TAR-120-M12 / TAR-3120-M12

EN50155 IEEE 802.11 Cellular VPN Router

User's Manual

Version 1.0

June, 2011

www.oring-networking.com

COPYRIGHT NOTICE

TRADEMARKS

 is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., No.542-2, Zhongzheng Rd., Xindian Dist., New Taipei City 23148, Taiwan
Tel: +886-2-2218-1066 // Fax: +886-2-2218-1014
Website: www.oring-networking.com

Technical Support
E-mail: support@oring-networking.com

Sales Contact
E-mail: sales@oring-networking.com (Headquarters)
sales@oring-networking.com.cn (China)

Table of Contents

Getting to Know your Wireless AP Router

1.1 Overview

The ORing TAR-120-M12 / TAR-3120-M12 Wireless AP router is designed to operate in industrial environments. The AP router provides fast and effective ways of communicating to the internet over wired or wireless LAN. In addition, multiple kinds of WAN connections are provided for easily access to the internet.

The ORing TAR-120-M12 / TAR-3120-M12 wireless AP router comes with IEEE 802.11a/b/g or IEEE 802.11b/g high-performance wireless technologies. It is capable of data transfer rates up to 54Mbps. It is easy for you to extend the network reach and increase the number of computers connected to your wireless network.

With built-in HSUPA WAN connection, the ORing TAR-120-M12 / TAR-3120-M12 wireless AP router can be mounted in harsh environment easily to provide internet access anytime and anywhere.

The ORing TAR-120-M12 / TAR-3120-M12 wireless AP router's VPN capability creates encrypted "Virtual Tunnels" through the internet, allowing remote or traveling users for secured connection with the network in your office.

1.2 Software Features

- High Speed Air Connectivity: WLAN interface supports up to 54Mbps link speed connection
- Highly Security Capability: WEP/WPA/WPA2/Radius/TKIP supported
- Secured Management by HTTPS
- Intuitive Web-based management user interface for simply and easily operation
- Functions of firewall provides many security features such as blocking attacks from hacker, especially IP Spoofing, Ping flood, Ping of Death, DOS, DRDOS, Stealth Scan, ICMP flooding etc.
- Advanced firewall configuration to extend the capability and security, such as Virtual Server, Port Trigger, DMZ host, UPnP auto Forwarding, IP Filter and MAC filter

- Switch Mode Supported: Daisy Chain support to reduce usage of switch ports
- Event Warning by Syslog, Email, SNMP Trap, Relay and Beeper

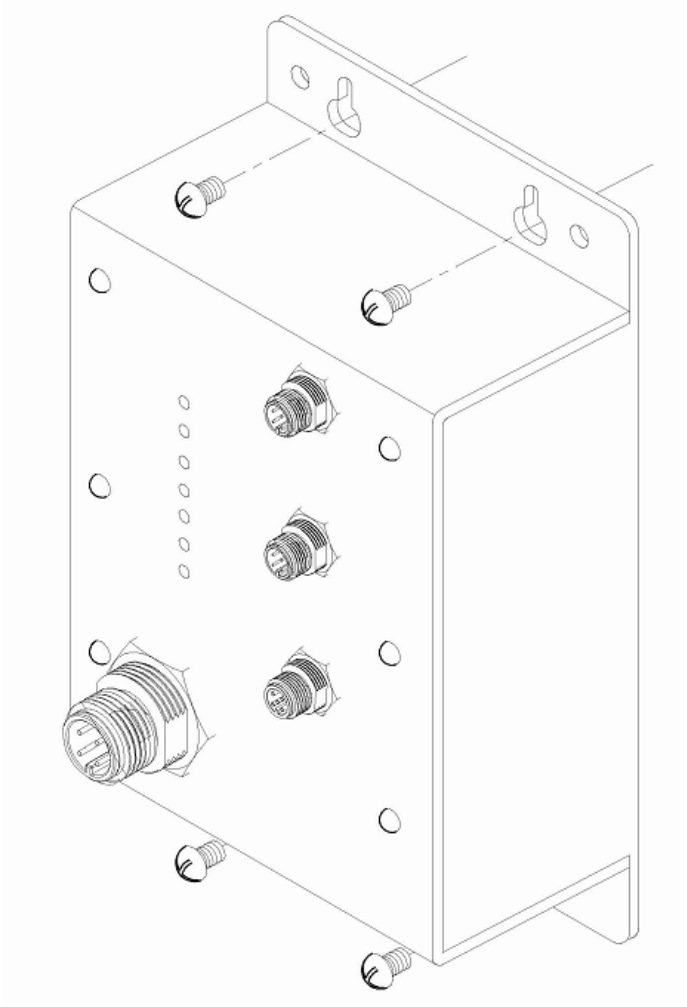
1.3 Hardware Features

- Built-in HSUPA Cellular Modem with SIM card slot included for WAN connection
- Two 10/100Base-T(X) Ethernet ports for WAN / LAN connection individually
- Redundant Power Inputs: Dual 12~48 VDC on M23 connector
- Casing: IP-40
- Dimensions (W x D x H) : 125(W) x 65(D) x 196(H) mm
- Operating Temperature: -20 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing

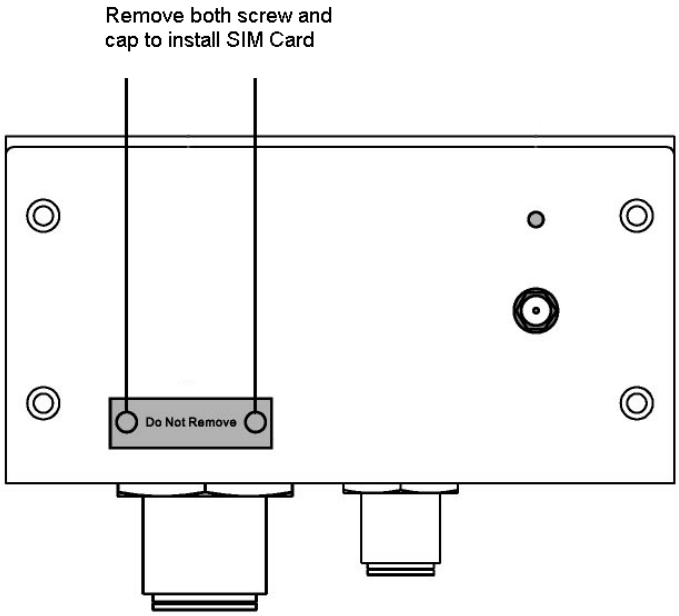
Hardware Installation

2.1 Wall Mounting Installation

Each AP router can be fixed on the wall. Use screws to mount the AP router on the wall:



2.2 SIM Card Installation



Important Notice: POWER DOWN THE TAR-120-M12 / TAR-3120-M12 BEFORE INSTALLING THE SIM CARD.

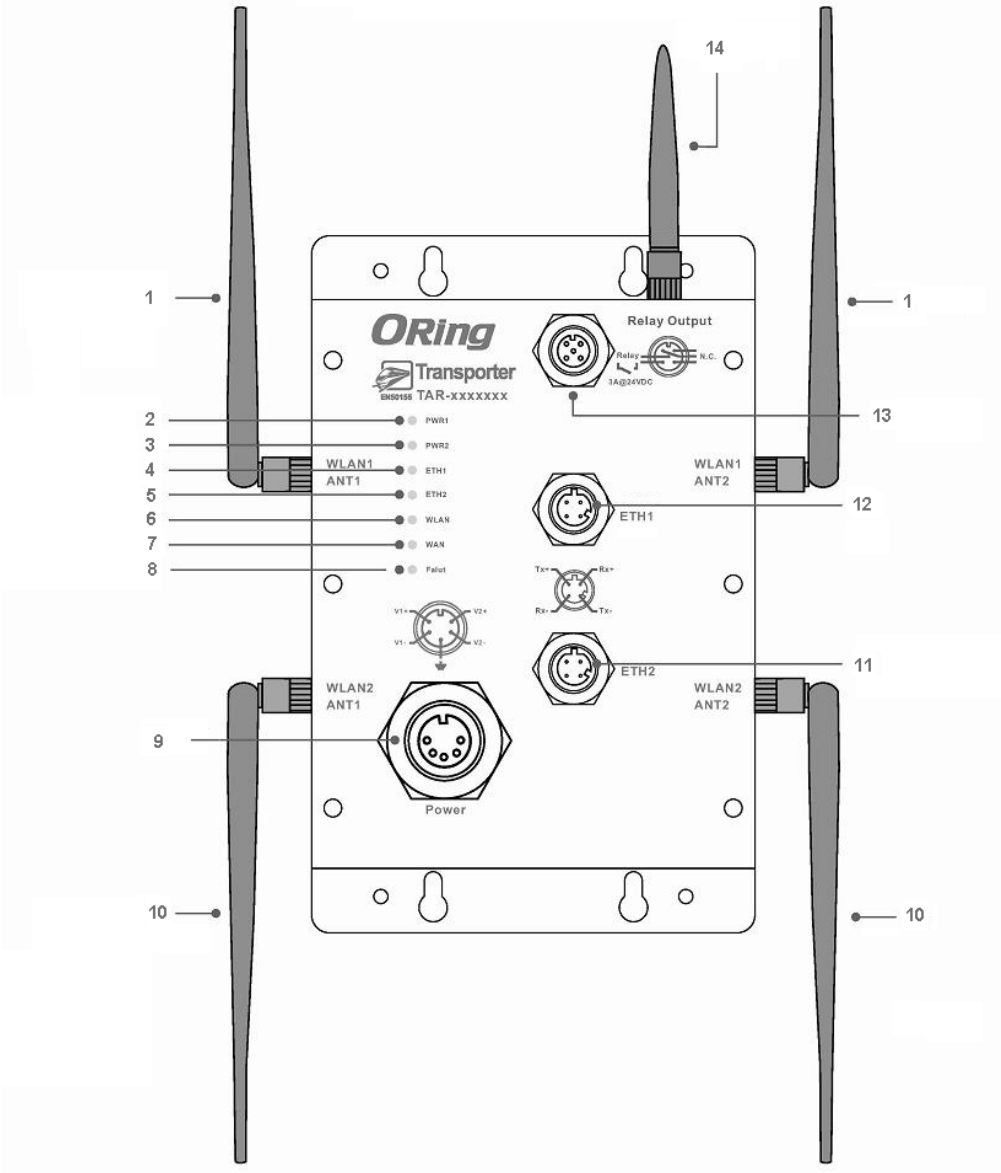
Hardware Overview

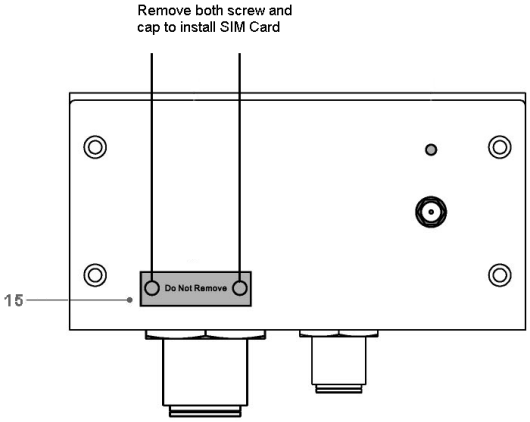
3.1 Front Panel

The following table describes the labels that stick on the TAR-120-M12 / TAR-3120-M12.

Port	Description
10/100 Base-T(X) fast Ethernet ports on M12 connector (D-coding)	2 10/100Base-T(X) fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto
Relay Output on M12 (A-coding) connector	Relay output to carry capacity of 3A at 24VDC
Redundant power inputs on M23 connector	Dual Power Inputs. 12~48 VDC on M23 connector (24 VDC Typ)

TAR-120-M12 / TAR-3120-M12





1. 2.4/5.8GHz antenna with typical 3.0 dBi antenna for IEEE 802.11a mode and 2 dBi for IEEE 802.11b/g mode
2. LED for PWR1 and system status. When PWR1 links, the green LED will light On.
3. LED for PWR2 and system status. When PWR2 links, the green LED will light On.
4. LED for Ethernet port1 status.
5. LED for Ethernet port2 status.
6. LED for WLAN link status.
7. LED for internal HSUPA modem connection
8. LED for Fault Relay. When the fault occurs, the red LED will light On.
9. Power Input port on M23 connector
10. 2.4/5.8GHz antenna for WLAN2 of TAR-3120-M12 (TAR-3120-M12 only)
11. Ethernet port1 on M12(D-coding) connector
12. Ethernet port2 on M12(D-coding) connector
13. Relay output on M12(A-coding) connector
14. 850/900/1800/2100MHz antenna for internal HSUPA modem
15. HSUPA Cellular Modem with SIM card slot

3.2 Front Panel LEDs

LED	Color	Status	Description
PWR1	Green/Red	Green On	DC power 1 activated.
		Green blinking	Device been located
		Red blinking	Indicates an IP conflict, or DHCP or BOOTP server did not respond properly
PWR2	Green/Red	Green On	DC power 2 activated.
		Green blinking	Device been located
		Red blinking	Indicates an IP conflict, or DHCP or BOOTP server did not respond properly
ETH1	Amber	On	Port link up at 10Mbps.
		Blinking	Data transmitted.
	Green	On	Port link up at 100Mbps.
		Blinking	Data transmitted.
ETH2	Amber	On	Port link up at 10Mbps.
		Blinking	Data transmitted.
	Green	On	Port link up at 100Mbps.

		Blinking	Data transmitted.
WLAN	Green	On	WLAN1 activated.
		Blinking	WLAN1 Data transmitted.
	Red(TAR-3120-M12 only)	On	WLAN2 activated.
		Blinking	WLAN2 Data transmitted.
WAN	Green	On	Modem Ready
		Blinking	Checking Modem status
Fault	Red	On	Fault relay. Power failure or Port down/fail.

Cables and Antenna

4.1 Ethernet Cables

The TAR-120-M12 / TAR-3120-M12 WLAN AP router has two 10/100Base-T(X) Ethernet ports. According to the link type, the AP use CAT 3, 4, 5,5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	M12(D-coding)
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	M12(D-coding)

4.2 100BASE-TX/10BASE-T Pin Assignments

With 100Base-T(X)/10Base-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

M12(4-pin, D-coding) Pin Assignments

Pin Number	Assignment
1	RD+
2	TD+
3	RD-
4	TD-

The TAR-120-M12 / TAR-3120-M12 supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC and AP. The following table below shows the 10Base-T/ 100Base-T(X) MDI and MDI-X port pin outs.

MDI/MDI-X pins assignment

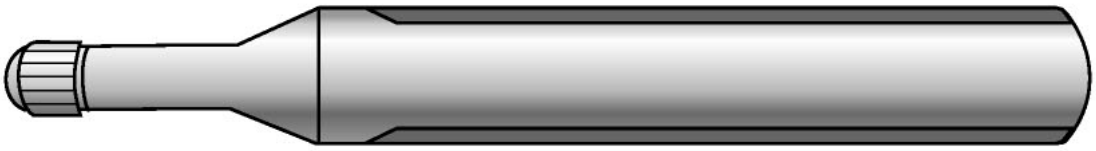
Pin Number	MDI port	MDI-X port
1	RD+(receive)	TD+(transmit)
2	TD+(transmit)	RD+(receive)
3	RD-(receive)	TD-(transmit)
4	TD-(transmit)	RD-(receive)

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.3 Wireless Antenna

2.4GHz/5.8GHz antenna is used for the WLAN interface of TAR120-M12 / TAR-3120-M12 and connected with a reversed SMA connector. 850/900/1800/2100MHz antenna is used for built-in HSUPA modem. External RF cable and antenna also can be applied with this connector.

Cellular Antenna



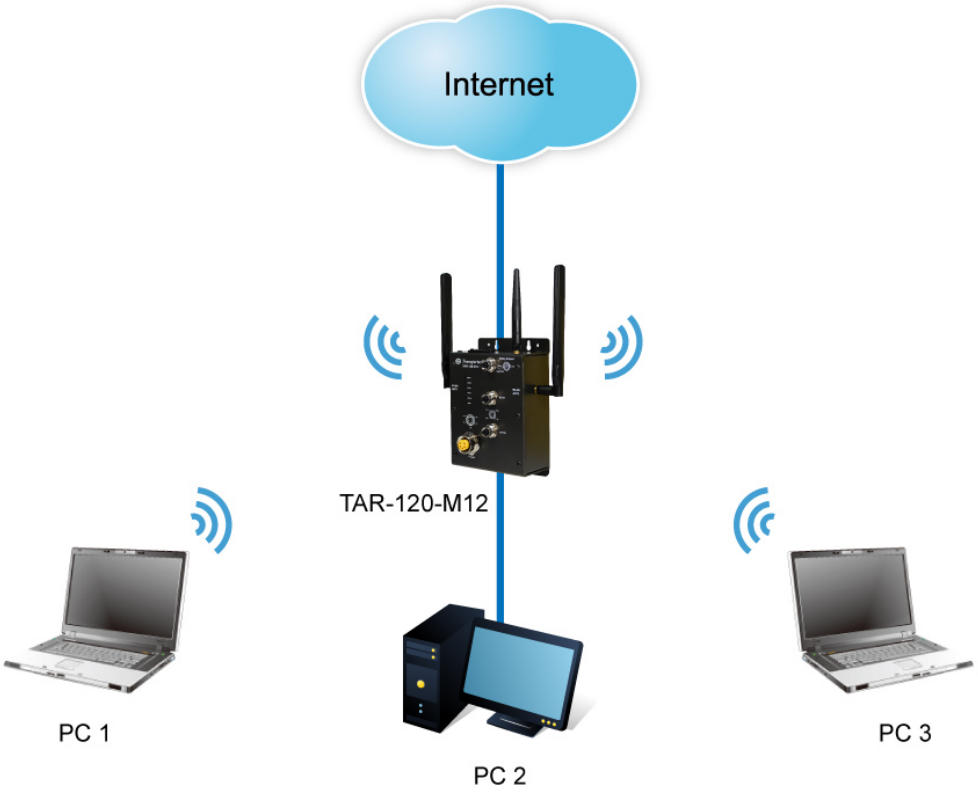
WLAN Antenna

WLAN Antenna

Management Interface

5.1 First-time Installation

Before installing the TAR-120-M12 / TAR-3120-M12 WLAN AP router, you need to access WLAN AP router with a computer via wired LAN connection or wireless LAN interface. Using wired LAN connection is much easier and is highly recommended.



