CHAPTER 25
Voice

25.1 Voice Overview

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider.

Use this chapter to:

- Connect an analog phone to the Zyxel Device.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

25.1.1 What You Can Do in this Chapter

These screens allow you to configure your Zyxel Device to make phone calls over the Internet and your regular phone line, and to set up the phone you connect to the Zyxel Device.

- Use the **SIP Account** screen to set up information about your SIP account, control which SIP accounts the phones connected to the Zyxel Device use, and configure audio settings such as volume levels for the phones connected to the Zyxel Device (Section 25.3 on page 421).
- Use the **SIP Service Provider** screen to configure the SIP server information, and the numbers for certain phone functions (Section 25.4 on page 427).
- Use the **SIP TLS Common** screen to change the default TLS local port if you need to, and select a local certificate for the SIP server to verify the Zyxel Device.(Section 25.5 on page 432).
- Use the **Phone** screens to change settings that depend on which region of the world the Zyxel Device is in (Section 25.6 on page 433).
- Use the **Call Rule** screen to set up shortcuts for dialing frequently-used (VoIP) phone numbers (Section 25.8 on page 436).
- Use the **Call History** screen to view a call history list (Section 25.9 on page 437).

You do not necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

25.1.2 What You Need to Know About VoIP

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signaling standard that lets one network device (like a computer or the Zyxel Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your Zyxel Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call. To access this screen, click **VoIP** > **SIP**.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the Zyxel Device to use your SIP account to make calls, the Zyxel Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you do not need a SIP account. It is possible for one SIP device (like the Zyxel Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup – figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

SIP Address

A SIP address is a URI (Uniform Resource Identifier) that resembles an email address, using the format: user@domain. It uniquely identifies a telephone extension over a VoIP system. A SIP address of 123-45-67@voip-provider.net tells a client to connect to voip-provider.net and request a connection to 123-45-67. While VoIP can only send voice messages over the Internet, SIP (though strictly speaking is a type of VoIP) can send voice, data, video, and other media. VoIP phones also need to be connected to a computer to function, whereas SIP phones only need to be connected to a modem.

25.2 Before You Begin

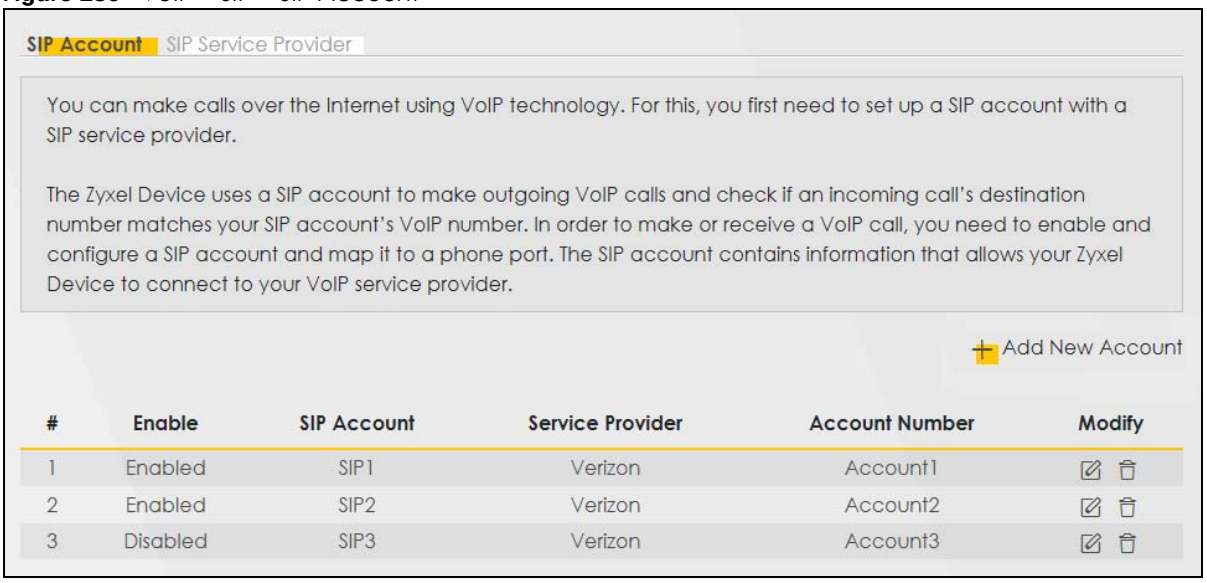
- Before you can use these screens, you need to have a VoIP account already set up. If you do not have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the Zyxel Device.

25.3 SIP Account

You can make calls over the Internet using VoIP technology. For this, you first need to set up a SIP account with a SIP service provider. The Zyxel Device uses a SIP account to make outgoing VoIP calls, and to check if an incoming call's destination number matches your SIP account's VoIP number. In order to make and receive VoIP calls, you need to enable and configure a SIP account, and then map it to a phone port. The SIP account contains information that allows your Zyxel Device to connect to your VoIP service provider.

To access this screen, click **VoIP** > **SIP** > **SIP Account.**

Figure 236 VoIP > SIP > SIP Account



The following table describes the labels in this screen.

Table 152 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
Add New Account	Click this to configure a SIP account.
#	This is the index number of the entry.
Enable	This shows whether the SIP account is activated or not. A yellow bulb signifies that this SIP account is activated. A gray bulb signifies that this SIP account is activated.
SIP Account	This shows the name of the SIP account.
Service Provider	This shows the name of the SIP service provider.
Account Number	This shows the SIP number.
Modify	Click the **Modify** icon to configure the SIP account.

25.3.1 Add or Edit SIP Account

Use this screen to configure a SIP account and map it to a phone port in the **Phone Device** screen. To access this screen, click the **Add New Account** button or click the **Edit** icon of an entry in the **VoIP** > **SIP** > **SIP Account** screen.

Note: You do not necessarily need to use all these fields to set up your account.

Figure 237 VoIP > SIP > SIP Account > Add Account or Edit

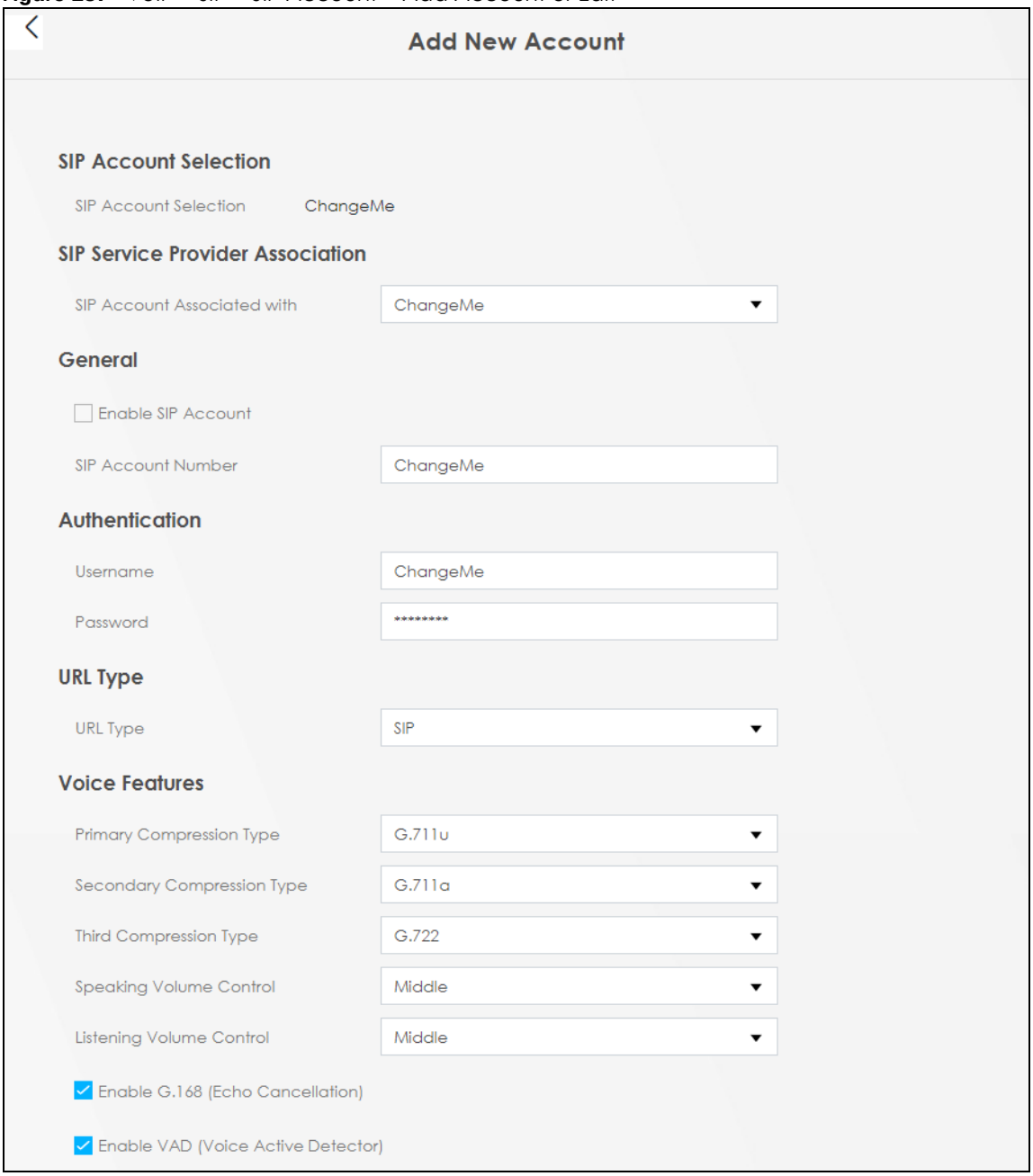
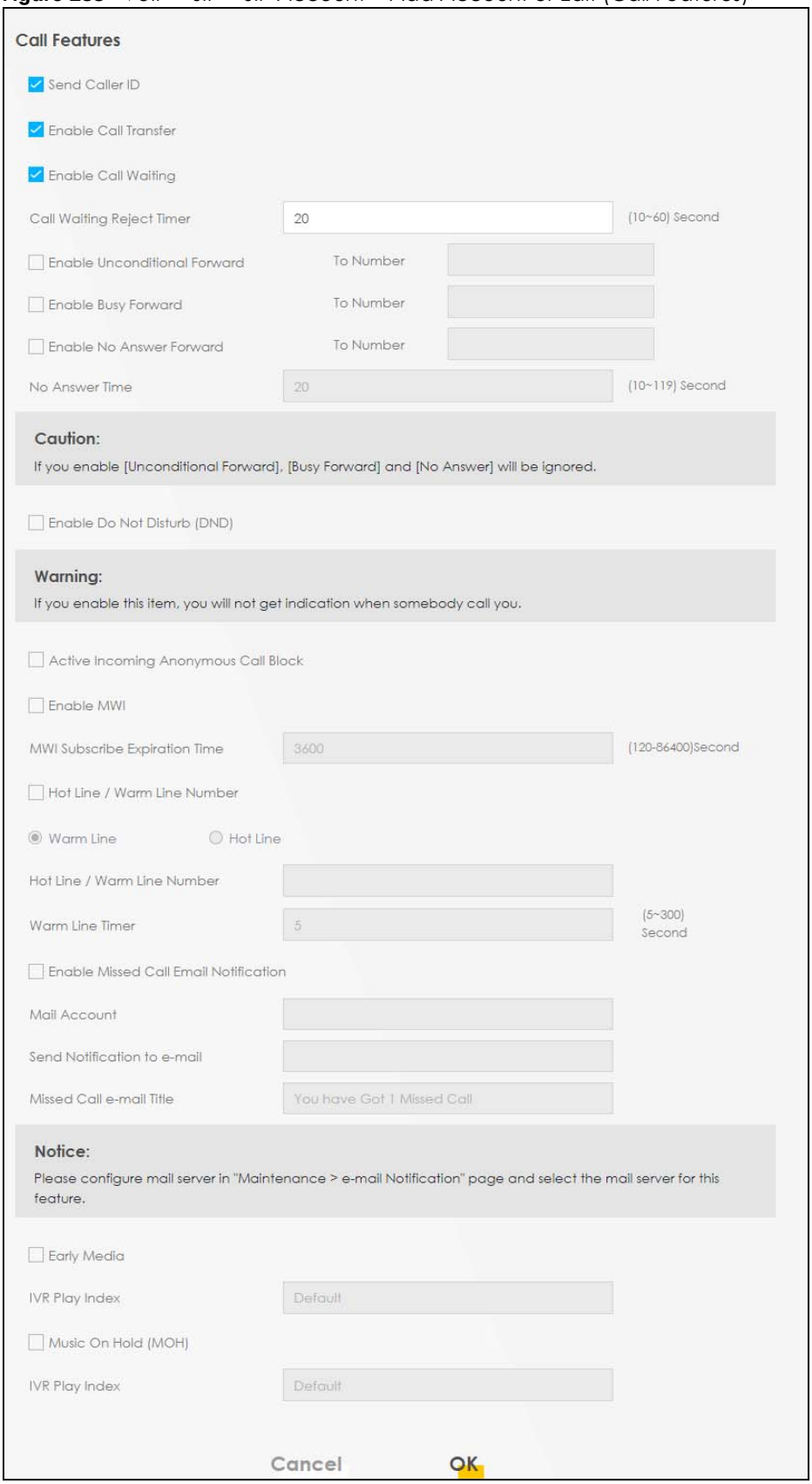


Figure 238 VoIP > SIP > SIP Account > Add Account or Edit (Call Features)



VoIPThe following table describes the labels in this screen.

Table 153 VoIP > SIP > SIP Account > SIP Account Entry Edit

LABEL	DESCRIPTION
SIP Account Selection	
SIP Account Selection	This field displays **ChangeMe** if you are creating a new SIP account or the SIP account you are modifying.
SIP Service Provider Association	
SIP Account Associated with	Select the SIP service provider profile to use for the SIP account you are configuring in this screen. You should already have configured a SIP service provider profile in the **SIP Service Provider** screen. This field is read-only when you are modifying an existing SIP account.
General	
Enable SIP Account	Select this if you want the Zyxel Device to use this account. Clear it if you do not want the Zyxel Device to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable characters and spaces.
Authentication	
Username	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 alphanumeric (0-9, a-z, A-Z), printable special characters and spaces.
Password	Enter the password for registering this SIP account, exactly as it was given to you. You can use up to 95 alphanumeric (0-9, a-z, A-Z), printable special characters and spaces.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the Zyxel Device sends the SIP number. **SIP** – include the SIP service domain name. **TEL** – do not include the SIP service domain name.
Voice Features	
Primary/Secondary/Third Compression Type	Select the type of voice coder or decoder (codec) that you want the Zyxel Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • **G.729** provides good sound quality and reduces the required bandwidth to 8 kbps. • **G.711a** is typically used in Europe. • **G.711u** is typically used in North America and Japan. • **G.726-24** operates at 24 kbps. • **G.726-32** operates at 32 kbps. • **G.722** operates at 6.3 kbps or 5.3 kbps. When two SIP devices start a SIP session, they must agree on a codec. Select the Zyxel Device's first choice for voice coder or decoder. Select the Zyxel Device's second choice for voice coder or decoder. Select **None** if you only want the Zyxel Device to accept the first choice. Select the Zyxel Device's third choice for voice coder or decoder. Select **None** if you only want the Zyxel Device to accept the first or second choice.
Speaking Volume Control	Select the loudness that the Zyxel Device uses for speech that it sends to the peer device. Choices are **Minimum**, **Middle**, and **Maximum**.

Table 153 VoIP > SIP > SIP Account > SIP Account Entry Edit (continued)

LABEL	DESCRIPTION
Listening Volume Control	Select the loudness that the Zyxel Device uses for speech that it receives from the peer device. Choices are **Minimum**, **Middle**, and **Maximum**.
Enable G. 168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Enable VAD (Voice Active Detector)	Select this if the Zyxel Device should stop transmitting when you are not speaking. This reduces the bandwidth the Zyxel Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Enable Call Transfer	Select this to enable call transfer on the Zyxel Device. This allows you to transfer an incoming call (that you have answered) to another phone.
Enable Call Waiting	Select this to enable call waiting on the Zyxel Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Call Waiting Reject Timer	Specify a time of seconds that the Zyxel Device waits before rejecting the second call if you do not answer it.
Enable Unconditional Forward	Select this if you want the Zyxel Device to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Enable Busy Forward	Select this if you want the Zyxel Device to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Enable No Answer Forward	Select this if you want the Zyxel Device to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the Zyxel Device should wait for you to answer an incoming call before it considers the call unanswered.
Enable Do Not Disturb (DND)	Select this to turn the do not disturb feature on. This has the Zyxel Device reject all calls destined to the phone line.
Active Incoming Anonymous Call Block	Select this to have the phone not ring for incoming calls with caller ID deactivated.
Enable MWI	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
MWI Subscribe Expiration Time	Keep the default value of this field unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the Zyxel Device subscribes to the service. Before this time passes, the Zyxel Device automatically subscribes again.
Hot Line / Warm Line Number	Select this to enable the hot line or warm line feature on the Zyxel Device.
Hot Line	Select this to have the Zyxel Device dial the specified hot line number immediately when you pick up the telephone.
Warm Line	Select this to have the Zyxel Device dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.

Table 153 VoIP > SIP > SIP Account > SIP Account Entry Edit (continued)

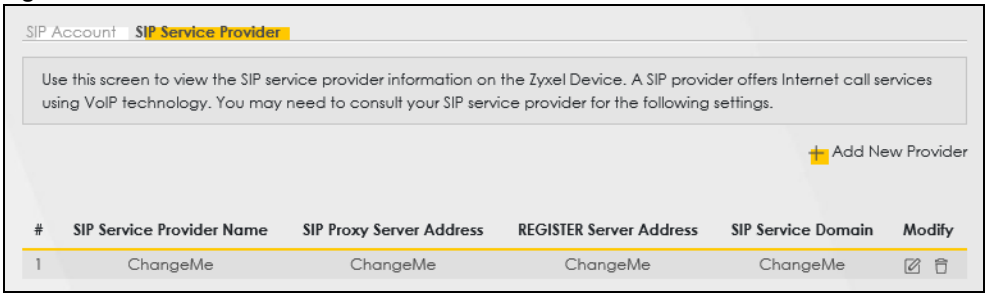
LABEL	DESCRIPTION
Hot Line / Warm Line Number	Enter the number of the hot line or warm line that you want the Zyxel Device to dial.
Warm Line Timer	Enter a number of seconds that the Zyxel Device waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Enable Missed Call Email Notification	Select this option to have the Zyxel Device email you a notification when there is a missed call.
Mail Account	Select a mail account for the email address specified below. If you select **None** here, email notifications will not be sent through email. You must have configured a mail account already in the **Email Notification** screen.
Send Notification to e-mail	Notifications are sent to the email address specified in this field. If this field is left blank, notifications will not be sent through email.
Missed Call e-mail Title	Type a title that you want to be in the subject line of the email notifications that the Zyxel Device sends.
Early Media	Select this if you want people to hear a customized recording when they call you.
IVR Play Index	Select the tone you want people to hear when they call you. This field is configurable only when you select **Early Media**. See Section 25.10 on page 438 for information on how to record these tones.
Music On Hold (MOH)	Select this to play a customized recording when you put people on hold.
IVR Play Index	Select the tone to play when you put someone on hold. This field is configurable only when you select **Music on Hold**, See Section 25.10 on page 438 for information on how to record these tones.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

25.4 SIP Service Provider

Use this screen to view the SIP service provider information on the Zyxel Device. A SIP provider offers Internet call services using VoIP technology. You may need to consult your SIP service provider for the following settings.

To access this screen, click **VoIP** > **SIP** > **SIP Service Provider**.

Figure 239 VoIP > SIP > SIP Service Provider



The following table describes the labels in this screen.

Table 154 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
Add New Provider	Click this button to add a new SIP service provider.
#	This is the index number of the entry.
SIP Service Provider Name	This shows the name of the SIP service provider.
SIP Proxy Server Address	This shows the IP address or domain name of the SIP server.
REGISTER Server Address	This shows the IP address or domain name of the SIP register server.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @symbol. You can use up to 127 printable ASCII Extended set characters.
Modify	Click the **Edit** icon to configure the SIP service provider. Click the **Delete** icon to delete this SIP service provider from the Zyxel Device.

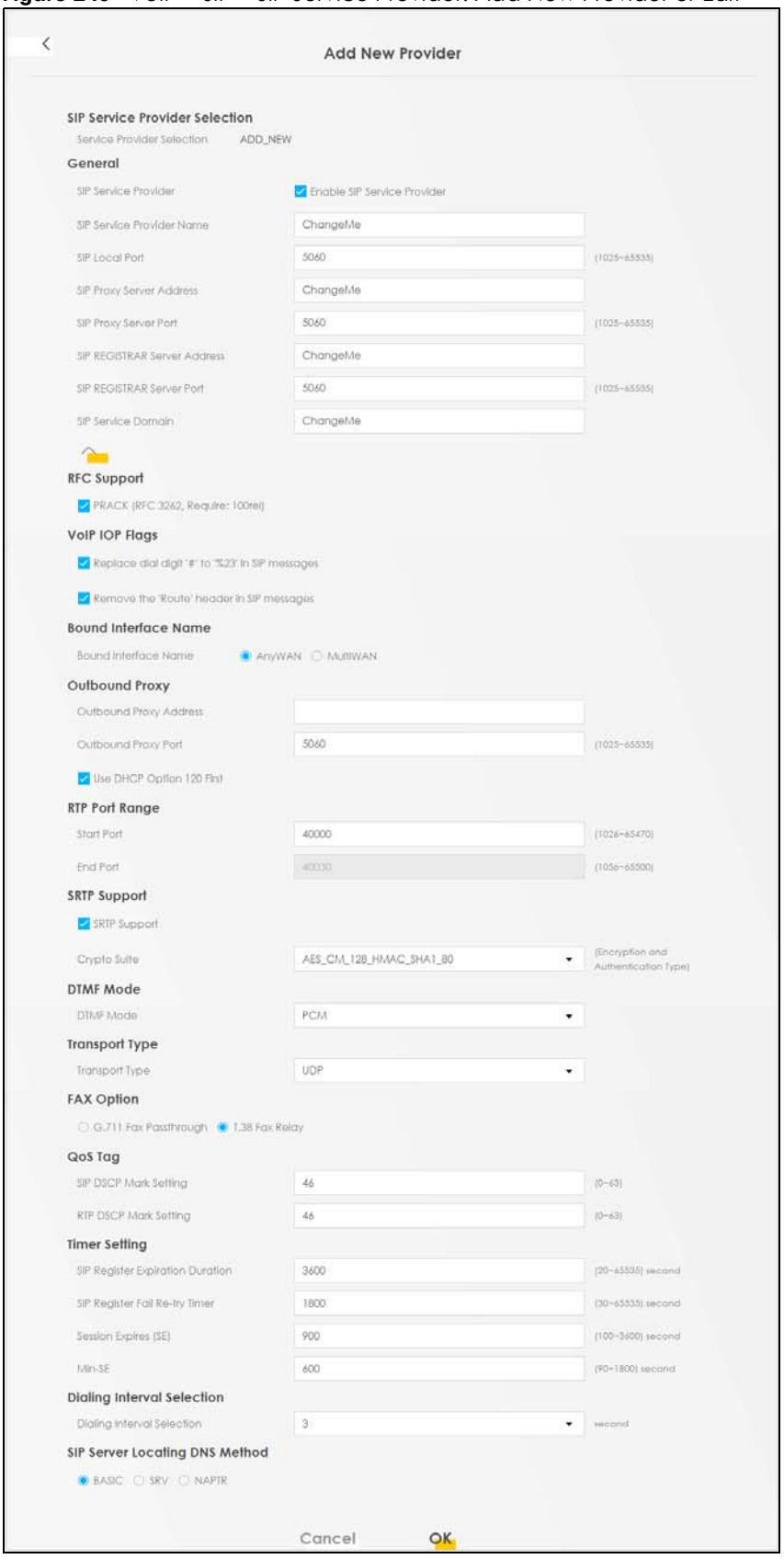
25.4.1 Provider Entry Add/Edit

Use this screen to configure the SIP server information, the numbers for certain phone functions and dialing plan for a SIP service provider.

Click the **Modify** icon next to a profile of SIP service provider settings in the **VoIP** > **SIP** > **SIP Service Provider** to open the following screen.

Note: Click this ( ) to see all the fields in the screen. You do not necessarily need to use all these fields to set up your account. Click again to see and configure only the fields needed for this feature.

Figure 240 VoIP > SIP > SIP Service Provider: Add New Provider or Edit



The following table describes the labels in this screen.

Table 155 VoIP > SIP > SIP Service Provider > Add New Provider or Edit

LABEL	DESCRIPTION
SIP Service Provider Selection	
Service Provider Selection	This field displays **ADD_NEW** if you are creating a new SIP service provider profile or the SIP service provider name you are modifying.
General	
SIP Service Provider	Select this if you want the Zyxel Device to use this SIP provider. Clear it if you do not want the Zyxel Device to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the Zyxel Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Proxy Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Proxy Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP REGISTRAR Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].
SIP REGISTRAR Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;].
RFC Support	
PRACK (RFC 3262, Require: 100rel)	During a call session, there are two types of SIP responses used – final and provisional. Final responses convey the result of a request and require a confirmation response. Provisional responses only convey the request processing progress and does not require a confirmation response, and are therefore considered unreliable. RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Which is, the Zyxel Device includes a SIP Require header field with the option tag 100rel in all INVITE requests. When the Zyxel Device receives a SIP response message indicating that the phone it called is ringing, the Zyxel Device sends a PRACK message to have both sides confirm the message is received. Select this to have the caller require the option tag 100rel to send provisional responses reliably.
VoIP IOP Flags – Select VoIP inter-operability settings.	
Replace dial digit '#' to '%23' in SIP messages	Replace a dial digit "#" with "%23" in the INVITE messages.
Remove the 'Route' header in SIP messages	Remove the 'Route' header in SIP packets.
Bound Interface Name	

Table 155 VoIP > SIP > SIP Service Provider > Add New Provider or Edit (continued)

LABEL	DESCRIPTION
Bound Interface Name	If you select **AnyWAN**, the Zyxel Device automatically activates the VoIP service when any WAN connection is up. If you select **MultiWAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Zyxel Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Zyxel Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
Use DHCP Option 120 first	Select this to have the Zyxel Device use DHCP Option 120 first.
RTP Port Range	
Start/End Port	Enter the listening port numbers for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
DTMF Mode	Control how the Zyxel Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** – send the DTMF tones in RTP packets. **PCM** – send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIP INFO** – send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the protocol used to transport the SIP packets. For **UDP** and **TCP**, see the Service appendix for more information on the example services and the required protocol and port number.
Ignore Direct IP	Select **Enable** to have the connected devices accept SIP requests only from the SIP proxy/register server specified above. SIP requests sent from other IP addresses will be ignored.
FAX Option	This field controls how the Zyxel Device handles fax messages.
QoS Tag	
SIP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Zyxel Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	

Table 155 VoIP > SIP > SIP Service Provider > Add New Provider or Edit (continued)

LABEL	DESCRIPTION
SIP Register Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Zyxel Device automatically tries to re-register your SIP account when one-half of this time has passed (The SIP register server might have a different expiration).
SIP Register Fall Re-try timer	Enter the number of seconds the Zyxel Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires [SE]	Enter the number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the Zyxel Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Zyxel Device accepts.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the Zyxel Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
SIP Server Location DNS Method	Select the method that the Zyxel Device used to query the ISP's DNS server for SIP server address. The Zyxel Device will use the query result to locate the SIP server for phone service registration. Select **BASIC** to have the Zyxel Device query the DNS server for a DNS A record that contains the IP address of the SIP server. Select **SRV** to have the Zyxel Device query the DNS server for a DNS Service (SRV) record. The SRV record is a list of all available SIP servers information that the DNS server maintains. The Zyxel Device will then use the SRV record to perform A query to get the SIP server IP. This is useful if your primary SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls. Select **NAPTR** to have the Zyxel Device query the DNS server for DNS Name Authority Pointer (NAPTR) records in order to find the available services (transport protocols) supported by the SIP server. The Zyxel Device will then perform an SRV or A query to get the SIP server information.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

25.5 SIP TLS Common

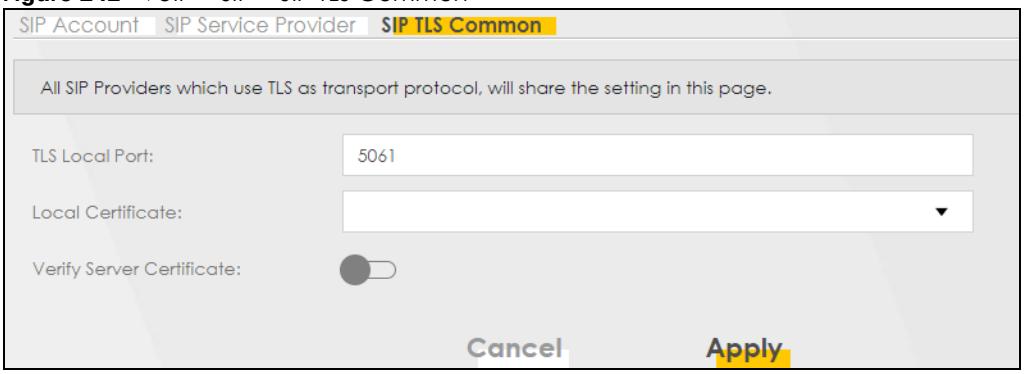
Use this screen to:

- Change the default TLS local port.
- Select a local certificate for the SIP server to verify the Zyxel Device.

