Moxa Tough AP TAP-323 User's Manual

Edition 1.0, November 2017

www.moxa.com/product

Moxa Tough AP TAP-323 User's Manual

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Table of Contents

1

Introduction

Moxa Tough AP TAP-323 with dual-RF wireless capability allows wireless users to access network resources more reliably. The TAP-323 is rated to operate at temperatures ranging from -40 to 75°C and is rugged enough for any harsh industrial environment.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Product Specifications**
- **Functions**
  - LED Indicators
  - Reset Button

Overview

The TAP-323 outdoor dual-RF track-side wireless AP provides a complete and flexible solution for railway train-to-ground applications in demanding environments. The TAP-323 is rated to operate at temperatures ranging from -40 to 75°C, and its dustproof and weatherproof design is IP68-rated, allowing you to install the unit outdoors in the open or in tunnels. With two independent RF modules, the TAP-323 supports a greater variety of wireless configurations and applications. It can also increase the reliability of your entire wireless network by enabling redundant wireless connections. The TAP-323 has two AC power inputs for redundancy to increase the reliability of the power supply, and can be powered via PoE. The TAP-323 is a fully integrated AP and switch, with fiber ports and AC power supply in one box, and is ideal for use as a track-side AP for train-to-ground communication applications, including Communication Based Train Control (CBTC) and Closed-Circuit Television (CCTV).

Package Checklist

- 1 TAP-323
- 1 wall-mounting kit, including 2 plates
- 1 fiber panel mounting kit
- 6 metal protective caps for Ethernet ports LAN-1 to LAN-4, the USB console port, and the ABC-02 USB storage port*
- 5 metal protective caps for 4 antenna ports and 1 optional antenna port
- 3 antenna glands for top side antenna
- 1 metal M23 male 6-pin crimp connector for power
- 1 plastic M23 dust cover for power
- Quick installation guide (printed)
- Warranty card

NOTE *The ABC-02 and SFP modules are not included and can be purchased separately.
For a list of recommended optional accessories, refer to the TAP-323 datasheet, available at:
http://www.moxa.com/product/TAP-323.htm

Product Features

- All-in-one design that combines a dual access point, a switch, and AC to DC power supply in one box to avoid interoperability issues between different components
- IP68-rated high-strength metal housing
- Isolated 110 to 220 VDC/VAC power input
- Dual-RF design
- Power supply through 4 PoE ports for wayside PoE devices
- 2 fiber SFP ports for backbone installation
- 2x2 MIMO technology
- Rugged M12 design for Ethernet port, console port, and USB port
- -40 to 75°C operating temperature range
- Certified against the EN 50121-4 railway standard
- Controller-based Turbo Roaming
- Supports Moxa's Turbo Chain*, which is a redundancy technology to provide fast recovery time and ensure non-stop operation of your wayside network
- Supports RSTP function to prevent network looping
- Supports 5.8 GHz band in the standard model

- Supports QoS function, which can help assign high priority to your critical traffic
- Provides advanced wireless security settings
- Provides 64-bit and 128-bit WEP/WPA/WPA2 encryption
- SSID Hiding, IEEE 802.1x security, and RADIUS
- Packet access control and filtering
- Supports SNMP, SNTP, SSH, HTTPS, TFTP for remote management
- Long-distance transmission support
  (There are many factors that affect the performance of a device when it is used in long-distance applications. These factors include: 1. Test architecture 2. Installation distance 3. Car speed 4. Antenna gain 5. Band 6. Transmission Power 7. Signal Strength. For details, please contact your Moxa sales representative.)
- Wall mountable

***100 ms recovery time**

Product Specifications

WLAN Interface

Standards:

IEEE 802.11a/b/g/n for Wireless LAN
IEEE 802.11i for Wireless Security
IEEE 802.3 for 10BaseT
IEEE 802.3u for 100BaseT(X)
IEEE 802.3ab for 1000BaseT
IEEE 802.3af for Power-over-Ethernet
IEEE 802.1D for Spanning Tree Protocol
IEEE 802.1w for Rapid STP
IEEE 802.1p for Class of Service
IEEE 802.1Q for VLAN

Spread Spectrum and Modulation (typical):

• DSSS with DBPSK, DQPSK, CCK
• OFDM with BPSK, QPSK, 16QAM, 64QAM
• 802.11b: CCK @ 11/5.5 Mbps, DQPSK @ 2 Mbps, DBPSK @ 11 Mbps
• 802.11a/g: 64QAM @ 54/48 Mbps, 16QAM @ 36/24 Mbps, QPSK @ 18/12 Mbps, BPSK @ 9/6 Mbps

Operating Channels (central frequency):

US:
2.412 to 2.462 GHz (11 channels)
5.180 to 5.240 GHz (4 channels)
5.260 to 5.320 GHz (4 channels)*
5.500 to 5.700 GHz (8 channels; excludes 5.600 to 5.640 GHz)* 5.745 to 5.825 GHz (5 channels)
EU:
2.412 to 2.472 GHz (13 channels)
5.180 to 5.240 GHz (4 channels)
5.260 to 5.320 GHz (4 channels)*
5.500 to 5.700 GHz (11 channels)*
JP:
2.412 to 2.484 GHz (14 channels, DSSS)
5.180 to 5.240 GHz (4 channels)
5.260 to 5.320 GHz (4 channels)*
5.500 to 5.700 GHz (11 channels)*
*Special frequency bands (such as 5.9 GHz) are available for customization.

Security:

• SSID broadcast enable/disable

• Firewall for MAC/IP/Protocol/Port-based filtering

• 64-bit and 128-bit WEP encryption, WPA /WPA2-Personal and Enterprise (IEEE 802.1X/RADIUS, TKIP and AES)

Transmission Rates:

802.11b: 1, 2, 5.5, 11 Mbps

802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

Protocol Support

General Protocols: Proxy ARP, DNS, HTTP, HTTPS, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP v1/v2/v3, PPPoE, DHCP

AP-only Protocols: ARP, BOOTP, DHCP, STP/RSTP (IEEE 802.1D/w)

Interface

Connector for External Antennas: N-type (female)

Fast Ethernet ports: 4, side cabling, M12 D-coded 4-pin female connector, 10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection, 802.1af PoE power budget

Console Port: M12 B-coded 5-pin female connector for the USB console

USB Port: M12 A-coded 5-pin female connector for ABC-02 USB storage

Fiber Ports: 2, 100/1000BaseSFP slot

LED Indicators: PWR1, PWR2, PoE1-4, FAULT1, FAULT2, STATUS, HEAD, TAIL, LAN1-6, WLAN1, WLAN2

Physical Characteristics

Housing: Metal, IP68 protection

Weight: 10 kg (22.22 lb)

Dimensions: 324 x 279 x 156 mm (12.76 x 10.98 x 6.142 in)

Installation: Wall mounting

Environmental Limits

Operating Temperature: -40 to 75°C (-40 to 167°F)

Storage Temperature: -40 to 85°C (-40 to 185°F)

Ambient Relative Humidity: 5% to 95% (non-condensing)

Power Requirements

Input Voltage: 110/220 VDC/VAC (88 to 300 VDC, 85 to 264 VAC)
Connector: M23
Input Current:
AC input: 110 to 220 VAC, 50 to 60 Hz, 1.1 A (max.)
DC input: 110 to 220 VDC, 1.1 A (max.)
Power Consumption:
Maximum 85 watts (with PSE ports fully loaded)
Reverse Polarity Protection: Present
Overload Current Protection: Present

Standards and Certifications

Safety: UL 60950-1, IEC 60950-1(CB), LVD EN 60950-1
EMC: EN 301 489-1/17, EN 55032/55024
EMI: CISPR 22, FCC Part 15B Class A
EMS :
IEC 61000-4-2 ESD: Contact: 6 kV; Air: 8 kV
IEC 61000-4-3 RS: 80 MHz to 1 GHz: 20 V/m
IEC 61000-4-4 EFT: Power: 2 kV; Signal: 2 kV
IEC 61000-4-5 Surge: Power: 2 kV; Signal: 2 kV
IEC 61000-4-6 CS: 10 V
IEC 61000-4-8
Radio: EN 301 489-1/17, EN 300 328, EN 301 893, TELEC, DFS, FCC, IC, WPC
Rail Traffic: EN 50155 (mandatory compliance*), EN 50121-4
*This product is suitable for rolling stock railway applications, as defined by the EN 50155 standard. For a more detailed statement, click here: www.moxa.com/doc/specs/EN_50155_Compliance.pdf.

Reliability

MTBF (mean time between failures):
290,937 hrs
Standard : Telcordia SR332

Warranty

Warranty Period: 5 years
Details: See www.moxa.com/warranty

ATTENTION

The TAP-323 is NOT a portable mobile device and should be located at least 20 cm away from the human body. The TAP-323 is NOT designed for the general consumer. A well-trained technician is required to safely deploy TAP-323 units and establish a wireless network.

Functions

LED Indicators

The LEDs on the front panel of TAP-323 allow you to quickly identity the wireless status and settings.

The **FAULT** LED will light up to indicate system failure or user-configured events. If the TAP-323 cannot retrieve the IP address from a DHCP server, the **FAULT** LED will blink at one second intervals.

The following table is a summary of the wireless settings and LED displays. You can check the status of the TAP-323 by reading these LEDs. More information about "Basic Wireless Settings" is presented in Chapter 3.

LED	Color	State	Description
PWR1	Green	On	Power is being supplied (from power input 1)
		Off	Power is **not** being supplied
PWR2	Green	On	Power is being supplied (from power input 2)
		Off	Power is **not** being supplied
FAULT1	Red	On	System is booting up
		Blinking (slow at 1-second intervals)	Cannot get an IP address from the DHCP server
		Blinking (fast at 0.5-second intervals)	IP address conflict
		Off	Normal status
STATUS	Green	On	System startup is complete and the system is in operation.
		Blinking (slow at 1-second intervals)	The AWK Search Utility has located the AWK device.
	Red	On	System is booting up

LED	Color	State	Description
HEAD	Green	On	The TAP unit is configured as the HEAD TAP unit of a Turbo Chain
		Blinking	The TAP unit's head port link is disconnected
		Off	The TAP unit is not configured as the HEAD TAP unit of a Turbo Chain
TAIL	Green	On	The TAP unit is configured as a TAIL TAP unit of a Turbo Chain
		Blinking	The TAP TAIL unit's port link is disconnected or in blocking state
		Off	The TAP unit is not configured as the TAIL TAP unit of a Turbo Chain
WLAN 1	Green	On	The WLAN is in **Slave** mode
		Blinking	The WLAN is transmitting data in **Slave** mode
		Off	The WLAN is not in use or is not working properly
	Amber	On	The WLAN is in **AP/ Master** mode
		Blinking	The WLAN is transmitting data in **AP/ Master** mode
		Off	The WLAN is not in use or is not working properly
WLAN 2	Green	On	The WLAN is in **Slave** mode.
		Blinking	The WLAN is transmitting data in **Slave** mode
		Off	The WLAN is not in use or is not working properly
	Amber	On	The WLAN is in **AP/Bridge/Master** mode
		Blinking	The WLAN is transmitting data in **AP/Bridge/Master** mode
		Off	The WLAN is not in use or is not working properly
LAN 1-4	Amber	On	The LAN port's 10/100 Mbps link is active
		Blinking	Data is being transmitted at 10/100 Mbps
		Off	The LAN port's 10/100 Mbps link is inactive
LAN 5-6	Green	On	The LAN port's 1000 Mbps link is active
		Blinking	Data is being transmitted at 1000 Mbps
		Off	The LAN port's 1000 Mbps link is inactive
	Amber	On	The LAN port's 100 Mbps link is active
		Blinking	Data is being transmitted at 100 Mbps
		Off	The LAN port's 100 Mbps link is inactive
PoE 1-4	Green	On	The PSE port is supplying power to a powered device
		Off	The PSE port is not supplying power

Note: The FAULT2 LED is reserved for future use.

ATTENTION

When the LEDs for **STATE** (Green), **FAULT**, **WLAN1**, and **WLAN2** all light up simultaneously and blink at one-second intervals, it means that the system failed to boot. This may be due to an improper operation or issues such as an unexpected shutdown during a firmware update. To recover the firmware, refer to "Firmware Recovery" in Chapter 7.

Reset Button

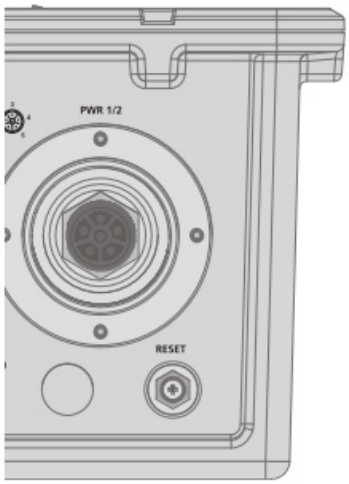
The **RESET** button is located on the bottom panel of the TAP-323. You can reboot the TAP-323 or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

- **System reboot:** Hold the **RESET** button down for less than 5 seconds and then release.
- **Reset to factory default:** Hold the **RESET** button down for over 5 seconds until the **STATE** LED starts blinking green. Release the button to reset the TAP-323.

