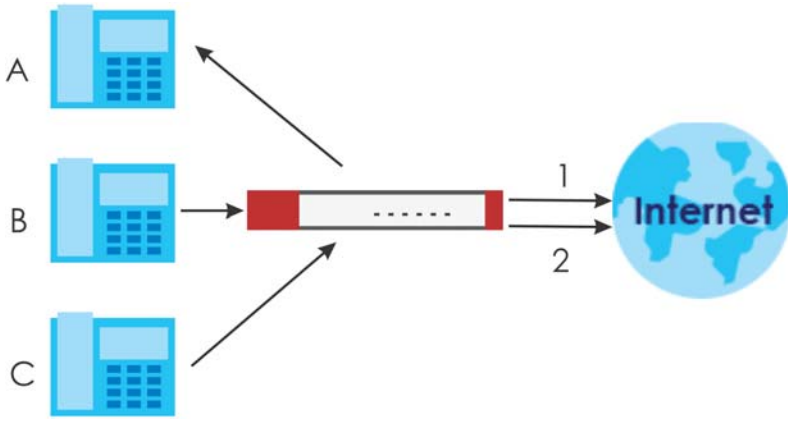
The Zyxel Device ALG can allow peer-to-peer VoIP calls for both H.323 and SIP. You must configure the security policy and NAT (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the security policy and NAT (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 (or SIP) calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the Zyxel Device correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the security policy and NAT to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 (or SIP) calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

Figure 247 VoIP Calls from the WAN with Multiple Outgoing Calls



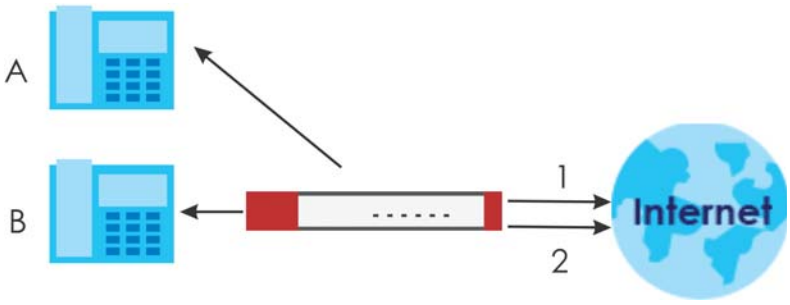
VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the Zyxel Device, you can configure different security policy and NAT (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 (or SIP) calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the Zyxel Device correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure security policy and NAT rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different security policy and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding

policy routes to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

Figure 248 VoIP with Multiple WAN IP Addresses



14.1.2 Before You Begin

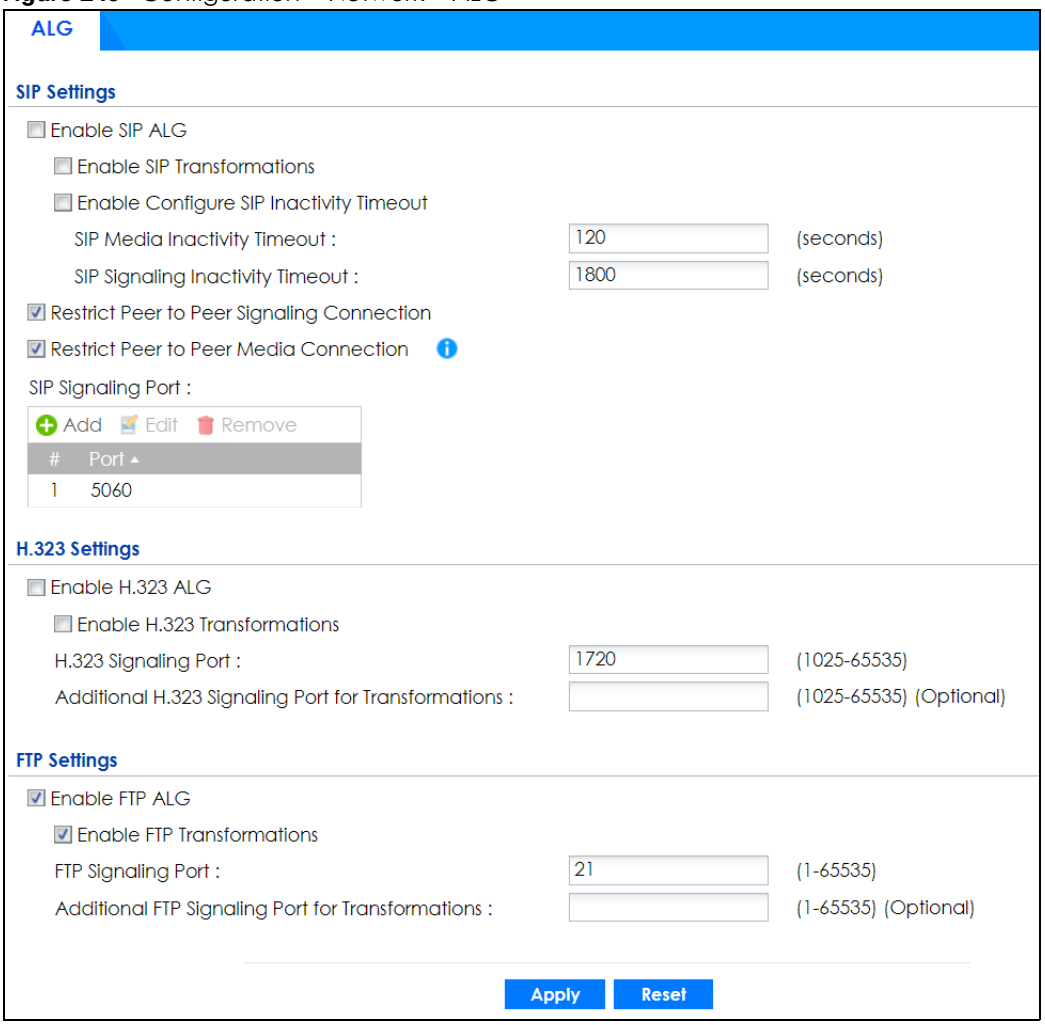
You must also configure the security policy and enable NAT in the Zyxel Device to allow sessions initiated from the WAN.

14.2 The ALG Screen

Click **Configuration > Network > ALG** to open the **ALG** screen. Use this screen to turn ALGs off or on, configure the port numbers to which they apply, and configure SIP ALG time outs.

Note: If the Zyxel Device provides an ALG for a service, you must enable the ALG in order to use the application patrol on that service's traffic.

Figure 249 Configuration > Network > ALG



The following table describes the labels in this screen.

Table 144 Configuration > Network > ALG

LABEL	DESCRIPTION
Enable SIP ALG	Turn on the SIP ALG to detect SIP traffic and help build SIP sessions through the Zyxel Device's NAT. Enabling the SIP ALG also allows you to use the application patrol to detect SIP traffic and manage the SIP traffic's bandwidth (see Chapter 26 on page 515).
Enable SIP Transformations	Select this to have the Zyxel Device modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload.
Enable Configure SIP Inactivity Timeout	Select this option to have the Zyxel Device apply SIP media and signaling inactivity time out limits. These timeouts will take priority over the SIP session time out "Expires" value in a SIP registration response packet.
SIP Media Inactivity Timeout	Use this field to set how many seconds (1~86400) the Zyxel Device will allow a SIP session to remain idle (without voice traffic) before dropping it. If no voice packets go through the SIP ALG before the timeout period expires, the Zyxel Device deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

Table 144 Configuration > Network > ALG (continued)

LABEL	DESCRIPTION
SIP Signaling Inactivity Timeout	Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the Zyxel Device. If the SIP client does not have this mechanism and makes no calls during the Zyxel Device SIP timeout, the Zyxel Device deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400).
Restrict Peer to Peer Signaling Connection	A signaling connection is used to set up the SIP connection. Enable this if you want signaling connections to only arrive from the IP address(es) you registered with. Signaling connections from other IP addresses will be dropped.
Restrict Peer to Peer Media Connection	A media connection is the audio transfer in a SIP connection. Enable this if you want media connections to only arrive from the IP address(es) you registered with. Media connections from other IP addresses will be dropped. You should disable this if have registered for cloud VoIP services.
SIP Signaling Port	If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here. Use the **Add** icon to add fields if you are also using SIP on additional UDP port numbers.
Enable H.323 ALG	Turn on the H.323 ALG to detect H.323 traffic (used for audio communications) and help build H.323 sessions through the Zyxel Device's NAT. Enabling the H.323 ALG also allows you to use the application patrol to detect H.323 traffic and manage the H.323 traffic's bandwidth (see Chapter 26 on page 515).
Enable H.323 Transformations	Select this to have the Zyxel Device modify IP addresses and port numbers embedded in the H.323 data payload. You do not need to use this if you have a H.323 device or server that will modify IP addresses and port numbers embedded in the H.323 data payload.
H.323 Signaling Port	If you are using a custom TCP port number (not 1720) for H.323 traffic, enter it here.
Additional H.323 Signaling Port for Transformations	If you are also using H.323 on an additional TCP port number, enter it here.
Enable FTP ALG	Turn on the FTP ALG to detect FTP (File Transfer Program) traffic and help build FTP sessions through the Zyxel Device's NAT. Enabling the FTP ALG also allows you to use the application patrol to detect FTP traffic and manage the FTP traffic's bandwidth (see Chapter 26 on page 515).
Enable FTP Transformations	Select this option to have the Zyxel Device modify IP addresses and port numbers embedded in the FTP data payload to match the Zyxel Device's NAT environment. Clear this option if you have an FTP device or server that will modify IP addresses and port numbers embedded in the FTP data payload to match the Zyxel Device's NAT environment.
FTP Signaling Port	If you are using a custom TCP port number (not 21) for FTP traffic, enter it here.
Additional FTP Signaling Port for Transformations	If you are also using FTP on an additional TCP port number, enter it here.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

14.3 ALG Technical Reference

Here is more detailed information about the Application Layer Gateway.

ALG

Some applications cannot operate through NAT (are NAT unfriendly) because they embed IP addresses and port numbers in their packets' data payload. The Zyxel Device examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the Zyxel Device uses an application for which the Zyxel Device has VoIP pass through enabled, the Zyxel Device translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the security policy so the application's traffic can come in from the WAN to the LAN.

ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The Zyxel Device does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

CHAPTER 15
UPnP

15.1 UPnP and NAT-PMP Overview

The Zyxel Device supports both UPnP and NAT-PMP to permit networking devices to discover each other and connect seamlessly.

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. In turn, a device can leave a network smoothly and automatically when it is no longer in use. A gateway that supports UPnP is called Internet Gateway Device (IGD). The standardized Device Control Protocol (DCP) is defined by the UPnP Forum for IGDs to configure port mapping automatically.

NAT Port Mapping Protocol (NAT-PMP), introduced by Apple and implemented in current Apple products, is used as an alternative NAT traversal solution to the UPnP IGD protocol. NAT-PMP runs over UDP port 5351. NAT-PMP is much simpler than UPnP IGD and mainly designed for small home networks. It allows a client behind a NAT router to retrieve the router's public IP address and port number and make them known to the peer device with which it wants to communicate. The client can automatically configure the NAT router to create a port mapping to allow the peer to contact it.

15.2 What You Need to Know

UPnP hardware is identified as an icon in the Network 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.

15.2.1 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.

See the NAT chapter for more information on NAT.

15.2.2 Cautions with UPnP and NAT-PMP

The automated nature of NAT traversal applications in establishing their own services and opening security policy 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 or NAT-PMP 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 or NAT-PMP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP or NAT-PMP if this is not your intention.

15.3 UPnP Screen

Use this screen to enable UPnP and NAT-PMP on your Zyxel Device.

Click **Configuration > Network > UPnP** to display the screen shown next.

Figure 250 Configuration > Network > UPnP

The following table describes the fields in this screen.

Table 145 Configuration > Network > UPnP

LABEL	DESCRIPTION
Enable UPnP	Select this check box to activate UPnP on the Zyxel Device. 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).
Enable NAT-PMP	NAT Port Mapping Protocol (NAT-PMP) automates port forwarding to allow a computer in a private network (behind the Zyxel Device) to automatically configure the Zyxel Device to allow computers outside the private network to contact it. Select this check box to activate NAT-PMP on the Zyxel Device. Be aware that anyone could use a NAT-PMP 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).
Allow UPnP or NAT-PMP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled or NAT-PMP-enabled applications to bypass the security policy. Clear this check box to have the security policy block all UPnP or NAT-PMP application packets (for example, MSN packets).
Outgoing WAN Interface	Select through which WAN interface(s) you want to send out traffic from UPnP-enabled or NAT-PMP-enabled applications. If the WAN interface you select loses its connection, the Zyxel Device attempts to use the other WAN interface. If the other WAN interface also does not work, the Zyxel Device drops outgoing packets from UPnP-enabled or NAT-PMP-enabled applications.
Support LAN List	The **Available** list displays the name(s) of the internal interface(s) on which the Zyxel Device supports UPnP and/or NAT-PMP. To enable UPnP and/or NAT-PMP on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the **Member** list. To remove an interface, select the name(s) in the **Member** list and click the left arrow button.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

15.4 Technical Reference

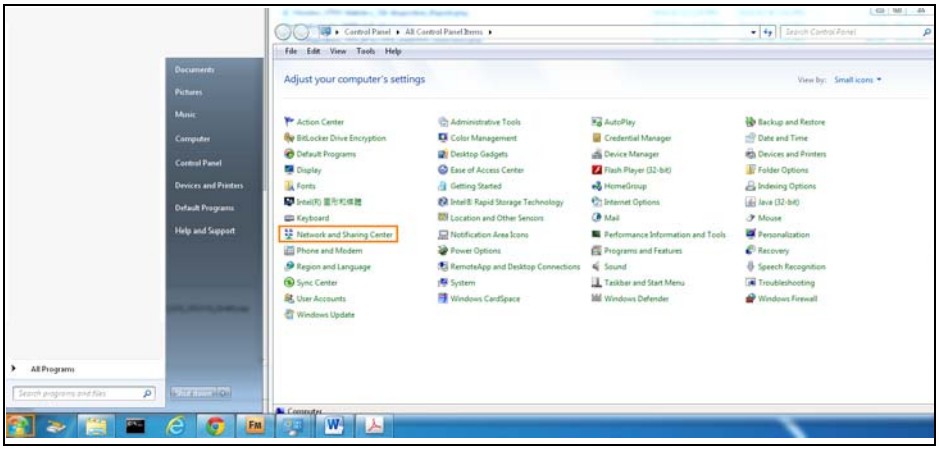
The sections show examples of using UPnP.

15.4.1 Turning on UPnP in Windows 7 Example

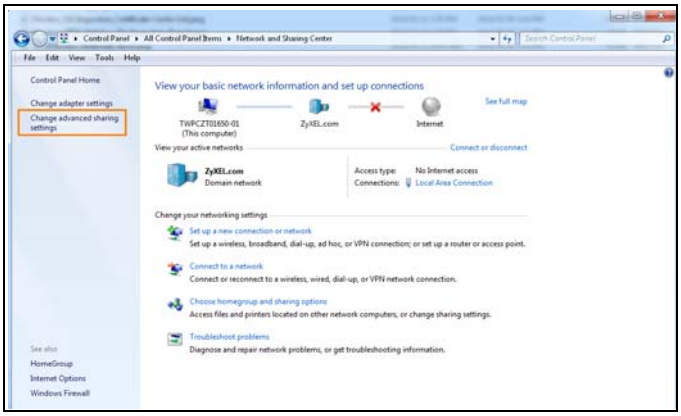
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the Zyxel Device.

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

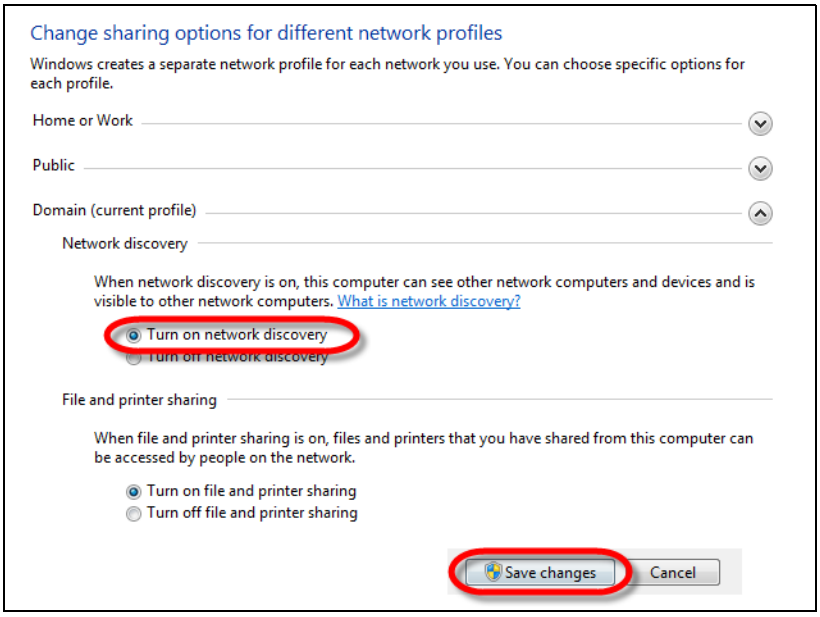
1 Click the start icon, **Control Panel** and then the **Network and Sharing Center.**



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.



15.4.1.1 Auto-discover Your UPnP-enabled Network Device

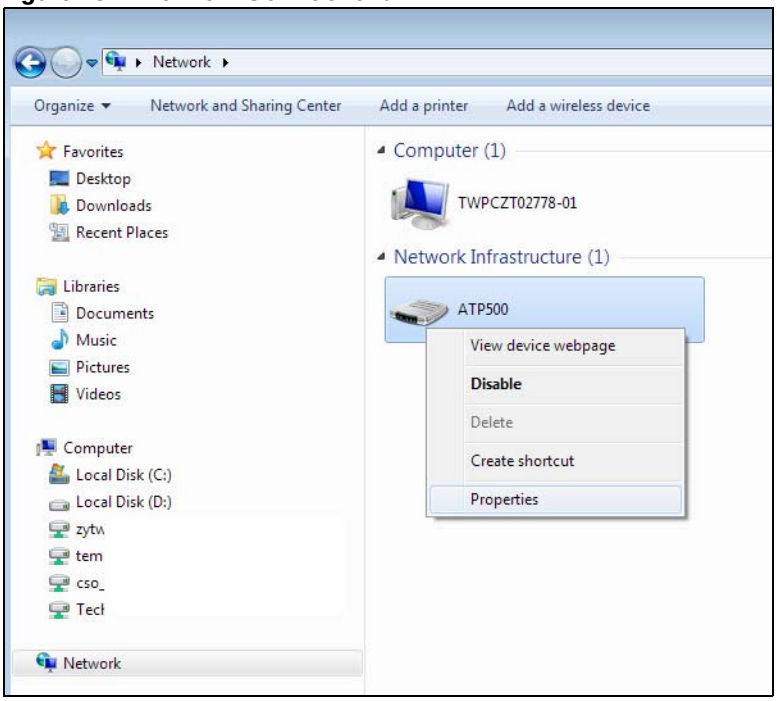
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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

1 Open the **Windows Explorer** and click **Network**.

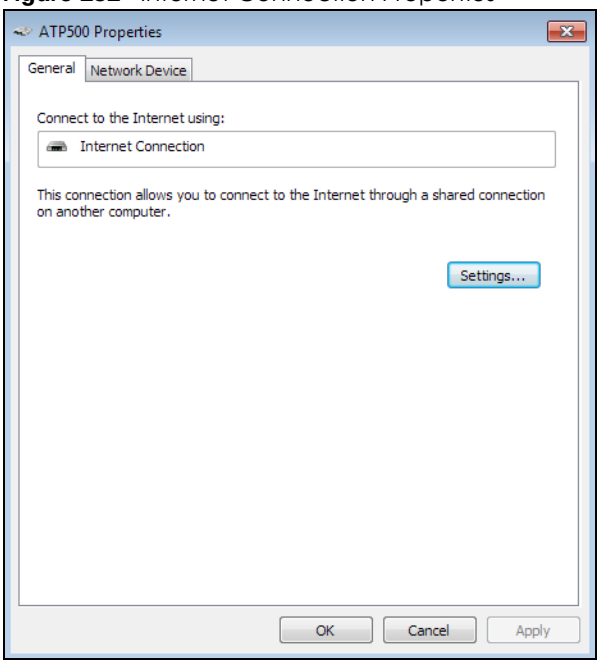
2 Right-click the device icon and select **Properties**.

Figure 251 Network Connections



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

Figure 252 Internet Connection Properties



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

Figure 253 Internet Connection Properties: Advanced Settings

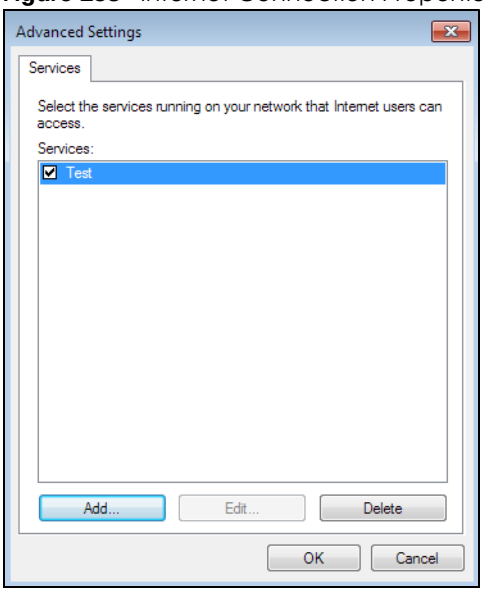
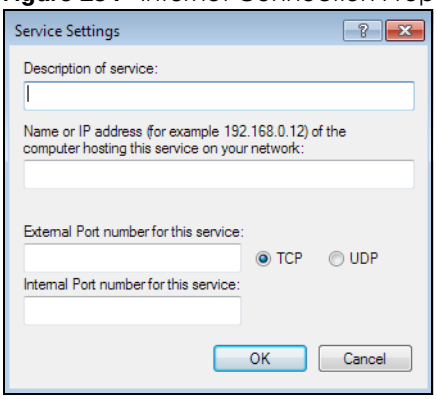


Figure 254 Internet Connection Properties: Advanced Settings: Add



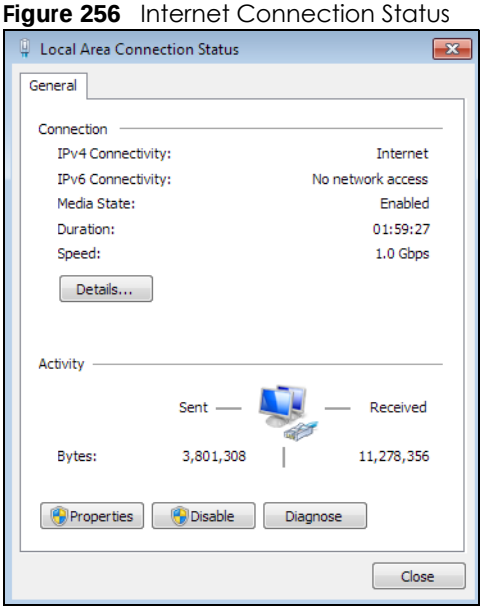
Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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

Figure 255 System Tray Icon

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

Figure 256 Internet Connection Status

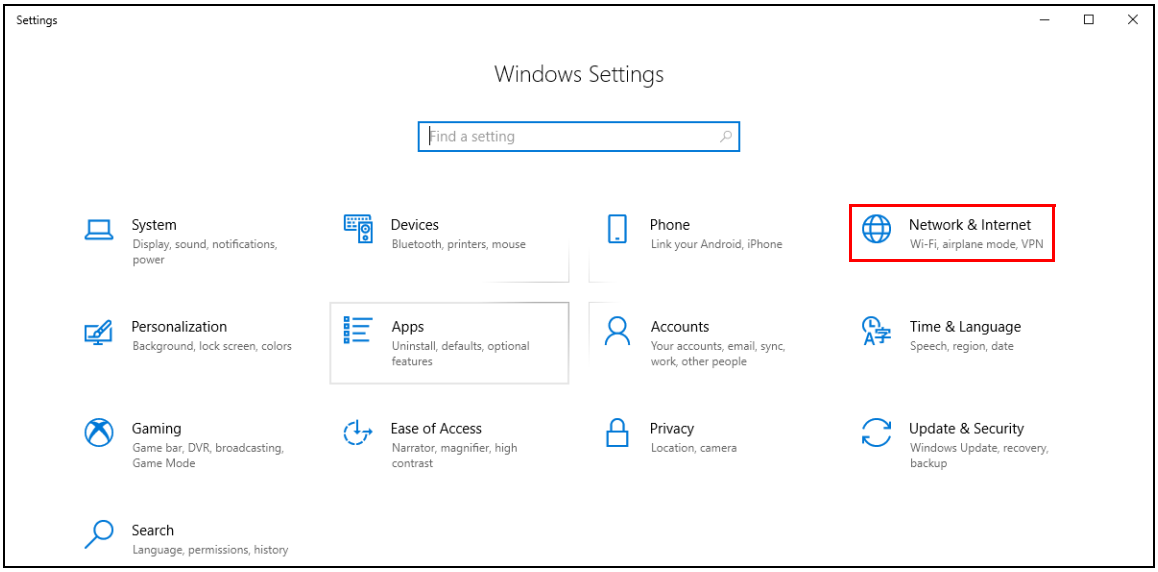


15.4.2 Turn on UPnP in Windows 10 Example

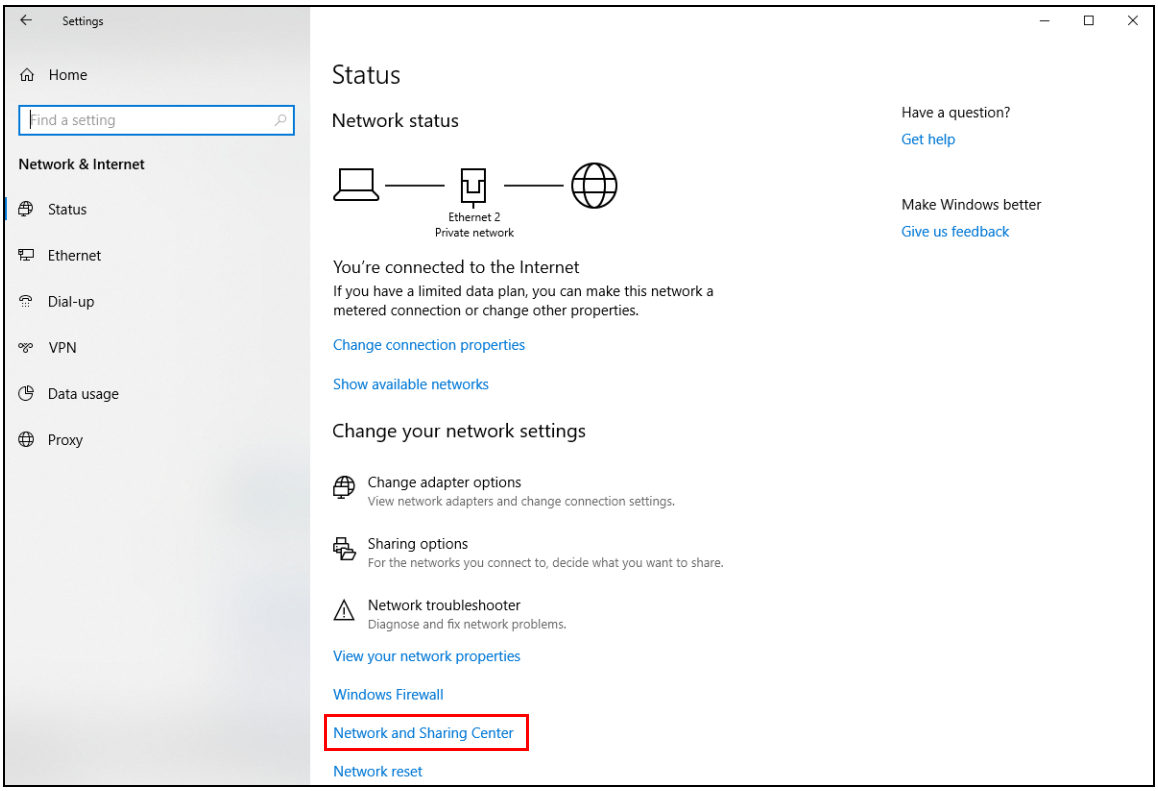
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the Zyxel Device by clicking **Network Setting > Home Networking > UPnP**.

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

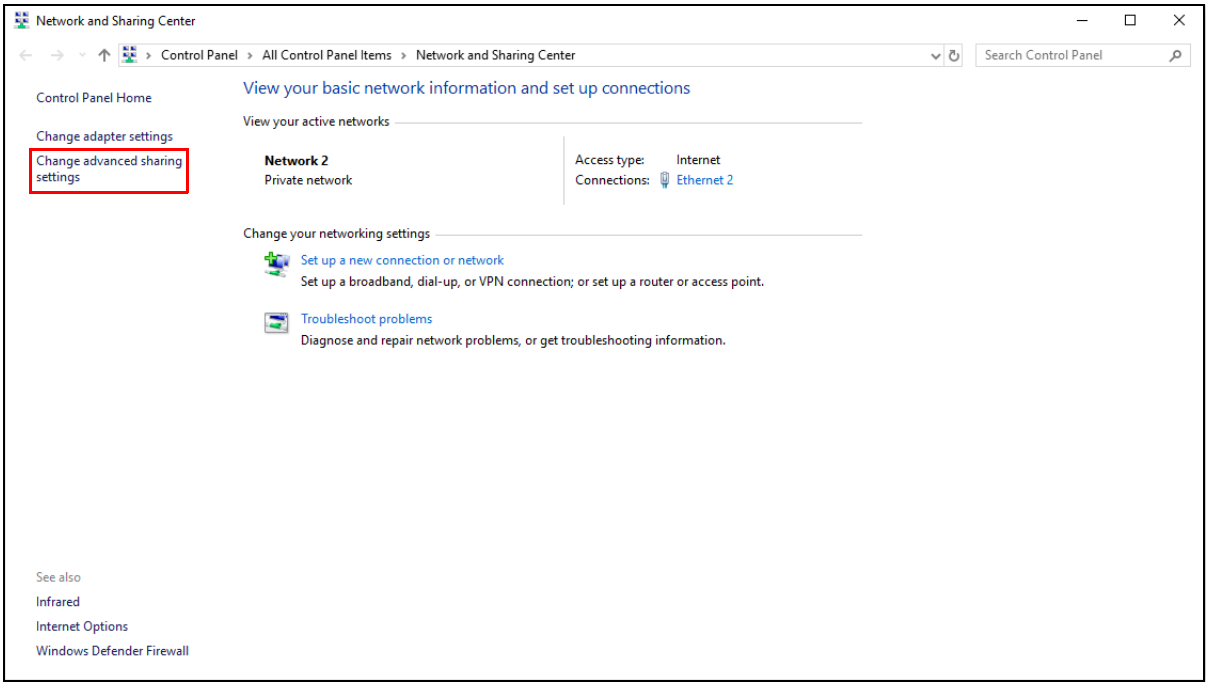
1 Click the start icon, **Settings** and then **Network & Internet**.



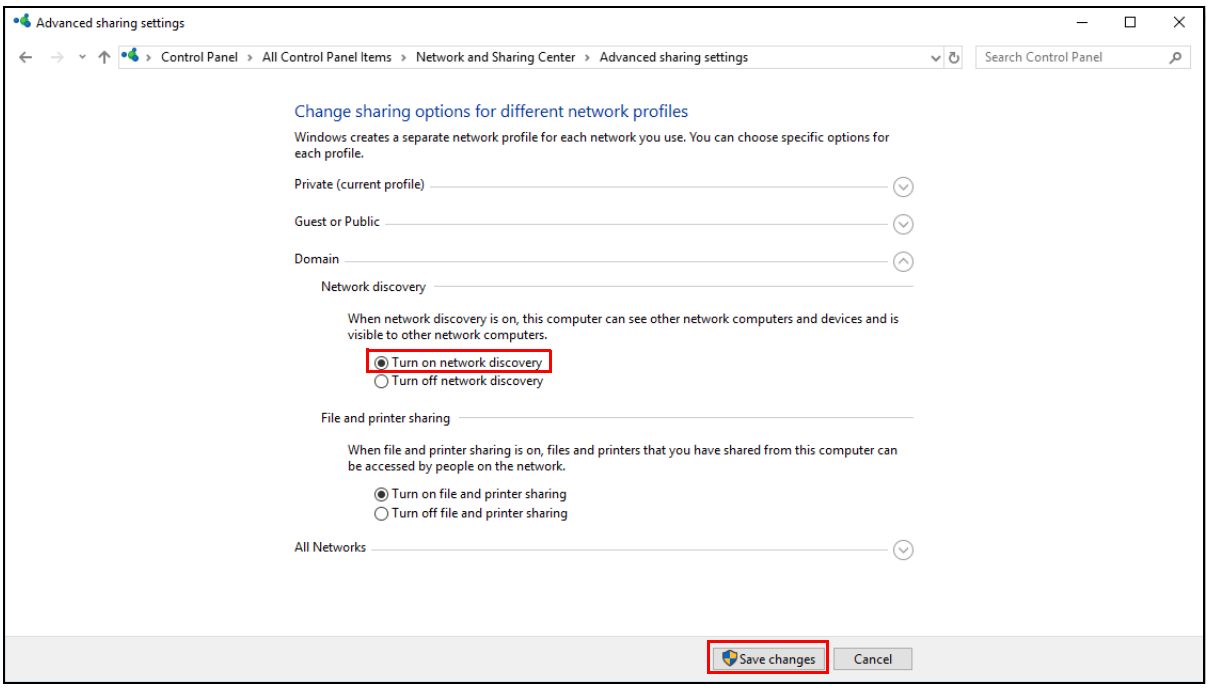
2 Click **Network and Sharing Center**.



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.



15.4.3 Auto-discover Your UPnP-enabled Network Device

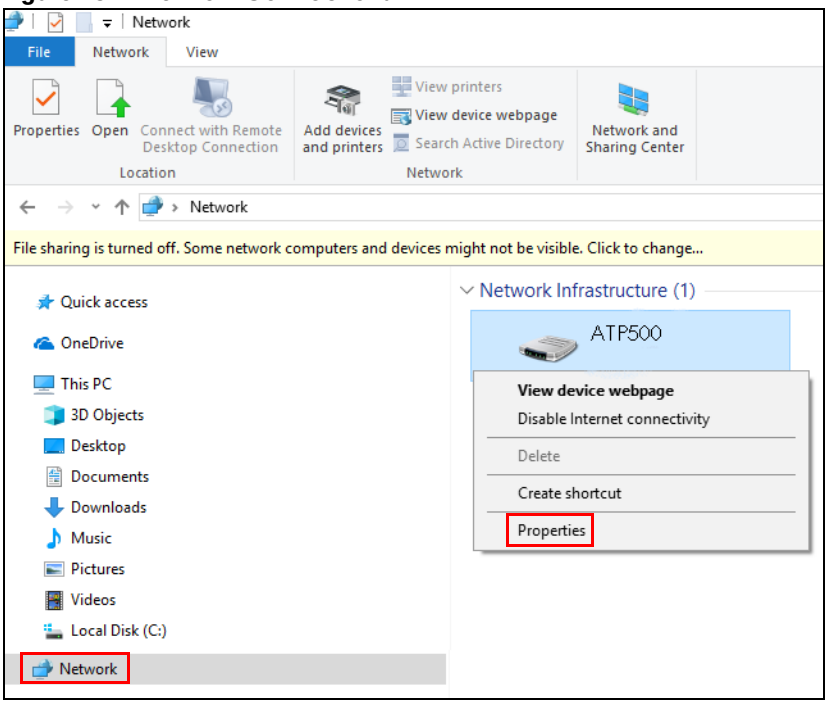
Before you follow these steps, make sure you already have UPnP activated on the Zyxel Device and in your computer.

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

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

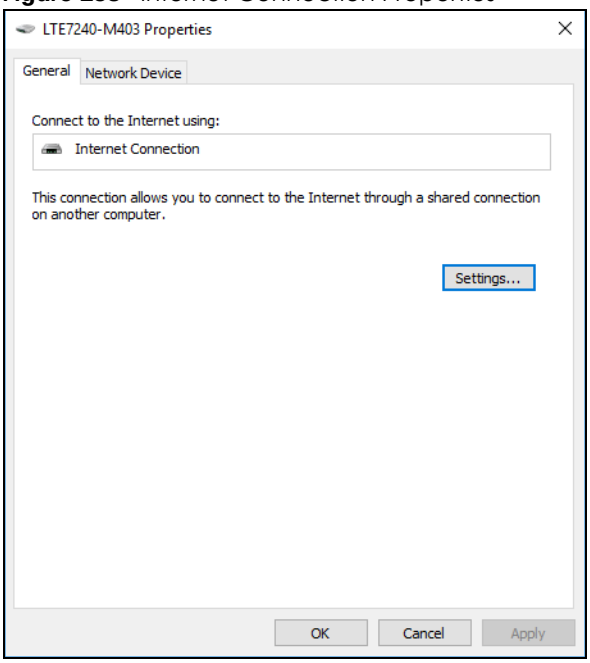
2 Right-click the Zyxel Device icon and select **Properties**.