Note: To activate **SIP TLS Common**, select **TLS** in **Transport Type** in the **SIP Service Provider** screen.

To access this screen, click **VoIP** > **SIP** > **SIP TLS Common**.

Figure 241 VoIP > SIP > SIP TLS Common



The following table describes the labels in this screen.

Table 156 VoIP > SIP > SIP TLS Common

LABEL	DESCRIPTION
TLS Local Port	Port 5061 is typically used for SIP over TLS. Enter the Zyxel Device's TLS local port number if your VoIP service provider gave you one. Otherwise, keep the default value.
Local Certificate	This is the certificate the SIP server uses to verify the Zyxel Device. Go to **Certificate** > **Local Certificate** and import a Zyxel Device certificate that the SIP server can use to verify the Zyxel Device, if required. Then select the certificate you imported in this field.
Verify Server Certificate	Click to enable this if you want the Zyxel Device to verify the certificate from the SIP server. If required or if your VoIP service provider gave you a certificate, import the dedicated CA in **Certificate** > **Trusted CA** in order for the Zyxel Device to authenticate the SIP server.

25.6 Phone

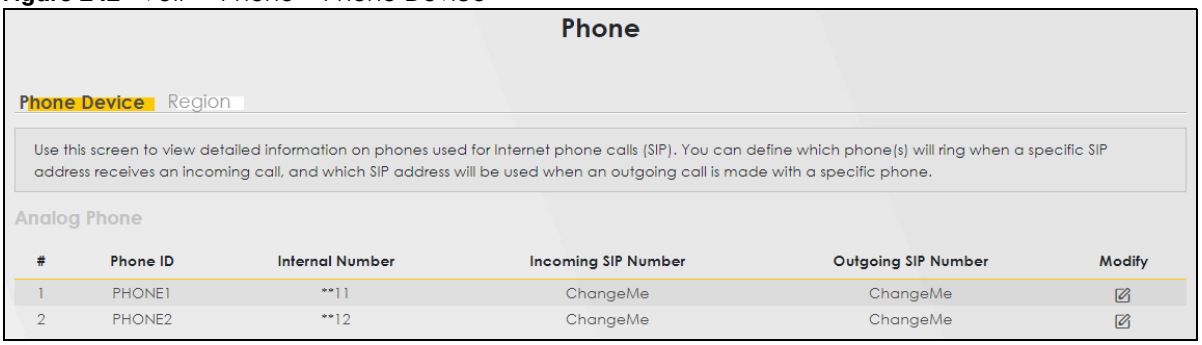
Use these screens to configure SIP numbers and regions for IP phones that are connected to the Zyxel Device.

25.6.1 Phone Device

Use this screen to view detailed information on phones used for Internet phone calls (SIP). You can define which phones will ring when a specific SIP address receives an incoming call, and which SIP address will be used when an outgoing call is made with a specific phone.

To access this screen, click **VoIP** > **Phone** > **Phone Device**.

Figure 242 VoIP > Phone > Phone Device



Each field is described in the following table.

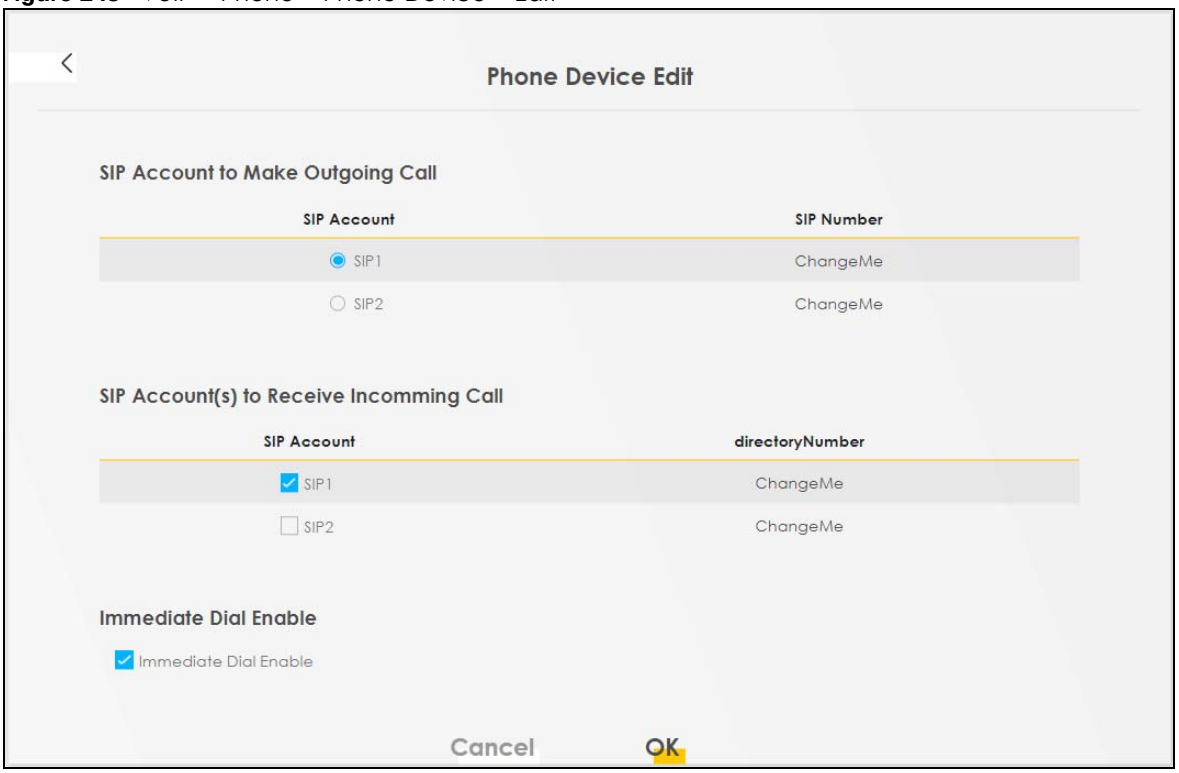
Table 157 VoIP > Phone > Phone Device

LABEL	DESCRIPTION
#	This displays the index number of the phone device.
Phone ID	This field displays the name of a phone port on the Zyxel Device.
Internal Number	This field displays the internal call prefix of a phone port on the Zyxel Device.
Incoming SIP Number	This field displays the SIP address that you use to receive calls on this phone port.
Outgoing SIP Number	This field displays the SIP address that you use to make calls on this phone port.
Modify	Click the **Edit** icon to configure the SIP account.

25.6.2 Phone Device Edit

Use this screen to control which SIP account and PSTN line each phone uses. Click an **Edit** icon in **VoIP** > **Phone** > **Phone Device** to open the following screen.

Figure 243 VoIP > Phone > Phone Device > Edit



Each field is described in the following table.

Table 158 VoIP > Phone > Phone Device > Edit

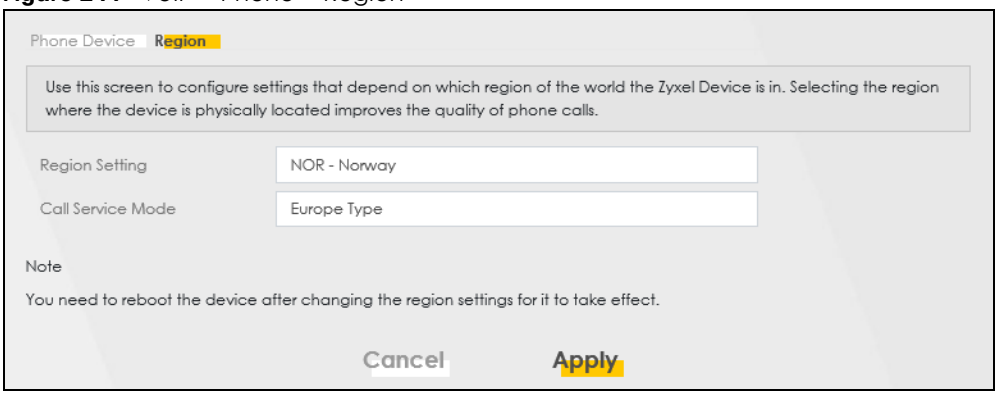
LABEL	DESCRIPTION
SIP Account to Make Outgoing Call	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Account(s) to Receive Incoming Call	Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port. If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
Immediate Dial Enable	Select this if you want to use the pound key (#) to tell the Zyxel Device to make the phone call immediately, instead of waiting for the number of second you selected in the **Dialog Interval Selection** field of the **VoIP** > **SIP** > **SIP Service Provider** > **Add New Provider** or **Edit** screen. If you select this, dial the phone number, and then press the pound key. The Zyxel Device makes the call immediately instead of waiting. You can still wait, if you want.
Cancel	Click **Cancel** to exit this screen without saving
OK	Click **OK** to save your changes.

25.7 Phone Region

Use this screen to configure settings that depend on which region of the world the Zyxel Device is in. Selecting the region where the device is physically located improves the quality of phone calls.

To access this screen, click **VoIP** > **Phone** > **Region**.

Figure 244 VoIP > Phone > Region



The following table describes the labels in this screen.

Table 159 VoIP > Phone > Region

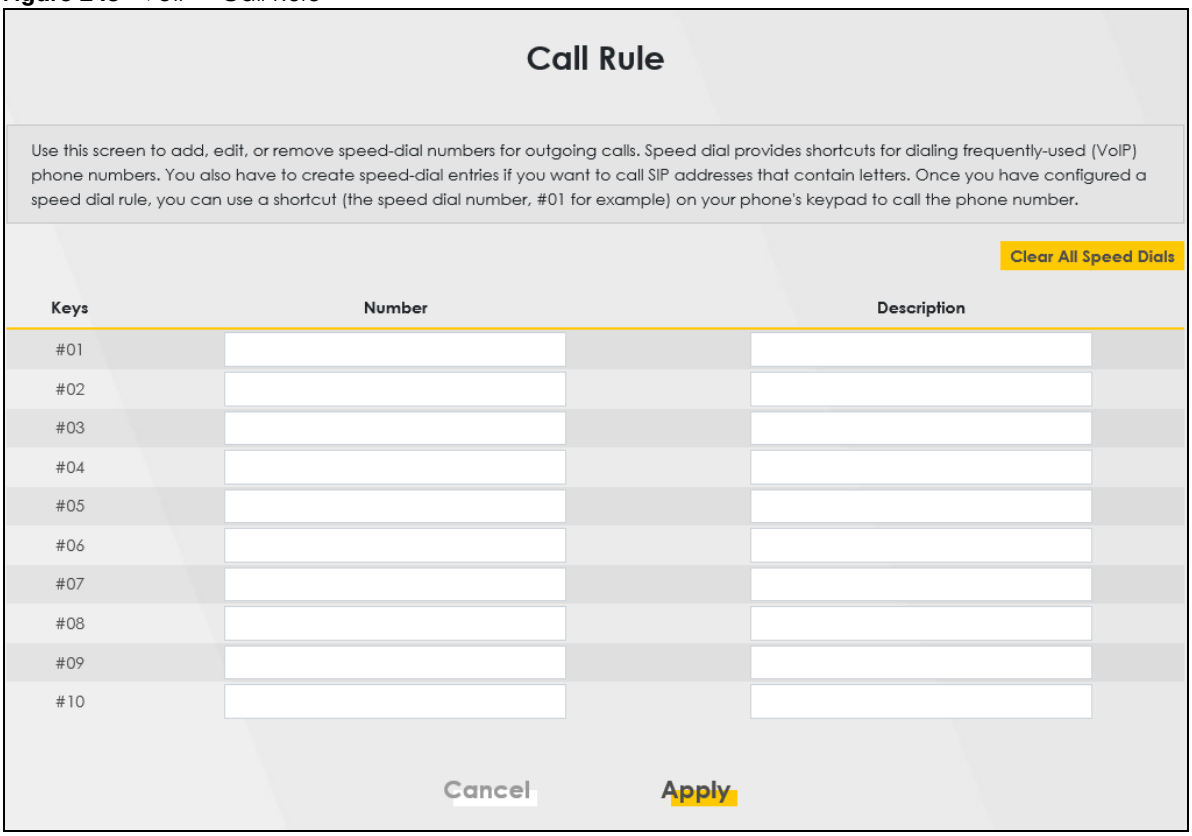
LABEL	DESCRIPTION
Region Setting	Select the place in which the Zyxel Device is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. • **Europe Type** – use supplementary phone services in European mode. • **USA Type** – use supplementary phone services American mode. You might have to subscribe to these services to use them. Contact your VoIP service provider.
Apply	Click this to save your changes and to apply them to the Zyxel Device.
Cancel	Click this to set every field in this screen to its last-saved value.

Note: You need to reboot the Zyxel Device after changing the region settings for it to take effect.

25.8 Call Rule

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number. To access this screen, click **VoIP** > **Call Rule**.

Figure 245 VoIP > Call Rule



The following table describes the labels in this screen.

Table 160 VoIP > Call Rule

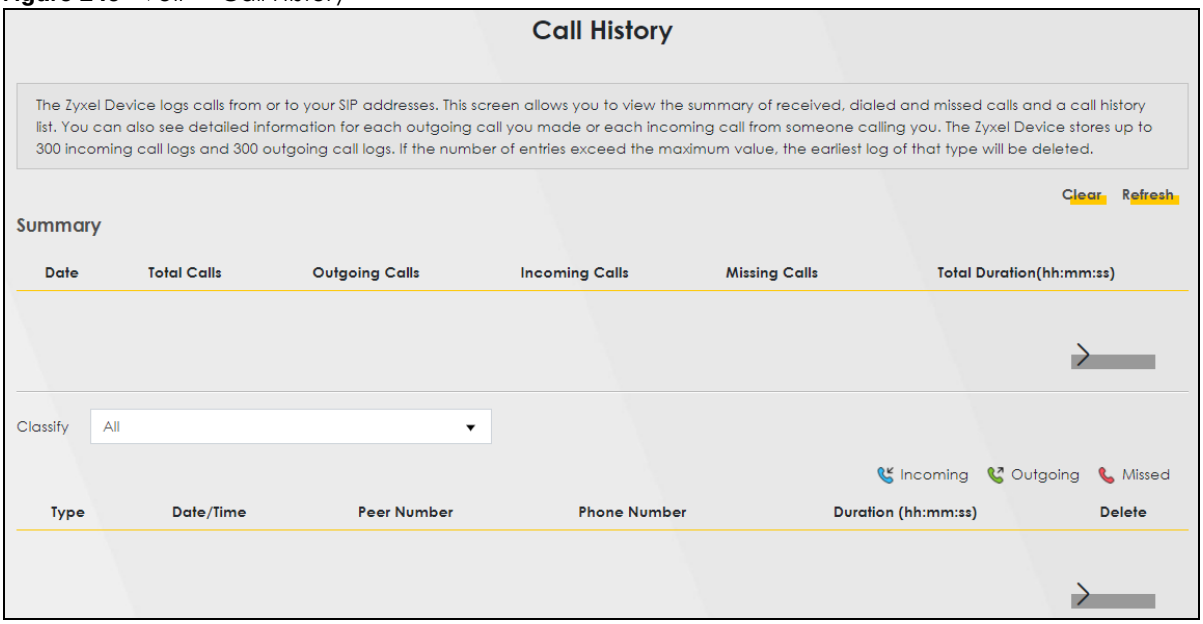
LABEL	DESCRIPTION
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the Zyxel Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Clear All Speed Dials	Click this button to remove all speed dials saved.
Apply	Click this to save your changes and to apply them to the Zyxel Device.
Cancel	Click this to set every field in this screen to its last-saved value.

25.9 Call History

The Zyxel Device logs calls from or to your SIP addresses. This screen allows you to view a summary of received, dialed and missed calls and a call history list. You can also view detailed information on each outgoing and incoming call.

To access this screen, click **VoIP** > **Call History**.

Figure 246 VoIP > Call History



Each field is described in the following table.

Table 161 VoIP > Call History

LABEL	DESCRIPTION
Clear	Click this button to remove all entries from the call history list.
Refresh	Click this button to renew the call history list.
Summary	
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP addresses that day.
Outgoing Calls	This displays how many calls originated from you that day.
Incoming Calls	This displays how many calls you received that day.
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration (hh:mm:ss)	This displays how long all calls lasted that day.
Classify	Select the type of the calls. The call types are: **All**, **Incoming**, **Outgoing** and **Missed**.
Type	This displays the type of the calls.
Date/Time	This displays the date and time when the calls were made.
Peer Number	This displays the SIP address that called you or you called.
Phone Number	This displays the phone number of the call.
Duration (hh:mm:ss)	This displays how long the call lasted.
Delete	Click the **Delete** icon to remove the call history.

25.10 Technical Reference

This section contains background material relevant to the **VoIP** screens.

VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

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 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.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an email address identifies an email account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an email address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

SIP Registration

Each Zyxel Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the Zyxel Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The Zyxel Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the Zyxel Device attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated through a challenge / response system using the HTTP digest mechanism (as detailed in RFC 3261, "SIP: Session Initiation Protocol").

SIP Servers

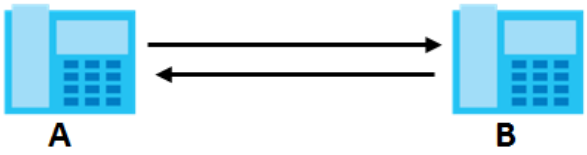
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP SIP user agent to receive the call.

Figure 247 SIP User Agent



SIP Proxy Server

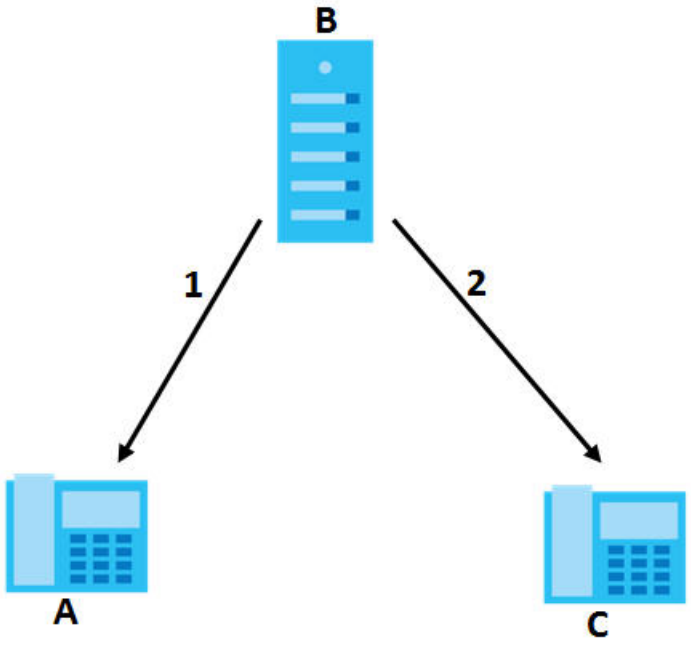
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).

2 The SIP proxy server forwards the call invitation to **C**.

Figure 248 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

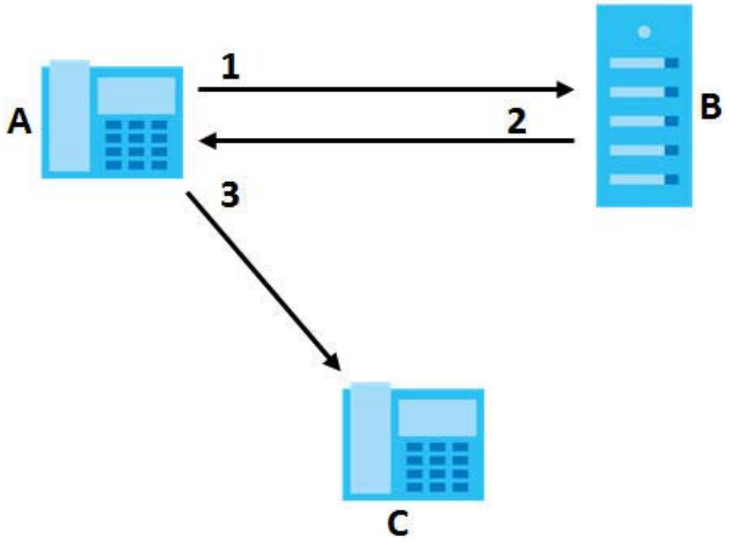
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).

2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

Figure 249 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

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

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 162 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	
	5.Dialogue (voice traffic)	
6. BYE	→	
	←	7. OK

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

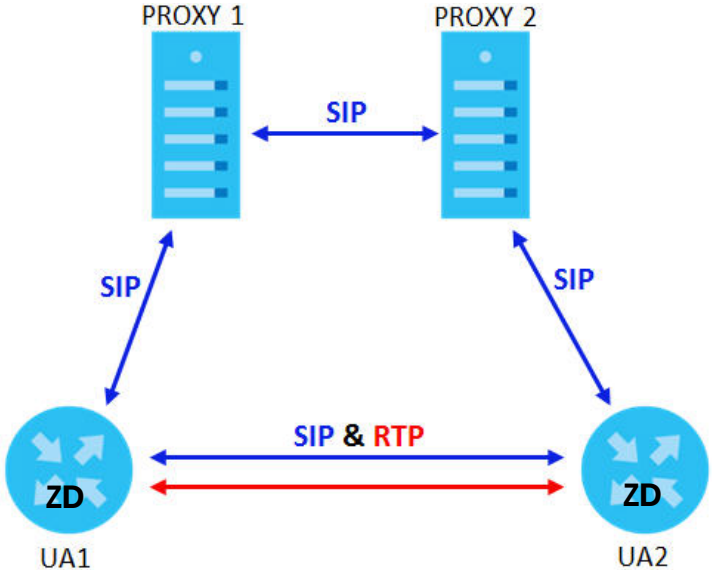
SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

Figure 250 SIP Call Through Proxy Servers

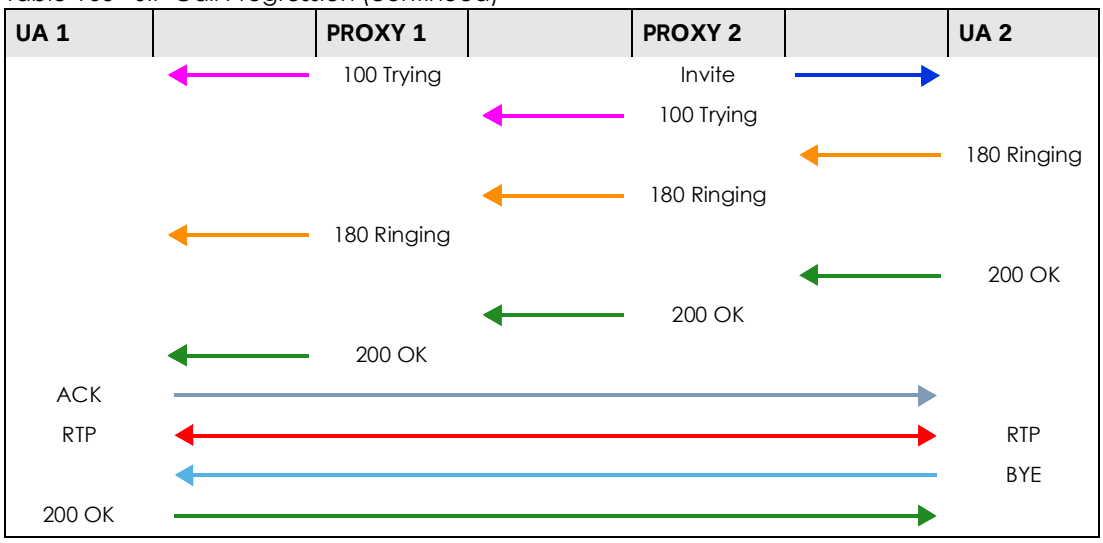


The following table shows the SIP call progression.

Table 163 SIP Call Progression

UA 1		PROXY 1		PROXY 2		UA 2
Invite →						
		Invite →				

Table 163 SIP Call Progression (continued)



1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.

2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.

3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** through **Proxy 1**.

5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** through **Proxy 1**.

6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.

7 When **User Agent 2** hangs up, he sends a BYE request.

8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The Zyxel Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.

- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Zyxel Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

Comfort Noise Generation

When using VAD, the Zyxel Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Zyxel Device. The Zyxel Device allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 164 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	900 seconds for all custom tones combined
Maximum Time per Individual Tone	180 seconds
Total Number of Tones Recordable	5 You can record up to 5 different custom tones but the total time must be 900 seconds or less.

Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1 Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1101~1105 on your phone followed by the "#" key.

3 Play your desired music or voice recording into the receiver's mouthpiece. Press the "#" key.

4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Listening to Custom Tones

Do the following to listen to a custom tone:

1 Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1201 – 1208 followed by the "#" key to listen to the tone.

3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Deleting Custom Tones

Do the following to delete a custom tone:

1 Pick up the phone and press "****" on your phone's keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1301 – 1308 followed by the "#" key to delete the tone of your choice. Press 14 followed by the "#" key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

25.10.1 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the Zyxel Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired.

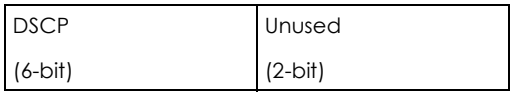
This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[3]

DSCP and Per-Hop Behavior

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

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

Figure 251 DiffServ: Differentiated Service Field



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

25.10.2 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The Zyxel Device supports the following services:

- Call Return
- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb
- IVR
- Call Completion
- CCBS
- Outgoing SIP

3. The Zyxel Device does not support DiffServ at the time of writing.

Note: To take full advantage of the supplementary phone services available through the Zyxel Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

25.10.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Zyxel Device.

You can invoke all the supplementary services by using the flash key.

25.10.2.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 165 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press "0".
- Disconnect the first call and answer the second call.

  Either press the flash key and press "1", or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then "2".

European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press "3" to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press "2".

25.10.2.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 166 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial "*98#" followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call (to party B).
3. When party B answers the second call, press the flash key to create a three-way conversation.
4. Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.

6 If you want to go back to the three-way conversation, press the flash key again.

7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

25.10.2.4 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

Table 167 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
*98#	Call transfer	Transfer a call to another phone. See Section 25.10.2.2 on page 448 (Europe type) and Section 25.10.2.3 on page 449 (USA type).
*66#	Call return	Place a call to the last person who called you.
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off.
#95#	Disable Do Not Disturb	
*41#	Enable Call Waiting	Use these to allow you to put a call on hold when you are answering another, or to turn this function off.
#41#	Disable Call Waiting	
****	IVR	Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold).
####	Internal Call	Call the phone(s) connected to the Zyxel Device.
*82	One Shot Caller Display Call	Activate or deactivate caller ID for the next call only.
*67	One Shot Caller Hidden Call	

CHAPTER 26
Log

26.1 What You Need To Know

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

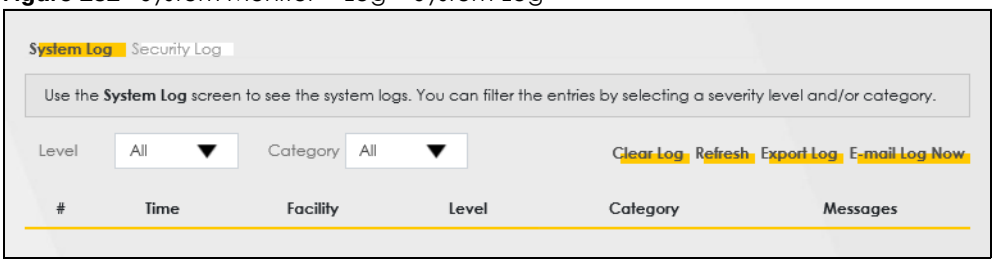
Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

26.2 System Log

Use the **System Log** screen to see the system logs. You can filter the entries by selecting a severity level and/or category. Click **System Monitor** > **Log** to open the **System Log** screen.