NOTE **For security reasons, the reset button can be configured to be disabled for 60 seconds after the device reboots.**

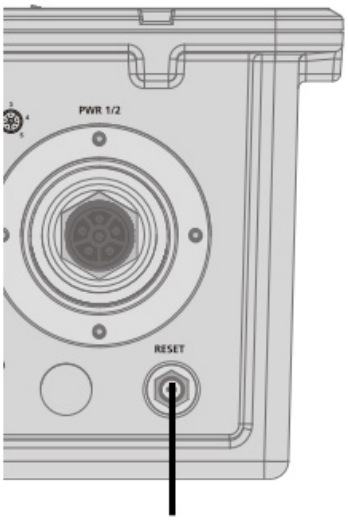
STEP 1:

Remove the reset button cover.



STEP 2:

Using a pointed object, press and hold the reset button.



2

Getting Started

This chapter explains how to install Moxa's TAP-323 for the first time, quickly set up your wireless network, and test whether or not the connection is running properly. With the function guide, you can easily find the functions you need.

The following topics are covered in this chapter:

- **First-Time Installation and Configuration**
- **Communication Testing**
  - How to Test One TAP-323
  - How to Test Two or More TAP Units
- **Function Guide Map**

First-Time Installation and Configuration

Take the following steps to configure your TAP-323. Refer to the section Panel Layout of the TAP-323 below to see where the various ports are located on the product.

Step 1: Select a power source

Connect the TAP-323 to either a 110 to 220 VDC or 110 to 220 VAC power source.

Step 2: Connect the TAP-323 to a computer

Use either a straight-through or crossover Ethernet cable to connect the TAP-323 to a computer. When the connection between the TAP-323 and the computer is established, the LED indicator on the TAP-323's LAN port will light up. See the section 10/100BaseT(X) Ethernet Ports below for detailed instructions.

Step 3: Set up the computer's IP address.

The computer's IP address must be on the same subnet as the TAP-323. Since the TAP-323's default IP address is 192.168.127.253, and the subnet mask is 255.255.255.0, set the computer's IP address to 192.168.127.252 (for example), and subnet mask to 255.255.255.0.

NOTE After you select **Maintenance → Load Factory Default** and click the **Submit** button, the TAP-323 will reset to factory default settings and the IP address will also reset to **192.168.127.253**.

Step 4: Use the web-based manager to configure the TAP-323

Open your computer's web browser and type http://192.168.127.253 in the address field to access the homepage of the web-based manager. Enter the User name and Password to open the TAP-323 homepage. If you are configuring the TAP-323 for the first time, enter the following:

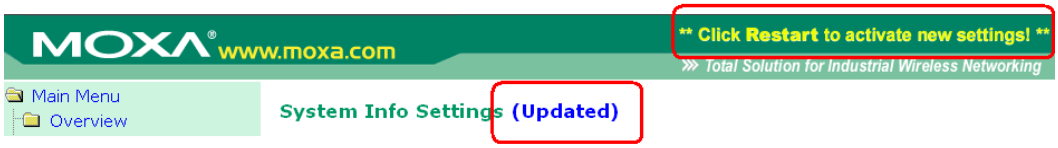
NOTE Default user name and password:

User Name: **admin**

Password: **moxa**

For security reasons, we strongly recommend changing the default password. To do so, select **Maintenance → Password**, and then follow the on-screen instructions.

NOTE After you click **Submit** to apply changes, the web page will refresh, and then the string "**(Updated)**" and a blinking reminder will be displayed on the upper-right corner of the page, as illustrated below.



To make the changes effective, click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the TAP-323 to complete its restart process.

Step 5: Select the operation mode

By default, the TAP-323's operation mode is set to Wireless redundancy. If you would like to use Wireless bridge or AP mode instead, you can change the setting in **Wireless Settings → Operation mode**. Detailed information about configuring the TAP-323's operation mode can be found in Chapter 3.

Step 6: Test the network connection

In the following sections we describe two methods that you can use to test that a network connection has been established.

Communication Testing

After installing the TAP-323 you can run a sample test to make sure the wireless connection on the TAP-323 is functioning normally. Two testing methods are described below. Use the first method if you are using only one TAP-323 device and the second method if you are using two or more TAP units.

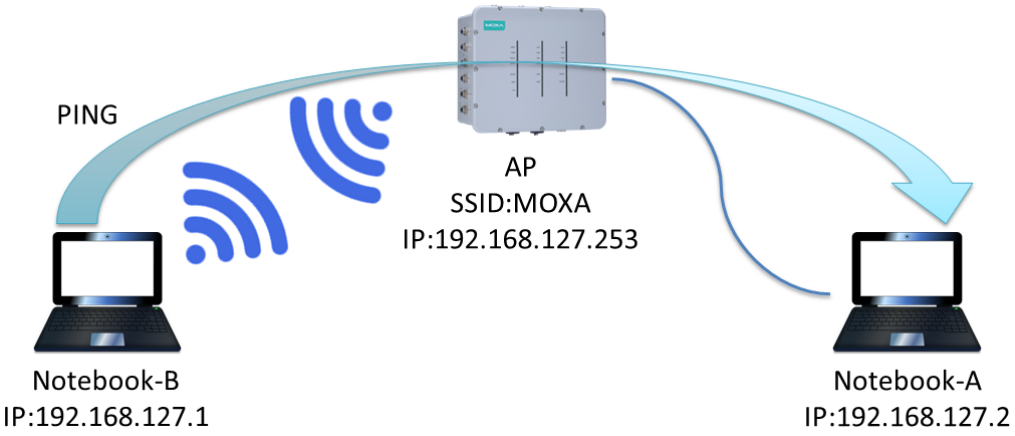
How to Test One TAP-323

If you are only using one TAP-323, you will need one additional notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the TAP-323 (NOTE: the default SSID is MOXA), and change the IP address of the second notebook (Notebook B) so that it is on the same subnet as the first notebook (Notebook A), which is connected to the TAP-323.

After configuring the WLAN card, establish a wireless connection with the TAP-323 and open a DOS window on Notebook B. At the prompt, type the following:

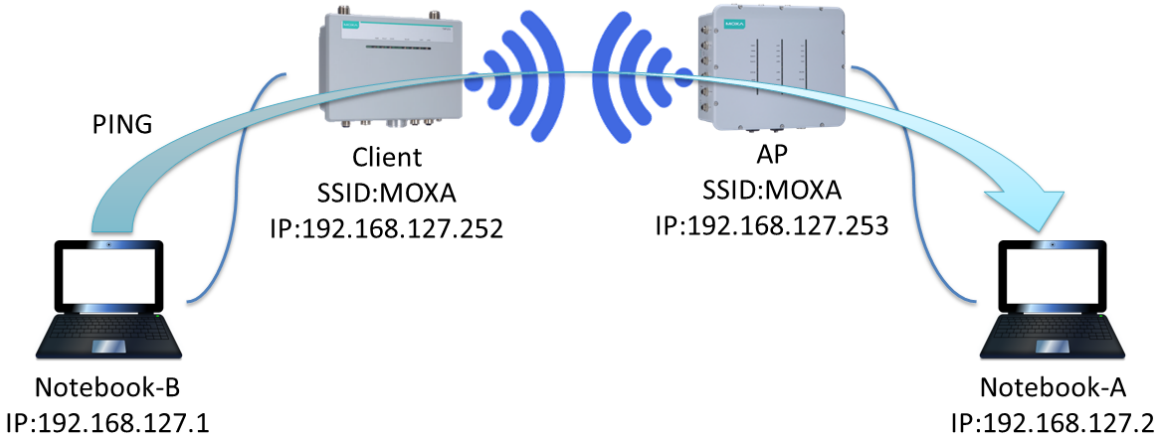
ping <IP address of notebook A>

and then press Enter (see the figure below). A "Reply from IP address …" response means the communication was successful. A "Request timed out." response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.



How to Test Two or More TAP Units

If you have one TAP-323 and oneTAP-323 unit, you will need a second notebook computer (Notebook B) equipped with an Ethernet port. Use the default settings for the TAP-323 connected to notebook A and change the TAP-323 connected to notebook B to Client mode, and then configure the notebooks and TAP units properly.



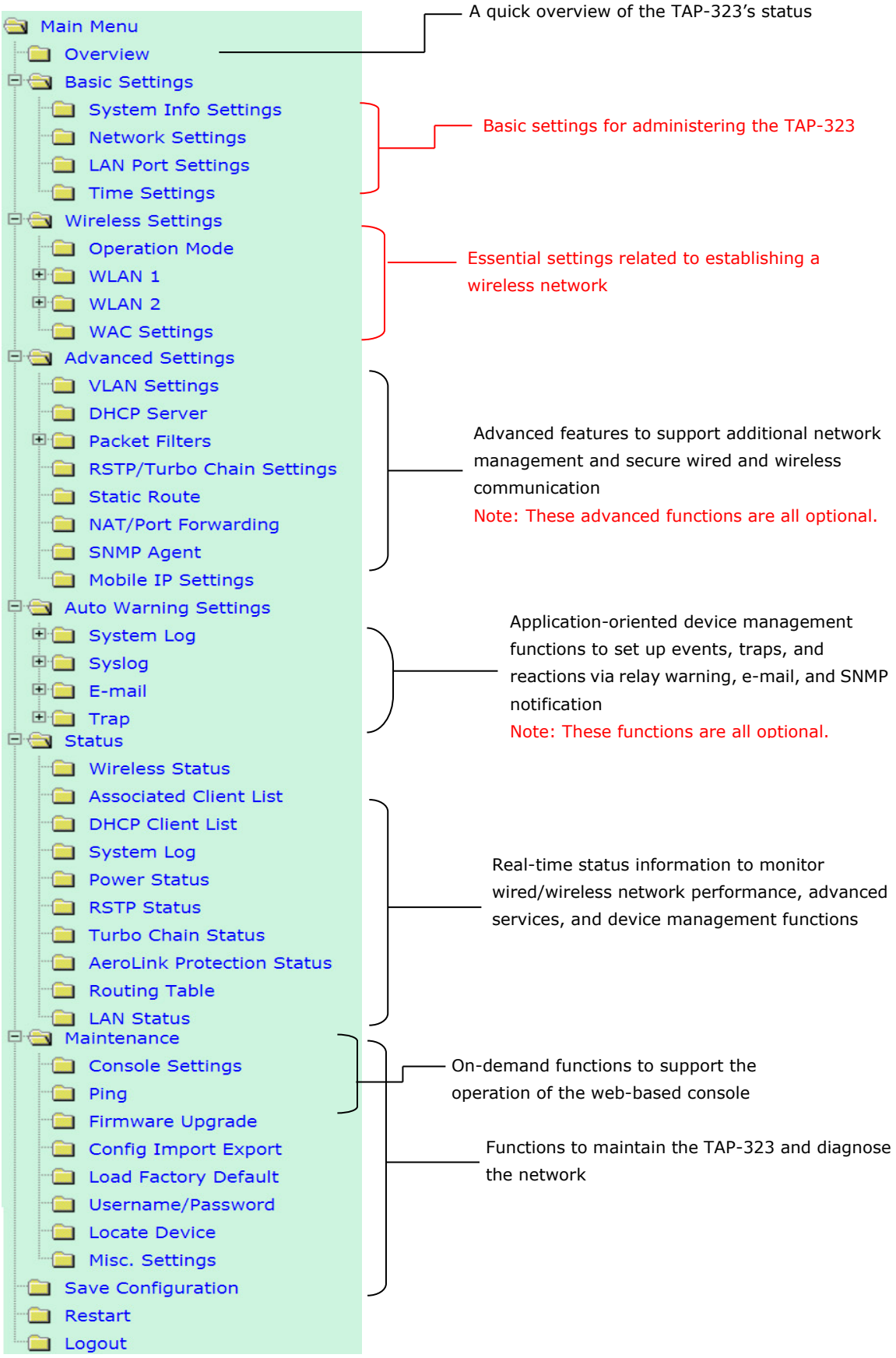
After setting up the testing environment, open a DOS window on notebook B. At the prompt type:

ping <IP address of notebook A>

and then press Enter. A "Reply from IP address …" response means the communication was successful. A "Request timed out" response means the communication failed. In the latter case, recheck the configuration to make sure the settings are correct.

Function Guide Map

The management functions are organized in a tree and shown in the left field of the web-based management console. You can efficiently locate the function you need with the following guiding map.



3

Web Console Configuration

In this chapter, we will explain each web management page of the web-based console configuration. Moxa's easy-to-use management functions will help you set up your TAP-323, as well as establish and maintain your wireless network easily.

