CERIO Corporation

DR-4000-CA

Multi WAN Gigabit AP Controller with Gateway Router

(128APs)

User's Manual

Default IP / Login Information	
IP Address	192.168.2.1
User Name	root
Password	default

1. Device and Software Configuration 6
1.1 Device appearance 6
1.2 Setup Preparation of Device 7
1.3 Login Web Page 9
2. Operating Mode Introduction 11
2.1 Control Mode 11
2.2 Router Mode 11
2.3 Captive Portal Mode 12
3. System Configuration 12
3.1 WAN Setup 12
3.2 WAN Traffic Setup 16
3.3 VLAN Setup 17
3.3.1 Network Button 19
3.3.2 Pull-down menu @ Bandwidth Control 20
3.3.3 Pull-down menu @ DHCP Server 21
3.4 Authentication(Hotspot Setup) 23
Authentication Button: 24
Authentication Dropdown Button 25
3.4.1 Guest 26
3.4.2 Local User 27
3.4.3 OAuth2.0 27
☐ # Sample for Google OAuth2.0 setup 27
☐ # Sample for Facebook OAuth2.0 setup 30
3.4.4 POP3 Server 34

3.4.5 Customize Page 34
3.4.6 Language 36
3.4.7 Walled Garden 36
3.4.8 Privilege Address 37
3.4.9 Profile 37
3.5 High Availability 38
3.6 VPN Server Setup 40
3.7 VPN Peer Setup 42
3.8 PPTP Server Setup 43
3.9 L2TP Server Setup 45
3.10 PPTP/L2TP Account Setup 46
3.11 PPTP/L2TP Client Setup 47
3.12 IPSec Setup 49
3.13 Management 52
3.14 Time Server 58
3.15 SNMP 59
3.16 DDNS 61
3.17 Log Server Setup 62
3.18 Notification Setup 64
4. AP Control 68
4.1 Scan Device 68
4.2 Batch Setup 70
4.3 AP Setup 71
4.4 Group Setup 73

4.5 Map Setup 74
4.6 Authentication Profile 77
4.7 Status 79
5. Account 80
5.1 RADIUS Server 80
5.2 Remote LDAP Setup 81
5.3 Package Setup 83
5.4 Create An Account 85
5.5 Search Account 86
5.6 Regenerated Tickets DB 87
5.7 Thermal Printer Setup 90
5.8 History Log 93
5.9 Online Log 93
5.10 Database Maintenance 94
6. Advance 94
6.1 IP Filter 94
6.2 IP Group 96
6.3 Port Group 97
6.4 MAC Filter 98
6.5 Virtual Server 99
6.6 Access Control 100
6.7 IP Routing Setup 102
6.8 IP Routing Rule Setup 104
6.9 Time Policy 105

7. Utility 106

7.1 Profile Setting 106

7.2 System Upgrade 108

7.3 Network Utility 109

7.4 Log Maintenance 110

7.5 Reboot 111

8. Status 112

8.1 Overview 112

8.2 Local System Log 112

8.3 Session Log 113

8.4 Authentication Log 115

8.5 Remote System Log 116

8.6 Wireless Location Tracking Log 117

9. Technical documents 120

9.1 Hotspot function used POS system application 120

Login management interface for SP-800 121

Install normal thermal printer 122

Install QR Code thermal printer 123

Set web authentication steps for POS system 126

9.2 Example for PPTP/L2TP setup 133

9.3 Example for Web Authentication Portal URL using HTTPS 136

9.4 Example of setting up IPSec VPN set LAN to LAN 142

1. Device and Software Configuration

1.1 Device appearance

1. **DC Jack Power interface** **(Power input- interface-1)**
2. **LED status indicator:**

	**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.
	**Fail LED :** System problem warning LED ,Operating system storage data cannot be accessed , (The light is always on when there is a fault).
	**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).
	**Ethernet port LED :** Link/Act connection LED from ETH1 port to ETH4 port

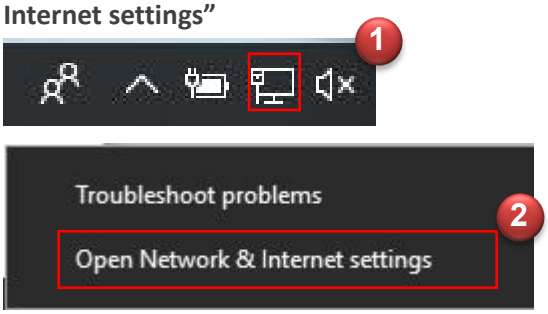
3. **Reset button** (to restore the factory default, please press it for about 10-15 seconds. The Online LED and Fail LED will flash at the same time, indicating confirmation. You can release the button and wait for the system to return to the factory default).
4. **Gigabit / ETH1 (POE) Ethernet port**, 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

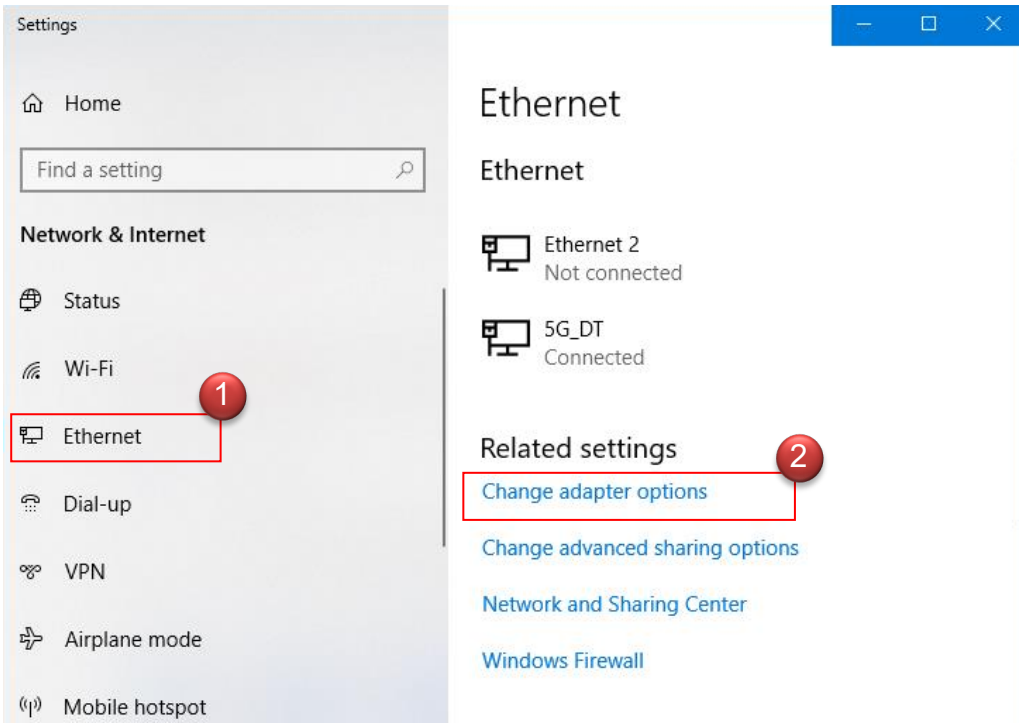
Please PC link to Device used cat5/6 Ethernet cable.

The following setup uses a Windows PC, user OS may vary.

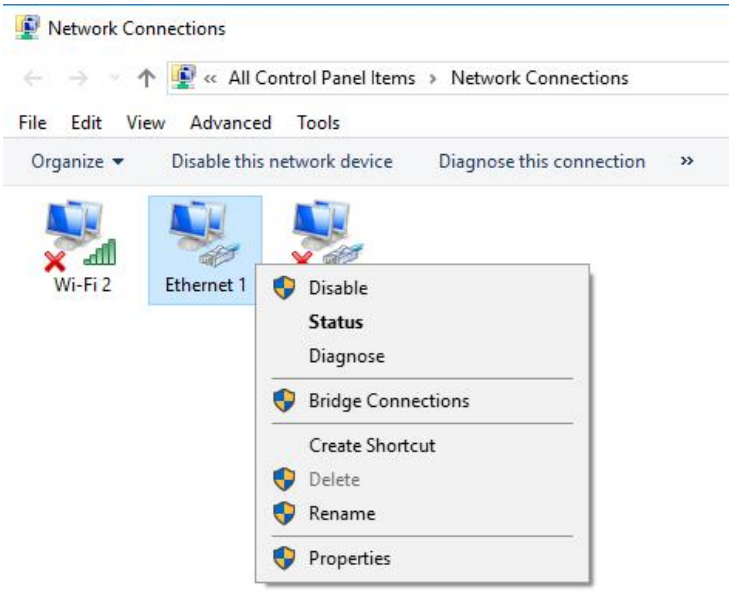
Step 1: Please click on the computer icon in the bottom right window, and click **"Open Network and Internet settings"**



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"**

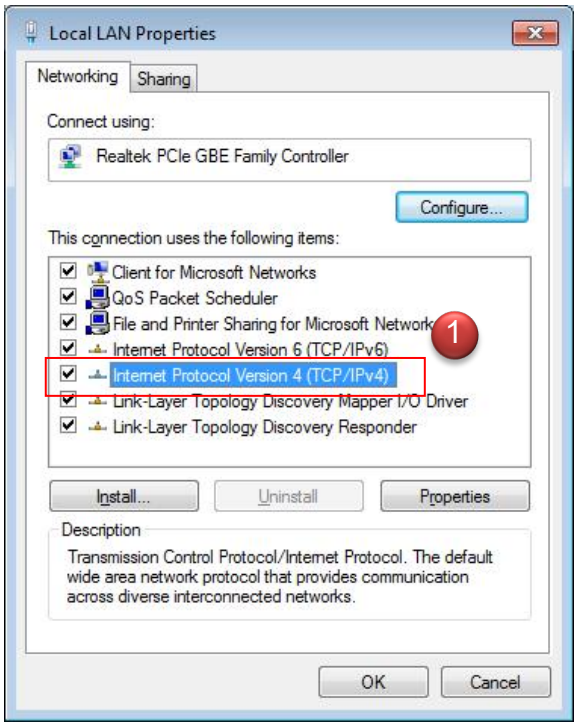


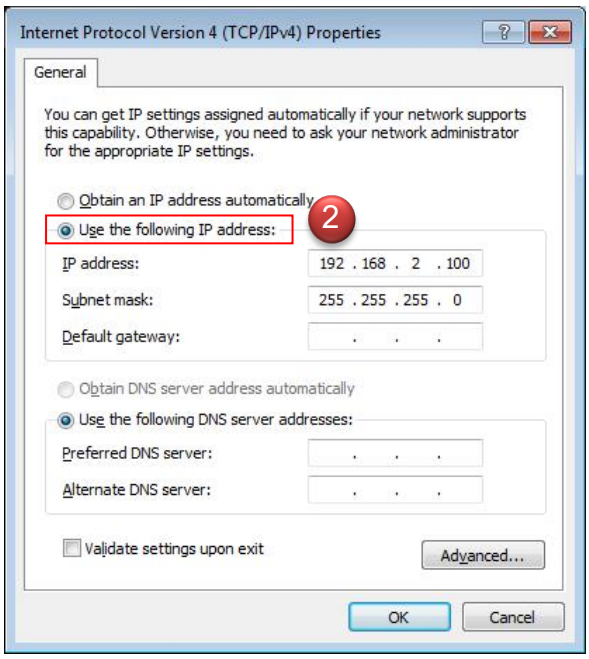
Step 4: In Properties page to setting IP address, please find **"Internet Protocol Version 4 (TCP/IPv4)"** and double click or click **"OK"** button.

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-CA supports web-based configuration. Upon the completion of hardware installation, **DR-4000-CA** 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**

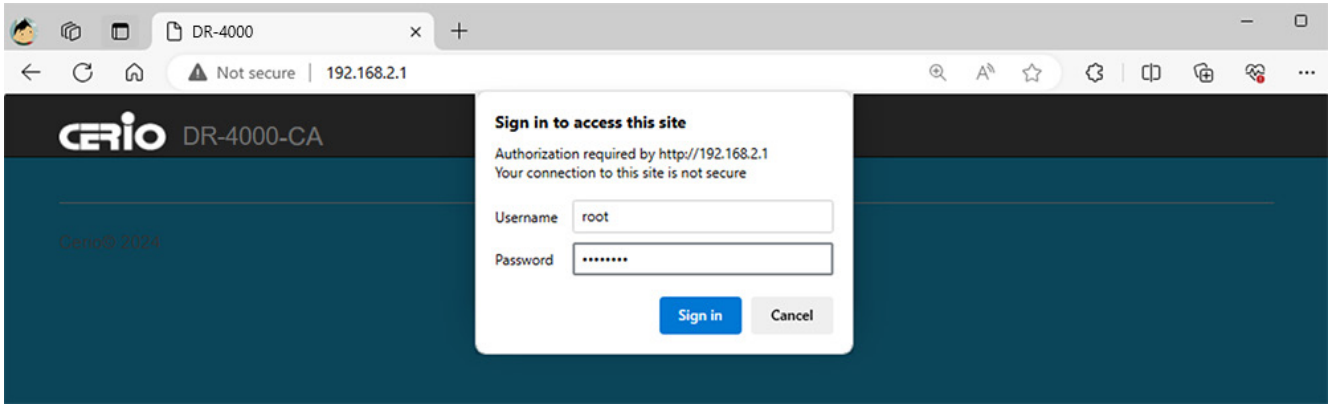
MODE	Router mode	
Management Account	Root Account	
Username	root	
Password	default	

Notice

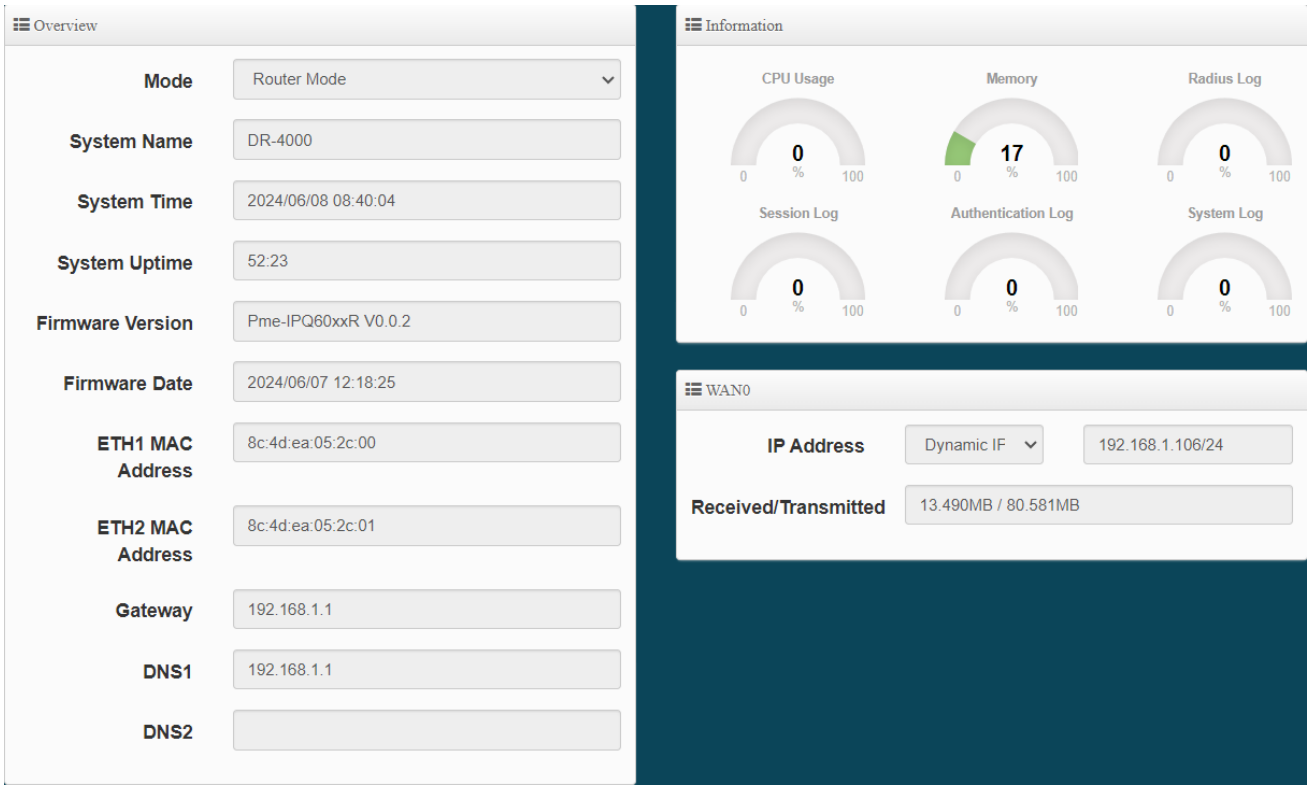
Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.1

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.



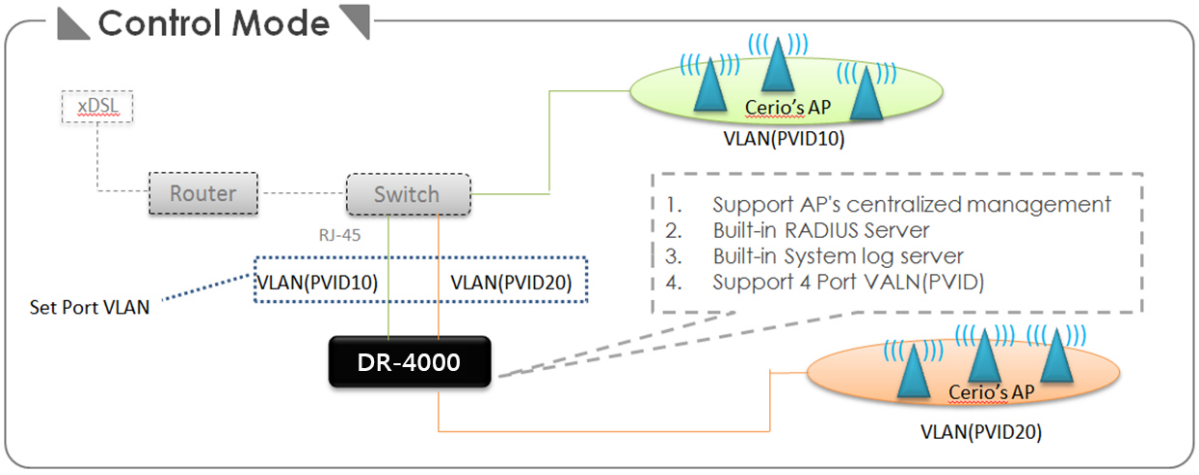
Please use default Users name: **"root"** and default password **"default"** to login.



2. Operating Mode Introduction

2.1 Control Mode

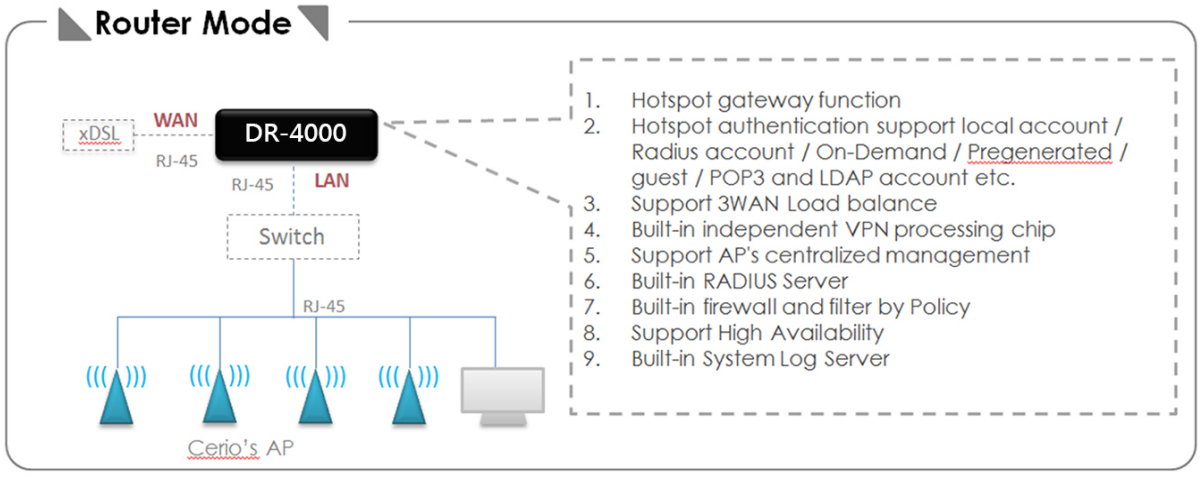
When the Control Mode is selected then **DR-4000-CA** will be pure AP centralized management controller, the system built-in RADIUS server, system log server and support port VLAN (PVID) setup. The Control mode can via VPN tunnel go to centralized management AP's (The mode is no Router NAT function in this mode).



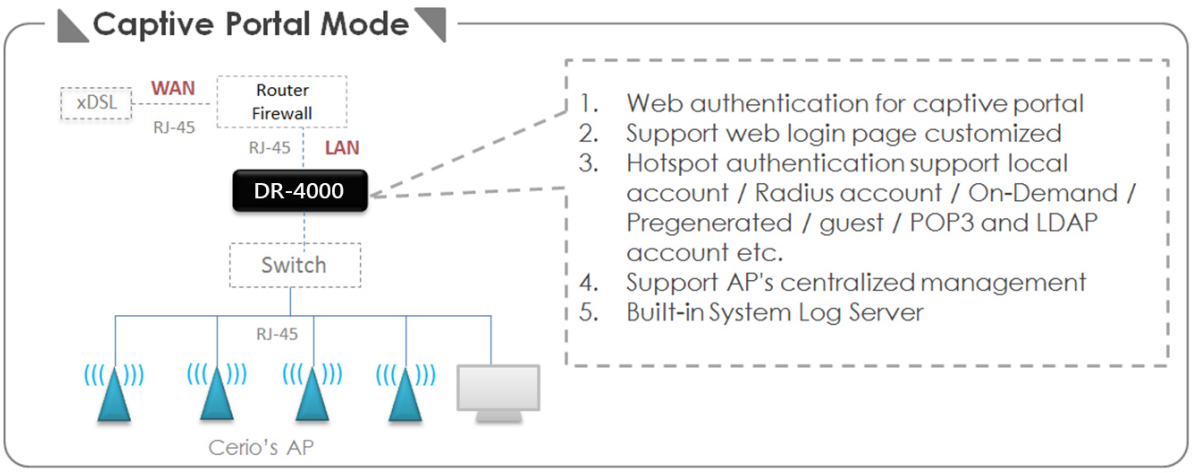
2.2 Router Mode

When administrator select use Route mode then system can set 1WAN 3LAN Router also can select 3WAN 1LAN outbound load balancer.

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



2.3 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)

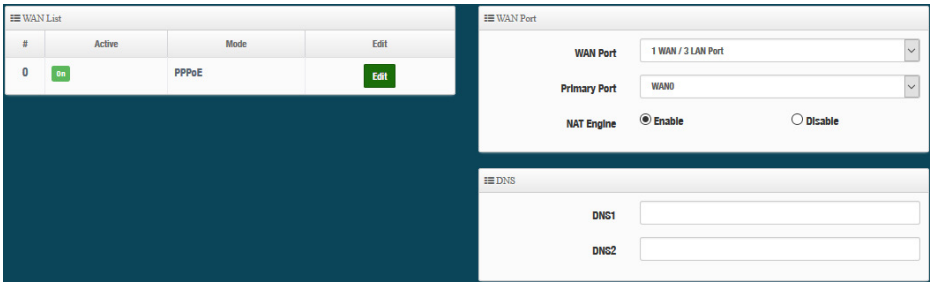
3. System Configuration

CERIO's **DR-4000-CA** is multifunctional authentication Gateway, support multi-WAN outbound load balance and can centralized managed CenOS5.0 AP. The **DR-4000-CA** 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.

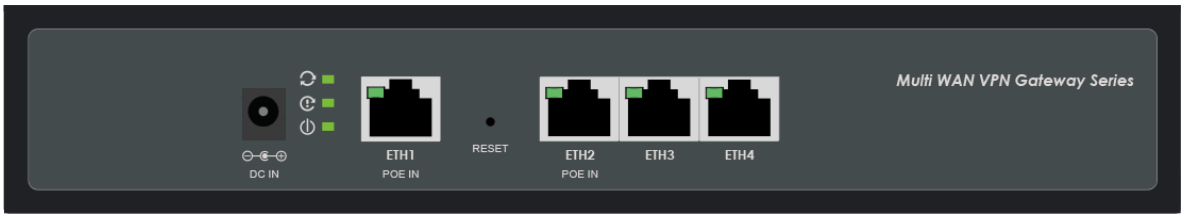
Please click System ➔ WAN Setup



WAN Port Setup

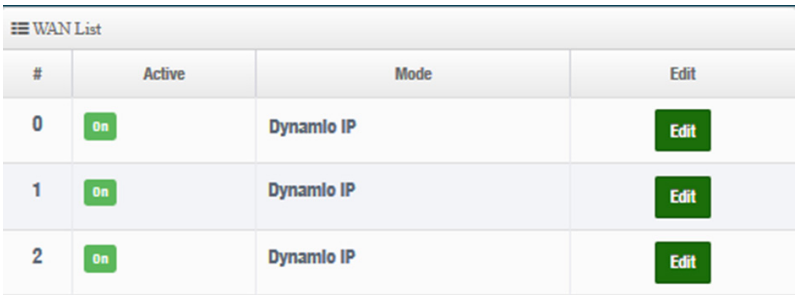
➢ **WAN Port:** Administrator can select 1WAN/3LAN or 1LAN/3WAN or 2WAN+/2LAN, the default is 1WAN/3LAN Port.

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) / WLLL	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.



Notice

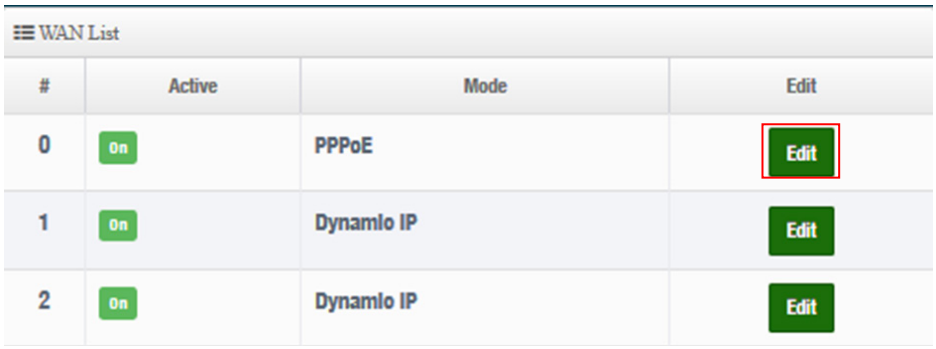
When selecting 2WAN up , you can set the load balancing priority setting on the WAN traffic setting function page.

- **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..

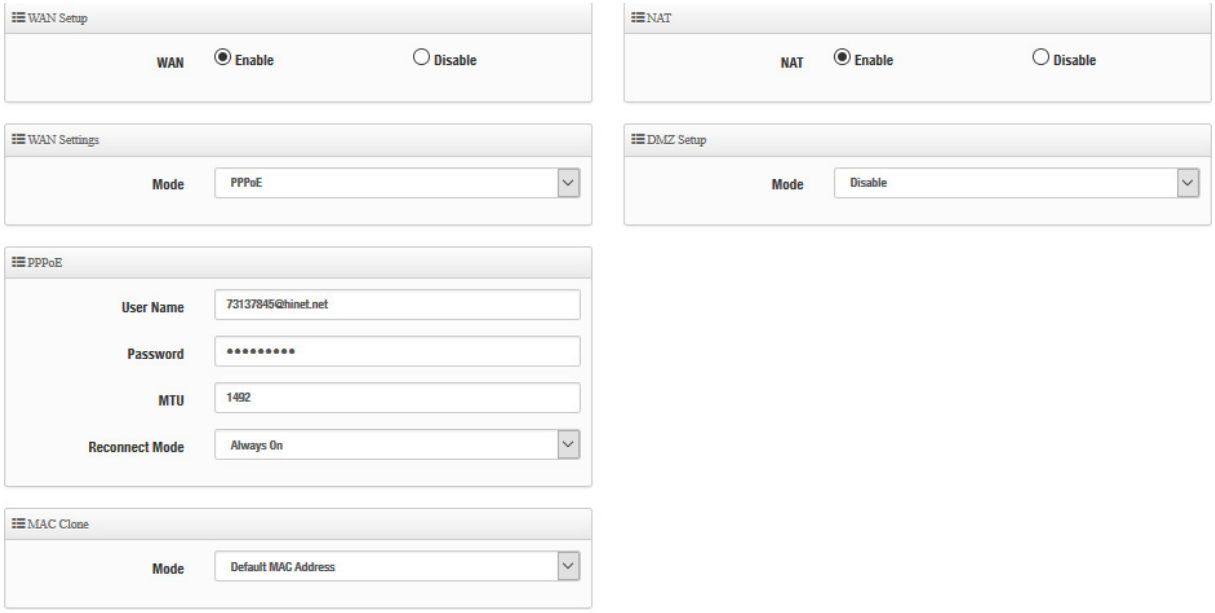
- **Primary Port:** If set 2 WAN or 3WAN function, administrator must select one primary for WAN Port, The WAN Port "primary port" setting,which mainly allows the system to use through the set WAN port, such as "system time" or DNS access, etc. If there is no special application, Please set to the default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



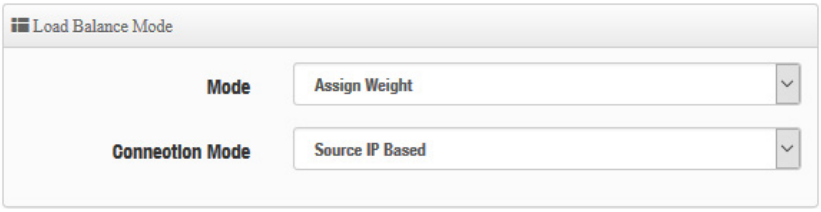
➢ **Edit:** Administrator can set WAN function.



- **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

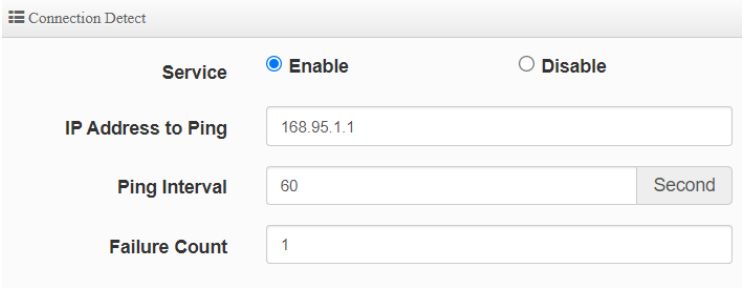
WAN Traffic setup function improves the distribution of workloads across multiple computing resources. WAN Traffic function aims to optimize network resource use maximize throughput or minimize response time and avoid overload of any single WAN port resource.
If administrator set multi-WAN configuration,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



- **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-CA** appliance to determine how much traffic each load balanced server can handle, and therefore more effectively balance load. The Weight set Max=10 unit.

  - **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.

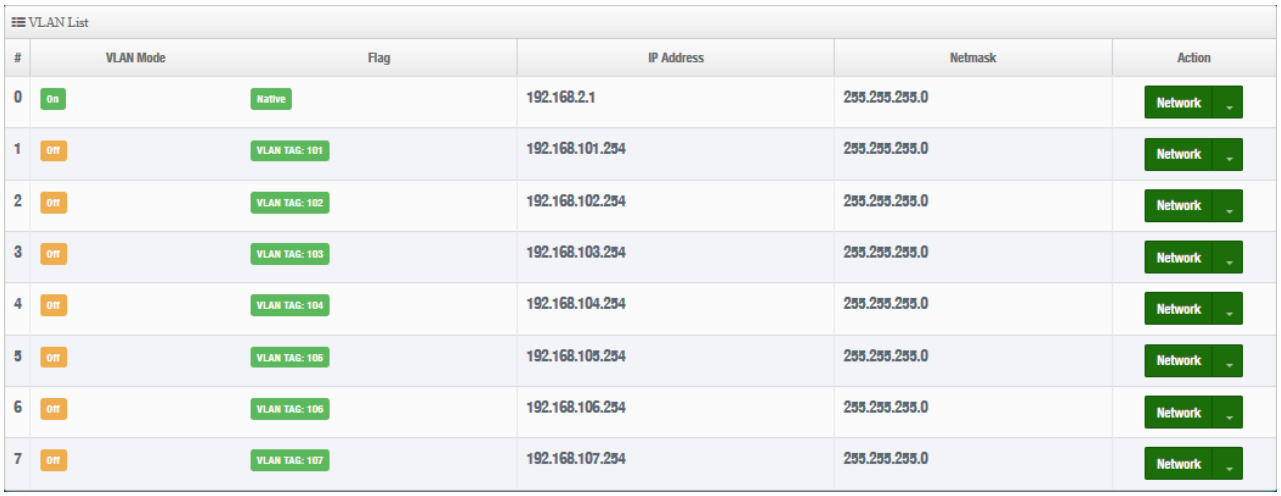
- **Connection Detect:** Enable connection detection, set the target IP of the specified Ping, and set the interval period of each Ping in "seconds". Set the Failure Count after the number of failures to truly enable WAN load balancing .



3.3 VLAN Setup

VLAN settings in default “Router mode”

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 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".

VLAN settings in "Control mode"

When change to the "Control Mode" of non-routing NAT state , 16 groups of virtual network services are also supported. By default, each virtual network supports the 802.1Q Tag VLAN function. The administrator only needs to click Enable, and the system will The setting of 802.1Q Tag VLAN can be completed.

VLAN List

#	VLAN Mode	Flag	IP Address	Netmask	Port	Action
0	On	Native	192.168.2.1	255.255.255.0	1 2 3 4	Network
1	Off	TAG: 101	192.168.101.254	255.255.255.0	1 2 3 4	Network
2	Off	TAG: 102	192.168.102.254	255.255.255.0	1 2 3 4	Network
3	Off	TAG: 103	192.168.103.254	255.255.255.0	1 2 3 4	Network
4	Off	TAG: 104	192.168.104.254	255.255.255.0	1 2 3 4	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.
- **Port**：Display the tags to be Flag by the four-port physical ethernet port. As shown in the following example, turn off the 3 and 4 operations under the second VLAN means that the 3 and 4 ports of the physical ethernet connection port do not have tag 101 but other ports have it tag 101.

VLAN List

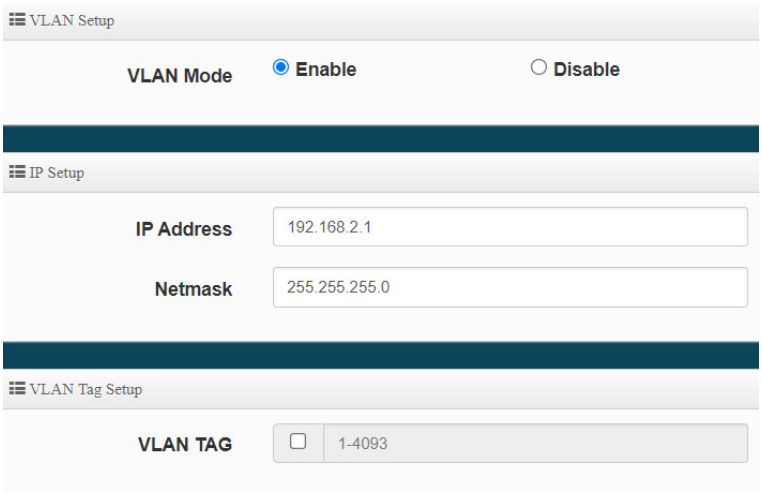
#	VLAN Mode	Flag	IP Address	Netmask	Port	Action
0	On	Native	192.168.2.1	255.255.255.0	1 2 3 4	Network
1	Off	TAG: 101	192.168.101.254	255.255.255.0	1 2 3 4	Network
2	Off	TAG: 102	192.168.102.254	255.255.255.0	1 2 3 4	Network

- **Action**： click  button o set VLAN network functions , click  Pull-down menu to 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.

Notice

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.

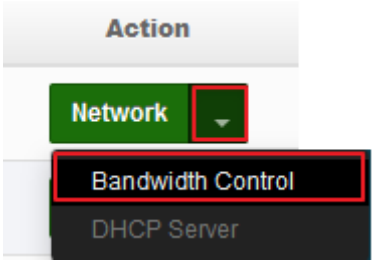
The following functions can be set in “Control Mode”

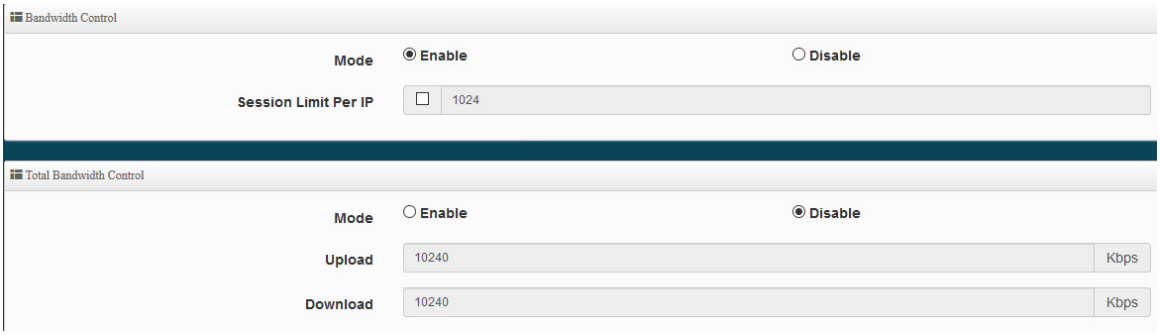
- ✓ **VLAN Tag**：Administrator can set this VLAN to 802. 1Q Tag VLAN

- ✓ **Port**：Enable or disable this physical port to this tag VLAN

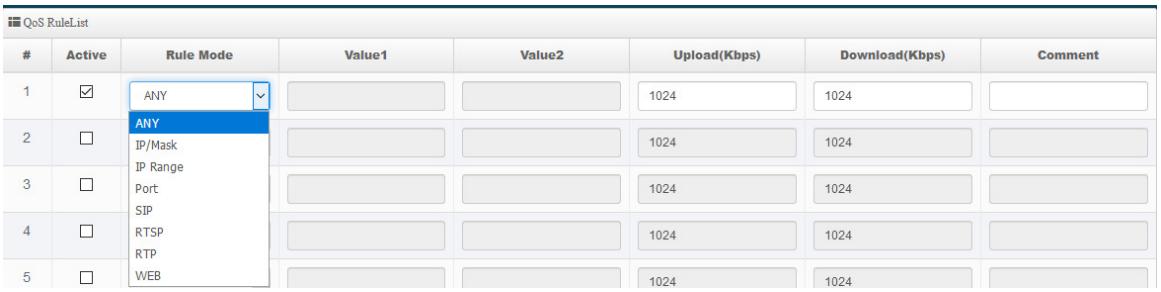
3.3.2 Pull-down menu @ Bandwidth Control

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.





- **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.

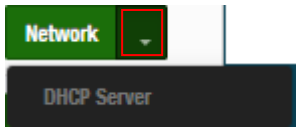


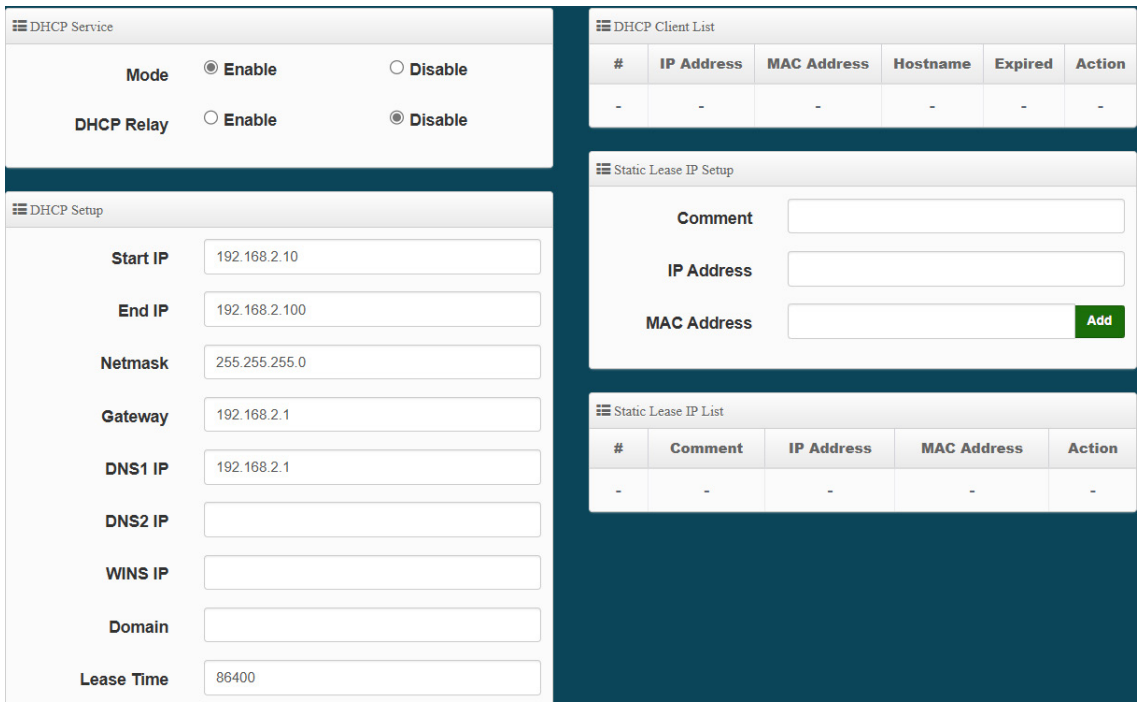
- **Any:** Bandwidth control by any protocol.
- **IP/MASK:** Bandwidth control by a subnet.
- **IP Range:** Bandwidth control by IP range.
- **Port:** Bandwidth control by port (service), ex. FTP port (20,21)
- **SIP:** Bandwidth control by Session Initiation Protocol.
- **RTSP/RTP:** Bandwidth control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

3.3.3 Pull-down menu @ DHCP Server

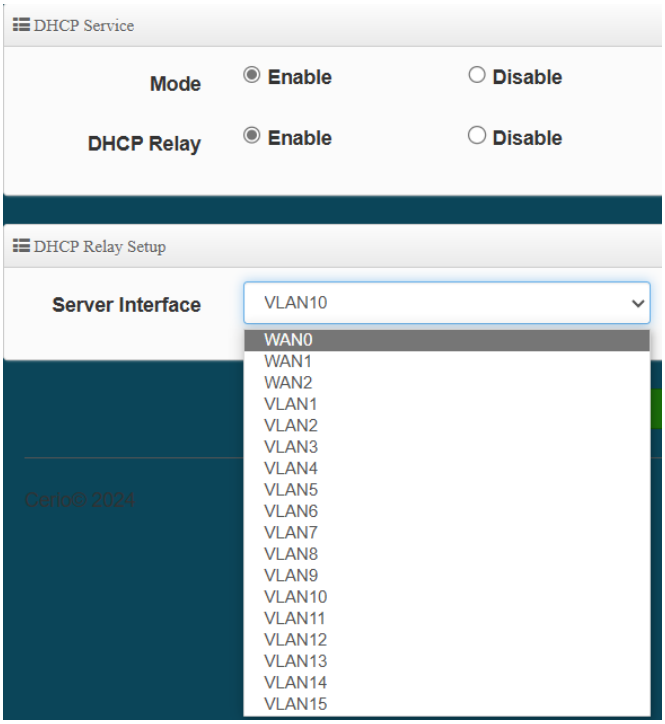
Administrator can set DHCP function. Please click 

pull-down button to set DHCP Server.



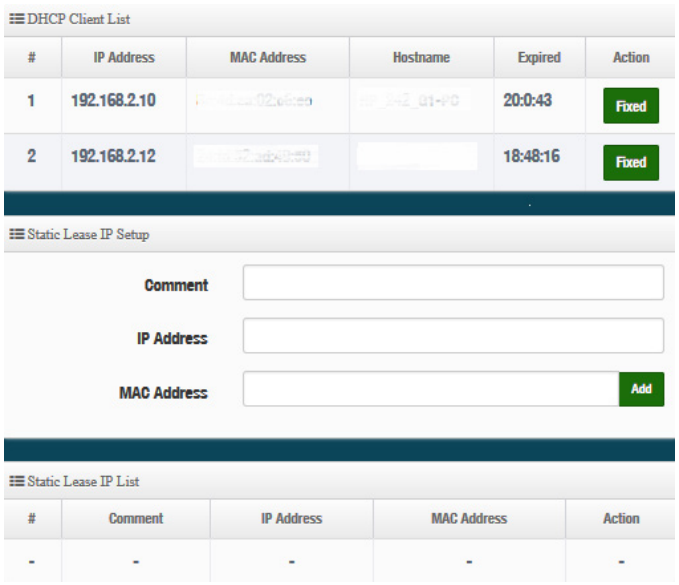


- ✓ **Mode:** Administrator can select enable / disable the function
- ✓ **DHCP Relay :** Administrator can select enable / disable the function



- **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

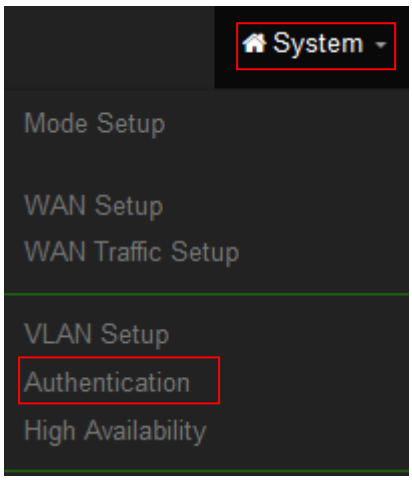


  - ➢ **DHCP Client List:** Administrator can view IP address used status of client users on each DHCP Server.
  - ➢ **Static Lease IP Setup:** Administrator can set be delivered fixed IP address to the users. (This MAC Address binding IP address function can bind up to 100 sets of settings).

