

CHAPTER 11

Firewall

11.1 Overview

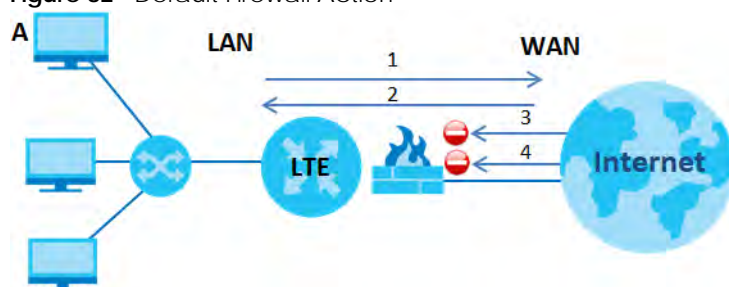
This chapter shows you how to enable the Zyxel Device firewall. Use the firewall to protect your Zyxel Device and network from attacks by hackers on the Internet and control access to it. The firewall:

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

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

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

Figure 82 Default Firewall Action



11.1.1 What You Need to Know About Firewall

DoS

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

ICMP

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

DoS Thresholds

For DoS attacks, the Zyxel Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

11.2 The Firewall Screen

11.2.1 What You Can Do in this Chapter

- Use the **General** screen to configure the security level of the firewall on the Zyxel Device ([Section 11.3 on page 110](#)).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules ([Section 11.4 on page 111](#)).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules ([Section 11.5 on page 113](#)).
- Use the **DoS** screen to activate protection against Denial of Service (DoS) attacks ([Section 11.6 on page 115](#)).

11.3 The Firewall General Screen

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

Figure 83 Security > Firewall > General

The firewall blocks unauthorized access to your network. Drag and drop the indicator to set a security level. Also note that a higher firewall level means more restrictions to the Internet activities you want to perform.

IPv4 Firewall ☒

IPv6 Firewall ☒

Low Medium (Recommended) High

LAN to WAN ☒ ☒ ☒

WAN to LAN ☒ ☒ ☒

Note

(1) LAN to WAN: Allow access to all Internet services

(2) WAN to LAN: Allow access from other computers on the Internet

(3) When the security level is set to "High", access to the following services is allowed: Telnet,FTP,HTTP,HTTPS,DNS,IMAP,POP3,SMTP and IPv6 Ping

Cancel Apply

Note: LAN to WAN is your access to all Internet services. WAN to LAN is the access of other computers on the Internet to devices behind the Zyxel Device.

When the security level is set to **High**, access to Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP, and IPv6 Ping are still allowed from the LAN.

The following table describes the labels in this screen.

Table 42 Security > Firewall > General

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

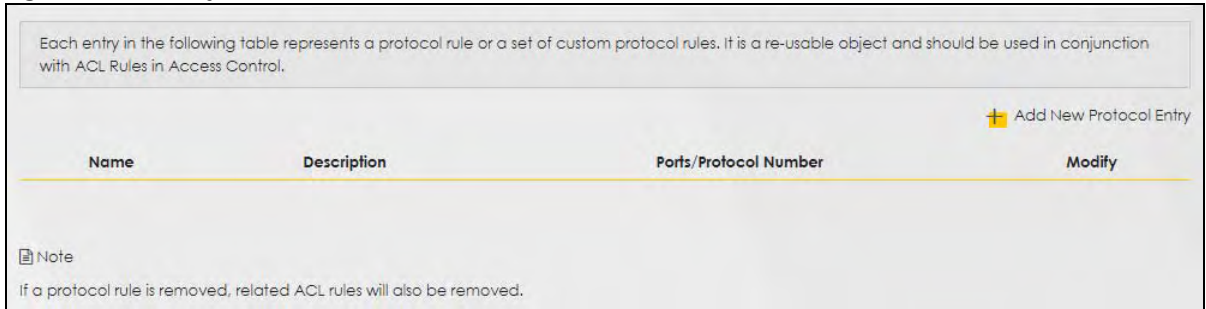
11.4 The Protocol (Customized Services) Screen

A protocol is a port number rule which defines a service. Services include Email, File sharing, Instant messaging, Online games, Print servers, Voice over IP and so on. Define services in this screen that you want to apply access control rules to in the **Firewall > Access Control** screen. For a comprehensive list of

port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click **Security > Firewall > Protocol** to display the following screen.

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

Figure 84 Security > Firewall > Protocol



Each entry in the following table represents a protocol rule or a set of custom protocol rules. It is a re-usable object and should be used in conjunction with ACL Rules in Access Control.

[Add New Protocol Entry](#)

Name	Description	Ports/Protocol Number	Modify
<p>Note</p> <p>If a protocol rule is removed, related ACL rules will also be removed.</p>			

The following table describes the labels in this screen.

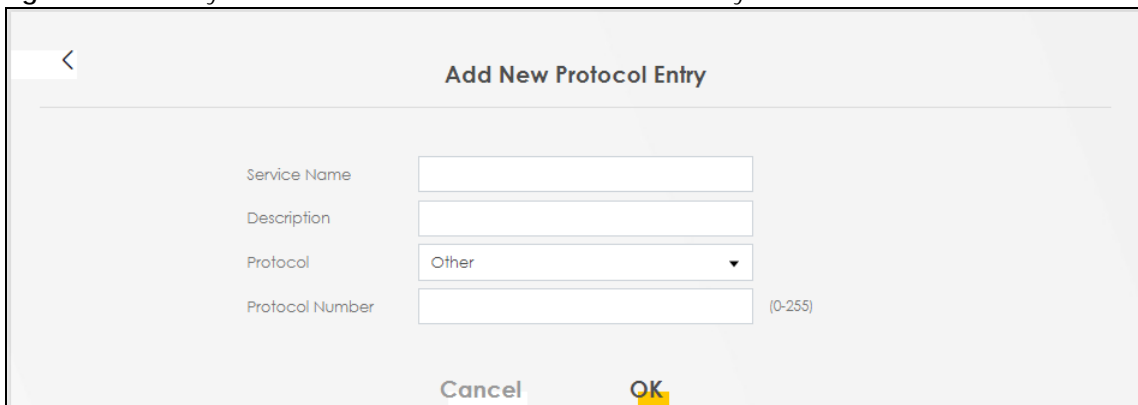
Table 43 Security > Firewall > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to configure a customized service.
Name	This is the name of your customized service.
Description	This is a description of your customized service.
Ports/Protocol Number	This shows the port number or range and the IP protocol (TCP or UDP) that defines your customized service.
Modify	Click this to edit a customized service.

11.4.1 Add Customized Service

Add a customized rule or edit an existing rule by specifying the IP port and the port number(s). Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

Figure 85 Security > Firewall > Protocol: Add New Protocol Entry



Add New Protocol Entry

Service Name

Description

Protocol

Protocol Number (0-255)

Cancel [OK](#)

The following table describes the labels in this screen.

Table 44 Security > Firewall > Protocol: Add New Protocol Entry

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Description	Enter a description for your custom port.
Protocol	Choose the IP port (TCP , UDP , ICMP , ICMPv6 , Other) that defines your customized port from the drop down list box.
Protocol Number	Type a single port number or the range of port numbers (0-255) that define your customized service.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

11.5 The Access Control (Rules) Screen

An Access Control List (ACL) rule is a manually-defined rule that can accept, reject, or drop incoming or outgoing packets from your network based on the type of service. For example, you could block users using Instant Messaging in your network. This screen displays a list of the configured incoming or outgoing filtering rules. Note the order in which the rules are listed. Click **Security > Firewall > Access Control** to display the following screen.

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

Figure 86 Security > Firewall > Access Control

An ACL rule is a manually defined rule to accept, reject, or drop the incoming or outgoing data of your network. You may need to create at least one Protocol entry in order to add an ACL rule.

Rules Storage Space Usage 0%

Add New ACL Rule

#	Name	Src IP	Dest IP	Service	Action	Modify
---	------	--------	---------	---------	--------	--------

The following table describes the labels in this screen.

Table 45 Security > Firewall > Rules

LABEL	DESCRIPTION
Rules Storage Space Usage	This read-only bar shows how much of the Zyxel Device's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Add New ACL Rule	Select an index number and click Add to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.
#	This field displays the rule index number. The ordering of your rules is important as rules are applied in turn.
Name	This field displays the rule name.
Src IP	This field displays the source IP addresses to which this rule applies.
Dest IP	This field displays the destination IP addresses to which this rule applies.
Service	This field displays the protocol (TCP, UDP, TCP+UDP or any) used to transport the packets for which you want to apply the rule.

Table 45 Security > Firewall > Rules (continued)

LABEL	DESCRIPTION
Action	Displays whether the firewall silently discards packets (Drop), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (Reject), or allow the passage of (Accept) packets that match this rule.
Modify	Click the Edit icon to edit the firewall rule. Click the Delete icon to delete an existing firewall rule.

11.5.1 Access Control Add New ACL Rule Screen

Use this screen to configure firewall rules. In the **Access Control** screen, select an index number and click **Add New ACL Rule** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

Figure 87 Security > Firewall > Access Control > Add New ACL Rule

The following table describes the labels in this screen.

Table 46 Security > Firewall > Access Control > Add New ACL Rule

LABEL	DESCRIPTION
Filter Name	Type a unique name for your filter rule.
Order	Assign the order of your rules as rules are applied in turn.

Table 46 Security > Firewall > Access Control > Add New ACL Rule (continued)

LABEL	DESCRIPTION
Select Source IP Address	If you want the source to come from a particular (single) IP, select Specific IP Address . If not, select from a detected device.
Source IP Address	If you selected Specific IP Address in the previous item, enter the source device's IP address here. Otherwise this field will be hidden if you select the detected device.
Select Destination Device	If you want your rule to apply to packets with a particular (single) IP, select Specific IP Address . If not, select a detected device.
Destination IP Address	If you selected Specific IP Address in the previous item, enter the destination device's IP address here. Otherwise this field will be hidden if you select the detected device.
IP Type	Select between IPv4 or IPv6 . Compared to IPv4 , IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 1038 IP addresses. The Zyxel Device can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and supports IPv6 rapid deployment (6RD).
Select Service	Select a service from the Select Service box.
Protocol	Select the protocol (ALL , TCP/UDP , TCP , UDP , ICMP , ICMPv6) used to transport the packets for which you want to apply the rule.
Custom Source Port	This is a single port number or the starting port number of a range that defines your rule.
Custom Destination Port	This is a single port number or the ending port number of a range that defines your rule.
Policy	Use the drop-down list box to select whether to discard (Drop), deny and send an ICMP destination-unreachable message to the sender (Reject), or allow the passage of (Accept) packets that match this rule.
Direction	Select WAN to LAN to apply the rule to traffic from WAN to LAN. Select LAN to WAN to apply the rule to traffic from LAN to WAN. Select WAN to Router to apply the rule to traffic from WAN to router. Select LAN to Router to apply the rule to traffic from LAN to router.
Enable Rate Limit	Click to enable (switch turns blue) the setting of maximum number of packets per maximum number of minute/second to limit the throughput of traffic that matches this rule. If not, the next item will be disabled.
Scheduler Rules	
packet(s) per (1-512)	Enter the maximum number of packets (1-512) per minute/second .
Add New Rule	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by clicking Add New Rule .
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

11.6 DoS Screen

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

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

Figure 88 Security > Firewall > DoS

The following table describes the labels in this screen.