The following topics are covered in this chapter:

- **Configuration by Web Browser**
- **Overview**
- **Basic Settings**
  - System Info Settings
  - Network and LAN Port Settings
  - Time Settings
- **Wireless Settings**
  - Operation Mode
  - WLAN Security Settings
  - Advanced Wireless Settings
  - WLAN Certification Settings (for EAP-TLS in Slave mode only)
  - WAC Settings (AP Mode Only)
- **Advanced Settings**
  - Using Virtual LAN
  - DHCP Server (for AP operation mode only)
  - Packet Filters
  - Introduction to Redundancy Protocol
  - RSTP/Turbo Chain Settings (For Master or Slave Mode Only)
  - SNMP Agent
  - PoE Settings
- **Auto Warning Settings**
  - System Log
  - Syslog
  - E-mail
  - Trap
- **Status**
  - Wireless Status
  - Associated Client List (for AP or Master Mode only)
  - DHCP Client List (for AP mode only)
  - System Log
  - RSTP Status
  - Turbo Chain Status
  - LAN Status
- **Maintenance**
  - Console Settings
  - Ping
  - Firmware Upgrade
  - Config Import Export
  - MIB Export
  - Load Factory Default
  - Username/Password
  - Locate Device
  - Misc. Settings
- **Save Configuration**
- **Restart**
- **Logout**

Configuration by Web Browser

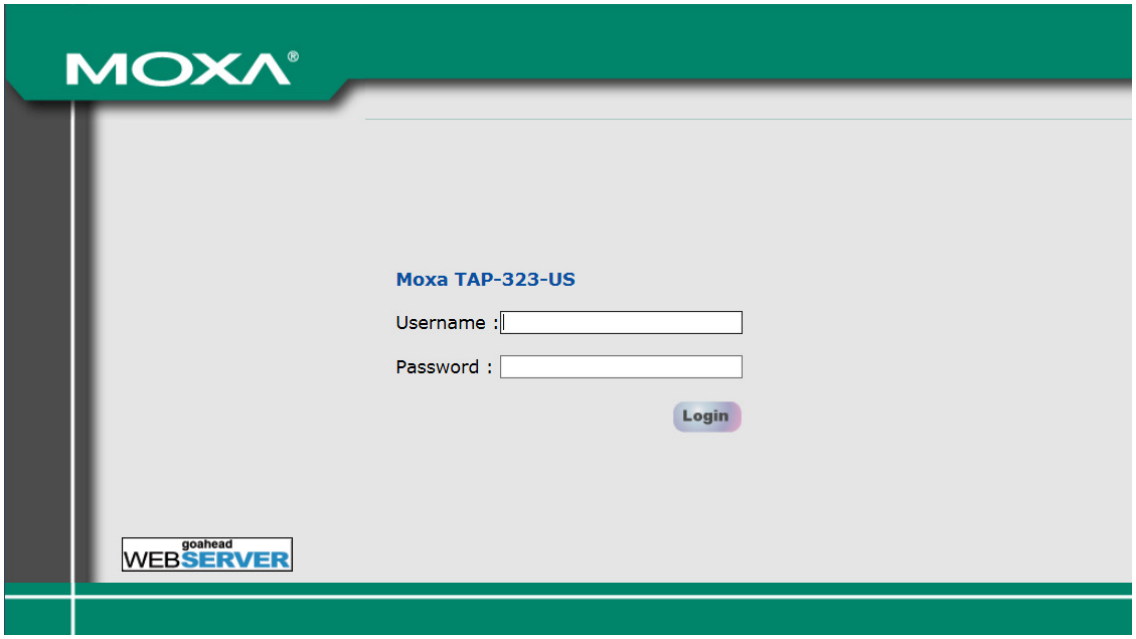
Moxa TAP-323's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions.

NOTE To use the TAP-323's management and monitoring functions from a PC host connected to the same LAN as the TAP-323, you must make sure that the PC host and TAP-323 are on the same logical subnet. Similarly, if the TAP-323 is configured for other VLAN settings, you must make sure your PC host is on the management VLAN. The Moxa TAP-323's default IP is **192.168.127.253**.

Follow the steps below to access the TAP-323's web-based console management.

1. Open your web browser (e.g., Internet Explorer) and type the TAP-323's IP address in the address field. Press **Enter** to establish the connection.

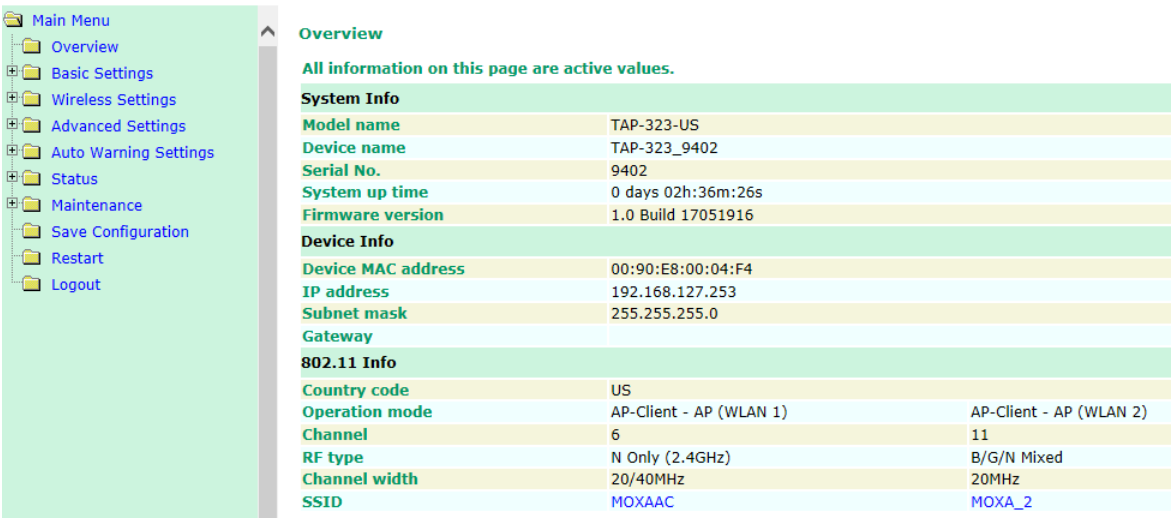
2. The Web Console Login page will open. Enter the password (User Name is set as **admin**; the default password is **moxa** if a new password has not been set.) and then click **Login** to continue.



You may need to wait a few moments for the web page to load on your computer. Note that the Model name and IP address of your TAP-323 are both displayed in the web page title. This information can help you identify multiple TAP-323 units.

You can use the menu tree on the left side of the window to open the function pages to access each of TAP-323's functions.

3. Use the menu tree on the left side of the window to open the configuration pages for the TAP-323's functions.



In the following sections, we will review each of the TAP-323's management functions in detail. You can also get a quick overview of these functions in the "Function Guide Map" section of Chapter 2.

ATTENTION

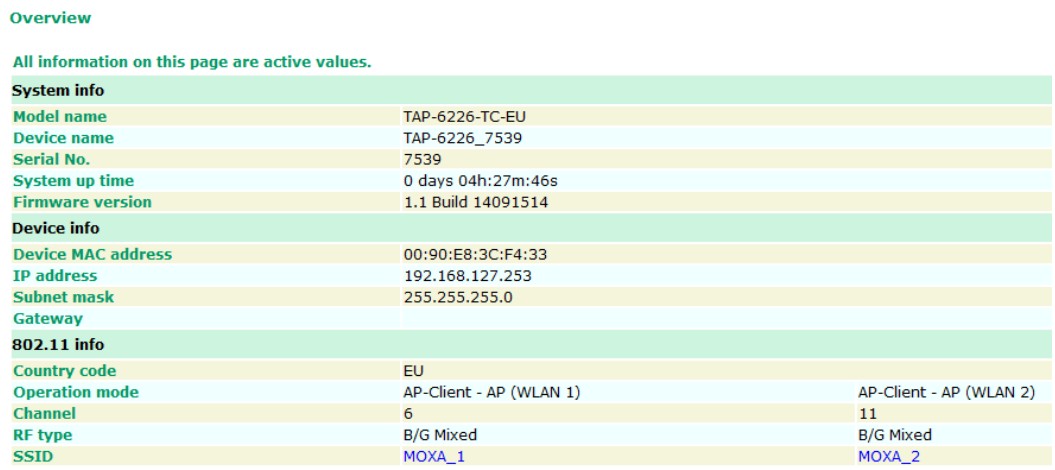
The model name of the TAP-323 is shown as TAP-323-XX where XX indicates the country code. The country code represents the TAP-323 version and which bandwidth it uses. We use **TAP-323-US** as an example in the following figures. The country code of the model name on the screen may vary if you are using a different version (band) TAP-323.

ATTENTION

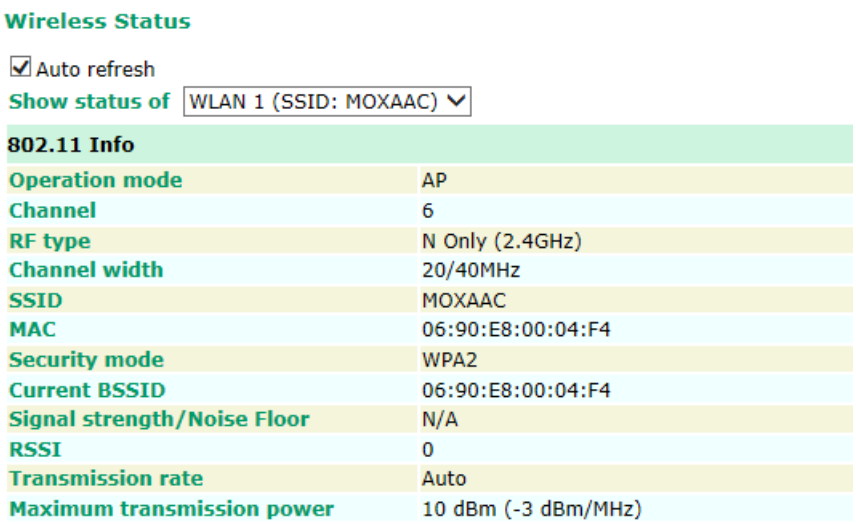
For security reasons, you will need to log back into the TAP-323 after a 3-minute time-out.

Overview

The **Overview** page summarizes the TAP-323's current status. The information is categorized into the groups: **System info**, **Device info**, and **802.11 info**.



Click on the SSID (MOXA, in this case) to display detailed information on 802.11as shown below:

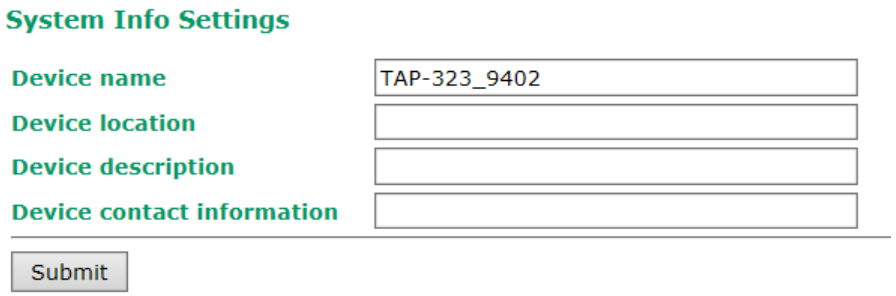


Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the TAP-323.

System Info Settings

The **System Info** items, especially ***Device name*** and ***Device description***, are displayed and included on the **Overview** page. Setting **System Info** items makes it easier to identify the different TAP-323s connected to your network.



Device name

Setting	Description	Factory Default
Max. 31 Characters	This option is useful for specifying the role or application of different TAP-323 units.	TAP-323_<Serial No. of this TAP-323>

Device location

Setting	Description	Factory Default
Max. 31 Characters	To specify the location of different TAP-323 units.	None

Device description

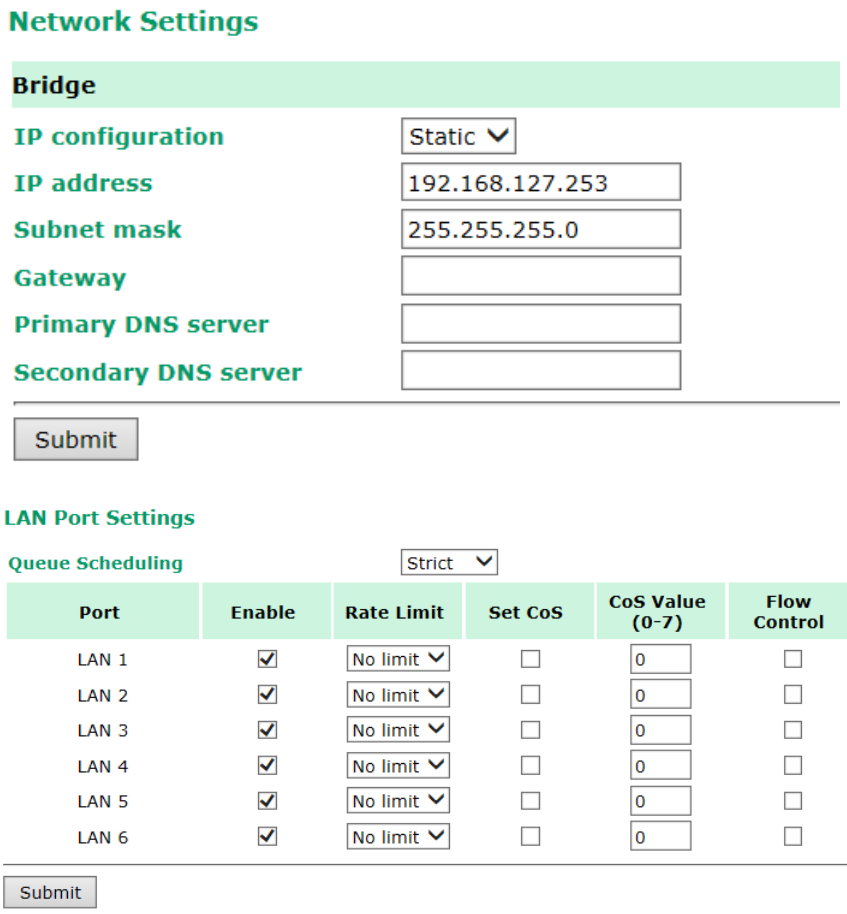
Setting	Description	Factory Default
Max. 31 Characters	Use this space to record a more detailed description of the TAP-323	None

Device contact information

Setting	Description	Factory Default
Max. 31 Characters	Use this space to record contact information of the person responsible for maintaining this TAP-323.	None

Network and LAN Port Settings

The Network and LAN Settings configuration allows you to modify the usual TCP/IP network parameters. An explanation of each configuration item is given below. The TAP-323's LAN ports also support management functions including queue scheduling, traffic rate limitation on the LAN ports for bandwidth management, and CoS (Class of Service).