Figure 257 Network Connections



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

Figure 258 Internet Connection Properties



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

Figure 259 Internet Connection Properties: Advanced Settings

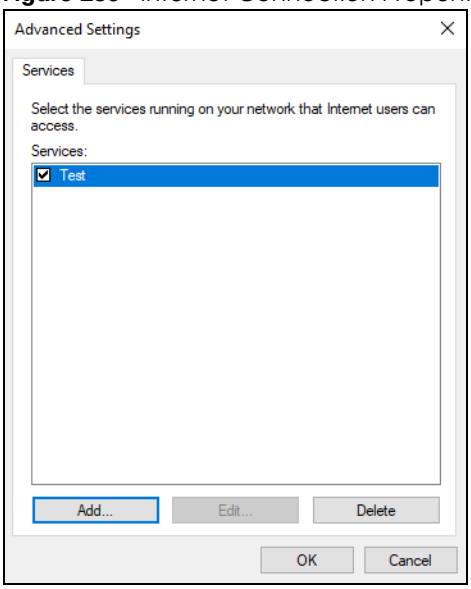
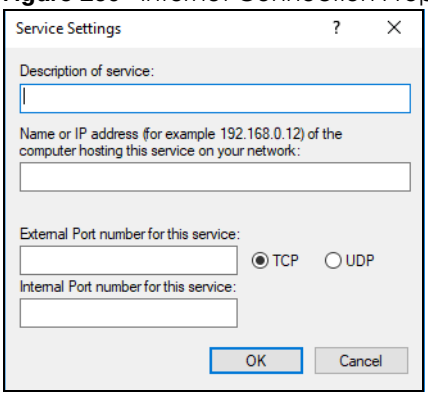


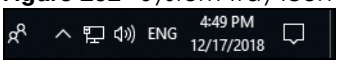
Figure 260 Internet Connection Properties: Advanced Settings: Add



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

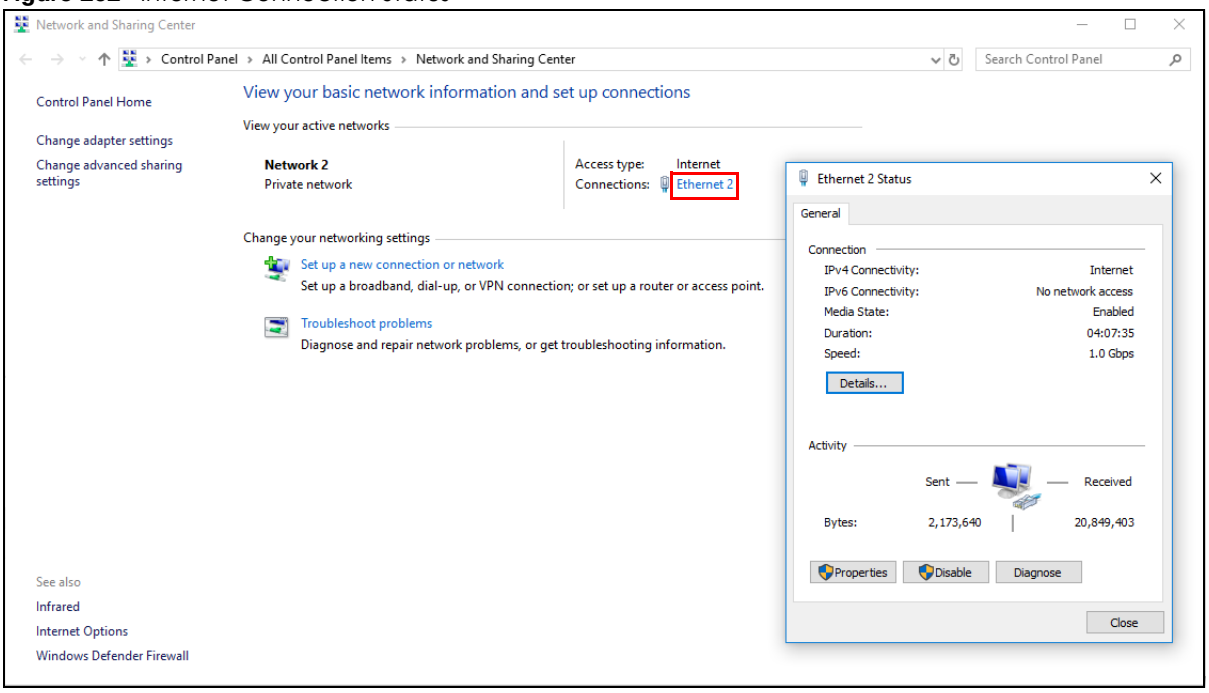
5 Click **OK**. Check the network icon on the system tray to see your Internet connection status.

Figure 261 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 262 Internet Connection Status



15.4.4 Web Configurator Easy Access in Windows 7

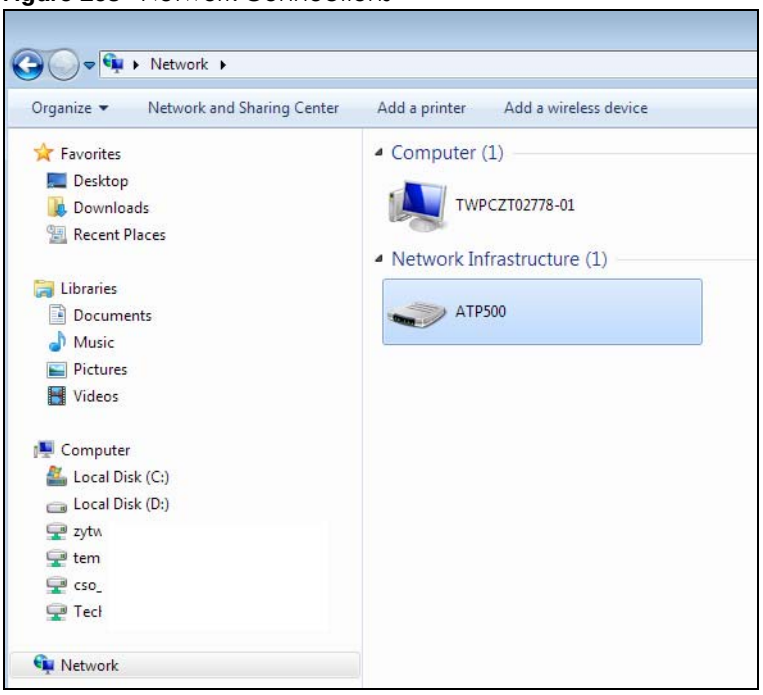
With UPnP, you can access the web-based configurator on the Zyxel Device without finding out the IP address of the Zyxel Device first. This comes helpful if you do not know the IP address of the Zyxel Device.

Follow the steps below to access the web configurator.

1 Open **Windows Explorer**.

2 Click **Network**.

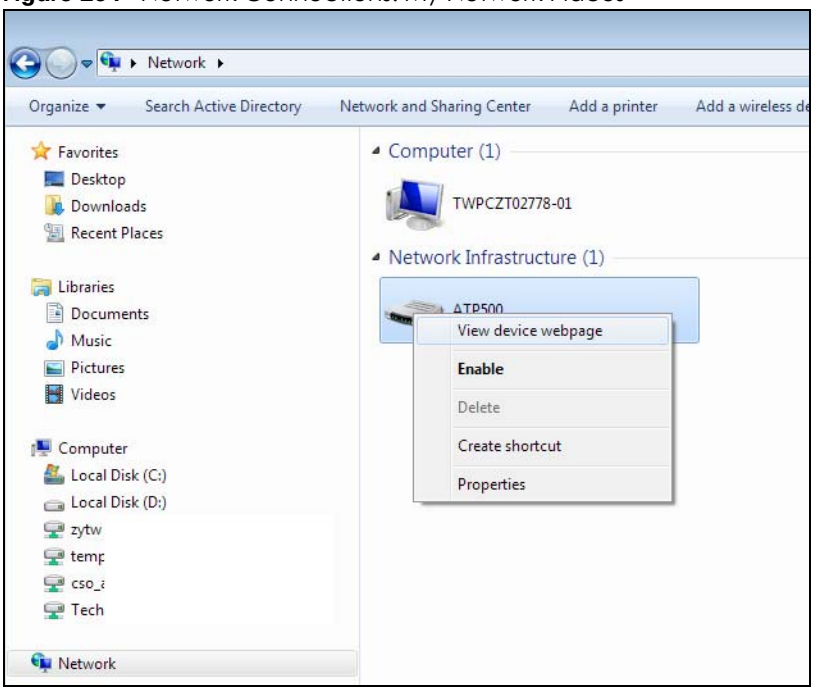
Figure 263 Network Connections



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

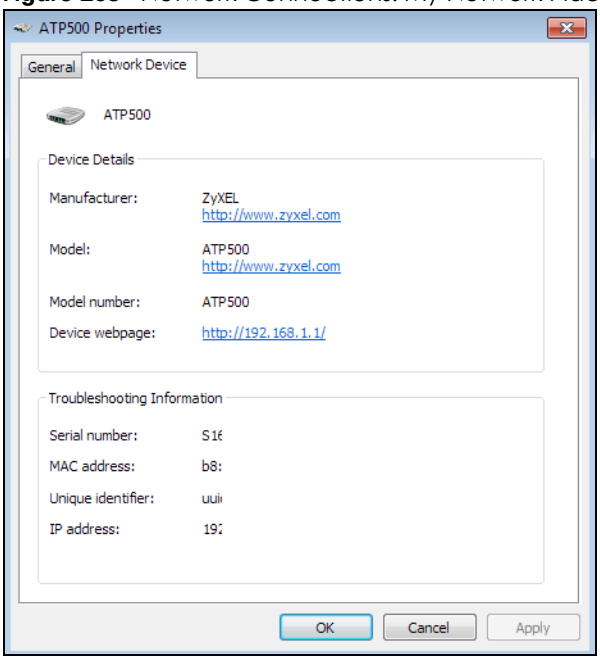
4 Right-click on the icon for your Zyxel Device and select **View device webpage**. The web configurator login screen displays.

Figure 264 Network Connections: My Network Places



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

Figure 265 Network Connections: My Network Places: Properties: Example



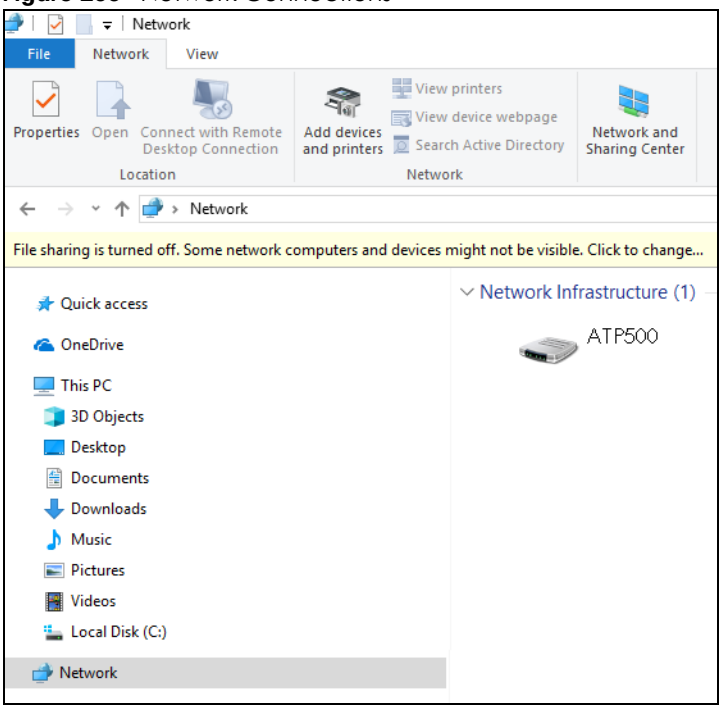
15.4.5 Web Configurator Easy Access in Windows 10

Follow the steps below to access the Web Configurator.

1 Open **File Explorer**.

2 Click **Network**.

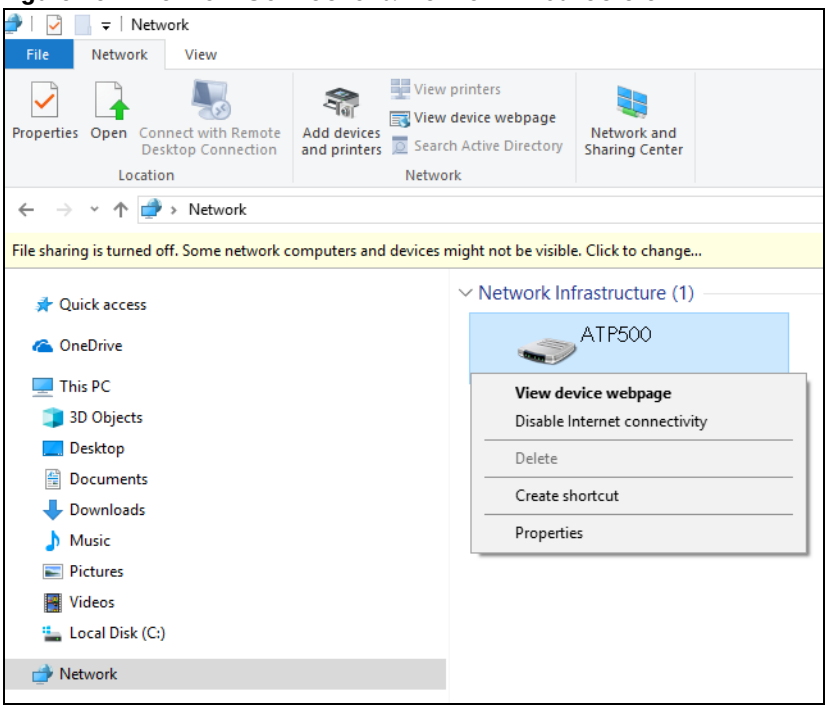
Figure 266 Network Connections



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

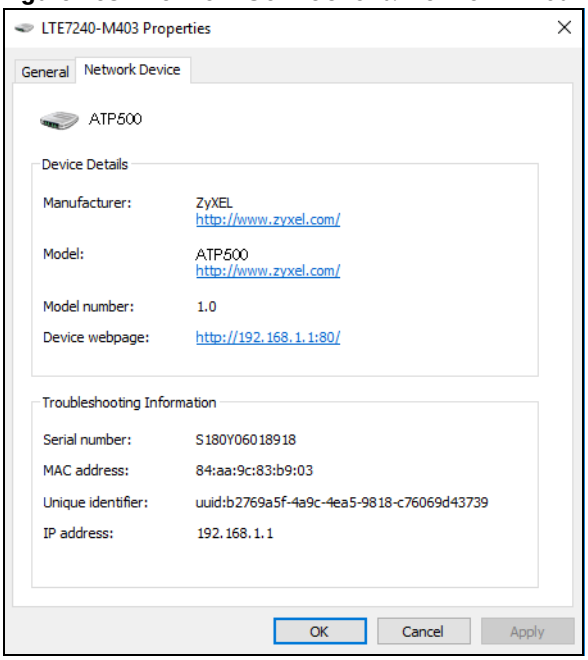
4 Right-click the icon for your Zyxel Device and select **View device webpage**. The Web Configurator login screen displays.

Figure 267 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 268 Network Connections: Network Infrastructure: Properties: Example



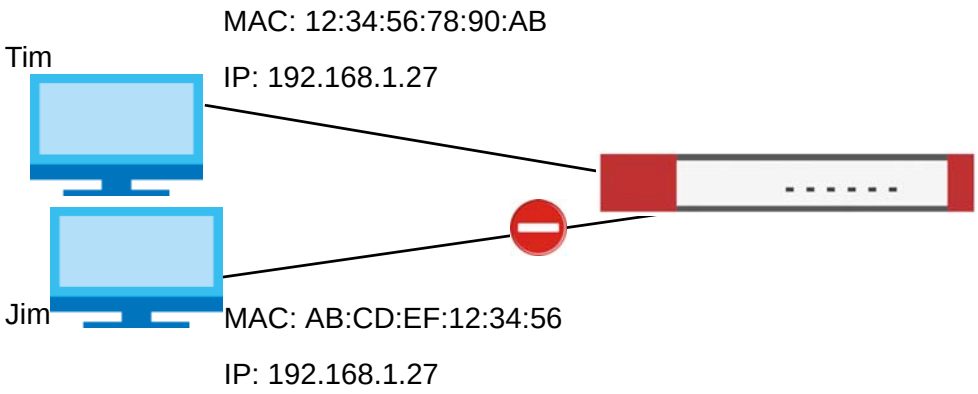
CHAPTER 16
IP/MAC Binding

16.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The Zyxel Device uses DHCP to assign IP addresses and records the MAC address it assigned to each IP address. The Zyxel Device then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the Zyxel Device.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 192.168.1.27 with another MAC address.

Figure 269 IP/MAC Binding Example



16.1.1 What You Can Do in this Chapter

- Use the **Summary** and **Edit** screens (Section 16.2 on page 380) to bind IP addresses to MAC addresses.
- Use the **Exempt List** screen (Section 16.3 on page 383) to configure ranges of IP addresses to which the Zyxel Device does not apply IP/MAC binding.

16.1.2 What You Need to Know

DHCP

IP/MAC address bindings are based on the Zyxel Device's dynamic and static DHCP entries.

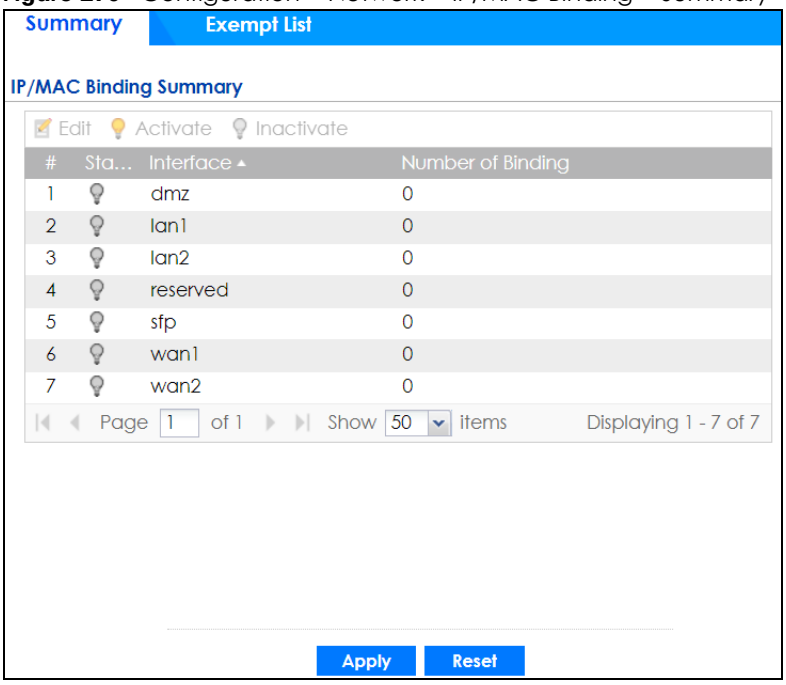
Interfaces Used With IP/MAC Binding

IP/MAC address bindings are grouped by interface. You can use IP/MAC binding with Ethernet, bridge, VLAN, and WLAN interfaces. You can also enable or disable IP/MAC binding and logging in an interface's configuration screen.

16.2 IP/MAC Binding Summary

Click **Configuration > Network > IP/MAC Binding** to open the **IP/MAC Binding Summary** screen. This screen lists the total number of IP to MAC address bindings for devices connected to each supported interface.

Figure 270 Configuration > Network > IP/MAC Binding > Summary



The following table describes the labels in this screen.

Table 146 Configuration > Network > IP/MAC Binding > Summary

LABEL	DESCRIPTION
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Interface	This is the name of an interface that supports IP/MAC binding.
Number of Binding	This field displays the interface's total number of IP/MAC bindings and IP addresses that the interface has assigned by DHCP.

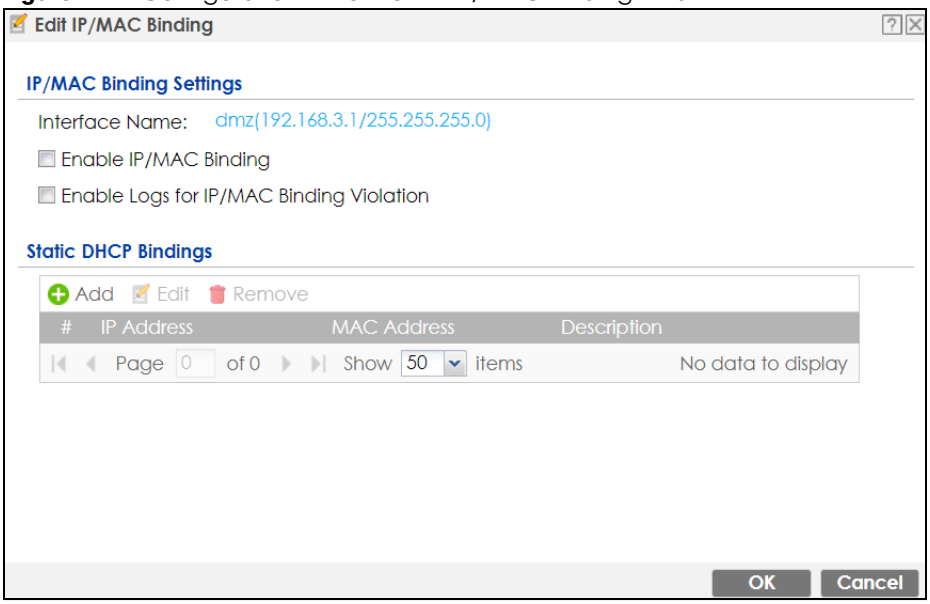
Table 146 Configuration > Network > IP/MAC Binding > Summary (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

16.2.1 IP/MAC Binding Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 271 Configuration > Network > IP/MAC Binding > Edit



The following table describes the labels in this screen.

Table 147 Configuration > Network > IP/MAC Binding > Edit

LABEL	DESCRIPTION
IP/MAC Binding Settings	
Interface Name	This field displays the name of the interface within the Zyxel Device and the interface's IP address and subnet mask.
Enable IP/MAC Binding	Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses.
Enable Logs for IP/MAC Binding Violation	Select this option to have the Zyxel Device generate a log if a device connected to this interface attempts to use an IP address not assigned by the Zyxel Device.
Static DHCP Bindings	This table lists the bound IP and MAC addresses. The Zyxel Device checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the Zyxel Device assigns the corresponding IP address. You can also access this table from the interface's edit screen.
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.

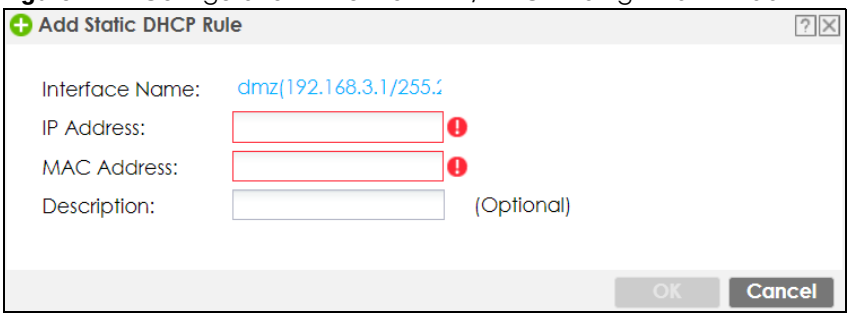
Table 147 Configuration > Network > IP/MAC Binding > Edit (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This is the index number of the static DHCP entry.
IP Address	This is the IP address that the Zyxel Device assigns to a device with the entry's MAC address.
MAC Address	This is the MAC address of the device to which the Zyxel Device assigns the entry's IP address.
Description	This helps identify the entry.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

16.2.2 Static DHCP Edit

Click **Configuration > Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Click the **Add** or **Edit** icon to open the following screen. Use this screen to configure an interface's IP to MAC address binding settings.

Figure 272 Configuration > Network > IP/MAC Binding > Edit > Add



The following table describes the labels in this screen.

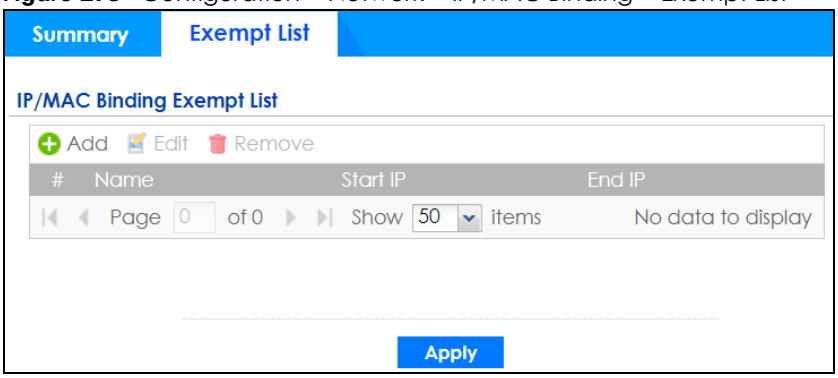
Table 148 Configuration > Network > IP/MAC Binding > Edit > Add

LABEL	DESCRIPTION
Interface Name	This field displays the name of the interface within the Zyxel Device and the interface's IP address and subnet mask.
IP Address	Enter the IP address that the Zyxel Device is to assign to a device with the entry's MAC address.
MAC Address	Enter the MAC address of the device to which the Zyxel Device assigns the entry's IP address.
Description	Enter up to 64 printable ASCII characters to help identify the entry. For example, you may want to list the computer's owner.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

16.3 IP/MAC Binding Exempt List

Click **Configuration > Network > IP/MAC Binding > Exempt List** to open the **IP/MAC Binding Exempt List** screen. Use this screen to configure ranges of IP addresses to which the Zyxel Device does not apply IP/MAC binding.

Figure 273 Configuration > Network > IP/MAC Binding > Exempt List



The following table describes the labels in this screen.

Table 149 Configuration > Network > IP/MAC Binding > Exempt List

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Click an entry or select it and click **Edit** to modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This is the index number of the IP/MAC binding list entry.
Name	Enter a name to help identify this entry.
Start IP	Enter the first IP address in a range of IP addresses for which the Zyxel Device does not apply IP/MAC binding.
End IP	Enter the last IP address in a range of IP addresses for which the Zyxel Device does not apply IP/MAC binding.
Add icon	Click the **Add** icon to add a new entry. Click the **Remove** icon to delete an entry. A window displays asking you to confirm that you want to delete it.
Apply	Click **Apply** to save your changes back to the Zyxel Device.

CHAPTER 17
Layer 2 Isolation

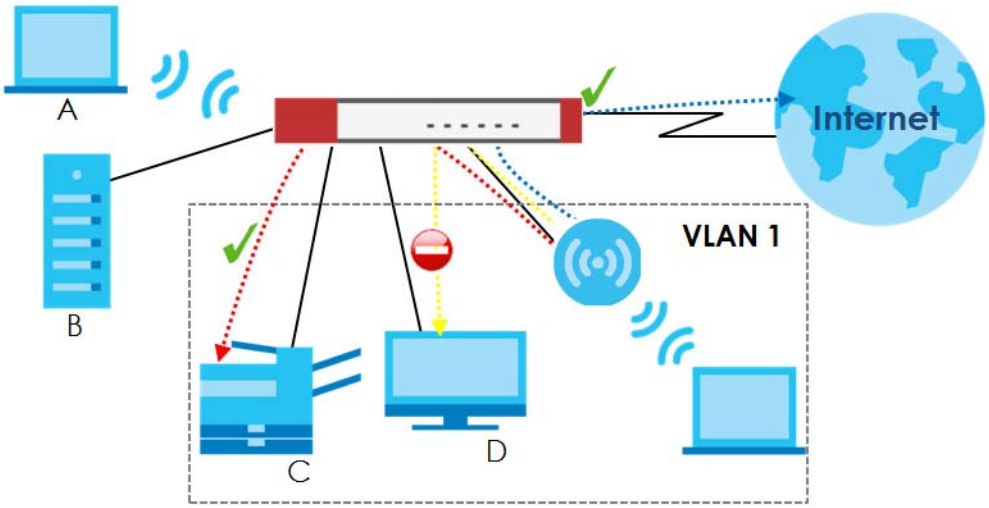
17.1 Overview

Layer-2 isolation is used to prevent connected devices from communicating with each other in the Zyxel Device's local network(s), except for the devices in the white list, when layer-2 isolation is enabled on the Zyxel Device and the local interface(s).

Note: The security policy control must be enabled before you can use layer-2 isolation.

In the following example, layer-2 isolation is enabled on the Zyxel Device's interface Vlan1. A printer, PC and AP are in the Vlan1. The IP address of network printer (**C**) is added to the white list. With this setting, the connected AP then cannot communicate with the PC (**D**), but can access the network printer (**C**), server (**B**), wireless client (**A**) and the Internet.

Figure 274 Layer-2 Isolation Application



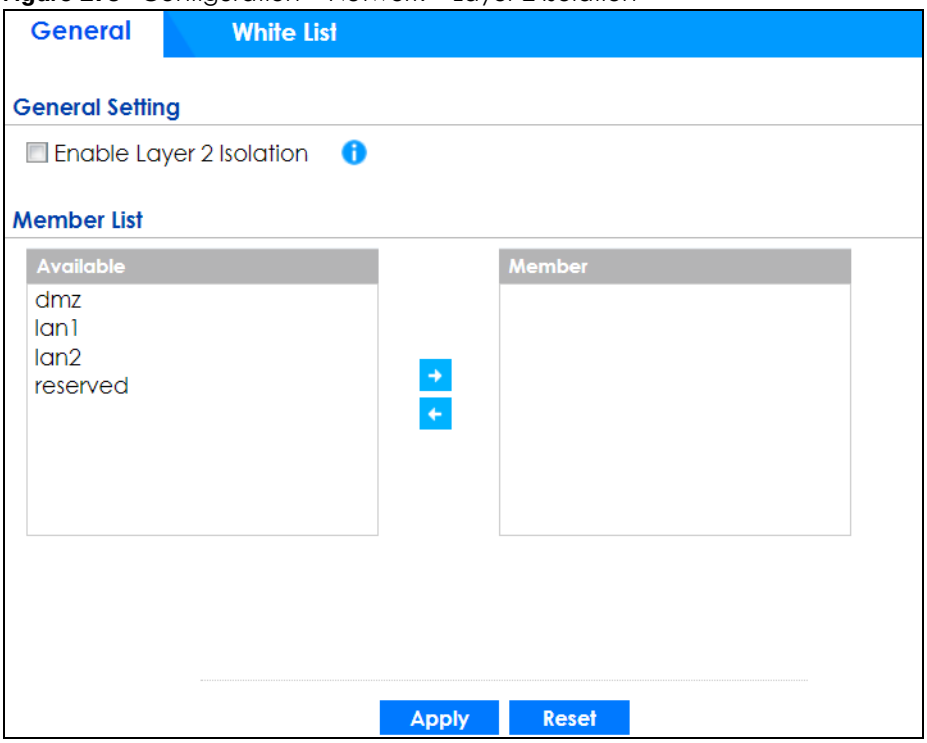
17.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 17.2 on page 384) to enable layer-2 isolation on the Zyxel Device and the internal interface(s).
- Use the **White List** screen (Section 17.3 on page 385) to enable and configures the white list.

17.2 Layer-2 Isolation General Screen

This screen allows you to enable Layer-2 isolation on the Zyxel Device and specific internal interface(s). To access this screen click **Configuration > Network > Layer 2 Isolation**.

Figure 275 Configuration > Network > Layer 2 Isolation



The following table describes the labels in this screen.

Table 150 Configuration > Network > Layer 2 Isolation

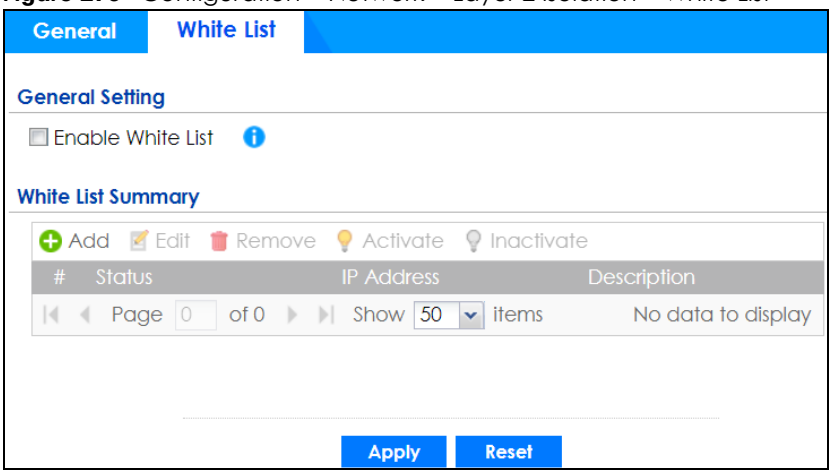
LABEL	DESCRIPTION
Enable Layer2 Isolation	Select this option to turn on the layer-2 isolation feature on the Zyxel Device. Note: You can enable this feature only when the security policy is enabled.
Member List	The **Available** list displays the name(s) of the internal interface(s) on which you can enable layer-2 isolation. To enable layer-2 isolation on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the **Member** list. To remove an interface, select the name(s) in the **Member** list and click the left arrow button.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

17.3 White List Screen

IP addresses that are not listed in the white list are blocked from communicating with other devices in the layer-2-isolation-enabled internal interface(s) except for broadcast packets.

To access this screen click **Configuration > Network > Layer 2 Isolation > White List**.

Figure 276 Configuration > Network > Layer 2 Isolation > White List



The following table describes the labels in this screen.

Table 151 Configuration > Network > Layer 2 Isolation > White List

LABEL	DESCRIPTION
Enable White List	Select this option to turn on the white list on the Zyxel Device. Note: You can enable this feature only when the security policy is enabled.
Add	Click this to add a new rule.
Edit	Click this to edit the selected rule.
Remove	Click this to remove the selected rule.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
#	This field is a sequential value, and it is not associated with a specific rule.
Status	This icon is lit when the rule is active and dimmed when the rule is inactive.
IP Address	This field displays the IP address of device that can be accessed by the devices connected to an internal interface on which layer-2 isolation is enabled.
Description	This field displays the description for the IP address in this rule.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

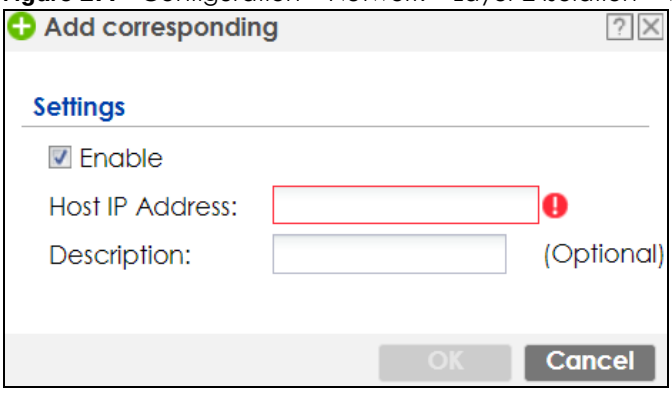
17.3.1 Add/Edit White List Rule

This screen allows you to create a new rule in the white list or edit an existing one. To access this screen, click the **Add** button or select an entry from the list and click the **Edit** button.

Note: You can configure up to 100 white list rules on the Zyxel Device.

Note: You need to know the IP address of each connected device that you want to allow to be accessed by other devices when layer-2 isolation is enabled.

Figure 277 Configuration > Network > Layer 2 Isolation > White List > Add/Edit



The following table describes the labels in this screen.