Basic connection for TAR-120-M12 / TAR-3120-M12

Step 1: Select the Power Source

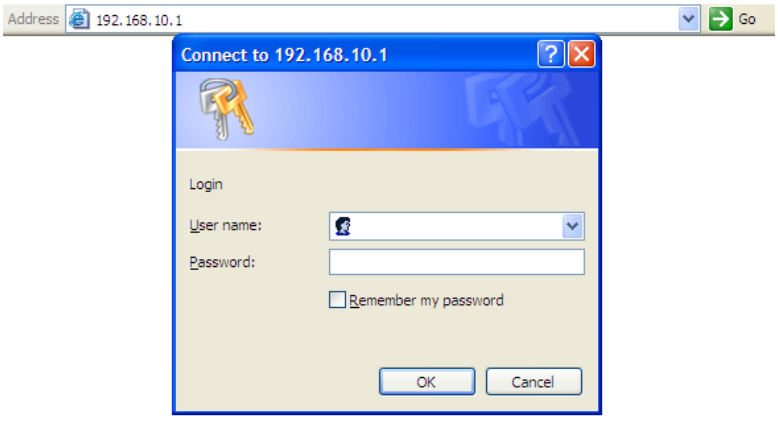
TAR-120-M12 / TAR-3120-M12 AP router can be powered by +12~48V DC power input.

Step 2: Connect a computer to TAR-120-M12 / TAR-3120-M12

Use an appropriate Ethernet cable (e.g. RJ-45 to M12) to connect the ETH2 port of TAR-120-M12 / TAR-3120-M12 AP router to the LAN port of a computer. If the LED of the LAN port lights up, it indicates that the connection is established. After that, the computer will initiate a DHCP request to get an IP address from the AP router.

Step 3: Use the web-based manager to configure TAR-120-M12 / TAR-3120-M12

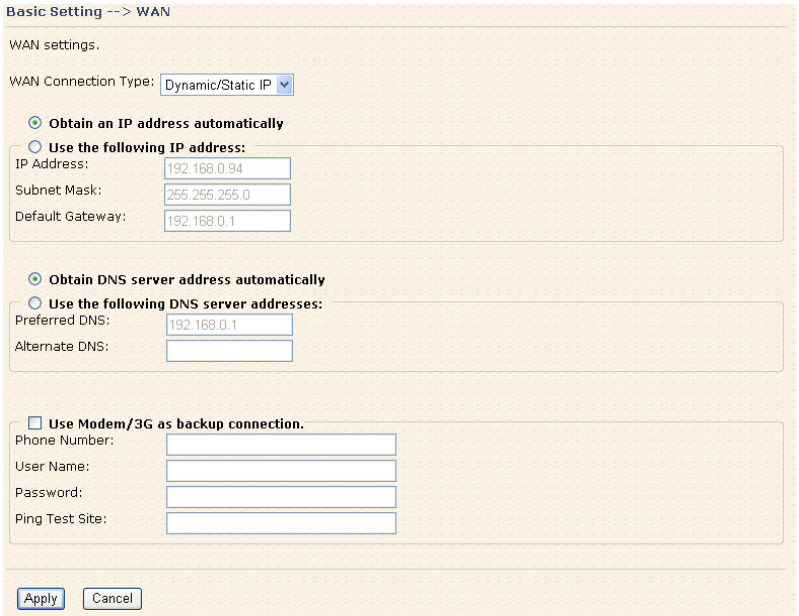
The default gateway IP of TAR-120-M12 / TAR-3120-M12 AP router is 192.168.10.1. Start the web browser of your computer and type http://192.168.10.1 in the address box to access the webpage. A login window will popup, and then enter the default login name **admin** and password **admin.**



Login screen

Step 4: Select WAN connection type

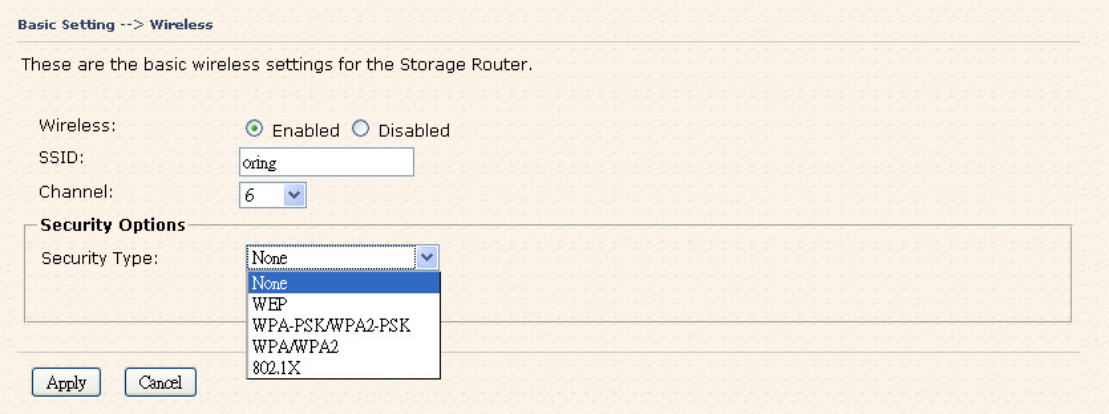
Click the **Basic Setting** in the top menu to enter the **WAN** configuration page. Select the proper connection type according to the information of your ISP.



WAN connection type

Step 5: Protect the wireless access in encryption mode

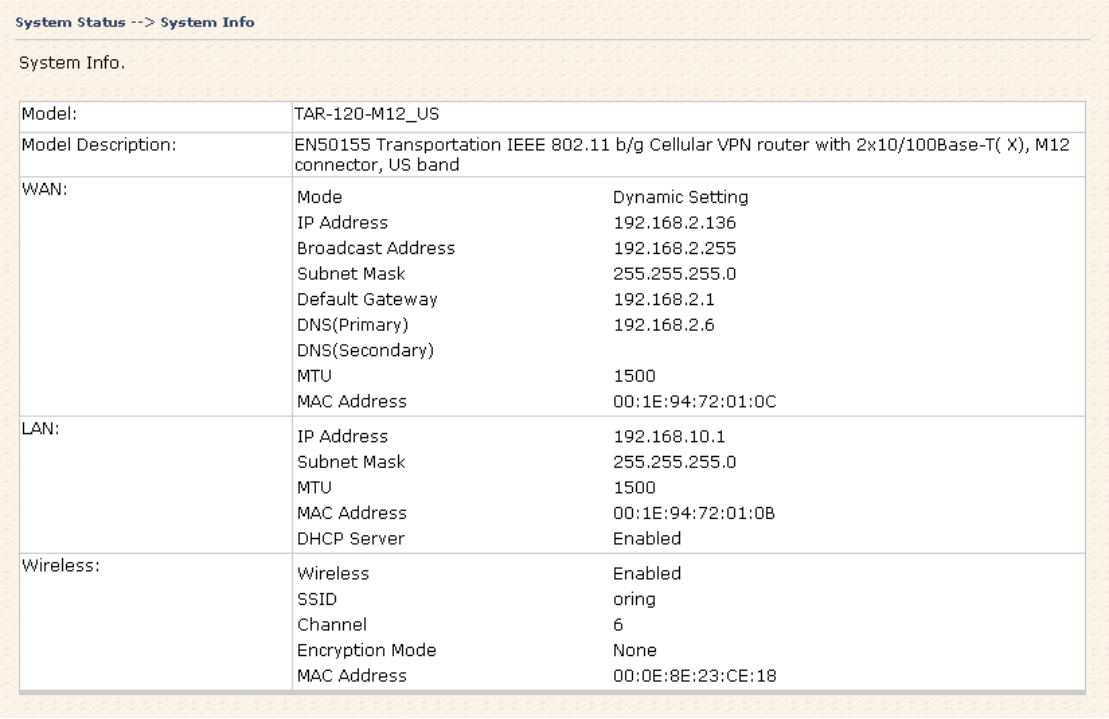
Click **Wireless** in **Basic Setting** menu. The default encryption mode is **None**. Choose WEP/WPA to enhance the security of wireless connection.



Wireless security option

Step 6: Review the router settings and check router status

Click the **System Status** in the top of the menu, the system info page will be shown. You can check all the configuration and status of the router.



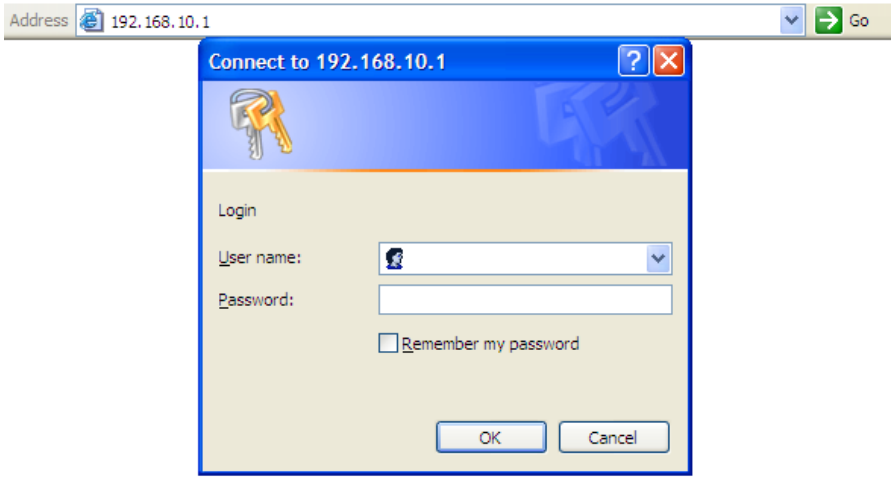
Model:	TAR-120-M12_US	
Model Description:	EN50155 Transportation IEEE 802.11 b/g Cellular VPN router with 2x10/100Base-T(X), M12 connector, US band	
WAN:	Mode	Dynamic Setting
	IP Address	192.168.2.136
	Broadcast Address	192.168.2.255
	Subnet Mask	255.255.255.0
	Default Gateway	192.168.2.1
	DNS(Primary)	192.168.2.6
	DNS(Secondary)	
	MTU	1500
	MAC Address	00:1E:94:72:01:0C
LAN:	IP Address	192.168.10.1
	Subnet Mask	255.255.255.0
	MTU	1500
	MAC Address	00:1E:94:72:01:0B
	DHCP Server	Enabled
Wireless:	Wireless	Enabled
	SSID	oring
	Channel	6
	Encryption Mode	None
	MAC Address	00:0E:8E:23:CE:18

System status Screen

5.2 Configure the Wireless Router

In this section, the web management page will be explained in detail.

With default setting, you can type http://192.168.10.1 in the address box of web browser to login the web management interface. A login window will be prompted, enter username **admin** & password **admin** to login.

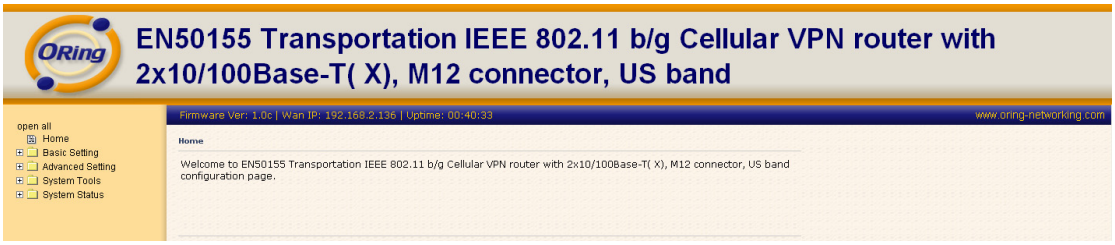


Login screen

For security reasons, we strongly recommend you to change the password. Click on **System Tools > Login Setting** and change the password.

5.3 Main Interface

The **Home** screen will be shown when login successfully.



Main Interface

In the page, you can check the Firmware version, the router running time and the WAN IP setting.

The following table describes the labels in this screen.

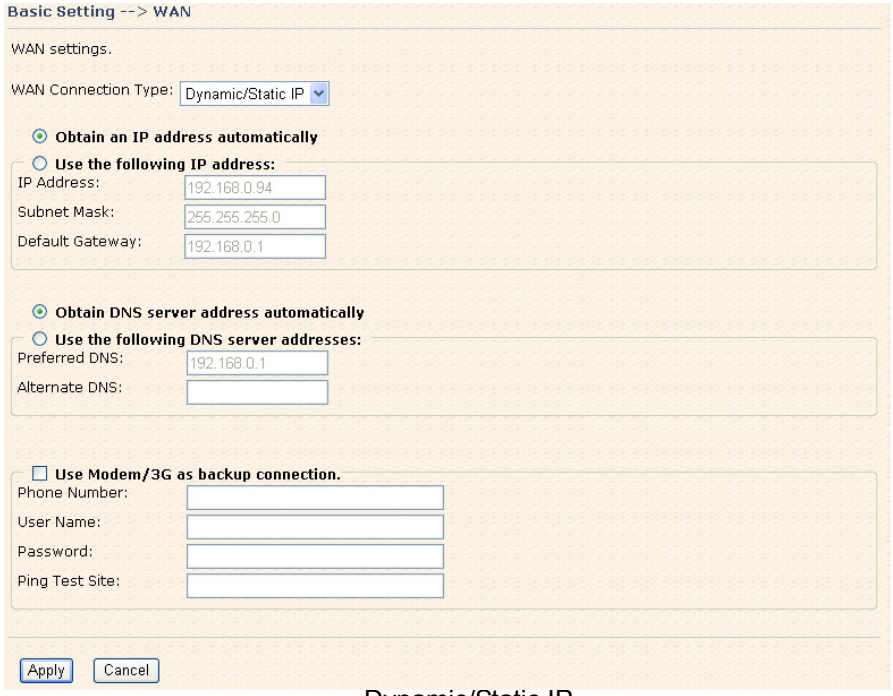
Label	Description
Firmware	Show the current firmware version.
Uptime	Show the elapsed time since the AP router is started.
Wan IP	Show the WAN IP address.

5.3.1 Basic Setting

WAN

The TAR-120-M12 / TAR-3120-M12 AP router provides three types of WAN connection.

1. WAN Connection Type: Dynamic/Static IP



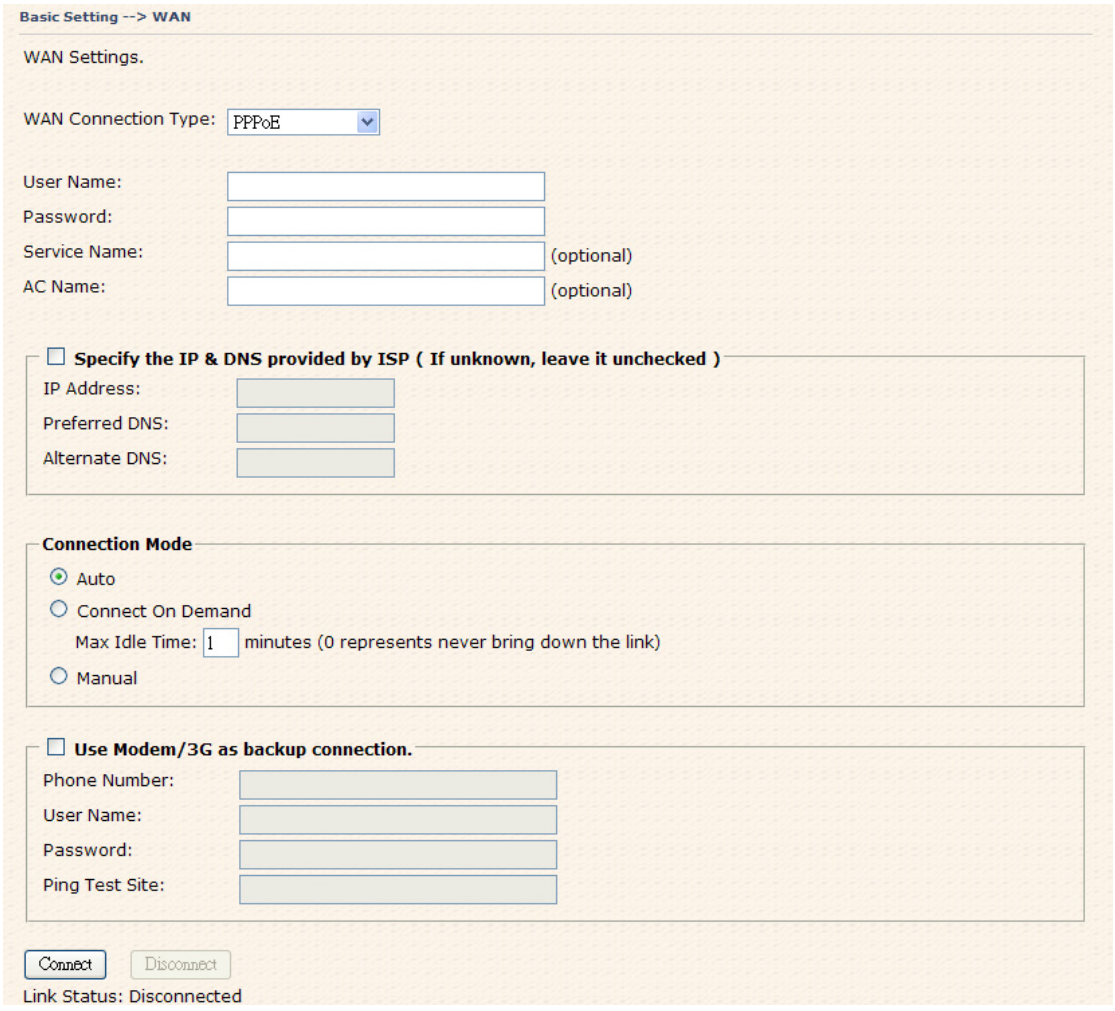
Dynamic/Static IP

The following table describes the labels in this screen.

Label	Description
Obtain an IP address automatically	Select this option if you would like to have an IP address assigned automatically from the WAN port by DHCP server in your network.
Use the following IP address	Select this option if you would like to assign an IP address to the WAN port manually. You should set the IP Address, Subnet Mask and Default gateway appropriately so that they comply with IP rules.
Obtain DNS server address automatically	Obtain DNS server from DHCP server. If the above **Obtain an IP address automatically** is selected, this option will be chosen accordingly.
Use the following DNS server addresses	Specify DNS server address manually.

Use Modem/3G as backup connection	Enable this option if you want to use built-in HSUPA modem as backup connection when normal connection is lost. **Phone Number, User Name and Password:** Use these settings to dial up the built-in HSUPA modem connection. **Ping Test Site:** Use this site address to check if the connection is alive or lost. Take **www.google.com** as an example.

