

CERIO Corporation

DR-4000

Multi WAN Gigabit VPN Gateway



User's Manual

Default IP / Login Information

IP Address	192.168.2.1
User Name	root
Password	default

1.	Device and Software Configuration	5
1.1	Device appearance.....	5
1.2	Setup Preparation of Device.....	6
1.3	Login Web Page.....	8
2.	Operating Mode Introduction	10
2.1	Router Mode	10
2.2	Captive Portal Mode	10
3.	System Configuration.....	11
3.1	WAN Setup	11
3.2	WAN Traffic Setup	14
3.3	VLAN Setup	15
3.3.1	Network Button	16
3.3.2	Pull-down menu @ Bandwidth Control	16
3.3.3	Pull-down menu @ DHCP Server	17
3.4	Authentication(Hotspot Setup)	20
	# Authentication Button:	21
	# Authentication Dropdown Button	22
3.4.1	Guest	23
3.4.2	Local User	24
3.4.3	OAuth2.0	24
<input type="checkbox"/>	# Sample for Google OAuth2.0 setup.....	24
<input type="checkbox"/>	# Sample for Facebook OAuth2.0 setup.....	27
3.4.4	POP3 Server	31
3.4.5	Customize Page	31
3.4.6	Language	33
3.4.7	Walled Garden	33
3.4.8	Privilege Address.....	34
3.4.9	Profile	34
3.5	High Availability	35
3.6	VPN Server Setup	37
3.7	VPN Peer Setup	39
3.8	PPTP Server Setup.....	40

3.9	L2TP Server Setup	42
3.10	PPTP/L2TP Account Setup	43
3.11	PPTP/L2TP Client Setup	44
3.12	IPSec Setup.....	46
3.13	Management.....	49
3.14	Time Server	54
3.15	SNMP	56
3.16	DDNS	57
3.17	Log Server Setup	59
3.18	Notification Setup.....	61
4.	Account	64
4.1	RADIUS Server.....	64
4.2	Remote LDAP Setup	64
4.3	Package Setup	66
4.4	Create An Account	68
4.5	Search Account	69
4.6	Regenerated Tickets DB	70
4.7	Thermal Printer Setup	73
4.8	History Log	76
4.9	Online Log	76
4.10	Database Maintenance.....	77
5.	Advance.....	78
5.1	IP Filter	78
5.2	IP Group.....	80
5.3	Port Group.....	81
5.4	MAC Filter.....	82
5.5	Virtual Server	83
5.6	Access Control.....	84
5.7	IP Routing Setup.....	85

5.8	IP Routing Rule Setup	87
5.9	Time Policy	88
6.	Utility.....	90
6.1	Profile Setting.....	90
6.2	System Upgrade	91
6.3	Network Utility	93
6.4	Log Maintenance	94
6.5	Reboot	95
7.	Status.....	96
7.1	Overview	96
7.2	Local System Log	96
7.3	Session Log	97
7.4	Authentication Log	99
7.5	Remote System Log.....	100
8.	Technical documents	102
8.1	Hotspot function used POS system application.....	102
	Login management interface for SP-800.....	103
	Install normal thermal printer	104
	Install QR Code thermal printer	105
	Set web authentication steps for POS system.....	108
8.2	Example for PPTP/L2TP setup	115
8.3	Example for Web Authentication Portal URL using HTTPS	118
8.4	Example of setting up IPSec VPN set LAN to LAN.....	124





1. Device and Software Configuration

1.1 Device appearance



1. DC Jack Power interface **(Power input- interface-1)**

2. LED status indicator:

	<p>PWR LED: When it is confirmed that the PoE input or DC input power is powered on, this LED is always on when the power is turned on.</p>
	<p>Fail LED : System problem warning LED ,Operating system storage data cannot be accessed , (The light is always on when there is a fault).</p>
	<p>Online LED : Online working LED , It flashes during the system startup process, and stays on after the system startup is successful and confirmed, (Indicating that the Ready state is successful).</p>
	<p>Ethernet port LED : Link/Act connection LED from ETH1 port to ETH4 port</p>

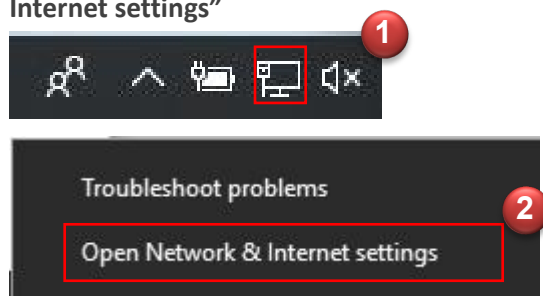
3. **Reset button** (to restore the factory default, please press it for about 10-15 seconds. The Online LED and Fail LED will flash at the same time, indicating confirmation. You can release the button and wait for the system to return to the factory default).
4. **Gigabit / ETH1 (POE) Ethernet port**, The WAN or LAN port can be changed through software configuration **(Power input- interface-2)**.
5. **Gigabit / ETH2 (POE) Ethernet port**, The WAN or LAN port can be changed through software configuration **(Power input- interface-3)**.
6. **Gigabit / ETH3 Ethernet port**, The WAN or LAN port can be changed through software configuration.
7. **Gigabit / ETH4 Ethernet port**, the WAN or LAN port can be changed through software configuration.
8. **GND** ground screw pad , The contact point for the housing ground screw of this device.

1.2 Setup Preparation of Device

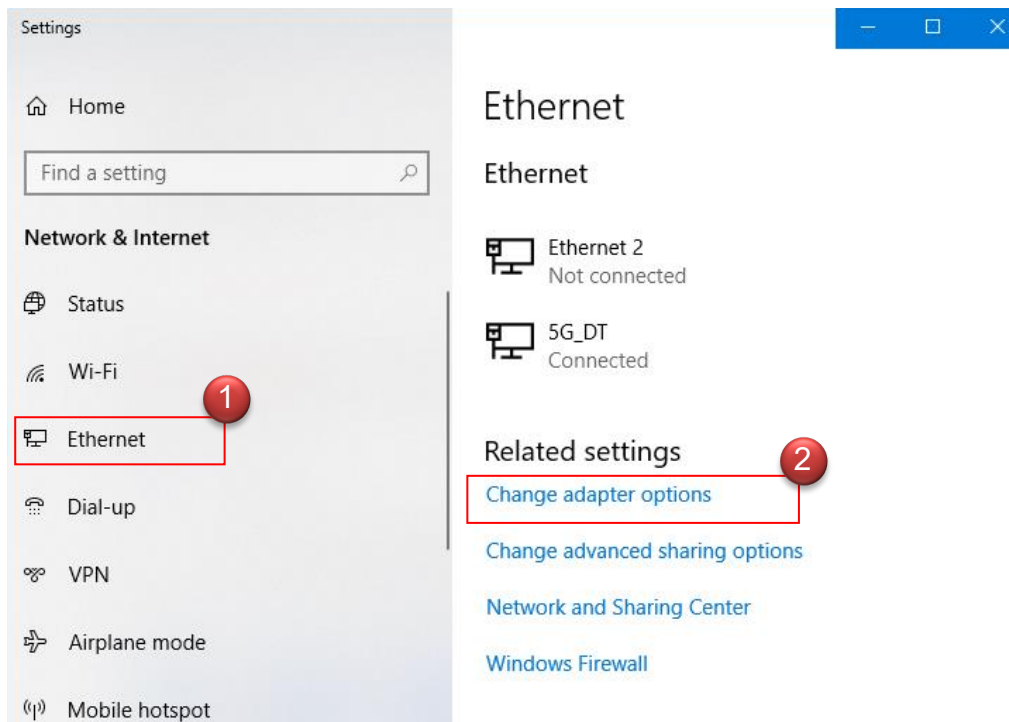
Please PC link to Device used cat5/6 Ethernet cable.

[The following setup uses a Windows PC, user OS may vary.](#)

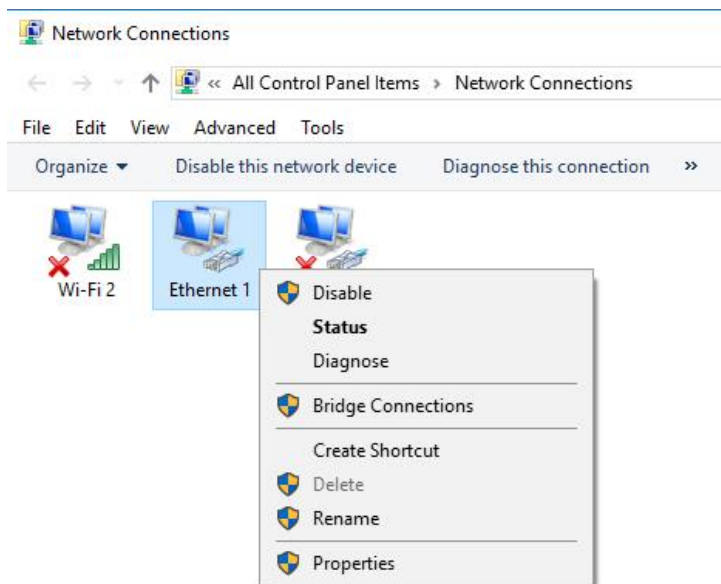
Step 1: Please click on the computer icon in the bottom right window, and click “Open Network and Internet settings”



Step 2: After click left side "Ethernet" function, click on the right side “Change adapter options” again.



Step 3: In “Change adapter options” Page. Please find Ethernet (Local LAN) and Click the right button on the mouse and Click “Properties”

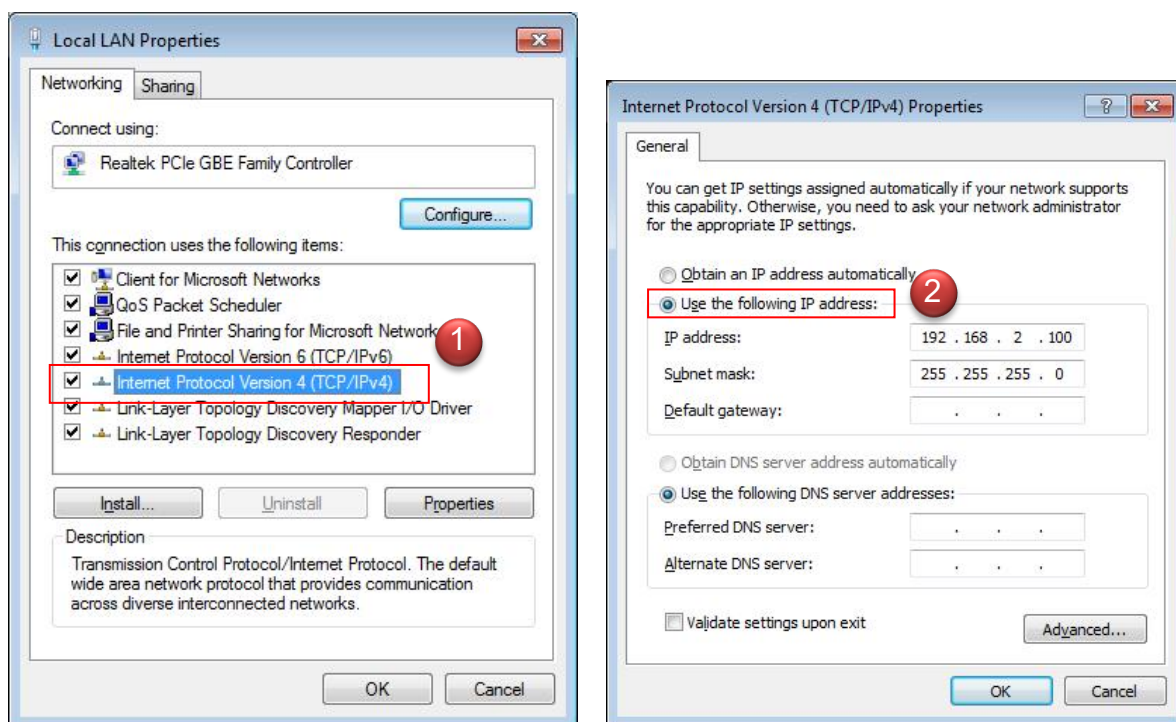


Step 4: In Properties page to setting IP address, please find “Internet Protocol Version 4 (TCP/IPv4)” and double click or click “OK” button.

Step 5 : Select “Use the following IP address”, and fix in IP Address : 192.168.2.#

ex. The # is any number by 1 to 253

Subnet mask : 255.255.255.0



And Click "OK" to complete the fixed computer IP setting

1.3 Login Web Page

DR-4000 supports web-based configuration. Upon the completion of hardware installation, **DR-4000** can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later version or similar browser.

- **Default IP Address:** 192.168.2.1
- **Default Subnet Mask:** 255.255.255.0
- **Default Username and Password**

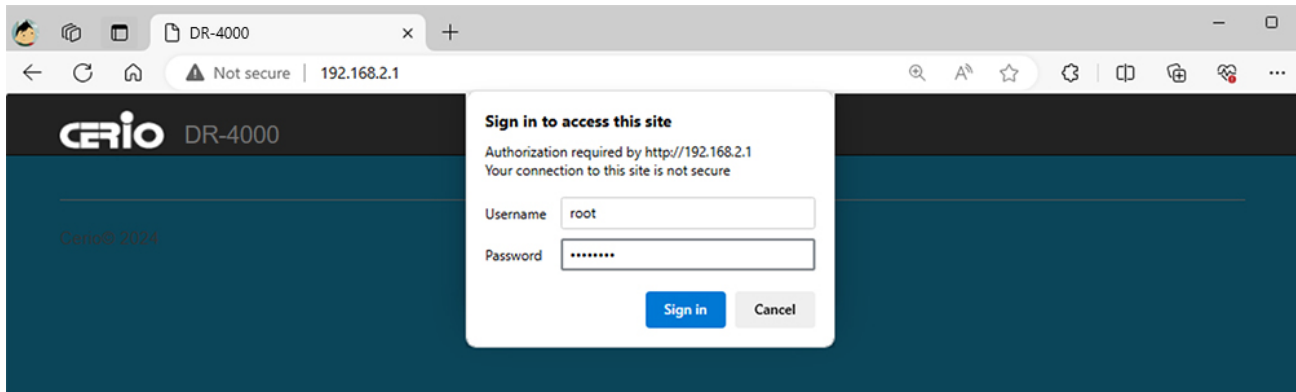
MODE	Router mode	
Management Account	Root Account	
Username	root	
Password	default	



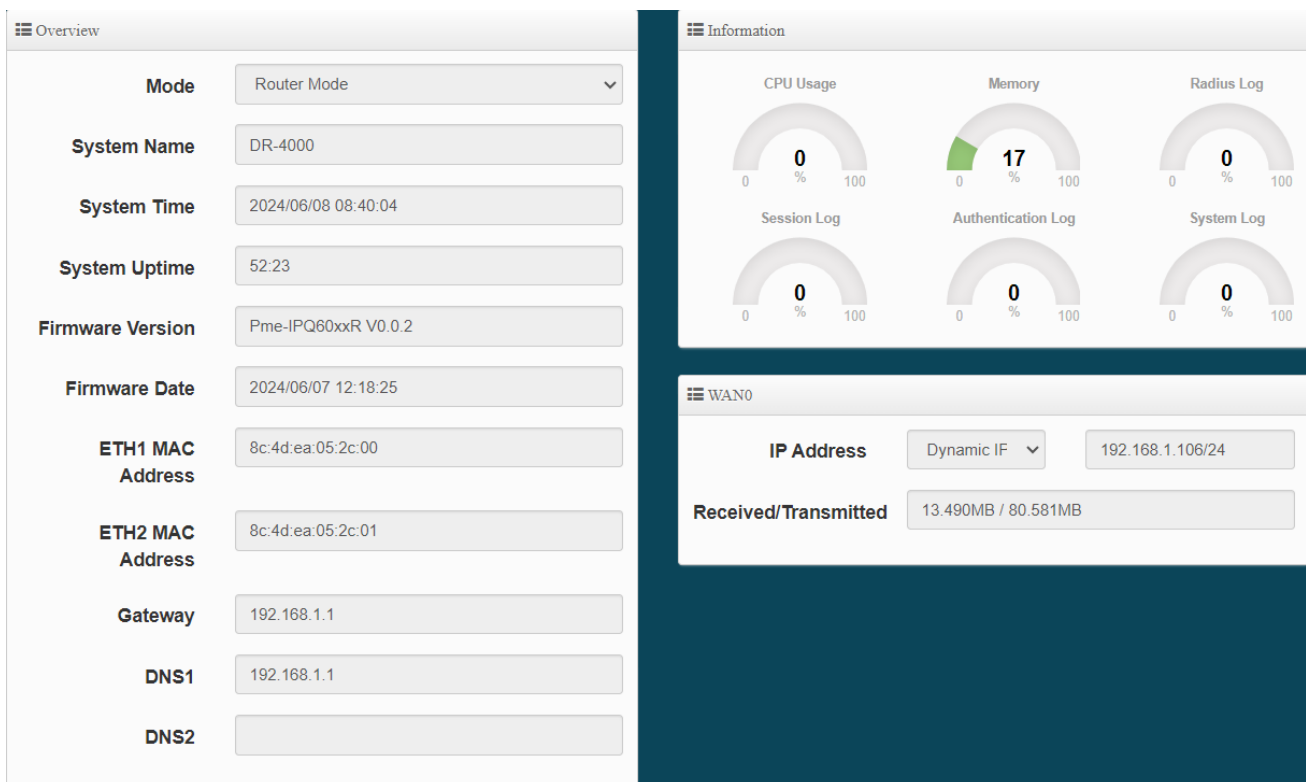
Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.1

Launch Web Browser

Open IE browser or other browsers such as Firefox, Chrome, and Edge, and enter the device default IP address in the URL address bar: <http://192.168.2.1> to open the WEB management interface.



Please use default Users name: **“root”** and default password **“default”** to login.

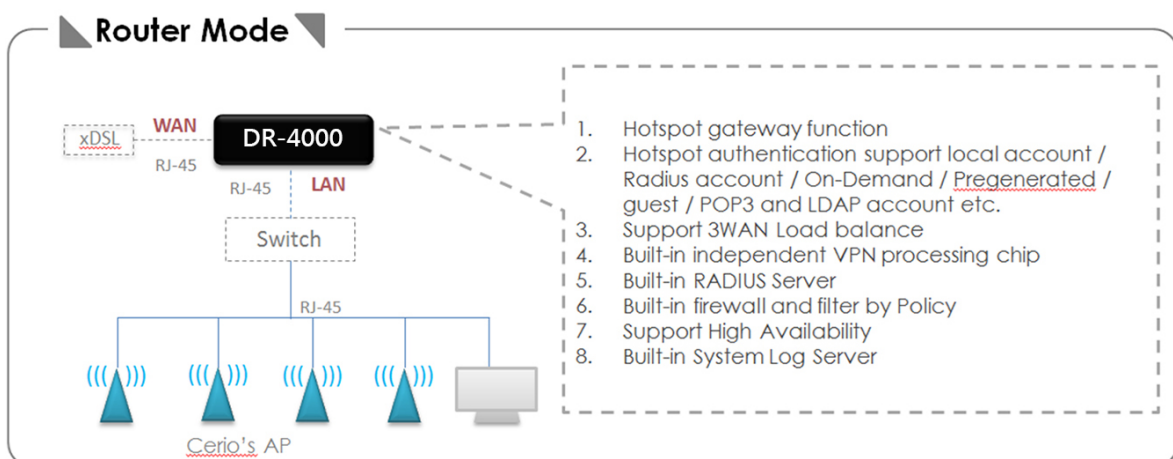


2. Operating Mode Introduction

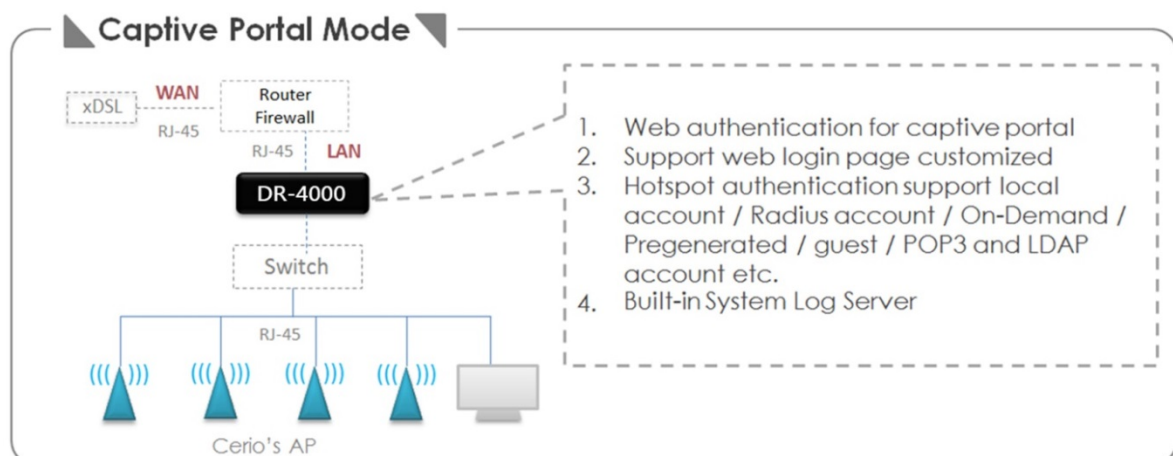
2.1 Router Mode

When administrator select use Route mode then system can set 1WAN 3LAN Router also can select 1LAN 3WAN and 2WAN/2LANoutbound load balancer.

This Router mode support IP Routing setup/Firewall/HA/VPN/Multi-WAN/QoS enforcement and Built-in AAA Radius server



2.2 Captive Portal Mode



If the environment already has a router or firewall device, administrator demand is only to add the new page hotspot function, this time can be switched to Captive Portal mode and connected in parallel to the router or firewall equipment can be completed (The mode is no Router NAT function in this mode).

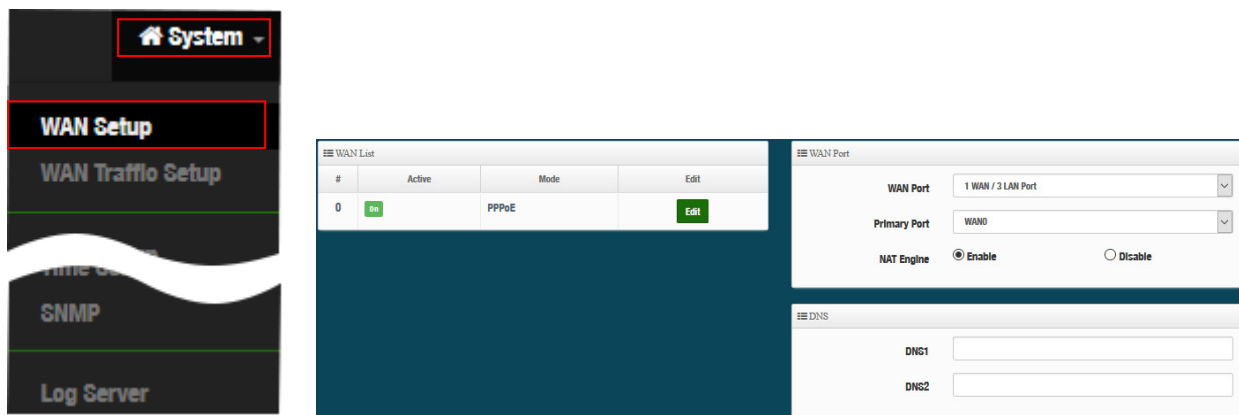
(The default IP of this mode is also 192.168.2.1, but it is not designed to be linked to the IP location of Router mode. When switching to this mode, please make sure that the IP network segment of the connected computer is also the same as 192.168.2.X. You have successfully entered this mode. model)

3. System Configuration

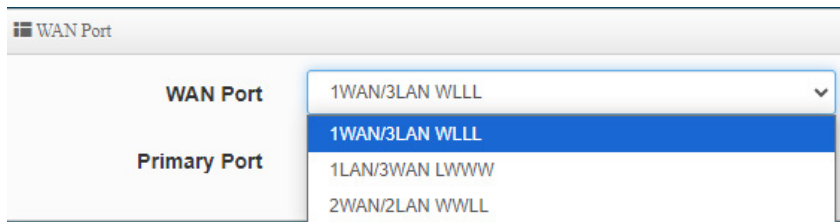
CERIO's **DR-4000** is multifunctional authentication Gateway, support multi-WAN outbound load balance. The **DR-4000** Built-in hardware independent VPN engine administrator can build a secure tunnel in the network environment and support High Availability can make sure that the network is working normally.

3.1 WAN Setup

Administrator can set one WAN or multi-WAN load balance in the WAN Setup function. Please click System → WAN Setup

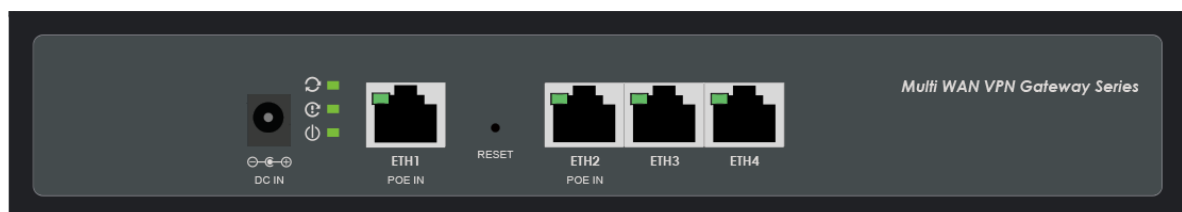


WAN Port Setup



- **WAN Port:** Administrator can select 1WAN/3LAN or 1LAN/3WAN or 2WAN+/2LAN, the default is 1WAN/3LAN Port.


Physical Ethernet Ports Settings Detailed list of different WAN and LAN ports:



Ethernet Speed		1Gb	1Gb	1Gb	1Gb
Mode / Port		ETH1	ETH2	ETH3	ETH4
1	1WAN(1Gb)/3WAN(1Gb+1Gb+1Gb) / WLL	WAN	LAN	LAN	LAN
2	1LAN(1Gb)/3WAN(1Gb+1Gb+1Gb) / LWWW	LAN	WAN	WAN	WAN
3	2WAN(1Gb+1Gb)/2LAN(1Gb) / WWLL	WAN	WAN	LAN	LAN

- **WAN List**: When selecting Multi-WAN, the WAN Priority setting will be displayed. Please click the Save button and the system will display the list of Multi-WAN.

WAN List			
#	Active	Mode	Edit
0	On	Dynamlp IP	Edit
1	On	Dynamlp IP	Edit
2	On	Dynamlp IP	Edit



When selecting 2WAN up , you can set the load balancing priority setting on the WAN traffic setting function page.

- **WAN Priority** : The system will first determine the priority of 3WAN,The smaller the value, the higher the priority. If setting to 1/1/2, it is WAN0/WAN1 Load Balance, and WAN2 is used as Backup function. If it is setting to 1/1, it is WAN0/WAN1 Load Balance. If it is setting to 1/2, WAN2 is used as Backup function..



WAN0 Priority

1

WAN1 Priority

1

WAN2 Priority

1

- **Primary Port**: If set 2 WAN or 3WAN function, administrator must select one primary for WAN Port, The WAN Port "primary port" setting,which mainly allows the system to use through the set WAN port, such as "system time" or DNS access, etc. If there is no special application, Please set to the default value "WAN0 ".
- **NAT Engine**: If enable the function then NAT will up performance, but firewall and routing rule of **DR-4000** will auto disable.
-

WAN List

Administrator can set four connection types for the WAN port: Static IP, Dynamic IP, PPPoE and PPTP, at the same time can also Enable or Disable for NAT or DMZ functions.

Please click Edit button in WAN List.

WAN List			
#	Active	Mode	Edit
0	<input checked="" type="checkbox"/>	PPPoE	<input checked="" type="button" value="Edit"/>
1	<input checked="" type="checkbox"/>	Dynamic IP	<input type="button" value="Edit"/>
2	<input checked="" type="checkbox"/>	Dynamic IP	<input type="button" value="Edit"/>

➤ **Edit:** Administrator can set WAN function.

WAN Setup

WAN

☒ Enable
 ☐ Disable

WAN Settings

Mode

PPPoE

PPPoE

User Name

73137845@hinet.net

Password

MTU

1492

Reconnect Mode

Always On

MAC Clone

Mode

Default MAC Address

NAT

☒ Enable
 ☐ Disable

DMZ Setup

Mode

Disable

- **WAN Setup:** Administrator can set Enable or Disable for the WAN Port function.
- **WAN Settings:** Administrator can select Static IP, Dynamic IP, PPPoE and PPTP type of the WAN Port.
- **MAC Clone:** The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.
- **NAT:** Administrator can set Enable or Disable the NAT function. If Disable NAT function administrator must manual to set routing.
- **DMZ:** DMZ is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet. External-facing

servers, resources and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet.

3.2 WAN Traffic Setup

WAN Traffic setup function improves the distribution of workloads across multiple computing resources. WAN Traffic function aims to optimize network resource use maximize throughput or minimize response time and avoid overload of any single WAN port resource.

If administrator set multi-WAN configuration, administrator can assign weights or speed weights to WAN in the "**WAN traffic setup**" function to indicate the percentage of traffic that should be sent to each WAN.



Load Balance Mode

Mode: Assign Weight

Connection Mode: Source IP Based

- **Mode:** If set multi-WAN, administrator can select Load Balance by Assign Weight or Line Speed Weight.
- **Assign Weight:** The WAN Assign Weight function can setup handle more requests and handle fewer requests. Assigning weights to WAN allows the **DR-4000** appliance to determine how much traffic each load balanced server can handle, and therefore more effectively balance load. The Weight set Max=10 unit.

Assign Weight

WAN0 Weight	1	33%
WAN1 Weight	1	33%
WAN2 Weight	1	33%

- **Line Speed Weight:** The function requires administrator to definitely specify the real upload and download line speed of each WAN interface, the system will calculates the maximum bandwidth for all WAN interfaces and then the flow distribution.

Line Speed Weight

WAN0 (U/D)kbps	<input type="text" value="1024000"/>	<input type="text" value="1024000"/>
WAN1 (U/D)kbps	<input type="text" value="1024000"/>	<input type="text" value="1024000"/>
WAN2 (U/D)kbps	<input type="text" value="1024000"/>	<input type="text" value="1024000"/>

- **Connection Detect:** Enable connection detection, set the target IP of the specified Ping, and set the interval period of each Ping in "seconds". Set the Failure Count after the number of failures to truly enable WAN load balancing .

Connection Detect

Service ☒ Enable ☐ Disable

IP Address to Ping

Ping Interval Second

Failure Count

3.3 VLAN Setup

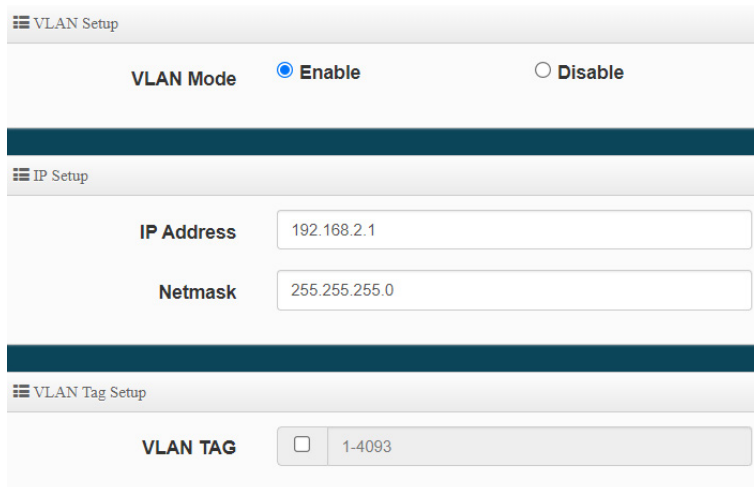
The default Router mode supports 16 groups of virtual network services. By default, each virtual network supports the 802.1Q Tag VLAN function. The administrator only needs to click Enable, and the system will be able to complete the setting of 802.1Q Tag VLAN.

VLAN List					
#	VLAN Mode	Flag	IP Address	Netmask	Action
0	<input checked="" type="checkbox"/>	Native	192.168.2.1	255.255.255.0	Network
1	<input type="checkbox"/>	VLAN TAG: 101	192.168.101.254	255.255.255.0	Network
2	<input type="checkbox"/>	VLAN TAG: 102	192.168.102.254	255.255.255.0	Network
3	<input type="checkbox"/>	VLAN TAG: 103	192.168.103.254	255.255.255.0	Network
4	<input type="checkbox"/>	VLAN TAG: 104	192.168.104.254	255.255.255.0	Network
5	<input type="checkbox"/>	VLAN TAG: 105	192.168.105.254	255.255.255.0	Network
6	<input type="checkbox"/>	VLAN TAG: 106	192.168.106.254	255.255.255.0	Network
7	<input type="checkbox"/>	VLAN TAG: 107	192.168.107.254	255.255.255.0	Network

- **VLAN Mode** : Display on/off for the VLAN network.
- **Flag** : Display master VLAN and VLAN Tag No. information.
- **IP Address** : Display IP Address for VLAN Network.
- **NetMask** : Display IP netmask.
- **Action** : click button o set VLAN network functions , click Pull-down menu to" Bandwidth Control" and "DHCP Server".

3.3.1 Network Button

Administrator can click  button to set VLAN network functions.