Table 152 Configuration > Network > Layer 2 Isolation > White List > Add/Edit

LABEL	DESCRIPTION
Enable	Select this option to turn on the rule.
Host IP Address	Enter an IPv4 address associated with this rule.
Description	Specify a description for the IP address associated with this rule. Enter up to 60 characters, spaces and underscores allowed.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

CHAPTER 18
DNS Inbound LB

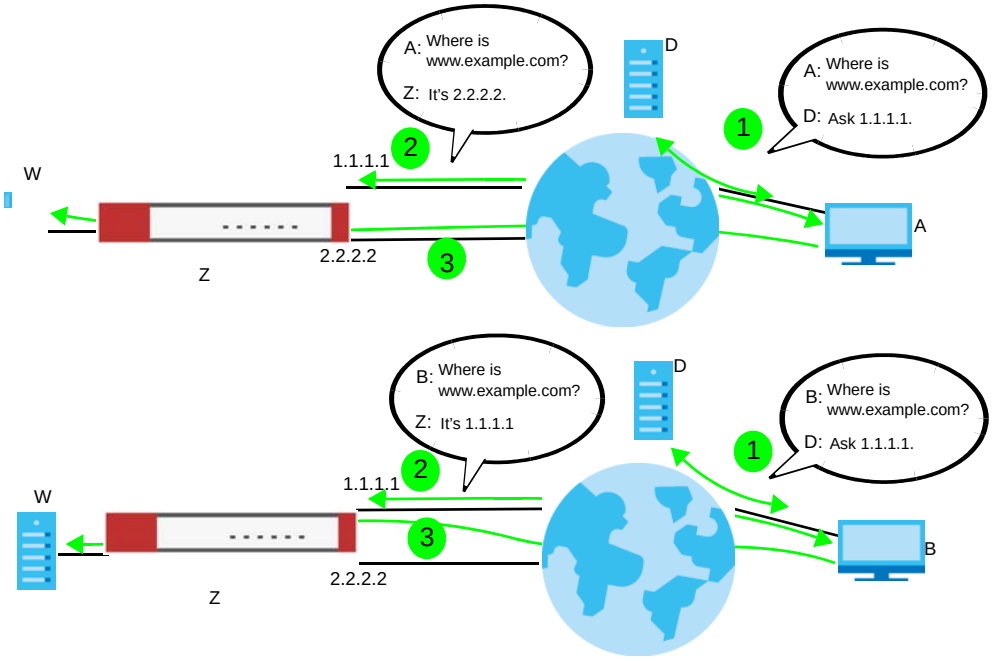
18.1 DNS Inbound Load Balancing Overview

Inbound load balancing enables the Zyxel Device to respond to a DNS query message with a different IP address for DNS name resolution. The Zyxel Device checks which member interface has the least load and responds to the DNS query message with the interface's IP address.

In the following figure, an Internet host (**A**) sends a DNS query message to the DNS server (**D**) in order to resolve a domain name of www.example.com. DNS server **D** redirects it to the Zyxel Device (**Z**)'s WAN1 with an IP address of 1.1.1.1. The Zyxel Device receives the DNS query message and responds to it with the WAN2's IP address, 2.2.2.2, because the WAN2 has the least load at that moment.

Another Internet host (**B**) also sends a DNS query message to ask where www.example.com is. The Zyxel Device responds to it with the WAN1's IP address, 1.1.1.1, since WAN1 has the least load this time.

Figure 278 DNS Load Balancing Example



18.1.1 What You Can Do in this Chapter

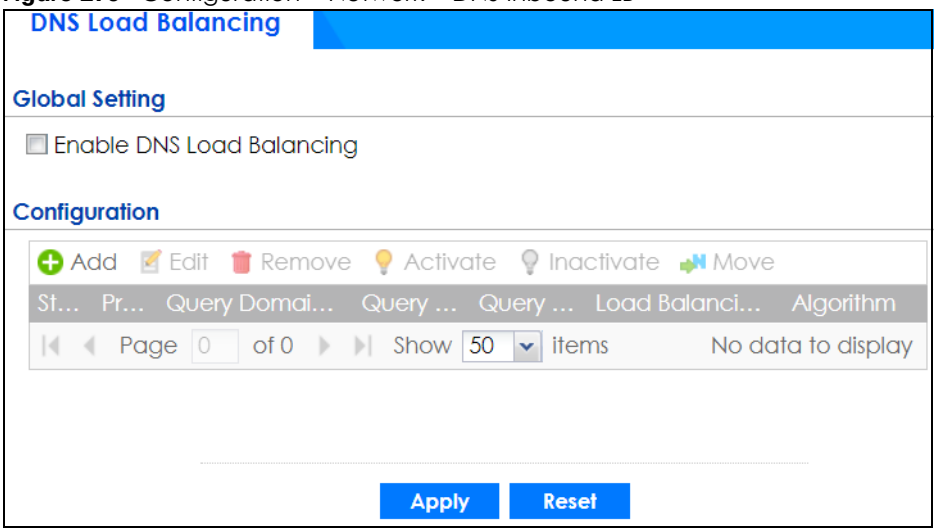
- Use the **Inbound LB** screen (see Section 18.2 on page 389) to view a list of the configured DNS load balancing rules.
- Use the **Inbound LB Add/Edit** screen (see Section 18.2.1 on page 390) to add or edit a DNS load balancing rule.

18.2 The DNS Inbound LB Screen

The **Inbound LB** screen provides a summary of all DNS load balancing rules and the details. You can also use this screen to add, edit, or remove the rules. Click **Configuration > Network > Inbound LB** to open the following screen.

Note: After you finish the inbound load balancing settings, go to security policy and NAT screens to configure the corresponding rule and virtual server to allow the Internet users to access your internal servers.

Figure 279 Configuration > Network > DNS Inbound LB



The following table describes the labels in this screen.

Table 153 Configuration > Network > DNS Inbound LB

LABEL	DESCRIPTION
Global Setting	
Enable DNS Load Balancing	Select this to enable DNS load balancing.
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This field displays the order in which the Zyxel Device checks the member interfaces of this DNS load balancing rule.
Query Domain Name	This field displays the domain name for which the Zyxel Device manages load balancing between the specified interfaces.

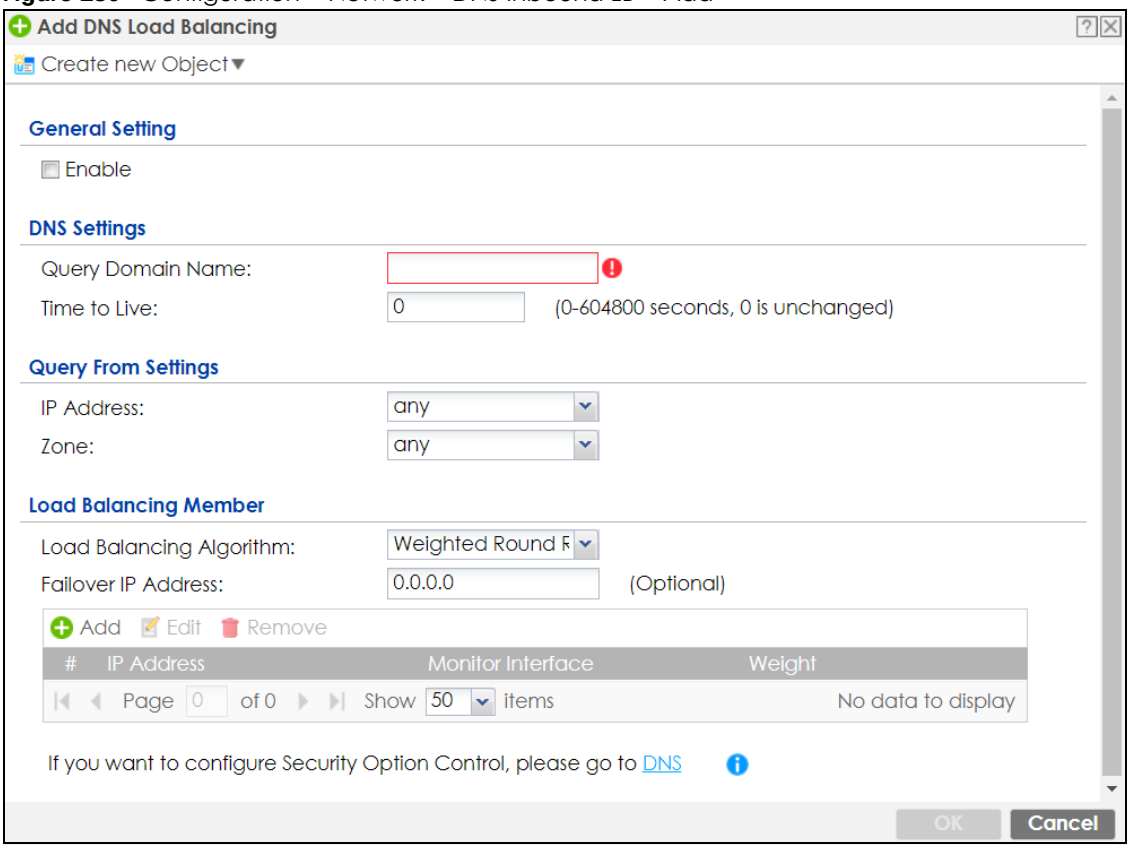
Table 153 Configuration > Network > DNS Inbound LB (continued)

LABEL	DESCRIPTION
Query From Address	This field displays the source IP address of the DNS query messages to which the Zyxel Device applies the DNS load balancing rule.
Query From Zone	The Zyxel Device applies the DNS load balancing rule to the query messages received from this zone.
Load Balancing Member	This field displays the member interfaces which the Zyxel Device manages for load balancing.
Algorithm	This field displays the load balancing method the Zyxel Device uses for this DNS load balancing rule. **Weighted Round Robin** - Each member interface is assigned a weight. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for 1 session's traffic in each round of 3 new sessions. **Least Connection** - The Zyxel Device chooses choose a member interface which is handling the least number of sessions. **Least Load - Outbound** - The Zyxel Device chooses a member interface which is handling the least amount of outgoing traffic. **Least Load - Inbound** - The Zyxel Device chooses a member interface which is handling the least amount of incoming traffic. **Least Load - Total** - The Zyxel Device chooses a member interface which is handling the least amount of outgoing and incoming traffic.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

18.2.1 The DNS Inbound LB Add/Edit Screen

The **Add DNS Load Balancing** screen allows you to add a domain name for which the Zyxel Device manages load balancing between the specified interfaces. You can configure the Zyxel Device to apply DNS load balancing to some specific hosts only by configuring the **Query From** settings. Click **Configuration > Network > Inbound LB** and then the **Add** or **Edit** icon to open this screen.

Figure 280 Configuration > Network > DNS Inbound LB > Add



The following table describes the labels in this screen.

Table 154 Configuration > Network > DNS Inbound LB > Add/Edit

LABEL	DESCRIPTION
Create New Object	Use this to configure any new setting objects that you need to use in this screen.
General Settings	
Enable	Select this to enable this DNS load balancing rule.
DNS Settings	
Query Domain Name	Type up to 255 characters for a domain name for which you want the Zyxel Device to manage DNS load balancing. You can use a wildcard (*) to let multiple domains match the name. For example, use *.example.com to specify any domain name that ends with "example.com" would match.
Time to Live	Enter the number of seconds the Zyxel Device recommends DNS request hosts to keep the DNS entry in their caches before removing it. Enter 0 to have the Zyxel Device not recommend this so the DNS request hosts will follow their DNS server's TTL setting.
Query From Setting	
IP Address	Select the name of an P address object, including geographic address object, of a computer or a DNS server which makes the DNS queries upon which to apply this rule. DNS servers process client queries using recursion or iteration: • In recursion, DNS servers make recursive queries on behalf of clients. So you have to configure this field to the DNS server's IP address when recursion is used. • In iteration, a client asks the DNS server and expects the best and immediate answer without the DNS server contacting other DNS servers. If the primary DNS server cannot provide the best answer, the client makes iteration queries to other configured DNS servers to resolve the name. You have to configure this field to the client's IP address when iteration is used.

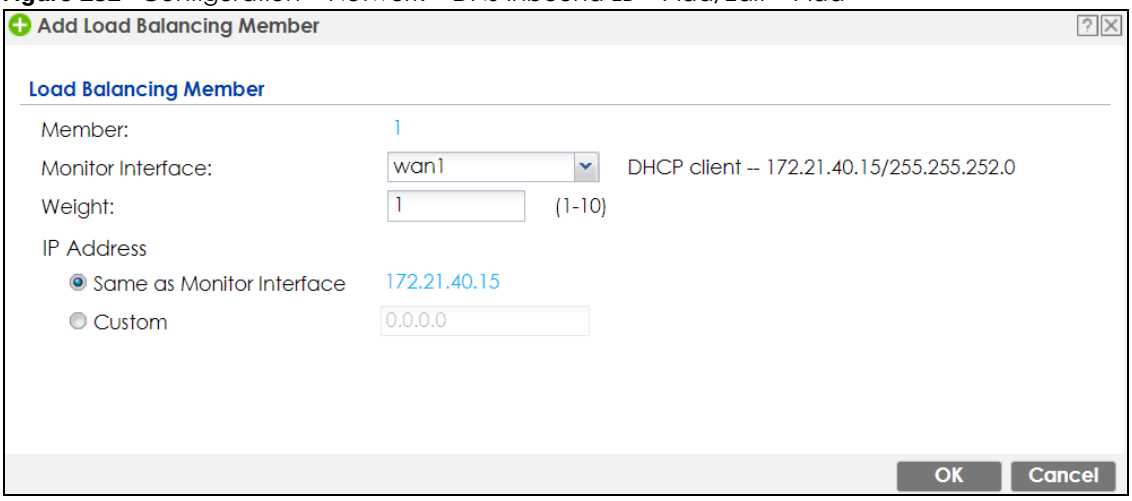
Table 154 Configuration > Network > DNS Inbound LB > Add/Edit (continued)

LABEL	DESCRIPTION
Zone	Select the zone of DNS query messages upon which to apply this rule.
Load Balancing Member	
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box. Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight. For example, if the weight ratio of wan1 and wan2 interfaces is 2:1, the Zyxel Device chooses wan1 for 2 sessions' traffic and wan2 for every session's traffic in each round of 3 new sessions. Select **Least Connection** to have the Zyxel Device choose the member interface which is handling the least number of sessions. Select **Least Load - Outbound** to have the Zyxel Device choose the member interface which is handling the least amount of outgoing traffic. Select **Least Load - Inbound** to have the Zyxel Device choose the member interface which is handling the least amount of incoming traffic. Select **Least Load - Total** to have the Zyxel Device choose the member interface which is handling the least amount of outgoing and incoming traffic.
Failover IP Address	Enter an alternate IP address with which the Zyxel Device will respond to a DNS query message when the load balancing algorithm cannot find any available interface.
Add	Click this to create a new member interface for this rule.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
#	This field displays the order in which the Zyxel Device checks this rule's member interfaces.
IP Address	This field displays the IP address of the member interface.
Monitor Interface	This field displays the name of the member interface. The Zyxel Device manages load balancing between the member interfaces.
Weight	This field is available if you selected **Weighted Round Robin** as the load balancing algorithm. This field displays the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

18.2.2 The DNS Inbound LB Add/Edit Member Screen

The **Add Load Balancing Member** screen allows you to add a member interface for the DNS load balancing rule. Click **Configuration > Network > DNS Inbound LB > Add or Edit** and then an **Add** or **Edit** icon to open this screen.

Figure 281 Configuration > Network > DNS Inbound LB > Add/Edit > Add



The following table describes the labels in this screen.

Table 155 Configuration > Network > DNS Inbound LB > Add/Edit > Add/Edit

LABEL	DESCRIPTION
Member	The Zyxel Device checks each member interface's loading in the order displayed here.
Monitor Interface	Select an interface to associate it with the DNS load balancing rule. This field also displays whether the IP address is a static IP address (**Static**), dynamically assigned (**Dynamic**) or obtained from a DHCP server (**DHCP Client**), as well as the IP address and subnet mask.
Weight	This field is available if you selected **Weighted Round Robin** for the load balancing algorithm. Specify the weight of the member interface. An interface with a larger weight gets more chances to transmit traffic than an interface with a smaller weight.
IP Address	
Same as Monitor Interface	Select this to send the IP address displayed in the **Monitor Interface** field to the DNS query senders.
Custom	Select this and enter another IP address to send to the DNS query senders.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

CHAPTER 19
IPnP

19.1 IPnP Overview

IP Plug and Play (IPnP) allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the Zyxel Device are not in the same subnet.

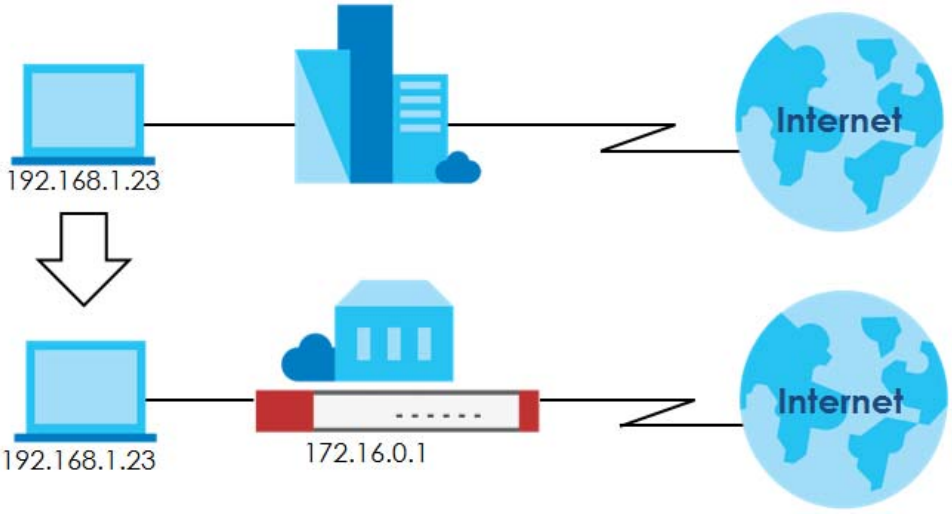
When you disable the IPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the Zyxel Device's LAN IP address can connect to the Zyxel Device or access the Internet through the Zyxel Device.

The IPnP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the Zyxel Device's IP address.

Note: You must enable NAT to use the IPnP feature.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a Zyxel Device is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the Zyxel Device are not in the same subnet.

Figure 282 IPnP Application



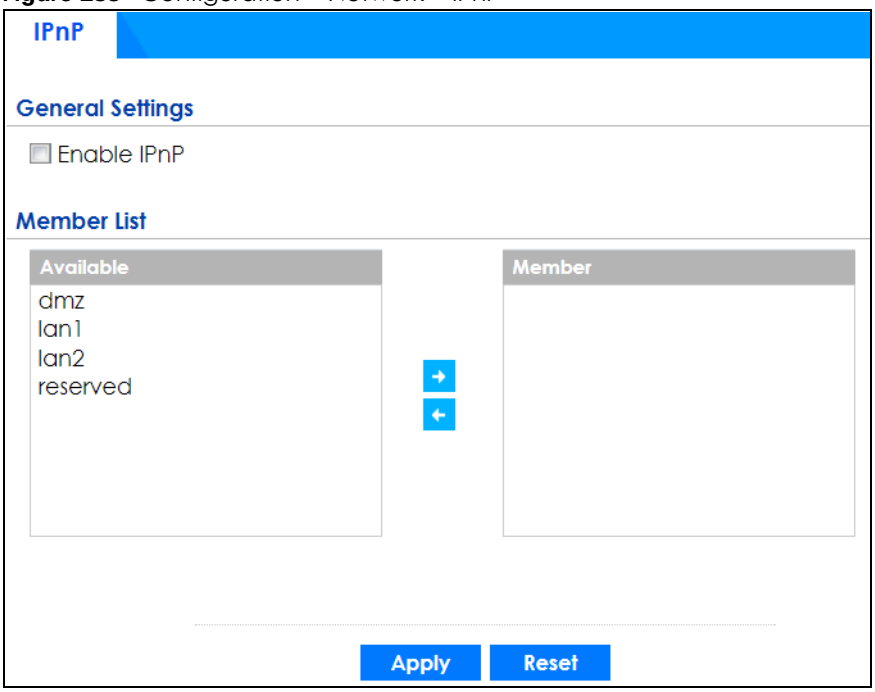
19.1.1 What You Can Do in this Chapter

Use the **IPnP** screen (Section 19.2 on page 395) to enable IPnP on the Zyxel Device and the internal interface(s).

19.2 IPnP Screen

This screen allows you to enable IPnP on the Zyxel Device and specific internal interface(s). To access this screen click **Configuration > Network > IPnP**.

Figure 283 Configuration > Network > IPnP



The following table describes the labels in this screen.

Table 156 Configuration > Network > IPnP

LABEL	DESCRIPTION
Enable IPnP	Select this option to turn on the IPnP feature on the Zyxel Device. Note: You can enable this feature only when the security policy is enabled.
Member List	The **Available** list displays the name(s) of the internal interface(s) on which you can enable IPnP. To enable IPnP on an interface, you can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and click the right arrow button to add to the **Member** list. To remove an interface, select the name(s) in the **Member** list and click the left arrow button.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 20
IPSec VPN

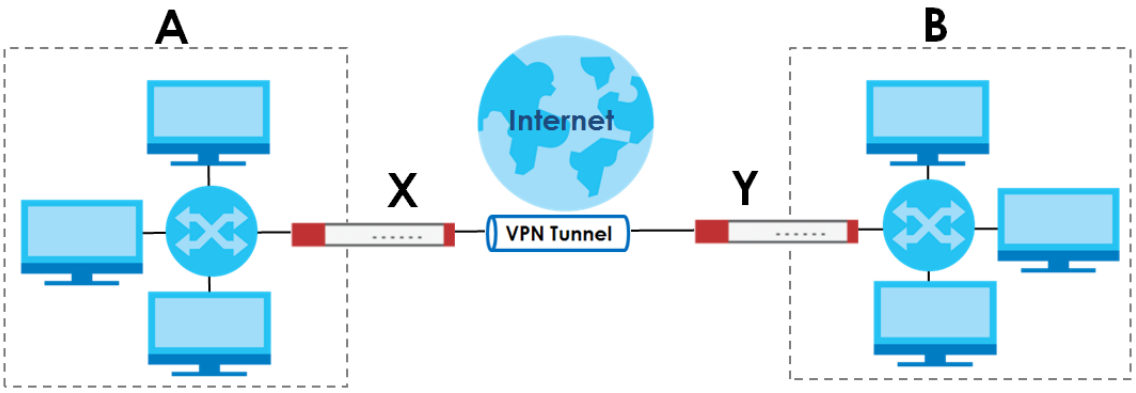
20.1 Virtual Private Networks (VPN) Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

IPSec VPN

Internet Protocol Security (IPSec) VPN connects IPSec routers or remote users using IPSec client software. This standards-based VPN offers flexible solutions for secure data communications across a public network. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The Zyxel Device can also combine multiple IPSec VPN connections into one secure network. Here local Zyxel Device **X** uses an IPSec VPN tunnel to remote (peer) Zyxel Device **Y** to connect the local (**A**) and remote (**B**) networks.

Figure 284 IPSec VPN Example



Internet Key Exchange (IKE): IKEv1 and IKEv2

The Zyxel Device supports IKEv1 and IKEv2 for IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely.

IKE uses certificates or pre-shared keys for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which encryption keys are derived. A security policy for each peer must be manually created.

IPSec VPN consists of two phases: Phase 1 and Phase 2. Phase 1's purpose is to establish a secure authenticated communication channel by using the Diffie–Hellman key exchange algorithm to generate a shared secret key to encrypt IKE communications. This negotiation results in one single bi-directional ISAKMP Security Association (SA). The authentication can be performed using either pre-

shared key (shared secret), signatures, or public key encryption. Phase 1 operates in either **Main Mode** or **Aggressive Mode**. **Main Mode** protects the identity of the peers, but **Aggressive Mode** does not.

During Phase 2, the remote IPSec routers use the secure channel established in Phase 1 to negotiate Security Associations for IPSec. The negotiation results in a minimum of two unidirectional security associations (one inbound and one outbound). Phase 2 uses Quick Mode (only). Quick mode occurs after IKE has established the secure tunnel in Phase 1. It negotiates a shared IPSec policy, derives shared secret keys used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires.

In the Zyxel Device, use the **VPN Connection** tab to set up Phase 2 and the **VPN Gateway** tab to set up Phase 1.

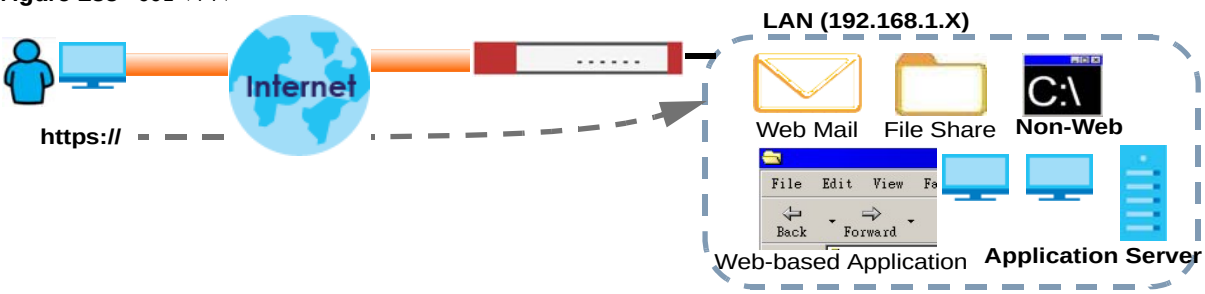
Some differences between IKEv1 and IKEv2 include:

- IKEv2 uses less bandwidth than IKEv1. IKEv2 uses one exchange procedure with 4 messages. IKEv1 uses two phases with Main Mode (9 messages) or Aggressive Mode (6 messages) in phase 1.
- IKEv2 supports Extended Authentication Protocol (EAP) authentication, and IKEv1 supports X-Auth. EAP is important when connecting to existing enterprise authentication systems.
- IKEv2 always uses NAT traversal and Dead Peer Detection (DPD), but they can be disabled in IKEv1 using Zyxel Device firmware (the default is on).
- Configuration payload (includes the IP address pool in the VPN setup data) is supported in IKEv2 (off by default), but not in IKEv1.
- Narrowed is supported in IKEv2, but not in IKEv1. Narrowed has the SA apply only to IP addresses in common between the Zyxel Device and the remote IPSec router.
- The IKEv2 protocol supports connectivity checks which is used to detect whether the tunnel is still up or not. If the check fails (the tunnel is down), IKEv2 can re-establish the connection automatically. The Zyxel Device uses firmware to perform connectivity checks when using IKEv1.

SSL VPN

SSL VPN uses remote users' web browsers to provide the easiest-to-use of the Zyxel Device's VPN solutions. A user just browses to the Zyxel Device's web address and enters his user name and password to securely connect to the Zyxel Device's network. Remote users do not need to configure security settings. Here a user uses his browser to securely connect to network resources in the same way as if he were part of the internal network. See Chapter 21 on page 432 for more on SSL VPN.

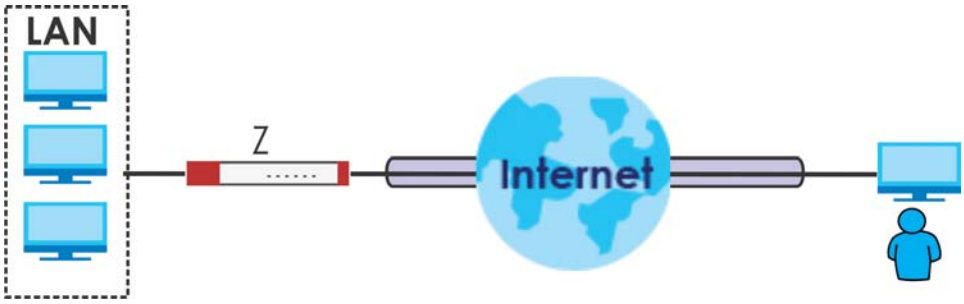
Figure 285 SSL VPN



L2TP VPN

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, or Windows operating systems for secure connections to the network behind the Zyxel Device. The remote users do not need their own IPSec gateways or third-party VPN client software. For example, configure sales representatives' laptops, tablets, or smartphones to securely connect to the Zyxel Device's network. See Chapter 22 on page 438 for more on L2TP over IPSec.

Figure 286 L2TP VPN



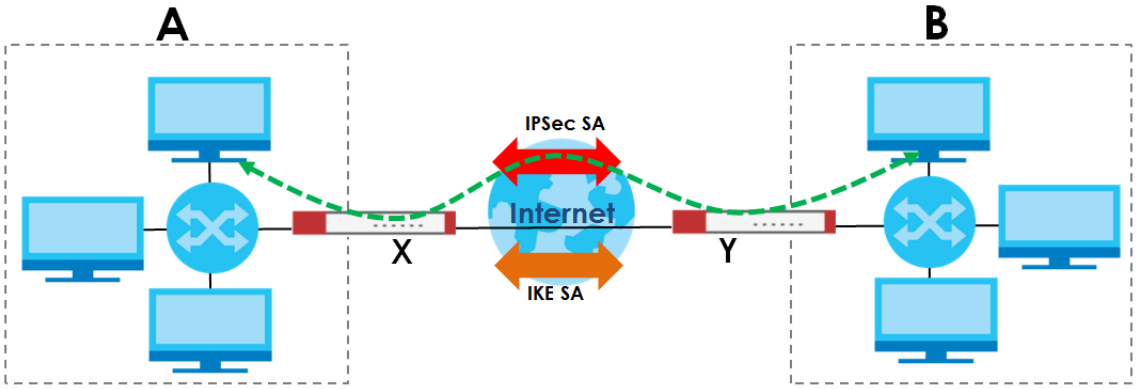
20.1.1 What You Can Do in this Chapter

- Use the **VPN Connection** screens (see Section 20.2 on page 401) to specify which IPSec VPN gateway an IPSec VPN connection policy uses, which devices behind the IPSec routers can use the VPN tunnel, and the IPSec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPSec SA).
- Use the **VPN Gateway** screens (see Section 20.2.1 on page 403) to manage the Zyxel Device's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.
- Use the **VPN Concentrator** screens (see Section 20.4 on page 418) to combine several IPSec VPN connections into a single secure network.
- Use the **Configuration Provisioning** screen (see Section 20.5 on page 420) to set who can retrieve VPN rule settings from the Zyxel Device using the Zyxel Device IPSec VPN Client.

20.1.2 What You Need to Know

An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the Zyxel Device and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the Zyxel Device and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the Zyxel Device and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

Figure 287 VPN: IKE SA and IPSec SA

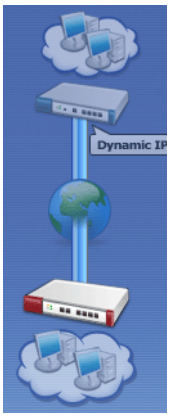
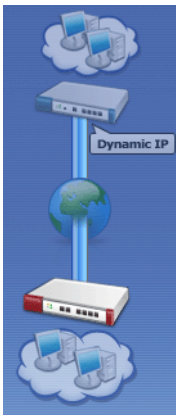


In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

Application Scenarios

The Zyxel Device's application scenarios make it easier to configure your VPN connection settings.

Table 157 IPSec VPN Application Scenarios

SITE-TO-SITE	SITE-TO-SITE WITH DYNAMIC PEER	REMOTE ACCESS (SERVER ROLE)	REMOTE ACCESS (CLIENT ROLE)	VPN TUNNEL INTERFACE
				
Choose this if the remote IPSec router has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. The remote IPSec router can also initiate the VPN tunnel if this Zyxel Device has a static IP address or a domain name.	Choose this if the remote IPSec router has a dynamic IP address. You don't specify the remote IPSec router's address, but you specify the remote policy (the addresses of the devices behind the remote IPSec router). This Zyxel Device must have a static IP address or a domain name. Only the remote IPSec router can initiate the VPN tunnel.	Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. You don't specify the addresses of the client IPSec routers or the remote policy. This creates a dynamic IPSec VPN rule that can let multiple clients connect. Only the clients can initiate the VPN tunnel.	Choose this to connect to an IPSec server. This Zyxel Device is the client (dial-in user). Client role Zyxel Devices initiate IPSec VPN connections to a server role Zyxel Device. This Zyxel Device can have a dynamic IP address. The IPSec server doesn't configure this Zyxel Device's IP address or the addresses of the devices behind it. Only this Zyxel Device can initiate the VPN tunnel.	Choose this to set up a VPN tunnel interface to bind with a VPN connection. The Zyxel Device can use the interface to do load balancing using a specific Trunk. The remote IPSec router should have a static IP address or a domain name.

Finding Out More

- See Section 20.6 on page 422 for IPSec VPN background information.
- See the help in the IPSec VPN quick setup wizard screens.

20.1.3 Before You Begin

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

You should set up the following features before you set up the VPN tunnel.

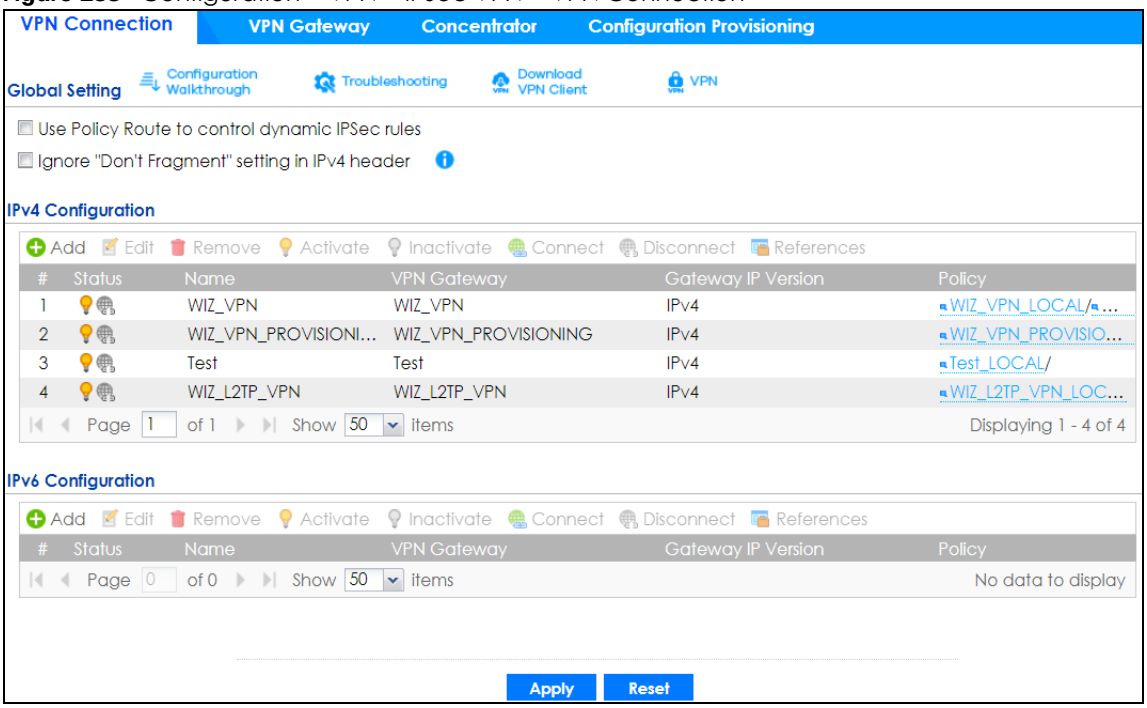
- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the Zyxel Device uses as its IP address when it establishes the IKE SA. You should set up the interface first.
- In a VPN gateway, you can enable extended authentication. If the Zyxel Device is in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the Zyxel Device authenticates the remote IPSec router.
- In a VPN gateway, the Zyxel Device and remote IPSec router can use certificates to authenticate each other. Make sure the Zyxel Device and the remote IPSec router will trust each other's certificates.

20.2 The VPN Connection Screen

Click **Configuration > VPN > IPSec VPN** to open the **VPN Connection** screen. The **VPN Connection** screen lists the VPN connection policies and their associated VPN gateway(s), and various settings. In addition, it also lets you activate or deactivate and connect or disconnect each VPN connection (each IPSec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Click on the icons to go to the OneSecurity website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 288 Configuration > VPN > IPSec VPN > VPN Connection



Each field is discussed in the following table.

Table 158 Configuration > VPN > IPSec VPN > VPN Connection

LABEL	DESCRIPTION
Global Setting	The following two fields are for all IPSec VPN policies. Click on the VPN icon to go to the Zyxel VPN Client product page at the Zyxel website.
Use Policy Route to control dynamic IPSec rules	Select this to be able to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must manually create these policy routes. The Zyxel Device automatically obtains source and destination addresses for dynamic IPSec rules that do not match any of the policy routes. Clear this to have the Zyxel Device automatically obtain source and destination addresses for all dynamic IPSec rules.
Ignore "Don't Fragment" setting in packet header	Select this to fragment packets larger than the MTU (Maximum Transmission Unit) that have the "Don't Fragment" bit in the IP header turned on. When you clear this the Zyxel Device drops packets larger than the MTU that have the "Don't Fragment" bit in the header turned on.
IPv4 / IPv6 Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Connect	To connect an IPSec SA, select it and click **Connect**.
Disconnect	To disconnect an IPSec SA, select it and click **Disconnect**.