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**



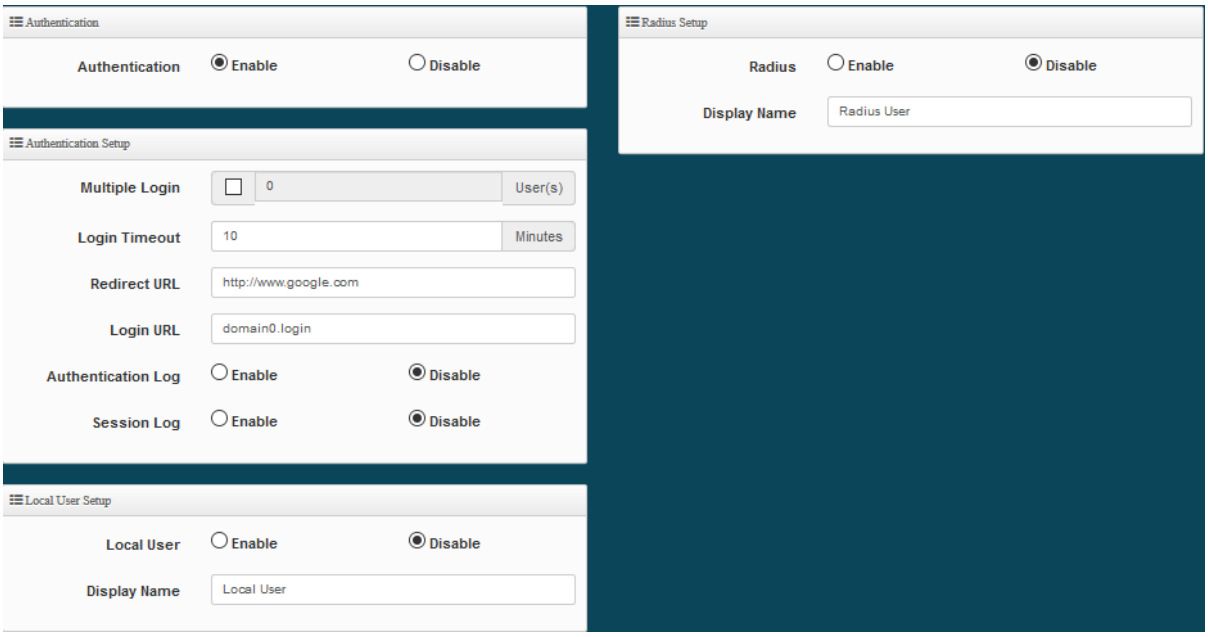
VLAN List

#	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)

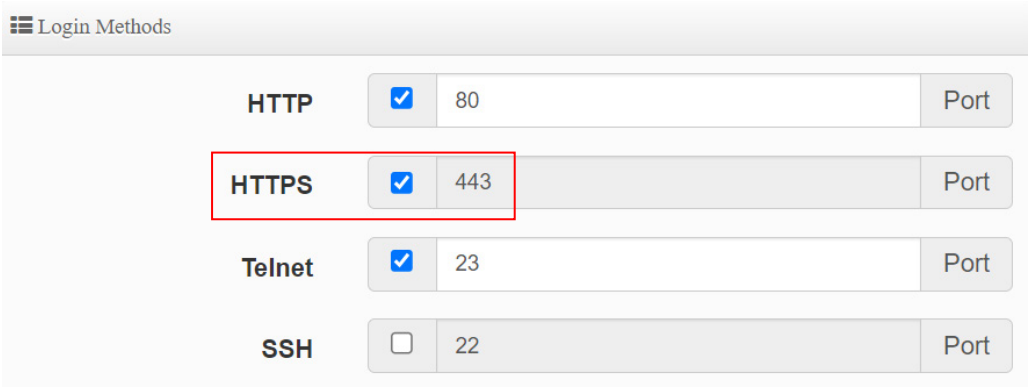
Authentication Button:

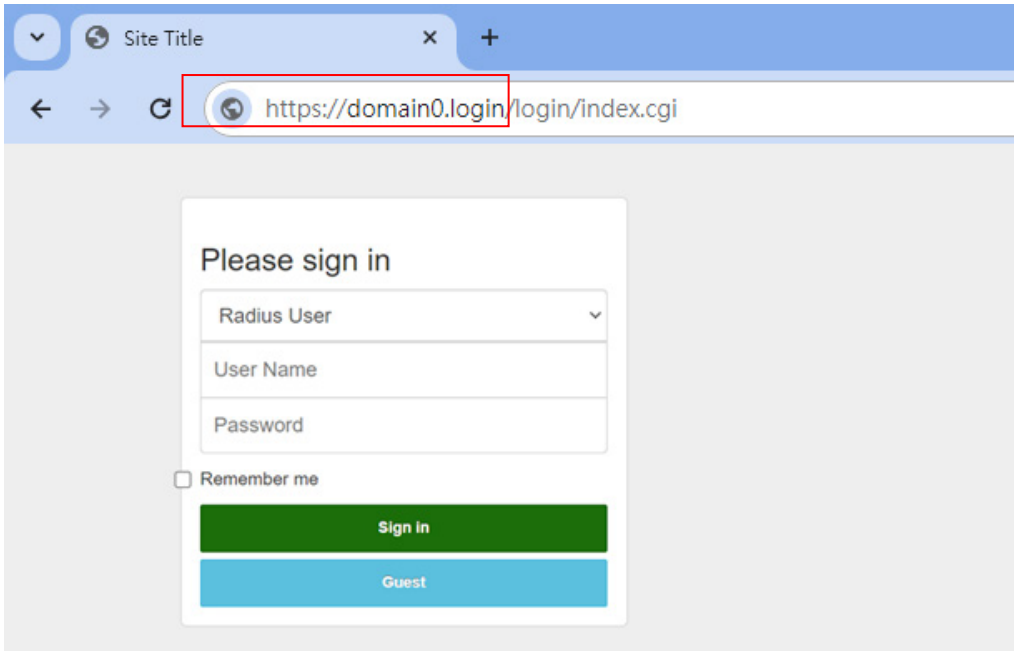
Authentication ：By clicking the Authentication button, administrator can enable or disable this function.



- **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.**

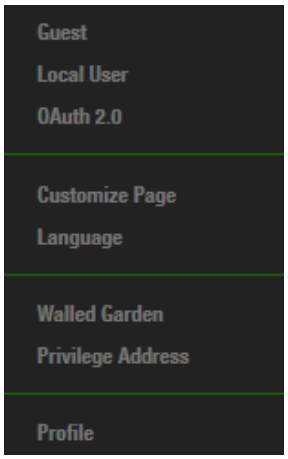




- **Authentication Log:** Account authentication log will copy to the device 's syslog server.
- **Session Log**：If network have Syslog server. Administrator can to system➔management setting IP address for syslog server and enable the function. Account session log will copy to the device 's syslog server.
- **Local User**：Administrator can enable authentication for local user. Create user account can to reference **"3.3.2 Local User".**
- **RADIUS**：Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.

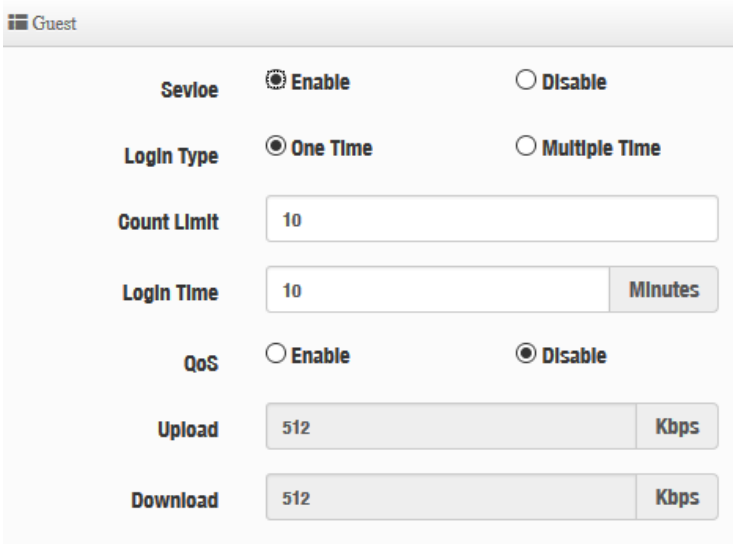
Authentication Dropdown Button

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



3.4.1 Guest

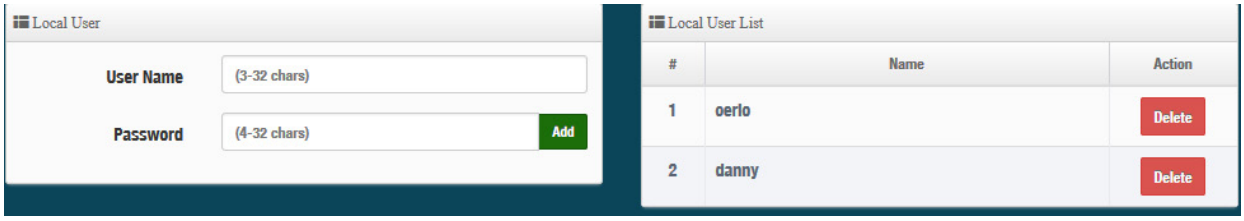
Administrator can enable or disable guest authentication. If enabled, the administrator can set guest Count Limit / login time and type and flow control.



- **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

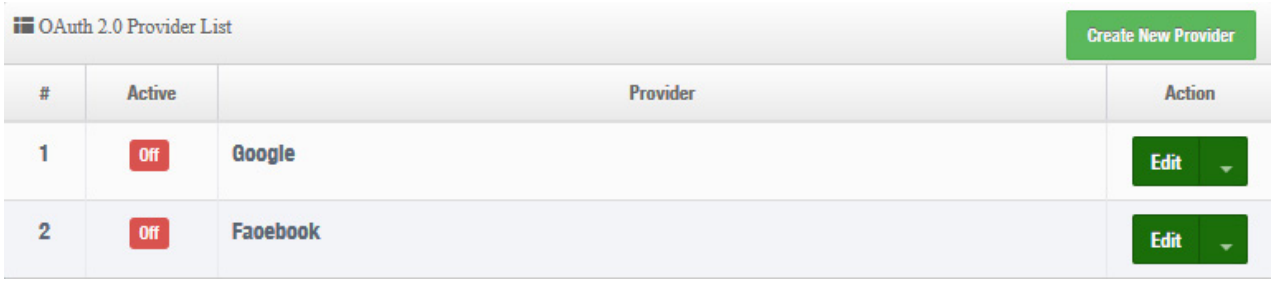
Administrator can create local user account for web login.



- **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.



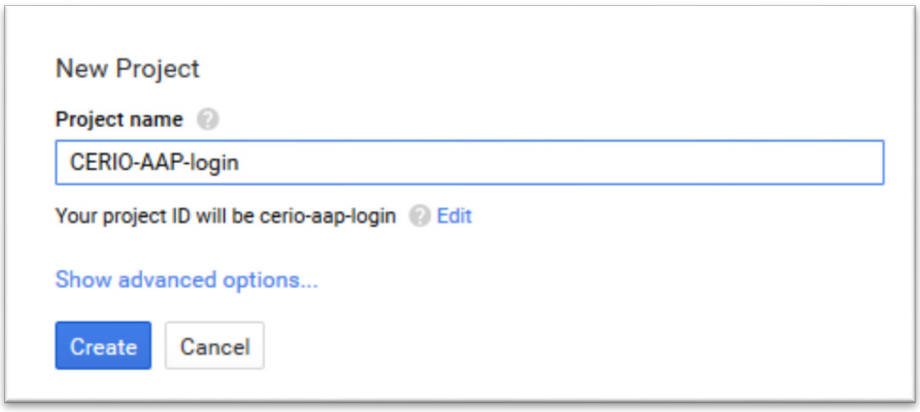
- **#**：Display items.
- **Active**：Display on/off status for the authentication.
- **Provider**：Display authentication server. The system default use authentication server for Google and Facebook

➔ # Sample for Google OAuth2.0 setup

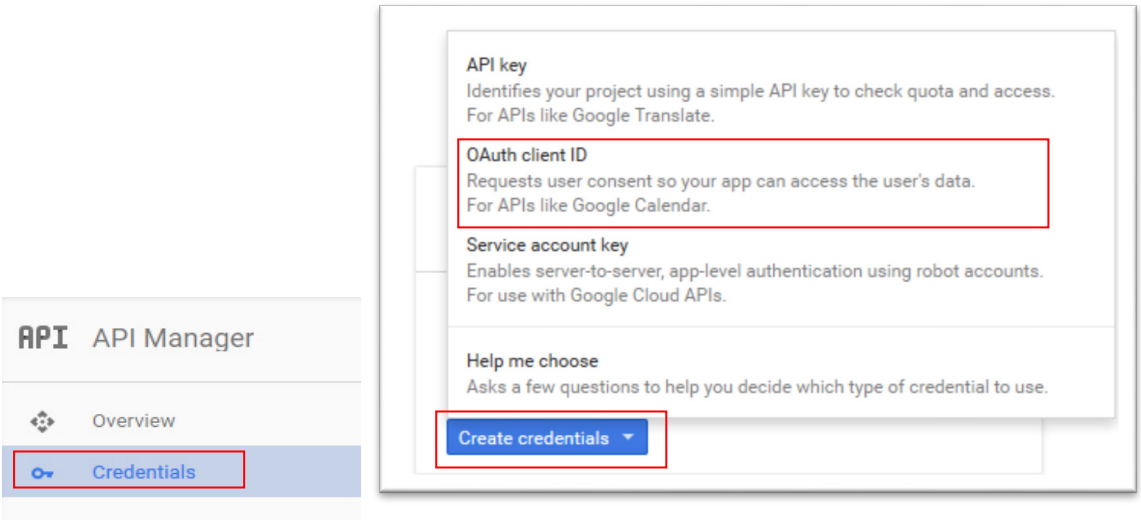
Please complete the application on the Google website to receive an account ID and password, follow the steps below.

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

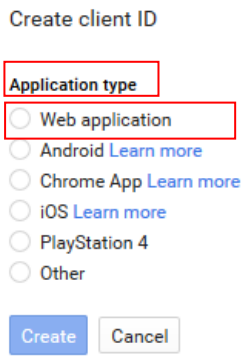
(Reference https://developers.google.com/identity/protocols/OAuth2)

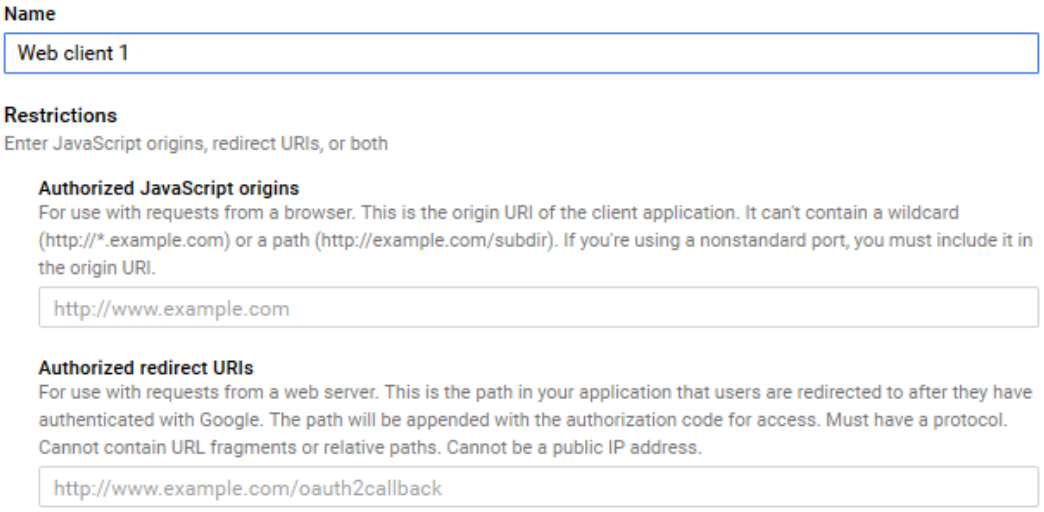


Step.2 Click Credentials to create OAuth client ID in the API manager page.



Step.3 Select web application in the "Application Type" section and set **"Restrictions"** URL.

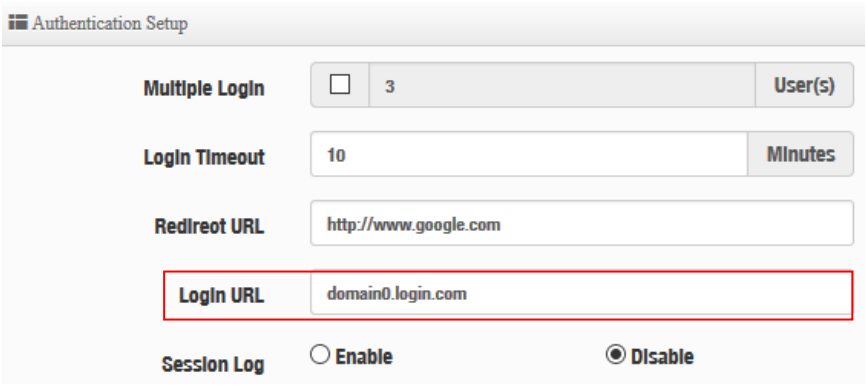




Step.4 Set Authorized JavaScript origins and Authorized redirect URLs (important)

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

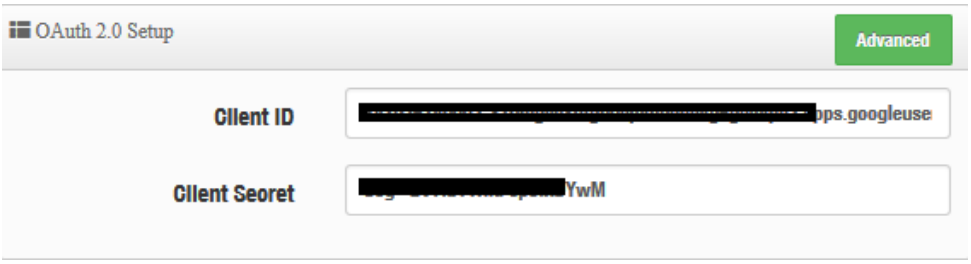
- Setup login URL in the device. Please Click **system➔Authentication** and enable the function.
- The "Authentication Setup" page to set Login URL



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**

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.

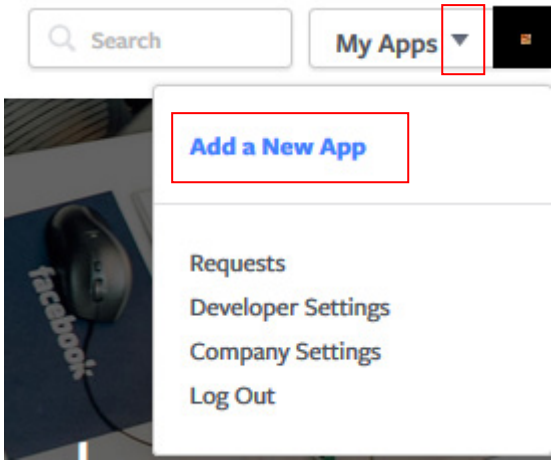


Save and reboot the AP system, complete the setup.

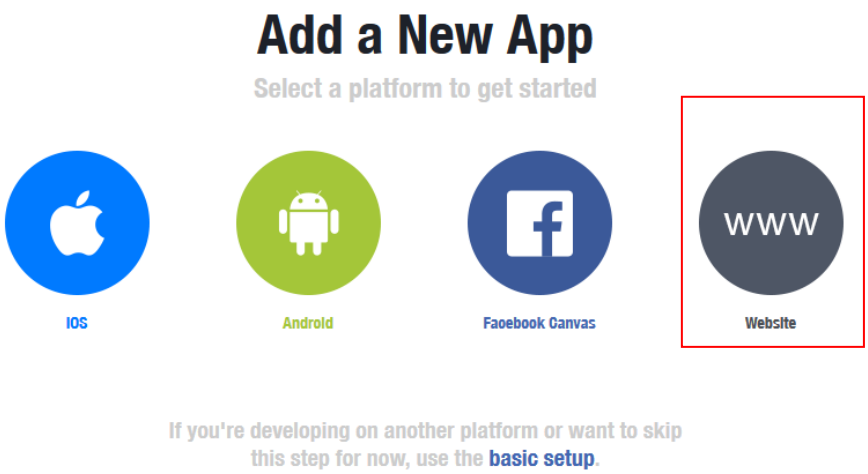
➔ # Sample for Facebook OAuth2.0 setup

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

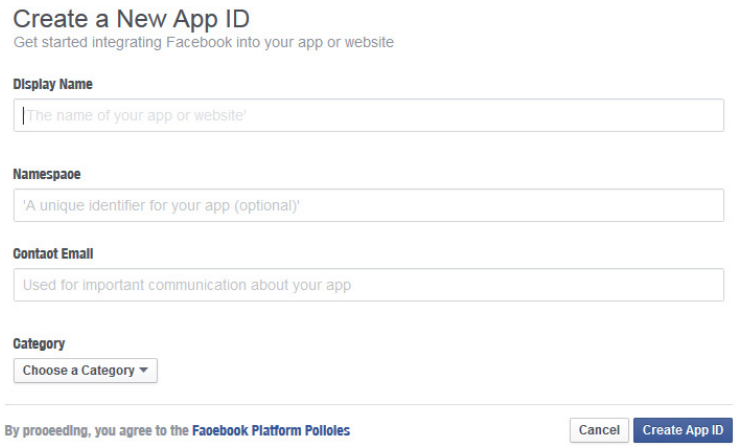
Step.1 Please to Facebook developer's page and add a New App



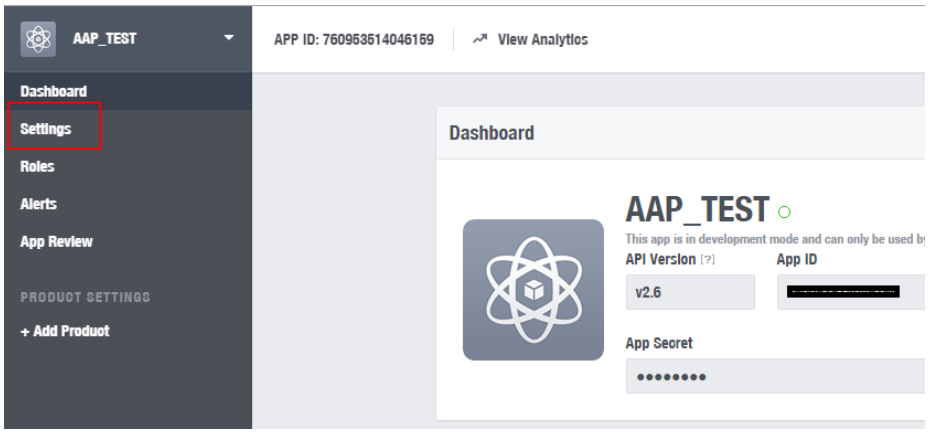
Step.2 Select WWW function



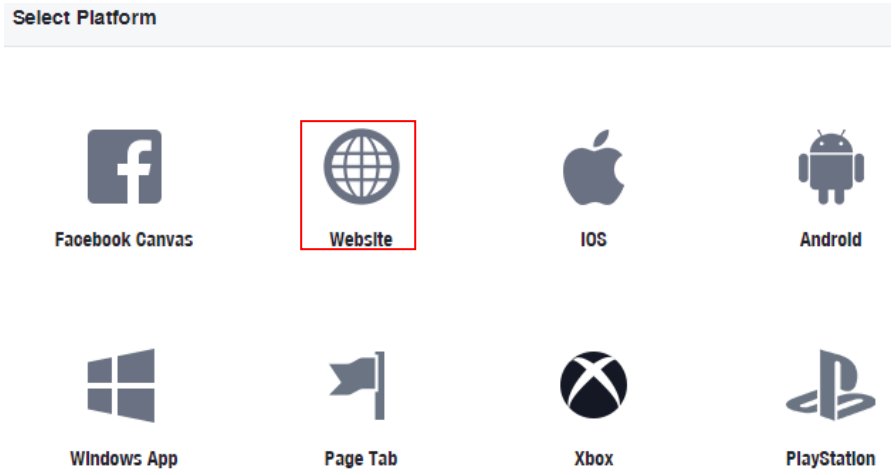
Step.3 Administrator must set www for your information.



Step.4 Please click **"Setting"** and add Platform



Step.5 Select Platform for "**Website**"



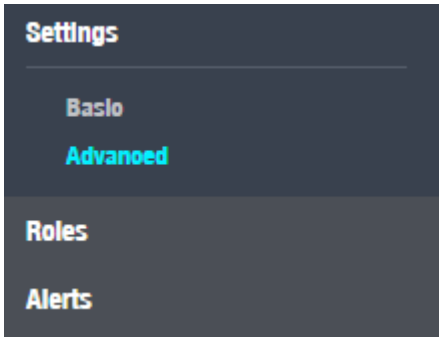
Step.6 Enter URL is **http://domain0.login.com/login/callback.cgi**

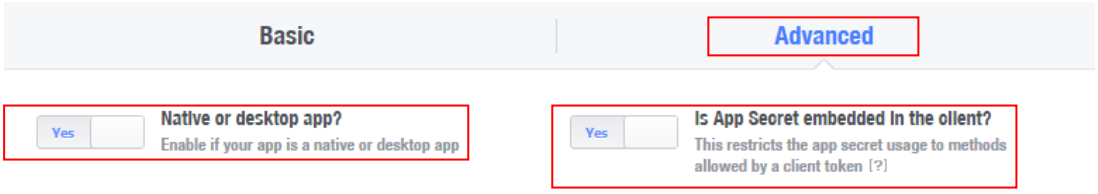
Administrator must set login URL in the device function. After complete set of login URL go to the "**Facebook** Site URL" function in web page. Follow the steps below to set login URLs

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

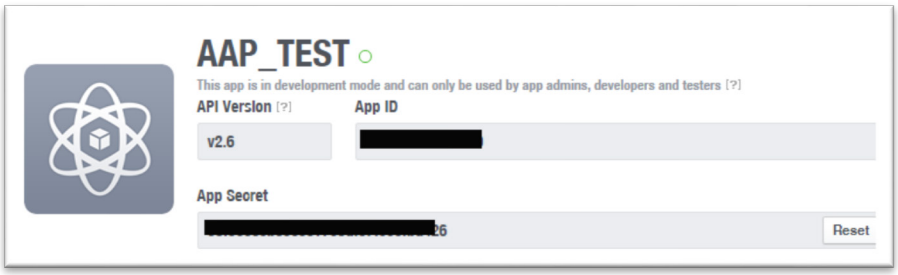
After complete set of login URL go to the "**Facebook** Site URL" function in web page. Copy and paste the login URL from the system display into the "Site URL" page on the Facebook website.

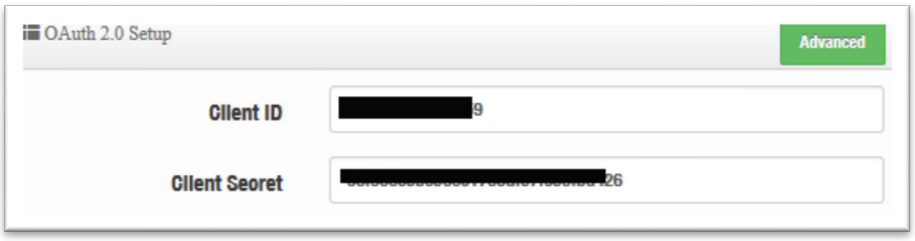
Step.7 Click Advanced function to enable the **"Native or desktop app?"** and **"Is App Secret embedded in the client? "**





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.



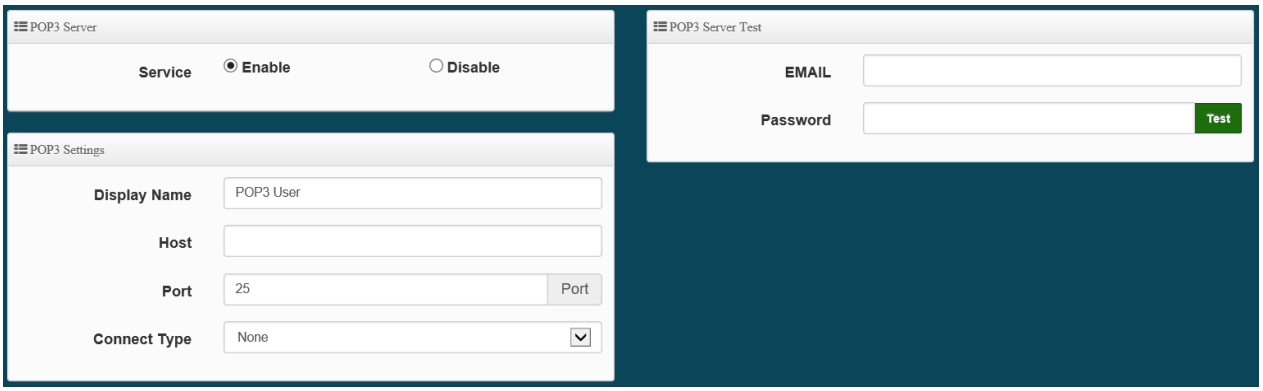


Notice

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

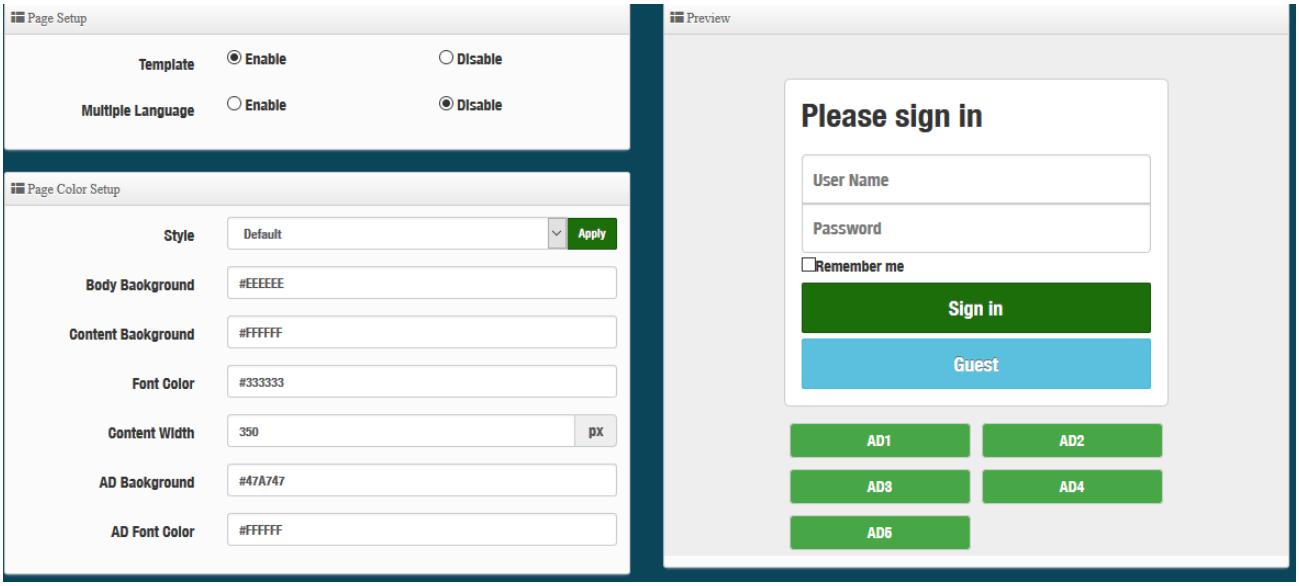
The purpose of this integrated function is to allow clients to link a POP3 server for receiving emails from a remote server.



- **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

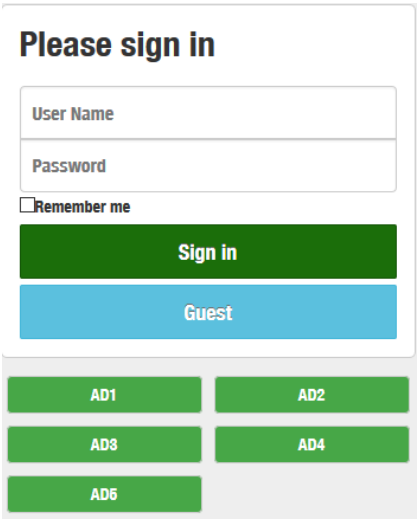
3.4.5 Customize Page

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

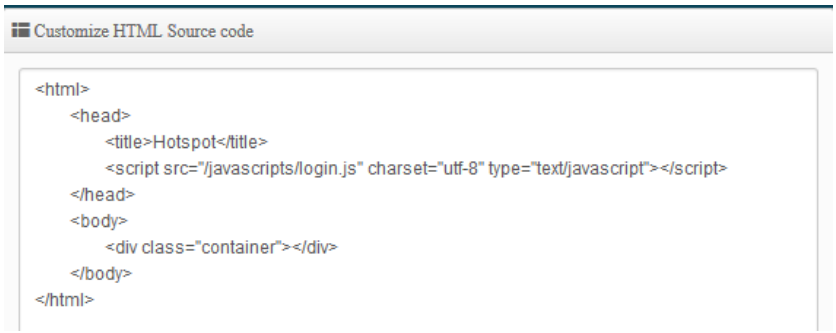


Page Setup

- **Template**：Administrator can select Enable or disable.
  - Select enable to active default Login Page



  - Select disable to active HTML Source code window for customization



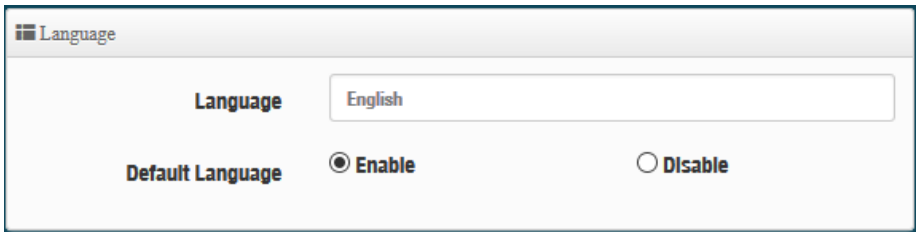
Sample: See sample login page below that is customized by html coding *(sample login page html code templates are available on Cerio website)*

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.

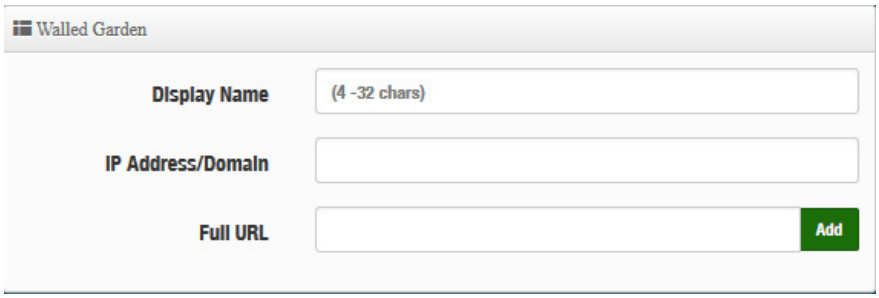
3.4.6 Language

Administrator can create other language for login page.



3.4.7 Walled Garden

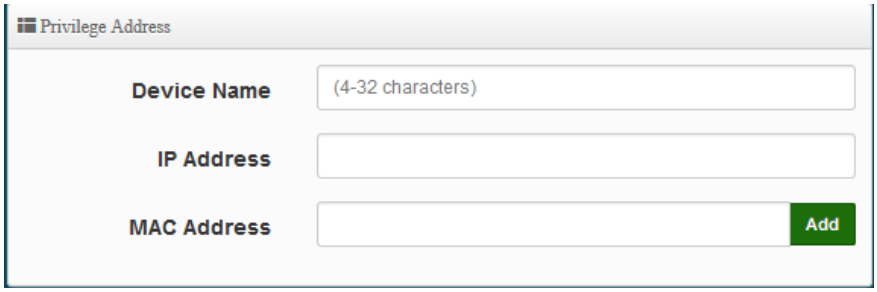
This function provides certain free services or advertisement web pages for users to access the websites listed before login and authentication. User without the network access right can still have a chance to experience the actual network service free of charge in Walled Garden URL list.



- **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

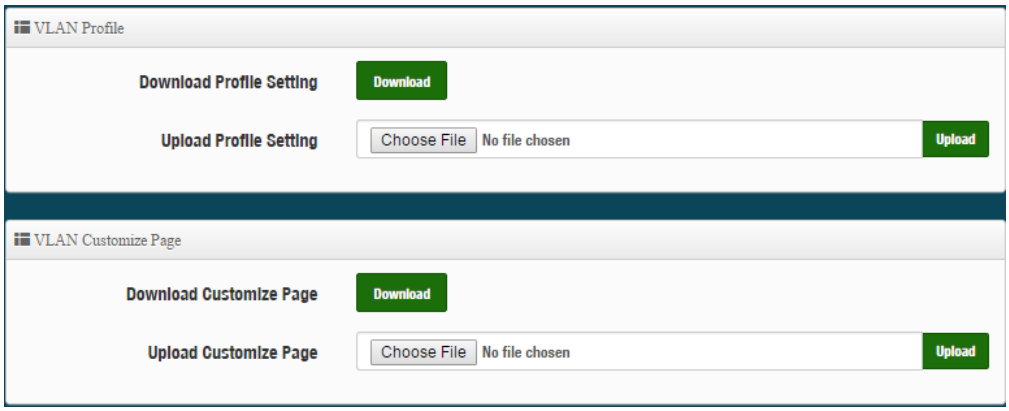
This function provides local device can access Internet without authentication. If there are some workstations belonging NGS Access Point that need to access to network without authentication, enter the IP or MAC address of these workstations in this list.



- **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.



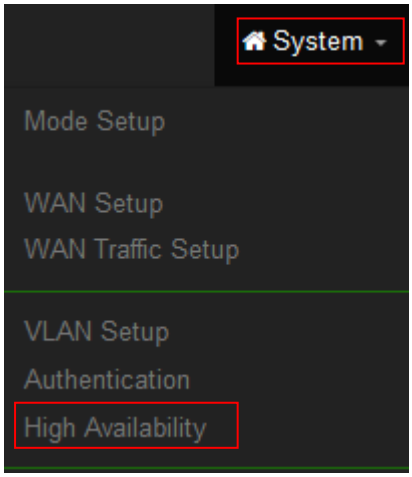
Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

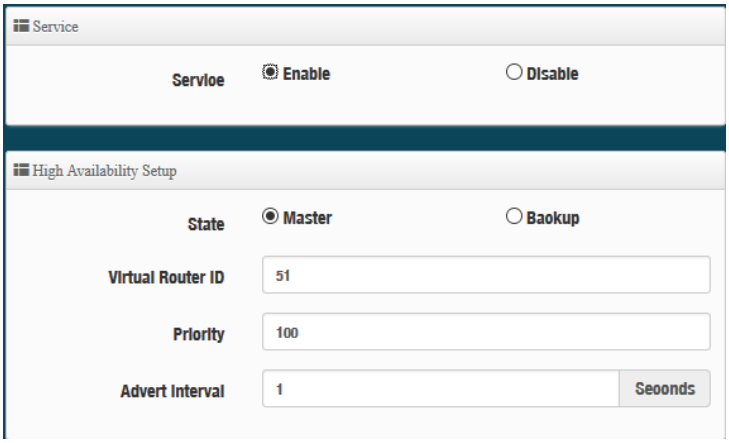
3.5 High Availability

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

Please click **"System"➔ "High Availability"** to set the function.



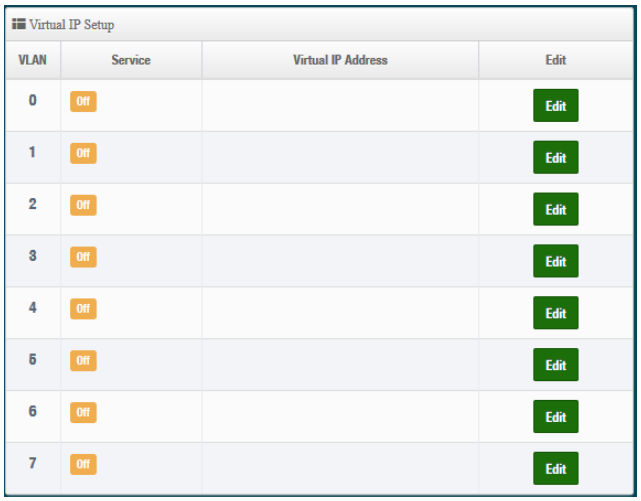


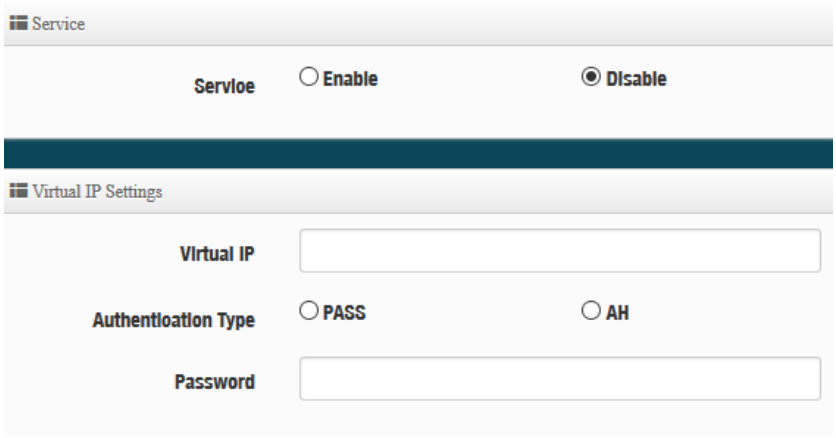
- **Service:** Administrator can select Enable or Disable the HA function.

High Availability Setup

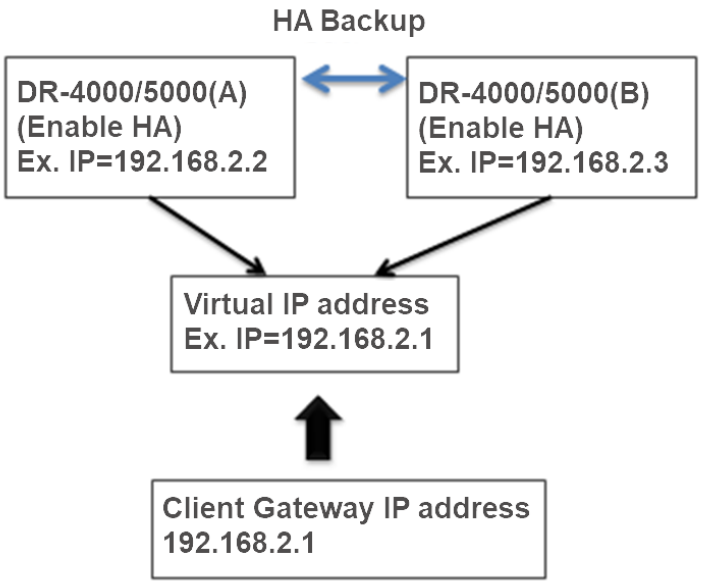
- **State:** Administrator can set HA type of the Master or Backup.
- **Virtual Router ID:** Administrator must set same virtual router ID in all the high availability devices
- **Priority:** Administrator can set the priority level.
- **Advert Interval:** After how many sec to the recovery.

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





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

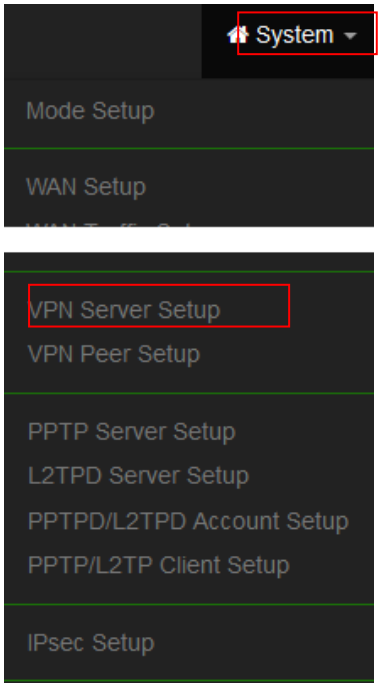


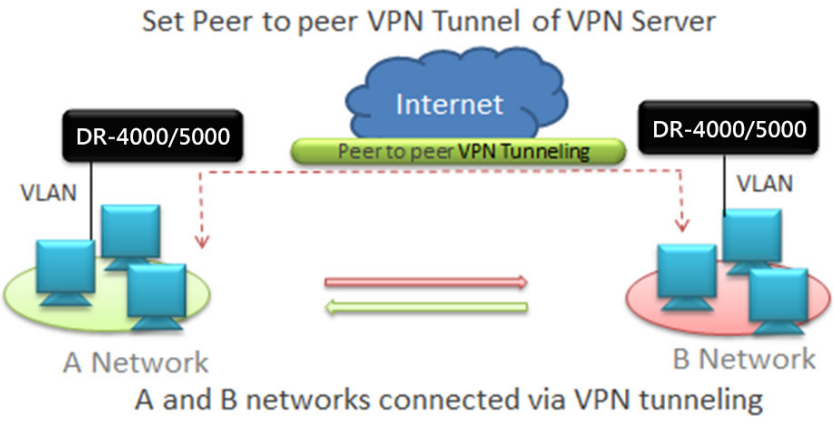
- **Authentication Type:** Administrator can select PASS or AH type for HA security.
- **Password:** Administrator can set password for the HA security.

3.6 VPN Server Setup

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.**

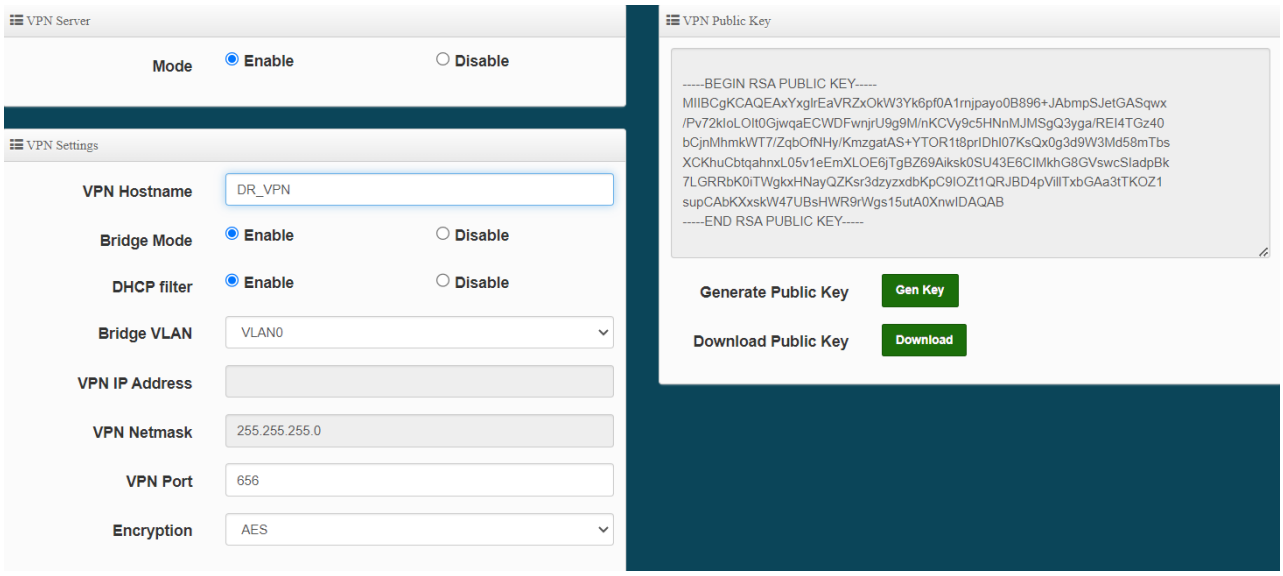
Please click **"System"➔"VPN Server Setup"** create VPN function.





VPN Service

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



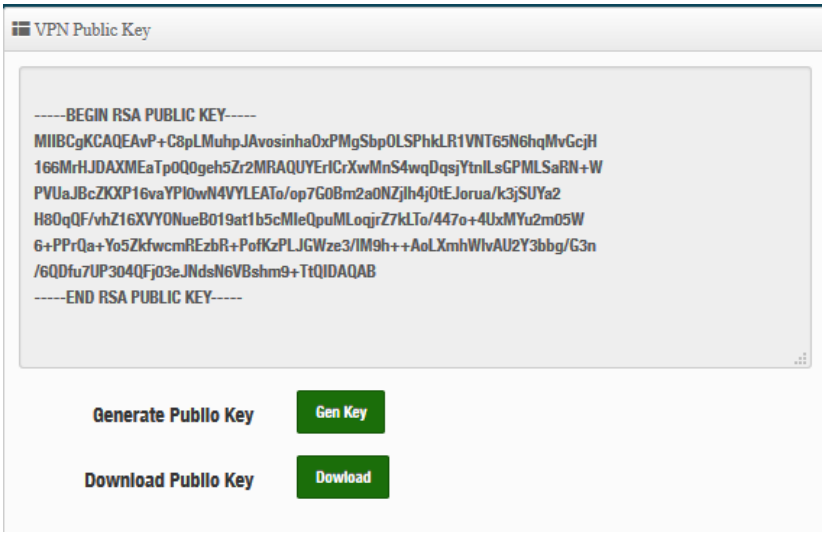
VPN Settings

- **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.
-

Notice	1. If administrator choose use bridge mode then VPN both sides beneath need use same c 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



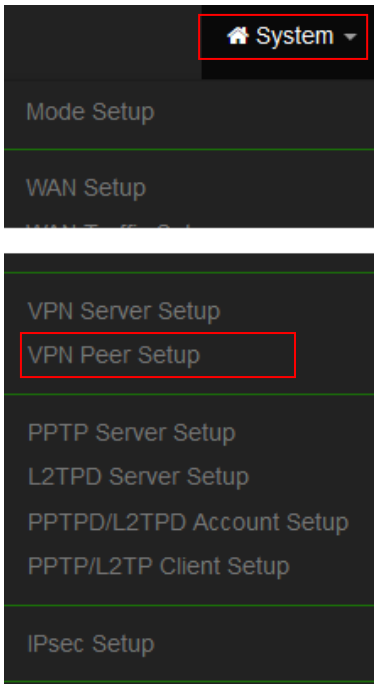
- **Generate Public Key:** Administrator can click the button to regenerate the VPN public key.
- **Download Public Key:** Administrator can click the button to download the VPN public key.

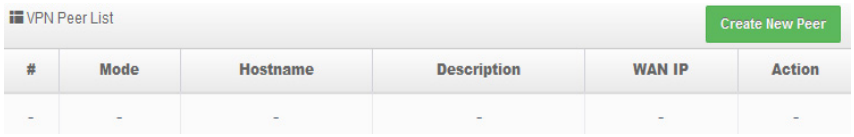
3.7 VPN Peer Setup

Notice	**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.

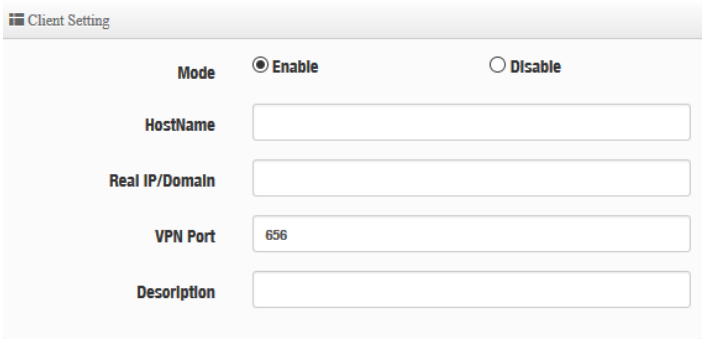
Please click "**System**"➔"**VPN Peer Setup**"





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.