Table 47 Security > Firewall > DoS

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

11.7 Firewall Technical Reference

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

11.7.1 Firewall Rules Overview

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

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

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

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

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

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

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

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

- WAN to LAN

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

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

- WAN to Router

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

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

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

For example, you may create rules to:

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

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the Zyxel Device's default rules.

11.7.2 Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via the Web Configurator.
- 2 Think about access control before you connect to the network in any way.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

11.7.3 Security Considerations

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

Consider these security ramifications before creating a rule:

- 1** Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC (Internet Relay Chat) is blocked, are there users that require this service?
- 2** Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3** Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4** Does this rule conflict with any existing rules?

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

CHAPTER 12

MAC Filter

12.1 MAC Filter Overview

You can configure the Zyxel Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the LAN client to configure this screen.

12.2 The MAC Filter Screen

Enable **MAC Address Filter** and add the host name and MAC address of a LAN client to the table if you wish to allow or deny them access to your network. Select **Security > MAC Filter**. The screen appears as shown.

Figure 89 Security > MAC Filter

MAC Filter

Enable MAC filters and add the MAC addresses of LAN client in your home or office network to the following table, if you wish to allow or deny them to access your network. Sometimes, MAC Filter is considered a method to increase the security of your network.

MAC Address Filter ☒ Enable ☐ Disable (Settings are invalid when disable)

MAC Restrict Mode ☒ Allow ☐ Deny

Add New Rule

Set	Active	Host Name	MAC Address	Delete
-----	--------	-----------	-------------	--------

Note
Only devices listed here are granted access to the network

Cancel Apply

You can choose to enable or disable the filters per entry; make sure that the check box under **Active** is selected if you want to use a filter, as shown in the example below.

Figure 90 Enabling individual MAC filters

Set	Active	Host Name	MAC Address	Delete
1	<input type="checkbox"/>	test	BC - 22 - 33 - 44 - 55 - AA	
2	<input checked="" type="checkbox"/>	Test	BC - 88 - 99 - 00 - 11 - 22	

The following table describes the labels in this screen.

Table 48 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select Enable to activate the MAC filter function.
MAC Restrict Mode	Select Allow to only permit the listed MAC addresses access to the Zyxel Device. Select Deny to permit anyone access to the Zyxel Device except the listed MAC addresses.
Add New Rule	Click this button to create a new entry.
Set	This is the index number of the MAC address.
Active	Select Active to enable the MAC filter rule. The rule will not be applied if Allow is not selected under MAC Restrict Mode .
Host Name	Enter the host name of the wireless or LAN clients that are allowed access to the Zyxel Device.
MAC Address	Enter the MAC addresses of the wireless or LAN clients that are allowed access to the Zyxel Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Delete	Click the Delete icon to delete an existing rule.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

CHAPTER 13

Certificates

13.1 Overview

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

13.1.1 What You Can Do in this Chapter

- Use the **Local Certificates** screen to view and import the Zyxel Device's CA-signed (Certification Authority) certificates ([Section 13.2 on page 121](#)).
- Use the **Trusted CA** screen to save the certificates of trusted CAs to the Zyxel Device. You can also export the certificates to a computer ([Section 13.3 on page 125](#)).

13.2 Local Certificates

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

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

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

Figure 91 Security > Certificates > Local Certificates

The screenshot shows the 'Local Certificates' configuration page. At the top, a text box explains that certificates (also known as digital IDs) can authenticate, and users can generate certification requests and import signed certificates, with a maximum of 4 certificates stored. Below this, there's a section for replacing the PrivateKey/Certificate file in PEM format. It includes a checkbox for 'Private Key is protected by password' which is checked, followed by a password input field. There is also a 'Choose File' button and the text 'No file chosen'. On the right side, there are two buttons: 'Import Certificate' and 'Create Certificate Request'. At the bottom, there is a table header with columns: 'Current File', 'Subject', 'Issuer', 'Valid From', 'Valid To', and 'Modify'.

Current File	Subject	Issuer	Valid From	Valid To	Modify
--------------	---------	--------	------------	----------	--------

The following table describes the labels in this screen.

Table 49 Security > Certificates > Local Certificates

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

13.2.1 Create Certificate Request

Click **Security > Certificates > Local Certificates** and then **Create Certificate Request** to open the following screen. Have the Zyxel Device generate a certification request. To create a certificate signing request, you need to enter a common name, organization name, state/province name, and the two-letter country code for the certificate.

Figure 92 Create Certificate Request

The following table describes the labels in this screen.

Table 50 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select Auto to have the Zyxel Device configure this field automatically. Or select Customize to enter it manually. Type the IP address (in dotted decimal notation), domain name or email address in the field provided. The domain name or email address can be up to 63 ASCII characters. The domain name or email address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Zyxel Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Cancel	Click Cancel to exit this screen without saving.
OK	Click OK to save your changes.

13.2.2 View Certificate Request

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

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

Figure 93 Certificate Request: View

The screenshot shows a window titled "View Certificate" with a close button in the top right corner. Below the title bar is a section labeled "Certificate Details".

Name	Test
Type	none
Subject	/CN=588BF3-VMG8825-B50B-S172V48000015/O=Zyxel/ST=Hsinchu/C=TW

Below the details table are three large text areas:

- Certificate:** A large empty text box for displaying the certificate content.
- Private Key:** A text box containing a long string of base64-encoded text, starting with "hGEzXjrKpkeJHmKBehzv..." and ending with "...fAdmacECaYFA+SlZJoWxoB90BopN1JP3t//IOLPznbs".
- Signing Request:** A text box containing a long string of base64-encoded text, starting with "-----BEGIN CERTIFICATE REQUEST-----" and ending with "NDQm4l3bs9rfwLqUMFck3F4HQ".

At the bottom center of the window is a yellow button labeled "Back".

The following table describes the fields in this screen.

Table 51 Certificate Request: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	<p>This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form.</p> <p>You can copy and paste the certificate into an email to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution.</p>
Private Key	This field displays the private key of this certificate.

Table 51 Certificate Request: View (continued)

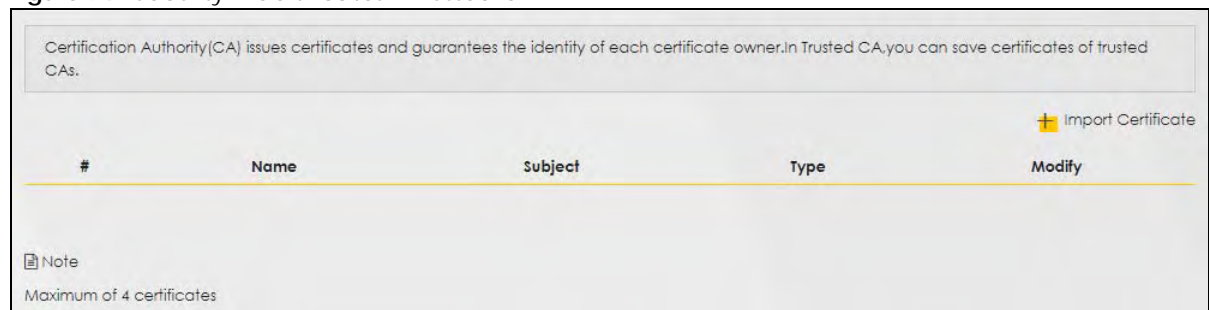
LABEL	DESCRIPTION
Signing Request	This field displays the CSR (Certificate Signing Request) information of this certificate. The CSR will be provided to a certificate authority, and it includes information about the public key, organization name, domain name, location, and country of this certificate.
Back	Click Back to return to the previous screen.

13.3 Trusted CA

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

Note: A maximum of 4 certificates can be stored.

Figure 94 Security > Certificates > Trusted CA



The following table describes the labels in this screen.

Table 52 Security > Certificates > Trusted CA

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

13.4 Import Trusted CA Certificate

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

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

Figure 95 Trusted CA > Import

The following table describes the labels in this screen.

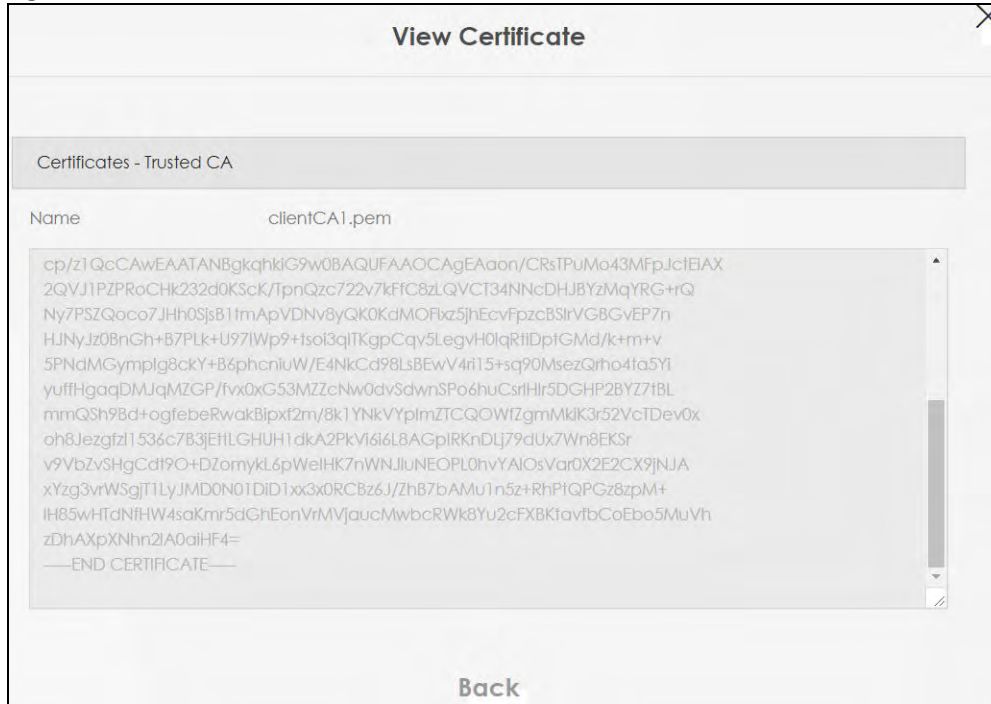
Table 53 Security > Certificates > Trusted CA > Import

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

13.5 View Trusted CA Certificate

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

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

Figure 96 Trusted CA: View

The following table describes the labels in this screen.

Table 54 Trusted CA: View

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

13.6 Certificates Technical Reference

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

Certification Authorities

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

Public and Private Keys

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

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

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

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

Advantages of Certificates

Certificates offer the following benefits.