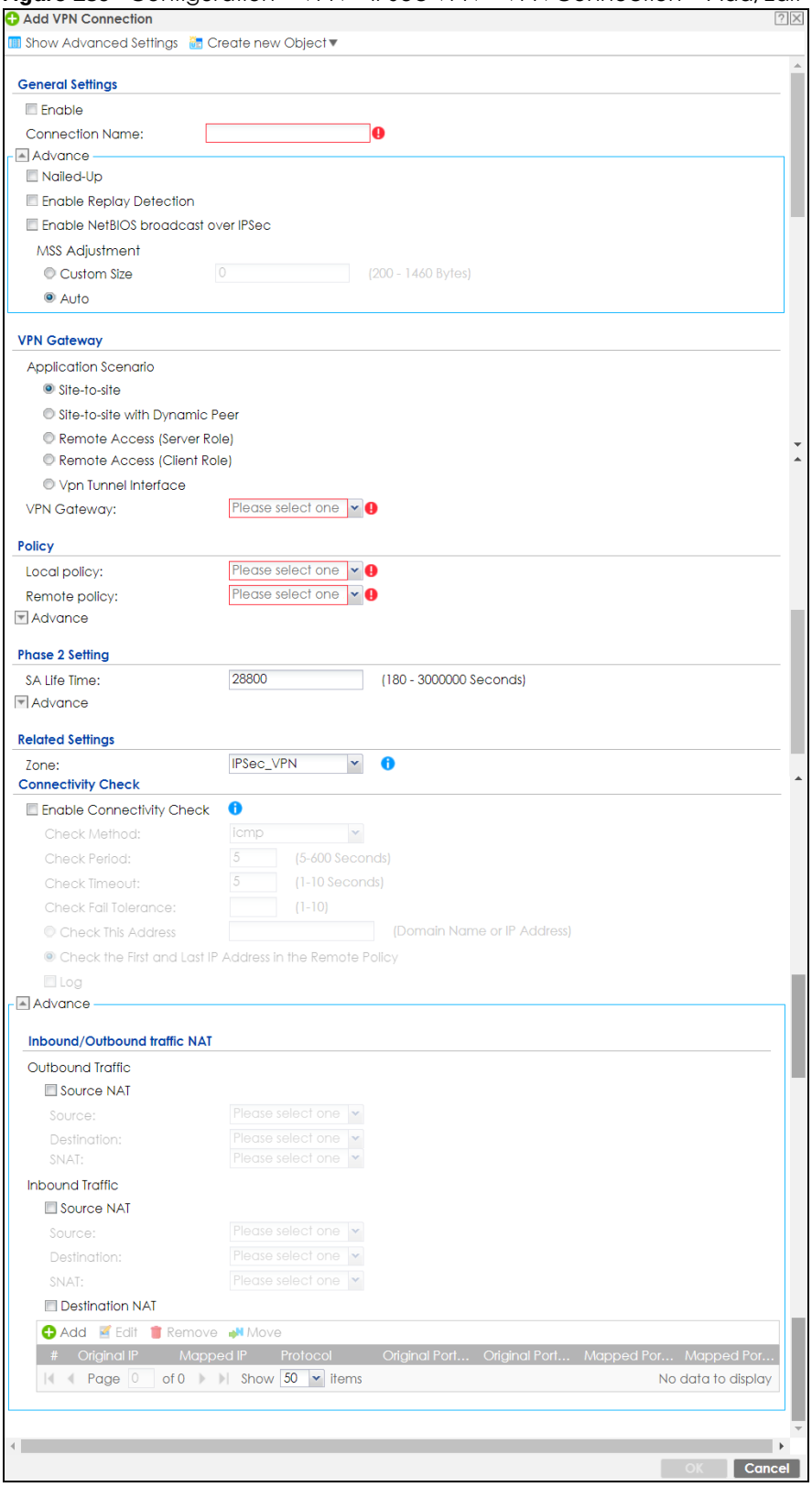
Table 158 Configuration > VPN > IPSec VPN > VPN Connection (continued)

LABEL	DESCRIPTION
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with a specific connection.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The connect icon is lit when the interface is connected and dimmed when it is disconnected.
Name	This field displays the name of the IPSec SA.
VPN Gateway	This field displays the VPN gateway in use for this VPN connection.
Gateway IP Version	This field displays what IP version the associated VPN gateway(s) is using. An IPv4 gateway may use an IKEv1 or IKEv2 SA. An IPv6 gateway may use IKEv2 only.
Policy	This field displays the local policy and the remote policy, respectively.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.2.1 The VPN Connection Add/Edit Screen

The **VPN Connection Add/Edit Gateway** screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the **Configuration > VPN Connection** screen (see Section 20.2 on page 401), and click either the **Add** icon or an **Edit** icon.

Figure 289 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit



Each field is described in the following table.

Table 159 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this check box to activate this VPN connection.
Connection Name	Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Nailed-Up	Select this if you want the Zyxel Device to automatically renegotiate the IPSec SA when the SA life time expires.
Enable Replay Detection	Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks.
Enable NetBIOS Broadcast over IPSec	Select this check box if you the Zyxel Device to send NetBIOS (Network Basic Input/ Output System) packets through the IPSec SA. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa.
MSS Adjustment	Select **Custom Size** to set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection. Some VPN clients may not be able to use a custom MSS size if it is set too small. In that case those VPN clients will ignore the size set here and use the minimum size that they can use. Select **Auto** to have the Zyxel Device automatically set the MSS for this VPN connection.
Narrowed	This is visible when you select any options in the **VPN Gateway** section except for **VPN Tunnel Interface**. If the IP range on the Zyxel Device (local policy) and the local IP range on the remote IPSec router overlap in an IKEv2 SA, then you may select **Narrowed** to have the SA only apply to the IP addresses in common. Here are some examples. Zyxel Device (local policy) Remote IPSec router IKEv2 SA-1 192.168.20.0/24 192.168.20.1 ~ 192.168.20.20 Narrowed 192.168.20.1 ~ 192.168.20.20 IKEv2 SA- 2 192.168.30.50 ~ 192.168.30.70 192.168.30.60 ~ 192.168.30.80 Narrowed 192.168.30.60 ~ 192.168.30.70
VPN Gateway	

Table 159 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Application Scenario	Select the scenario that best describes your intended VPN connection. **Site-to-site** - Choose this if the remote IPSec router has a static IP address or a domain name. This Zyxel Device can initiate the VPN tunnel. **Site-to-site with Dynamic Peer** - Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. **Remote Access (Server Role)** - Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. **Remote Access (Client Role)** - Choose this to connect to an IPSec server. This Zyxel Device is the client (dial-in user) and can initiate the VPN tunnel. **VPN Tunnel Interface** - Choose this to set up a VPN tunnel interface to bind with a VPN connection. The Zyxel Device can use the interface to do load balancing using a specific Trunk. The remote IPSec router should have a static IP address or a domain name. See **Configuration > Network > Interface > VTI**.
VPN Gateway	Select the VPN gateway this VPN connection is to use or select **Create Object** to add another VPN gateway for this VPN connection to use.
Policy	
Local Policy	Select the address corresponding to the local network. Use **Create new Object** if you need to configure a new one.
Remote Policy	Select the address corresponding to the remote network. Use **Create new Object** if you need to configure a new one.
Enable GRE over IPSec	Select this to allow traffic using the Generic Routing Encapsulation (GRE) tunneling protocol through an IPSec tunnel.
Policy Enforcement	Clear this to allow traffic with source and destination IP addresses that do not match the local and remote policy to use the VPN tunnel. Leave this cleared for free access between the local and remote networks. Selecting this restricts who can use the VPN tunnel. The Zyxel Device drops traffic with source and destination IP addresses that do not match the local and remote policy.
Mode Config	This is visible when you select **Remote Access (Server Role)** and a **VPN Gateway**.
Enable Mode Config	Select this to have the IPSec VPN client receive an IP address, DNS and WINS information from the Zyxel Device.
IP Address Pool	Select an address object from the drop-down list box.
First DNS Server (Optional)	The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN. Enter a DNS server's IP address.
Second DNS Server (Optional)	Enter a secondary DNS server's IP address that is checked if the first one is unavailable.
First WINS Server (Optional)	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Second WINS Server (Optional)	Enter a secondary WINS server's IP address that is checked if the first one is unavailable.
Configuration Payload	This is only available when you have created an IKEv2 Gateway and are using **Remote Access (Server Role)**.
Enable Configuration Payload	Select this to have at least have the IP address pool included in the VPN setup data.
IP Address Pool:	Select an address object from the drop-down list box.

Table 159 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
First DNS Server (optional)	The Domain Name System (DNS) maps a domain name to an IP address and vice versa. The Zyxel Device uses these (in the order you specify here) to resolve domain names for VPN. Enter a DNS server's IP address.
Second DNS Server (Optional)	Enter a secondary DNS server's IP address that is checked if the first one is unavailable.
First WINS Server (Optional)	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Second WINS Server (Optional)	Enter a secondary WINS server's IP address that is checked if the first one is unavailable.
Phase 2 Settings	
SA Life Time	Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The Zyxel Device automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources.
Active Protocol	Select which protocol you want to use in the IPSec SA. Choices are: **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication** algorithm. **ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption** algorithm and **Authentication** algorithm. Both **AH** and **ESP** increase processing requirements and latency (delay). The Zyxel Device and remote IPSec router must use the same active protocol.
Encapsulation	Select which type of encapsulation the IPSec SA uses. Choices are **Tunnel** - this mode encrypts the IP header information and the data. **Transport** - this mode only encrypts the data. The Zyxel Device and remote IPSec router must use the same encapsulation.
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the Zyxel Device accepts from the remote IPSec router for negotiating the IPSec SA.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.

Table 159 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Encryption	This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are: **NULL** - no encryption key or algorithm **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The Zyxel Device and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key. Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than **MD5**, but it is also slower. The Zyxel Device and the remote IPSec router must both have a proposal that uses the same authentication algorithm.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **none** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number **DH5** - enable PFS and use a 1536-bit random number **DH14** - enable PFS and use a 2048 bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.
Related Settings	
Zone	Select the security zone into which to add this VPN connection policy. Any security rules or settings configured for the selected zone apply to this VPN connection policy.
Connectivity Check	The Zyxel Device can regularly check the VPN connection to the gateway you specified to make sure it is still available.
Enable Connectivity Check	Select this to turn on the VPN connection check.
Check Method	Select how the Zyxel Device checks the connection. The peer must be configured to respond to the method you select. Select **icmp** to have the Zyxel Device regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings. Select **tcp** to have the Zyxel Device regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP connection.

Table 159 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Check Port	This field displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check.
Check Period	Enter the number of seconds between connection check attempts.
Check Timeout	Enter the number of seconds to wait for a response before the attempt is a failure.
Check Fail Tolerance	Enter the number of consecutive failures allowed before the Zyxel Device disconnects the VPN tunnel. The Zyxel Device resumes using the first peer gateway address when the VPN connection passes the connectivity check.
Check this Address	Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it.
Check the First and Last IP Address in the Remote Policy	Select this to have the Zyxel Device check the connection to the first and last IP addresses in the connection's remote policy. Make sure one of these is the peer gateway's LAN IP address.
Log	Select this to have the Zyxel Device generate a log every time it checks this VPN connection.
Inbound/Outbound traffic NAT	
Outbound Traffic	
Source NAT	This translation hides the source address of computers in the local network. It may also be necessary if you want the Zyxel Device to route packets from computers outside the local network through the IPSec SA.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the remote network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address object for the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Inbound Traffic	
Source NAT	This translation hides the source address of computers in the remote network.
Source	Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the remote network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination	Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the local network.
SNAT	Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address that hides the original source address. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**).
Destination NAT	This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.

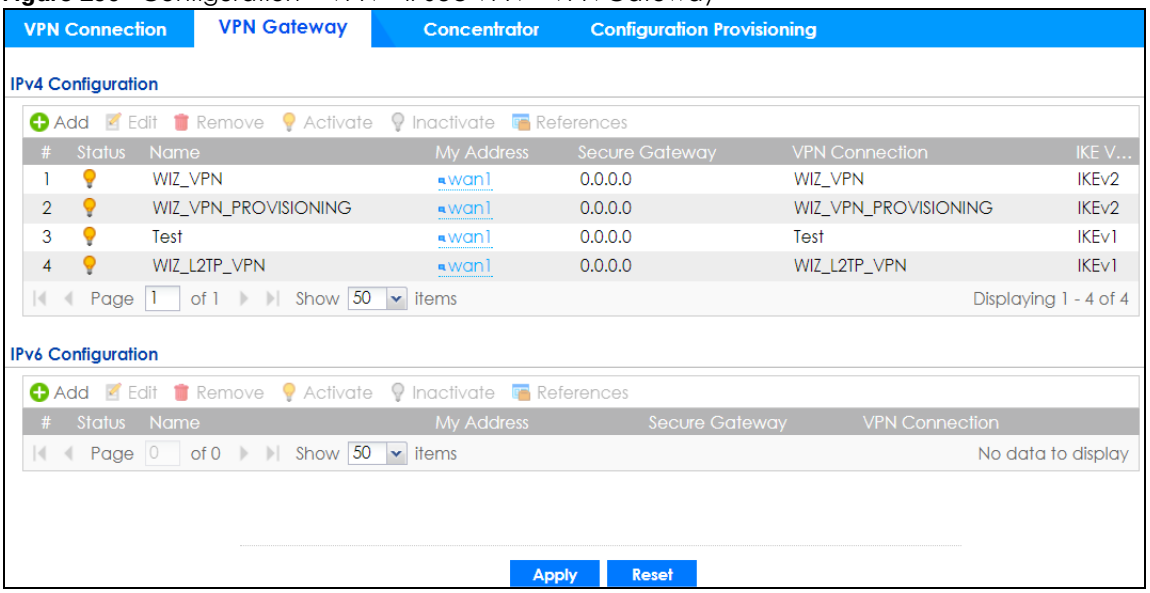
Table 159 Configuration > VPN > IPSec VPN > VPN Connection > Add/Edit (continued)

LABEL	DESCRIPTION
Move	To change an entry's position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
#	This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed.
Original IP	Select the address object that represents the original destination address. This is the address object for the remote network.
Mapped IP	Select the address object that represents the desired destination address. For example, this is the address object for the mail server.
Protocol	Select the protocol required to use this translation. Choices are: **TCP**, **UDP**, or **All**.
Original Port Start / Original Port End	These fields are available if the protocol is **TCP** or **UDP**. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range.
Mapped Port Start / Mapped Port End	These fields are available if the protocol is **TCP** or **UDP**. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range.
OK	Click **OK** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

20.3 The VPN Gateway Screen

The **VPN Gateway** summary screen displays the IPSec VPN gateway policies in the Zyxel Device, as well as the Zyxel Device's address, remote IPSec router's address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway. To access this screen, click **Configuration > VPN** > **Network** > **IPSec VPN** > **VPN Gateway**. The following screen appears.

Figure 290 Configuration > VPN > IPSec VPN > VPN Gateway



Each field is discussed in the following table. See Section 20.3.1 on page 411 for more information.

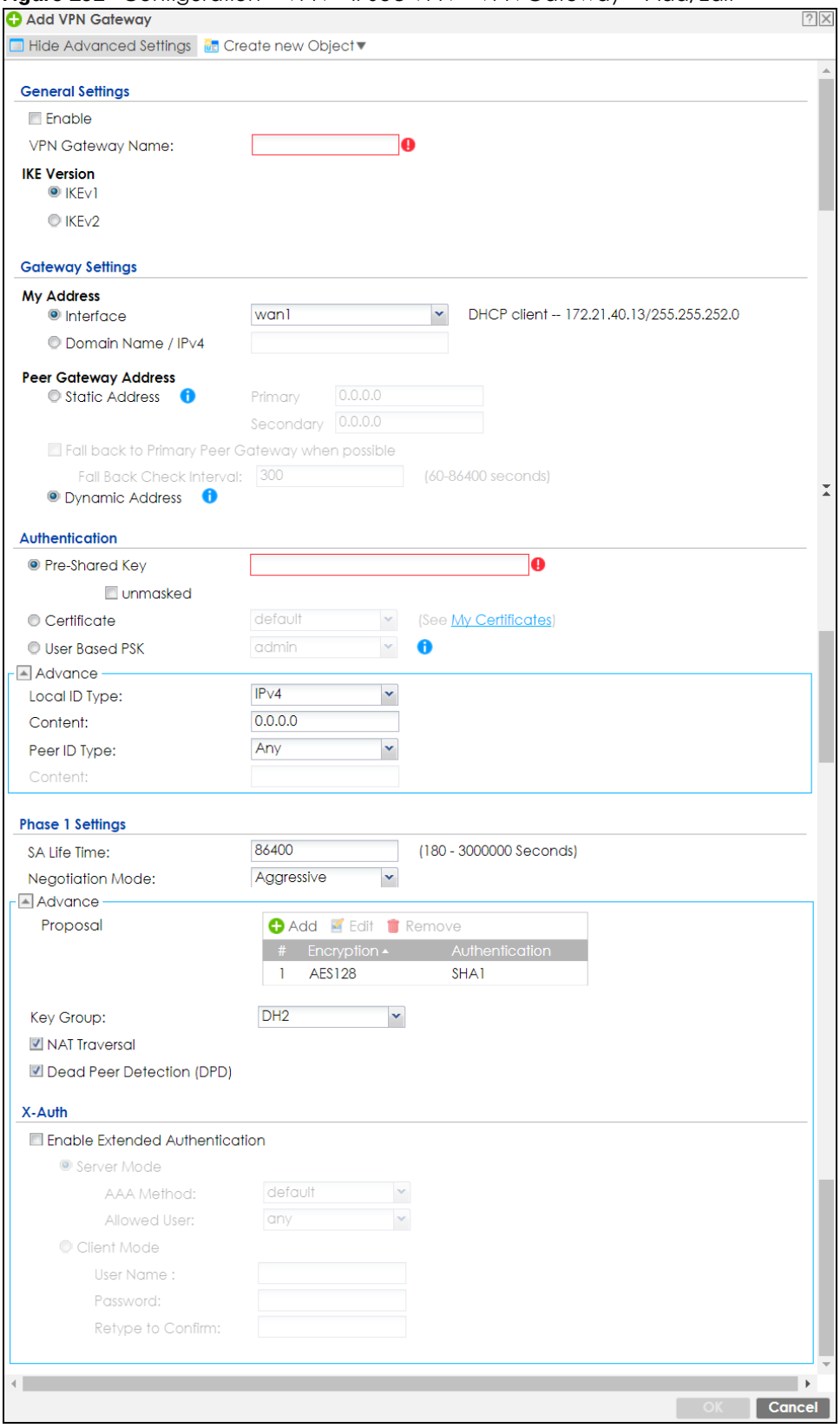
Table 160 Configuration > VPN > IPSec VPN > VPN Gateway

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. See Section 9.4.4 on page 240 for an example.
#	This field is a sequential value, and it is not associated with a specific VPN gateway.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the name of the VPN gateway
My address	This field displays the interface or a domain name the Zyxel Device uses for the VPN gateway.
Secure Gateway	This field displays the IP address(es) of the remote IPSec routers.
VPN Connection	This field displays VPN connections that use this VPN gateway.
IKE Version	This field displays whether the gateway is using **IKEv1** or **IKEv2**. **IKEv1** applies to IPv4 traffic only. **IKEv2** applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 20.1 on page 396 for more information on IKEv1 and IKEv2.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.3.1 The VPN Gateway Add/Edit Screen

The **VPN Gateway Add/Edit** screen allows you to create a new VPN gateway policy or edit an existing one. To access this screen, go to the **VPN Gateway summary** screen (see Section 20.3 on page 410), and click either the **Add** icon or an **Edit** icon.

Figure 291 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit



Each field is described in the following table.

Table 161 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create New Object	Use to configure any new settings objects that you need to use in this screen.
General Settings	
Enable	Select this to activate the VPN Gateway policy.
VPN Gateway Name	Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IKE Version	
IKEv1 / IKEv2	Select **IKEv1** or **IKEv2**. **IKEv1** applies to IPv4 traffic only. IKEv2 applies to both IPv4 and IPv6 traffic. IKE (Internet Key Exchange) is a protocol used in setting up security associations that allows two parties to send data securely. See Section 20.1 on page 396 for more information on IKEv1 and IKEv2.
Gateway Settings	
My Address	Select how the IP address of the Zyxel Device in the IKE SA is defined. If you select **Interface**, select the Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface or PPPoE/PPTP interface. The IP address of the Zyxel Device in the IKE SA is the IP address of the interface. If you select **Domain Name / IP**, enter the domain name or the IP address of the Zyxel Device. The IP address of the Zyxel Device in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is not generally recommended as it has the Zyxel Device accept IPSec requests destined for any interface address on the Zyxel Device.
Peer Gateway Address	Select how the IP address of the remote IPSec router in the IKE SA is defined. Select **Static Address** to enter the domain name or the IP address of the remote IPSec router. You can provide a second IP address or domain name for the Zyxel Device to try if it cannot establish an IKE SA with the first one. **Fall back to Primary Peer Gateway when possible**: When you select this, if the connection to the primary address goes down and the Zyxel Device changes to using the secondary connection, the Zyxel Device will reconnect to the primary address when it becomes available again and stop using the secondary connection. Users will lose their VPN connection briefly while the Zyxel Device changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection. In the **Fallback Check Interval** field, set how often to check if the primary address is available. Select **Dynamic Address** if the remote IPSec router has a dynamic IP address (and does not use DDNS).
Authentication	Note: The Zyxel Device and remote IPSec router must use the same authentication method to establish the IKE SA.

Table 161 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Pre-Shared Key	Select this to have the Zyxel Device and remote IPSec router use a pre-shared key (password) of up to 128 characters to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be: • alphanumeric characters or ,;. | `~!@#$%^&*()_+\{}':./<>=-" • pairs of hexadecimal (0-9, A-F) characters, preceded by "0x". Type "0x" at the beginning of a hexadecimal key. For example, "0x0123456789ABCDEF" is in hexadecimal format; "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs. The Zyxel Device and remote IPSec router must use the same pre-shared key. Select **unmasked** to see the pre-shared key in readable plain text.
Certificate	Select this to have the Zyxel Device and remote IPSec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the Zyxel Device uses to identify itself to the remote IPSec router. This certificate is one of the certificates in **My Certificates**. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA. Note: The IPSec routers must trust each other's certificates. The Zyxel Device uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.
User-based PSK	User-based PSK (IKEv1 only) generates and manages separate pre-shared keys for every user. This enables multiple users, each with a unique key, to access the same VPN gateway policy with one-to-one authentication and strong encryption. Access can be denied on a per-user basis thus allowing VPN SA user-based policies. Click **User-Based PSK** then select a user or group object who is allowed VPN SA access using this VPN gateway policy. This is for IKEv1 only.
Local ID Type	This field is read-only if the Zyxel Device and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the Zyxel Device during authentication. Choices are: **IPv4** or **IPv6** - the Zyxel Device is identified by an IP address **DNS** - the Zyxel Device is identified by a domain name **E-mail** - the Zyxel Device is identified by the string specified in this field
Content	This field is read-only if the Zyxel Device and remote IPSec router use certificates to identify each other. Type the identity of the Zyxel Device during authentication. The identity depends on the **Local ID Type**. **IP** - type an IP address; if you type 0.0.0.0, the Zyxel Device uses the IP address specified in the **My Address** field. This is not recommended in the following situations: • There is a NAT router between the Zyxel Device and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Local ID Type**. **DNS** - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. **E-mail** - the Zyxel Device is identified by the string you specify here; you can use up to 63 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.

Table 161 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Peer ID Type	Select which type of identification is used to identify the remote IPSec router during authentication. Choices are: **IP** - the remote IPSec router is identified by an IP address **DNS** - the remote IPSec router is identified by a domain name **E-mail** - the remote IPSec router is identified by the string specified in this field **Any** - the Zyxel Device does not check the identity of the remote IPSec router If the Zyxel Device and remote IPSec router use certificates, there is one more choice. **Subject Name** - the remote IPSec router is identified by the subject name in the certificate
Content	This field is disabled if the **Peer ID Type** is **Any**. Type the identity of the remote IPSec router during authentication. The identity depends on the **Peer ID Type**. If the Zyxel Device and remote IPSec router do not use certificates, **IP** - type an IP address; see the note at the end of this description. **DNS** - type the fully qualified domain name (FQDN). This value is only used for identification and can be any string that matches the peer ID string. **E-mail** - the remote IPSec router is identified by the string you specify here; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. If the Zyxel Device and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router. **IP** - subject alternative name field; see the note at the end of this description. **DNS** - subject alternative name field **E-mail** - subject alternative name field **Subject Name** - subject name (maximum 255 ASCII characters, including spaces) Note: If **Peer ID Type** is **IP**, please read the rest of this section. If you type 0.0.0.0, the Zyxel Device uses the IP address specified in the **Secure Gateway Address** field. This is not recommended in the following situations: • There is a NAT router between the Zyxel Device and remote IPSec router. • You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses. In these situations, use a different IP address, or use a different **Peer ID Type**.
Phase 1 Settings	
SA Life Time (Seconds)	Type the maximum number of seconds the IKE SA can last. When this time has passed, the Zyxel Device and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however.
Negotiation Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are **Main** - this encrypts the Zyxel Device's and remote IPSec router's identities but takes more time to establish the IKE SA **Aggressive** - this is faster but does not encrypt the identities The Zyxel Device and the remote IPSec router must use the same negotiation mode.
Proposal	Use this section to manage the encryption algorithm and authentication algorithm pairs the Zyxel Device accepts from the remote IPSec router for negotiating the IKE SA.
Add	Click this to create a new entry.

Table 161 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly.
Encryption	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The Zyxel Device and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1**, **SHA256**, **SHA512** and **MD5**. SHA is generally considered stronger than **MD5**, but it is also slower. The remote IPSec router must use the same authentication algorithm.
Key Group	Select which Diffie-Hellman key group (DHx) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number **DH5** - use a 1536-bit random number **DH14** - use a 2048 bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
NAT Traversal	Select this if any of these conditions are satisfied. • This IKE SA might be used to negotiate IPSec SAs that use ESP as the active protocol. • There are one or more NAT routers between the Zyxel Device and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged. This field applies for IKEv1 only. NAT Traversal is always performed when you use IKEv2.
Dead Peer Detection (DPD)	Select this check box if you want the Zyxel Device to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the Zyxel Device sends a message to the remote IPSec router. If the remote IPSec router responds, the Zyxel Device transmits the data. If the remote IPSec router does not respond, the Zyxel Device shuts down the IKE SA. If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 20.2.1 on page 403). This field applies for IKEv1 only. Dead Peer Detection (DPD) is always performed when you use IKEv2.
X Auth / Extended Authentication Protocol	This part of the screen displays **X-Auth** when using **IKEv1** and **Extended Authentication Protocol** when using **IKEv2**.

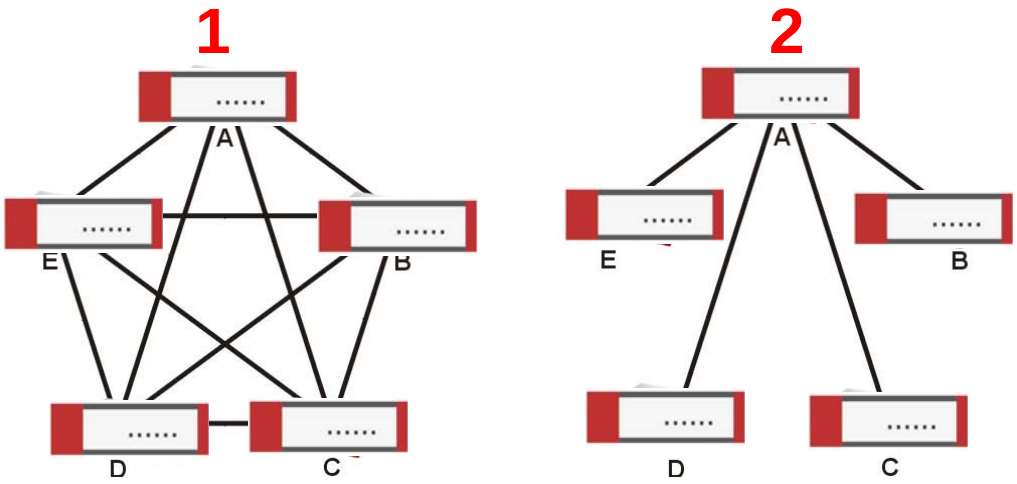
Table 161 Configuration > VPN > IPSec VPN > VPN Gateway > Add/Edit (continued)

LABEL	DESCRIPTION
X-Auth	This displays when using IKEv1. When different users use the same VPN tunnel to connect to the Zyxel Device (telecommuters sharing a tunnel for example), use X-auth to enforce a user name and password check. This way even though telecommuters all know the VPN tunnel's security settings, each still has to provide a unique user name and password.
Enable Extended Authentication	Select this if one of the routers (the Zyxel Device or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server.
Server Mode	Select this if the Zyxel Device authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the Zyxel Device authenticates this information.
AAA Method	Select the authentication method, which specifies how the Zyxel Device authenticates this information.
Allowed User	Extended authentication now supports an allowed user. Select what users should be authenticated.
Client Mode	Select this radio button if the Zyxel Device provides a username and password to the remote IPSec router for authentication. You also have to provide the **User Name** and the **Password**.
User Name	This field is required if the Zyxel Device is in **Client Mode** for extended authentication. Type the user name the Zyxel Device sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the Zyxel Device is in **Client Mode** for extended authentication. Type the password the Zyxel Device sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Retype to Confirm	Type the exact same password again here to make sure an error was not made when typing it originally.
Extended Authentication Protocol	This displays when using **IKEv2**. EAP uses a certificate for authentication.
Enable Extended Authentication Protocol	Select this if one of the routers (the Zyxel Device or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server or a certificate.
Allowed Auth Method	This field displays the authentication method that is used to authenticate the users.
Server Mode	Select this if the Zyxel Device authenticates the user name and password from the remote IPSec router. You also have to select an AAA method, which specifies how the Zyxel Device authenticates this information and who may be authenticated (**Allowed User**).
Client Mode	Select this radio button if the Zyxel Device provides a username and password to the remote IPSec router for authentication. You also have to provide the **User Name** and the **Password**.
User Name	This field is required if the Zyxel Device is in **Client Mode** for extended authentication. Type the user name the Zyxel Device sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Password	This field is required if the Zyxel Device is in **Client Mode** for extended authentication. Type the password the Zyxel Device sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed.
Retype to Confirm	Type the exact same password again here to make sure an error was not made when typing it originally.
OK	Click **OK** to save your settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

20.4 VPN Concentrator

A VPN concentrator combines several IPSec VPN connections into one secure network.

Figure 292 VPN Topologies (Fully Meshed and Hub and Spoke)



In a fully-meshed VPN topology (**1** in the figure), there is a VPN connection between every pair of routers. In a hub-and-spoke VPN topology (**2** in the figure), there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**), which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.

A VPN concentrator reduces the number of VPN connections that you have to set up and maintain in the network. You might also be able to consolidate the policy routes in each spoke router, depending on the IP addresses and subnets of each spoke.

However a VPN concentrator is not for every situation. The hub router is a single failure point, so a VPN concentrator is not as appropriate if the connection between spoke routers cannot be down occasionally (maintenance, for example). There is also more burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out to which spoke to route it, encrypts it, and sends it to the appropriate spoke. Therefore, a VPN concentrator is more suitable when there is a minimum amount of traffic between spoke routers.

20.4.1 VPN Concentrator Requirements and Suggestions

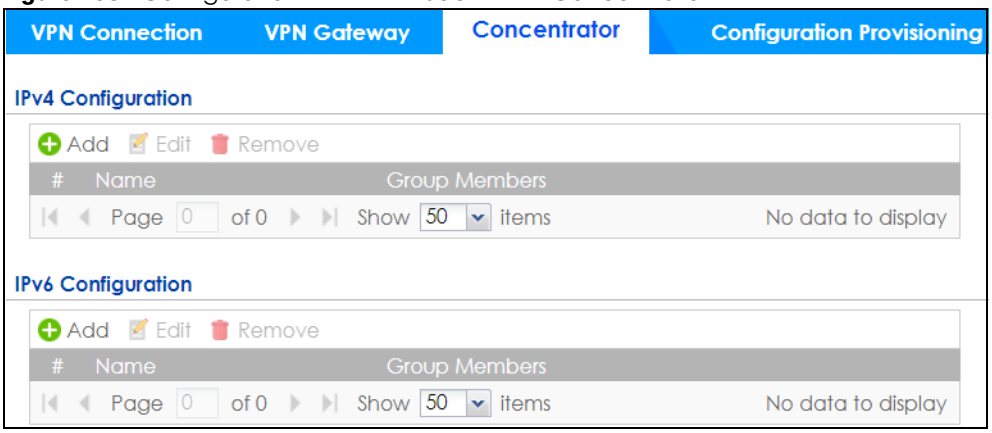
Consider the following when using the VPN concentrator.

- The local IP addresses configured in the VPN rules should not overlap.
- The concentrator must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule for each spoke.
- To have all Internet access from the spoke routers go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Your security policies can still block VPN packets.

20.4.2 VPN Concentrator Screen

The **VPN Concentrator** summary screen displays the VPN concentrators in the Zyxel Device. To access this screen, click **Configuration > VPN** > **IPSec VPN** > **Concentrator**.

Figure 293 Configuration > VPN > IPSec VPN > Concentrator



Each field is discussed in the following table. See Section 20.4.3 on page 419 for more information.

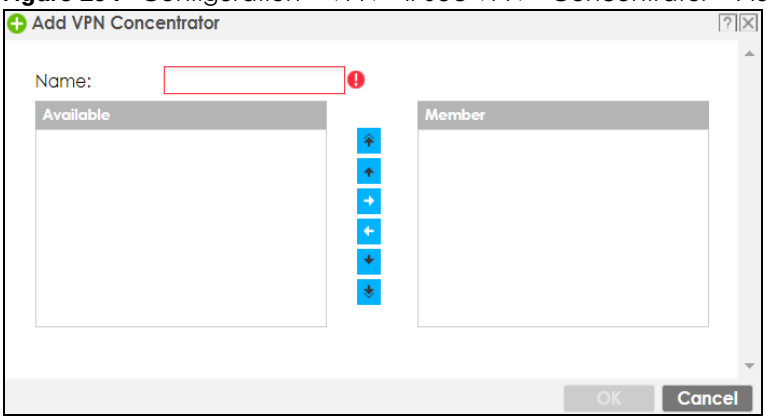
Table 162 Configuration > VPN > IPSec VPN > Concentrator

LABEL	DESCRIPTION
IPv4/IPv6 Configuration	Choose to configure for IPv4 or IPv6 traffic.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This field is a sequential value, and it is not associated with a specific concentrator.
Name	This field displays the name of the VPN concentrator.
Group Members	These are the VPN connection policies that are part of the VPN concentrator.

20.4.3 The VPN Concentrator Add/Edit Screen

Use the **VPN Concentrator Add/Edit** screen to create or edit a VPN concentrator. To access this screen, go to the **VPN Concentrator summary** screen (see Section 20.4 on page 418), and click either the **Add** icon or an **Edit** icon.

Figure 294 Configuration > VPN > IPSec VPN > Concentrator > Add/Edit



Each field is described in the following table.

Table 163 VPN > IPSec VPN > Concentrator > Add/Edit

LABEL	DESCRIPTION
Name	Enter the name of the concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member	Select the concentrator's IPSec VPN connection policies. Note: You must disable policy enforcement in each member. See Section 20.2.1 on page 403. IPSec VPN connection policies that do not belong to a VPN concentrator appear under **Available**. Select any VPN connection policies that you want to add to the VPN concentrator and click the right arrow button to add them. The VPN concentrator's member VPN connections appear under **Member**. Select any VPN connections that you want to remove from the VPN concentrator, and click the left arrow button to remove them.
OK	Click **OK** to save your changes in the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

20.5 Zyxel Device IPSec VPN Client Configuration Provisioning

Use the **Configuration > VPN > IPSec VPN > Configuration Provisioning** screen to configure who can retrieve VPN rule settings from the Zyxel Device using the Zyxel Device IPSec VPN Client. In the Zyxel Device IPSec VPN Client, you just need to enter the IP address of the Zyxel Device to get all the VPN rule settings automatically. You do not need to manually configure all rule settings in the Zyxel Device IPSec VPN client.

