

Table 4 Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
	DoS	Use this screen to activate protection against Denial of Service (DoS) attacks.
MAC Filter	MAC Filter	Use this screen to block or allow traffic from devices of certain MAC addresses to the Zyxel Device.
Parental Control	Parental Control	Use this screen to block web sites with the specific URL.
Scheduler Rule	Scheduler Rule	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
System Monitor		
Log	System Log	Use this screen to view the status of events that occurred to the Zyxel Device. You can export or e-mail the logs.
	Security Log	Use this screen to view all security related events. You can select level and category of the security events in their proper drop-down list window.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the Zyxel Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the Zyxel Device.
	NAT	Use this screen to view NAT statistics for connected hosts.
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Routing Table	Routing Table	Use this screen to view the routing table on the Zyxel Device.
Multicast Status	IGMP Status	Use this screen to view the status of all IGMP settings on the Zyxel Device.
	MLD Status	Use this screen to view the status of all MLD settings on the Zyxel Device.
WLAN Station Status	WLAN Station Status	Use this screen to view the wireless stations that are currently associated with the Zyxel Device.
Maintenance		
System	System	Use this screen to set Device name and Domain name.
User Account	User Account	Use this screen to change user password on the Zyxel Device.
Remote Management	MGMT Services	Use this screen to enable specific traffic directions for network services.
	Trust Domain	Use this screen to view a list of public IP addresses which are allowed to access the Zyxel Device through the services configured in the Maintenance > Remote Management > MGMT Services screen.
SNMP	SNMP	Use this screen to configure SNMP (Simple Network Management Protocol) settings.
Time	Time	Use this screen to change your Zyxel Device's time and date.
E-mail Notification	E-mail Notification	Use this screen to configure up to two mail servers and sender addresses on the Zyxel Device.
Log Settings	Log Setting	Use this screen to change your Zyxel Device's log settings.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your Zyxel Device.

Table 4 Configuration Menus Summary (continued)

LINK	TAB	FUNCTION
Backup/Restore	Backup/Restore	Use this screen to backup and restore your Zyxel Device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the Zyxel Device without turning the power off.
Diagnostic	Ping&Traceroute &Nslookup	Use this screen to identify problems with the Zyxel Device. You can use Ping, TraceRoute, or Nslookup to help you identify problems.
	802.1ag	Use this screen to configure CFM (Connectivity Fault Management) MD (maintenance domain) and MA (maintenance association), perform connectivity tests and view test reports.
	802.3ah	Use this screen to configure link OAM port parameters,

2.2.1.2 Icons

The navigation panel provides some icons on the right hand side.



The icons provide the following functions.

Table 5 Web Configurator Icons



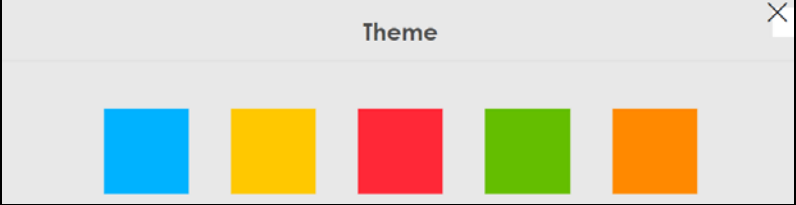



ICON	DESCRIPTION
	Wizard: Click this icon to open screens where you can configure the Zyxel Device's time zone Internet access, and wireless settings. See Chapter 3 on page 31 for more information about the Wizard screens.
	Theme: Click this icon to select a color that you prefer and apply it to the Web Configurator. 

Table 5 Web Configurator Icons

ICON	DESCRIPTION
 Language	Language: Select the language you prefer.
 Restart	Restart: Click this icon to reboot the Zyxel Device without turning the power off.
 Logout	Logout: Click this icon to log out of the Web Configurator.

CHAPTER 3

Quick Start Wizard

3.1 Overview

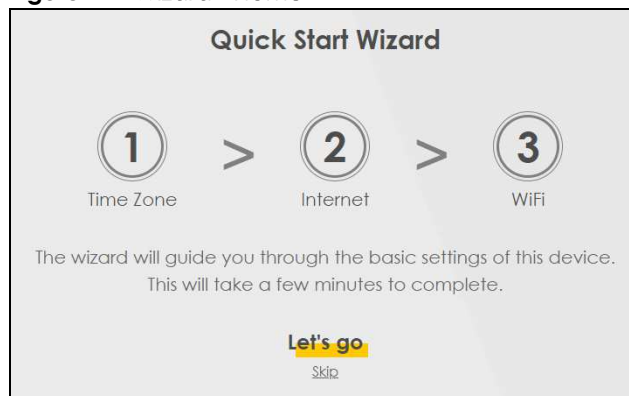
Use the **Wizard** screens to configure the Zyxel Device's time zone, basic Internet access, and wireless settings.

Note: See the technical reference chapters (starting on [Chapter 4 on page 36](#)) for background information on the features in this chapter.

3.2 Wizard Setup

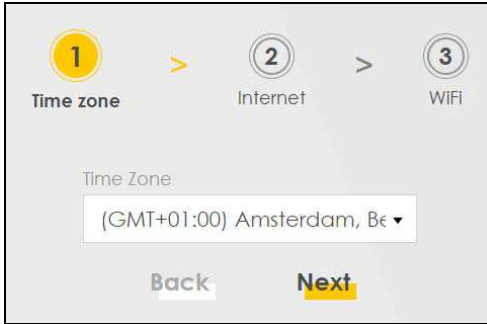
You can click the **Wizard** icon in the navigation panel to open the **Wizard** screens. See [Section 2.2.1 on page 25](#) for more information about the navigation panel. After you click the **Wizard** icon, the following screen appears. Click **Let's Go** to proceed with settings on time zone, basic Internet access, and wireless networks. It will take you a few minutes to complete the settings on the **Wizard** screens. You can also click **Skip** to leave the **Wizard** screens.

Figure 12 Wizard - Home



3.2.1 Time Zone

Select the time zone of your location. Click **Next**.

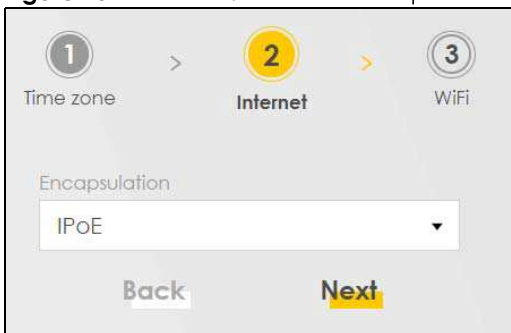
Figure 13 Wizard - Time Zone

3.2.2 Internet

- 1 The Zyxel Device will check the Internet status automatically, and determine your connection type. Click **Next** to proceed. You can also click **Skip** to pass Internet settings in the **Wizard**.

Figure 14 Wizard - Internet

- 2 If the following screen displays, select the encapsulation type your ISP uses. Click **Next**.

Figure 15 Wizard - Select the Encapsulation Type

- 3 Enter your Internet connection information. The screen and fields to enter may vary depending on your current connection type. Click **Next**.

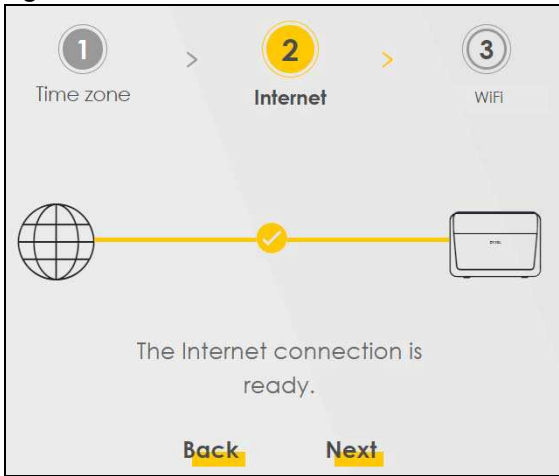
Figure 16 Wizard - Internet Connection Information



The screenshot shows the 'Internet' step of a wizard. At the top, there are three numbered steps: 1 (Time zone), 2 (Internet), and 3 (WiFi). Step 2 is highlighted. Below the steps, there are three input fields: 'Encapsulation' with the value 'PPPoE', 'User Name' with the value 'benvenuto', and 'Password' with six dots. A toggle icon is visible to the right of the password field.

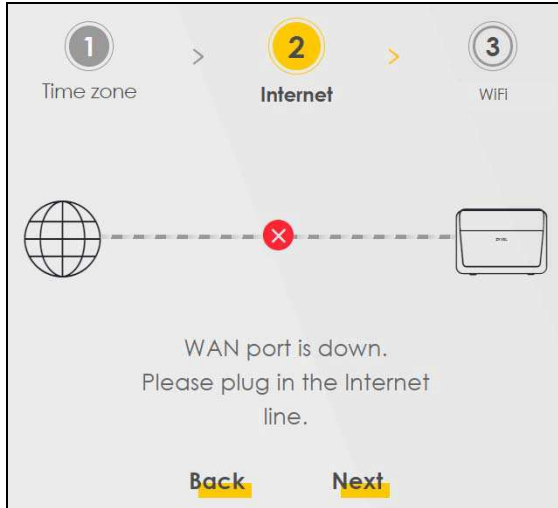
- 4 Click **Next** when the Zyxel Device has a successful Internet connection.

Figure 17 Wizard - Successful WAN Connection



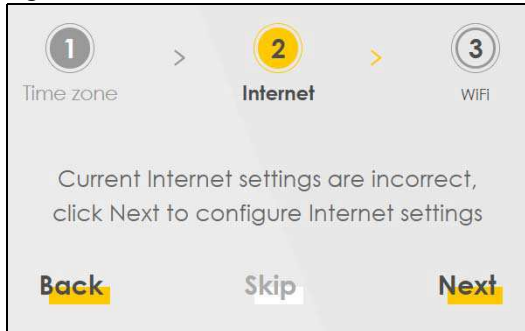
Unsuccessful Internet Connection

The following screen displays when the Zyxel Device did not detect a WAN connection. Connect the WAN port to a broadband modem or router for Internet access if you have not connected any. Click **Next**.

Figure 18 Wizard - WAN Connection is Down

Incorrect Internet Information

If the following screen displays, click **Next** to configure the Internet settings.