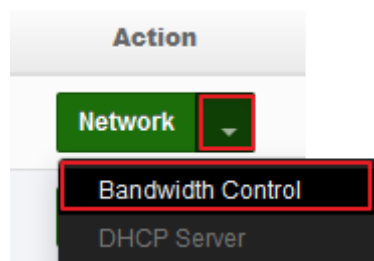
- ✓ **VLAN Mode** : Administrator can select Enable or disable for the VLAN Network.
- ✓ **IP Mode** : Administrator can select enable or disable function for VLAN IP.
- ✓ **IP Address/ NetMask** : Administrator can set IP address and netmask for the VLAN.



VLAN services and IP addresses must have at least one set of VLAN services. **Do not turn off the default set of virtual network service (VLAN) functions (equal to no LAN state), which will cause the need to return to the default values. Need to re-setting again for the device.**

3.3.2 Pull-down menu @ Bandwidth Control

Administrators can set bandwidth limit the max/min bandwidth of the Wi-Fi users, Bandwidth control can set IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP and WEB.



Bandwidth Control

Mode: ☒ Enable ☐ Disable

Session Limit Per IP: ☐ 1024

Total Bandwidth Control

Mode: ☐ Enable ☒ Disable

Upload: Kbps

Download: Kbps

- **Mode : IP:** Administrators can choose to enable or disable bandwidth control function.
- **Session Limit Per IP:** Session limit by all IP address, The default value is to limit the use of each user IP to 1024 Sessions
- **Total Bandwidth Control:** UP/Download bandwidth limit by VLAN
- **OoS Rule List:** Administrator can set IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP and WEB to management bandwidth, Max can set 10 rule.

#	Active	Rule Mode	Value1	Value2	Upload(Kbps)	Download(Kbps)	Comment
1	<input checked="" type="checkbox"/>	ANY			1024	1024	
2	<input type="checkbox"/>	IP/Mask			1024	1024	
3	<input type="checkbox"/>	IP Range			1024	1024	
4	<input type="checkbox"/>	Port			1024	1024	
5	<input type="checkbox"/>	SIP			1024	1024	
		RTSP			1024	1024	
		RTP			1024	1024	
		WEB			1024	1024	

- **Any:** Bandwidth control by any protocol.
- **IP/MASK:** Bandwidth control by a subnet.
- **IP Range:** Bandwidth control by IP range.
- **Port:** Bandwidth control by port (service), ex. FTP port (20,21)
- **SIP:** Bandwidth control by Session Initiation Protocol.
- **RTSP/RTP:** Bandwidth control by Streaming.
- **WEB:** Bandwidth control by web protocol.

3.3.3 Pull-down menu @ DHCP Server

Administrator can set DHCP function. Please click **Network** pull-down button to set DHCP Server.

Network ▼

DHCP Server

DHCP Service

Mode ☒ Enable ☐ Disable
DHCP Relay ☐ Enable ☒ Disable

DHCP Setup

Start IP
End IP
Netmask
Gateway
DNS1 IP
DNS2 IP
WINS IP
Domain
Lease Time

DHCP Client List

#	IP Address	MAC Address	Hostname	Expired	Action
-	-	-	-	-	-

Static Lease IP Setup

Comment
IP Address
MAC Address

Static Lease IP List

#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

- ✓ **Mode:** Administrator can select enable / disable the function
- ✓ **DHCP Relay :** Administrator can select enable / disable the function

DHCP Service

Mode ☒ Enable ☐ Disable
DHCP Relay ☒ Enable ☐ Disable

DHCP Relay Setup

Server Interface

CenOS 2024

WAN0
 WAN1
 WAN2
 VLAN1
 VLAN2
 VLAN3
 VLAN4
 VLAN5
 VLAN6
 VLAN7
 VLAN8
 VLAN9
 VLAN10
 VLAN11
 VLAN12
 VLAN13
 VLAN14
 VLAN15

- **Server Interface :** For this function, you can choose to have DHCP Relay follow the interface, you can choose the enabled WAN0~2 interface, or choose the DHCP settings of other VLAN interfaces VLAN1~VLAN15.
- ✓ **Start IP:** Set Start IP for DHCP Service.
- ✓ **End IP:** Set End IP for DHCP Service.

- ✓ **Netmask: Set IP Netmask, the default is 255.255.255.0**
- ✓ **Gateway: Set Gateway IP for DHCP Service.**
- ✓ **DNS (1-2) IP: Set DNS IP for DHCP Service.**
- ✓ **WINS IP: Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.**
- ✓ **Domain: Enter the domain name for this network.**
- ✓ **Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds**

DHCP Client List

#	IP Address	MAC Address	Hostname	Expired	Action
1	192.168.2.10	08:00:27:00:00:00	cerio_01-10	20:0:43	Fixed
2	192.168.2.12	08:00:27:00:00:00		18:48:16	Fixed

Static Lease IP Setup

Comment

IP Address

MAC Address

Add

Static Lease IP List

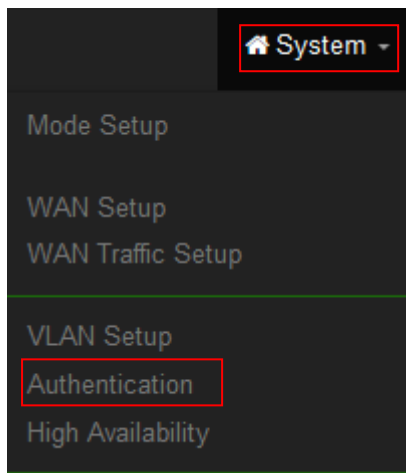
#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

- **DHCP Client List:** Administrator can view IP address used status of client users on each DHCP Server.
- **Static Lease IP Setup:** Administrator can set be delivered fixed IP address to the users. (This MAC Address binding IP address function can bind up to 100 sets of settings).

3.4 Authentication(Hotspot Setup)

The function is for hotspot Authentication. It supports authentication for local users / RADIUS Server / OAuth2.0 and Guest. RADIUS Server authentication support PoP3 / LDAP(AD) and Package.

Please click on **System -> Authentication**



VLAN List			
#	VLAN Mode	Authentication	Action
0	On	Off	Authentication
1	Off	Off	Authentication
2	Off	Off	Authentication
3	Off	Off	Authentication
4	Off	Off	Authentication
5	Off	Off	Authentication
6	Off	Off	Authentication
7	Off	Off	Authentication

- **#** : Display 8 VLANs list of Authentication.
- **VLAN Mode** : Displays VLAN on/off status.
- **Authentication** : Displays VLAN# whether enable or disable web authentication.
- **Action** : The function has 2 buttons (Authentication and Dropdown)

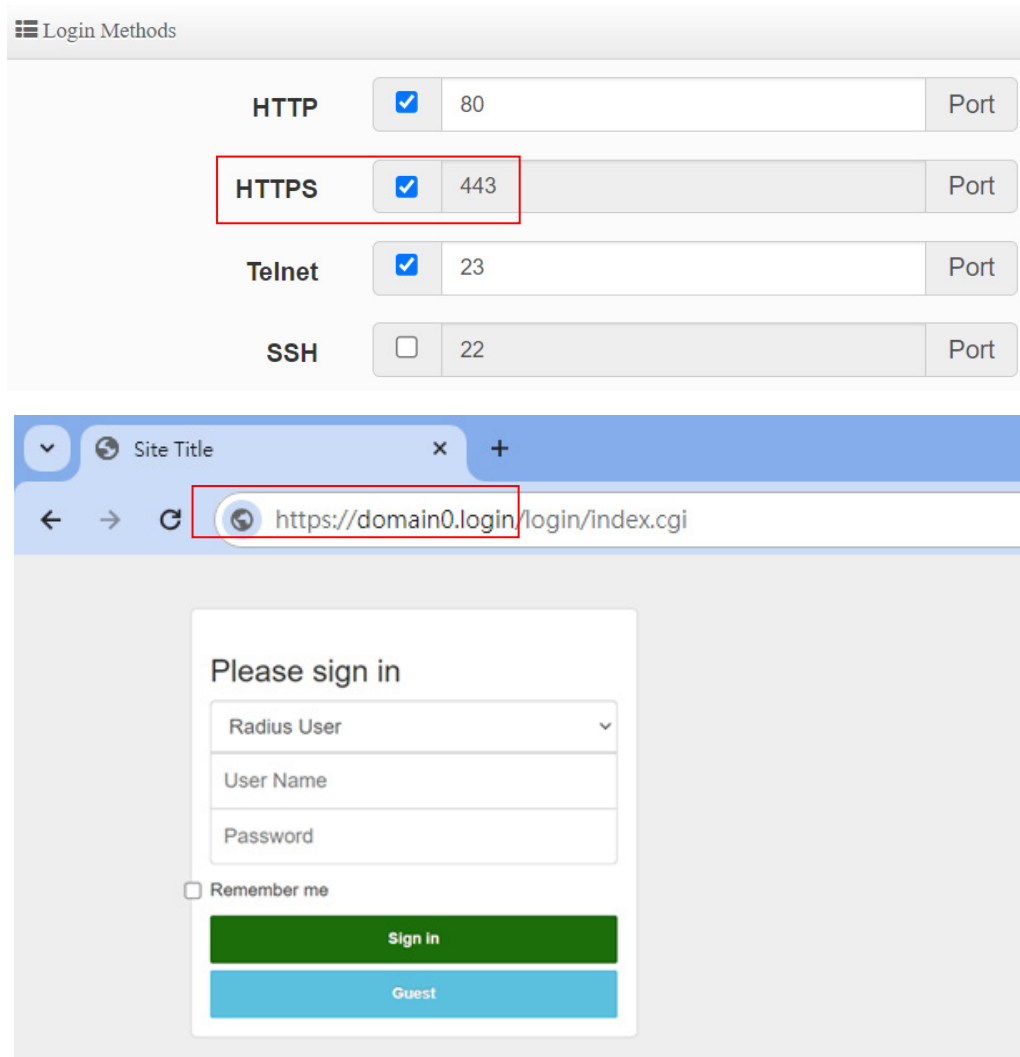
Authentication Button:

Authentication : By clicking the Authentication button, administrator can enable or disable this function.

The screenshot displays the Cerio web interface with three main configuration panels. The 'Authentication' panel on the left has a toggle set to 'Enable'. Below it, the 'Authentication Setup' panel includes fields for 'Multiple Login' (checkbox), 'Login Timeout' (10 minutes), 'Redirect URL' (http://www.google.com), and 'Login URL' (domain0.login). It also has radio buttons for 'Authentication Log' and 'Session Log', both set to 'Disable'. The 'Radius Setup' panel on the right has a toggle set to 'Disable' and a 'Display Name' field containing 'Radius User'. The 'Local User Setup' panel at the bottom has a toggle set to 'Disable' and a 'Display Name' field containing 'Local User'.

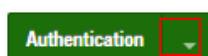
- **Authentication** : Administrator can enable or disable authentication function.
- **Multiple Login** : Administrator can set one account to multiple users simultaneously login and the users can set limit.(0 = not limited)
- **Login Timeout** : After account login for some time no traffic, system will automatic timeout for account. Administrator can enter a time(Minutes).
- **Redirect URL** : After the success of the login, system will redirect to URL. Administrator can enter web site URL.
- **Login URL** : Administrator can set URL for login page. Set the URL that automatically triggers the login page. When you start the web page and want to log in, directly enter the default login page URL <http://domain0.login>, and you can quickly jump to the complete login authentication login page <http://domain0.login/login/index.cgi>. , if you want to use <https://domain0.login>, please be sure to confirm whether HTTPS login is enabled and open for use in the "Management Interface Login Settings". Please refer to 3.13 System Management → "Login Methods" Settings, or as shown below.

If you want to use the HTTPS secure transmission function, you must also import the corresponding SSL security certificate file (such as owner name, organization, location, etc.). For how to import the SSL certificate function, please refer to 6.1 "Utility" → "Profile Setting" → "Management" → ☐ From Instructions for **Update SSL Certification From Local Hard Drive.**

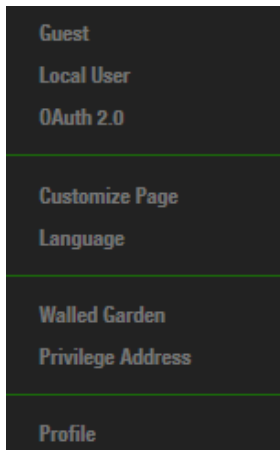


- **Authentication Log:** Account authentication log will copy to the device 's syslog server.
- **Session Log :** If network have Syslog server. Administrator can to system→management setting IP address for syslog server and enable the function. Account session log will copy to the device 's syslog server.
- **Local User :** Administrator can enable authentication for local user. Create user account can to reference **"3.4.2 Local User"**.
- **RADIUS :** Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.

Authentication Dropdown Button



: By Clicking the Dropdown button, Administrators can set authentication functions.



3.4.1 Guest

Administrator can enable or disable guest authentication. If enabled, the administrator can set guest Count Limit / login time and type and flow control.

- **Service** : Administrator can select enable or disable this function.
- **Login Type** :
 - **One Time**: Login to start counting until the end of time.
 - **Multiple Times**: logout time will stop counting until the next re-login to time start counting.
- **Count Limit**: Administrator can set guest limit.
- **Login Time**: Within a certain timeframe with no traffic, the system will auto logout. (The default is 10 minutes, you can fill in 0-720 minutes and 0 is unlimited).
- **QoS**: Administrator can restrict the traffic of guest. Traffic management can set users upload and download traffic.

3.4.2 Local User

Administrator can create local user account for web login.

Local User

User Name

(3-32 chars)

Password

(4-32 chars)

Add

Local User List

#	Name	Action
1	oerio	Delete
2	danny	Delete

- **User Name** : Administrator can create users account.
- **Password** : Set account password.

3.4.3 OAuth2.0

The OAuth2.0 function supports Facebook and Google by default. Users can add additional OAuth2.0 servers through UI settings.

OAuth 2.0 Provider List				Create New Provider
#	Active	Provider	Action	
1	Off	Google	Edit	
2	Off	Facebook	Edit	

- **#** : Display items.
- **Active** : Display on/off status for the authentication.
- **Provider** : Display authentication server. The system default use authentication server for Google and Facebook

➔ # Sample for Google OAuth2.0 setup

Please complete the application on the Google website to receive an account ID and password, follow the steps below.

Step.1 Please go to the **Google Developers Console** page and **create a project**

(Reference <https://developers.google.com/identity/protocols/OAuth2>)

New Project

Project name ?

Your project ID will be cerio-aap-login ? [Edit](#)

[Show advanced options...](#)

[Create](#) [Cancel](#)

Step.2 Click Credentials to create OAuth client ID in the API manager page.

API API Manager

- Overview
- Credentials**

API key
Identifies your project using a simple API key to check quota and access. For APIs like Google Translate.

OAuth client ID
Requests user consent so your app can access the user's data. For APIs like Google Calendar.

Service account key
Enables server-to-server, app-level authentication using robot accounts. For use with Google Cloud APIs.

Help me choose
Asks a few questions to help you decide which type of credential to use.

[Create credentials](#)

Step.3 Select web application in the “Application Type” section and set “Restrictions” URL.

Create client ID

Application type

☒ Web application

☐ Android [Learn more](#)

☐ Chrome App [Learn more](#)

☐ iOS [Learn more](#)

☐ PlayStation 4

☐ Other

[Create](#) [Cancel](#)

Name

Web client 1

Restrictions

Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://www.example.com

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

http://www.example.com/oauth2callback

Step.4 Set Authorized JavaScript origins and Authorized redirect URLs (important)

Administrator must set login URL in the device function. After complete set of login URL go to the “**Restrictions**” function in web page. Follow the steps below to set login URLs

- Setup login URL in the device. Please Click **system** ➔ **Authentication** and enable the function.
- The “Authentication Setup” page to set Login URL

Authentication Setup

Multiple Login

☐ 3

User(s)

Login Timeout

10

Minutes

Redireot URL

http://www.google.com

Login URL

domain0.login.com

Session Log

☐ Enable
 ☒ Disable

After complete set of login URL go to the “**Restrictions**” function in web page. Copy and paste the login URL from the system display into the “Restriction” page on the Google Developer website.

- Google Authorized JavaScript origins URL is **http://domain0.login.com** (same as Login URL)
- Google Authorized redirect URLs is **http://domain0.login.com/login/callback.cgi**

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://domain0.login.com

http://www.example.com

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

http://domain0.login.com/login/callback.cgi

Step.5 After completing the “Restrictions” setup, click the create button. An OAuth Client page will pop-up with your “client ID” and “client secret”. Administrators must copy and paste their client ID and secret into the OAuth 2.0 Setup page in our software UI.

OAuth client

Here is your client ID

googleusercontent.com

Here is your client secret

kDYwM

OK

OAuth 2.0 Setup Advanced

Client ID

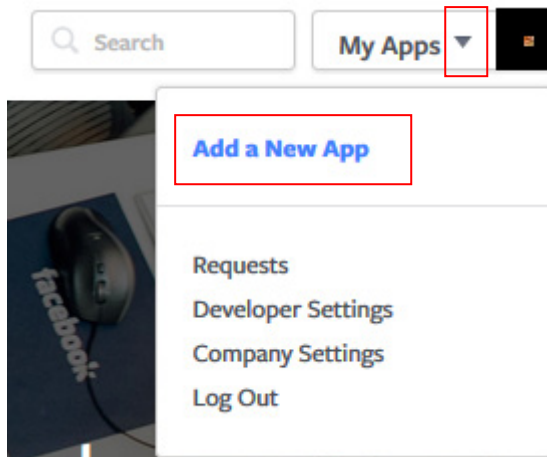
Client Secret

Save and reboot the AP system, complete the setup.

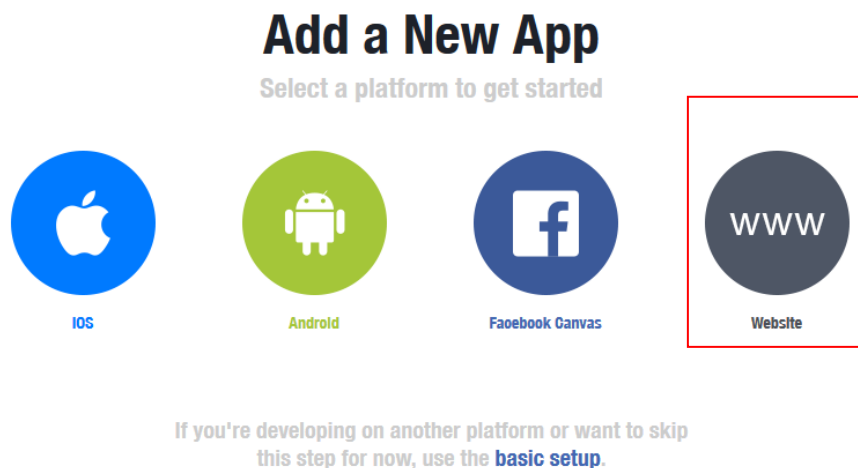
➔ # Sample for Facebook OAuth2.0 setup

Please complete the application on the Facebook website to receive an account ID and password, follow the steps below.

Step.1 Please to Facebook developer's page and add a New App



Step.2 Select WWW function



Step.3 Administrator must set www for your information.

Create a New App ID
Get started integrating Facebook into your app or website

Display Name

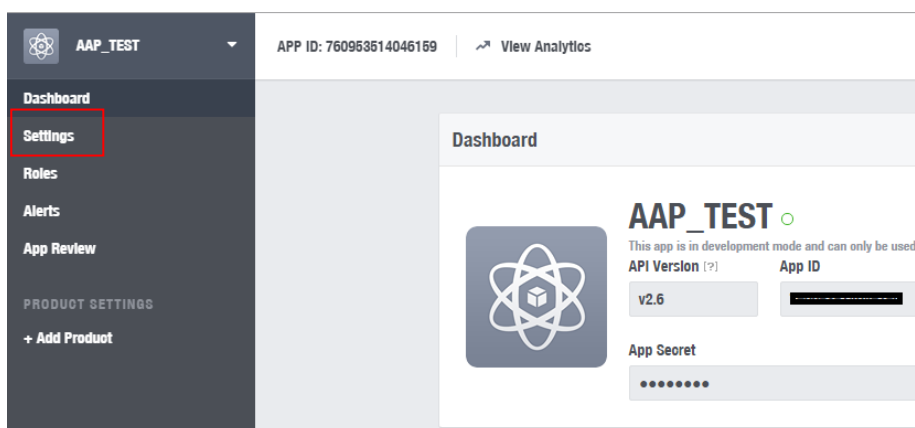
Namespace

Contact Email

Category

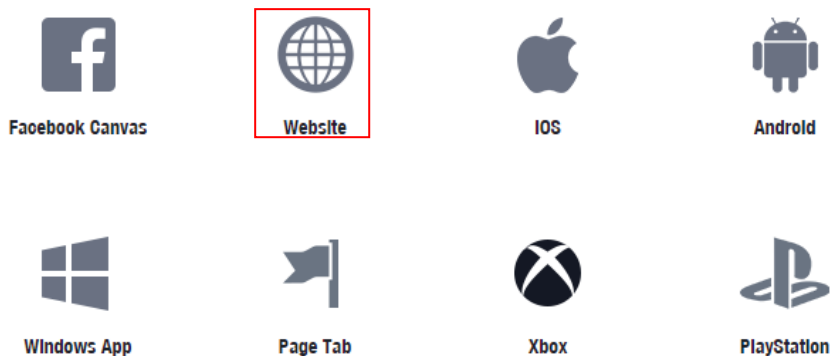
By proceeding, you agree to the [Facebook Platform Policies](#)

Step.4 Please click “Setting” and add Platform



Step.5 Select Platform for “Website”

Select Platform



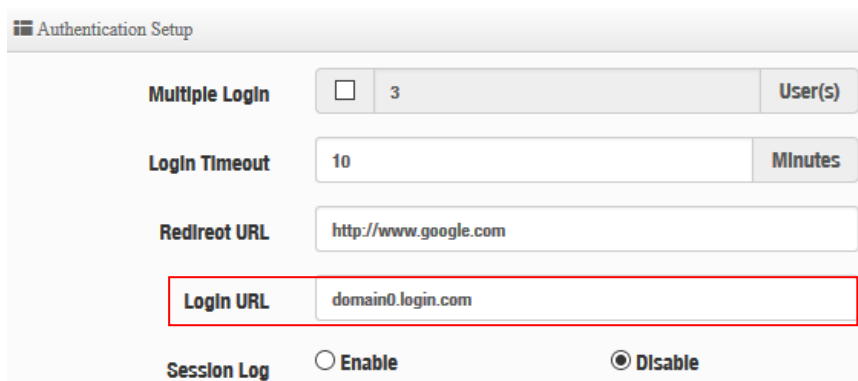
Step.6 Enter URL is **http://domain0.login.com/login/callback.cgi**

Site URL

http://domain0.login.com/login/callback.cgi

Administrator must set login URL in the device function. After complete set of login URL go to the “Facebook Site URL” function in web page. Follow the steps below to set login URLs

- Setup login URL in the device. Please Click **system** ➔ **Authentication** and enable the function.
- The “**Authentication Setup**” page to set Login URL



Authentication Setup

Multiple Login ☐ 3 **User(s)**

Login Timeout 10 **Minutes**

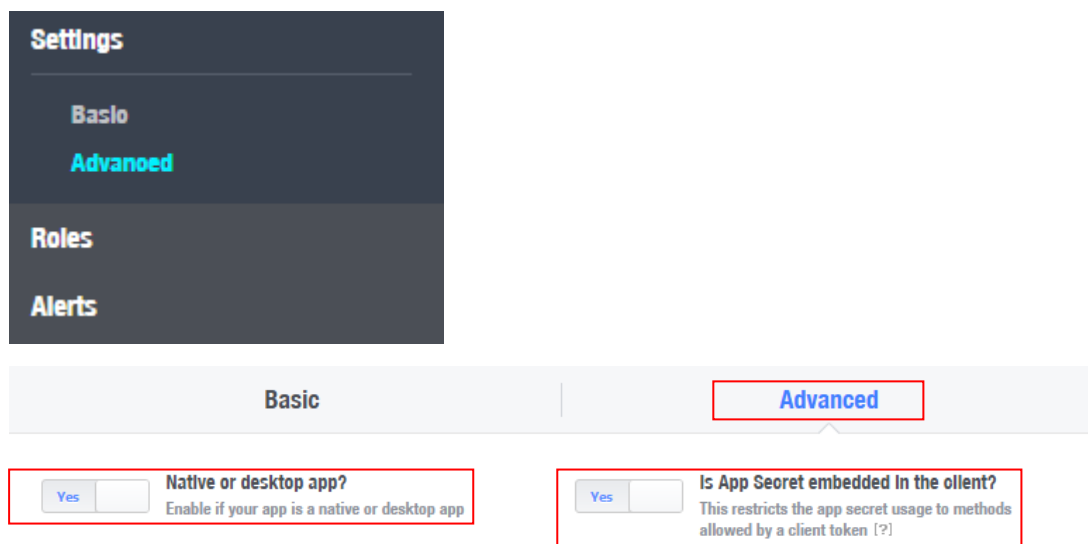
Redireot URL http://www.google.com

Login URL domain0.login.com

Session Log ☐ Enable ☒ Disable

After complete set of login URL go to the “**Facebook** Site URL” function in web page. Copy and paste the login URL from the system display into the “Site URL” page on the Facebook website.

Step.7 Click Advanced function to enable the “**Native or desktop app?**” and “**Is App Secret embedded in the client?**”



Settings

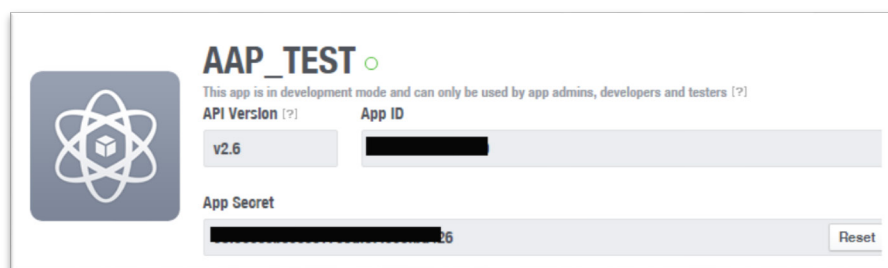
- Basic
- Advanced**
- Roles
- Alerts


Basic | **Advanced**

☒ **Native or desktop app?**
Enable if your app is a native or desktop app

☒ **Is App Seoret embedded In the olient?**
This restricts the app secret usage to methods allowed by a client token [?]

Step.8 After completing the “**Facebook** Site URL” setup. Administrators must copy and paste their App ID and App secret into the OAuth 2.0 Setup page in our software UI.



AAP_TEST 

This app is in development mode and can only be used by app admins, developers and testers [?]

API Version [?] **App ID**

v2.6 [Redacted]

App Secret

[Redacted] 6 **Reset**



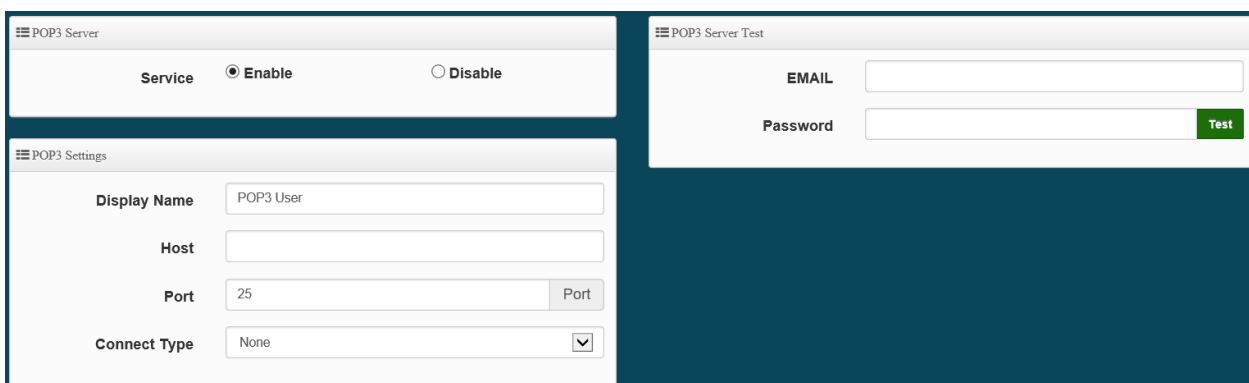
The OAuth 2.0 Setup form is titled "OAuth 2.0 Setup" and has an "Advanced" button in the top right corner. It contains two input fields: "Client ID" with a value ending in "9" and "Client Secret" with a value ending in "26".



Client ID and Client Secret setup by third parties such as Facebook and Google are subject to change. The instructions above follow the 2016 setup procedure. Any future changes to the Facebook/Google process may lead to our instructions becoming invalid.

3.4.4 POP3 Server

The purpose of this integrated function is to allow clients to link a POP3 server for receiving emails from a remote server.

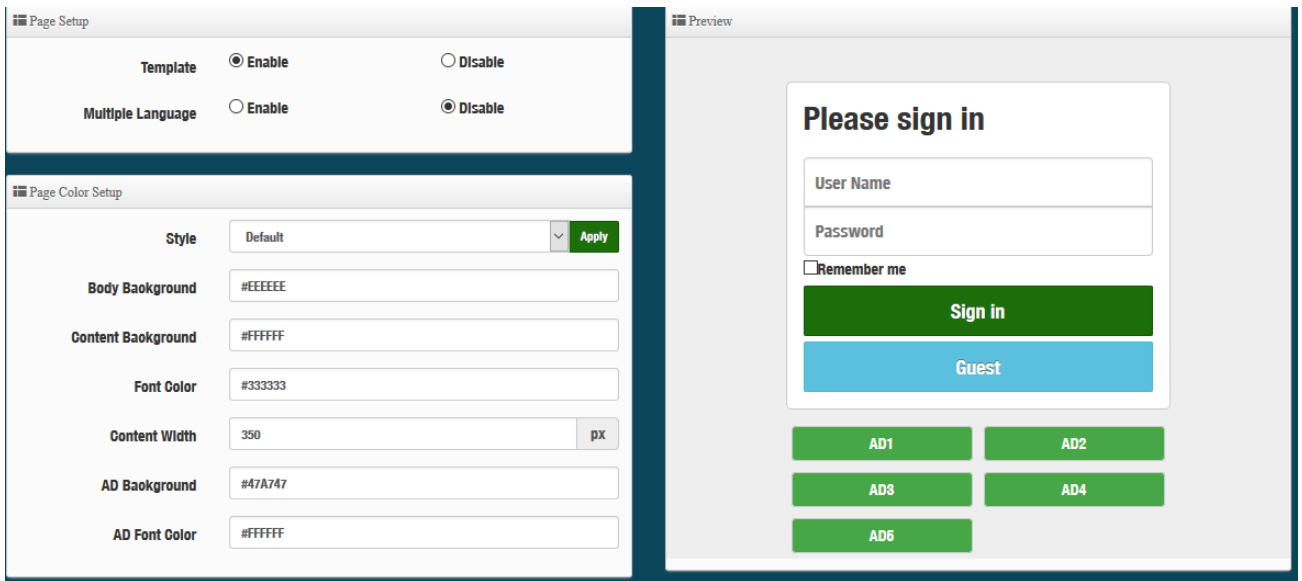


The image shows two side-by-side forms. The left form is titled "POP3 Server" and has a "Service" section with "Enable" (selected) and "Disable" radio buttons. Below it is the "POP3 Settings" section with fields for "Display Name" (POP3 User), "Host", "Port" (25), and "Connect Type" (None). The right form is titled "POP3 Server Test" and has fields for "EMAIL" and "Password", with a "Test" button.

- **POP3 Server** : Click "Enable" or "Disable" to activate this function
- **Display Name** : Set the "Display Name" based on the appropriate POP3 user or client
- **Host** : Define the desired Host server name
- **Port** : Input the proper port number for the corresponding server
- **Connect Type** : Select the Connect type with options of "STARTTLS", "SSL/TTL", or "None"
- **POP3 Server Test** : Use this tool to test if the POP3 server is operating correctly with your selected email

3.4.5 Customize Page

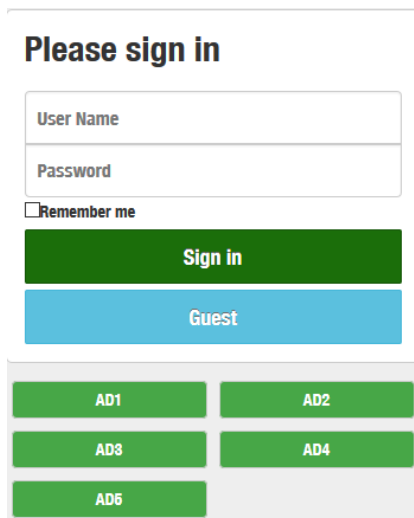
This function is to customize the user Login Page. This supports Multiple Language and allows comprehensive customization through HTML editing.



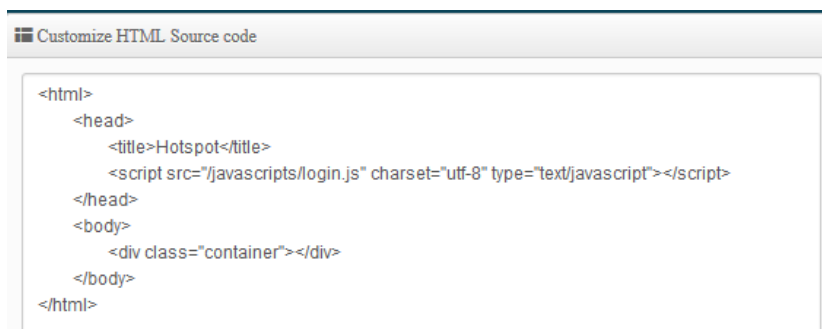
Page Setup

- **Template** : Administrator can select Enable or disable.