VPN rules for the Zyxel Device IPSec VPN Client have certain restrictions. They must *not* contain the following settings:

- **AH** active protocol
- **NULL** encryption
- **SHA512** authentication

- A subnet or range remote policy

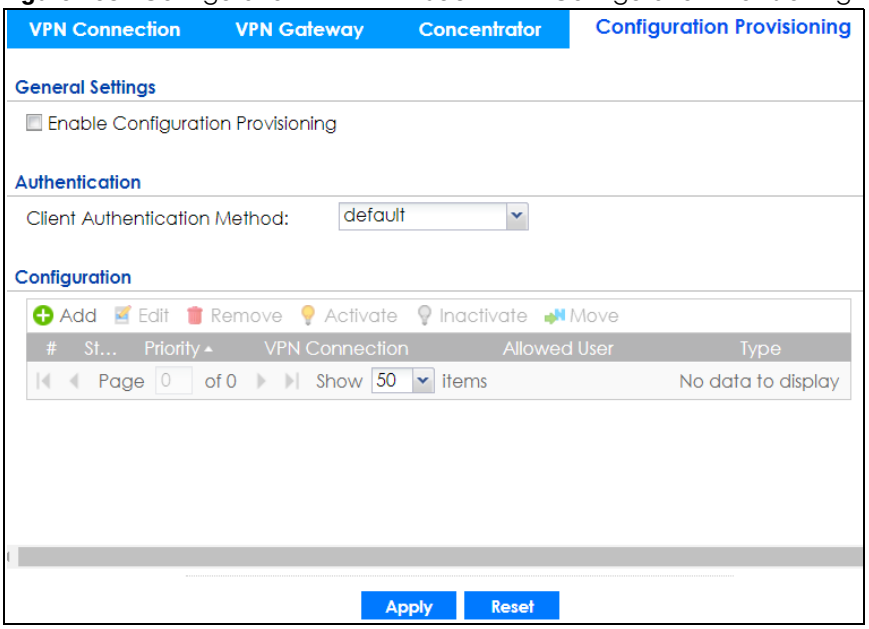
The following VPN Gateway rules configured on the Zyxel Device cannot be provisioned to the IPSec VPN Client:

- IPv4 rules with IKEv2 version
- IPv4 rules with User-based PSK authentication

Note: You must enable IPv6 in System > IPv6 to activate IPv6 VPN tunneling rules.

In the Zyxel Device **Quick Setup** wizard, you can use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that will not violate these restrictions.

Figure 295 Configuration > VPN > IPSec VPN > Configuration Provisioning



Each field is discussed in the following table.

Table 164 Configuration > VPN > IPSec VPN > Configuration Provisioning

LABEL	DESCRIPTION
Enable Configuration Provisioning	Select this for users to be able to retrieve VPN rule settings using the Zyxel Device IPSec VPN client.
Client Authentication Method	Choose how users should be authenticated. They can be authenticated using the local database on the Zyxel Device or an external authentication database such as LDAP, Active Directory or RADIUS. **default** is a method you configured in **Object > Auth Method.** You may configure multiple methods there. If you choose the local database on the Zyxel Device, then configure users using the **Object > User/Group** screen. If you choose LDAP, Active Directory or RADIUS authentication servers, then configure users on the respective server.
Configuration	When you add or edit a configuration provisioning entry, you are allowed to set the **VPN Connection** and **Allowed User** fields. Duplicate entries are not allowed. You cannot select the same **VPN Connection** and **Allowed User** pair in a new entry if the same pair exists in a previous entry. You can bind different rules to the same user, but the Zyxel Device will only allow VPN rule setting retrieval for the first match found.

Table 164 Configuration > VPN > IPSec VPN > Configuration Provisioning (continued)

LABEL	DESCRIPTION
Add	Click **Add** to bind a configured VPN rule to a user or group. Only that user or group may then retrieve the specified VPN rule settings. If you click **Add** without selecting an entry in advance then the new entry appears as the first entry. Entry order is important as the Zyxel Device searches entries in the order listed here to find a match. After a match is found, the Zyxel Device stops searching. If you want to add an entry as number three for example, then first select entry 2 and click **Add**. To reorder an entry, use **Move**.
Edit	Select an existing entry and click **Edit** to change its settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**. Make sure that **Enable Configuration Provisioning** is also selected.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	Use **Move** to reorder a selected entry. Select an entry, click **Move**, type the number where the entry should be moved, press <ENTER>, then click **Apply**.
Status	This icon shows if the entry is active (yellow) or not (gray). VPN rule settings can only be retrieved when the entry is activated (and **Enable Configuration Provisioning** is also selected).
Priority	Priority shows the order of the entry in the list. Entry order is important as the Zyxel Device searches entries in the order listed here to find a match. After a match is found the Zyxel Device stops searching.
VPN Connection	This field shows all configured VPN rules that match the rule criteria for the Zyxel Device IPSec VPN client. Select a rule to bind to the associated user or group.
Allowed User	Select which user or group of users is allowed to retrieve the associated VPN rule settings using the Zyxel Device IPSec VPN client. A user may belong to a number of groups. If entries are configured for different groups, the Zyxel Device will allow VPN rule setting retrieval based on the first match found. Users of type **admin** or **limited-admin** are not allowed.
Type	This field shows how traffic is tunneled from the Zyxel Device to the Zyxel VPN client: • **6in4** (tunnel IPv6 traffic from the Zyxel Device to the Zyxel client in an IPv4 network); • **4in6** (tunnel IPv4 traffic from the Zyxel Device to the Zyxel VPN client in an IPv6 network); • **4in4** (tunnel IPv4 traffic from the Zyxel Device to the Zyxel VPN client in an IPv4 network).
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

20.6 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

IKE SA Overview

The IKE SA provides a secure connection between the Zyxel Device and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode. Main mode is used in various examples in the rest of this section.

The Zyxel Device supports IKEv1 and IKEv2. See Section 20.1 on page 396 for more information.

IP Addresses of the Zyxel Device and Remote IPSec Router

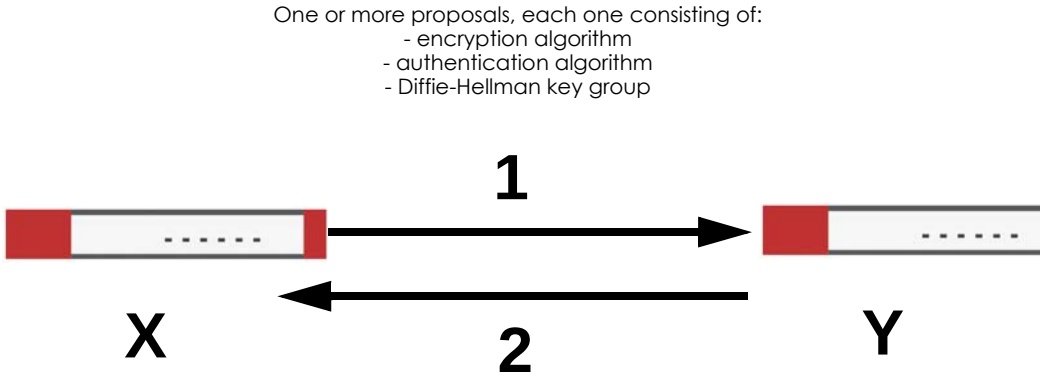
To set up an IKE SA, you have to specify the IP addresses of the Zyxel Device and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your Zyxel Device might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the Zyxel Device does not know the IP address of the remote IPSec router. This is often used for telecommuters.

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the Zyxel Device and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

Figure 296 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The Zyxel Device sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the Zyxel Device wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the Zyxel Device. If the remote IPSec router rejects all of the proposals, the Zyxel Device and remote IPSec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most Zyxel Devices, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.

- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some Zyxel Devices also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most Zyxel Devices, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

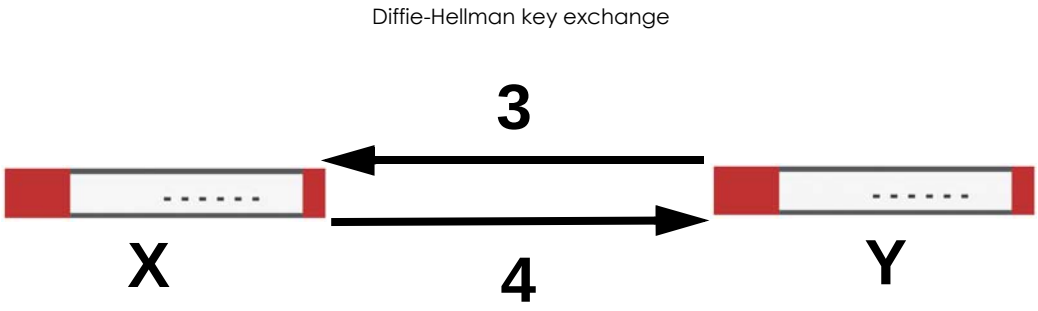
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
- SHA256 (Secure Hash Algorithm) produces a 256-bit digest to authenticate packet data.
- SHA512 (Secure Hash Algorithm) produces a 512-bit digest to authenticate packet data.

See Diffie-Hellman (DH) Key Exchange on page 424 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The Zyxel Device and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

Figure 297 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



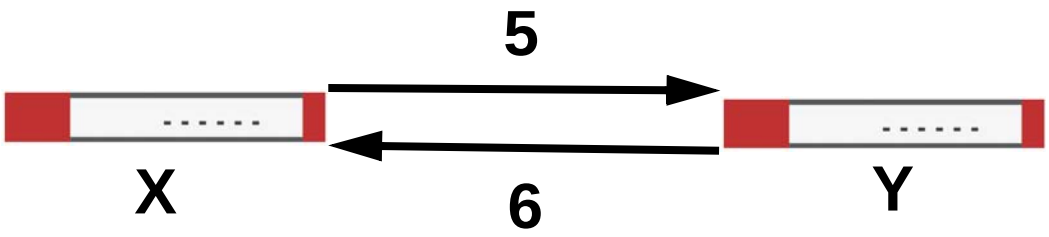
DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

Authentication

Before the Zyxel Device and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the Zyxel Device and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the Zyxel Device and remote IPSec router selected in previous steps.

Figure 298 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)



You have to create (and distribute) a pre-shared key. The Zyxel Device and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

Note: The Zyxel Device and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and content. The ID type can be domain name, IP address, or email address, and the content is a (properly-formatted) domain name, IP address, or email address. The content is only used for identification. Any domain name or email address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the Zyxel Device's or remote IPSec router's properties.

The Zyxel Device and the remote IPSec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

Note: The Zyxel Device's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in the next table, the Zyxel Device and the remote IPSec router authenticate each other successfully. In contrast, in the following table, the Zyxel Device and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

Table 165 VPN Example: Matching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

Table 166 VPN Example: Mismatching ID Type and Content

ZYXEL DEVICE	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.20	Peer ID content: tom@yourcompany.com

It is also possible to configure the Zyxel Device to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is less secure, so you should only use this if your Zyxel Device provides another way to check the identity of the remote IPSec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

Additional Topics for IKE SA

This section provides more information about IKE SA.

Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The Zyxel Device sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the Zyxel Device.

Steps 3 - 4: The Zyxel Device and the remote IPSec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

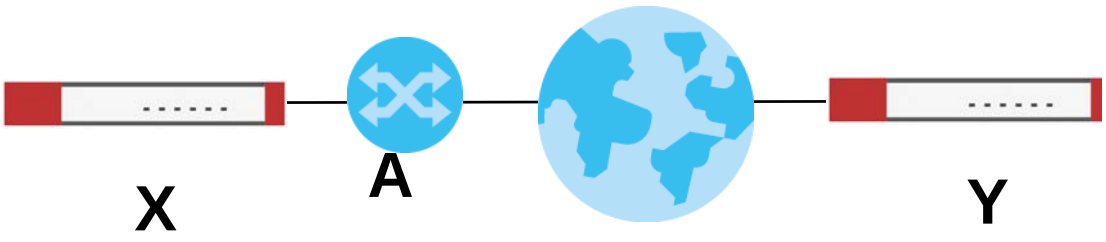
Steps 5 - 6: Finally, the Zyxel Device and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the Zyxel Device and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 299 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-thru feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Active Protocol on page 428 for more information about active protocols.)

If router A does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the Zyxel Device and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the Zyxel Device and remote IPSec router support.

X-Auth / Extended Authentication

X-Auth / Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the Zyxel Device or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the Zyxel Device to provide a user name and password to the remote IPSec router, or you can set up the Zyxel Device to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

Certificates

It is possible for the Zyxel Device and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the Zyxel Device and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the Zyxel Device and remote IPSec router first.

IPSec SA Overview

Once the Zyxel Device and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

Local Network and Remote Network

In an IPSec SA, the local network, the one(s) connected to the Zyxel Device, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The Zyxel Device and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the Zyxel Device and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The Zyxel Device and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 300 VPN: Transport and Tunnel Mode Encapsulation

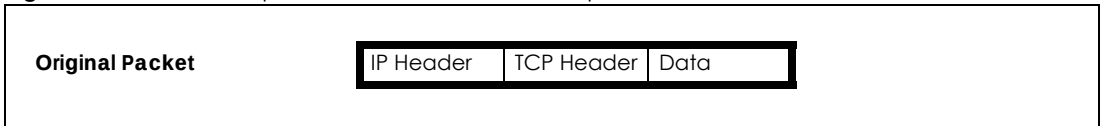
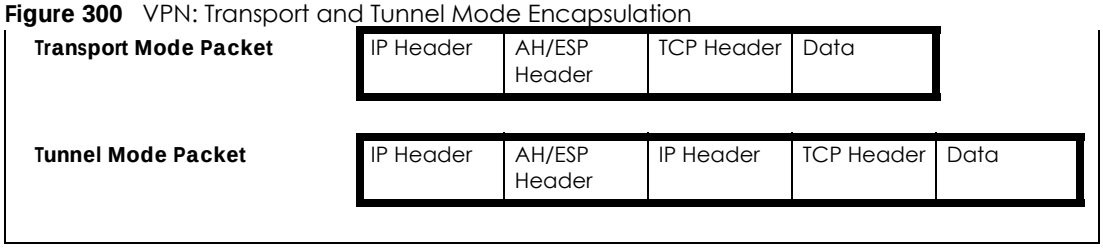


Figure 300 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the Zyxel Device uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the Zyxel Device or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the Zyxel Device or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the Zyxel Device includes part of the original IP header when it encapsulates the packet. With ESP, however, the Zyxel Device does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal), except that you also have the choice whether or not the Zyxel Device and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the Zyxel Device and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the Zyxel Device and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

PFS is ignored in initial IKEv2 authentication but is used when re-authenticating.

Additional Topics for IPSec SA

This section provides more information about IPSec SA in your Zyxel Device.

Authentication and the Security Parameter Index (SPI)

For authentication, the Zyxel Device and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The Zyxel Device and remote IPSec router must use the same SPI.

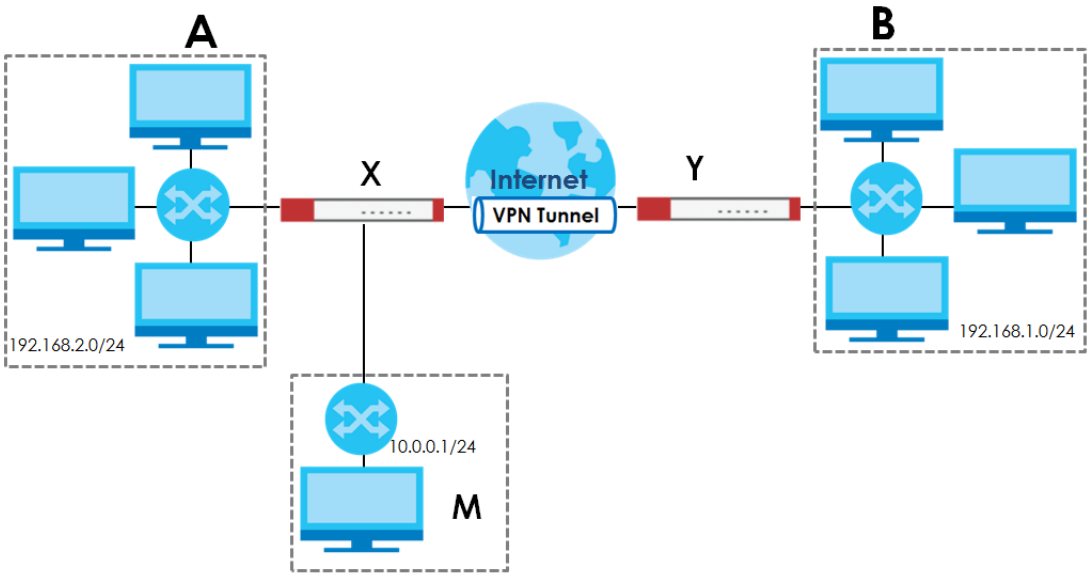
NAT for Inbound and Outbound Traffic

The Zyxel Device can translate the following types of network addresses in IPSec SA.

- Source address in outbound packets - this translation is necessary if you want the Zyxel Device to route packets from computers outside the local network through the IPSec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

Figure 301 VPN Example: NAT for Inbound and Outbound Traffic



Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the Zyxel Device route packets from computers that are not part of the specified local network (local policy) through the IPSec SA. For example, in Figure 301 on page 430, you have to configure this kind of translation if you want computer **M** to establish a connection with any computer in the remote network (**B**). If you do not configure it, the remote IPSec router may not route messages for computer **M** through the IPSec SA because computer **M**'s IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer **M**'s network.
- Destination - the original destination address; the remote network (**B**).
- SNAT - the translated source address; the local network (**A**).

Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (**B**).
- Destination - the original destination address; the local network (**A**).
- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the Zyxel Device to forward some packets from the remote network to a specific computer in the local network. For example, in Figure 301 on page 430, you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (**A**).

You have to specify one or more rules when you set up this kind of NAT. The Zyxel Device checks these rules similar to the way it checks rules for a security policy. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (**B**).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in Figure 301 on page 430, it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

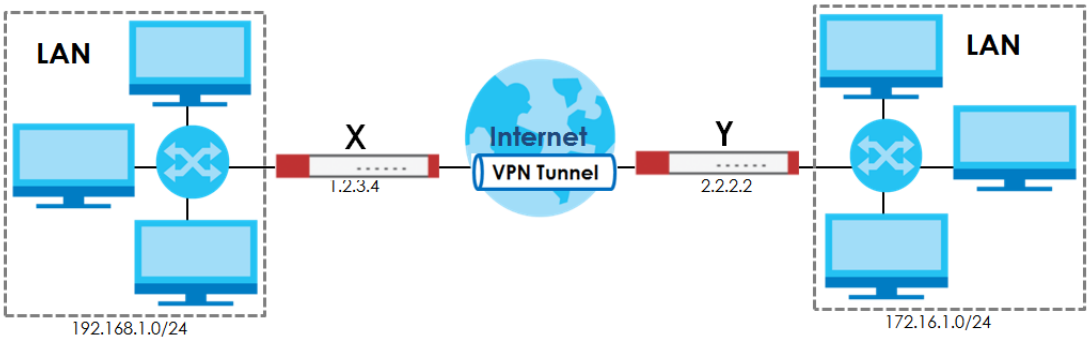
- Mapped IP - the translated destination address; in Figure 301 on page 430, the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

IPSec VPN Example Scenario

Here is an example site-to-site IPSec VPN scenario.

Figure 302 Site-to-site IPSec VPN Example



CHAPTER 21
SSL VPN

21.1 Overview

Use SSL VPN to allow users to use a web browser for secure remote user login. The remote users do not need a VPN router or VPN client software.

21.1.1 What You Can Do in this Chapter

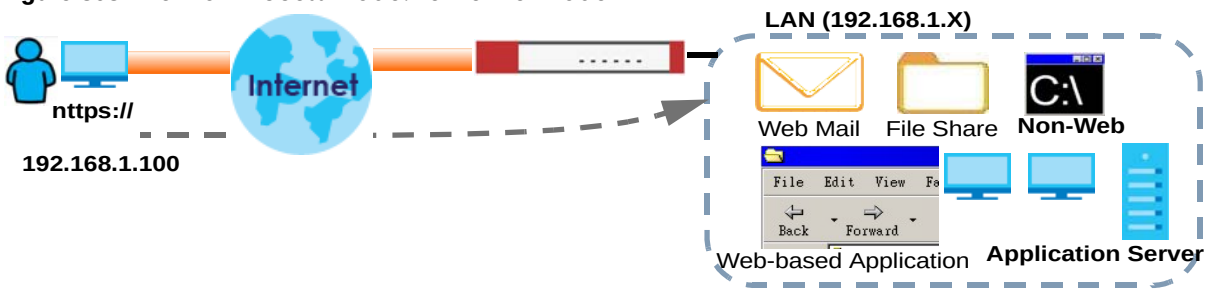
- Use the **VPN > SSL VPN > Access Privilege** screens (see Section 21.2 on page 433) to configure SSL access policies.
- Use the Click **VPN > SSL VPN** > **Global Setting** screen (see Section 21.3 on page 436) to set the IP address of the Zyxel Device (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

21.1.2 What You Need to Know

Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

Figure 303 Network Access Mode: Full Tunnel Mode



SSL Access Policy

An SSL access policy allows the Zyxel Device to perform the following tasks:

- limit user access to specific applications or file sharing server on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

SSL Access Policy Objects

The SSL access policies reference the following objects. If you update this information, in response to changes, the Zyxel Device automatically propagates the changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

Table 167 Objects

OBJECT TYPE	OBJECT SCREEN	DESCRIPTION
User Accounts	User Account/ User Group	Configure a user account or user group to which you want to apply this SSL access policy.
Application	SSL Application	Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access.
IP Pool	Address	Configure an address object that defines a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection.
Server Addresses	Address	Configure address objects for the IP addresses of the DNS and WINS servers that the Zyxel Device sends to the VPN connection users.
VPN Network	Address	Configure an address object to specify which network segment users are allowed to access through a VPN connection.

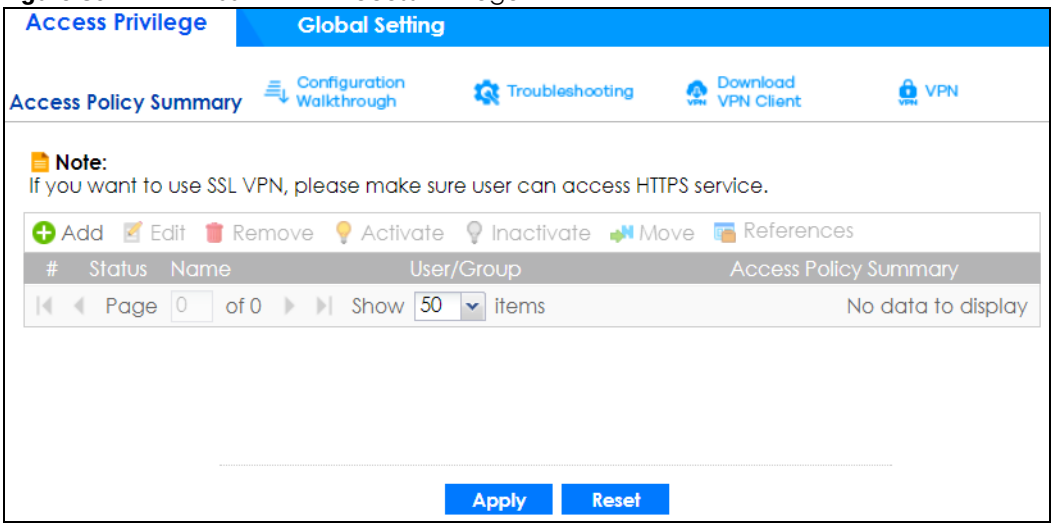
You cannot delete an object that is referenced by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

21.2 The SSL Access Privilege Screen

Click **VPN > SSL VPN** to open the **Access Privilege** screen. This screen lists the configured SSL access policies.

Click on the icons to go to the OneSecurity website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 304 VPN > SSL VPN > Access Privilege



The following table describes the labels in this screen.

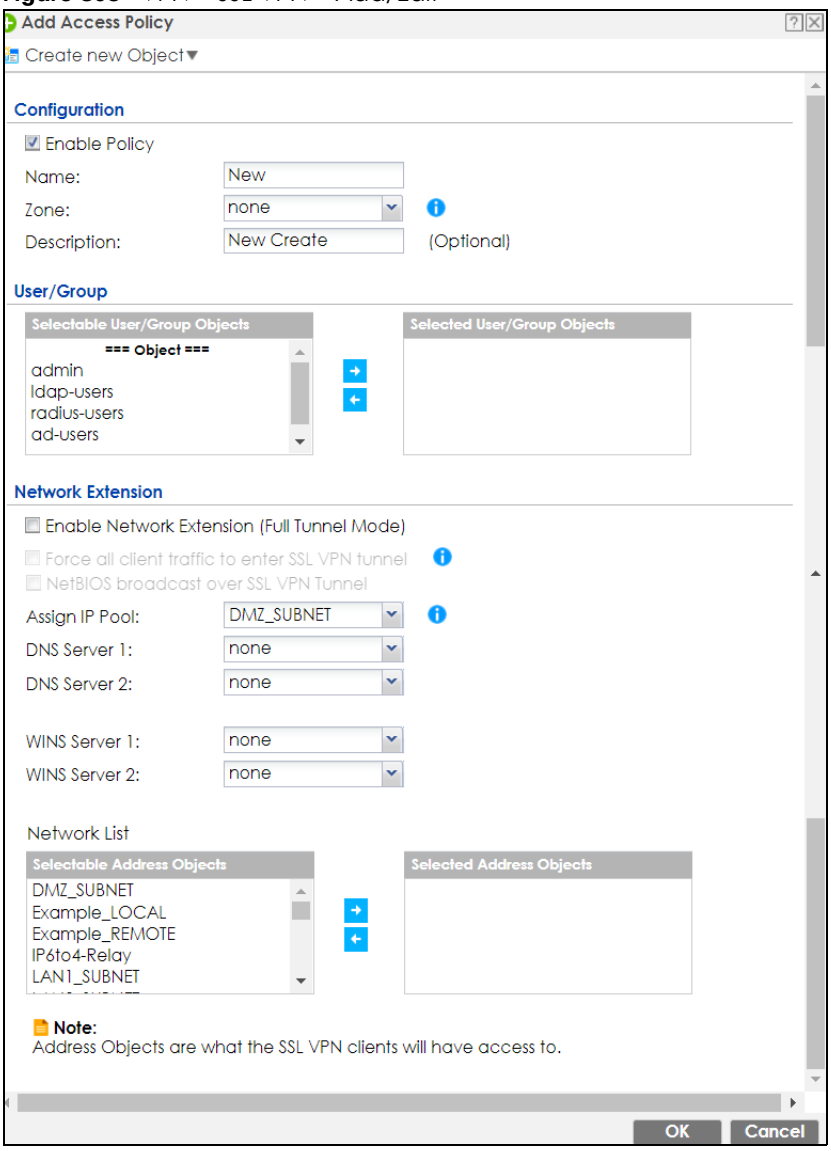
Table 168 VPN > SSL VPN > Access Privilege

LABEL	DESCRIPTION
Access Policy Summary	This screen shows a summary of SSL VPN policies created. Click on the VPN icon to go to the Zyxel VPN Client product page at the Zyxel website.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
References	Select an entry and click **References** to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This field displays the index number of the entry.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Name	This field displays the descriptive name of the SSL access policy for identification purposes.
User/Group	This field displays the user account or user group name(s) associated to an SSL access policy. This field displays up to three names.
Access Policy Summary	This field displays details about the SSL application object this policy uses including its name, type, and address.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to discard all changes.

21.2.1 The SSL Access Privilege Policy Add/Edit Screen

To create a new or edit an existing SSL access policy, click the **Add** or **Edit** icon in the **Access Privilege** screen.

Figure 305 VPN > SSL VPN > Add/Edit



The following table describes the labels in this screen.

Table 169 VPN > SSL VPN > Access Privilege > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable Policy	Select this option to activate this SSL access policy.
Name	Enter a descriptive name to identify this policy. You can enter up to 31 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed.
Zone	Select the zone to which to add this SSL access policy. You use zones to apply security settings such as security policy and remote management.
Description	Enter additional information about this SSL access policy. You can enter up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").

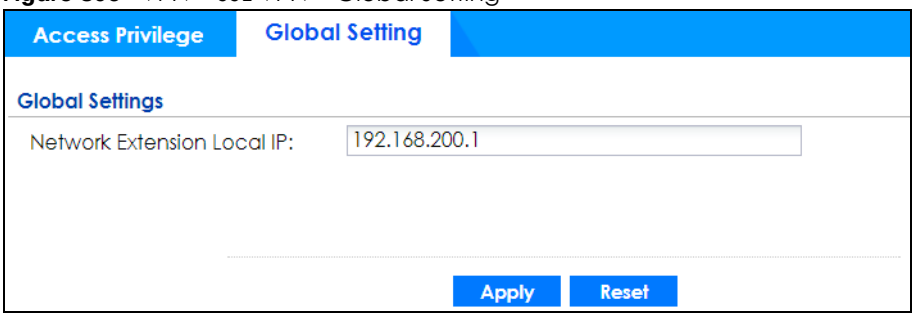
Table 169 VPN > SSL VPN > Access Privilege > Add/Edit (continued)

LABEL	DESCRIPTION
User/Group	The **Selectable User/Group Objects** list displays the name(s) of the user account and/or user group(s) to which you have not applied an SSL access policy yet. To associate a user or user group to this SSL access policy, select a user account or user group and click the right arrow button to add to the **Selected User/Group Objects** list. You can select more than one name. To remove a user or user group, select the name(s) in the **Selected User/Group Objects** list and click the left arrow button. Note: Although you can select admin and limited-admin accounts in this screen, they are reserved for device configuration only. You cannot use them to access the SSL VPN portal.
Network Extension (Optional)	
Enable Network Extension	Select this option to create a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network. This includes access to resources not supported by SSL application objects. For example this lets users Telnet to the internal network even though the Zyxel Device does not have SSL application objects for Telnet. Clear this option to disable this feature. Users can only access the applications as defined by the VPN tunnel's selected SSL application settings and the remote user computers are not made to be a part of the local network.
Force all client traffic to SSL VPN tunnel	Select this to send all traffic from the SSL VPN clients through the SSL VPN tunnel. This replaces the default gateway of the SSL VPN clients with the SSL VPN gateway.
NetBIOS broadcast over SSL VPN Tunnel	Select this to search for a remote computer and access its applications as if it was in a Local Area Network. The user can find a computer not only by its IP address but also by computer name.
Assign IP Pool	Define a separate pool of IP addresses to assign to the SSL users. Select it here. The SSL VPN IP pool should not overlap with IP addresses on the Zyxel Device's local networks (LAN and DMZ for example), the SSL user's network, or the networks you specify in the SSL VPN **Network List**.
DNS/WINS Server 1..2	Select the name of the DNS or WINS server whose information the Zyxel Device sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses.
Network List	To allow user access to local network(s), select a network name in the **Selectable Address Objects** list and click the right arrow button to add to the **Selected Address Objects** list. You can select more than one network. To block access to a network, select the network name in the **Selected Address Objects** list and click the left arrow button.
OK	Click **OK** to save the changes and return to the main **Access Privilege** screen.
Cancel	Click **Cancel** to discard all changes and return to the main **Access Privilege** screen.

21.3 The SSL Global Setting Screen

Click **VPN > SSL VPN** and click the **Global Setting** tab to display the following screen. Use this screen to set the IP address of the Zyxel Device (or a gateway device) on your network for full tunnel mode access.

Figure 306 VPN > SSL VPN > Global Setting



The following table describes the labels in this screen.

Table 170 VPN > SSL VPN > Global Setting

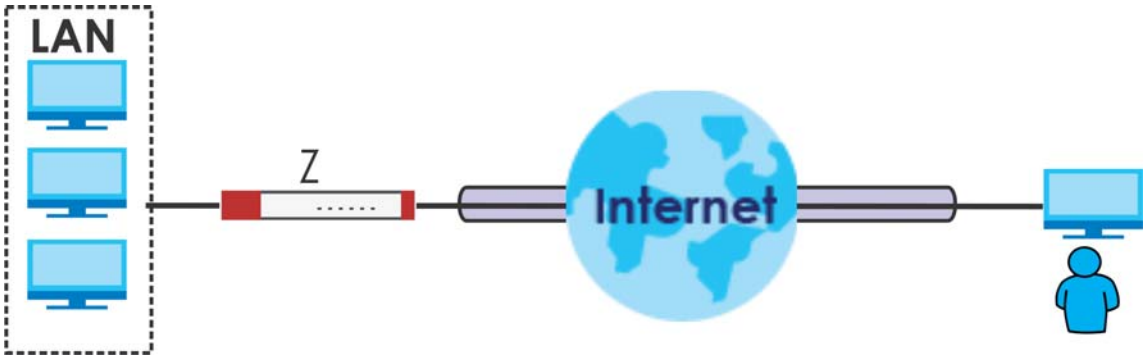
LABEL	DESCRIPTION
Global Setting	
Network Extension Local IP	Specify the IP address of the Zyxel Device (or a gateway device) for full tunnel mode SSL VPN access. Leave this field to the default settings unless it conflicts with another interface.
Apply	Click **Apply** to save the changes and/or start the logo file upload process.
Reset	Click **Reset** to return the screen to its last-saved settings.

CHAPTER 22
L2TP VPN

22.1 Overview

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, Windows or Mac OS X operating systems for secure connections to the network behind the Zyxel Device. The remote users do not need their own IPSec gateways or third-party VPN client software.

Figure 307 L2TP VPN Overview



If you install the IPSec VPN Client software from Zyxel to a Windows computer, enable Windows **IKE and AuthIP IPsec Keying Modules** to use L2TP over IPSec:

1 Click **Start** > **Control Panel** > **Administrative Tools** > **Services**

2 Select **IKE and AuthIP IPsec Keying Modules**, and click **Restart the service**.

22.1.1 What You Can Do in this Chapter

- Use the **L2TP VPN** screen (see Section 22.2 on page 439) to configure the Zyxel Device's L2TP VPN settings.
- Use the **VPN Setup Wizard** screen in **Quick Setup** (Chapter 4 on page 75) to configure the Zyxel Device's L2TP VPN settings.

22.1.2 What You Need to Know

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it. See Chapter 20 on page 396 for information on IPSec VPN.

IPSec Configuration Required for L2TP VPN

You must configure an IPSec VPN connection prior to proper L2TP VPN usage (see Chapter 22 on page 438 for details). The IPSec VPN connection must:

- Be enabled.
- Use transport mode.
- Use **Pre-Shared Key** authentication.
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

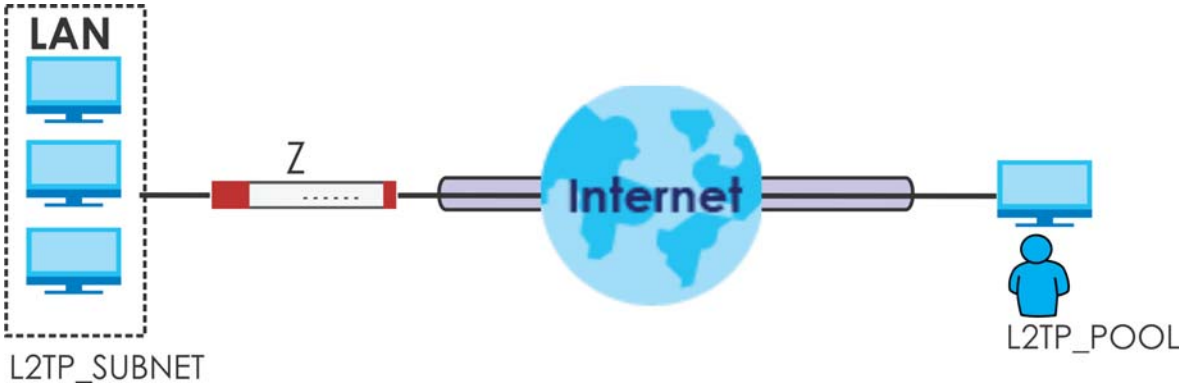
Using the Quick Setup VPN Setup Wizard

The **VPN Setup Wizard** is an easy and convenient way to configure the L2TP VPN settings. Click **Configuration** > **Quick Setup** > **VPN Setup** > **VPN Settings for L2TP VPN Settings** to get started.

Policy Route

The Policy Route for return traffic (from LAN to L2TP clients) is automatically created when Zyxel Device adds a new L2TP connection, allowing users access the resources on a network without additional configuration. However, if some of the traffic from the L2TP clients needs to go to the Internet, you will need to create a policy route to send that traffic from the L2TP tunnels out through a WAN trunk. This task can be easily performed by clicking the Allow L2TP traffic through WAN checkbox at **Quick Setup** > **VPN Setup** > **Allow L2TP traffic through WAN**.

