
***4ipnet* WHG303**
Quick Installation Guide

Copyright Notice

This document is protected by USA copyright laws and other laws and is the property of 4IPNET, INC. You may not copy, reproduce, distribute, publish, display, perform, or modify any part of this publication in any form or by any means without prior written permission from 4IPNET, INC. You may not alter or remove any copyright or other notice from copies of the content. All other brand and product names are claimed or registered marks of their respective companies or organizations.

All rights reserved.

FCC Caution

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

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

Preface

4ipnet WHG303 Secure WLAN Controller is an ideal solution for small to medium hotspot deployments, such as in hotels, hospitals, convention centers, libraries, airport terminals, and MDUs/MTUs. The WHG303 integrates “secure access control”, “visitor account provisioning”, “flexible accounting and billing”, and “high-speed secure wireless connection” into one box to fulfill the needs demanded by a public wireless network. It also provides advanced functions suitable for larger networks to accommodate more users with multiple APs to cover a wider service area.

This Quick Installation Guide provides instructions and reference materials for getting started with 4ipnet WHG303. This guide will also show how to connect WHG303 to other network devices.

Package Contents

1. 4ipnet WHG303 x 1
2. Quick Installation Guide x 1
3. CD-ROM (with User Manual and QIG) x 1
4. Power Cord x 1
5. Power Adaptor (12DC, 2A) x 1
6. Cross-over Ethernet RJ-45 Cable x 1
7. RS-232 DB9 Console Cable x 1



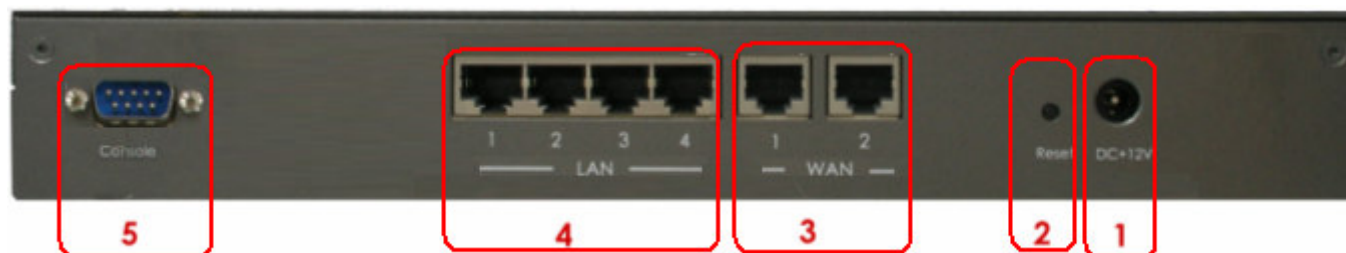
It is recommended to keep the original packing material for possible future shipment when repair or maintenance is required. Any returned product should be packed in its original packaging to prevent damage during delivery.

System Overview

Front Panel



1. **Power :** ON indicates the power on, and OFF indicates the power off.
2. **Status :** Power and Status both ON indicate system ready, OFF indicates BIOS running, and BLINKING indicates OS running.
3. **WAN :** ON indicates connection, OFF indicates no connection, and BLINKING indicates data transmitting.
4. **LAN :** ON indicates connection, OFF indicates no connection, and BLINKING indicates data transmitting.

Rear Panel

1. **DC+12V** : Attach the power adaptor here.

2. **Reset** :

- Press and hold the Reset button for about 5 seconds and the LED status indicator on the front panel will start to blink before restarting the system.
- Press and hold the Reset button for more than 10 seconds and the LED status indicator on the front panel will start to speed up blinking before resetting the system to default configuration.