Figure 252 System Monitor > Log > System Log



The following table describes the fields in this screen.

Table 168 System Monitor > Log > System Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.

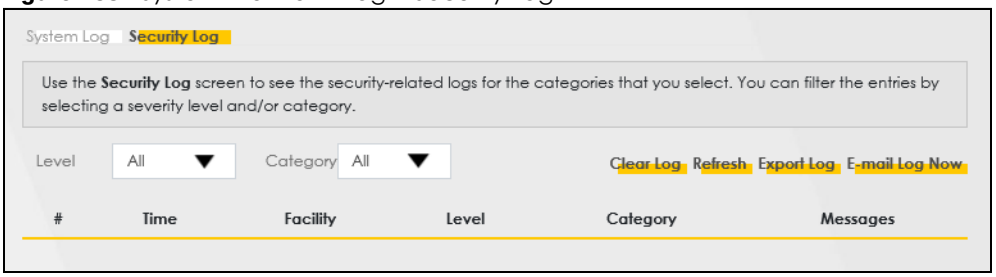
Table 168 System Monitor > Log > System Log (continued)

LABEL	DESCRIPTION
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the Zyxel Device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

26.3 Security Log

Use the **Security Log** screen to see the security-related logs for the categories that you select. You can filter the entries by selecting a severity level and/or category. Click **System Monitor** > **Log** > **Security Log** to open the following screen.

Figure 253 System Monitor > Log > Security Log



The following table describes the fields in this screen.

Table 169 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Zyxel Device searches through all logs of that severity or higher.
Category	Select the type of logs to display.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected logs.
E-mail Log Now	Click this to send the log files to the email address you specify in the **Maintenance** > **Log Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the log that the Zyxel Device is to send to this syslog server.
Category	This field displays the type of the log.
Messages	This field states the reason for the log.

CHAPTER 27
Traffic Status

27.1 Traffic Status Overview

Use the **Traffic Status** screens to look at the network traffic status and statistics of the WAN/LAN interfaces and NAT.

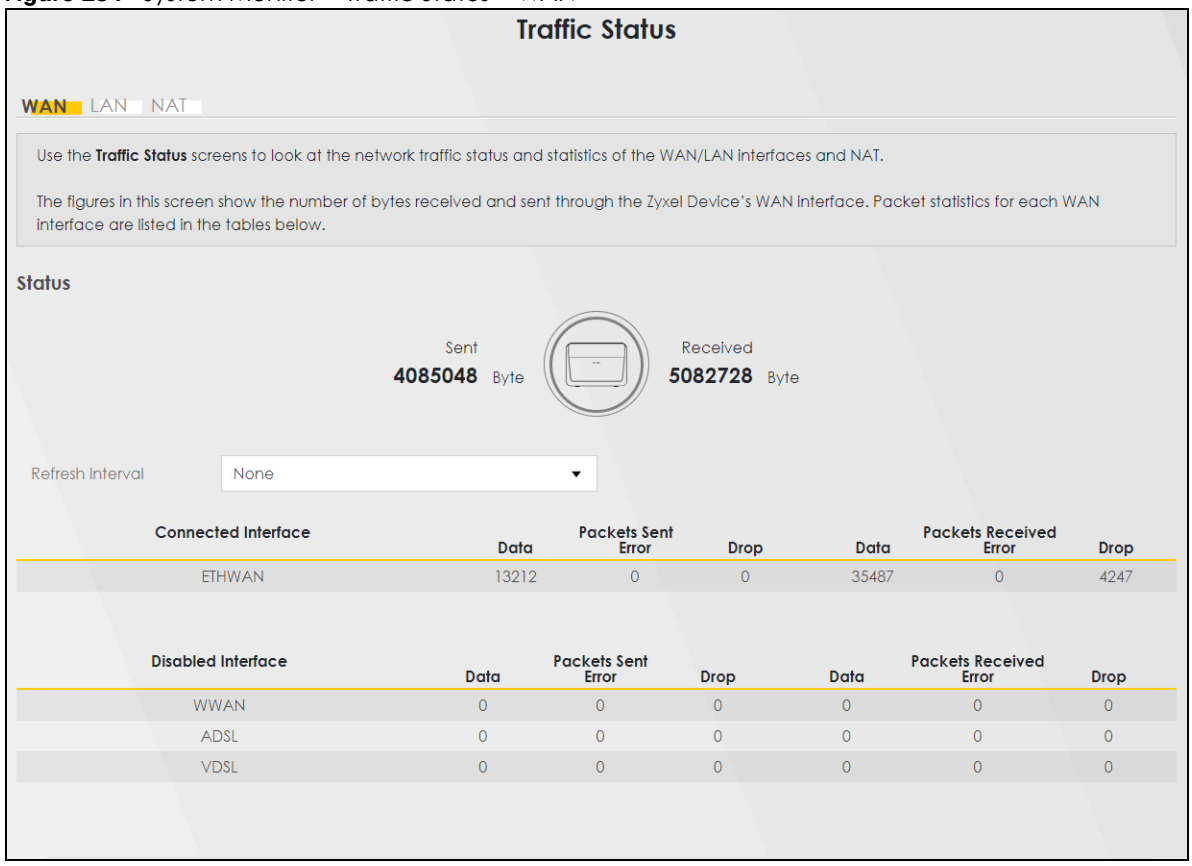
27.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 27.2 on page 454).
- Use the **LAN** screen to view the LAN traffic statistics (Section 27.3 on page 456).
- Use the **NAT** screen to view the NAT status of the Zyxel Device's clients (Section 27.4 on page 457).

27.2 WAN Status

Click **System Monitor** > **Traffic Status** to open the **WAN** screen. The figures in this screen show the number of bytes received and sent through the Zyxel Device's WAN interface. The table below shows packet statistics for each WAN interface.

Figure 254 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 170 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
Disabled Interface	This shows the name of the WAN interface that is currently disabled.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.

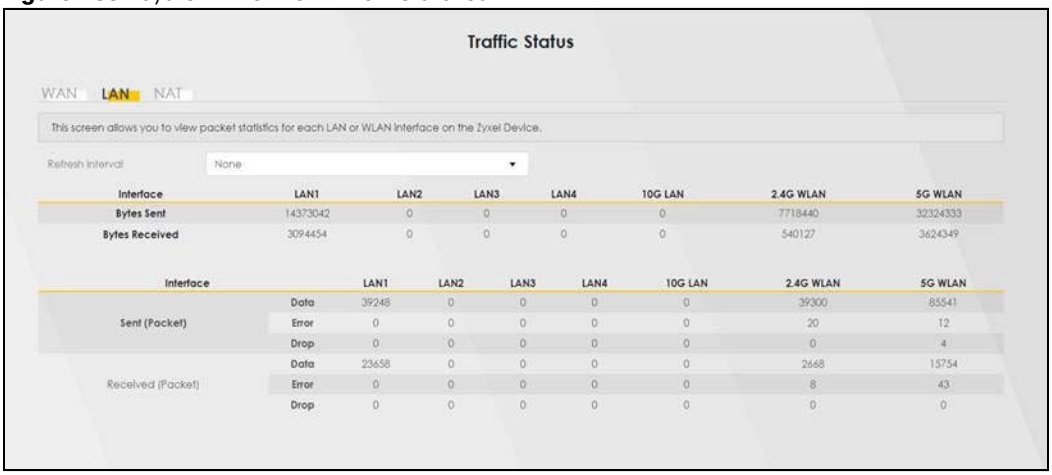
Table 170 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

27.3 LAN Status

Click **System Monitor** > **Traffic Status** > **LAN** to open the following screen. This screen allows you to view packet statistics for each LAN or WLAN interface on the Zyxel Device.

Figure 255 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

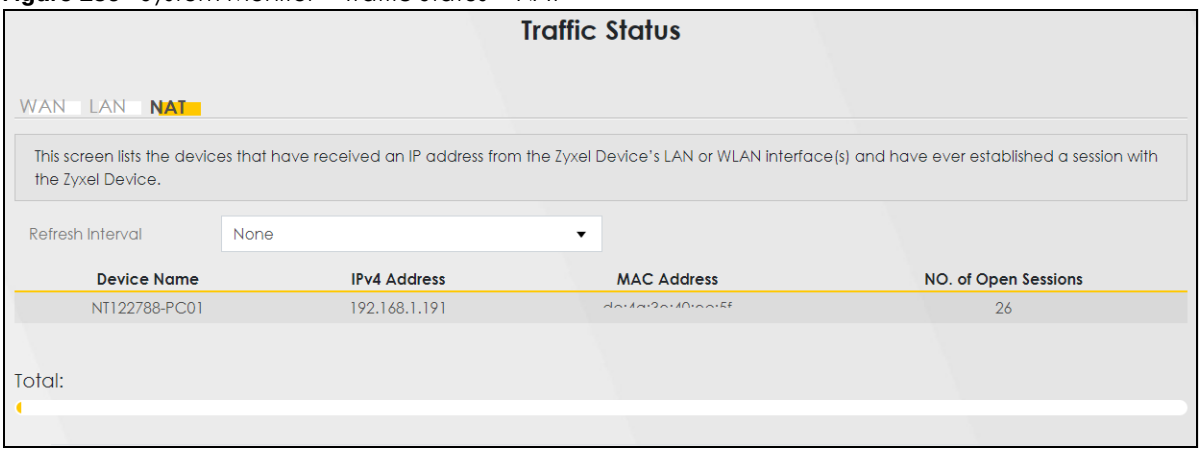
Table 171 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interfaces.
Sent (Packets)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packets)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

27.4 NAT Status

Click **System Monitor** > **Traffic Status** > **NAT** to open the following screen. This screen lists the devices that have received an IP address from the Zyxel Device LAN or WLAN interfaces and have ever established a session with the Zyxel Device.

Figure 256 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 172 System Monitor > Traffic Status > NAT

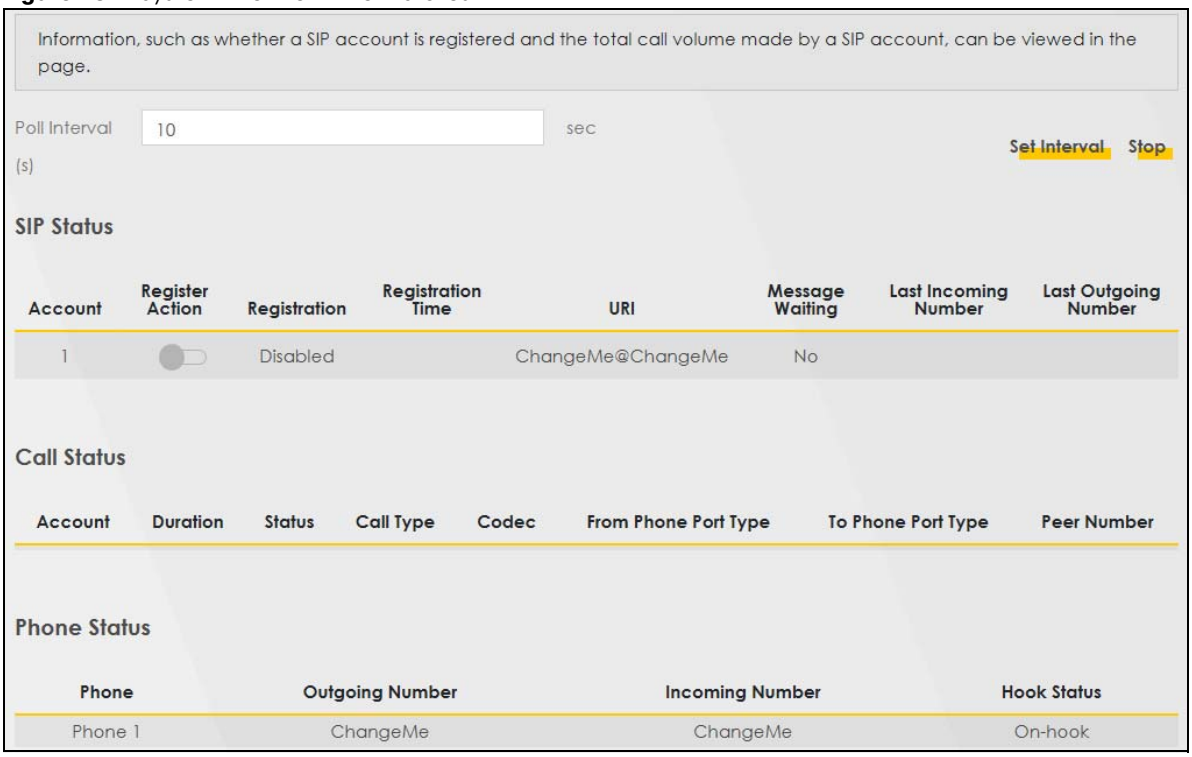
LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
Device Name	This displays the name of the connected host.
IPv4 Address	This displays the IP address of the connected host.
MAC Address	This displays the MAC address of the connected host.
No. of Open Sessions	This displays the number of NAT sessions currently opened for the connected host.
Total	This displays what percentage of NAT sessions the Zyxel Device can support is currently being used by all connected hosts. You can also see the number of active NAT sessions and the maximum number of NAT sessions the Zyxel Device can support

CHAPTER 28
VoIP Status

28.1 VoIP Status Screen

Click **System Monitor** > **VoIP Status** to open the following screen. You can view the Voice over IP (VoIP) registration, current call status and phone numbers in this screen.

Figure 257 System Monitor > VoIP Status



The following table describes the labels in this screen.

Table 173 System Monitor > VoIP Status

LABEL	DESCRIPTION
Poll Interval	Enter the number of seconds the Device needs to wait before updating this screen and then click **Set Interval**. Click **Stop** to have the Device stop updating this screen.
SIP Status	
Account	This column displays each SIP account in the Device.
Register Action	Click on this switch to register/unregister the SIP account. This switch will turn blue if a registration attempt is successful; otherwise, it will revert to its unregistered setting. Unregistering an account does not delete the SIP account itself, but removes the mapping between your SIP identity and your IP address or domain name,

Table 173 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Registration	This field displays the current registration status of the SIP account. **Registered** - The SIP account is activated and has been registered with a SIP server. You can use it to make a VoIP call. **Unregistered** - The SIP account is activated, but the last time the Zyxel Device tried to register the SIP account with the SIP server, the attempt failed. Use the **Register Action** switch to register the account again. The Zyxel Device will also automatically try to register the SIP account again after a period of time that you configured in **VoIP > SIP > SIP Service Provider > Add/Edit > SIP Register Fail Re-Try Timer**. **Disabled** - The SIP account is not active. Make sure the corresponding SIP Service Provider and SIP Account are both enabled in **VoIP > SIP > SIP Service Provider > Add/Edit** and **VoIP > SIP > SIP Account > Add/Edit**.
Registration Time	This field displays the last time the Device successfully registered the SIP account. The field is blank if the Device has never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in the **VoIP** > **SIP** screen.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** – There are no current VoIP calls, incoming calls or outgoing calls being made. **Dial** – The callee's phone is ringing. **Ring** – The phone is ringing for an incoming VoIP call. **Process** – There is a VoIP call in progress. **DISC** – The callee's line is busy, the callee hung up or your phone was left off the hook.

Table 173 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Call Type	This field displays the call direction type of the current VoIP call. Outgoing Call – It is a SIP VoIP call made by local phone ports, and this SIP account is able to issue a (SIP-based) call setup to the SIP account of remote peers for a VoIP call establishment. This (SIP-based) call setup signal is sent to the SIP server first, and then the SIP server would relay it to the target peer after correctly resolving and locating the target peer. During the call setup (signaling) phase, Calling state is displayed in the Status field, and it turns to InCall state once the call is successfully established. Incoming Call – It is a SIP VoIP call made or originated by remote SIP accounts to connect to this local SIP account. One or more local phone ports can be configured to receive this type of call, see the Incoming Number below, and all of them should begin to ring during the call setup (signaling phase), see the Status above. Once some remote SIP accounts start to ring one local phone, answer by off-hook to the call, and the call is successfully established. The other ringing local phone ports will stop ringing and turning to InCall state in the Status field. Internal Call – It is a local VoIP call between two different local phone ports. No SIP signaling is needed and thus no SIP server is involved to establish this type of call. This type of call is established through the Internal and Non-SIP local setup signaling procedure between the call- originating and call-terminating local phone ports. In general, one or more local phone ports can be designed to receive this type of call, and once any of the ringing phones answer the call, the other ringing ones will stop ringing. During the call setup phase (signaling phase), Calling state is displayed in Status field, and turns to InCall state once the call is successfully established.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
From Phone Port Type	This field displays the phone ports type used to originate, start, or create the current VoIP call. Type Two possible type values will be displayed here: SIP – For the current call which is categorized as Incoming Call in the Call Type filed, this field will show the type SIP. FXS – As for the other cases: Outgoing Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device.
To Phone Port Type	This field displays the phone ports type used to receive the current VoIP call. Three possible type Type values will be displayed here: SIP – For the current call which is categorized as Outgoing Call in the Call Type field, this field will show the type SIP. FXS and Unknown – As for the other cases: Incoming Call and Internal Call, this field will show the corresponding local phone port type: FXS, the legacy analog phone port on the device. While the call is established, this field shows Unknown during the call setup phase (signaling phase). This is because one or more local phone ports can be configured or designed to receive these two types of calls, see the Call Type above, and the local phone port will answer the call that hasn't been determined yet at that time.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays the name of a phone port on the Device.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Hook Status	This field displays whether the phone is in the on or off hook status. **Off-Hook** means a telephone connected to one of the phone port has its receiver off the hook. **On-Hook** means a telephone connected to one of the phone port has its receiver on the hook.

CHAPTER 29
ARP Table

29.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol (IP) address to a physical machine address, known as a Media Access Control (MAC) address, on the local area network.

An IP version 4 address is 32 bits long. MAC addresses are 48 bits long. The ARP table maintains an association between each MAC address and its corresponding IP address.

29.1.1 How ARP Works

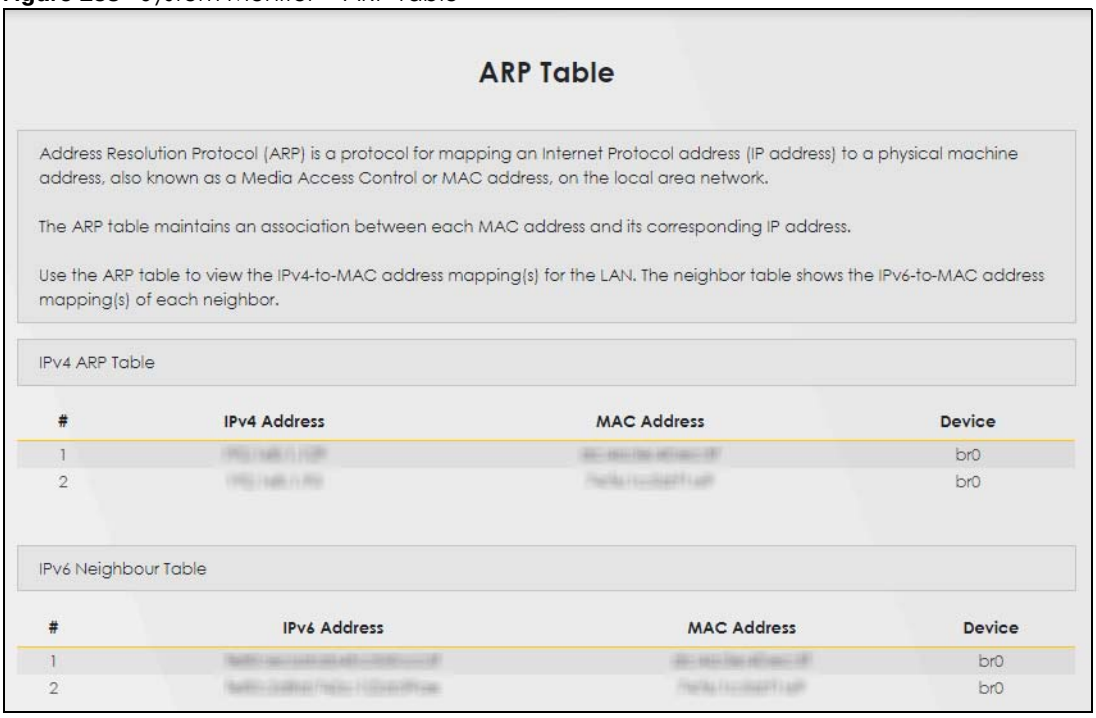
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP table for future reference and then sends the packet to the MAC address that replied.

29.2 ARP Table

Use the ARP table to view the IPv4-to-MAC address mappings for each device connected to the Zyxel Device. The neighbor table shows the IPv6-to-MAC address mappings of each IPv6 neighbor. To open this screen, click **System Monitor** > **ARP Table**.

Figure 258 System Monitor > ARP Table



The following table describes the labels in this screen.

Table 174 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IPv4 / IPv6 Address	This is the learned IPv4 or IPv6 IP address of a device connected to the Zyxel Device.
MAC Address	This is the MAC address of the connected device with the listed IP address.
Device	This is the type of interface used by the connected device. You can click the device type to go to its configuration screen.

CHAPTER 30
Routing Table

30.1 Routing Table Overview

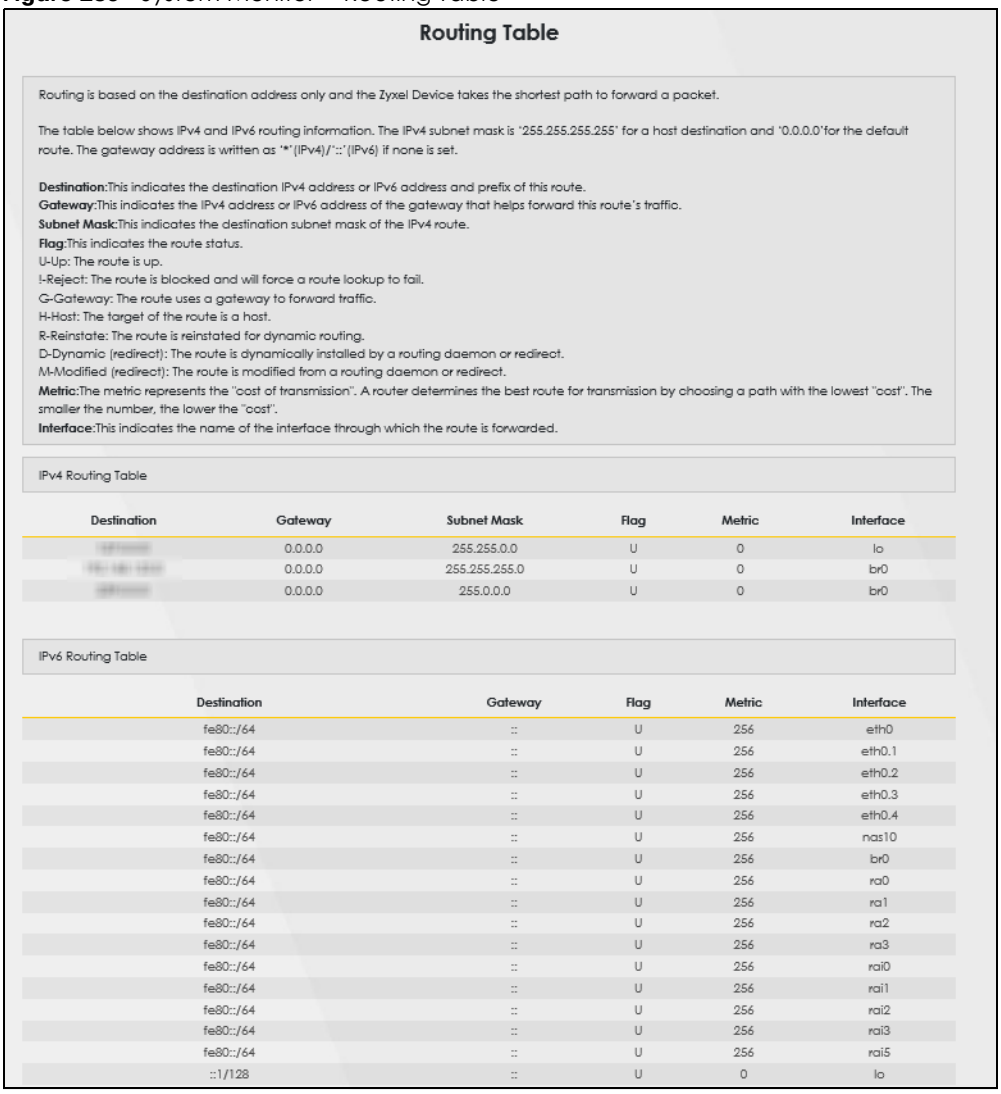
Routing is based on the destination address only and the Zyxel Device takes the shortest path to forward a packet.

30.2 Routing Table

The table below shows IPv4 and IPv6 routing information. The IPv4 subnet mask is '255.255.255.255' for a host destination and '0.0.0.0' for the default route. The gateway address is written as '*'(IPv4)/'::'(IPv6) if none is set.

Click **System Monitor** > **Routing Table** to open the following screen.

Figure 259 System Monitor > Routing Table



The following table describes the labels in this screen.

Table 175 System Monitor > Routing Table

LABEL	DESCRIPTION
IPv4 / IPv6 Routing Table	
Destination	This indicates the destination IPv4 address or IPv6 address and prefix of this route.
Gateway	This indicates the IPv4 address or IPv6 address of the gateway that helps forward this route's traffic.
Subnet Mask	This indicates the destination subnet mask of the IPv4 route.

Table 175 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	This indicates the route status. **U–Up:** The route is up. **!–Reject:** The route is blocked and will force a route lookup to fail. **G–Gateway:** The route uses a gateway to forward traffic. **H–Host:** The target of the route is a host. **R–Reinstate:** The route is reinstated for dynamic routing. **D–Dynamic (redirect):** The route is dynamically installed by a routing daemon or redirect. **M–Modified (redirect):** The route is modified from a routing daemon or redirect.
Metric	The metric represents the "cost of transmission." A router determines the best route for transmission by choosing a path with the lowest "cost." The smaller the number, the lower the "cost."
Interface	This indicates the name of the interface through which the route is forwarded. • **brx** indicates a LAN interface where x can be 0 – 3 to represent LAN1 to LAN4 respectively. • **ptm0** indicates a VDSL (including G.fast) WAN interface using IPoE or in bridge mode. • **ethx** indicates an Ethernet WAN interface using IPoE or in bridge mode. • **ppp0** indicates a WAN interface using PPPoE. • **wlx** indicates a wireless interface where x can be 0 – 1.

CHAPTER 31
Multicast Status

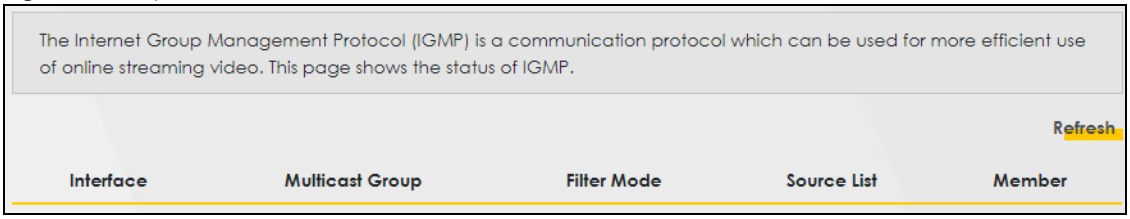
31.1 Multicast Status Overview

Use the **Multicast Status** screens to look at IGMP/MLD group status and traffic statistics.