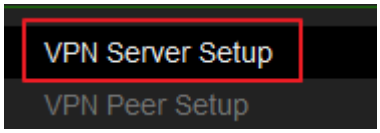


- **Mode:** Administrator can select Enable or Disable the service.
- **HostName:** Administrator can set VPN host name in this field.
- **Real IP/Domain:** Administrator can set remote real IP address or Domain name in this field.
- **VPN Port:** Administrator can set connection Port for VPN.
- **Description:**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

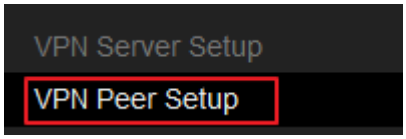
Basic instructions for setting the program

In the two end points A and B for example

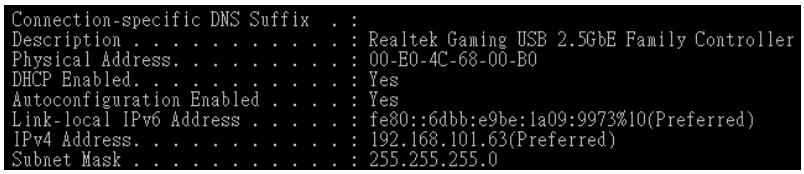
1. Set the VPN server on the A side, and download and store the VPN Public Key, the A Public Key upload it to the B endpoint for authentication. The same is true for the B endpoint setting. (Two-end exchange public key)



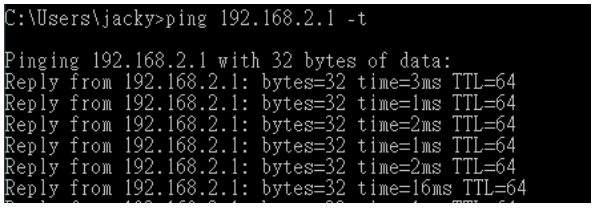
2. Establish remote VPN Server information and upload the remote Public Key to this location.



3. 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.



A Side



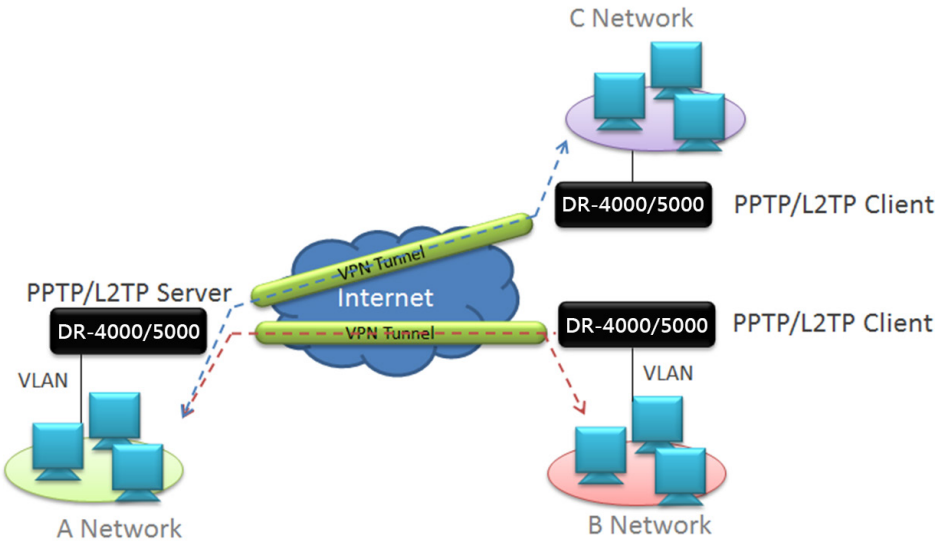
B Side

4. 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.
5. 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.

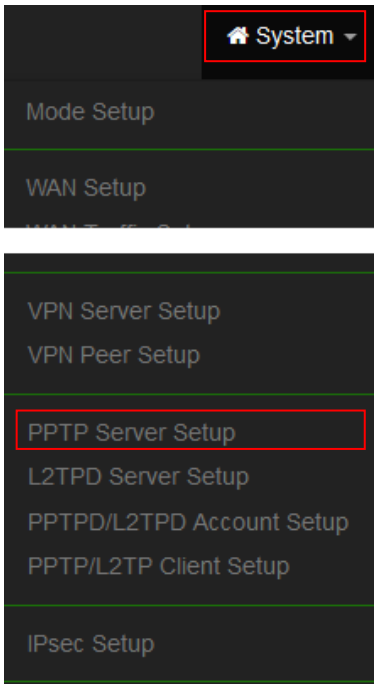
3.8 PPTP Server Setup

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.**

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**"



- **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).**

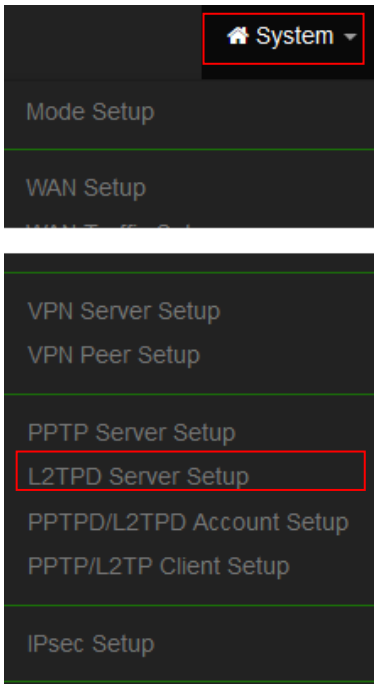
- **Remote Start/ End IP Address:** Set start to end IP address for dynamic configuration, can give VPN client automatically obtain a virtual IP address.
- **MPPT40/128:** Administrator can choose use VPN security for 40 or 128 bit.

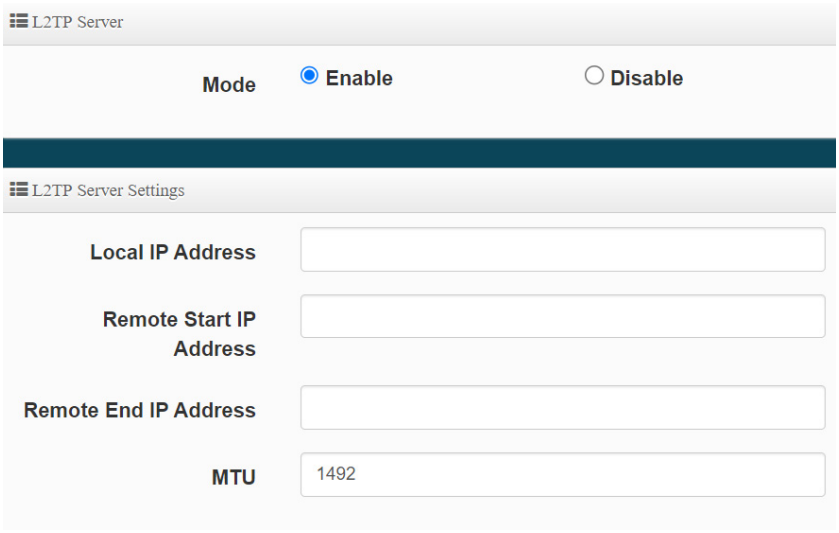
3.9 L2TP Server Setup

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.**

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**"

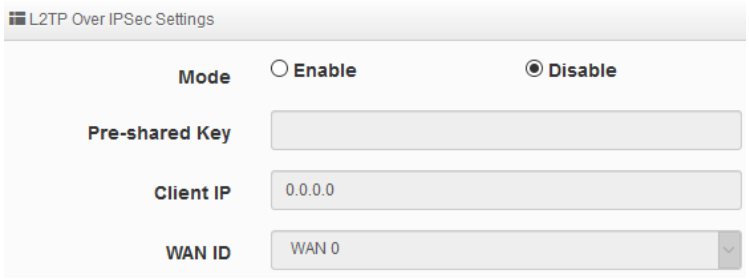




- **Local IP Address:** Set virtual IP address for VPN server.

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.

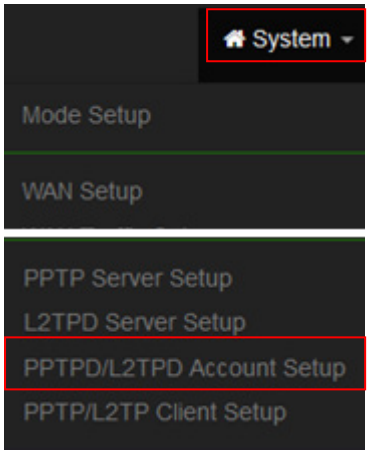


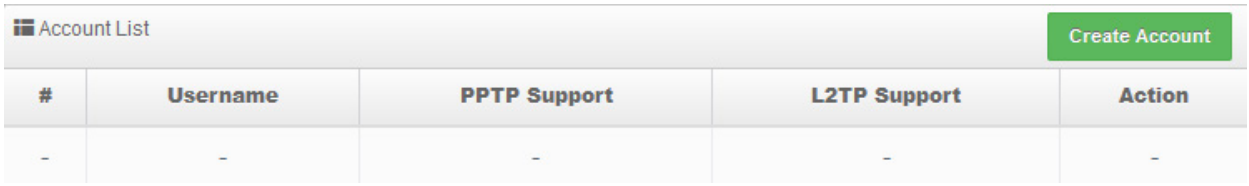
- **Mode:** Administrator can choose Enable or disable this function.
- **Pre-shared Key:** Set a security key for Pre-shared Key

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

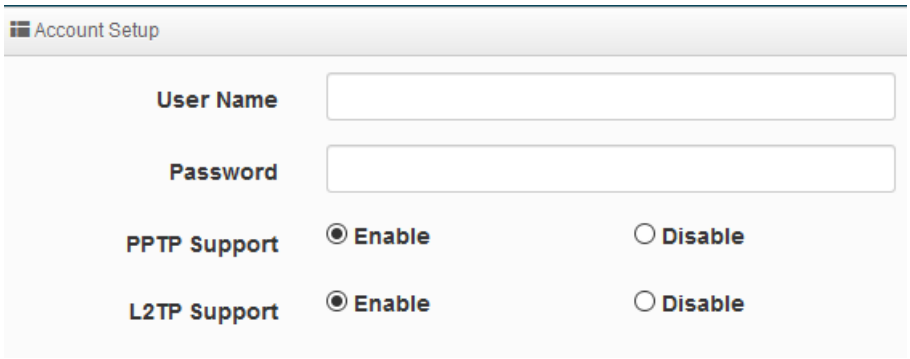
3.10 PPTP/L2TP Account Setup

Create PPTP / L2TP authentication account with maximum of 60 VPN accounts.
Please click “System”➔”PPTP/L2TP Account Setup”





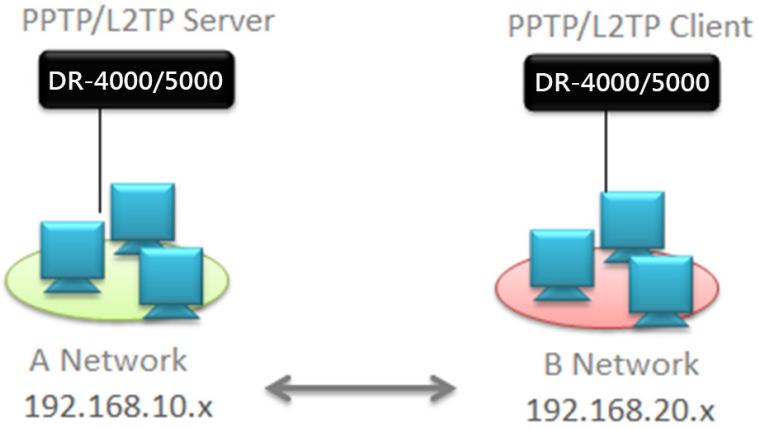
- **Create Account:** Administrator can click the button to create authentication account of client.



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

Routing Rule:

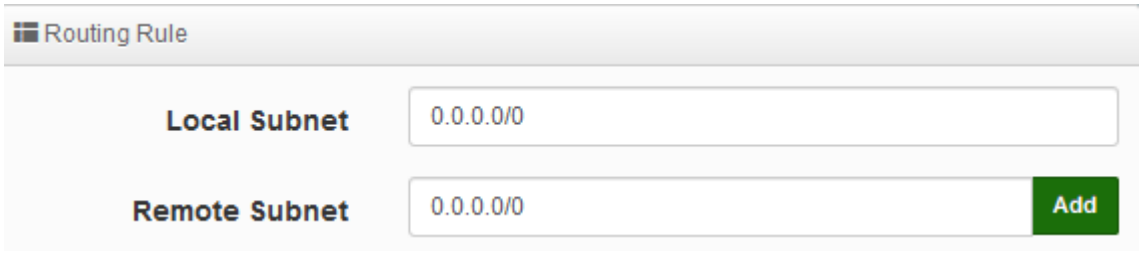
Set routing of both network, As figure below, the local end is the Server endpoint and the remote end is the Client endpoint.



Example :

Local Subnet: 192.168.10.0/24

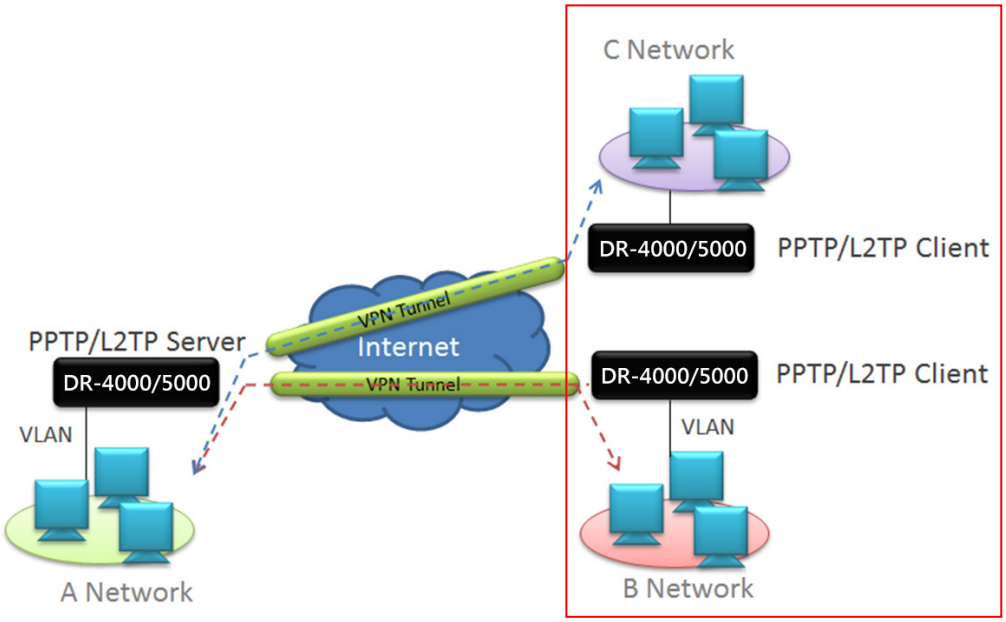
Remote Subnet : 192.168.20.0/24

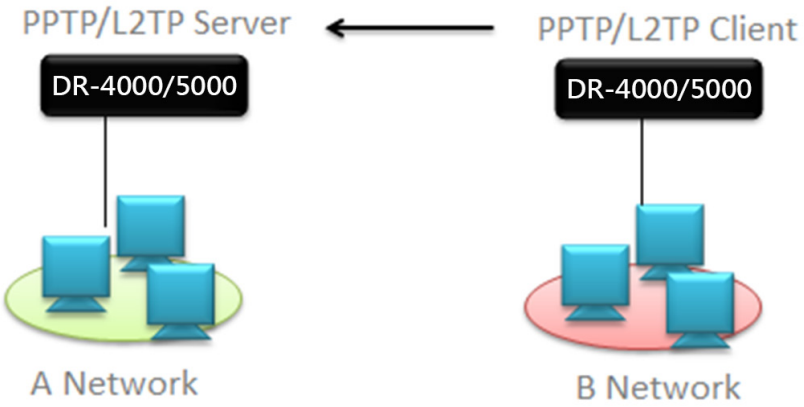


- **Local Subnet:** Set network subnet of local.
- **Remote Subnet:** Set network subnet of Remote.

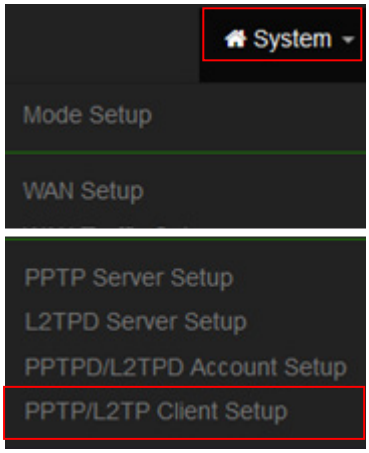
3.11 PPTP/L2TP Client Setup

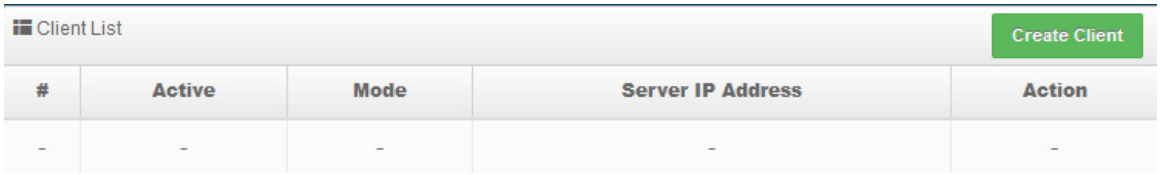
If remote have PPTP/L2TP VPN server, administrator can used PPTP/L2TP client function connection to remote VPN server.



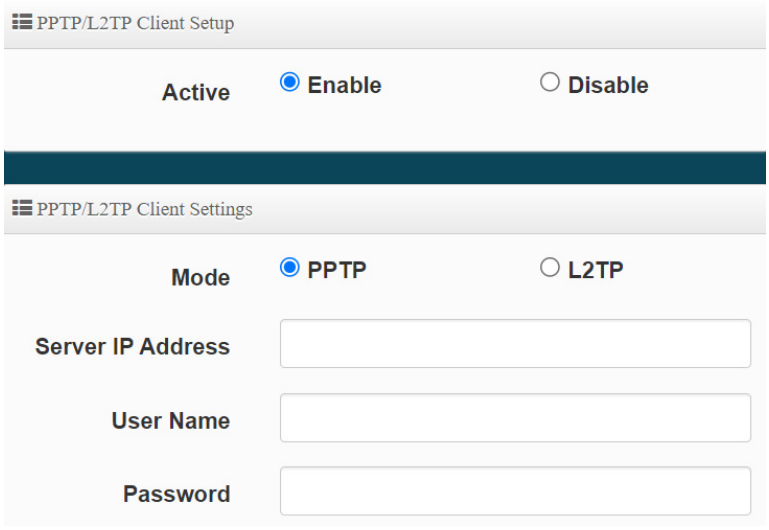


Please click "System"➔"PPTP/L2TP Client setup"



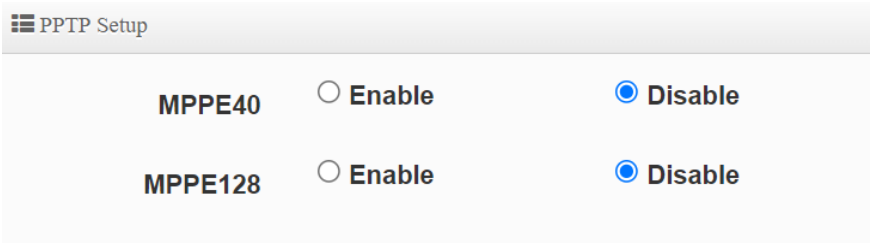


Please click the Create Client button to set client conditions. U Up to 60 client of PPTP/L2TP Client can be created.



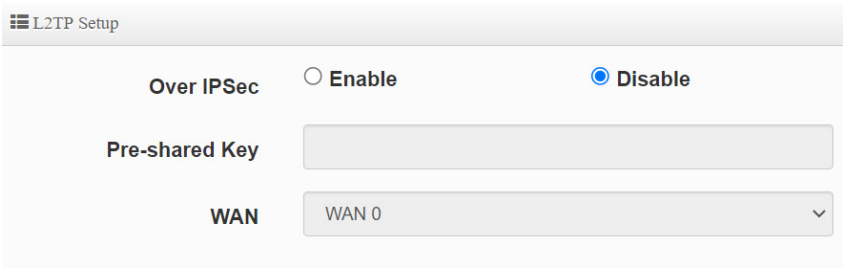
- **Mode:** Administrator can select use PPTP or L2TP protocol connection to remote VPN server. If VPN server used PPTP Protocol then please choose PPTP.
- **Server IP Address:** Administrator must set remote VPN server used real IP address.
- **User Name / Password:** Set VPN authentication account and password (Please Refer to 3.9 Account Setup)

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



- **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



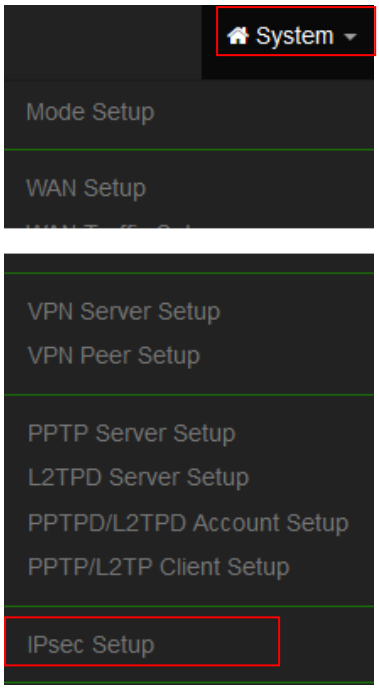
- **Over IPsec :** Choose to enable or disable the Over IPsec VPN protocol.
- **Pre-shared Key :** You can enter a set of password keys
- **WAN :** elect L2TP VPN through the WAN related user interface.

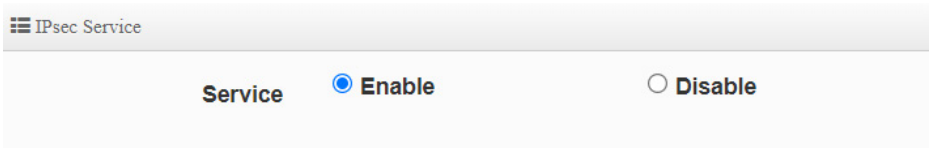
3.12 IPSec Setup

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.**

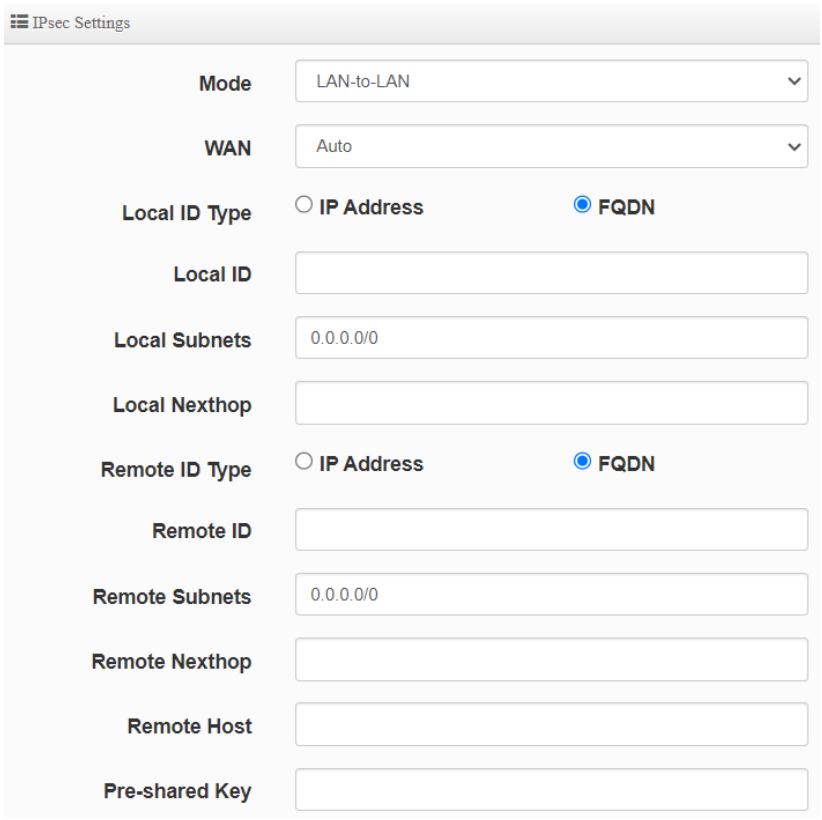
Administrator can create new VPN connection for the IPSec.

Please Click “**System**”➔”**IPSec Setup**”



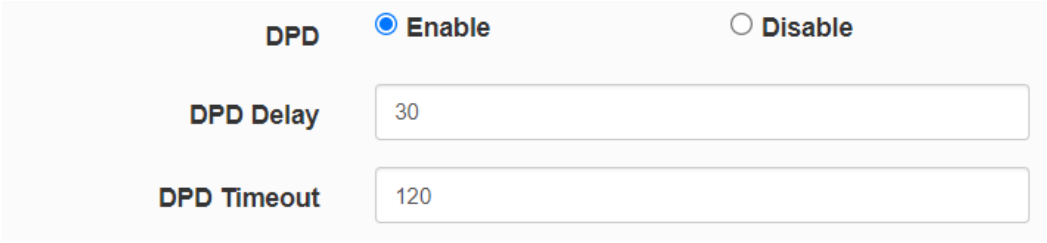


- **Service:** You can choose to turn on or off this function service



- **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".

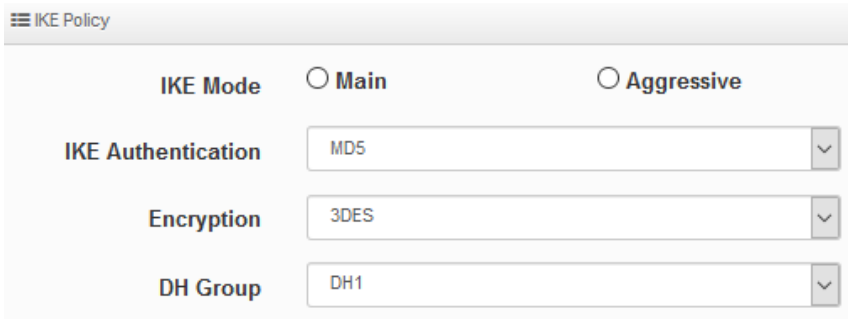
- **Local Nexthop:** Administrator can add a VPN Next hop address for Local.
- **Remote ID Type:** Administrator can select use IP address or FQDN for Remote IP Type.
- **Remote Subnet:** Administrator must set remote Subnet for the VPN "LAN to LAN".
- **Remote Nexthop:** Administrator can add a VPN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



- **DPD:** 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.)

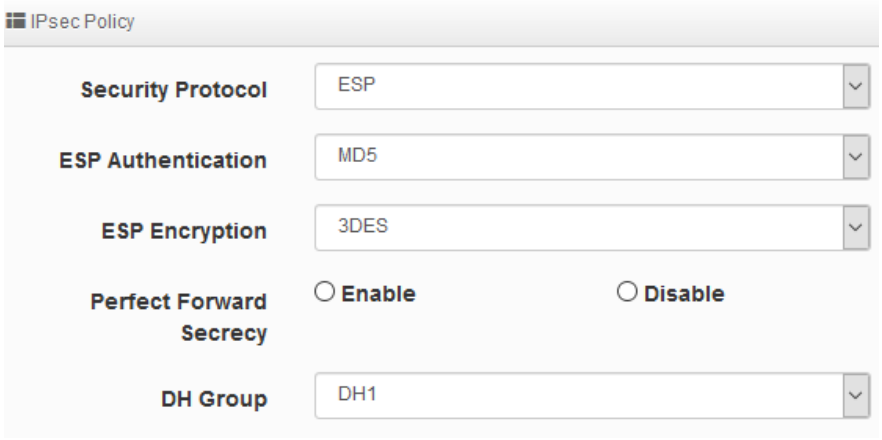
IKE Policy:

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 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-Hellma 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:

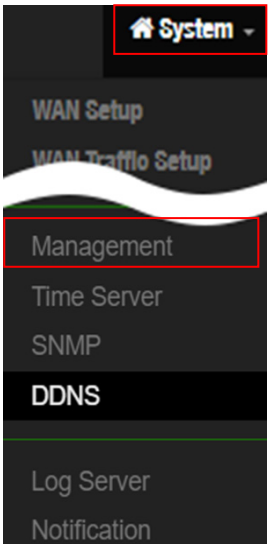


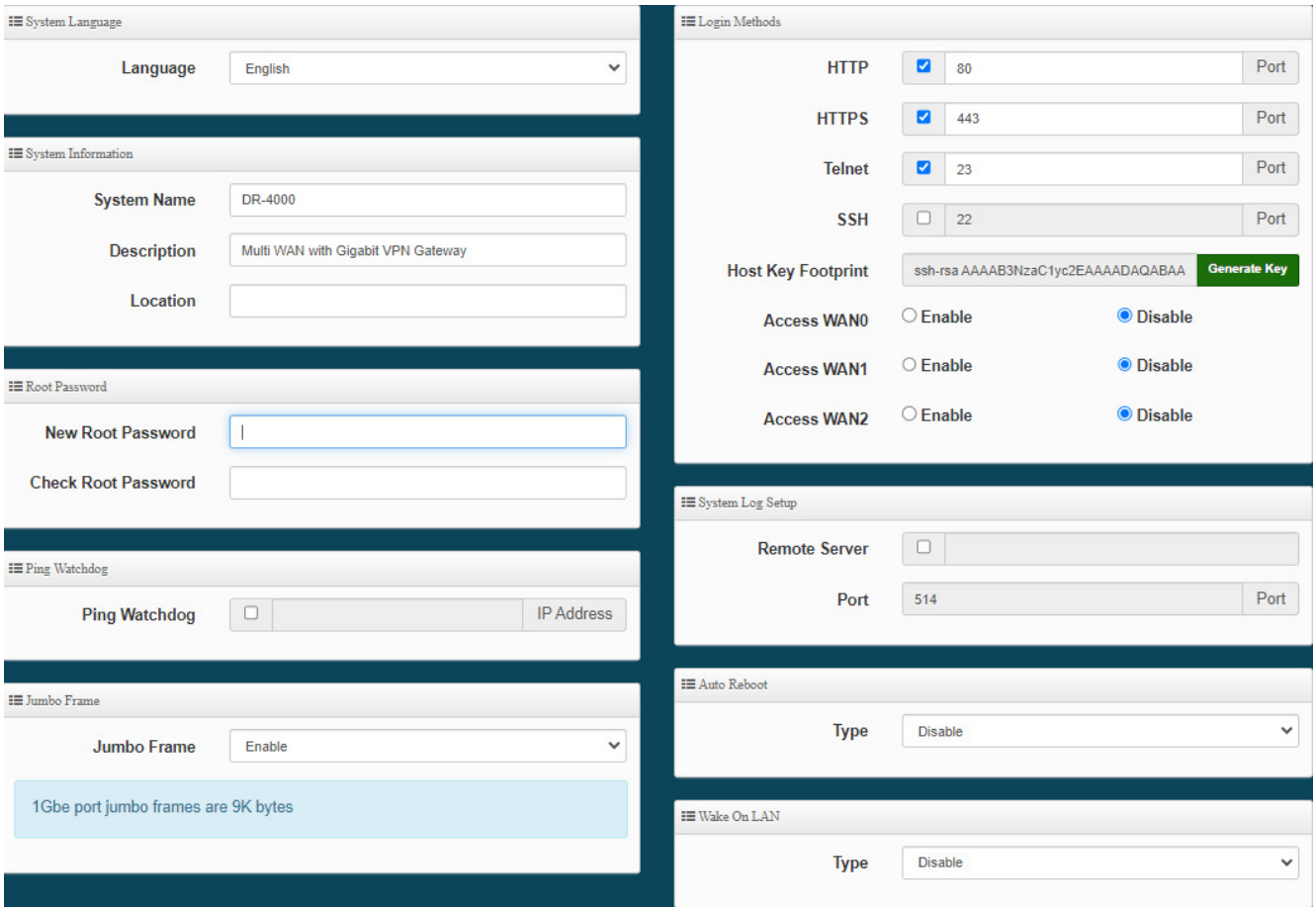
- **Security Protocol:** The IPSec security use ESP protocol.
- **ESP Authentication:** Administrator can select authentication method for MD5, SHA1, SHA2_256.
- **ESP Encryption:** Set encryption method for ESP. Administrator can select use 3DES and AES128/192/256.
- **Perfect Forward Secrecy:** Administrator 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

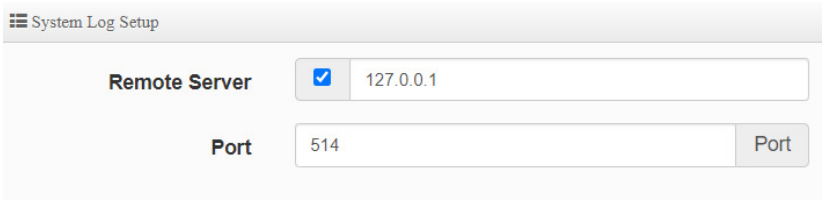
Administrators can specify geographical location of the system via instructions in this page and modify system login password and select use system login protocol by 80, 443, 23, 22 Port.
The management page support syslog server function and system auto reboot function.

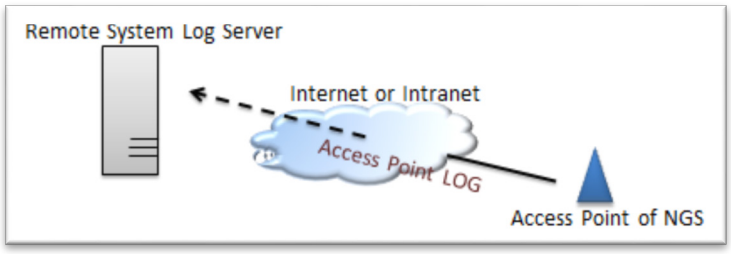
Please Click "**System**"➔"**Management**"





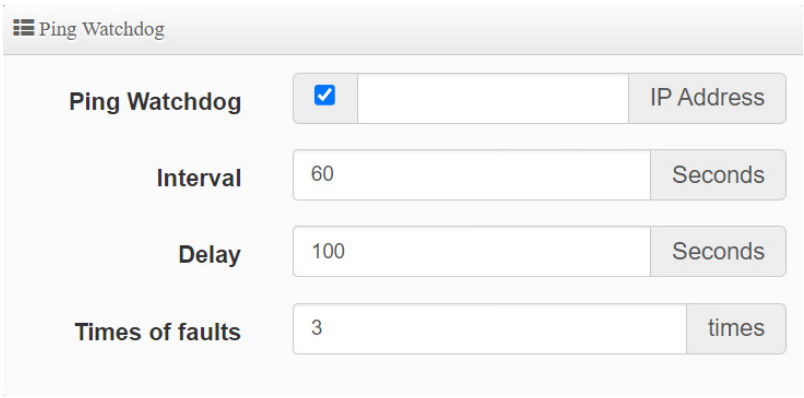
- **Language:** Administrators can choose to change the language of the English or Chinese.
- **System Information:** Administrator can set the system name / Description and Location.
- **Root Password:** Administrator can change system login password.
- **System Log Setup:** Administrator can be backup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





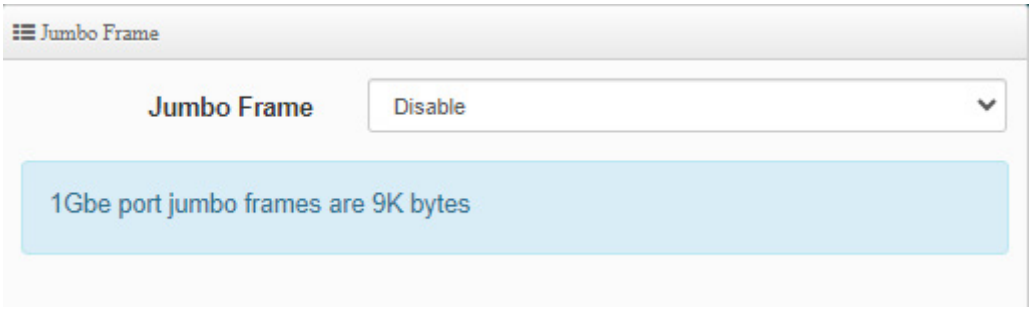
- **Remote Server:** Set the IP address of the remote system Log server。
- **Port:** Set the port number of the remote system Log server. The default Port is 514.

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

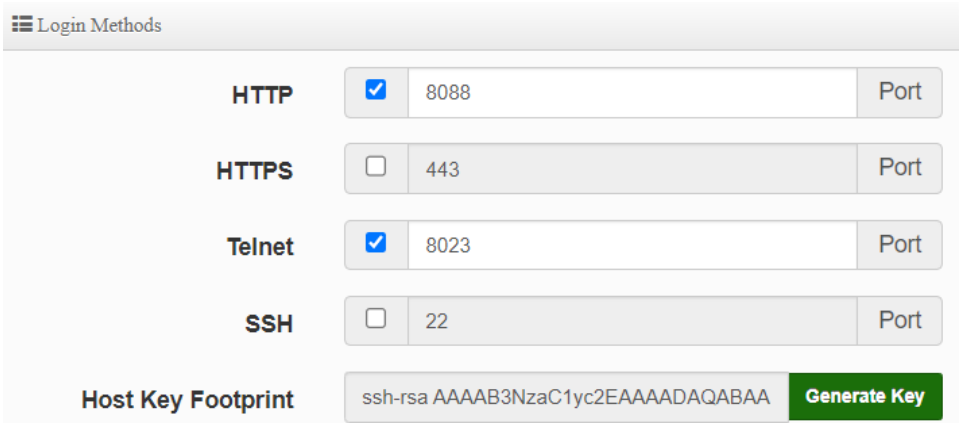


- **Ping Watchdog**：Set the IP address to be monitored for ping.
- **Interval**：Set the interval to ping the IP address.
- **Delay**：When ping fails, how long should you delay before ping again.
- **Times of faults**：When the above conditions are true multiple times, let the system reboot.

➢ **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.



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

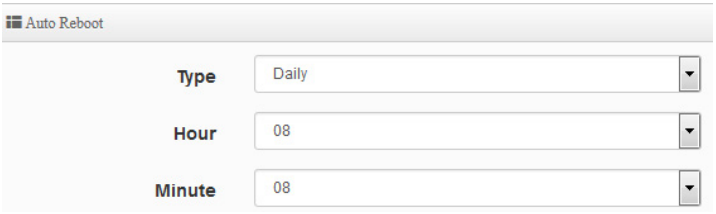


- **HTTP Management**：Check this item will enable the WEB interface to enter the management interface. The default is port 80. (recommended port number between 1025 and 65535)
- **HTTPS Management**：Check this item will enable the WEB interface to enter the management interface. The default is port 443. (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.

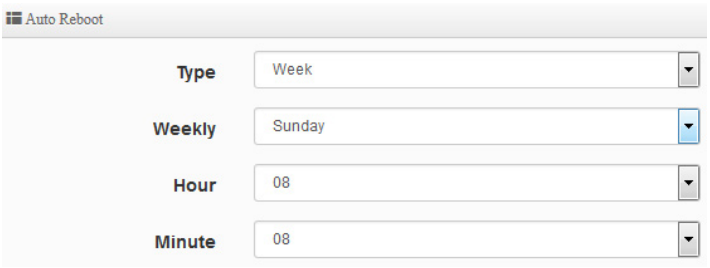
- **Access WAN#:** If enable this WAN# then external (Internet) will can access management interface for **DR-4000-CA**. The default is Disable. (This function can only be used in Router mode).

- **Auto Reboot:** The functions can Auto-reboot the system by Date/time management.

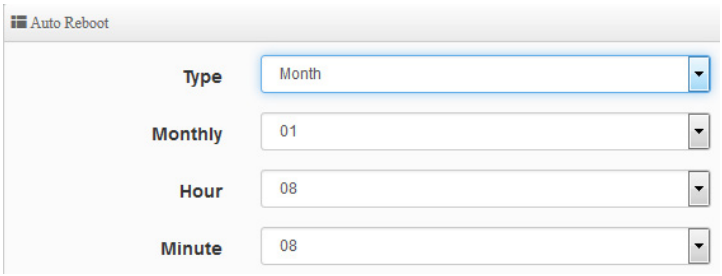
  - **Daily**： Setting time to system reboot.



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

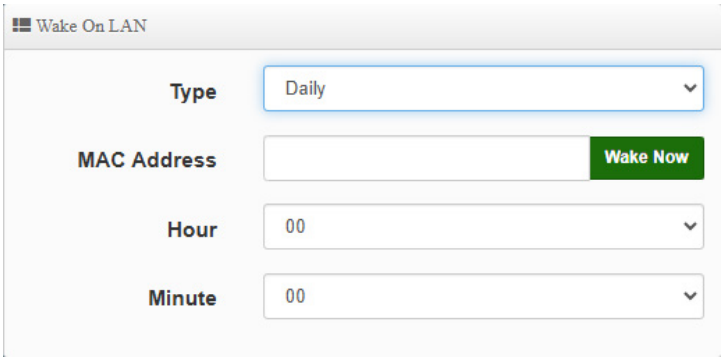


  - **Monthly :** Setting Every month, fixed date and time to system reboot

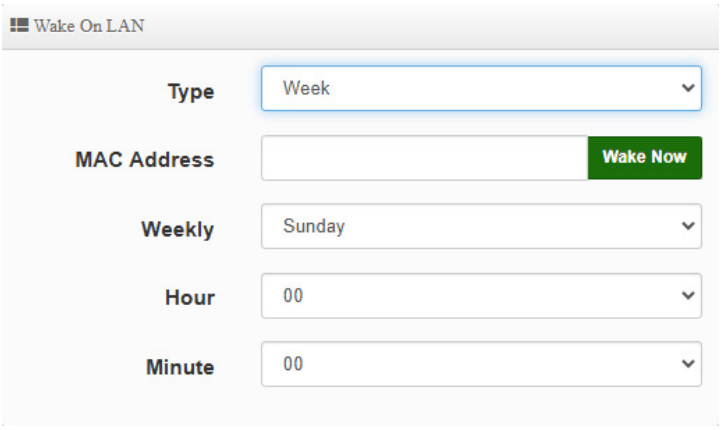


- **Wake On LAN:** This function can fix in the remote MAC address of network card to allow the system to wake up a remote network MAC address device immediately or periodically.

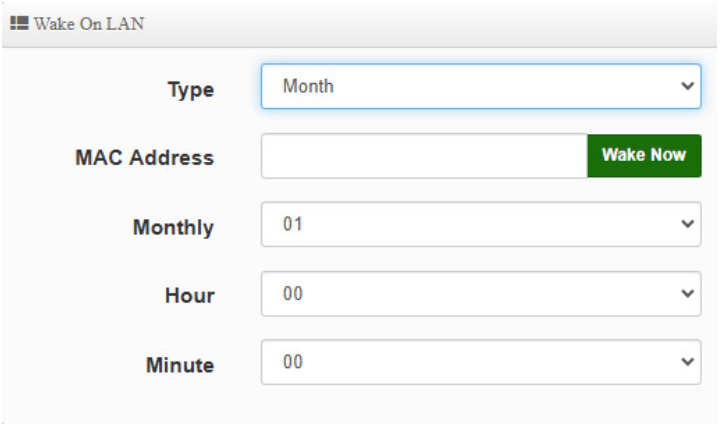
  - **Daily**： Setting every day time for the system to wake up a device with a remote network MAC address.



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

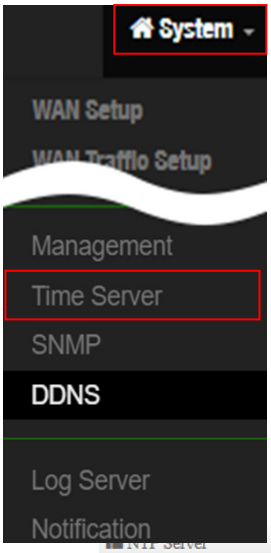


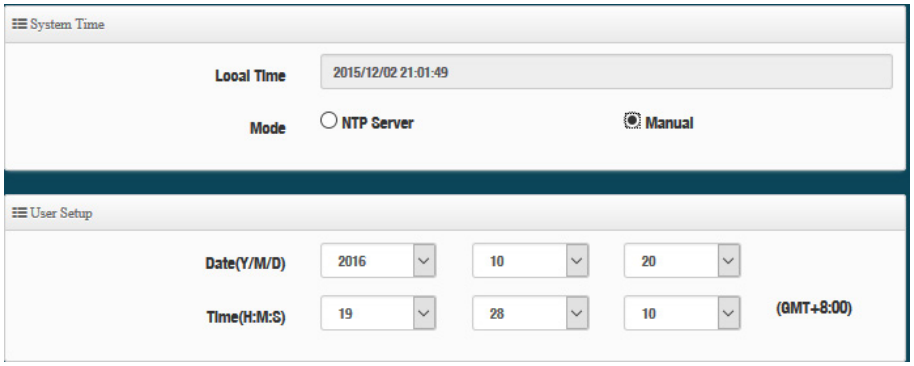
- **Monthly :** Setting Every month time for the system to wake up a device with a remote network MAC address.

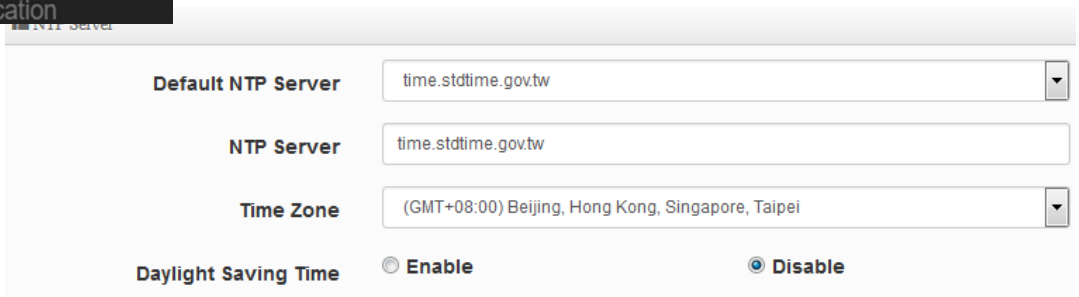


3.14 Time Server

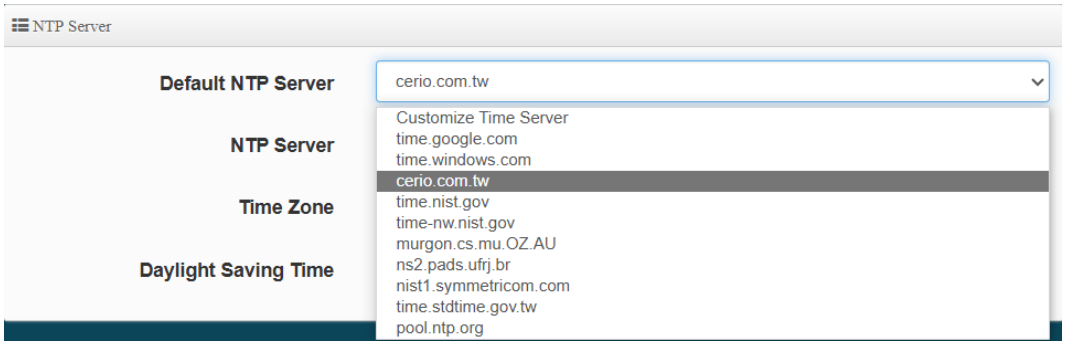
Administrator can select manual or via a NTP server to modify system time for the right local time.
If select update the system time for manual, when administrator reboot system the system time will reply default.
If select update the system time for the NTP Server, system must set gateway and DNS server, the system can be connected internet.





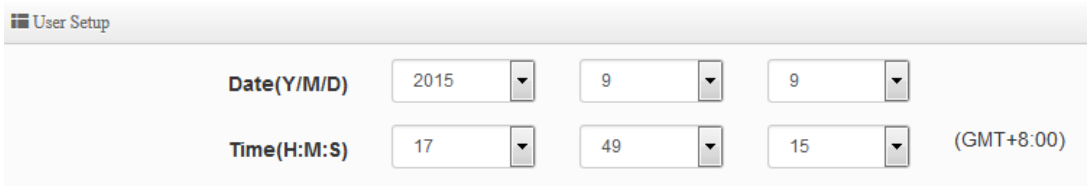


- **Mode:** Administrator can select NTP Server or Manual.
  - **NTP Server:** System can auto update the system time. Administrator needs setting as NTP Server. **For example, select the time server of "cerio.com.tw" on the Internet as the basis for NTP time calibration as follows.**



- ✓ **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.