3. **WAN** :

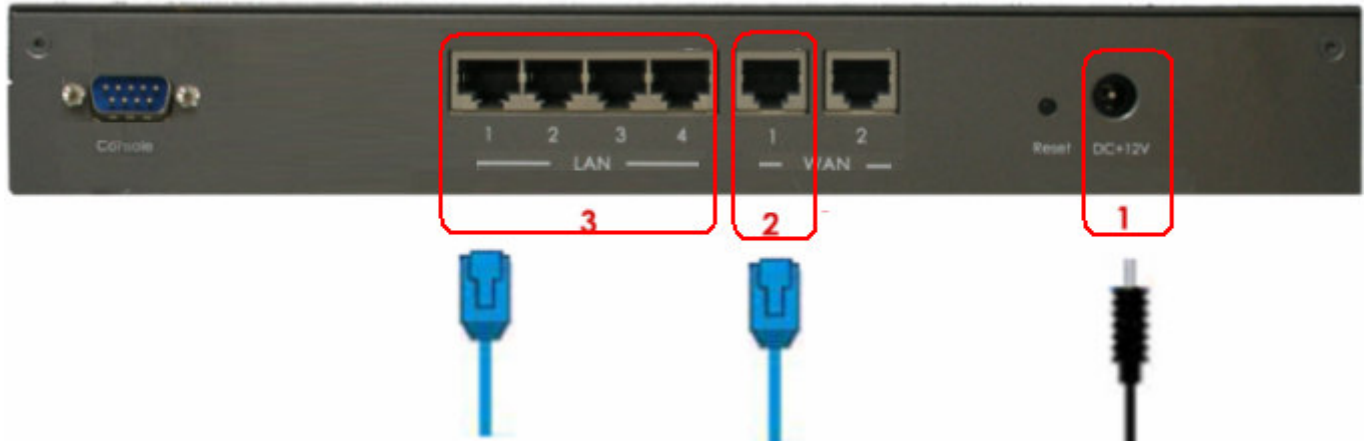
- For connecting to external networks which are not managed by WHG303 via ADSL or Cable Modem, or connecting to a certain LAN of an organization via Switch or Hub.

4. **LAN** :

- For connecting to the networks managed by WHG303, such as client networking devices.
- WHG303 supports Service Zone function including Port-Based mode and Tag-Based mode. Under Tag-Based mode, service zones are distinguished by VLAN tagging instead of physical LAN ports, and vice versa. By default, the system is in Port-Based mode and all LAN ports are set to the default service zone.

5. **Console** : For displaying text data on an extended monitor via a RS-232 DB9 cable.

Hardware Installation



1. Connect the **Power adapter** to the power socket on the rear panel. The Power LED on the front panel should be ON to indicate a proper connection.



Using a non-certified power adapter may damage this system.

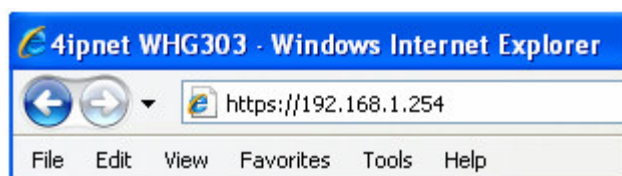
2. Connect an **Ethernet cable** to WAN1 Port on the rear panel. Per your needs, connect the other end of the cable to a networking device such as ADSL modem, cable modem, switch or hub. The WAN1 LED indicator should be ON to indicate a proper connection.
3. Connect an **Ethernet cable** to any LAN Port on the rear panel. Connect the other end of the cable to a PC for configuring the WHG303 system. The LED indicator should be ON to indicate a proper connection.

Getting Started

4ipnet WHG303 supports web-based configuration. Upon the completion of hardware installation, WHG303 can be configured through a PC by using its web browser with JavaScript enabled such as Internet Explorer version 6.0.

Steps:

1. Set DHCP in TCP/IP of the administrator PC to get an IP address dynamically. Connect the PC to any LAN Port of WHG303. An IP address will be assigned to the PC automatically via the WHG303 built-in DHCP server.
2. Launch a web browser to access the web management interface of WHG303 by entering “**https://192.168.1.254**” or “**http://192.168.1.254**” in the address field.



►► **Note:** “https” is used for a secured connection.

3. The following Administrator Login Page will then appear. Enter “**admin**” (the default value) in the *Username* and *Password* fields, and then click **Login** to log in.



4. The **Home Page** will appear after a successful login.



►► **Note:**

To logout, simply click the **Logout** button at the upper right hand corner of the interface to return to the Administrator Login Page.