31.2 The IGMP Status Screen

Use this screen to look at the current list of multicast groups the Zyxel Device manages through IGMP. Configure IGMP in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > IGMP Status**.

Figure 260 System Monitor > Multicast Status > IGMP Status



The following table describes the labels in this screen.

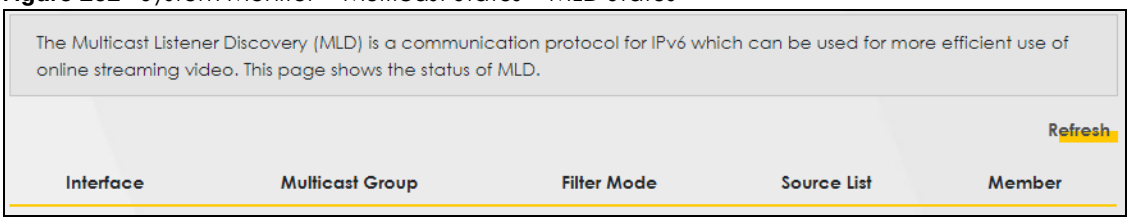
Table 176 System Monitor > Multicast Status > IGMP Status

LABEL	DESCRIPTION
Refresh	Click this button to update the information on this screen.
Interface	This field displays the name of an interface on the Zyxel Device that belongs to an IGMP multicast group.
Multicast Group	This field displays the name of the IGMP multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of the members of the multicast group.

31.3 The MLD Status Screen

Use this screen to look at the current list of multicast groups the Zyxel Device manages through MLD. Configure MLD in **Network Setting > IGMP/MLD**. To open this screen, click **System Monitor > Multicast Status > MLD Status**.

Figure 261 System Monitor > Multicast Status > MLD Status



The following table describes the labels in this screen.

Table 177 System Monitor > Multicast Status > MLD Status

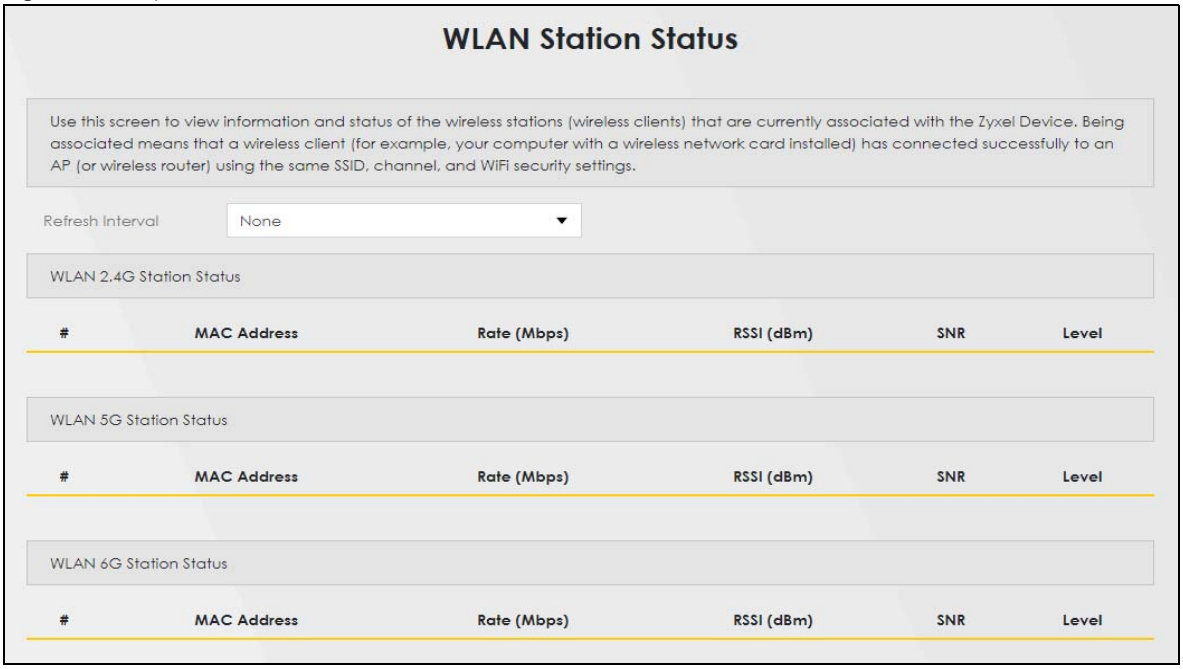
LABEL	DESCRIPTION
Refresh	Click this button to update the status on this screen.
Interface	This field displays the name of an interface on the Zyxel Device that belongs to an MLD multicast group.
Multicast Group	This field displays the name of the MLD multicast group to which the interface belongs.
Filter Mode	**INCLUDE** means that only the IP addresses in the **Source List** get to receive the multicast group's traffic. **EXCLUDE** means that the IP addresses in the **Source List** are not allowed to receive the multicast group's traffic but other IP addresses can.
Source List	This is the list of IP addresses that are allowed or not allowed to receive the multicast group's traffic depending on the filter mode.
Member	This is the list of members in the multicast group.

CHAPTER 32
WLAN Station Status

32.1 WLAN Station Status Overview

Click **System Monitor** > **WLAN Station Status** to open the following screen. Use this screen to view information and status of the WiFi stations (WiFi clients) that are currently associated with the Zyxel Device. Being associated means that a WiFi client (for example, your computer with a WiFi network card installed) has connected successfully to an AP (or WiFi router) using the same SSID, channel, and WiFi security settings.

Figure 262 System Monitor > WLAN Station Status



The following table describes the labels in this screen.

Table 178 System Monitor > WLAN Station Status

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the Zyxel Device to update this screen.
#	This is the index number of an associated WiFi station.
MAC Address	This field displays the MAC address of an associated WiFi station.
Rate (Mbps)	This field displays the transmission rate of WiFi traffic between an associated WiFi station and the Zyxel Device.
RSSI (dBm)	The RSSI (Received Signal Strength Indicator) field shows the WiFi signal strength of the station's WiFi connection. The normal range is –30dBm to –79dBm. If the value drops below –80dBm, try moving the associated WiFi station closer to the Zyxel Device to get better signal strength.

Table 178 System Monitor > WLAN Station Status (continued)

LABEL	DESCRIPTION
SNR	The Signal-to-Noise Ratio (SNR) is the ratio between the received signal power and the received noise power. The greater the number, the better the quality of WiFi. The normal range is 15 to 40. If the value drops below 15, try moving the associated WiFi station closer to the Zyxel Device to get better quality WiFi.
Level	This field displays a number which represents the strength of the WiFi signal between an associated WiFi station and the Zyxel Device. The Zyxel Device uses the RSSI and SNR values to determine the strength of the WiFi signal. **5** means the Zyxel Device is receiving an excellent WiFi signal. **4** means the Zyxel Device is receiving a very good WiFi signal. **3** means the Zyxel Device is receiving a weak WiFi signal, **2** means the Zyxel Device is receiving a very weak WiFi signal. **1** means the Zyxel Device is not receiving a WiFi signal.

CHAPTER 33
Cellular Statistics

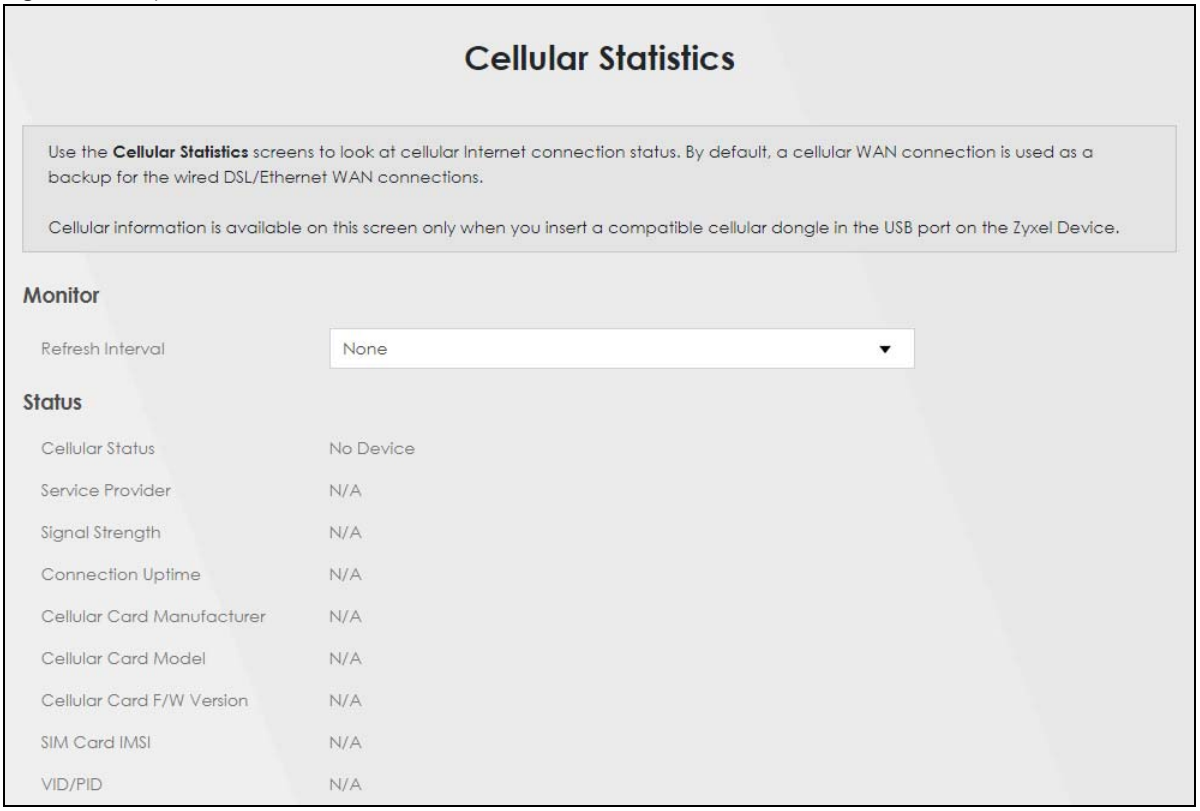
33.1 Cellular Statistics Overview

Use the **Cellular Statistics** screens to look at cellular Internet connection status. By default, a cellular WAN connection is used as a backup for the wired DSL or Ethernet WAN connections.

33.2 Cellular Statistics Settings

To open this screen, click **System Monitor** > **Cellular Statistics**. Cellular information is available on this screen only when you insert a compatible cellular dongle in the USB port on the Zyxel Device.

Figure 263 System Monitor > Cellular Statistics



The following table describes the labels in this screen.

Table 179 System Monitor > Cellular Statistics

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Select how often you want the Zyxel Device to update this screen. Select **None** to stop refreshing.
Status	
Cellular Status	This field displays the status of the cellular Internet connection. This field can display: **GSM** – Global System for Mobile Communications, 2G **GPRS** – General Packet Radio Service, 2.5G **EDGE** – Enhanced Data rates for GSM Evolution, 2.75G **WCDMA** – Wideband Code Division Multiple Access, 3G **HSDPA** – High-Speed Downlink Packet Access, 3.5G **HSUPA** – High-Speed Uplink Packet Access, 3.75G **HSPA** – HSDPA+HSUPA, 3.75G
Service Provider	This field displays the name of the service provider.
Signal Strength	This field displays the strength of the signal in dBm.
Connection Uptime	This field displays the time the connection has been up.
Cellular Card Manufacturer	This field displays the manufacturer of the cellular card.
Cellular Card Model	This field displays the model name of the cellular card.
Cellular Card F/W Version	This field displays the firmware version of the cellular card.
SIM Card IMSI	The International Mobile Subscriber Identity or IMSI is a unique identification number associated with all cellular networks. This number is provisioned in the SIM card.
VID/PID	This field displays the USB Vendor ID and Product ID of the cellular card.

CHAPTER 34
Optical Signal Status

34.1 Overview

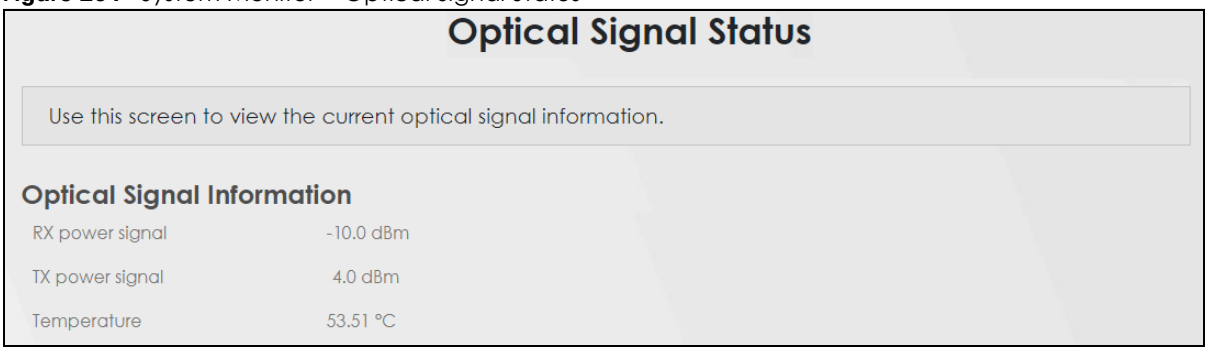
Use this screen to view the PON (Passive Optical Network) transceiver's TX power and RX power level and temperature.

34.2 The Optical Signal Status Screen

Click **System Monitor** > **Optical Signal Status** to open the **Optical Signal Status** screen to see the real-time DDMI (Digital Diagnostics Monitoring Interface) parameters.

The PON transceiver's support for the DDMI function lets you monitor the PON transceiver's parameters to perform component monitoring, fault isolation, and failure prediction tasks. This allows proactive, preventative network maintenance to help ensure service continuity.

Figure 264 System Monitor > Optical Signal Status



The following table describes the labels in this screen.

Table 180 System Monitor > Optical Signal Status

LABEL	DESCRIPTION
Optical Signal Information	
RX power signal	This displays the PON transceiver's receiving power in dBm. The normal range is –9 to –28 dBm. The lower the value, the stronger the signal as there is less background noise. For example, –28 dBm is a stronger signal than –9 dBm.
TX power signal	This displays the PON transceiver's transmitting power in dBm. The normal range is 4 to 9 dBm.
Temperature	This displays the PON transceiver's temperature in degrees Celsius. The normal range is 0 to 85 degrees Celsius (185 degrees Fahrenheit).

Note: Make sure the fiber optic cable is well connected to the PON port.

Note: If the TX and RX power signals of the DDMI are out of range, inspect the fiber optic cable for dirt, any fiber optic cable bends or excessive curves. If the fiber optic cable is clean and undamaged, use the power meter to measure whether the actual RX power signal of the Zyxel Device falls within the range of –9.0 to –28 dBm.

CHAPTER 35
System

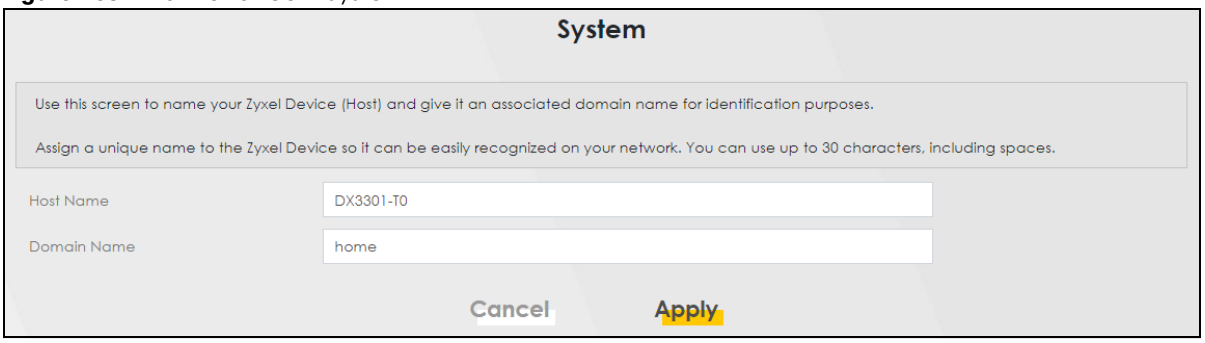
35.1 System Overview

Use this screen to name your Zyxel Device (Host) and give it an associated domain name for identification purposes.

35.2 System

Click **Maintenance** > **System** to open the following screen. Assign a unique name to the Zyxel Device so it can be easily recognized on your network. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.

Figure 265 Maintenance > System



The following table describes the labels in this screen.

Table 181 Maintenance > System

LABEL	DESCRIPTION
Host Name	Enter a descriptive host name for your Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. For some models, the supported maximum input length is 16 alphanumeric characters.
Domain Name	Enter a domain name for your host Zyxel Device. You can use up to 30 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Cancel	Click **Cancel** to abandon this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 36
User Account

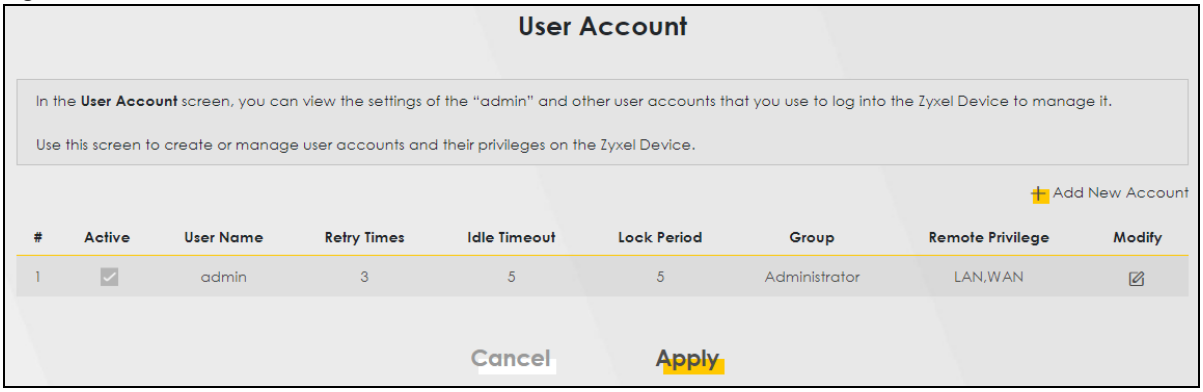
36.1 User Account Overview

In the **User Account** screen, you can view the settings of the "admin" that you use to log into the Zyxel Device to manage it.

36.2 User Account

Click **Maintenance** > **User Account** to open the following screen. Use this screen to create and manage user accounts and their privileges on the Zyxel Device.

Figure 266 Maintenance > User Account



The following table describes the labels in this screen.

Table 182 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account (up to four **Administrator** accounts and four **User** accounts).
#	This is the index number.
Active	This indicates whether the user account is active or not. The checkbox is selected when the user account is enabled. It is cleared when it is disabled.
User Name	This displays the name of the account used to log into the Zyxel Device Web Configurator.
Retry Times	This displays the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	This displays the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	This field displays the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.

Table 182 Maintenance > User Account (continued)

LABEL	DESCRIPTION
Group	This field displays this user has **Administrator** privileges.
Remote Privilege	This field displays whether this user can access the Zyxel Device with HTTP, Telnet or SSH through the **WAN**, **LAN** or **LAN/WAN**.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Cancel	Click **Cancel** to restore your previously saved settings.
Apply	Click **Apply** to save your changes.

36.2.1 User Account Add or Edit

Add or change the name of the user account, set the security password and the retry times, and whether this user will have **Administrator** or **User** privileges. Click **Add New Account** or the **Edit** icon of an existing account in the **Maintenance** > **User Account** to open the following screen.

Figure 267 Maintenance > User Account: Add

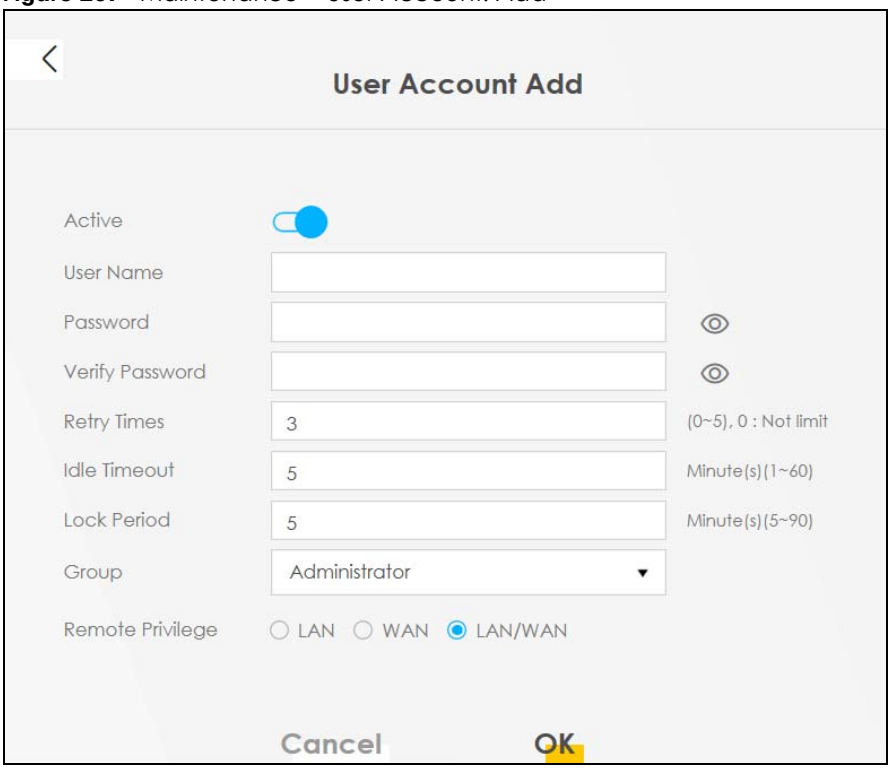
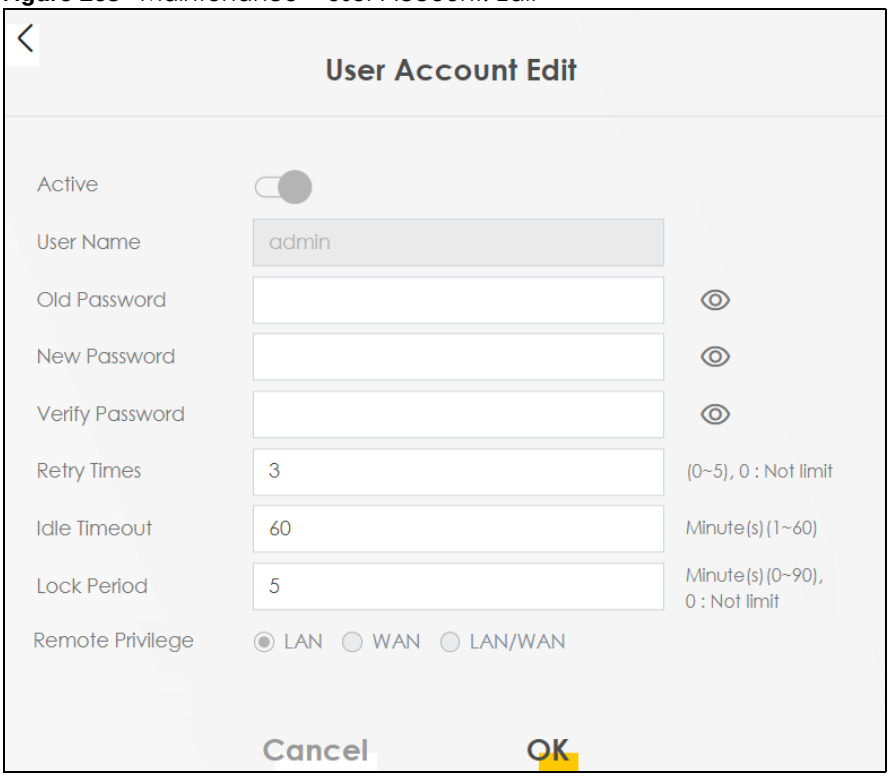


Figure 268 Maintenance > User Account: Edit



The following table describes the labels in this screen.

Table 183 Maintenance > User Account > User Account Add/Edit

LABEL	DESCRIPTION
Active	Click to enable (switch turns blue) or disable (switch turns gray) to activate or deactivate the user account.
User Name	Enter a name for this account. You can use up to 31 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed.
Password	Enter your new system password. The password must contain at least one numeric and one alphabetic character. You can use 6 – 64 alphanumeric (0-9, a-z, A-Z) and special characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Zyxel Device. If you are changing your existing password, you have to first enter your **Old Password** then enter your **New Password**.
Verify Password	Enter the new password again for confirmation.
Retry Times	Enter the number of times consecutive wrong passwords can be entered for this account. 0 means there is no limit.
Idle Timeout	Enter the length of inactive time before the Zyxel Device will automatically log the user out of the Web Configurator.
Lock Period	Enter the length of time a user must wait before attempting to log in again after a number of consecutive wrong passwords have been entered as defined in **Retry Times**.

Table 183 Maintenance > User Account > User Account Add/Edit (continued)

LABEL	DESCRIPTION
Group	Specify whether this user will have **Administrator** or **User** privileges. An **Administrator** account can access all Web Configurator menus. A **User** account can only access **Monitor** and **Maintenance** menus. The maximum account number of **Administrator** and **User** are both four. The total number of the users allowed to log in the Zyxel Device at the same time is eight. **The Administrator** privileges are the following: • **Quick Start** setup. • The following screens are visible for setup: **Broadband**, **Wireless**, **Home Networking**, **Routing**, **NAT**, **DNS**, **Firewall**, **MAC Filter**, **Voice, Log**, **Traffic Status**, **ARP Table**, **Routing Table**, **Cellular WAN Status**, **System**, **User Account**, **Remote Management**, **Time**, **Email Notification**, **Log Setting**, **Firmware Upgrade**, **Backup/Restore**, **Reboot**, **Diagnostic**. **The User** privileges are the following: • The following screens are visible for setup: **Log, Traffic Status**, **ARP Table**, **Routing Table**, **Cellular WAN Status**, **User Account**, **Remote Management**, **Time**, **Email Notification**, **Log Setting**, **Firmware Upgrade**, **Backup/Restore**, **Reboot**, **Diagnostic**.
Remote Privilege	Select whether this user can access the Zyxel Device with HTTP, Telnet or SSH through the **WAN**, **LAN** or **LAN/WAN**. Only the **Administrator** is allowed to use Telnet and SSH for remote management.
Cancel	Click **Cancel** to restore your previously saved settings.
OK	Click **OK** to save your changes.

CHAPTER 37
Remote Management

37.1 Remote Management Overview

Remote management controls through which interfaces, which web services (such as HTTPS, SSH, SNMP, and Ping) can access the Zyxel Device.

Note: The Zyxel Device is managed using the Web Configurator.