2. WAN Connection Type: PPPoE



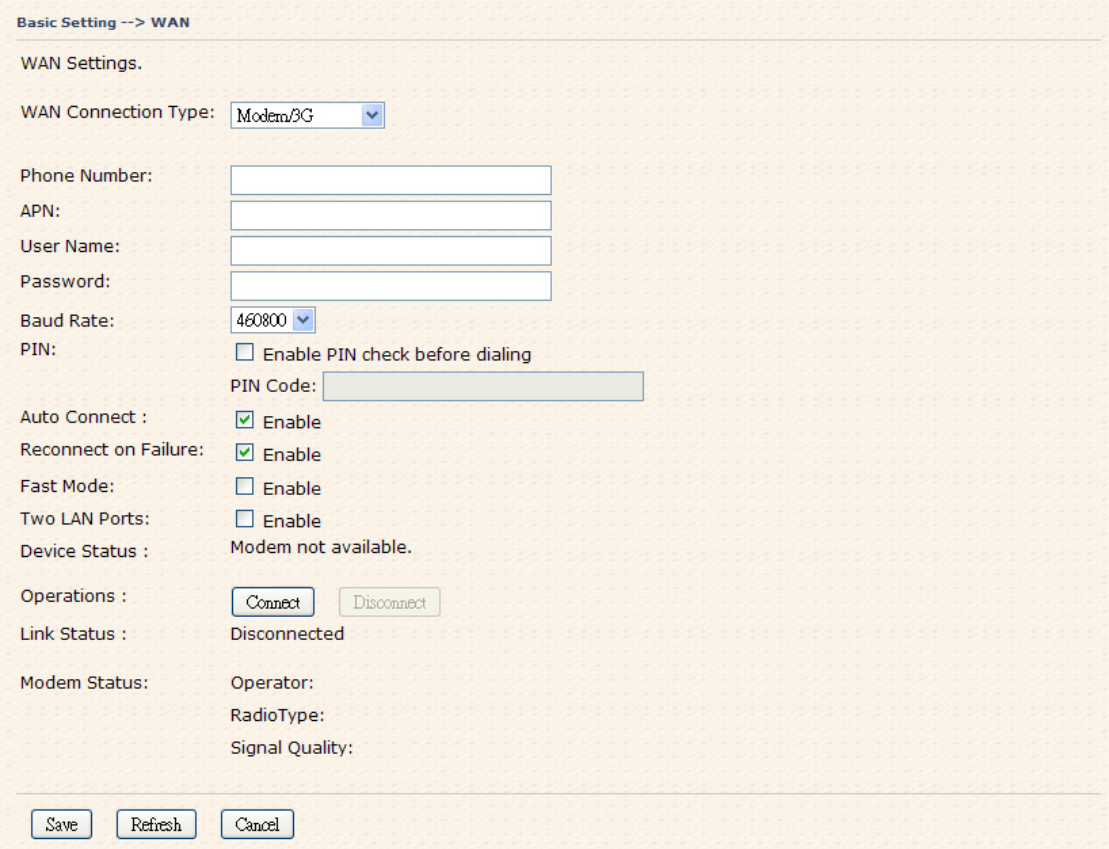
PPPoE Screen

The following table describes the labels in this screen.

Label	Description
User Name / Password	Enter the username & password provided by your Internet Service Provider (ISP).
Service Name	Enter the service name provided by your ISP.
AC Name	Enter the name of the access concentrator as provided by your ISP.
Specify the IP & DNS provided by ISP	Enter static IP and DNS address which may required by some ISP
Connection Mode	**Auto:** Connect automatically when the router boots up. **Connect on Demand:** Select to disconnect the PPP session if the router has had no traffic for the specified amount of time. Enter the Max Idle Time in minutes. **Manual:** Select this option to use only the Connect/Disconnect buttons to call up or close the connection.
Use Modem/3G as backup connection	Enable this option if you want to use built-in HSUPA modem as a backup connection when PPPoE connection is lost. **Phone Number, User Name and Password:** Use these settings to dial up the built-in HSUPA modem connection. **Ping Test Site:** Use this site address to check if the connection is alive or lost. Example is as **www.google.com**

3. WAN Connection Type: Modem / 3G

For using this type of connection, use the built-in HSUPA modem.

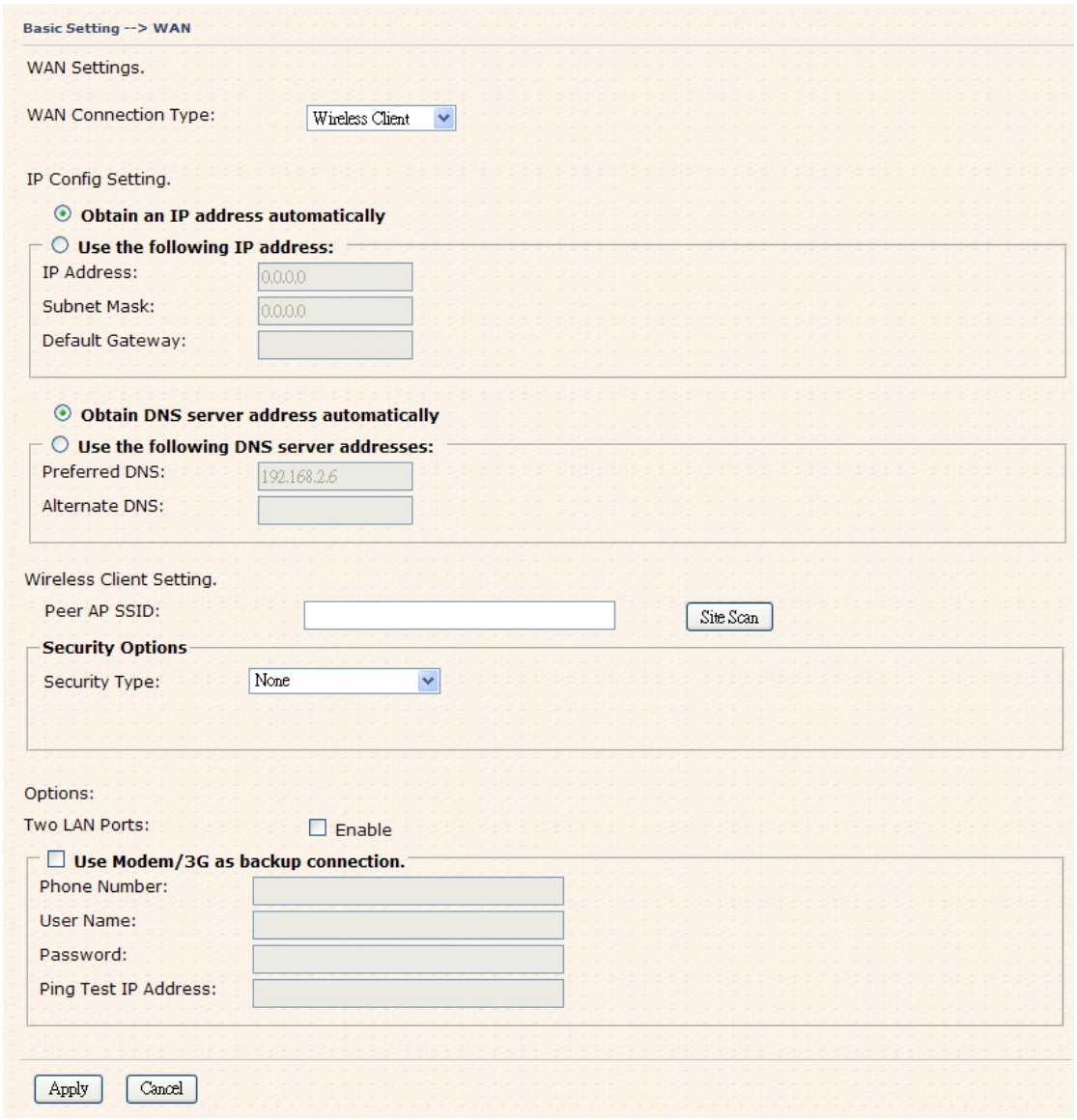


Modem/3G Screen

The following table describes the labels in this screen.

Label	Description
Phone Number	Telephone number provided by your ISP.
APN	Enter the APN value it is optional
User Name	User name provided by your ISP.
Password	Password provided by your ISP.
PIN	Enter the PIN code if PIN check is required.
Auto Connect	If this option is enabled, the connection will be called up when router boots up.
Device Status	Show the status of built-in HSUPA modem device.
Operations	Click "**Connect**" to call up the built-in HSUPA modem. Click "**Disconnect**" to shut down the connection.
Link Status	Show the status of connection, **up**, **down** or **connecting**.

4. WAN Connection Type: Wireless client



Wireless Client on WAN

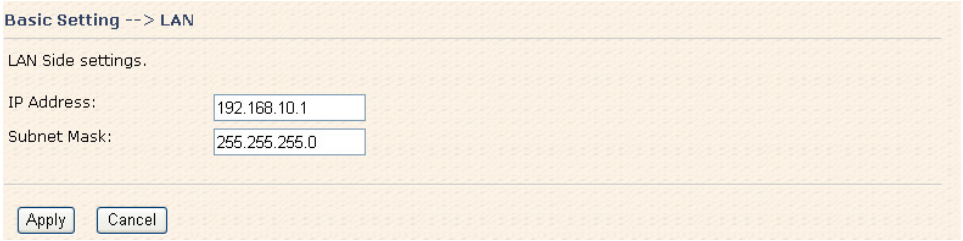
The following table describes the labels in this screen.

Label	Description
Obtain an IP address automatically	Select this option if you would like to have an IP address assigned automatically from the WAN port by DHCP server in your network.
Use the following IP address	Select this option if you would like to assign an IP address to the WAN port manually. You should set the IP Address, Subnet Mask and Default gateway appropriately so that they comply with IP rules.

Obtain DNS server address automatically	Obtain DNS server from DHCP server. If the above **Obtain an IP address automatically** is selected, this option will be chosen accordingly.
Use the following DNS server addresses	Specify DNS server address manually.
Peer AP SSID	Enter the other AP or AR SSID which you want to client.
Site Scan	You can scan the SSIDs which used for AP mode in the certainty area.
Security Type	Set the same security with the Client unit which you want to connect.
Use Modem/3G as backup connection	Enable this option if you want to use built-in HSUPA modem as a backup connection when normal connection is lost. **Phone Number, User Name and Password:** Use these settings to dial up the built-in HSUPA modem connection. **Ping Test Site:** Use this site address to check if the connection is alive or lost. Take **www.google.com** as an example.

LAN

These are the IP settings of the LAN interface for the TAR-120-M12 / TAR-3120-M12 WLAN AP router. The LAN IP address is privately for your internal network and can not be exposed on the Internet.



LAN Screen

The following table describes the labels in this screen.

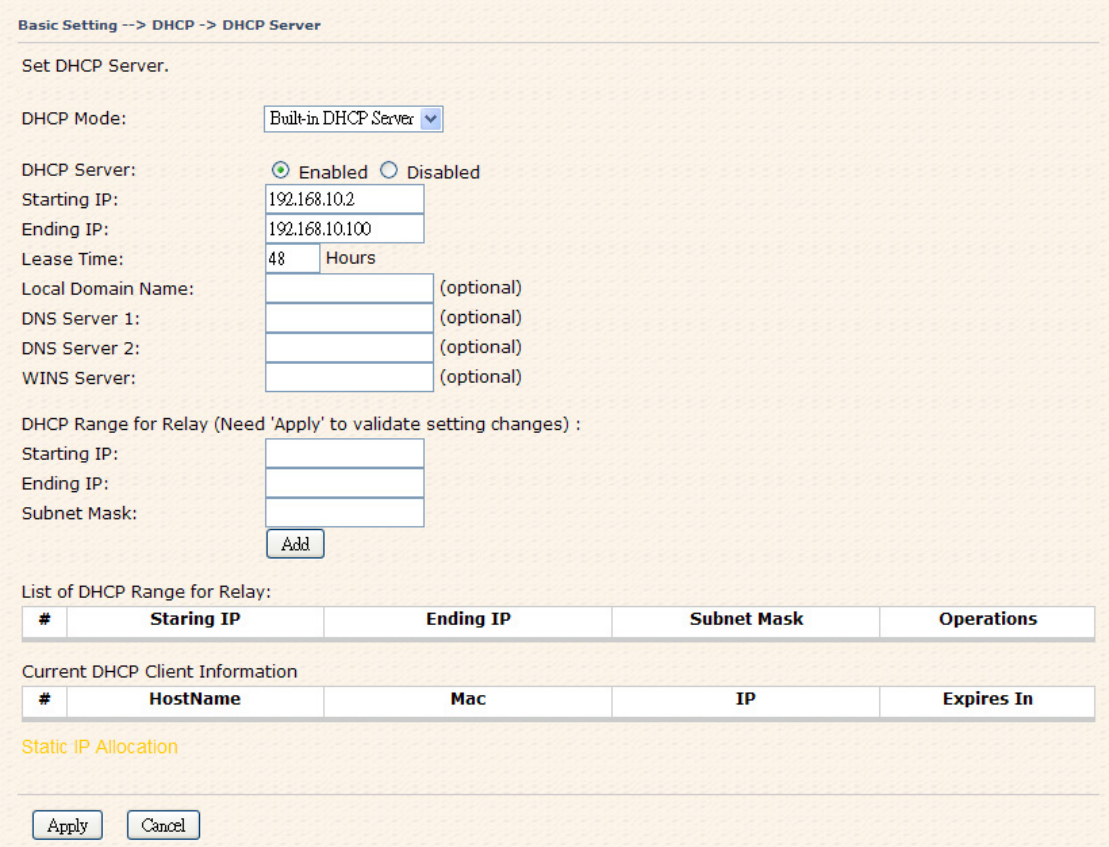
Label	Description
IP Address	The IP address of the LAN interface, the default IP address is 192.168.10.1
Subnet Mask	The Subnet Mask of the LAN interface, the default Subnet mask is 255.255.255.0

DHCP

DHCP stands for Dynamic Host Control Protocol. The TAR-120-M12 / TAR-3120-M12 AP router was built-in DHCP server. The internal DHCP server will assign an IP address to the computers (DHCP client) on the LAN automatically.

Set your computers to be DHCP clients by setting their TCP/IP settings to obtain an IP address automatically. The DHCP server will allocate an unused IP address from the IP address pool to the requesting computer automatically.

1. DHCP Sever



DHCP Server Screen

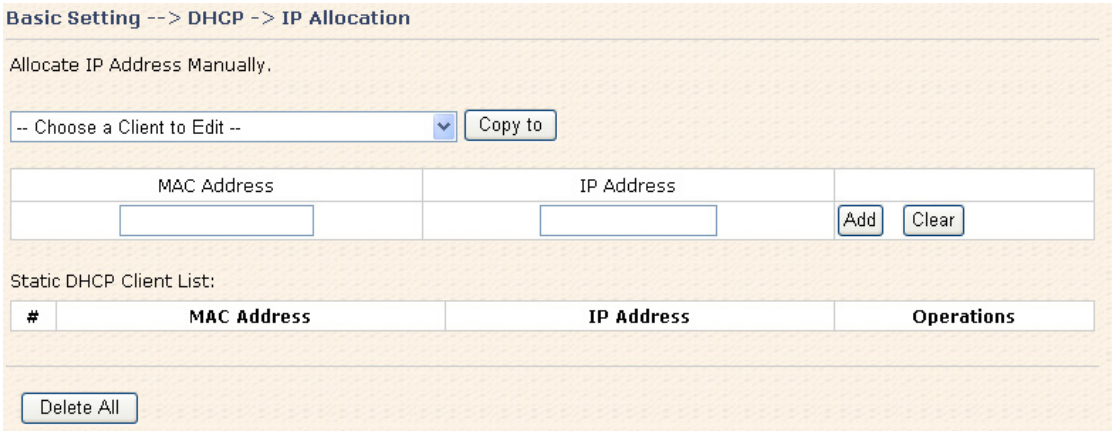
The following table describes the labels in this screen.

Label	Description
DHCP Mode	Select built-in DHCP server or DHCP Forwarder
DHCP Server	Enable or Disable the DHCP Server. The default setting is *Enabled*.
Starting IP	The starting IP address of the IP range for the DHCP server
Ending IP	The ending IP address of the IP range for the DHCP server

Lease Time	The period of time for the IP to be leased. Enter the Lease time. The default setting is 48 hours.
Local Domain Name	Enter the local domain name of private network. It is optional.
DNS Server 1&2	Enter the DNS Server. It is optional.
WINS Server	Enter the WINS Server. It is optional.
DHCP Relay start IP	Enter DHCP Relay starting IP
DHCP Relay end IP	Enter DHCP Relay Ending IP
Subnet Mask	Enter DHCP Relay IP Subnet mask
List of DHCP Range for relay	List DHCP Relay IP range
Current DHCP Client Information	List of the computers on your network that are assigned an IP address by internal DHCP server.

2. IP Allocation

The IP Allocation provides one-to-one mapping of MAC address to IP address. When a computer with the MAC address requests an IP address from the TAR-120-M12 / TAR-3120-M12 AP router, it will be assigned with the IP address according to the mapping. You can choose one from the client lists and add it to the mapping relationship.



IP Allocation Screen

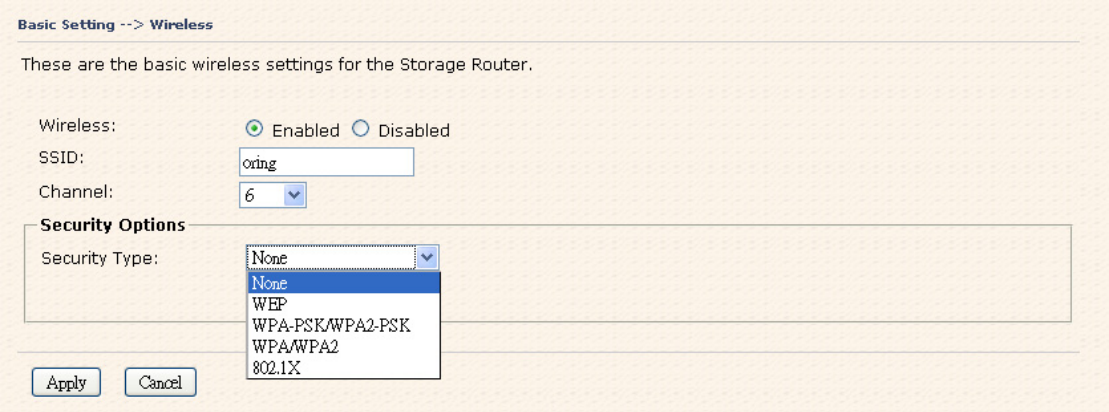
The following table describes the labels in this screen.

Label	Description
Choose a Client to Edit	The list shows the MAC addresses and IP addresses that are already assigned by TAR-120-M12 / TAR-3120-M12. Choose one from the list and click **Copy to** button for editing.
MAC Address	The MAC addresses of the computer.

IP Address	The IP address to be related to the MAC address.
Static DHCP Client List	The list shows the MAC address and IP address one-to-one relationship.

Wireless (WLAN 1 and WLAN 2)

There are two wireless interfaces for TAR-3120-M12: WLAN 1 (5 GHz band) and WLAN 2 (2.4 GHz band). Settings for both interfaces are the same and can be set separately.