Common Settings

< Setup Wizard >

WHG303 provides a **Setup Wizard** for quick configuration. To quickly configure WHG303 by using the **Setup Wizard**, click on the **Setup Wizard** button to start the configuration process.



Step 1: General

- Enter a new password in the *New Password* field, and re-enter it again in the *Verify Password* field (a maximum of 20 characters and no spaces allowed in between).
- Select an appropriate time zone from the *Time Zone* drop-down list box to set up the system time.
- Click **Next** to continue.

 A screenshot of the 4ipnet Setup Wizard, Step 1: General. The interface has a red header with the 4ipnet logo and navigation links. On the left, a sidebar shows steps 1 through 4, with Step 1 highlighted. The main content area is titled 'General' and contains fields for 'New Password' and 'Verify Password', both masked with dots. Below these is a 'Time Zone' dropdown menu showing '(GMT+08:00)Taipei'. A 'Next' button is at the bottom right. A yellow warning icon is visible on the left sidebar.


For security concern, it is strongly recommended to change the administrator's password

Step 2: WAN1 Interface

For setting up both wired WAN and wireless LAN functions:

- Select a proper type of Internet connection for WAN1 interface from the following three available connections: **Static**, **Dynamic**, or **PPPoE**. Your ISP or network administrator can advise on the connection type available to you. Below depicts an example for **Dynamic**.
- Click **Next** to continue.

 A screenshot of the 4ipnet Setup Wizard, Step 2: WAN1 Interface. The interface has a red header with the 4ipnet logo and navigation links. On the left, a sidebar shows steps 1 through 4, with Step 2 highlighted. The main content area is titled 'WAN1 Interface' and contains three radio button options: 'Static (Use the following IP settings)', 'Dynamic (IP settings assigned automatically)' (which is selected), and 'PPPoE'. Below the options are 'Back' and 'Next' buttons.

Step 3: Local User Account (Optional)

New local accounts can be created and added into the database via this optional function. If local user accounts are not required, click **Skip** to go directly to **Step 4**. However, It is recommended to create at least one local user account in order to verify the system's readiness upon completion of this **Setup Wizard**.

- Enter the *Username* (e.g. "testuser") and *Password* (e.g. "testuser") to create a new local account.
- Click **Next** to continue.
- More local accounts can be added by clicking the **Back** button in **Step 4**.

Step 4: Confirm and Restart

- Click **Finish** to save current settings and restart the system.

- A confirmation dialog box will then appear. Click **OK** to continue.



- A **Confirm and Restart** message will appear on the screen during the restarting process. Please do not interrupt the system until the Administrator Login Page appears.

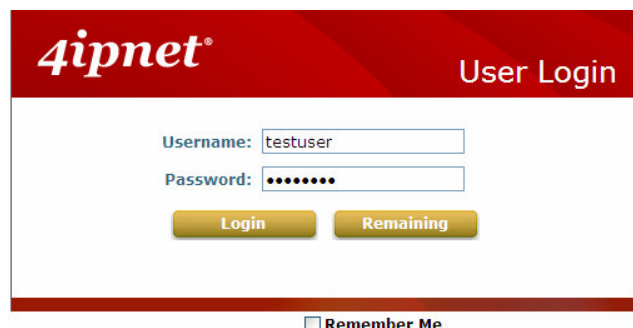
► **Note:** The system is trying to locate a DNS server at this stage. Therefore, a longer startup time is required if the configured DNS cannot be found.

- When the following Administrator Login Page appears, it means the restart process is now completed.

< User Login >

To verify whether the configuration of the new local user account(s) created via the **Setup Wizard** has been completed successfully:

1. Connect a client device (e.g. laptop, PC) to any LAN Port of WHG303. The device will obtain an IP address automatically via DHCP.
2. Open a web browser on a client device, access any URL, and then the default **User Login Page** will appear.
3. Enter the *Username* and *Password* of a local user account previously generated via Setup Wizard (e.g. “testuser@local” as the *Username* and “testuser” as the *Password*); then Click **Login**.