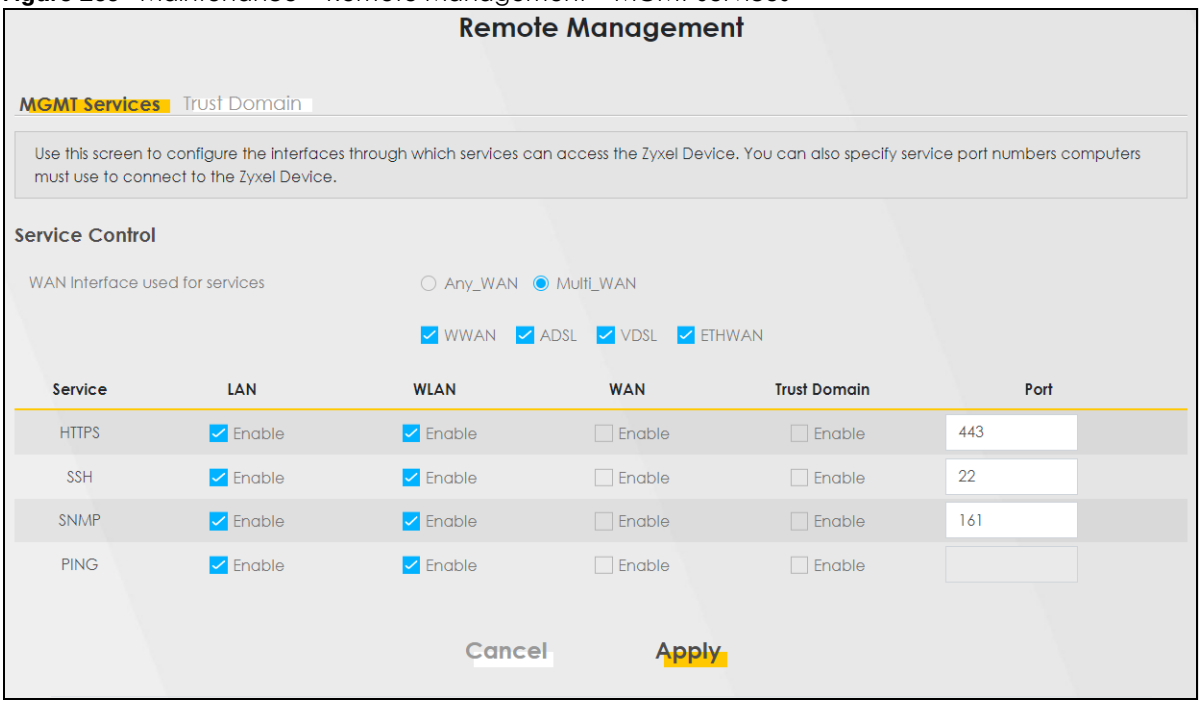
37.1.1 What You Can Do in this Chapter

- Use the **MGMT Services** screen to allow various approaches to access the Zyxel Device remotely from a WAN and/or LAN connection (Section 37.2 on page 479).
- Use the **Trust Domain** screen to enable users to permit access from local management services by entering specific IP addresses (Section 37.3 on page 481).

37.2 MGMT Services

Use this screen to configure the interfaces through which services can access the Zyxel Device. You can also specify service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance** > **Remote Management** > **MGMT Services** to open the following screen.

Figure 269 Maintenance > Remote Management > MGMT Services



The following table describes the fields in this screen.

Table 184 Maintenance > Remote Management > MGMT Services

LABEL	DESCRIPTION
Service Control	
WAN Interface used for services	Select **Any_WAN** to have the Zyxel Device automatically activate the remote management service when any WAN connection is up. Select **Multi_WAN** and then select one or more WAN connections to have the Zyxel Device activate the remote management service when the selected WAN connections are up.
WWAN	Enable the WWAN (cellular) connection configured in **Network Setting** > **Broadband** > **Cellular Backup** to access the service on the Zyxel Device.
ETHWAN	Enable the Ethernet WAN connection configured in **Network Setting** > **Broadband** > **Ethernet WAN** to access the service on the Zyxel Device.
ADSL	Enable the ADSL connection configured in **Network Setting** > **Broadband** > **Add New WAN Interface** or **Modify** to access the service on the Zyxel Device.
VDSL	Enable the VDSL WAN connection configured in **Network Setting** > **Broadband** > **Add New WAN Interface** or **Modify** to access the service on the Zyxel Device.
GPON	Enable the Gigabit Ethernet Passive Optical Network WAN connection configured in **Network Setting** > **Broadband** > **Add New WAN Interface** or **Modify** to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the LAN.
WLAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the WLAN.
WAN	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the **Enable** checkbox for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.

Table 184 Maintenance > Remote Management > MGMT Services (continued)

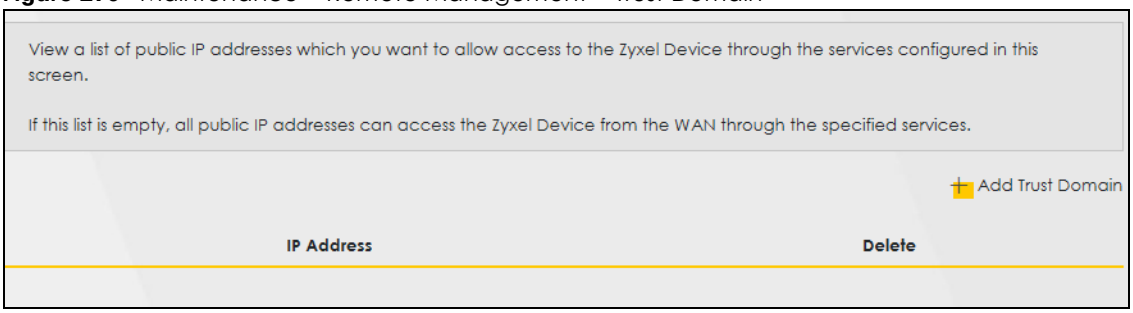
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Redirect	To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server. For example, if you enter http://192.168.1.1 in your browser to access the Web Configurator, then the Zyxel Device will automatically change this to the more secure https://192.168.1.1 for access.
Apply	Click **Apply** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

37.3 Trust Domain

Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the **Maintenance** > **Remote Management** > **MGMT Services** screen. Click **Maintenance** > **Remote Management** > **Trust Domain** to open the following screen.

Note: Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Figure 270 Maintenance > Remote Management > Trust Domain



The following table describes the fields in this screen.

Table 185 Maintenance > Remote Management > Trust Domain

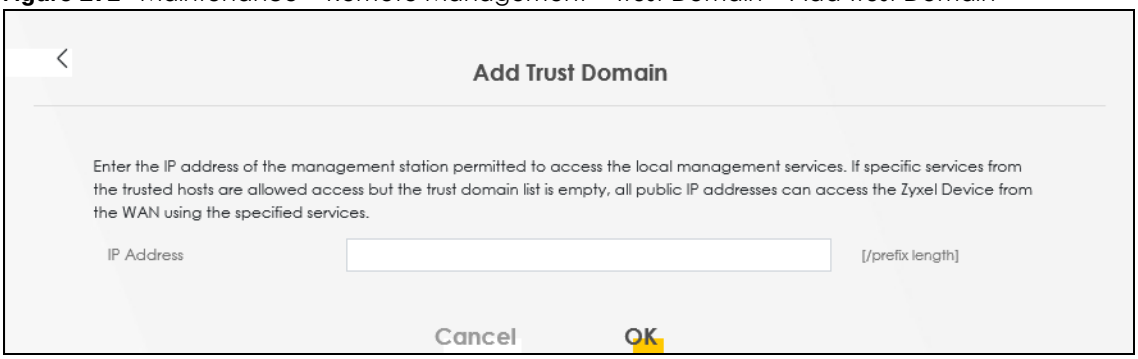
LABEL	DESCRIPTION
Add Trust Domain	Click this to add a trusted host IP address.
IP Address	This field shows a trusted host IP address.
Delete	Click the **Delete** icon to remove the trusted host IP address.

37.3.1 Add Trust Domain

Use this screen to add a public IP addresses or a complete domain name of a device which is allowed to access the Zyxel Device. Enter the IP address of the management station permitted to access the local management services. If specific services from the trusted-hosts are allowed access but the trust domain list is empty, all public IP addresses can access the Zyxel Device from the WAN using the specified services.

Click the **Add Trust Domain** button in the **Maintenance** > **Remote Management** > **Trust Domain** screen to open the following screen.

Figure 271 Maintenance > Remote Management > Trust Domain > Add Trust Domain



The following table describes the fields in this screen.

Table 186 Maintenance > Remote Management > Trust Domain > Add Trust Domain

LABEL	DESCRIPTION
IP Address	Enter a public IPv4/IPv6 IP address which is allowed to access the service on the Zyxel Device from the WAN.
OK	Click **OK** to save your changes back to the Zyxel Device.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 38
Power Monitor

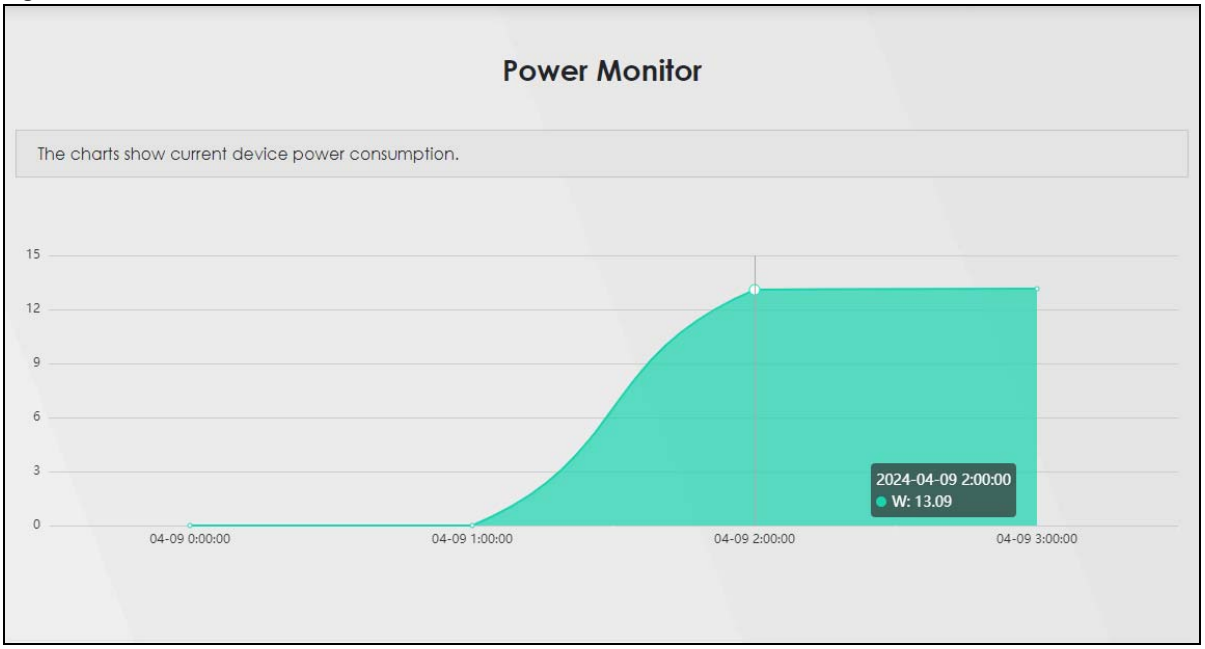
38.1 Power Monitor Overview

This chapter explains how to monitor the power consumption of the Zyxel Device.

38.2 Power Monitoring

Click **Maintenance** > **Power Monitor** to open the following screen. Use this screen to view the current and past amount of power consumed by the Zyxel Device.

Figure 272 Maintenance > Power Monitor



The following table describes the fields in this screen.

Table 187 Maintenance > Power Monitor

LEGEND	DESCRIPTION
Y-axis	The y-axis shows the amount of power consumed by the Zyxel Device in watts.
X-axis	The x-axis shows the period over which the power consumption is recorded. The maximum period for recording is 48 hours. After 48 hours, the power consumption data wraps around and new ones replace the earliest ones.

Note: The power consumption data is lost when you turn off the power to your Zyxel Device or when the Zyxel Device is reset to its factory default setting.

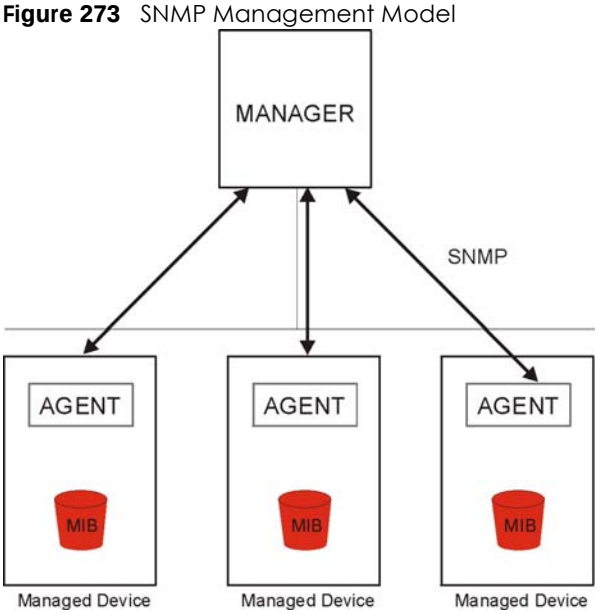
CHAPTER 39
SNMP

39.1 SNMP Overview

This chapter explains how to configure the SNMP settings on the Zyxel Device.

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Zyxel Device supports SNMP agent functionality, which allows a manager station to manage and monitor the Zyxel Device through the network. The Zyxel Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 273 SNMP Management Model



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

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

The managed devices contain object variables or managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status, and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

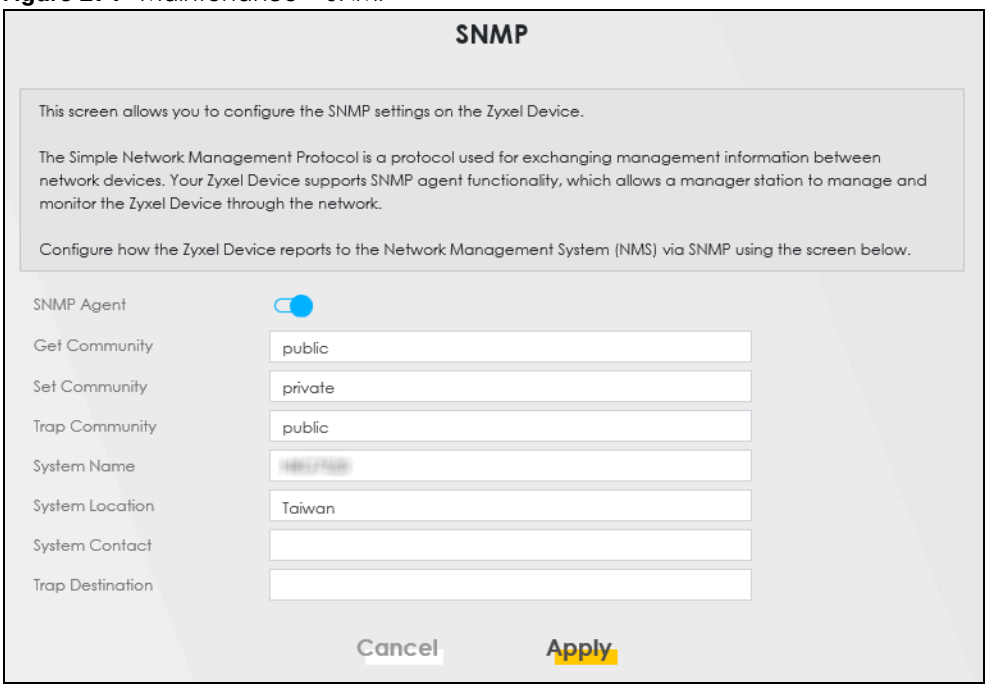
SNMP itself is a simple request/response protocol based on the manager or agent model. The manager issues a request and the agent returns responses using the following protocol operations:

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

39.2 SNMP Settings

Click **Maintenance** > **SNMP** to open the following screen. Use this screen to configure the Zyxel Device SNMP settings.

Figure 274 Maintenance > SNMP



The following table describes the fields in this screen.

Table 188 Maintenance > SNMP

LABEL	DESCRIPTION
SNMP Agent	Click the switch (turns blue) to let the Zyxel Device act as an SNMP agent, which allows a manager station to manage and monitor the Zyxel Device through the network. Otherwise, click the switch (turns gray) to turn this feature off.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station.
Trap Community	Enter the **Trap Community**, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.

Table 188 Maintenance > SNMP (continued)

LABEL	DESCRIPTION
System Contact	Enter the SNMP system contact.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click this to save your changes back to the Zyxel Device.
Cancel	Click this to restore your previously saved settings.

CHAPTER 40
Time Settings

40.1 Time Settings Overview

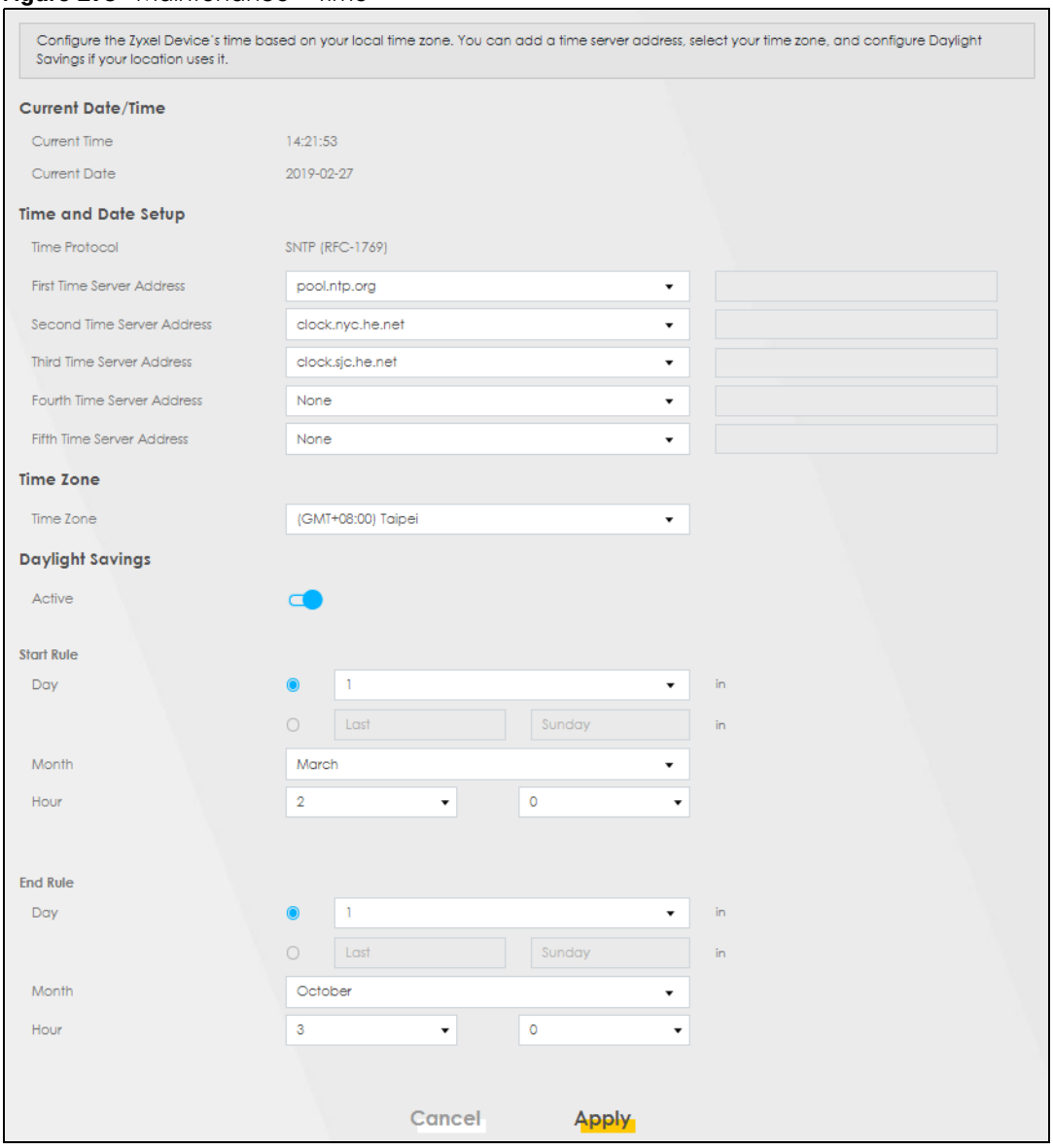
This chapter shows you how to configure system related settings, such as system date and time.

40.2 Time

For effective scheduling and logging, the Zyxel Device system time must be accurate. Use this screen to configure the Zyxel Device's time based on your local time zone. You can enter a time server address, select the time zone where the Zyxel Device is physically located, and configure Daylight Savings settings if needed.

To change your Zyxel Device's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 275 Maintenance > Time



The following table describes the fields in this screen.

Table 189 Maintenance > Time

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This displays the time of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the time with the time server.
Current Date	This displays the date of your Zyxel Device. Each time you reload this screen, the Zyxel Device synchronizes the date with the time server.
Time and Date Setup	
Time Protocol	This displays the time protocol used by your Zyxel Device.

Table 189 Maintenance > Time (continued)

LABEL	DESCRIPTION
First – Fifth Time Server Address	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 printable characters in length) of your time server. Select **None** if you do not want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.	
Active	Click this switch to enable or disable Daylight Saving Time. When the switch turns blue, the function is enabled. Otherwise, it is not.
Start Rule	Configure the day and time when Daylight Saving Time starts if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States, set the day to **Second**, **Sunday**, the month to **March** and the time to **2** in the **Hour** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday** and the month to **March**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Rule	Configure the day and time when Daylight Saving Time ends if you enabled Daylight Saving. You can select a specific date in a particular month or a specific day of a specific week in a particular month. The **Time** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would set the day to **First**, **Sunday**, the month to **November** and the time to **2** in the **Hour** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would set the day to **Last**, **Sunday**, and the month to **October**. The time you select in the **o'clock** field depends on your time zone. In Germany for instance, you would select **2** in the **Hour** field because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Cancel	Click **Cancel** to exit this screen without saving.
Apply	Click **Apply** to save your changes.

CHAPTER 41
Email Notification

41.1 Email Notification Overview

A mail server is an application or a computer that can receive, forward and deliver email messages.

To have the Zyxel Device send reports, logs or notifications through email, you must specify an email server and the email addresses of the sender and receiver.

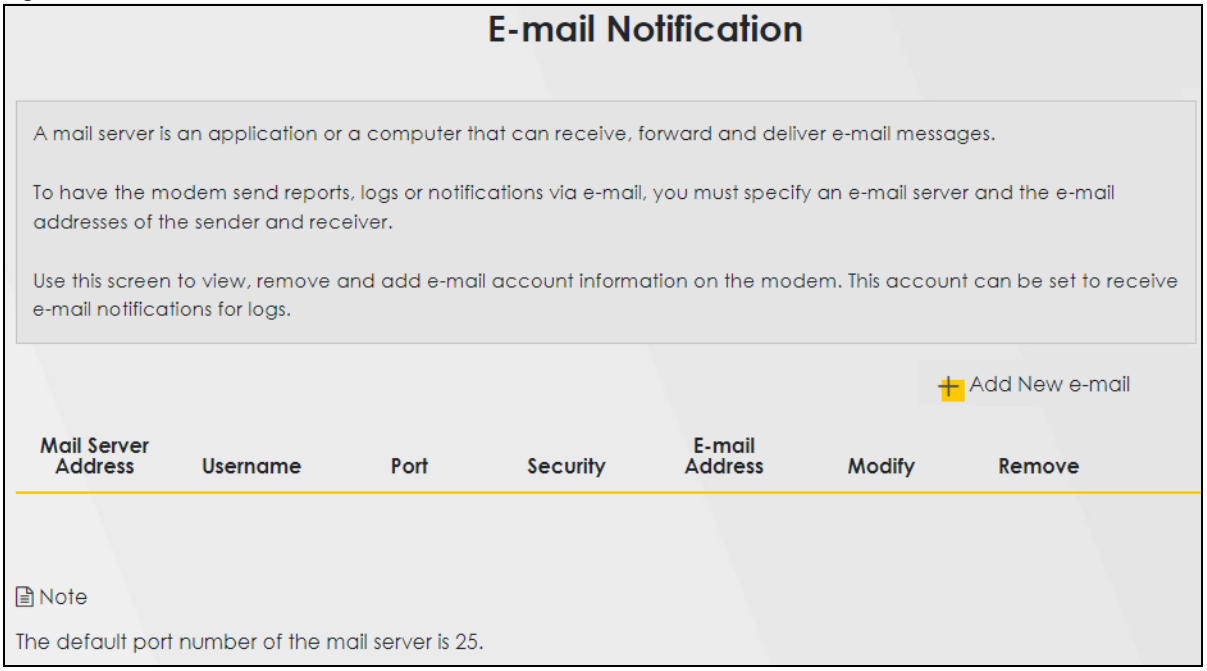
41.2 Email Notification

Use this screen to view, remove and add email account information on the Zyxel Device. This account can be set to send email notifications for logs.

Click **Maintenance** > **E-mail Notification** to open the **E-mail Notification** screen.

Note: The default port number of the mail server is 25.

Figure 276 Maintenance > E-mail Notification



The following table describes the labels in this screen.

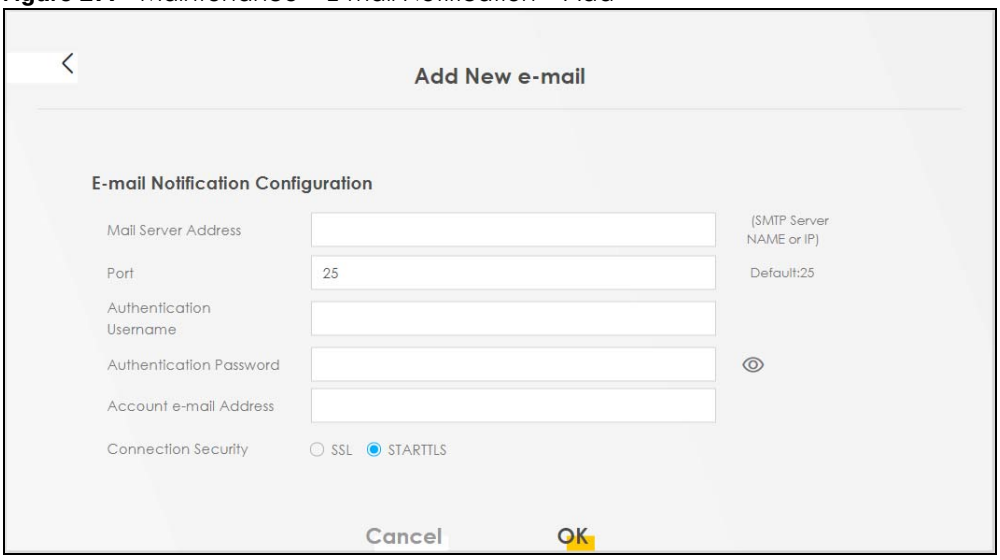
Table 190 Maintenance > E-mail Notification

LABEL	DESCRIPTION
Add New e-mail	Click this button to create a new entry (up to 32 can be created).
Mail Server Address	This displays the server name or the IP address of the mail server.
Username	This displays the user name of the sender's mail account.
Port	This field displays the port number of the mail server.
Security	This field displays the protocol used for encryption.
E-mail Address	This field displays the email address that you want to be in the from or sender line of the email that the Zyxel Device sends.
Modify	Click the **Edit** icon to configure the entry. Click the **Delete** icon to remove the entry.
Remove	Click this button to delete the selected entries.

41.2.1 E-mail Notification Edit

Click the **Add** button in the **E-mail Notification** screen. Use this screen to configure the required information for sending email through a mail server.

Figure 277 Maintenance > E-mail Notification > Add



The following table describes the labels in this screen.

Table 191 Maintenance > E-mail Notification > Add

LABEL	DESCRIPTION
Mail Server Address	Enter the server name or the IP address of the mail server for the email address specified in the **Account e-mail Address** field. If this field is left blank, reports, logs or notifications will not be sent through email.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Enter the user name. You can use up to 32 printable characters except ["], [`], ['], [<], [>], [^], [$], [|], [&], or [;]. Spaces are allowed. This is usually the user name of a mail account you specified in the **Account email Address** field.

Table 191 Maintenance > E-mail Notification > Add (continued)

LABEL	DESCRIPTION
Authentication Password	Enter the password associated with the user name above.
Account e-mail Address	Enter the email address that you want to be in the from or sender line of the email notification that the Zyxel Device sends. If you activate SSL/TLS authentication, the email address must be able to be authenticated by the mail server as well.
Connection Security	Select **SSL** to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) if you want encrypted communications between the mail server and the Zyxel Device. Select **STARTTLS** to upgrade a plain text connection to a secure connection using SSL/TLS.
Cancel	Click this button to begin configuring this screen afresh.
OK	Click this button to save your changes and return to the previous screen.