Figure 19 Wizard - Incorrect Internet Information

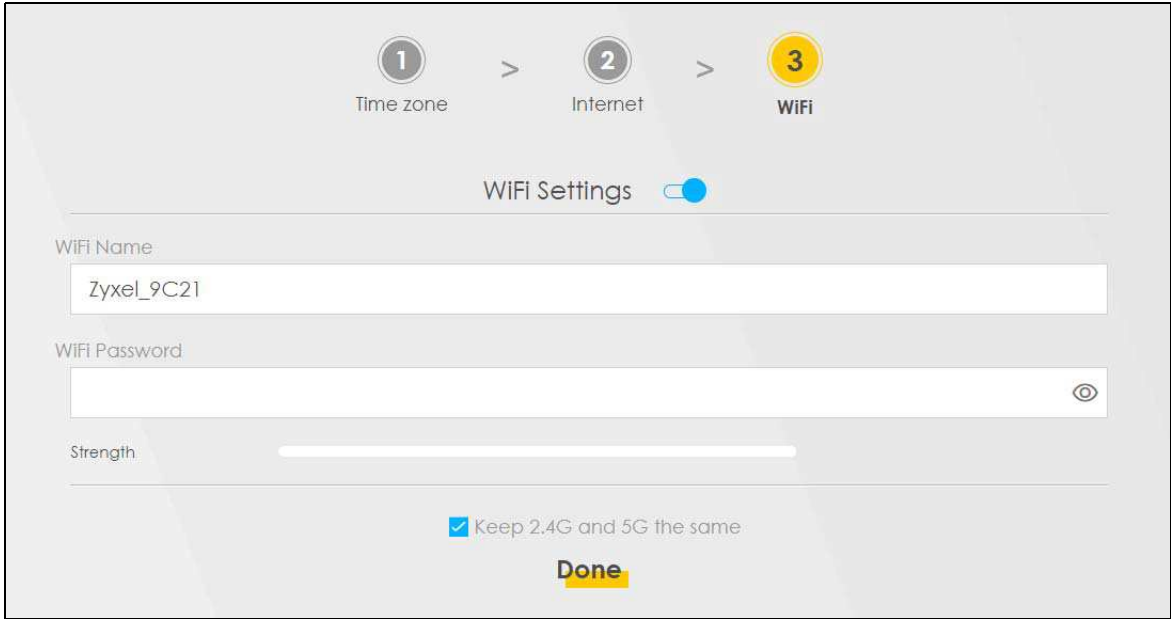
3.2.3 WiFi

Turn WiFi on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the Zyxel Device.

Click the **Keep 2.4G and 5G the same** check box to use the same SSID for 2.4G and 5G wireless networks. Otherwise, deselect the check box to have two different SSIDs for 2.4G and 5G wireless networks. The screen and fields to enter may vary when you select or deselect the check box.

Click **Done** to complete the setup and close the **Wizard** screen.

Figure 20 Wizard - WiFi



CHAPTER 4

Tutorials

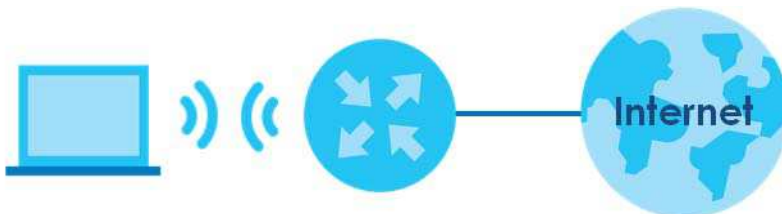
4.1 Overview

This chapter shows you how to use the Zyxel Device's various features.

- [Setting Up a Secure Wireless Network](#), see page 36
- [Setting Up Multiple Wireless Groups](#), see page 43
- [Configuring Static Route for Routing to Another Network](#), see page 48
- [Configuring QoS Queue and Class Setup](#), see page 50
- [Access the Zyxel Device Using DDNS](#), see page 54
- [Configuring the MAC Address Filter](#), see page 56

4.2 Setting Up a Secure Wireless Network

Thomas wants to set up a wireless network so that he can use his notebook to access the Internet. In this wireless network, the Zyxel Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the Zyxel Device. Then he can set up a wireless network using WPS ([Section 4.2.2 on page 38](#)) or manual configuration ([Section 4.2.3 on page 42](#)).

4.2.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network.

SSID	Example
Security Mode	WPA2-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n/ax Mixed

- 1 Click **Network Setting > Wireless** to open the **General** screen. Select **More Secure** as the security level and **WPA2-PSK** as the security mode. Configure the screen using the provided parameters (see [page 36](#)). Click **Apply**.

A Wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than no security to protect your data from unauthorized access or damage via wireless network.

Wireless

Wireless Keep the same settings for 2.4G and 5G wireless networks

Wireless Network Setup

Band: 2.4GHz

Wireless:

Channel: Auto Current : / MHz

Bandwidth: 20MHz

Control Sideband: None

Wireless Network Settings

Wireless Network Name: Example

Max Clients: 32

Hide SSID ! Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.

Multicast Forwarding

Max. Upstream Bandwidth: Kbps

Max. Downstream Bandwidth: Kbps

Note

- (1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.
- (2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.
- (3) If Max. Upstream/Downstream Bandwidth is empty, the device sets the value automatically.
- (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID

Security Level

No Security More Secure (Recommended)

▼

Security Mode: WPA2-PSK

Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits ["0-9", "A-F"].

Password: DoNotStealMyWirelessNetwork 🔒

Strength: strong

Encryption: AES

Timer: 3600 sec

Cancel Apply

- Go to the **Wireless > Others** screen and select **802.11b/g/n/ax Mixed** in the **802.11 Mode** field. Click **Apply**.

The configurations below are the advanced wireless settings.

RTS/CTS Threshold	2347	
Fragmentation Threshold	2346	
Output Power	100%	
Beacon Interval	100	ms
DTIM Interval	1	ms
802.11 Mode	802.11b/g/n/ax Mixed	
802.11 Protection	Auto	
Preamble	Long	
Protected Management Frames	Capable	

Thomas can now use the WPS feature to establish a wireless connection between his notebook and the Zyxel Device (see [Section 4.2.2 on page 38](#)). He can also use the notebook's wireless client to search for the Zyxel Device (see [Section 4.2.3 on page 42](#)).

4.2.2 Using WPS

This section gives you an example of how to set up a wireless network using WPS. This example uses the Zyxel Device as the AP and a WPS-enabled Android smartphone as the wireless client.

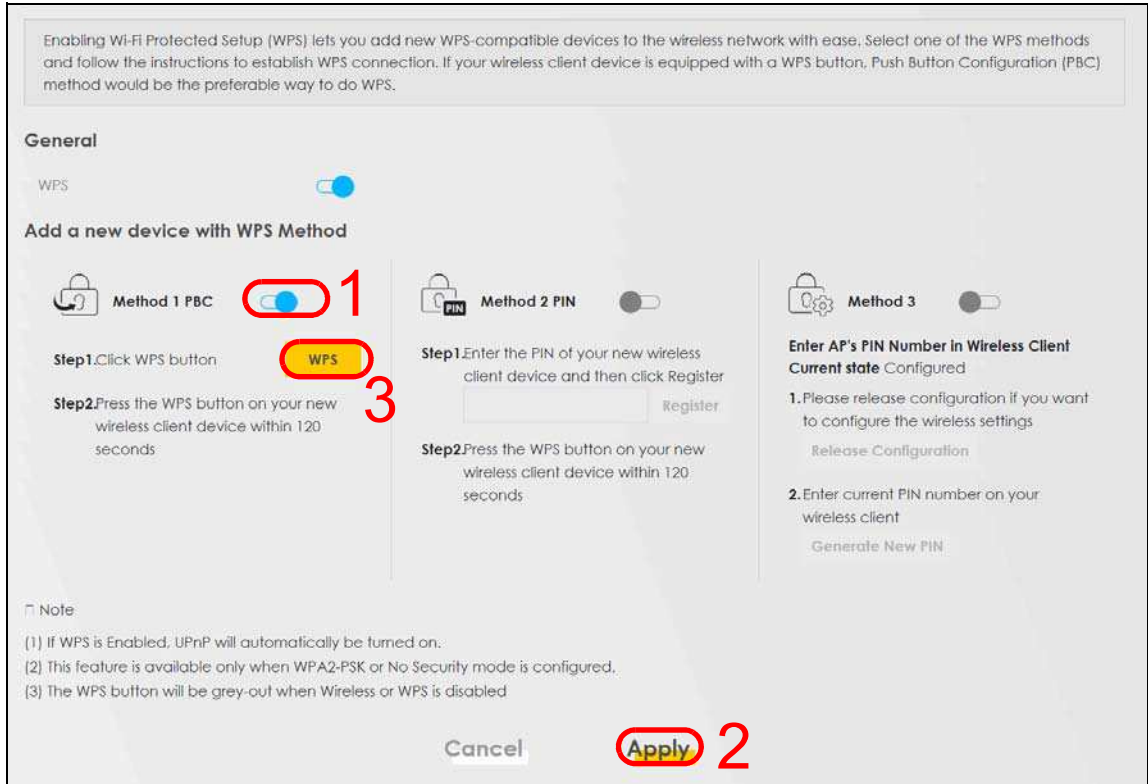
There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section on page 38](#). This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the Zyxel Device's interface. See [Section on page 40](#). This is the more secure method, since one device can authenticate the other.

Note: [When using WPS in the Web Configurator, and depending on your Band selection \(2.4GHz or 5GHz\), the secure connection will apply for the selected Band only.](#)

Push Button Configuration (PBC)

- Make sure that your Zyxel Device is turned on and your notebook is within the cover range of the wireless signal.
- Push and hold the **WPS** button located on the Zyxel Device's front panel for one second. Alternatively, you may log into the Zyxel Device's Web Configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function for method 1 and click **Apply**. Then click the **Connect** button.



Note: Your ZyXel Device has a WPS button located on its side panel as well as a WPS button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It does not matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The ZyXel Device sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the ZyXel Device securely.

The following figure shows you how to set up wireless network and security by pressing a button on both ZyXel Device and wireless client (the Android phone in this example).