Wireless Screen

The following table describes the labels in this screen.

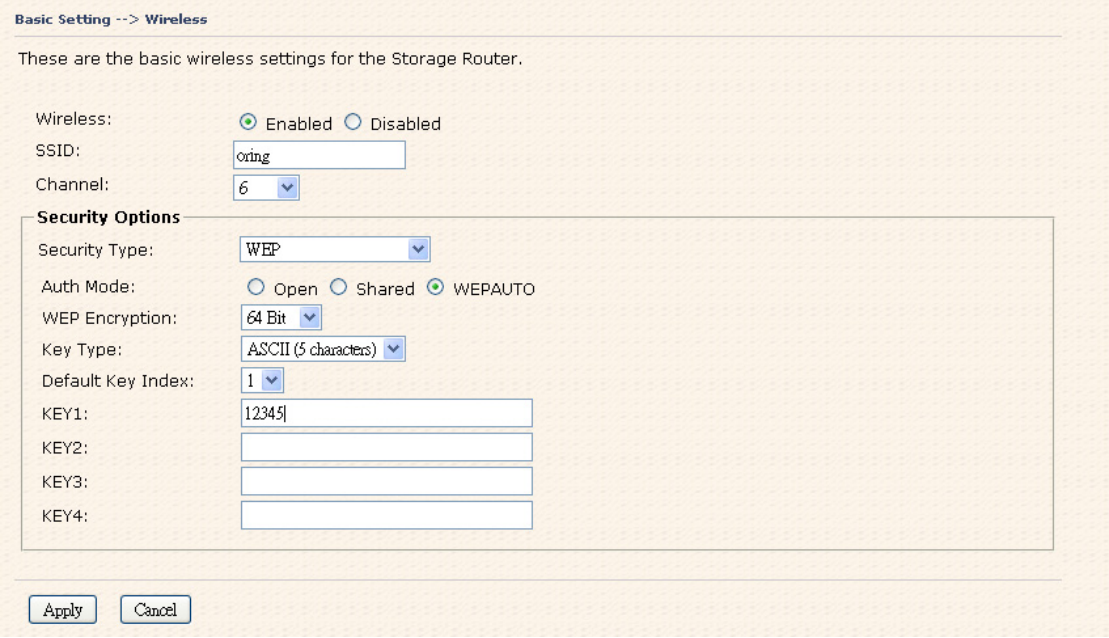
Label	Description
SSID	Service Set Identifier (SSID) is a unique name that identifies a network. All devices on the network must set the same SSID name in order to communicate on the network. If you change the SSID from the default setting, input your new SSID name in this field.
Channel	Channel 36 is the default channel for WLAN 1 and Channel 6 for WLAN 2. All devices on the network must share the same channel.* ***Note:** The wireless devices will automatically scan and match the wireless setting of the AP router with the same SSID.
Security options	Select the type of security for WLAN connection: **None:** disable encryption. **WEP:** Wired Equivalent Privacy (WEP) is a wireless security protocol for WLAN. WEP provides data encryption for communicating over the WLAN. **WPA-PSK/WPA2-PSK:** WPA-PSK or WPA2-PSK with a

	pre-shared key, each authorized computer is given the same pass phrase. **WPA/WPA2:** Wi-Fi Protected Access (WPA) authentication in conjunction with a RADIUS server. **802.1x:** Authentication through RADIUS server

Security Type – None

No security protection for WLAN.

Security Type – WEP

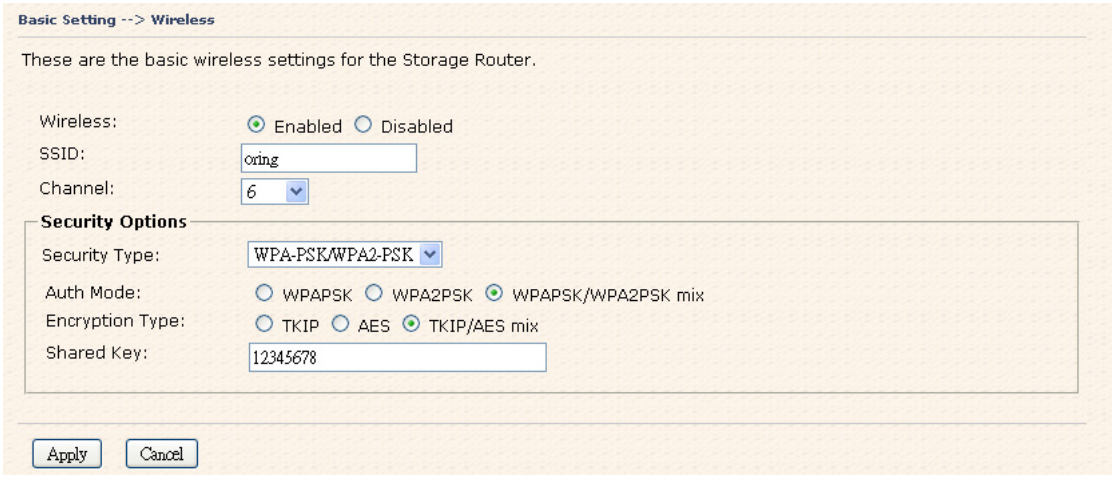


Wireless Security Type-WEP Screen

1. Choose one of three Auth Modes: **Open**, **Share** and **WEPAUTO**
2. WEP Encryption: Select 64 Bit or 128 Bit WEP encryption.
3. Key Type: Select **ASCII** or **Hex** key type.
4. Default Key Index: Select one of the keys to be the active key.
5. Key 1-4: Input up to four encryption keys.

ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127. **Hex** digits consist of the numbers 0-9 and the letters A-F.

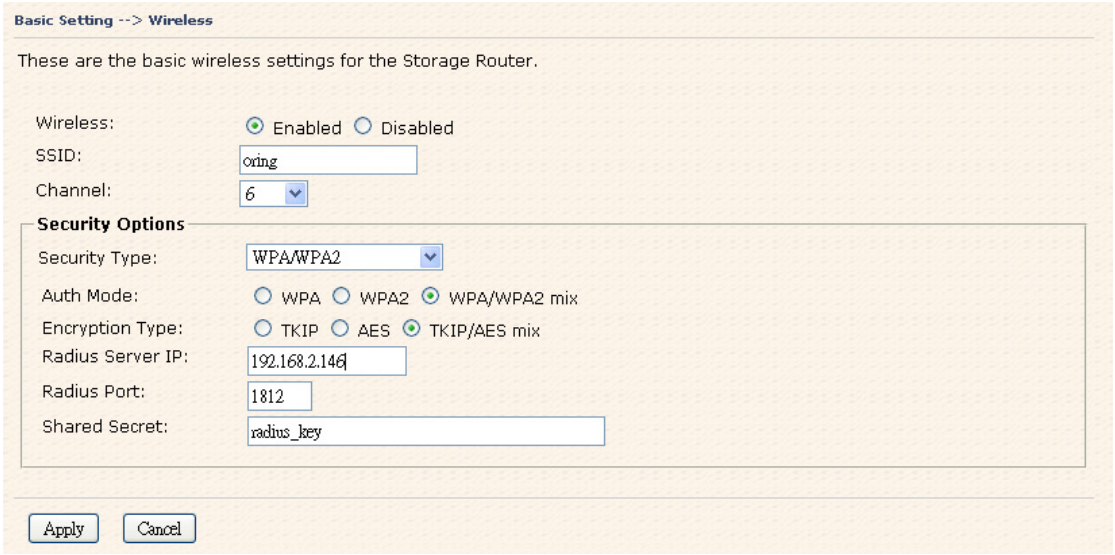
Security Type – WPA-PSK/WPA2-PSK



Wireless Security Type-WPA-PSK/WPA2-PSK Screen

1. Security Type: Select **WPA-PSK/WPA2-PSK**.
2. Choose one of three Auth Modes: **WPAPSK**, **WPA2PSK**, **WPAPSK/WPA2PSK mix**
3. Encryption Type: Select **TKIP** or **AES** or **TKIP/AES mix**.
4. Share Key: Enter your pass phase. The pass phase should be between 8 and 64 characters.

Security Type – WPA /WPA2

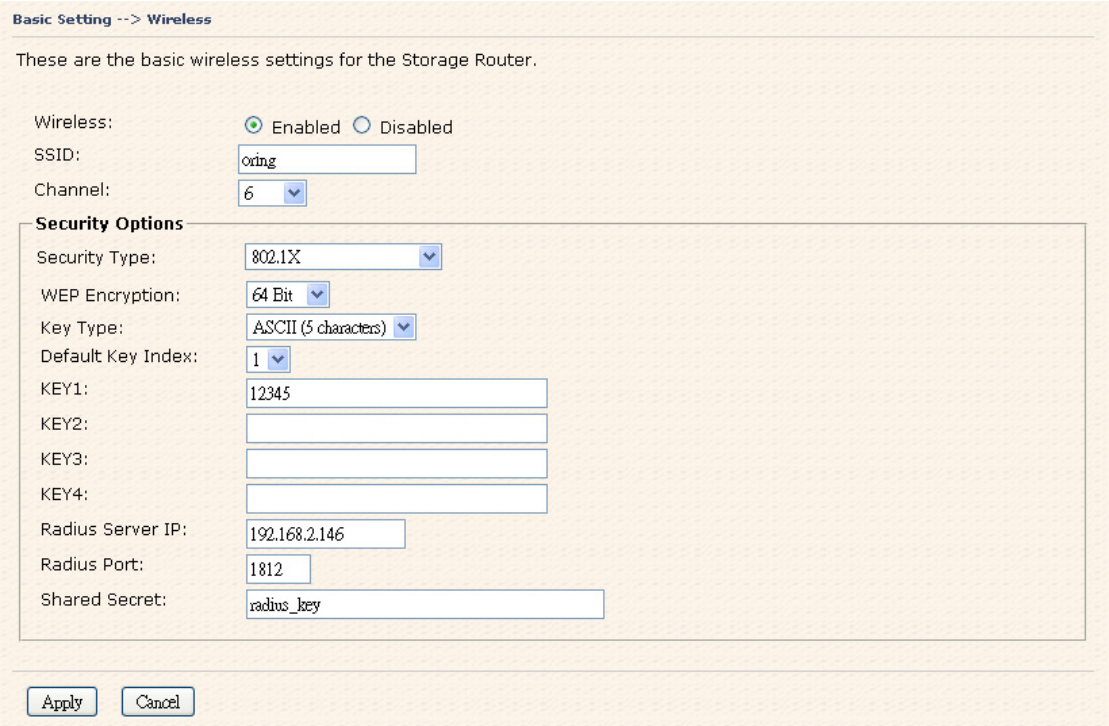


Wireless Security Type-WPA/WPA2 Screen

1. Security Type: Select **WPA/WPA2**

2. Auth Mode: Choose one of three Auth Modes: **WPA**, **WPA2**, **WPA/WPA2 mix**.
3. Encryption Type: Choose one of three Encryption Types: **TKIP**, **AES**, **TKIP/AES mix**.
4. Radius Server IP: Enter the IP address of the RADIUS Server.
5. Port: Enter the RADIUS port (1812 is default).
6. Shared Secret: Enter the RADIUS password or key.

Security Type – 802.1X



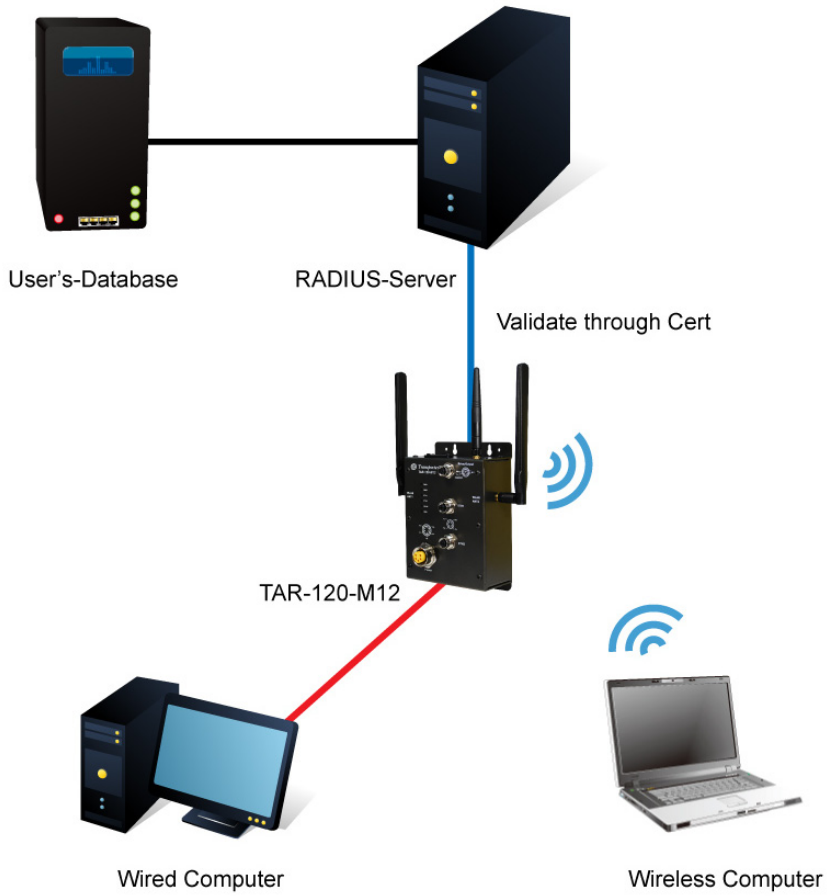
Wireless Security Type-802.1X Screen

1. Security Type: Select **802.1X**
2. WEP Encryption: Select 64 Bit or 128 Bit WEP encryption.
3. Key Type: Select ASCII or Hex key type.
4. Default Key Index: Select one of the keys to be the active key.
5. Key 1-4: Input up to four encryption keys.
6. Radius Server IP: Enter the IP address of the RADIUS Server.
7. Port: Enter the RADIUS port (1812 is default).
8. Shared Secret: Enter the RADIUS password or key.

RADIUS, or Remote Authentication Dial-In User Service, is a widely-deployed protocol that enables companies to authenticate, authorize and account for remote users who want access to a system or service from a central network server.

RADIUS server validates your proof and also carries on the authorization. So the RADIUS server received by ISA server responded (point out the customer carries proof to be not granted) and it means that the RADIUS server did not authorize you to carry. Even if the proof has already passed an identify verification, the ISA server may also refuse you to carry a claim according to the authorization strategy of the RADIUS server.

The principle of the RADIUS server is shown in the following pictures:

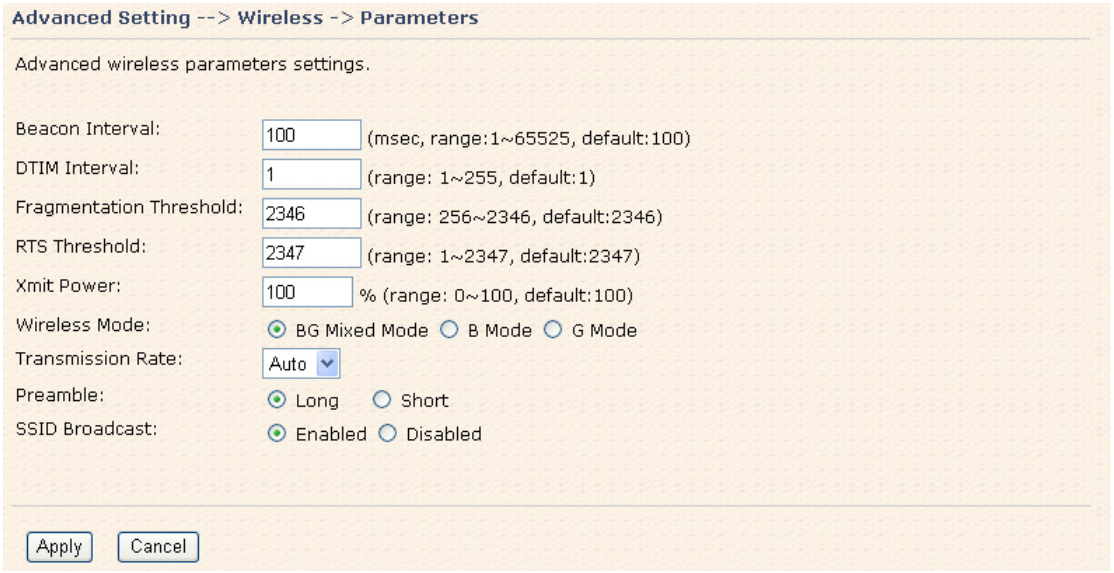


Connection to RADIUS server

5.3.2 Advanced Setting

Wireless (WLAN 1 and WLAN 2)

1. Parameters



Parameters Screen

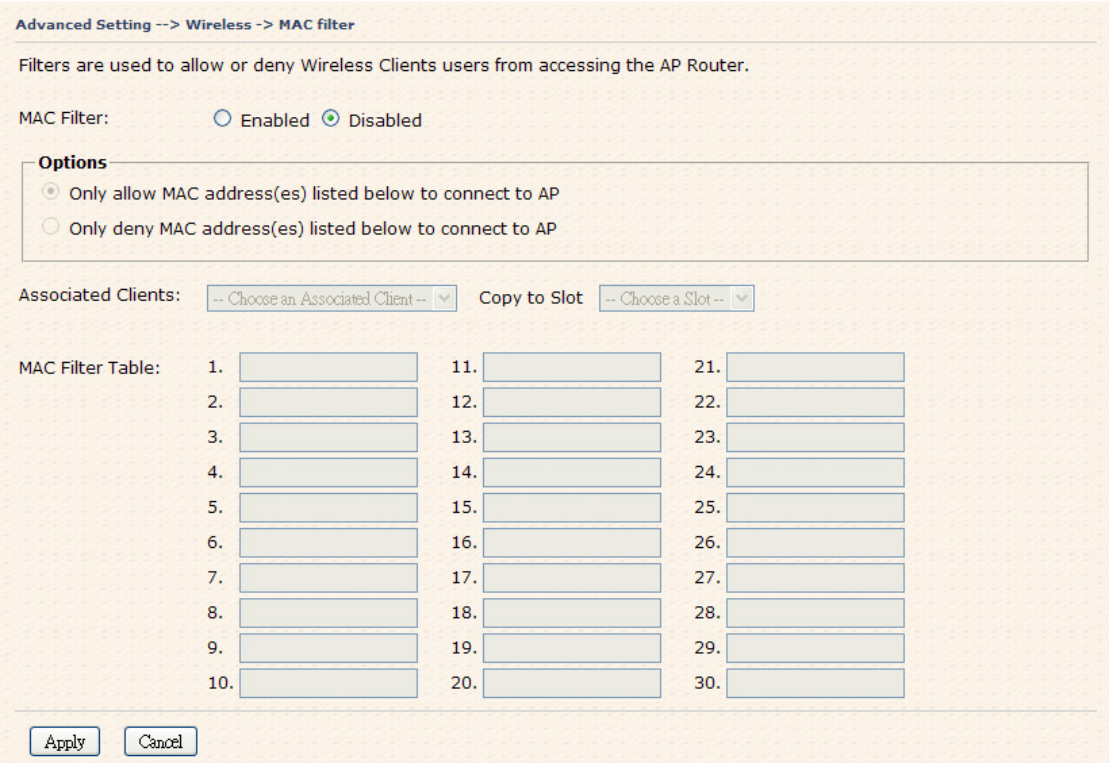
The following table describes the labels in this screen.