IP configuration

Setting	Description	Factory Default
DHCP	The TAP-323's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the TAP-323's IP address manually.	

IP address

Setting	Description	Factory Default
TAP-323's IP address	Identifies the TAP-323 on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
TAP-323's subnet mask	Identifies the type of network to which the TAP-323 is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

Setting	Description	Factory Default
TAP-323's default gateway	The IP address of the router that connects the LAN to an outside network.	None

Primary/ Secondary DNS server

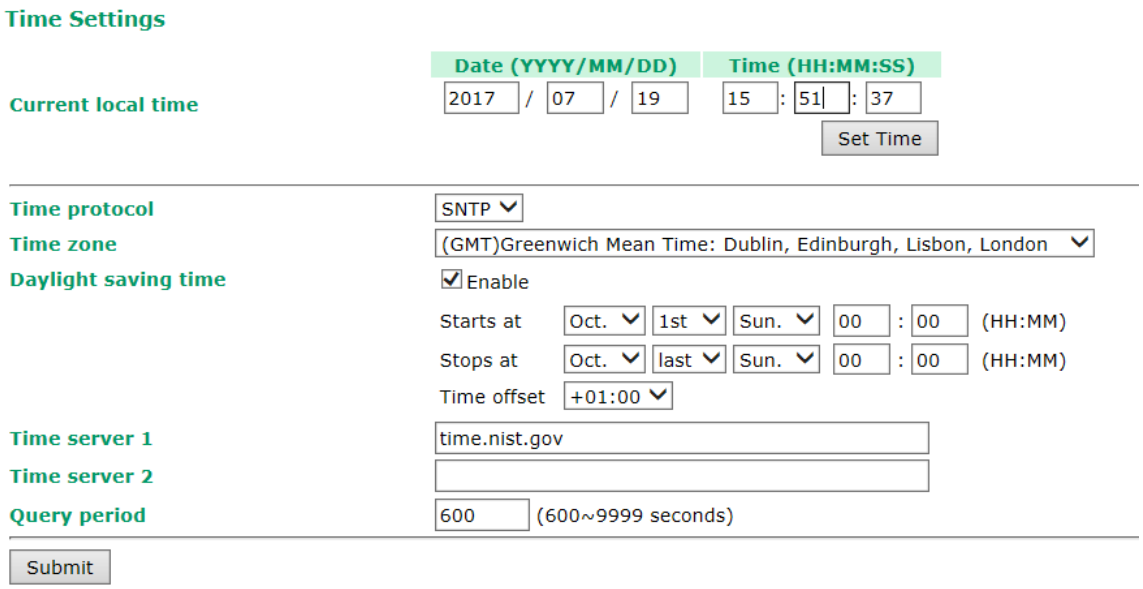
Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the TAP-323's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Queue Scheduling

Setting	Description	Factory Default
Queue Scheduling	Weight: This method services all traffic queues, with priority given to the higher priority queues. In most circumstances, the weight method gives precedence to high priority over low priority, but if the high priority traffic does not reach the link capacity, lower priority traffic is not blocked. Strict: This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The strict method always gives precedence to high priority over low priority.	Strict
Enable	Checked: Allows data transmission through the port. Unchecked: Immediately shuts off port access.	checked
Rate limit	Select the LAN traffic rate limit (% of max. throughput) for all packets, from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	No limit
Set CoS	Checked or unchecked the Moxa TAP for inspecting 802.1p CoS tags in the MAC frame to determine the priority of each frame.	unchecked
CoS Value (0~7)	Maps different CoS values to 4 different egress queues. 0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High	0
Flow Control	This setting enables or disables flow control for the port when the port's Speed is set to Auto. The final result will be determined by the Auto process between the Moxa TAP and connected devices. Checked: Enables flow control for this port when the port's Speed is set to Auto. Unchecked: Disables flow control for this port when the port's Speed is set to Auto.	Unchecked

Time Settings

The TAP-323 has a time calibration function that can update the date and time information based on an NTP server or the date and time information specified by the user.



The **Current local time** shows the TAP-323's system time when you open this web page. After you update the date and time setting, click on the **Set Time** button to activate the new date and time. An "(Updated)" string is displayed next to the date and time fields to indicate that the change is complete. Any change in the date and time setting is effective immediately and does not need a system restart.

NOTE The TAP-323 has a built-in real time clock (RTC). The RTC is a computer clock (most often in the form of an integrated circuit) that keeps track of the current time. We strongly recommend that users update the Time Settings of the TAP-323 after the initial setup is complete or when the TAP is switched on after a long-term shutdown, especially if the network does not have an Internet connection for accessing a NTP server or there is no NTP server on the LAN.

Current local time

Setting	Description	Factory Default
User adjustable time	The date and time parameters allow configuration of the local time with immediate activation. Use 24-hour format: ***yyyy/mm/dd hh:mm:ss***	None

Time zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows the conversion from GMT (Greenwich Mean Time) to the local time.	GMT

ATTENTION

Changing the time zone will automatically adjust the **Current local time**. You should configure the **Time zone** before setting the **Current local time**.

Daylight saving time

Setting	Description	Factory Default
Enable/ Disable	Daylight saving time (also known as DST or summer time) involves advancing clocks (usually 1 hour) during the summer time to provide an extra hour of daylight in the afternoon.	Disable

When **Daylight saving time** is enabled, the following parameters can be shown:

- The **Starts at** parameter allows users to enter the date that daylight saving time begins.
- The **Stops at** parameter allows users to enter the date that daylight saving time ends.
- The **Time offset parameter** indicates how many hours forward the clock should be advanced.

Time server 1/2

Setting	Description	Factory Default
The 1st/2nd time server IP/Name	IP or Domain address of NTP time server. The 2nd time will be used if the 1st NTP server fails to connect.	time.nist.gov

Query period

Setting	Description	Factory Default
Query period time (1 to 9999 seconds)	This parameter determines how often the time is updated from the NTP server.	600 (seconds)

Wireless Settings

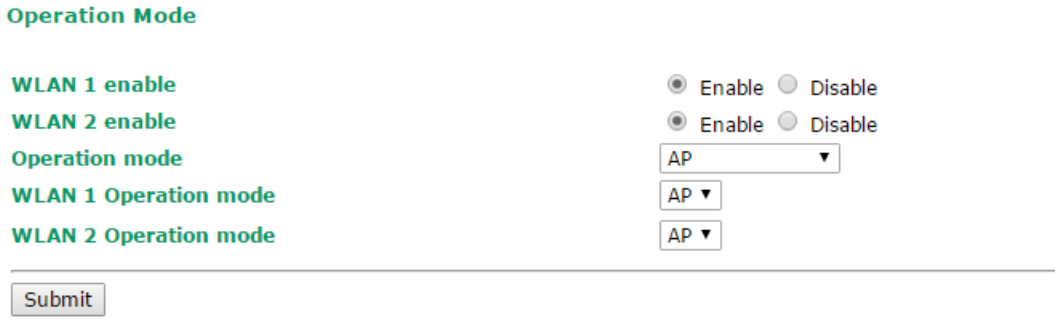
The essential settings for wireless networks are presented in this function group. You must configure the settings correctly before establishing your wireless network.

Operation Mode

The essential settings for wireless networks are presented in the wireless settings function group. You must configure these settings correctly before you establish your wireless network. Familiarize yourself with the following terms before starting the configuration process:

AP

In a wireless local area network (WLAN), an access point is a station that transmits and receives data.



Matching Table for AP's WLANs:

WLAN 1	WLAN 2	Allowable Setting
AP	AP	Allow

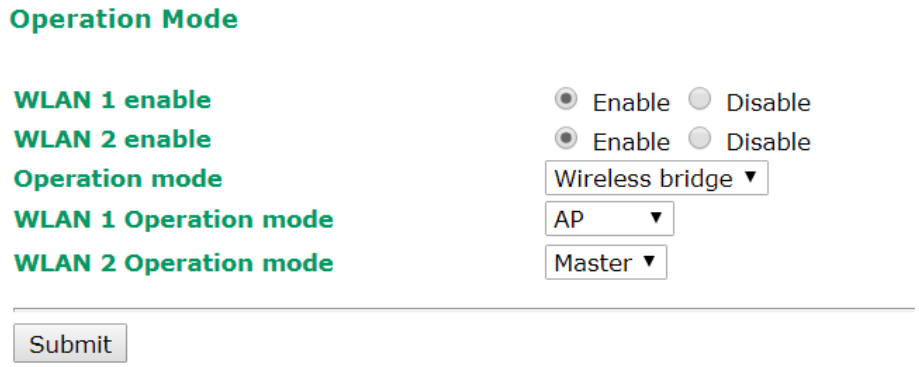
NOTE TAP-323 units are meant to be used as trackside access points and hence the client operation mode is not supported.

Wireless Bridge

A bridge is a network component that connects two networks. The TAP-323's bridge operation is based on the AP (**Master**) and Client (**Slave**) concept. Both sides of the connection must have the same RF type, SSID, and security settings.

For single RF mesh networks, we can use WDS to establish a static bridge link. In this case, the APs at both ends of the WDS link must be configured manually with each other's MAC addresses. The performance of a single RF bridge will be poor if more nodes are added.

The TAP-323's dual RF bridge concept is different from using a single RF, because the TAP-323 has dual RFs that offer users a cascade link to bridge the two ends without narrowing down the throughput.



WLAN 1/WLAN 2 Enable

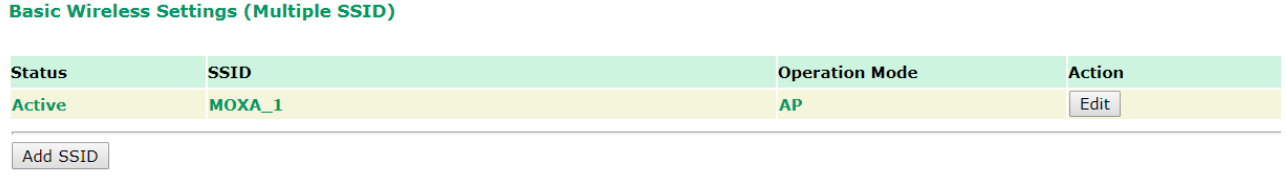
Setting	Description	Factory Default
WLAN1 enable	Turn on/off the WLAN 1 radio by selecting Enable or Disable	Enable
WLAN2 enable	Turn on/off the WLAN 2 radio by selecting Enable or Disable	

WLAN 1/WLAN 2 Operation mode

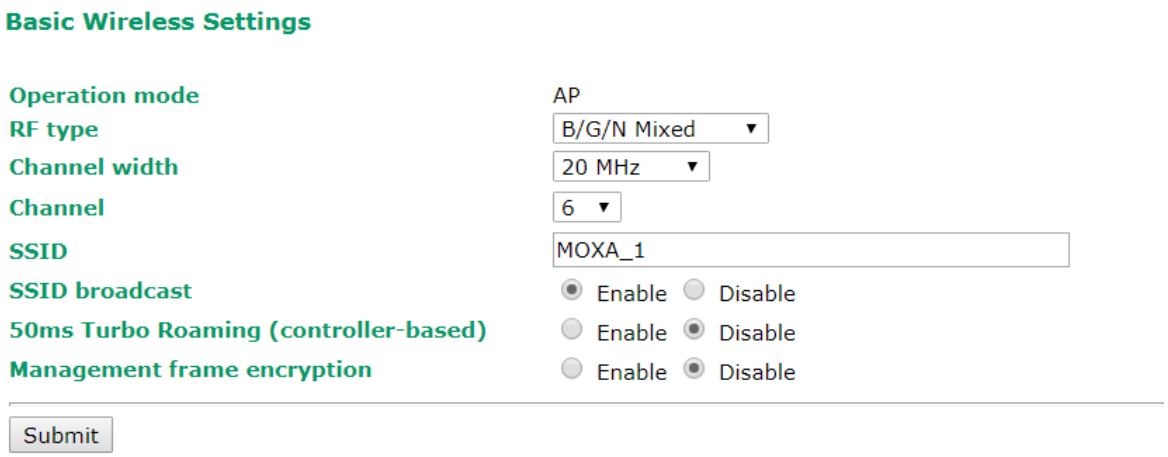
Setting	Description	Factory Default
Master	Master mode can build a connection with a Slave that has the same RF type, SSID, and security settings.	AP for WLAN 1 Master for WLAN 2
Slave	Slave mode can build a connection with a master that has the same RF type, SSID, and security settings.	
AP	The most common mode used by a TAP-323 wherein it plays the role of a wireless AP	

Basic Wireless Settings (Multiple SSIDs)

You can add new SSIDs or edit existing ones in the WLAN Basic Setting Selection panel. You can configure up to 9 SSIDs for a TAP and configure each SSID differently. An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. All of the SSIDs that you configure for an AP are active at the same time. That is, client devices can use any of the SSIDs to associate with the AP.