Figure 21 Example WPS Process: PBC Method

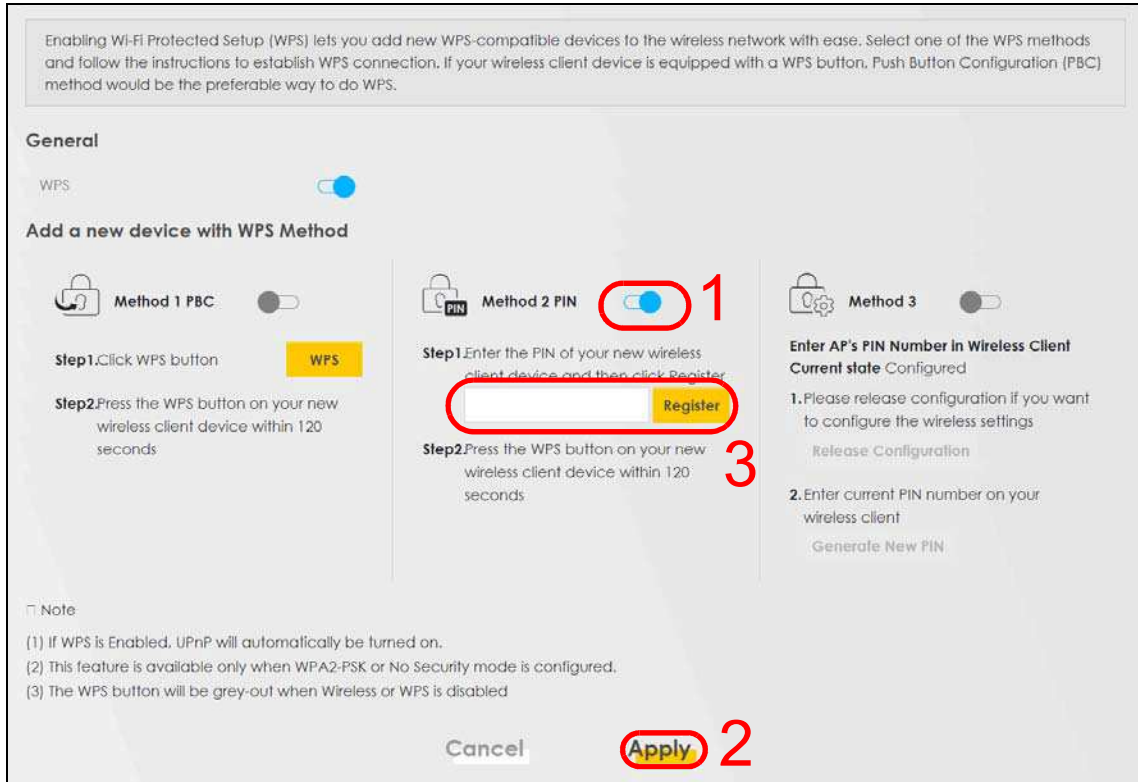
Wireless Client



PIN Configuration

When you use the PIN configuration method, you need to check the client's PIN number and use the Zyxel Device's configuration interface.

- 1 Go to your phone settings and turn on WiFi. Open the WiFi networks list and tap **WPS PIN Entry** to get a PIN number.
- 2 Log into Zyxel Device's Web Configurator and go to the **Network Setting > Wireless > WPS** screen. Enable the WPS function and click **Apply**.



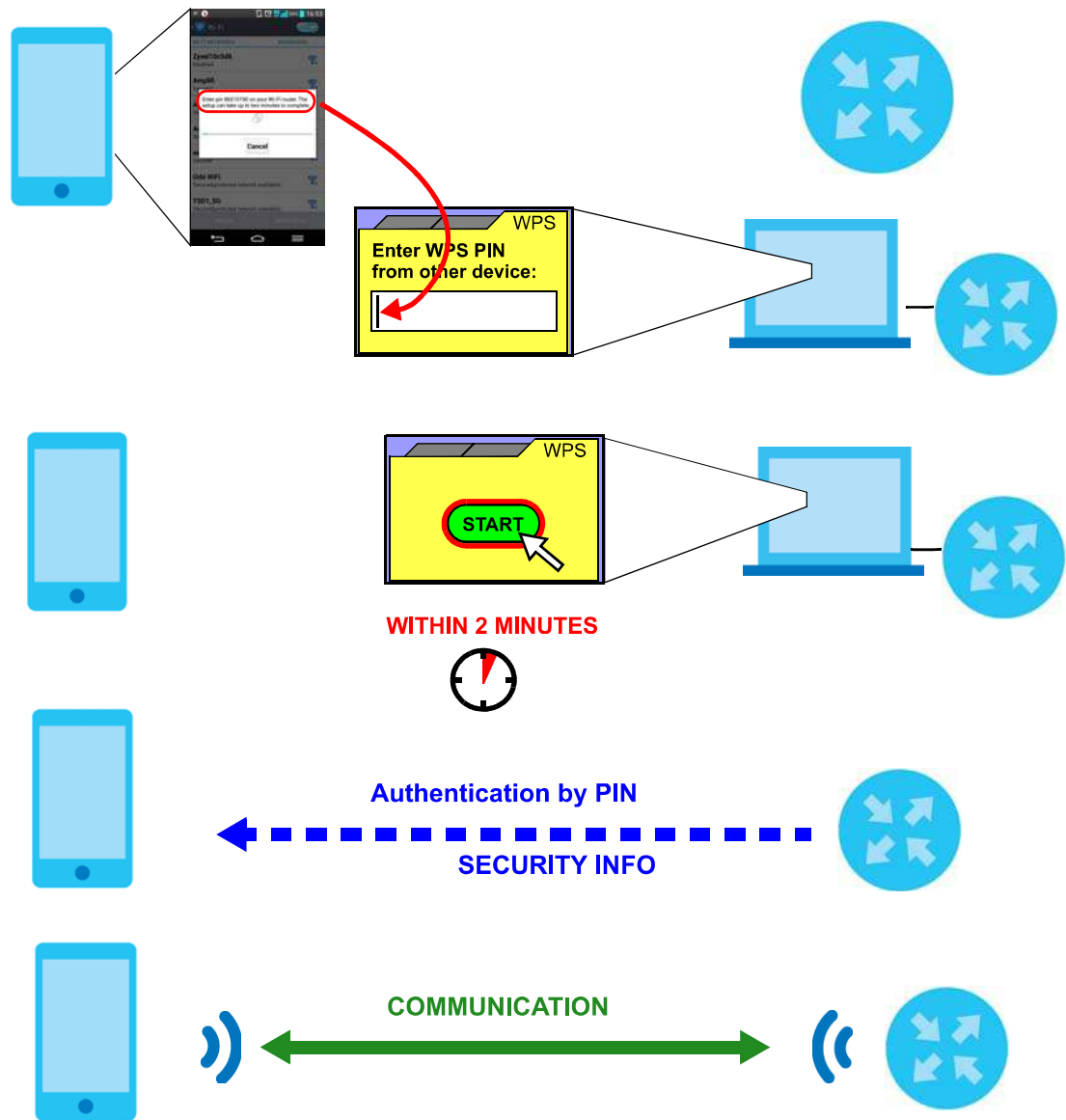
- 3 Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.

The ZyXel Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the ZyXel Device securely.

The following figure shows you how to set up wireless network and security on ZyXel Device and wireless client (Android smartphone in this example) by using the PIN method.

Figure 22 Example WPS Process: PIN Method

Wireless Client



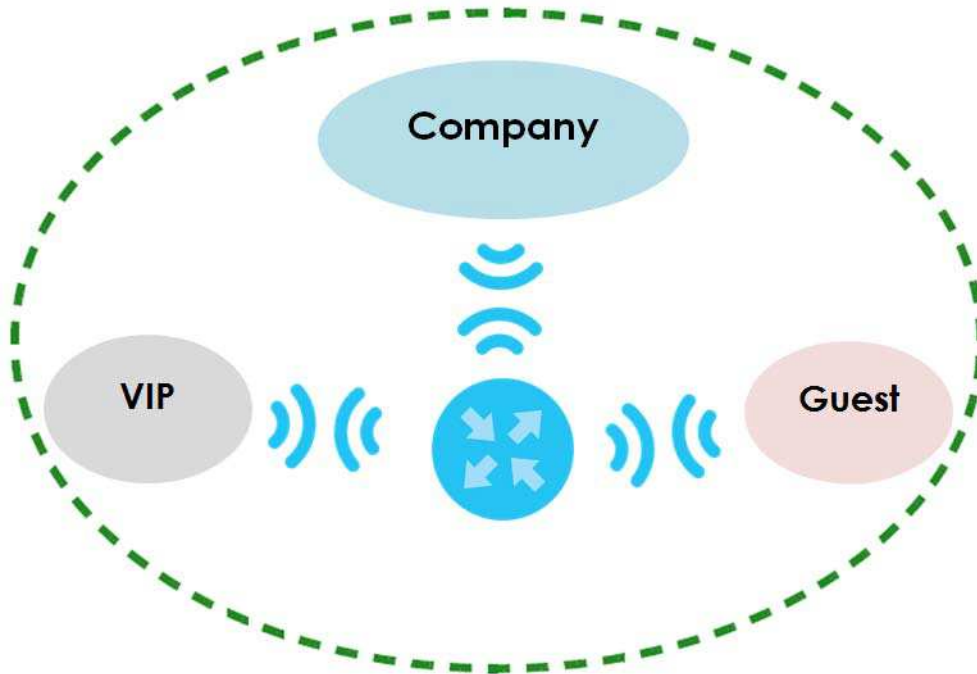
4.2.3 Without WPS

Use the wireless adapter's utility installed on the notebook to search for the "Example" SSID. Then enter the "DoNotStealMyWirelessNetwork" pre-shared key to establish a wireless Internet connection.

Note: The Zyxel Device supports IEEE 802.11 a/b/g/n/ac/ax wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

4.3 Setting Up Multiple Wireless Groups

Company A wants to create different wireless network groups for different types of users as shown in the following figure. Each group has its own SSID and security mode.



- Employees in Company A will use a general **Company** wireless network group.
- Higher management level and important visitors will use the **VIP** group.
- Visiting guests will use the **Guest** group, which has a different SSID and password.

Company A will use the following parameters to set up the wireless network groups.

	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	More Secure
Security Mode	WPA2-PSK	WPA2-PSK	WPA2-PSK
Pre-Shared Key	ForCompanyOnly	123456789	guest123

- 1 Click **Network Setting > Wireless** to open the **General** screen. Use this screen to set up the company's general wireless network group. Configure the screen using the provided parameters and click **Apply**.

A Wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than no security to protect your data from unauthorized access or damage via wireless network.

Wireless

Wireless Keep the same settings for 2.4G and 5G wireless networks

Wireless Network Setup

Band: 2.4GHz
Wireless:
Channel: Auto
Bandwidth: 20MHz
Control Sideband: None

Wireless Network Settings

Wireless Network Name: Company
Max Clients: 32
 Hide SSID i Hide SSID does not support WPS 2.0. You should disable WPS in WPS page.
 Multicast Forwarding
Max. Upstream Bandwidth: Kbps
Max. Downstream Bandwidth: Kbps

Note

- (1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.
- (2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.
- (3) If Max. Upstream/Downstream Bandwidth is empty, the device sets the value automatically.
- (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID







Security Level

No Security More Secure (Recommended)

Security Mode: WPA2-PSK
 Generate password automatically
Enter 8-63 ASCII characters or 64 hexadecimal digits ("0-9", "A-F").
Password: For CompanyOnly
Strength: strong

Cancel Apply

- 2 Click **Network Setting > Wireless > Guest/More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.