Figure 308 Policy Route for L2TP VPN



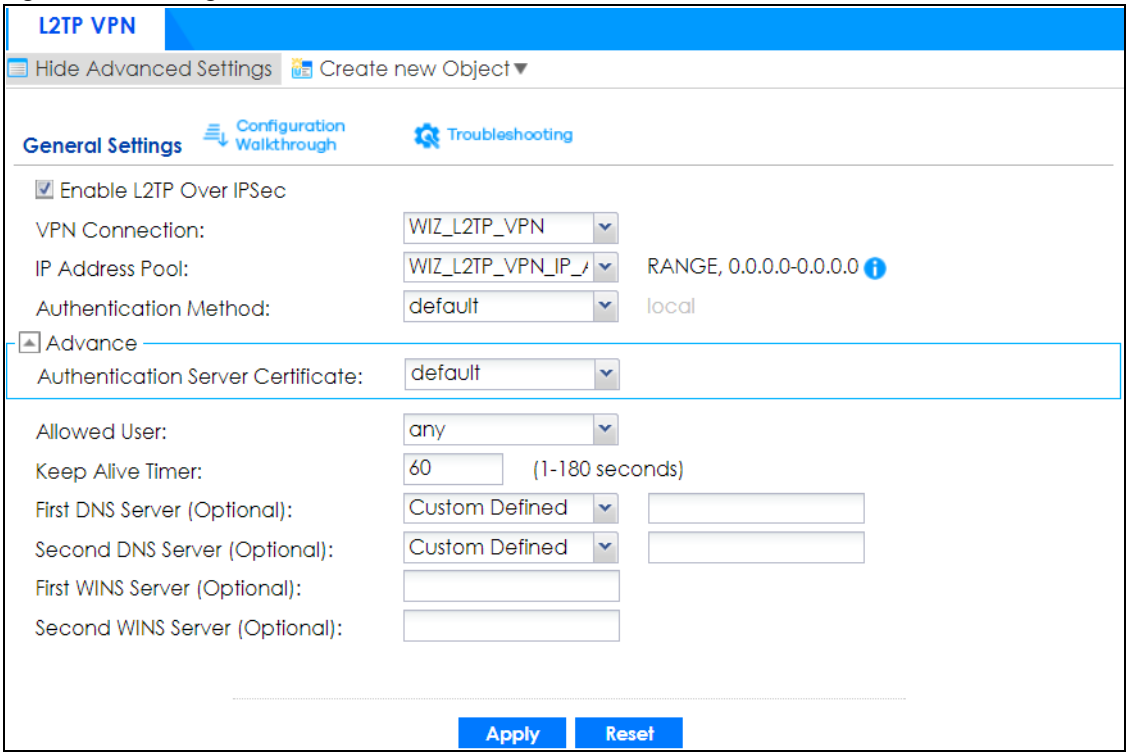
22.2 L2TP VPN Screen

Click **Configuration > VPN > L2TP VPN** to open the following screen. Use this screen to configure the Zyxel Device's L2TP VPN settings.

Note: Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

Click on the icons to go to the OneSecurity website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 309 Configuration > VPN > L2TP VPN



The following table describes the fields in this screen.

Table 171 Configuration > VPN > L2TP VPN

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable L2TP Over IPSec	Use this field to turn the Zyxel Device's L2TP VPN function on or off.
VPN Connection	Select the IPSec VPN connection the Zyxel Device uses for L2TP VPN. All of the configured VPN connections display here, but the one you use must meet the requirements listed in IPSec Configuration Required for L2TP VPN. Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
IP Address Pool	Select the pool of IP addresses that the Zyxel Device uses to assign to the L2TP VPN clients. Use **Create new Object** if you need to configure a new pool of IP addresses. This should not conflict with any WAN, LAN, DMZ or WLAN subnet even if they are not in use.
Authentication Method	Select how the Zyxel Device authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the Zyxel Device check a user's user name and password against the Zyxel Device's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these.

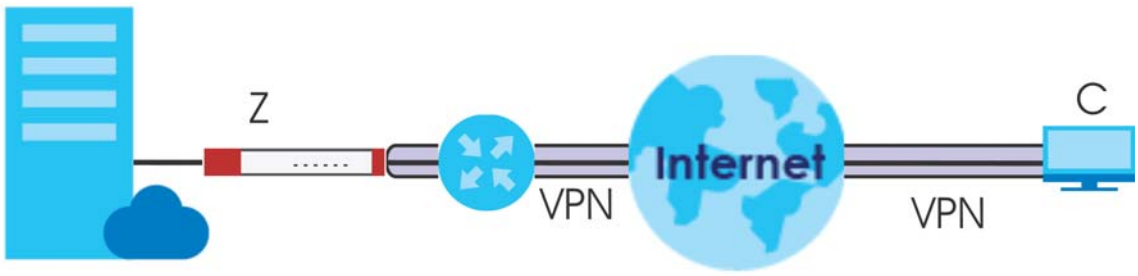
Table 171 Configuration > VPN > L2TP VPN (continued)

LABEL	DESCRIPTION
Authentication Server Certificate	Select the certificate to use to identify the Zyxel Device for L2TP VPN connections. You must have certificates already configured in the **My Certificates** screen. The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols.
Allowed User	The remote user must log into the Zyxel Device to use the L2TP VPN tunnel. Select a user or user group that can use the L2TP VPN tunnel. Use **Create new Object** if you need to configure a new user account. Otherwise, select **any** to allow any user with a valid account and password on the Zyxel Device to log in.
Keep Alive Timer	The Zyxel Device sends a Hello message after waiting this long without receiving any traffic from the remote user. The Zyxel Device disconnects the VPN tunnel if the remote user does not respond.
First DNS Server, Second DNS Server	Specify the IP addresses of DNS servers to assign to the remote users. You can specify these IP addresses two ways. **Custom Defined** - enter a static IP address. **From ISP** - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users. You can specify these IP addresses two ways.
Apply	Click **Apply** to save your changes in the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

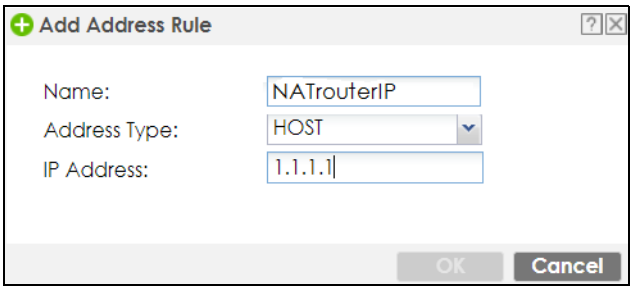
22.2.1 Example: L2TP and Zyxel Device Behind a NAT Router

If the Zyxel Device (Z) is behind a NAT router (N), then do the following for remote clients (C) to access the network behind the Zyxel Device (Z) using L2TP over IPv4.

Figure 310 L2TP and Zyxel Device Behind a NAT Router



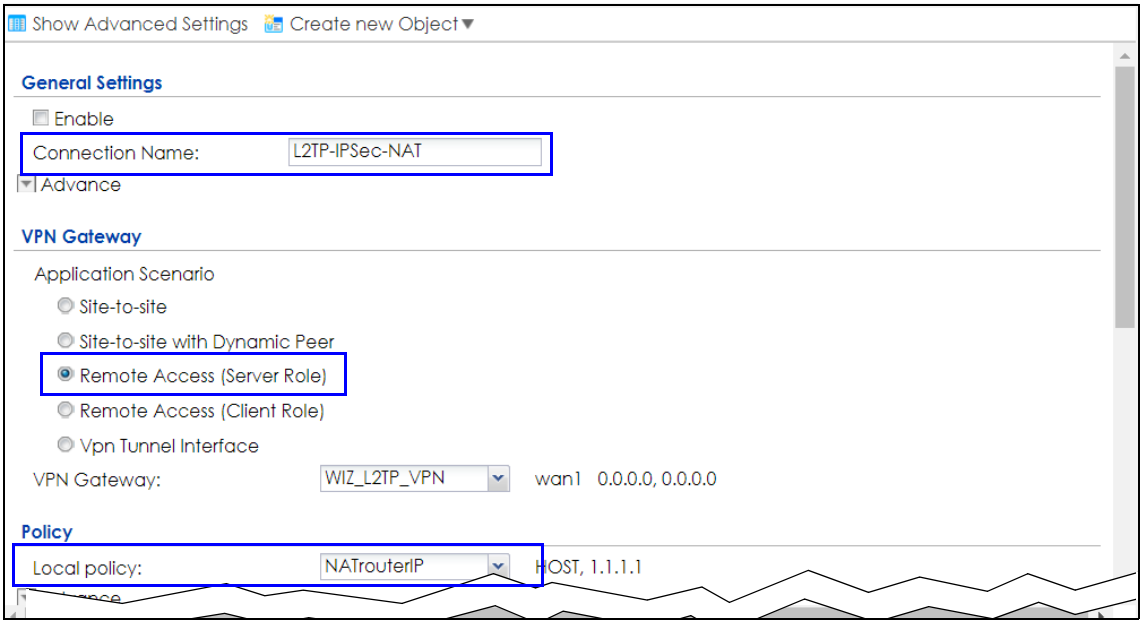
1 Create an address object in **Configuration > Object > Address/GEO IP > Address** for the WAN IP address of the NAT router.



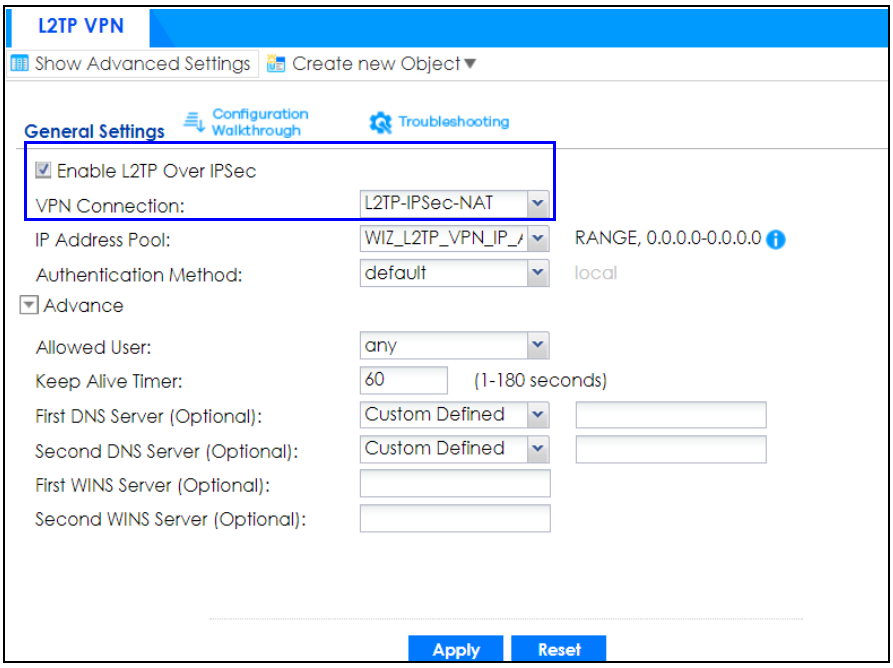
2 Go to **Configuration > VPN > IPSec VPN > VPN Connection** and click **Add** for **IPv4 Configuration** to create a new VPN connection.

3 Select **Remote Access (Server Role)** as the VPN scenario for the remote client.

4 Select the NAT router WAN IP address object as the **Local Policy**.



5 Go to **Configuration > VPN > L2TP VPN** and select the **VPN Connection** just configured.


L2TP VPN
Show Advanced Settings
Create new Object
General Settings
Configuration Walkthrough
Troubleshooting
Enable L2TP Over IPSec
VPN Connection:
L2TP-IPSec-NAT
IP Address Pool:
WIZ_L2TP_VPN_IP_
RANGE, 0.0.0.0-0.0.0.0
Authentication Method:
default
local
Advance
Allowed User:
any
Keep Alive Timer:
60
(1-180 seconds)
First DNS Server (Optional):
Custom Defined
Second DNS Server (Optional):
Custom Defined
First WINS Server (Optional):
Second WINS Server (Optional):
Apply
Reset

CHAPTER 23
BWM (Bandwidth Management)

23.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

23.1.1 What You Can Do in this Chapter

Use the **BWM** screens (see Section 23.2 on page 448) to control bandwidth for services passing through the Zyxel Device, and to identify the conditions that define the bandwidth control.

23.1.2 What You Need to Know

When you allow a service, you can restrict the bandwidth it uses. It controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over TCP and UDP traffic policies.

If you want to use a service, make sure both the security policy allow the service's packets to go through the Zyxel Device.

Note: The Zyxel Device checks security policies before it checks bandwidth management rules for traffic going through the Zyxel Device.

Bandwidth management examines every TCP and UDP connection passing through the Zyxel Device. Then, you can specify, by port, whether or not the Zyxel Device continues to route the connection.

BWM Type

The Zyxel Device supports three types of bandwidth management: **Shared**, **Per user** and **Per-Source-IP**.

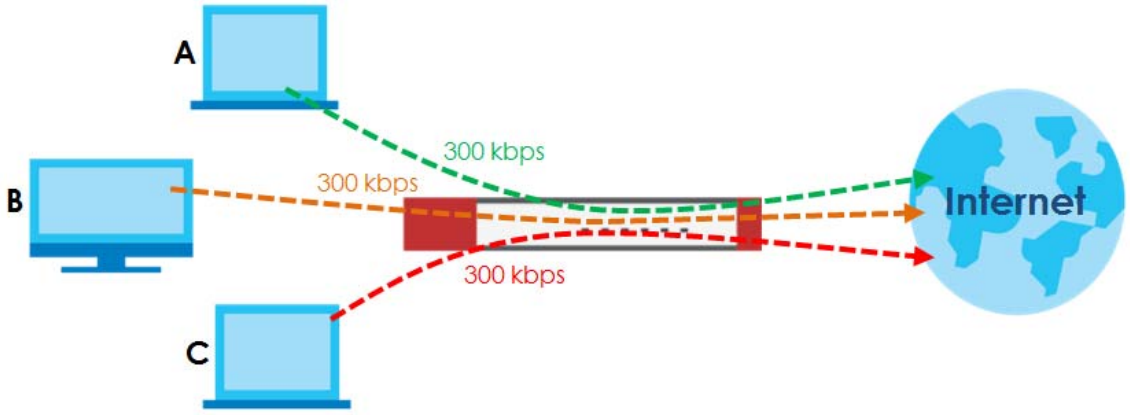
The **Shared** BWM type is selected by default in a bandwidth management rule. All matched traffic shares the bandwidth configured in the rule.

If the BWM type is set to **Per user** in a rule, each user that matches the rule can use up to the configured bandwidth by his/her own.

Select the **Per-Source-IP** type when you want to set the maximum bandwidth for traffic from an individual source IP address.

In the following example, you configure a **Per user** bandwidth management rule for radius-users to limit outgoing traffic to 300 kbs. Then all radius-users (**A**, **B** and **C**) can send 300 kbps of traffic.

Figure 311 Bandwidth Management Per User Type



DiffServ and DSCP Marking

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.

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.

Connection and Packet Directions

Bandwidth management looks at the connection direction, that is, from which interface the connection was initiated and to which interface the connection is going.

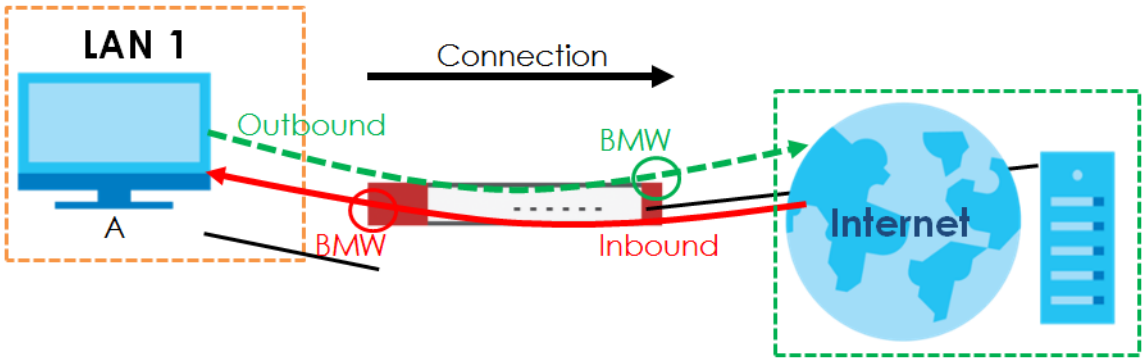
A connection has outbound and inbound packet flows. The Zyxel Device controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 device to a WAN device. Bandwidth management is applied before sending the packets out a WAN interface on the Zyxel Device.
- Inbound traffic comes back from the WAN device to the LAN1 device. Bandwidth management is applied before sending the traffic out a LAN1 interface.

Figure 312 LAN1 to WAN Connection and Packet Directions

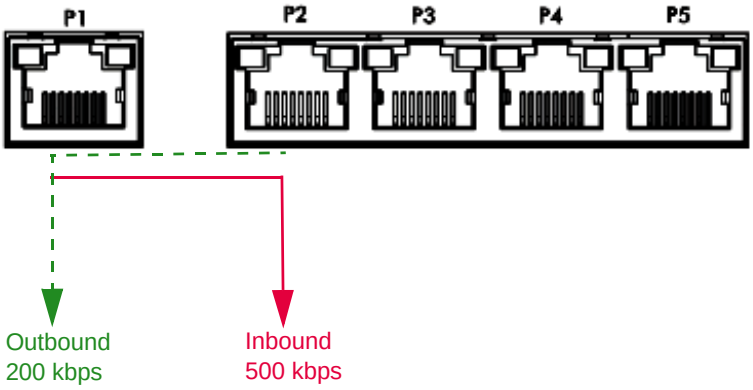


Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbs. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

Figure 313 LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps



Bandwidth Management Priority

- The Zyxel Device gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The Zyxel Device uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.
- The Zyxel Device automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to "borrow" any unused bandwidth on the out-going interface.

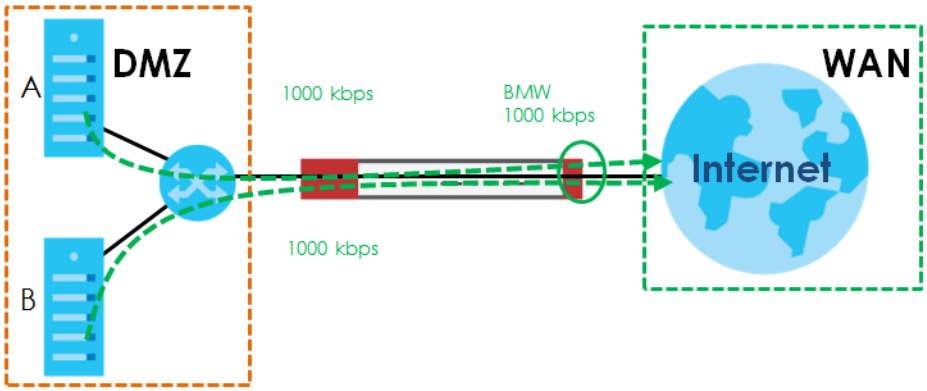
After each application gets its configured bandwidth rate, the Zyxel Device uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers **A** and **B**. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server **A**'s traffic and policy B for server **B**'s traffic.

Figure 314 Bandwidth Management Behavior



Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 172 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

Priority Effect

Here the configured rates total more than the available bandwidth. Because server **A** has higher priority, it gets up to it's configured rate (800 kbps), leaving only 200 kbps for server **B**.

Table 173 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server **A** gets its configured rate of 300 kbps and server **B** gets its configured rate of 200 kbps. Then the Zyxel Device divides the remaining bandwidth (1000 - 500 = 500) equally between the two (500 / 2 = 250 kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server **A** gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server **B** gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 174 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

Priority and Over Allotment of Bandwidth Effect

Server **A** has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the Zyxel Device still attempts to let all traffic get through and not be lost, regardless of its priority, server **B** gets almost no bandwidth with this configuration.

Table 175 Priority and Over Allotment of Bandwidth Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

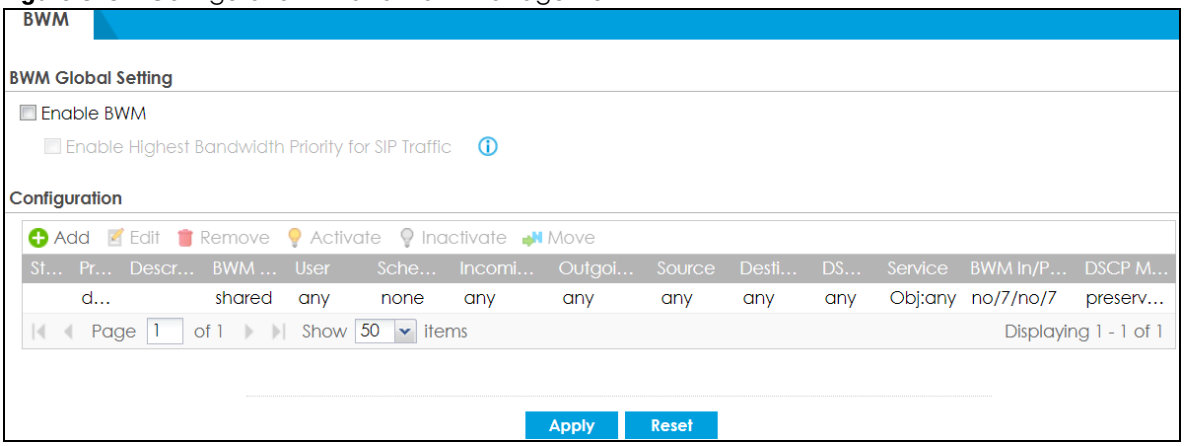
23.2 The Bandwidth Management Configuration

The Bandwidth management screens control the bandwidth allocation for TCP and UDP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify how the Zyxel Device handles the DSCP value and allocate bandwidth for the matching packets.

Click **Configuration > BWM** to open the following screen. This screen allows you to enable/disable bandwidth management and add, edit, and remove user-defined bandwidth management policies.

The default bandwidth management policy is the one with the priority of "default". It is the last policy the Zyxel Device checks if traffic does not match any other bandwidth management policies you have configured. You cannot remove, activate, deactivate or move the default bandwidth management policy.

Figure 315 Configuration > Bandwidth Management



The following table describes the labels in this screen. See Section 23.2.1 on page 451 for more information as well.

Table 176 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Enable BWM	Select this check box to activate management bandwidth.
Enable Highest Bandwidth Priority for SIP Traffic	Select this to maximize the throughput of SIP traffic to improve SIP-based VoIP call sound quality. This has the Zyxel Device immediately send SIP traffic upon identifying it. When this option is enabled the Zyxel Device ignores any other application patrol rules for SIP traffic (so there is no bandwidth control for SIP traffic) and does not record SIP traffic bandwidth usage statistics.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To change an entry's position in the numbered list, select it and click **Move** to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The status icon is not available for the default bandwidth management policy.
Priority	This field displays a sequential value for each bandwidth management policy and it is not associated with a specific setting. This field displays **default** for the default bandwidth management policy.
Description	This field displays additional information about this policy.
BWM Type	This field displays the below types of BWM: • **Shared**, when the policy is set for all matched traffic • **Per User**, when the policy is set for an individual user or a user group • **Per-Source-IP**, when the policy is set for a source IP

Table 176 Configuration > Bandwidth Management

LABEL	DESCRIPTION
User	This is the type of user account to which the policy applies. If **any** displays, the policy applies to all user accounts.
Schedule	This is the schedule that defines when the policy applies. **none** means the policy always applies.
Incoming Interface	This is the source interface of the traffic to which this policy applies.
Outgoing Interface	This is the destination interface of the traffic to which this policy applies.
Source	This is the source address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. If **any** displays, the policy is effective for every source.
Destination	This is the destination address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. If **any** displays, the policy is effective for every destination.
DSCP Code	These are the DSCP code point values of incoming and outgoing packets to which this policy applies. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. **any** means all DSCP value or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" options stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences.
Service	**App** and the service name displays if you selected **Application Object** for the service type. An **Application Object** is a pre-defined service. **Obj** and the service name displays if you selected **Service Object** for the service type. A **Service Object** is a customized pre-defined service or another service. Mouse over the service object name to view the corresponding IP protocol number.
BWM In/Pri/Out/Pri	This field shows the amount of bandwidth the traffic can use. **In** - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the inbound traffic. **Out** - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the Zyxel Device sends out from a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the outbound traffic. **Pri** - This is the priority for the incoming (the first **Pri** value) or outgoing (the second **Pri** value) traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The Zyxel Device ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.

Table 176 Configuration > Bandwidth Management

LABEL	DESCRIPTION
DSCP Marking	This is how the Zyxel Device handles the DSCP value of the incoming and outgoing packets that match this policy. **In** - Inbound, the traffic the Zyxel Device sends to a connection's initiator. **Out** - Outbound, the traffic the Zyxel Device sends out from a connection's initiator. If this field displays a DSCP value, the Zyxel Device applies that DSCP value to the route's outgoing packets. **preserve** means the Zyxel Device does not modify the DSCP value of the route's outgoing packets. **default** means the Zyxel Device sets the DSCP value of the route's outgoing packets to 0. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Reset	Click **Reset** to return the screen to its last-saved settings.

23.2.1 The Bandwidth Management Add/Edit Screen

The **Configuration > Bandwidth Management Add/Edit** screen allows you to create a new condition or edit an existing one.

802.1P Marking

Use 802.1P to prioritize outgoing traffic from a VLAN interface. The **Priority Code** is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest.

Table 177 Single Tagged 802.1Q Frame Format

			DA	SA	**TPID**	**Priority**	**VID**	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame

Table 178 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
TPID	Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

The following table is a guide to types of traffic for the priority code.

Table 179 Priority Code and Types of Traffic

PRIORITY	TRAFFIC TYPES
0 (lowest)	Background
1	Best Effort
2	Excellent Effort
3	Critical Applications
4	Video, less than 100 ms latency and jitter
5	Voice, less than 10 ms latency and jitter

Table 179 Priority Code and Types of Traffic

PRIORITY	TRAFFIC TYPES
6	Internetwork Control
7 (highest)	Network Control

To access this screen, go to the **Configuration > Bandwidth Management** screen (see Section 23.2 on page 448), and click either the **Add** icon or an **Edit** icon.

Figure 316 Configuration > Bandwidth Management > Edit (For the Default Policy)

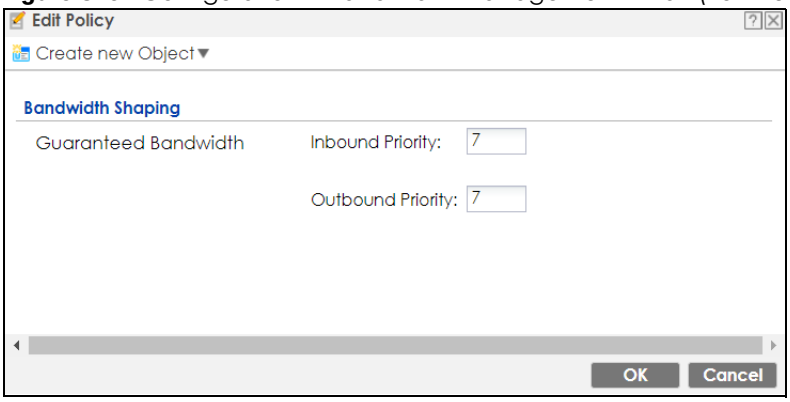
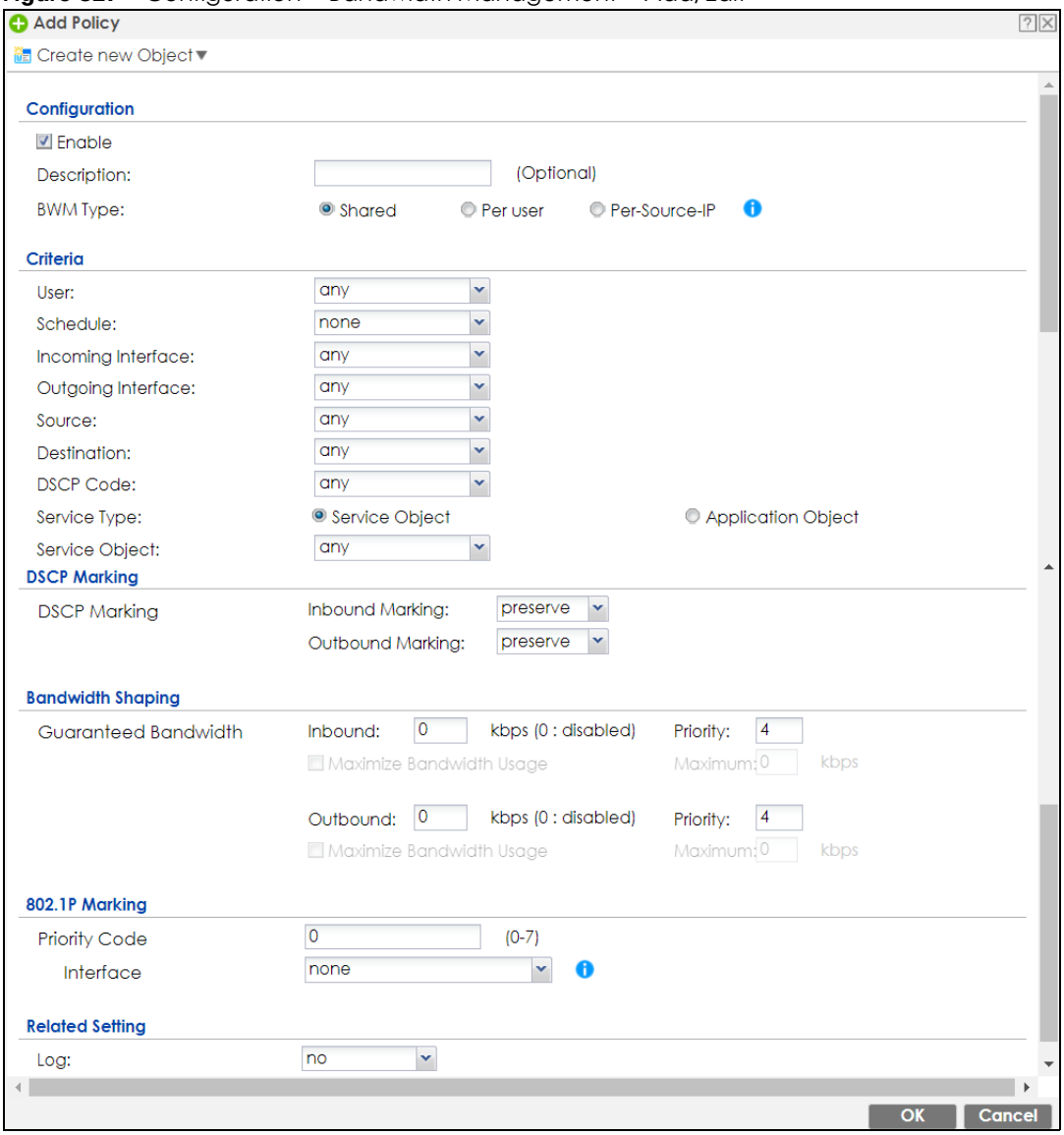


Figure 317 Configuration > Bandwidth Management > Add/Edit



The following table describes the labels in this screen.

Table 180 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this check box to turn on this policy.
Description	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Criteria	Use this section to configure the conditions of traffic to which this policy applies.
BWM Type	This field displays the below types of BWM rule: • Shared, when the policy is set for all users • Per User, when the policy is set for an individual user or a user group • Per Source IP, when the policy is set for a source IP

Table 180 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
User	Select a user name or user group to which to apply the policy. Use **Create new Object** if you need to configure a new user account. Select **any** to apply the policy for every user.
Schedule	Select a schedule that defines when the policy applies or select **Create Object** to configure a new one. Otherwise, select **none** to make the policy always effective.
Incoming Interface	Select the source interface of the traffic to which this policy applies.
Outgoing Interface	Select the destination interface of the traffic to which this policy applies.
Source	Select a source address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Use **Create new Object** if you need to configure a new one. Select **any** if the policy is effective for every source.
Destination	Select a destination address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Use **Create new Object** if you need to configure a new one. Select **any** if the policy is effective for every destination.
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select **User Defined** to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. **any** means all DSCP value or no DSCP marker. **default** means traffic with a DSCP value of 0. This is usually best effort traffic The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Service Type	Select **Service Object** or **Application Object** if you want a specific service (defined in a service object) or application patrol service to which the policy applies.
Service Object	This field is available if you selected **Service Object** as the service type. Select a service or service group to identify the type of traffic to which this policy applies. **any** means all services.
Application Object	This field is available if you selected **Application Object** as the service type. Select an application patrol service to identify the specific traffic to which this policy applies.
DSCP Marking	Set how the Zyxel Device handles the DSCP value of the incoming and outgoing packets that match this policy. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. Outbound refers to the traffic the Zyxel Device sends out from a connection's initiator. Select one of the pre-defined DSCP values to apply or select **User Defined** to specify another DSCP value. The "**af**" choices stand for Assured Forwarding. The number following the "**af**" identifies one of four classes and one of three drop preferences. Select **preserve** to have the Zyxel Device keep the packets' original DSCP value. Select **default** to have the Zyxel Device set the DSCP value of the packets to 0.
Bandwidth Shaping	Configure these fields to set the amount of bandwidth the matching traffic can use.

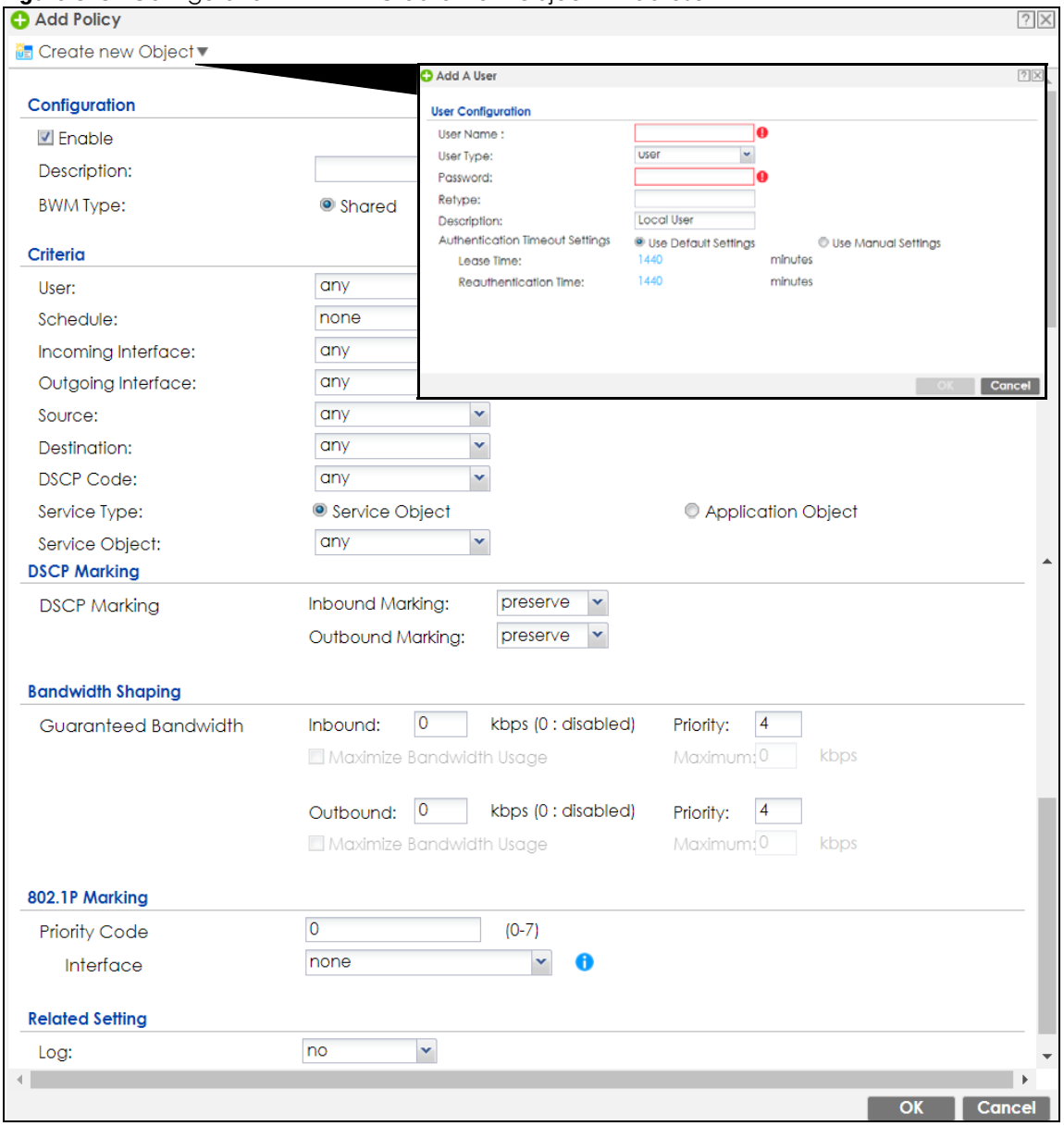
Table 180 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Inbound kbps	Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the Zyxel Device sends to a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the Zyxel Device sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Outbound kbps	Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the Zyxel Device sends out from a connection's initiator. If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the Zyxel Device sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7). If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.
Priority	This field displays when the inbound or outbound bandwidth management is not set to 0. Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The Zyxel Device uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority. The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.
Maximize Bandwidth Usage	This field displays when the inbound or outbound bandwidth management is not set to 0 and the **BWM Type** is set to **Shared**. Enable maximize bandwidth usage to let the traffic matching this policy "borrow" all unused bandwidth on the out-going interface. After each application or type of traffic gets its configured bandwidth rate, the Zyxel Device uses the fairness-based scheduler to divide any unused bandwidth on the out-going interface among applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.
Maximum	If you did not enable **Maximize Bandwidth Usage**, then type the maximum unused bandwidth that traffic matching this policy is allowed to "borrow" on the out-going interface (in Kbps), here.
802.1P Marking	Use 802.1P to prioritize outgoing traffic from a VLAN interface.
Priority Code	This is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest. See Table 179 on page 451. The setting configured here overwrites existing priority settings.
Interface	Choose a VLAN interface to which to apply the priority level for matching frames.
Related Setting	
Log	Select whether to have the Zyxel Device generate a log (**log**), log and alert (**log alert**) or neither (**no**) when any traffic matches this policy.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving your changes.