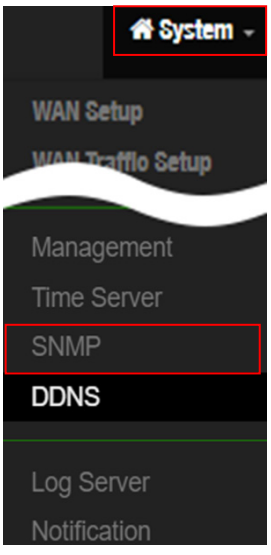
Notice

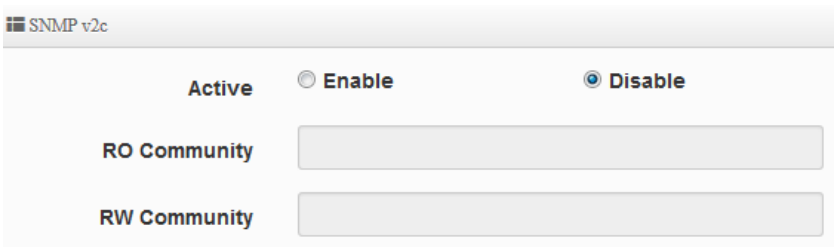
This product supports hardware battery power supply to RTC (Real Time Clock Module) IC real-time clock memory storage module design. When "Manual Update" is selected, if the time cannot be saved and it will always be invalid and return to the default time, then The machine board hardware battery must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

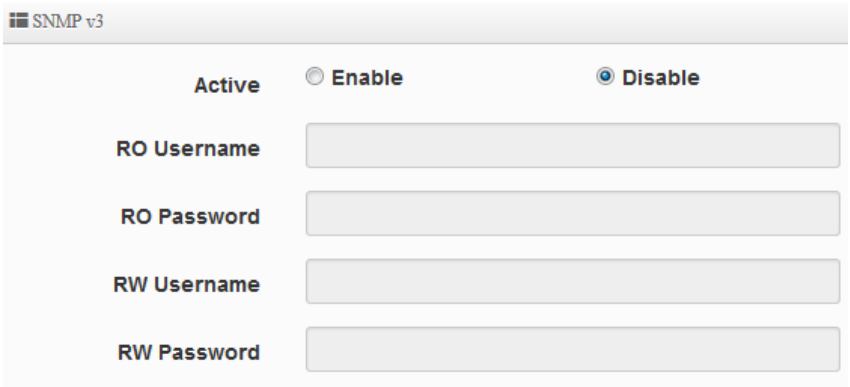




SNMP v2c function

- **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

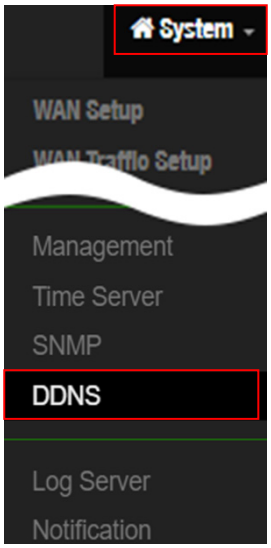
Events such as cold start interface up & down, and association & disassociation will report to an assigned server.

- **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.

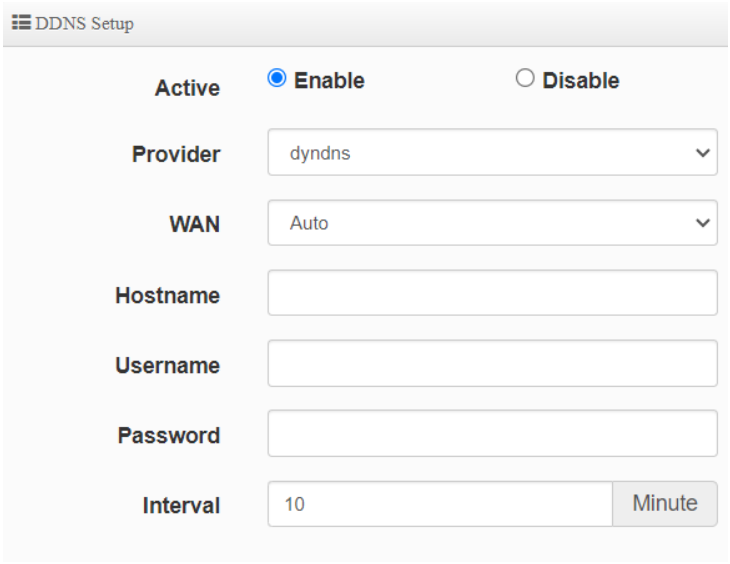
Please click on **System -> DDNS** and follow the below setting.



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

DDNS List

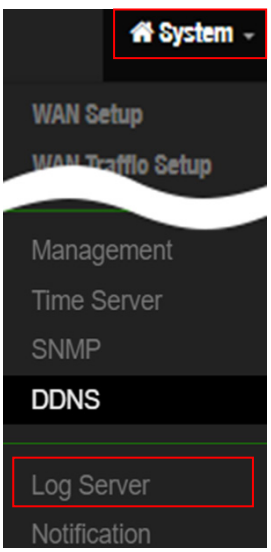
#	Active	Provider	WAN	Hostname	Edit
0	InActive	dyndns	Auto		Edit
1	InActive	dyndns	Auto		Edit
2	InActive	dyndns	Auto		Edit

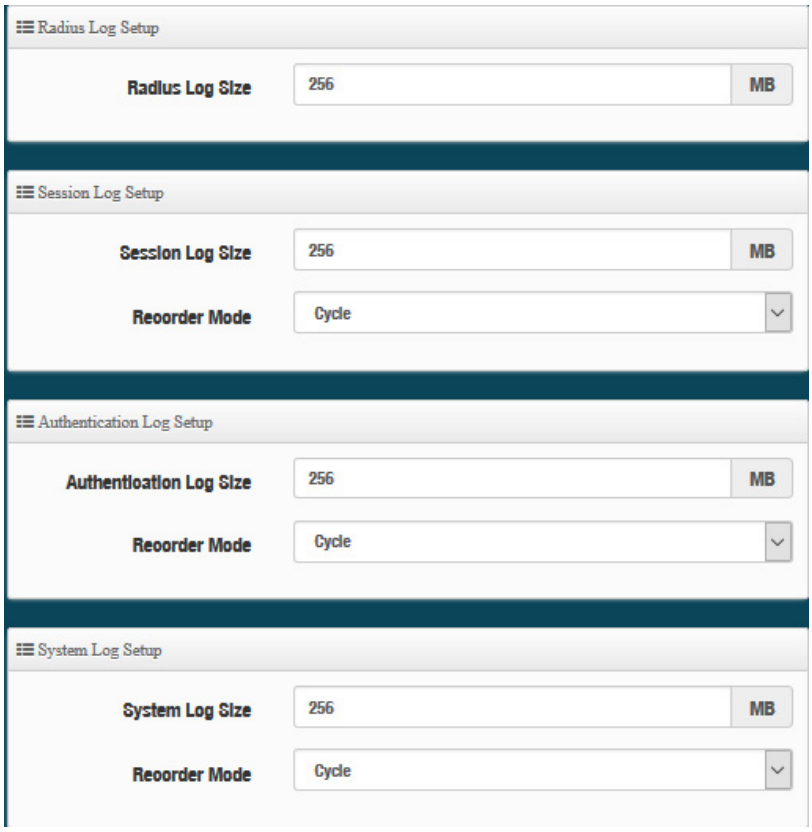


- **Active:** Choose to enable or disable the function.
- **Provider:** Choose the Service provider , built-in support for 2 service providers, namely dyndns and no-ip.
- **WAN:** Select the port for external connection of this machine
- **Hostname:** Enter the host name
- **Username/Password:** Enter 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.





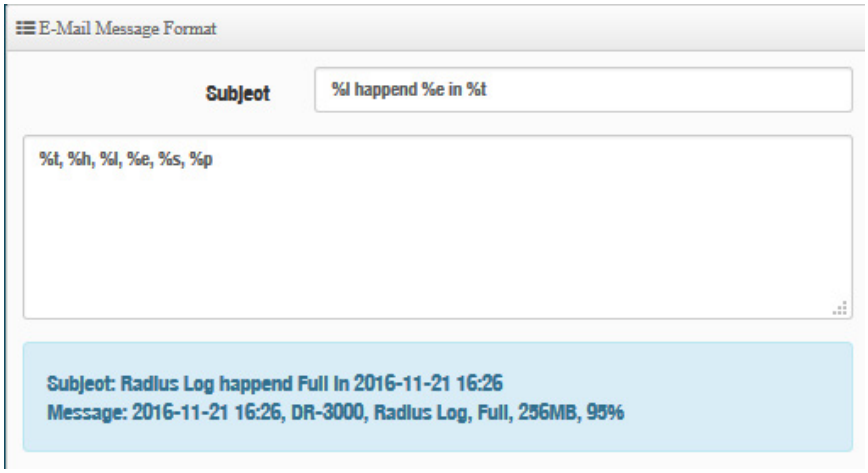
- **Log Size:** Administrator can set storage space for RADIUS/session/authentication and system log.(max.512MB)
- **Recorder Mode:** The function can auto clear Log information or stop services.
  - **Cycle:** System will auto clear log by cycle.
  - **Retention Period:** System will auto clear log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

Notice	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.



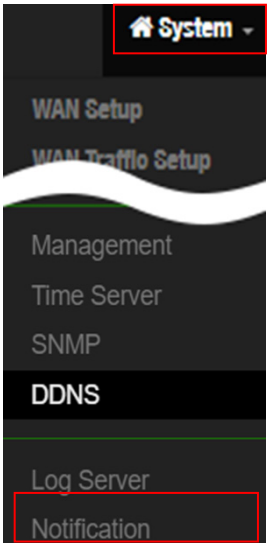
Message Format

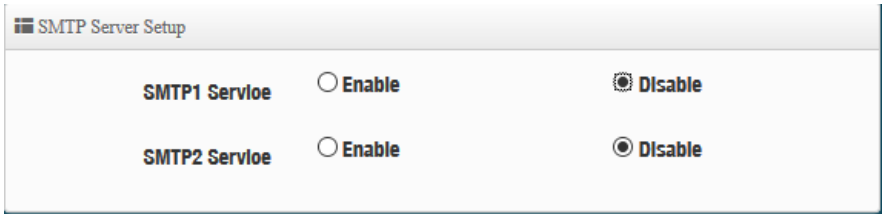
Format	Description
%h	Hostname
%t	Time
%l	Log Type(Radius Log/Session Log/Authentication Log/System Log)
%s	File Size
%p	File Peroentage
%e	Event Type(Full/ Stop Service/ Start Service)

3.18 Notification Setup

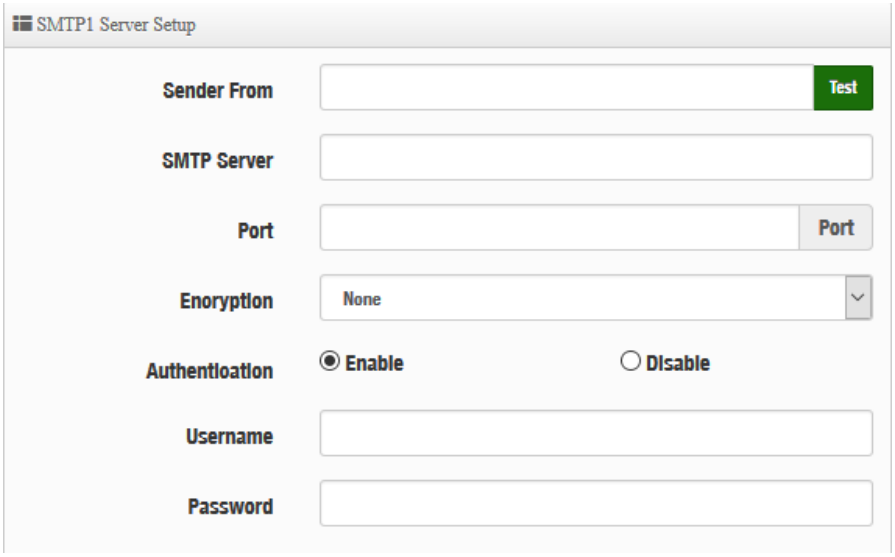
Administrator can automatically send the notification of Radius Log, Session Log, Authentication Log and System Log of 2 particular E-mail addresses. The E-Mail notification setting support SMTP server test, once administrator completed setting up of SMTP, server will able to use the test tool to confirm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

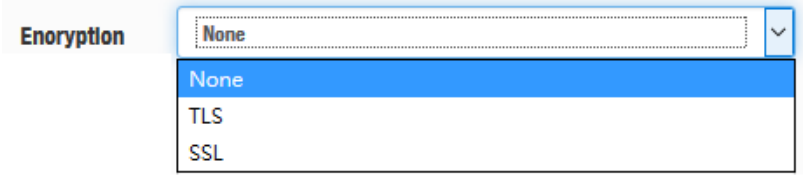




- **SMPT1/2 Service:** Administrator can select Enable or Disable the SMPT functions. If administrator select enable the function will following explains how to configure the SMTP functions.



- **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.

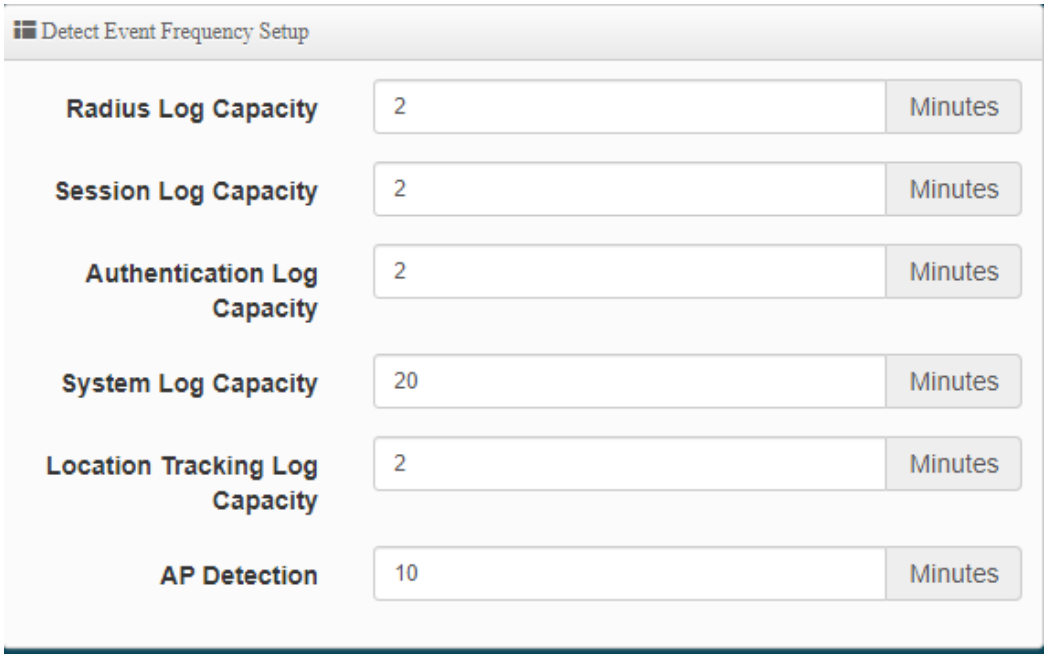


- **Authentication:** If SMTP Server must use authentication, Administrator can select enable the SMTP server authentication for E-Mail user account.

Notification Setup

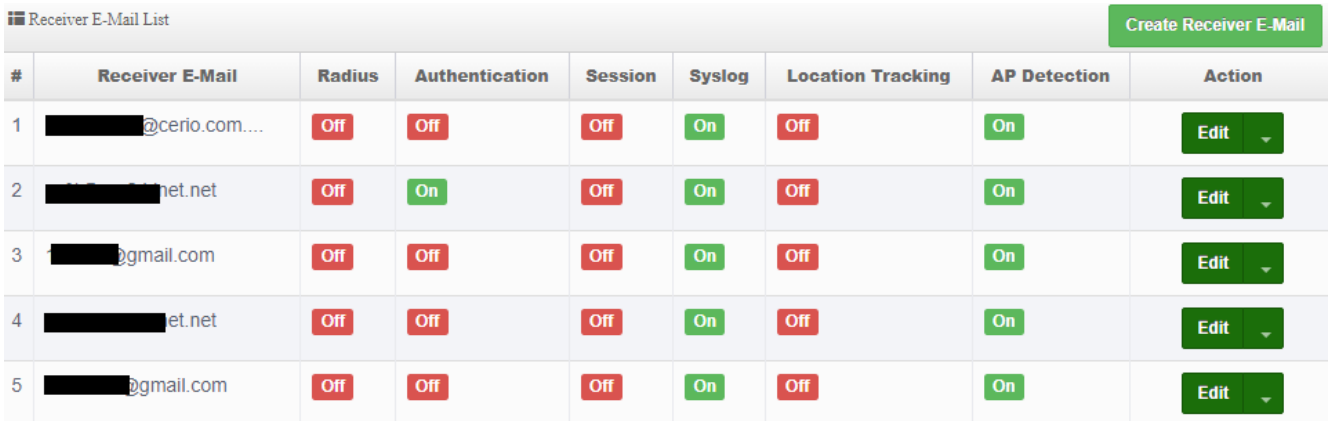
Administrator can set frequency or time for the RADIUS, Session, Authentication and System Log Capacity, Location Tracking Log Capacity, and AP Detection, and send to administrator E-Mail.

For example:



Receiver E-Mail List

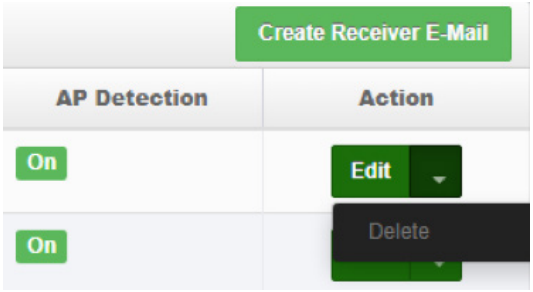
Administrator can click “Create Receiver E-Mail” button to add administrator E-mail address(es.)



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

Deleting the Notification

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

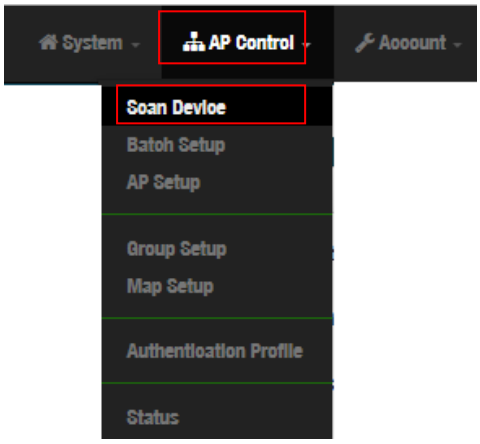


4. AP Control

This function is primarily to control all the CERIO managed AP.
Administrator can use AP Control functions to centralize management of APs in the network architecture. AP control Setting functions have “Scan Device”, “Batch Setup”, “AP Setup”, “Group / Map setup” and Authentication Profile setup etc..
Please click **“AP Control”** to enter AP Management settings

4.1 Scan Device

This management page can discover all managed APs in the network. Administrator can set IP address / Password and VLAN tag for managed APs. After the setup is complete, Administrator must import all managed APs to databases.



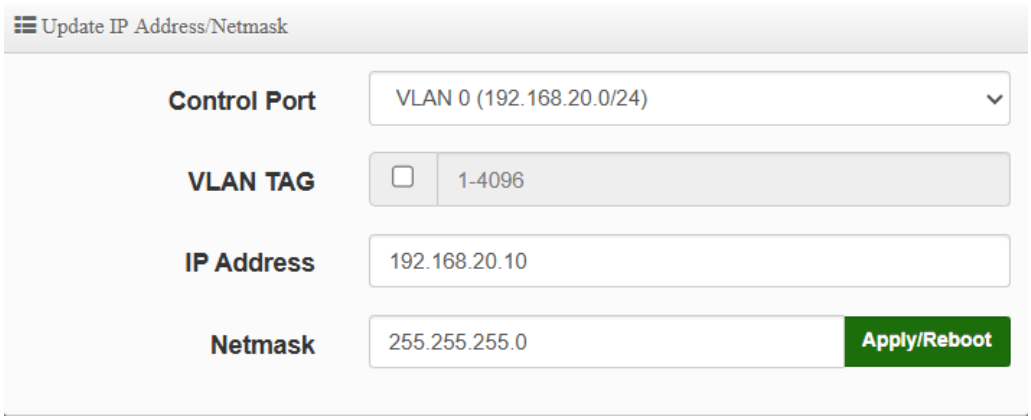
Centralized Management APs operating Instructions:

1) Click **“Scan Device”** to discover Access Points in the network architecture.
2) Set IP address for all managed Access Points and reboot managed Access Points.
3) Re-Scan managed APs and Import to databases.
4) Centralize managed AP settings by clicking “**AP control**” ➔ **“Batch setup”**
5) After the setup is complete for managed APs function, administrator must reboot all managed APs.

This management page can discover all managed APs in the network. Administrator can set IP address / Password and VLAN tag for managed APs. After the setup is complete, Administrator must import all managed APs to databases.

- **VLAN# :** Administrator can select VLAN network to discovery managed Aps
- **Default Password:** Set login system password by managed Aps.
- **Sort**: Administrator can select discovery managed Aps Type. (IP or MAC)

- **#**： Display managed APs items.
- **Device**：Administrator can select all or single for managed Aps**.**
- **IP Address**： Display IP address for managed AP.
- **MAC Address**：Display MAC address for managed AP.
- **Host Name**：Display host name for managed AP.
- **F/W Version**：Display firmware version for managed AP.
- **F/W Date**：Display firmware Release date for managed AP.
- **IP Address**：Administrator can set single IP address for Managed AP.
- **Netmask**：Administrator can set single Netmask for Managed AP.
- **Default**：Administrator click the button will can reset to default for select managed APs.

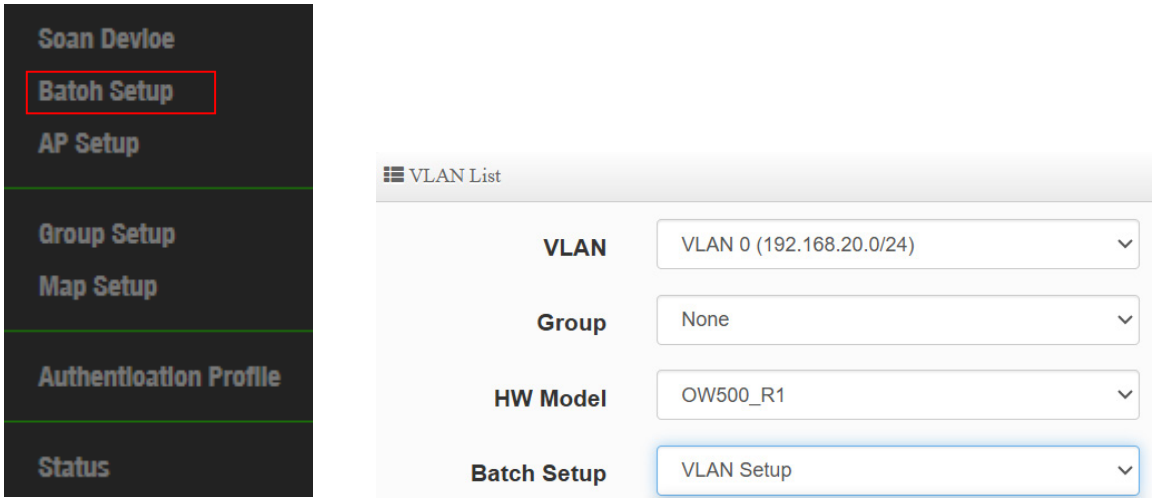


- **Control Port**：Administrator can change VLAN network for managed APs.
- **VLAN TAG**：Administrator can set VLAN TAG ID for managed APs.
- **IP Address**：Administrator can set IP address for managed APs, the IP address is auto-incrementally.
- **NetMask**：Administrator can set NetMask for managed APs.

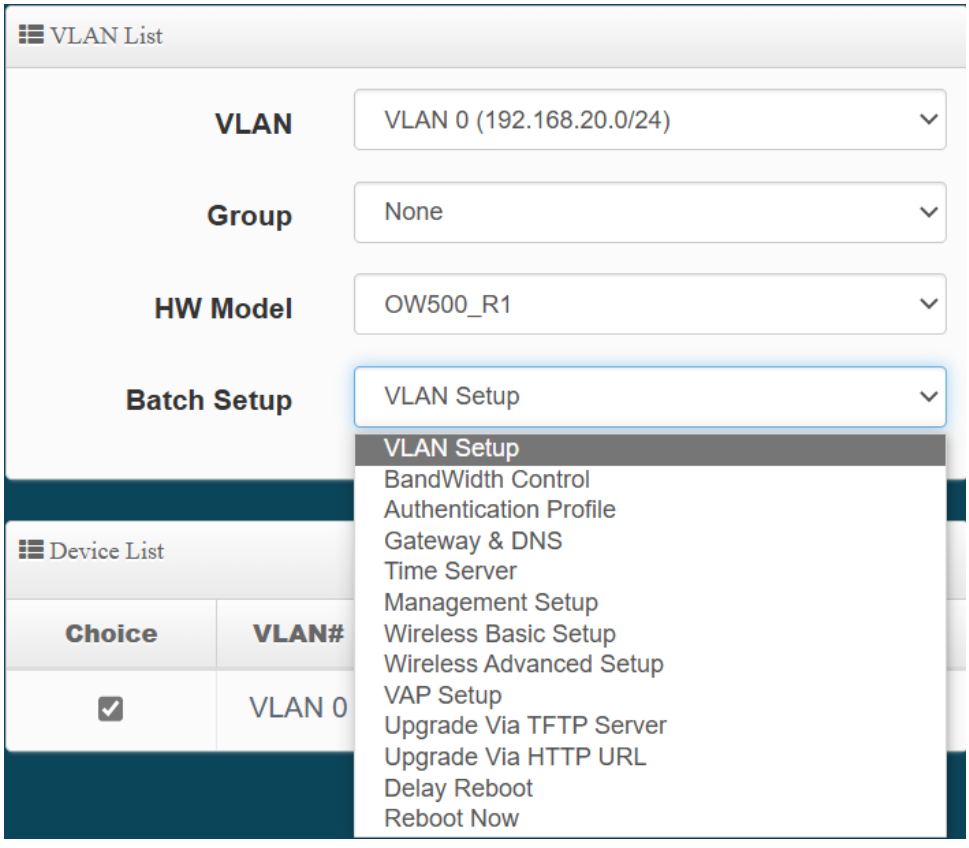
When the setting managed APs is completed, please click Apply & Reboot button to complete the setup process.

4.2 Batch Setup

The AP control function supports centralized configuration of managed APs. Administrator can change VLAN network / Group and batch setup for managed APs.



- **LAN**：When VLAN Tag function is enabled (please refer to 3.3 System VLAN Setup), administrator can change VLAN tag for managed APs.
- **Group**：When AP Groups are created (please refer to 4.4 Group setup), Administrators can select and change group settings of managed APs.
- **Batch Setup**：Administrator can centralize setting changes for managed APs.



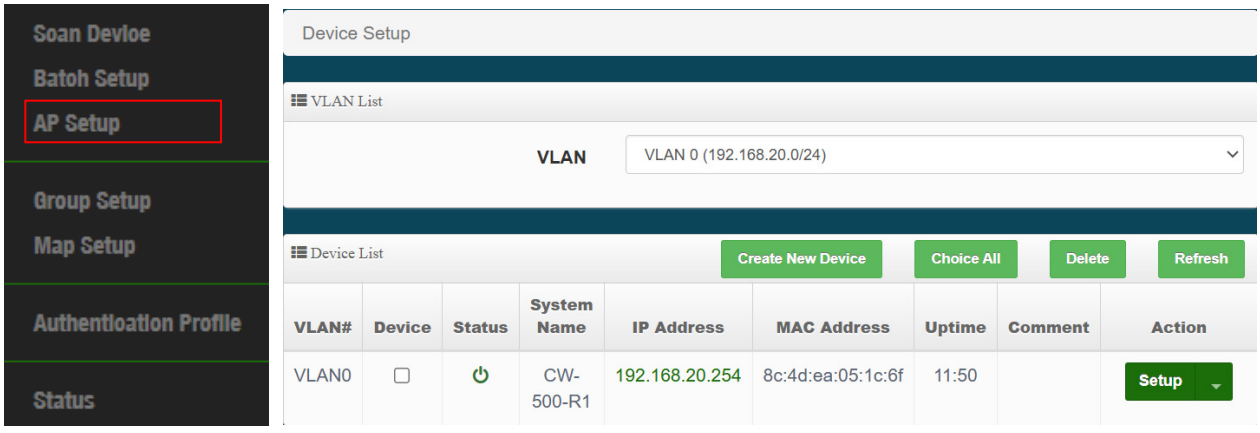
- **VLAN Setup**：Administrator can set VLAN Tag, IP address and Wi-Fi on/off for the managed APs.
- **BandWidth Control :** The maximum/minimum bandwidth can be managed. User bandwidth management can limit the bandwidth limits of IP/MASK, IP Range, Port(Service), SIP, RTP/RTSP, WEB, etc.
- **Authentication Profile**：After creating Profiles, See: “4.6 Authentication Profile” users can conveniently apply Authentication profiles
- **Gateway & DNS:** Setting Gateway and DNS for managed APs.
- **Time Server:** Setting System Time for managed APs. (
- **Management Setup:** Setting system name/ system login port and system log server service for managed APs. (Please refer to 3.13 system management)
- **Wireless Batch Setup:** Setting Wi-Fi configurations for managed APs.

Notice	Wireless AP station: If the managed AP is a 2.4G frequency,, Radio 0 (2.4G) must be selected, and if it is a 5G frequency and Radio 1 (5G) must be selected.

- **Wireless Advanced Setup:** Setting Wi-Fi Advanced settings for managed APs.
- **VAP Setup**：Wi-Fi SSID / channel or security settings for managed APs.
- **Upgrade via TFTP Server:** Administrator can centrally upgrade firmware via TFTP Server for the managed APs.
- **Upgrade via HTTP Server:** Administrator can centrally upgrade firmware via HTTP Server for the managed APs.
- **Delay Reboot:** Administrators can set managed APs to reboot after the wait time
- **Reboot:** Administrator can reboot managed APs.

4.3 AP Setup

Administrator can monitor statuses and modify managed APs information.

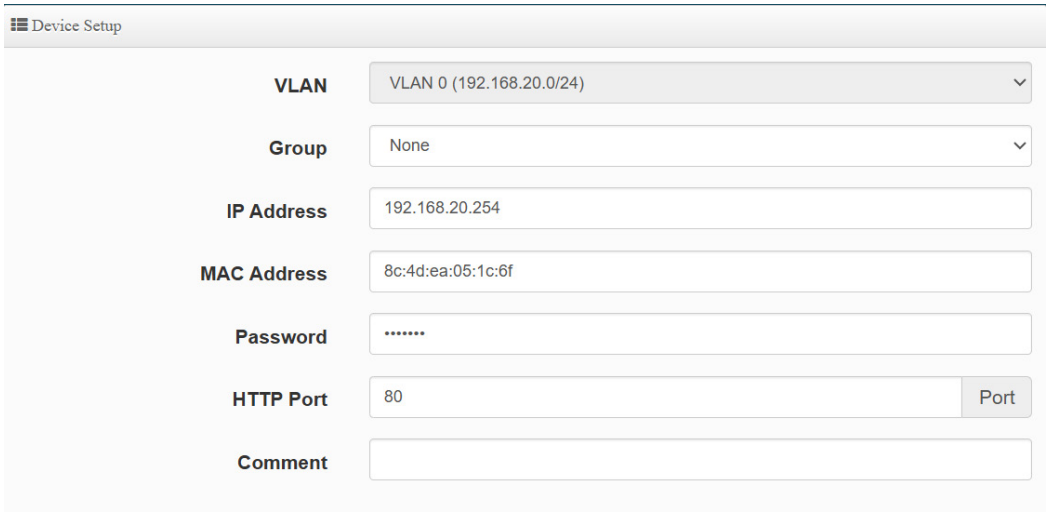


#Device List

- **VLAN** : Select desired VLAN for AP setup
- **Device** : Select a specific managed AP.
- **Status** : Displays whether the managed AP is currently offline or online. (Green means online operation, red means offline)
- **System name** : If the managed AP has a system name set, the system name of the managed AP will be displayed.
- **IP address** : Displays the IP address of the currently managed AP
- **MAC Address** : Displays the MAC address of the currently managed AP
- **Uptime** : Displays the startup time of the currently managed AP system.
- **Comments** : Display customized comments.
- **Action** : You can delete the managed AP's list in the management database, or modify the IP address and information of the managed AP, etc..

☐ # Active for Setup

- **Setup**：Administrator can modify IP addresses, system login passwords, and web login port for managed APs. If administrator has change AP devices, administrator can modify MAC address of the new managed AP.

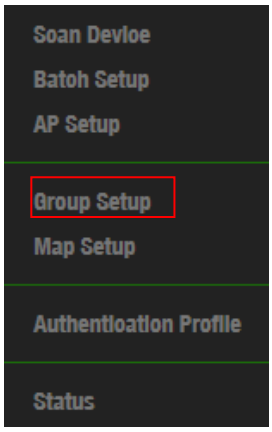


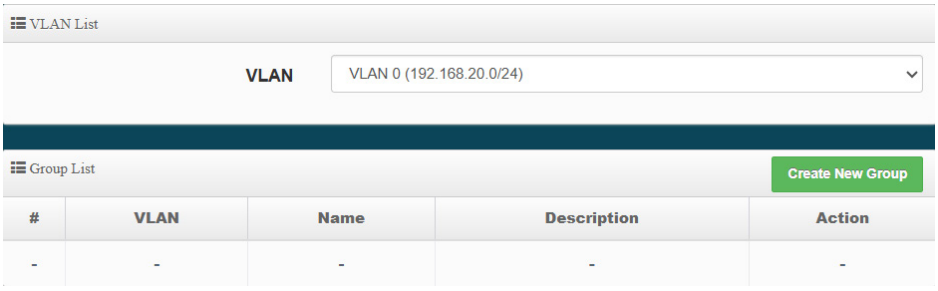
- VLAN: Displays the VLAN to which this wireless base station belongs.
- Group: You can choose to add this wireless base station to a group or change the group.
- IP address: Displays the IP address of this wireless AP station. You can also change the IP address here.
- MAC Address: Display the MAC address of this wireless AP station.
- Password: You can modify the management interface login password of this wireless AP station.

- HTTP Port: The port number used to log in to the management interface of this wireless AP station. The default is 80 Port.
- Comments: You can customize your own comments here.

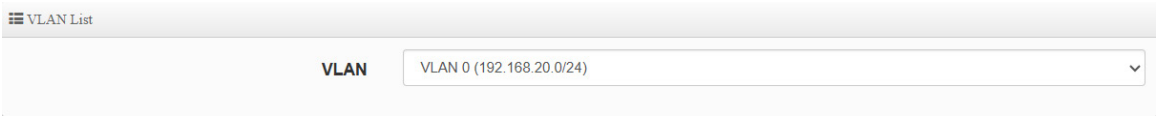
4.4 Group Setup

Administrator can create Groups within the same VLAN.





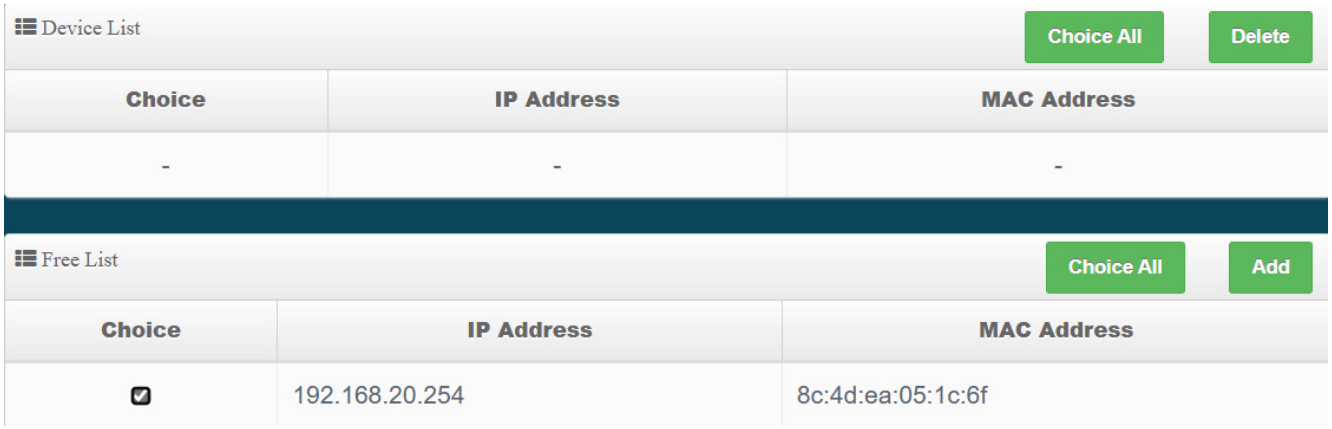
➢ **VLAN**：Select VLAN, Administrators can choose which VLAN to create the group under



➢ **Create New Group**：Click the button to create a new AP Group

✓ 

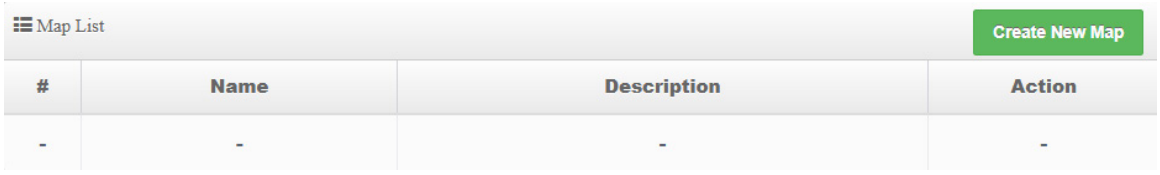
: Administrator can select the **Device button** managed APs and import them into the Group.



- ✧ The above list is the list of APs currently managed by this group. If you select a specific wireless base station and press the "Delete" button, the selected wireless base station will be kicked out of the group. ◦
- ✧ The above list is a list of managed APs that are not currently added to the group. Administrators can select the wireless base station they want to add and click the "Add" button. The selected wireless base station will enter the "AP Device List" field. , indicating that the selected wireless base stations are indeed in the same group ◦

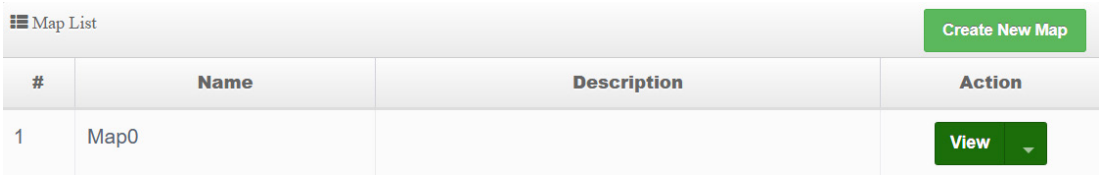
4.5 Map Setup

The Map Setup feature allows administrators to upload a floor plan image to **DR-4000-CA** server and then use the image to import the map into the AP user interface. Once the image is uploaded, administrators can use the Map Setup function to map out the locations of the AP network.



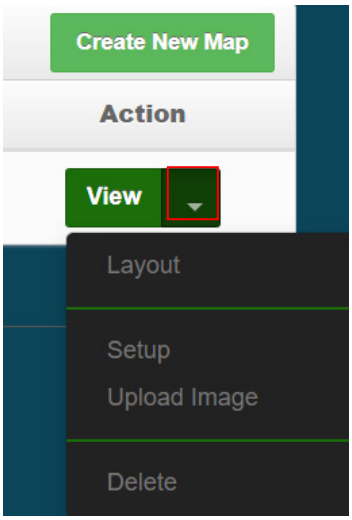
Administrator can click **“Create New Map”** button to upload Map image.

- ➢ **Map Name:** Administrator can set Map name.
- ➢ **Description:** Administrator can set description for map.



View ：Once the Map is created and properly in the Map List, administrators can click the "Layout" button in the action tab to map out the AP network. Managed APs will appear in the "Device List" section of the layout page. Administrators can simply drag the AP (IP Address) to the correct installation location.

Operation sequence for View Pull-down menu

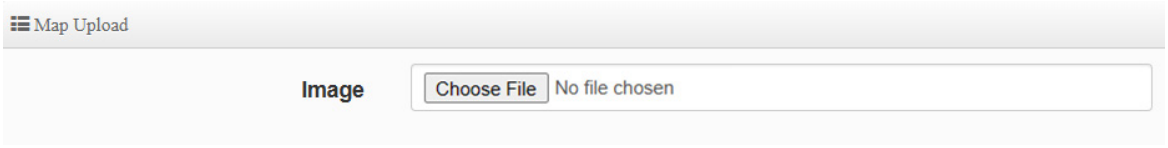


- **Layout:** This function can mainly drag the AP to the location where it is set up on the map, so that the administrator can clearly know the location of the AP and facilitate management. As shown in the figure below, the upper field is the wireless base station. Use the mouse drag method to pull the AP to the correct installation position. After confirming that it is completed, click the Save button to complete the saving action..
- **Setup:** You can re-modify the name and description of the Map.
- **Upload Image**：Upload area floor plan.
- **Delete:** Delete this Map data.

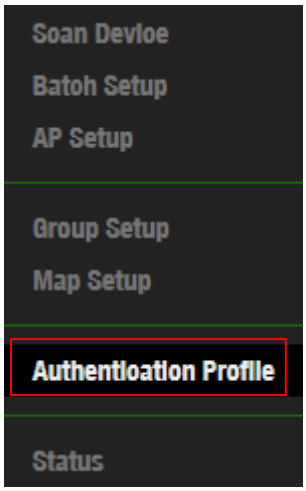
1) Administrator must first click **"Upload Image"** to upload the image.
2) Administrators can click the **"Layout"** function to map out the AP network.

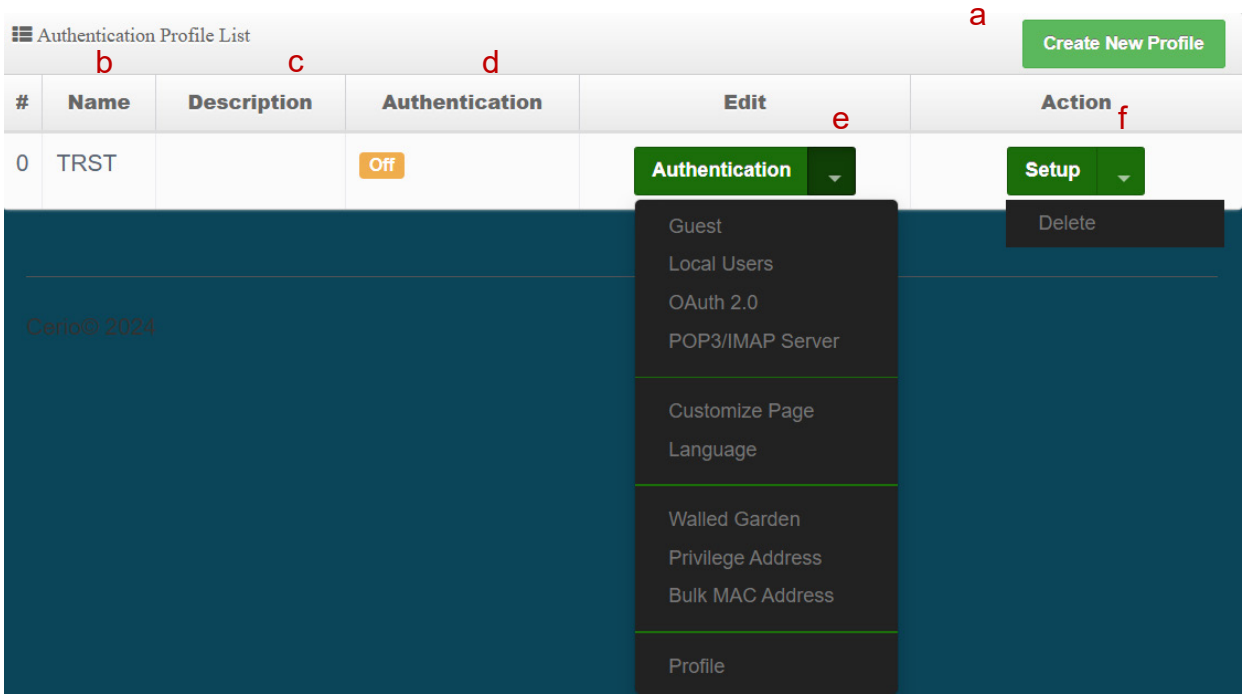
3) Once complete, administrators can click the "**View**" button to monitor AP statuses and locations.

4) If administrator must modify the description of the Map, please click "Setup" to modify.



4.6 Authentication Profile





a : Create an authentication profile, name and description, etc.

b: Displays the name of the authentication profile.

c: Display the description of the profile.

d: Displays whether the web authentication function of this profile should be enabled.

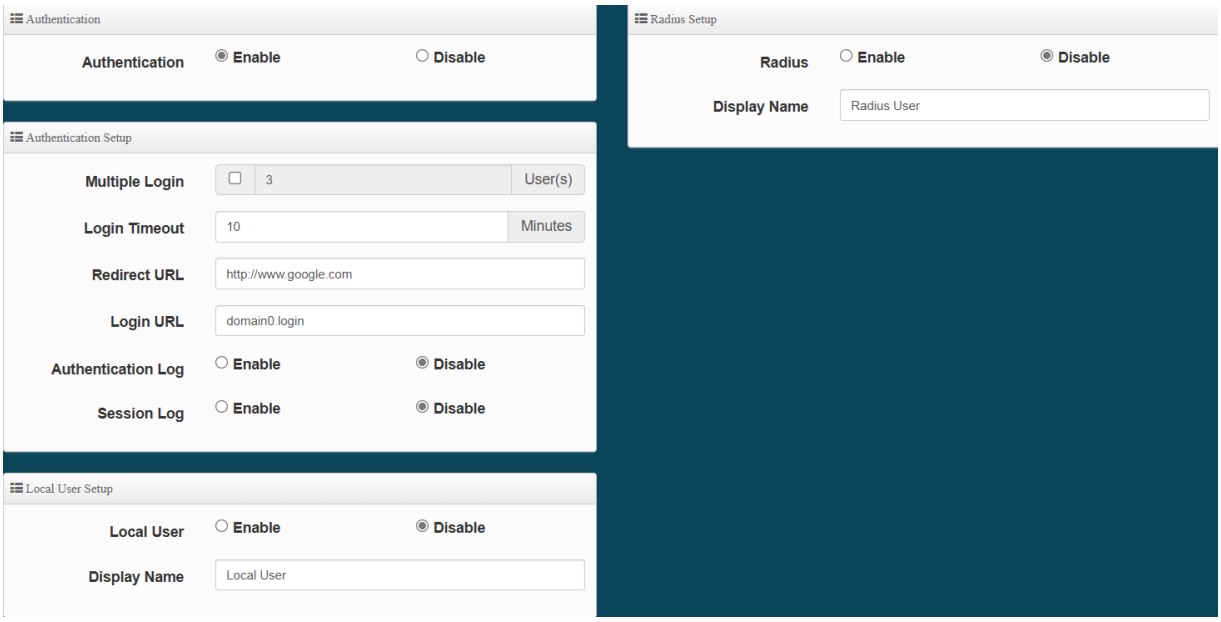
e: Edit the functional conditions for web page authentication. Once this condition is set, the setting values for multiple managed APs can be applied in "4.2 Batch Settings", so that the web page authentication conditions of all managed APs can be applied. All use this profile.

Notice	For advanced instructions on setting this drop-down item function, please refer to Chapter 3.4 “Authentication” Function Detailed Instructions.

f: You can delete this profile or modify the name description of this profile.

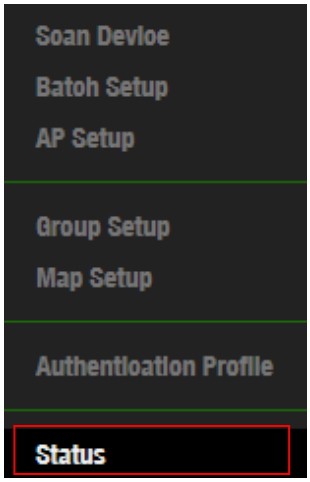
- **Create New Profile**：Administrator can create authentication profile.
- **Edit**： 

Click the Authentication button to Enable or Disable authentication function.