The screenshot shows the 4ipnet User Login page. It has a red header with the 4ipnet logo and 'User Login' text. Below the header, there are two input fields: 'Username:' with the value 'testuser' and 'Password:' with masked characters '*****'. There are two buttons: 'Login' and 'Remaining'. At the bottom, there is a checkbox labeled 'Remember Me'.

» Note:

1. WHG303 supports multiple authentication options including built-in local user database and external authentication database (e.g. RADIUS). The system will automatically identify which authentication option is used from the full username entered.
2. The format of a full (valid) username is **userid@postfix**, where “userid” is the user ID and “postfix” is the name of the selected authentication option.
3. **Exception:** The postfix can be omitted only when the default authentication option is used. For example, “**LOCAL**” is the default authentication option at this system;

therefore, you may enter either “**testuser**” or “**testuser@local**” in the *Username* field.

Congratulation!

The Login Success Page will appear after a client has successfully logged into WHG303 and has been authenticated by the system.

The appearance of Login Success Page means that WHG303 has been installed and configured properly.

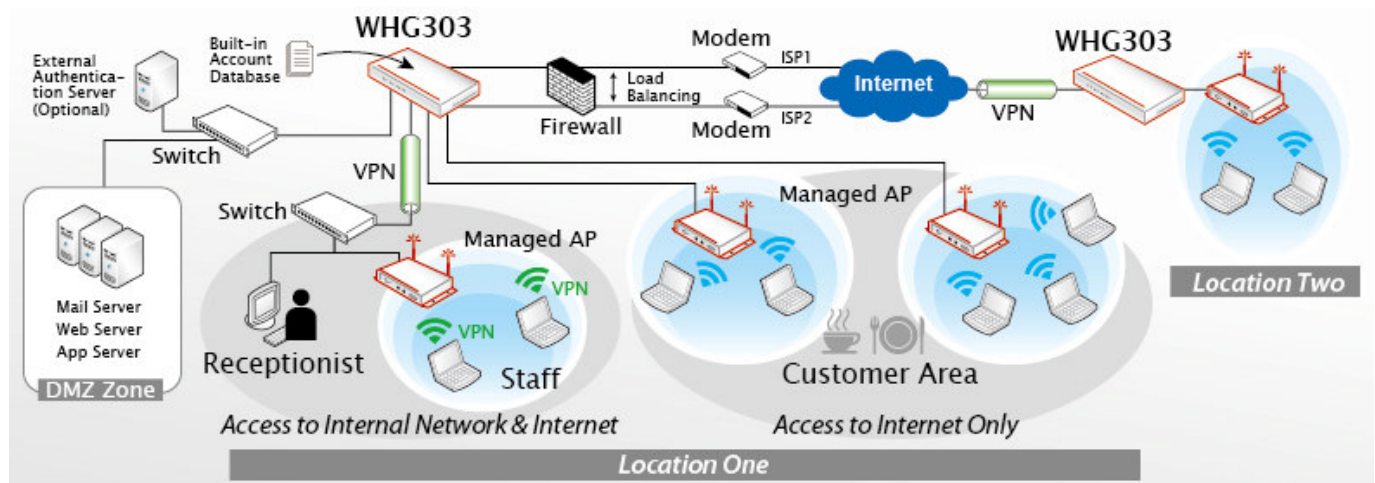


Service Zone – Deployment Example

< Small and Mid-size Business Network Environment >

In a Small and Mid-size Business (SMB) network environment, devices such as switches, hubs, and access points are commonly used, and Internet connection is usually via an ADSL or a cable modem. WHG303 uses virtual LAN (VLAN) technology to partition one physical network under its control into nine logical virtual networks, called Service Zones, including one untagged zone and eight tagged zones. The untagged zone is also referred as the Default Service Zone in this system, which is always enabled. On the other hand, the other four tagged zones can be enabled or disabled respectively. By default, port-based configuration is used and all of the four physical LAN ports are set to use the Default Service Zone.