#	Status	SSID	Security	Guest WLAN	Modify
1		ZyxeL_9DE5_guest1	WPA2-Personal	External Guest	
2		ZyxeL_9DE5_guest2	WPA2-Personal	External Guest	
3		ZyxeL_9DE5_guest3	WPA2-Personal	External Guest	

- 3 Configure the screen using the provided parameters and click **Apply**.

More AP Edit

Wireless security can protect the data from unauthorized access or damage via wireless network. You need a wireless network name (also known as SSID) and security mode to set up the wireless security.

Wireless Network Setup

Wireless

Security Level

Wireless Network Name

Hide SSID

Guest WLAN

Access Scenario

Max. Upstream Bandwidth Kbps

Max. Downstream Bandwidth Kbps

Note

(1) Max. Upstream Bandwidth: This field allows you to configure the maximum bandwidth of this SSID to WAN.
 (2) Max. Downstream Bandwidth: This field allows you to configure the maximum bandwidth of WAN to this SSID.
 (3) If Max. Upstream/Downstream Bandwidth is empty, the device sets the value automatically.
 (4) Using Max. Upstream/Downstream Bandwidth will significantly decrease the wireless performance.

BSSID

SSID Subnet

Security Level

No Security More Secure (Recommended)

Security Mode

Generate password automatically

Enter 8-63 ASCII characters or 64 hexadecimal digits [0-9, "A-F"].

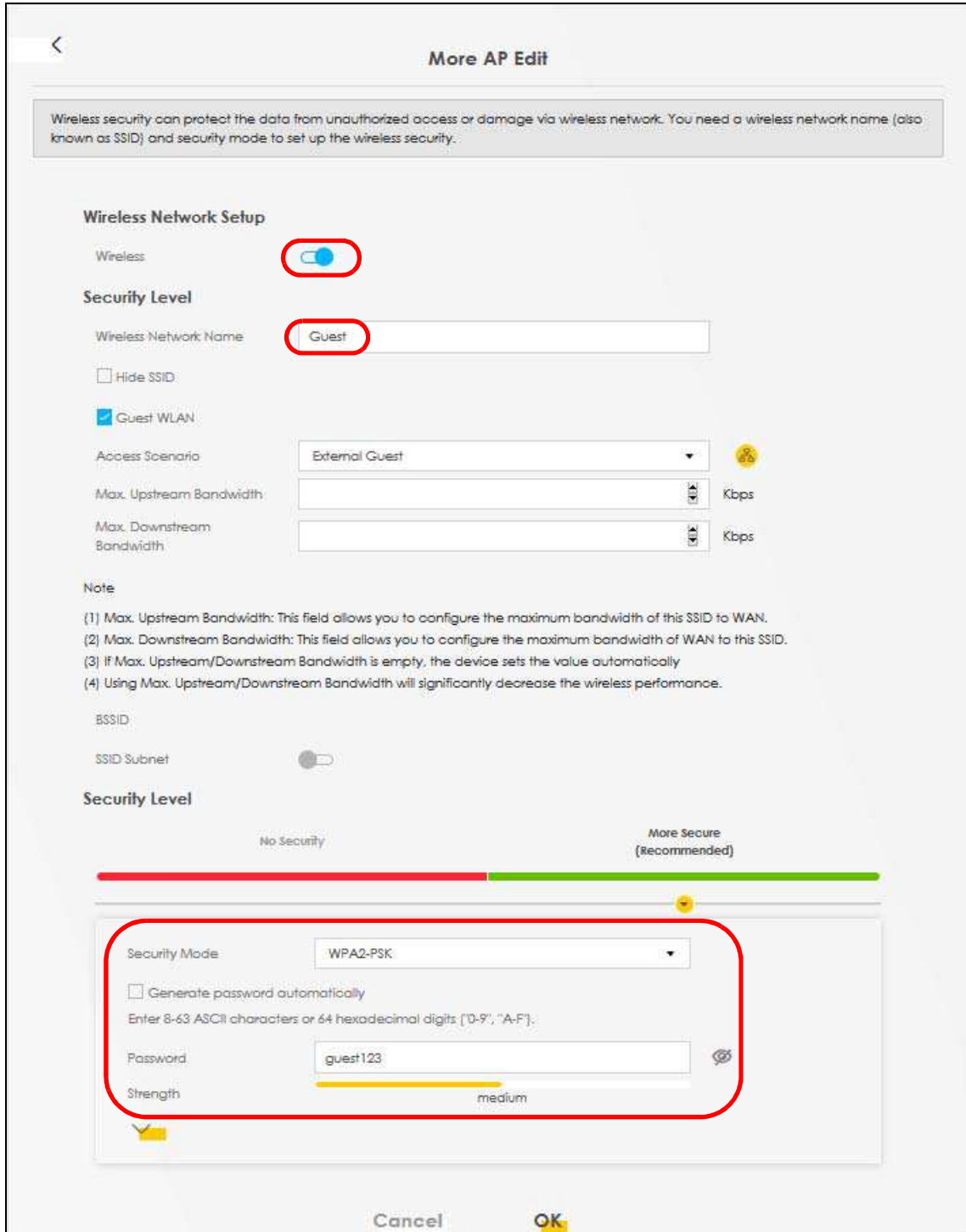
Password

Strength medium

Cancel OK

Note: The Guest SSID (**Wireless Network Name**) depends on the state of the Main SSID. For example, when the 2.4GHz Main SSID is enabled, then the 2.4GHz Guest SSID can be enabled. But when the 2.4GHz Main SSID is disabled, then the 2.4GHz Guest SSID is automatically disabled (cannot be enabled by the user).

- 4 In the **Guest/More AP** screen, click the **Edit** icon to configure the third wireless network group. Configure the screen using the provided parameters and click **Apply**.



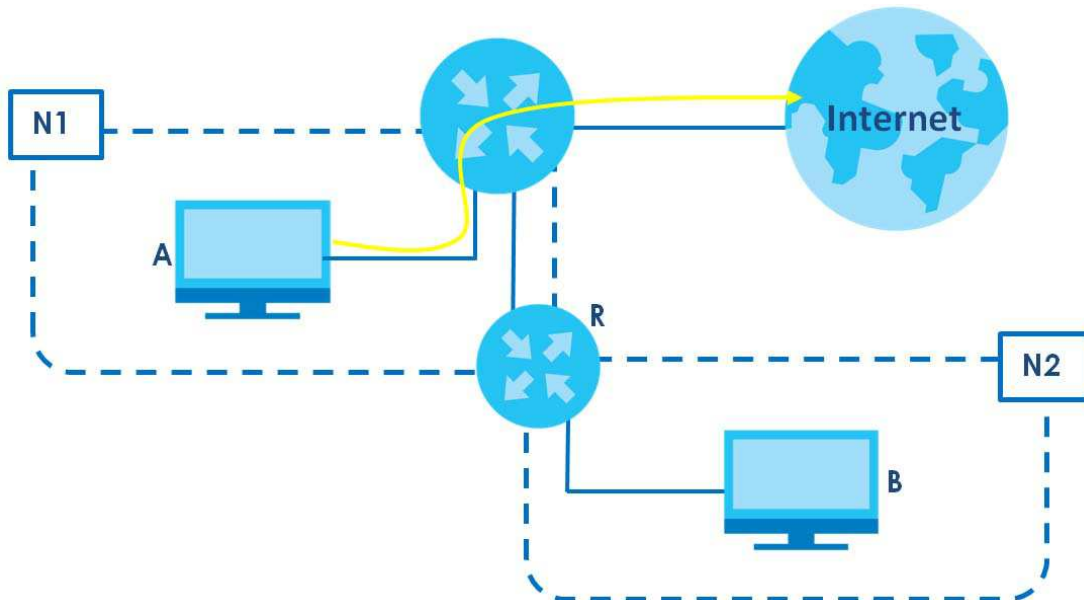
- 5 Check the status of **VIP** and **Guest** in the **Guest/More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

#	Status	SSID	Security	Guest WLAN	Modify
1		Home&Life SuperWIFI-F0FD_guest1	WPA2-Personal	External Guest	
2		VIP	WPA2-Personal	External Guest	
3		Guest	WPA2-Personal	External Guest	

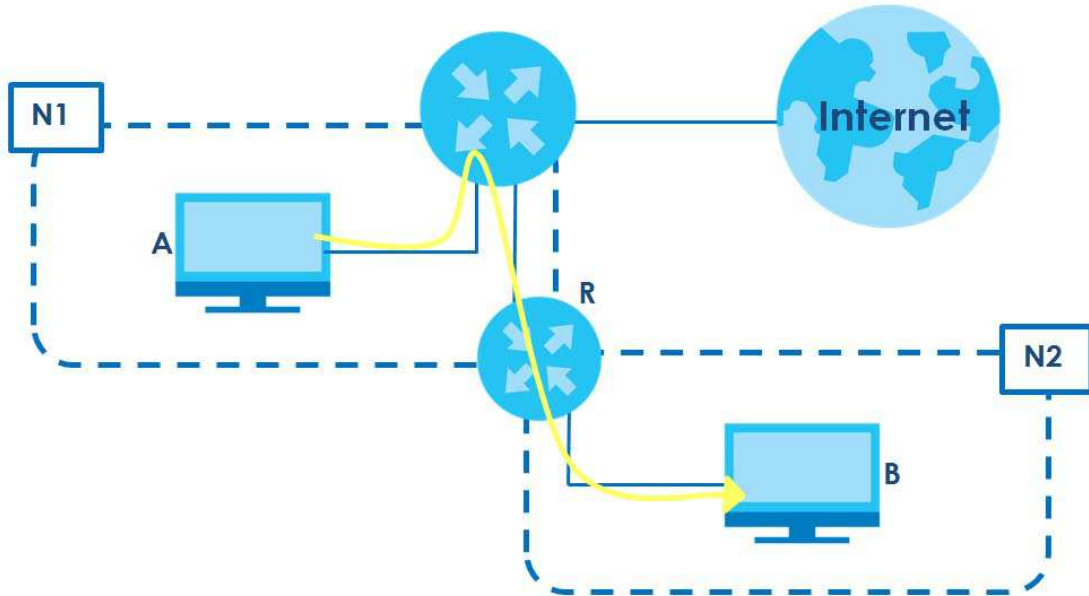
4.4 Configuring Static Route for Routing to Another Network