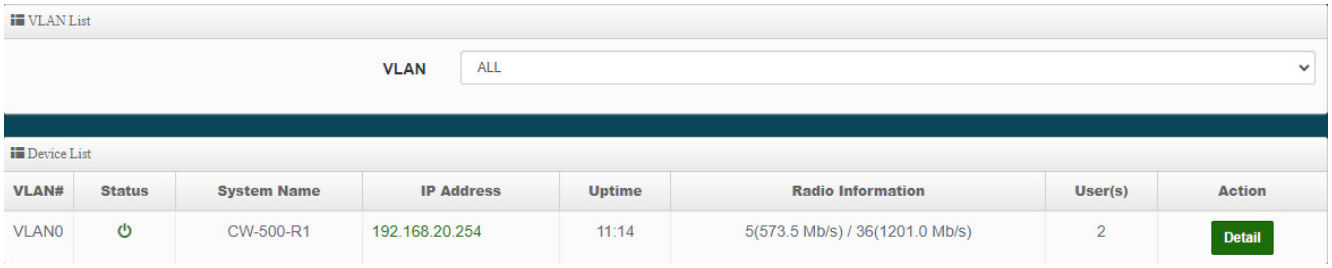


Notice	For instructions on setting this "Authentication function", please refer to Chapter 3.4 Detailed Description of “Authentication” Function.

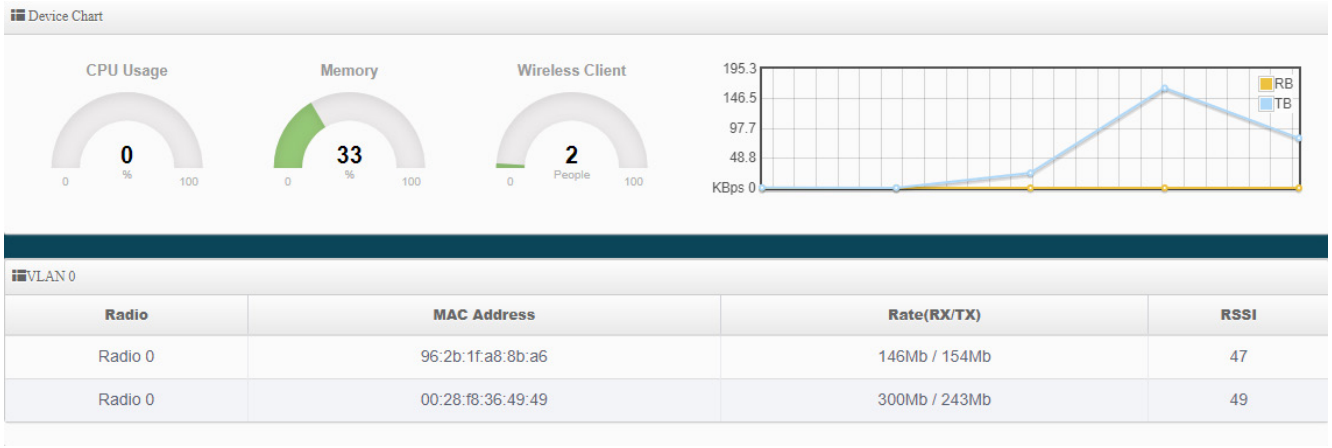
4.7 Status



Administrator can monitor Tx/Rx flow information, show online users and check system CPU / Memory information and on/off line for the managed APs. The information data display support graphical interface.



- **VLAN#**：Displays the VLAN information to which the managed AP belongs.
- **Status**：Displays the operating status of the managed AP, whether offline or online.
- **System name**：Displays the name information of the managed AP.
- **IP address**：Displays the IP address information used by the managed AP.
- **Uptime**：Displays the operating time of the managed AP.
- **Radio information**：Displays the WiFi channel information enabled by the managed AP.
- **User(s)**：Displays the current client users of Wi-Fi connections to the managed AP.
- **Action**：Click “Detail” to enter, including viewing the system’s CPU/Memory usage and displaying traffic charts as images.

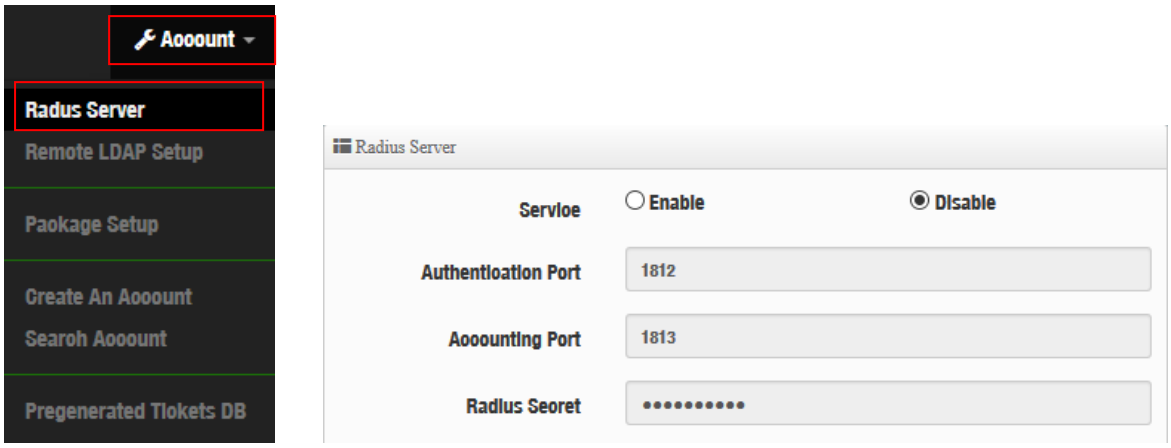


- **Radio :** Displays the Radio information accessed by the connected wireless network. Radio is a 2.4Ghz AP and Radio1 is a 5Ghz AP.
- **MAC Address** ：WiFi users connected to the WiFi AP for access client card MAC address information.
- **Rate(RX)** Reception：Displays the WiFi receiving connection speed of the managed AP.
- **Rate(TX)** Transmission：Displays the managed AP wireless transmission connection speed.
- **RSSI**：The connection quality of the wireless network access connected to the WiFi AP station, expressed in RSSI. The higher the value, the better the quality.

5. Account

This function is a RADIUS server, and allows managed Cerio APs to utilize the RADIUS server authentication of **DR-4000-CA**, and its many authentication types. When managed Cerio APs enable authentication through external RADIUS server, administrators must first set the IP address of **DR-4000-CA** in each managed access point to properly redirect authentication clients.
Cerio's **DR-4000-CA** Account functions support Package, Pregenerated Tickets and remote LDAP(AD) authentication type.

5.1 RADIUS Server

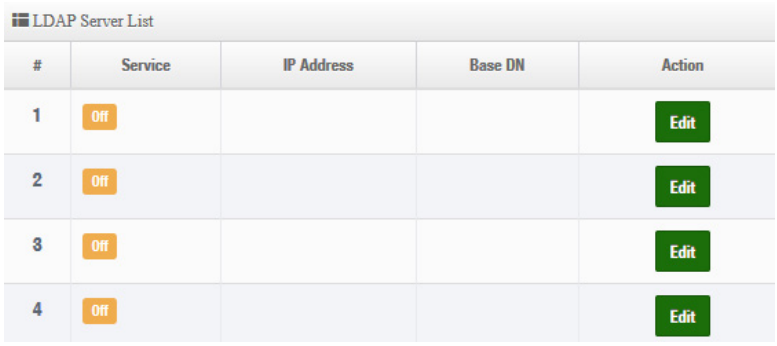


- **Service:** Administrator can select Enable or Disable the RADIUS Server.
- **Authentication Port:** Administrator can set authentication port for RADIUS Server, the default port is 1812.
- **Accounting Port:** Administrator can set accounting port for RADIUS Server, the default port is 1813.
- **Radius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

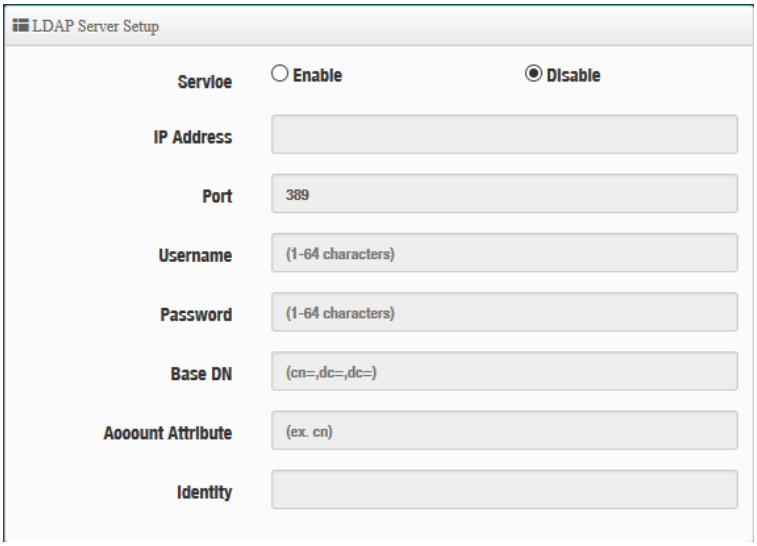
5.2 Remote LDAP Setup

Remote LDAP Setup enables Remote LDAP authentication for managed access points. Administrators wishing to enable Remote LDAP authentication must copy and paste **DR-4000-CA**'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.

- **Service:** Administrator can select Enable or Disable the authentication function.
- **Radius Port:** Administrators can set the Radius server port of the **DR-4000-CA** to provide Cerio managed APs links. If Cerio managed 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.



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



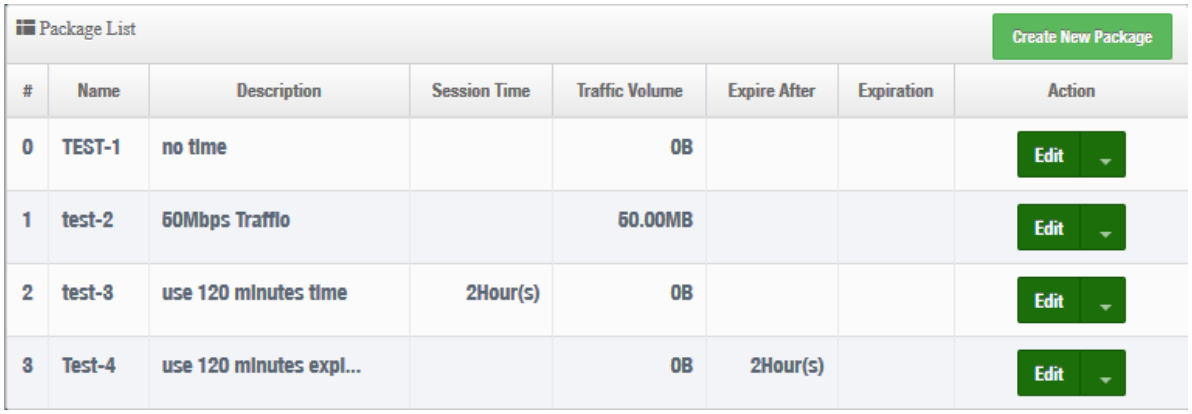
- **Service:** Administrator can select Enable or Disable the function.
- **IP Address:** Set IP address for remote LDAP(AD) server.
- **Port:** Set Port for remote LDAP(AD) server.
- **Username:** Set login account for remote LDAP(AD) server.
- **Password:** Set login account use password for remote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

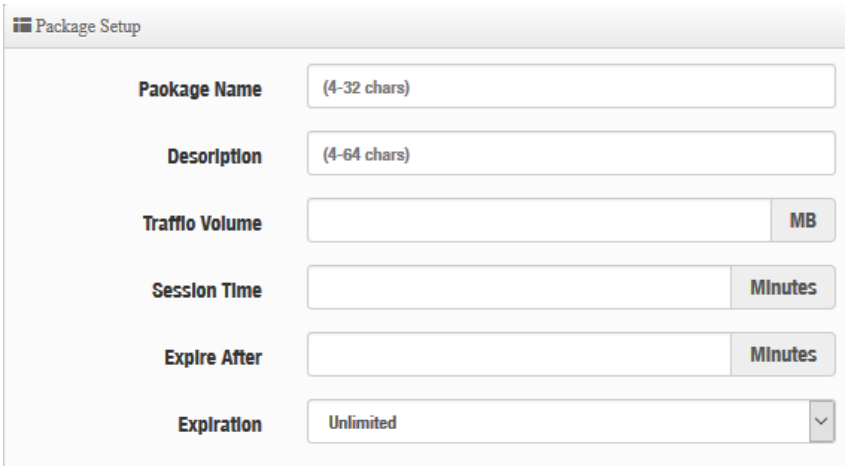
Administrator can set remote LDAP(AD) timeout.

5.3 Package Setup

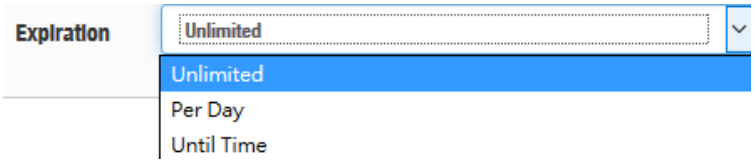
Administrator can set internet time rules for package authentication type.



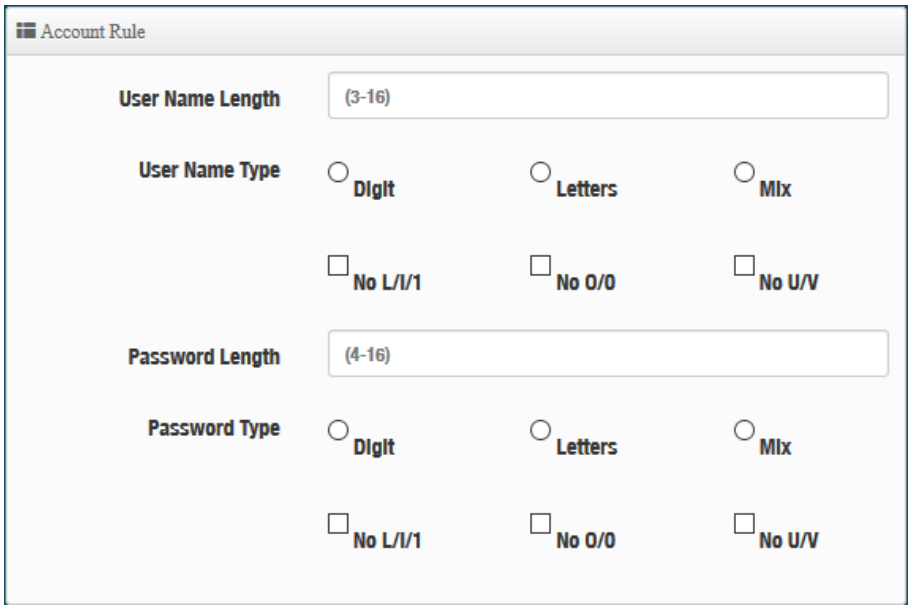
- **Create New Package:** Administrator can click **"Create New Package"** button to set package rules.
- **# :** Package list (0~9) is Network control server (SP-800) code, administrator can choose code to print account.



- **Package 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.

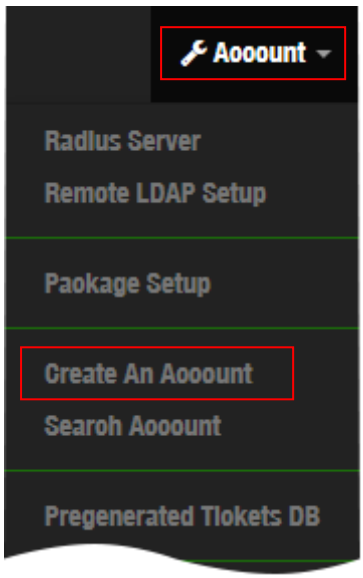


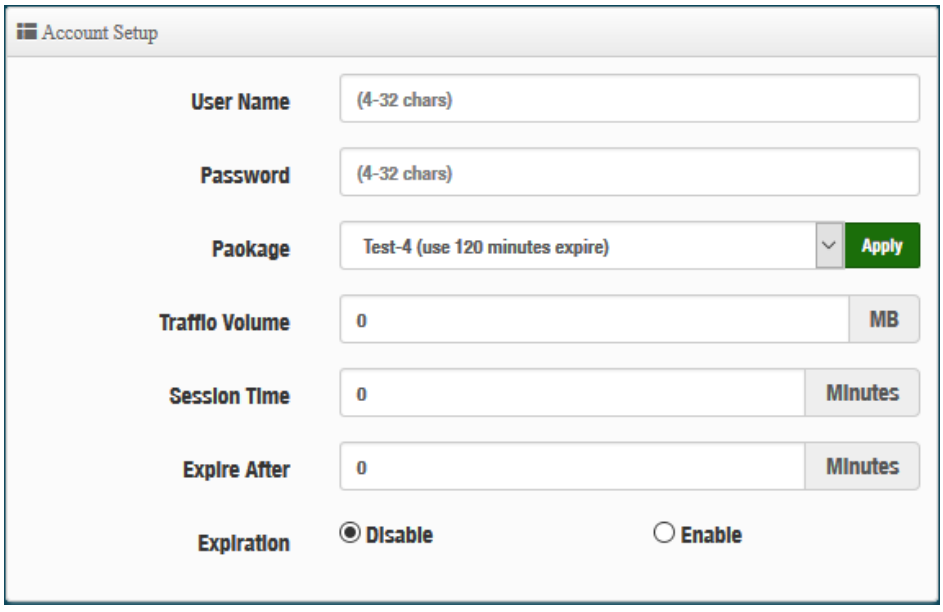
- ➢ **User Name Length:** Administrator can set account length limit for package rules.
- ➢ **User Name Type:** Administrator can create account use digit or Letters or Mix for package rules. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.
- ➢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

5.4 Create An Account

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

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

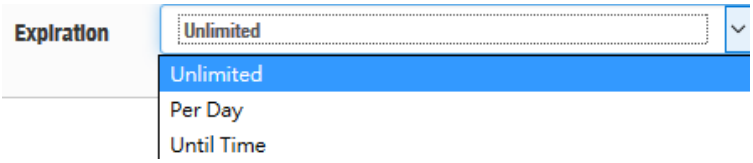




- **User Name**：Administrator can set an account for RADIUS Server.
- **Password**：Enter Password for user name account.
- **Package:** Administrator can choose apply mechanically Package function policy.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package 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.

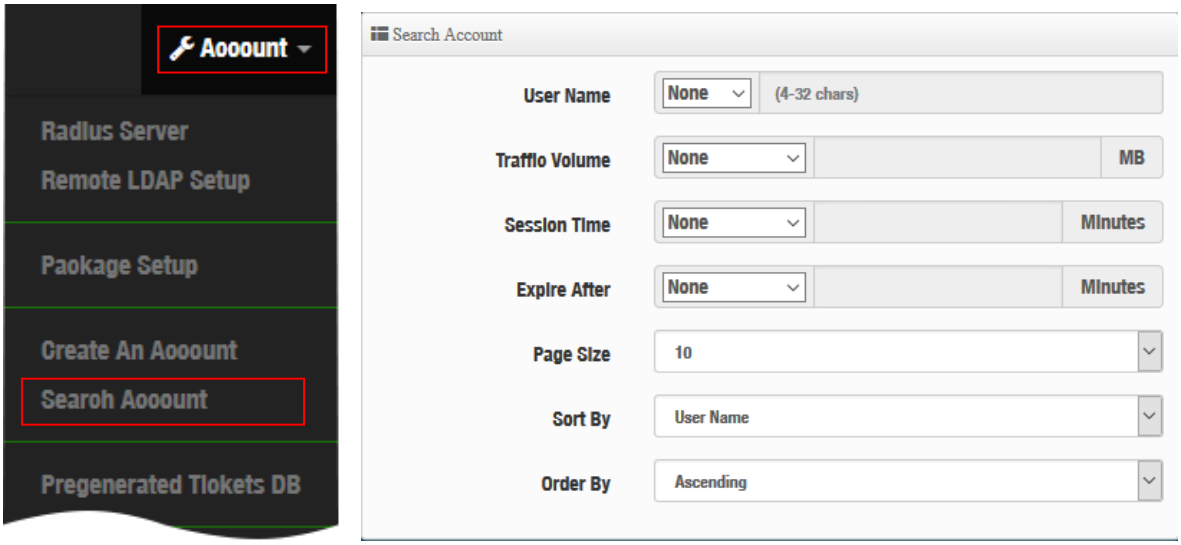


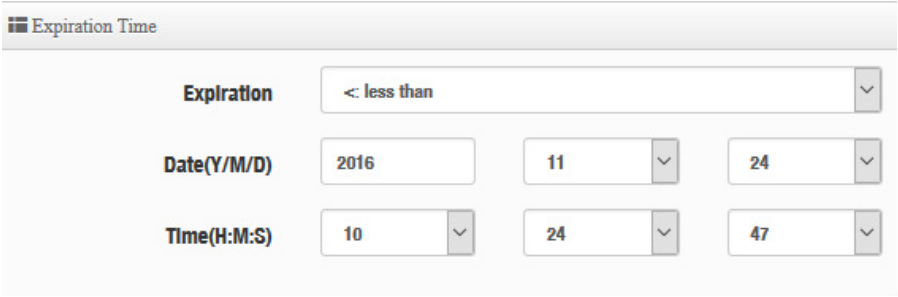
- **Unlimited:** After the account is signed in, the system does not count the time
- **Per Day:** After the account is signed in, the system start counted time until the end time.
- **Until Time**: After the account is signed in, the system will begin counting until the set time is used up. The counting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

5.5 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"**





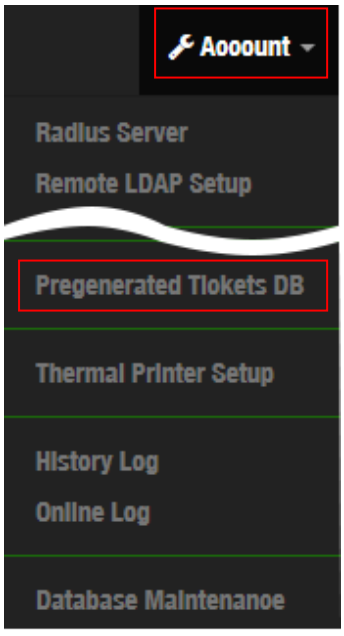
Administrators can choose different data type in the search engines.

- **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.

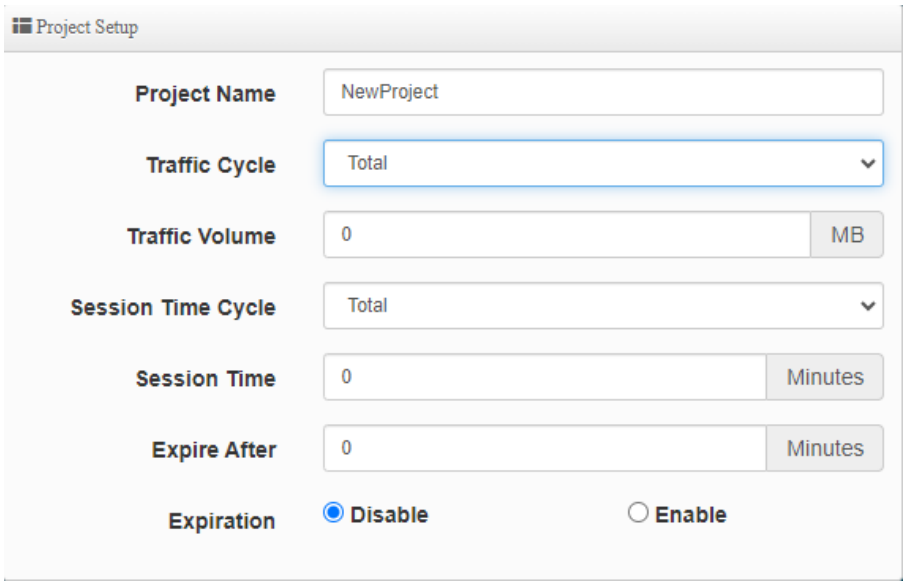
5.6 Regenerated Tickets DB

Administrators can use system auto create accounts in a databases.

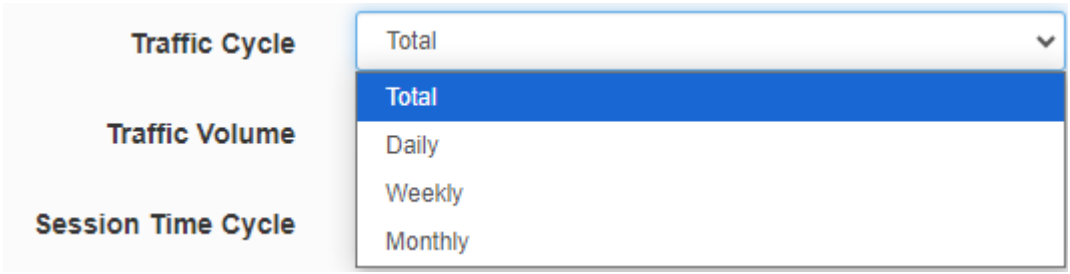
Please click **“Account”➔”Regenerated Tickets DB”** to create databases.



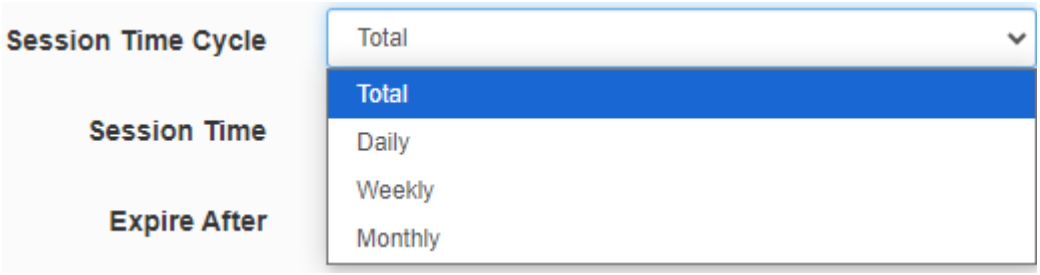
Administrator can click Create New Project to set function.



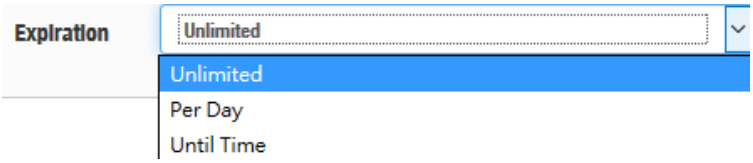
- **Project Nama:** Administrator can set a Databases name.



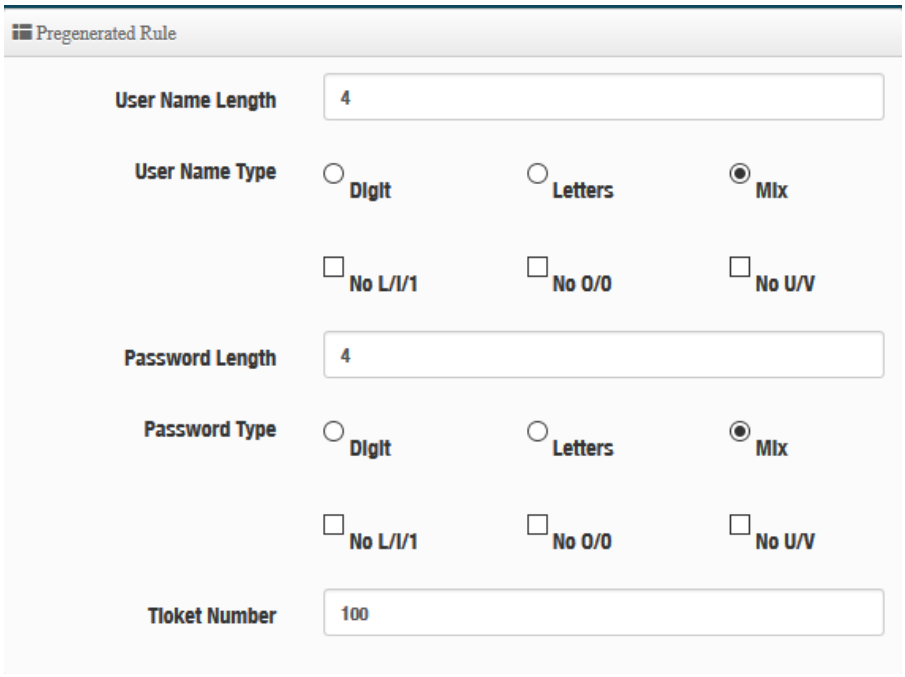
- **Traffic Cycle:** There is a reset period for traffic usage, and the pre-vouched account password will be eligible for repeated active use due to this reset period.
  - ✓ **Total**：Based on a one-time total calculation, the total amount of pre-ticketed account traffic will no longer be usable after 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:** 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.



- **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.



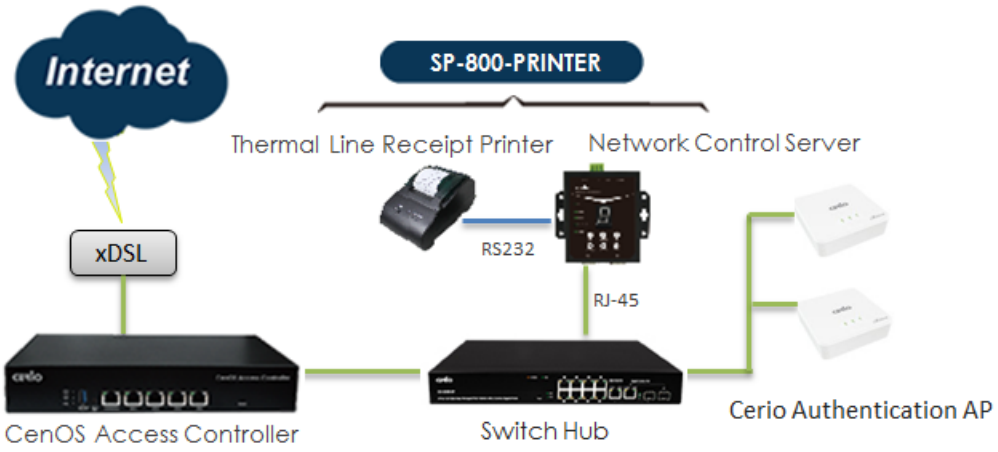
- **User Name Length:** Administrator can set account length limit for package rules.
- **User Name Type:** Administrator can create account use digit or Letters or Mix for package rules. If administrator select Letters or Mix can filter L/l/digit 1 and O/ digit 0 and U/V for letters and Mix.
- **Password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

5.7 Thermal Printer Setup

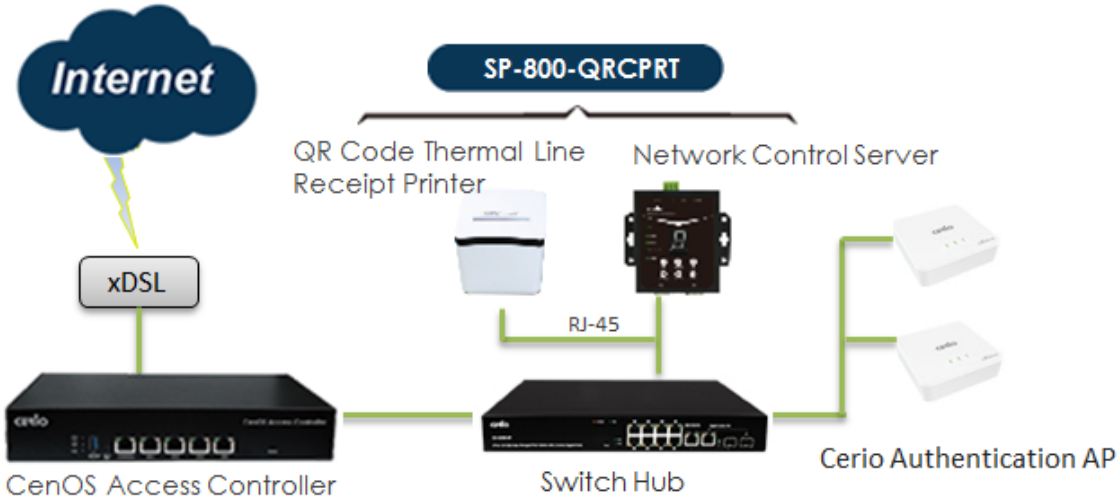
The function must match Account Ticket Generator POS System for Cerio's SP-800-PRINTER / SP-800-QRCPRT.

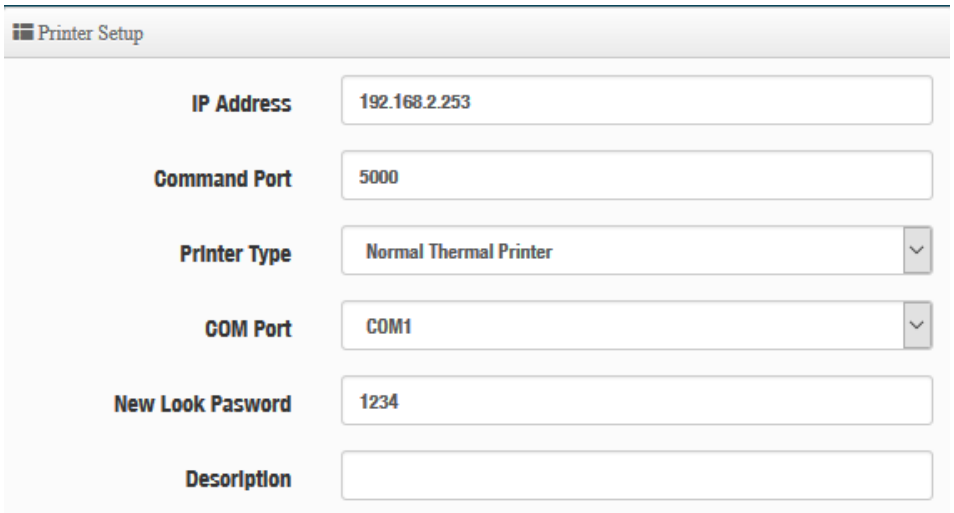
Application architecture is as follows.

 # Match SP-800-PRINTER



 # Match SP-800-QRCPRT



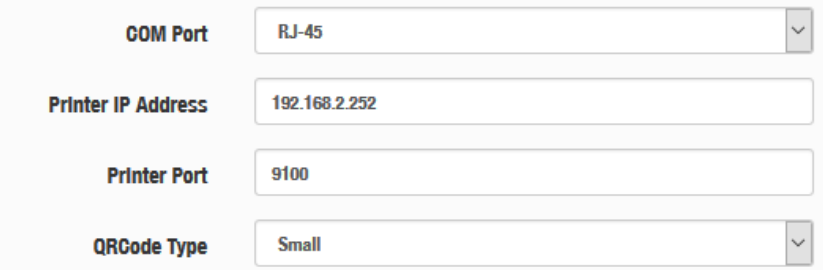


- **IP Address:** Please set IP address for Network control server (SP-800)
- Command Port: Enter command port for Network control server (SP-800)
- **Printer Type:** Administrator can select Normal Thermal Printer or QR Code Thermal Printer.

- **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.



✓ **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-CA** 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.

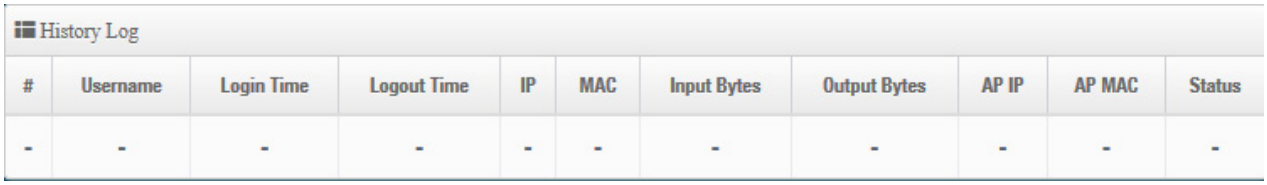
Package List

Package#	Enable	Name	Description
1	☐	TEST-1	no time
2	☐	test-2	60Mbps Traffic
3	☐	test-3	use 120 minutes time
4	☐	Test-4	use 120 minutes expi...

Administrator can choose box to enable Packages rule.

5.8 History Log

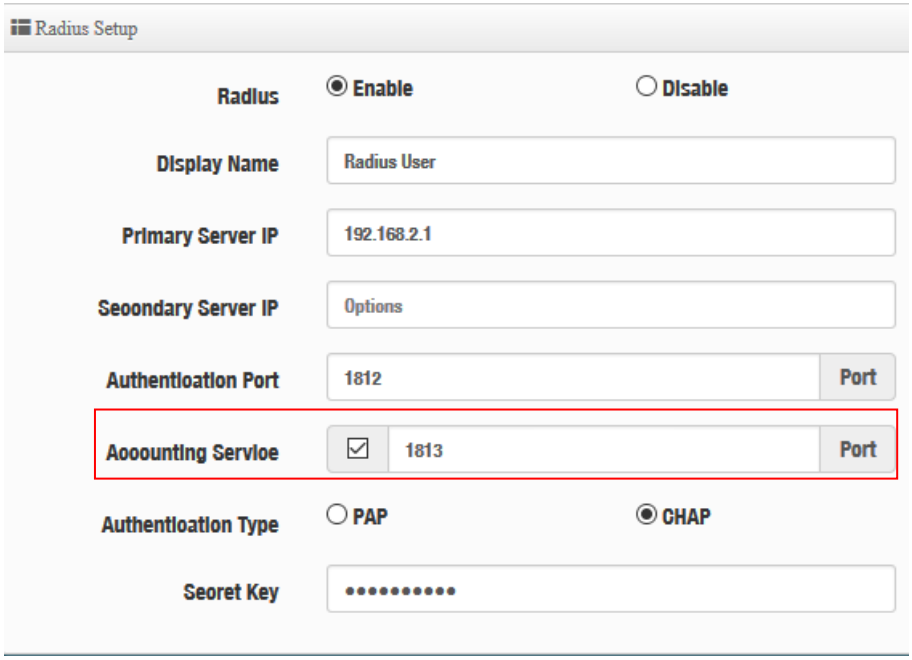
The Page can display account login/logout information.



5.9 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



 # DR-4000-CA online Log page

5.10 Database Maintenance

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

Notice Administrator click “Clear” button, the databases all account will be deleted.

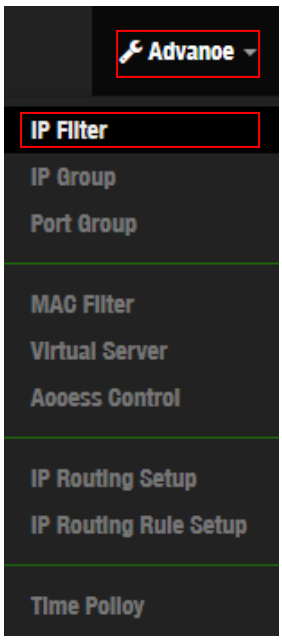
6. Advance

6.1 IP Filter

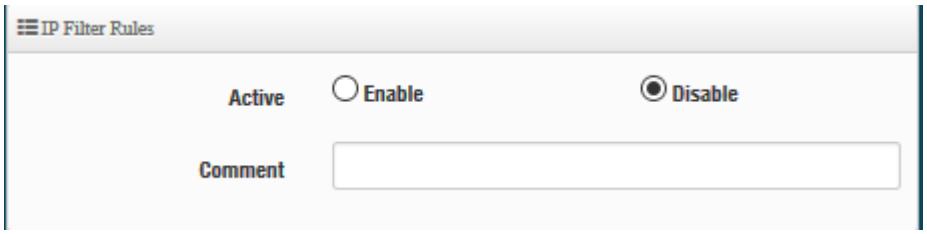
Can allow or deny filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules support IP/ Port Groups, could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important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

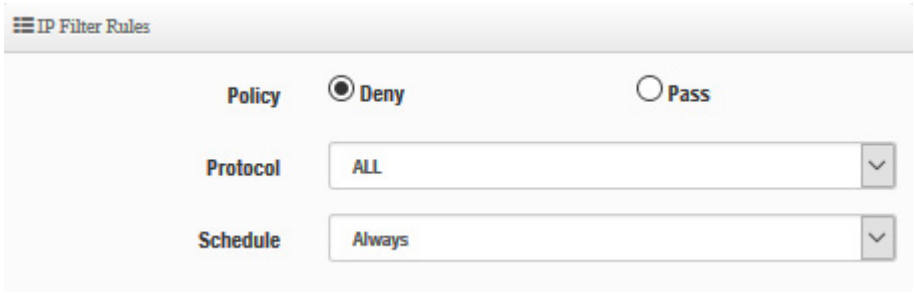


- Please click **Edit** button to setting IP filter.



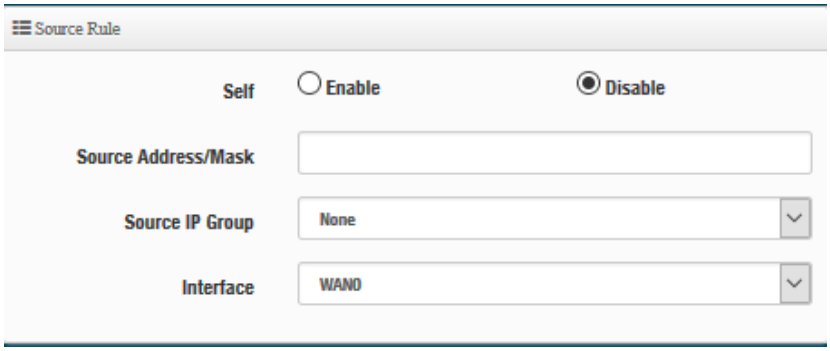
- **Active:** Administrator can selected Enable or Disable for the IP filter rules function.
- **Comment:** Enter rule description.

IP Filter Rules

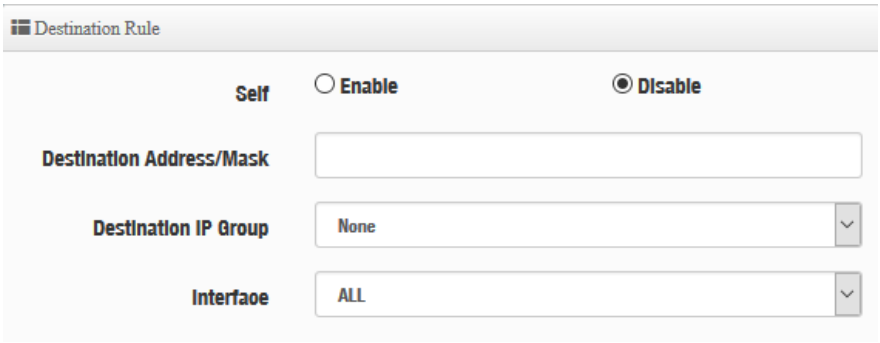


- **Policy:** Administrator can select Deny or Pass for IP filter rules.
- **Protocol:** Administrator can select type for IP protocol.
- **Schedule:** Can choose to use rule by "**Time Policy**".

Source Rule



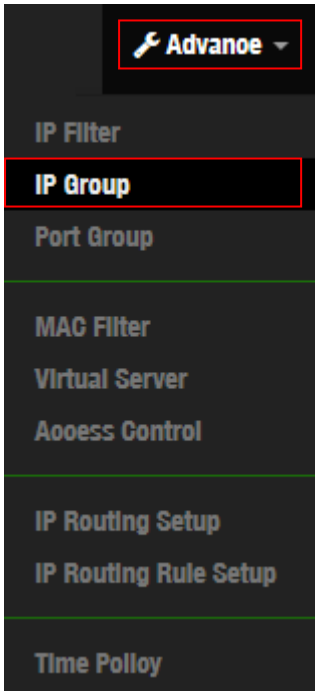
- **Self:** Administrator can choose Enable or Disable, if administrator select Enable, the source is self.
- **Source Address/Mask:** Administrator can set IP address and Mask for source.
- **Source IP Group:** Administrator can select belonging to group for IP Address.
- **Interface:** Administrator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

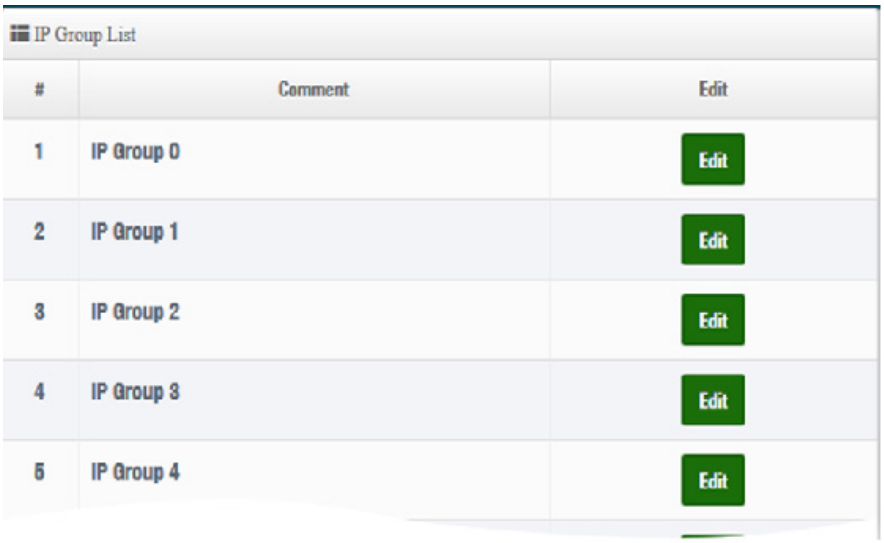


- **Self:** Administrator can choose Enable or Disable, if administrator select Enable, the source is self.
- **Destination Address/Mask:** Administrator can set IP address and Mask for destination.
- **Destination IP Group:** Administrator can select belonging to group for IP Address.
- **Interface:**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

6.2 IP Group

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

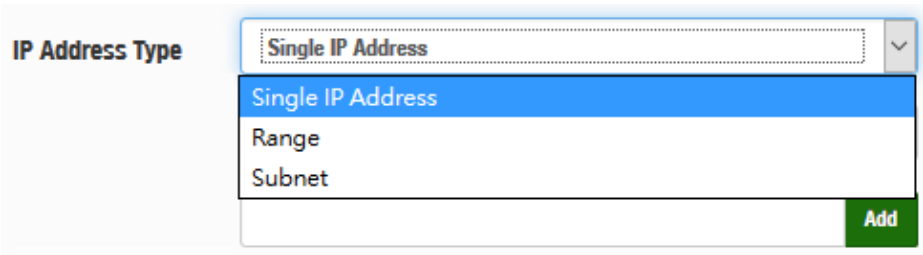




Please click "**Edit"** button to create new IP Groups.

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

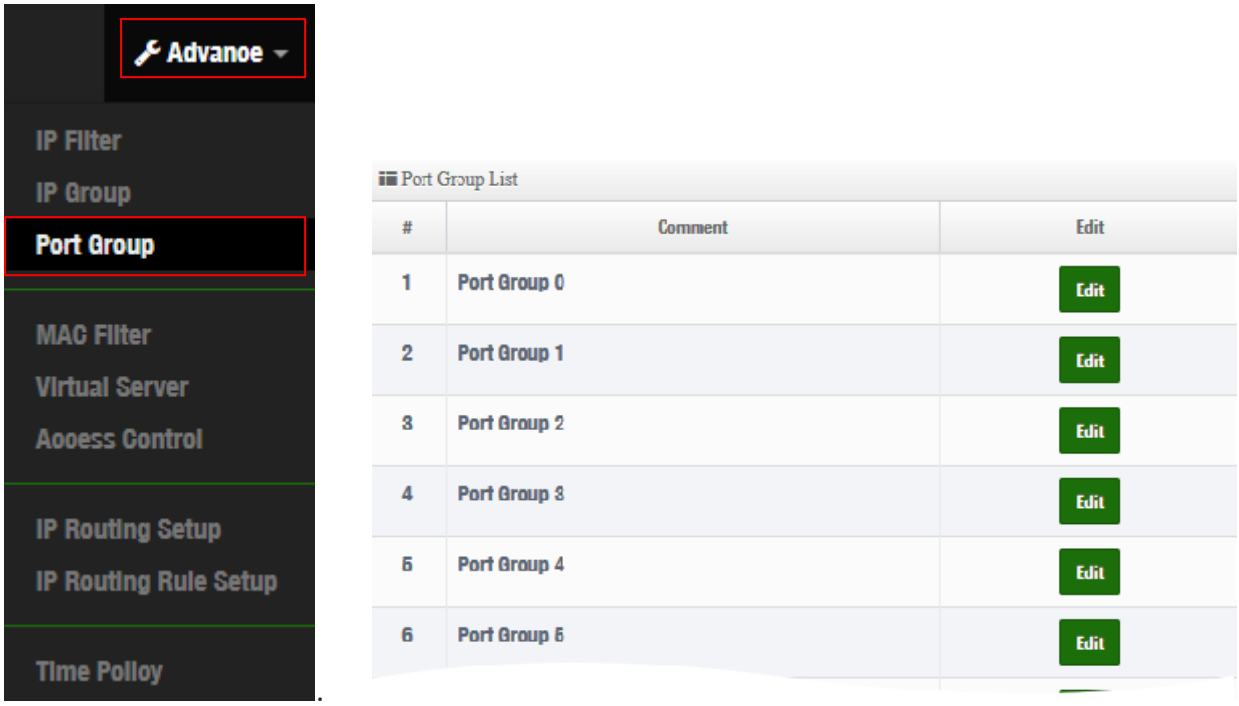
- **IP Address Type:** Administrator can select single / range / subnet type to set IP Address.