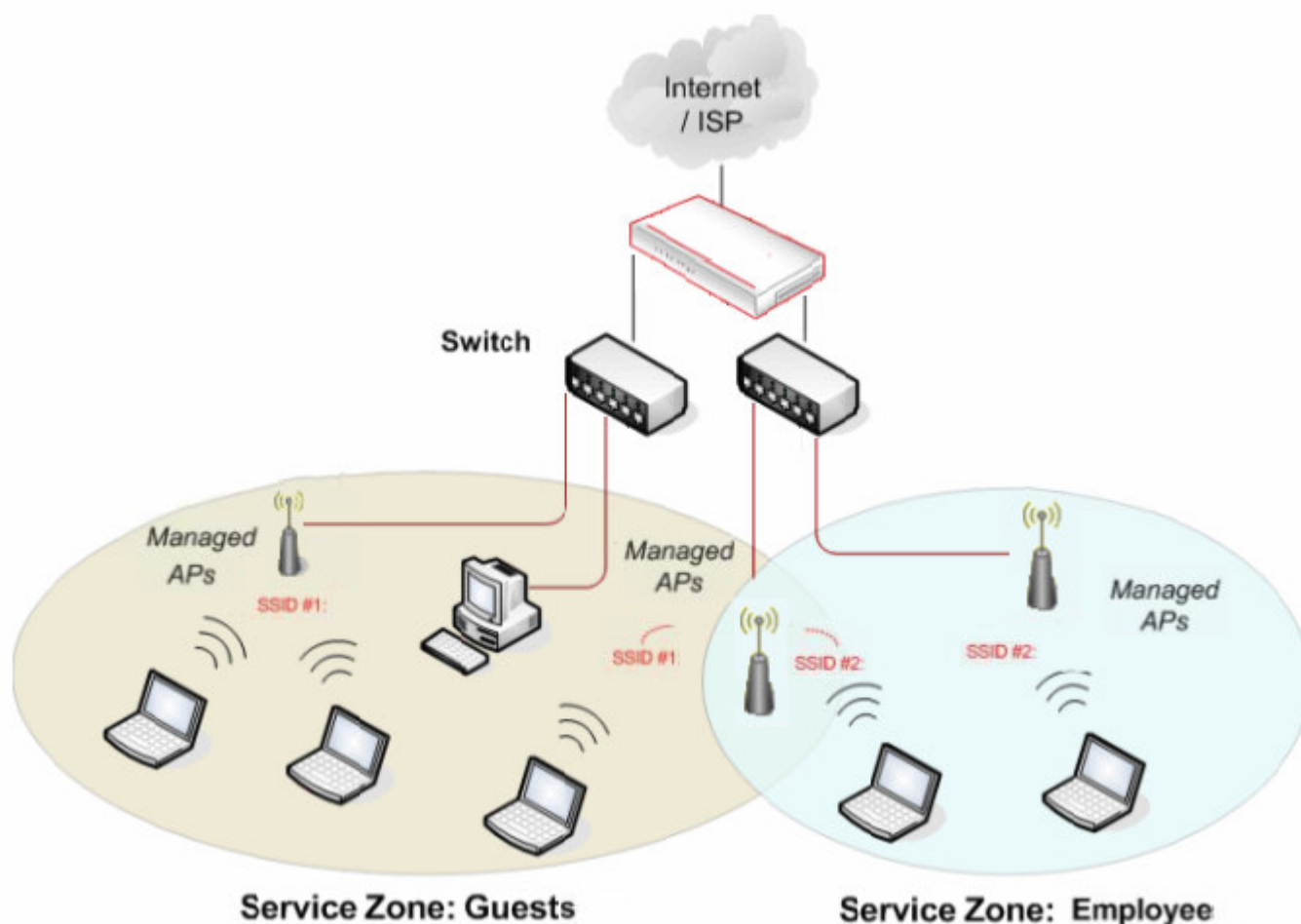
The figure below demonstrates an example of the SMB network deployed with WHG303. Both LAN and WLAN of the system can be secured by IPsec VPN. WHG303 will actively establish VPN tunnels while the selected users are logging in. Not only the traffic within the office network will be protected by IPsec VPN, this VPN module can be configured to support site-to-site IPsec VPN tunnels across remote branch offices. The same clientless VPN setup implementation can also be extended to remote users in accessing office network from public Internet via PPTP VPN tunnels. Once the remote client-to-site PPTP VPN tunnels are established, traveling Employee can connect back to the office network via reliable, secure connections using their portable devices.