23.2.1.1 Adding Objects for the BWM Policy

Objects are parameters to which the Policy rules are built upon. There are three kinds of objects you can add/edit for the BWM policy, they are **User**, **Schedule** and **Address** objects. Click **Configuration** > **BWM** > **Add** > **Create New Object** > **Add User** to see the following screen.

Figure 318 Configuration >BWM > Create New Object > Add User



The following table describes the fields in the above screen.

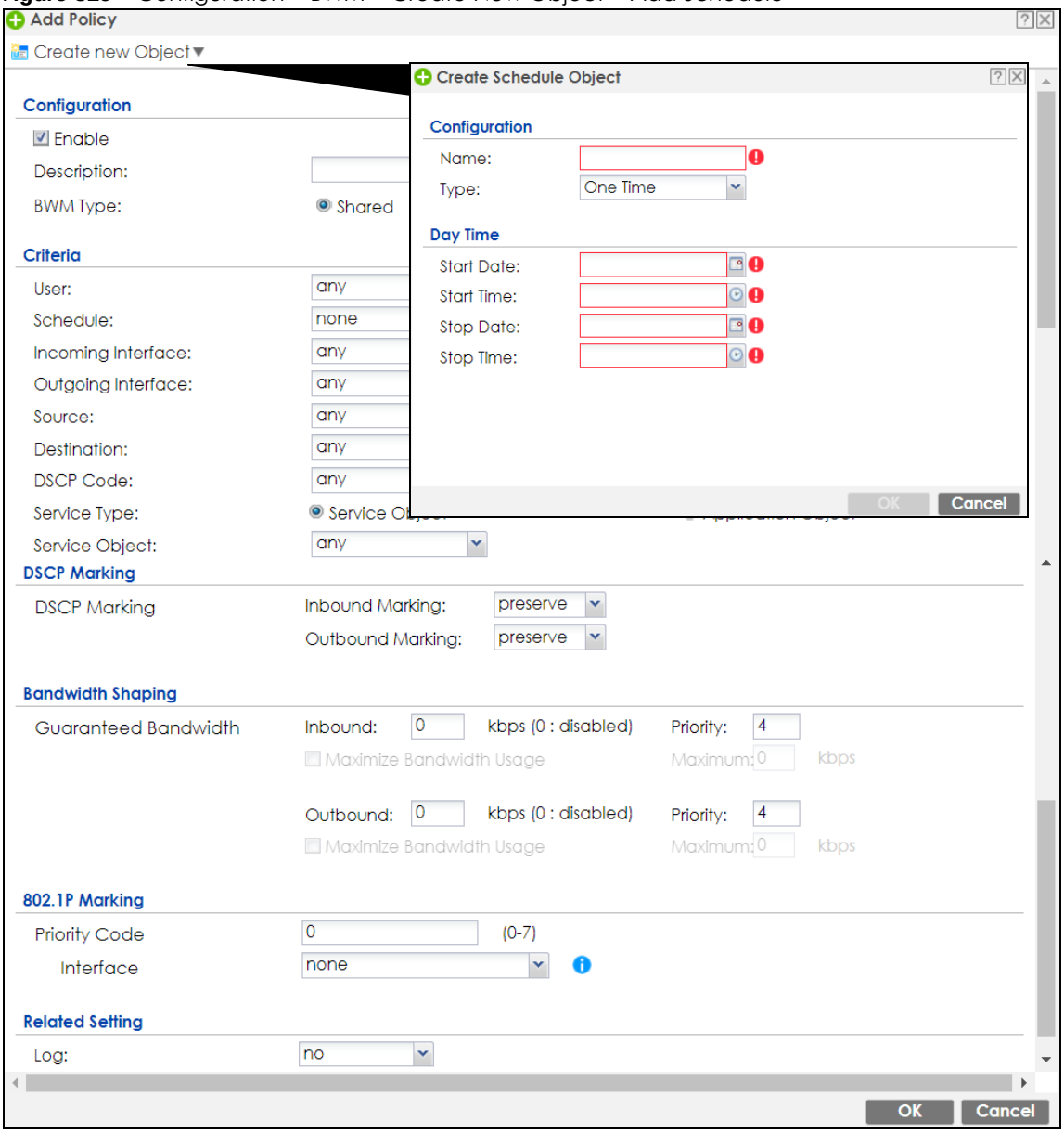
Table 181 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
User Name	Type a user or user group object name of the rule.
User Type	Select a user type from the drop down menu. The user types are Admin, Limited admin, User, Guest, Ext-user, Ext-group-user.

Table 181 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
Password	Type a password for the user object. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ ()), and it can be up to eight characters long.
Retype	Retype the password to confirm.
Description	Enter a description for this user object. It is not used elsewhere. You can use alphanumeric and `()+/:=?!*#@$_%-` characters, and it can be up to 60 characters long.
Authentication Timeout Settings	Choose either **Use Default** setting option, which shows the default Lease Time of 1,440 minutes and Reauthentication Time of 1,440 minutes or you can enter them manually by choosing Use Manual Settings option.
Lease Time	This shows the **Lease Time** setting for the user, by default it is 1,440 minutes.
Reauthentication Time	This shows the **Reauthentication Time** for the user, by default it is 1,440 minutes.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon this screen.

Figure 319 Configuration > BWM > Create New Object > Add Schedule

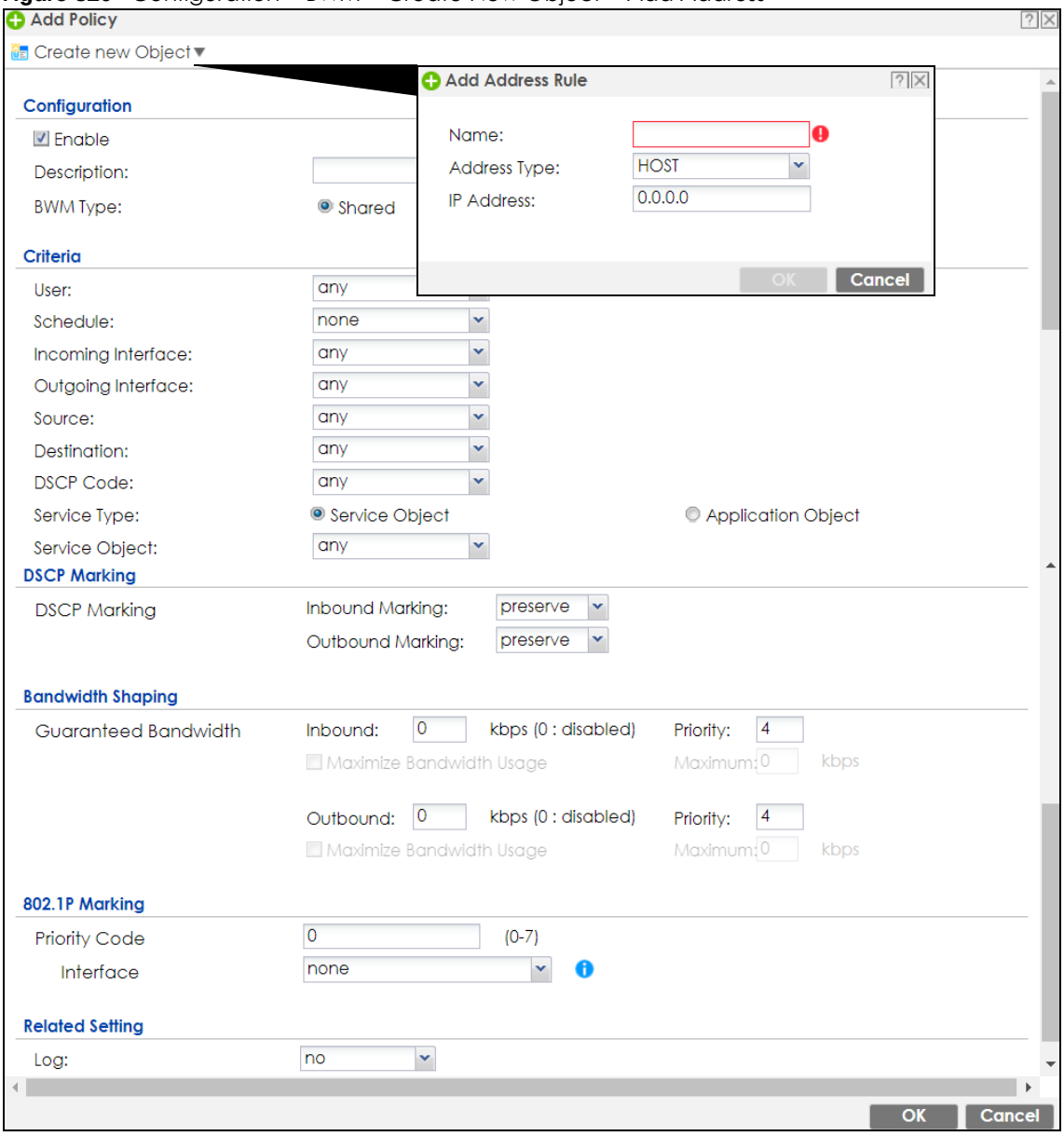


The following table describes the fields in the above screen.

Table 182 Configuration > BWM > Create New Object > Add Schedule

LABEL	DESCRIPTION
Name	Enter a name for the schedule object of the rule.
Type	Select an option from the drop down menu for the schedule object. It will show **One Time or Recurring.**
Start Date	Click the icon menu on the right to choose a Start Date for the schedule object.
Start Time	Click the icon menu on the right to choose a Start Time for the schedule object.
Stop Date	Click the icon menu on the right to choose a Stop Date for schedule object.
Stop Time	Click the icon menu on the right to choose a Stop Time for the schedule object.

Figure 320 Configuration > BWM > Create New Object > Add Address



The following table describes the fields in the above screen.

Table 183 Configuration > BWM > Create New Object > Add Address

LABEL	DESCRIPTION
Name	Enter a name for the Address object of the rule.
Address Type	Select an Address Type from the drop down menu on the right. The Address Types are Host, Range, Subnet, Interface IP, Interface Subnet, and Interface Gateway.
IP Address	Enter an IP address for the Address object.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon the setting.

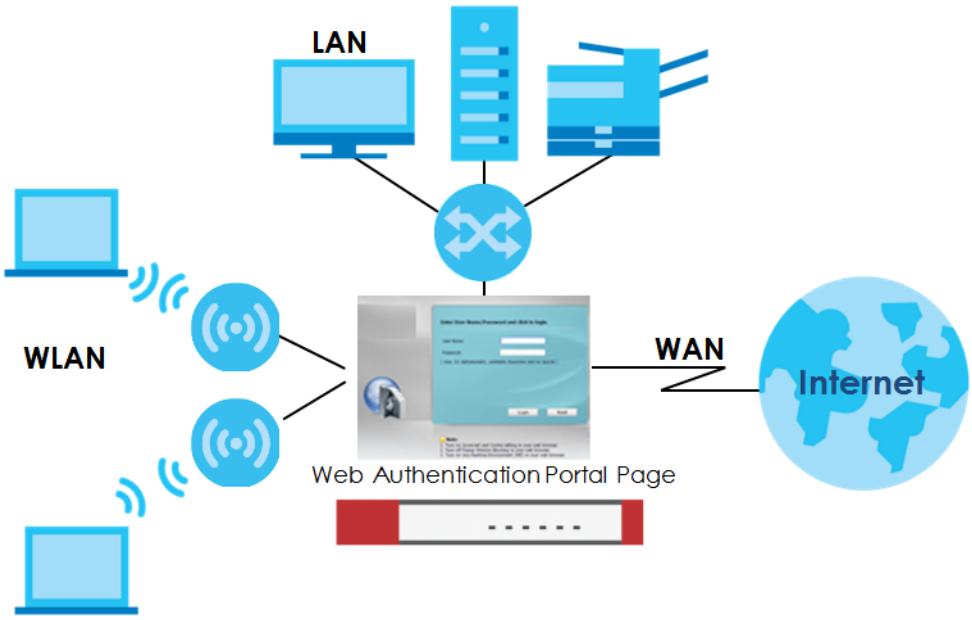
CHAPTER 24
Web Authentication

24.1 Web Auth Overview

Web authentication can intercept network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. This means all web page requests can initially be redirected to a special web page that requires users to authenticate their sessions. Once authentication is successful, they can then connect to the rest of the network or Internet.

As soon as a user attempt to open a web page, the Zyxel Device reroutes his/her browser to a web portal page that prompts him/her to log in.

Figure 321 Web Authentication Example



The web authentication page only appears once per authentication session. Unless a user session times out or he/she closes the connection, he or she generally will not see it again during the same session.

24.1.1 What You Can Do in this Chapter

- Use the **Configuration > Web Authentication** screens (Section 24.2 on page 461) to create and manage web authentication policies.
- Use the **Configuration > Web Authentication > SSO** screen (Section 24.3 on page 477) to configure how the Zyxel Device communicates with a Single Sign-On agent.

24.1.2 What You Need to Know

Single Sign-On

A SSO (Single Sign On) agent integrates Domain Controller and Zyxel Device authentication mechanisms, so that users just need to log in once (single) to get access to permitted resources.

Forced User Authentication

Instead of making users for which user-aware policies have been configured go to the Zyxel Device **Login** screen manually, you can configure the Zyxel Device to display the **Login** screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet.

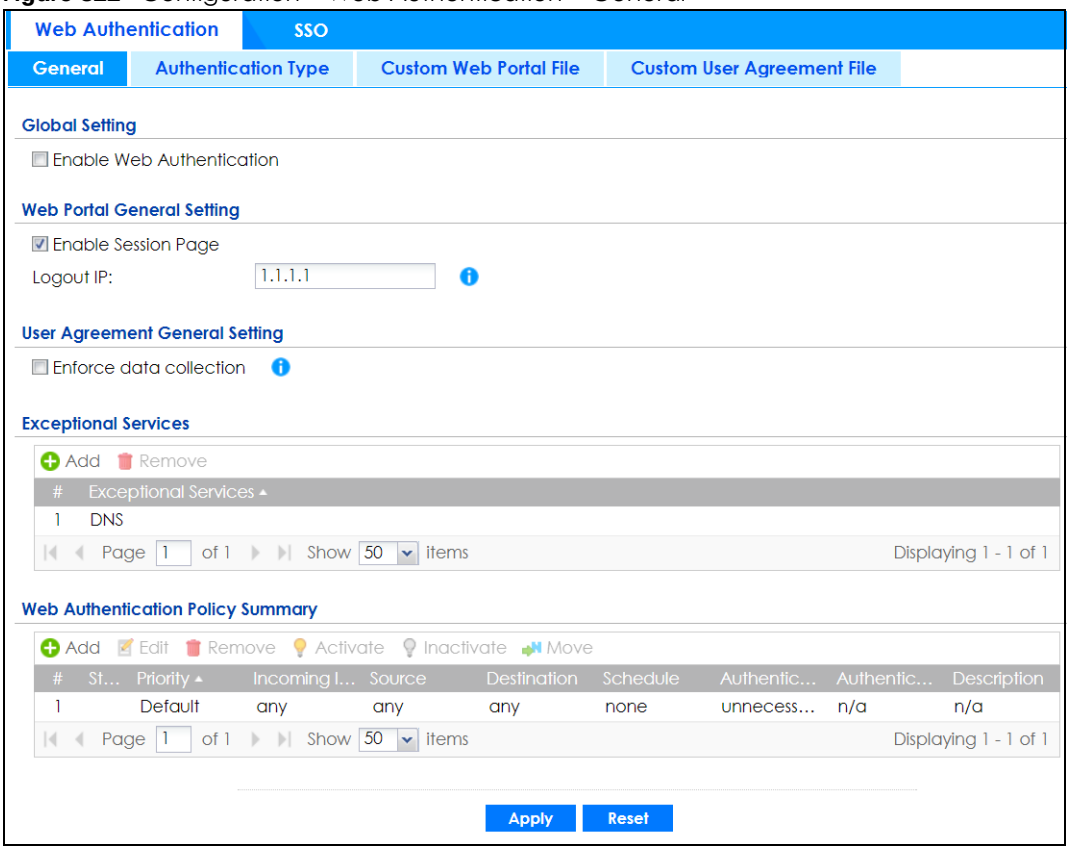
Note: This works with HTTP traffic only. The Zyxel Device does not display the **Login** screen when users attempt to send other kinds of traffic.

The Zyxel Device does not automatically route the request that prompted the login, however, so users have to make this request again.

24.2 Web Authentication General Screen

The **Web Authentication General** screen displays the general web portal settings and web authentication policies you have configured on the Zyxel Device. Use this screen to enable web authentication on the Zyxel Device.

Figure 322 Configuration > Web Authentication > General



The following table gives an overview of the objects you can configure.

Table 184 Configuration > Web Authentication > General

LABEL	DESCRIPTION
Global Setting	
Enable Web Authentication	Select the check box to turn on the web authentication feature. Otherwise, clear the check box to turn it off. Once enabled, all network traffic is blocked until a client authenticates with the Zyxel Device through the specifically designated web portal or user agreement page.
Web Portal General Setting	
Enable Session Page	Select this to display a page showing information on the user session after s/he logs in. It displays remaining time with an option to renew or log out immediately.
Logout IP	Specify an IP address that users can use to terminate their sessions manually by entering the IP address in the address bar of the web browser.
User Agreement General Setting	
Enforce data collection	Select this to require users to fill in their registration information (name, telephone number, address and email address) on the **User Agreement** (PC or mobile) page.

Table 184 Configuration > Web Authentication > General (continued)

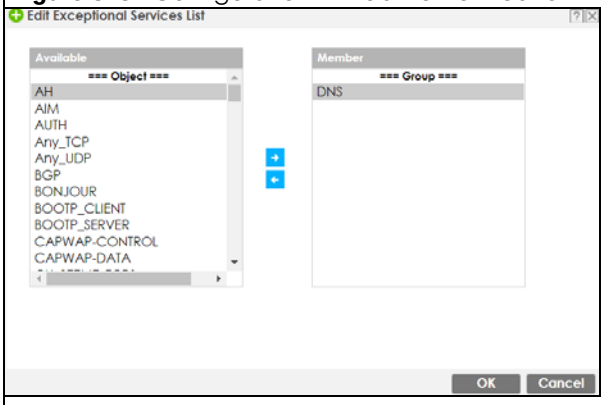
LABEL	DESCRIPTION
Exceptional Services	Use this table to list services that users can access without logging in. Click **Add** to change the list's membership. A screen appears. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button to add them. The member services are on the right. Select any service that you want to remove from the member list, and click the left arrow button to remove them. Keeping DNS as a member allows users' computers to resolve domain names into IP addresses. **Figure 323** Configuration > Web Authentication > Add Exceptional Service  In the table, select one or more entries and click **Remove** to delete it or them.
Web Authentication Policy Summary	Use this table to manage the Zyxel Device's list of web authentication policies.
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.
Activate	To turn on an entry, select it and click **Activate**.
Inactivate	To turn off an entry, select it and click **Inactivate**.
Move	To move an entry to a different number in the list, click the **Move** icon. In the field that appears, specify the number to which you want to move the interface.
#	This field is a sequential value showing the number of the profile. The profile order is not important.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Priority	This is the position of the authentication policy in the list. The priority is important as the policies are applied in order of priority. **Default** displays for the default authentication policy that the Zyxel Device uses on traffic that does not match any exceptional service or other authentication policy. You can edit the default rule but not delete it.
Incoming Interface	This field displays the interface on which packets for this policy are received.
Source	This displays the source address object, including geographic address and FQDN (group) objects, to which this policy applies.
Destination	This displays the destination address object, including geographic address and FQDN (group) objects, to which this policy applies.
Schedule	This field displays the schedule object that dictates when the policy applies. **none** means the policy is active at all times if enabled.

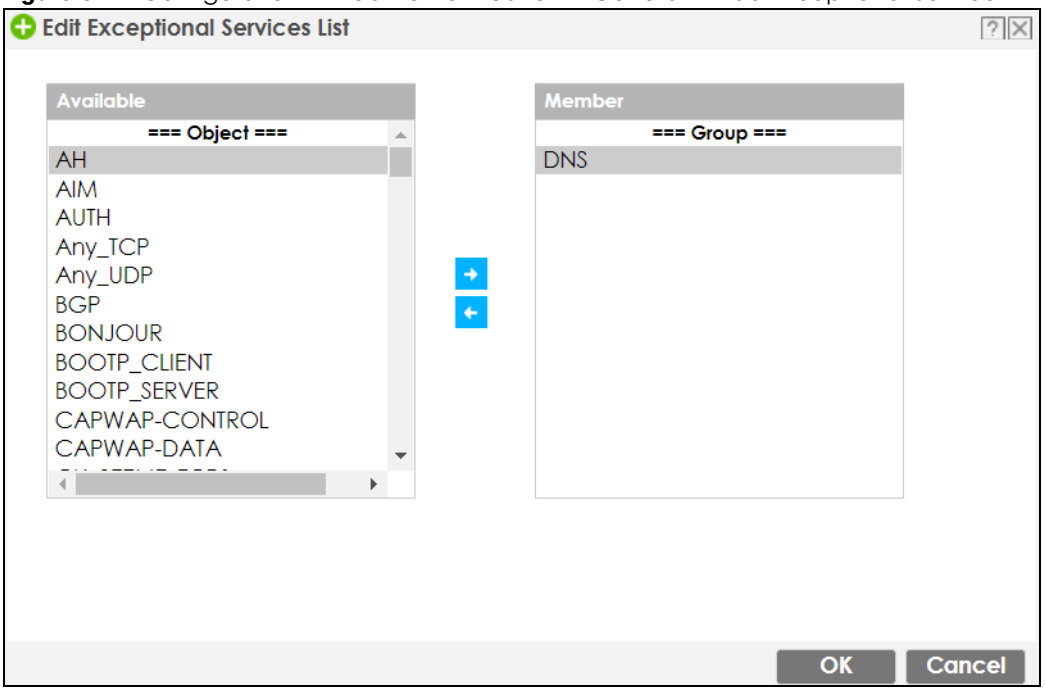
Table 184 Configuration > Web Authentication > General (continued)

LABEL	DESCRIPTION
Authentication	This field displays the authentication requirement for users when their traffic matches this policy. **unnecessary** - Users do not need to be authenticated. **required** - Users need to be authenticated. They must manually go to the login screen or user agreement page. The Zyxel Device will not redirect them to the login screen. **force** - Users need to be authenticated. The Zyxel Device automatically displays the login screen or user agreement page whenever it routes HTTP traffic for users who have not logged in yet.
Authentication Type	This field displays the name of the authentication type profile used in this policy to define how users authenticate their sessions. It shows **n/a** if **Authentication** is set to **unnecessary**.
Description	If the entry has a description configured, it displays here. This is **n/a** for the default policy.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings.

Creating Exceptional Services

This screen lists services that users can access without logging in. Click **Add** under **Exceptional Services** in the previous screen to display this screen. You can change the list's membership here. Available services appear on the left. Select any services you want users to be able to access without logging in and click the right arrow button **->** to add them. The member services are on the right. Select any service that you want to remove from the member list, and click the left arrow **<-** button to remove them. Then click **OK** to apply the changes and return to the main **Web Authentication** screen. Alternatively, click **Cancel** to discard the changes and return to the main **Web Authentication** screen.

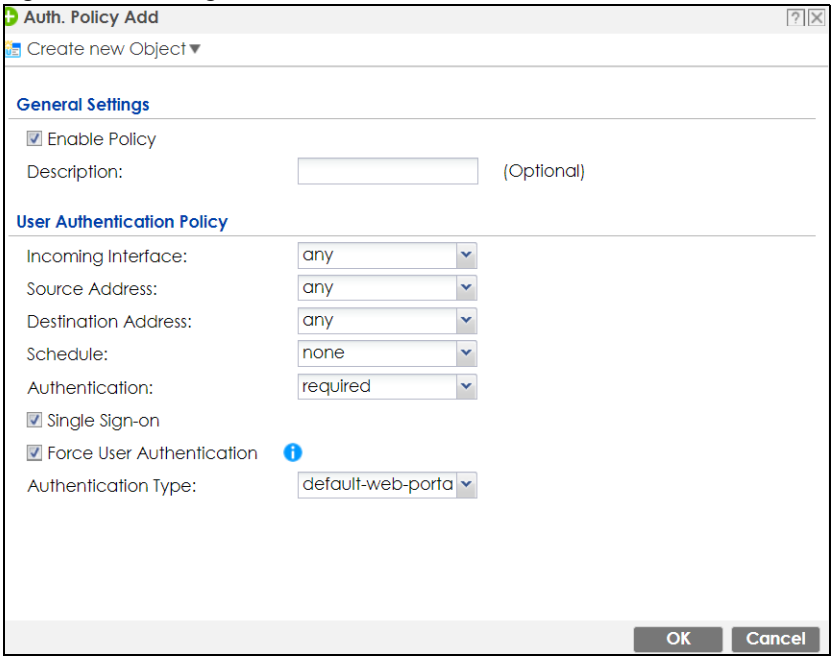
Figure 324 Configuration > Web Authentication > General > Add Exceptional Service



Creating/Editing an Authentication Policy

Open the **Configuration > Web Authentication > General** screen, then click the **Add** icon or select an entry and click the **Edit** icon in the **Web Authentication Policy Summary** section to open the **Auth. Policy Add/Edit** screen. Use this screen to configure an authentication policy.

Figure 325 Configuration > Web Authentication > General > Add Authentication Policy



The following table gives an overview of the objects you can configure.

Table 185 Configuration > Web Authentication > General > Add Authentication Policy

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen. Select Address or Schedule.
Enable Policy	Select this check box to activate the authentication policy. This field is available for user-configured policies.
Description	Enter a descriptive name of up to 60 printable ASCII characters for the policy. Spaces are allowed. This field is available for user-configured policies.
User Authentication Policy	Use this section of the screen to determine which traffic requires (or does not require) the senders to be authenticated in order to be routed.
Incoming Interface	Select the interface on which packets for this policy are received.
Source Address	Select a source address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Select **any** if the policy is effective for every source. This is **any** and not configurable for the default policy.
Destination Address	Select a destination address or address group, including geographic address and FQDN (group) objects, for whom this policy applies. Select **any** if the policy is effective for every destination. This is **any** and not configurable for the default policy.
Schedule	Select a schedule that defines when the policy applies. Otherwise, select **none** and the rule is always effective. This is **none** and not configurable for the default policy.

Table 185 Configuration > Web Authentication > General > Add Authentication Policy (continued)

LABEL	DESCRIPTION
Authentication	Select the authentication requirement for users when their traffic matches this policy. **unnecessary** - Users do not need to be authenticated. **required** - Users need to be authenticated. If **Force User Authentication** is selected, all HTTP traffic from unauthenticated users is redirected to a default or user-defined login page. Otherwise, they must manually go to the login screen. The Zyxel Device will not redirect them to the login screen.
Single Sign-on	This field is available for user-configured policies that require Single Sign-On (SSO). Select this to have the Zyxel Device enable the SSO feature. You can set up this feature in the SSO screen.
Force User Authentication	This field is available for user-configured policies that require authentication. Select this to have the Zyxel Device automatically display the login screen when users who have not logged in yet try to send HTTP traffic.
Authentication Type	Select an authentication method. **default-web-portal**: the default login page built into the Zyxel Device. **default-user-agreement**: the default user agreement page built into the Zyxel Device.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

24.2.1 User-aware Access Control Example

You can configure many policies and security settings for specific users or groups of users. Users can be authenticated locally by the Zyxel Device or by an external (RADIUS) authentication server.

In this example the users are authenticated by an external RADIUS server at 172.16.1.200. First, set up the user accounts and user groups in the Zyxel Device. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

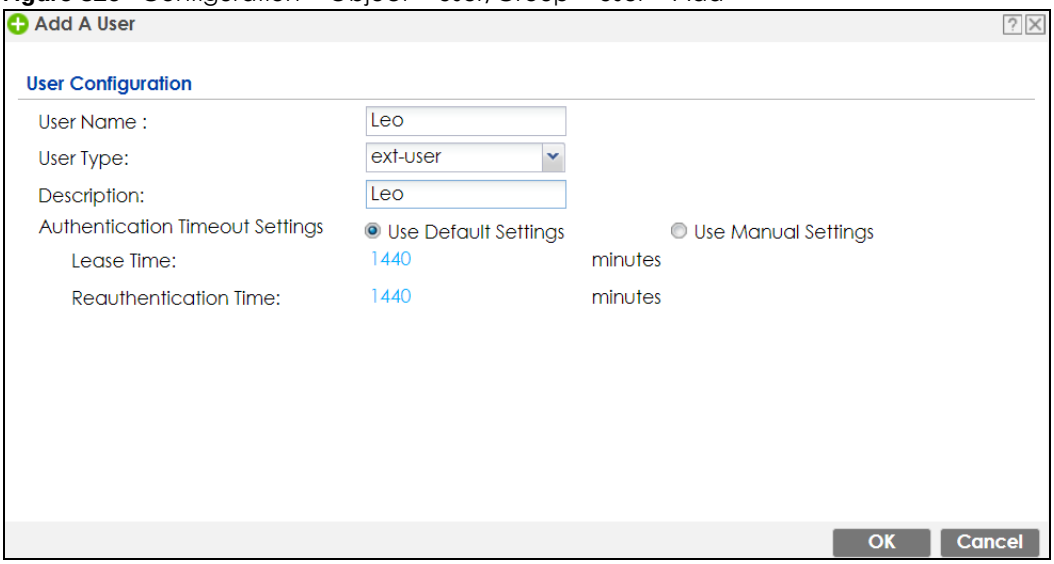
24.2.1.1 Set Up User Accounts

Set up user accounts in the RADIUS server. This example uses the Web Configurator. If you can export user names from the RADIUS server to a text file, then you might configure a script to create the user accounts instead.

1 Click **Configuration > Object > User/Group > User**. Click the **Add** icon.

2 Enter the same user name that is used in the RADIUS server, and set the **User Type** to **ext-user** because this user account is authenticated by an external server. Click **OK**.

Figure 326 Configuration > Object > User/Group > User > Add



3 Repeat this process to set up the remaining user accounts.

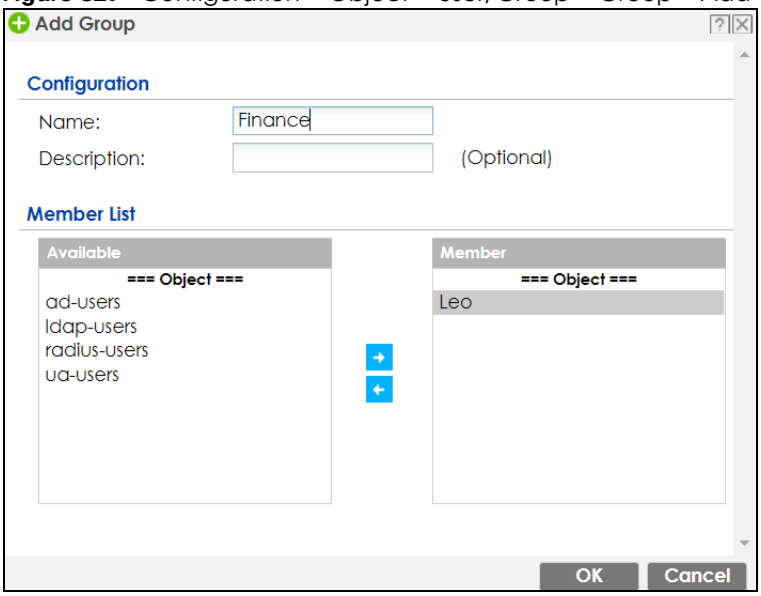
24.2.1.2 Set Up User Groups

Set up the user groups and assign the users to the user groups.

1 Click **Configuration > Object > User/Group > Group**. Click the **Add** icon.

2 Enter the name of the group. In this example, it is "Finance". Then, select **Object/Leo** and click the right arrow to move him to the **Member** list. This example only has one member in this group, so click **OK**. Of course you could add more members later.

Figure 327 Configuration > Object > User/Group > Group > Add



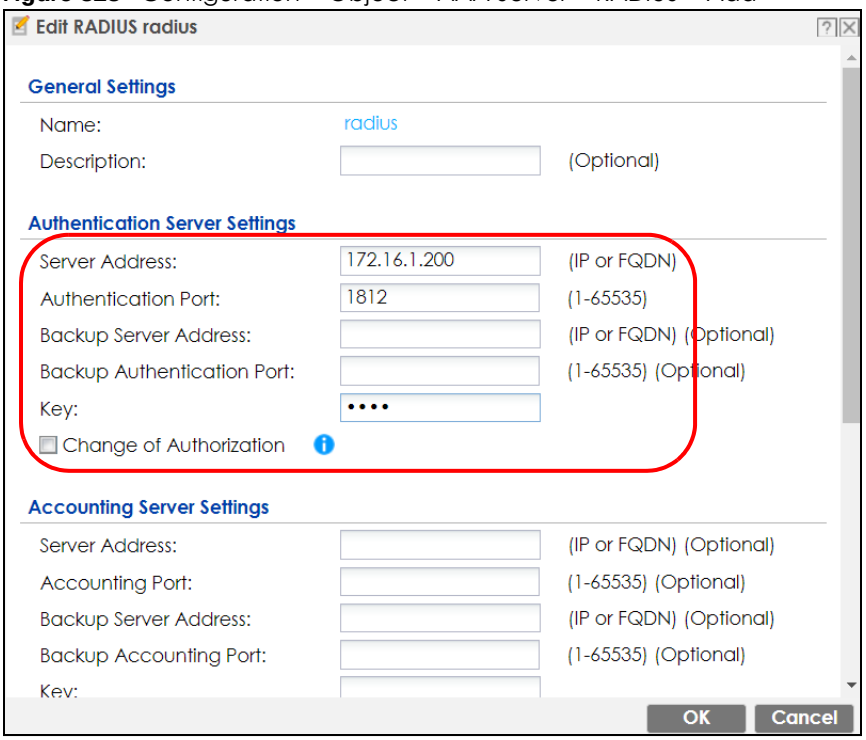
3 Repeat this process to set up the remaining user groups.

24.2.1.3 Set Up User Authentication Using the RADIUS Server

This step sets up user authentication using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the Zyxel Device to use the authentication method. Finally, force users to log into the Zyxel Device before it routes traffic for them.

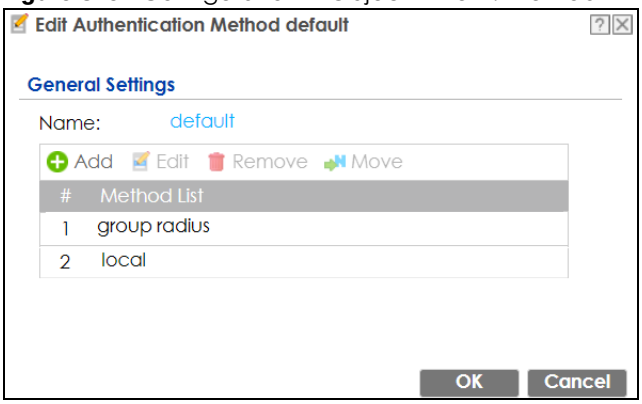
1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Configure the RADIUS server's address, authentication port (1812 if you were not told otherwise), and key. Click **OK**.