CHAPTER 42
Log Setting

42.1 Log Setting Overview

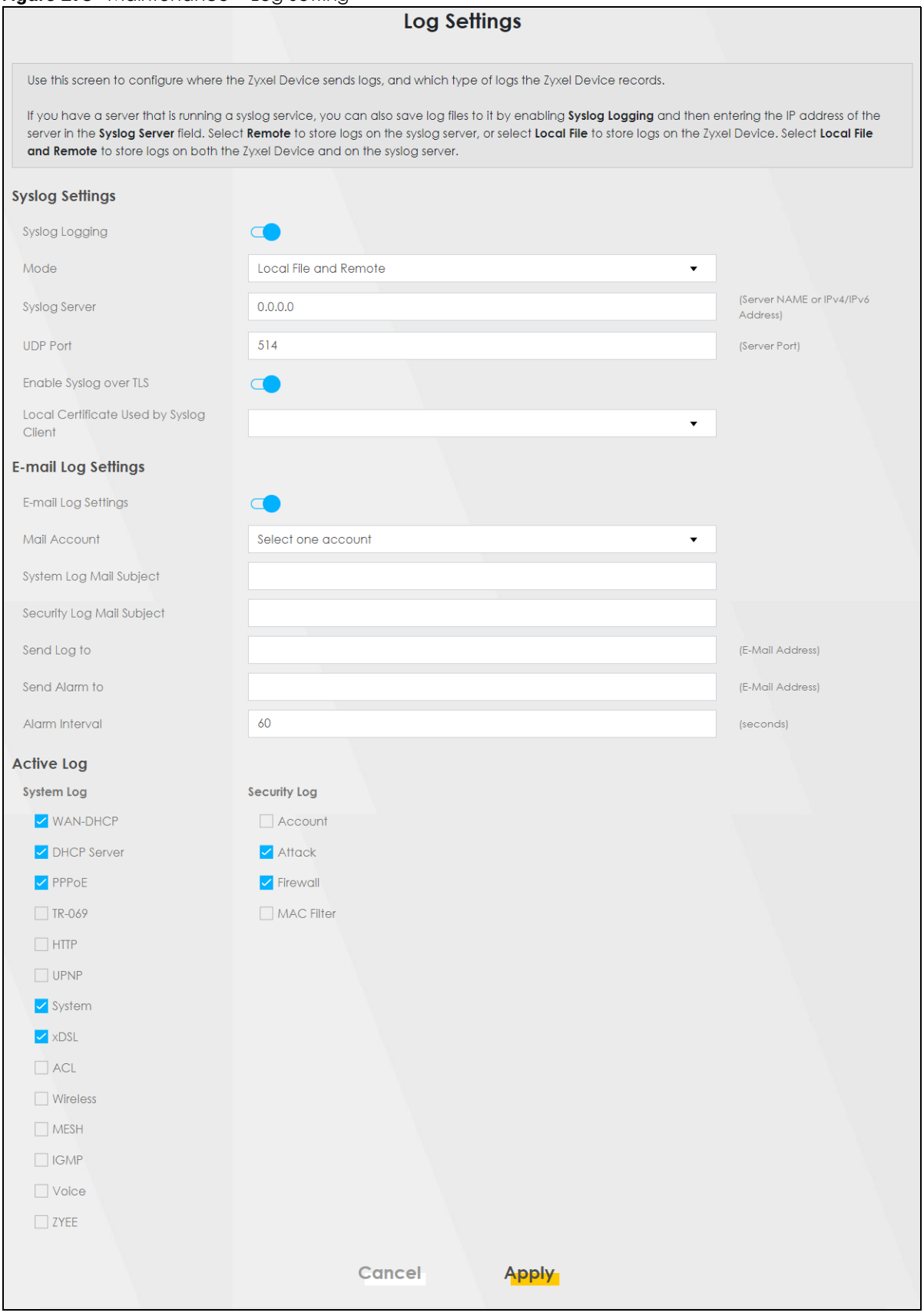
You can configure where the Zyxel Device sends logs and which type of logs the Zyxel Device records in the **Logs Setting** screen.

42.2 Log Setting

Use this screen to configure where the Zyxel Device sends logs, and which type of logs the Zyxel Device records.

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging**, and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the Zyxel Device. Select **Local File and Remote** to store logs on both the Zyxel Device and the syslog server. To change your Zyxel Device's log settings, click **Maintenance** > **Log Setting**. The screen appears as shown.

Figure 278 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 192 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Slide the switch to the right to enable syslog logging.
Mode	Select **Remote** to have the Zyxel Device send it to an external syslog server. Select **Local File** to have the Zyxel Device save the log file on the Zyxel Device itself. Select **Local File and Remote** to have the Zyxel Device save the log file on the Zyxel Device itself and send it to an external syslog server. Note: A warning appears upon selecting **Remote** or **Local File and Remote**. Just click **OK** to continue.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
Enable Syslog over TLS	Use **Syslog over TLS** to securely send logs from the Zyxel Device to the syslog server using TLS encryption. On the Zyxel Device, first generate a certificate for syslog authentication of the Zyxel Device. The CN (Certificate Name) must match the IP address of the Zyxel Device's interface to the syslog server. Go to **Certificates** > **Local CA** and import a certificate for syslog authentication. This is required.
Local Certificate Used by Syslog Client	Optionally, the Syslog server may also request a certificate from the Zyxel Device for mutual authentication. Go to **Certificates** > **Local Certificate** and import a Zyxel Device certificate that the syslog server can use to verify the Zyxel Device.
E-mail Log Settings	
E-mail Log Settings	Slide the switch to the right to allow the sending through email the system and security logs to the email address specified in **Send Log to**. Note: Make sure that the **Mail Server Address** field is not left blank in the **Maintenance** > **E-mail Notifications** screen.
Mail Account	Select a server specified in **Maintenance** > **E-mail Notifications** to send the logs to.
System Log Mail Subject	This field allows you to enter a descriptive name for the system log email (for example Zyxel System Log). Up to 127 printable characters are allowed for the **System Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Security Log Mail Subject	This field allows you to enter a descriptive name for the security log email (for example Zyxel Security Log). Up to 127 printable characters are allowed for the **Security Log Mail Subject** including special characters inside the square brackets [!#%()*+,–./:=?@[]\{}~].
Send Log to	This field allows you to enter the log's designated email recipient. The log's format is plain text file sent as an email attachment.
Send Alarm to	This field allows you to enter the alarm's designated e-mail recipient. The alarm's format is plain text file sent as an email attachment.
Alarm Interval	Select the frequency of showing of the alarm.
Active Log	
System Log	Select the categories of **System Log**s that you want to record.
Security Log	Select the categories of **Security Log**s that you want to record.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

42.2.1 Example Email Log

An 'End of Log' message displays for each mail in which a complete log has been sent. The following is an example of a log sent by email.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- '`End of Log`' message shows that a complete log has been sent.

Figure 279 Email Log Example

```
Subject:
        Firewall Alert From
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |

End of Firewall Log
```

CHAPTER 43
Firmware Upgrade

43.1 Firmware Upgrade Overview

This chapter explains how to upload new firmware to your Zyxel Device if you get new firmware releases from your service provider.

43.2 Firmware Upgrade

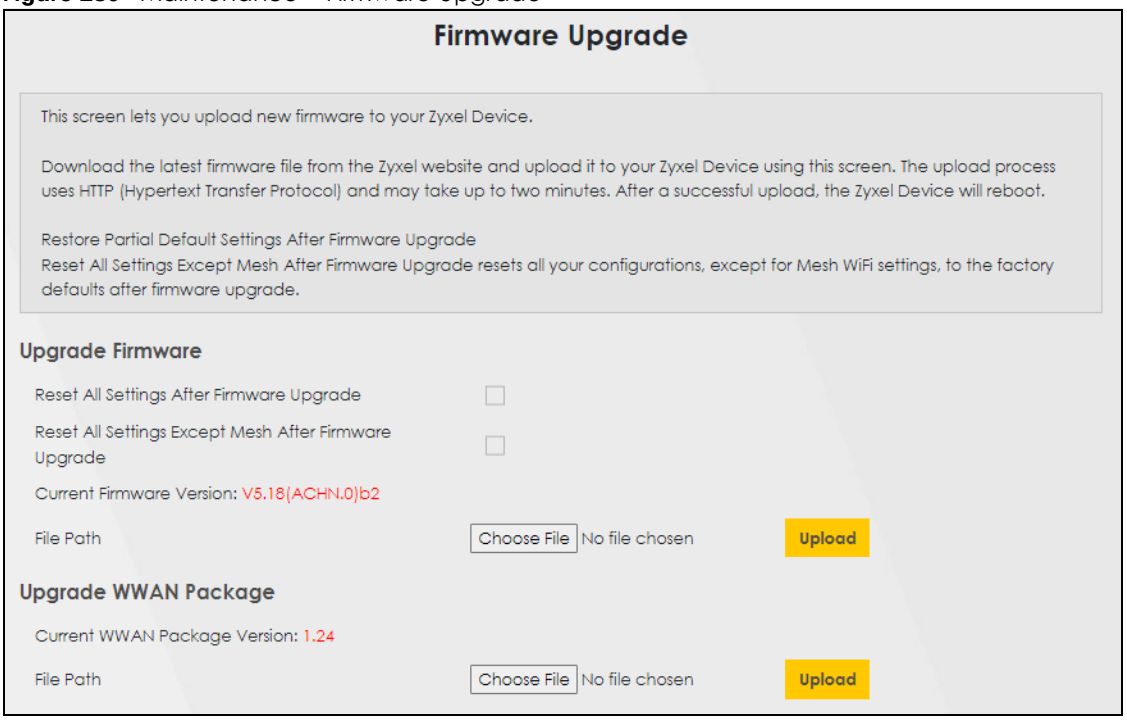
This screen lets you upload new firmware to your Zyxel Device.

Get the latest firmware from your service provider. Then upload the firmware file to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol). The upload may take up to 3 minutes. After a successful upload, the Zyxel Device will reboot.

Click **Maintenance** > **Firmware Upgrade** to open the **following** screen.

Do NOT turn off the Zyxel Device while firmware upload is in progress!

Figure 280 Maintenance > Firmware Upgrade



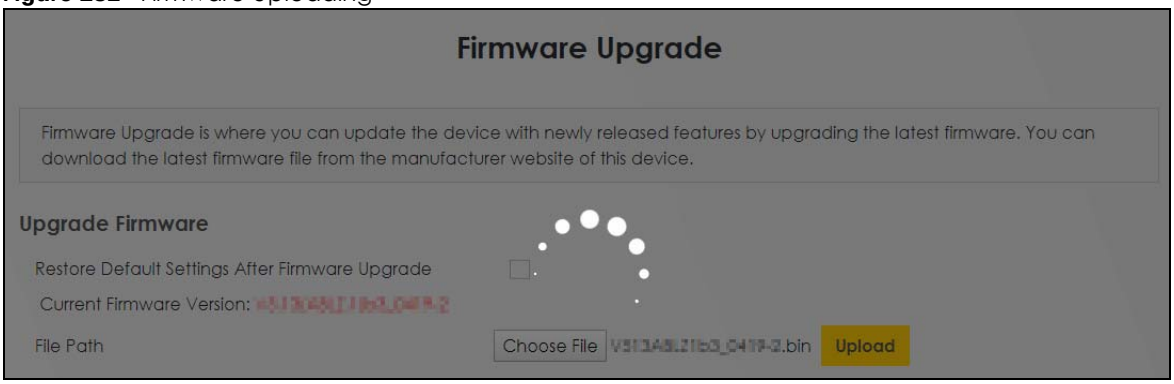
The following table describes the labels in this screen.

Table 193 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	
Restore Default Settings After Firmware Upgrade	Select this to reset all your configurations, including Mesh WiFi settings, to the factory defaults after firmware upgrade. Otherwise, make sure this is cleared if you do not want the Zyxel Device to lose all its current configurations and return to the factory defaults. Note: Make sure to back up the Zyxel Device's configuration settings first in case the reset all settings process is not successful.
Reset All Settings Except Mesh After Firmware Upgrade	Select this to reset all your configurations, except for Mesh WiFi settings, to the factory defaults after firmware upgrade. This minimizes interruption to your Mesh WiFi network after upgrading firmware. Mesh WiFi settings include: • Controller/Agent Mode • Mesh Internet Access • Main and Guest SSIDs including Guest WiFi isolation • 2.4GHz & 5GHz Radios • 802.11 Mode • Protected Management Frames • Encryption and WPA keys
Current Firmware Version	This is the current firmware version.
File Path	Enter the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it.
Choose File/ Browse	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to 3 minutes. Note: Only use firmware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device. For example, if the Zyxel Device's current firmware version is V5.70(ACDZ.0)B4, you must upload the firmware file containing "ACDZ".
Upgrade WWAN Package	
Current WWAN Package Version	This is the current version or the WWAN (Wireless Wide Area Network) package installed in the Zyxel Device. A WWAN package adds support for more 4G USB dongles without you having to upgrade the Zyxel Device's firmware.
File Path	Enter the location of the file you want to upload in this field or click **Choose File**/**Browse** to find it.
Choose File/ Browse	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to 3 minutes.

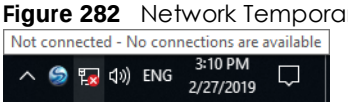
After you see the firmware updating screen, wait a few minutes before logging into the Zyxel Device again.

Figure 281 Firmware Uploading



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

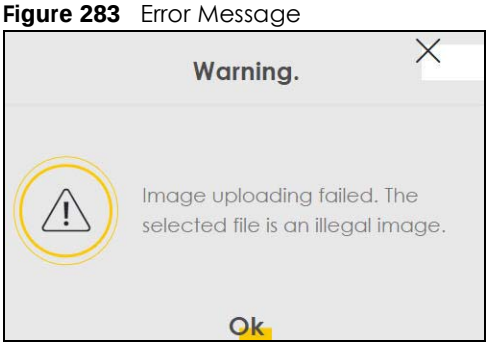
Figure 282 Network Temporarily Disconnected



After 2 minutes, log in again and check your new firmware version in the **Connection Status** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 283 Error Message



CHAPTER 44
Backup/Restore

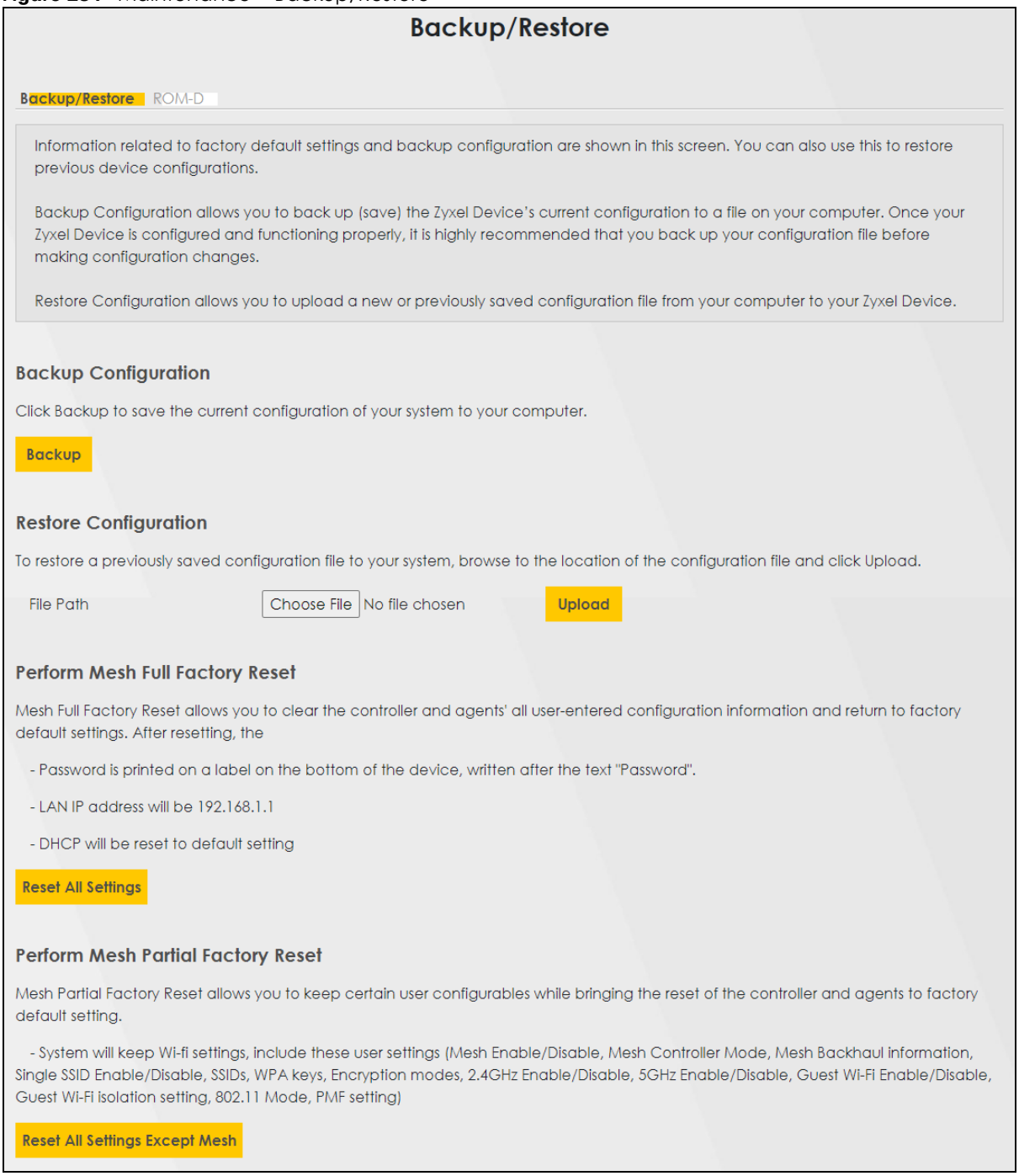
44.1 Backup/Restore Overview

Information related to factory default settings and backup configuration are shown in this screen. You can also use this to restore Zyxel Device's previous configurations.

44.2 Backup/Restore

Click **Maintenance** > **Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 284 Maintenance > Backup/Restore



Backup Configuration

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

Click **Backup** to save the Zyxel Device's current configuration to your computer.

Restore Configuration

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

Table 194 Maintenance > Backup/Restore: Restore Configuration

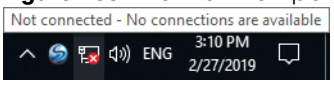
LABEL	DESCRIPTION
File Path	Enter in the location of the file you want to upload in this field or click **Choose File** / **Browse** to find it.
Choose File / Browse	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your Zyxel Device settings back to the factory default.

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

After the Zyxel Device configuration has been restored successfully, the login screen appears. Login again to restart the Zyxel Device.

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

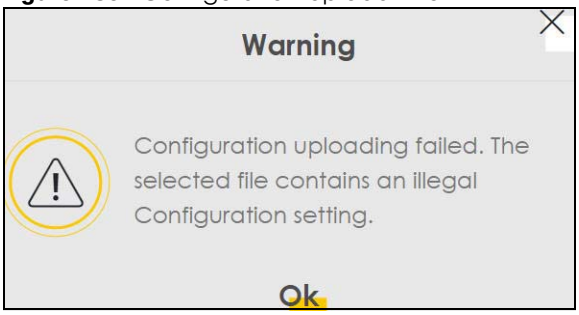
Figure 285 Network Temporarily Disconnected



If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default Zyxel Device IP address (192.168.1.1 – 192.168.225.225).

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 286 Configuration Upload Error

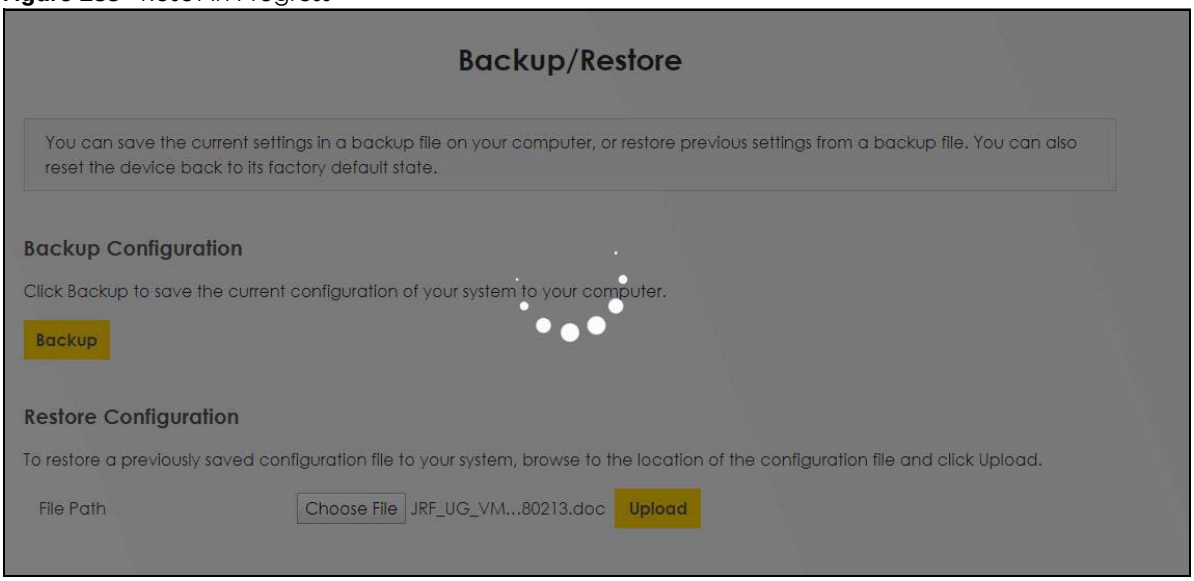


Back to Factory Default Settings

Click the **Reset All Settings** button to clear all user-entered configuration information and return the Zyxel Device to its factory defaults. The following warning screen appears.

Figure 287 Reset Warning Message

Figure 288 Reset In Progress



You can also press the **RESET** button on the panel to reset the factory defaults of your Zyxel Device.

Perform Partial Factory Reset

Click the **Reset All Settings Except Mesh** button to clear all user-entered configuration information and return the Zyxel Device to its factory defaults except for Mesh WiFi settings. The following warning screen appears.

Figure 289 Reset Warning Message

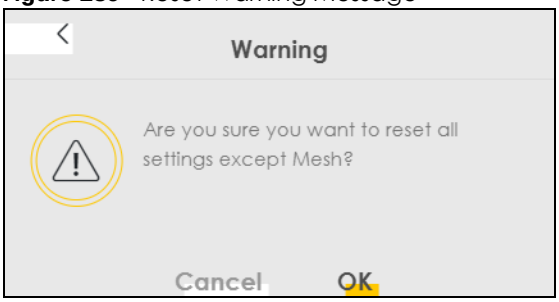
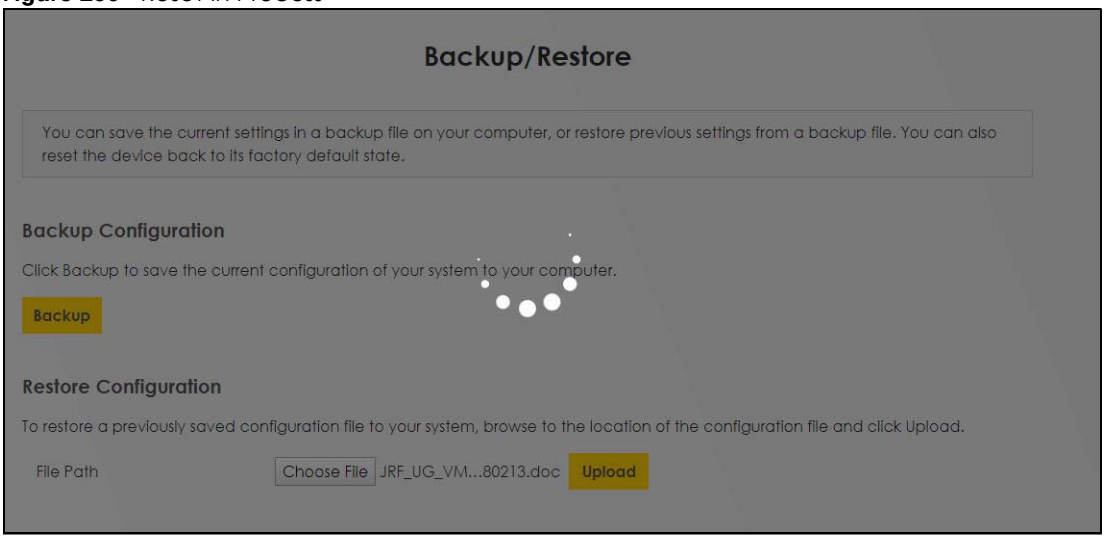


Figure 290 Reset In Process

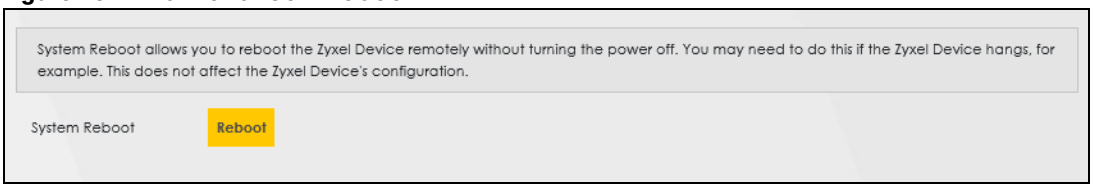


44.3 Reboot

System **Reboot** allows you to reboot the Zyxel Device remotely without turning the power off. You may need to do this if the Zyxel Device hangs, for example. This does not affect the Zyxel Device's configuration.

Click **Maintenance** > **Reboot**. Click **Reboot** to have the Zyxel Device reboot.

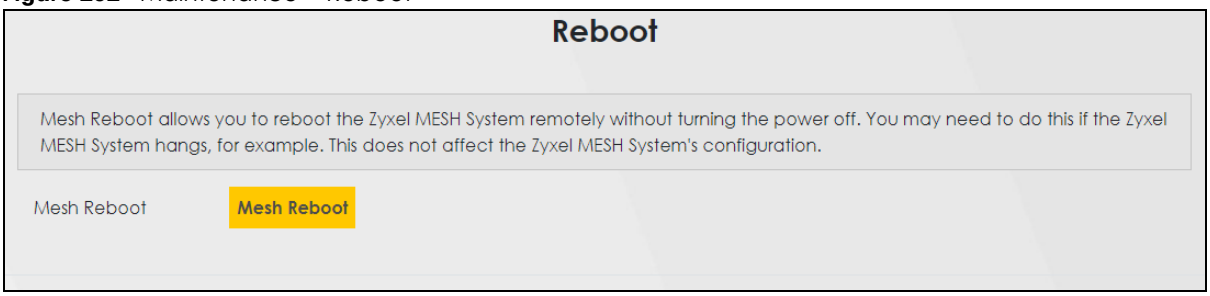
Figure 291 Maintenance > Reboot



Mesh Reboot allows you to reboot the Zyxel Mesh system remotely without turning the power off. You may need to do this if the Mesh system hangs, for example. This does not affect the Zyxel Mesh system's configuration.

Click **Maintenance** > **Reboot**. Click **Mesh Reboot** to have the Zyxel Mesh system reboot.

Figure 292 Maintenance > Reboot



CHAPTER 45
Diagnostic

45.1 Diagnostic Overview

The **Diagnostic** screen displays information to help you identify Internet connection problems with the Zyxel Device.

The route between an Ethernet switch and one of its Customer-Premises Equipment (CPE) may go through switches owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscriber's network access. In order to eliminate the management and maintenance efforts, IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults. Through discovery and verification of the path, CFM can detect, analyze and isolate connectivity faults in bridged LANs.

45.1.1 What You Can Do in this Chapter

- The **Ping&Traceroute&Nslookup** screen lets you ping an IP address or trace the route packets take to a host (Section 45.3 on page 506).
- The **802.1ag** screen lets you perform CFM actions (Section 45.4 on page 507).
- The **802.3ah** screen lets you configure link OAM port parameters (Section 45.5 on page 508).
- The **OAM Ping** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC (Section 45.6 on page 510).

45.2 What You Need to Know

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

How CFM Works

A Maintenance Association (MA) defines a VLAN and associated Maintenance End Point (MEP) ports on the device under a Maintenance Domain (MD) level. An MEP port has the ability to send Connectivity Check Messages (CCMs) and get other MEP ports information from neighbor devices' CCMs within an MA.

CFM provides two tests to discover connectivity faults.