To create an SSID for your TAP, click on **Add SSID**. To edit an existing SSID and assign different configuration settings to it, click on the Edit button corresponding to the SSID. A configuration panel is displayed as follows:



RF type

Setting	Description	Factory Default
2.4 GHz		
B	Only supports the IEEE 802.11b standard	B/G/N Mixed
G	Only supports the IEEE 802.11g standard	
B/G Mixed	Supports IEEE 802.11b/g standards, but 802.11g might operate at a slower speed when 802.11b clients are on the network	
G/N Mixed	Supports IEEE 802.11g/n standards, but 802.11n might operate at a slower speed if 802.11g clients are on the network	
B/G/N Mixed	Supports IEEE 802.11b/g/n standards, but 802.11g/n might operate at a slower speed if 802.11b clients are on the network	
N Only (2.4GHz)	Only supports the 2.4 GHz IEEE 802.11n standard	
5 GHz		
A	Only supports the IEEE 802.11a standard	
A/N Mixed	Supports IEEE 802.11a/n standards, but 802.11n may operate at a slower speed if 802.11a clients are on the network	
N Only (5GHz)	Only supports the 5 GHz IEEE 802.11n standard	

Channel (for AP mode only)

Setting	Description	Factory Default
The available channels vary with the RF type setting	The channel on which the TAP should operate. The TAP-323 plays the role of a wireless AP here.	6 (in B/G/N Mixed mode)

Channel Width (for any 11N RF type only)

Setting	Description	Factory Default
20 MHz	Select the channel width.	20 MHz
20/40 MHz	If you are not sure, use the 20/40 MHz (Auto) option	

Channel bonding

If you have selected **20/40 MHz only** in the **Channel Width** setting, this setting will automatically set the channel based on the **Channel** setting.

SSID

Setting	Description	Factory Default
Maximum of 31 characters	The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other.	MOXA

SSID broadcast (for AP mode only)

Setting	Description	Factory Default
Enable/Disable	Use this setting to specify if the SSID can be broadcast or not	Enable

Management frame encryption

Setting	Description	Factory Default
Enable/Disable	Enables management frame encryption to protect your wireless network from DoS attacks. This function only works with Moxa's TAP series.	Disable

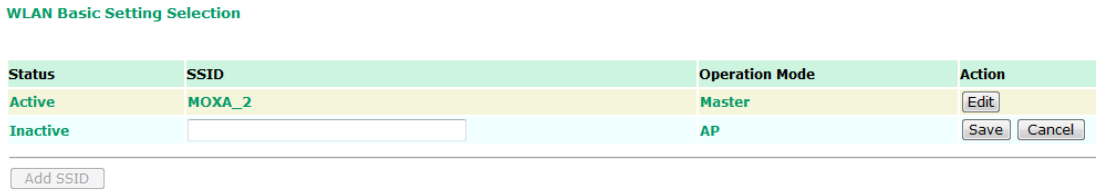
50ms Turbo Roaming (controller-based)

Setting	Description	Factory Default
Enable/Disable	Determines whether or not the TAP-323 supports 50 ms roaming. This function only works with the WAC-1001, WAC-2004, and TAP series.	Disable

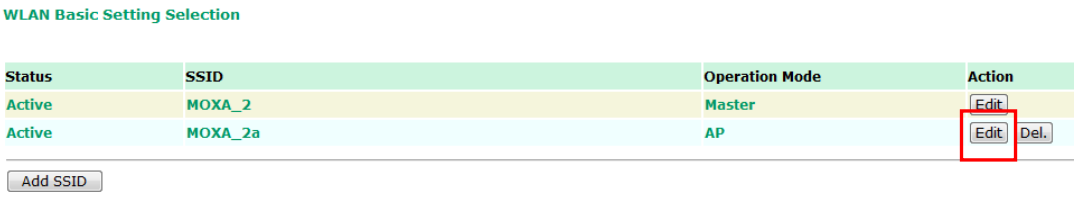
Wireless Bridge Mode's Master

You can change this AP's functionality to Enable or Disable on the basic wireless settings page. If AP functionality is set to Enable, the Status will appear as **Active**, which means that the WLAN is ready to operate in the selected operation mode. For AP functionality settings, click on Edit, as described below.

Click on **Add SSID** and enter a unique SSID to add a virtual SSID to the Master interface to service other clients.



Click on **Edit** to configure the virtual AP interface.

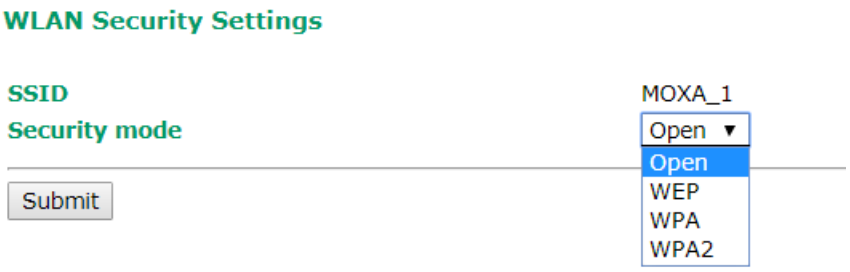


WLAN Security Settings

The TAP-323 provides four standardized wireless security modes: **Open**, **WEP** (Wired Equivalent Privacy), **WPA** (Wi-Fi Protected Access), and **WPA2**. Several security modes are available in the TAP-323 by selecting ***Security mode*** and ***WPA type***:

- **Open**: No authentication, no data encryption.
- **WEP**: Static WEP (Wired Equivalent Privacy) keys must be configured manually.
- **WPA/WPA2-Personal**: Also known as WPA/WPA2-PSK. You will need to specify the Pre-Shared Key in the Passphrase field, which will be used by the TKIP or AES engine as a master key to generate keys that actually encrypt outgoing packets and decrypt incoming packets.
- **WPA/WPA2-Enterprise**: Also called WPA/WPA2-EAP (Extensible Authentication Protocol). In addition to device-based authentication, WPA/WPA2-Enterprise enables user-based authentication via IEEE 802.1X.

The TAP-323 can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.



Security mode

Setting	Description	Factory Default
Open	No authentication	Open
WEP	Static WEP is used	
WPA	WPA is used	
WPA2	Fully supports IEEE 802.11i with "TKIP/AES + 802.1X"	

Open

For security reasons, you should NOT set security mode to Open System, since authentication and data encryption are NOT performed in Open System mode.

WEP (Only for Legacy Mode)

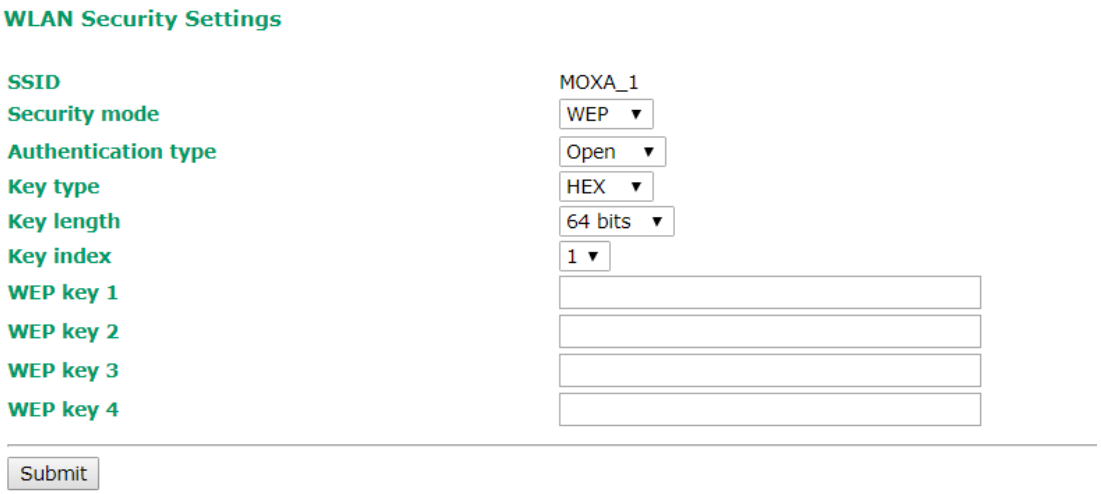
NOTE Moxa includes **WEP** security mode only for legacy purposes. **WEP** is highly insecure and is considered fully deprecated by the Wi-Fi alliance. We do not recommend the use of WEP security under any circumstances.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption to maintain confidentiality. **Shared** (or **Shared Key**) authentication type is used if WEP authentication and data encryption are both needed. Normally, **Open** (or **Open System**) authentication type is used when WEP data encryption is run with authentication.

When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The TAP-323 provides 4 entities of WEP key settings that can be selected to use with **Key index**.

The selected key setting specifies the key to be used as a send-key for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as receive-keys to decrypt traffic from the wireless client side to the AP side.

The WEP key can be presented in two **Key types**, HEX and ASCII. Each ASCII character has 8 bits, so a 40-bit (or 64-bit) WEP key contains 5 characters, and a 104-bit (or 128-bit) key has 13 characters. In hex, each character uses 4 bits, so a 40-bit key has 10 hex characters, and a 128-bit key has 26 characters.



Authentication type

Setting	Description	Factory Default
Open	Data encryption is enabled, but no authentication.	Open
Shared	Data encryption and authentication are both enabled.	

Key type

Setting	Description	Factory Default
HEX	Specifies WEP keys in hex-decimal number form	HEX
ASCII	Specifies WEP keys in ASCII form	

Key length

Setting	Description	Factory Default
64 bits	Uses 40-bit secret keys with 24-bit initialization vector	64 bits
128 bits	Uses 104-bit secret key with 24-bit initialization vector	

Key index

Setting	Description	Factory Default
1-4	Specifies which WEP key is used	Open

WEP key 1-4

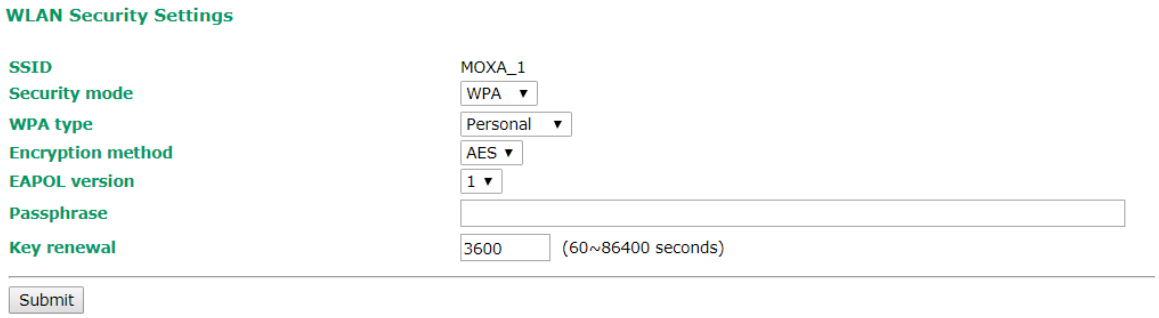
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13 chars **HEX type:** 64 bits: 10 HEX chars 128 bits: 26 HEX chars	A string that can be used as a WEP seed for an RC4 encryption engine.	None

WPA/WPA2-Personal

WPA (Wi-Fi Protected Access) and WPA2 represent significant improvements over the WEP encryption method. WPA is a security standard based on 802.11i draft 3, while WPA2 is based on the fully ratified version of 802.11i. The initial vector is transmitted, encrypted, and enhanced with its 48 bits, twice as long as WEP. The key is regularly changed so that true session is secured.

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The TAP-323 also supports AES algorithms in WPA and WPA2 for better compatibility.

Personal versions of WPA/WPA2, also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of encrypting a wireless connection for high confidentiality. A ***Passphrase*** is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complicated and as long as possible. There must be at least 8 ASCII characters in the Passphrase, and it could go up to 63. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.



WPA Type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP**	Temporal Key Integrity Protocol is enabled	AES
AES	Advance Encryption System is enabled	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used. Note: This option is available in AP or Master mode only, and cannot support AES-enabled clients.	