[Example: Managed network deployment]

< Port-Based Service Zone Configuration Example >

In **Port-Based** mode, each LAN port can only serve traffic from one Service Zone. An example of network application diagram is shown as below: one Service Zone for **Guests** and one for **Employee**.



The switches deployed under WHG303 in **Port-Based** mode must be **Layer 2 switches** only.


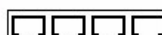

Configuration Steps:

Step 1: Configure Service Zone 1 for Guests

Assume that **LAN1** is assigned to the **Service Zone 1 (SZ1)** for **Guests**. Click the **System** menu and select the **Service Zones** tab. Click **Configure** of SZ1.

General | WAN1 | WAN2 | WAN Traffic | LAN Port Mapping | Service Zones

[Main Menu](#) > [System](#) > Service Zone

Service Zone Settings							
Service Zone Name	LAN Port Mapping	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default		4ipnet	None	Policy 1	Server 1	Enabled	Configure
SZ1		4ipnet-1	None	Policy 1	Server 1	Disabled	Configure
SZ2		4ipnet-2	None	Policy 1	Server 1	Disabled	Configure

Step 2: Configure Basic Settings for SZ1

Check the **Enabled** radio button of *Service Zone Status* to activate SZ1.

Enter a name for SZ1 (e.g. “**Guests**”) in the *Service Zone Name* field.

General	WAN1	WAN2	WAN Traffic	LAN Port Mapping	Service Zones
Main Menu > System > Service Zone > Service Zone Configuration					
Basic Settings					
Service Zone Status		<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled			
Service Zone Name		<input type="text" value="Guests"/>			
Network Interface		Operation Mode <input checked="" type="radio"/> NAT <input type="radio"/> Router IP Address : <input type="text" value="192.168.11.254"/> * Subnet Mask : <input type="text" value="255.255.255.0"/> *			

Step 3: Configure Authentication Settings for SZ1

Check the **Enabled** radio button to enable *Authentication Required for the Zone*.

Check the **Default** button and **Enabled** box of *Guest Users* to set **ONDEMAND** authentication method as default.

Disable all other authentication options. Then, click **Apply** to activate the settings made so far. A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

Authentication Settings					
Authentication Required For the Zone	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input type="radio"/>	<input type="checkbox"/>
	Server 2	POP3	pop3	<input type="radio"/>	<input type="checkbox"/>
	Server 3	RADIUS	radius	<input type="radio"/>	<input type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input type="checkbox"/>
	On-demand User	ONDEMAND	ondemand	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>

Step 4: Configure LAN Port Mapping for SZ1

Select the **LAN Port Mapping** tab from the **System** menu to enter the **LAN Ports and Service Zone Mapping** page. Select **Guests** from the drop-down list box of LAN1. Click **Apply** to save the selection.

General
WAN1
WAN2
WAN Traffic
LAN Port Mapping
Service Zones

[Main Menu](#) > [System](#) > Service Zone Port Role

LAN Ports and Service Zone Mapping

Select the mode for Service Zone ☒ Port-Based ☐ Tag-Based

Specify a desired Service Zone for each LAN Port:

Guest:
LAN1

Default
LAN2

Default
LAN3

Default
LAN4

Apply
Clear

A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.


General WAN1 WAN2 WAN Traffic LAN Port Mapping Service Zones


[Main Menu](#) > [System](#) > Service Zone Port Role


LAN Ports and Service Zone Mapping


Select the mode for Service Zone ☒ Port-Based ☐ Tag-Based

Specify a desired Service Zone for each LAN Port:

Guests ▼


Default ▼


Default ▼


Default ▼


LAN1
LAN2
LAN3
LAN4

You should restart the system to activate the changes. [Restart](#)













LAN1 is now configured for **Guests**.

Step 5: Configure Service Zone 2 for Employee

Assume that **LAN2** is assigned to the **Service Zone 2 (SZ2)** for **Employee**. Select the **Service Zones** tab and click **Configure** of SZ2.