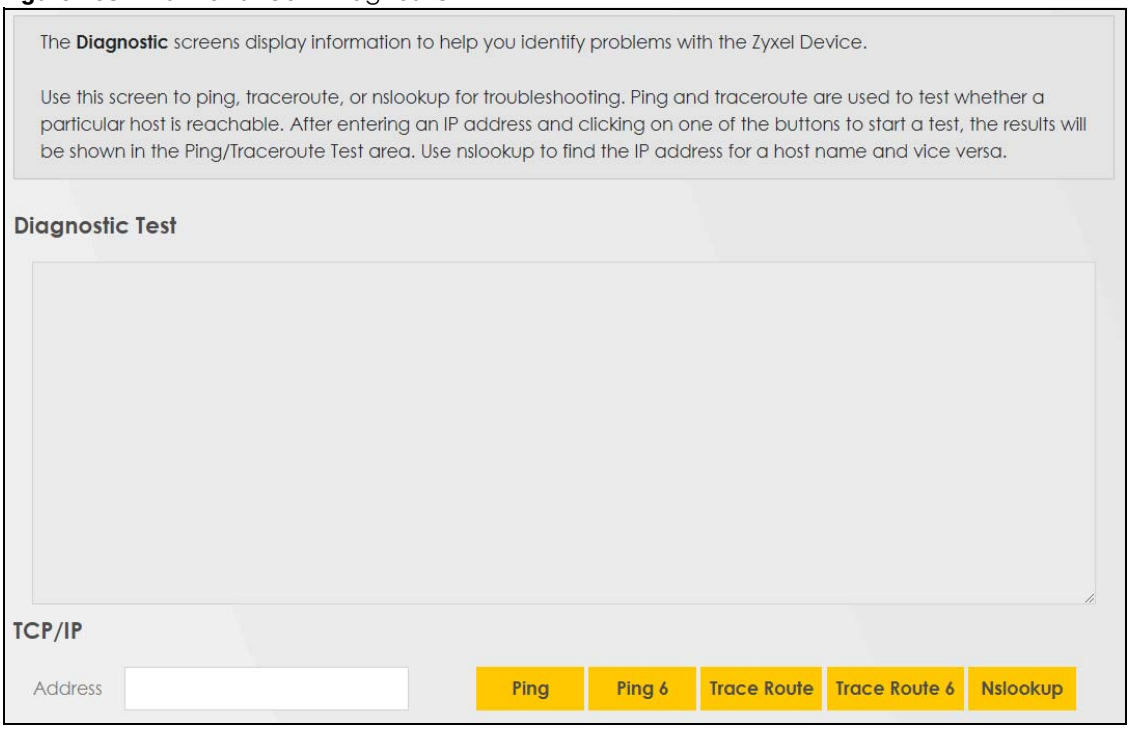
- Loopback test – checks if the MEP port receives its Loop Back Response (LBR) from its target after it sends the Loop Back Message (LBM). If no response is received, there might be a connectivity fault between them.
- Link trace test – provides additional connectivity fault analysis to get more information on where the fault is. If an MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

45.3 Diagnostic

Use this screen to ping, traceroute, nslookup, or speed test for troubleshooting. Ping and traceroute are used to test whether a particular host is reachable. After entering an IP address and clicking one of the buttons to start a test, the results will be shown in the screen. Use nslookup to find the IP address for a host name and the host name for an IP address. Use speed test to perform an upload and download throughput test for applications such as file transfer, web browsing and email.

Click **Maintenance** > **Diagnostic** to open the following screen.

Figure 293 Maintenance > Diagnostic



The following table describes the fields in this screen.

Table 195 Maintenance > Diagnostic

LABEL	DESCRIPTION
	The result of tests is shown here in the info area.
Select Test Method	
Ping	Select this to perform a ping test on the IPv4 address or host name in order to test a connection. The ping statistics will show in the info area.
Ping 6	Select this to perform a ping test on the IPv6 address or host name in order to test a connection. The ping statistics will show in the info area.
Trace Route	Select this to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Select this to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Select this to perform a DNS lookup on the IP address or host name.
TCP/IP	

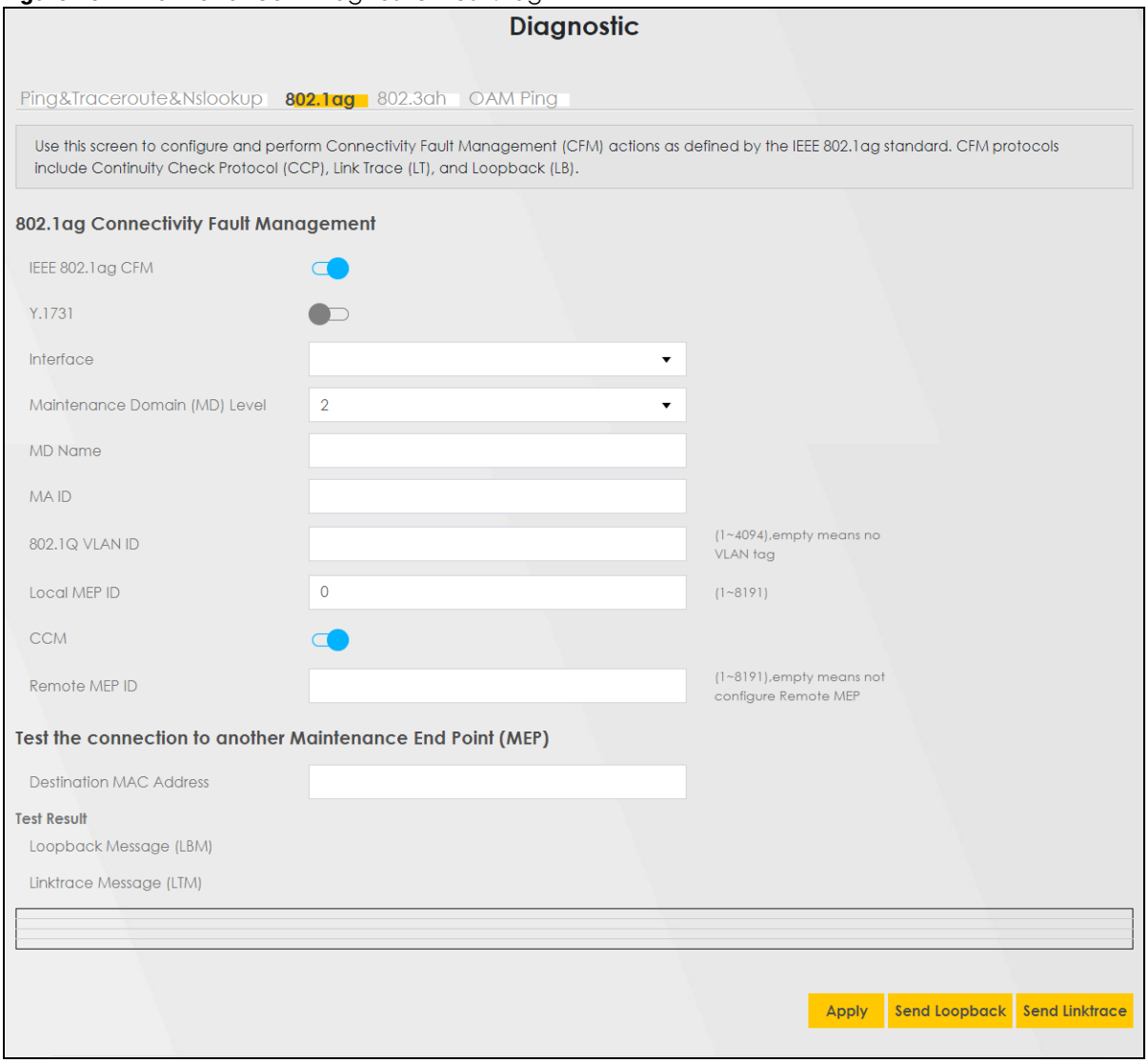
Table 195 Maintenance > Diagnostic (continued)

LABEL	DESCRIPTION
Address	Enter the IP address of a computer that you want to perform ping, trace route, nslookup, or speed test in order to test a connection.
Start Test	Click this to perform the selected test method.

45.4 802.1ag (CFM)

Click **Maintenance** > **Diagnostic** > **802.1ag** to open the following screen. Use this screen to configure and perform Connectivity Fault Management (CFM) actions as defined by the IEEE 802.1ag standard. CFM protocols include Continuity Check Protocol (CCP), Link Trace (LT), and Loopback (LB).

Figure 294 Maintenance > Diagnostic > 802.1ag



The following table describes the fields in this screen.

Table 196 Maintenance > Diagnostic > 802.1ag

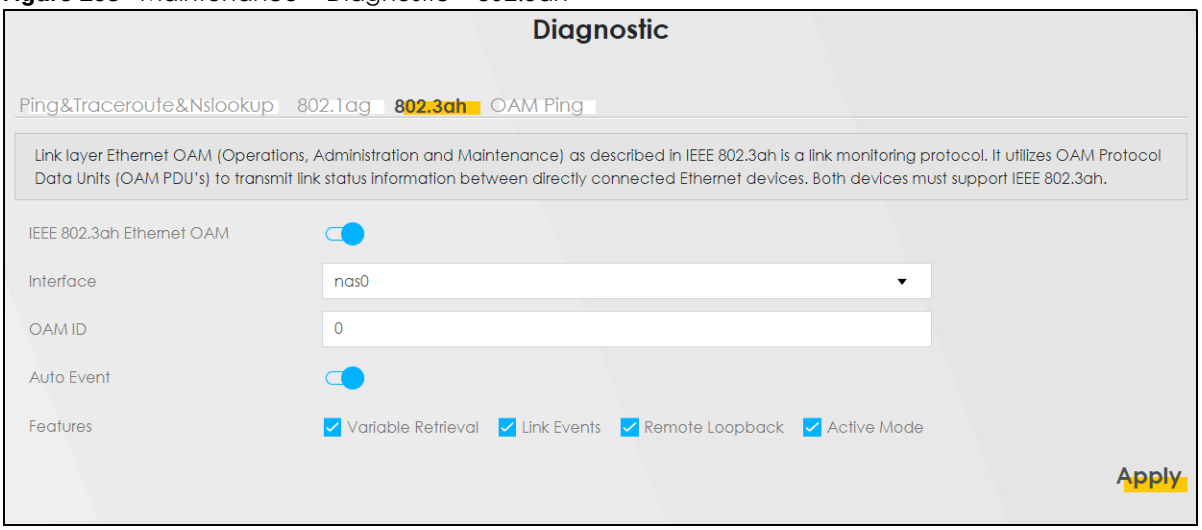
LABEL	DESCRIPTION
802.1ag Connectivity Fault Management	
IEEE 802.1ag CFM	Click this switch to enable or disable the IEEE802.1ag CFM specification, which allows network administrators to identify and manage connection faults. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Y.1731	Click this switch to enable or disable Y.1731, which monitors Ethernet performance. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEE 802.1ag CFM.
Maintenance Domain (MD) Level	Select a level (0 – 7) under which you want to create an MA.
MEG ID	Enter a descriptive name to identify the Maintenance Entity Group. This field only appears if the **Y.1731** field is enabled.
MD Name	Enter a descriptive name for the MD (Maintenance Domain). This field only appears if the **Y.1731** field is disabled.
MA ID	Enter a descriptive name to identify the Maintenance Association (MA). This field only appears if the **Y.1731** field is disabled.
MEG ID	Enter a descriptive name to identify the Maintenance Entity Group. This field only appears if the **Y.1731** field is enabled.
802.1Q VLAN ID	Enter a VLAN ID (1 – 4094) for this MA.
Local MEP ID	Enter the local Maintenance Endpoint Identifier (1 – 8191).
CCM	Click the switch to the right to continue sending MEP information by CCM (Connectivity Check Messages). When CCMs are received the Zyxel Device will always process it, whether **CCM** is enabled or not.
Remote MEP ID	Enter the remote Maintenance Endpoint Identifier (1 – 8191).
Test the connection to another Maintenance End Point (MEP)	
Destination MAC Address	Enter the target device's MAC address to which the Zyxel Device performs a CFM loopback and linktrace test.
Test Result	
Loopback Message (LBM)	This shows **Pass** if a Loop Back Messages (LBMs) responses are received. If LBMs do not get a response it shows **Fail**.
Linktrace Message (LTM)	This shows the MAC address of MEPs that respond to the LTMs.
Apply	Click this button to save your changes.
Send Loopback	Click this button to have the selected MEP send the LBM (Loop Back Message) to a specified remote end point.
Send Linktrace	Click this button to have the selected MEP send the LTMs (Link Trace Messages) to a specified remote end point.

45.5 802.3ah (OAM)

Click **Maintenance** > **Diagnostic** > **803.ah** to open the following screen. Link layer Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol.

It utilizes OAM Protocol Data Units (OAM PDU's) to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah.

Figure 295 Maintenance > Diagnostic > 802.3ah



The following table describes the labels in this screen.

Table 197 Maintenance > Diagnostics > 802.3ah

LABEL	DESCRIPTION
IEEE 802.3ah Ethernet OAM	Click this switch to enable or disable the Ethernet OAM on the specified interface. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Interface	Select the interface on which you want to enable the IEEE802.3ah.
OAM ID	Enter a positive integer to identify this node.
Auto Event	Click this switch to detect link status and send a notification when an error (such as errors in symbol, frames, or seconds) is detected. Otherwise, disable this and you will not be notified. When the switch goes to the right, the function is enabled. Otherwise, it is not.
Features	Select **Variable Retrieval** so the Zyxel Device can respond to requests for information, such as requests for Ethernet counters and statistics, about link events. Select **Link Events** so the Zyxel Device can interpret link events, such as link fault and dying asp.Link events are set in event notification PDUs (Protocol Data Units), and indicate when the number of errors in a certain given interval (time, number of frames, number of symbols, or number of error frame seconds) exceeds a specified threshold. Organizations may create organization-specific link event TLVs as well. Select **Remote Loopback** so the Zyxel Device can accept loopback control PDUs to convert Zyxel Device into loopback mode. Select **Active Mode** so the Zyxel Device initiates OAM discovery, send information PDUs; and may send event notification PDUs, variable request/response PDUs, or loopback control PDUs.
Apply	Click this button to save your changes.

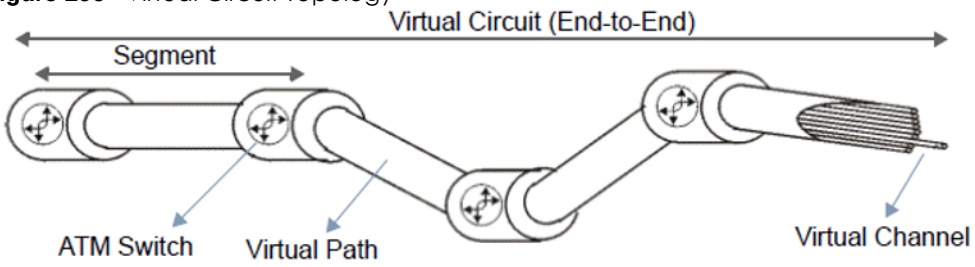
45.6 OAM Ping

Click **Maintenance** > **Diagnostic** > **OAM Ping** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The DX5301-B2/B3 sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the DX5301-B2/B3. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel (VC) Logical connections between ATM devices
- Virtual Path (VP) A bundle of virtual channels
- Virtual Circuits A series of virtual paths between circuit end points

Figure 296 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefined Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

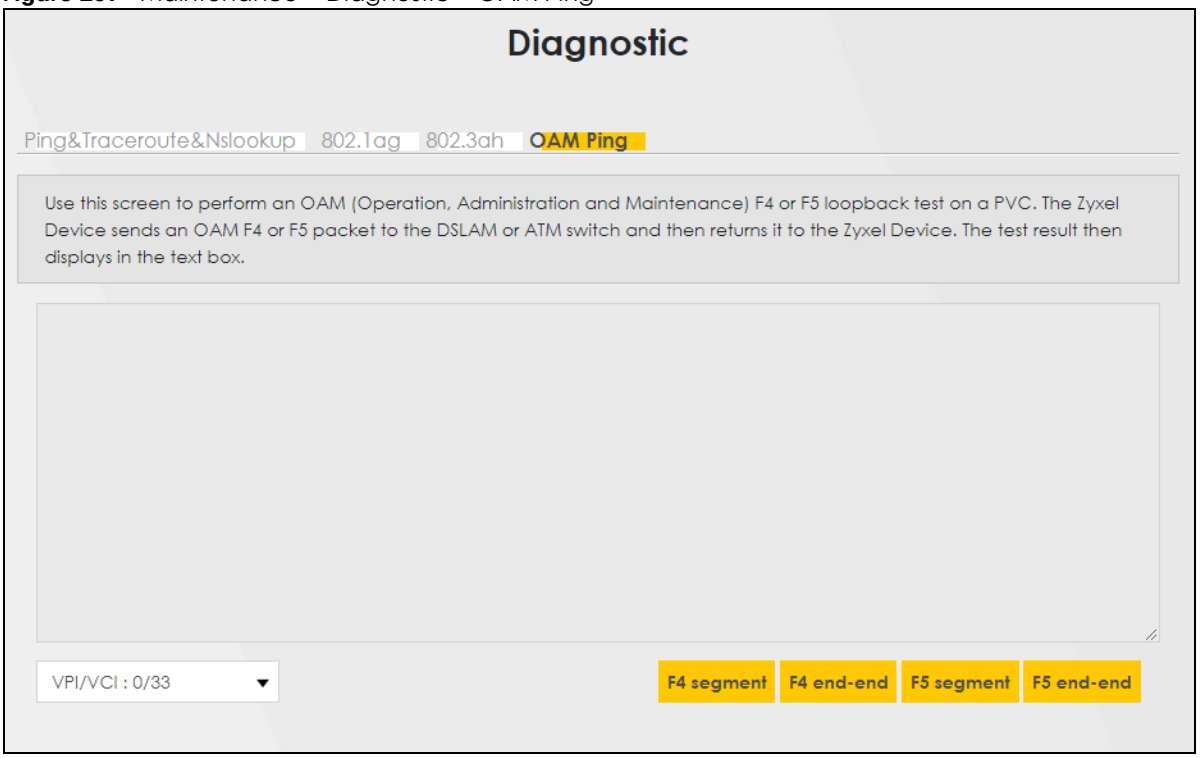
- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availability between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the DX5301-B2/B3 is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface using DX5301-B2/B3.

Figure 297 Maintenance > Diagnostic > OAM Ping



The following table describes the labels in this screen.

Table 198 Maintenance > Diagnostics > OAM Ping

LABEL	DESCRIPTION
Select a PVC on which you want to perform the loopback test.	
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

PART III
Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your Zyxel Device.

CHAPTER 46
Troubleshooting

46.1 Troubleshooting Overview

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

- Power and Hardware Problems
- Device Access Problems
- Internet Problems
- WiFi Problems
- USB Problems
- VoIP Problems
- UPnP Problems

46.2 Power and Hardware Problems

The Zyxel Device does not turn on.

1. Make sure you are using the power adapter included with the Zyxel Device.
2. Make sure the power adapter is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adapter to the Zyxel Device.
4. Make sure you have pressed the **POWER** button to turn on the Zyxel Device.
5. If the problem continues, contact the vendor.

The LED does not behave as expected.

1. Make sure you understand the normal behavior of the LED.
2. Check the hardware connections.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the Zyxel Device off and on.

5 If the problem continues, contact the vendor.

46.3 Device Access Problems

I do not know the IP address of the Zyxel Device.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address, you might be able to find the IP address of the Zyxel Device by looking up the IP address of your computer's default gateway. To do this in Microsoft Windows, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Zyxel Device, depending on your network environment.

3 If this does not work, reset the Zyxel Device to its factory defaults.

I forgot the admin password.

1 See the Zyxel Device label or this document's cover page for the default admin password.

2 If you changed the password from default and cannot remember the new one, you have to reset the Zyxel Device to its factory default settings.

I cannot access the Web Configurator login screen.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten the new address, see the troubleshooting suggestions for I do not know the IP address of the Zyxel Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.

4 Clear the Internet browser cache and try accessing the Web Configurator login screen again.

5 If it is possible to log in from another interface, check the service control settings for HTTP and HTTPS (**Maintenance** > **Remote Management**).

6 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address.

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

Advanced Suggestions

- Make sure you have logged out of any earlier management sessions using the same user account even if they were through a different interface or using a different browser.
- Try to access the Zyxel Device using another service, such as Telnet. If you can access the Zyxel Device, check the remote management settings and firewall rules to find out why the Zyxel Device does not respond to HTTP.

I cannot log into the Zyxel Device.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These both user name and password are case-sensitive, so make sure [Caps Lock] is not on.

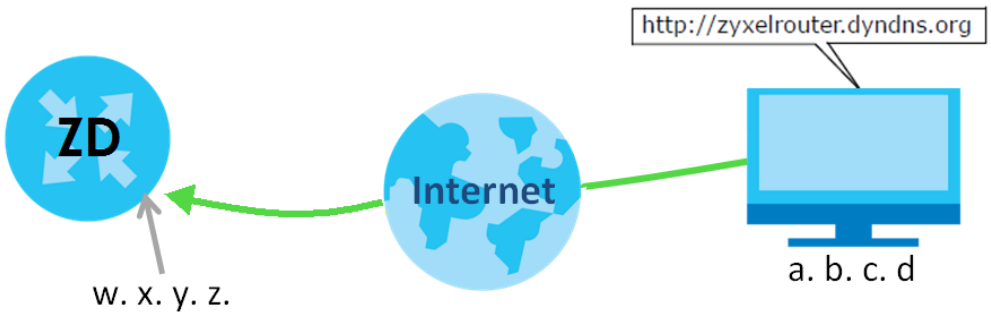
2 You cannot log in to the Web Configurator while someone is using Telnet to access the Zyxel Device. Log out of the Zyxel Device in the other session, or ask the person who is logged in to log out.

3 Turn the Zyxel Device off and on.

4 If this does not work, you have to reset the Zyxel Device to its factory default.

I cannot log into the Zyxel Device using DDNS.

If you connect your Zyxel Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the Zyxel Device from the Internet. The Zyxel Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the Zyxel Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

Note: If you have a private WAN IP address, then you cannot use DDNS.

Here are the three steps to use a domain name to log in the Web Configurator:

Step 1 Register for a DDNS Account on www.dyndns.org

1 Open a browser and enter **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**
- IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Status** page.

Then you will need to configure the same account and host name on the Zyxel Device later.

Step 2 Configure DDNS on Your Zyxel Device

Configure the following settings in the **Network Setting** > **DNS** > **Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **www.DynDNS.com** as the service provider.
- Enter **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**). Click **Apply**.

Step 3 Test the DDNS Setting

Now you should be able to access the Zyxel Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Enter **http://zyxelrouter.dyndns.org** and press [Enter].

3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

I cannot connect to the Zyxel Device using FTP, Telnet, SSH, or Ping.

1 See the Remote Management section for details on allowing web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) to access the Zyxel Device.

2 Check the server **Port** number field for the web service in the **Maintenance** > **Remote Management** screen. You must use the same port number in order to use that web service for remote management.

3 Try the troubleshooting suggestions for I cannot access the Web Configurator login screen. Ignore the suggestions about your browser.

The SIM card cannot be detected.

1. Disconnect the Zyxel Device from the power supply.
2. Remove the SIM card from its slot.
3. Clean the SIM card slot of any loose debris using compressed air.
4. Clean the gold connectors on the SIM card with a clean lint-free cloth.
5. Insert the SIM card into its slot and connect the Zyxel Device to the power supply to restart it.

I get an **Invalid** SIM card alert.

1. Make sure you have an active plan with your ISP.
2. Make sure that the Zyxel Device is in the coverage area of a cellular network.
3. Enable **Data Roaming** in **Network Setting** > **Broadband** > **Cellular WAN** to keep the Zyxel Device connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered, such as a different country. Then, restart the Zyxel Device.

1. Check the signal strength. Look at the LEDs, and check the LED section for more information. If the signal strength is low, try moving the Zyxel Device closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (such as microwaves, other wireless networks).
2. Select **Auto** in **Network Setting** > **Broadband** > **Cellular Band**: **Preferred Access Technology** and slide the switch to the right to enable **Band Auto Selection**.
3. Find the location of your nearest cellular base stations, then install the Zyxel Device towards the direction of those sites. The nearest site or site with a direct line-of-sight is usually preferred.

46.4 Internet Problems

I cannot access the Internet.

1. Check the hardware connections and make sure the LEDs are behaving as expected. See the **Quick Start Guide**.
2. Make sure you entered your ISP account information correctly on the **Network Setting** > **Broadband** screen. Fields on this screen are case-sensitive, so check if [Caps Lock] is on of off.

3 If you are trying to access the Internet wirelessly, make sure that you enabled the WiFi in the Zyxel Device and your WiFi client and that the WiFi settings in the WiFi client are the same as the settings in the Zyxel Device.

4 Disconnect all the cables from your Zyxel Device and reconnect them.

5 If the problem continues, contact your ISP.

I cannot connect to the Internet using an Ethernet connection.

1 Make sure you have the Ethernet WAN port connected to a Modem or Router.

2 Make sure you configured a proper Ethernet WAN interface (**Network Setting** > **Broadband** screen) with the Internet account information provided by your ISP and that it is enabled.

3 Check that the WAN interface you are connected to is in the same interface group as the Ethernet connection (**Network Setting** > **Interface Group**).

4 If you set up a WAN connection using bridging service, make sure you turn off the DHCP feature in the **Network Setting** > **Home Networking** > **LAN Setup** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot connect to the Internet using a Fiber connection.

1 Make sure the Fiber/SFP port has a compatible SFP/SFP+ transceiver installed with a fiber/Ethernet cable connected to it.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the **Quick Start Guide**.

The **PON** LED is off if the optical transceiver has malfunctioned or the fiber cable is not connected or is broken or damaged enough to break the PON connection.

The **LOS** LED is red if the GPON Device is not receiving an optical signal.

The **LOS** LED blinks red if the GPON Device is receiving a weak optical signal.

3 Disconnect all the cables from your device and reconnect them. Make sure the fiber cable is not curved too much.

4 If that does not work, restart your Zyxel Device.

5 If the problems continues, contact your ISP.

I cannot connect to the Internet using a cellular connection.

1 The DSL and Ethernet connections have priority in that order. If the DSL or Ethernet connection is up, then the cellular connection will be down.

2 Make sure you have connected a compatible cellular dongle to the USB port, if required.

3 Make sure you have configured **Network Setting** > **Broadband** > **Cellular Backup** correctly.

4 Check that the Zyxel Device is within range of a cellular base station.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. If the Zyxel Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 If your Zyxel Device keeps alternating between ISPs, then choose a fixed ISP. Go to the **Network Setting** > **Cellular PLMN** screen, disable **PLMN Auto Selection** and then choose your preferred ISP.

3 Turn the Zyxel Device off and on.

4 If the problem continues, contact the network administrator or vendor, or try the advanced suggestions in I cannot access the Web Configurator login screen.

Note: If your Zyxel Device is an outdoor-type, inclement weather like rain and hot weather may affect cellular signals.

46.5 WiFi Problems

I cannot connect to the Zyxel Device WiFi.

1 Check the WiFi LED status to make sure the Zyxel Device WiFi is on.

2 Make sure your WiFi client is within transmission range of the Zyxel Device.

3 Make sure you entered the correct SSID and password. See the Zyxel Device back label for the default SSID and password.

4 Make sure your WiFi client is using the same WiFi security type (WPA2-PSK, WPA3-SAE, or none) as the Zyxel Device.

5 Make sure the WiFi adapter on your WiFi client is working properly. Right-click your computer's network adapter then select **Properties** to check your network adapter status.

6 Make sure the WiFi adapter on your WiFi client is IEEE 802.11-compatible and supports the same WiFi standard as the Zyxel Device radio.

The WiFi connection is slow and intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your WiFi connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the WiFi client.
- Reduce the number of WiFi clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Place the Zyxel Device where there are minimum obstacles (such as walls and ceilings) between the Zyxel Device and the WiFi client. Avoid placing the Zyxel Device inside any type of box that might block WiFi signals.

46.6 USB Problems

The Zyxel Device fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the Zyxel Device.
3. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
4. Reconnect your USB device to the Zyxel Device.

46.7 VoIP Problems

I cannot make phone calls through the phone connected to the Zyxel Device.