Label	Description
Beacon Interval	The default value is 100. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the AP to synchronize the wireless network. 50 is recommended in poor connection.
DTIM Interval	The default value is 1. This value, between 1 and 255 milliseconds, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
Fragmentation Threshold	This value should remain at its default setting of 2346. The range is 256-2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold

	too low may result in poor network performance. Only minor modifications of this value are recommended.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0-2347 bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The AP sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Xmit Power	This value ranges from 1 - 100 percent, default value is 100 percent.
Wireless Network Mode	If you have IEEE802.11g and IEEE802.11b devices in your network, then keep the default setting, **BG Mixed mode**. If you have only IEEE802.11g devices, select **G Mode**. If you would like to limit your network to only IEEE802.11b devices, then select **B Mode**.
Transmission Rate	The default setting is **Auto**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, **Auto**, to have the AP automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best and possible connection speed between the AP and a wireless client.
Preamble	Values are **Long** and **Short**, default value is **Long**. If your wireless device supports the short preamble and you are having trouble getting it to communicate with other IEEE802.11b devices, make sure that it is set to use the long preamble
SSID Broadcast	When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the AP. To broadcast the AP SSID, keep the default setting, **Enable**. If you do not want to broadcast the AP SSID, then select **Disable**.

2. MAC Filter

Use **MAC Filter** to allow or deny wireless clients to associate with TAR-120-M12 / TAR-3120-M12 AP router. You can manually add a MAC address or select the MAC address from **Associated Clients** that are currently associated with TAR-120-M12 / TAR-3120-M12.



MAC Filter Screen

The following table describes the labels in this screen.

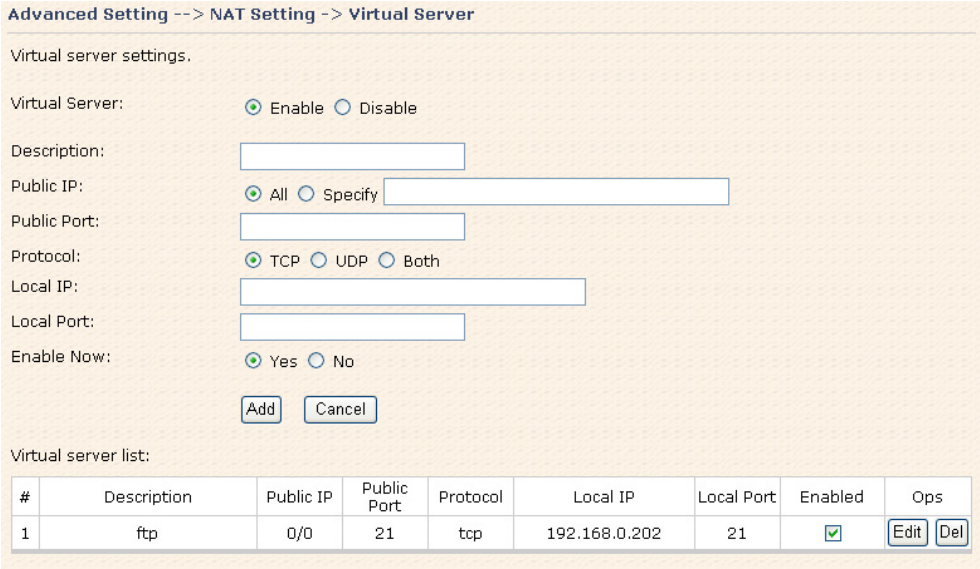
Label	Description
MAC Filter	Enable or disable the function of MAC filter.
MAC Filter List	This list shows the MAC addresses that are in the selected filter.
Connected Clients	This list shows the wireless MAC addresses that associated with AP.
MAC Address	MAC addresses for editing.
Apply	Click Apply to activate the configurations.

NAT Setting

1. Virtual Server

Virtual Server is used for setting up public services on the LAN, such as DNS, FTP and

Email. Virtual Server is defined as a Local Port to the LAN servers, and all requests from Internet to this Local port will be redirected to the computer specified by the Local IP. Any PC that was used for a virtual server must have static or reserved IP Address because its IP address may change when requesting IP by DHCP.



Virtual Server

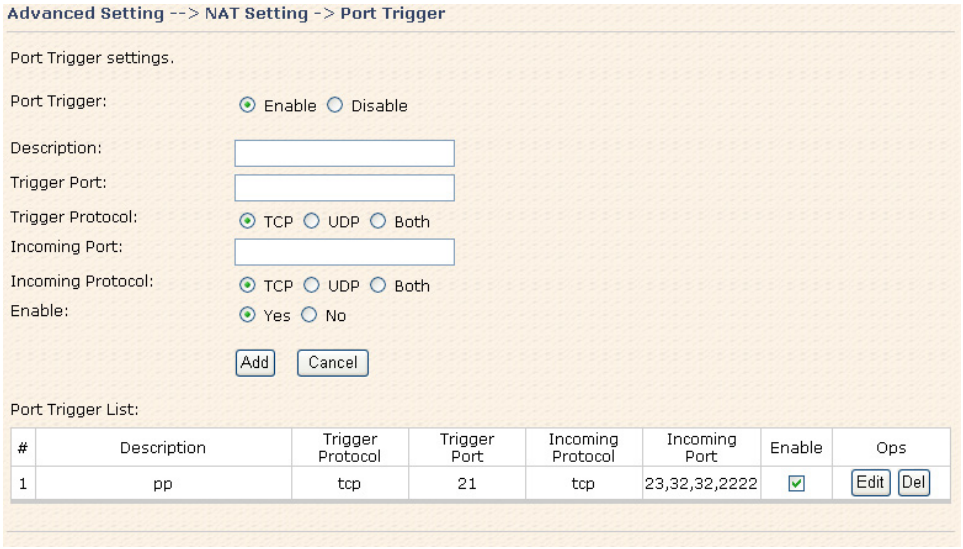
The following table describes the labels in this screen.

Label	Description
Virtual Server	Enable or disable Virtual Server.
Description	Enter the description of the entry. Acceptable characters consist of '**0-9**', '**a-z**', '**A-Z**'. This field accepts null value.
Public IP	Enter the public IP that is allowed to access the virtual service, if not specified, choose All.
Public Port	The port number on the WAN (Wide Area Network) side that will be used to access the virtual service.
Protocol	The protocol used for the virtual service.
Local IP	The IP of the computer that will be providing the virtual service.
Local Port	The port number of the service used by the Private IP computer.
Enable Now	Enable the virtual server entry after adding it.
Virtual server list	Click **Edit** to edit the virtual service entry, **Del** to delete the entry.

2 Port Trigger

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port

Trigger is used for some of the applications that can work with an NAT router.



Port Trigger Screen

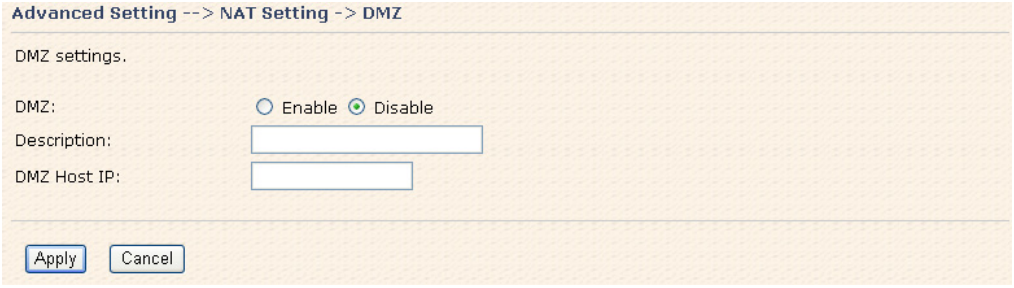
The following table describes the labels in this screen.

Label	Description
Port Trigger	Enable or disable Port Trigger.
Description	This is the description for the entry.
Trigger Port	This is the port used to trigger the application.
Trigger Protocol	This is the protocol used to trigger the application.
Incoming Port	This is the port number on the WAN side that will be used to access the application.
Enable	Enable the rule after adding the entry.
Port Trigger List	Click **Edit** to edit the entry, click **Del** to delete the entry.

3. DMZ

It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes.

Enter the IP address of the internal computer that will be the DMZ host. Adding a client to the DMZ may expose your local network with variety of security risks, so only use this option carefully.



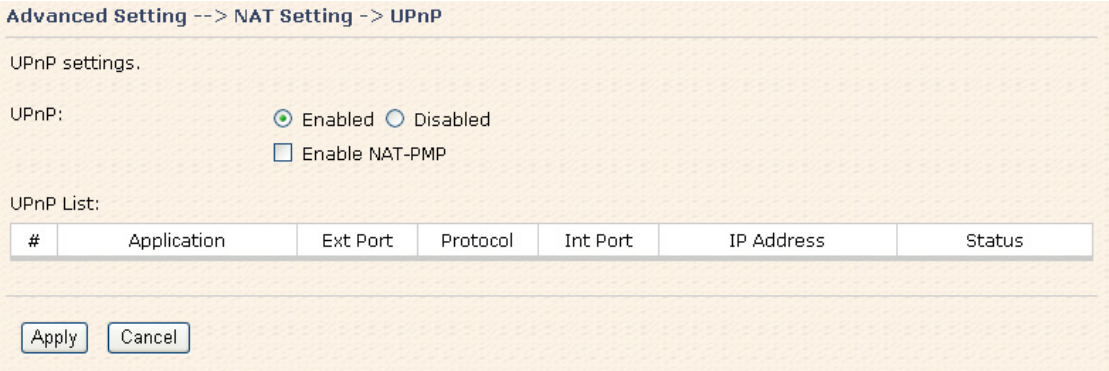
DMZ Screen

The following table describes the labels in this screen.

Label	Description
DMZ	Enable or disable the DMZ.
Description	Description for the DMZ host entry.
DMZ Host IP	Enter the IP address of the computer to be in the DMZ.

4. UPnP

The UPnP (Universal Plug and Play) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.



UPnP Screen

The following table describes the labels in this screen.

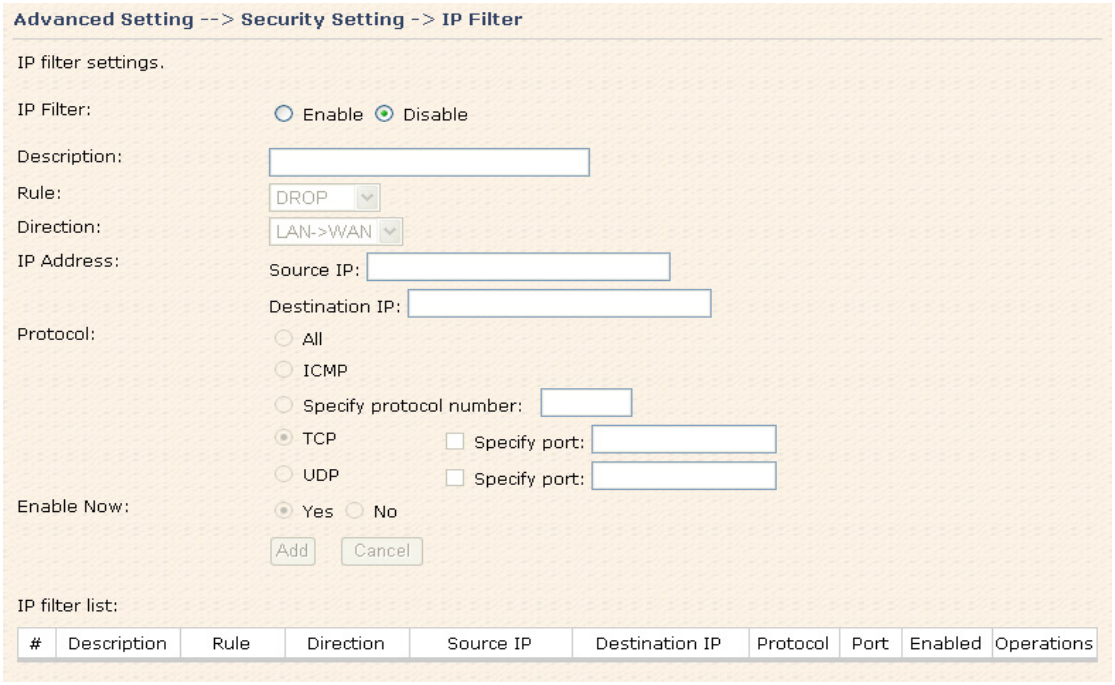
Label	Description
UPnP	Enable or disable UPnP.
Enable NAT-PMP	NAT-PMP allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact with each other. NAT-PMP operates with UDP. It essentially automates the process of port

	forwarding. Check the box to enable NAT-PMP.
UPnP List	This table lists the current auto port forwarding information. **Application:** The application that generates this port forwarding. **Ext Port:** The port opened on WAN side. **Protocol:** The protocol type. **Int Port:** The port redirected to the local computer. **IP Address:** The IP address of local computer to be redirected to. **Status:** This status shows if the entry is valid or not.

Security Setting

1. IP Filter

Filters are used to deny or allow LAN computers from accessing the internet. It also allows or denies WAN hosts to access LAN computers.



IP Filter Screen

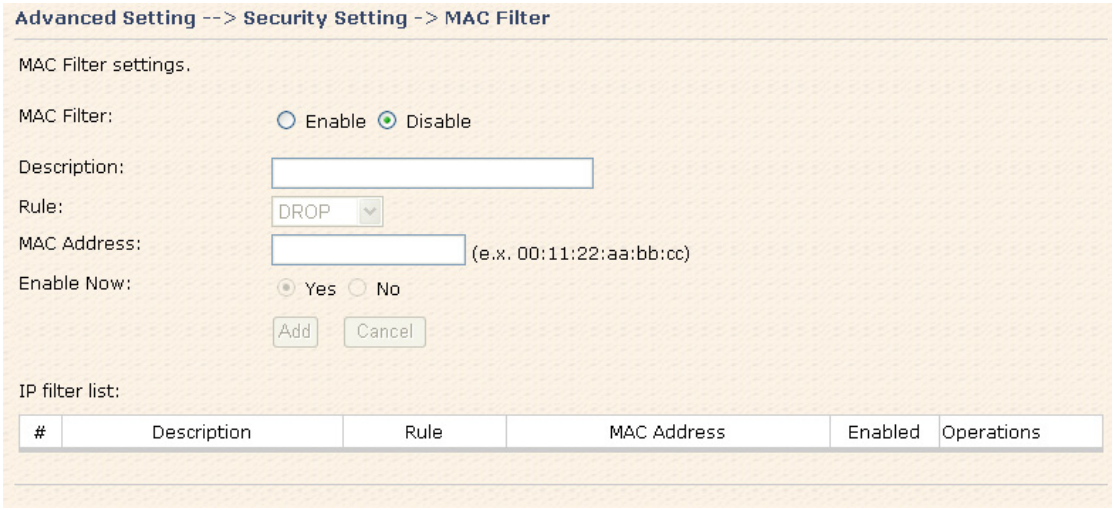
The following table describes the labels in this screen.

Label	Description
IP Filter	Enable or disable the IP Filter.
Description	Enter description for the entry.
Rule	Select **DROP**, **ACCEPT** and **REJECT** rule for the entry.
Direction	Specify the direction of the data flow that is to be filtered.

IP Address	Enter the IP address of the source and destination computer.
Protocol	Choose which protocol to be filtered.
Enable Now	Enable the entry after adding it.
IP filter list	Click **edit** for editing the entry, click **Del** to delete the entry.

2. MAC Filter

Filters are used to deny or allow LAN computers from accessing the internet, according to their MAC address.



MAC Filter Screen

The following table describes the labels in this screen.

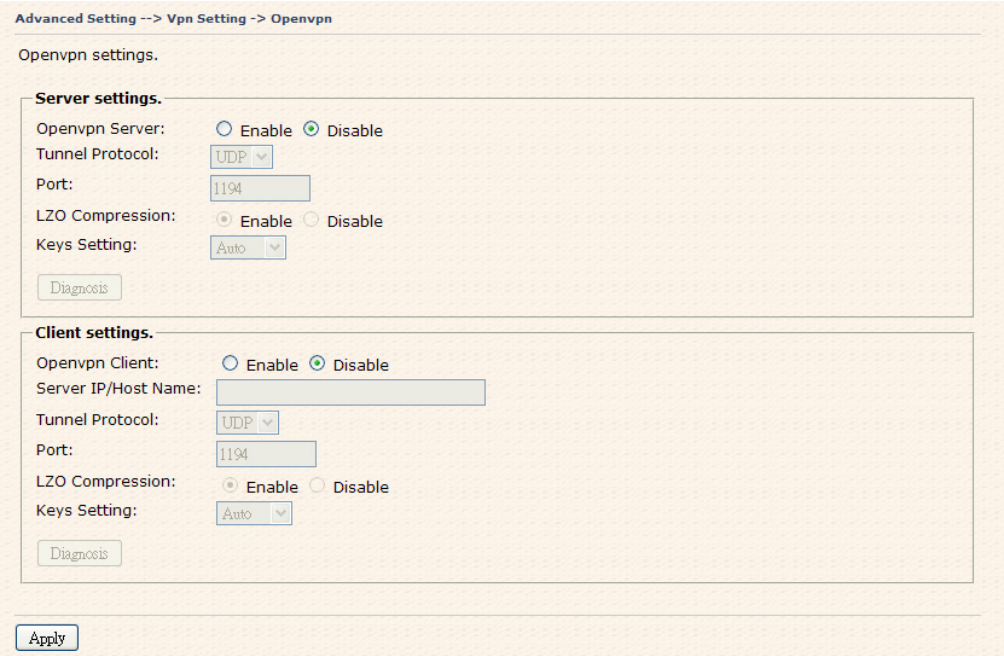
Label	Description
MAC Filter	Enable or disable the MAC Filter.
Description	Enter the description for the entry.
Rule	Select **DROP**, **ACCEPT** and **REJECT** rule for the entry.
MAC Address	Enter the MAC address to be filtered.
Enable Now	Enable the entry after adding it.
IP filter list	Click **Edit** for editing the entry, click **Del** to delete the entry.