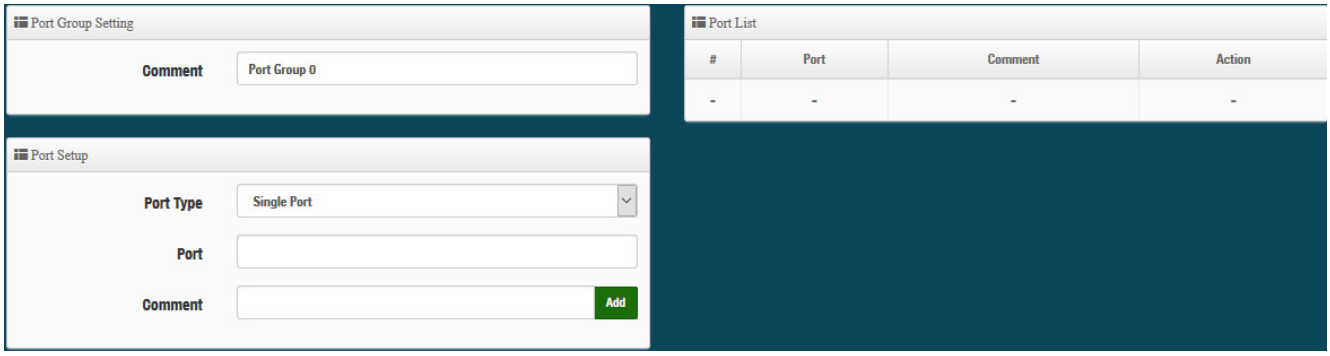
- **Single IP Address:** Enter single IP Address.
- **Range:** Enter start / end IP address.
- **Subnet:** Enter Net/MasK.

6.3 Port Group

Administrator can create Port group



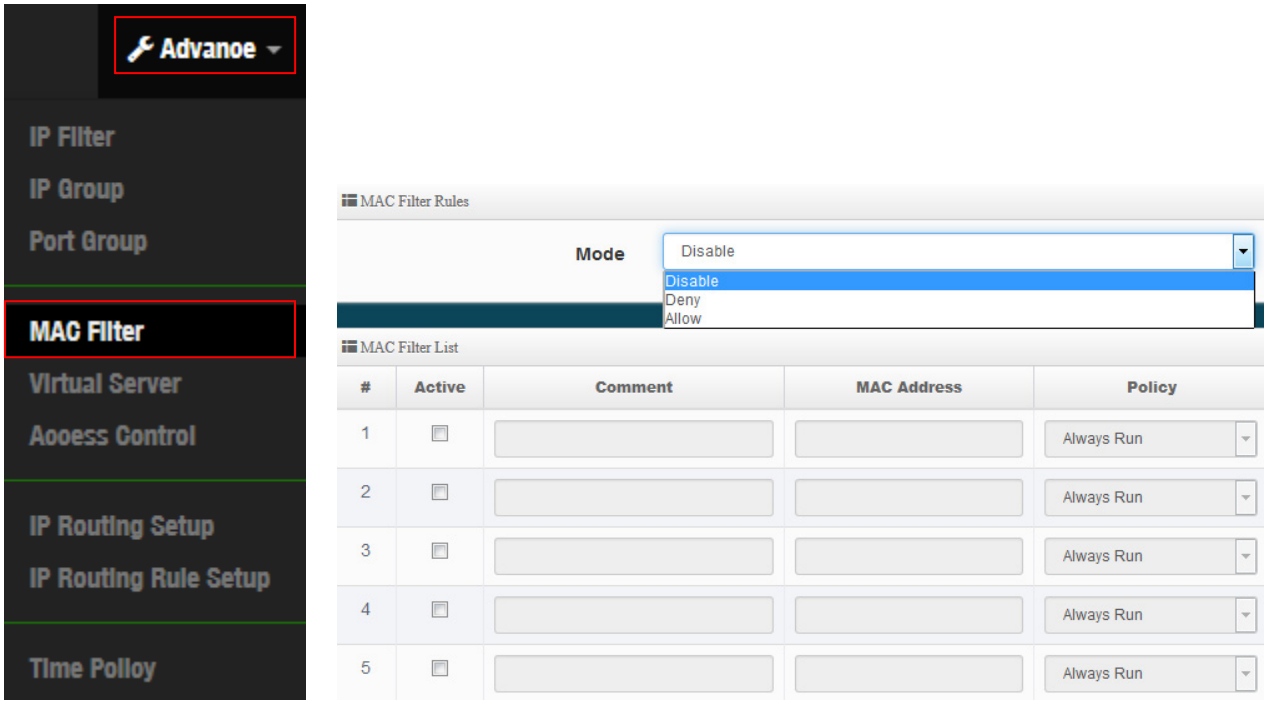
Please click "**Edit"** button to create new Port Groups.



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

6.4 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.

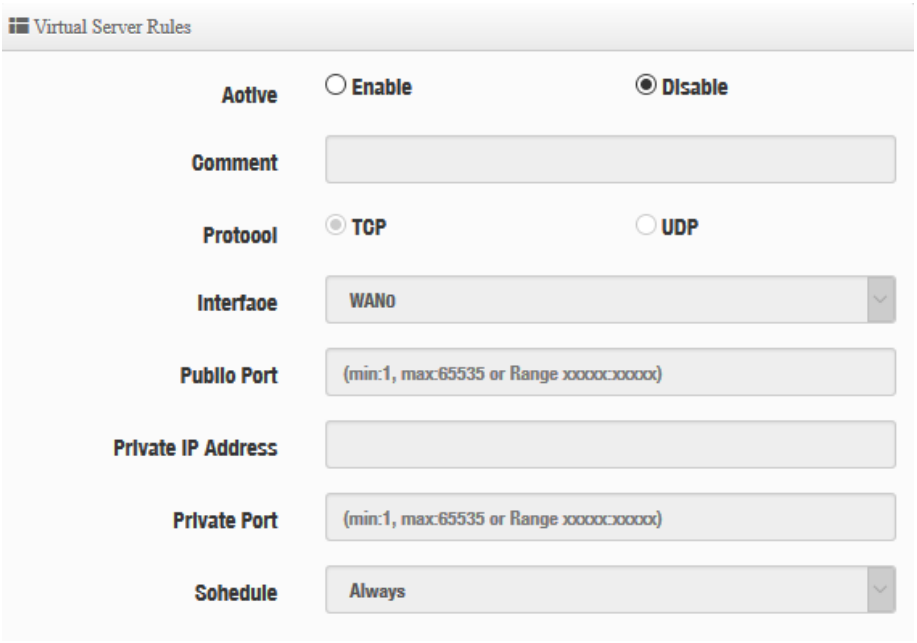


- **Mode:** Administrator can select Deny or Allow.
  - **Deny:** The MAC Filter List will be **denied** to access (LAN to WAN). Others will be allowed.
  - **Allow:** The MAC Filter List will be **allowed** to access (LAN to WAN). Others will be denied.
- **Comment:** Enter the description of MAC filter 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".**

6.5 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.

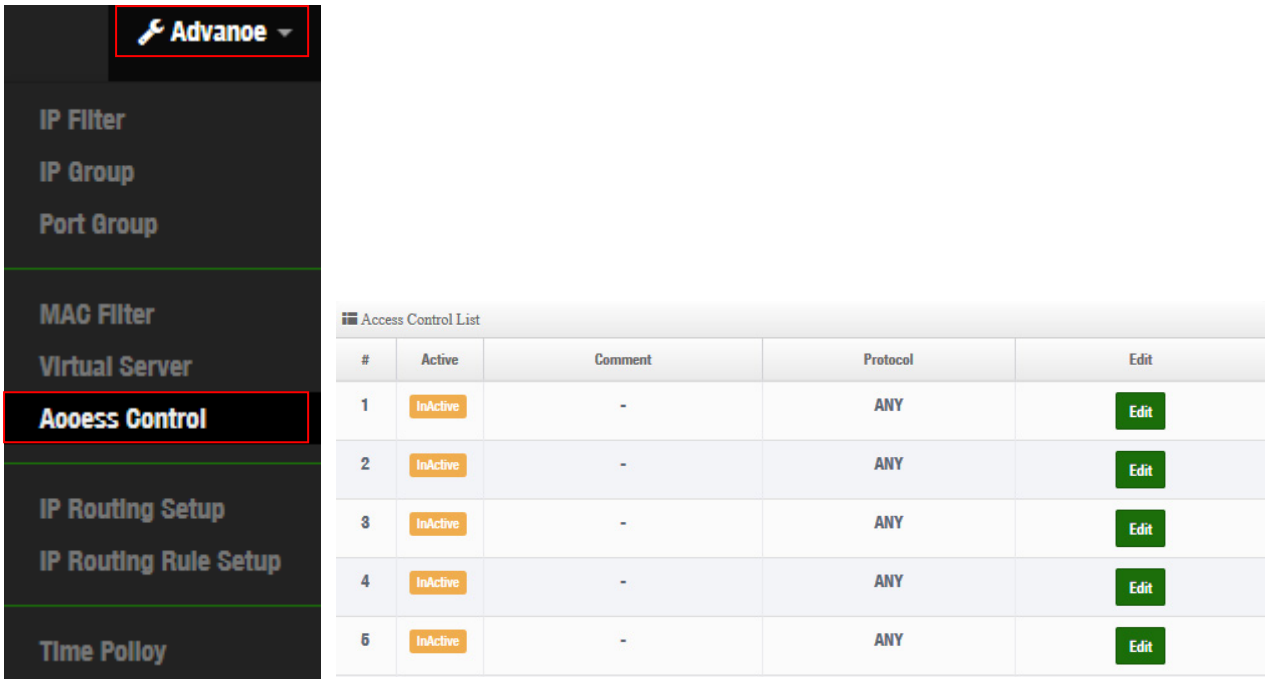


- **Active:** Administrator can select Virtual server rule to Enable or disable.
- **Comment:** Enter the description of virtual server rule.
- **Protocol:** Administrator can select service protocol of TCP or UDP.
- **Public Port:** Enter service port No. for public.
- **Private IP Address:** Enter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

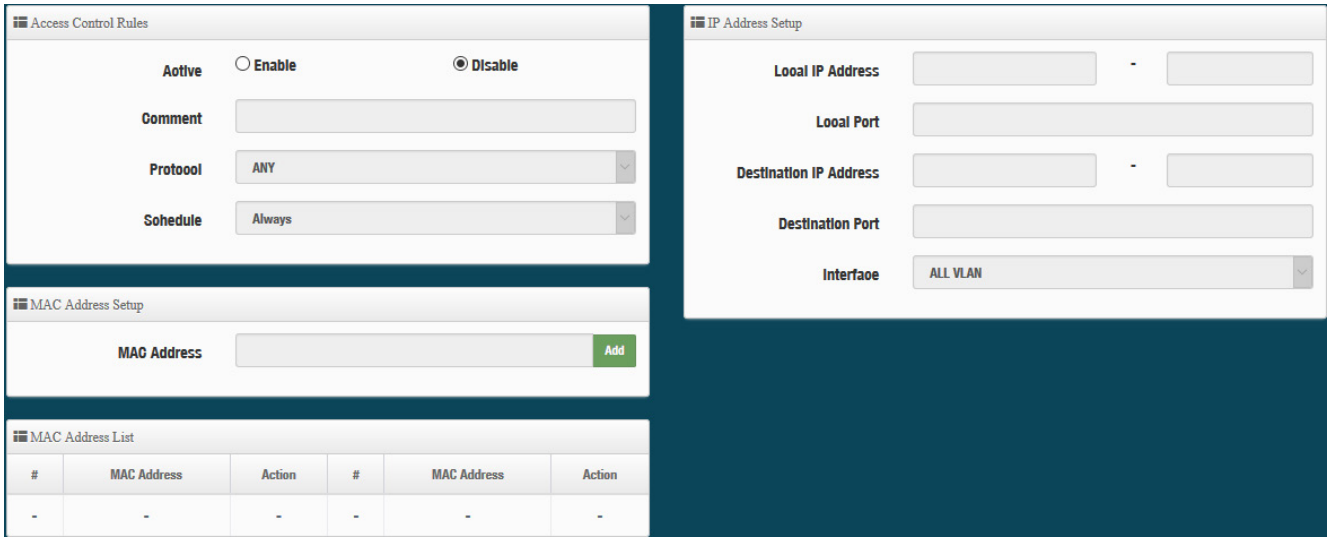
6.6 Access Control

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.

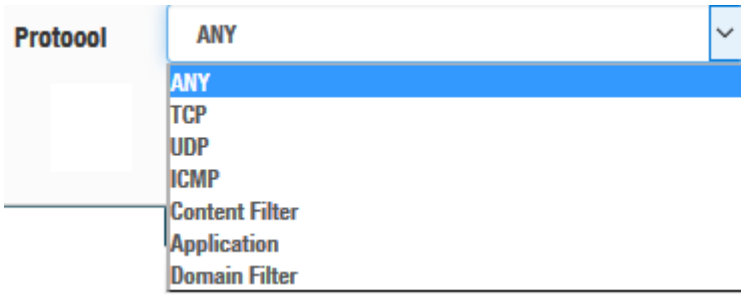


- **#**：Display access control list.
- **Active**：Display Active or InActive for the access control rule.
- **Comment:** Display information for the rule.
- **Protocol**：Display information for the protocol.
- **Edit**：Administrator can click the button to set Access Control rule.



 # Access control rules：

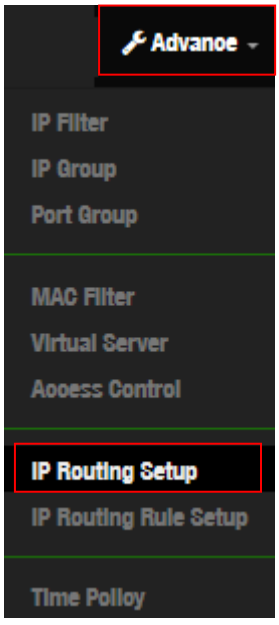
- **Active**：Administrator can select Enable or Disable for the Access control rule.
- **Comment**：Administrator can enter comment for the role.
- **Protocol**：Administrator can to select management protocol by TCP/UDP/ICMP/Content Filter/Application and Domain Filter.

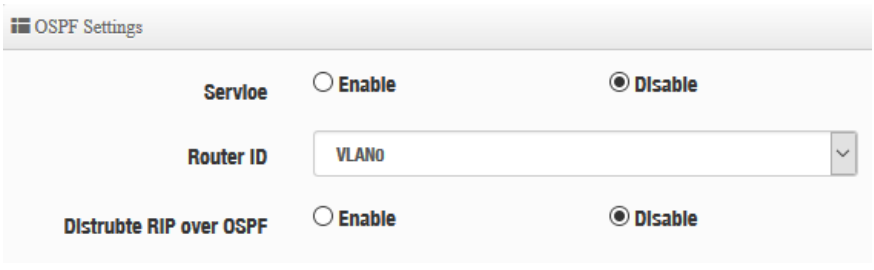


- ✓ **ANY:** Select **"Any"** is all deny Protocol, administrator can filter local IP / IP range go to destination IP / IP range and use protocol.
- ✓ **TCP:** Deny TCP Protocol, Administrator can set TCP protocol and assign IP / IP range.
- ✓ **UDP:** Deny UDP Protocol, Administrator can set UDP protocol 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.

6.7 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.



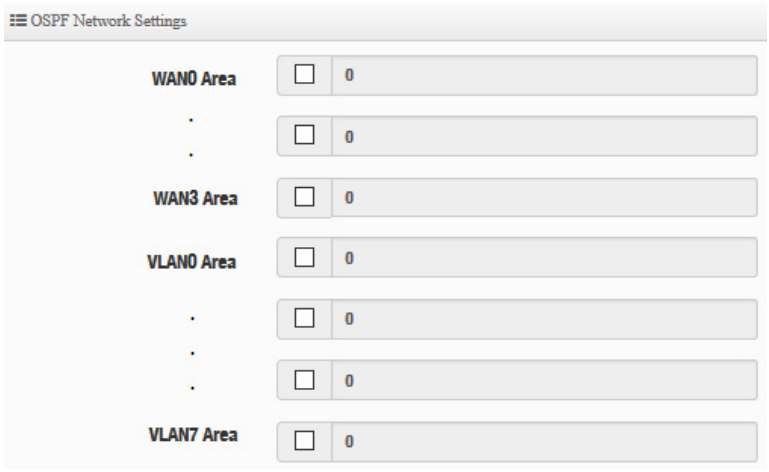


➢ **OSPF Settings :**

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

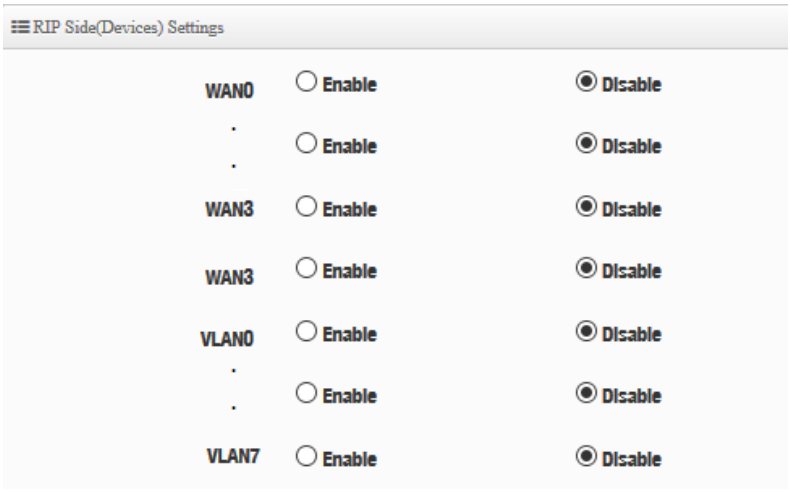


✓ **#Area:** Represents the area code of the OSPF routing protocol, which can be any digit in decimal, default is 0.

➢ **RIP Settings :**

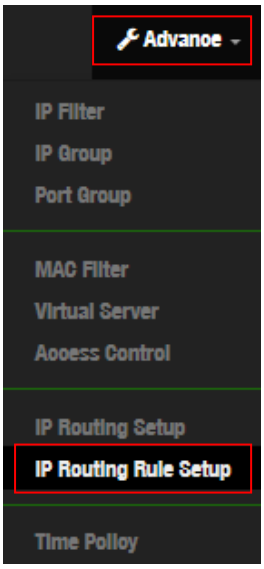
RIP defines a way for routers, which connect networks using the IP, to share information about how to route traffic among networks. RIP prevents routing loops by implementing limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15, which 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.

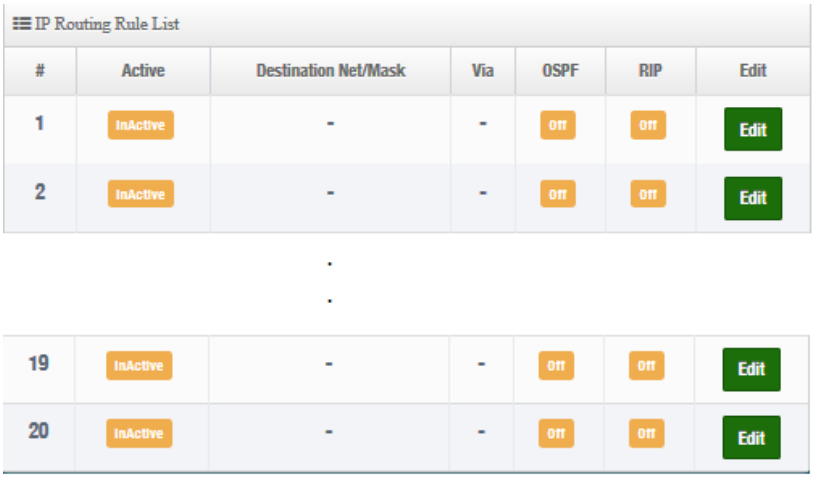
- **Service:** Administrator can select enable or disable Service for RIP.
- **Distribute OSPF over RIP:** Administrator can select enable or disable, if select enable system can allow OSPF routes will redistributed into RIP.



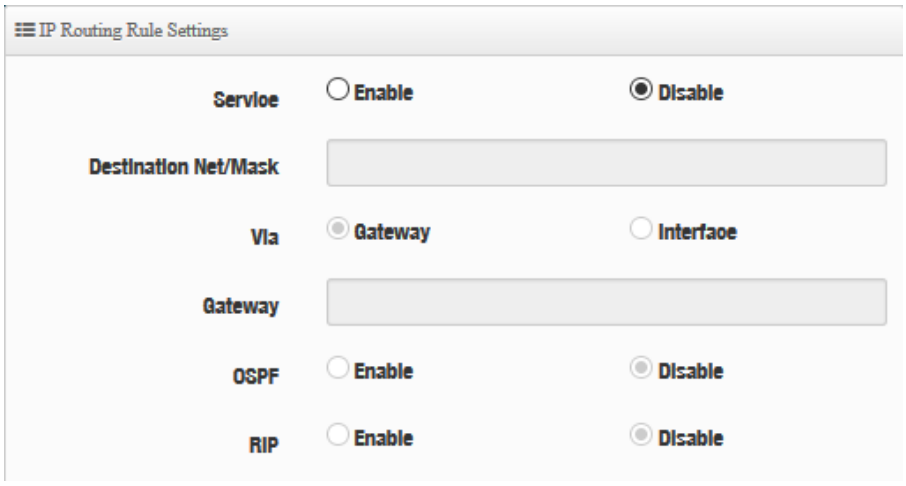
✓ **RIP Side(Devices) Settings:** Administrator can choose enable or deniable for WAN/LAN interface

6.8 IP Routing Rule Setup



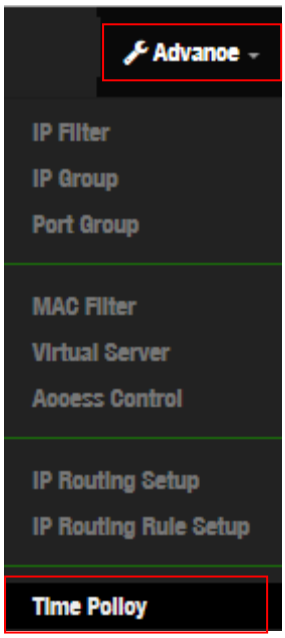


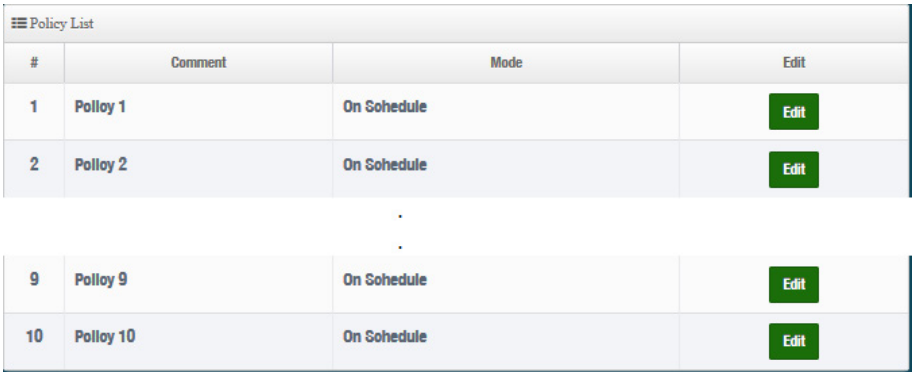
Please click **Edit** button to setting IP Routing Rule.



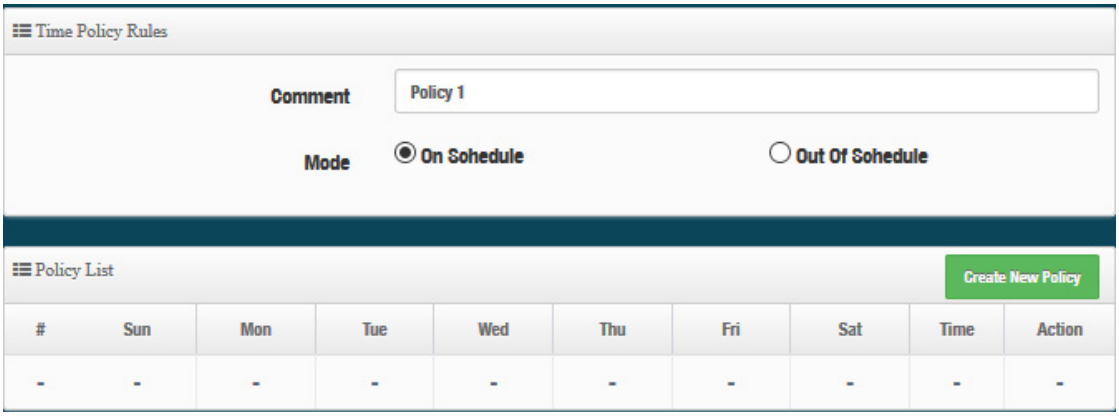
- **Service:** Administrator can select Enable or Disable for the IP Routing Rule.
- **Destination Net/Mask:** If administrator select enable for service, will be able set destination Net/Mask.
- **Via:** Administrator can select use Gateway or Interface
  - **Gateway:** enter Gateway IP address.
  - **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.

6.9 Time Policy





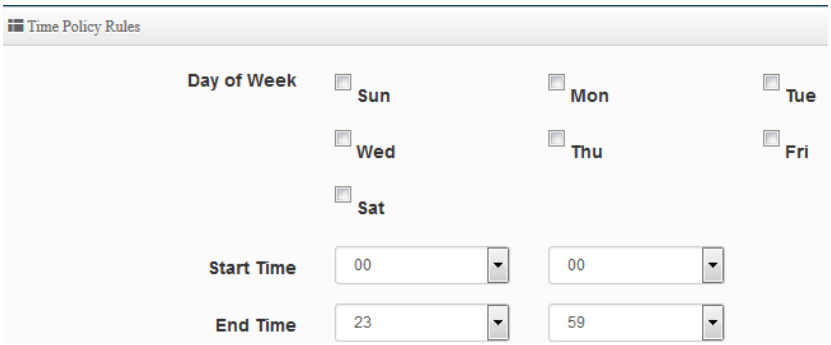
Please click **Edit** button to setting time policy rules.



- 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.



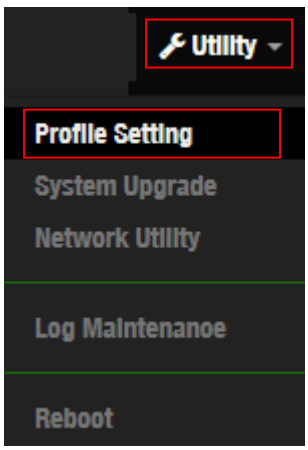
Click "**Save**" button to add schedule to policy. There are 300 schedule rules maximum allowed in the each time policy. All schedules can be edited or removed in the each time policy. Click Reboot button to activate your changes.

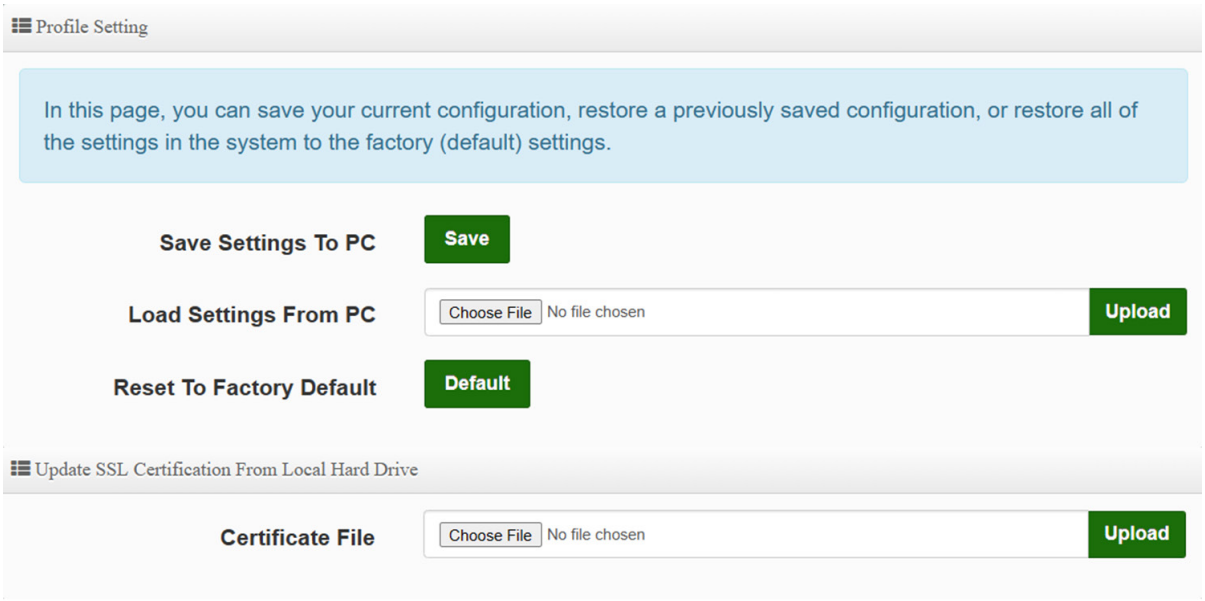
7. Utility

7.1 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



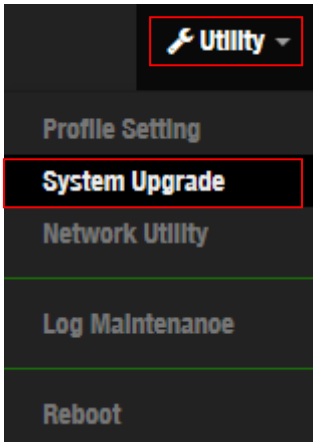


- **Save Settings to PC:** Click ***Save*** button to save the current configuration to a local disk.
- **Load Settings from PC:** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.
- **Reset To Factory Default:** Click ***Default*** button 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.

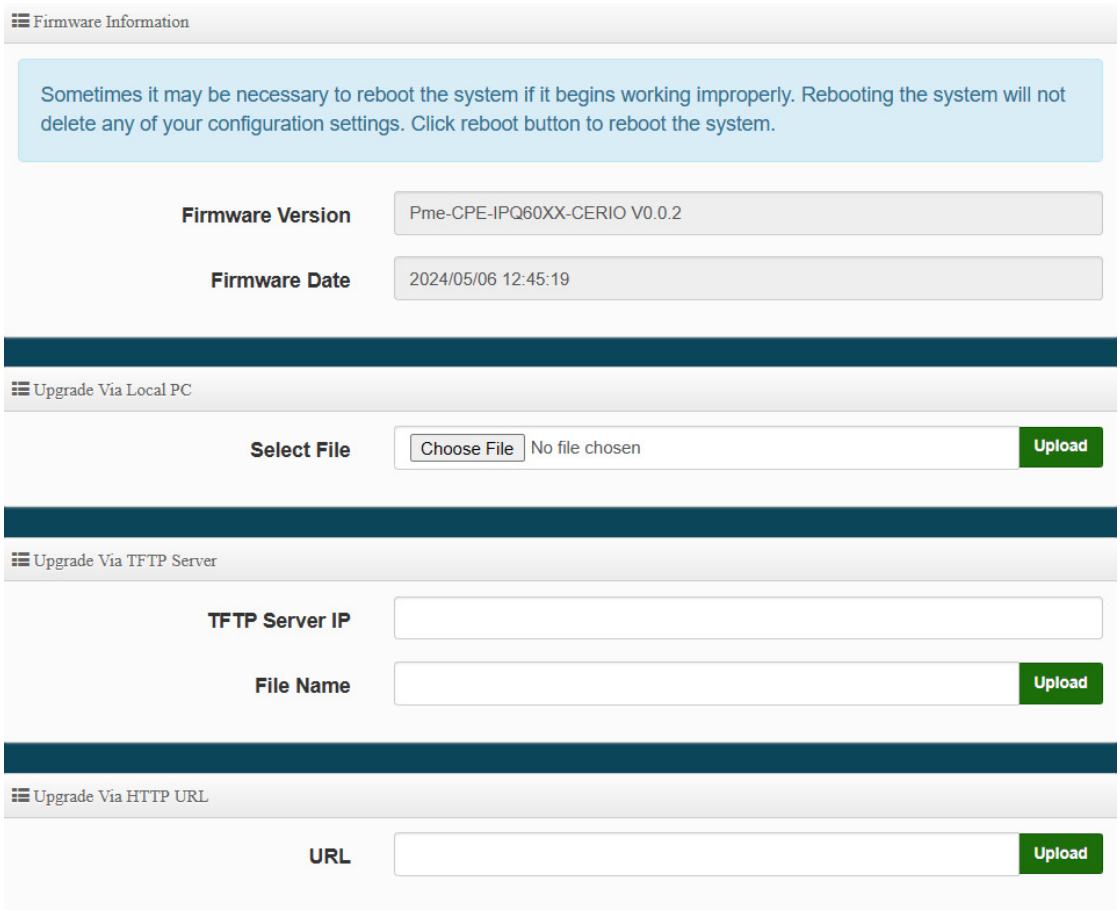
7.2 System Upgrade

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.



Upgrade Via Local PC and TFTP Server:

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

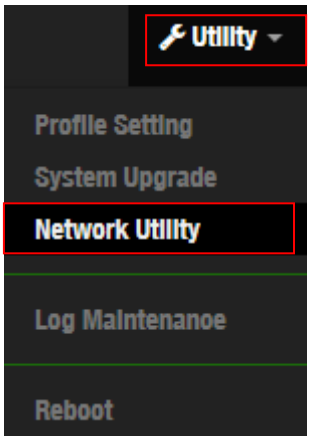
- **Select File:** Administrator can select Firmware file in Local PC.
- **TFTP Server:** Enter IP address for TFTP Server.
- **File Name:** Enter file name.
- **URL:** Administrator can enter path for Firmware file.

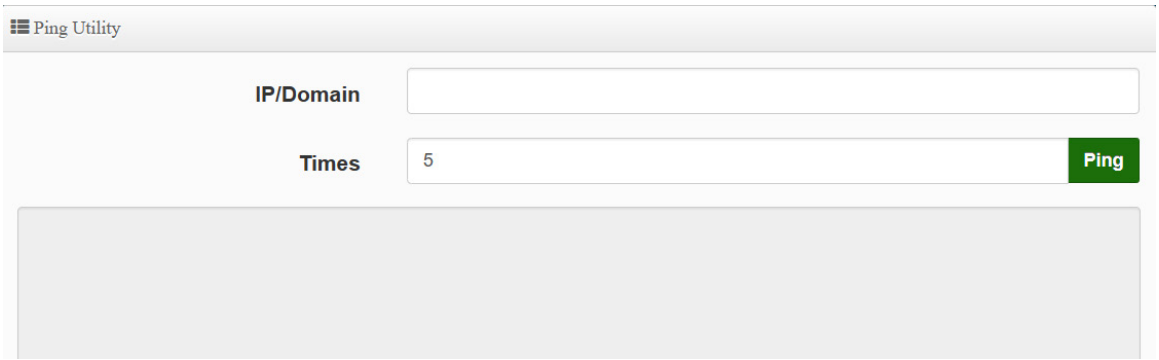
Notice

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.*

7.3 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.

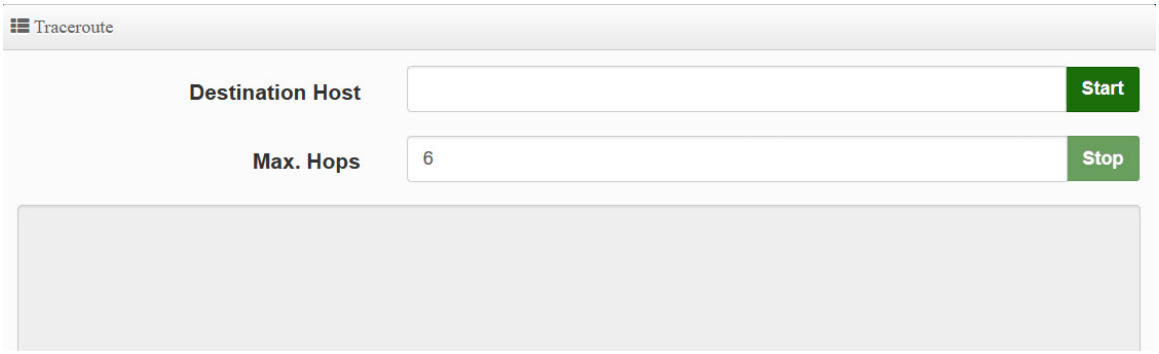




- **Ping**：This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two

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.

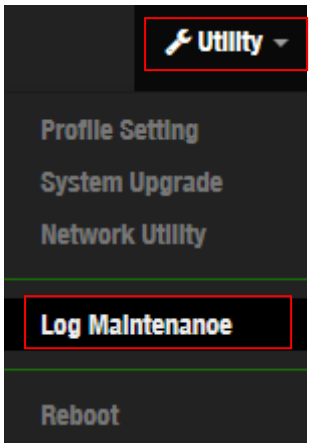


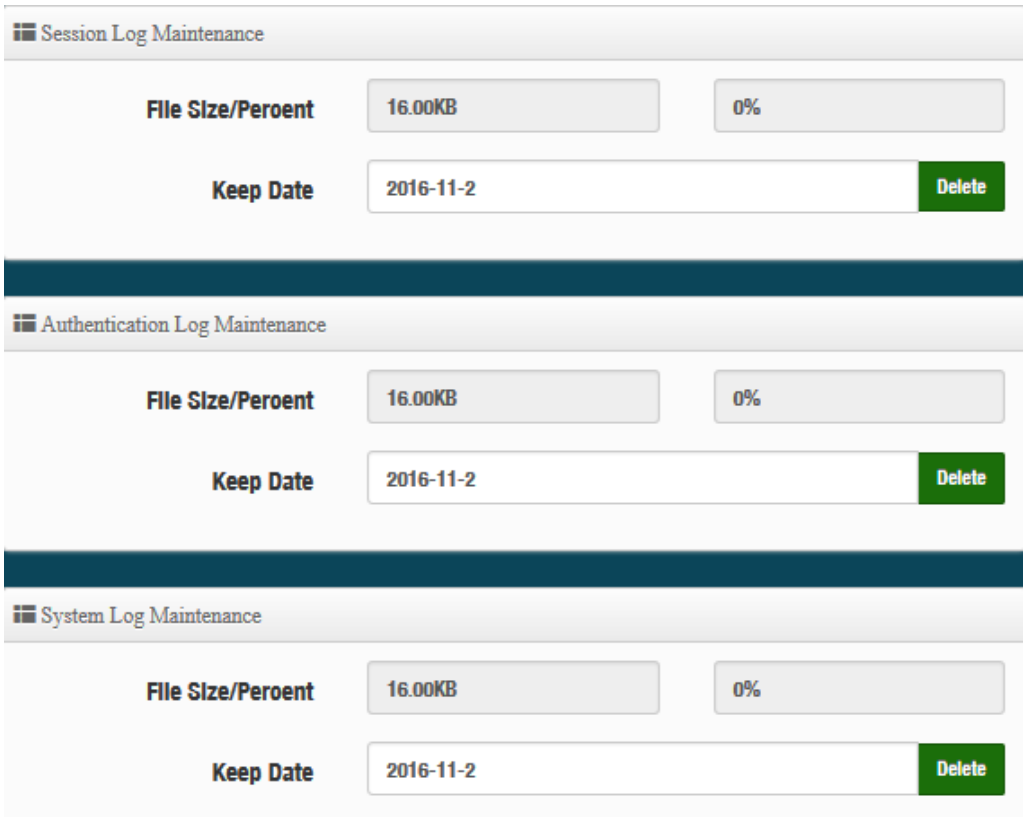
➢ **Traceroute**：Allows tracing the hops from the DR-4000-CA device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test.

- **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.

7.4 Log Maintenance

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

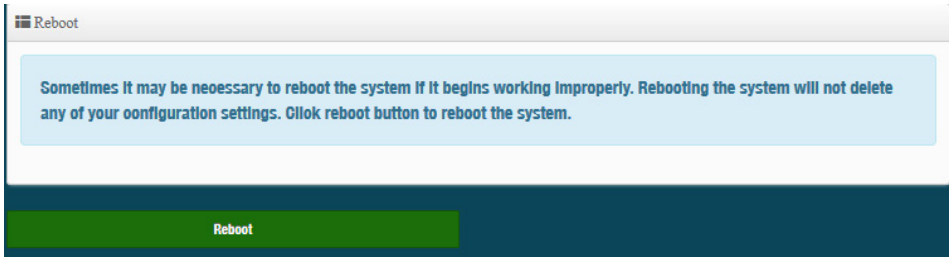




- **File Size/Percent:** Display used volume and percentage.
- **Keep Date:** Display creation date.
  - **Delete button:** Administrator can click “delete” button to clear log information.

7.5 Reboot

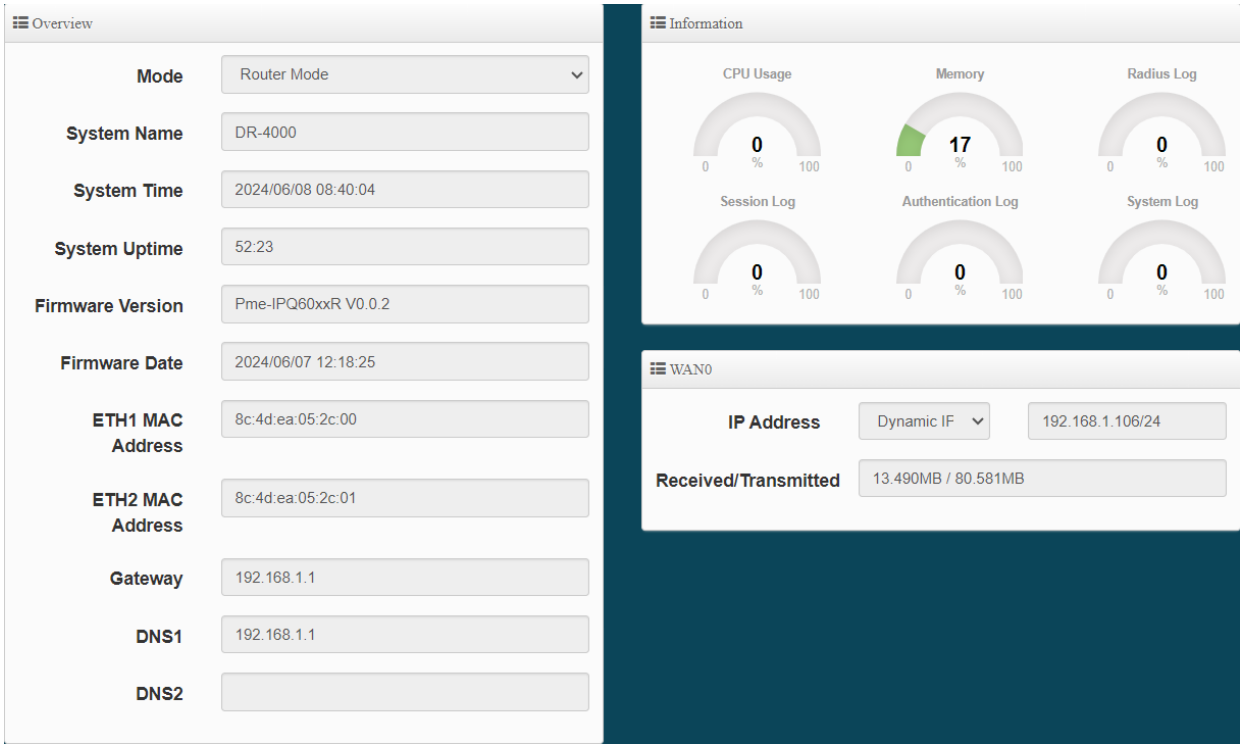
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



8. Status

8.1 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.

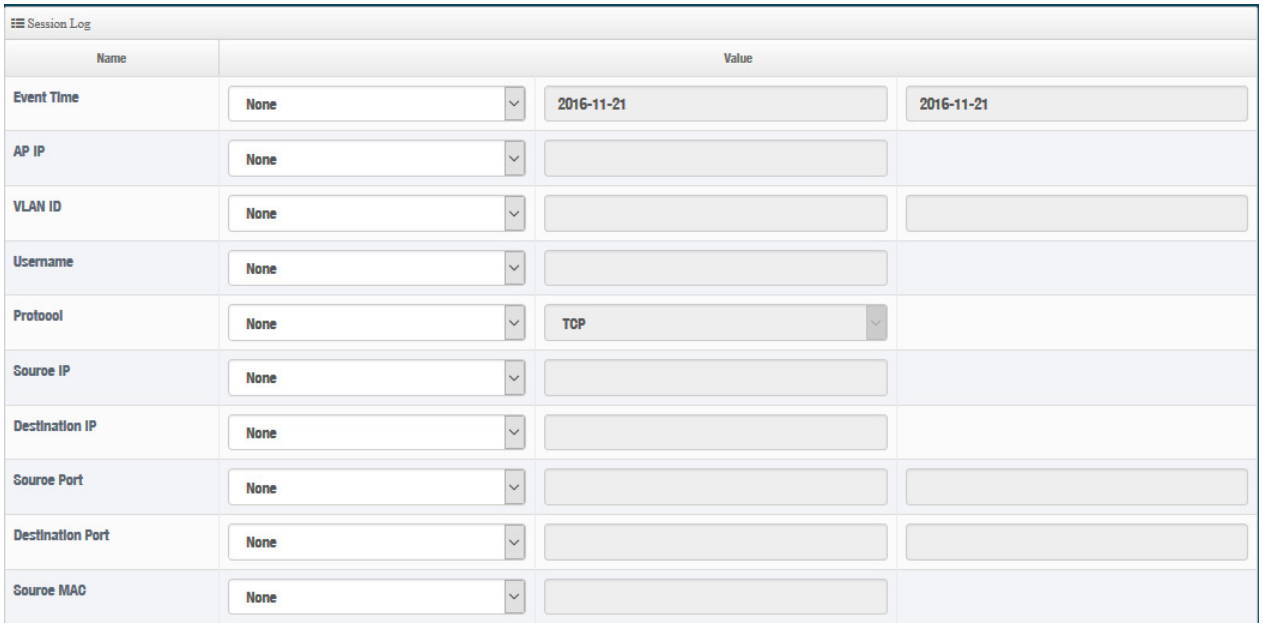
8.2 Local System Log

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.

- **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.
-

8.3 Session Log

If enable “syslog server” in the “**Session Log”** (Hotsport 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.



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.