** This option is only available for legacy mode in APs and does not support AES-enabled clients.*

*** This option is only available with 802.11a/b/g standard*

Passphrase

Setting	Description	Factory Default
8 to 63 characters	Master key to generate keys for encryption and decryption	None

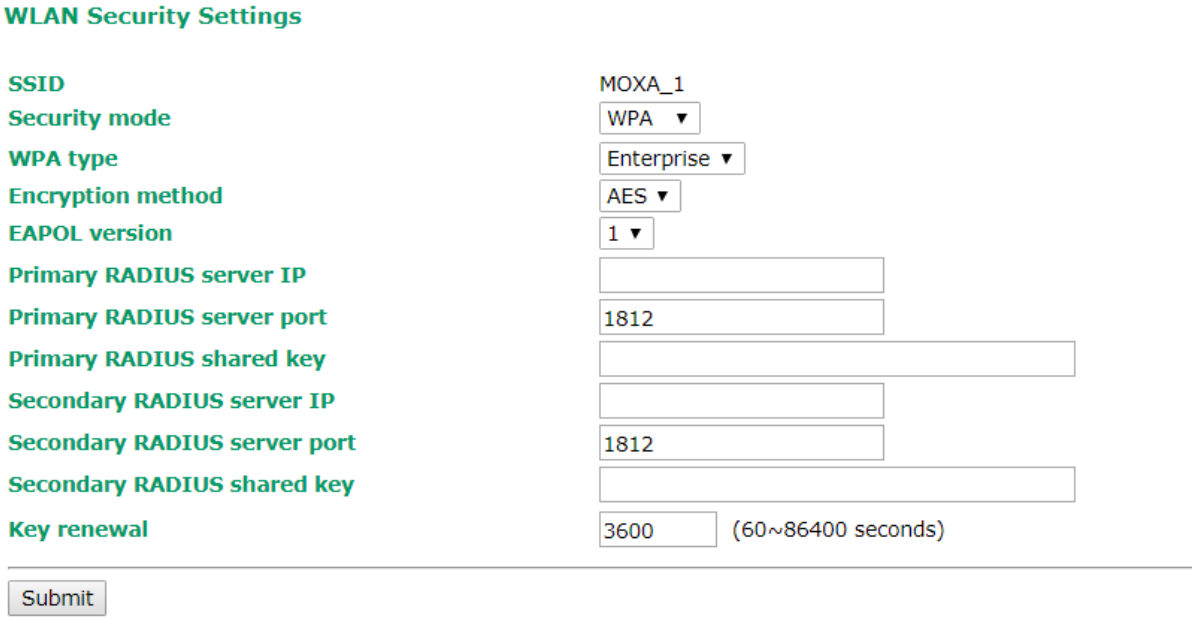
Key renewal (for AP or Master Mode only)

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 day)	Specifies the time period of group key renewal	3600 (seconds)

NOTE The **key renewal** value dictates how often the wireless AP encryption keys should be changed. The security level is generally higher if you set the key renewal value to a shorter number, which forces the encryption keys to be changed more frequently. The default value is 3600 seconds (6 minutes). Longer time periods can be considered if the line is not very busy.

WPA/WPA2-Enterprise (for AP or Master Mode)

By selecting ***WPA type*** as **Enterprise**, you can use **EAP** (*Extensible Authentication Protocol*), a framework authentication protocol used by 802.1X to provide network authentication. In these Enterprise-level security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1X functionality is enabled in WPA /WPA2. The IEEE 802.1X protocol also offers the possibility of carrying out efficient connection authentication on a large-scale network. In this case, it is not necessary to exchange keys or pass phrases.



WPA Type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP**	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advance Encryption System is enabled	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used.	

* This option is available only for legacy mode in APs and does not support AES-enabled client.

** This option is only available with 802.11a/b/g standard

Primary/Secondary RADIUS server IP

Setting	Description	Factory Default
The IP address of RADIUS server	Specifies the delegated RADIUS server for EAP	None

Primary/Secondary RADIUS port

Setting	Description	Factory Default
Port number	Specifies the port number of the delegated RADIUS server	1812

Primary/Secondary RADIUS shared key

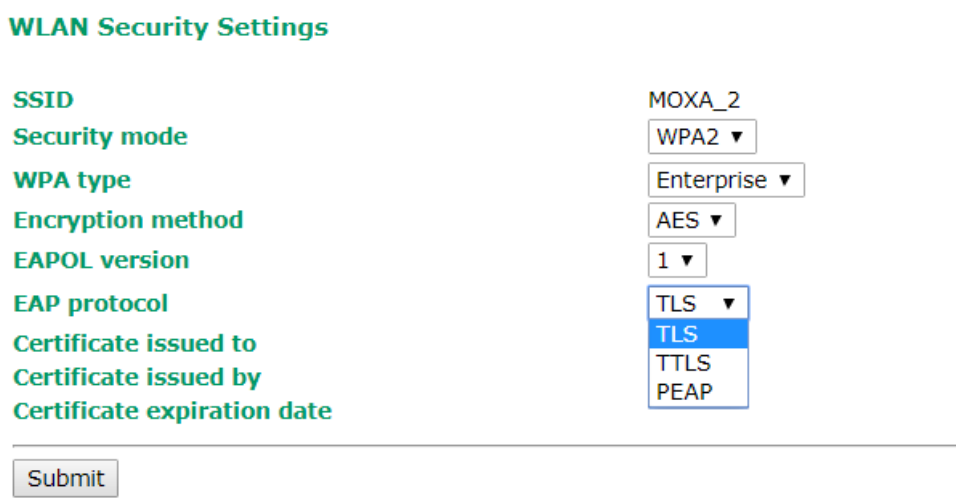
Setting	Description	Factory Default
Max. 31 characters	The secret key shared between AP and RADIUS server	None

Key renewal

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 day)	Specifies the time period of group key renewal	3600 (seconds)

WPA/WPA2-Enterprise (for Slave mode)

In a slave role, the TAP-323 can support three EAP methods (or ***EAP protocols***): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA-Enterprise settings on the AP side.



Encryption method

Setting	Description	Factory Default
TKIP**	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advance Encryption System is enabled	

** This option is only available with 802.11a/b/g standard

EAP Protocol

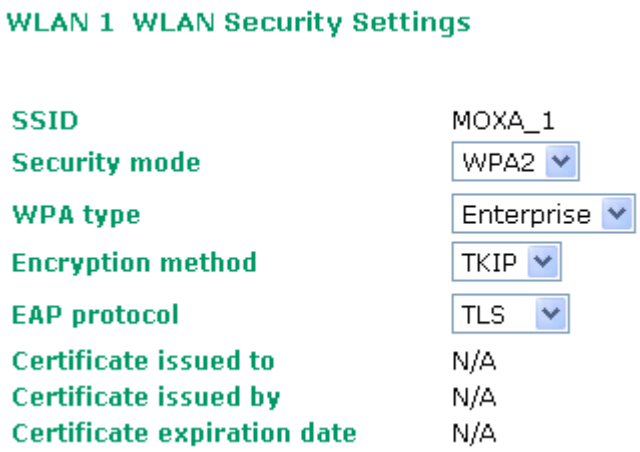
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

Before choosing the EAP protocol for your WPA/WPA2-Enterprise settings on the client end, please contact the network administrator to make sure the system supports the protocol on the AP end. Detailed information on these three popular EAP protocols is presented in the following sections:

EAP-TLS

TLS is the standards-based successor to Secure Socket Layer (SSL). It can establish a trusted communication channel over a distrusted network. TLS provides mutual authentication through certificate exchange. EAP-TLS is also secure to use. You are required to submit a digital certificate to the authentication server for validation, but the authentication server must also supply a certificate.

You can use **WLAN 1/2 → WLAN Certificate Settings** to import your WLAN certificate and enable EAP-TLS on the client end.



You can check the current certificate status in ***Current Status*** if it is available.

Certificate issued to: Shows the certificate user.
Certificate issued by: Shows the certificate issuer.
Certificate expiration date: Indicates when the certificate expires

EAP-TTLS

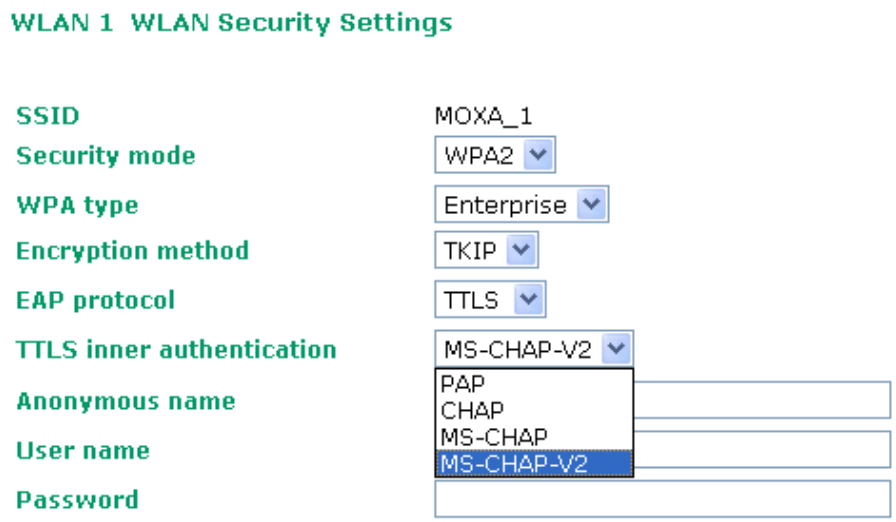
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than create a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called "legacy authentication methods."

TTLS and PEAP work in a similar way. First, they establish a TLS tunnel, like EAP-TLS, and validate whether the network is trustworthy with digital certificates on the authentication server. This step is run to establish a tunnel that protects the next step (or "inner" authentication) so it is sometimes referred to as the "outer" authentication. Then the TLS tunnel is used to encrypt an older authentication protocol that authenticates the user for the network.

As you can see, digital certificates are still needed for the outer authentication in a simplified form. Only a small number of certificates are required, which can be generated by a small certificate authority. Certificate reduction makes TTLS and PEAP much more popular than EAP-TLS.

The TAP-323 provides some non-cryptographic EAP methods including **PAP**, **CHAP**, **MS-CHAP**, and **MS-CHAP-V2**. These EAP methods are not recommended for direct use on wireless networks. However, they may be useful as inner authentication methods with TTLS or PEAP.

Because the inner and outer authentications can use distinct user names in TTLS and PEAP, you can use an anonymous user name for the outer authentication, while the true user name is shown only through the encrypted channel. Remember, not all client software supports anonymous altercation. Confirm this with the network administrator before you enable identity hiding in TTLS and PEAP.



TTL Inner Authentication

Setting	Description	Factory Default
PAP	Password Authentication Protocol is used	MS-CHAP-V2
CHAP	Challenge Handshake Authentication Protocol is used	
MS-CHAP	Microsoft CHAP is used	
MS-CHAP-V2	Microsoft CHAP version 2 is used	

Anonymous

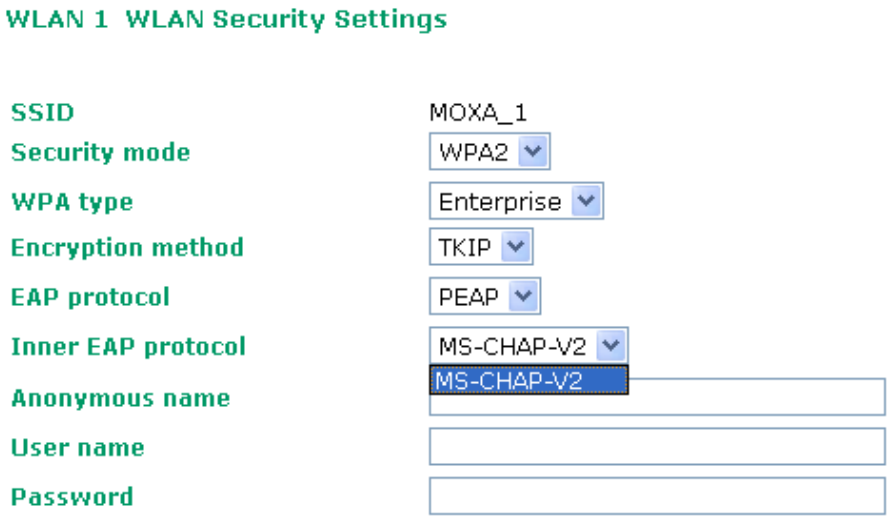
Setting	Description	Factory Default
Max. 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

PEAP

There are a few differences in the inner authentication procedures for TTLS and PEAP. TTLS uses the encrypted channel to exchange attribute-value pairs (AVPs), while PEAP uses the encrypted channel to start a second EAP exchange inside of the tunnel. The TAP-323 provides **MS-CHAP-V2** merely as an EAP method for inner authentication.