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

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



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



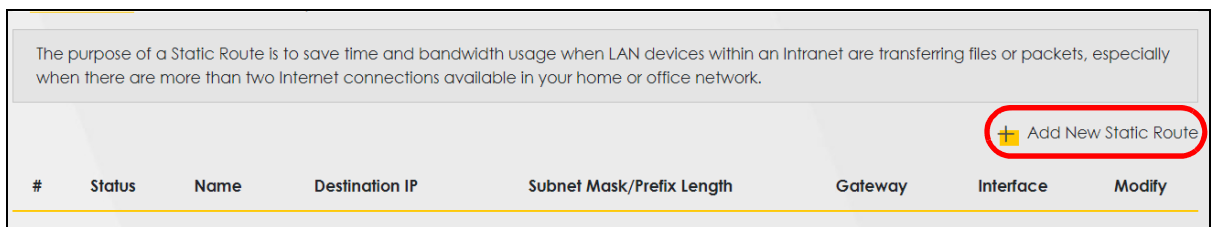
This tutorial uses the following example IP settings:

Table 6 IP Settings in this Tutorial



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

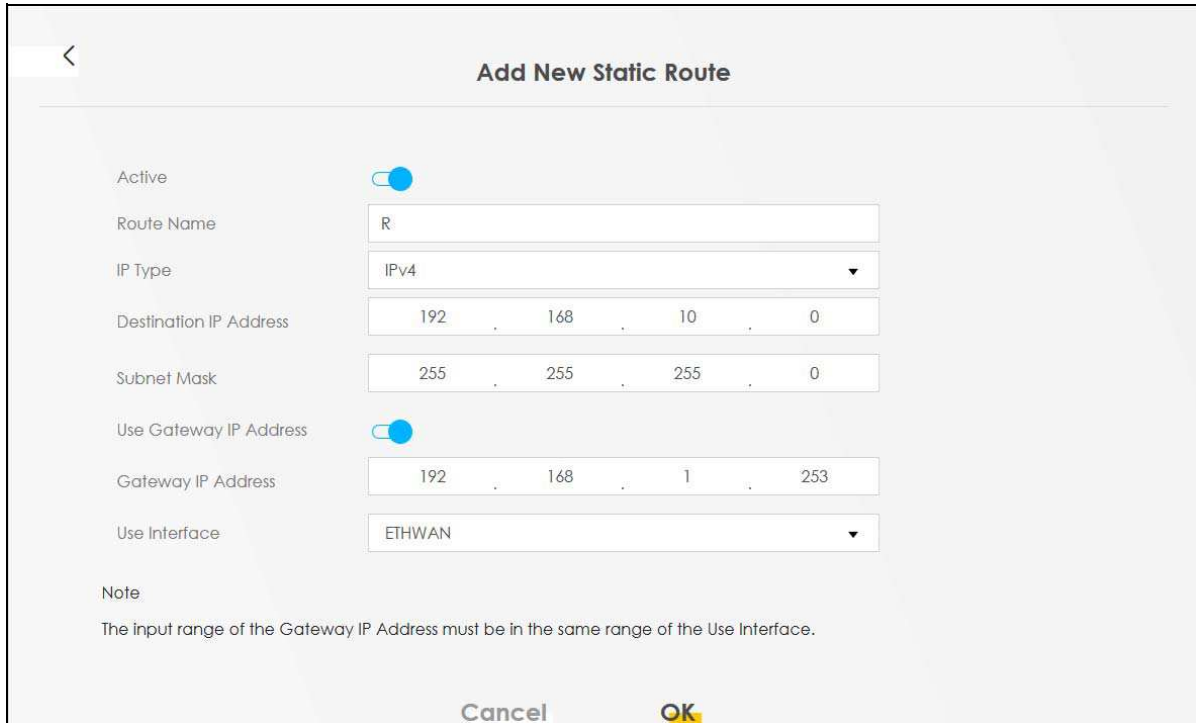
To configure a static route to route traffic from **N1** to **N2**:

- 1 Log into the Zyxel Device's Web Configurator in advanced mode.
- 2 Click **Network Setting > Routing**.
- 3 Click **Add new Static Route** in the **Static Route** screen.



- 4 Create a new static route using the following settings:

- 4a** Click the **Active** button to enable this static route. When the switch goes to the right () , the function is enabled. Enter the **Route Name** as **R**.
- 4b** Set **IP Type** to **IPv4**.
- 4c** Type the **Destination IP Address** **192.168.10.0** and **IP Subnet Mask** **255.255.255.0** for the destination, **N2**.
- 4d** Click the **Use Gateway IP Address** button to enable this function. When the switch goes to the right () , the function is enabled. Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.
- 4e** Select **ETHWAN** as the **Use Interface**.



Add New Static Route

Active

Route Name

IP Type

Destination IP Address

Subnet Mask

Use Gateway IP Address

Gateway IP Address

Use Interface

Note
The input range of the Gateway IP Address must be in the same range of the Use Interface.

Cancel OK

- 4a** Click **OK**.

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

4.5 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

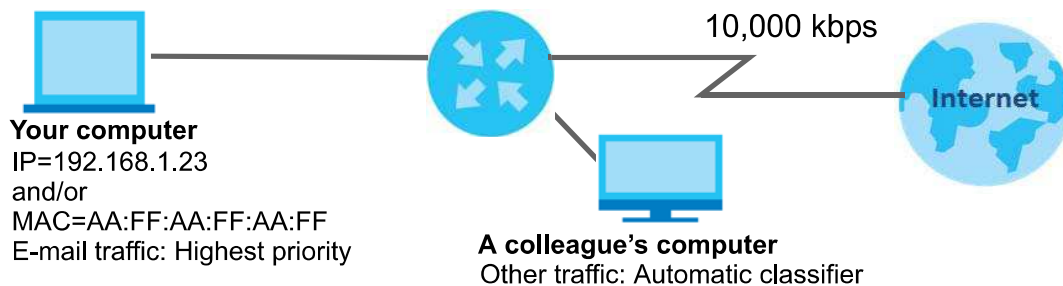
Let us say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.


In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

- Configure a queue to assign the highest priority queue (1) to e-mail traffic going to the WAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the Zyxel Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the Zyxel Device.



- 1 Click **Network Setting > QoS > General** and click the **QoS** button to enable. When the switch goes to the right () , the function is enabled. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the Zyxel Device automatically determine this figure). Click **Apply**.

Quality of Service (QoS) defines the traffic priority of Internet services to the home network.

QoS

WAN Managed Upstream Bandwidth (kbps)

LAN Managed Downstream Bandwidth (kbps)


Upstream Traffic Priority Assigned by

Note

(1) You can assign the upstream bandwidth manually. If the field is empty, the CPE set the value automatically.

(2) If Upstream Traffic Priority is selected, 8 level strict priority QoS will be applied automatically according to the selected criteria. In this mode, user manually defined QoS will not be applied until Auto-Priority Mapping is disabled.

(3) If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

- 2 Click **Network > Queue Setup > Add new Queue** to create a new queue. In the screen that opens, click the **Active** field to enable. When the switch goes to the right () , the function is enabled. Enter or select the following values:

- **Name:** E-mail

- **Interface:** WAN
- **Priority:** 1 (High)
- **Weight:** 8
- **Rate Limit:** 5,000 (kbps)

The screenshot shows a configuration window titled "Add New Queue". It contains the following fields and settings:

Active	<input checked="" type="checkbox"/>
Name	E-mail
Interface	WAN
Priority	1 (highest)
Weight	8
Buffer Management	Drop Tail(DT)
Rate Limit	5000 (kbps)

At the bottom of the window, there are two buttons: "Cancel" and "OK". The "OK" button is highlighted with a yellow border.

- 3 Click **Network > QoS > Classification Setup > Add new Classification** to create a new class. Select **Enable** in the **Active** field and follow the settings as shown in the screen below.

✕

Add New Classification

Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active

Class Name:

Classification Order:

Step2: Criteria Configuration

Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule.

Basic

From Interface:

Ether Type:

Source

Address: Subnet Mask: Exclude

Port Range: ~ Exclude

MAC: MAC Mask: Exclude

Destination

Address: Subnet Mask: Exclude

Port Range: ~ Exclude

MAC: MAC Mask: Exclude

Others

Service: Exclude

IP protocol: Exclude

DHCP: Exclude

IP Packet Length: ~ Exclude

DSCP: (0-63) Exclude

802.1P: Exclude

VLAN ID: (1-4094) Exclude

TCP ACK: Exclude

Step3: Packet Modification

The content of the packet can be modified by applying the following settings:

DSCP Mark: (0-63)

VLAN ID Tag: (1-4094)

802.1P Mark:

Step4: Class Routing

This module can route a packet to a certain interface according to the class setting

Forward To Interface:

Step5: Outgoing Queue Selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface.

To Queue Index:

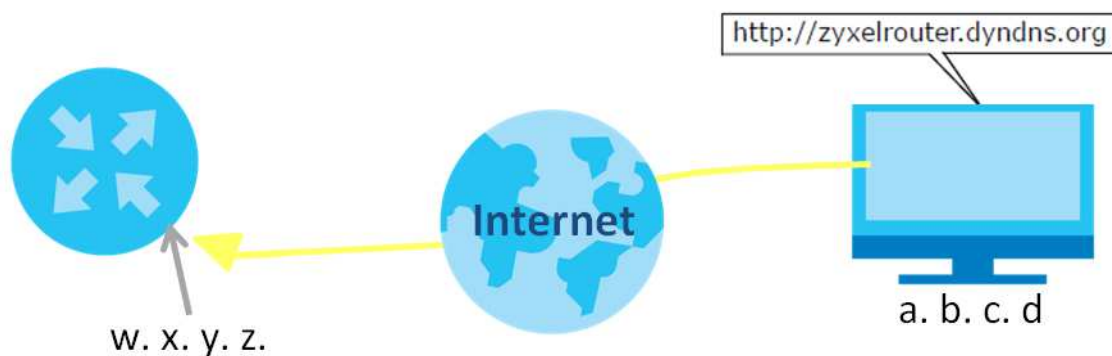
Cancel OK

Class Name	Give a class name to this traffic, such as E-mail in this example.
From Interface	This is the interface from which the traffic will be coming from. Select LAN1 for this example.
Ether Type	Select IP to identify the traffic source by its IP address or MAC address.
IP Address	Type the IP address of your computer - 192.168.1.23 . Type the IP Subnet Mask if you know it.
MAC Address	Type the MAC address of your computer - AA:FF:AA:FF:AA:FF . Type the MAC Mask if you know it.
To Queue Index	Link this to an item in the Network Setting > QoS > Queue Setup screen, which is the E-mail queue created in this example.

This maps e-mail traffic coming from port 25 to the highest priority, which you have created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to the **E-mail** queue (see the **Source** fields).

4.6 Access the Zyxel Device Using DDNS

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



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

This tutorial covers:

- [Registering a DDNS Account on \[www.dyndns.org\]\(http://www.dyndns.org\)](#)
- [Configuring DDNS on Your Zyxel Device](#)
- [Testing the DDNS Setting](#)

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

4.6.1 Registering a DDNS Account on www.dyndns.org

- 1 Open a browser and type **<http://www.dyndns.org>**.
- 2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
- 3 Log into www.dyndns.org using your account.