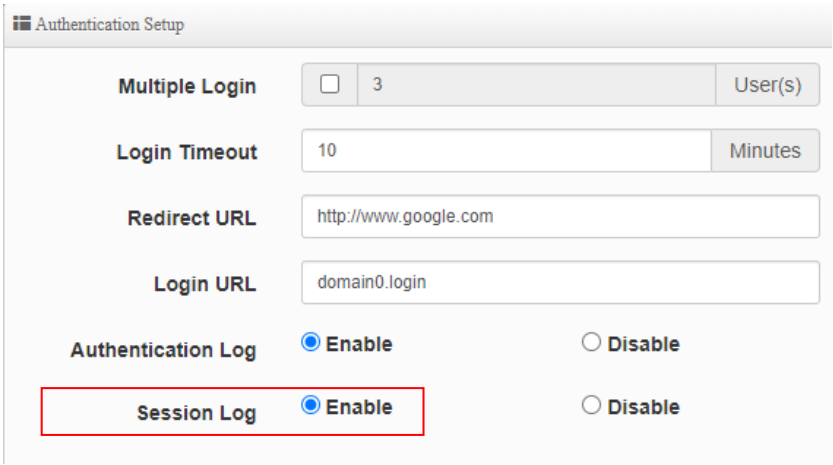
Session Log List

#	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	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	[illegible]	62368	80	8C:4D:EA:02:C6:EC

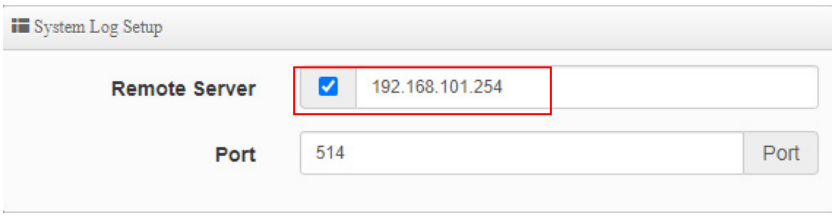
If the session interception function setting used is not configured on the front-end Cerio AP on this machine, you can store the logs of the Cerio AP to this log server. Please enter the management settings of the Cerio AP and set the "Session Log" Setup points the IP to the device and enables the "session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

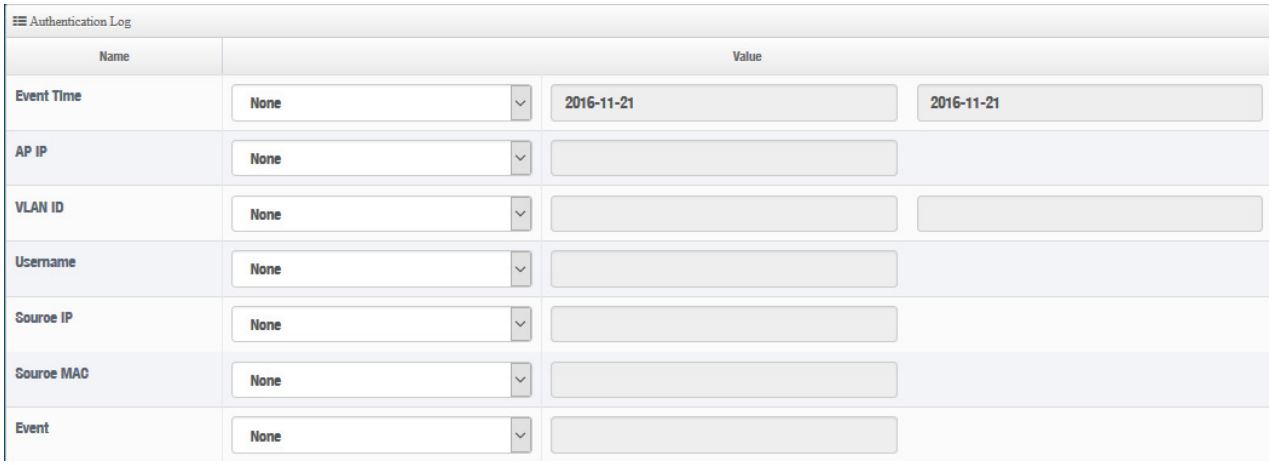


 # Setup 2 : Please click Cerio AP to “Management”➔”System Log Setup” to fill in remote Server IP Address.



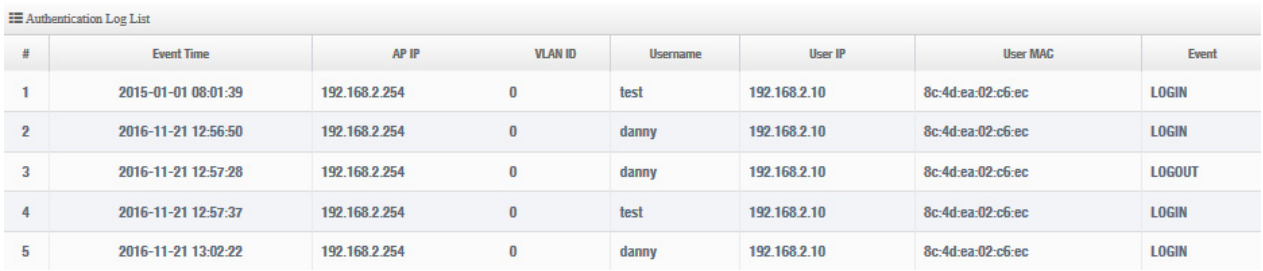
8.4 Authentication Log

If enable “syslog server” in the “**Authentication Log”** (Hotsport 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.



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.

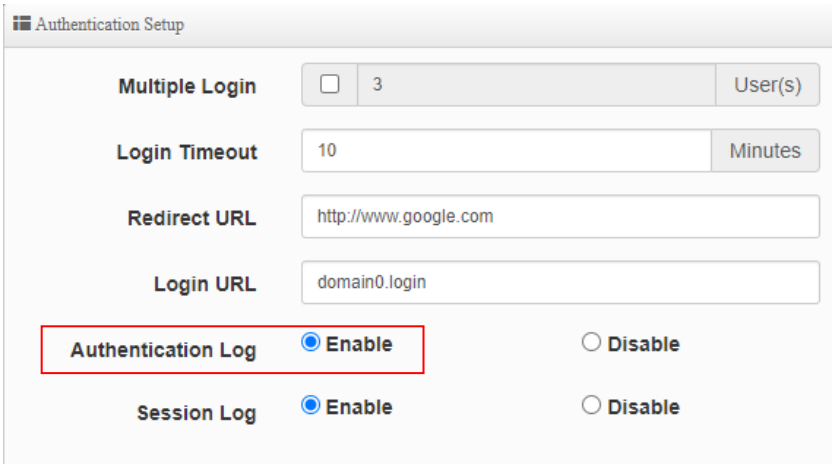

Authentication Log List

#	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

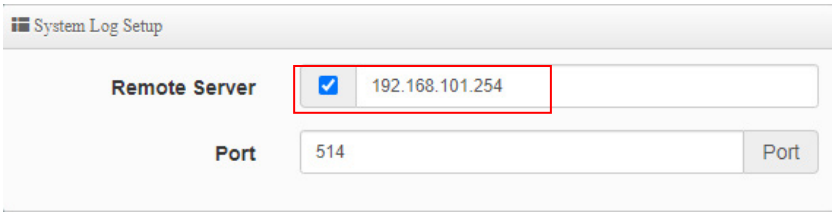
If the authentication interception function setting used is not configured on the front-end Cerio AP on this machine, you can store the logs of the Cerio AP to this log server. Please enter the management settings of the Cerio AP and set the "System Log" Setup points the IP to the device and enables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

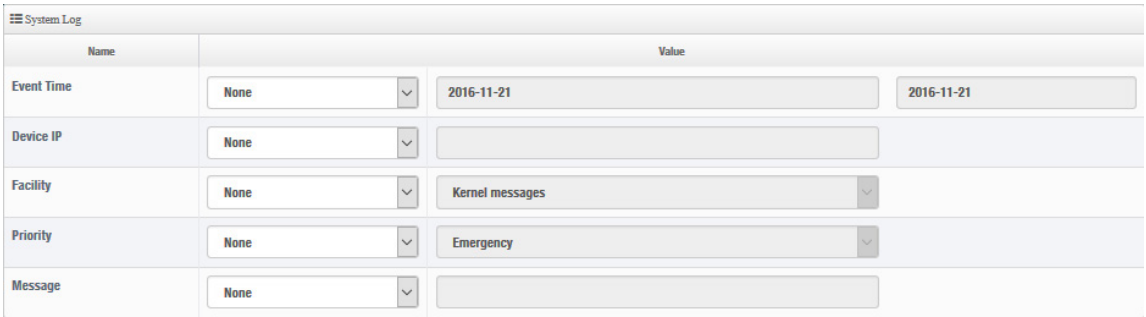


 # Setup 2 : Please click Cerio AP to “Management”➔”System Log Setup” to fill in remote Server IP Address.



8.5 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.



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.

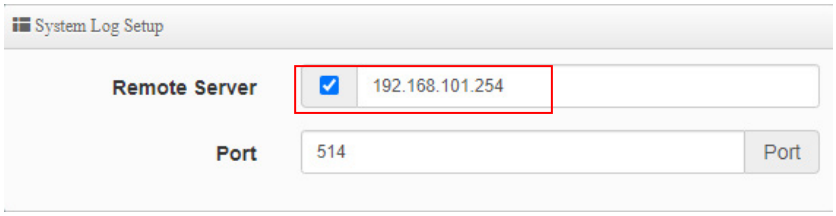
System Log List

#	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.



8.6 Wireless Location Tracking Log

If the administrator enables the syslog server in Cerio's AP, this page can specifically record the “**Wireless Location Tracking Log”** of Cerio AP.

Wireless Location Tracking Log

Name	Value		
Event Time	None	2024/06/12	2024/06/12
AP IP	None		
VLAN ID	None		
Radio ID	None		
BSSID	None		
Client MAC	None		
RSSI	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.

Wireless Location Tracking Log List

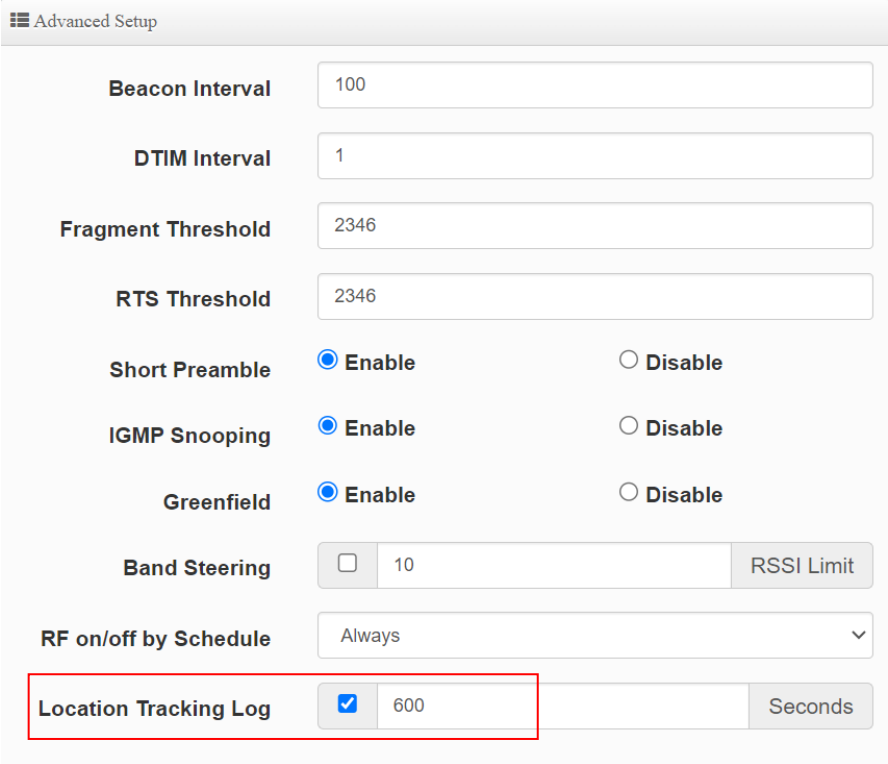
#	Event Time	AP IP	VLAN ID	Radio ID	BSSID	Client MAC	RSSI
1	2024-06-12 22:59:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	dc:4f:22:29:d3:a0	-51
2	2024-06-12 22:59:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	ec:fa:bc:26:48:14	-56
3	2024-06-12 22:59:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	dc:4f:22:29:97:5c	-56
4	2024-06-12 23:09:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	ec:fa:bc:26:48:14	-57
5	2024-06-12 23:09:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	ec:fa:bc:26:4c:2b	-63
6	2024-06-12 23:09:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	dc:4f:22:29:d3:a0	-51
7	2024-06-12 23:09:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	dc:4f:22:29:97:5c	-56
8	2024-06-12 23:19:30	192.168.101.48	0	0	8c:4d:ea:05:22:57	ec:fa:bc:26:48:14	-56

If the wireless location tracking interception function settings used are not configured on the local front-end Cerio AP, the logs of the Cerio AP can be stored in this log server

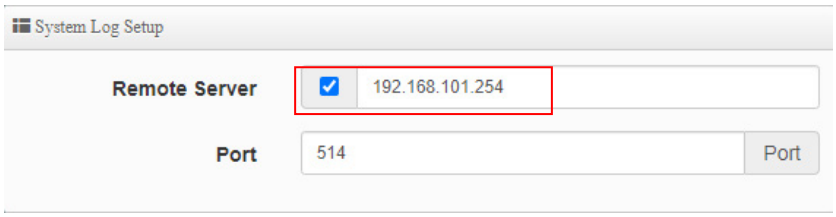
.

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

 # Setup 1 : Please click Cerio AP to “Wireless”➔”Advanced Setup” to enable for “Location Tracking Log “setting



 # Setup 2 : Please click Cerio AP to “Management”➔”System Log Setup” to fill in remote Server IP Address.



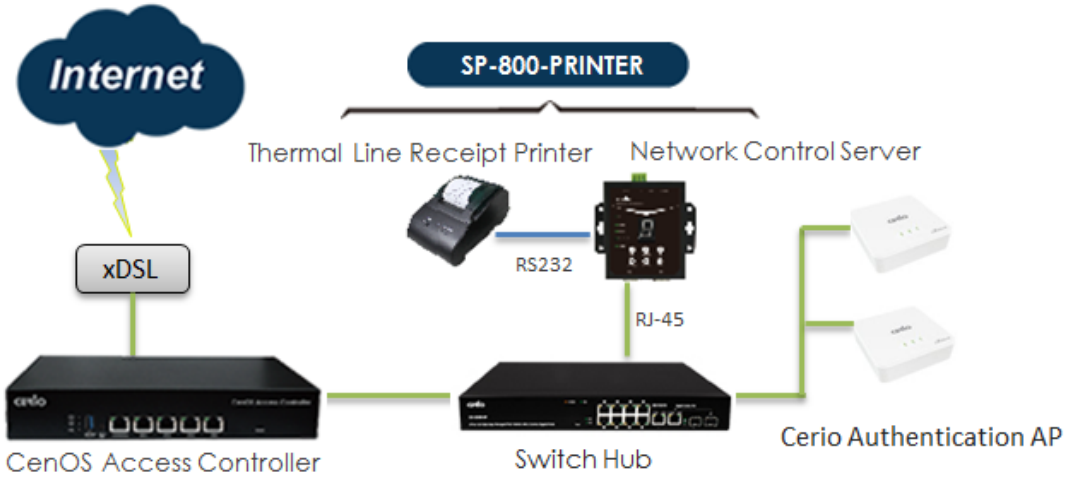
9. Technical documents

9.1 Hotspot function used POS system application

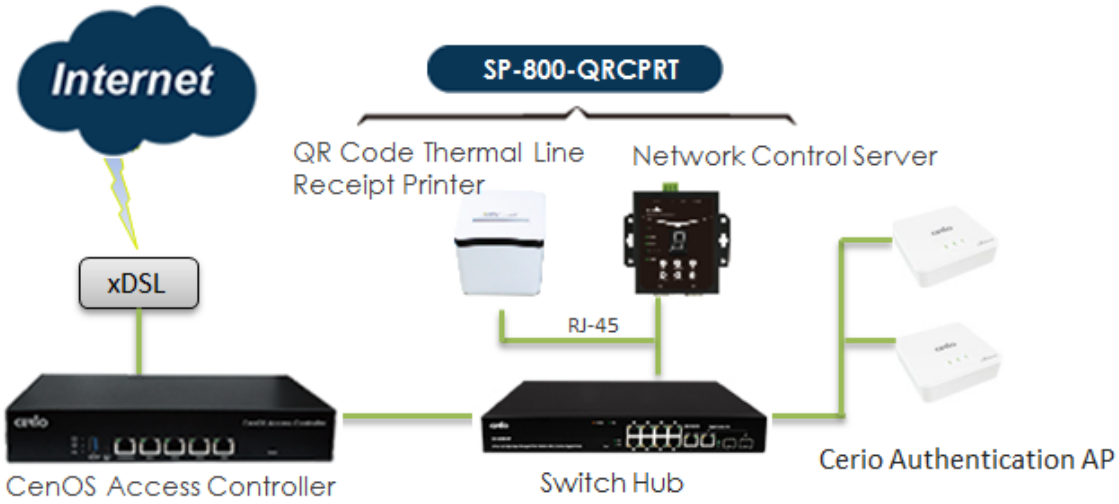
Notice	Cerio's POS system device by optional.

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

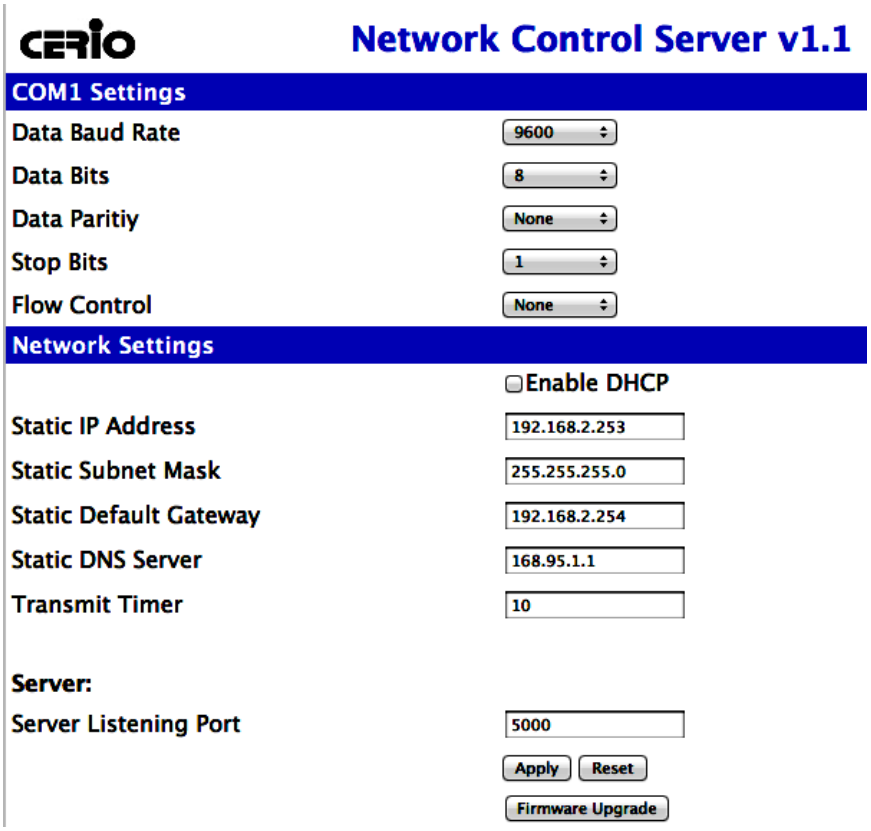


Cerio's controller mounted SP-800-QRCPRT for POS system application diagram.



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.



- **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

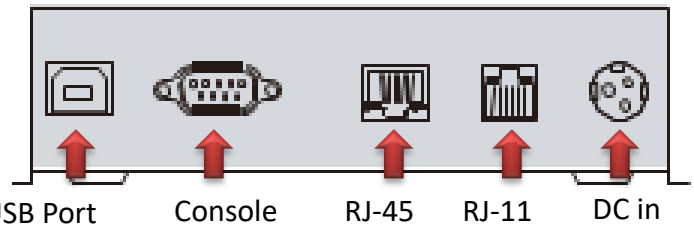
Install step for thermal paper

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

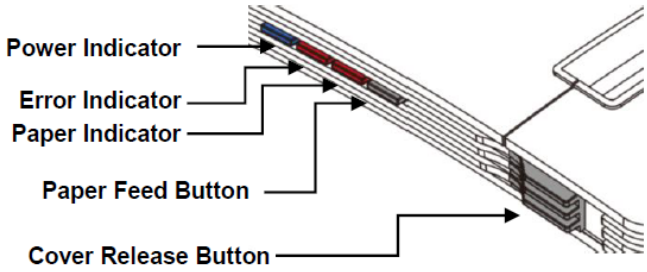
1) SP-800 connection to thermal printer use console port
2) DC Power in.
3) Power on/off switch.

Install QR Code thermal printer

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

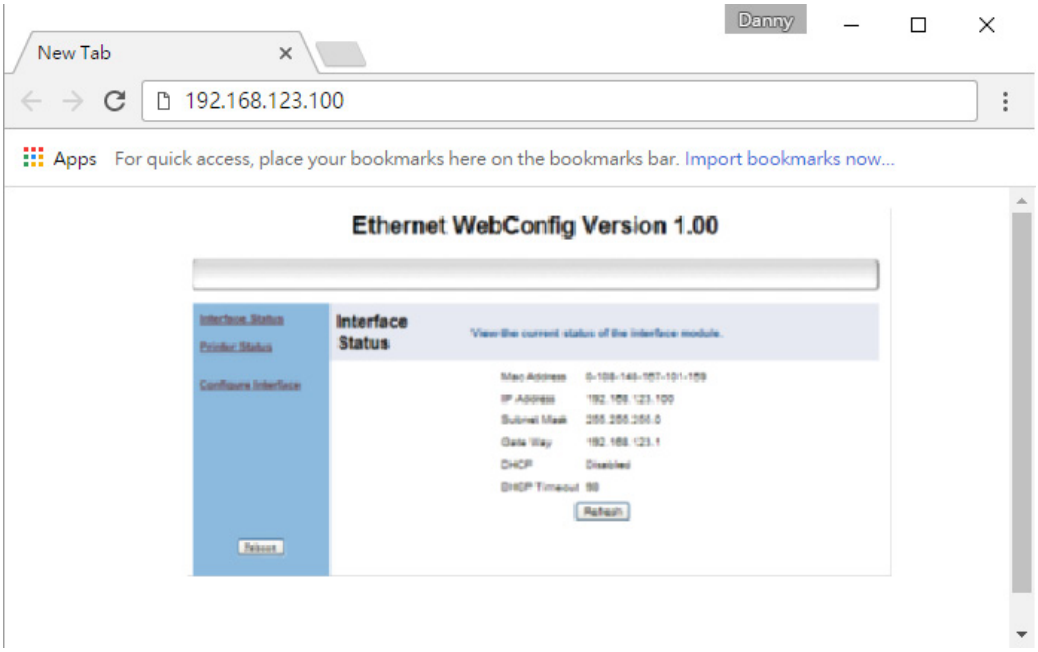


PS. Connect the controller only need to use RJ-45 and power.



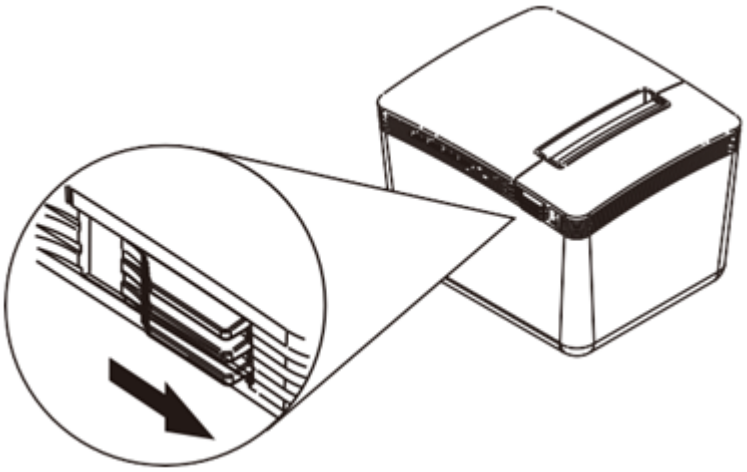
 # Login web page for QR Code printer.

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

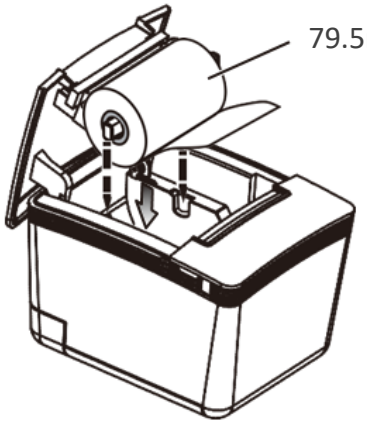


Install or Replace Paper Roll for QR code printer

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

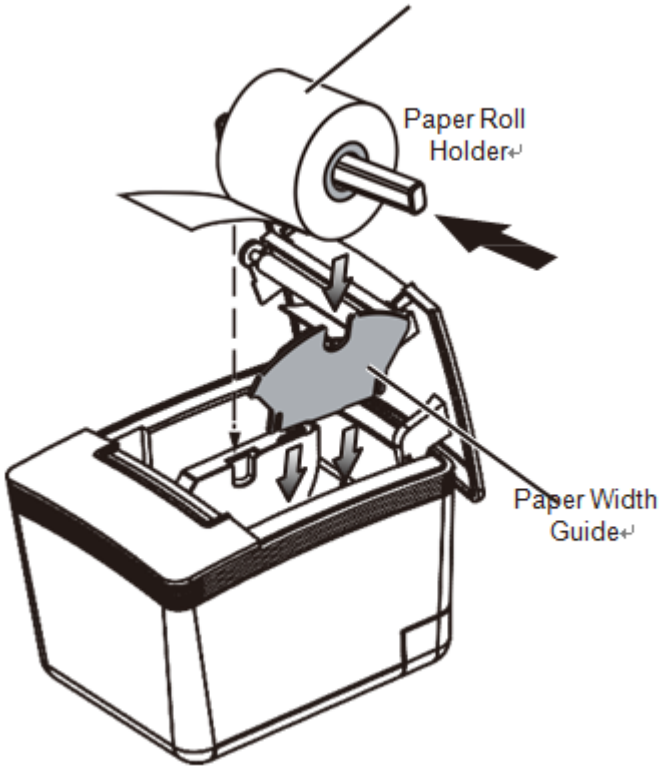


2) Roll out and install the Paper Roll with Holder into the Printer. (with the edges of the paper roll holder fitted onto the holder slots)



79.5mm size for thermal paper

57.5mm size for thermal paper

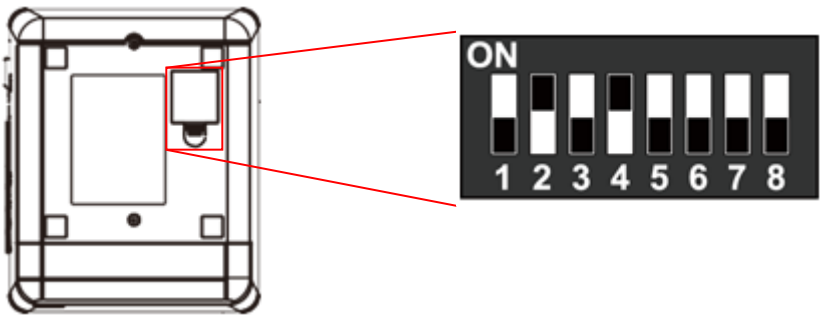


When using a paper roll in smaller width, install the Paper Width Guide first, and then install the paper roll with holder.

3) Please close the lid for thermal printer.

DIP Switch Setting for QR code Printer

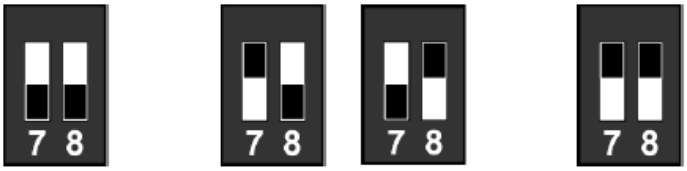
DIP Switch in printer bottom.



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)



19200 (*Default) 9600 115200 38400

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-CA** 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"

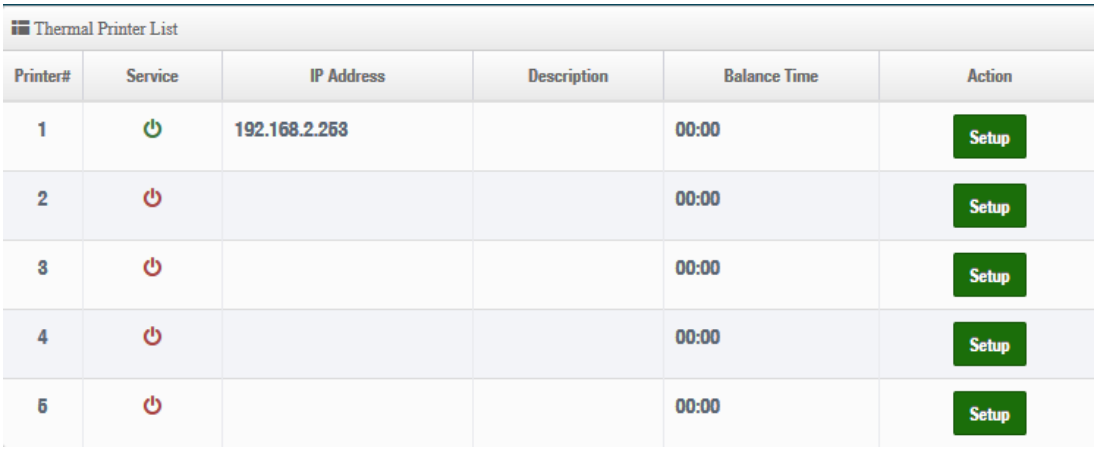
Steps3

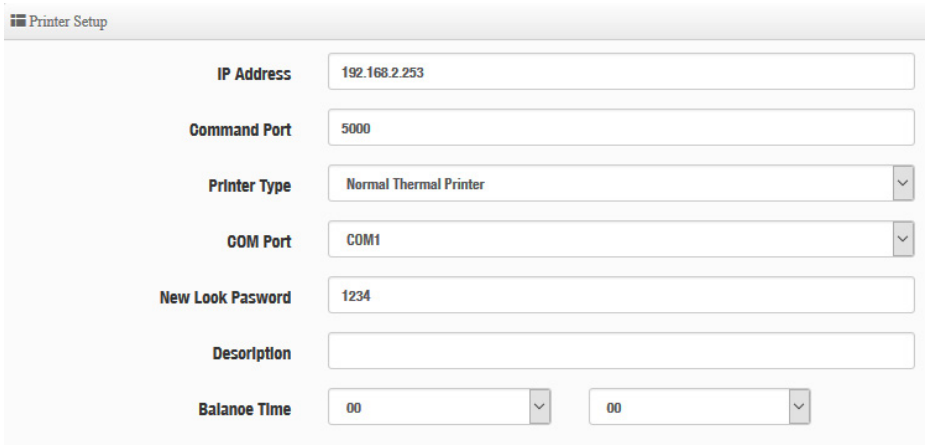
Login Cerio's Controller "**DR-4000-CA**" page (Refer controller user manual) to enable RADIUS Server. As follows

Please click menu **"Account"➔"RADIUS Server"** for Cerio's **DR-4000-CA**

Steps4

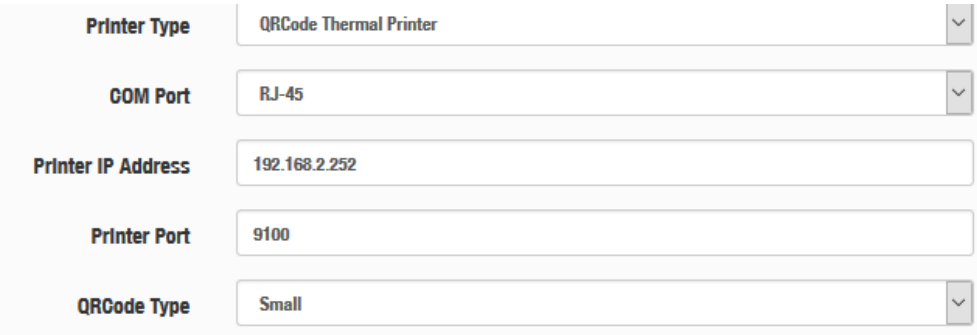
Set the connection between **DR-4000-CA** and SP-800. Please click menu **"Account"➔" Thermal Printer Setup**" to enable function, as follows





- **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 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.

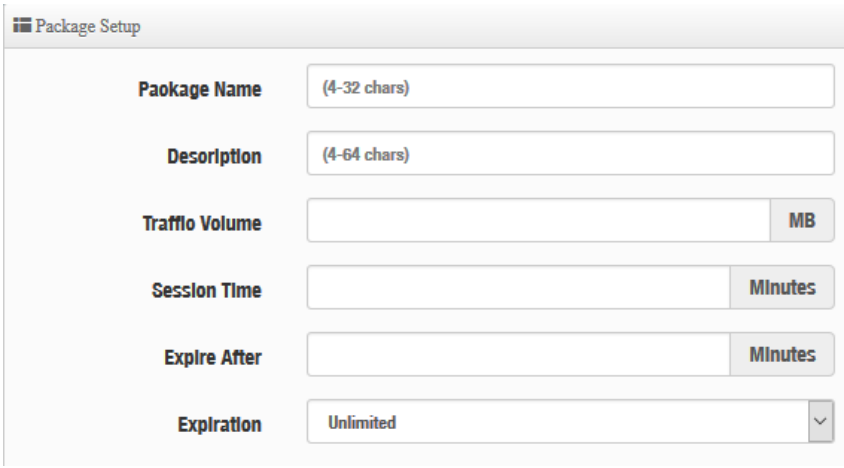
Notice	1. If use normal thermal printer and connect to com1 port of the SP-800, please select COM1

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

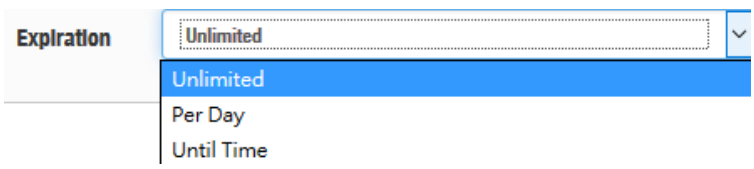
- **New Lock Password**：Enter pass key of the **DR-4000-CA** to connect SP-800
- **Description**：Administrator can enter description.

Steps5

Setup internet time rules for package authentication type (**DR-4000-CA**). Please click menu "**Account**" ➔ "**Package setup**". As follows

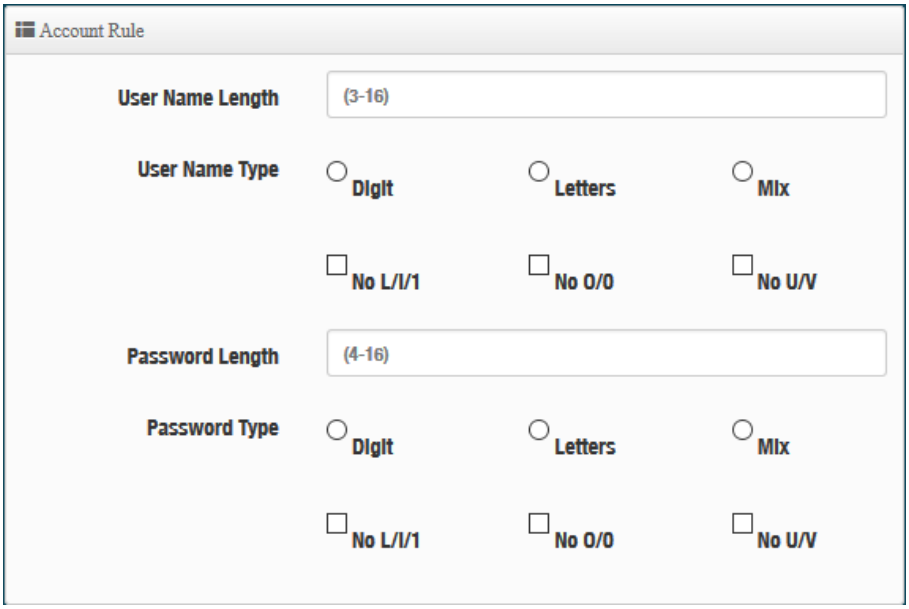


- **Package Name:** Administrator can set Identify name for the package rules.
- **Description**: Administrator can set the description for package rules.
- **Traffic Volume:** Administrator can set authentication account use traffic limit for the package rules.
- **Session Time:** Administrator can 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.

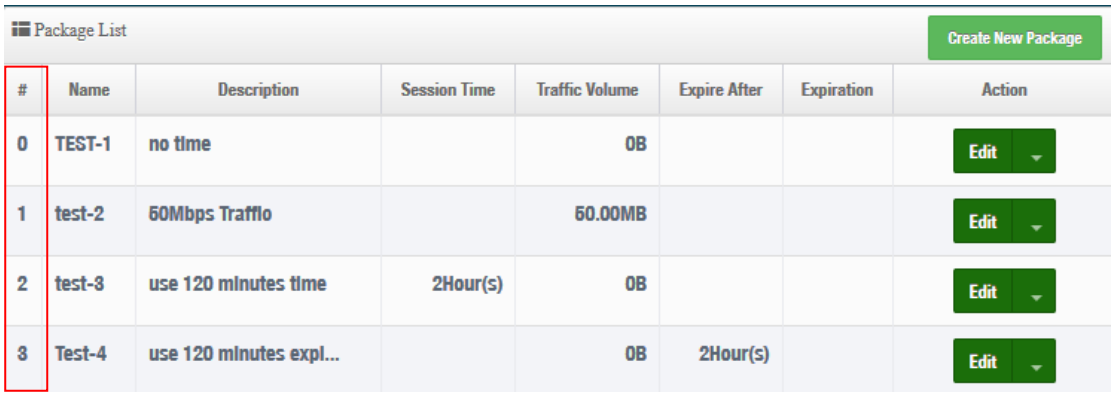


- ✓ **Unlimited:** After the account is signed in, the system does not count the time
- ✓ **Per Day:** After the account is signed in, the system start counted time until the end time.

✓ **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.



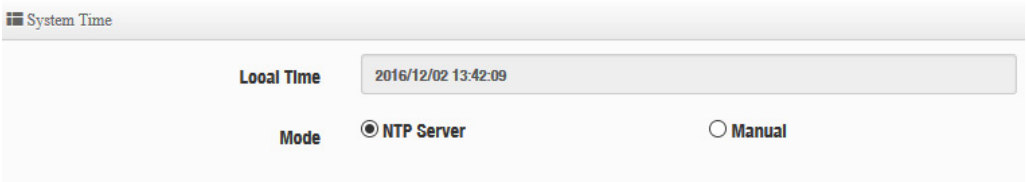
PS. Package list (0~9) is Network control server (SP-800) code, administrator can choose number to print out account.



Steps6

The system time is very important, administrator must set system time is right. Please click **DR-4000-CA** 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-CA** setting

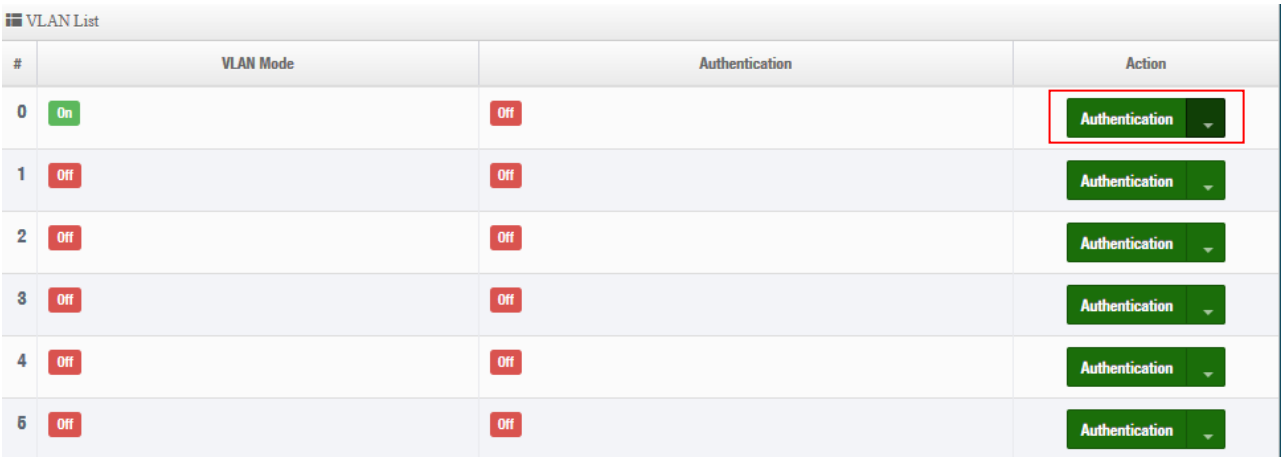
Enable Web authentication for Access Point

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

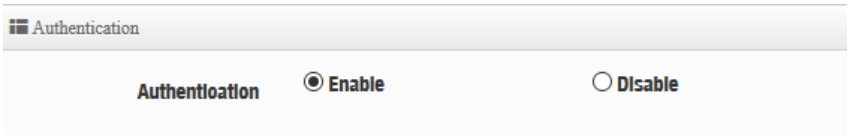
Steps7

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.

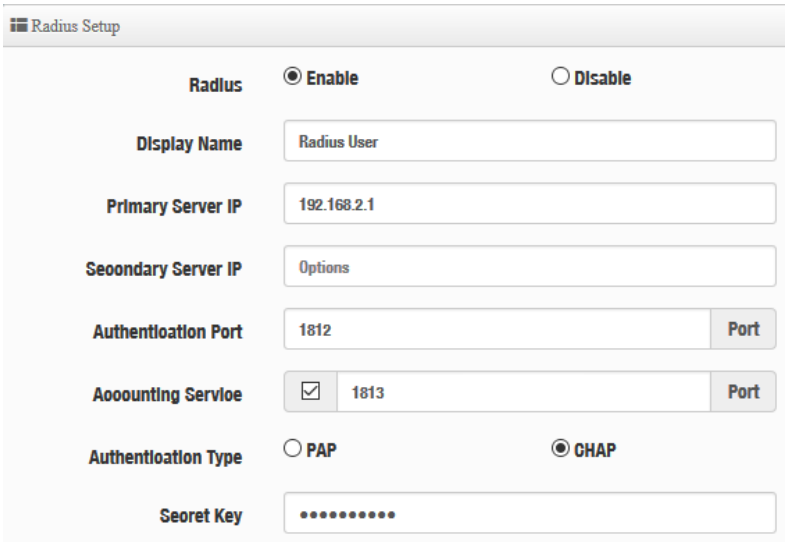
1) Enables web authentication function. Please click "System"➔"Authentication" for Cerio's Access Point.



2) Click Authentication button and enable the function.



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



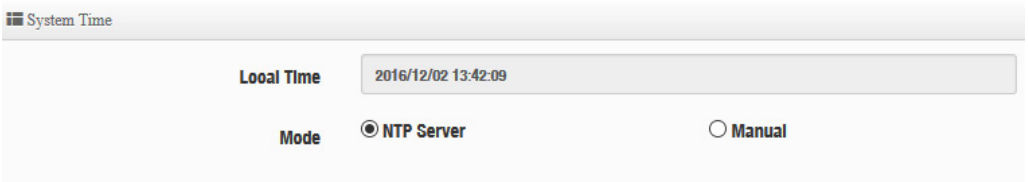
Steps8

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 (Cerio's Access Point) menu "**System**"➔"**Time Server**" to set system time.

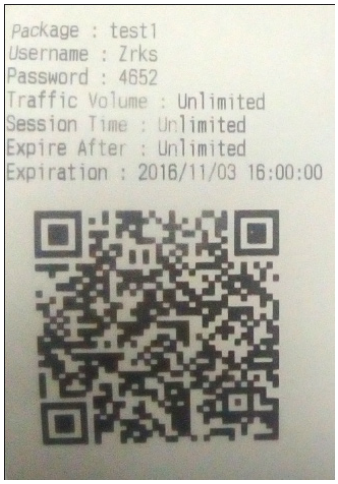
PS. Recommend select update the system time for the NTP Server

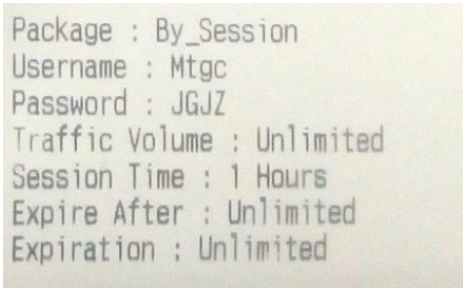


This completes all architecture settings

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

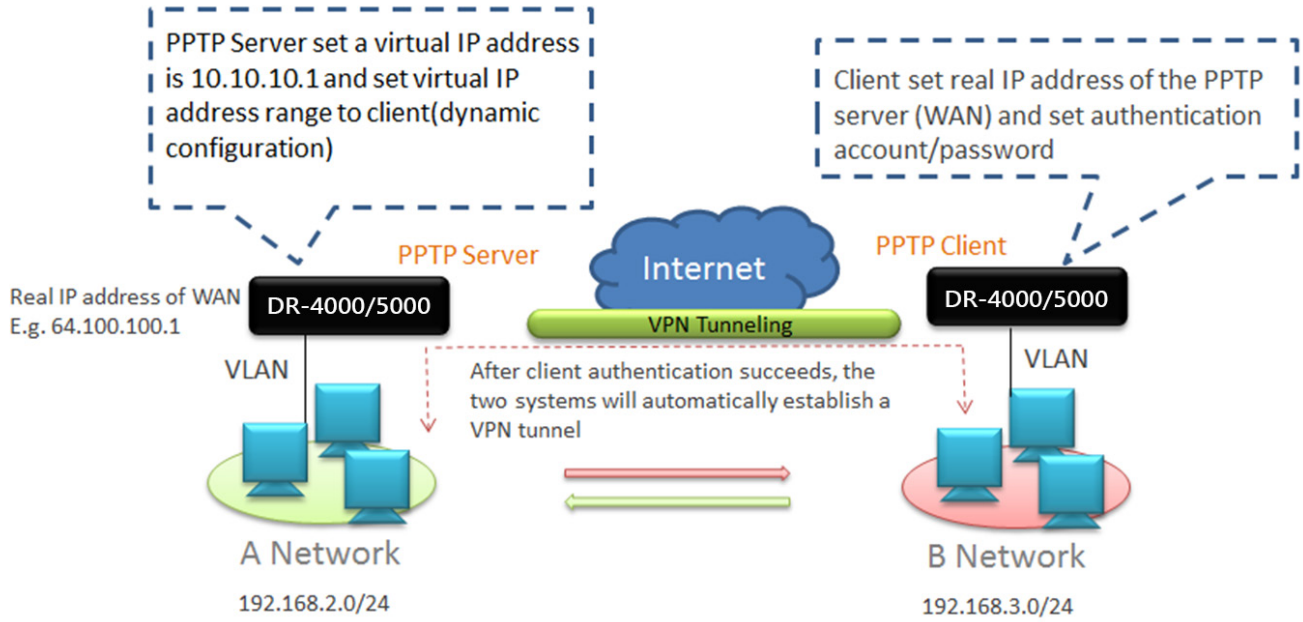
As follows





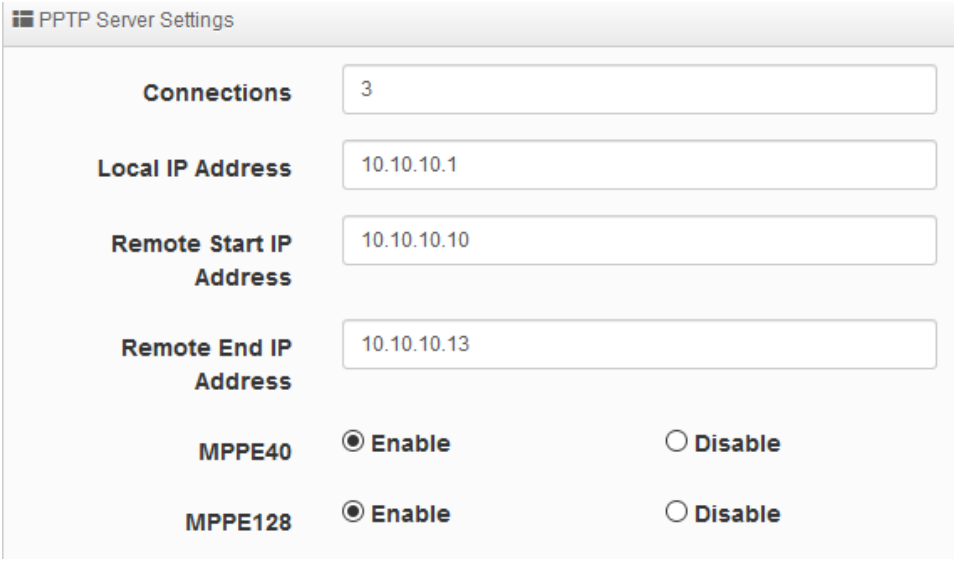
9.2 Example for PPTP/L2TP setup

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

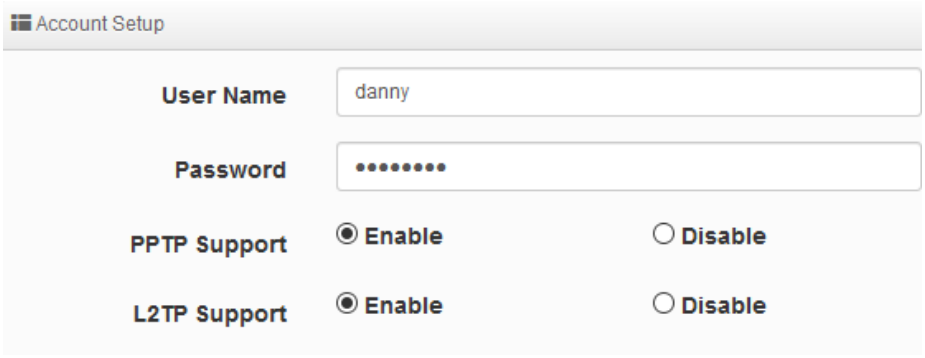


PPTP Server setup step

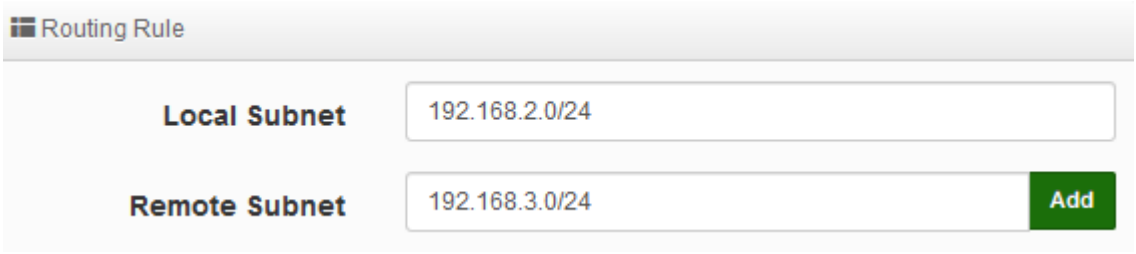
1. Enable PPTP/LTP Server and set VPN used virtual IP address.
   (Refer to 3.6 /3.7 for instructions)



2. Create authentication of client account and password

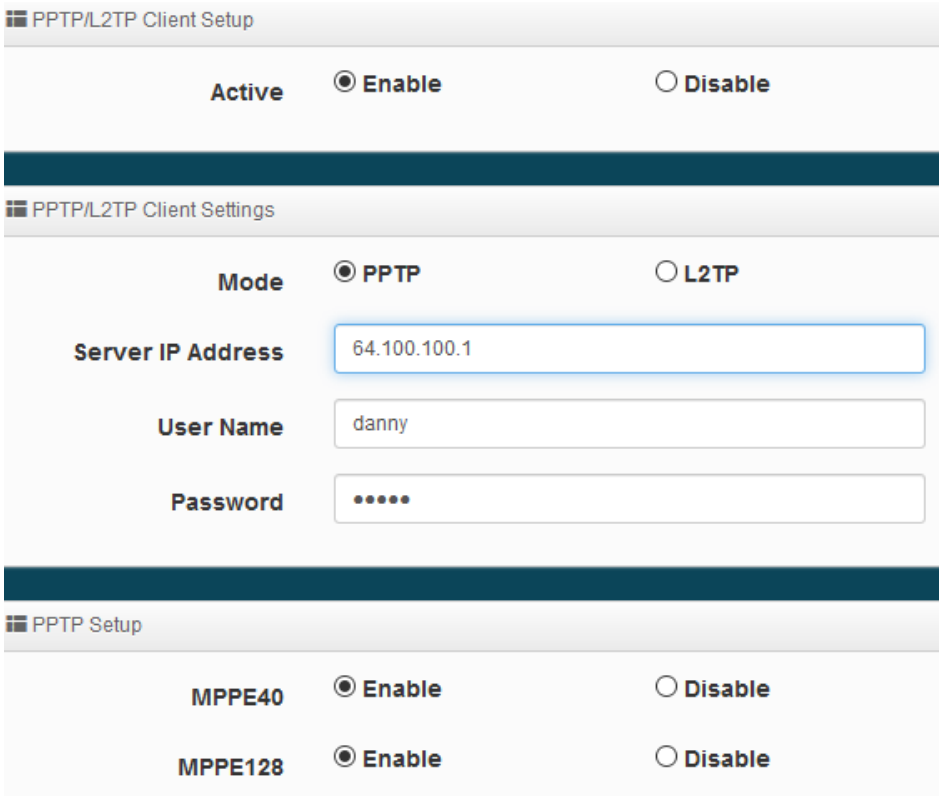


Setup routing between the two networks



PPTP Client setup step

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

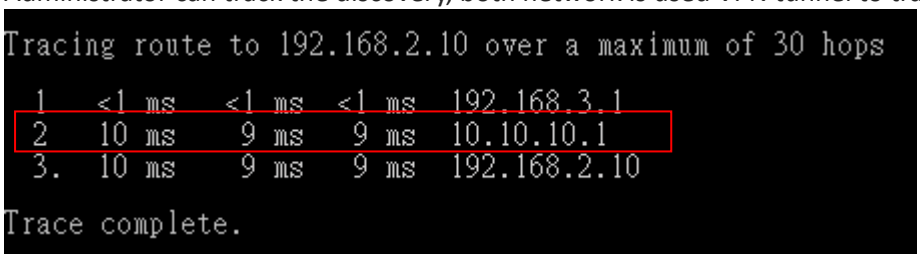


2. Setup routing between the two networks

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.