VPN Setting

VPN Setting is settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin, authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

1. Open VPN

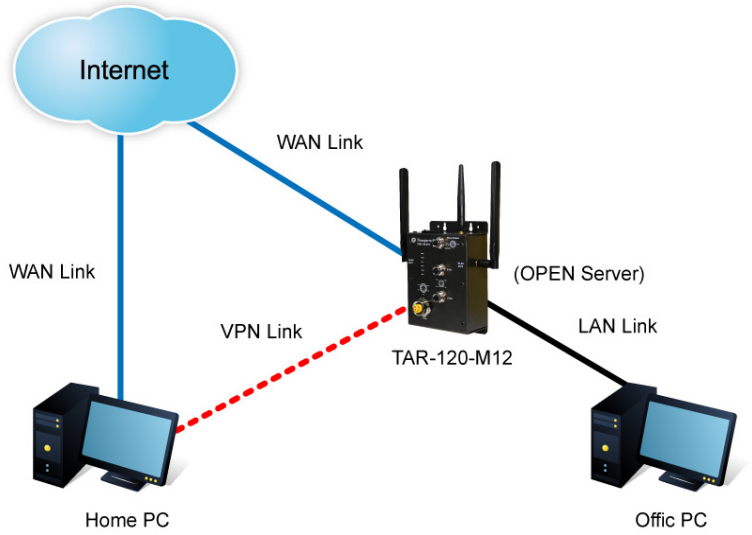
Open VPN is a full-functioned SSL VPN solution which can accommodates a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls.



Open VPN Screen

The following topology shows the common use of VPN connection from WAN side.

1: Open VPN Server



Connection to Open VPN Server

Before connecting to the Openvpn server of TAR-120-M12 / TAR-3120-M12 AP router, please install Openvpn client software for your windows PC. It can be downloading from http://Openvpn.net/download.html#stablel. The current version of Openvpn used in TAR-120-M12 / TAR-3120-M12 is version 2.0.9. The corresponding software for client should be installed.

The following table describes the labels in this screen.

Label	Description
Open VPN Server	Enable or disable the function of Open VPN Server.
Tunnel Protocol	Select UDP or TCP protocol.
Port	Input the number about the port, and the default is 1194.
LZO Compression	Enable or disable the function of LZO Compression.
Keys Setting	Select Auto to use the preset certificates, select Manual to paste your certificates. Please install Openvpn client software to generate your certificates and paste them here. For more information, please visit Openvpn website.

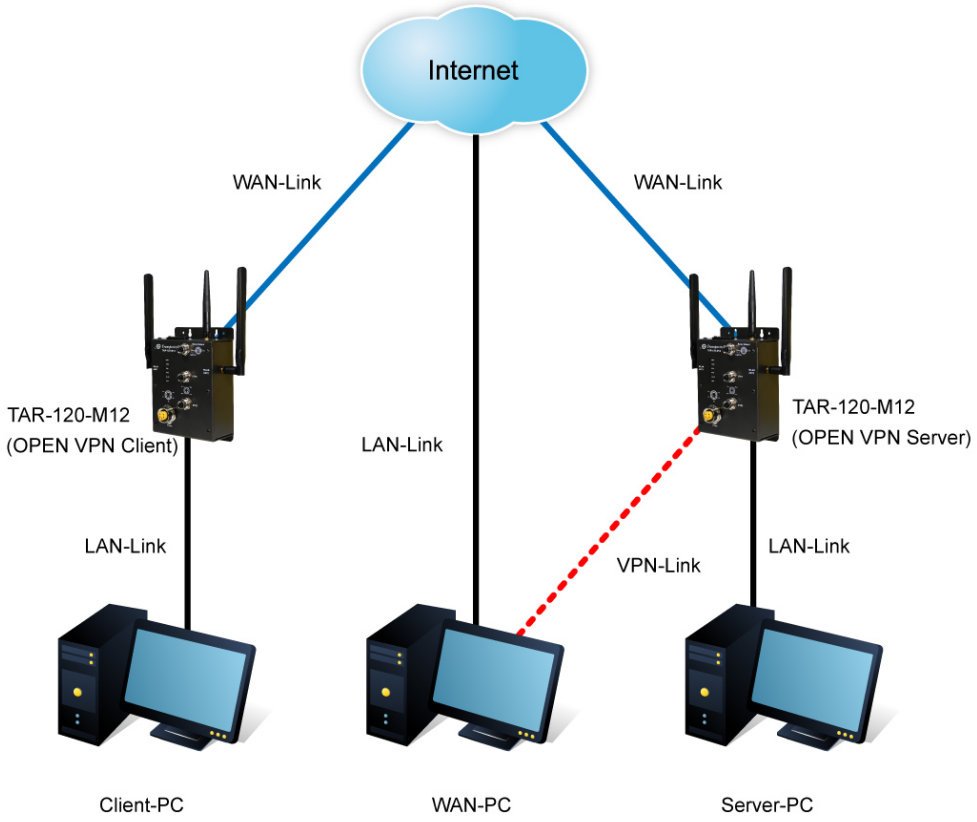
2: Open VPN Client

Two routers are needed for creating site-to-site VPN connection using this mode.

The following table describes the labels in this screen.

Label	Description
Open VPN Client	Enable or disable the function of Open VPN Client. You can allow or deny the Open VPN Client with this option.
Server IP	Enter the Open VPN Server IP address.
Tunnel Protocol	Select UDP or TCP protocol.
Port	Enter the port number, default is 1194.
LZO Compression	Enable or disable the LZO Compression.
Keys Setting	Select **Auto** to use the preset certificates, select **Manual** to paste your certificates. Please install software for Openvpn client to generate your certificates and paste them here. For more information, please visit Openvpn website.

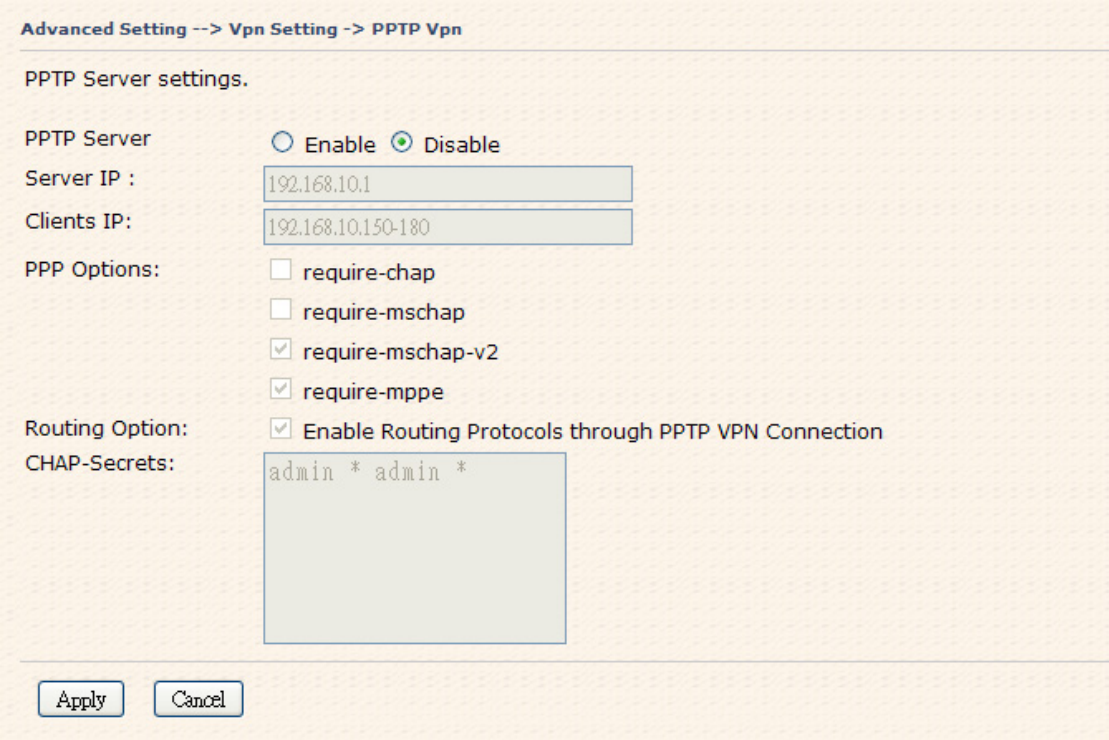
3: Open VPN Server VS Client



The chart above displays the connection of Open VPN Server and Client. The Server IP and Client IP address should configure with the same network domain.

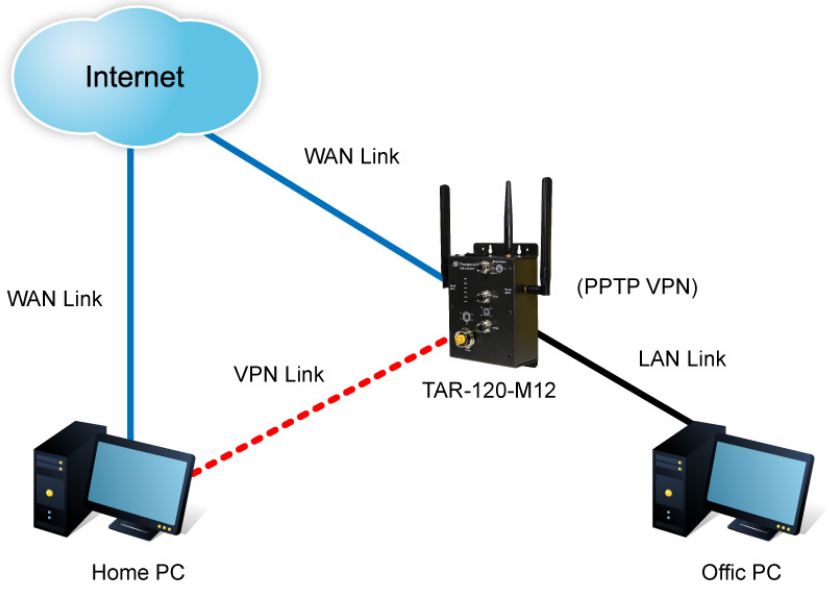
2. PPTP VPN

The PPTP (Point to Point Tunneling Protocol) VPN feature allows PC connected to the router from WAN port, just like connecting in the LAN. To create a PPTP connection to the router, you should create a PPTP network connection if you are using a window PC. The steps are: **Right click Network > property > create a new connection > connect to my work space (VPN) > use VPN to internet > enter the user name and password** which are set in the page.



PPTP VPN Screen

The following topology shows the common use of PPTP connection from the internet.



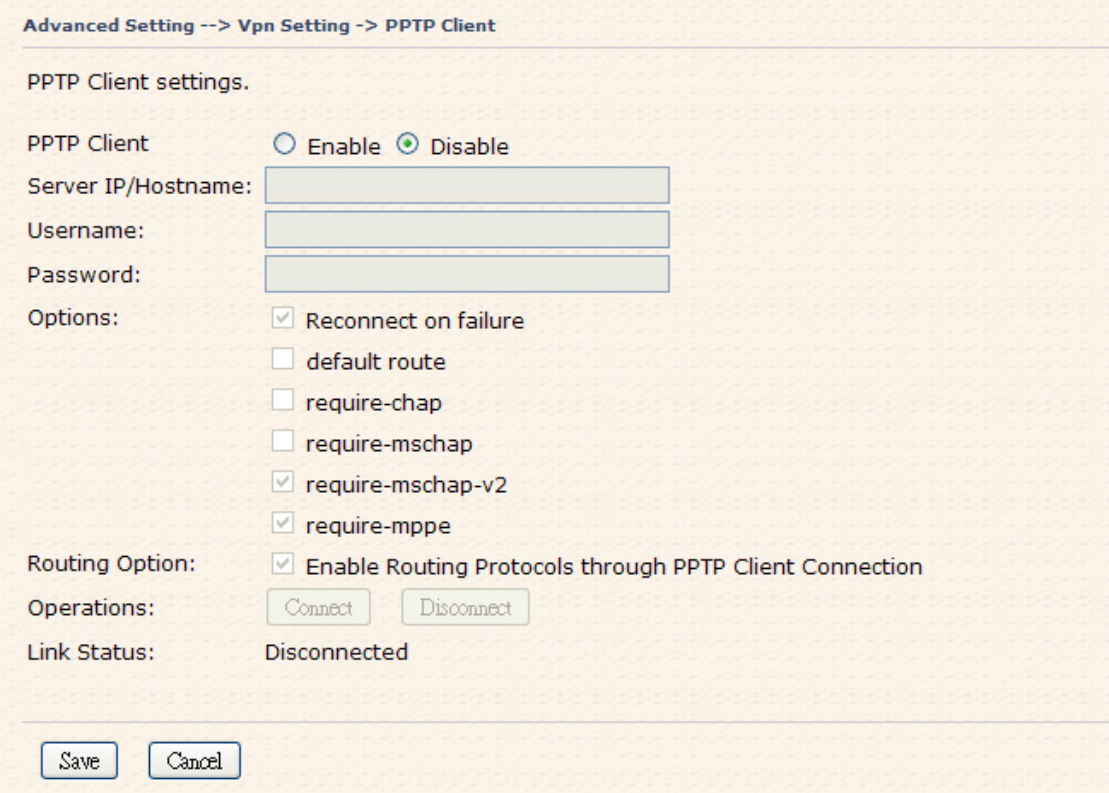
Connection to PPTP VPN Server

The following table describes the labels in this screen.

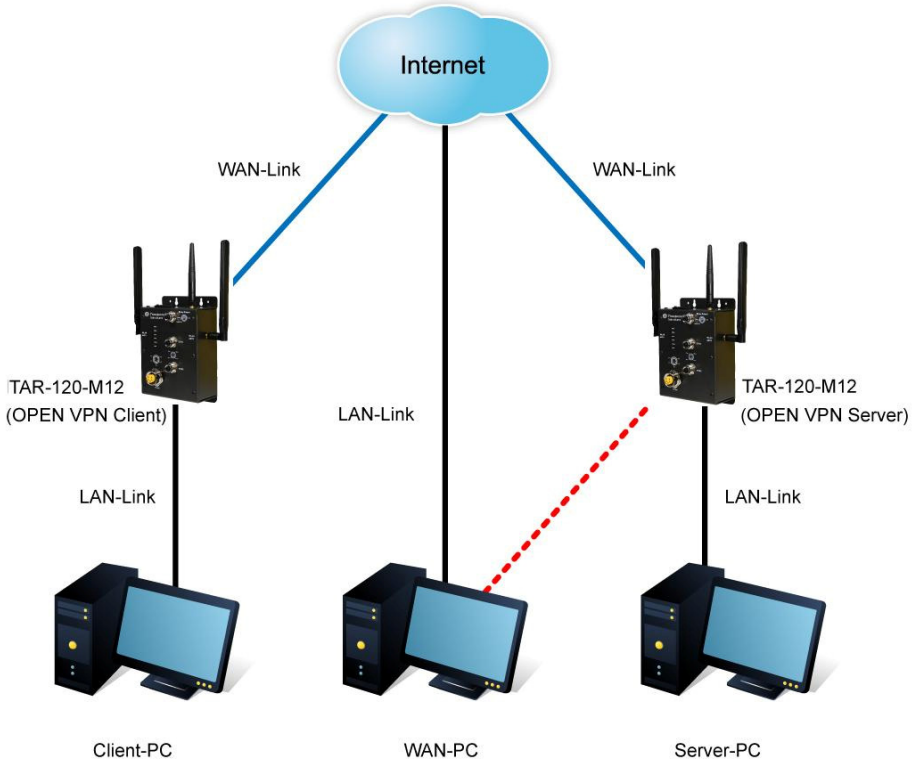
Label	Description
PPTP Server	Enable or disable PPTP VPN Server.
Server IP	Enter the server side IP address, default is the LAN port IP.
Client IP	Enter the IP address range, format is as **192.168.10.xx-xx**, connected client will be assigned the IP address.
CHAP-Secrets	Enter the username and password pairs, format is as **user * pass ***, multiple username password pairs are allowed.

3. PPTP Client

If the router A want to link with the others which is not in the same network with the router A, the function of PPTP client should support in the router page.



PPTP client settings screen



Client-PC and connect to Server-PC,WAN-PC

The following table describes the labels in this screen.

Label	Description
PPTP Client	Enable or disable PPTP Client.
Server IP/Hostname	Enter the server IP address or hostname.
Username/Password	Enter the username and password which is signed by PPTP server.
Option	**Reconnect on failure:** Pitch on this option, it will be reconnect when the link is on failure. **Require MPPE:** Choose Enable Require MPPE (Microsoft Point-to-Point Encryption) to encrypt data across Point-to-Point Protocol (PPP) and Virtual Private Network links.
Operations	Click "Connect" to link the server, if or not, you can click ""Disconnect" to break off from the server.
Link Status	Show the status about the link.

Routing Protocol (Routing Setting)

This page shows the information of routing table. The initial state of the router connect to the WAN, it will be based on the outside networks to access the routing table automatically. You can refer the shows about the bellow page.

Current Routing Table:

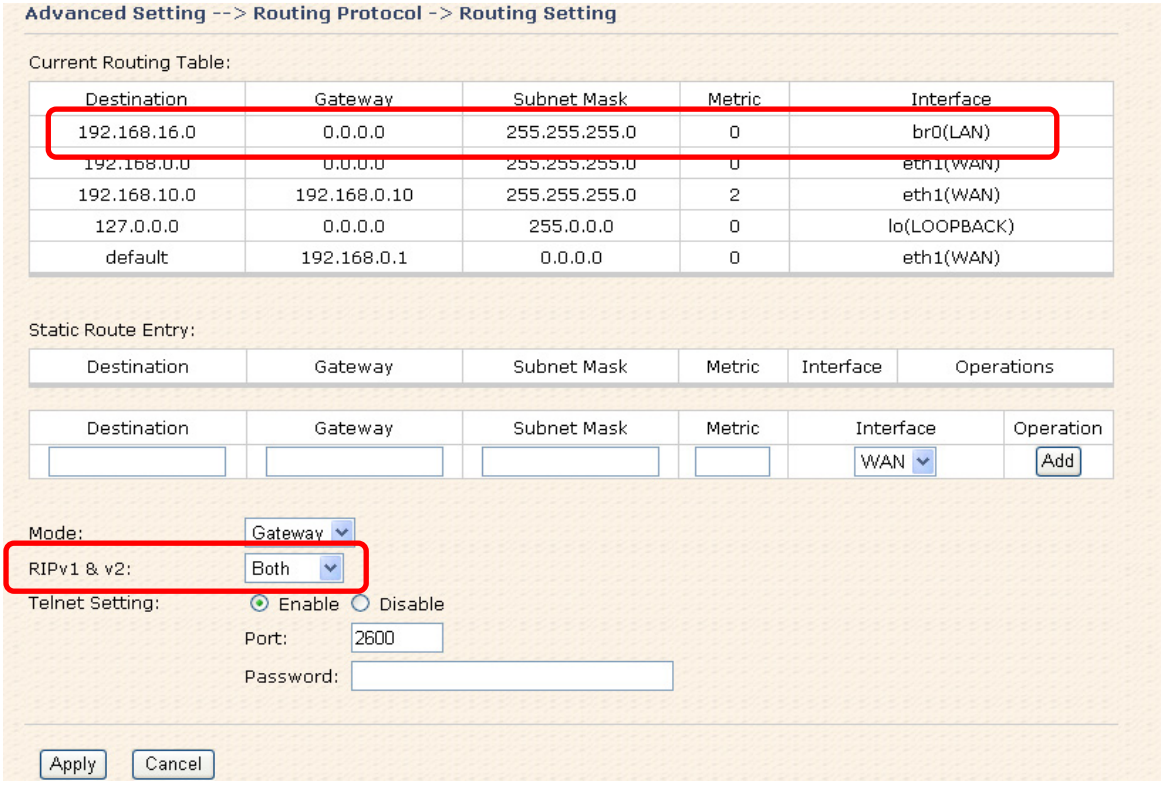
Destination	Gateway	Subnet Mask	Metric	Interface
192.168.16.0	0.0.0.0	255.255.255.0	0	br0(LAN)
192.168.0.0	0.0.0.0	255.255.255.0	0	eth1(WAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)
default	192.168.0.1	0.0.0.0	0	eth1(WAN)

The table shows the normal routing table

1. Use Dynamic Routing

Use the dynamic routing, you should not choose "Disable" about the **RIPv1 & v2** in the routers.