- 4 Add a new DDNS host name. This tutorial uses the following settings as an example.
 - Hostname: **zyxelrouter.dyndns.org**
 - Service Type: **Host with IP address**
 - IP Address: Enter the WAN IP address that your Zyxel Device is currently using. You can find the IP address on the Zyxel Device's Web Configurator **Status** page.

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

4.6.2 Configuring DDNS on Your Zyxel Device

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

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

Dynamic DNS can update your current dynamic IP into a hostname. Use the settings to set up dynamic DNS information.

Dynamic DNS Setup

Dynamic DNS Enable Disable (Settings are invalid when disable)

Service Provider

Host Name

Username

Password

Enable Wildcard Option

Enable Off Line Option (Only applies to custom DNS)

Dynamic DNS Status

User Authentication Result

Last Updated Time

Current Dynamic IP

Click **Apply**.

4.6.3 Testing the DDNS Setting

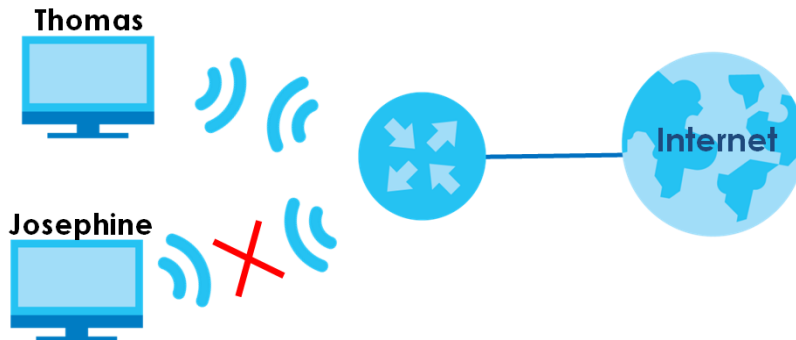
Now you should be able to access the Zyxel Device from the Internet. To test this:

- 1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
- 2 Type **http://zyxelrouter.dyndns.org** and press [Enter].
- 3 The Zyxel Device's login page should appear. You can then log into the Zyxel Device and manage it.

4.7 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the Zyxel Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



- 1 Click **Security > MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.
- 2 Select **Allow**. Click **Add a new setting** to add a new entry. Then enter the host name and MAC address of Thomas' computer in this screen. Click **Apply**.

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
1	<input checked="" type="checkbox"/>	Thomas	00 - 24 - 21 - A8 - 1F - 0C	🗑️

Note
Only devices listed here are granted access to the network.

Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the Zyxel Device.

PART II

Technical Reference

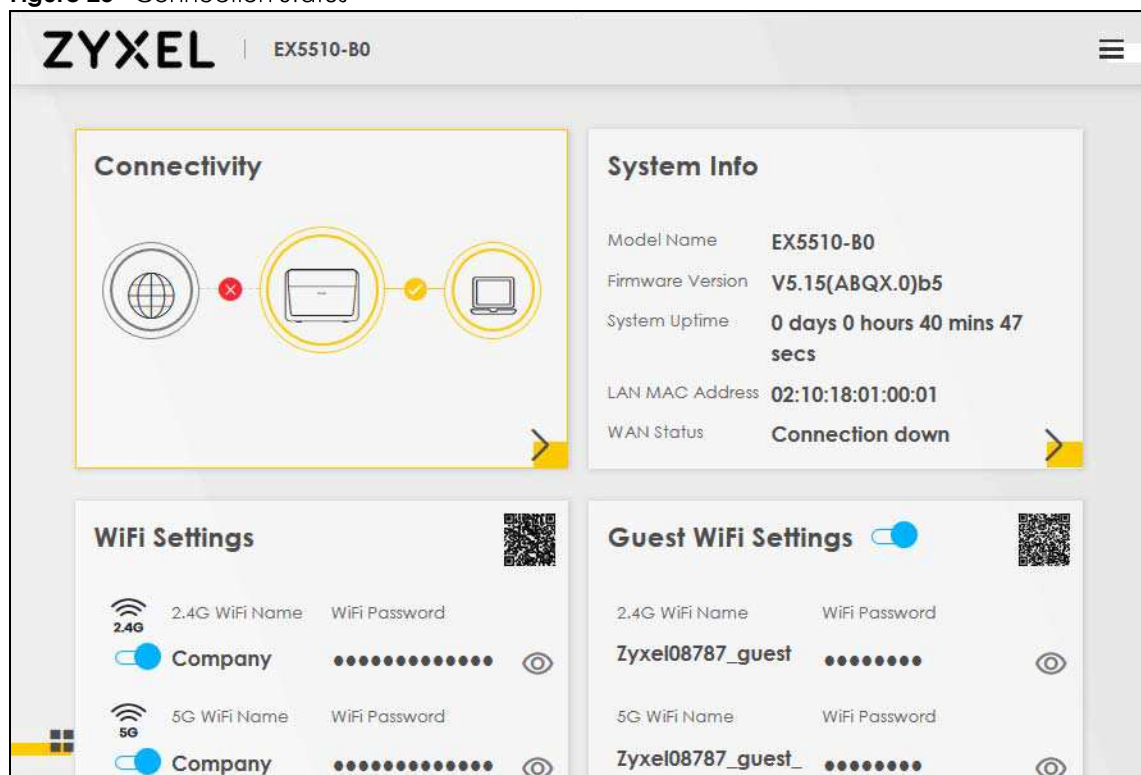
CHAPTER 5

Connection Status



5.1 Overview

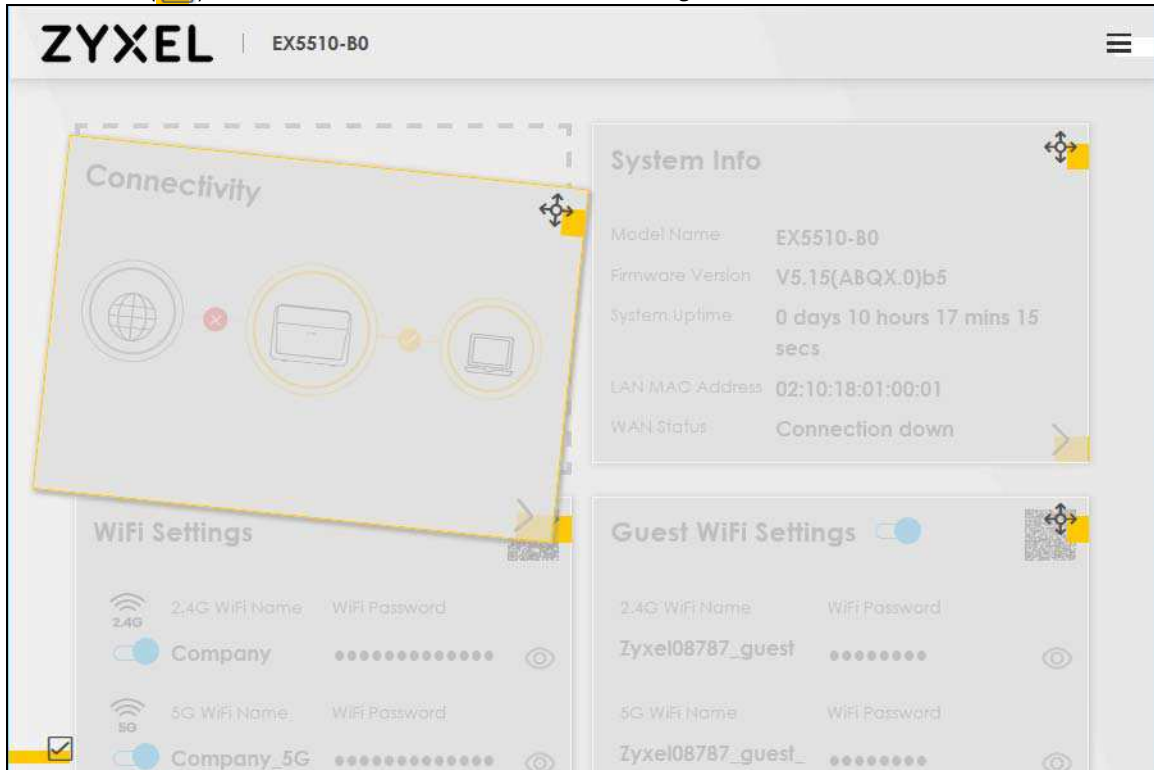
After you log into the Web Configurator, the **Connection Status** screen appears. You can configure basic Internet access, wireless settings, and parental control settings in this screen. It also shows the network status of the Zyxel Device and computers/devices connected to it.

Figure 23 Connection Status



5.1.1 Layout Icon

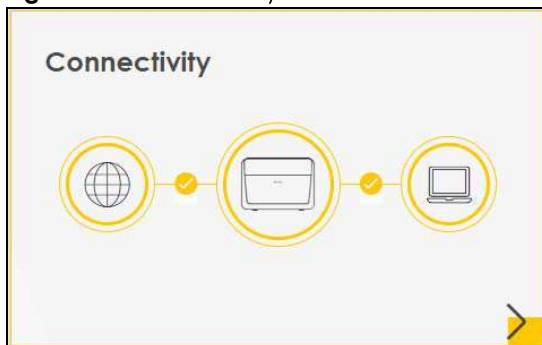
Click this icon () to arrange the screen order. Select a block and hold it to move around. Click the Check icon () in the lower left corner to save the changes.




5.1.2 Connectivity

Use this screen to view the network connection status of the Zyxel Device and its clients.

Figure 24 Connectivity



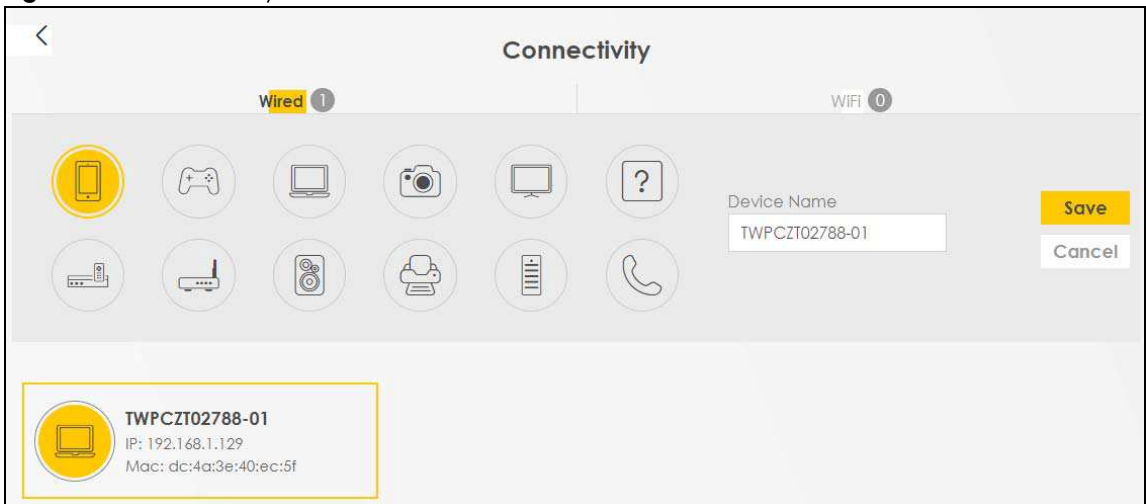
Click the Arrow icon () to open the following screen. Use this screen to view IP addresses and MAC addresses of the wireless and wired devices connected to the Zyxel Device.