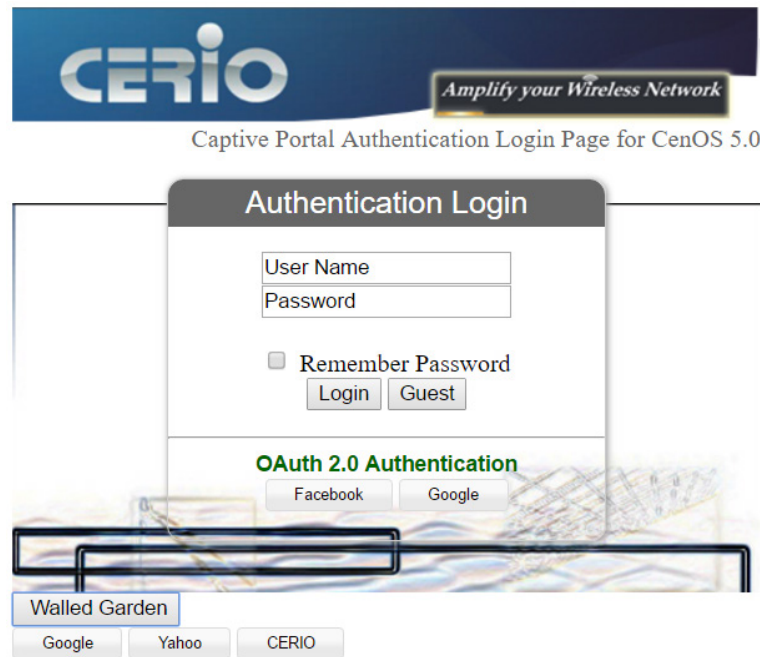
- Select enable to active default Login Page



- Select disable to active HTML Source code window for customization



Sample: See sample login page below that is customized by html coding (*sample login page html code templates are available on Cerio website*)



The following function uses the enabled Template

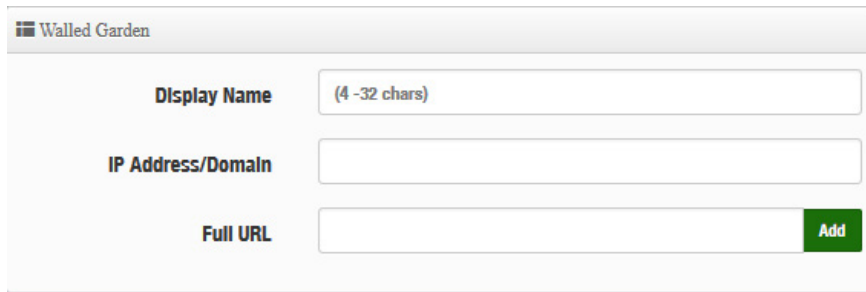
- **Multiple Language** : Administrator can select enable or disable multiple language for login page. Administrator must to Language function create new language.
- **Page Color Setup** : Administrator can change the login page color.

3.4.6 Language

Administrator can create other language for login page.

3.4.7 Walled Garden

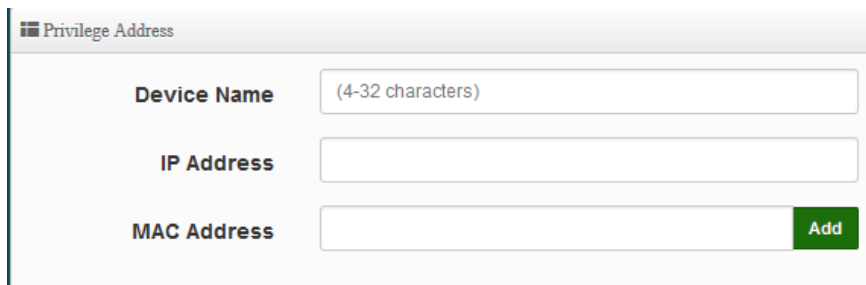
This function provides certain free services or advertisement web pages for users to access the websites listed before login and authentication. User without the network access right can still have a chance to experience the actual network service free of charge in Walled Garden URL list.



- **Display Name:** Set name of Website.
- **IP Address/Domain:** Set IP or Domain of the Open the website.
- **Full URL:** Set full website name.

3.4.8 Privilege Address

This function provides local device can access Internet without authentication. If there are some workstations belonging NGS Access Point that need to access to network without authentication, enter the IP or MAC address of these workstations in this list.



- **Device Name:** Enter Device or Users Name.
- **IP Address:** Enter used IP Address of Device or Users PC.
- **MAC Address:** Enter MAC Address of Device or Users PC.

3.4.9 Profile

Administrator can backup current authentication configuration and login page for HTML Source code. But also can recover.

The screenshot shows two sections of the web interface. The top section, titled 'VLAN Profile', contains two rows. The first row has 'Download Profile Setting' and a green 'Download' button. The second row has 'Upload Profile Setting', a 'Choose File' button, a text field showing 'No file chosen', and a green 'Upload' button. The bottom section, titled 'VLAN Customize Page', also contains two rows. The first row has 'Download Customize Page' and a green 'Download' button. The second row has 'Upload Customize Page', a 'Choose File' button, a text field showing 'No file chosen', and a green 'Upload' button.

Click “**Save**” button to save your changes. Then click **Reboot** button to activate your changes.

3.5 High Availability

When Gateway systems downtime working, the all network will can't normal work. If administrator set the high availability feature will be able to reduce the accidental interruption of the network and prevent against data loss.

CERIO **DR-4000** support system backup of the high availability function can mirror backup to many **DR-4000**.

Please click “**System**” → “**High Availability**” to set the function.

The image shows two parts of the web interface. On the left is a dark sidebar menu with options: 'Mode Setup', 'WAN Setup', 'WAN Traffic Setup', 'VLAN Setup', 'Authentication', and 'High Availability' (which is highlighted with a red box). On the right is the 'High Availability Setup' configuration page. At the top, under 'Service', there are radio buttons for 'Enable' (selected) and 'Disable'. Below this, under 'High Availability Setup', there are radio buttons for 'State' with 'Master' (selected) and 'Backup'. There are three input fields: 'Virtual Router ID' with the value '51', 'Priority' with the value '100', and 'Advert Interval' with the value '1' and a 'Seconds' label.

- **Service:** Administrator can select Enable or Disable the HA function.

High Availability Setup

- **State:** Administrator can set HA type of the Master or Backup.
- **Virtual Router ID:** Administrator must set same virtual router ID in all the high availability devices
- **Priority:** Administrator can set the priority level.
- **Advert Interval:** After how many sec to the recovery.

Virtual IP Setup: Administrator can set HA function in different VLAN.

Virtual IP Setup			
VLAN	Service	Virtual IP Address	Edit
0	<input type="checkbox"/>		<input type="button" value="Edit"/>
1	<input type="checkbox"/>		<input type="button" value="Edit"/>
2	<input type="checkbox"/>		<input type="button" value="Edit"/>
3	<input type="checkbox"/>		<input type="button" value="Edit"/>
4	<input type="checkbox"/>		<input type="button" value="Edit"/>
5	<input type="checkbox"/>		<input type="button" value="Edit"/>
6	<input type="checkbox"/>		<input type="button" value="Edit"/>
7	<input type="checkbox"/>		<input type="button" value="Edit"/>

Service

☐ Enable
 ☒ Disable

Virtual IP Settings

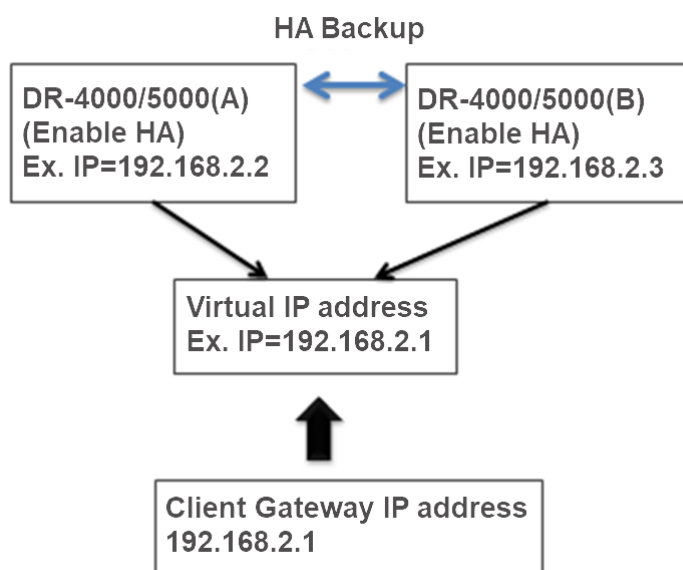
Virtual IP

Authentication Type

☐ PASS
 ☐ AH

Password

- **Virtual IP:** Administrator must set a Virtual IP address for HA device.
(The following concepts)



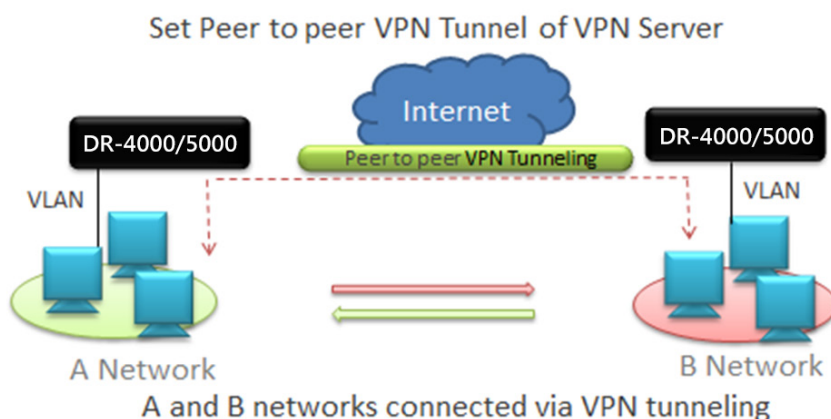
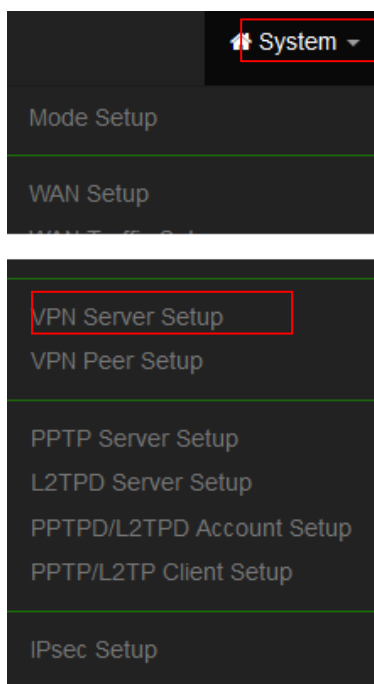
- **Authentication Type:** Administrator can select PASS or AH type for HA security.
- **Password:** Administrator can set password for the HA security.

3.6 VPN Server Setup



This VPN function support three protocol are VPN Server 、PPTP/L2TP and IPsec, the VPN tunnel of these three types only select one VPN protocol to used it.

Please click “System”→“VPN Server Setup” create VPN function.



VPN Service

Mode ☐ Enable ☒ Disable

VPN Service

➤ **Mode:** Administrator can select Enable or Disable the VPA function.

VPN Server

Mode ☒ Enable ☐ Disable

VPN Settings

VPN Hostname

Bridge Mode ☒ Enable ☐ Disable

DHCP filter ☒ Enable ☐ Disable

Bridge VLAN

VPN IP Address

VPN Netmask

VPN Port

Encryption

VPN Public Key

-----BEGIN RSA PUBLIC KEY-----
MIIBBgKCAQEAXYxglrEaVRZxOkW3Yk6pt0A1rnjpayo0B896+JAbmpSJtGASqwx
/Pv72kIoL0t0GjwqaECWDFwnjrU9g9M/nKCvY9c5HNnMJMSgQ3yga/REI4TGz40
bCjnMhmkWT7/ZqbOfNHj/KmzgatAS+YTOR18prIDhI07KsQx0g3d9W3Md58mTbs
XCkhuCbtqahnxL05v1eEmXLOE6jTgBZ69Aiksk0SU43E6CImKhG8GVswcSladpBk
7LGRRBk0ITWgkxHNayQZKsr3dzyzxdbKpC9IOZt1QRJBD4pVlltXbGAa3TKOZ1
supCAbKOxskW47UBshWR9rWgs15utA0XnwlDAQAB
-----END RSA PUBLIC KEY-----

Generate Public Key

Download Public Key

VPN Settings

- **VPN Hostname:** Administrator can set a VPN host name. Each VPN host name can't be the same and can't have special symbols.
- **Bridge Mode:** Administrator can select bridge mode by VLAN or Manual.
- **DHCP filter:** You can choose to enable or disable it. When it is enabled, it can prevent the DHCP server IPs of the physical area network at both ends from sending IPs out of bounds. (You only need to enable this function unilaterally. If the DHCP filter is turned on at both ends, the network logic will be incorrect and the VPN cannot be successfully connected)
- **Bridge VLAN:** If bridge mode select VLAN, administrator can select set VLAN 0~7 for VPN bridge.
- **VPN IP Address/Netmask:** If bridge mode select manual, administrator must set an IP address/netmask for the VPN link and must set routing of LAN.



1. If administrator choose use bridge mode then VPN both sides beneath need use same class network.
2. If administrator choose use manual set IP address then must set IP routing of LAN

- **VPN Port:** Administrator can set Port for VPN.
- **Encryption:** Select VPN security of encryption type.

VPN Public Key

VPN Public Key

-----BEGIN RSA PUBLIC KEY-----

MIIBCgKCAQEAAP+C8pLMuhpJAvosinha0xPMgSbpOLSPHkLR1VNT65N6hqMvGcjH
166MrHJDAXMEaTp0Q0geh5Zr2MRAQUYErICrXwMnS4wqDqsjYtnLsGPMLSaRN+W
PVUaJBcZKXP16vaYPI0wN4VYLEAto/op7G08m2a0NZjIh4j0tEJorua/k3jSUYa2
H80qQF/vhZ16XVYONueB019at1b5cMleQpuMLoqjrZ7kLto/447o+4UxMYu2m05W
6+PPRQa+Yo5ZkfwcmREzBR+PofKzPLJGWze3/IM9h++AoLXmhWlvAU2Y3bbg/G3n
/6QDfu7UP304QFj03eJNdsN6VBshM9+TtQIDAQAB

-----END RSA PUBLIC KEY-----

Generate Publio Key

Gen Key

Download Publio Key

Download

- **Generate Public Key:** Administrator can click the button to regenerate the VPN public key.
- **Download Public Key:** Administrator can click the button to download the VPN public key.

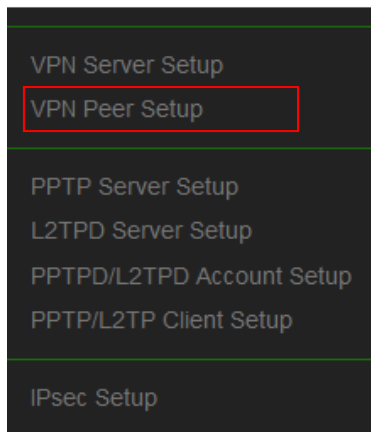
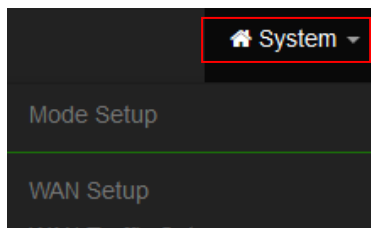
3.7 VPN Peer Setup



When administrator set 3.6 VPN server is complete, this page must setup a real IP address and upload VPN key of the other end.

Administrator can create new VPN connection for the VPN Peer.

Please click “**System**” → “**VPN Peer Setup**”



VPN Peer List						Create New Peer
#	Mode	Hostname	Description	WAN IP	Action	
-	-	-	-	-	-	

Create New Peer: Administrator can click the button to create a VPN bridge(peer to peer).

Up to 20 groups of VPN Peer settings can be created.

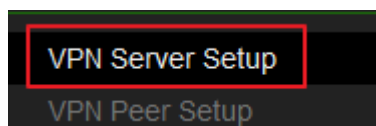
Client Setting	
Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HostName	<input type="text"/>
Real IP/Domain	<input type="text"/>
VPN Port	<input type="text" value="656"/>
Description	<input type="text"/>

- **Mode:** Administrator can select Enable or Disable the service.
- **HostName:** Administrator can set VPN host name in this field.
- **Real IP/Domain:** Administrator can set remote real IP address or Domain name in this field.
- **VPN Port:** Administrator can set connection Port for VPN.
- **Description:** Enter the description for the VPN Peer. (This is optional fill in and will not affect VPN connection settings)

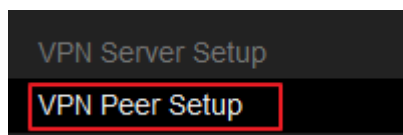
Basic instructions for setting the program

In the two end points A and B for example

1. Set the VPN server on the A side, and download and store the VPN Public Key, the A Public Key upload it to the B endpoint for authentication. The same is true for the B endpoint setting. (Two-end exchange public key)



2. Establish remote VPN Server information and upload the remote Public Key to this location.



- After completion, administrator can use ping command go to ping remote network IP address. If A ping to B side can get respond indicates that the VPN tunnel has been successfully established.

```
Connection-specific DNS Suffix . : 
Description . . . . . : Realtek Gaming USB 2.5GbE Family Controller
Physical Address. . . . . : 00-E0-4C-68-00-B0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::6dbb:e9be:1a09:9973%10(Preferred)
IPv4 Address. . . . . : 192.168.101.63(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

A Side