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

Certificate File Format

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

13.6.1 Verifying a Certificate

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

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

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

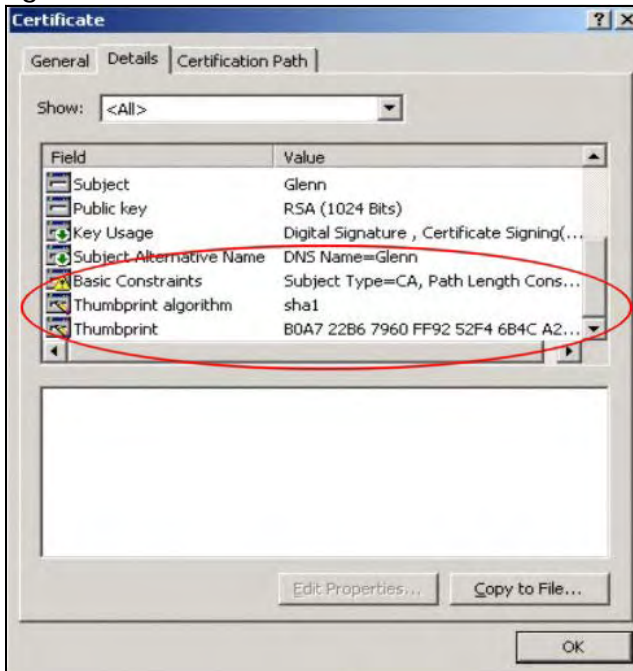
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 97 Certificates on Your Computer



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

Figure 98 Certificate Details



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

CHAPTER 14

Log

14.1 Log Overview

These screens allow you to determine the categories of events and/or alerts that the Zyxel Device logs and then display these logs or have the Zyxel Device send them to an administrator (through email) or to a syslog server.

14.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs ([Section 14.2 on page 131](#)).
- Use the **Security Log** screen to see the security-related logs for the categories that you select ([Section 14.3 on page 131](#)).

14.1.2 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.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 55 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.

Table 55 Syslog Severity Levels

CODE	SEVERITY
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

14.2 The System Log Screen

Export or email the system logs. You can filter the entries by clicking the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log** to open the **System Log** screen.

Figure 99 System Monitor > Log > System Log

The screenshot shows the 'System Log' interface. At the top, a message states: 'All system events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.' Below this, there are two drop-down menus: 'Level' (set to 'All') and 'Category' (set to 'All'). To the right of these menus are four buttons: 'Clear Log', 'Refresh', 'Export Log', and 'E-mail Log Now'. Below the filters is a table with the following headers: '#', 'Time', 'Facility', 'Level', 'Category', and 'Messages'.

The following table describes the fields in this screen.

Table 56 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 log(s).
Email Log Now	Click this to send the log file(s) to the email address you specify in the Maintenance > Logs 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 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.

14.3 The Security Log Screen

View the security-related logs for the categories that you select. You can filter the entries by clicking the **Level** and/or **Category** drop-down list boxes. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 100 System Monitor > Log > Security Log

All security events will be logged and displayed in the following table. Select a level from the pull-down menu to show filtered results.

Level: Category: [Clear Log](#) [Refresh](#) [Export Log](#) [E-mail Log Now](#)

#	Time	Facility	Level	Category	Messages
---	------	----------	-------	----------	----------

The following table describes the fields in this screen.

Table 57 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 log(s).
Email Log Now	Click this to send the log file(s) to the email address you specify in the Maintenance > Logs 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 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 15

Traffic Status

15.1 Traffic Status Overview

View the network traffic status and statistics of the WAN/LAN interfaces.

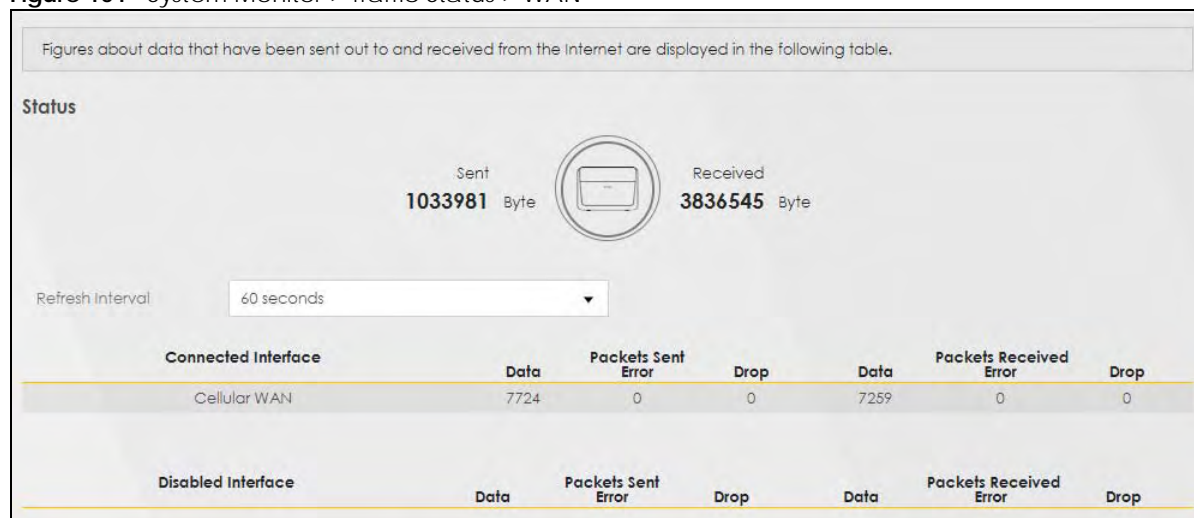
15.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics ([Section 15.2 on page 133](#)).
- Use the **LAN** screen to view the LAN traffic statistics ([Section 15.3 on page 134](#)).

15.2 The WAN Status Screen

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. Detailed information about each interface are listed in the tables below.

Figure 101 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 58 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	

Table 58 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
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.
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.

15.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figures in this screen show the number of bytes received and sent from each LAN port and wireless network.

Figure 102 System Monitor > Traffic Status > LAN

Figures about data that have been sent to and received from each LAN port (including WiFi) are displayed in the following table.

Refresh Interval: 60 seconds

Interface	LAN1	2.4G WLAN
Bytes Sent	4587507	0
Bytes Received	1349352	0

Interface	LAN1	2.4G WLAN
Sent (Packet)	Data	11012
	Error	0
	Drop	0
Received (Packet)	Data	9141
	Error	0
	Drop	12

The following table describes the fields in this screen.

Table 59 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.

CHAPTER 16

ARP Table

16.1 ARP Table Overview

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

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

16.1.1 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.

16.2 ARP Table Screen

Use the ARP table to view the IPv4-to-MAC address mapping(s) for the LAN. The neighbor table shows the IPv6-to-MAC address mapping(s) of each neighbor. To open this screen, click **System Monitor > ARP Table**.

Figure 103 System Monitor > ARP Table

ARP Table			
ARP Table displays the IPv4 address and MAC address of each DHCP connection. Neighbour Table displays the IPv6 address and MAC address of each Neighbour.			
IPv4 ARP Table			
#	IPv4 Address	MAC Address	Device
1	192.168.1.129	dc:4a:3e:40:ec:5f	br0
IPv6 Neighbour Table			
#	IPv6 Address	MAC Address	Device
1	fe80::ecad:ab45:c530:cc3f	dc:4a:3e:40:ec:5f	br0

The following table describes the labels in this screen.

Table 60 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 a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click the device type to go to its configuration screen.

CHAPTER 17

Routing Table

17.1 Routing Table Overview

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

17.2 The Routing Table Screen

The table below shows IPv4 and IPv6 routing information. The destination can be a network or host. 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. Flags can be U - up, ! - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), or M - modified (redirect). Metric is the distance to the target (usually counted in hops). Interface is how the packets for this route will be sent.

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

Figure 104 System Monitor > Routing Table

Routing Table					
Destination: The destination network or destination host. Gateway: The gateway address or "*" (IPv4) / "::" (IPv6) if none set. Subnet Mask (IPv4): The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route. Flags: U - up, I - reject, G - gateway, C - cache, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). Metric: the distance to the target (usually counted in hops). Interface: Interface to which packets for this route will be sent.					
IPv4 Routing Table					
Destination	Gateway	Subnet Mask	Flag	Metric	Interface
0.0.0.0	10.148.66.85	0.0.0.0	UG	0	wwan0
10.148.66.80	0.0.0.0	255.255.255.248	U	0	wwan0
127.0.0.0	0.0.0.0	255.255.0.0	U	0	lo
192.168.1.0	0.0.0.0	255.255.255.0	U	0	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	br0
IPv6 Routing Table					
Destination	Gateway	Flag	Metric	Interface	
fe80::/64	::	U	256	eth2	
fe80::/64	::	U	256	br0	
fe80::/64	::	U	256	ra0	
fe80::/64	::	U	256	wwan0	
::1/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::/128	::	U	0	lo	
fe80::8420:d5ff:fee9:3ced/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b903/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b903/128	::	U	0	lo	
fe80::86aa:9cff:fe83:b904/128	::	U	0	lo	
ff02::1/128	::	UC	0	br0	
ff00::/8	::	U	256	eth2	
ff00::/8	::	U	256	br0	
ff00::/8	::	U	256	ra0	
ff00::/8	::	U	256	wwan0	

The following table describes the labels in this screen.

Table 61 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 61 System Monitor > Routing Table (continued)

LABEL	DESCRIPTION
Flag	<p>This indicates the route status.</p> <p>U-Up: The route is up.</p> <p>!-Reject: The route is blocked and will force a route lookup to fail.</p> <p>G-Gateway: The route uses a gateway to forward traffic.</p> <p>H-Host: The target of the route is a host.</p> <p>R-Reinstate: The route is reinstated for dynamic routing.</p> <p>D-Dynamic (redirect): The route is dynamically installed by a routing daemon or redirect.</p> <p>M-Modified (redirect): The route is modified from a routing daemon or redirect.</p>
Metric	<p>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."</p>
Interface	<p>This indicates the name of the interface through which the route is forwarded.</p>

CHAPTER 18

Cellular WAN Status

18.1 Cellular WAN Status Overview

View the LTE connection details and WiFi signal strength value that you can use as reference for positioning the Zyxel Device, as well as SIM card and module information.

18.2 The Cellular WAN Status Screen

To open this screen, click **System Monitor > Cellular WAN Status**. Cellular information is available on this screen only when you insert a valid SIM card in the Zyxel Device.

Figure 105 System Monitor > Cellular WAN Status

Cellular WAN Status

Cellular WAN Status

Refresh Interval: 60 seconds

Module Information

IMEI: 861107033477226
 Module SW Version: EC25EFAR02A09M4G

SIM Status

SIM Card Status: Available
 IMSI: 466011801162600
 ICCID: 89886018157703499511
 PIN Protection: Disable
 PIN Remaining Attempts: 3

IP Passthrough Status

IP Passthrough Enable: Disable

Service Information

Cellular Status: Up
 Data Roaming: Disable
 Operator: Far EastOne
 PLMN: 46601
 Access Technology: LTE
 Band: LTE_BC7
 RSSI: -39
 Cell ID: 56410647
 RFCH: 3250
 RSRP: -70
 RSRQ: -8
 RSCP: N/A
 EcNo: N/A
 TAC: 59242
 LAC: N/A
 RAC: N/A
 BSIC: N/A

The following table describes the labels in this screen.