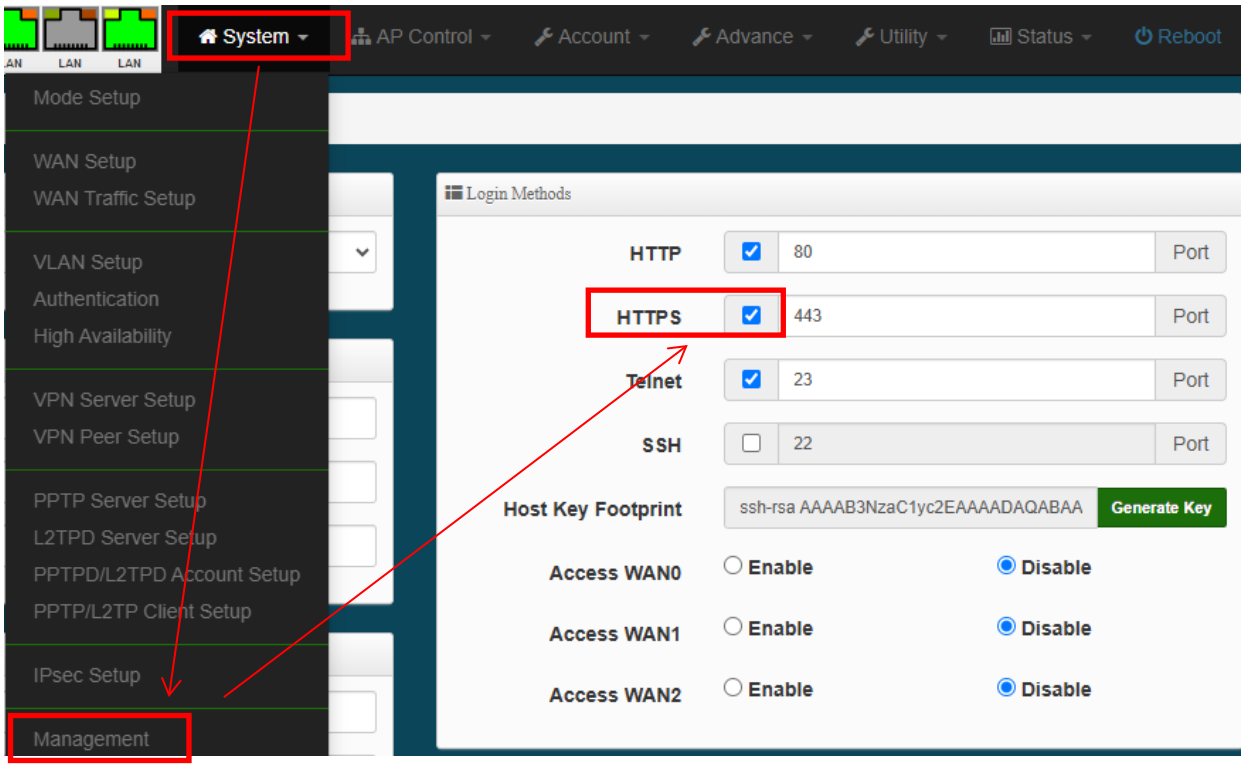


9.3 Example for Web Authentication Portal URL using HTTPS

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.

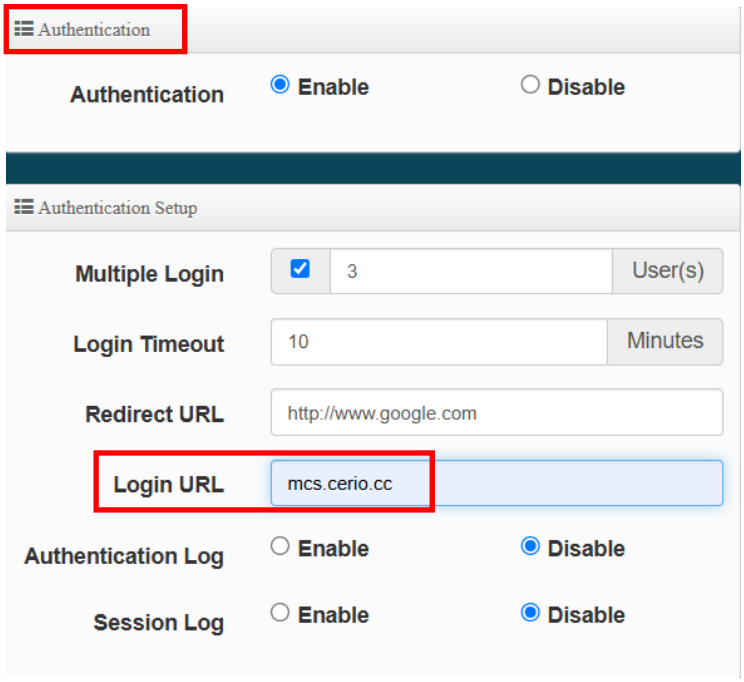


Note that in addition to enabling the https secure transmission function, you need to have a main domain or subdomain URL, and also obtain an SSL certificate for the relative domain URL. If it is enabled without importing the SSL certificate, it will cause "User Every time the browser used by the computer (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.



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.

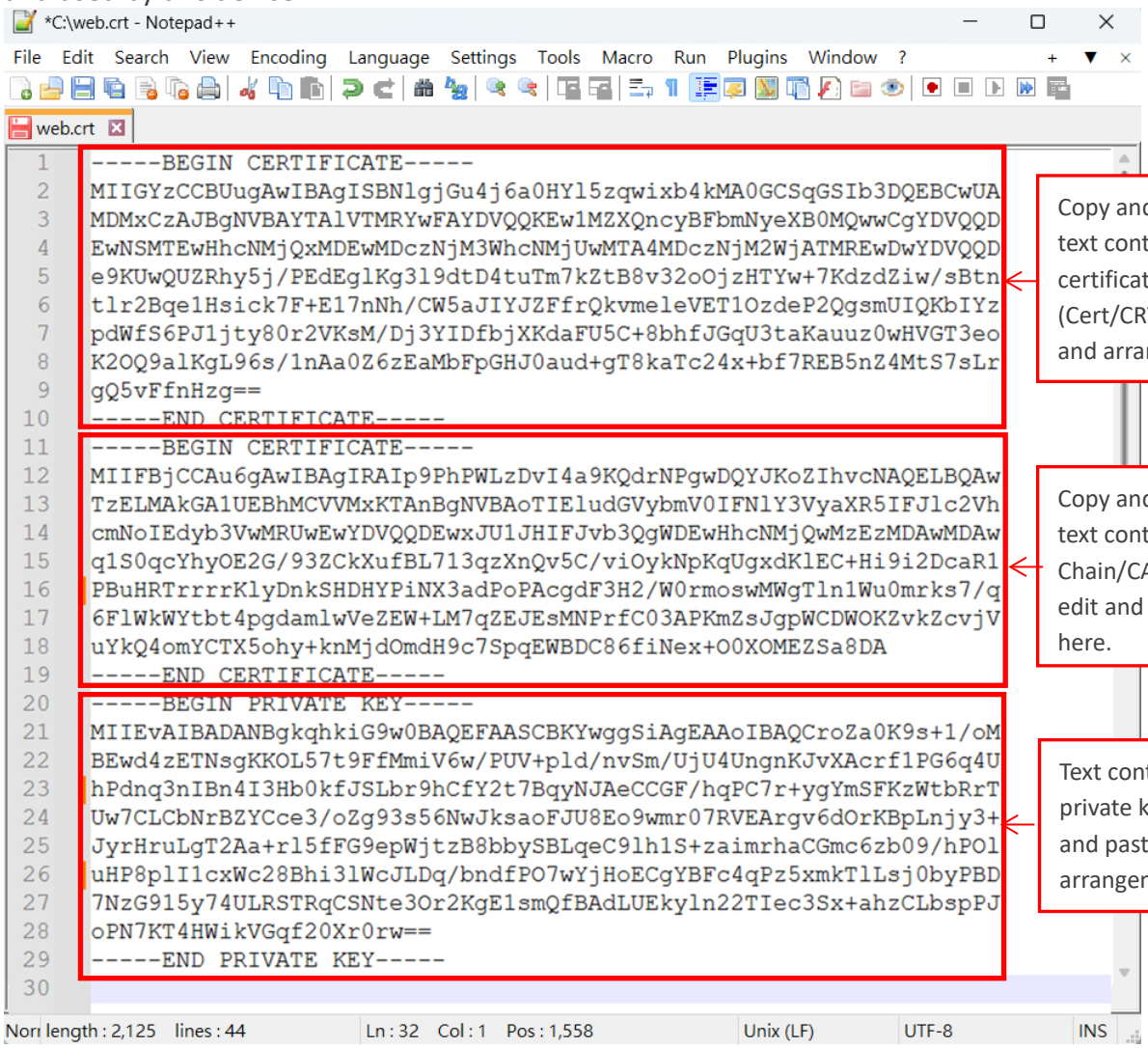
The free software Notepad++ (plain text/code editor) is used as the editing display of plain text below. The merged certificate content (displayed with regular alphanumeric characters) and format legend of multiple certificate files are *and omitted* displayed as follows:

-----BEGIN CERTIFICATE-----
MIIGYzCCBUugAwIBAgISBNlgjGu4j6a0HYl5zqwixb4kMA0GCSqGSIb3DQEBCwUA
MDMxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQww*.....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.

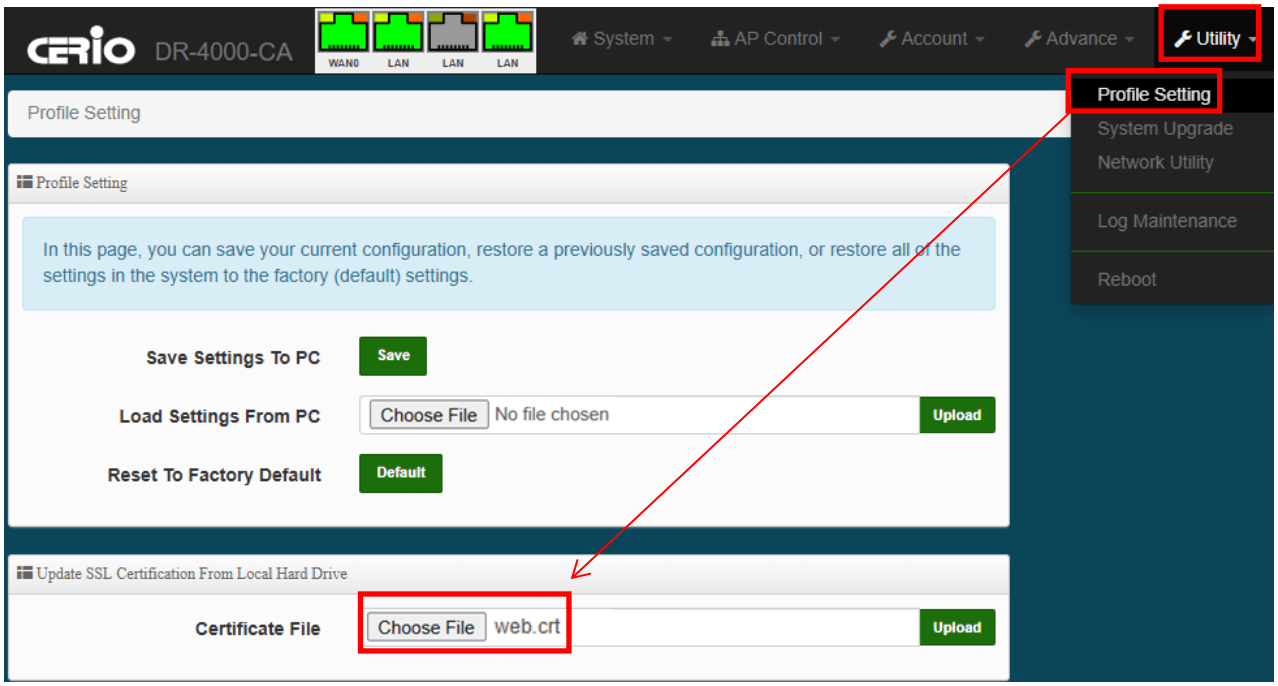
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgT+MOdVmQOx6kUqQr
LislRau2XKztqDgCn/VTqe0Mom2hRANCAAQ+6vD8vf6J1sWVHxECvqZlN9FeG3dU*.....and omitted*
-----END PRIVATE KEY -----

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.

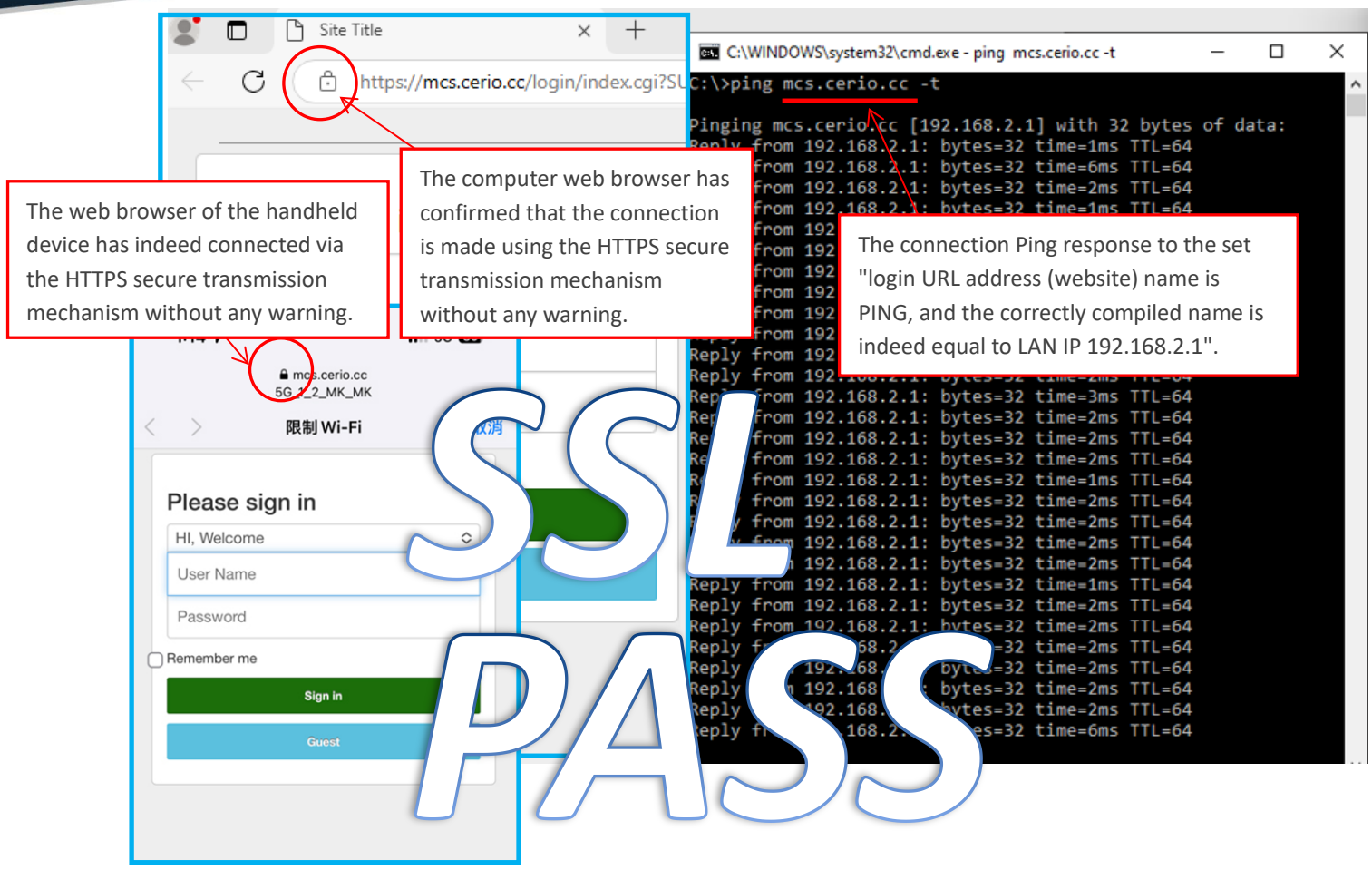


Please go to "Utility" → "Profile System " → "Update SSL Certification From Local Hard Drive" in the UI interface of this device to upload and import the obtained SSL certificate file. You must merge the text contents of the multiple certificate files you have. into a file file for smooth uploading and 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.

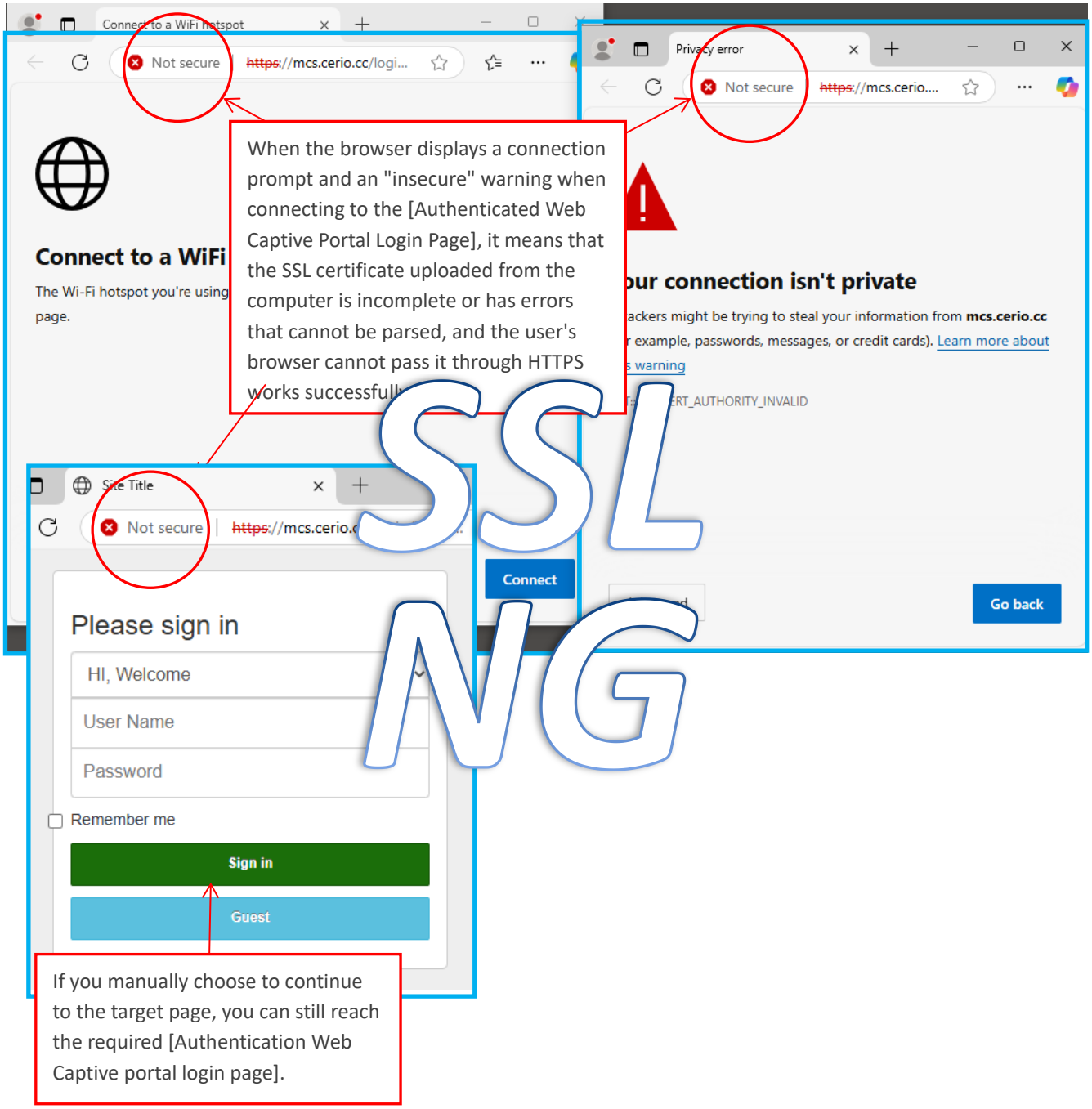


Verify the setting results:

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.

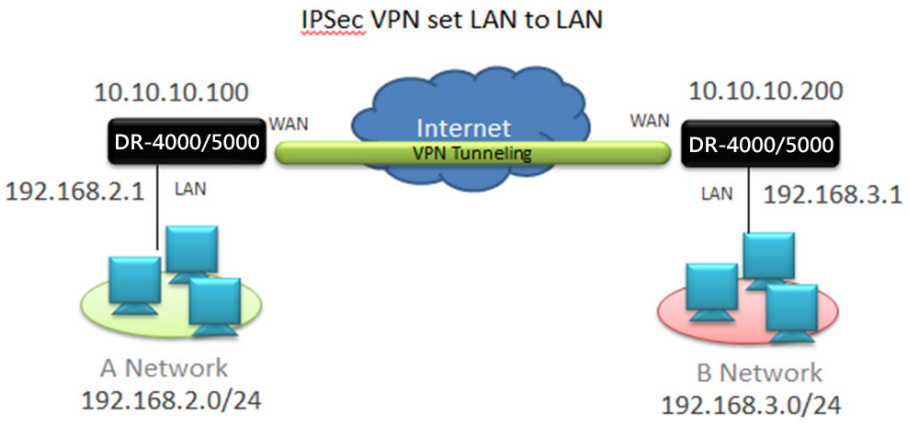


After restarting for the settings to take effect, if the browser that the user is trying to operate enters the [Authentication Web Captive portal login page] and the browser jumps out the following message, it means that the credentials are incorrect or the upload failed, and the browser cannot correctly 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.


Connect to a WiFi hotspot
Not secure
https://mcs.cerio.cc/logi...
Connect to a WiFi
The Wi-Fi hotspot you're using
page.
When the browser displays a connection prompt and an "insecure" warning when connecting to the [Authenticated Web Captive Portal Login Page], it means that the SSL certificate uploaded from the computer is incomplete or has errors that cannot be parsed, and the user's browser cannot pass it through HTTPS
Privacy error
Not secure
https://mcs.cerio....
our connection isn't private
ackers might be trying to steal your information from mcs.cerio.cc
example, passwords, messages, or credit cards). Learn more about
warning
ERT_AUTHORITY_INVALID
Go back
Site Title
Not secure
https://mcs.cerio.
Connect
Please sign in
HI, Welcome
User Name
Password
Remember me
Sign in
Guest
SSL
NG
If you manually choose to continue to the target page, you can still reach the required [Authentication Web Captive portal login page].

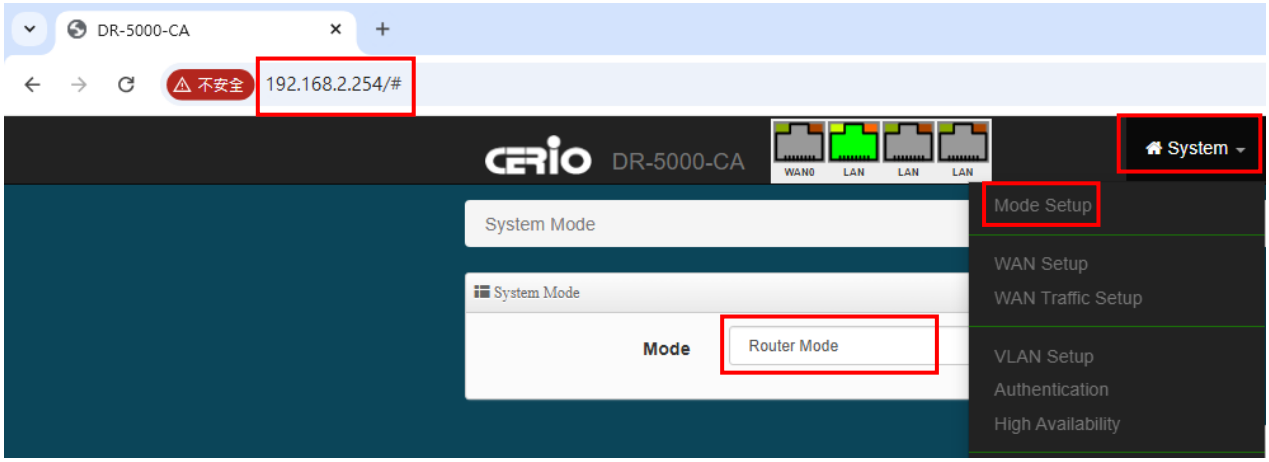
9.4 Example of setting up IPSec VPN set LAN to LAN

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:



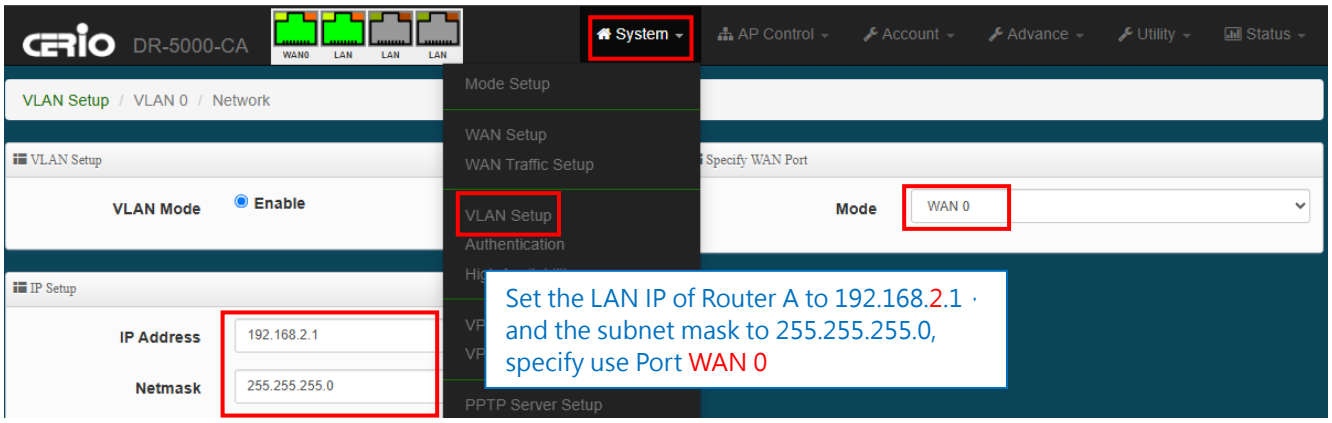
Step-1: We take two sets of Router(two environments) with different LAN segments as a sample case, and set the LAN IP of the two routers to different network segments.

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

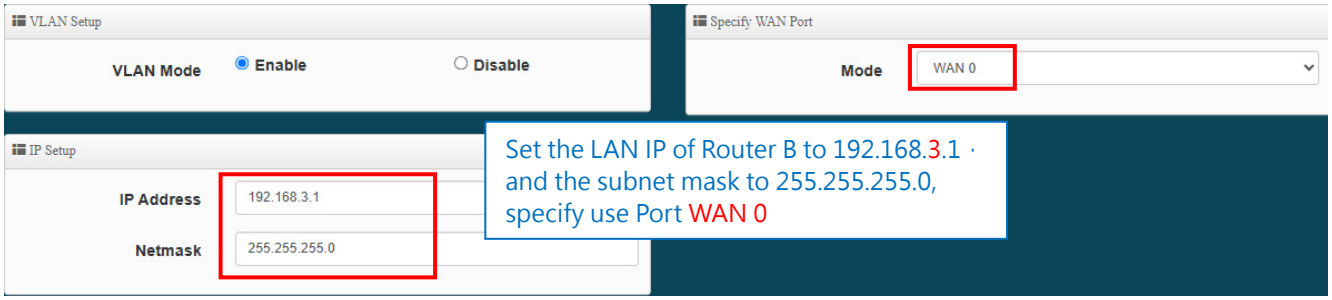
192.168.2.1. Set the IP address so that the LAN IP of the A Network and the B Network will be separated into two segments, and then use the changed IP address after the setting is saved. The subnet mask is the same as 255.255.255.0. Select the specified port as WAN0.

	IP Address	Netmask	Specify WAN Port
Router A	192.168.2.1	255.255.2555.0	WAN 0
Router B	192.168.3.1	255.255.2555.0	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.

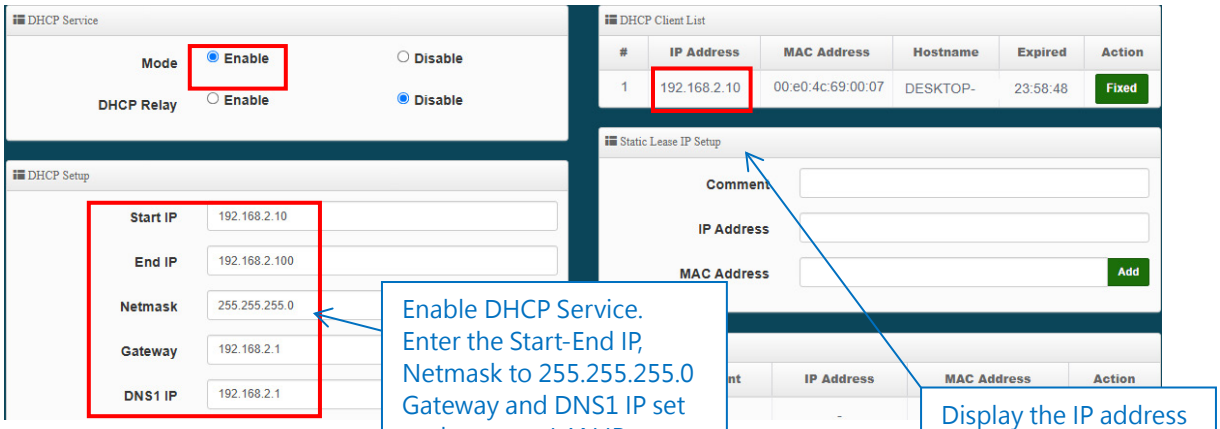
After saving the configuration and restarting the router, you must set the user computer (DHCP client Users) to “Obtain IP address automatically”, so that the user computer can automatically

obtain the IP address assigned by the router.

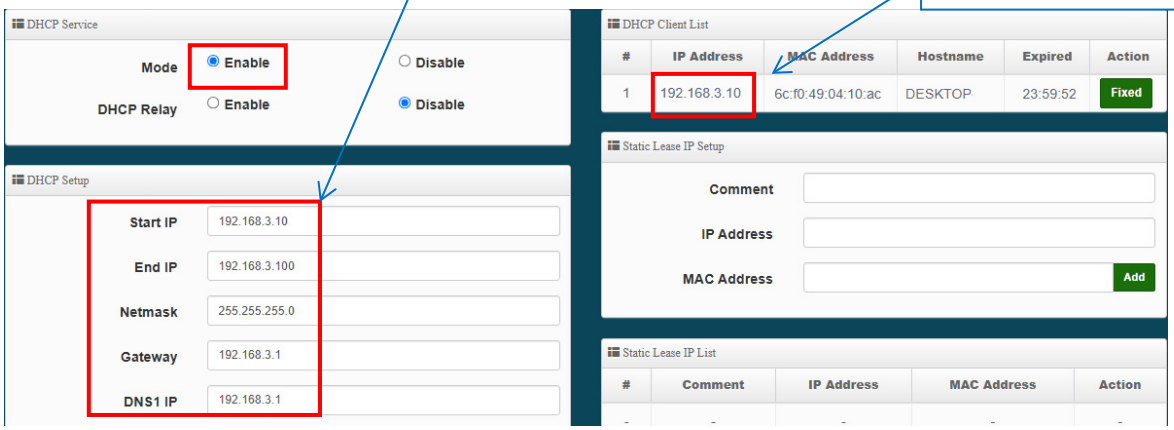
The following as example:

	Start IP	End IP	Netmask	Gateway	DNS 1 IP
Router A	192.168.2.10	192.168.2.100	255.255.2555.0	192.168.2.1	192.168.2.1
Router B	192.168.3.10	192.168.3.100	255.255.2555.0	192.168.3.1	192.168.3.1

Confirm Router A：



Confirm Router B：



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).

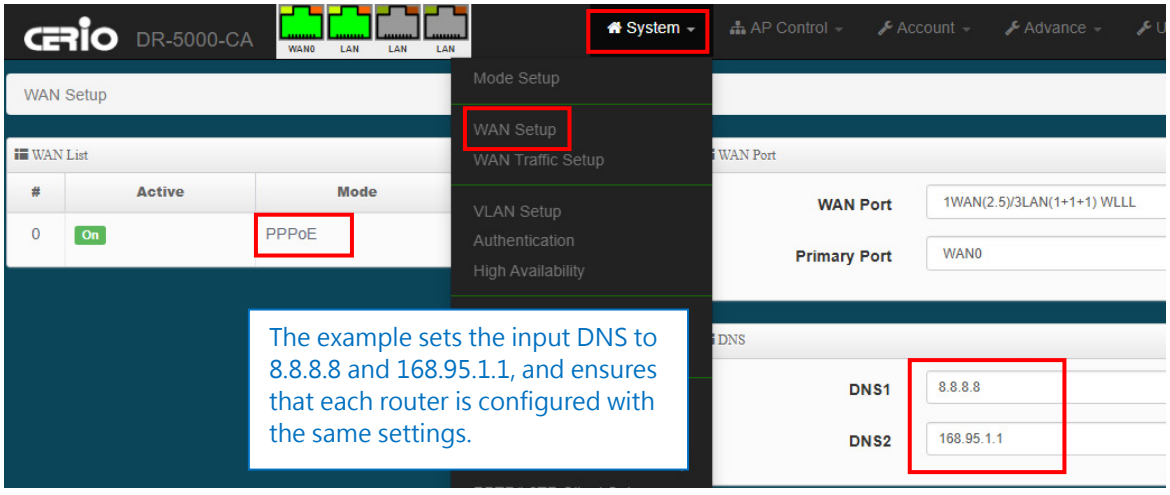
Select“PPPoE”as the WAN Mode, enter the username and password provided by the Internet Service Provider (ISP), and remember to enable NAT (if you choose not to enable NAT, it will be a transparent Bridged passthrough that directly uses a WAN IP to connect to the outside world, and you will not be able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

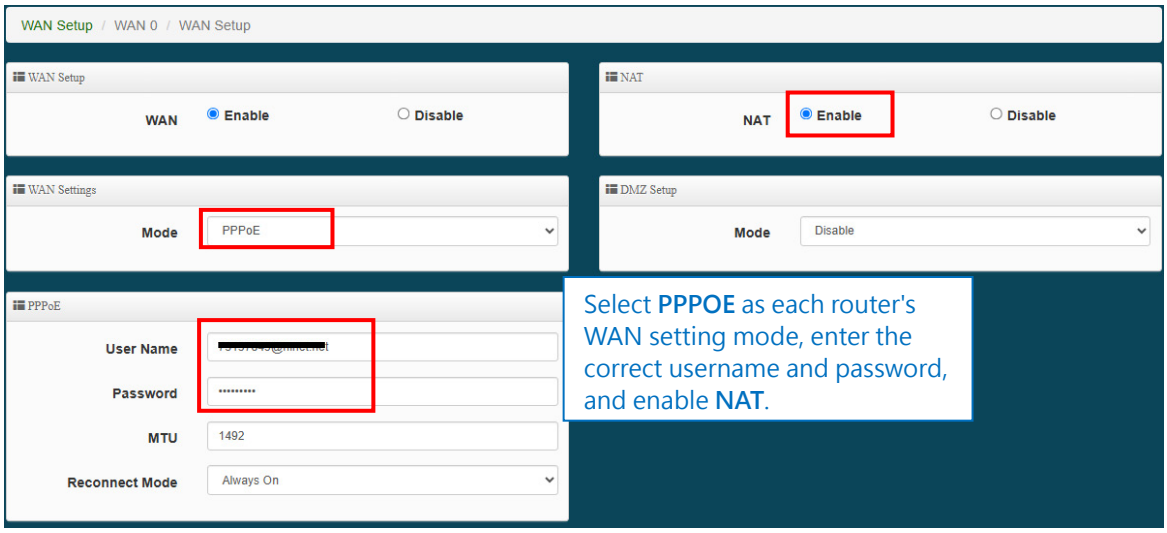
After saving the configuration and reboot, enter the interface and click " **System > Overview** " to check the WAN IP provided by PPPoE. This IP is the public IP address of the router. At this time, the computer can connect to the Internet through the DR-4000/DR-5000 series.

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

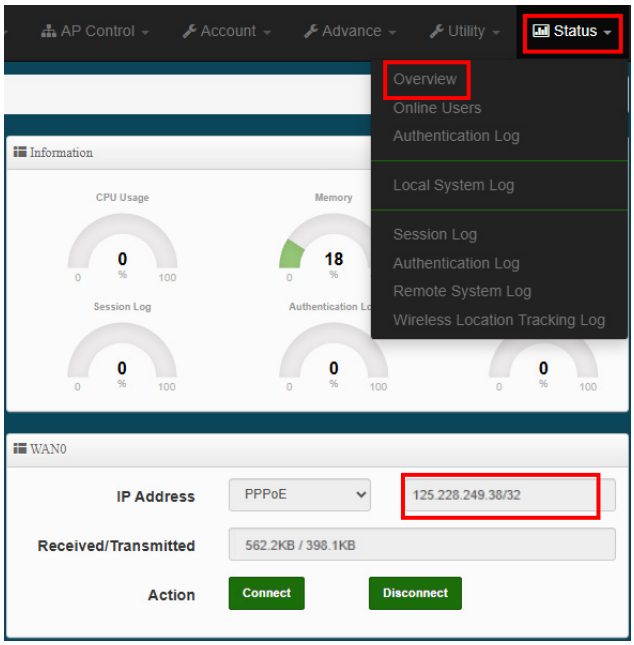
The following example:

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



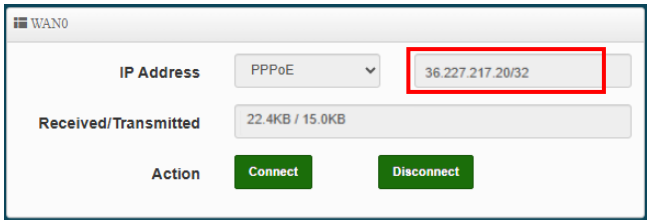


Confirm Router A：



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

Confirm Router B：



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

Step-4: Set IPSec VPN parameters, shared authenticaition 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 :

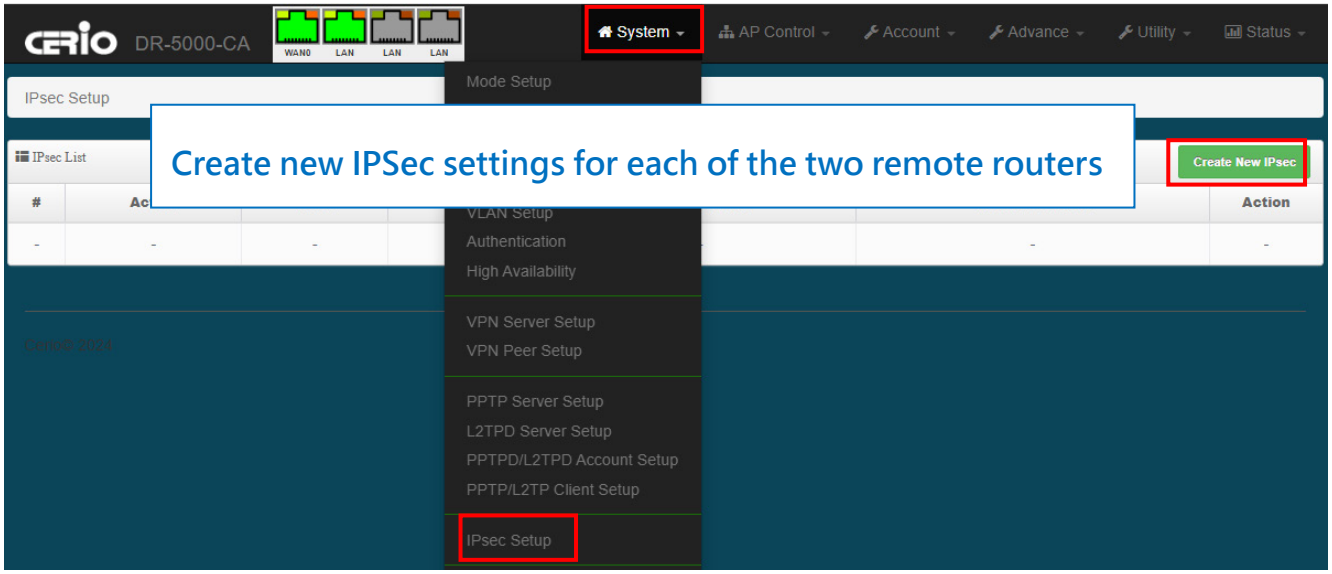
Enable IPSec service, select LAN-to-LAN for Mode , select WAN 0 for WAN interface, select IP address for ID type, and Nexthop can be set to 0.0.0.0. Check whether the basic configurations of the two site routers are matched: Remote Host (the other side WAN IP), Local Subnets, Remote Subnets, pre-shared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

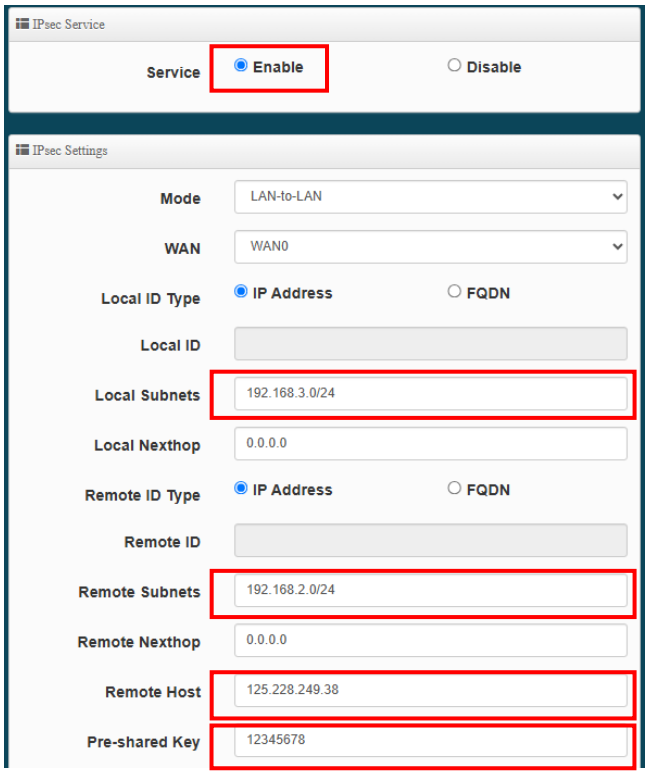
IKE Mode: Main / Aggressive
IKE Authentication: MD5
Encryption: 3DES
DH Group: DH2

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：



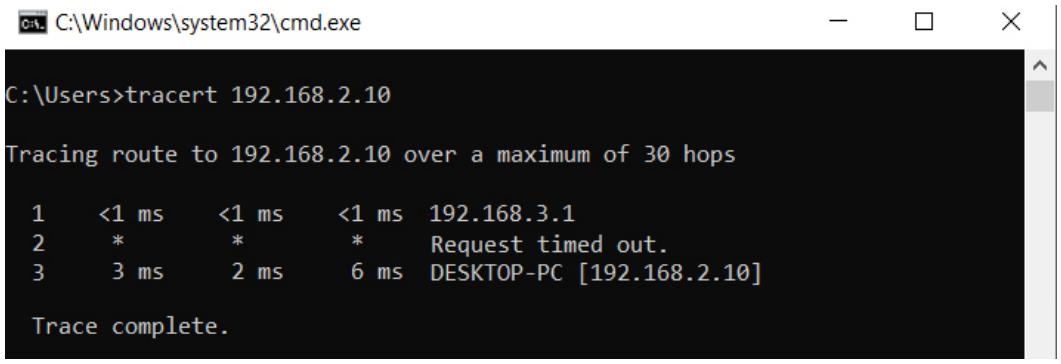
Example settings for Router B:
Local Subnets to 192.168.3.0/24,
Remote Subnets to 192.168.2.0/24,
Remote Host to 125.228.249.38
Pre-shared Key to 12345678

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:



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.