Inner EAP protocol

Setting	Description	Factory Default
MS-CHAP-V2	Microsoft CHAP version 2 is used	MS-CHAP-V2

Anonymous

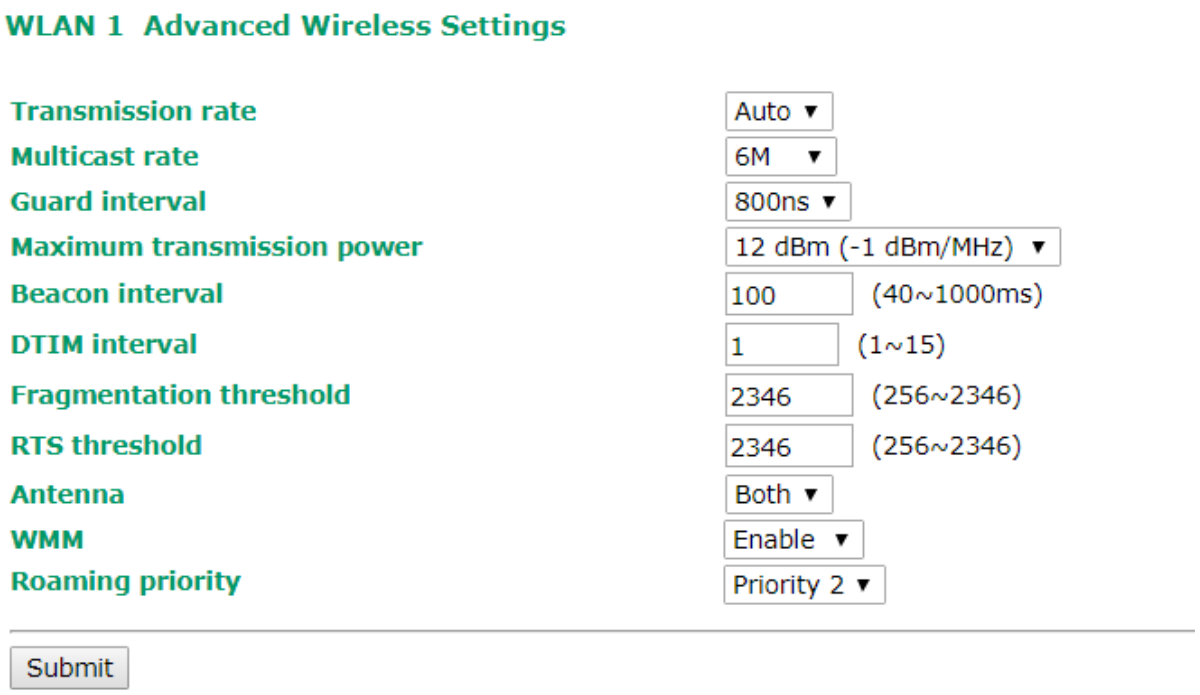
Setting	Description	Factory Default
Max. 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

Advanced Wireless Settings

Additional wireless-related parameters are presented in this section to help you set up your wireless network in detail.



Transmission Rate (for A, B, G, B/G mixed, and N modes only)

Setting	Description	Factory Default
Auto	The TAP-323 will sense and adjust the data rate automatically	Auto
Available rates	Users can manually select a target transmission data rate	

Multicast Rate (for AP mode only)

Setting	Description	Factory Default
Multicast rate (6-54 M)	You can set a fixed multicast rate for the transmission of broadcast and multicast packets on a per-radio basis. This parameter can be useful in an environment where multicast video streaming is occurring in the wireless medium, provided that the wireless clients are capable of handling the configuration rate.	6 M

Guard Interval

Setting	Description	Factory Default
Guard Interval (6-54 M)	Guard interval is used to ensure that distinct transmissions do not interfere with one another. You can select the guard interval manually for Wireless-N connections. The two options are Short (400 ns) and Long (800 ns). NOTE: This function can be modified in N mode only	800 ns.

Multicast Rate (for AP mode only)

Setting	Description	Factory Default
Multicast rate (6-54 M)	You can set a fixed multicast rate for the transmission of broadcast and multicast packets on a per-radio basis. This parameter can be useful in an environment where multicast video streaming is occurring in the wireless medium, provided that the wireless clients are capable of handling the configuration rate.	6 M

Maximum Transmission Power

Setting	Description	Factory Default
Available Power	Users can manually select a target power to mask max output power. Because different transmission rates might have their own max output power, please reference product datasheet. The available setting is from 3 to 26.dBm/MHz, which gives the density of the transmission power in channel width.	12 dBm (-1 dBm/MHz)

NOTE Most countries define a limit for the Equivalent Isotropically Radiated Power (EIRP) for an RF transmitting system. The EIRP should not exceed the allowed value. EIRP = transmission power + antenna gain (dBi).

Beacon Interval (for AP and Master mode only)

Setting	Description	Factory Default
Beacon Interval (40 to 1000 ms)	This value indicates the frequency interval of the beacon	100 (ms)

DTIM Interval (for AP and Master mode only)

Setting	Description	Factory Default
Data Beacon Rate (1 to 15)	This value indicates how often the TAP-323 sends out a Delivery Traffic Indication Message	1

Fragment threshold

Setting	Description	Factory Default
Fragment Length (256 to 2346)	This parameter specifies the maximum size a data packet must be before splitting and creating a new packet	2346

RTS threshold

Setting	Description	Factory Default
RTS/CTS Threshold (256-2346)	Determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication	2346

Antenna

Setting	Description	Factory Default
A/B/Both	Specifies the output antenna port. Setting Antenna to Auto allows 2x2 MIMO communication under 802.11n and 2T2R* communication in legacy 802.11a/b/g modes.	Both

*Note: Different from 802.11n's multiple spatial data stream (2x2 MIMO), which doubles the throughput. 2T2R transmits/receives the same piece of data on both antenna ports.

WMM

WMM is a QoS standard for WLAN traffic. Voice and video data will be given priority bandwidth when enabled with WMM supported wireless clients.

NOTE: This setting can be enabled/disabled only in A, B, and B/G Mixed modes. For N, G/N Mixed, B/G/N Mixed, and A/N Mixed modes, this setting is enabled by default.

<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>Enable/Disable</td><td>WMM is a Quality of Service standard for WLAN traffic. Voice and video data will be given priority bandwidth when enabled with WMM supported wireless clients.

<table>
<tr><th>802.1p Priority</th><th>WMM Access Category</th></tr>
<tr><td>1</td><td rowspan="2">Background</td></tr>
<tr><td>2</td></tr>
<tr><td>0</td><td rowspan="2">Best effort</td></tr>
<tr><td>3</td></tr>
<tr><td>4</td><td rowspan="2">Video</td></tr>
<tr><td>5</td></tr>
<tr><td>6</td><td rowspan="2">Video</td></tr>
<tr><td>7</td></tr>
</table>
</td><td>Disable</td></tr>
</table>

NOTE **READ THIS BEFORE CHANGING THE DFS SETTING**

DFS (Dynamic Frequency Selection) is a mechanism to allow unlicensed wireless devices to share spectrum with existing radar systems by detecting radar systems and avoid causing interference with them.

Roaming Priority (only for AP mode)

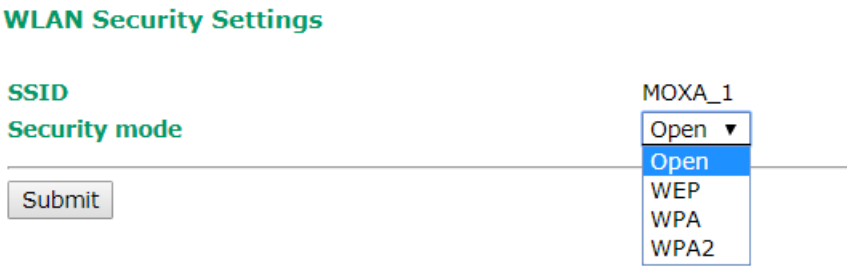
Setting	Description	Factory Default
Priority 1/2	The roaming priority should be set according to the radio deployment method along the trackside. Priority 1: radios along the trackside are deployed with leaky feeder-like coverage patterns. Priority 2: radios along the trackside are deployed with open air radiating antennas. Due to the difference in coverage pattern between different deployment scenarios, properly selecting the roaming priority will impact the roaming performance.	Priority 2

RF Index

Setting	Description	Factory Default
RF Index 1 /RF Index 2	In an L3 roaming scenario, trackside APs can be arranged in different VLAN gateways within different subnets. The RF index setting identifies the AP within a particular VLAN gateway.	RF Index 1

WLAN Certification Settings (for EAP-TLS in Slave mode only)

When EAP-TLS is used, a WLAN Certificate will be required at the client end to support WPA/WPA2-Enterprise. The TAP-323 can support the **PKCS #12**, also known as *Personal Information Exchange Syntax Standard*, certificate formats that define file formats commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.



Current Status displays information for the current WLAN certificate, which has been imported into the TAP-323. Nothing will be shown if a certificate is not available.

Certificate issued to: shows the certificate user
Certificate issued by: shows the certificate issuer
Certificate expiration date: indicates when the certificate becomes invalid

You can import a new WLAN certificate in ***Import WLAN Certificate*** by following these steps, in order:

1. Input the corresponding password (or key) in the **Certificate private password** field, and then click **Submit** to set the password.
2. The password will be displayed in the Certificate private password field. Click on the **Browse** button in ***Select certificate/key file*** and select the certificate file.
3. Click **Upload Certificate File** to import the certificate file. If the import succeeds, you can see the information uploaded in ***Current Certificate***. If it fails, you may need to return to step 1 to set the password correctly and then import the certificate file again.

NOTE The WLAN certificate will remain after the TAP-323 reboots. Even though it is expired, it can still be seen on Current Certificate.

WAC Settings (AP Mode Only)

Controller-based Turbo Roaming function is automatically enabled when you enable the **50ms Turbo Roaming (controller-based)** option on the **Wireless Settings** > **WLAN** > **Basic Wireless Settings** > **Edit** page. The **Primary WAC IP address**, **Backup WAC IP address**, and **Roaming domain fields** are displayed.

Primary WAC IP address

Setting	Description	Factory Default
IP address	Enter the IP address of the primary WAC-1001	None

Backup WAC IP address

Setting	Description	Factory Default
IP address	Enter the IP address of the backup WAC-1001	None

Roaming domain

Setting	Description	Factory Default
6 Hex characters	Specifies the area served by the WAC-1001/2004. All related controllers, APs, and clients use this as identification to work and communicate with each other	None

Advanced Settings

Several advanced functions are available to increase the functionality of your TAP-323 and wireless network system. A VLAN is a collection of clients and hosts grouped together as if they were connected to the broadcast domains in a layer-2 network. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the TAP-323 can support STP/RSTP protocol to increase reliability across the entire network, and SNMP support can make network management easier.

Using Virtual LAN

Setting up Virtual LANs (VLANs) on your AWK series increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The Virtual LAN (VLAN) Concept

What is a VLAN?

A virtual LAN, or VLAN, is a collection of hosts with a common set of requirements. The hosts communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows you to group end stations together even if they are not connected to the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs can extend as far as the access point signal can reach. Clients can be segmented into wireless sub-networks based on SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

Benefits of VLANs

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
- Improve network performance and reduce latency
- Increase security
- Secure networks limit members to using resources on their own VLAN
- Clients can roam without compromising security

VLAN Workgroups and Traffic Management

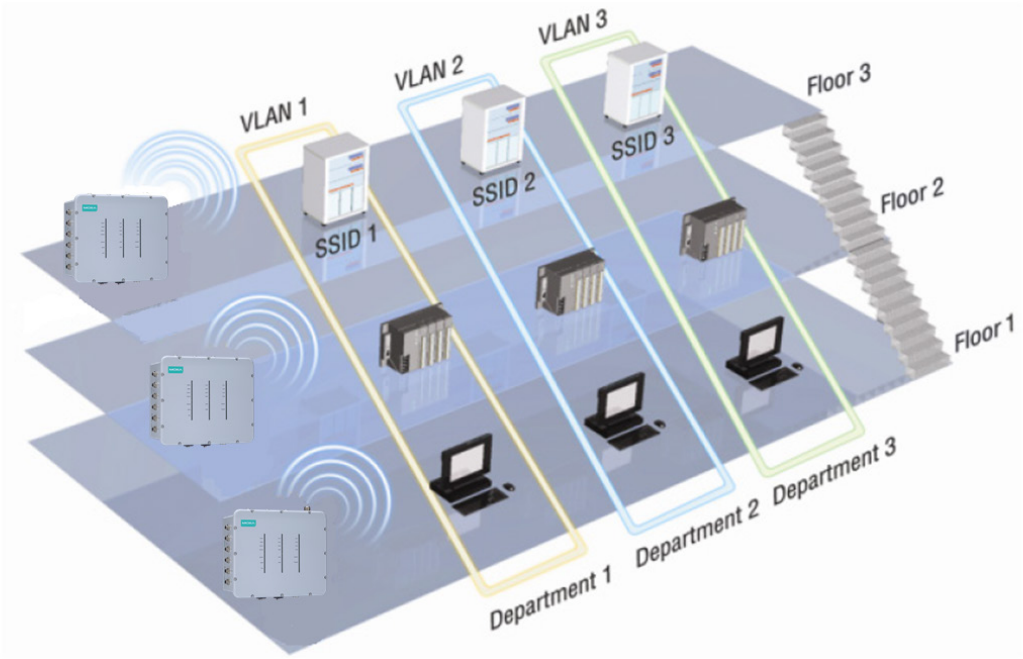
The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN, eliminating unnecessary traffic on the wireless LAN, conserving bandwidth, and maximizing throughput.

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a department workgroup; for example, one VLAN could be used for a marketing department and the other for a human resources department.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as marketing or human resources, depending on which wireless client received it. The AP would insert VLAN headers or "tags" with identifiers into the packets transmitted on the wired backbone to a network switch.