Click "Apply", and you can see the more information in the **Current Routing Table**, which shows the network segment of the other router.



Routing setting screen

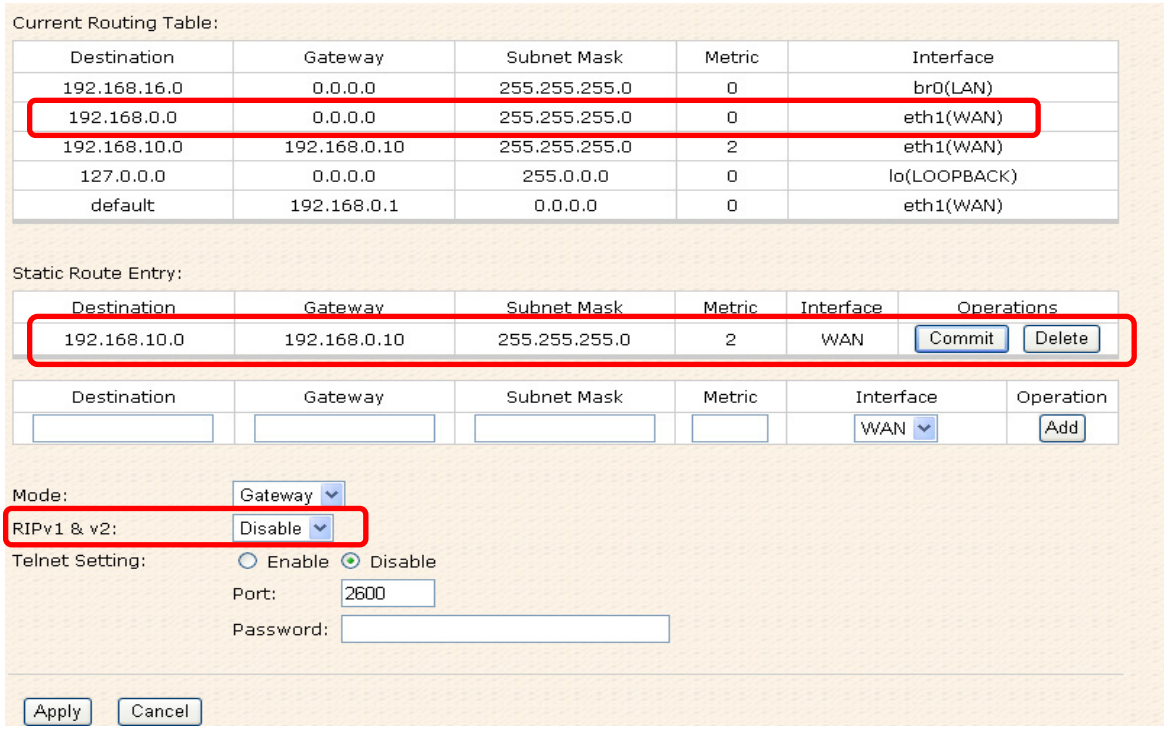
The following table describes the labels in this screen.

Label	Description
Current Routing Table	Show the current the routing information.
Static Router Entry	Not RIP and enter the right value in the textbox will be showing.
Mode	If you want to the PC in the router can visit the outside network, only choose the **Gateway Mode**; if or not, you choose the **Router Mode.**
RIPv1 &v2	Choose "Disable" in the Static routing.
Telnet Setting	Only use in the Dynamic routing.

2. Use Static Routing

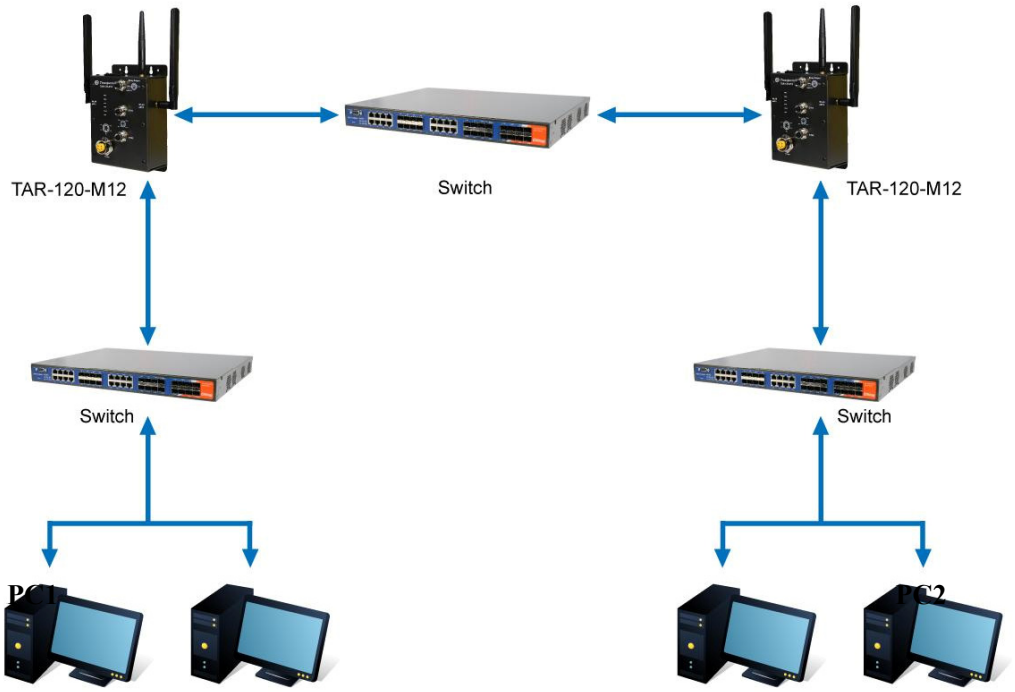
Use the Static routing, you should choose "Disable" about the **RIPv1 & v2** in the routers.

Click "Apply", and you can see the more information in the **Current Routing Table** and **Static Route Entry**, which shows the network segment of the other router.



Static route setting screen

Use the dynamic routing; it will have many ways such as RIP, OSPF.BGP. In this router, we use the RIP Protocol to finish the dynamic routing table.



The Routing Topography

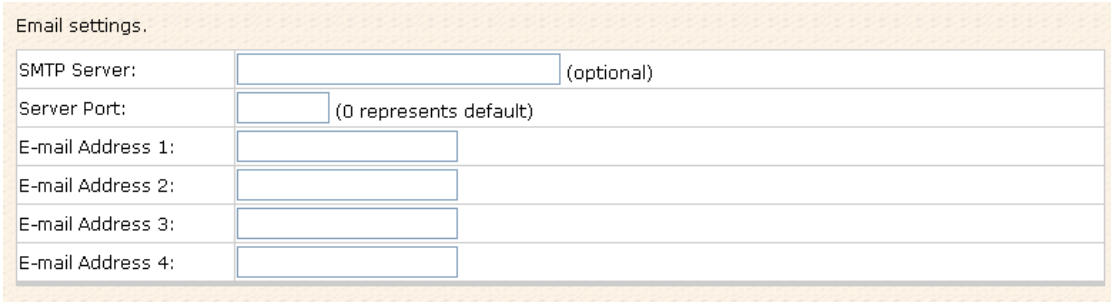
RIP, Routing Information Protocol, is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP) using the distance-vector routing algorithm.

After all settings, PC1 can visit PC2 which is different network segment of the PC1.

Notification

1. Email/SNMP/Syslog

Email Settings

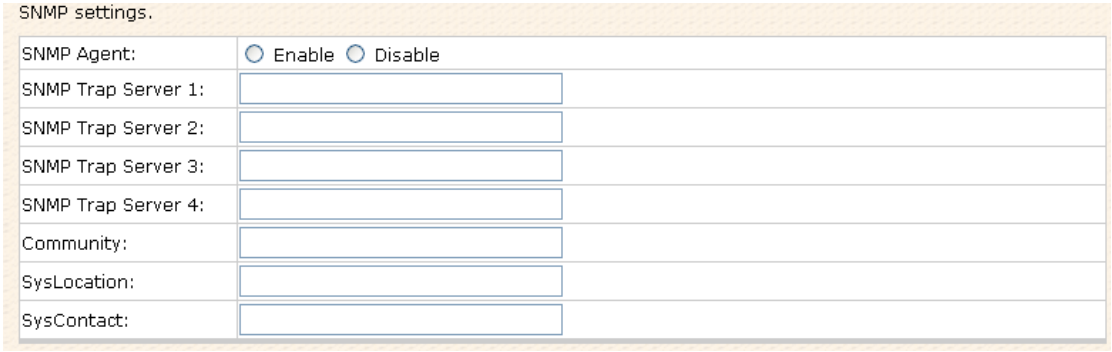


Email Settings Screen

The following table describes the labels in this screen.

Label	Description
SMTP Server	Simple Message Transfer Protocol, enter the backup host to use if primary host is not available while sending mail by SMTP server.
Server Port	Specify the port where MTA can be contacted via SMTP server.
E-mail Address 1-4	Enter the mail addresses.

SNMP Settings



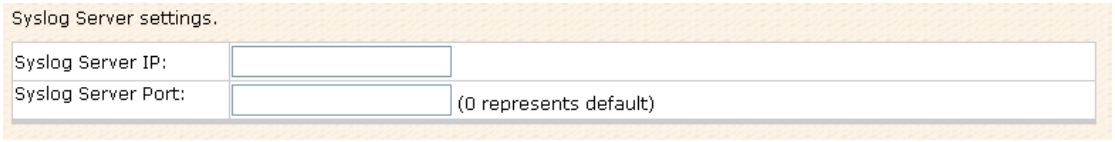
SNMP Settings

The following table describes the labels in this screen.

Label	Description
SNMP Agent	SNMP (Simple Network Management Protocol) agent communicates with the SNMP manager. The agent provides management information to the NMS by keeping track of various operational aspects of the system. Turn on to open this service and off to disable it.
SNMP Trap Server 1-4	Specify the IP address of trap server, which is the address to which SNMP trap messages are sent.

Community	Community is essentially password to establish trust between managers and agents. Normally "public" is used for read-write community.
SysLocation	Specify sysLocation string.
SysContact	Specify sysContact string.

Syslog Server Settings



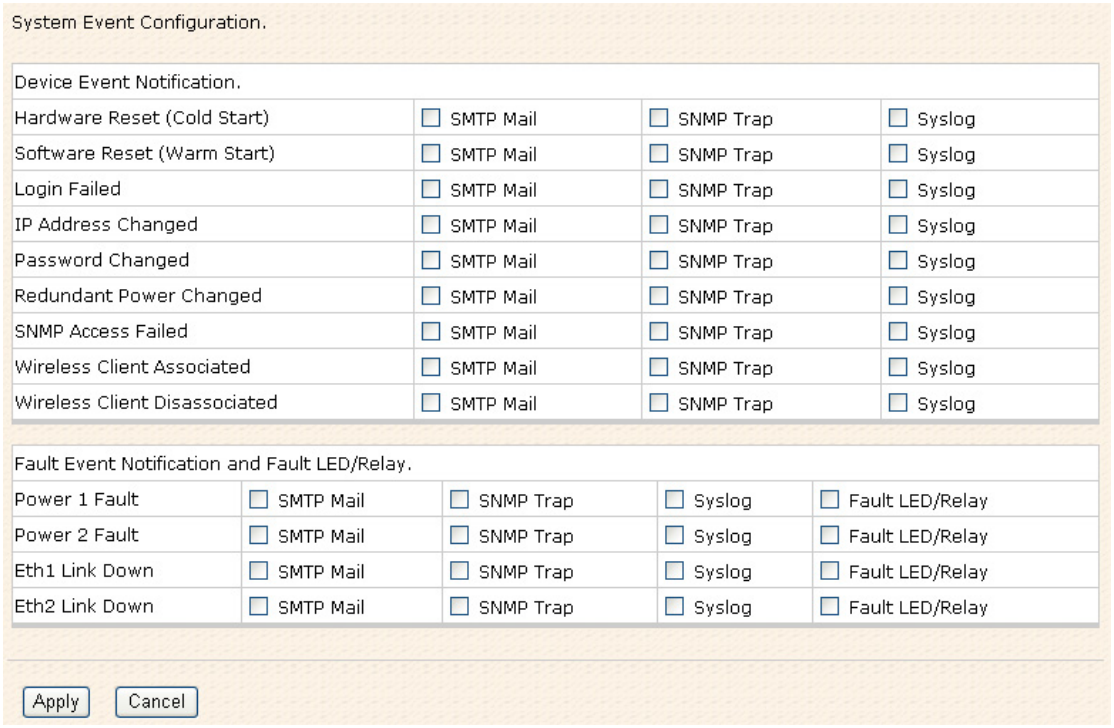
Syslog Server Screen

The following table describes the labels in this screen.

Label	Description
Syslog Server IP	Not only the Syslog keeps the logs locally, it can also log to remote server. Specify the IP of remote server. Leave it blank to disable logging remotely.
Syslog Server Port	Specify the port of remote logging. Default port is 514.

2. System Event

When specified event is triggered, the notification procedure will be performed according to the type of the event. Which notification would be performed depends on the selection of corresponding option in the **Advanced Setting > Notification > System Event** page.

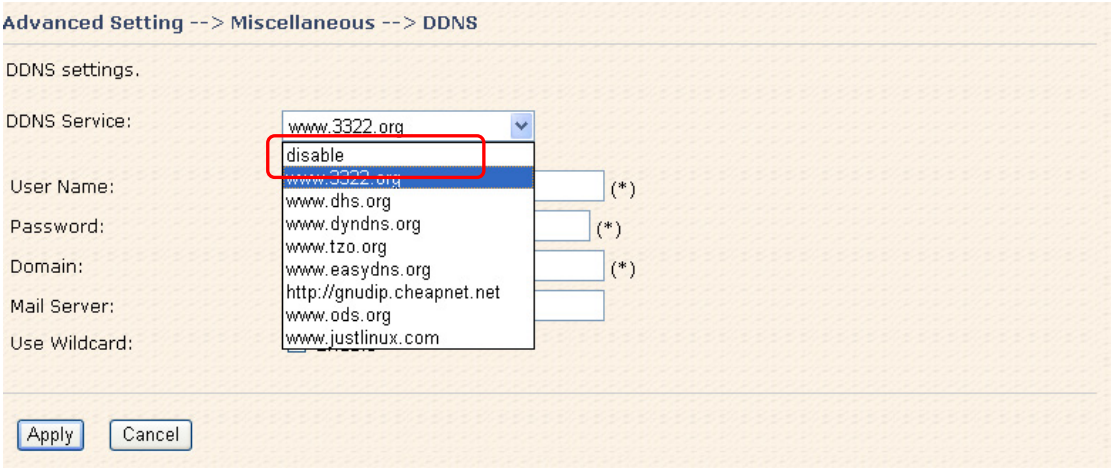


System Event Screen

System events record the activities of the Wireless Router system. When the setting changes or action performs, the event will be sent to administrator by email. A trap will also be sent to SNMP trap server. The Syslog will record the event locally and may send the Syslog remotely to a Syslog server. If serious event occurred, such as the power failure or link down, the fault led will be switched on as warning indication.

Miscellaneous (DDNS)

Dynamic Domain Name Server is to keep a domain name linked to a dynamic IP address.



DDNS Screen

For example, Choose DDNS Service: www.3322.org and configure the following instructions:

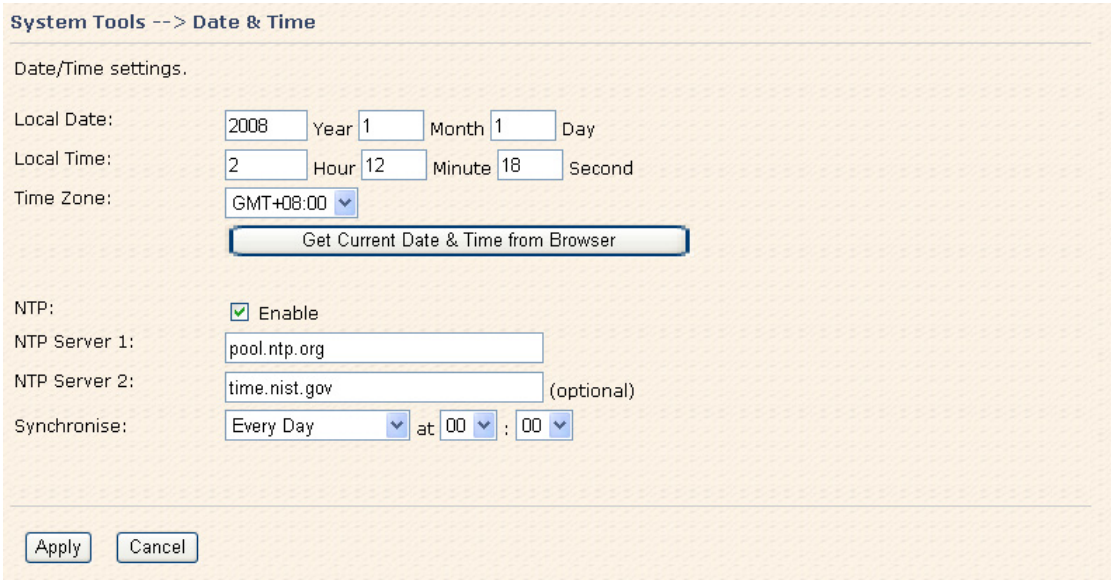
The following table describes the labels in this screen.