```
C:\Users\jacky>ping 192.168.2.1 -t

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=3ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64
Reply from 192.168.2.1: bytes=32 time=16ms TTL=64
```

B Side

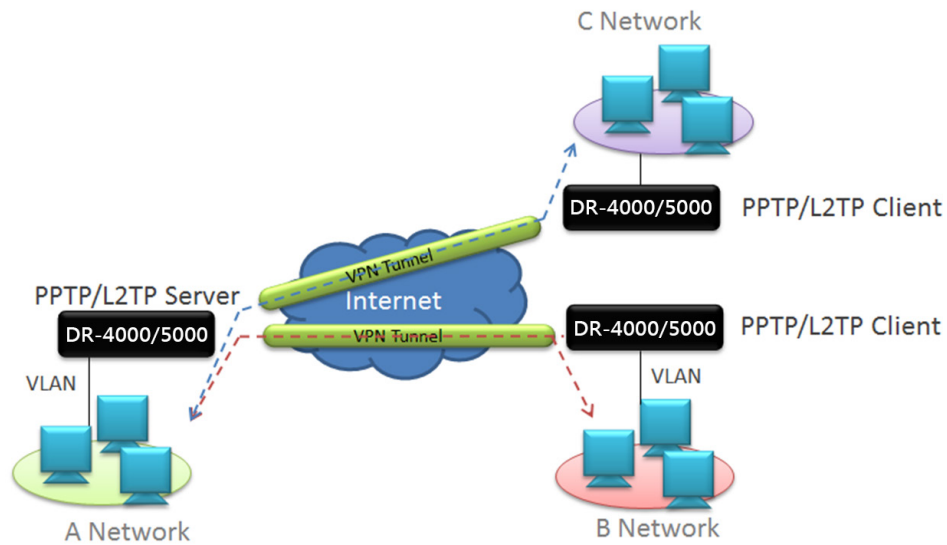
- Special attention to the fact that the respective Client settings of the final VPN server and the VPN Peer settings of both parties must be enabled for the VPN Peer connection to be successful.
- Kindly remind, please set up correctly and enable the DHCP filtering function. When using DHCP Server to allocate IP, it can be enabled according to the environment to prevent the physical area networks at both ends from crossing the boundary and allocating IPs to each other, causing the IP obtained not to be the real IP allocation. You will then be unable to access the Internet normally. You must choose to enable filtering on either side to prevent non-local DHCP servers from assigning IPs and thus avoid cross-border assignments. Please pay special attention to this part and do not enable this feature on both ends. If DHCP filtering is enabled on both ends, a network logic error will occur, causing the VPN connection to fail.

3.8 PPTP Server Setup

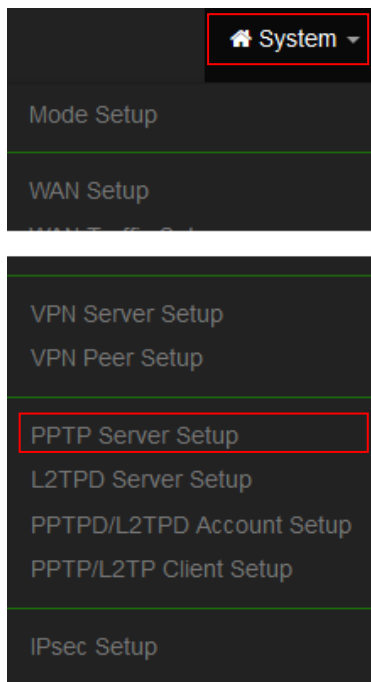


This VPN function support three protocol are VPN Server 、PPTP/L2TP and IPsec, the VPN tunnel of these three types only select one VPN protocol to used it.

Use the PPTP protocol to build a VPN tunnel; administrator can setup PPTP server of the VPN tunnel in the function.



Please click “System” → “PPTP Server Setup”



PPTP Server Settings	
Connections	<input type="text" value="10"/>
Local IP Address	<input type="text"/>
Remote Start IP Address	<input type="text"/>
Remote End IP Address	<input type="text"/>
MPPE40	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MPPE128	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

- **Connections:** Administrator can set connected VPN client Qty.
- **Local IP Address:** Set virtual IP address for VPN server.



Notice

This IP address is set as a VPN-specific virtual IP address tunnel, the IP address can't set same subnet of the WAN and LAN (network).

- **Remote Start/ End IP Address:** Set start to end IP address for dynamic configuration, can give VPN client automatically obtain a virtual IP address.
- **MPPE40/128:** Administrator can choose use VPN security for 40 or 128 bit.

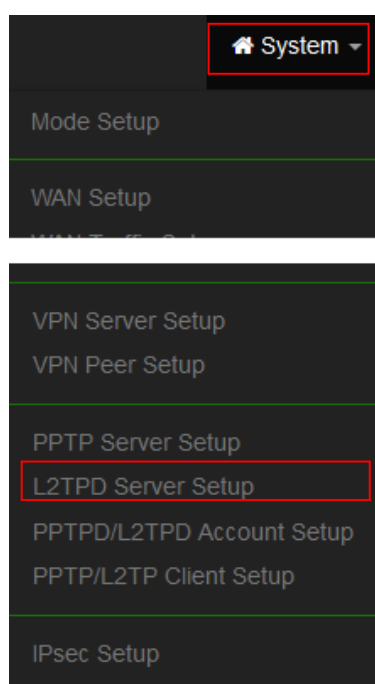
3.9 L2TP Server Setup



This VPN function support three protocol are VPN Server 、PPTP/L2TP and IPsec, the VPN tunnel of these three types only select one VPN protocol to used it.

Same as PPTP, L2TP protocol to build a VPN tunnel; administrator can setup L2TP server of the VPN tunnel in the function.

Please click “System” → “P2TP Server Setup”



- **Local IP Address:** Set virtual IP address for VPN server.



This IP address is set as a VPN-specific virtual IP address tunnel, the IP address can't set same subnet of the WAN and LAN (network).

- **Remote Start/ End IP Address:** Set start to end IP address for dynamic configuration, can give VPN client automatically obtain a virtual IP address.

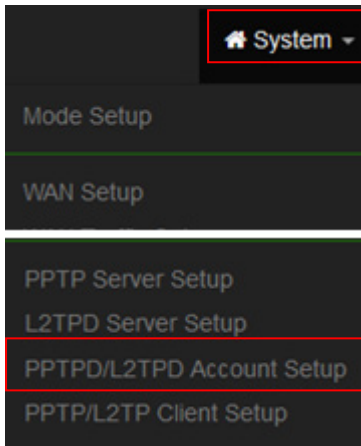
- **Mode:** Administrator can choose Enable or disable this function.
- **Pre-shared Key:** Set a security key for Pre-shared Key

- **Client IP:** Set a IP address of client.
- **WAN ID:** Select a access passage.

3.10 PPTP/L2TP Account Setup

Create PPTP / L2TP authentication account with maximum of 60 VPN accounts.

Please click "System" → "PPTP/L2TP Account Setup"



Account List Create Account				
#	Username	PPTP Support	L2TP Support	Action
-	-	-	-	-

- **Create Account:** Administrator can click the button to create authentication account of client.

Account Setup

User Name

Password

PPTP Support

☒ Enable
 ☐ Disable

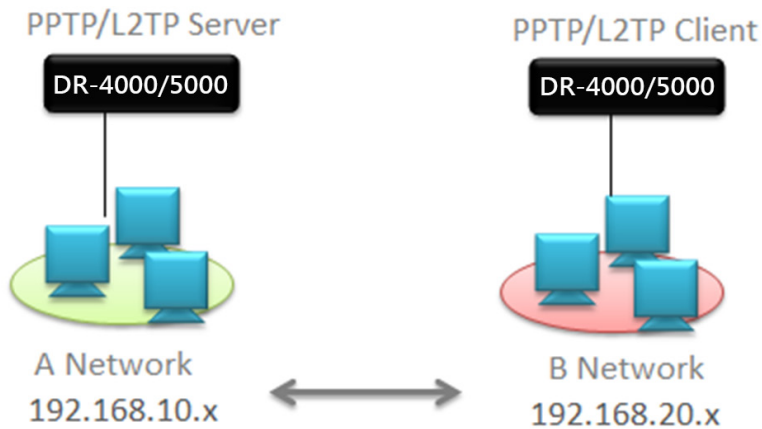
L2TP Support

☒ Enable
 ☐ Disable

- **User Name/Password:** Set authentication account of name/password.
- **PPTP/L2TP Support:** Set account used to PPTP or L2TP protocol.

Routing Rule:

Set routing of both network, As figure below, the local end is the Server endpoint and the remote end is the Client endpoint.



Example :

Local Subnet: 192.168.10.0/24

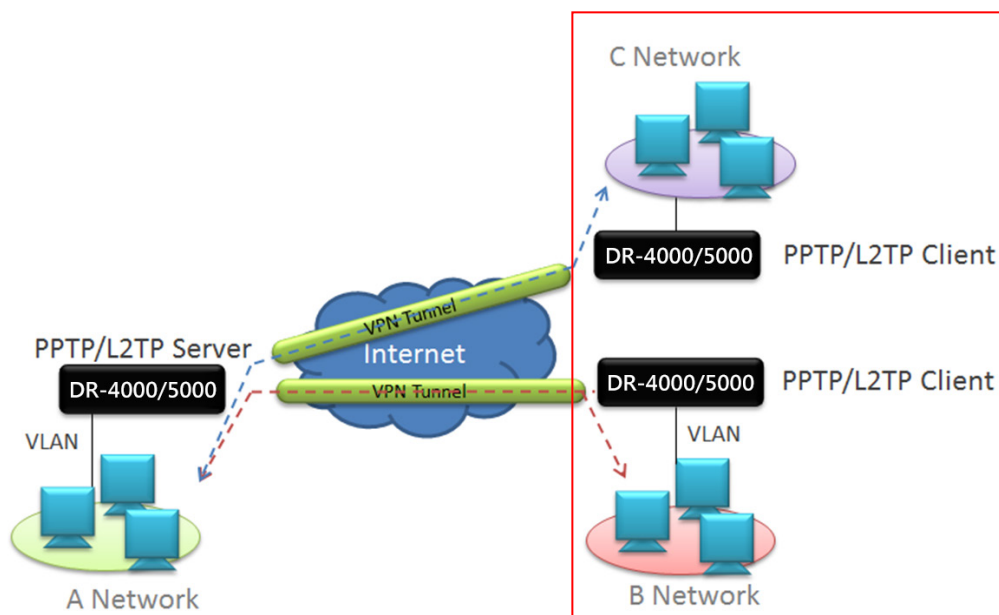
Remote Subnet : 192.168.20.0/24

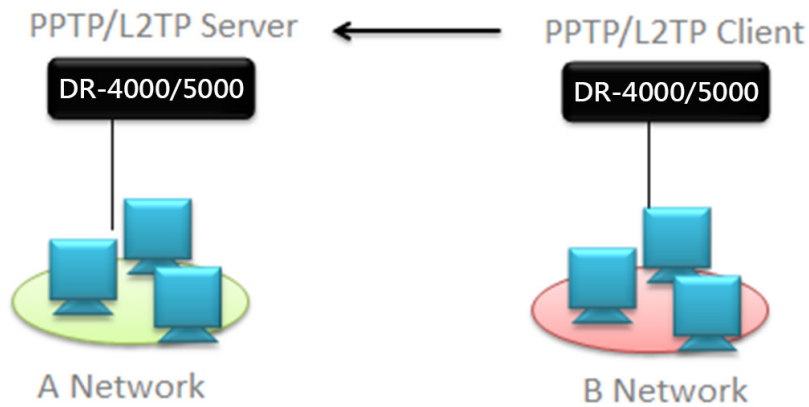
Routing Rule	
Local Subnet	<input type="text" value="0.0.0.0/0"/>
Remote Subnet	<input type="text" value="0.0.0.0/0"/> Add

- **Local Subnet:** Set network subnet of local.
- **Remote Subnet:** Set network subnet of Remote.

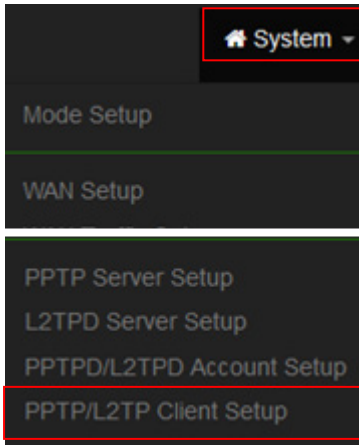
3.11 PPTP/L2TP Client Setup

If remote have PPTP/L2TP VPN server, administrator can used PPTP/L2TP client function connection to remote VPN server.





Please click "System" → "PPTP/L2TP Client setup"



Client List Create Client				
#	Active	Mode	Server IP Address	Action
-	-	-	-	-

Please click the Create Client button to set client conditions. **Up to 60 client of PPTP/L2TP Client can be created.**

PPTP/L2TP Client Setup

Active ☒ Enable ☐ Disable

PPTP/L2TP Client Settings

Mode ☒ PPTP ☐ L2TP

Server IP Address

User Name

Password

- **Mode:** Administrator can select use PPTP or L2TP protocol connection to remote VPN server. If VPN server used PPTP Protocol then please choose PPTP.
- **Server IP Address:** Administrator must set remote VPN server used real IP address.
- **User Name / Password:** Set VPN authentication account and password (Please Refer to 3.10 Account Setup)

If you use PPTP protocol, please select the encryption type, as shown below

The screenshot shows the 'PPTP Setup' window. It contains two rows of settings. The first row is for 'MPPE40' with radio buttons for 'Enable' and 'Disable', where 'Disable' is selected. The second row is for 'MPPE128' with radio buttons for 'Enable' and 'Disable', where 'Disable' is also selected.

- **MPPE40/128:** Enable or disable security options based on using remote VPN servers.

If you use L2TP protocol, please enter the Pre-share Key and confirm which WAN to use as the external VPN channel, as shown below

The screenshot shows the 'L2TP Setup' window. It includes an 'Over IPsec' section with 'Enable' and 'Disable' radio buttons, where 'Disable' is selected. Below this is a 'Pre-shared Key' text input field. At the bottom, there is a 'WAN' dropdown menu currently showing 'WAN 0'.

- **Over IPsec :** Choose to enable or disable the Over IPsec VPN protocol.
- **Pre-shared Key :** You can enter a set of password keys
- **WAN :** elect L2TP VPN through the WAN related user interface.

3.12 IPSec Setup

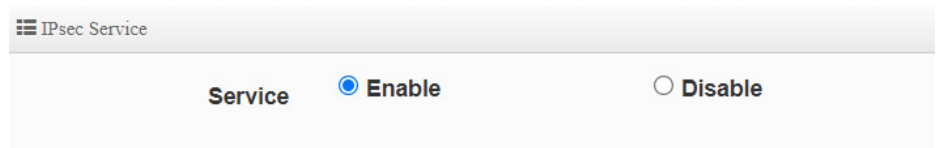
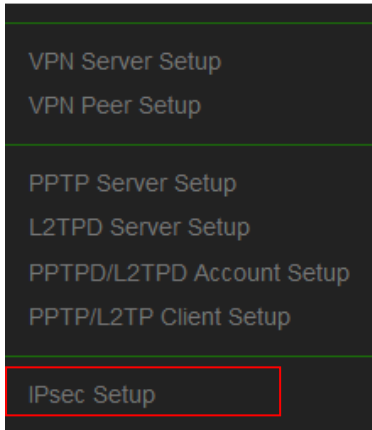
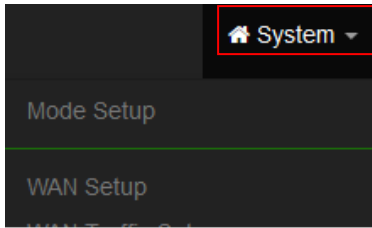


Notice

This VPN function support three protocol are VPN Server 、PPTP/L2TP and IPsec, the VPN tunnel of these three types only select one VPN protocol to used it.

Administrator can create new VPN connection for the IPsec.

Please Click “System” ➔ “IPSec Setup”



- **Service:** You can choose to turn on or off this function service

IPsec Settings

Mode	LAN-to-LAN
WAN	Auto
Local ID Type	<input type="radio"/> IP Address <input checked="" type="radio"/> FQDN
Local ID	
Local Subnets	0.0.0.0/0
Local Nexthop	
Remote ID Type	<input type="radio"/> IP Address <input checked="" type="radio"/> FQDN
Remote ID	
Remote Subnets	0.0.0.0/0
Remote Nexthop	
Remote Host	
Pre-shared Key	

- **Mode:** Administrator can be according to different needs select use LAN to LAN or Client to LAN.
- **WAN:** Administrator can choose use specific WAN Port connection.
- **Local ID Type:** Administrator can select use IP address or FQDN for Local IP Type.
- **Local Subnet:** Administrator must set Local Subnet for the VPN "LAN to LAN".
- **Local Nexthop:** Administrator can add a VPN Next hop address for Local.

- **Remote ID Type:** Administrator can select use IP address or FQDN for Remote IP Type.
- **Remote Subnet:** Administrator must set remote Subnet for the VPN "LAN to LAN".
- **Remote Nexthop:** Administrator can add a VPN Next hop address for Remote
- **Pre-shared Key:** Enter Pre-shared Key for VLAN.

DPD	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
DPD Delay	<input type="text" value="30"/>	
DPD Timeout	<input type="text" value="120"/>	

- **DPD:** DPD (Dead peer detection) is a method that network devices use to verify the current existence and availability of other peer devices. The system can waiting for DPD acknowledgements (R-U-THERE-ACK messages) from the peer. **The DPD function must be enabled on both ends of the VPN host. The system on one side can wait for a delay time packet access from the remote stationary device and respond with the packet to ensure that the host knows that both parties are active. normal status. When no response message is received from the host after the set Timeout time, the host will use the DPD mechanism to automatically start the VPN reconnection process. This feature is enabled by default. Administrators are recommended to use this feature. This is to avoid the possibility of the VPN not being able to automatically reconnect after being disconnected.**
- **DPD Delay:** Administrator can set delay time (seconds) for DPD. **(The default value is 30 seconds for packet access to the opposite VPN host.)**
- **DPD Timeout:** Administrator can set timeout of times for DPD. **(The default value is 120 seconds. When the peer host does not respond normally according to the access period set by Delay, the DPD automatic VPN connection process is automatically started.)**

IKE Policy:

This function is verification the VPN identity. The VPN to establish a connection with each other must be certified to establish a trust relationship between each other, this function supports IKE Phase 1/2.

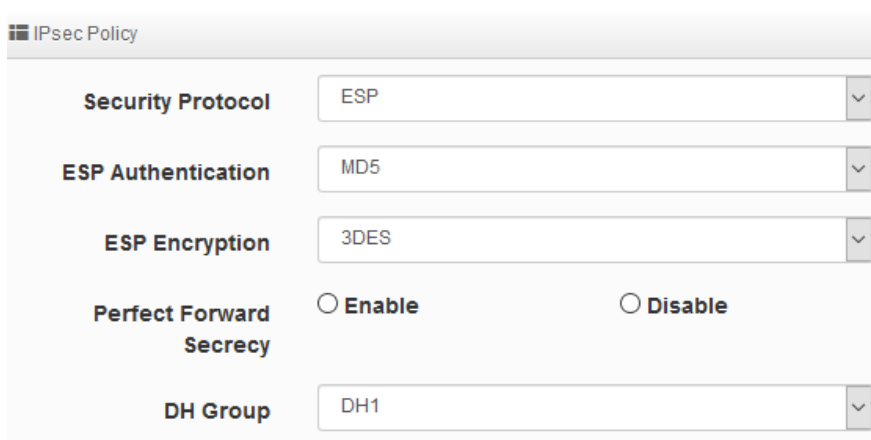
IKE Policy	
IKE Mode	<input type="radio"/> Main <input type="radio"/> Aggressive
IKE Authentication	<input type="text" value="MD5"/>
Encryption	<input type="text" value="3DES"/>
DH Group	<input type="text" value="DH1"/>

- **IKE Mode:** Administrator can select Main or Aggressive of the IKE. If device uses Router

mode then suggest use Main mode is high security.

- **IKE Authentication:** Administrator can select authentication method for MD5, SHA1, SHA2_256.
- **Encryption:** Set encryption method for IKE. Administrator can select use 3DES and AES128/192/256.
- **DH Group:** Diffie-Hellman is key exchange. Allows two devices to establish a shared secret over an unsecure network. In terms of VPN it is used in the in IKE or Phase1 part of setting up the VPN tunnel. This DH Group support DH1/2/5/14.

IPSec Policy:



The image shows a screenshot of the 'IPsec Policy' configuration window. It contains several settings:

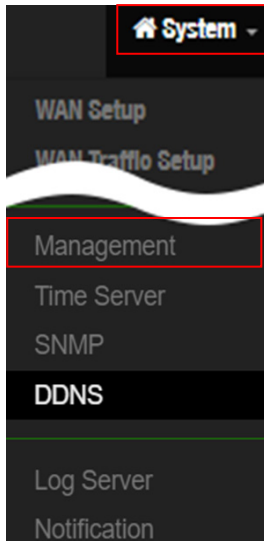
- Security Protocol:** A dropdown menu with 'ESP' selected.
- ESP Authentication:** A dropdown menu with 'MD5' selected.
- ESP Encryption:** A dropdown menu with '3DES' selected.
- Perfect Forward Secrecy:** Two radio buttons, 'Enable' and 'Disable', with 'Enable' selected.
- DH Group:** A dropdown menu with 'DH1' selected.

- **Security Protocol:** The IPSec security use ESP protocol.
- **ESP Authentication:** Administrator can select authentication method for MD5, SHA1, SHA2_256.
- **ESP Encryption:** Set encryption method for ESP. Administrator can select use 3DES and AES128/192/256.
- **Perfect Forward Secrecy:** Administrator can select enable or disable for DH Group.
- **DH Group:** Diffie-Hellman is a key exchange and supports DH1/2/5/14. This function mainly allows two parties to create keys through an unsecured channel without requiring any information from the other party.

3.13 Management

Administrators can specify geographical location of the system via instructions in this page and modify system login password and select use system login protocol by 80, 443, 23, 22 Port. The management page support syslog server function and system auto reboot function.

Please Click **"System" → "Management"**



System Language

Language: English

System Information

System Name: DR-4000

Description: Multi WAN with Gigabit VPN Gateway

Location:

Root Password

New Root Password:

Check Root Password:

Ping Watchdog

Ping Watchdog: ☐ IP Address

Jumbo Frame

Jumbo Frame: Enable

1Gbe port jumbo frames are 9K bytes

Login Methods

HTTP	<input checked="" type="checkbox"/>	80	Port
HTTPS	<input checked="" type="checkbox"/>	443	Port
Telnet	<input checked="" type="checkbox"/>	23	Port
SSH	<input type="checkbox"/>	22	Port

Host Key Footprint: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ= Generate Key

Access WAN0: ☐ Enable ☒ Disable

Access WAN1: ☐ Enable ☒ Disable

Access WAN2: ☐ Enable ☒ Disable

System Log Setup

Remote Server: ☐

Port: 514 Port

Auto Reboot

Type: Disable

Wake On LAN

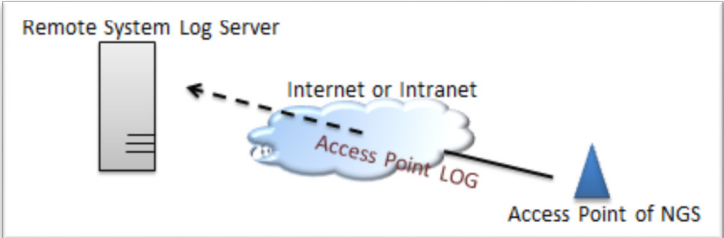
Type: Disable

- **Language:** Administrators can choose to change the language of the English or Chinese.
- **System Information:** Administrator can set the system name / Description and Location.
- **Root Password:** Administrator can change system login password.
- **System Log Setup:** Administrator can be backup system log or authentication log to remote server. Please enter IP address and port of remote syslog server.

System Log Setup

Remote Server ☒ 127.0.0.1

Port 514 Port



- **Remote Server:** Set the IP address of the remote system Log server .
- **Port:** Set the port number of the remote system Log server. The default Port is 514.

➤ **Ping Watchdog :** Ping Watchdog helps administrator to automatically reboot the system when its not working properly.

Ping Watchdog

Ping Watchdog ☒ IP Address

Interval 60 Seconds

Delay 100 Seconds

Times of faults 3 times

- **Ping Watchdog :** Set the IP address to be monitored for ping.
- **Interval :** Set the interval to ping the IP address.
- **Delay :** When ping fails, how long should you delay before ping again.
- **Times of faults :** When the above conditions are true multiple times, let the system reboot.

➤ **Jumbo Frame :** Can be enabled or disabled to determine whether all physical Ethernet ports use Gigabit 9K Jumbo Frame as the primary packet transmission format.

Jumbo Frame: Disable

1Gbe port jumbo frames are 9K bytes

➤ **Login Methods:** Administrator can set system login protocol of the http/https/telnet and ssh.

Protocol	Enabled	Port	Action
HTTP	<input checked="" type="checkbox"/>	8088	Port
HTTPS	<input type="checkbox"/>	443	Port
Telnet	<input checked="" type="checkbox"/>	8023	Port
SSH	<input type="checkbox"/>	22	Port

Host Key Footprint: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA **Generate Key**

- **HTTP Management** : Check this item will enable the WEB interface to enter the management interface. The default is port 80. (recommended port number between 1025 and 65535)
- **HTTPS Management** : Check this item will enable the WEB interface to enter the management interface. The default is port 443. (recommended port number between 1025 and 65535)
If this Web HTTPS secure communication transmission protocol function is enabled, and the web page authentication function is also enabled, the "Login URL Address" to be set as the [Authentication Web Captive portal login page] will also operate under the HTTPS transmission mechanism, ensuring the smooth operation of HTTPS. At the same time, it is also necessary to have an SSL certificate and import it before it can operate normally.
- **Telnet Management** : Check this item will enable Telnet to enter the management interface. The default is port 23. (recommended port number between 1025 and 65535)
- **SSH Management** : Check this item will allow SSH to enter the management interface. The default port is 22.
- **Host key Footprint** : Click to generate SSH certificate key.

- **Access WAN#:** If enable this WAN# then external (Internet) will can access management interface for **DR-4000**. The default is Disable. (This function can only be used in Router mode).
- **Auto Reboot:** The functions can Auto-reboot the system by Date/time management.

- **Daily :** Setting time to system reboot.

The screenshot shows the 'Auto Reboot' configuration page. The 'Type' dropdown is set to 'Daily'. The 'Hour' dropdown is set to '08' and the 'Minute' dropdown is set to '08'.

- **Weekly :** Setting frequency (ex. Weekly) and time of system reboot

The screenshot shows the 'Auto Reboot' configuration page. The 'Type' dropdown is set to 'Week'. The 'Weekly' dropdown is set to 'Sunday'. The 'Hour' dropdown is set to '08' and the 'Minute' dropdown is set to '08'.

- **Monthly :** Setting Every month, fixed date and time to system reboot

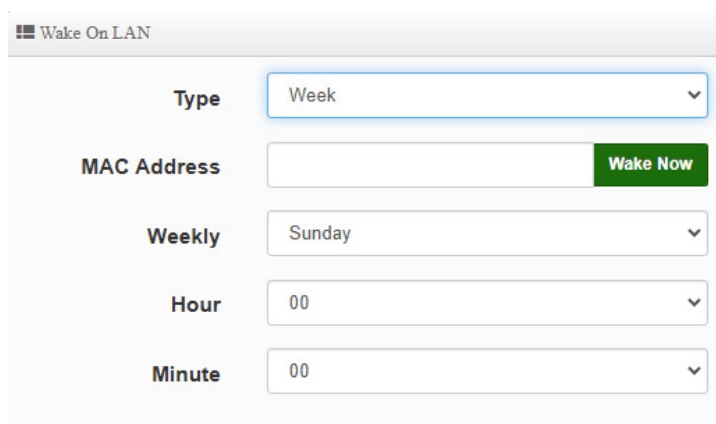
The screenshot shows the 'Auto Reboot' configuration page. The 'Type' dropdown is set to 'Month'. The 'Monthly' dropdown is set to '01'. The 'Hour' dropdown is set to '08' and the 'Minute' dropdown is set to '08'.

- **Wake On LAN:** This function can fix in the remote MAC address of network card to allow the system to wake up a remote network MAC address device immediately or periodically.
- **Daily :** Setting every day time for the system to wake up a device with a remote network MAC address.

The screenshot shows the 'Wake On LAN' configuration page. The 'Type' dropdown is set to 'Daily'. The 'MAC Address' field is empty, and there is a green 'Wake Now' button next to it. The 'Hour' dropdown is set to '00' and the 'Minute' dropdown is set to '00'.

- **Weekly :** Setting frequency (ex. Weekly) time for the system to wake up a device with a

remote network MAC address.



Wake On LAN

Type: Week

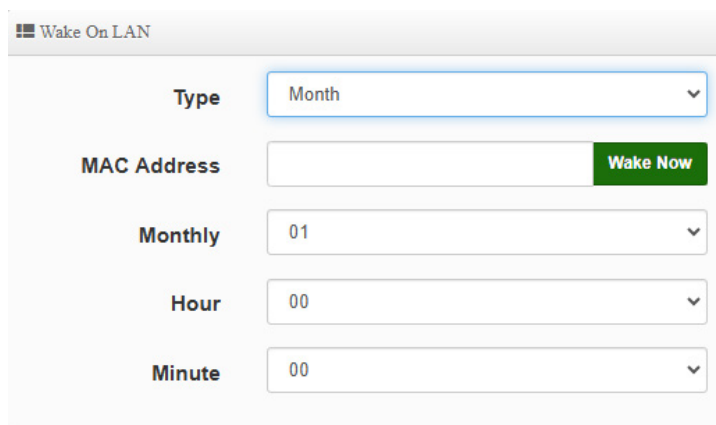
MAC Address: Wake Now

Weekly: Sunday

Hour: 00

Minute: 00

- **Monthly** : Setting Every month time for the system to wake up a device with a remote network MAC address.



Wake On LAN

Type: Month

MAC Address: Wake Now

Monthly: 01

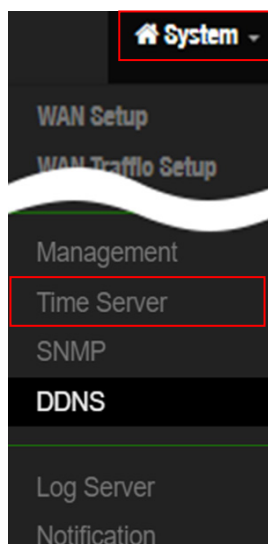
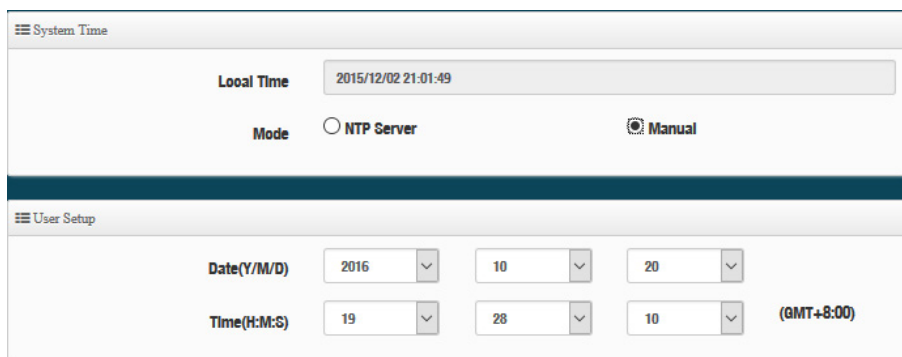
Hour: 00

Minute: 00

3.14 Time Server

Administrator can select manual or via a NTP server to modify system time for the right local time. If select update the system time for manual, when administrator reboot system the system time will reply default.

If select update the system time for the NTP Server, system must set gateway and DNS server, the system can be connected internet.

System Time

Local Time: 2015/12/02 21:01:49

Mode: ☐ NTP Server ☒ Manual

User Setup

Date(Y/M/D): 2016 10 20

Time(H:M:S): 19 28 10 (GMT+8:00)

NTP Server

Default NTP Server: time.stdtime.gov.tw

NTP Server: time.stdtime.gov.tw

Time Zone: (GMT+08:00) Beijing, Hong Kong, Singapore, Taipei

Daylight Saving Time: ☐ Enable ☒ Disable

- **Mode:** Administrator can select NTP Server or Manual.
- **NTP Server:** System can auto update the system time. Administrator needs setting as NTP Server.
For example, select the time server of "cerio.com.tw" on the Internet as the basis for NTP time calibration as follows.

NTP Server

Default NTP Server: cerio.com.tw

NTP Server: [Dropdown menu open showing options: Customize Time Server, time.google.com, time.windows.com, cerio.com.tw, time.nist.gov, time-nw.nist.gov, murgon.cs.mu.OZ.AU, ns2.pads.ufrj.br, nist1.symmetricom.com, time.stdtime.gov.tw, pool.ntp.org]

Time Zone: [Dropdown menu]

Daylight Saving Time: [Radio buttons]

- ✓ **Default NTP Server:** Administrator can select NTP Server.
- ✓ **NTP Server:** Administrator can setting as NTP Server.
- ✓ **Time Zone:** Administrator can select a desired time zone from the drop-down list.
- ✓ **Daylight saving Time:** Enable or disable Daylight saving.
- **Manual:** Administrator need to set the system time.

User Setup

Date(Y/M/D): 2015 9 9

Time(H:M:S): 17 49 15 (GMT+8:00)

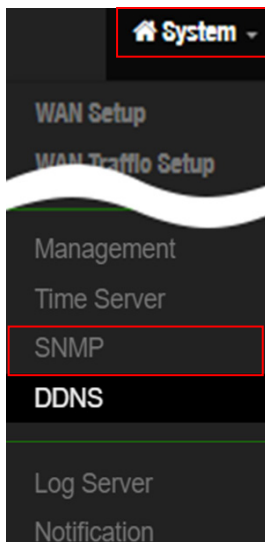


This product supports hardware battery power supply to RTC (Real Time Clock Module) IC real-time clock memory storage module design. When "Manual Update" is selected, if the time cannot be saved and it will always be invalid and return to the default time, then The machine board hardware battery must be checked and replaced.

3.15 SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP** and follow the below setting.



SNMP v2c function

- **Active:** Administrator can select Enable or Disable the service.
- **RO Community:** Set a community string to authorize read-only access.
- **RW Community:** Set a community string to authorize read/write access.

SNMP v3 function

- **Active:** Administrator can select Enable or Disable the service.
- **RO username:** Set a community string to authorize read-only access.
- **Ro password:** Set a password to authorize read-only access.
- **RW username:** Set a community string to authorize read/write access.
- **RW password:** Set a password to authorize read/write access.

SNMP Trap

Events such as cold start interface up & down, and association & disassociation will report to an assigned server.



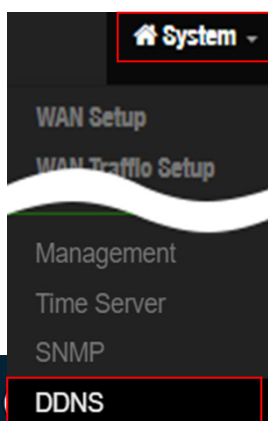
The image shows a web-based configuration interface for the SNMP Trap service. At the top, there is a title bar labeled 'SNMP Trap'. Below it, there are three radio buttons for 'Active': 'Enable' and 'Disable'. The 'Disable' option is selected. Below the radio buttons, there are five input fields labeled 'Community', 'IP 1', 'IP 2', 'IP 3', and 'IP 4'. Each input field is currently empty.

- **Active:** Administrator can select Enable or Disable the service.
- **Community:** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- **IP(1~4) :** Enter the IP addresses of the remote hosts to receive trap messages.

3.16 DDNS

Dynamic Domain Name Server, referred to as DDNS dynamic DNS technology. According to the Internet domain name establishment rules, domain names must follow a fixed IP address. However, the dynamic DNS system provides a fixed name server (Name server) for the dynamic domain, which allows external users to connect to the dynamic user's URL through real-time updates. **This system has built-in support for 2 service providers, namely dyndns and no-ip.**

Please click on **System -> DDNS** and follow the below setting.



Select and edit settings according to the corresponding WAN. Supports 3 sets of corresponding WAN IP settings..

☰ DDNS List

#	Active	Provider	WAN	Hostname	Edit
0	InActive	dyndns	Auto		Edit
1	InActive	dyndns	Auto		Edit
2	InActive	dyndns	Auto		Edit

☰ DDNS Setup

Active ☒ Enable ☐ Disable

Provider

WAN

Hostname

Username

Password

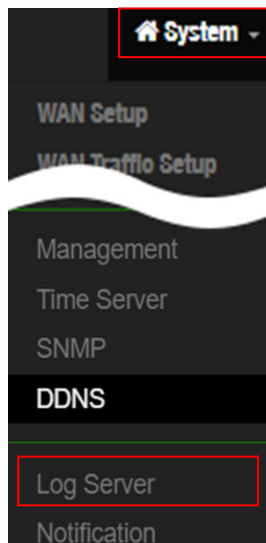
Interval Minute

- **Active:** Choose to enable or disable the function.
- **Provider:** Choose the Service provider , built-in support for 2 service providers, namely dyndns and no-ip.
- **WAN:** Select the port for external connection of this machine
- **Hostname:** Enter the host name
- **Username/Password:** Enter the account password applied by the DDNS service provider
- **Interval:** Enter the interval for the host to automatically provide the physical address to the DDNS service provider.

3.17 Log Server Setup

If devices used CERIO products and support syslog server function, the devices log can be transferred to this server and record devices log. Administrator can set storage space for the session/authentication and devices system log.

System can use e-mail send log Message to administrator.



A screenshot of the 'Log Server Setup' configuration page in the CERIO web interface. The page is divided into four sections, each with a title and a collapse icon (three horizontal lines):

- Radius Log Setup:** Contains a 'Radius Log Size' input field set to '256' and a 'MB' button.
- Session Log Setup:** Contains a 'Session Log Size' input field set to '256' and a 'MB' button, and a 'Reorder Mode' dropdown menu set to 'Cycle'.
- Authentication Log Setup:** Contains an 'Authentification Log Size' input field set to '256' and a 'MB' button, and a 'Reorder Mode' dropdown menu set to 'Cycle'.
- System Log Setup:** Contains a 'System Log Size' input field set to '256' and a 'MB' button, and a 'Reorder Mode' dropdown menu set to 'Cycle'.

- **Log Size:** Administrator can set storage space for RADIUS/session/authentication and system log.(max.512MB)
- **Recorder Mode:** The function can auto clear Log information or stop services.
 - **Cycle:** System will auto clear log by cycle.
 - **Retention Period:** System will auto clear log by Retention Period. Administrator can set days for retention period. (Max. 90 days)



When the log record file exceeds the set space size, the system will stop recording, so be sure to calculate the retention days and space size. For example, if the retention period is set to 7 days, but the storage space is full on the third day, the system will automatically stop recording at this time.

- **Stop Service:** If the system storage is full, the system will auto stop recording.

E-Mail Message setting

Administrator can set E-Mail messenger format and set **3.16 Notification Setup** function send e-mail to administrator.

E-Mail Message Format

Subject

%l happend %e in %t

%t, %h, %l, %e, %s, %p

Subject: Radius Log happend Full In 2016-11-21 16:26

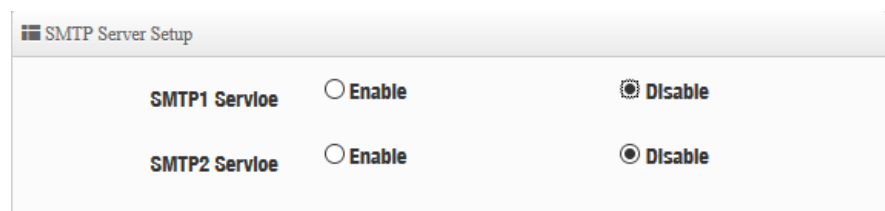
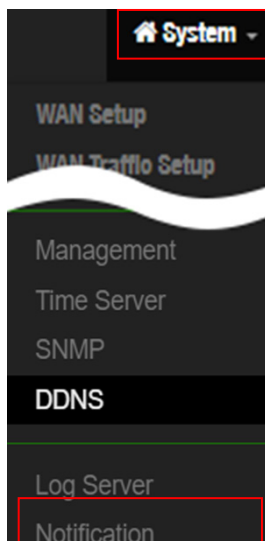
Message: 2016-11-21 16:26, DR-3000, Radius Log, Full, 236MB, 95%

Message Format	
Format	Description
%h	Hostname
%t	Time
%l	Log Type(Radius Log/Session Log/Authentication Log/System Log)
%s	File Size
%p	File Percentage
%e	Event Type(Full/ Stop Service/ Start Service)

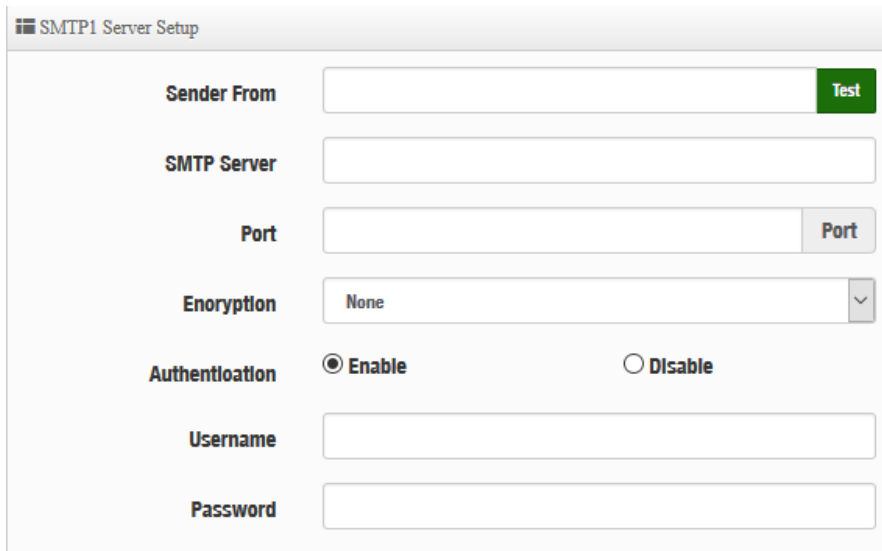
3.18 Notification Setup

Administrator can automatically send the notification of Radius Log, Session Log, Authentication Log and System Log of 2 particular E-mail addresses. The E-Mail notification setting support SMTP server test, once administrator completed setting up of SMTP, server will able to use the test tool to confirm SMTP is working properly.

Please click **“System”** → **“Notification,”** functions of Notification E-mail Setup will appear, and fill in the related information, and select the desired function, and then, click on **“Save”** to apply the settings.



- **SMTP1/2 Service:** Administrator can select Enable or Disable the SMTP functions. If administrator select enable the function will following explains how to configure the SMTP functions.



SMTP1 Server Setup

Sender From: Test

SMTP Server:

Port: Port

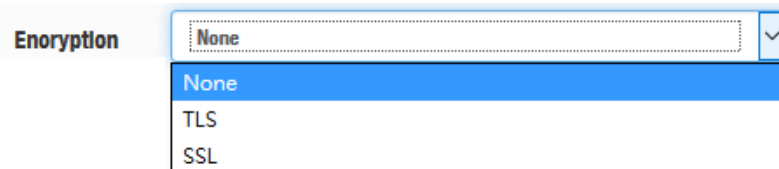
Encryption: None ▼

Authentication: ☒ Enable ☐ Disable

Username:

Password:

- **Sender From:** Administrator can set E-Mail address by from.
- **SMTP Server:** Administrator can set E-Mail SMTP server.
- **Port:** Administrator can set SMPT Server used Port.
- **Encryption:** Administrator can select use TLS or SSL encryption type for the SMPT Server.



Encryption

None

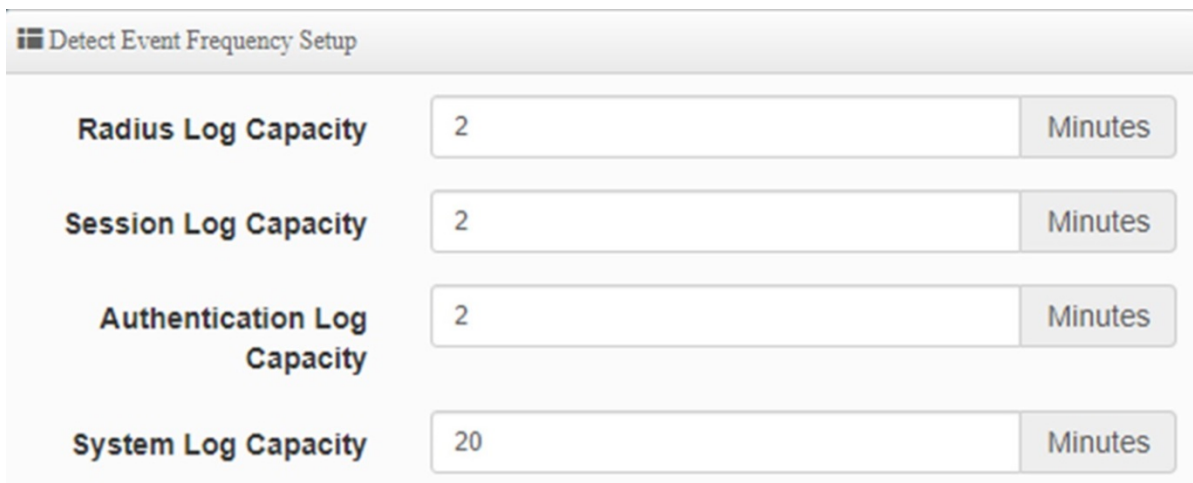
TLS

SSL

- **Authentication:** If SMTP Server must use authentication, Administrator can select enable the SMTP server authentication for E-Mail user account.

Notification Setup

Administrator can set frequency or time for the RADIUS, Session, Authentication and System Log Capacity, and send to administrator E-Mail. For example:



Detect Event Frequency Setup

Radius Log Capacity: Minutes

Session Log Capacity: Minutes

Authentication Log Capacity: Minutes

System Log Capacity: Minutes

Receiver E-Mail List

Administrator can click “Create Receiver E-Mail” button to add administrator E-mail address(es.)

Receiver E-Mail List						Create Receiver E-Mail
#	Receiver E-Mail	Radius	Authentication	Session	Syslog	Action
1	████████@cerio.com....	Off	Off	Off	On	Edit ▾