Figure 328 Configuration > Object > AAA Server > RADIUS > Add



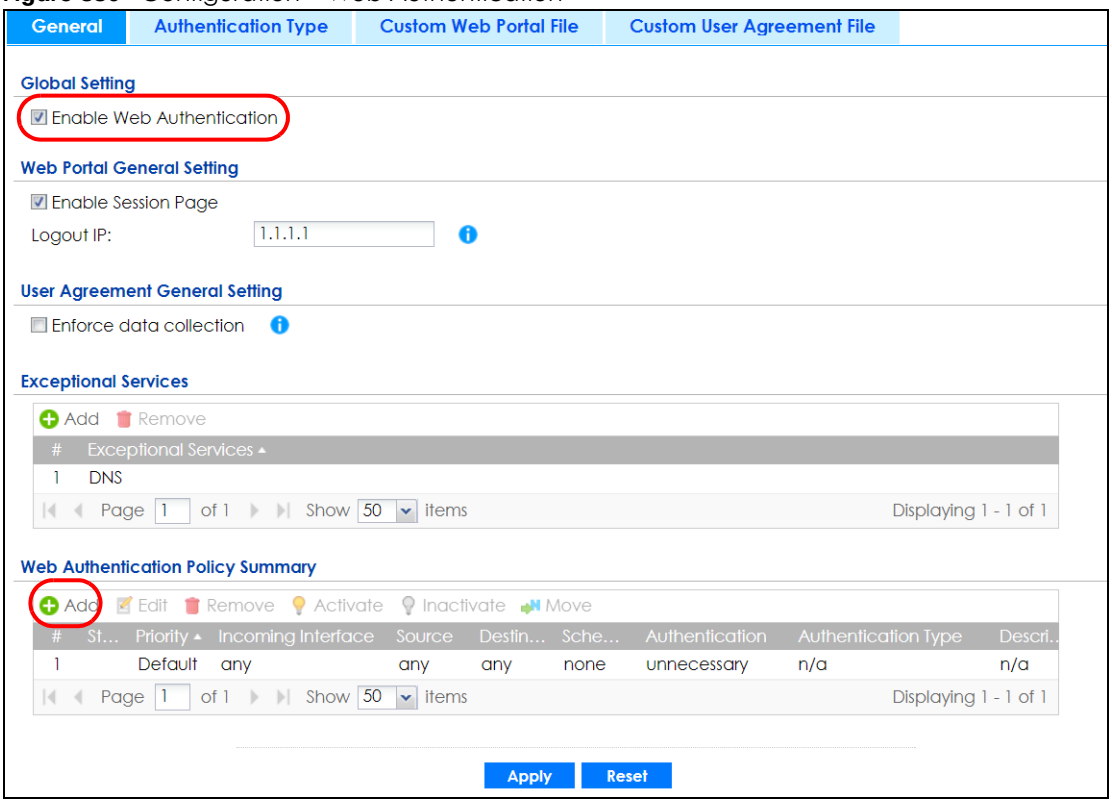
2 Click **Configuration > Object > Auth. Method**. Double-click the **default** entry. Click the **Add** icon. Select **group radius** because the Zyxel Device should use the specified RADIUS server for authentication. Click **OK**.

Figure 329 Configuration > Object > Auth. method > Edit



3 Click **Configuration > Web Authentication**. In the **Web Authentication > General** screen, select **Enable Web Authentication** to turn on the web authentication feature and click **Apply**.

Figure 330 Configuration > Web Authentication

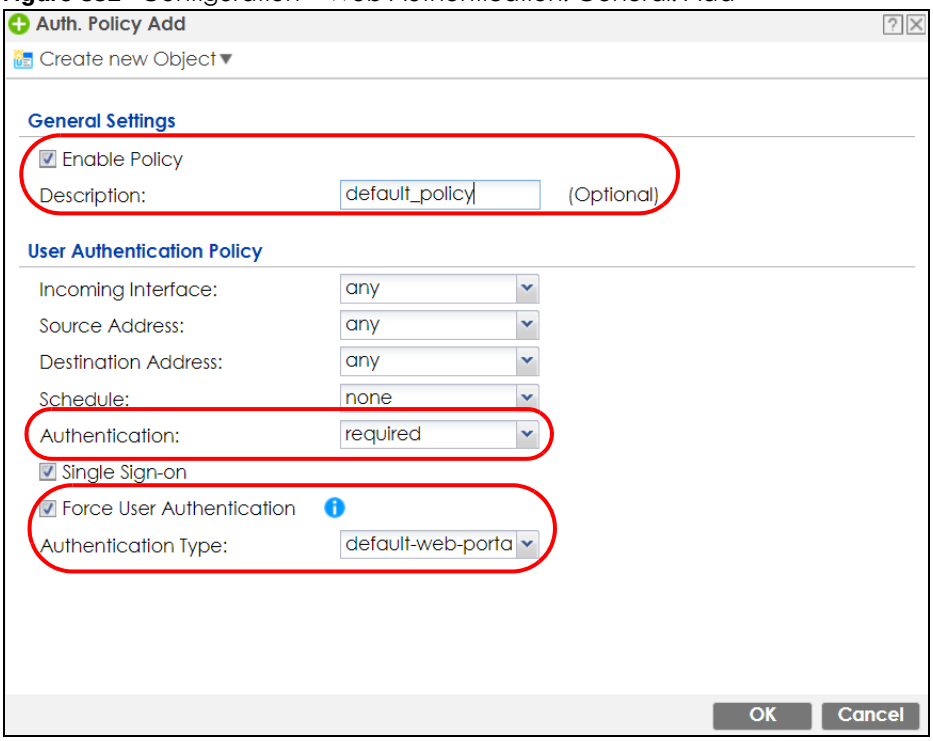


4 In the **Web Authentication Policy Summary** section, click the **Add** icon to set up a default policy that has priority over other policies and forces every user to log into the Zyxel Device before the Zyxel Device routes traffic for them.

5 Select **Enable Policy**. Enter a descriptive name, "default_policy" for example. Set the **Authentication** field to **required**, and make sure **Force User Authentication** is selected. Select an authentication type profile ("default-web-portal" in this example). Keep the rest of the default settings, and click **OK**.

Note: The users must log in at the Web Configurator login screen before they can use HTTP or MSN.

Figure 331 Configuration > Web Authentication: General: Add



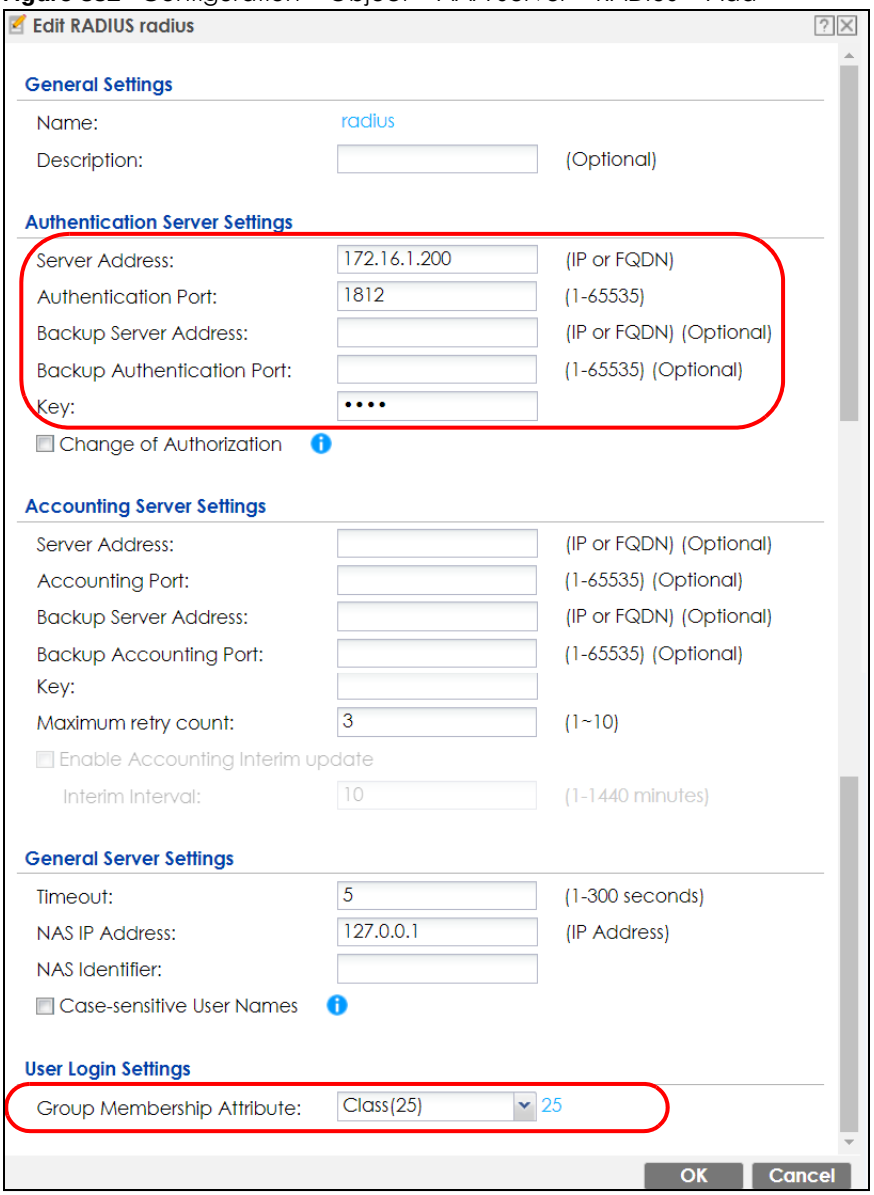
When the users try to browse the web (or use any HTTP application), the login screen appears. They have to log in using the user name and password in the RADIUS server.

24.2.1.4 User Group Authentication Using the RADIUS Server

The previous example showed how to have a RADIUS server authenticate individual user accounts. If the RADIUS server has different user groups distinguished by the value of a specific attribute, you can make a couple of slight changes in the configuration to have the RADIUS server authenticate groups of user accounts defined in the RADIUS server.

1 Click **Configuration > Object > AAA Server > RADIUS**. Double-click the **radius** entry. Besides configuring the RADIUS server's address, authentication port, and key; set the **Group Membership Attribute** field to the attribute that the Zyxel Device is to check to determine to which group a user belongs. This example uses **Class**. This attribute's value is called a group identifier; it determines to which group a user belongs. In this example the values are Finance, Engineer, Sales, and Boss.

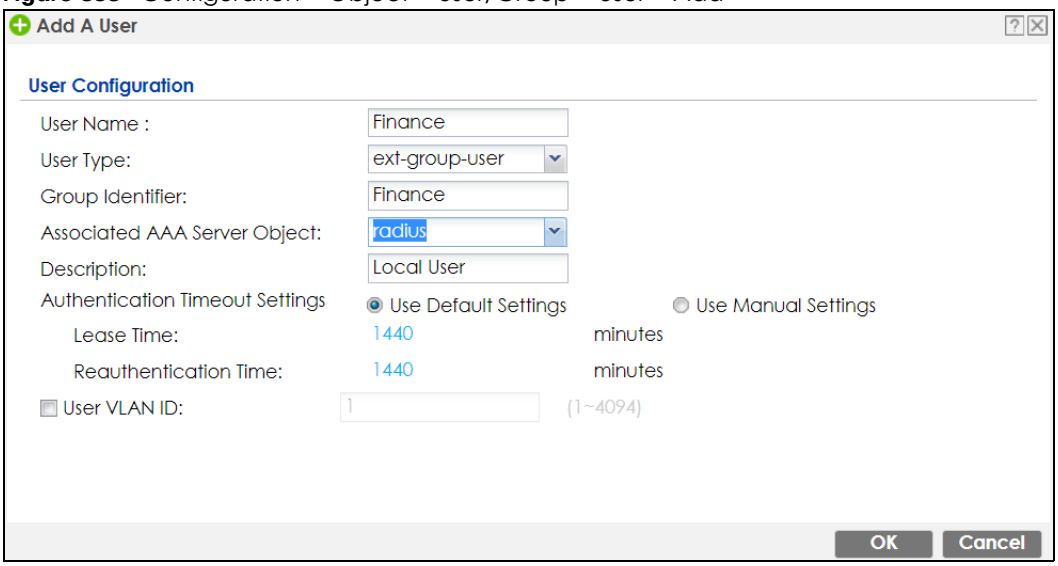
Figure 332 Configuration > Object > AAA Server > RADIUS > Add



2 Now you add ext-group-user objects to identify groups based on the group identifier values. Set up one user account for each group of user accounts in the RADIUS server. Click **Configuration > Object > User/ Group > User**. Click the **Add** icon.

Enter a user name and set the **User Type** to **ext-group-user**. In the **Group Identifier** field, enter Finance, Engineer, Sales, or Boss and set the **Associated AAA Server Object** to **radius**.

Figure 333 Configuration > Object > User/Group > User > Add

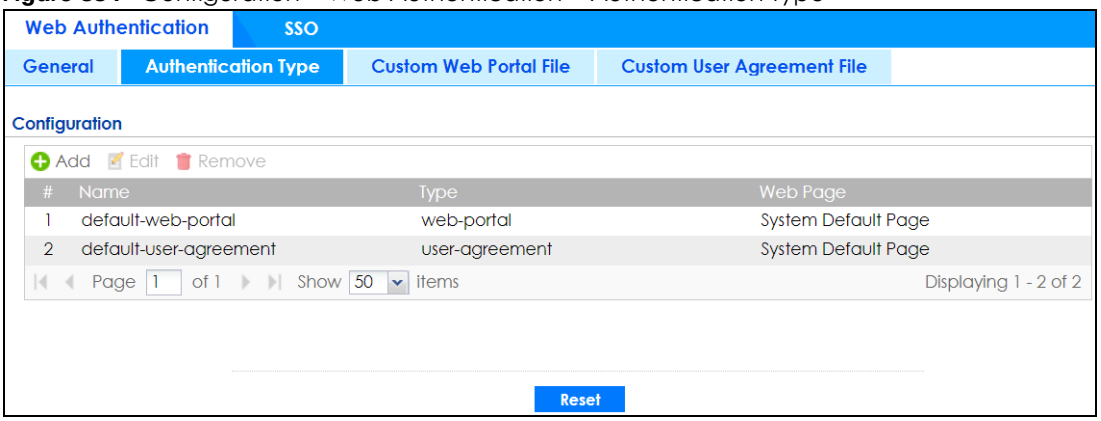


3 Repeat this process to set up the remaining groups of user accounts.

24.2.2 Authentication Type Screen

Use this screen to view, create and manage the authentication type profiles on the Zyxel Device. An authentication type profile decides which type of web authentication pages to be used for user authentication. Go to **Configuration > Web Authentication** and then select the **Authentication Type** tab to display the screen.

Figure 334 Configuration > Web Authentication > Authentication Type



The following table describes the labels in this screen.

Table 186 Configuration > Web Authentication > Authentication Type

LABEL	DESCRIPTION
Add	Click this to create a new entry. Select an entry and click **Add** to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click **Edit** to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click **Remove**. The Zyxel Device confirms you want to remove it before doing so.

Table 186 Configuration > Web Authentication > Authentication Type (continued)

LABEL	DESCRIPTION
#	This field is a sequential value, and it is not associated with a specific entry.
Name	This field displays the name of the profile. default-web-portal: the default login page built into the Zyxel Device. Note: You can also customize the default login page built into the Zyxel Device in the **System > WWW > Login Page** screen. default-user-agreement: the default user agreement page built into the Zyxel Device.
Type	This field displays the type of the web authentication page used by this profile.
Web Page	This field displays whether this profile uses the default web authentication page built into the Zyxel Device (**System Default Page**) or custom web authentication pages from an external web server (**External Page**).
Reset	Click **Reset** to return the screen to its last-saved settings.

Add/Edit an Authentication Type Profile

Click the **Add** icon or select an entry in the **Web Authentication > Authentication Type** screen and click the **Edit** icon to display the screen. The screen differs depending on what you select in the **Type** field.

Figure 335 Configuration > Web Authentication > Authentication Type: Add/Edit (Web Portal)

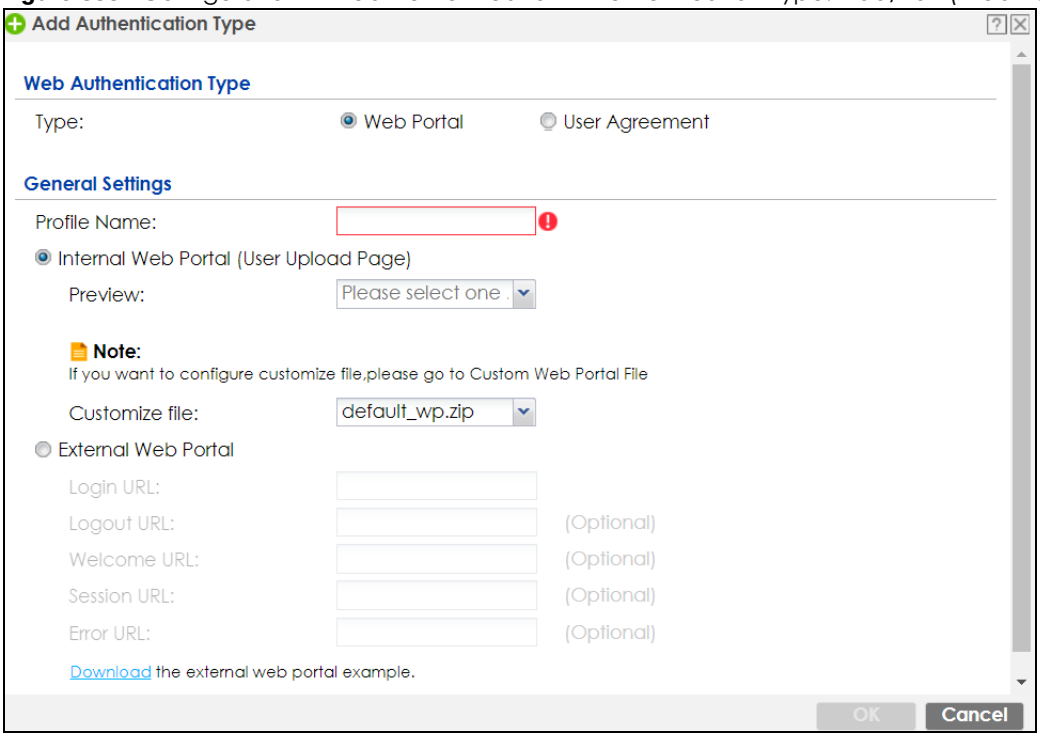
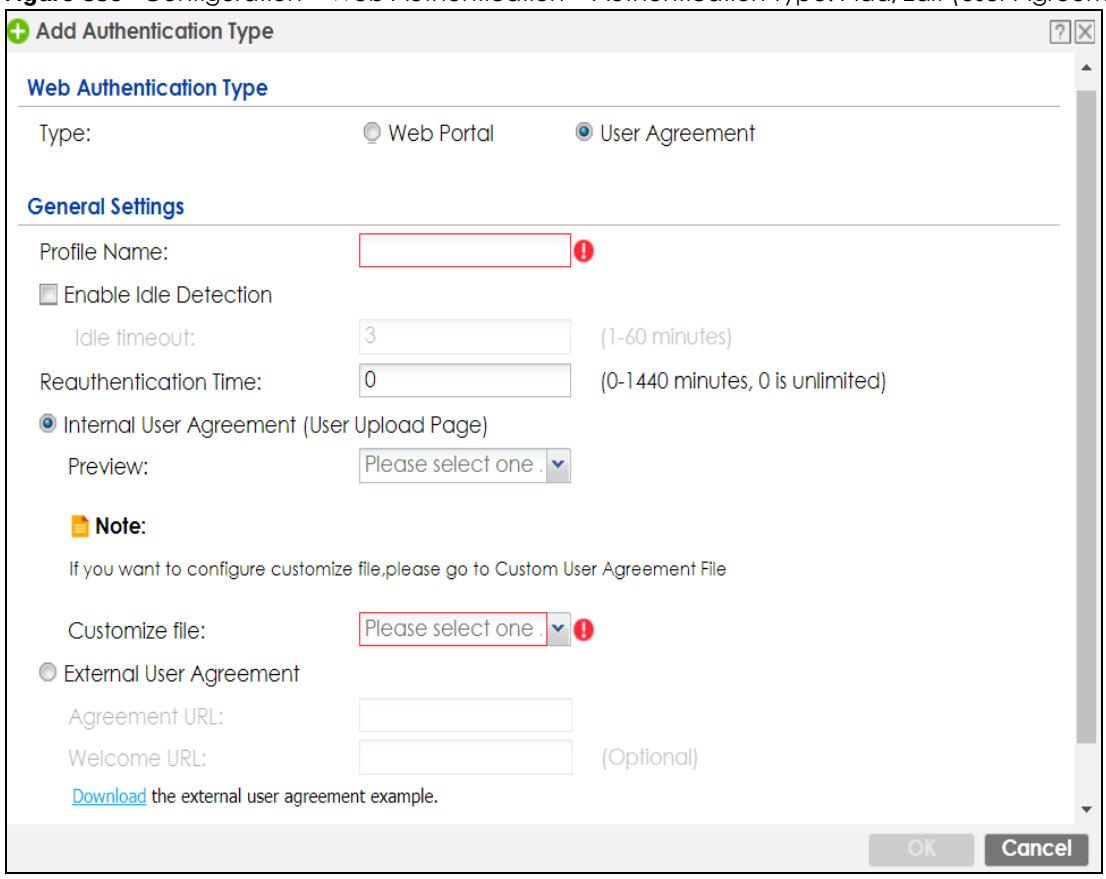


Figure 336 Configuration > Web Authentication > Authentication Type: Add/Edit (User Agreement)



The following table describes the labels in this screen.

Table 187 Configuration > Web Authentication > Authentication Type: Add/Edit

LABEL	DESCRIPTION
Type	Select the type of the web authentication page through which users authenticate their connections. If you select **User Agreement**, by agreeing to the policy of user agreement, users can access the Internet without a guest account.
Profile Name	Enter a name for the profile. You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
The following fields are available if you set **Type** to **Web Portal**.	
Internal Web Portal	Select this to use the web portal pages uploaded to the Zyxel Device. The login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network.
Preview	Select to display the page you uploaded to the Zyxel Device in a new frame. Note: You must select a custom file uploaded to the Zyxel Device before you can preview the pages.
Customize file	Select the file name of the web portal file in the Zyxel Device. Note: You can upload zipped custom web portal files to the Zyxel Device using the **Configuration > Web Authentication > Web Portal Customize File** screen.

Table 187 Configuration > Web Authentication > Authentication Type: Add/Edit (continued)

LABEL	DESCRIPTION
External Web Portal	Select this to use a custom login page from an external web portal instead of the one uploaded to the Zyxel Device. You can configure the look and feel of the web portal page.
Login URL	Specify the login page's URL; for example, http://IIS server IP Address/login.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Logout URL	Specify the logout page's URL; for example, http://IIS server IP Address/logout.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Welcome URL	Specify the welcome page's URL; for example, http://IIS server IP Address/welcome.html. Users will be redirected to the welcome page after authentication. This field is optional. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Session URL	Specify the session page's URL; for example, http://IIS server IP Address/session.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Error URL	Specify the error page's URL; for example, http://IIS server IP Address/error.html. The Internet Information Server (IIS) is the web server on which the web portal files are installed.
Download	Click this to download an example external web portal file for your reference.
The following fields are available if you set **Type** to **User Agreement**.	
Enable Idle Detection	This is applicable for access users. Select this check box if you want the Zyxel Device to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The Zyxel Device automatically logs out the access user once the **Idle timeout** has been reached.
Idle timeout	This is applicable for access users. This field is effective when **Enable Idle Detection** is checked. Type the number of minutes each access user can be logged in and idle before the Zyxel Device automatically logs out the access user.
Reauthentication Time	Enter the number of minutes the user can be logged into the Zyxel Device in one session before having to log in again.
Internal User Agreement	Select this to use the user agreement pages in the Zyxel Device. The user agreement page appears whenever the Zyxel Device intercepts network traffic, preventing unauthorized users from gaining access to the network.
Preview	Select to display the page you uploaded to the Zyxel Device in a new frame. Note: You must select a custom file uploaded to the Zyxel Device before you can preview the pages.
Customize file	Select the file name of the user agreement file in the Zyxel Device. Note: You can upload zipped custom user agreement files to the Zyxel Device using the **Configuration > Web Authentication > User Agreement Customize File** screen.
External User Agreement	Select this to use custom user agreement pages from an external web server instead of the default one built into the Zyxel Device. You can configure the look and feel of the user agreement page.
Agreement URL	Specify the user agreement page's URL; for example, http://IIS server IP Address/logout.html. The Internet Information Server (IIS) is the web server on which the user agreement files are installed.

Table 187 Configuration > Web Authentication > Authentication Type: Add/Edit (continued)

LABEL	DESCRIPTION
Welcome URL	Specify the welcome page's URL; for example, http://IIS server IP Address/welcome.html. The Internet Information Server (IIS) is the web server on which the user agreement files are installed. If you leave this field blank, the Zyxel Device will use the welcome page of internal user agreement file.
Download	Click this to download an example external user agreement file for your reference.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to exit this screen without saving.

24.2.3 Custom Web Portal / User Agreement File Screen

Use this screen to upload the zipped custom web portal or user agreement files to the Zyxel Device. You can also download the custom files to your computer.

Click **Configuration > Web Authentication** and then select the **Custom Web Portal File** or **Custom User Agreement File** tab to display the screen.

Figure 337 Configuration > Web Authentication > Custom Web Portal File

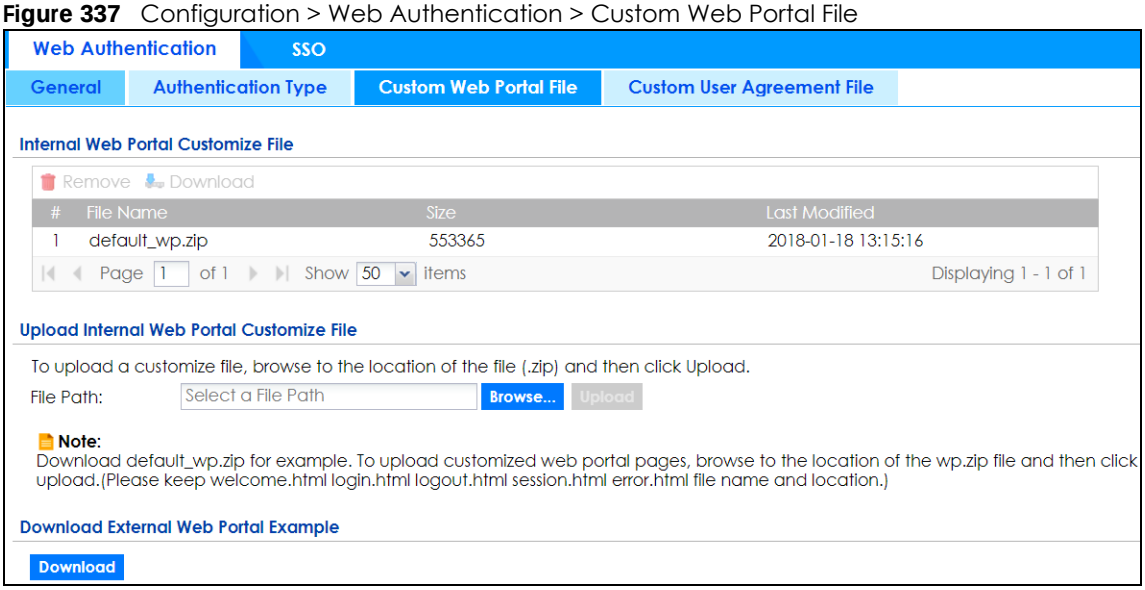
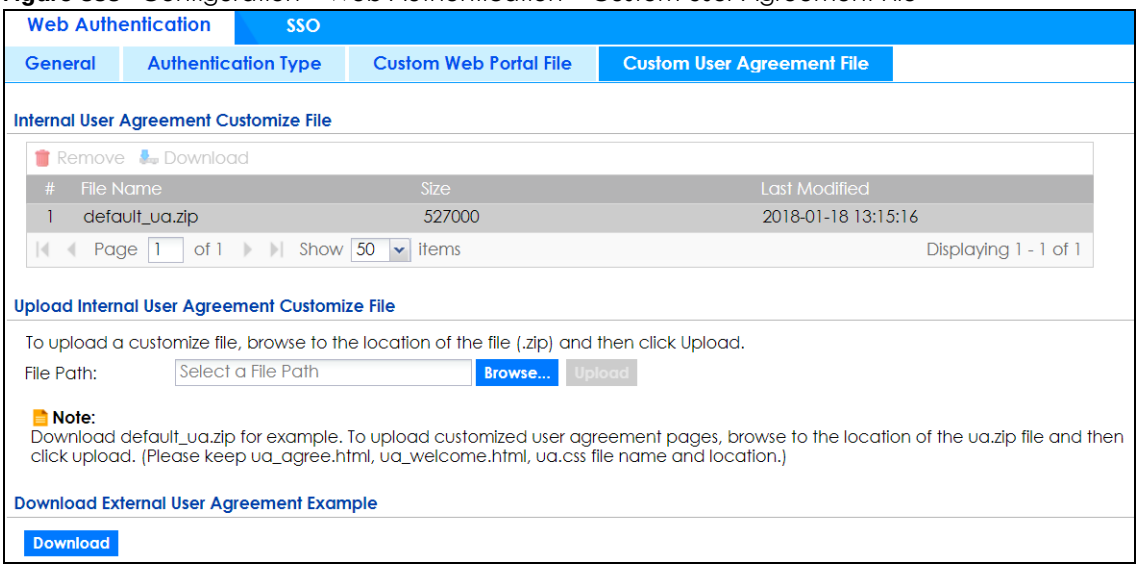


Figure 338 Configuration > Web Authentication > Custom User Agreement File



The following table describes the labels in this screen.

Table 188 Configuration > Web Authentication > Custom Web Portal / User Agreement File

LABEL	DESCRIPTION
Remove	Click a file's row to select it and click **Remove** to delete it from the Zyxel Device.
Download	Click a file's row to select it and click **Download** to save the zipped file to your computer.
#	This column displays the index number for each file entry. This field is a sequential value, and it is not associated with a specific entry.
File Name	This column displays the label that identifies a web portal or user agreement file.
Size	This column displays the size (in KB) of a file.
Last Modified	This column displays the date and time that the individual files were last changed or saved.
Browse / Upload	Click **Browse...** to find the zipped file you want to upload, then click the **Upload** button to put it on the Zyxel Device.
Download	Click this to download an example external web portal or user agreement file for your reference.

24.3 SSO Overview

The SSO (Single Sign-On) function integrates Domain Controller and Zyxel Device authentication mechanisms, so that users just need to log in once (single login) to get access to permitted resources.

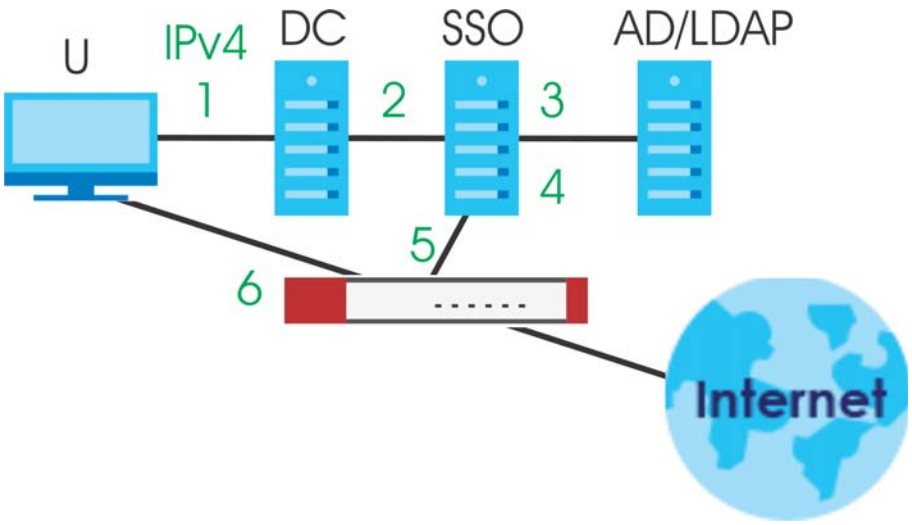
In the following figure, **U** user logs into a Domain Controller (**DC**) which passes the user's login credentials to the SSO agent. The SSO agent checks that these credentials are correct with the AD server, and if the AD server confirms so, the SSO then notifies the Zyxel Device to allow access for the user to the permitted resource (Internet access, for example).

Note: The Zyxel Device, the DC, the SSO agent and the AD server must all be in the same domain and be able to communicate with each other.

SSO does not support IPv6, LDAP or RADIUS; you must use it in an IPv4 network environment with Windows AD (Active Directory) authentication database.

You must enable Web Authentication in the **Configuration > Web Authentication** screen.

Figure 339 SSO Overview



U	User
DC	Domain Controller
SSO	Single Sign-On agent
AD	Active Directory

Install the SSO Agent on one of the following platforms:

- Windows 7 Professional (32-bit and 64-bit)
- Windows Server 2008 Enterprise (32-bit and 64-bit)
- Windows 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)

24.4 SSO - Zyxel Device Configuration

This section shows what you have to do on the Zyxel Device in order to use SSO.

Table 189 Zyxel Device - SSO Agent Field Mapping

ZYXEL DEVICE		SSO	
SCREEN	**FIELD**	**SCREEN**	**FIELD**
Web Authentication > SSO	Listen Port	Agent Configuration Page > Gateway Setting	Gateway Port
Web Authentication > SSO	Primary Agent Port	Agent Configuration Page	Agent Listening Port
Object > User/Group > User > Add	Group Identifier	Agent Configuration Page > Configure LDAP/AD Server	Group Membership
Object > AAA Server > Active Directory > Add	Base DN	Agent Configuration Page > Configure LDAP/AD Server	Base DN
Object > AAA Server > Active Directory > Add	Bind DN	Agent Configuration Page > Configure LDAP/AD Server	Bind DN
Object > User/Group > User > Add	User Name	Agent Configuration Page > Configure LDAP/AD Server	Login Name Attribute
Object > AAA Server > Active Directory > Add	Server Address	Agent Configuration Page > Configure LDAP/AD Server	Server Address
Network > Interface > Ethernet > wan (IPv4)	IP address	Agent Configuration Page > Gateway Setting	Gateway IP

24.4.1 Configuration Overview

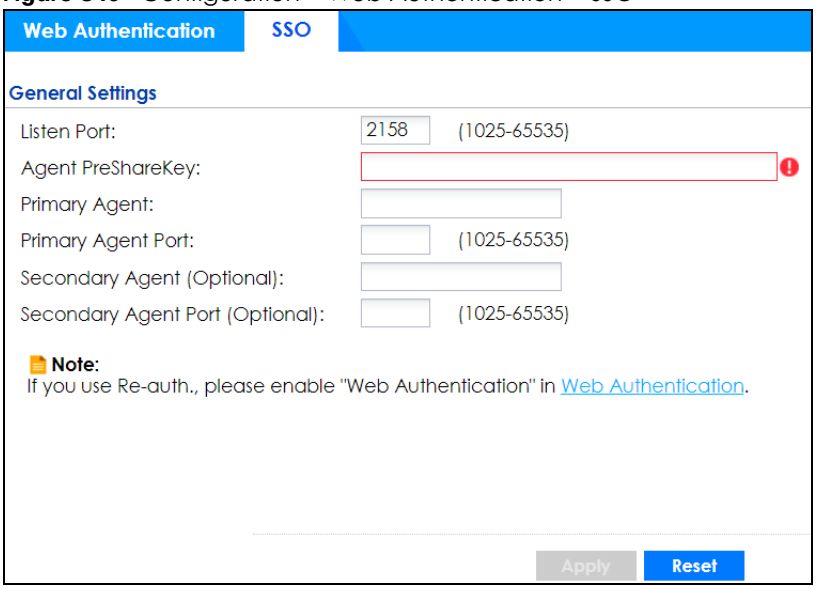
These are the screens you need to configure:

- Configure the Zyxel Device to Communicate with SSO on page 479
- Enable Web Authentication on page 480
- Create a Security Policy on page 482
- Configure User Information on page 483
- Configure an Authentication Method on page 484
- Configure Active Directory on page 485 or Configure Active Directory on page 485

24.4.2 Configure the Zyxel Device to Communicate with SSO

Use **Configuration > Web Authentication > SSO** to configure how the Zyxel Device communicates with the Single Sign-On (**SSO**) agent.

Figure 340 Configuration > Web Authentication > SSO



The following table gives an overview of the objects you can configure.

Table 190 Configuration > Web Authentication > SSO

LABEL	DESCRIPTION
Listen Port	The default agent listening port is 2158. If you change it on the Zyxel Device, then change it to the same number in the **Gateway Port** field on the SSO agent too. Type a number ranging from 1025 to 65535.
Agent PreShareKey	Type 8-32 printable ASCII characters or exactly 32 hex characters (0-9; a-f). The Agent PreShareKey is used to encrypt communications between the Zyxel Device and the SSO agent.
Primary Agent	Type the IPv4 address of the SSO agent. The Zyxel Device and the SSO agent must be in the same domain and be able to communicate with each other.
Primary Agent Port	Type the same port number here as in the **Agent Listening Port** field on the SSO agent. Type a number ranging from 1025 to 65535.
Secondary Agent Address (Optional)	Type the IPv4 address of the backup SSO agent if there is one. The Zyxel Device and the backup SSO agent must be in the same domain and be able to communicate with each other.
Secondary Agent Port (Optional)	Type the same port number here as in the **Agent Listening Port** field on the backup SSO agent if there is one. Type a number ranging from 1025 to 65535.
Apply	Click this button to save your changes to the Zyxel Device.
Reset	Click this button to return the screen to its last-saved settings

24.4.3 Enable Web Authentication

Enable **Web Authentication** and add a web authentication policy.