Place your mouse within the device block, and an Edit icon () will appear. Click the Edit icon to change the icon and name of a connected device.

Figure 25 Connectivity: Connected Devices

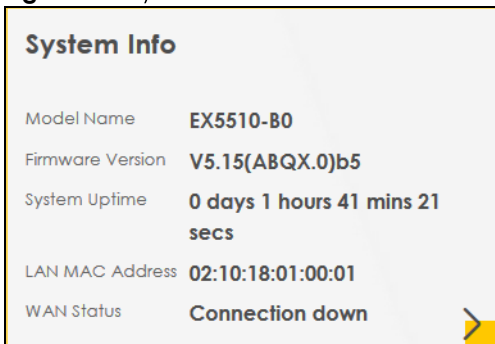
Icon and Device Name

You can change the icon and name of a connected device by clicking the device's Edit icon. Select an icon and/or enter a name in the **Device Name** field for a connected device. Click **Save** to save your changes.

Figure 26 Connectivity: Edit

5.1.3 System Info

Use this screen to view the basic system information of the Zyxel Device.

Figure 27 System Info


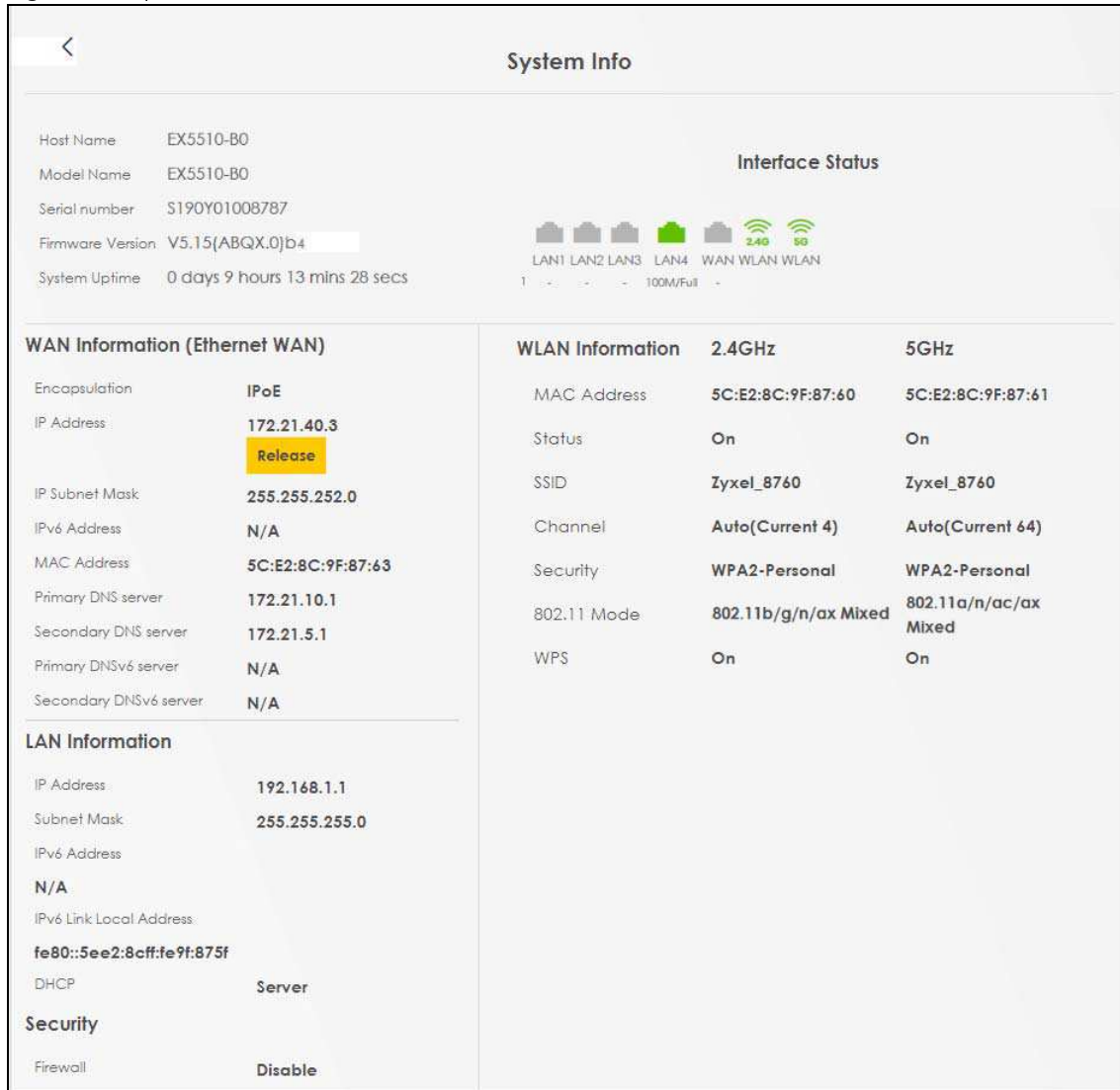
Click the Arrow icon () to open the following screen. Use this screen to view more information on the status of your firewall and interfaces (WAN, LAN, and WiFi).

Figure 28 System Info: Detailed Information



Each field is described in the following table.

Table 7 System Info: Detailed Information

LABEL	DESCRIPTION
Host Name	This field displays the Zyxel Device system name. It is used for identification.
Model Name	This shows the model number of your Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This is the current version of the firmware on the Zyxel Device.
System Up Time	This field displays how long the Zyxel Device has been running since it last started up. The Zyxel Device starts up when you plug it in, when you restart it (Maintenance > Reboot), or when you reset it.
Interface Status	
Virtual ports are shown here. You can see whether the ports are in use and their transmission rate.	

Table 7 System Info: Detailed Information (continued)

LABEL	DESCRIPTION
WAN Information (These fields display when you have an Internet connection.)	
Encapsulation	This field displays the current encapsulation method.
IP Address	This field displays the current IPv4 address of the Zyxel Device. Click the Release button to release the IP address provided by a DHCP server. Click the Renew button to renew the IP address. Click the Disconnect button to disconnect the PPP WAN when PPP WAN has an IPv4 address. Click the Connect button to connect the PPP WAN. The Web Configurator will display the loading panel until the IP address has been released/renewed/disconnected/connected.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
IPv6 Address	This field displays the current IPv6 address of the Zyxel Device.
MAC Address	This field displays the WAN Ethernet adapter MAC (Media Access Control) address of your Zyxel Device.
Primary DNS server	This field displays the first DNS server address assigned by the ISP.
Secondary DNS server	This field displays the second DNS server address assigned by the ISP.
Primary DNSv6 server	This field displays the first DNS server IPv6 address assigned by the ISP.
Secondary DNSv6 server	This field displays the second DNS server IPv6 address assigned by the ISP.
LAN Information (These fields display information about the LAN ports.)	
IP Address	This is the current IPv4 address of the Zyxel Device in the LAN.
Subnet Mask	This is the current subnet mask in the LAN.
IPv6 Address	This is the current IPv6 address of the Zyxel Device in the LAN.
IPv6 Link Local Address	This field displays the current link-local address of the Zyxel Device for the LAN interface.
DHCP	This field displays what DHCP services the Zyxel Device is providing to the LAN. The possible values are: Server - The Zyxel Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. Relay - The Zyxel Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. None - The Zyxel Device is not providing any DHCP services to the LAN.
MAC Address	This field displays the LAN MAC (Media Access Control) address of your Zyxel Device.
Security	
Firewall	This displays the firewall's current security level.
WLAN 2.4G/5G Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) address of the wireless interface.
Status	This displays whether WiFi is activated.
SSID	This is the descriptive name used to identify the Zyxel Device in a wireless LAN.
Channel	This is the channel number used by the wireless interface now.
Security	This displays the type of security mode the wireless interface is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the wireless interface is using in the wireless LAN.
WPS	This displays whether WPS is activated on the wireless interface.

5.2 WiFi Settings



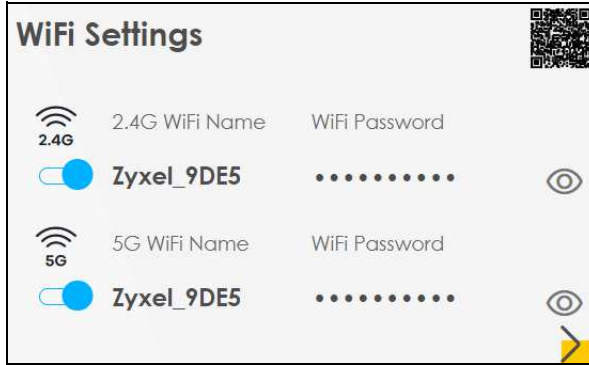
Use this screen to enable or disable the main 2.4G and/or 5G wireless networks. When the switch goes to the right (), the function is enabled. Otherwise, it is not. You can use this screen or the QR code on the upper right corner to check the SSIDs (WiFi network name) and passwords of the main wireless networks. If you want to show or hide your WiFi passwords, click the Eye icon ().

Figure 29 WiFi Settings






Click the Arrow icon () to open the following screen. Use this screen to configure the SSIDs and/or passwords for your main wireless networks. Select **Keep 2.4G and 5G the same** to use the same SSID for 2.4 GHz and 5 GHz bands.

Figure 30 WiFi Settings: Configuration



Each field is described in the following table.

Table 8 WiFi Settings: Configuration

LABEL	DESCRIPTION
Keep 2.4G and 5G the same	Select this and the 2.4G and 5G wireless networks will use the same SSID. If you deselect this, the screen will change. You need to assign different SSIDs for the 2.4G and 5G wireless networks.
2.4G/5G WiFi	Click this switch to enable or disable the 2.4G and/or 5G wireless networks. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.
WiFi Password	If you selected Random Password , this field displays a pre-shared key generated by the Zyxel Device. If you did not select Random Password , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password for your wireless network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the Zyxel Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.
Hide WiFi Name	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID.
Save	Click Save to save your changes.