General WAN1 WAN2 WAN Traffic LAN Port Mapping Service Zones

[Main Menu](#) > [System](#) > Service Zone

Service Zone Settings							
Service Zone Name	LAN Port Mapping	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default	   	4ipnet	None	Policy 1	Server 1	Enabled	Configure
Guests	   	4ipnet-1	None	Policy 1	On-demand User	Enabled	Configure
SZ2	   	4ipnet-2	None	Policy 1	Server 1	Disabled	Configure

Step 6: Configure Basic Settings for SZ2

Check the **Enabled** radio button of **Service Zone Status** to activate SZ2.

Enter a name for SZ2 (e.g. **Employee**) in the **Service Zone Name** field.

General WAN1 WAN2 WAN Traffic LAN Port Mapping **Service Zones**

[Main Menu](#) > [System](#) > [Service Zone](#) > Service Zone Configuration

Basic Settings	
Service Zone Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Service Zone Name	<input type="text" value="Employee"/>
Network Interface	Operation Mode <input checked="" type="radio"/> NAT <input type="radio"/> Router IP Address : <input type="text" value="192.168.12.254"/> * Subnet Mask : <input type="text" value="255.255.255.0"/> *

Step 7: Configure Authentication Settings for SZ2

Check the **Enabled** radio button to enable *Authentication Required for the Zone*.

Check the **Default** button and **Enabled** box of *Server 1* to set **LOCAL** authentication method as default. Disable all other authentication options. Then, click **Apply** to activate the settings made so far. A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

Authentication Settings					
Authentication Required For the Zone	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
	Server 2	POP3	pop3	<input type="radio"/>	<input type="checkbox"/>
	Server 3	RADIUS	radius	<input type="radio"/>	<input type="checkbox"/>
	Server 4	LDAP	ldap	<input type="radio"/>	<input type="checkbox"/>
	On-demand User	ONDEMAND	ondemand	<input type="radio"/>	<input type="checkbox"/>
	SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>

Step 8: Configure LAN Port Mapping for SZ2

Select the **LAN Port Mapping** tab from the **System** menu to enter the **LAN Ports and Service Zone Mapping** page. Select **Employee** from the drop-down list box of LAN2. Click **Apply** to save the selection.

General
WAN1
WAN2
WAN Traffic
LAN Port Mapping
Service Zones

[Main Menu](#) > [System](#) > Service Zone Port Role

LAN Ports and Service Zone Mapping

Select the mode for Service Zone ☒ Port-Based ☐ Tag-Based

Specify a desired Service Zone for each LAN Port:

Guest: ▾

Emplo: ▾

Defaul ▾

Defaul ▾

LAN1
LAN2
LAN3
LAN4

Apply
Clear

A warning message “**You should restart the system to activate the changes.**” will appear at the bottom of the page. Click the hyperlink of **Restart** to restart the system and activate all configurations.

General
WAN1
WAN2
WAN Traffic
LAN Port Mapping
Service Zones

[Main Menu](#) > [System](#) > Service Zone Port Role

LAN Ports and Service Zone Mapping

Select the mode for Service Zone ☒ Port-Based ☐ Tag-Based

Specify a desired Service Zone for each LAN Port:

Guest: ▾

Emplo: ▾

Defaul ▾

Defaul ▾

LAN1
LAN2
LAN3
LAN4

You should restart the system to activate the changes. [Restart](#)






Please do not interrupt the system during the restarting process.

Once the settings of two Service Zones are completed, the configured result will be displayed in the **Service Zone Settings** page: **SZ1** and **SZ2** are both enabled.

General WAN1 WAN2 WAN Traffic LAN Port Mapping **Service Zones**

[Main Menu](#) > [System](#) > Service Zone

Service Zone Settings							
Service Zone Name	LAN Port Mapping	SSID	WLAN Encryption	Applied Policy	Default Authen Option	Status	Details
Default		4ipnet	None	Policy 1	Server 1	Enabled	Configure
Guests		4ipnet-1	None	Policy 1	On-demand User	Enabled	Configure
Employee		4ipnet-2	None	Policy 1	Server 1	Enabled	Configure

For configuration of Tag-based/Port-Based service zone and information, please refer to the User's Manual, Appendix D. Service Zone Deployment Example.

P/N: V10020090218