2	████████net.net	Off	On	Off	On	Edit ▾
3	████████@gmail.com	Off	Off	Off	On	Edit ▾
4	████████et.net	Off	Off	Off	On	Edit ▾
5	████████@gmail.com	Off	Off	Off	On	Edit ▾

- **Receiver E-Mail:** Administrator can set receiver e-mail addresses.
- **Edit:** Administrator can select the **Radius**, **Authentication**, **Session**, and **System Log**, to receiver Emails through **Edit** function.

Deleting the Notification

Administrator can delete the notifications setting of receiver E-mail set previously.

Create Receiver E-Mail	
Syslog	Action
On	Edit ▾
On	Delete ▾

4. Account

This function is a RADIUS server such as the Cerio APs to utilize the RADIUS server authentication of **DR-4000**, and its many authentication types. When Cerio APs enable authentication through external RADIUS server, administrators must first set the IP address of **DR-4000** in each managed access point to properly redirect authentication clients.

Cerio's **DR-4000** Account functions support Package, Pregenerated Tickets and remote LDAP(AD) authentication type.

4.1 RADIUS Server

The screenshot shows the 'Radius Server' configuration page. The sidebar on the left has a menu with 'Account' at the top, followed by 'Radius Server' (highlighted with a red box), 'Remote LDAP Setup', 'Package Setup', 'Create An Account', 'Search Account', and 'Pregenerated Tickets DB'. The main content area is titled 'Radius Server' and contains a 'Service' section with radio buttons for 'Enable' and 'Disable' (selected). Below this are three input fields: 'Authentication Port' with the value '1812', 'Accounting Port' with the value '1813', and 'Radius Secret' with a masked password '.....'.

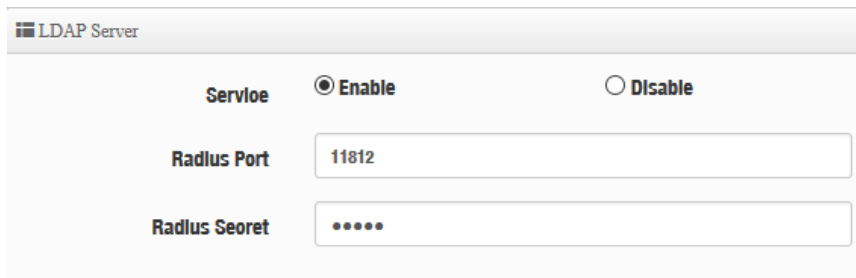
- **Service:** Administrator can select Enable or Disable the RADIUS Server.
- **Authentication Port:** Administrator can set authentication port for RADIUS Server, the default port is 1812.
- **Accounting Port:** Administrator can set accounting port for RADIUS Server, the default port is 1813.
- **Radius Secret:** Administrator can set password (Secret key) for RADIUS Server.

4.2 Remote LDAP Setup

Remote LDAP Setup enables Remote LDAP authentication for managed access points.

Administrators wishing to enable Remote LDAP authentication must copy and paste **DR-4000's** LDAP Server "**RADIUS Port**" number into the managed APs "Authentication Port" box, which is found in the managed Cerio APs "**Radius Setup**" window.

Administrator can set up 4 remote LDAP Server.



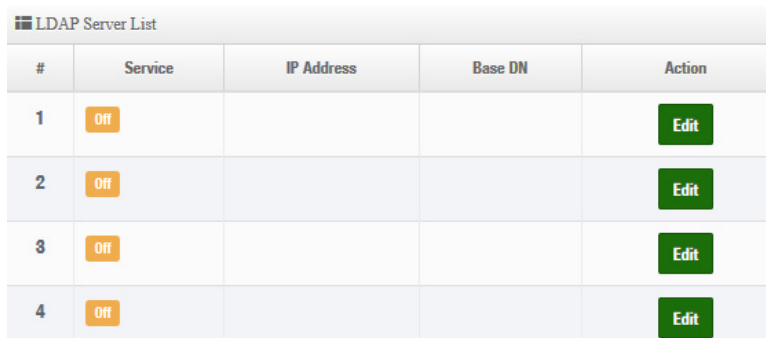
LDAP Server

Service ☒ Enable ☐ Disable

Radius Port

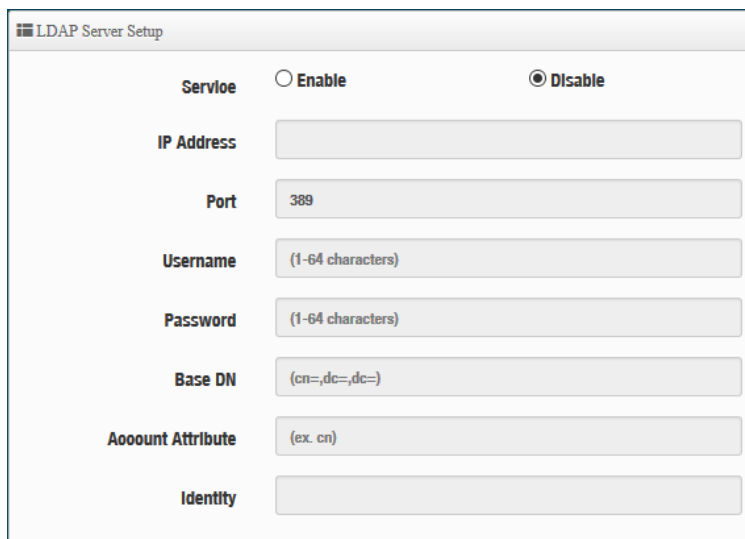
Radius Secret

- **Service:** Administrator can select Enable or Disable the authentication function.
- **Radius Port:** Administrators can set the Radius server port of the **DR-4000** to provide such as Cerio APs links. If Cerio APs set this Radius Port will can use remote LDAP(AD) type to authentication.
- **Radius Secret:** Administrator can set password (Secret key) for RADIUS Server.



#	Service	IP Address	Base DN	Action
1	<input type="button" value="Off"/>			<input type="button" value="Edit"/>
2	<input type="button" value="Off"/>			<input type="button" value="Edit"/>
3	<input type="button" value="Off"/>			<input type="button" value="Edit"/>
4	<input type="button" value="Off"/>			<input type="button" value="Edit"/>

- **Edit:** Administrator can click Edit to set remote LDAP Server information.



LDAP Server Setup

Service ☐ Enable ☒ Disable

IP Address

Port

Username

Password

Base DN

Account Attribute

Identity

- **Service:** Administrator can select Enable or Disable the function.
- **IP Address:** Set IP address for remote LDAP(AD) server.
- **Port:** Set Port for remote LDAP(AD) server.
- **Username:** Set login account for remote LDAP(AD) server.
- **Password:** Set login account use password for remote LDAP(AD) server.

- **Base DN:** Set Base DN path for remote LDAP(AD) server.
- **Account Attribute:** Set LDAP cn account for remote LDAP(AD) server.

LDAP Setting

Administrator can set remote LDAP(AD) timeout.

LDAP Settings

Timeout	<input type="text" value="4"/>	Seconds
Time Limit	<input type="text" value="3"/>	Seconds
Net Timeout	<input type="text" value="1"/>	Seconds

4.3 Package Setup

Administrator can set internet time rules for package authentication type.

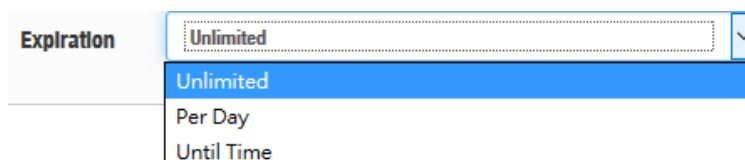
Package List							Create New Package
#	Name	Description	Session Time	Traffic Volume	Expire After	Expiration	Action
0	TEST-1	no time		0B			Edit
1	test-2	60Mbps Trafflo		60.00MB			Edit
2	test-3	use 120 minutes time	2Hour(s)	0B			Edit
3	Test-4	use 120 minutes expl...		0B	2Hour(s)		Edit

- **Create New Package:** Administrator can click “Create New Package” button to set package rules.
- **# :** Package list (0~9) is Network control server (SP-800) code, administrator can choose code to print account.

Package Setup

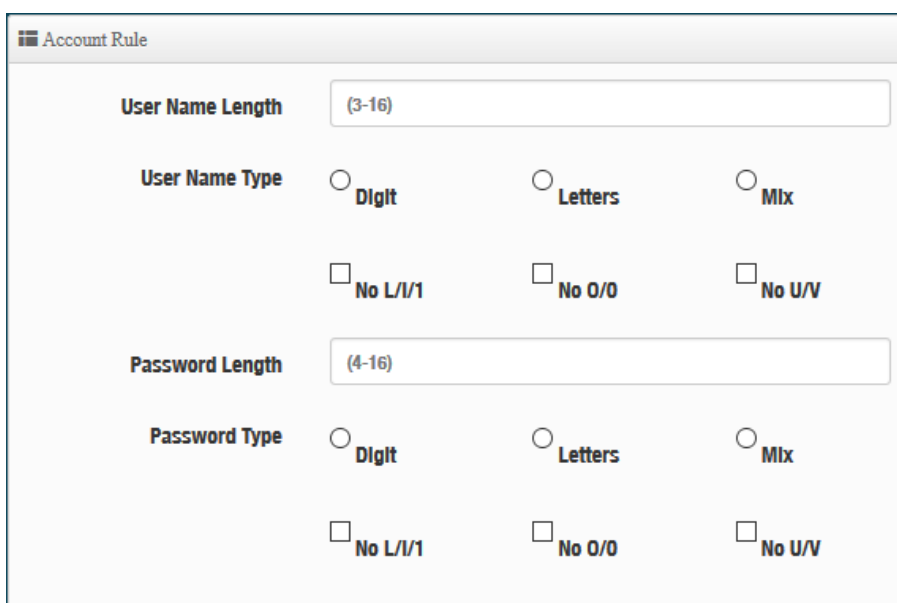
Package Name	<input type="text" value="(4-32 chars)"/>
Description	<input type="text" value="(4-64 chars)"/>
Trafflo Volume	<input type="text"/> MB
Session Time	<input type="text"/> Minutes
Expire After	<input type="text"/> Minutes
Expiration	Unlimited

- **Package Name:** Administrator can set Identify name for the package rules.
- **Description:** Administrator can set the description for package rules.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.
- **Session Time:** Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)
- **Expire After:** Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)
- **Expiration:** Administrator can select Unlimited or Per Day or Until Time.



The image shows a web interface for setting account rules. Under the 'Expiration' label, there is a dropdown menu. The menu is currently open, showing three options: 'Unlimited' (which is highlighted in blue), 'Per Day', and 'Until Time'.

- ✓ **Unlimited:** After the account is signed in, the system does not count the time
- ✓ **Per Day:** After the account is signed in, the system start counted time until the end time.
- ✓ **Until Time:** After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.



The image shows a window titled 'Account Rule'. It contains several configuration fields:

- User Name Length:** A text input field containing '(3-16)'.
- User Name Type:** Three radio buttons labeled 'Digit', 'Letters', and 'Mix'. Below them are three checkboxes labeled 'No L/I/1', 'No O/0', and 'No U/V'.
- Password Length:** A text input field containing '(4-16)'.
- Password Type:** Three radio buttons labeled 'Digit', 'Letters', and 'Mix'. Below them are three checkboxes labeled 'No L/I/1', 'No O/0', and 'No U/V'.

- **User Name Length:** Administrator can set account length limit for package rules.
- **User Name Type:** Administrator can create account use digit or Letters or Mix for

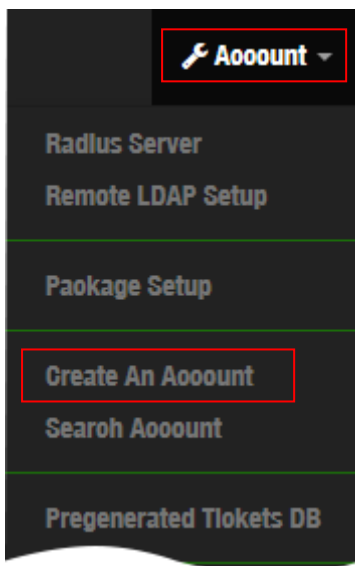
package rules. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.

- **Password Length:** Administrator can set password length limit for account.
- **Password Type:** Administrator can set password use digit or Letters or Mix for account. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.

4.4 Create An Account

Administrator can set and create an account of validity for the RADIUS Server.

Please click **“Account”** ➔ **“Create an account”**



 A screenshot of the 'Account Setup' form in the Cerio web interface. The form contains the following fields and options:

- User Name:** Text input field with a placeholder '(4-32 chars)'.
- Password:** Text input field with a placeholder '(4-32 chars)'.
- Package:** Dropdown menu showing 'Test-4 (use 120 minutes expire)' with an 'Apply' button.
- Traffic Volume:** Text input field with '0' and a unit selector 'MB'.
- Session Time:** Text input field with '0' and a unit selector 'Minutes'.
- Expire After:** Text input field with '0' and a unit selector 'Minutes'.
- Expiration:** Radio button options for 'Disable' (selected) and 'Enable'.

- **User Name** : Administrator can set an account for RADIUS Server.
- **Password** : Enter Password for user name account.
- **Package**: Administrator can choose apply mechanically Package function policy.
- **Traffic Volume**: Administrator can set authentication account use traffic limit for the package rules.
- **Session Time**: Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)
- **Expire After**: Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)
- **Expiration**: Administrator can select Unlimited or Per Day or Until Time.

Expiration	Unlimited	▼
	Unlimited	
	Per Day	
	Until Time	

- **Unlimited**: After the account is signed in, the system does not count the time
- **Per Day**: After the account is signed in, the system start counted time until the end time.
- **Until Time**: After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.

4.5 Search Account

Administrator can search all account in the databases. The search function built-in smart-search engine, administrator can set want to query account the conditions.

Please click **“Account”** ➔ **“Search Account”**

The screenshot displays two sections of the CERIO web interface. On the left is a dark sidebar menu with options: 'Radius Server', 'Remote LDAP Setup', 'Package Setup', 'Create An Account', 'Search Account' (highlighted with a red box), and 'Pre-generated Tickets DB'. The main content area is divided into two panels. The top panel, titled 'Search Account', contains search criteria: 'User Name' (dropdown: None, text: (4-32 chars)), 'Traffic Volume' (dropdown: None, text: MB), 'Session Time' (dropdown: None, text: Minutes), 'Expire After' (dropdown: None, text: Minutes), 'Page Size' (text: 10), 'Sort By' (dropdown: User Name), and 'Order By' (dropdown: Ascending). The bottom panel, titled 'Expiration Time', contains: 'Expiration' (dropdown: < less than), 'Date(Y/M/D)' (text: 2016, dropdown: 11, dropdown: 24), and 'Time(H:M:S)' (dropdown: 10, dropdown: 24, dropdown: 47).

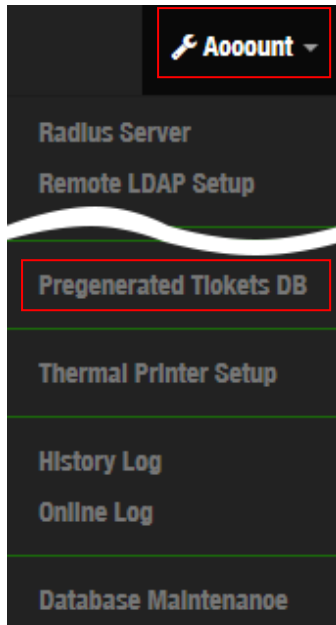
Administrators can choose different data type in the search engines.

- **None:** The program doesn't judge characters, search all the information
- **Greater then:** Search values for greater than
- **Equal:** Search values for equal.
- **Less then:** Search values for less then.
- **Between:** Search values for between.
- **Like:** Search similar strings.

4.6 Regenerated Tickets DB

Administrators can use system auto create accounts in a databases.

Please click **"Account" → "Regenerated Tickets DB"** to create databases.



#	Project	Session Time	Traffic Volume	Expire After	Expiration	Count	Action
-	-	-	-	-	-	-	-

Administrator can click Create New Project to set function.

➤ **Project Nama:** Administrator can set a Databases name.

➤ **Traffic Cycle:** There is a reset period for traffic usage, and the pre-vouched account

password will be eligible for repeated active use due to this reset period.

- ✓ **Total** : Based on a one-time total calculation, the total amount of pre-ticketed account traffic will no longer be usable after it is exhausted.
 - ✓ **Daily** : Set "Daily" as the limit traffic reset to zero cycle period. The system fixes 00:00 every day as the "Day" reset point.
 - ✓ **Weekly** : Set "weekly" as the cycle period for the quota traffic to be reset to zero. The system fixes 00:00 every Sunday as the "week" reset point.
 - ✓ **Monthly** : Set "monthly" as the cycle period for resetting the limit traffic to zero. The system fixes 00:00 on the last day of each month as the "month" reset point.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.

Session Time Cycle	Total ▼
Session Time	Total
Expire After	Daily
	Weekly
	Monthly

- **Session Time Cycle:** The session time uses a reset period, and the pre-ticket account password will be eligible for repeated and active use due to this reset period.
- ✓ **Total** : Calculated based on a one-time total, the pre-voucher account password Session time expires and can no longer be used.
 - ✓ **Daily** : Set "Daily" as the Session available time reset to zero cycle period, and the system fixes 00:00 every day as the "Day" reset span point.
 - ✓ **Weekly** : Set "weekly" as the reset zero cycle period for the session's available time. The system fixes 00:00 every Sunday as the "week" reset span point.
 - ✓ **Monthly** : Set "monthly" as the reset zero cycle period for the session's available time. The system fixes 00:00 on the last day of each month as the "month" reset point.
- **Session Time:** Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)
- **Expire After:** Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)
- **Expiration:** Administrator can select Unlimited or Per Day or Until Time.

Expiration	Unlimited	▼
	Unlimited	
	Per Day	
	Until Time	

- **Unlimited:** After the account is signed in, the system does not count the time
- **Per Day:** After the account is signed in, the system start counted time until the end time.
- **Until Time:** After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.

Pregenerated Rule

User Name Length	<input type="text" value="4"/>		
User Name Type	<input type="radio"/> Digit	<input type="radio"/> Letters	<input checked="" type="radio"/> Mix
	<input type="checkbox"/> No L/I/1	<input type="checkbox"/> No O/0	<input type="checkbox"/> No U/V
Password Length	<input type="text" value="4"/>		
Password Type	<input type="radio"/> Digit	<input type="radio"/> Letters	<input checked="" type="radio"/> Mix
	<input type="checkbox"/> No L/I/1	<input type="checkbox"/> No O/0	<input type="checkbox"/> No U/V
Ticket Number	<input type="text" value="100"/>		

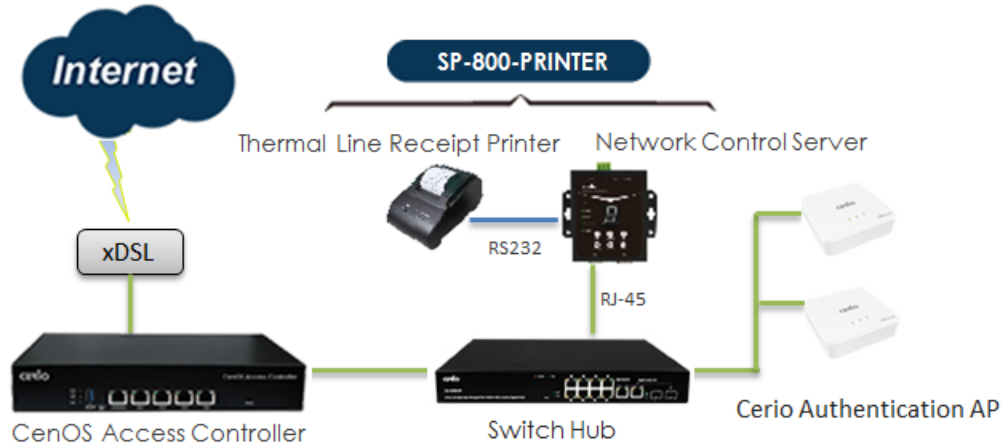
- **User Name Length:** Administrator can set account length limit for package rules.
- **User Name Type:** Administrator can create account use digit or Letters or Mix for package rules. If administrator select Letters or Mix can filter L/I/digit 1 and O/ digit 0 and U/V for letters and Mix.
- **Password Length:** Administrator can set password length limit for account.
- **Password Type:** Administrator can set password use digit or Letters or Mix for account. If administrator select Letters or Mix can filter L/I/digit 1 and O/ digit 0 and U/V for letters and Mix.
- **Ticket Number:** Administrator can set number in the databases, the system will auto create accounts

4.7 Thermal Printer Setup

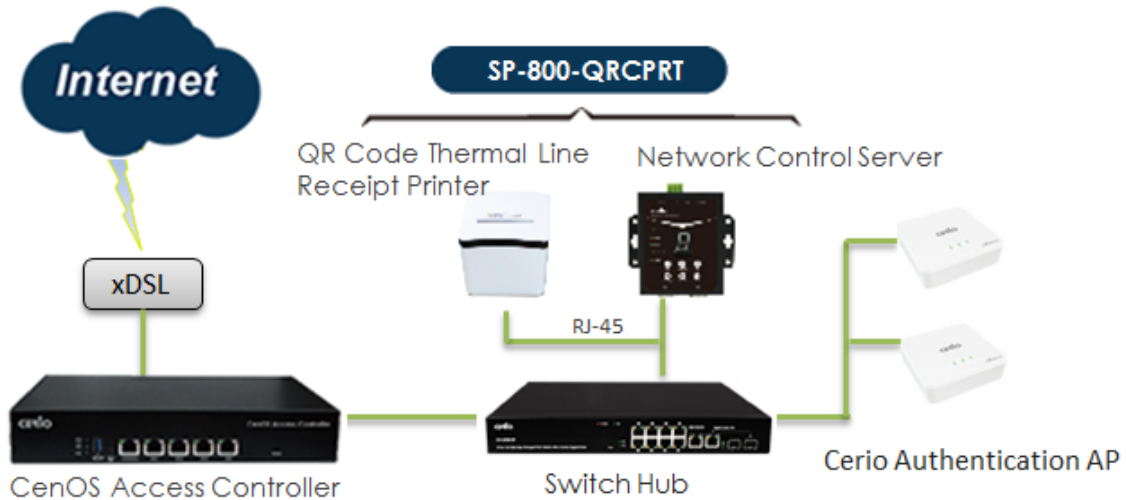
The function must match Account Ticket Generator POS System for Cerio's SP-800-PRINTER / SP-800-QRCPRT.

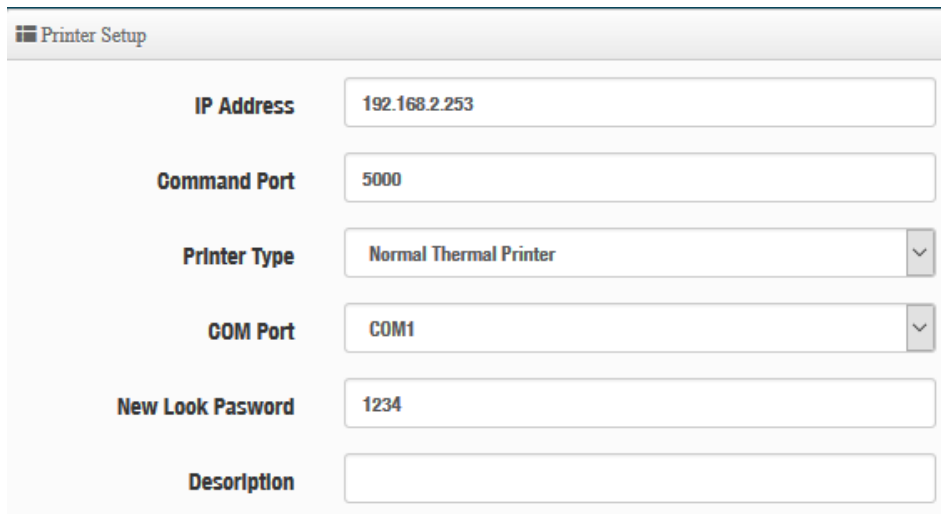
Application architecture is as follows.

Match SP-800-PRINTER



Match SP-800-QRCPRT

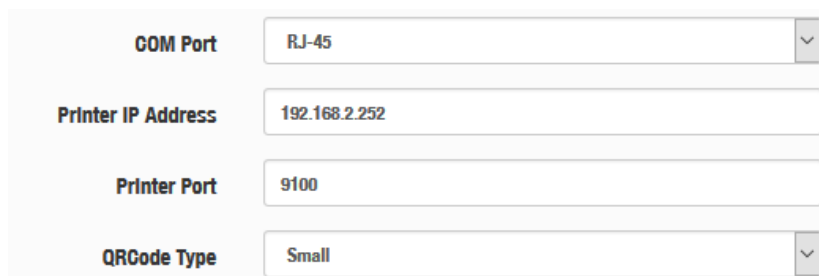




Printer Setup

IP Address	192.168.2.253
Command Port	5000
Printer Type	Normal Thermal Printer
COM Port	COM1
New Look Password	1234
Description	

- **IP Address:** Please set IP address for Network control server (SP-800)
- **Command Port:** Enter command port for Network control server (SP-800)
- **Printer Type:** Administrator can select Normal Thermal Printer or QR Code Thermal Printer.
 - **Normal Thermal Printer:** If use Cerio's SP-800-PRINTER POS system, administrator can select Normal Thermal Printer function.
 - **QR Code Thermal Printer:** If use Cerio's SP-800-QRCPRT POS system, administrator can select QR Code Thermal Printer function.
- **COM Port:** Administrator can select connected COM1/2 or RJ-45 for Printer Port.
 - **RJ-45:** If printer type selected QR Code Thermal Printer, administrator can select use RJ-45 and set Printer IP address.



COM Port	RJ-45
Printer IP Address	192.168.2.252
Printer Port	9100
QRCode Type	Small

- ✓ **Printer IP Address:** Administrator can set IP address for QR code Printer.
- ✓ **Printer Port:** Administrator can set Port for QR code Printer. The default Port is 9100 for Cerio's SP-800-QRCPRT
- ✓ **QR Code Type:** Administrator can select print QR Code size or close.
- **New Look Password:** The password is Network control server(SP-800) connect to **DR-4000** use key lock. Administrator can change password, default password is 1234
- **Description:** Administrator can enter Description.

Package List

Print tickets account must have created Package; administrator can refer to "[4.3 Package Setup](#)" description.

Package List			
Package#	Enable	Name	Description
1	<input type="checkbox"/>	TEST-1	no time
2	<input type="checkbox"/>	test-2	60Mbps Trafflo
3	<input type="checkbox"/>	test-3	use 120 minutes time
4	<input type="checkbox"/>	Test-4	use 120 minutes expl...

Administrator can choose box to enable Packages rule.

4.8 History Log

The Page can display account login/logout information.

History Log										
#	Username	Login Time	Logout Time	IP	MAC	Input Bytes	Output Bytes	AP IP	AP MAC	Status
-	-	-	-	-	-	-	-	-	-	-

4.9 Online Log

The Page can display online user information. The online user information must match Cerio's AP's; Administrator must enable RADIUS Accounting Port 1813 in the Cerio's AP's, as follows

Cerio's APs for CenOS5.0 interface

Radius Setup

Radius

☒ Enable
 ☐ Disable

Display Name

Primary Server IP

Secondary Server IP

Authentication Port

Port

Accounting Service

☒ 1813

Port

Authentication Type

☐ PAP
 ☒ CHAP

Secret Key

DR-4000 online Log page

Online Log									
Online Log									
#	Username	Login Time	Session Time	IP	MAC	Input Bytes	Output Bytes	AP IP	AP MAC
-	-	-	-	-	-	-	-	-	-

4.10 Database Maintenance

Administrator can clear account for Expiration / Pregenerated / All databases.

Account Database

Expiration of Account

0

Clear

Pregenerated of Account

0

Clear

All of Account

0

Clear



Administrator click "Clear" button, the databases all account will be deleted.

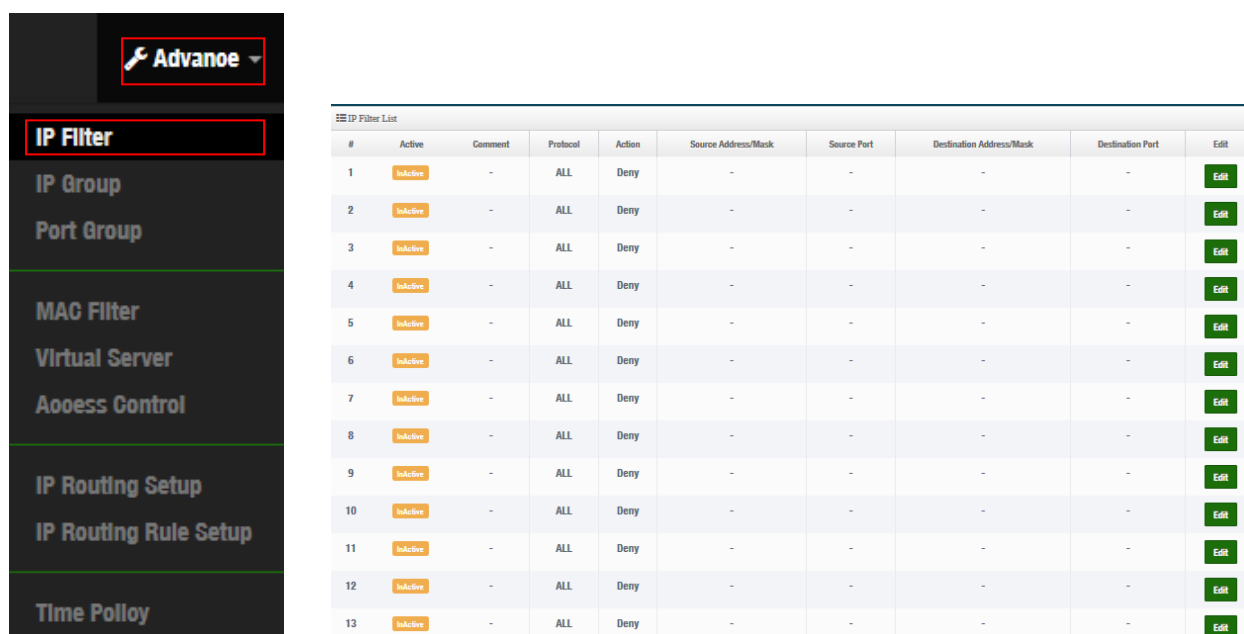
5. Advance

5.1 IP Filter

Can allow or deny filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or (WAN) ports. Filter rules support IP/ Port Groups, could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Access control rules.

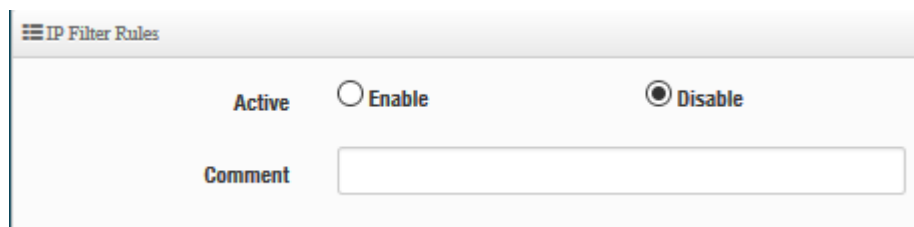
Administrator can set IP Filter rules: 64

Please click “**Advance**” → “**IP Filter**” setup.



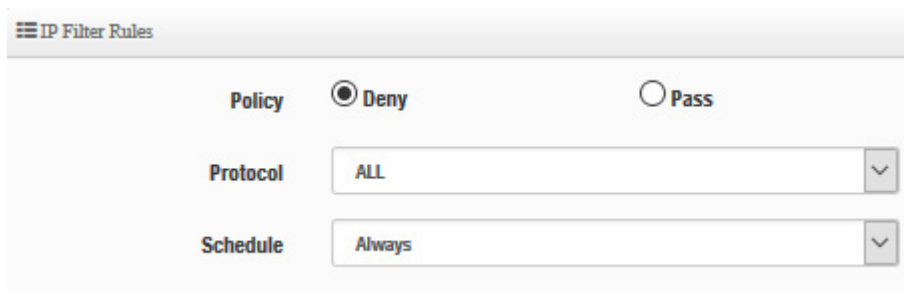
#	Active	Comment	Protocol	Action	Source Address/Mask	Source Port	Destination Address/Mask	Destination Port	Edit
1	Inactive	-	ALL	Deny	-	-	-	-	Edit
2	Inactive	-	ALL	Deny	-	-	-	-	Edit
3	Inactive	-	ALL	Deny	-	-	-	-	Edit
4	Inactive	-	ALL	Deny	-	-	-	-	Edit
5	Inactive	-	ALL	Deny	-	-	-	-	Edit
6	Inactive	-	ALL	Deny	-	-	-	-	Edit
7	Inactive	-	ALL	Deny	-	-	-	-	Edit
8	Inactive	-	ALL	Deny	-	-	-	-	Edit
9	Inactive	-	ALL	Deny	-	-	-	-	Edit
10	Inactive	-	ALL	Deny	-	-	-	-	Edit
11	Inactive	-	ALL	Deny	-	-	-	-	Edit
12	Inactive	-	ALL	Deny	-	-	-	-	Edit
13	Inactive	-	ALL	Deny	-	-	-	-	Edit

➤ Please click **Edit** button to setting IP filter.



- **Active:** Administrator can selected Enable or Disable for the IP filter rules function.
- **Comment:** Enter rule description.

IP Filter Rules



IP Filter Rules

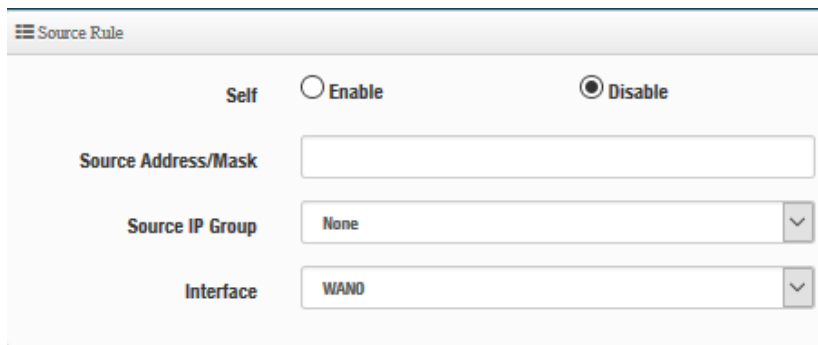
Policy ☒ Deny ☐ Pass

Protocol

Schedule

- **Policy:** Administrator can select Deny or Pass for IP filter rules.
- **Protocol:** Administrator can select type for IP protocol.
- **Schedule:** Can choose to use rule by “Time Policy”.

Source Rule



Source Rule

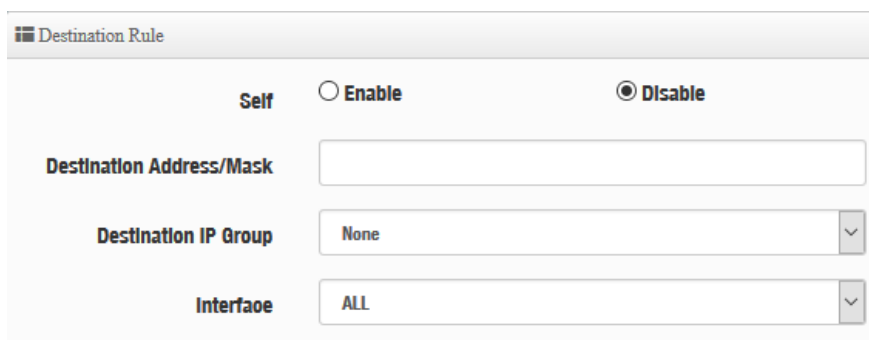
Self ☐ Enable ☒ Disable

Source Address/Mask

Source IP Group

Interface

- **Self:** Administrator can choose Enable or Disable, if administrator select Enable, the source is self.
- **Source Address/Mask:** Administrator can set IP address and Mask for source.
- **Source IP Group:** Administrator can select belonging to group for IP Address.
- **Interface:** Administrator can select interface for source.



Destination Rule

Self ☐ Enable ☒ Disable

Destination Address/Mask

Destination IP Group

Interface

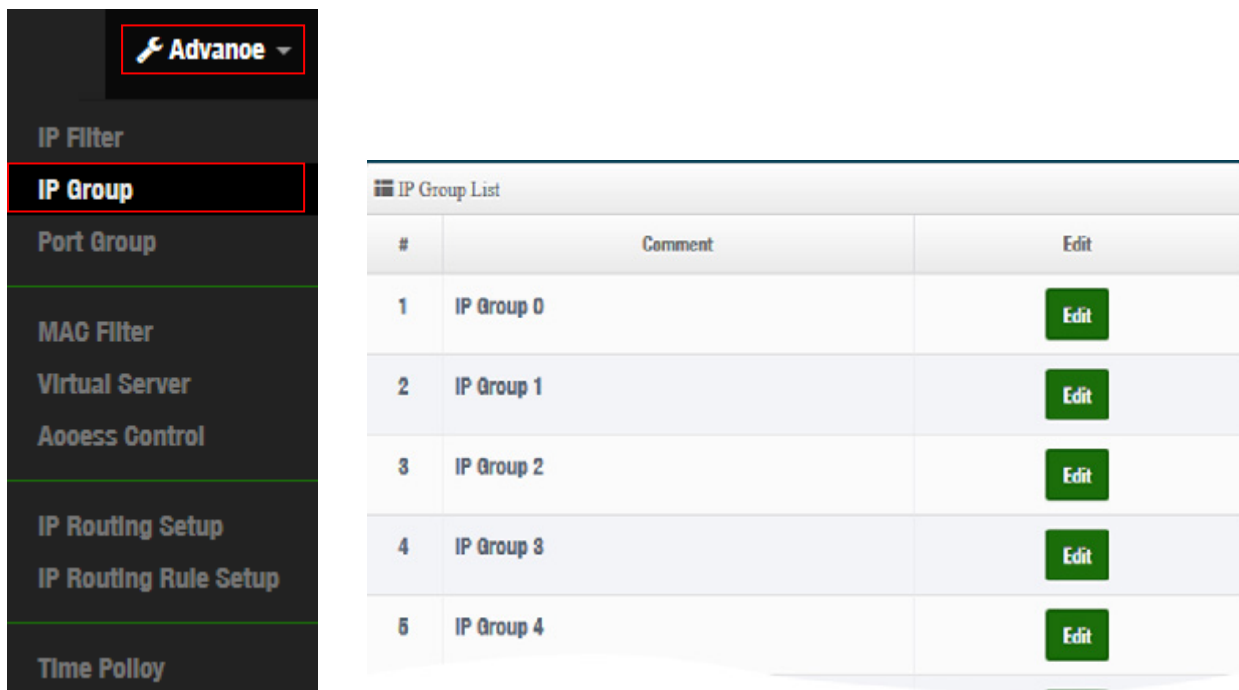
- **Self:** Administrator can choose Enable or Disable, if administrator select Enable, the source

is self.

- **Destination Address/Mask:** Administrator can set IP address and Mask for destination.
- **Destination IP Group:** Administrator can select belonging to group for IP Address.
- **Interface:** Administrator can select interface for destination.

5.2 IP Group

Administrator can create IP group for IP address range or subnet.



#	Comment	Edit
1	IP Group 0	Edit
2	IP Group 1	Edit
3	IP Group 2	Edit
4	IP Group 3	Edit
5	IP Group 4	Edit

Please click “**Edit**” button to create new IP Groups.



IP Group Setting

Comment

- **Comment:** Enter IP Group description.

IP Address Setup

IP Address Type

Single IP Address

IP Address

Comment

Add

➤ **IP Address Type:** Administrator can select single / range / subnet type to set IP Address.

IP Address Type

Single IP Address

Single IP Address

Range

Subnet

Add

- **Single IP Address:** Enter single IP Address.
- **Range:** Enter start / end IP address.
- **Subnet:** Enter Net/Mask.

5.3 Port Group

Administrator can create Port group

⚙ Advance

IP Filter

IP Group

Port Group

MAC Filter

Virtual Server

Access Control

IP Routing Setup

IP Routing Rule Setup

Time Policy

Port Group List		
#	Comment	Edit
1	Port Group 0	Edit
2	Port Group 1	Edit
3	Port Group 2	Edit
4	Port Group 3	Edit
5	Port Group 4	Edit
6	Port Group 5	Edit

Please click “**Edit**” button to create new Port Groups.

Port Group Setting

Comment

Port Setup

Port Type

Port

Comment

Port List

#	Port	Comment	Action
-	-	-	-

- **Comment:** Enter Port Group description.
- **Port Type:** Administrator can select single or range Port.
- **Port:** Administrator can set service port.

5.4 MAC Filter

Allows creating MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important and must note. That MAC filter rules have precedence over IP Filter rules.

Advance

IP Filter
IP Group
Port Group
MAC Filter
Virtual Server
Access Control
IP Routing Setup
IP Routing Rule Setup
Time Policy

MAC Filter Rules

Mode

Disable
Deny
Allow

MAC Filter List

#	Active	Comment	MAC Address	Policy
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Always Run
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Always Run
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Always Run
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Always Run
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Always Run

- **Mode:** Administrator can select Deny or Allow.
 - **Deny:** The MAC Filter List will be **denied** to access (LAN to WAN). Others will be allowed.
 - **Allow:** The MAC Filter List will be **allowed** to access (LAN to WAN). Others will be denied.
- **Comment:** Enter the description of MAC filter rule.
- **MAC Address:** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click “Add” button, then the

MAC address should display in the MAC Filter List.

- **Policy:** Administrator can select to use rule by “**Time Policy**”.

5.5 Virtual Server

The “**Virtual Server**” can also referred to as “Port Forward” as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don’t repeat ports’ usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

- **Active:** Administrator can select Virtual server rule to Enable or disable.
- **Comment:** Enter the description of virtual server rule.
- **Protocol:** Administrator can select service protocol of TCP or UDP.
- **Public Port:** Enter service port No. for public.
- **Private IP Address:** Enter corresponding IP address for internal.
- **Private Port:** Enter internal service port No. for private.
- **Schedule :** Administrator can select to used rule of “**Time Policy**”

5.6 Access Control

The Access Control function administrator can to block or allow specific kinds of TCP/UDP/ICMP protocol, such as Internet access, designated services, and websites. The Access Control function can set 20 profiles.

Please click on **Advance** -> **Access Control** and follow the below setting.

⚙ Advance ▾

IP Filter

IP Group

Port Group

MAC Filter

Virtual Server

Access Control

IP Routing Setup

IP Routing Rule Setup

Time Polloy

#	Active	Comment	Protocol	Edit
1	InActive	-	ANY	Edit
2	InActive	-	ANY	Edit
3	InActive	-	ANY	Edit
4	InActive	-	ANY	Edit
5	InActive	-	ANY	Edit

- **#** : Display access control list.
- **Active** : Display Active or InActive for the access control rule.
- **Comment**: Display information for the rule.
- **Protocol** : Display information for the protocol.
- **Edit** : Administrator can click the button to set Access Control rule.

Access Control Rules

Active
☐ Enable ☒ Disable

Comment

Protocol ANY

Schedule Always

MAC Address Setup

MAC Address
Add

MAC Address List

#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

IP Address Setup

Local IP Address -

Local Port

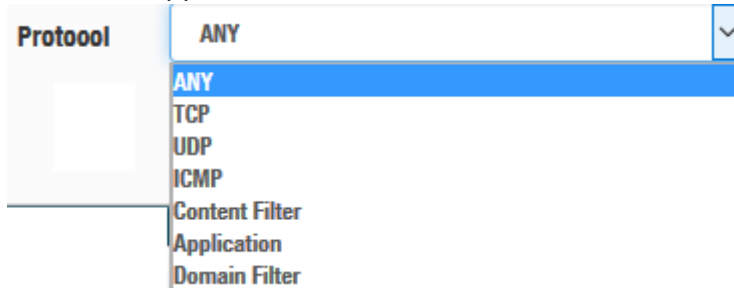
Destination IP Address -

Destination Port

Interface ALL VLAN

Access control rules :

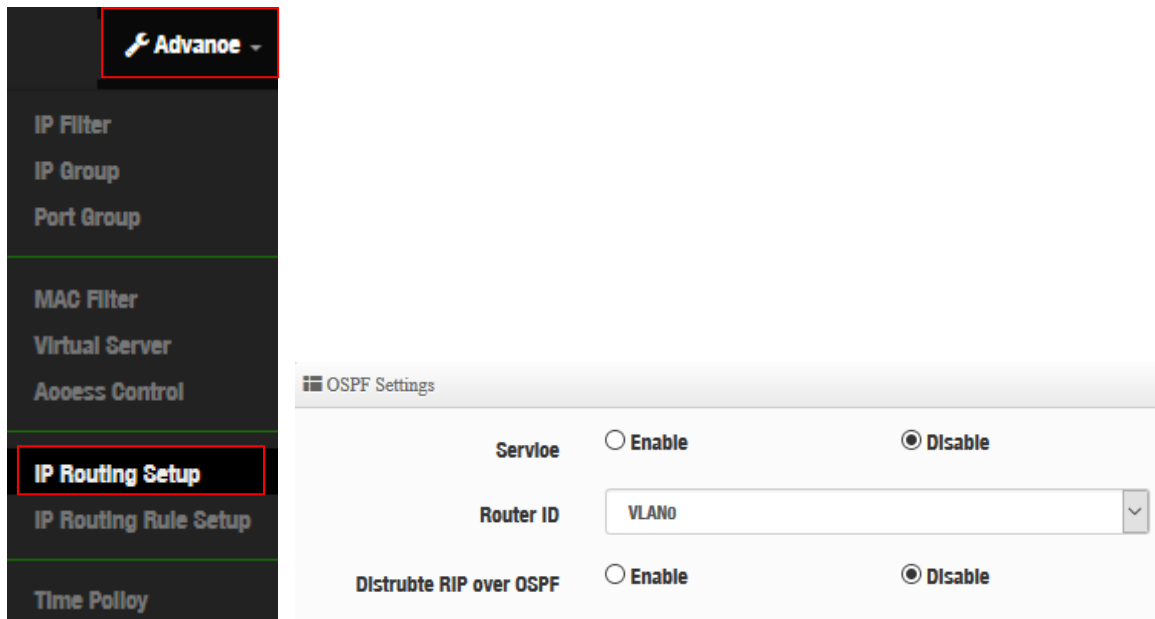
- **Active** : Administrator can select Enable or Disable for the Access control rule.
- **Comment** : Administrator can enter comment for the role.
- **Protocol** : Administrator can to select management protocol by TCP/UDP/ICMP/Content Filter/Application and Domain Filter.



- ✓ **ANY:** Select "Any" is all deny Protocol, administrator can filter local IP / IP range go to destination IP / IP range and use protocol.
- ✓ **TCP:** Deny TCP Protocol, Administrator can set TCP protocol and assign IP / IP range.
- ✓ **UDP:** Deny UDP Protocol, Administrator can set UDP protocol and assign IP / IP range.
- ✓ **ICMP:** Deny ICMP Protocol, Administrator can assign IP / IP range.
- ✓ **Content Filter:** Administrator can set web Keyword to filter.
- ✓ **Application:** System built-in multiple applications data, Administrator can select application data to filter.
- ✓ **Domain:** Administrator can set domain name to filter.
- **Schedule** : The rule can apply Time Policy.

5.7 IP Routing Setup

The IP Routing Settings allows configure routing feature in the gateway. The system supports RIP(Routing Information Protocol) and OSPF(Open Shortest Path First) dynamic routing and allows you to manually configure static network routes. Please click on Advance -> IP Routing and follow the below setting.

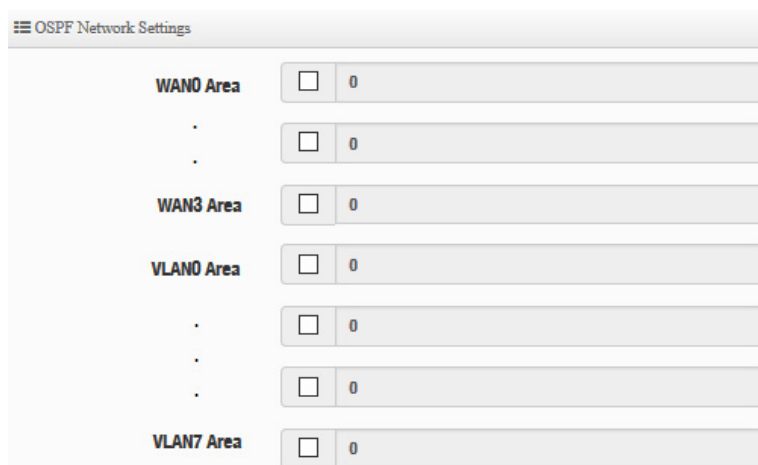


➤ OSPF Settings :

OSPF (Open Shortest Path First) is a router protocol used to find the best path for packets as they pass through a set of connected networks.

- **Service:** Administrator can select enable or disable Service for OSPF.
- **Route ID:** Administrator can select WAN0~3 and VLAN0~7 interface (IP) for the Route ID.
- **Distribute RIP over OSPF:** Administrator can select enable or disable, if select enable system can allow RIP routes will redistributed into OSPF.

OSPF Network Setting




- ✓ **#Area:** Represents the area code of the OSPF routing protocol, which can be any digit in decimal, default is 0.

➤ RIP Settings :


RIP defines a way for routers, which connect networks using the IP, to share information about how to route traffic among networks. RIP prevents routing loops by implementing

limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and the route is considered unreachable.

 RIP Settings

Service	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Distribute OSPF over RIP	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

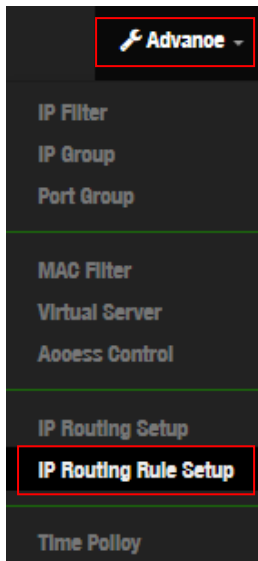
- **Service:** Administrator can select enable or disable Service for RIP.
- **Distribute OSPF over RIP:** Administrator can select enable or disable, if select enable system can allow OSPF routes will redistributed into RIP.