5.3 Guest WiFi Settings


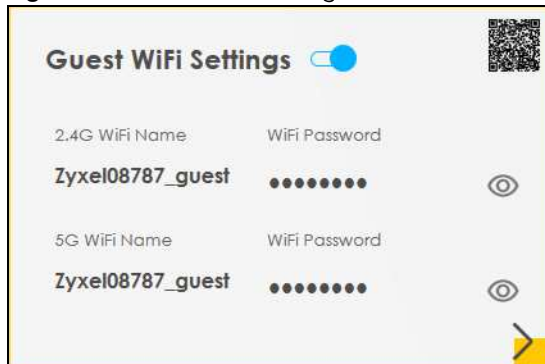
Use this screen to enable or disable the guest 2.4G and/or 5G wireless networks. When the switch goes to the right () , the function is enabled. Otherwise, it is not. You can check their SSIDs (WiFi network name) and passwords from this screen. If you want to show or hide your WiFi passwords, click the Eye icon.

Figure 31 Guest WiFi Settings




Click the Arrow icon () to open the following screen. Use this screen to configure the 2.4G and 5G SSIDs and/or passwords for your guest wireless networks.

Figure 32 Guest WiFi Settings: Configuration

To assign different SSIDs to the 2.4G and 5G guest wireless networks, clear the **Keep 2.4G and 5G the same** check box in the **WiFi Settings** screen, and the **Guest WiFi Settings** screen will change.

Figure 33 Guest WiFi Settings: Different SSIDs

Each field is described in the following table.

Table 9 WiFi Settings: Configuration



LABEL	DESCRIPTION
WiFi 2.4G/5G WiFi	Click this switch to enable or disable the 2.4G and/or 5G wireless networks. When the switch goes to the right  , the function is enabled. Otherwise, it is not.
WiFi Name	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for WiFi.

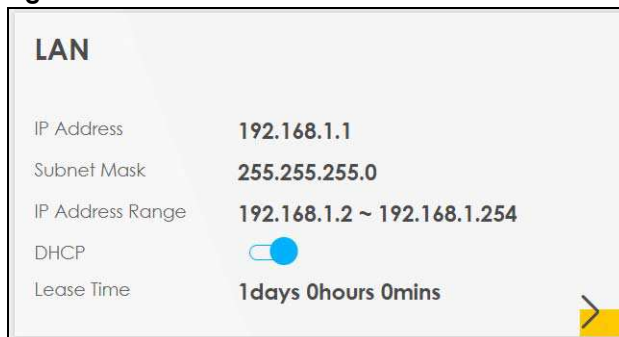
Table 9 WiFi Settings: Configuration (continued)

LABEL	DESCRIPTION
WiFi Password	If you selected Random Password , this field displays a pre-shared key generated by the Zyxel Device. If you did not select Random Password , you can manually type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
	Click the Eye icon to show or hide the password of your wireless network. When the Eye icon is slashed  , you'll see the password in plain text. Otherwise, it is hidden.
Random Password	Select this option to have the Zyxel Device automatically generate a password. The WiFi Password field will not be configurable when you select this option.
Hide WiFi Name	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. Note: Disable WPS in the Network Setting > Wireless > WPS screen to hide the SSID.
Save	Click Save to save your changes.

5.4 LAN Settings

Use this screen to view the LAN IP address, subnet mask, and DHCP settings of your Zyxel Device.

Figure 34 LAN




Click the Arrow icon () to open the following screen. Use this screen to configure the LAN IP address and DHCP setting for your Zyxel Device.

Figure 35 LAN Setup

Each field is described in the following table.

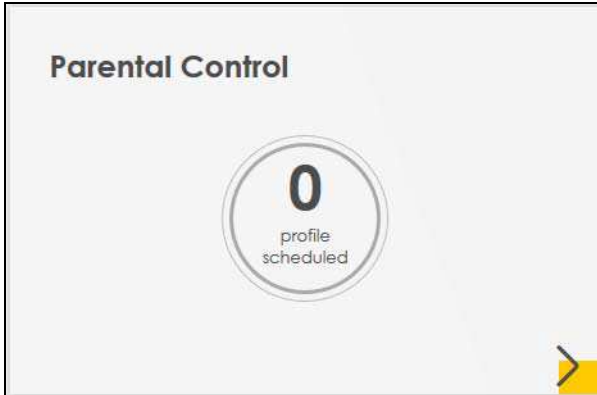
Table 10 Status Screen

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IPv4 address you want to assign to your Zyxel Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your Zyxel Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
IP Addressing Values	
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
DHCP Server State	
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
Days/Hours/Minutes	Enter the lease time of the DHCP server.
Save	Click Save to save your changes.

5.5 Parental Control

Use this screen to view the number of profiles that were created for parental control.

Figure 36 Parental Control




Click the Arrow icon () to open the following screen. Use this screen to enable parental control and add more profiles. Add a profile to create restricted access schedules. Go to the **Security > Parental Control > Add New PCP/Edit** screen to configure URL filtering settings to block the users on your network from accessing certain web sites.

Figure 37 Parental Control: Scheduled Profile (no profile)

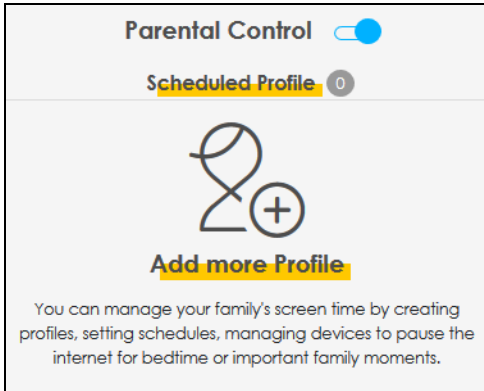
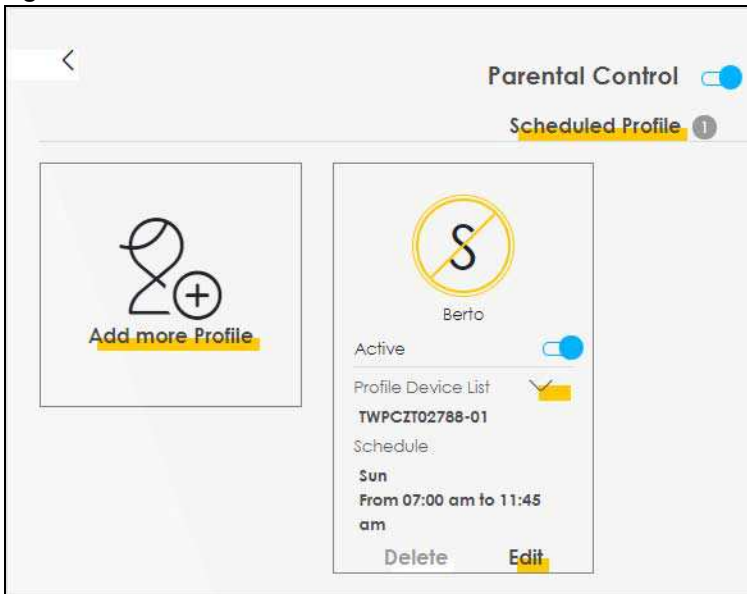





Figure 38 Parental Control: Scheduled Profile



Each field is described in the following table.

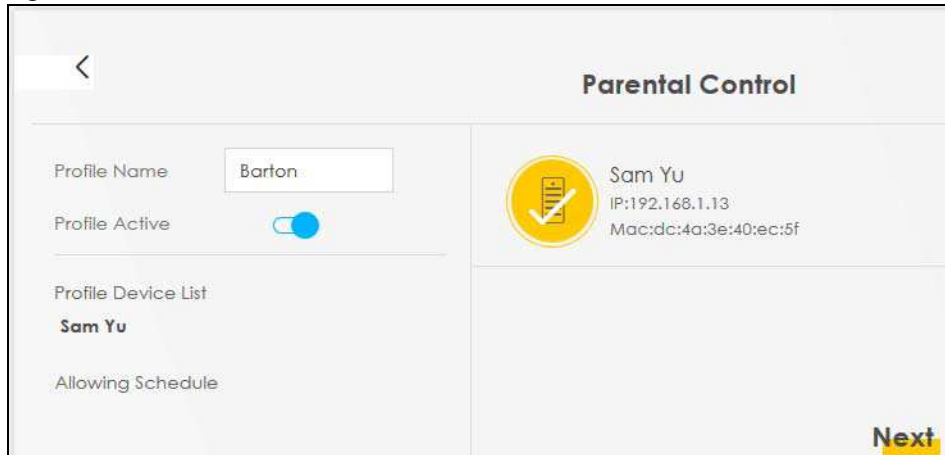
Table 11 Parental Control: Schedule

LABEL	DESCRIPTION
Parental Control	Click this switch to enable or disable parental control. When the switch goes to the right (), the function is enabled. Otherwise, it is not.
Active	Click this switch to enable or disable a created profile. When the switch goes to the right (), this profile is active. Otherwise, it is not.
Scheduled Profile	This screen shows all the created profile(s). Click  beside Profile Device List to view more information about the profile. You can click Delete to remove the profile or click Edit to change the profile settings.
Add more Profile	Click this button or tab to create a new profile.

5.5.1 Create/Edit a Parental Control Profile


Click **Add more Profile** to create a profile or click **Edit** of an existing profile to change its settings. Use this screen to add a device(s) in a profile and block Internet access on the profile device(s).

Figure 39 Parental Control: Select Device



Each field is described in the following table.

Table 12 Parental Control: Select Device

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable the profile. When the switch goes to the right (), the profile is enabled. Otherwise, it is disabled.
Profile Device List	This field shows the devices selected on the right for this profile.
Allowing Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
	Select the device(s) on your network for this profile and click Next .


5.5.2 Define a Schedule

This screen allows you to define time periods and days during which Internet access is blocked on the profile device(s).

Figure 40 Parental Control: Time Limit

Each field is described in the following table.

Table 13 Parental Control: Time Limit

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile.
Profile Active	Click this switch to enable or disable the profile. When the switch goes to the right  , the profile is enabled. Otherwise, it is disabled.
Profile Device List	This field shows the devices selected on the right for this profile.
Allowing Schedule	This field shows the time during which Internet access is blocked on the profile device(s).
Schedule	
Add New Schedule	Click this to add a new block for scheduling.
Start/End blocking	Select the time period when Internet access is blocked on the profile device(s). Select Whole Week and the scheduler rule will be activated everyday of the week.
Repeat On	Select the days when Internet access is blocked on the profile device(s).
Back	Click Back to return to the previous screen.
Save	Click Save to save your changes.