Table 62 System Monitor > Cellular WAN Status

LABEL	DESCRIPTION
Refresh Interval	Select the time interval the Zyxel Device will check and refresh the fields shown on this screen. Select None to stop detection.
Module Information	
IMEI	This shows the International Mobile Equipment Identity of the Zyxel Device.
Module SW Version	This shows the software version of the Zyxel Device.
SIM Status	

Table 62 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
SIM Card Status	<p>This displays the SIM card status:</p> <p>None - the Zyxel Device does not detect that there is a SIM card inserted.</p> <p>Available - the SIM card could either have or doesn't have PIN code security.</p> <p>Locked - the SIM card has PIN code security, but you did not enter the PIN code yet.</p> <p>Blocked - you entered an incorrect PIN code too many times, so the SIM card has been locked; call the ISP for a PUK (Pin Unlock Key) to unlock the SIM card.</p> <p>Error - the Zyxel Device detected that the SIM card has errors.</p>
IMSI	This displays the International Mobile Subscriber Identity (IMSI) of the installed SIM card. An IMSI is a unique ID used to identify a mobile subscriber in a mobile network.
ICCID	Integrated Circuit Card Identifier (ICCID). This is the serial number of the SIM card.
PIN Protection	<p>A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card.</p> <p>Shows Enable if the service provider requires you to enter a PIN to use the SIM card.</p> <p>Shows Disable if the service provider lets you use the SIM without inputting a PIN.</p>
PIN Remaining Attempts	This is how many more times you can try to enter the PIN code before the ISP blocks your SIM card.
IP Passthrough Status	
Cellular Status	This displays the status of the cellular Internet connection.
Data Roaming	<p>This displays if data roaming is enabled on the Zyxel Device.</p> <p>4G roaming is to use your Zyxel Device in an area which is not covered by your service provider. Enable roaming to ensure that your Zyxel Device is kept connected to the Internet when you are traveling outside the geographical coverage area of the network to which you are registered.</p>
Operator	This displays the name of the service provider.
PLMN	This displays the PLMN number.
Access Technology	This displays the type of the mobile network (such as LTE, UMTS, GSM) to which the Zyxel Device is connecting.
Band	This displays the current LTE band of your Zyxel Device (WCDMA2100).
RSSI	<p>This displays the strength of the WiFi signal between an associated wireless station and an AP.</p> <p>The normal range is -30dBm to -79dBm. If the value drops below -80dBm, try moving the associated wireless station closer to the Zyxel Device to get better signal strength.</p>
Cell ID	<p>This shows the cell ID, which is a unique number used to identify the Base Transceiver Station to which the Zyxel Device is connecting.</p> <p>The value depends on the Current Access Technology:</p> <ul style="list-style-type: none"> For GPRS, it is the Cell Identity as specified in 3GPP-TS.25.331. For UMTS, it is the Cell Identity as defined in SIB3 3GPP-TS.25.331, 3GPP-TS.24.008. For LTE, it is the 28-bit binary number Cell Identity as specified in SIB1 in 3GPP-TS.36.331. <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>

Table 62 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
RFCN	<p>This displays the Radio Frequency Channel Number of DL carrier frequency used by the mobile network to which the Zyxel Device is connecting.</p> <p>The value depends on the Current Access Technology:</p> <ul style="list-style-type: none"> For GPRS, it is the ARFCN (Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.45.005. For UMTS, it is the UARFCN (UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.25.101. For LTE, it is the EARFCN (E-UTRA Absolute Radio-Frequency Channel Number) as specified in 3GPP-TS.36.101. <p>The value is '0' (zero) or 'N/A' if there is no network connection.</p>
RSRP	<p>This displays the Reference Signal Receive Power (RSRP), which is the average received power of all Resource Element (RE) that carry cell-specific Reference Signals (RS) within the specified bandwidth.</p> <p>The received RSRP level of the connected E-UTRA cell, in dBm, is as specified in 3GPP-TS.36.214. The reporting range is specified in 3GPP-TS.36.133.</p> <p>An undetectable signal is indicated by the lower limit, example -140 dBm.</p> <p>This parameter is for LTE only. The normal range is -30 to -140. The value is -140 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.</p>
RSRQ	<p>This displays the Reference Signal Receive Quality (RSRQ), which is the ratio of RSRP to the E-UTRA carrier RSSI and indicates the quality of the received reference signal.</p> <p>The received RSRQ level of the connected E-UTRA cell, in 0.1 dB, is as specified in 3GPP-TS.36.214. An undetectable signal is indicated by the lower limit, example -240.</p> <p>This parameter is for LTE only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not LTE. The value is 'N/A' if there is no network connection.</p>
RSCP	<p>This displays the Received Signal Code Power, which measures the power of channel used by the Zyxel Device.</p> <p>The received signal level, in dBm, is of the CPICH channel (Ref. 3GPP TS 25.133). An undetectable signal is indicated by the lower limit, example -120 dBm.</p> <p>This parameter is for UMTS only. The normal range is -30 to -120. The value is -120 if the Current Access Technology is not UMTS. The value is 'N/A' if there is no network connection.</p>
EcNo	<p>This displays the ratio (in dB) of the received energy per chip and the interference level.</p> <p>The measured EcNo is in 0.1 dB and is received in the downlink pilot channel. An undetectable signal is indicated by the lower limit, example -240 dB.</p> <p>This parameter is for UMTS only. The normal range is -30 to -240. The value is -240 if the Current Access Technology is not UMTS or there is no network connection.</p>
TAC	<p>This displays the Tracking Area Code (TAC), which is used to identify the country of a mobile subscriber.</p> <p>The physical cell ID of the connected E-UTRAN cell, is as specified in 3GPP-TS.36.101.</p> <p>This parameter is for LTE only. The value is '0' (zero) or 'N/A' if the Current Access Technology is not LTE or there is no network connection.</p>
LAC	<p>This displays the 2-octet Location Area Code (LAC), which is used to identify a location area within a PLMN.</p> <p>The LAC of the connected cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC) and LAC uniquely identifies the LAI (Location Area ID) [3GPP-TS.23.003].</p> <p>This parameter is for UMTS or GPRS. The value is '0' (zero) if the Current Access Technology is not UMTS or GPRS. The value is 'N/A' if there is no network connection.</p>

Table 62 System Monitor > Cellular WAN Status (continued)

LABEL	DESCRIPTION
RAC	<p>This displays the RAC (Routing Area Code), which is used in mobile network “packet domain service” (PS) to identify a routing area within a location area.</p> <p>In a mobile network, it uses LAC (Location Area Code) to identify the geographical location for the old 3G voice only service, and use RAC to identify the location of data service like HSDPA or LTE.</p> <p>The RAC of the connected UTRAN cell is as defined in SIB 1 [3GPP-TS.25.331]. The concatenation of PLMN ID (MCC+MNC), LAC, and RAC uniquely identifies the RAI (Routing Area ID) [3GPP-TS.23.003].</p> <p>This parameter is for UMTS or GPRS. The value is ‘0’ (zero) if the Current Access Technology is not UMTS or GPRS. The value is ‘N/A’ if there is no network connection.</p>
BSIC	<p>The Base Station Identity Code (BSIC), which is a code used in GSM to uniquely identify a base station.</p> <p>This parameter is for GPRS only. The value is ‘0’ (zero) if the Current Access Technology is not GPRS. The value is ‘N/A’ if there is no network connection.</p>

CHAPTER 19

System

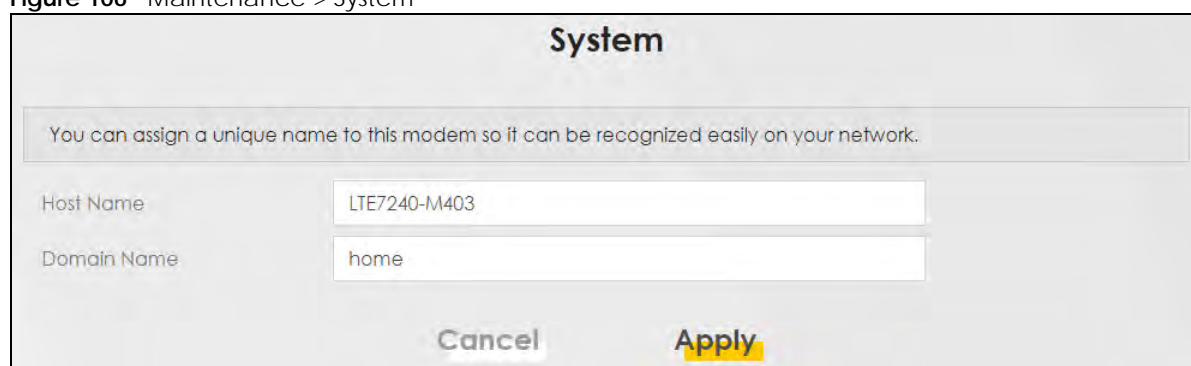
19.1 System Overview

Give a name to your Zyxel Device (host) and an associated domain name for identification purposes.

19.2 The System Screen

Click **Maintenance > System** to open the following screen. Assign a unique name so it can be easily recognized on your network. You can use up to 30 characters, including spaces.

Figure 106 Maintenance > System



System

You can assign a unique name to this modem so it can be recognized easily on your network.

Host Name: LTE7240-M403

Domain Name: home

Cancel **Apply**

The following table describes the labels in this screen.

Table 63 Maintenance > System

LABEL	DESCRIPTION
Host Name	Type a host name for your Zyxel Device. Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes.
Domain Name	Type a Domain name for your host Zyxel Device.
Cancel	Click Cancel to abandon this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 20

User Account

20.1 User Account Overview

View the settings of the “admin” and other user accounts that you use to log into the Zyxel Device.

20.2 The User Account Screen

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

Figure 107 Maintenance > User Account

#	Active	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	<input checked="" type="checkbox"/>	admin	3	60	5	Administrator	

The following table describes the labels in this screen.

Table 64 Maintenance > User Account

LABEL	DESCRIPTION
Add New Account	Click this button to add a new user account (up to 4 Administrator accounts and 4 User accounts).
#	This is the index number.
Active	This indicates whether the user account is active or not. The check box 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.

Table 64 Maintenance > User Account (continued)

LABEL	DESCRIPTION
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 .
Group	This field displays whether this user has Administrator or User privileges.
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.

20.2.1 The User Account Add/Edit Screen

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 108 Maintenance > User Account > Add/Edit

The following table describes the labels in this screen.

Table 65 Maintenance > 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 new name for the account (up to 15 characters). Special characters are allowed except the following: double quote (") back quote (`) apostrophe or single quote (') less than (<) greater than (>) caret or circumflex accent (^) dollar sign (\$) vertical bar () ampersand (&) semicolon (;)
Password	Type your new system password (up to 256 characters). 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.
Verify Password	Type the new password again for confirmation.

Table 65 Maintenance > User Account > Add/Edit (continued) (continued)

LABEL	DESCRIPTION
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 .
Group	<p>Specify whether this user will have Administrator or User privileges.</p> <p>The Administrator privileges are the following:</p> <ul style="list-style-type: none"> • Quick Start setup. • The following screens are visible for setup: Broadband, Wireless, Home Networking, Routing, NAT, DNS, Firewall, MAC Filter, Certificates, Log, Traffic Status, ARP Table, Routing Table, Cellular WAN Status, System, User Account, Remote Management, TR-069 Client, Time, Email Notification, Log Setting, Firmware Upgrade, Backup/Restore, Reboot, Diagnostic. <p>The User privileges are the following:</p> <ul style="list-style-type: none"> • 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.
Cancel	Click Cancel to restore your previously saved settings.
OK	Click OK to save your changes.