 RIP Side(Devices) Settings

WAN0	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
.	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
.		
WAN3	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
WAN3	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
VLAN0	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
.	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
.		
VLAN7	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

- ✓ **RIP Side(Devices) Settings:** Administrator can choose enable or deniable for WAN/LAN interface

5.8 IP Routing Rule Setup



IP Routing Rule List						
#	Active	Destination Net/Mask	Via	OSPF	RIP	Edit
1	InActive	-	-	Off	Off	Edit
2	InActive	-	-	Off	Off	Edit
...						
19	InActive	-	-	Off	Off	Edit
20	InActive	-	-	Off	Off	Edit

Please click **Edit** button to setting IP Routing Rule.

IP Routing Rule Settings

Service

☐ Enable
 ☒ Disable

Destination Net/Mask

Via

☒ Gateway
 ☐ Interface

Gateway

OSPF

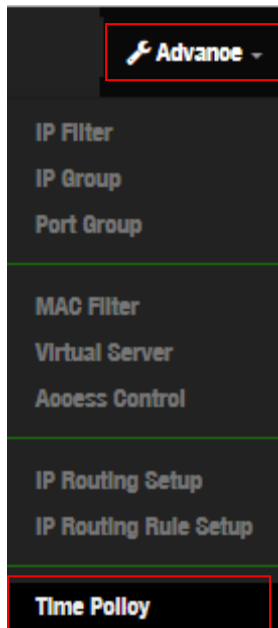
☐ Enable
 ☒ Disable

RIP

☐ Enable
 ☒ Disable

- **Service:** Administrator can select Enable or Disable for the IP Routing Rule.
- **Destination Net/Mask:** If administrator select enable for service, will be able set destination Net/Mask.
- **Via:** Administrator can select use Gateway or Interface
 - **Gateway:** enter Gateway IP address.
 - **Interface:** Select WAN / LAN interface.
- **OSPF/RIP:** Administrator can select enable or disable, if select enable will apply “IP Routing Setup” of OSPF/RIP function.

5.9 Time Policy



Policy List			
#	Comment	Mode	Edit
1	Polloy 1	On Sohedule	Edit
2	Polloy 2	On Sohedule	Edit
...			
9	Polloy 9	On Sohedule	Edit
10	Polloy 10	On Sohedule	Edit

Please click **Edit** button to setting time policy rules.

Time Policy Rules

Comment

Mode

☒ On Sohedule
 ☐ Out Of Schedule

Policy List

Create New Policy

#	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Action
-	-	-	-	-	-	-	-	-	-

- Comment: Enter the description of Time Policy rule. **There are maximum 10 for the time policy.**
- Mode: Administrator can select on schedule or Out of schedule to execution the rules.

Create New Policy button:

Administrator can set time for week / start time and end time.

Time Policy Rules

Day of Week

☐ Sun
 ☐ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☐ Sat

Start Time

End Time

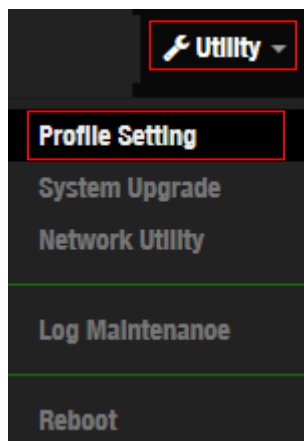
Click “**Save**” button to add schedule to policy. **There are 300 schedule rules maximum allowed in the each time policy.** All schedules can be edited or removed in the each time policy. Click Reboot button to activate your changes.

6. Utility

6.1 Profile Setting

This Functions purpose is to backup current configuration, restore prior configuration or reset back to factory default configurations.

Please click on **Utility -> Profile Setting** and follow the below setting



Profile Setting

In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

Save Settings To PC	<input type="button" value="Save"/>
Load Settings From PC	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>
Reset To Factory Default	<input type="button" value="Default"/>

Update SSL Certification From Local Hard Drive

Certificate File	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>
------------------	---

- **Save Settings to PC:** Click **Save** button to save the current configuration to a local disk.

- **Load Settings from PC:** Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default:** Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.
- **Update SSL Certification From Local Hard Drive :** If the environment unit already has an SSL security certificate for the corresponding domain or subdomain, the administrator can set up the configuration to use the HTTPS security mechanism when using [Authentication Web Captive portal login page]. This function can be used to transfer the SSL of the unit [Authentication Web Captive portal login page] to upload secure credentials to run the browser HTTPS security mechanism smoothly.



Notice

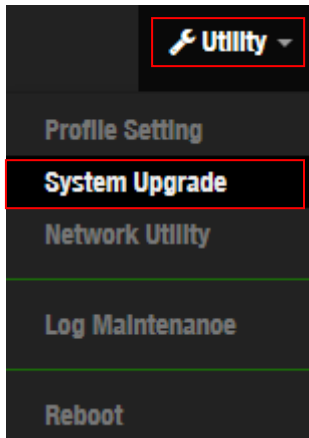
This certificate import function supports the one-time import of a single file. You can use Notepad to directly open multiple obtained certificate files and merge and edit the content text into one certificate file for uploading and importing.

The file name and extension of the certificate file to be uploaded and imported are not restricted. The text format of the content of a single SSL certificate file uploaded from the computer should at least include the certification information (Cert/CRT) and the private key (Privkey/ Key) two types, if they include relay certificate (Chain/CA Bundle) or other text such as root certificate file content, please merge them into a single file and then import the file.

6.2 System Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around 2 minutes to upgrade due to complexity of firmware. To upgrade system firmware, click Browse button to locate the new firmware, and then click Upgrade button to upgrade.





Firmware Information:

Display the system firmware information.

Firmware Information

Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Firmware Version

Pme-CPE-IPQ60XX-CERIO V0.0.2

Firmware Date

2024/05/06 12:45:19

Upgrade Via Local PC

Select File

Choose File

No file chosen

Upload

Upgrade Via TFTP Server

TFTP Server IP

File Name

Upload

Upgrade Via HTTP URL

URL

Upload

Upgrade Via Local PC and TFTP Server:

The upgrade firmware will support via local PC and TFTP Server and HTTP URL to upgrade system.

- **Select File:** Administrator can select Firmware file in Local PC.
- **TFTP Server:** Enter IP address for TFTP Server.
- **File Name:** Enter file name.
- **URL:** Administrator can enter path for Firmware file.

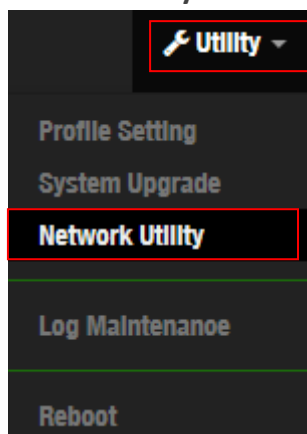


Notice

1. To prevent data loss during firmware upgrade, please back up current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.

6.3 Network Utility

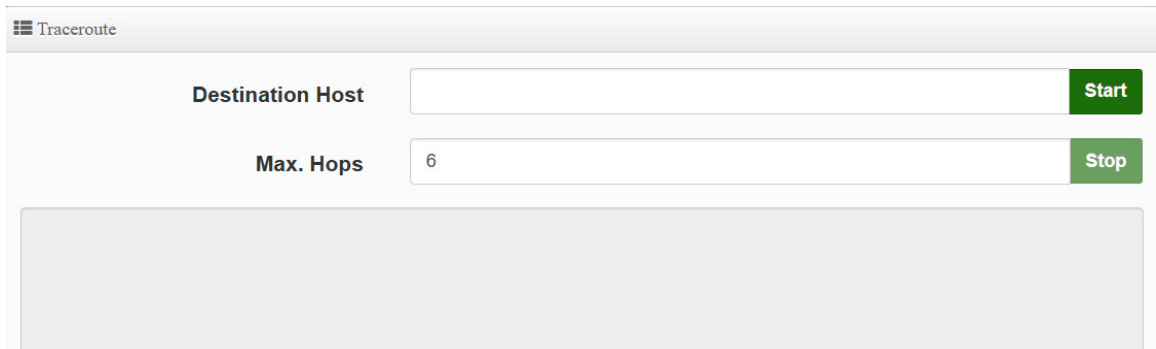
The administrator can diagnose network connectivity via the PING or TRACEROUTE utility. Please click on **Utility** -> **Network Utility** and follow the below setting.



- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
- **IP/Domain**: Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ping button to proceed. The ping result will be shown in the Result field.



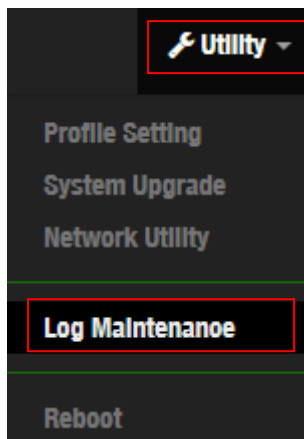
- **Times:** By default, its 5 and the range is from 1 to 50. It indicates number of connectivity test.



- **Traceroute** : Allows tracing the hops from the DR-4000 device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test.
- **Destination Host:** Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
- **MAX Hops:** Specifies the maximum number of hops (max time-to-live value) trace route will probe.

6.4 Log Maintenance

Administrator can monitor Log storage status for Session/Authentication and System. Please click on **Utility ->Log Maintenance** and follow the below setting.



Session Log Maintenance

File Size/Peroent

16.00KB

0%

Keep Date

2016-11-2

Delete

Authentication Log Maintenance

File Size/Peroent

16.00KB

0%

Keep Date

2016-11-2

Delete

System Log Maintenance

File Size/Peroent

16.00KB

0%

Keep Date

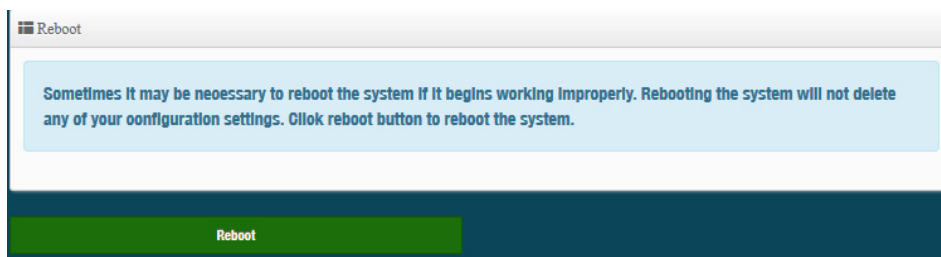
2016-11-2

Delete

- **File Size/Percent:** Display used volume and percentage.
- **Keep Date:** Display creation date.
 - **Delete button:** Administrator can click “delete” button to clear log information.

6.5 Reboot

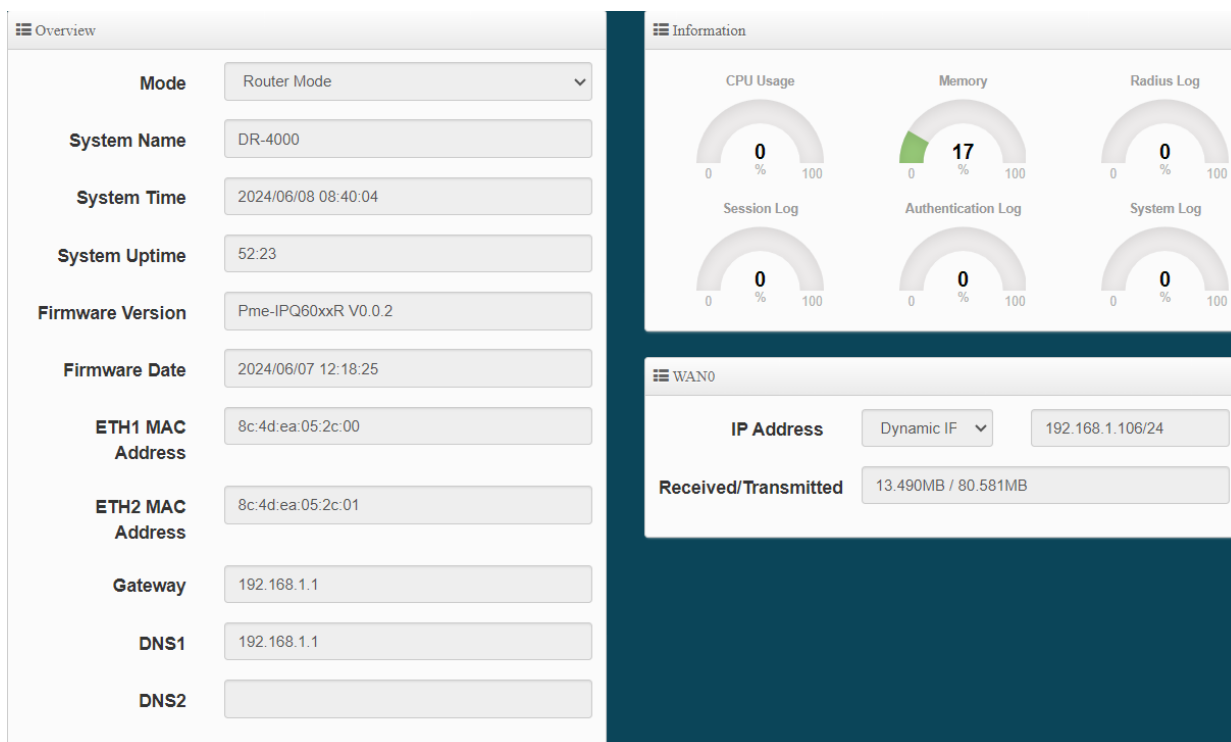
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



7. Status

7.1 Overview

Detailed information on System, Network can be reviewed via this page.



- **WAN#:** Display information for WAN Port setting. Administrator can click Action button to connect or disconnect for WAN Ports.

7.2 Local System Log

The system log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log				Refresh	Clear
Time	Facility	Severity	Message		
-	-	-	-		

- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such "System" or "User"
- **Severity** : Severity level that a specific event is associated such as "info", "error", "warning", etc.
- **Message** : Description of the event.
- Click "**Refresh**" button to renew the log
- Click "**Clear**" button to clear all the record.

7.3 Session Log

If enable "syslog server" in the "**Session Log**" (Hotspot Setup, Please refer to Chapter 3.4) and, the page can record account for session log. Session log page built-in smart-search function will display account use session information, administrator can use keyword or date approach to discover.

Session Log			
Name	Value		
Event Time	None	2016-11-21	2016-11-21
AP IP	None		
VLAN ID	None		
Username	None		
Protocol	None	TCP	
Source IP	None		
Destination IP	None		
Source Port	None		
Destination Port	None		
Source MAC	None		

Administrators can choose different data type in the search engines.

- **None**: The program doesn't judge characters, search all the information
- **Greater then**: Search values for greater than
- **Equal**: Search values for equal.
- **Less then**: Search values for less then.
- **Between**: Search values for between.
- **Like**: Search similar strings.

#	Event Time	AP IP	VLAN ID	Username	Protocol	Source IP	Destination IP	Source Port	Destination Port	Source MAC
1	2015-01-01 08:01:41	192.168.2.254	0	test	UDP	192.168.2.10	192.168.2.10	62461	1900	8C:4D:EA:02:C6:EC
2	2015-01-01 08:01:41	192.168.2.254	0	test	TCP	192.168.2.10	192.168.2.10	62362	443	8C:4D:EA:02:C6:EC
3	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10	192.168.2.1	59448	53	8C:4D:EA:02:C6:EC
4	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10	192.168.2.1	54064	53	8C:4D:EA:02:C6:EC
5	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10	192.168.2.1	53759	53	8C:4D:EA:02:C6:EC
6	2015-01-01 08:01:42	192.168.2.254	0	test	TCP	192.168.2.10	192.168.2.1	62364	443	8C:4D:EA:02:C6:EC
7	2015-01-01 08:01:44	192.168.2.254	0	test	UDP	192.168.2.10	192.168.2.1	62461	1900	8C:4D:EA:02:C6:EC
8	2015-01-01 08:01:46	192.168.2.254	0	test	TCP	192.168.2.10	192.168.2.1	62366	443	8C:4D:EA:02:C6:EC
9	2015-01-01 08:01:46	192.168.2.254	0	test	UDP	192.168.2.10	192.168.2.1	57436	53	8C:4D:EA:02:C6:EC
10	2015-01-01 08:01:46	192.168.2.254	0	test	TCP	192.168.2.10	192.168.2.1	62367	5222	8C:4D:EA:02:C6:EC
11	2015-01-01 08:01:47	192.168.2.254	0	test	UDP	192.168.2.10	192.168.2.1	62461	1900	8C:4D:EA:02:C6:EC
12	2015-01-01 08:01:48	192.168.2.254	0	test	TCP	192.168.2.10	192.168.2.1	62368	80	8C:4D:EA:02:C6:EC

If the session interception function setting used is not configured on the front-end Cerio AP on this machine, you can store the logs of the Cerio AP to this log server. Please enter the management settings of the Cerio AP and set the "Session Log" Setup points the IP to the device and enables the "session log" for the Cerio AP feature.

The following is a reference to the relevant settings of Cerio AP.

Setup 1 : Please click Cerio AP to "System" → "Authentication Setup" to enable to Session Log setting.

Authentication Setup

Multiple Login

☐ 3
 User(s)

Login Timeout

Minutes

Redirect URL

Login URL

Authentication Log

☒ Enable
 ☐ Disable

Session Log

☒ Enable
 ☐ Disable

Setup 2 : Please click Cerio AP to "Management" → "System Log Setup" to fill in remote Server IP Address.

System Log Setup

Remote Server

☒ 192.168.101.254

Port

514

Port

7.4 Authentication Log

If enable “syslog server” in the “**Authentication Log**” (Hotspot Setup, Please refer to Chapter 3.4) and authentication log in Cerio's AP, the page can record account for authentication log. Authentication log page built-in smart-search function will display account use session information, administrator can use keyword or date approach to discover.

Authentication Log

Name	Value	
Event Time	None	2016-11-21
AP IP	None	
VLAN ID	None	
Username	None	
Source IP	None	
Source MAC	None	
Event	None	

Administrators can choose different data type in the search engines.

- **None:** The program doesn't judge characters, search all the information
- **Greater then:** Search values for greater than
- **Equal:** Search values for equal.
- **Less then:** Search values for less then.
- **Between:** Search values for between.
- **Like:** Search similar strings.

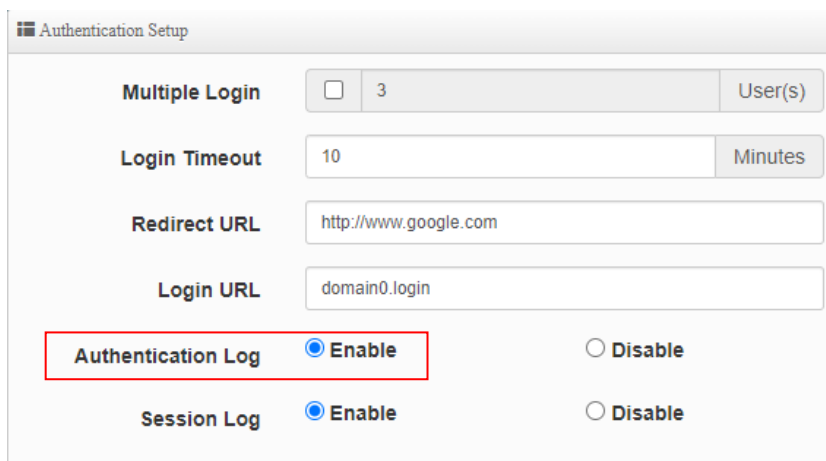
#	Event Time	AP IP	VLAN ID	Username	User IP	User MAC	Event
1	2015-01-01 08:01:39	192.168.2.254	0	test	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
2	2016-11-21 12:56:50	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
3	2016-11-21 12:57:28	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGOUT
4	2016-11-21 12:57:37	192.168.2.254	0	test	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
5	2016-11-21 13:02:22	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN

If the authentication interception function setting used is not configured on the front-end Cerio

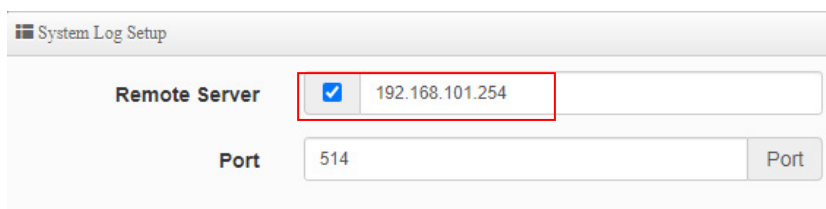
AP on this machine, you can store the logs of the Cerio AP to this log server. Please enter the management settings of the Cerio AP and set the "System Log" Setup points the IP to the device and enables the authentication log for the Cerio AP feature.

The following is a reference to the relevant settings of Cerio AP.

Setup 1 : Please click Cerio AP to "System" → "Authentication Setup" to enable for Authentication Log setting.



Setup 2 : Please click Cerio AP to "Management" → "System Log Setup" to fill in remote Server IP Address.



7.5 Remote System Log

If enable "syslog server" in the "Remote System Log" and Remote System log in Cerio's AP, The page can record Remote system log for Cerio Aps too.

Name	Value	
Event Time	None	2016-11-21
Device IP	None	
Facility	None	Kernel messages
Priority	None	Emergency
Message	None	

Administrators can choose different data type in the search engines.

- **None:** The program doesn't judge characters, search all the information
- **Greater then:** Search values for greater than
- **Equal:** Search values for equal.
- **Less then:** Search values for less then.
- **Between:** Search values for between.
- **Like:** Search similar strings.

System Log List					
#	Event Time	AP IP	Facility	Priority	Message
1	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPP BSD Compression module registered
2	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPP MPPE Compression module registered
3	2016-01-01 08:00:00	192.168.2.254	user	Informational	NET: Registered protocol family 24
4	2016-01-01 08:00:00	192.168.2.254	local0	Informational	started, version 2.22 cachesize 150
5	2016-01-01 08:00:00	192.168.2.254	local0	Informational	cleared cache
6	2016-01-01 08:00:00	192.168.2.254	local0	Informational	reading /etc/resolv.conf
7	2016-01-01 08:00:00	192.168.2.254	local0	Informational	using nameserver 192.168.2.1#53
8	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPPoL2TP kernel driver, V1.0

If the remote system interception function setting used is not configured on the front-end Cerio AP on this machine, you can store the logs of the Cerio AP to this log server. Please enter the management settings of the Cerio AP and set the "System Log" Setup points the IP to the device for the Cerio AP feature.

The following is a reference to the relevant settings of Cerio AP.

Setup 1 : Please click Cerio AP to "Management" ➔ "System Log Setup" to fill in remote Server IP Address.

System Log Setup	
Remote Server	<input checked="" type="checkbox"/> 192.168.101.254
Port	514

8. Technical documents

8.1 Hotspot function used POS system application

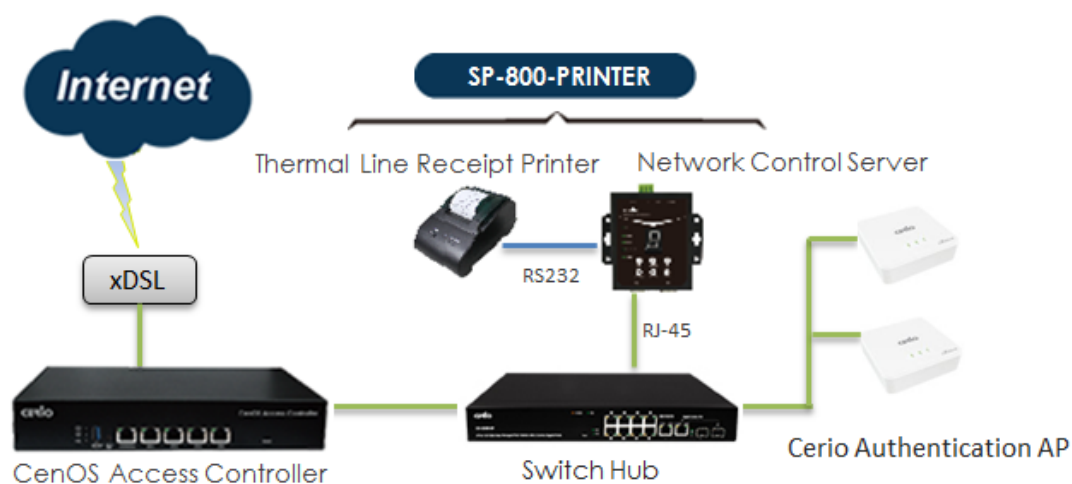


Cerio's POS system device by optional.

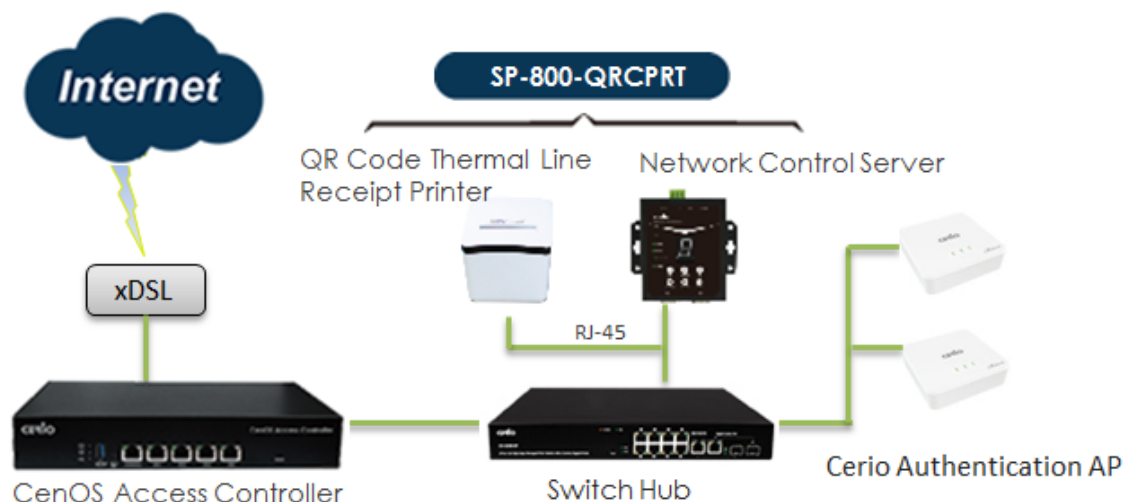
POS system is authentication device of the special use network control server (SP-800) + Thermal printer. You can refer to SP-800-PRINTER and SP-800-QRCPRT for Cerio's .

Administrator can use SP-800 to generate a new account for the remote control Cerio's Web authentication device and print authentication account.

Cerio's controller mounted SP-800-PRINTER for POS system application diagram




Cerio's controller mounted SP-800-QRCPRT for POS system application diagram.



Login management interface for SP-800

Network control server(SP-800) built-in web management interface. After install POS system architecture, administrator can use network connect to SP-800 interface and management. The SP-800 manager URL is <http://192.168.2.253/setting.htm>, please open IE or Firefox browser and enter URL address to set function.

 **Network Control Server v1.1**

COM1 Settings

Data Baud Rate	9600 ▾
Data Bits	8 ▾
Data Parity	None ▾
Stop Bits	1 ▾
Flow Control	None ▾

Network Settings

<input type="checkbox"/> Enable DHCP	
Static IP Address	192.168.2.253
Static Subnet Mask	255.255.255.0
Static Default Gateway	192.168.2.254
Static DNS Server	168.95.1.1
Transmit Timer	10

Server:

Server Listening Port	5000
-----------------------	------

- **COM1 Setting:** Recommend use default °
- **Network Setting:**
 - **Enable DHCP:** Administrator can select enable or disable DHCP client.
 - **Static IP Address:** Administrator can set IP address for SP-800.
 - **Static DNS Server:** Administrator can set IP address for DNS server. °
 - **Transmit Timer:** system to detect controller connect status (millisecond).
 - **Server Listening Port:** SP-800 connection to controller use Port. (SP-800 and controller must be set the same port).

After setting is complete, please click Apply button.

Install normal thermal printer

Install step for thermal paper

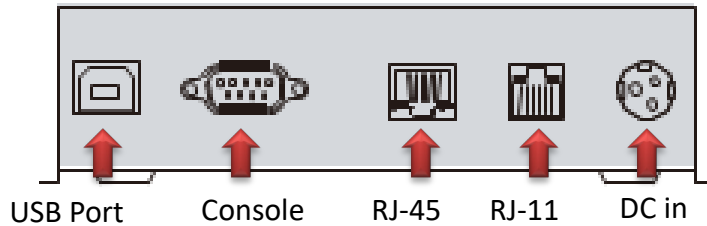
- 1) Open the cover for thermal printer
- 2) Place the thermal paper in the printer groove
- 3) After pull the paper out a small portion please close the lid for thermal printer



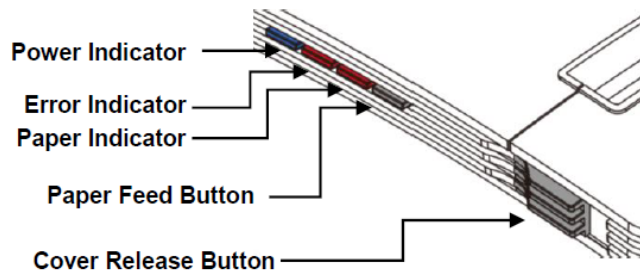
- 1) SP-800 connection to thermal printer use console port
- 2) DC Power in.
- 3) Power on/off switch.

Install QR Code thermal printer

Behind the printer connection functions support USB / console / RJ-45 / RJ-11 and Power.
As follows



PS. Connect the controller only need to use RJ-45 and power.

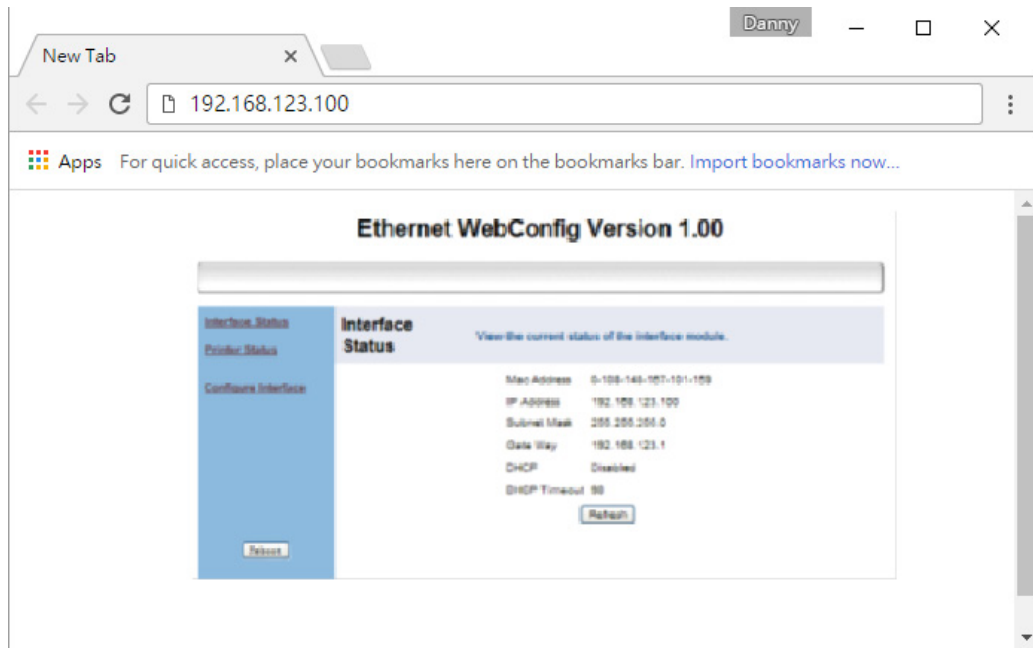


Login web page for QR Code printer.

The QR Code printer support web management interface, administrator can login web page and modify IP address for the QR Code printer.

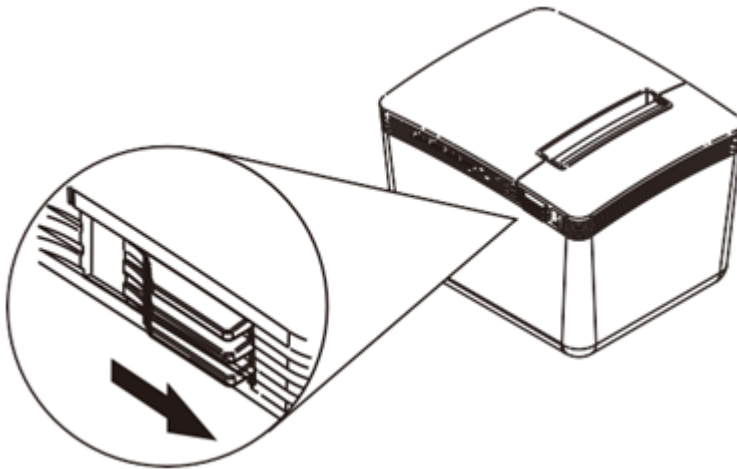
QR Code Printer default IP address: **192.168.123.100**

As follows

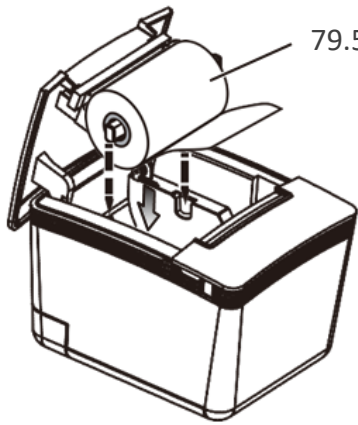


Install or Replace Paper Roll for QR code printer

- 1) Pull the Cover Release Button to open the Cover.

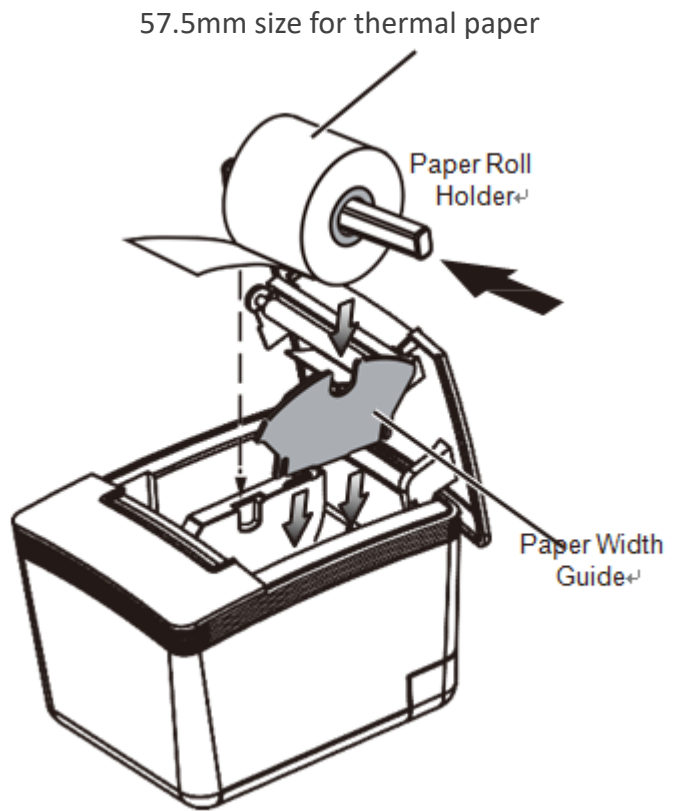


- 2) Roll out and install the Paper Roll with Holder into the Printer. (with the edges of the paper roll holder fitted onto the holder slots)



79.5mm size for thermal paper

When using a paper roll in smaller width, install the Paper Width Guide first, and then install the paper roll with holder.



57.5mm size for thermal paper

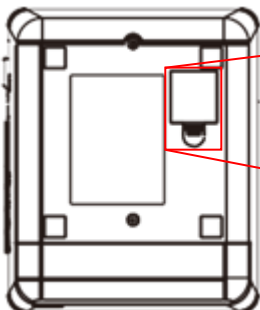
Paper Roll Holder

Paper Width Guide

3) Please close the lid for thermal printer.

DIP Switch Setting for QR code Printer

DIP Switch in printer bottom.



DIP	Function	ON	OFF
-----	----------	----	-----

1	Paper Cutter	No	Yes *
2	Audio Alarm	Yes *	No
3	Print Density	Dark	Light *
4	Two-byte Character Code	*No	Yes
5	Character Per Line	42	48 *
6	Cutter with Cash Drawer	Yes	No *
7 & 8	Baud Rate Setting	---	OFF*

Baud Rate Setting (DIP 7, DIP 8)



Set web authentication steps for POS system

Cerio's Web Authentication System consists of the controller and SP-800 + Printer; administrator can use SP-800 remote control Cerio's controller to create an account and print out. The architecture can refer to "POS system application" description

Set web authentication steps, as follows

(Take Cerio's **DR-4000** as the case)

Steps1

Login SP-800 web interface to set IP address and set same network segment
You can refer to "Login management interface for SP-800"

Steps2

If SP-800 with QR code Printer, administrator must set IP address for QR code Printer (same network

segment for your network). You can refer to “Install QR Code printer”

Steps3

Login Cerio’s Controller “**DR-4000**” page (Refer controller user manual) to enable RADIUS Server.

As follows

Please click menu “**Account**” → “**RADIUS Server**” for Cerio’s **DR-4000**

 Radius Server

Service

☒ Enable ☐ Disable






Authentioation Port

Aooounting Port

Radius Seoret

Steps4

Set the connection between **DR-4000** and SP-800. Please click menu “**Account**” → “**Thermal Printer Setup**” to enable function, as follows

Thermal Printer List					
Printer#	Service	IP Address	Description	Balance Time	Action
1		192.168.2.253		00:00	<div>Setup</div>
2				00:00	<div>Setup</div>
3				00:00	<div>Setup</div>
4				00:00	<div>Setup</div>
5				00:00	<div>Setup</div>

Printer Setup

Service ☒ Enable ☐ Disable

Printer Setup

IP Address: 192.168.2.253

Command Port: 5000

Printer Type: Normal Thermal Printer

COM Port: COM1

New Look Password: 1234

Description:

Balance Time: 00 00

- **IP address:** Please enter IP address for SP-800 (You can refer to Login SP-800)
- **Command port:** Please enter Command for SP-800 (You can refer to Login SP-800)
- **Printer Type:** Administrator can select Printer for normal or QR Code Printer.
- **QR code Printer :** If select QR Code printer, administrator must choose use connection for IP address or com Port.(Recommend use IP address manner.)

Printer Type: QRCode Thermal Printer

COM Port: RJ-45

Printer IP Address: 192.168.2.252

Printer Port: 9100

QRCode Type: Small

- ✓ **Printer IP Address :** Please enter IP address for QR code printer. (You can refer to Install QR Code Printer).
- ✓ **Printer Port :** Please enter command port for QR Code Printer. (You can refer to Install QR Code Printer)
- ✓ **QR Code Type :** Administrator can select print out size for QR code.
- **COM Port:** Please select connection type for printer.



1. If use normal thermal printer and connect to com1 port of the SP-800, please select COM1

2. If use QR Code Printer, please select RJ-45

- **New Lock Password** : Enter pass key of the **DR-4000** to connect SP-800
- **Description** : Administrator can enter description.

Steps5

Setup internet time rules for package authentication type (**DR-4000**). Please click menu “**Account**” → “**Package setup**”. As follows

- **Package Name:** Administrator can set Identify name for the package rules.
- **Description:** Administrator can set the description for package rules.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.
- **Session Time:** Administrator can set authentication account use session limit for the package rules. (After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.)
- **Expire After:** Administrator can set authentication account use how many hours expire.(After the account is signed in, the system start counted time until the end time.)
- **Expiration:** Administrator can select Unlimited or Per Day or Until Time.

- ✓ **Unlimited:** After the account is signed in, the system does not count the time
- ✓ **Per Day:** After the account is signed in, the system start counted time until the end time.

- ✓ **Until Time:** After the account is signed in, the system will begin counting until the set time is used up. The counting will stop when users log out, and begin counting again once the user signs back in.

Account Rule

User Name Length

(3-16)

User Name Type

☐ Digit
☐ Letters
☐ Mix

☐ No L/I/1
☐ No O/0
☐ No U/V

Password Length

(4-16)

Password Type

☐ Digit
☐ Letters
☐ Mix

☐ No L/I/1
☐ No O/0
☐ No U/V

PS. Package list (0~9) is Network control server (SP-800) code, administrator can choose number to print out account.

Package List							Create New Package
#	Name	Description	Session Time	Traffic Volume	Expire After	Expiration	Action
0	TEST-1	no time		0B			Edit
1	test-2	50Mbps Traffic		50.00MB			Edit
2	test-3	use 120 minutes time	2Hour(s)	0B			Edit
3	Test-4	use 120 minutes expl...		0B	2Hour(s)		Edit

Steps6

The system time is very important, administrator must set system time is right. Please click **DR-4000** menu **"System" → "Time Server"** to set system time.

PS. Recommend select update the system time for the NTP Server

The above procedure will complete the **DR-4000** setting

Enable Web authentication for Access Point

Hot spots web authentication architecture must be with combine Cerio's CenOS5.0 access point. As follows

Steps7

Enable Web authentication for Cerio's CenOS5.0 Access Point. (You can refer user manual for Access Point), As follows for Cerio's Access Point.

- 1) Enables web authentication function. Please click "System" → "Authentication" for Cerio's Access Point.

#	VLAN Mode	Authentication	Action
0	On	Off	Authentication
1	Off	Off	Authentication
2	Off	Off	Authentication
3	Off	Off	Authentication
4	Off	Off	Authentication
5	Off	Off	Authentication
6	Off	Off	Authentication

- 2) Click Authentication button and enable the function.

- 3) Enable authentication for RADIUS Server and set IP address for **DR-4000**.

Radius Setup

Radius ☒ Enable ☐ Disable

Display Name

Primary Server IP

Secondary Server IP

Authentioation Port

Accounting Servioe ☒

Authentioation Type ☐ PAP ☒ CHAP

Secret Key

Steps8

Set system time for Cerio's Access Point. Please click menu "System" → "Time server".

Steps9

The system time is very important, administrator must set system time is right. Please click menu "System" → "Time Server" to set system time.

System Time

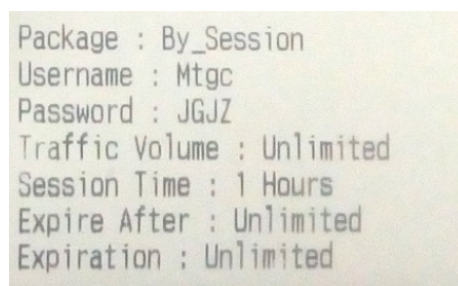
Local Time

Mode ☒ NTP Server ☐ Manual

This completes all architecture settings

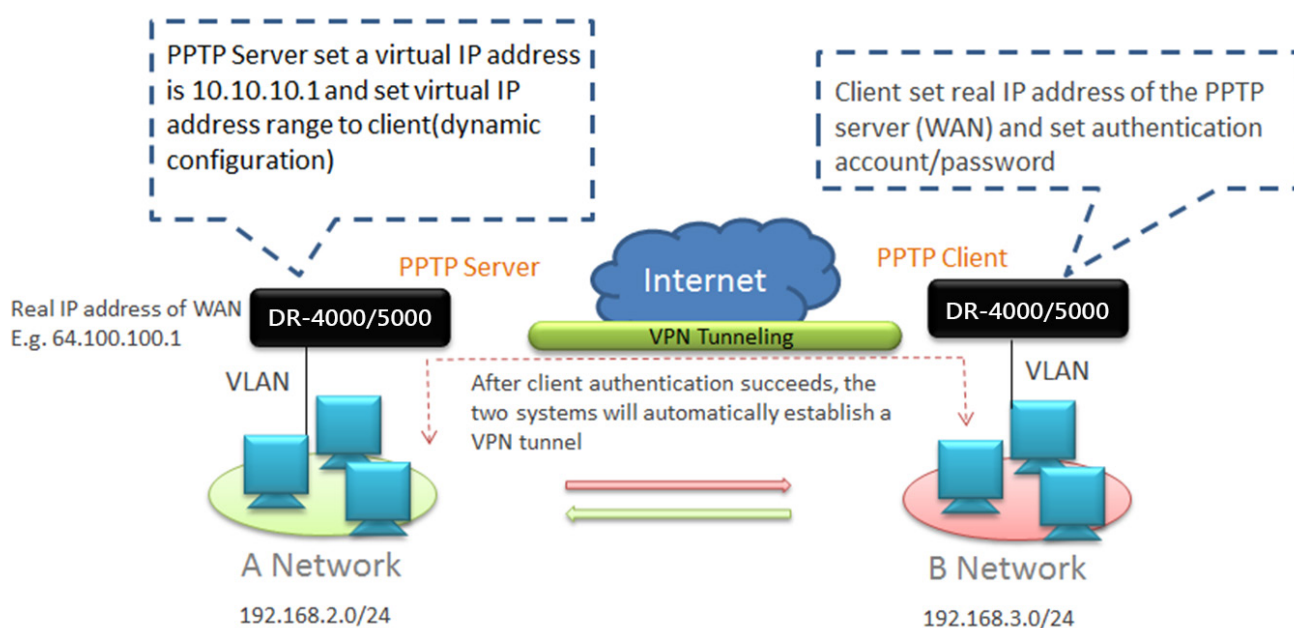
Administrator can click SP-800 "Print" button will print account and password of the tickets.

As follows



8.2 Example for PPTP/L2TP setup

Create a VPN tunnel use server / client bridge for the PPTP / L2TP protocol, if PPTP server set virtual IP address is 10.10.10.1 then must also set start to end IP address for dynamic configuration, can give VPN client automatically obtain a virtual IP address. The following concept map



PPTP Server setup step

1. Enable PPTP/L2TP Server and set VPN used virtual IP address.
(Refer to 3.6 /3.7 for instructions)

PPTP Server Settings

Connections	<input type="text" value="3"/>
Local IP Address	<input type="text" value="10.10.10.1"/>
Remote Start IP Address	<input type="text" value="10.10.10.10"/>
Remote End IP Address	<input type="text" value="10.10.10.13"/>
MPPE40	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MPPE128	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

2. Create authentication of client account and password

Account Setup

User Name

Password

PPTP Support

☒ Enable
 ☐ Disable

L2TP Support

☒ Enable
 ☐ Disable

Setup routing between the two networks

Routing Rule

Local Subnet

Remote Subnet

Add

PPTP Client setup step

- Set real IP address of remote VPN server and authentication account / password.

PPTP/L2TP Client Setup

Active

☒ Enable
 ☐ Disable

PPTP/L2TP Client Settings

Mode

☒ PPTP
 ☐ L2TP

Server IP Address

User Name

Password

PPTP Setup

MPPE40

☒ Enable
 ☐ Disable

MPPE128

☒ Enable
 ☐ Disable

2. Setup routing between the two networks

Routing Rule List

#	Local Subnet	Remote Subnet	Action
1	192.168.3.0/24	192.168.2.0/24	Delete

When the setting is complete, the both of the network will be through the VPN tunnel for data transmission.

Administrator can track the discovery, both network is used VPN tunnel to transmission.