1. Pick up the phone and check the phone tone. You should hear the dial tone if your configuration on the Zyxel Device is correct, and your phone is successfully connected to the SIP server.
2. Make sure your phone is connected to the Zyxel Device phone port through an RJ-11 cable. Check the Zyxel Device phone LED for the corresponding phone status.
3. Make sure the Zyxel Device has an Internet connection. See Section 46.4 on page 517 for more information.
4. Make sure your SIP account is registered and your SIP service plan is valid. Use the **System Monitor** > **VoIP Status** screen to check the account **Registration** status.
5. Make sure your SIP server settings (in the **VoIP** > **SIP** > **SIP Service Provider** and the **VoIP** > **SIP** > **SIP Account** screens) use the correct information from your SIP service provider. For example, your SIP service provider name, SIP account and password.
6. Make sure your phone settings (in the **VoIP** > **Phone** > **Phone Device** screen) are correct.
7. Contacting the SIP server administrator and make sure your SIP server isn't down.

46.8 UPnP Problems

My computer cannot detect UPnP settings from the Zyxel Device.

1. Make sure that UPnP is enabled in your computer.
2. On the Zyxel Device, make sure that UPnP is enabled on the **Network Settings** > **Home Networking** > **UPnP** screen.
3. Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.
4. Reconnect the Ethernet cable.
5. Restart your computer.

46.9 Getting More Troubleshooting Help

Search for support information for your model at *https://service-provider.zyxel.com/global/en/tech-support* and *community.zyxel.com* for more troubleshooting suggestions.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the Zyxel Device.

For Zyxel Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Kazakhstan
- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

Europe

Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria

- *https://www.zyxel.com/bg/bg*

Czech Republic

- Zyxel Communications Czech s.r.o.
- *https://www.zyxel.com/cz/cs*

Denmark

- Zyxel Communications A/S
- *https://www.zyxel.com/dk/da*

Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

France

- Zyxel France
- *https://www.zyxel.com/fr/fr*

Germany

- Zyxel Deutschland GmbH.
- *https://www.zyxel.com/de/de*

Hungary

- Zyxel Hungary & SEE
- *https://www.zyxel.com/hu/hu*

Italy

- Zyxel Communications Italy S.r.l.
- *https://www.zyxel.com/it/it*

Norway

- Zyxel Communications A/S
- *https://www.zyxel.com/no/no*

Poland

- Zyxel Communications Poland
- *https://www.zyxel.com/pl/pl*

Romania

- Zyxel Romania
- *https://www.zyxel.com/ro/ro*

Russian Federation

- Zyxel Communications Corp.
- https://www.zyxel.com/ru/ru

Slovakia

- Zyxel Slovakia
- https://www.zyxel.com/sk/sk

Spain

- Zyxel Iberia
- https://www.zyxel.com/es/es

Sweden

- Zyxel Communications A/S
- https://www.zyxel.com/se/sv

Switzerland

- Studerus AG
- https://www.zyxel.com/ch/de-ch
- https://www.zyxel.com/fr/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en-gb

Ukraine

- Zyxel Ukraine
- https://www.zyxel.com/ua/uk-ua

South America

Argentina

- Zyxel Communications Corp.
- https://www.zyxel.com/co/es-co

Brazil

- Zyxel Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX B
Wireless LANs

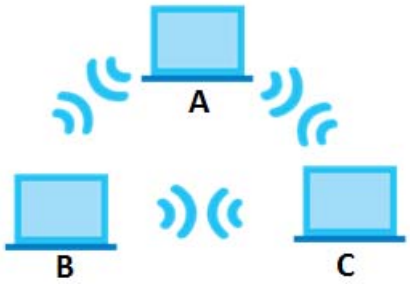
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 298 Peer-to-Peer Communication in an Ad-hoc Network

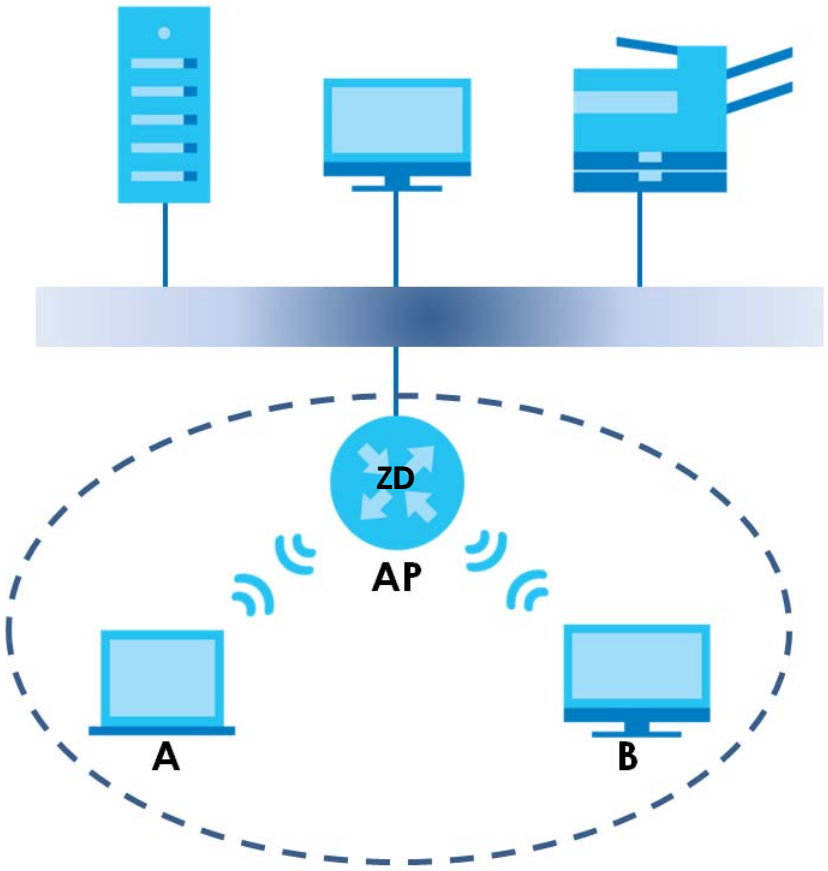


BSS

A Basic Service Set (BSS) exists when all communications between WiFi clients or between a WiFi client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between WiFi clients in the BSS. When Intra-BSS is enabled, WiFi client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, WiFi client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 299 Basic Service Set



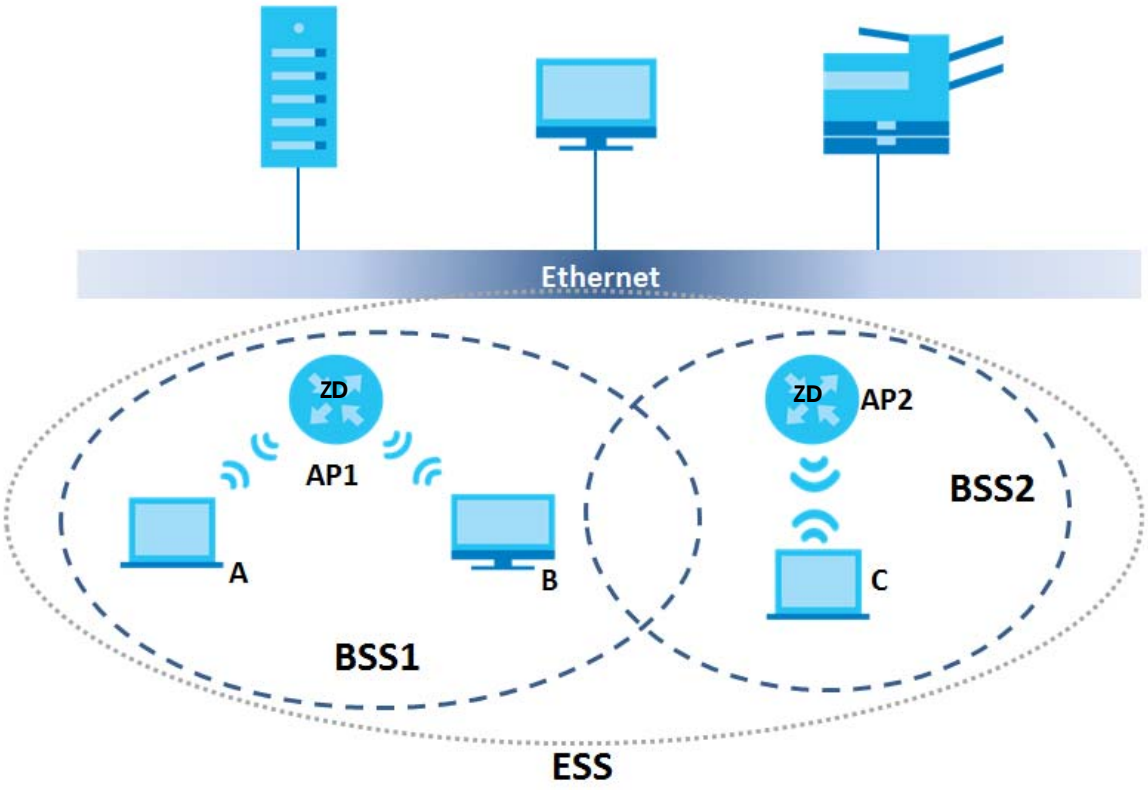
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated WiFi clients within the same ESS must have the same ESSID in order to communicate.

Figure 300 Infrastructure WLAN



Channel

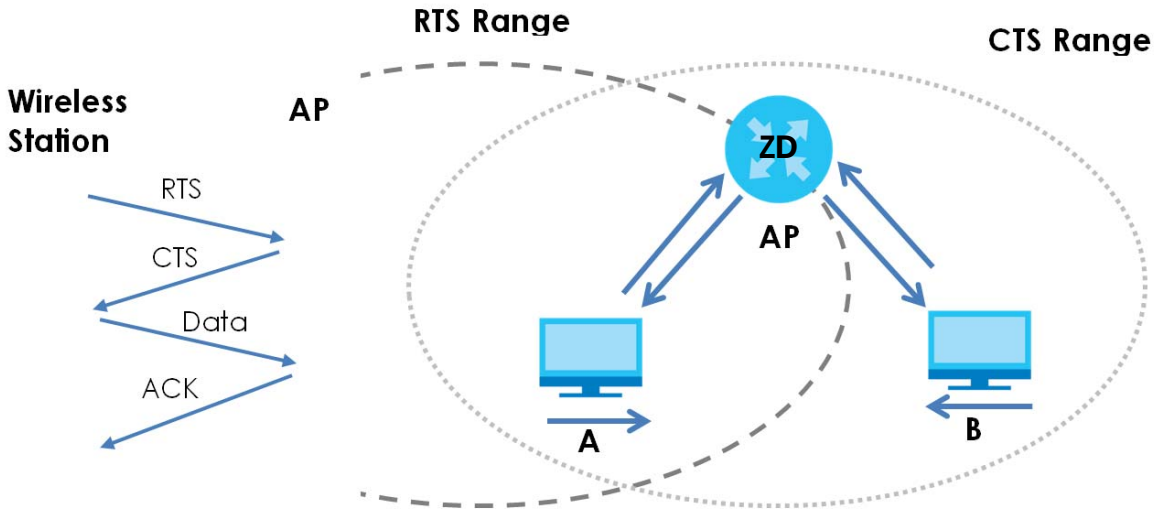
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 301 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 199 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between WiFi clients, access points and the wired network.

Wireless security methods available on the Zyxel Device are data encryption, WiFi client authentication, restricting access by device MAC address and hiding the Zyxel Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your Zyxel Device.

Table 200 Wireless Security Levels

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

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

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the WiFi clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

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

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the WiFi client. The WiFi client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the WiFi clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 201 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

WiFi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the WiFi clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless

gateway and WiFi client. As long as the passwords match, a WiFi client will be granted access to a WLAN.

If the AP or the WiFi clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or WiFi clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a WiFi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate WiFi clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a WiFi client to store the PMK it derived through a successful authentication with an AP. The WiFi client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the WiFi client (already connected to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

WiFi Client WPA Supplicants

A WiFi client supplicant is the software that runs on an operating system instructing the WiFi client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

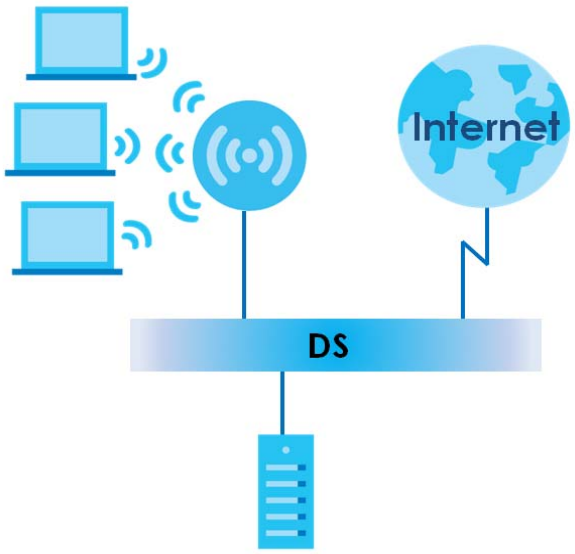
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" WiFi client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the WiFi client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the WiFi clients.

Figure 302 WPA(2) with RADIUS Application Example

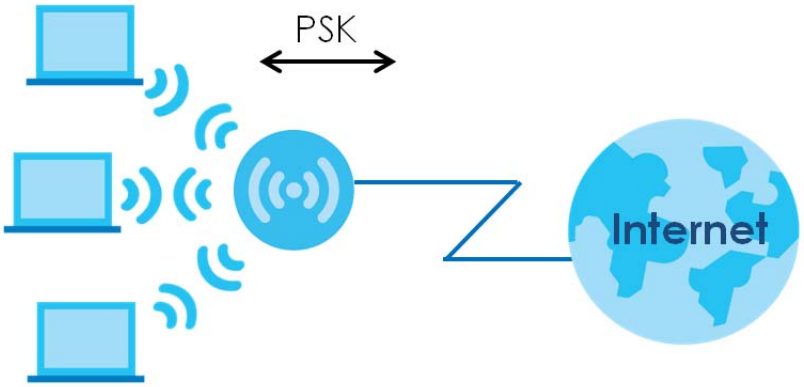


WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all WiFi clients. The Pre-Shared Key (PSK) must consist of between 8 to 63 alphanumeric (0-9, a-z, A-Z) and special characters, including spaces.
2. The AP checks each WiFi client's password and allows it to join the network only if the password matches.
3. The AP and WiFi clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
4. The AP and WiFi clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 303 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 202 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable

Table 202 Wireless Security Relational Matrix (continued)

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4 GHz (IEEE 802.11b and IEEE 802.11g) or 5 GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WiFi

There are two types of antennas used for WiFi applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.

- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

APPENDIX C
IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

Link-local Address

A link-local address uniquely identifies a device on the local network (the LAN). It is similar to a "private IP address" in IPv4. You can have the same link-local address on multiple interfaces on a device. A link-local unicast address has a predefined prefix of fe80::/10. The link-local unicast address format is as follows.

Table 203 Link-local Unicast Address Format

1111 1110 10	0	Interface ID
10 bits	54 bits	64 bits

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a "public IP address" in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

An unspecified address (0:0:0:0:0:0:0:0 or ::) is used as the source address when a device does not have its own address. It is similar to "0.0.0.0" in IPv4.

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to "127.0.0.1" in IPv4.

Multicast Address

In IPv6, Multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A Multicast address allows a host to send packets to all hosts in a Multicast group.

Multicast scope allows you to determine the size of the Multicast group. A Multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined Multicast addresses.

Table 204 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP severs on a local site.

The following table describes the Multicast addresses which are reserved and cannot be assigned to a Multicast group.

Table 205 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 206

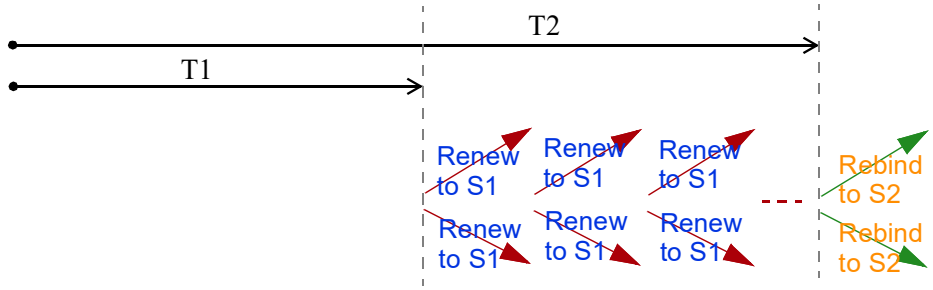
MAC	00	:	13	:	49	:	12	:	34	:	56

Table 207

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.
The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Zyxel Device uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by Multicast, the Zyxel Device passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical Multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Zyxel Device maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Zyxel Device configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Zyxel Device also sends out a neighbor solicitation message. When the Zyxel Device

receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Zyxel Device uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Zyxel Device creates an entry in the default router list cache if the router can be used as a default router.

When the Zyxel Device needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Zyxel Device uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is unlink, the address is considered as the next hop. Otherwise, the Zyxel Device determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Zyxel Device looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Zyxel Device cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

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

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive Multicast packets and the IP addresses of Multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which Multicast groups a port can join.

MLD Messages

A Multicast router or switch periodically sends general queries to MLD hosts to update the Multicast forwarding table. When an MLD host wants to join a Multicast group, it sends an MLD Report message for that address.

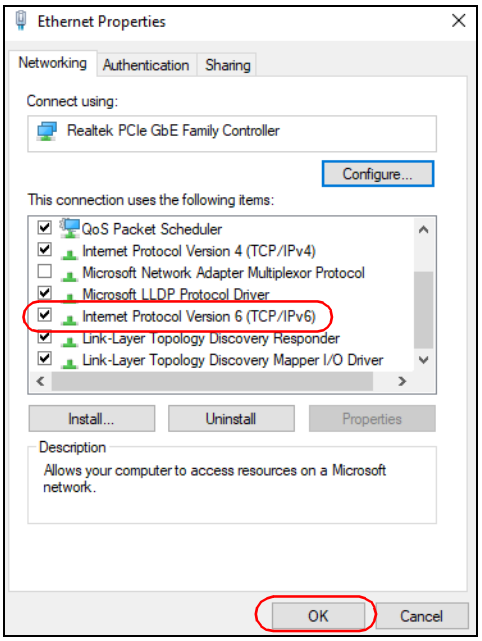
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a Multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 10 computer.

To enable IPv6 in Windows 10:

1. Click the start icon, **Settings** and then **Network & Internet**.
2. Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
3. Click **OK** to save the change.



4 Click the Search icon ( ) and then enter "cmd" in the search box..

5 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . : 172.16.100.61
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:f
```

APPENDIX D
Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 208 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance *www.zyxel.com*) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by email.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for email.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.

Table 208 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get email from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 208 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

APPENDIX E
Legal Information

Copyright

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America

The following information applies if you use the product within USA area.

FCC Statement

- The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Radiation Exposure Statement

- This device complies with FCC Radio Frequency (RF) radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

The following information applies for products operating in the 5.925-7.125 GHz band.

Low-power Indoor Access Point

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Standard Power Access Point

- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Industry Canada radiation exposure statement

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 23 cm (EE6601-00) and 20 cm (all other models) between the radiator and your body.

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 23 cm (EE6601-00) et 20 cm (tous les autres modèles) de distance entre la source de rayonnement et votre corps.

The following information applies for products operating in the 5.925-7.125 GHz band.

RLAN Devices

- Devices shall not be used for control of or communications with unmanned aircraft systems.

dispositifs RLAN

- Les dispositifs ne doivent pas être utilisés pour commander des systèmes d'aéronef sans pilote ni pour communiquer avec de tels systèmes.

Low-power indoor access points and indoor subordinate devices

- Operation shall be limited to indoor use only.
- Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited except for on large aircraft flying above 3,048 m (10,000 ft).

Points d'accès intérieurs de faible puissance et dispositifs subordonnés intérieurs

- leur utilisation doit être limitée à l'intérieur seulement;
- leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite, sauf à bord d'un gros aéronef volant à plus de 3 048 m (10 000 pi) d'altitude.

Standard-power access points and fixed client devices

- Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited.
- Information for antenna type(s), antenna model(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 4.5.4.c shall be clearly indicated.

Points d'accès de puissance normale et dispositifs clients fixes

- leur utilisation à bord de plateformes de forage pétrolier, d'automobiles, de trains, de navires maritimes et d'aéronefs doit être interdite;
- le ou les types d'antennes, le ou les modèles d'antennes et le ou les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la section 4.5.4(c) sur le masque de p.i.r.e par rapport à l'angle de site doivent être clairement indiqués.

Europe and the United Kingdom

The following information applies if you use the product within the European Union and United Kingdom.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK Radio Equipment Regulations 2017

Model List: AX7501-B0, AX7501-B1, DX3300-T0, DX3300-T1, DX3301-T0, DX5401-B0, DX5401-B1, EX3300-T0, EX3300-T1, EX3301-T0, EX3500-T0, EX3501-T0, EX3600-T0, EX5401-B0, EX5401-B1, EX5600-T1, EX5601-T0, EX5601-T1, EX7501-B0, PX3321-T1, PX5301-T0, PX5311-T0, EE6601-00

- Compliance information for wireless products relevant to the EU, United Kingdom, and other Countries following the EU Directive 2014/53/EU (RED) and UK Radio Equipment Regulations 2017. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU, United Kingdom, and other European countries, the 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz wireless LANs.
- If this device operates in the 5150 to 5350 MHz band, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF operating power for each band is as follows:
- DX3300-T0 / DX3301-T0 / EX3300-T0 / EX3301-T0
  - 95.28 mW for the 2,400 to 2,483.5 MHz band
  - 192.31 mW for the 5,150 to 5,350 MHz band
  - 912.01 mW for the 5,470 to 5,725 MHz band
- AX7501-B0
  - 96.38 mW for the 2,400 to 2,483.5 MHz band
  - 184.50 mW for the 5,150 to 5,350 MHz band
  - 905.73 mW for the 5,470 to 5,725 MHz band
- AX7501-B1
  - 90.16 mW for the 2,400 to 2,483.5 MHz band
  - 194.98 mW for the 5,150 to 5,350 MHz band
  - 993.12 mW for the 5,470 to 5,725 MHz band
- DX5401-B0 / EX5401-B0
  - 8.57 mW for the 2,400 to 2,483.5 MHz band (Zigbee)
  - 97.72 mW for the 2,400 to 2,483.5 MHz band (Wi-Fi)
  - 177.42 mW for the 5,150 to 5,350 MHz band
  - 857.04 mW for the 5,470 to 5,725 MHz band

- DX5401-B1 / EX5401-B1
  - 96.61 mW for the 2,400 to 2,483.5 MHz band
  - 193.64 mW for the 5,150 to 5,350 MHz band
  - 698.23 mW for the 5,470 to 5,725 MHz band
- EX3500-T0 / EX3501-T0
  - 97.72 mW for the 2,400 to 2,483.5 MHz band
  - 191.43 mW for the 5,150 to 5,350 MHz band
  - 916.22 mW for the 5,470 to 5,725 MHz band
- EX3600-T0
  - 19.59 dBm for the 2,400 to 2,483.5 MHz band
  - 22.85 dBm for the 5,150 to 5,350 MHz band
  - 27.8 dBm for the 5,470 to 5,725 MHz band
  - 22.62 dBm for the 5,725 to 5,850 MHz band (UK only)
- EX5600-T1 / EX5601-T0 / EX5601-T1
  - 86.5 mW for the 2,400 to 2,483.5 MHz band
  - 176.6 mW for the 5,150 to 5,350 MHz band
  - 870.1 mW for the 5,470 to 5,725 MHz band
  - 170.61 mW for the 5,725 to 5,850 MHz band (UK only)
- EX7501-B0
  - 88.51 mW for the 2,400 to 2,483.5 MHz band
  - 179.47 mW for the 5,150 to 5,350 MHz band
  - 883.08 mW for the 5,470 to 5,725 MHz band
  - 177.42 mW for the 5.725 to 5.850 MHz band (UK only)
- DX3300-T1 / EX3300-T1
  - 97.5 mW for the 2,400 to 2,483.5 MHz band
  - 194.09 mW for the 5,150 to 5,350 MHz band
  - 922.57 mW for the 5,470 – 5,725 MHz band
- PX3321-T1 / PX5301-T0
  - 99.31 mW for the 2,400 to 2,483.5 MHz band
  - 194.98 mW for the 5,150 to 5,350 MHz band
  - 997.7 mW for the 5,470 to 5,725 MHz band
- EE6601-00
  - 83.95 mW for the 2,400 to 2,483.5 MHz band
  - 165.58 mW for the 5,150 to 5,350 MHz band
  - 749.89 mW for the 5,470 to 5,725 MHz band
  - 170.22 mW for the 5,725 to 5,850 MHz band (UK only)
  - 165.96 mW for the 5,945 to 6,425 MHz band

Belgium (English) België (Flemish) Belgique (French)	**National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check *http://www.bipt.be* for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie *http://www.bipt.be* voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez *http://www.bipt.be* pour de plus amples détails.
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.

Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check *https://www.mise.gov.it/it/* for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare *https://www.mise.gov.it/it/* per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС.

Notes:

- Not all European states that implement EU Directive 2014/53/EU are European Union (EU) members.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not put the device in a place that is humid, dusty, has extreme temperatures, or that blocks the device ventilation slots. These conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for power rating of the device and operating temperature.
- There is a remote risk of electric shock from lightning: (1) Do not use the device outside, and make sure all the connections are indoors. (2) Do not install or service this device during a thunderstorm.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the Zyxel Device. Opening or removing the device covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connected cables carefully so that no one will step on them or stumble over them.
- Disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect the power adaptor or cord to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove the damaged power adaptor or cord from the device and the power source. Contact your local vendor to order a new one.
- CAUTION: There is a risk of explosion if you replace the device battery with an incorrect one. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do not leave a battery in an extremely high temperature environment or surroundings since it can result in an explosion or the leakage of flammable liquid or gas.
- Do not subject a battery to extremely low air pressure since it may result in an explosion or the leakage of flammable liquid or gas.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  – For a permanently connected device, a readily accessible method to disconnect the device shall be incorporated externally to the device;

  – For a pluggable device, the socket-outlet shall be installed near the device and shall be easily accessible.
- This product is intended to be supplied by a DC power source marked 'L.P.S' or `Limited Power Source'. The rating for each model is as follows:
  - AX7501-B0 / AX7501-B1 / EX7501-B0: 12 Vdc / 3.5 A / Tma 40 °C
  - DX3300-T0 / DX3301-T0 / EX3300-T0 / EX3301-T0: 12 Vdc / 1.5 A or 2 A / Tma 40 °C
  - DX3300-T1 / EX3300-T1 / EX3500-T0 / EX3501-T0 / PX3321-T1 / PX5301-T0 / PX5311-T0: 12 Vdc / 1.5A / Tma 40 °C
  - DX5401-B0 / EX5401-B0 / DX5401-B1 / EX5401-B1 / EX5600-T1 / EX5601-T0 / EX5601-T1: 12 Vdc / 3A / Tma 40 °C
  - EX3600-T0: 12Vdc / 2A / Tma 40 °C
  - EE6601-00: 12 Vdc / 3.5 A / Tma 40 °C

The following information applies for products with SFP:

- CLASS 1 LASER PRODUCT & “IEC 60825-1:2014”
- CLASS 1 CONSUMER LASER PRODUCT & "EN 50689:2021"
- Caution – Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.
- CLASS 1 CONSUMER LASER PRODUCT & "EN 50689:2021"

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.
- Attention: L'utilisation des commandes ou reglages ou l'execution des procedures autres que celles specifiees dans les presents exigences peuvent etre la cause d'une exposition a un rayonnement dangereux

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8 W, and/or
- Off mode power consumption < 0.5 W, and/or
- Standby mode power consumption < 0.5 W.

(Wireless setting, please refer to the chapter about wireless settings for more detail.)

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 本機限在不干擾合法電台與不被干擾保障條件下於室內使用。本產品使用時建議應距離人體 20 cm 以上。
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 – 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  – 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  – 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 （如：台灣供應電壓 110 伏特）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  – 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  – 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to *http://www.zyxel.com* to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor.

Registration

Register your product online at *www.zyxel.com* to receive e-mail notices of firmware upgrades and related information.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: *https://service-provider.zyxel.com/global/en/gpl-oss-software-notice*.

Index

Numbers

A

B

C

D

E

F

G

H

I

K

L

M

Q

R

S

T

U

V

W

Z