CHAPTER 21

Remote Management

21.1 Overview

Remote management controls through which interface(s), which web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) can access the Zyxel Device.

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

21.2 The MGMT Services Screen

Configure which interface(s) you can use to access the Zyxel Device for a given service. You can also specify the service port numbers computers must use to connect to the Zyxel Device. Click **Maintenance > Remote Management** to open the following screen.

Figure 109 Maintenance > Remote Management

Remote MGMT enables various approaches to access this modem remotely from a WAN and/or LAN connection.

Service Control

WAN Interface used for services ☐ Any_WAN ☒ Multi_WAN

☒ Cellular WAN

Service	LAN/WLAN	WAN	Trust Domain	Port
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	443
FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	23
SSH	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
PING	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	

The following table describes the fields in this screen.

Table 66 Maintenance > Remote Management

LABEL	DESCRIPTION
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.
Cellular WAN	Enable the LTE WAN connection configured in Network Setting > Broadband > Cellular WAN to access the service on the Zyxel Device.
Service	This is the service you may use to access the Zyxel Device.
LAN/WLAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the LAN/WLAN.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
Trust Domain	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from the trusted host IP address.
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.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

21.3 The MGMT Services for IP Passthrough Screen

Configure which interface(s) you can use to access the Zyxel Device in **IP Passthrough** mode (bridge mode) for a given service. You can also specify the service port numbers computers must use to connect to the Zyxel Device. IP Passthrough allows Internet traffic to go to a LAN computer behind the Zyxel Device without going through NAT. Make sure to enable IP Passthrough in **Network Setting > Broadband > Cellular IP Passthrough**. See [Section 5.6 on page 40](#) for details.

Click **Maintenance > Remote Management > MGMT Services for IP Passthrough** to open the following screen.

Figure 110 Maintenance > Remote Management > MGMT Services for IP Passthrough

Remote MGMT enables various approaches to access this modem remotely from a WAN and/or LAN connection.

Service Control

Service	WAN	Port
PT_HTTP	<input checked="" type="checkbox"/> Enable	20080
PT_HTTPS	<input checked="" type="checkbox"/> Enable	20443
PT_FTP	<input checked="" type="checkbox"/> Enable	20021
PT_TELNET	<input checked="" type="checkbox"/> Enable	20023
PT_SSH	<input checked="" type="checkbox"/> Enable	20022

Cancel Apply

The following table describes the fields in this screen.

Table 67 Maintenance > Remote Management > MGMT Services for IP Passthrough

LABEL	DESCRIPTION
Service	This is the service you may use to access the Zyxel Device.
WAN	Select the Enable check box for the corresponding services that you want to allow access to the Zyxel Device from all WAN connections.
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.
Apply	Click Apply to save your changes back to the Zyxel Device.
Cancel	Click Cancel to restore your previously saved settings.

21.4 The Trust Domain Screen

View a list of public IP addresses which you want to allow access to the Zyxel Device through the services configured in this screen. Click **Maintenance > Remote Management > Trust Domain** to open the following screen.

Note: If this list is empty, all public IP addresses can access the Zyxel Device from the WAN through the specified services.

Figure 111 Maintenance > Remote Management > Trust Domain

Click the 'Add Trust Domain' button to enter the IP address of the management station permitted to access the local management services.

+ Add Trust Domain

IP Address	Delete
------------	--------

The following table describes the fields in this screen.

Table 68 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.

21.5 The Add Trust Domain Screen

Configure a public IP address which you want to allow access to the Zyxel Device. Click the **Add Trust Domain** button in the **Maintenance > Remote Management > Trust Domain** screen to open the following screen.

Figure 112 Maintenance > Remote Management > Trust Domain > Add Trust Domain

The following table describes the fields in this screen.

Table 69 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 22

TR-069 Client

22.1 Overview

This chapter explains how to configure the Zyxel Device's TR-069 auto-configuration settings.

22.2 The TR-069 Client Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your Zyxel Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the Zyxel Device, modify settings, perform firmware upgrades as well as monitor and diagnose the Zyxel Device. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Allow your Zyxel Device to be managed remotely by an Auto Configuration Server (ACS) using TR-069.

Click **Maintenance > TR-069 Client** to open the following screen.

Figure 113 Maintenance > TR-069 Client

TR-069 Client

TR-069 is a remote management tool on this modem. The operator can upgrade firmware, modify settings, and diagnose problems remotely when TR-069 is enabled.

CWMP Active ☒

Inform ☒

Inform Interval

IP Protocol ☐ TR069 on IPv4 Only ☐ TR069 on IPv6 Only ☒ Auto Select

ACS URL (URL or IPv4 Address / Global IPv6 Address)

ACS User Name

ACS Password

WAN Interface Used by TR-069 Client ☐ Any_WAN ☒ Multi_WAN

☒ Cellular WAN

Display SOAP Messages on Serial Console ☒

Connection Request Authentication ☒

Connection Request User Name

Connection Request Password

Connection Request URL

Validate ACS certificate ☒

Local Certificate Used by TR-069 Client

[Cancel](#) [Apply](#)

The following table describes the fields in this screen.

Table 70 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP Active	CPE WAN Management Protocol (CWMP) enables the Zyxel Device to be remotely configured via a WAN link. Communication between the Zyxel Device and the management server is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC). Click to enable (switch turns blue) to allow the Zyxel Device to be managed by a management server. Otherwise, click to disable (switch turns gray) to disallow the Zyxel Device to be managed by a management server.
Inform	Click to enable (switch turns blue) the Zyxel Device to send periodic inform via TR-069 on the WAN. Otherwise, click to disable (switch turns gray).
Inform Interval	Enter the time interval (in seconds) at which the Zyxel Device sends information to the auto-configuration server.
IP Protocol	Select the type of IP protocol to allow TR-069 to operate on.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.

Table 70 Maintenance > TR-069 Client (continued)

LABEL	DESCRIPTION
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	<p>Select a WAN interface through which the TR-069 traffic passes.</p> <p>If you select Any_WAN, the Zyxel Device automatically passes the TR-069 traffic when any WAN connection is up.</p> <p>If you select Multi_WAN, you also need to select two or more pre-configured WAN interfaces. The Zyxel Device automatically passes the TR-069 traffic when one of the selected WAN connections is up.</p>
Cellular WAN	The Zyxel Device automatically passes the TR-069 traffic when cellular WAN connection is up.
Display SOAP messages on serial console	Click to enable (switch turns blue) the dumping of all SOAP messages during the ACS server communication with the CPE.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	<p>Enter the connection request user name.</p> <p>When the ACS makes a connection request to the Zyxel Device, this user name is used to authenticate the ACS.</p>
Connection Request Password	<p>Enter the connection request password.</p> <p>When the ACS makes a connection request to the Zyxel Device, this password is used to authenticate the ACS.</p>
Connection Request URL	<p>This shows the connection request URL.</p> <p>The ACS can use this URL to make a connection request to the Zyxel Device.</p>
Validate ACS Certificate	Click to enable (switch turns blue) the validation of a local certificate used by TR-069 client.
Local certificate used by TR-069 client	You can choose a local certificate used by TR-069 client. The local certificate should be imported in the Security > Certificates > Local Certificates screen.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore the screen's last saved settings.

CHAPTER 23

Time Settings

23.1 Time Settings Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

23.2 The Time Screen

Configure the Zyxel Device's time based on your local time zone. You can add a time server address, select your time zone, and configure Daylight Savings if your location uses it.

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

Figure 114 Maintenance > Time

In order to get a correct time for the modem, fill in a time server address, select the time zone where this modem is physically located, and complete the daylight saving settings if needed.

Current Date/Time

Current Time 17:38:26
Current Date 2018-12-13

Time and Date Setup

Time Protocol: SNTP (RFC-1769)

First Time Server Address: pool.ntp.org
Second Time Server Address: clock.nyc.he.net
Third Time Server Address: clock.sjc.he.net
Fourth Time Server Address: Other
Fifth Time Server Address: Other

Time Zone

Time Zone: (GMT+08:00) Taipei

Daylight Savings

Active: ☒

Start Rule

Day: ☐ 1 in ☒ Last in Sunday
Month: March
Hour: 2 0

End Rule

Day: ☐ 1 in ☒ Last in Sunday
Month: October
Hour: 3 0


Cancel Apply

The following table describes the fields in this screen.

Table 71 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 71 Maintenance > Time (continued)

LABEL	DESCRIPTION
First ~ Fifth Time Server Address	<p>Select an NTP time server from the drop-down list box.</p> <p>Otherwise, select Other and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server.</p> <p>Select None if you don't want to configure the time server.</p> <p>Check with your ISP/network administrator if you are unsure of this information.</p>
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's not.
Start Rule	<p>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:</p> <p>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.</p> <p>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).</p>
End Rule	<p>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:</p> <p>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.</p> <p>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).</p>
Cancel	Click Cancel to exit this screen without saving.
Apply	Click Apply to save your changes.

CHAPTER 24

Email Notification

24.1 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 via email, you must specify an email server and the email addresses of the sender and receiver.

24.2 The Email Notification Screen

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

Click **Maintenance > Email Notification** to open the **Email Notification** screen.

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

Figure 115 Maintenance > Email Notification

The following table describes the labels in this screen.

Table 72 Maintenance > Email Notification

LABEL	DESCRIPTION
Add New email	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.
User name	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.

Table 72 Maintenance > Email Notification (continued)

LABEL	DESCRIPTION
Email Address	This field displays the email address that you want to be in the from/sender line of the email that the Zyxel Device sends.
Remove	Click this button to delete the selected entry(ies).

24.2.1 Email Notification Edit

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

Figure 116 Email Notification > Add

The screenshot shows the 'Add New e-mail' configuration screen. It features a title bar with a back arrow and the text 'Add New e-mail'. Below this is the 'E-mail Notification Configuration' section. It contains several input fields: 'Mail Server Address' (with a note '(SMTP Server NAME or IP)'), 'Port' (with '25' entered and a note 'Default:25'), 'Authentication Username', 'Authentication Password' (with a visibility toggle icon), and 'Account e-mail Address'. At the bottom of the configuration section are radio buttons for 'Connection Security', with 'STARTTLS' selected. At the very bottom of the screen are 'Cancel' and 'OK' buttons.

The following table describes the labels in this screen.

Table 73 Email 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 email Address field. If this field is left blank, reports, logs or notifications will not be sent via email.
Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication User name	Enter the user name (up to 32 characters). This is usually the user name of a mail account you specified in the Account email Address field.
Authentication Password	Enter the password associated with the user name above.
Account email Address	Enter the email address that you want to be in the from/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.

Table 73 Email Notification > Add (continued)

LABEL	DESCRIPTION
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 25

Log Setting

25.1 Log Setting Overview

You can configure where the Zyxel Device sends logs and which logs and/or immediate alerts the Zyxel Device records.