Label	Description
User Name	Enter the user name for your DDNS account.
Password	Enter the password for your DDNS account.
Domain	Enter the domain names provided by your dynamic DNS service provider.
Mail Server	Enter the mail server if provided.
Use Wildcard	Check the box the enable wildcard option.

5.3.3 System Tools

Date & Time

In this page, you can set the date & time of the device. The correct date & time will be helpful for logging of system events. A NTP (Network Time Protocol) client can be used to synchronize date & time with NTP server through internet.



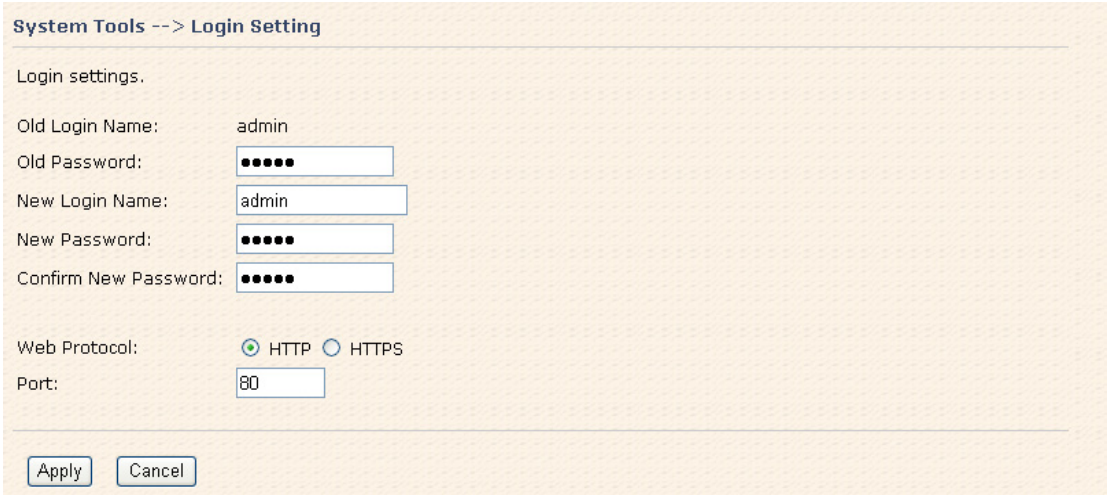
Date & Time Screen

The following table describes the labels in this screen.

Label	Description
Local Date	Set local date manually.
Local Time	Set local time manually.
Time Zone	Select the time zone manually
Get Current Date & Time from Browser	Click this button; you can set the time from your browser.
NTP	Enable or disable NTP function to synchronize time from the NTP server.
NTP Server 1	The primary NTP Server.
NTP Server 2	The secondary NTP Server.
Synchronize	This is the scheduled time when the NTP synchronization performed.

Login Setting

At this page, the administrator can change the login name and password. The default name and password is **admin** and **admin**.



Login Setting Screen

The following table describes the labels in this screen.

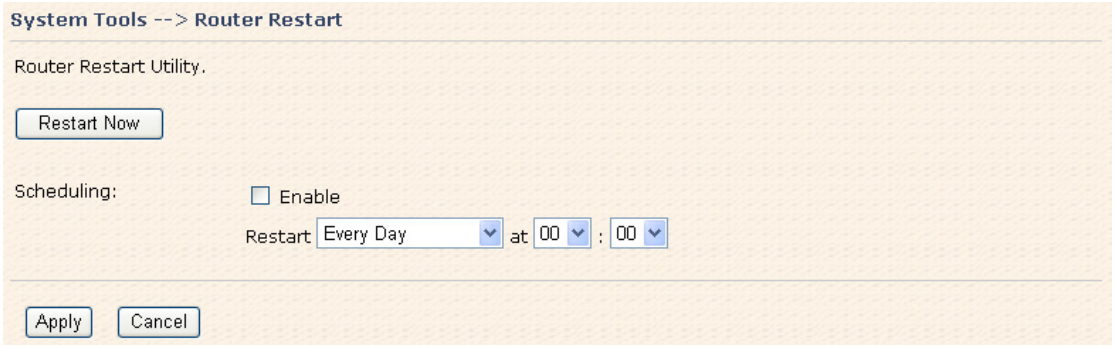
Label	Description
Old Name	This field shows the old login name.
Old Password	Before making a new setting, you should provide the old password for verification. Acceptable characters of this field

	contains '**0-9**', '**a-z**', '**A-Z**' and must be between 0 to 15 characters in length. An empty password is also acceptable.
New Name	Enter a new login name. Acceptable characters of this field contains '**0-9**', '**a-z**', '**A-Z**' and must be between 1 to 15 characters in length. An empty name is not acceptable.
New Password	Enter a new login password. Acceptable characters of this field contains '**0-9**', '**a-z**', '**A-Z**' and must be between 0 to 15 characters in length.
Confirm New Password	Retype the password to confirm it. Acceptable inputs of this field contains '**0-9**', '**a-z**', '**A-Z**' and must be between 0 to 15 characters in length.
Web Protocol	Choose the web management page protocol. HTTP and HTTPS are both supported.
Port	Choose the web management page port number. For HTTP, default port is 80; For HTTPS, default port is 443.

HTTPS (HTTP over SSL) is a Web protocol which encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

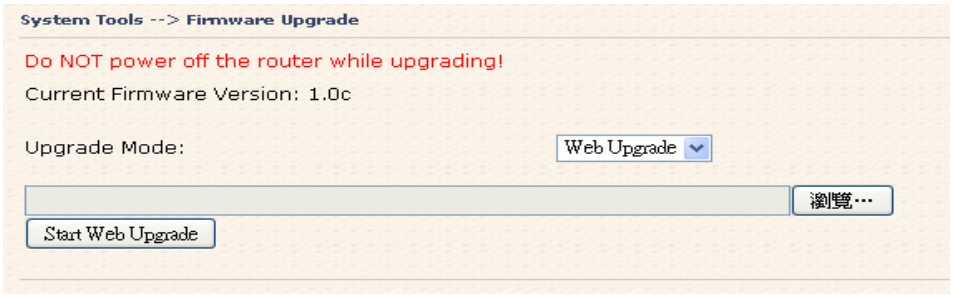
Router Restart

If you want restart the router through the **Warm Reset**, click **Restart Now** to restart the Wireless Router. Also, you can set a **Scheduling** time to make the router restart.



Router Restart Screen

Firmware Upgrade

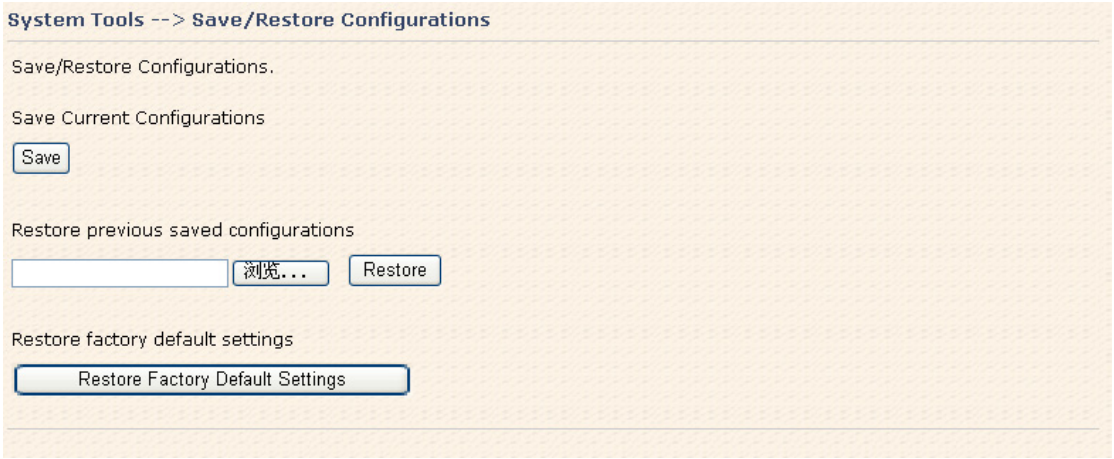


Firmware Upgrade Screen

Newer firmware may provide better performance or function extensions. To upgrade the new firmware, you need a firmware file which matches the model of this AP router. It will take several minutes to upload and update the firmware. After the upgrade is done successfully, reboot the router to utilized new firmware.

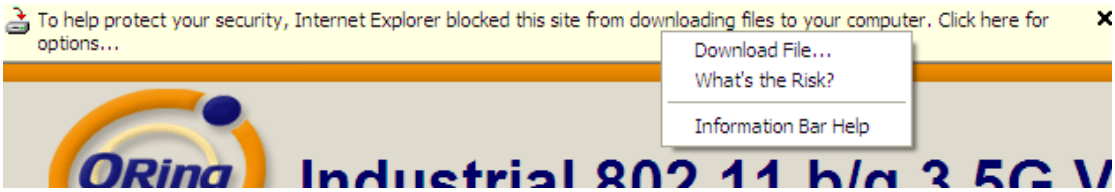
Important Notice: DO NOT POWER OFF THE ROUTER OR PRESS THE RESET BUTTON WHILE THE FIRMWARE IS BEING UPGRADED.

Save/Restore Configurations



Save/Restore Configurations Screen

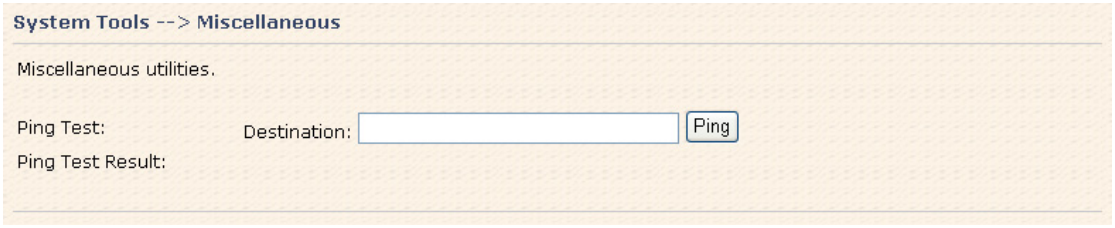
Save: The configuration file can be downloaded. (Internet Explorer user will need to click on the protection bar on top and click choose "download files")



The following table describes the labels in this screen.

Label	Description
Download configuration	The current system settings can be saved as a file into your PC.
Upload configuration	The configuration can be restored to the router. To reload a system settings file, click on **Browse** to browse your local hard drive and locate the system settings file previously saved. Click **Upload** when you have selected the file.
Restore Default Settings	You may also reset the router to the factory settings by clicking on **Restore Default Settings**. The router will reboot to validate the default settings.

Miscellaneous (Ping)



Miscellaneous Screen

The Ping Test is used to send Ping packets to test if a computer whether it is on the Internet or test if the WAN connection is OK. Enter a domain or IP in the destination box and click Ping to test.

5.3.4 System Status

System Info

System Status --> System Info

System Info.

Model:	TAR-120-M12_US	
Model Description:	EN50155 Transportation IEEE 802.11 b/g Cellular VPN router with 2x10/100Base-T(X), M12 connector, US band	
WAN:	Mode	Dynamic Setting
	IP Address	192.168.2.136
	Broadcast Address	192.168.2.255
	Subnet Mask	255.255.255.0
	Default Gateway	192.168.2.1
	DNS(Primary)	192.168.2.6
	DNS(Secondary)	
	MTU	1500
	MAC Address	00:1E:94:72:01:0C
LAN:	IP Address	192.168.10.1
	Subnet Mask	255.255.255.0
	MTU	1500
	MAC Address	00:1E:94:72:01:0B
	DHCP Server	Enabled
Wireless:	Wireless	Enabled
	SSID	oring
	Channel	6
	Encryption Mode	None
	MAC Address	00:0E:8E:23:CE:18

System Info Screen

This page displays the details information for the AP router including model name, model description, firmware version, WAN, LAN and wireless settings.

System Log

System Status --> System Log

System log.

Log Option:

☐ DHCP Server ☐ Boot Message
☐ NTP Client ☐ PPTP VPN
☐ PPPoE Client ☐ OpenVpn
☐ System Event ☐ UPNP
☐ Firewall ☐ Modem

Select All | Deselect All | Save Option

System Log: Refresh | Clear Logs

#	Date Time	Item	Content

Apply | Cancel

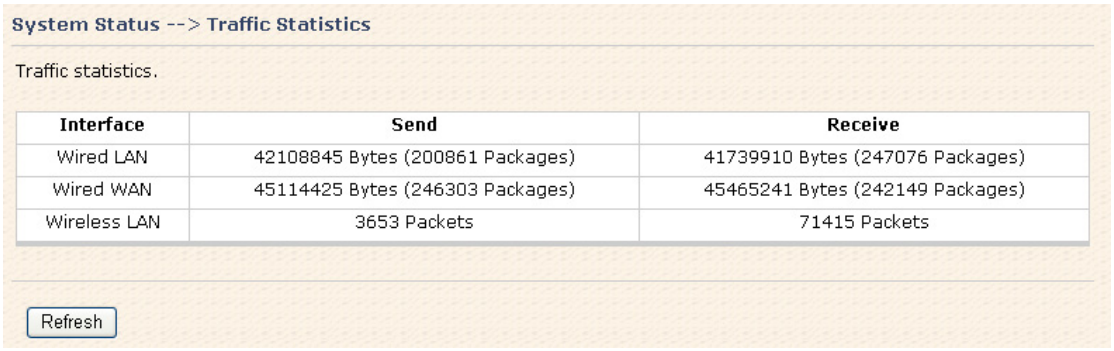
System Log Screen

The router keeps a running log of events and activities occurring on the router, several filters are provided for displaying related log entries.

Click the button '**Refresh**' to refresh the page.

Click the button '**Clear Logs**' to clear the log entries.

Traffic Statistics



Traffic Statistics Screen

This page displays the network traffic statistics for both received and transmitted packets through the Ethernet port and wireless connections.

Wired/Wireless Clients

Wired/Wireless Clients Screen

This page of the list displays the **Mac Address** and **Lease IP Address** of the wired/wireless clients connected. **Communication Type** shows the physical connection type of the client.

Technical Specifications

ORing EN50155 WLAN Access Point Router Model	**TAR-120-M12**	**TAR-3120-M12**
LAN Interface		
Ethernet Ports in M12 connector (4-pin, D-coding)	2 x 10/100Base-T(X), Auto MDI/MDI-X	
Protocols	ICMP, IP, TCP, UDP, DHCP, BOOTP, ARP/RARP, DNS, SNMP MIB II, HTTPS, SSH, SNMPV1/V2, Trap, Private MIB	
WLAN Interface		
Operating Mode	AP mode/ AP client / Client mode / Bridge mode	
Antenna and Connector	2 antennas with 2dBi for IEEE802.1 a/b/g mode in reverse SMA connector	4 antennas with 2dBi for IEEE802.1 a/b/g mode in reverse SMA connector
Radio Frequency Type	DSSS, OFDM	
Modulation	IEEE802.11b: CCK, DQPSK, DBPSK IEEE802.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM	
Frequency Band	America/FCC: 2.412~2.462 GHz (11channels) Europe CE/ETSI: 2.412~2.472 GHz (13channels)	America/FCC: 2.412~2.462 GHz (11channels) 5.15~5.825 GH (13 channel) Europe CE/ETSI: 2.412~2.472 GHz (13channels) 5.15~5.724 GH (19 channel)
Transmission Rate	IEEE802.11b: 1/2/5.5/11 Mbps IEEE802.11g: 6/9/12/18/24/36/48/54 Mbps	IEEE802.11b: 1/2/5.5/11 Mbps IEEE802.11 a/g: 6/9/12/18/24/36/48/54 Mbps
Transmit Power	IEEE802.11b/g: 20dBm max	IEEE802.11 a/b/g: 20dBm max
Receiver Sensitivity	-81dBm@11Mbps, PER< 8%; -64dBm@54Mbps, PER< 10%	-86dBm@11Mbps, PER< 8%; -77dBm@54Mbps, PER< 10%
Encryption Security	WEP: (64-bit, 128-bit key supported) WPA/WPA2:802.11i (WEP and AES encryption) WPA-PSK (256-bit key pre-shared key supported) 802.1X and Radius supported TKIP encryption	

Wireless Security	SSID broadcast disable	
LED Indicators	PWR 1(2) / Ready: 1) Red On: Power is on and booting up. 2) Green On: Power is on and functioning normally. ETH1(2) Link / ACT: Orange ON/Blinking: 10 Mbps Ethernet Green ON/Blinking: 100 Mbps Ethernet WLAN Link/ACT: Green ON/Blinking for WLAN interface WAN Link: Green for HSUPA modem connected Fault indicator: Red On: Ethernet link down or power down	PWR 1(2) / Ready: 1) Red On: Power is on and booting up. 2) Green On: Power is on and functioning normally. ETH1(2) Link / ACT: Orange ON/Blinking: 10 Mbps Ethernet Green ON/Blinking: 100 Mbps Ethernet WLAN Link/ACT: Green ON/Blinking for WLAN 1 interface / Red ON/Blinking for WLAN 2 interface WAN Link: Green for HSUPA modem connected Fault indicator: Red On: Ethernet link down or power down
HSUPA Cellular Interface		
Cellular Standard	GSM/GPRS/EGPRS/EDGE/WCDMA/HSDPA/HSUPA	
Band Option	Dual-band : HSUPA 1900 / 2100 MHZ Quad-band : GSM / GPRS / EDGE 850 / 900 / 1800 / 1900MHz WCDMA / HSDPA 850/900/1900/2100 MHZ	
Antenna and Connector	1 antenna with 2dBi for 850/900/1900/2100 MHZ in reverse SMA connector	
Power Requirements		
Power Input Voltage	Dual power inputs PWR1/2: 12 ~ 48VDC in M23 connector	
Reverse Polarity Protection	Present	
Power Consumption	5.8 Watts	9.6 Watts
Environmental		
Operating Temperature	-20 to 70°C	
Storage Temperature	-40 to 85°C	
Operating Humidity	5% to 95%, non-condensing	

Mechanical	
Dimensions (W x D x H)	125(W)mm x 65(D)mm x 196(H)mm
Casing	IP-40 protection
Regulatory Approvals	
EMI	FCC Part 15, CISPR (EN55022) class A, EN50155 (EN50121-3-2)
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27, EN61373
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6, EN61373
Rail Traffic	EN50155
Cooling	EN60068-2-1
Dry Heat	EN60068-2-2
Safety	EN60950-1
Warranty	3 years