```
Tracing route to 192.168.2.10 over a maximum of 30 hops
```

```
  1  <1 ms  <1 ms  <1 ms  192.168.3.1
  2  10 ms   9 ms   9 ms  10.10.10.1
  3  10 ms   9 ms   9 ms  192.168.2.10
```

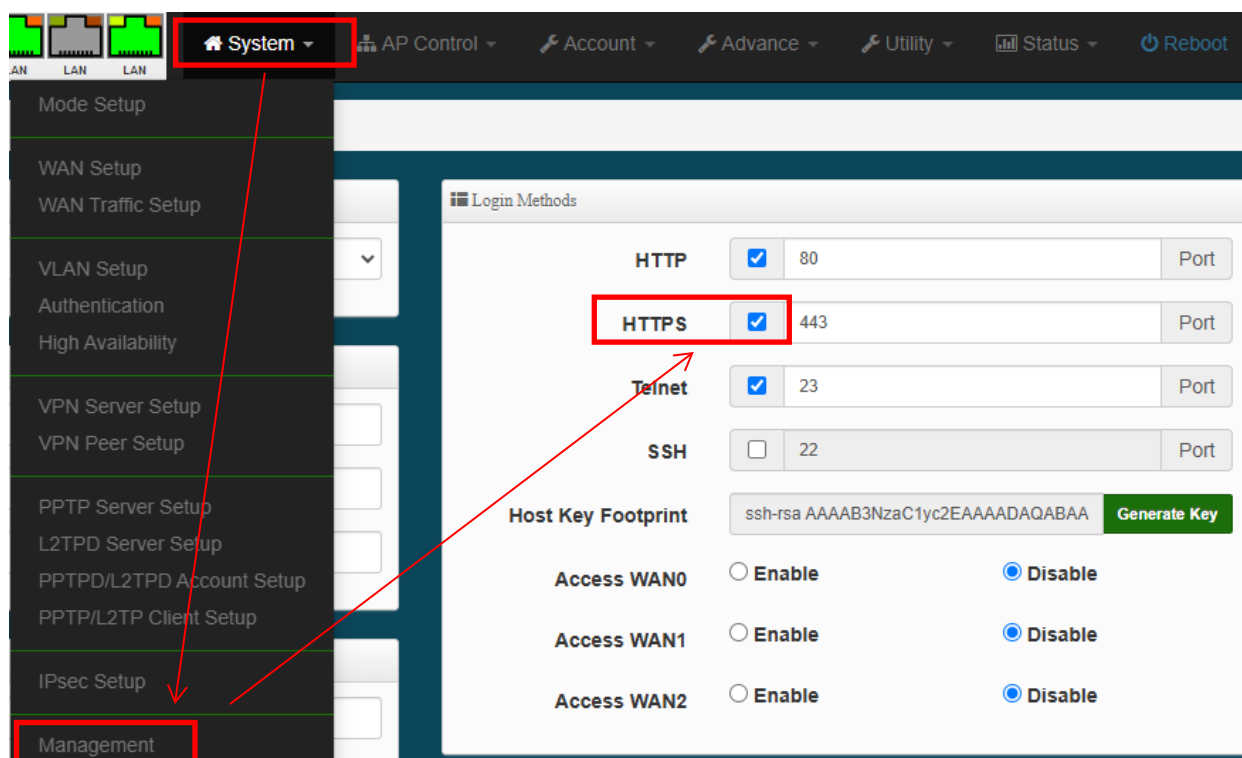
```
Trace complete.
```

8.3 Example for Web Authentication Portal URL using HTTPS

If the [Authentication Web Captive portal login page] is set up without using the traditional HTTPS web transmission protocol as the URL, the key steps on how to import the SSL certificate to complete the setting of the [Authentication Web Captive portal login page] using the HTTPS secure transmission mechanism are as follows:

Steps1

Make sure the https secure transmission management function is enabled. For this function, please go to "System " → "Management" and check the HTTPS management option to enable it.



Note that in addition to enabling the https secure transmission function, you need to have a main domain or subdomain URL, and also obtain an SSL certificate for the relative domain URL. If it is enabled without importing the SSL certificate, it will cause "User Every time the browser used by the computer (including computer browsers and browsers on all handheld devices) enters the [Authentication Web Captive portal login page], the browser will not be able to use HTTPS secure transmission normally because the https URL list does not have an SSL certificate. The browser interface operated by the user will automatically be deemed as "untrusted or unsafe" and other related pop-ups or display windows.

Steps2

In order to comply with the basic premise that the SSL certificate needs to verify the domain owner, please make sure that the "login URL address" you want to set is a domain name that is registered and actually owned by the domain. It is recommended to use the name of your

organization/unit/ Add a set of exclusive "subdomain" URL names under the existing web server main domain URL of the company/location (for example, the main URL is the cerio.cc URL) as the exclusive URL for the [Authentication Web Captive portal login page] , (for example, in the example below, the mcs.cerio.cc URL is used as the [Authentication Web Captive portal login page]exclusive URL) to truly distinguish the web server URL outside the WAN from the [Authentication Web Captive portal login page]URL within the LAN.

Authentication

Authentication ☒ Enable ☐ Disable

Authentication Setup

Multiple Login ☒ 3 User(s)

Login Timeout 10 Minutes

Redirect URL http://www.google.com

Login URL mcs.cerio.cc

Authentication Log ☐ Enable ☒ Disable

Session Log ☐ Enable ☒ Disable

After the web authentication function is enabled, this device will automatically translate the website name of the "login URL address" into a LAN IP address in a LAN environment. For example, the default LAN IP address used by this device and interface is 192.168. 2.1 address, and after setting the URL name of "Login URL Address" to the "mcs.cerio.cc" address, pinging the "mcs.cerio.cc" URL in a LAN environment is equivalent to Ping 192.168.2.1 (LAN IP address of this device).

Steps3

Use notepad to open the text content in the certificate information (Cert/CRT) file, private key (Privkey/Key) file, and relay certificate (Chain/CA Bundle) file respectively, copy and paste them. Consolidated into a single credential archive file.

The format type of the certificate (archive file) depends on the certificate unit that is issued. If the SSL certificate of the unit that is issued does not have a relay certificate (Chain/CA Bundle), please ignore it and there is no need to incorporate it.

The free software Notepad++ (plain text/code editor) is used as the editing display of plain text below. The merged certificate content (displayed with regular alphanumeric characters) and format legend of multiple certificate files are *and omitted* displayed as follows:

-----BEGIN CERTIFICATE-----

MIIGYzCCBUugAwIBAgISBNlgjGu4j6a0HYl5zqwixb4kMA0GCSqGSIb3DQEBCwUA

MDMxCzAJBgNVBAYTAIVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXBOMQww.....and omitted

-----END CERTIFICATE-----

If there is "-----BEGIN CERTIFICATE-----" in the SSL certificate file opened as above, it means that it is a certificate information or a relay certificate.

-----BEGIN PRIVATE KEY-----

MIGHAgEAMBMGBYqGSM49AgEGCCqGSM49AwEHBG0wawIBAQqT+M0dVmQOx6kUqQr

LisIRau2XKztqDgCn/VTqe0Mom2hRANCAAQ+6vD8vf6J1sWVHxECvqZIN9FeG3dU.....and omitted

-----END PRIVATE KEY-----

If the SSL certificate file opened above contains "-----BEGIN PRIVATE KEY-----", it means that it is a private key certificate.

The numerical and alphabetical content in the following certificate file is shown in a *and omitted* example legend. It can be integrated and edited into a file file and then archived to be imported and used by this device.

The screenshot shows a Notepad++ window with the following content:

```

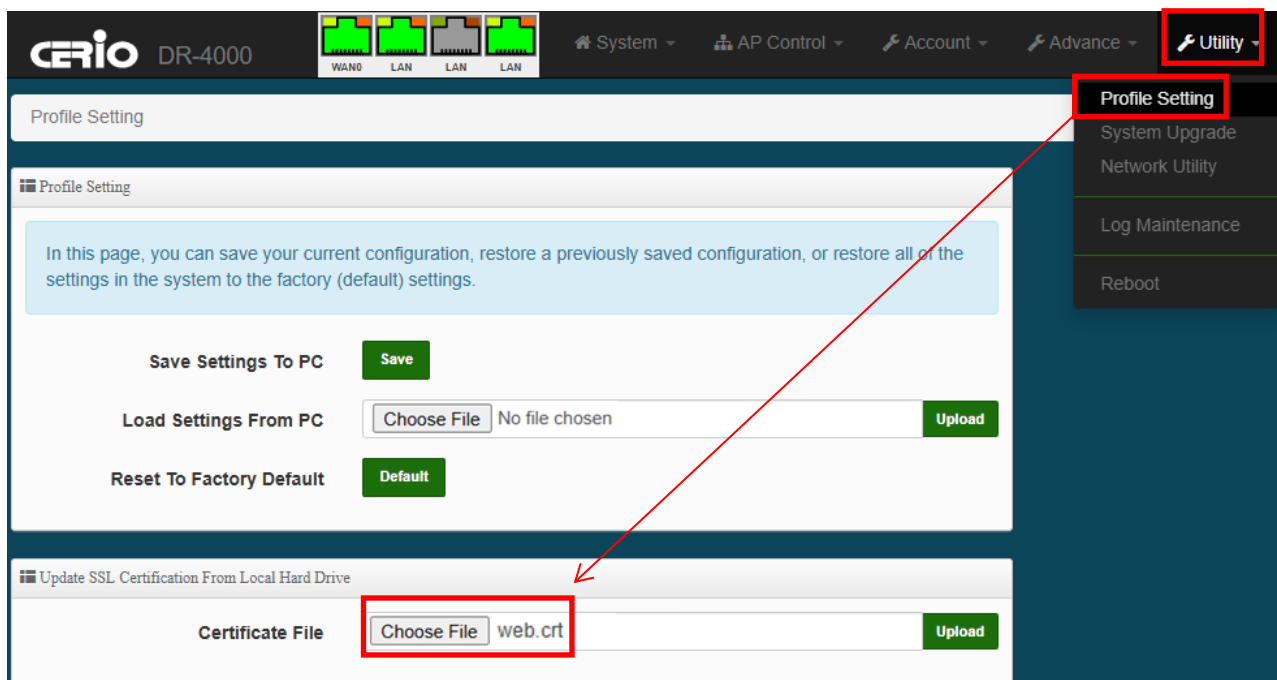
1  -----BEGIN CERTIFICATE-----
2  MIIGYzCCBUugAwIBAgISBNlgjGu4j6a0HYl5zqwixb4kMA0GCSqGSIb3DQEBCwUA
3  MDMxCzAJBgNVBAYTAIVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXBOMQwwCgYDVQQD
4  EwNSMTEwHhcNMjQxMDEwMDczNjM3WhcNMjQxMDEwMDczNjM3WjATMREwDwYDVQQD
5  e19KUwQUZURhy5j/PEdEglKg3l9dtD4tuTm7kZtB8v32OjzHTYw+7KdzdZiw/sBtn
6  tlr2BqelHsick7F+E17nNh/CW5aJIYJZFfrQkvmeleVET1OzdeP2QgsmUIQKbIYz
7  pdWfs6PJ1jty80r2VKsM/Dj3YIDfbjXKdaFU5C+8bhfJGqU3taKauuz0wHVGt3eo
8  K2OQ9a1KgL96s/lnAa0Z6zEaMbFpGHJ0aud+gT8kaTc24x+bf7REB5nZ4MtS7sLr
9  gQ5vFfnHzg==
10 -----END CERTIFICATE-----
11 -----BEGIN CERTIFICATE-----
12 MIIFBjCCAU6gAwIBAgIRAIp9PhPWLzDvI4a9KQdrNPgwDQYJKoZIhvcNAQELBQAw
13 TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
14 cmNoIEdyb3VwMRUwEwYDVQQDEw1UJHIFJvb3QgWDEwHhcNMjQxMDEwMDczNjM3
15 q1S0qcYhyOE2G/93ZCkXufBL713qzXnQv5C/viOykNpKqUgxdKlEC+Hi9i2DcaR1
16 PBuHRTrrrrKlyDnkSHDHYPiNX3adPoPacgdF3H2/W0rmoswMWgTln1Wu0mrks7/q
17 6FlWkWYtbt4pgdamlwVeZEW+LM7qZEJEsmNPrfC03APKmZsJgpWCDWOKZvk2cvjV
18 uYkQ4omYCTX5ohy+knMjdOmdH9c7SpqEWBDC86fiNex+00XOMEZSa8DA
19 -----END CERTIFICATE-----
20 -----BEGIN PRIVATE KEY-----
21 MIEvAIBADANBgkqhkiG9w0BAQEFAASCByYwggSiAgEAAoIBAQCroZa0K9s+1/oM
22 BEwd4zETNsgKKOL57t9FfMmiV6w/PUV+pld/nvSm/UjU4UngnKJvXAcrlfPG6q4U
23 hpDnq3nIBn4I3Hb0kfJSLbr9hCfY2t7BqyNJAeCCGF/hqPC7r+ygYmSFKzWtbRrT
24 Uw7CLCbNrBZYCce3/oZg93s56NwJksaoFJU8Eo9wmr07RVEArgv6dOrKBpLnjy3+
25 JyrHruLgT2Aa+r15fFG9epWjtzB8bbySBLqeC9lh1S+zaimrhaCGmc6zb09/hPOL
26 uHP8pl1lcWc28Bhi3lWcJLDq/bndfPO7yYjHoECgyBFc4qPz5xmkt1Lsj0byPBD
27 7NzG915y74ULRSTRqCSNte3Or2KgElsmQfBAdLUEkyln22Tiec3Sx+ahzCLbspPJ
28 oPN7KT4HWikVGqf20Xr0rw==
29 -----END PRIVATE KEY-----
30

```

Instructions from the diagram:

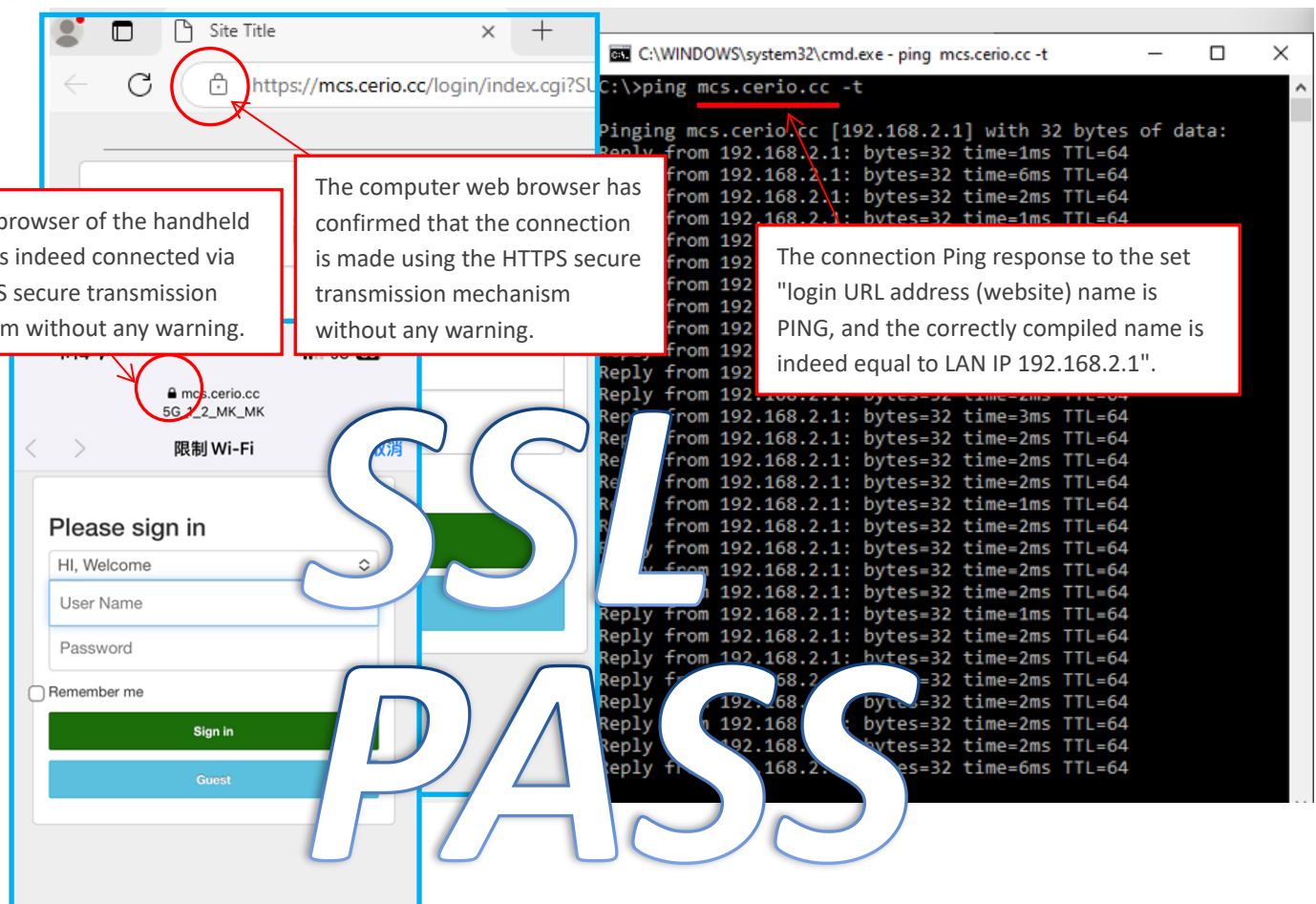
- Copy and paste the text content of the certificate information (Cert/CRT) file to edit and arrange it here.
- Copy and paste the text content of the Chain/CA Bundle file to edit and arrange it here.
- Text content of the private key file, copy and paste the edited arrangement here.

Please go to "Utility" → "Profile System" → "Update SSL Certification From Local Hard Drive" in the UI interface of this device to upload and import the obtained SSL certificate file. You must merge the text contents of the multiple certificate files you have. into a file file for smooth uploading and importing. The following is edited and merged and saved as the file name "web.crt" and temporarily saved on the computer. Then upload the "web.crt" certificate file as the file to upload the SSL certificate from the computer. After completion Allow the system to restart for the settings to take effect.

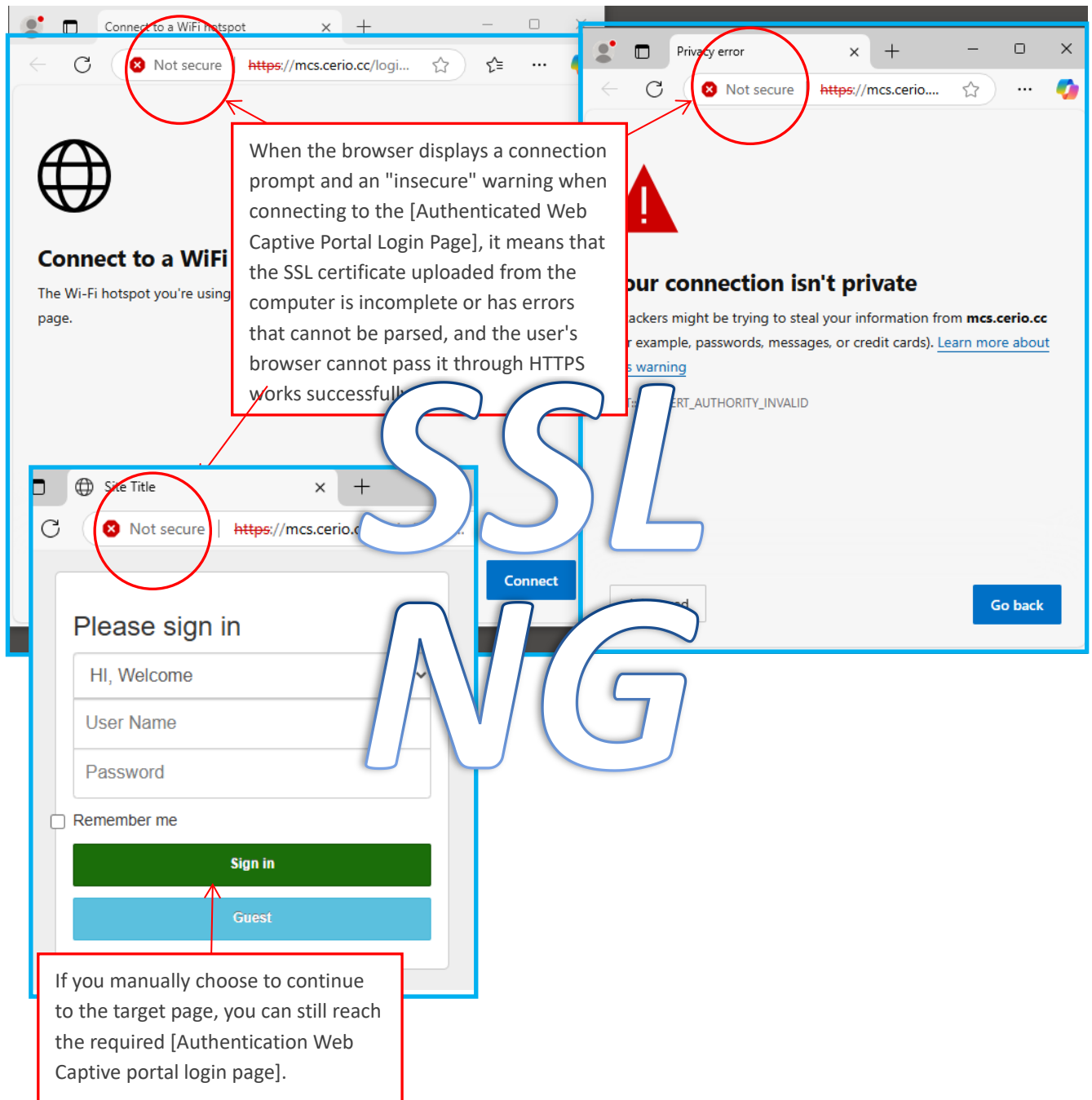


Verify the setting results:

After restarting for the settings to take effect, you can try to enter the [Authentication Web Captive portal login page] using the browser operated by the user to check that https secure transmission is in operation. You can also use MSDOS to operate the PING command to check the login URL of mcs.cerio.cc The PING address (website address) has been successfully responded to correctly.

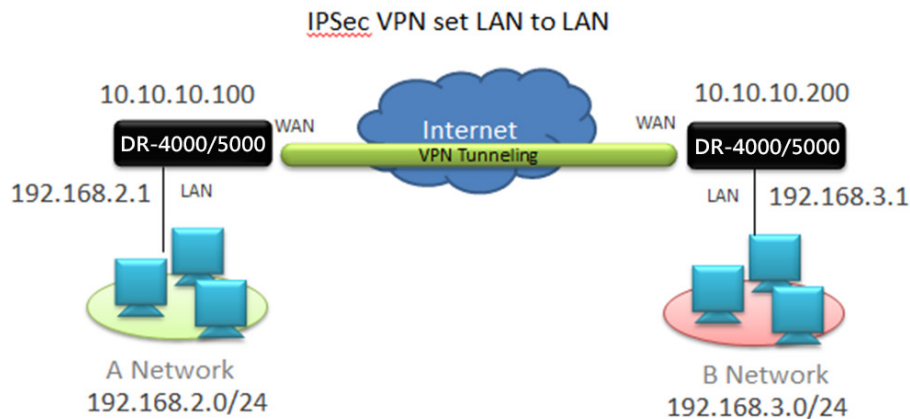


After restarting for the settings to take effect, if the browser that the user is trying to operate enters the [Authentication Web Captive portal login page] and the browser jumps out the following message, it means that the credentials are incorrect or the upload failed, and the browser cannot correctly parse the settings. The URL name of "Login URL Address" and the required SSL certificate content must be obtained accordingly. As shown in the figure below, an "Insecure" prompt will be displayed. **Please double-check whether the certificate content obtained in steps3 and the upload and import operation are correct. question.**



8.4 Example of setting up IPsec VPN set LAN to LAN

Use DR-4000/DR-5000 series router to establish IPsec VPN set LAN to LAN allows different regional networks to become a shared network over the Internet.



Using Router mode to set up IPsec

Connect network cable to the LAN port, change computer to static ip address 192.168.2.*(2-254), After entering the DR-4000/DR-5000 series device UI setting interface from 192.168.2.1, Click "**System > Mode Setup**" to confirm that the system mode is in Router mode. The steps are as follows:



Step-1: We take two sets of Router(two environments) with different LAN segments as a sample case, and set the LAN IP of the two routers to different network segments.

Click the "**System > VLAN Setup > Network**" management page to set the LAN IP of two Routers (two environments) on different network segments, the default LAN IP of the Router is

192.168.2.1. Set the IP address so that the LAN IP of the A Network and the B Network will be separated into two segments, and then use the changed IP address after the setting is saved. The subnet mask is the same as 255.255.255.0. Select the specified port as WAN0.

	IP Address	Netmask	Specify WAN Port
Router A	192.168.2.1	255.255.255.0	WAN 0
Router B	192.168.3.1	255.255.255.0	WAN 0

Confirm Router A :

Confirm Router B :

Step-2: Set up the DHCP server, and let the DR-4000/DR-5000 series be responsible for DHCP server to assign IP addresses to the LAN.

Click the “VLAN Setup > VLAN 0>DHCP server” management page and enable the DHCP service. The router is responsible for allocating the LAN IP address to the connected user computers. The default IP range of DHCP server is 192.168.*.10~192.168.*.100. The subnet mask is the same as 255.255.255.0, and the default gateway and primary DNS server address are both set to the router's LAN IP.

After saving the configuration and restarting the router, you must set the user computer (DHCP client Users) to “Obtain IP address automatically”, so that the user computer can automatically

obtain the IP address assigned by the router.

The following as example:

	Start IP	End IP	Netmask	Gateway	DNS 1 IP
Router A	192.168.2.10	192.168.2.100	255.255.255.0	192.168.2.1	192.168.2.1
Router B	192.168.3.10	192.168.3.100	255.255.255.0	192.168.3.1	192.168.3.1

Confirm Router A :

Confirm Router B :

The interface for Router B shows similar configuration. The 'DHCP Service' section has 'Mode' set to 'Enable' (highlighted with a red box). The 'DHCP Setup' section has 'Start IP' (192.168.3.10), 'End IP' (192.168.3.100), 'Netmask' (255.255.255.0), 'Gateway' (192.168.3.1), and 'DNS1 IP' (192.168.3.1) all highlighted with a red box. The 'DHCP Client List' table shows one client with IP 192.168.3.10 (highlighted with a red box) and a green 'Fixed' button.

Step-3: Set up PPPoE (WAN/Internet) Internet connection for the environment and confirm the host public IP address

Here is the most common PPPoE as example, enter the “**System > WAN Setup**” page, set the DNS, and click “Edit” to set the connection mode of WAN 0 as PPPoE dial-up connection.

For each of the router in two environment, enter DNS1 : "8.8.8.8" (Google's public DNS server address), and DNS2 : "168.95.1.1" (Chunghwa Telecom DNS server).

Select "PPPoE" as the WAN Mode, enter the username and password provided by the Internet Service Provider (ISP), and remember to enable NAT (if you choose not to enable NAT, it will be a transparent Bridged passthrough that directly uses a WAN IP to connect to the outside world, and you will not be able to build a virtual LAN (and therefore cannot virtualize multiple computers NAT to connect to the Internet)).

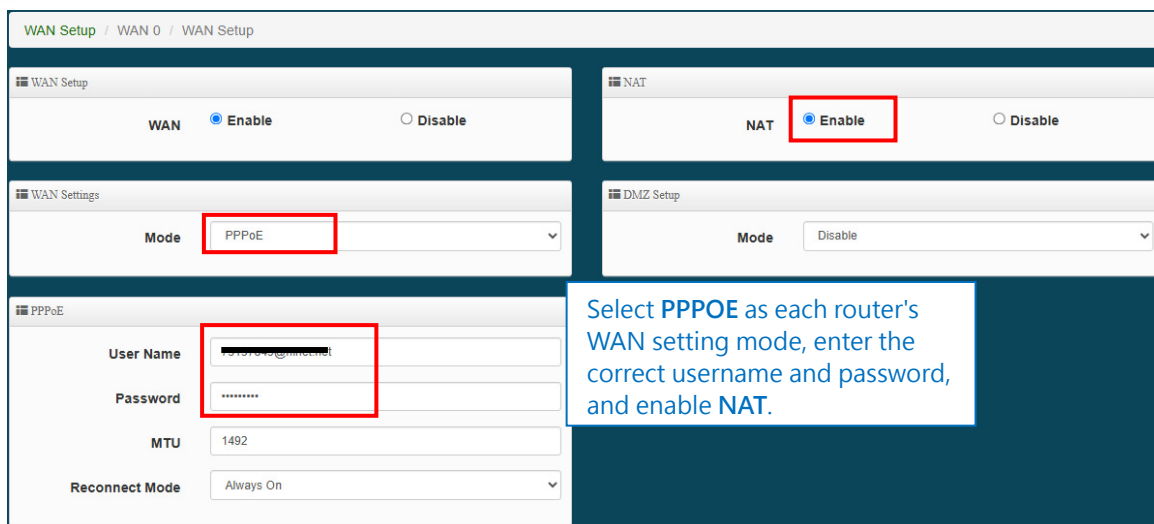
After saving the configuration and reboot, enter the interface and click " **System > Overview** " to check the WAN IP provided by PPPoE. This IP is the public IP address of the router. At this time, the computer can connect to the Internet through the DR-4000/DR-5000 series.

It is recommended to use static IP for both routers in the environment. For example, use " PPPoE With Static IP Assignment "

The following example:

	WAN Settings	NAT	WAN IP(PPPoE Static IP)
Router A	PPPoE	Enable	125.228.249.38
Router B	PPPoE	Enable	36.277.192.118

The example sets the input DNS to 8.8.8.8 and 168.95.1.1, and ensures that each router is configured with the same settings.



WAN Setup / WAN 0 / WAN Setup

WAN Setup

WAN ☒ Enable ☐ Disable

NAT

NAT ☒ Enable ☐ Disable

WAN Settings

Mode **PPPoE**

PPPoE

User Name

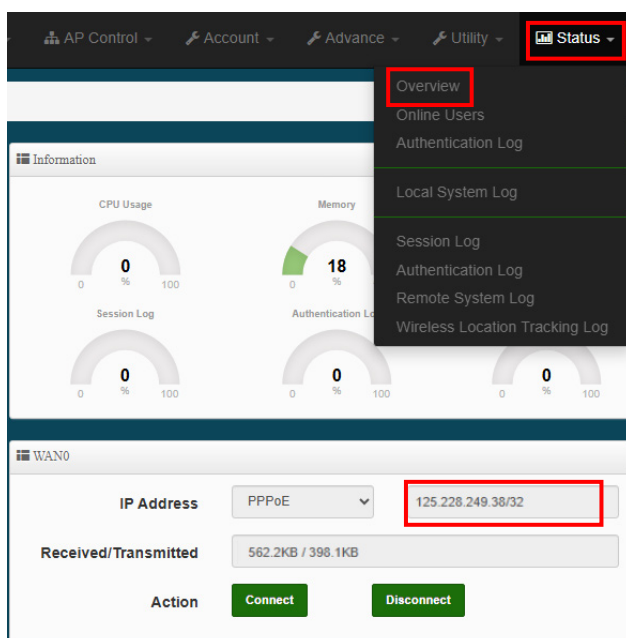
Password

MTU

Reconnect Mode

Select PPPOE as each router's WAN setting mode, enter the correct username and password, and enable NAT.

Confirm Router A :



AP Control Account Advance Utility **Status**

Overview
Online Users
Authentication Log
Local System Log
Session Log
Authentication Log
Remote System Log
Wireless Location Tracking Log

Information

CPU Usage **0** %
Memory **18** %
Session Log **0** %
Authentication Log **0** %

WAN0

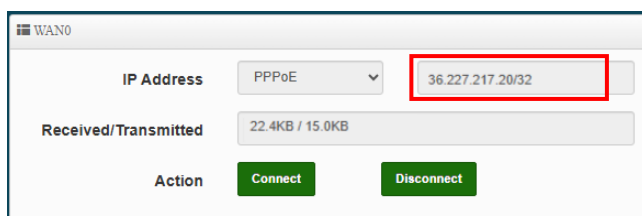
IP Address **PPPoE** **125.228.249.38/32**

Received/Transmitted **562.2KB / 398.1KB**

Action **Connect** **Disconnect**

Check the WAN IP (outward-facing IP address) assigned to Router A by ISP via PPPOE.

Confirm Router B :



WAN0

IP Address **PPPoE** **36.227.217.20/32**

Received/Transmitted **22.4KB / 15.0KB**

Action **Connect** **Disconnect**

Check the WAN IP (outward-facing IP address) assigned to Router B by ISP via PPPOE.

Step-4: Set IPSec VPN parameters, shared authentication and key must keep consistent

Click "System > IPSec Setup", and then "Creat new IPSec". Enter the settings for each of the routers on the A side and the B side in two different environments, and make sure that both sides use the same authentication and key. (If the settings are inconsistent, the VPN connection will

not be established).

Enter “**IPSec Setup > IPSec 0**” page, Configure the IPSec VPN parameters of router :

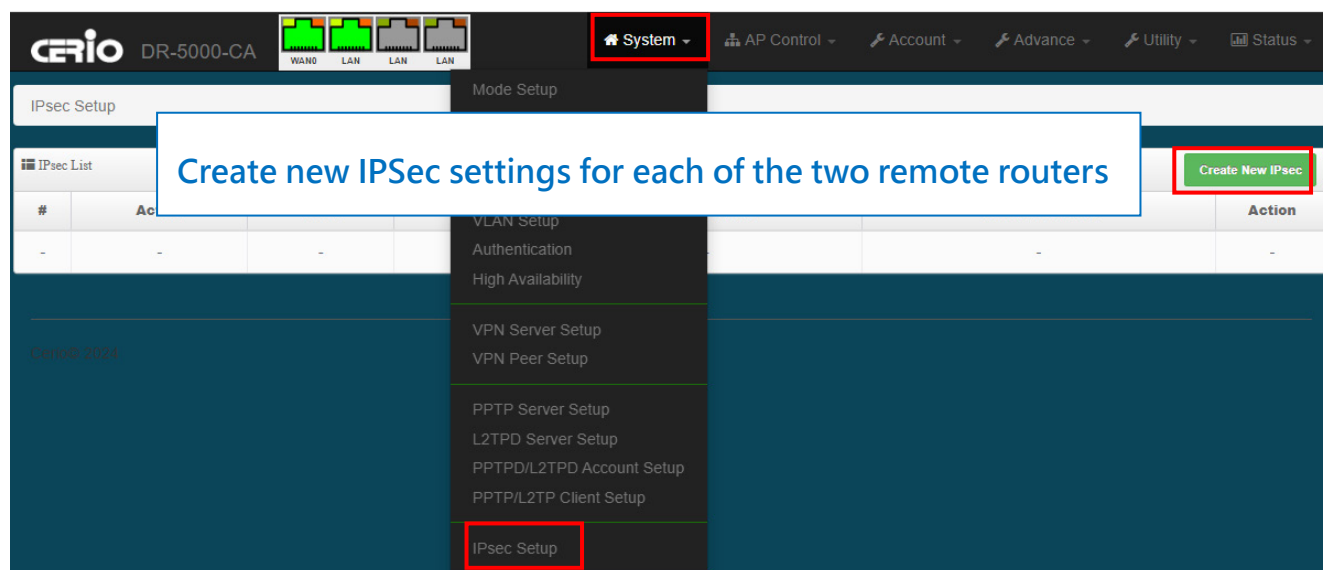
Enable IPSec service, select **LAN-to-LAN** for Mode , select **WAN 0** for WAN interface, select **IP address** for ID type, and Nexthop can be set to 0.0.0.0. Check whether the basic configurations of the two site routers are matched: Remote Host (the other side WAN IP), Local Subnets, Remote Subnets, pre-shared key and WAN interface.

Please note that the Local Subnets and Remote Subnets of the routers at both endpoints must correspond to each other, do not set the same settings at both endpoints. Keep the same Pre-shared Key (4~32 characters) for IKE negotiation at both router, and keep the rest of the settings as default.

After saving the settings and restarting, the two routers can establish a VPN channel, so that the virtual LAN IP users of router A and router B can exchange encrypted data and access the transmission, and users can also access the Internet at the same time.

The following as example :

	Local Subnets	Remote Subnets	Remote Host	Pre-shared Key
Router A	192.168.2.0/24	192.168.3.0/24	36.277.192.118	12345678
Router B	192.168.3.0/24	192.168.2.0/24	125.228.249.38	12345678



Router A :

IPsec List							Create New IPsec
#	Active	WAN	Mode	Local Subnet	Remote Subnet	Action	
1	On	WAN0	LAN-to-LAN	192.168.2.0/24	192.168.3.0/24	Edit	

Router B :

IPsec List							Create New IPsec
#	Active	WAN	Mode	Local Subnet	Remote Subnet	Action	
1	On	WAN0	LAN-to-LAN	192.168.3.0/24	192.168.2.0/24	Edit	

Confirm Router A :

IPsec Service

Service ☒ Enable ☐ Disable

IPsec Settings

Mode: LAN-to-LAN

WAN: WAN0

Local ID Type: ☒ IP Address ☐ FQDN

Local ID:

Local Subnets: 192.168.2.0/24

Local Nexthop: 0.0.0.0

Remote ID Type: ☒ IP Address ☐ FQDN

Remote ID:

Remote Subnets: 192.168.3.0/24

Remote Nexthop: 0.0.0.0

Remote Host: 36.227.217.20

Pre-shared Key: 12345678

DPD: ☒ Enable ☐ Disable

DPD Delay: 30

DPD Timeout: 120

IKE Policy

IKE Mode: ☒ Main ☐ Aggressive

IKE Authentication: MD5

Encryption: 3DES

DH Group: DH2

IPsec Policy

Security Protocol: ESP

ESP Authentication: MD5

ESP Encryption: 3DES

Perfect Forward Secrecy: ☐ Enable ☒ Disable

DH Group: DH2

Example settings for Router A:
 Local Subnets to 192.168.2.0/24,
 Remote Subnets to 192.168.3.0/24,
 Remote Host to 36.227.192.118
 Pre-shared Key to 12345678

Confirm Router B :

IPsec Service

Service ☒ Enable ☐ Disable

IPsec Settings

Mode LAN-to-LAN

WAN WAN0

Local ID Type ☒ IP Address ☐ FQDN

Local ID

Local Subnets 192.168.3.0/24

Local Nexthop 0.0.0.0

Remote ID Type ☒ IP Address ☐ FQDN

Remote ID

Remote Subnets 192.168.2.0/24

Remote Nexthop 0.0.0.0

Remote Host 125.228.249.38

Pre-shared Key 12345678

Example settings for Router B:
Local Subnets to 192.168.3.0/24,
Remote Subnets to 192.168.2.0/24,
Remote Host to 125.228.249.38
Pre-shared Key to 12345678

Step-4: Confirm IPsecVPN connection

After the router restarts, the two endpoints automatically establish a VPN encrypted channel through IPsec:

By tracing the route from the 192.168.3.0/24 domain (endpoint B) to the device at 192.168.2.0/24 (endpoint A), it is clear that both ends have been successfully routed through the VPN encrypted channel.

The following uses the CMD traceroute at the command "**tracert**" to trace the remote IP 192.168.2.10:

```
C:\Windows\system32\cmd.exe

C:\Users>tracert 192.168.2.10

Tracing route to 192.168.2.10 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  192.168.3.1
  2  *      *      *      Request timed out.
  3  3 ms   2 ms   6 ms  DESKTOP-PC [192.168.2.10]

Trace complete.
```

After configuring the IPsec function, if the two separate virtual LANs cannot communicate (i.e. the remote 192.168.2.X network user IP and the other remote 192.168.3.X network user IP

cannot ping or transmit to each other), there maybe the following reasons:

1. Please note that the encryption and decryption methods of the two remote settings maybe inconsistent.
2. Errors in basic IPSec settings: such as remote host, local subnets, remote subnets, pre-shared key and WAN interface settings.
3. Errors in the data transmission for defining IPSec encapsulation. You need to restart the IPSec service or restart the DR-4000/DR-5000 series host.