25.2 The Log Setting Screen

If there is a LAN client on your network or a remote server that is running a syslog utility, you can save log files from LAN computers to it by enabling **Syslog Logging**, selecting **Remote** or **Local File and Remote** in the **Mode** field, and entering the IP address of the syslog server in the **Syslog Server** field. **Remote** allows you to store logs on a syslog server, while **Local File** allows you to store them on the Zyxel Device. **Local File and Remote** means your logs are stored both on the Zyxel Device and on a syslog server. To change your Zyxel Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 117 Maintenance > Log Setting

Syslog Setting

Syslog Logging ☒

Mode Local File and Remote

Syslog Server 0.0.0.0 (Server NAME or IPv4/IPv6 Address)

UDP Port 514 (Server Port)

E-mail Log Settings

E-mail Log Settings ☒

Mail Account Select one account

System Log Mail Subject

Security Log Mail Subject

Send Log to (E-Mail Address)

Send Alarm to (E-Mail Address)

Alarm Interval 60 (seconds)

Active Log

System Log

☐ WAN-DHCP

☒ DHCP Server

☒ TR-069

☐ HTTP

☐ UPNP

☐ System

☐ ACL

☒ Wireless

☒ 3G/LTE

Security Log

☒ Account

☐ Attack

☐ Firewall

☐ MAC Filter

Cancel Apply

The following table describes the fields in this screen.

Table 74 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Settings	
Syslog Logging	Click the switch (it will turn blue) to enable syslog logging.
Mode	<p>Select Remote to have the Zyxel Device send it to an external syslog server.</p> <p>Select Local File to have the Zyxel Device save the log file on the Zyxel Device itself.</p> <p>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.</p> <p>Note: A warning appears upon selecting Remote or Local File and Remote. Just click OK to continue.</p>
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.

Table 74 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
UDP Port	Enter the port number used by the syslog server.
Email Log Settings	
Email Log Setting	Click the switch (it will turn blue) to allow the sending via 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 > Email Notifications screen.
Mail Account	Select a server specified in Maintenance > Email 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 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 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 email 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 Logs that you want to record.
Security Log	Select the categories of Security Logs that you want to record.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

CHAPTER 26

Firmware Upgrade

26.1 Overview

This chapter explains how to upload new firmware to your Zyxel Device. You can download new firmware releases from your nearest Zyxel FTP site (or www.zyxel.com) to use to upgrade your Zyxel Device's performance.

Only use firmware for your Zyxel Device's specific model. Refer to the label on the bottom of your Zyxel Device.

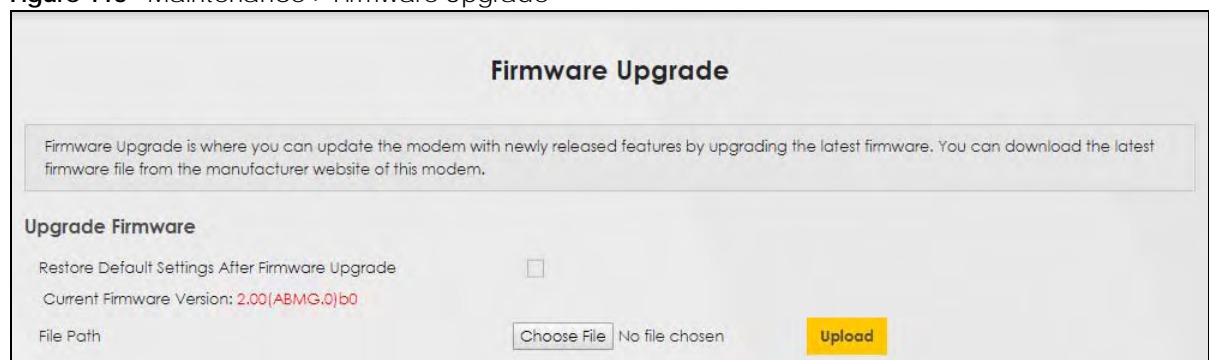
26.2 The Firmware Upgrade Screen

Upload new firmware to your Zyxel Device by downloading the latest firmware file from the Zyxel website. Then, upload it to your Zyxel Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three 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 118 Maintenance > Firmware Upgrade



The screenshot shows the 'Firmware Upgrade' web interface. At the top, the title 'Firmware Upgrade' is centered. Below it, a text box explains: 'Firmware Upgrade is where you can update the modem with newly released features by upgrading the latest firmware. You can download the latest firmware file from the manufacturer website of this modem.' Under the heading 'Upgrade Firmware', there is a checkbox for 'Restore Default Settings After Firmware Upgrade' which is currently unchecked. Below this, the 'Current Firmware Version' is displayed as '2.00(ABMG.0)b0'. At the bottom, there is a 'File Path' label, a 'Choose File' button, the text 'No file chosen', and a yellow 'Upload' button.

The following table describes the labels in this screen.

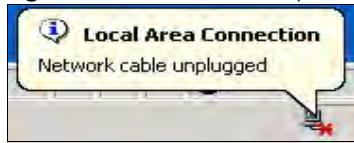
Table 75 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	Use these fields to upload firmware to the Zyxel Device.
Restore Default Settings After Firmware Upgrade	Click to enable this option that restores the factory-default to the Zyxel Device after upgrading the firmware. Note: Make sure to backup the Zyxel Device's configuration settings first in case the restore to factory-default process is not successful. Refer to Section 27.2 on page 169 .
Current Firmware Version	This is the present firmware version.
File Path	Type in the location of the file you want to upload in this field or click Choose File to find it.
Choose File	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 three minutes.

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

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 119 Network Temporarily Disconnected



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

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

CHAPTER 27

Backup/Restore

27.1 Backup/Restore Overview

Back up and restore your Zyxel Device configurations. You can also reset your Zyxel Device settings back to the factory default.

27.2 The Backup/Restore Screen

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

Figure 120 Maintenance > Backup/Restore

The screenshot shows the 'Backup/Restore' web interface. At the top, there's a title 'Backup/Restore'. Below it, a message box states: 'You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.' The interface is divided into three main sections: 'Backup Configuration', 'Restore Configuration', and 'Back to Factory Default Settings'. The 'Backup Configuration' section has a 'Backup' button. The 'Restore Configuration' section has a 'File Path' label, a 'Choose File' button, a 'No file chosen' text, and an 'Upload' button. The 'Back to Factory Default Settings' section has a 'Reset' button and a list of default settings: Password will be 1234, LAN IP address will be 192.168.1.1, and DHCP will be reset to default setting.

Backup/Restore

You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.

Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Backup

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path No file chosen

Back to Factory Default Settings

Click Reset to clear all user-entered configuration information and return to factory default settings. After resetting, the

- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to default setting

Reset

Backup Configuration

Backup Configuration allows you to back up (save) the Zyxel Device's current configuration to a file on your computer. Once the 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 76 Restore Configuration

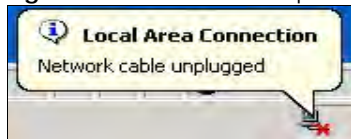
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Choose File to find it.
Choose File	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the 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 121 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).

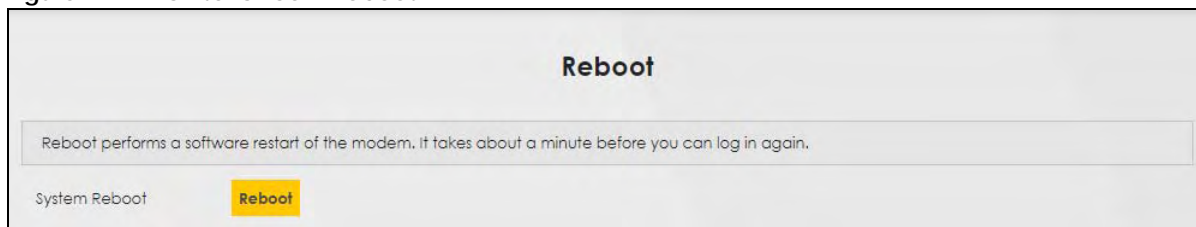
If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

27.3 The Reboot Screen

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 122 Maintenance > Reboot



CHAPTER 28

Diagnostic

28.1 Diagnostic Overview

You can use different diagnostic methods to test a connection and see the detailed information. The **Diagnostic** screens display information to help you identify problems with the Zyxel Device.

28.2 The Ping/TraceRoute/Nslookup Test Screen

Perform ping, traceroute, or nslookup 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 Ping/Traceroute Test area. Use nslookup to find the IP address for a host name and vice versa. Click **Maintenance > Diagnostic** to open the **Ping/TraceRoute/Nslookup** screen shown next.

Figure 123 Maintenance > Diagnostic > Ping/Trace Route/Nslookup

The screenshot displays the 'Diagnostic' web interface. At the top, the title 'Diagnostic' is centered. Below it, a text box explains: 'Ping and TraceRoute are network utilities used to test whether a particular host is reachable. Enter either an IP address or a host name and click one of the buttons to start a Ping or TraceRoute test. The test result will be shown in the Info area.' Underneath this is the 'Ping/TraceRoute Test' section, which contains a large, empty rectangular area for test results. At the bottom left, there is a 'TCP/IP' label and an 'Address' input field. To the right of the input field are five yellow buttons: 'Ping', 'Ping 6', 'Trace Route', 'Trace Route 6', and 'Nslookup'.

The following table describes the fields in this screen.

Table 77 Maintenance > Diagnostic

LABEL	DESCRIPTION
Ping/ TraceRoute Test	The result of tests is shown here in the info area.
TCP/IP	
Address	Enter either an IP address or a host name to start a test.
Ping	Click this button 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	Click this button 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	Click this button to perform the IPv4 trace route function. This determines the path a packet takes to the specified host.
Trace Route 6	Click this button to perform the IPv6 trace route function. This determines the path a packet takes to the specified host.
Nslookup	Click this button to perform a DNS lookup on the IP address or host name.

CHAPTER 29

Troubleshooting

29.1 Overview

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

- [Power and Hardware Connections](#)
- [Zyxel Device Access and Login](#)
- [Internet Access](#)
- [UPnP](#)
- [SIM Card](#)
- [Wireless Signal](#)

29.2 Power and Hardware Connections

[The Zyxel Device does not turn on.](#)

- 1 Make sure the Zyxel Device is turned on.
- 2 Make sure you are using the power adapter and cable (Power over Ethernet, PoE) included with the Zyxel Device.
- 3 Make sure the PoE is connected to the Zyxel Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the Zyxel Device off and on.
- 5 If the problem continues, contact the vendor.

29.3 Zyxel Device Access and Login

[I forgot the IP address for the Zyxel Device.](#)

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the Zyxel Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, 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 (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the Zyxel Device to its factory defaults. Refer to [Section 27.2 on page 169](#).

I forgot the password.

- 1 The default admin password is **1234**.
- 2 If you can't remember the password, you have to reset the Zyxel Device to its factory defaults. Refer to [Section 27.2 on page 169](#).

I cannot see or access the **Login** screen in the Web Configurator.

- 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 ([Section 7.2 on page 66](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Zyxel Device](#).
- 2 Check the hardware connections, see the Quick Start Guide.
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
- 4 Reset the Zyxel Device to its factory default, and try to access the Zyxel Device with the default IP address. Refer to [Section 27.2 on page 169](#).
- 5 If the problem continues, contact the network administrator or vendor, or try the advanced suggestion.

Advanced Suggestion

- 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 can see the **Login** screen, but I cannot log in to the Zyxel Device.

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields 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. See [Section 29.2 on page 174](#).

[I cannot use FTP, Telnet, SSH or Ping to access the Zyxel Device.](#)

See the Remote Management [Section on page 150](#) for details on allowing web services (such as HTTP, HTTPS, FTP, Telnet, SSH and Ping) to access the Zyxel Device.

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.

29.4 Internet Access

[I cannot access the Internet.](#)

- 1 Check the hardware connections and make sure the LEDs are behaving as expected. See the **Quick Start Guide** and [Section 1.6 on page 15](#).
- 2 Check the SIM card. Maybe it has wrong settings (refer to [Section 5.3 on page 36](#)), the account has expired, it became loose (remove and reinsert it - refer to the Quick Start Guide) or it's missing (stolen). See [Section 29.6 on page 178](#) for possible SIM card problems.
- 3 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 4 If the problem continues, contact your ISP.

[I cannot access the Internet anymore. I had access to the Internet \(with the Zyxel Device\), but my Internet connection is not available anymore.](#)

- 1 Check the hardware connections (refer to the Quick Start Guide).
- 2 Turn the Zyxel Device off and on.
- 3 If the problem continues, contact your ISP.

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 Turn the Zyxel Device off and on.
- 3 If the problem continues, contact the network administrator or vendor, or try the advanced suggestion (refer to [I cannot see or access the Login screen in the Web Configurator](#) in this chapter).

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

29.5 UPnP

When using UPnP and the Zyxel Device reboots, my computer cannot detect UPnP and refresh [My Network Places > Local Network](#).

- 1 Make sure that UPnP is enabled in your computer. For Windows 7, see [Section 7.6 on page 74](#). For Windows 10, see [Section 7.7 on page 77](#).
- 2 Make sure that UPnP is enabled in the **Network Settings > Home Networking > UPnP** screen. See [Section 7.4 on page 72](#) for details.
- 3 Disconnect the Ethernet cable from the Zyxel Device's Ethernet port or from your computer.
- 4 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN Messenger.

- 1 Wait more than three minutes.
- 2 Restart the applications.

29.6 SIM Card

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.

29.7 Cellular Signal

How should I position the Zyxel Device to get a strong cellular signal?

- 1 Find the location of your nearest cellular base station(s), 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.

Note: It is best to test towards more than one cellular site, as the nearest site / line-of-sight is not always the best due to the terrain, interference, density of usage, etc. All of these factors influence the stability, availability and throughput of the link to the Zyxel Device.

- 2 Position the Zyxel Device towards a direction where coverage is expected (example the nearest town).
- 3 Conduct test measurements using the Web Configurator's **System Monitor > Cellular WAN Status** screen to obtain a report of the cellular network signal strength and quality at various test positions.

Note: It is best to reboot the Zyxel Device before each test measurement is taken to ensure that it is not camping on the previous cellular site. This is because the Zyxel Device can 'lock' onto the previous cellular site even when the new cellular site is at a much better signal level and quality.

Although installing the Zyxel Device as high as possible is the usual rule of thumb, it is sometimes possible that the Zyxel Device is in a weak coverage spot at that specific height. Adjust the height to achieve the best service possible.

Note: Cellular network signals and quality can fluctuate. A measurement taken now and a few moments later can differ substantially even if nothing apparent has changed – this can be due to many aspects, such as fading, reflections, interference, capacity due to high network traffic, etc.

It is possible that the network topology and usage changes over time, even from one minute to the next as network utilization increases. If poor performance is experienced at a later stage, re-test different installation locations again. It is possible that the current serving cellular site has become over utilized or is out-of-service. As the network design and topology changes, so will the experience change, either for the better or for the worse.

PART III

Appendices

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

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.

See <http://www.zyxel.com/homepage.shtml> and also http://www.zyxel.com/about_zyxel/zyxel_worldwide.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 Zyxel Device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- Zyxel Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- Zyxel Kazakhstan
- <http://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- Zyxel BY
- <http://www.zyxel.by>

Belgium

- Zyxel Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

Bulgaria

- Zyxel България
- <http://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- Zyxel Communications A/S
- <http://www.zyxel.dk>

Estonia

- Zyxel Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- Zyxel Communications
- <http://www.zyxel.fi>

France

- Zyxel France
- <http://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- Zyxel Hungary & SEE
- <http://www.zyxel.hu>

Italy

- Zyxel Communications Italy
- <http://www.zyxel.it/>

Latvia

- Zyxel Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- Zyxel Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- Zyxel Benelux
- <http://www.zyxel.nl>

Norway

- Zyxel Communications
- <http://www.zyxel.no>

Poland

- Zyxel Communications Poland
- <http://www.zyxel.pl>

Romania

- Zyxel Romania
- <http://www.zyxel.com/ro/ro>

Russia

- Zyxel Russia
- <http://www.zyxel.ru>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- Zyxel Communications ES Ltd
- <http://www.zyxel.es>

Sweden

- Zyxel Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

- Zyxel Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- Zyxel Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Ecuador

- Zyxel Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- Zyxel Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- Zyxel Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

Oceania

Australia

- Zyxel Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

APPENDIX B

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 3.4×10^{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 78 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 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 (0:0:0:0:0:1 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 79 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 servers on a local site.

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

Table 80 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

Table 80 Reserved Multicast Address (continued)

MULTICAST ADDRESS
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 ffe 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.

MAC	00 : 13 : 49 : 12 : 34 : 56
EUI-64	02 : 13 : 49 : FF : FE : 12 : 34 : 56

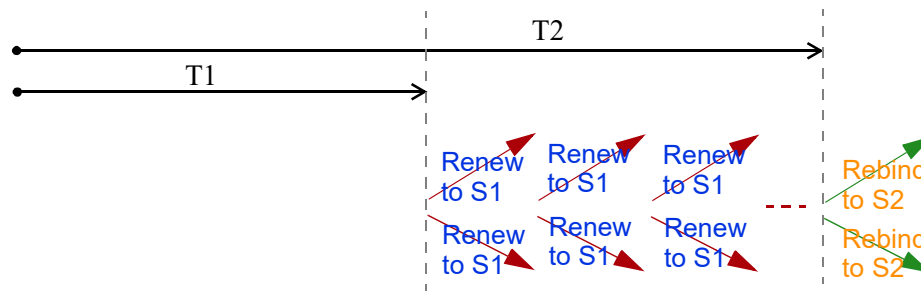
Identity Association

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 unreach, 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.

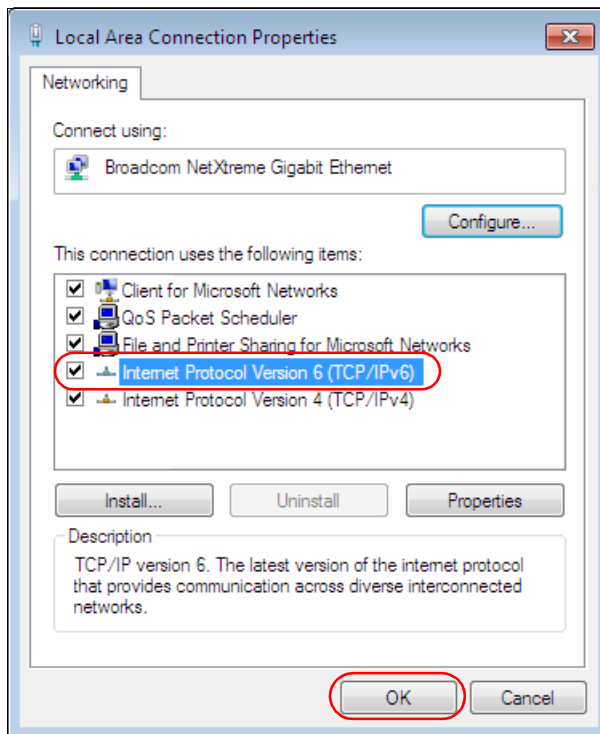
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected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

Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 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:feaa:7125%11  
                                172.16.100.254
```

APPENDIX B

Legal Information

Copyright

Copyright © 2019 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

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 EMC statement

- This 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. generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- This product has been tested and complies with the specifications 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 according to 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 device does cause harmful interference to radio or television reception, which is found 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 or devices
 - Connect the equipment to an outlet other than the receiver's
 - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area

FCC Radiation exposure statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This transmitter must be at least 30 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.

CANADA

The following information applies if you use the product within Canada area

Innovation, Science and Economic Development Canada ICES statement

CAN ICES-3 (B)/NMB-3(B)

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 statement

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter (2468C-LTE7461M602) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Antenna information

Chain NO.	Antenna Type	Frequency range	WiFi Gain (dBi)	LTE Gain (dBi)	Connector
WLAN-ANT0	PIFA	2.4 ~ 2.4835 GHz	6	N.A.	iPEX
WLAN-ANT1	PIFA	2.4 ~ 2.4835 GHz	5	N.A.	iPEX
WWAN	Dipole	2500 ~ 2570 MHz	N.A.	9	iPEX
		698 ~ 716 MHz	N.A.	3.5	iPEX
		777 ~ 787 MHz	N.A.	3	iPEX
		1850 ~ 1915 MHz	N.A.	8	iPEX
		814 ~ 849 MHz	N.A.	3.6	iPEX
		2305 ~ 2315 MHz	N.A.	9	iPEX
		1710 ~ 1780 MHz	N.A.	7	iPEX

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,

- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna models(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the produce with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz, the following attention must be paid.

- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands

5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit

- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio (2468C-LTE7461M602) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

informations antenne

Chaîne NB.	Antenne Type	Gamme de fréquences	WiFi Gain (dBi)	LTE Gain (dBi)	Connecteur
WLAN-ANT0	PIFA	2.4 ~ 2.4835 GHz	6	N.A.	iPEX
WLAN-ANT1	PIFA	2.4 ~ 2.4835 GHz	5	N.A.	iPEX
WWAN	Dipole	2500 ~ 2570 MHz	N.A.	9	iPEX
		698 ~ 716 MHz	N.A.	3.5	iPEX
		777 ~ 787 MHz	N.A.	3	iPEX
		1850 ~ 1915 MHz	N.A.	8	iPEX
		814 ~ 849 MHz	N.A.	3.6	iPEX
		2305 ~ 2315 MHz	N.A.	9	iPEX
		1710 ~ 1780 MHz	N.A.	7	iPEX

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes

- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

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 30 cm 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 30 cm de distance entre la source de rayonnement et votre corps.

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your Zyxel Device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the Zyxel Device ventilation slots as insufficient airflow may harm your Zyxel Device. For example, do not place the Zyxel Device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this Zyxel Device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the Zyxel Device.
- Do not open the Zyxel Device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this Zyxel Device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this Zyxel 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 adapter first before connecting it to a power outlet.
- Do not allow anything to rest on the power adapter or cord and do NOT place the product where anyone can walk on the power adapter or cord.
- Please use the provided or designated connection cables/power cables/adapters. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adapter or cord is damaged, it might cause electrocution. Remove it from the Zyxel Device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- The following warning statements apply, where the disconnect device is not incorporated in the Zyxel Device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected Zyxel Device, a readily accessible disconnect device shall be incorporated external to the Zyxel Device;
 - For pluggable devices, the socket-outlet shall be installed near the Zyxel Device and shall be easily accessible.

Environment Statement

European Union - 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

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，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。
- 第十四條 低功率射頻電機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。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機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。
- 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，使用或維修此設備。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。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 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 is 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. You may also refer to the warranty policy for the region in which you bought the Zyxel Device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive email notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

A

- access
 - troubleshooting [174](#)
- Access Control (Rules) screen [113](#)
- ACS [155](#)
- activation
 - firewalls [110](#)
- Add New ACL Rule screen [114](#)
- Address Resolution Protocol [136](#)
- Any_WAN
 - Remote Management [151](#)
 - TR-069 traffic [157](#)
- APN information
 - obtain [34](#)
- APN Settings [35](#)
- Application Layer Gateway (ALG) [103](#)
- applications
 - Internet access [13](#)
- ARP Table [136](#), [138](#)
- ARP Table screen [137](#)
- authentication [54](#), [56](#)
 - RADIUS server [56](#)
- Authentication Type
 - APN [36](#)
- Auto Configuration Server, see ACS [155](#)

B

- backup
 - configuration [169](#)
- backup configuration [169](#)
- Backup/Restore screen [169](#)
- Band Configuration Screen [37](#)
- Basic Service Set, see BSS
- blinking LEDs [14](#)
- Broadband [33](#)
- BSS [57](#)
 - example [57](#)

C

- CA [127](#)
- Cellular WAN [151](#)
 - TR-069 traffic [157](#)
- Cellular WAN Screen [34](#)
- Cellular WAN screen [34](#)
- certificate
 - details [129](#)
 - factory default [122](#)
 - file format [128](#)
 - file path [126](#)
 - import [122](#), [125](#)
 - public and private keys [128](#)
 - verification [128](#)
- certificate request
 - create [122](#)
 - view [123](#)
- certificates [121](#)
 - advantages [128](#)
 - authentication [121](#)
 - CA [127](#)
 - creating [122](#)
 - public key [121](#)
 - replacing [122](#)
 - storage space [122](#)
 - thumbprint algorithms [129](#)
 - thumbprints [129](#)
 - trusted CAs [126](#)
 - verifying fingerprints [128](#)
- Certification Authority, see CA
- certifications [196](#)
 - viewing [198](#)
- channel, wireless LAN [54](#)
- client list [70](#)
- configuration
 - backup [169](#)
 - firewalls [110](#)
 - restoring [170](#)
 - static route [106](#)
- contact information [179](#)
- copyright [192](#)

Create Certificate Request screen [122](#)
creating certificates [122](#)
CTS threshold [51, 54](#)
customer support [179](#)
customized service
 add [112](#)
customized services [112, 113](#)

D

data fragment threshold [51, 54](#)
Data Roaming
 enable [35](#)
Denials of Service, see DoS
DHCP [65](#)
DHCP Server Lease Time [68](#)
DHCP Server State [68](#)
diagnostic [172](#)
diagnostic screens [172](#)
digital IDs [121](#)
disclaimer [192](#)
DMZ screen [103](#)
DNS [66](#)
DNS Values [68](#)
domain name system, see DNS
DoS [109](#)
 thresholds [110](#)
DoS protection blocking
 enable [116](#)
dynamic DNS [105](#)
 wildcard [105](#)
Dynamic Host Configuration Protocol, see DHCP
DYNDNS wildcard [105](#)

E

email
 log setting [166](#)
Extended Service Set IDentification [44](#)

F

factory-default
 RESET button [15](#)
filters
 MAC address [46, 55](#)
firewall
 enhancing security [117](#)
 security considerations [118](#)
 traffic rule direction [115](#)
Firewall DoS screen [115](#)
Firewall General screen [111](#)
firewall rules
 direction of travel [116](#)
firewalls [109, 110](#)
 actions [115](#)
 configuration [110](#)
 customized services [112, 113](#)
 DoS [109](#)
 thresholds [110](#)
 ICMP [109](#)
 rules [116](#)
 security [117](#)
firmware [167](#)
 version [28](#)
Firmware Upgrade screen [167](#)
firmware upload [167](#)
firmware version
 check [168](#)
fragmentation threshold [51, 54](#)
FTP [96](#)
 unusable [176](#)

G

General wireless LAN screen [43](#)

H

hardware connections
 troubleshooting [174](#)

I

- IANA [73](#)
- ICMP [109](#)
- Import Certificate screen [126](#)
- importing trusted CAs [126](#)
- Internet
 - no access [176](#)
 - wizard setup [23](#)
- Internet access [13](#)
 - wizard setup [23](#)
- Internet Assigned Numbers Authority
 - See IANA
- Internet connection
 - slow or erratic [176](#)
- Internet Control Message Protocol, see ICMP
- Internet Protocol version 6, see IPv6
- IP address
 - WAN [34](#)
- IP Passthrough mode [41](#)
- IP Passthrough screen [20, 40](#)
- IPv4 firewall [111](#)
- IPv6 [185](#)
 - addressing [185](#)
 - EUI-64 [187](#)
 - global address [185](#)
 - interface ID [187](#)
 - link-local address [185](#)
 - Neighbor Discovery Protocol [185](#)
 - ping [185](#)
 - prefix [185](#)
 - prefix length [185](#)
 - unspecified address [186](#)
- IPv6 firewall [111](#)

L

- LAN [65](#)
 - client list [70](#)
 - MAC address [71](#)
 - status [29, 32](#)
- LAN IP address [68](#)
- LAN IPv6 Mode Setup [68](#)
- LAN Setup screen [66](#)
- LAN subnet mask [68](#)

- limitations
 - wireless LAN [56](#)
 - WPS [63](#)
- Local Area Network, see LAN
- local certificate
 - TR-069 client [157](#)
- Local Certificates screen [121](#)
- Log Setting screen [164](#)
- login [16](#)
 - passwords [16](#)
 - troubleshooting [174](#)
- Login screen
 - no access [175](#)
- logs [130, 133, 141, 164](#)

M

- MAC Address
 - LAN [71](#)
- MAC address [47, 71](#)
 - filter [46, 55](#)
- MAC authentication [46](#)
- Mac filter [119](#)
- managing the device
 - good habits [14](#)
 - using FTP. See FTP.
- MGMT Services screen [150, 151](#)
- MSN Messenger
 - problem [177](#)
- Multi_WAN
 - Remote Management [151](#)
 - TR-069 traffic [157](#)

N

- NAT
 - default server [103](#)
 - DMZ host [103](#)
 - multiple server example [97](#)
- NAT ALG screen [103](#)
- Network Address Translation, see NAT
- network disconnect
 - temporary [168](#)

network map [20, 26](#)

network type
select [38](#)

Nslookup test [173](#)

P

password
admin [175](#)
good habit [14](#)
lost [175](#)
user [175](#)

passwords [16](#)

PBC [58](#)

PIN Protection [37](#)

PIN, WPS [58](#)
example [60](#)

Ping
unusable [176](#)

Ping test [173](#)

Ping/TraceRoute/Nslookup screen [172](#)

PLMN Configuration Screen [38](#)

PoE injector [13](#)

port forwarding rule
add/edit [98](#)

Port Forwarding screen [97, 98](#)

Port Triggering
add new rule [101](#)

Port Triggering screen [99](#)

ports [14](#)

power
troubleshooting [174](#)

preamble [52, 54](#)

preamble mode [57](#)

problem
troubleshooting [174](#)

Protocol (Customized Services) screen [111](#)

Protocol Entry
add [112](#)

Push Button Configuration, see PBC

push button, WPS [58](#)

R

RADIUS server [56](#)

Reboot screen [170](#)

remote management
TR-069 [155](#)

Remote Procedure Calls, see RPCs [155](#)

RESET Button [15](#)

restart system [170](#)

restore default settings
after firmware upgrade [168](#)

restoring configuration [170](#)

RFC 1058. See RIP.

RFC 1389. See RIP.

RFC 1631 [95](#)

RFC 3164 [130](#)

RIP [93](#)

router features [13](#)

Routing Information Protocol. See RIP

Routing Table screen [139](#)

RPPCs [155](#)

RTS threshold [51, 54](#)

S

security
network [117](#)
wireless LAN [54](#)

Security Log [131](#)

service access control [150, 151, 153](#)

Service Set [44](#)

setup
firewalls [110](#)
static route [106](#)

SIM card
status [143](#)

SIM configuration [36](#)

SSH
unusable [176](#)

SSID [55](#)

Static DHCP
Configuration [71](#)

Static DHCP screen [70](#)

- static route [87, 93](#)
 - configuration [106](#)
- status [26](#)
 - firmware version [28](#)
 - LAN [29, 32](#)
 - WAN [28](#)
 - wireless LAN [29](#)
- status indicators [14](#)
- syslog
 - protocol [130](#)
 - severity levels [130](#)
- syslog logging
 - enable [165](#)
- syslog server
 - name or IP address [165](#)
- system
 - firmware [167](#)
 - version [28](#)
 - passwords [16](#)
 - status [26](#)
 - LAN [29, 32](#)
 - WAN [28](#)
 - wireless LAN [29](#)
 - time [158](#)

T

- Telnet
 - unusable [176](#)
- The [34](#)
- thresholds
 - data fragment [51, 54](#)
 - DoS [110](#)
 - RTS/CTS [51, 54](#)
- time [158](#)
- TR-069 [155](#)
 - ACS setup [155](#)
 - authentication [157](#)
- TR-069 Client screen [155](#)
- Trace Route test [173](#)
- troubleshooting [174](#)
- Trust Domain
 - add [153](#)
- Trust Domain screen [152](#)
- Trusted CA certificate

- view [126](#)
- Trusted CA screen [125](#)
- Turning on UPnP
 - Windows 7 example [74](#)

U

- Universal Plug and Play, see UPnP
- upgrading firmware [167](#)
- UPnP [72](#)
 - forum [66](#)
 - security issues [66](#)
 - State [72](#)
 - undetectable [177](#)
 - usage confirmation [66](#)
- UPnP screen [72](#)
- UPnP-enabled Network Device
 - auto-discover [75, 79](#)

W

- WAN
 - status [28](#)
 - Wide Area Network, see WAN [33](#)
- warranty [198](#)
 - note [199](#)
- Web Configurator
 - easy access [82](#)
- web configurator
 - login [16](#)
 - passwords [16](#)
- WEP Encryption [46](#)
- Wireless General screen [43](#)
- wireless LAN [42](#)
 - authentication [54, 56](#)
 - BSS [57](#)
 - example [57](#)
 - channel [54](#)
 - example [53](#)
 - fragmentation threshold [51, 54](#)
 - limitations [56](#)
 - MAC address filter [46, 55](#)
 - preamble [52, 54](#)
 - RADIUS server [56](#)

- RTS/CTS threshold [51](#), [54](#)
- security [54](#)
- SSID [55](#)
- status [29](#)
- WPS [58](#), [60](#)
 - example [61](#)
 - limitations [63](#)
 - PIN [58](#)
 - push button [58](#)
- wizard setup
 - Internet [23](#)
- WPS [58](#), [60](#)
 - example [61](#)
 - limitations [63](#)
 - PIN [58](#)
 - example [60](#)
 - push button [58](#)