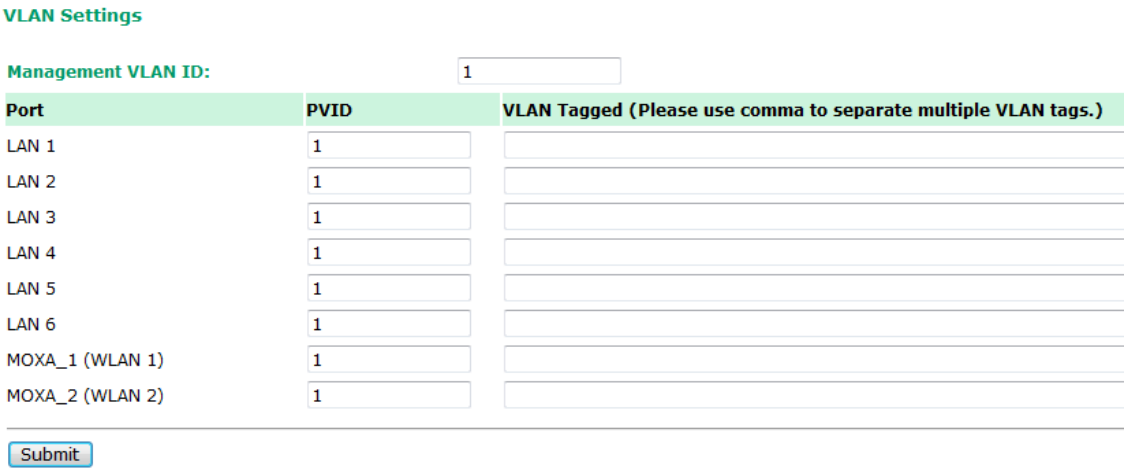
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resources department could be restricted to a gateway that allowed access to only the Internet. A member of the human resources department could send and receive email and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.



Configuring a Virtual LAN

VLAN Settings

To configure a VLAN on the AWK, use the VLAN Settings page to configure the ports.



Management VLAN ID

Setting	Description	Factory Default
VLAN ID (ranges from 1 to 4094)	Set the management VLAN of this AWK.	1

Port

Type	Description	Trunk Port
LAN	This port is the LAN port on the AWK.	Yes
WLAN	This is a wireless port for the specific SSID. This field will refer to the SSID that you have created. If more SSIDs have been created, new rows will be added.	

Port PVID

Setting	Description	Factory Default
VLAN ID ranging from 1 to 4094	Set the port's VLAN ID for devices that connect to the port. The port can be a LAN port or WLAN ports.	1

VLAN Tagged

Setting	Description	Factory Default
A comma-separated list of VLAN IDs. Each VLAN ID must be between 1 and 4094.	Specify which VLANs can communicate with this specific VLAN.	(Empty)

NOTE The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN ID, then those wireless clients who are members of that VLAN will have AP management access.
CAUTION: Once a VLAN Management ID is configured and is equivalent to one of the VLAN IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership to those with legitimate access to the AP.

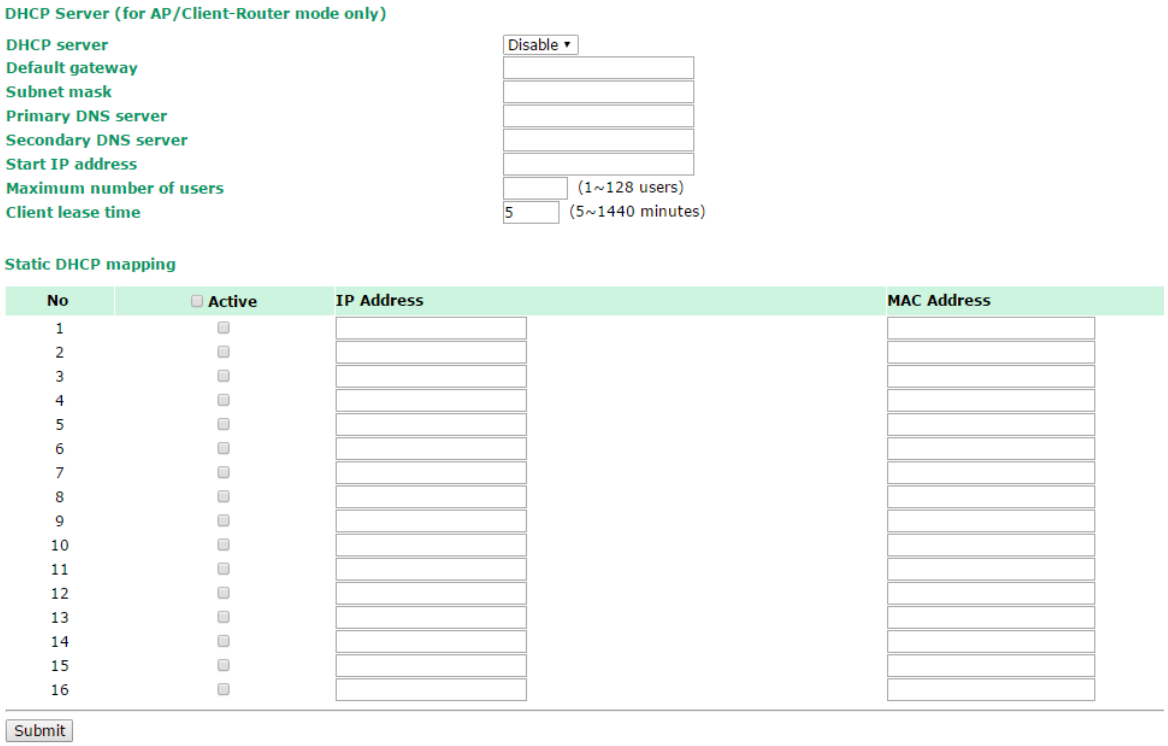
DHCP Server (for AP operation mode only)

DHCP (Dynamic Host Configuration Protocol) is a networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

The TAP-323 can act as a simplified DHCP server and easily assign IP addresses to your wireless clients by responding to the DHCP requests from the client ends. The IP-related parameters you set on this page will also be sent to the client.

You can also assign a static IP address to a specific client by entering its MAC address. The TAP-323 provides a **Static DHCP mapping** list with up to 16 entities. Remember to check the **Active** check box for each entity to activate the setting.

You can check the IP assignment status under **Status → DHCP Client List**.



DHCP server (AP only)

Setting	Description	Factory Default
Enable	Enables TAP-323 as a DHCP server	Disable
Disable	Disables the DHCP server function	

Default gateway

Setting	Description	Factory Default
IP address of a default gateway	The IP address of the router that connects to an outside network	None

Subnet mask

Setting	Description	Factory Default
subnet mask	Identifies the type of sub-network (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network)	None

Primary/ Secondary DNS server

Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can use URLs. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Start IP address

Setting	Description	Factory Default
IP address	Indicates the starting IP address that the TAP-323 can assign.	None

Maximum number of users

Setting	Description	Factory Default
1 to 128 users	Specifies how many IP addresses can be assigned continuously	None

Client lease time

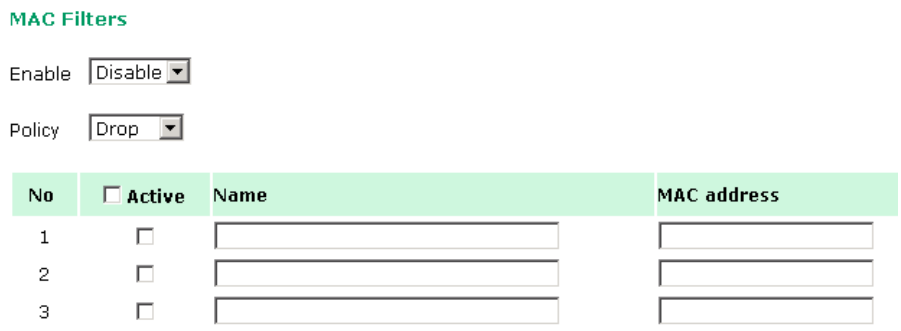
Setting	Description	Factory Default
5 – 1440 minutes	The lease time for which an IP address is assigned. The IP address may expire after the lease time is reached.	5 minutes

Packet Filters

The TAP-323 includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filter

The TAP-323's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The TAP-323 provides eight fields for filtered MAC addresses. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables MAC filter	Disable
Disable	Disables MAC filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets from the listed addresses will be allowed.	Drop
Drop	Any packet from the listed addresses will be denied.	

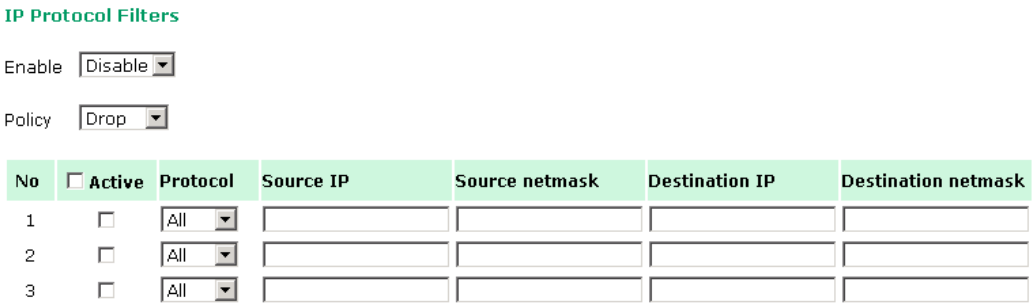
ATTENTION

Be careful when you enable the filter function:
Drop + "**no** entity on list is activated" = all packets are **allowed** (i.e., drop nothing)
Accept + "**no** entity on list is activated" = all packets are **denied** (i.e., accept nothing)

IP Protocol Filter

The TAP-323's IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocol and source/destination IP addresses.

The TAP-323 provides eight fields for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All**, **ICMP**, **TCP**, and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables IP protocol filter	Disable
Disable	Disables IP protocol filter	

Policy

Setting	Description	Factory Default
Accept	Only the packets from the listed addresses will be allowed	Drop
Drop	Any packet from the listed addresses will be denied	

ATTENTION

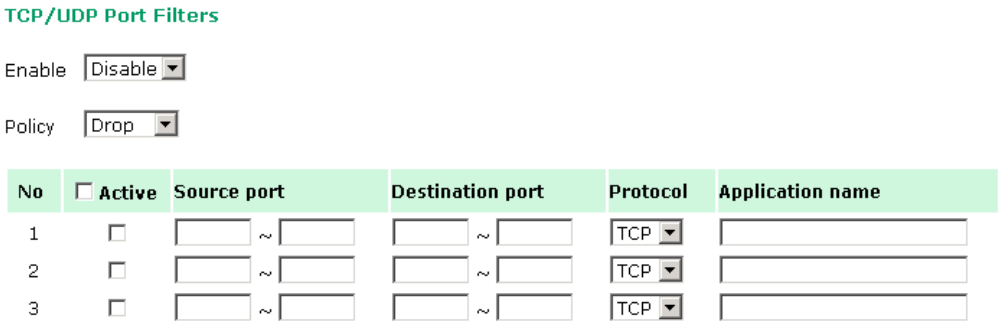
Be careful when you enable the filter function:
Drop + "**no** entity on list is activated" = all packets are **allowed** (i.e., drop nothing)
Accept + "**no** entity on list is activated" = all packets are **denied** (i.e., accept nothing)

TCP/UDP Port Filter

The TAP-323's TCP/UDP port filter is a policy-based filter that can allow or filter out TCP/UDP-based packets with a specified source or destination port.

The TAP-323 provides eight fields for setting the range of source/destination ports of a specific protocol. In addition to selecting TCP or UDP protocol, you can set either the source port, destination port, or both. The end port can be left empty if only a single port is specified. Of course, the end port cannot be larger than the start port.

The **Application name** is a text string that describes the corresponding entity with up to 31 characters. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables TCP/UDP port filter	Disable
Disable	Disables TCP/UDP port filter	

Policy

Setting	Description	Factory Default
Accept	Only packets from the listed ports are allowed.	Drop
Drop	Any packet from the listed ports will be denied.	

ATTENTION

Be careful when you enable the filter function:
Drop + "**no** entity on list is activated" = all packets are **allowed** (i.e., drop nothing)
Accept + "**no** entity on list is activated" = all packets are **denied** (i.e., accept nothing)

Introduction to Redundancy Protocol

Setting up Redundancy Protocol on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum. Redundancy Protocol allows you to set up redundant loops in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the Moxa TAP-323 is used as a key communications component of a production line, several minutes of downtime could cause a big loss in production and revenue. The Moxa TAP-323 supports two protocols to support this Redundancy Protocol function:

- Turbo Chain
- Rapid Spanning Tree and Spanning Tree Protocols (IEEE 802.1W/802.1D-2004)

When configuring a redundant chain, all APs on the same chain must be configured to use the same redundancy protocol. You cannot mix the Turbo Chain and STP/RSTP protocols on the same chain.

The following table lists the key differences between the features of each protocol. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network. redundancy protocol. You cannot mix the Turbo Chain and STP/RSTP protocols on the same chain. The following table lists the key differences between the features of each protocol. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	Turbo Chain	**RSTP**
Topology	Chain	Ring, Mesh
Fast Ethernet Recovery Time	<20 ms	Up to 5 sec.
Gigabit Ethernet Recovery Time	<50 ms	

The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures on a network, and provide an automatic means of avoiding loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. Moxa switches' STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every Moxa switch connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE 802.1D-2004. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backwards compatible with STP, making it relatively easy to deploy. For example:
  - Defaults to sending 802.1D style BPDUs if packets with this format are received.
  - STP (802.1D) and RSTP (802.1w) can operate on different ports of the same switch, which is particularly helpful when switch ports connect to older equipment such as legacy switches.

You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see the Differences between STP and RSTP section in this chapter.

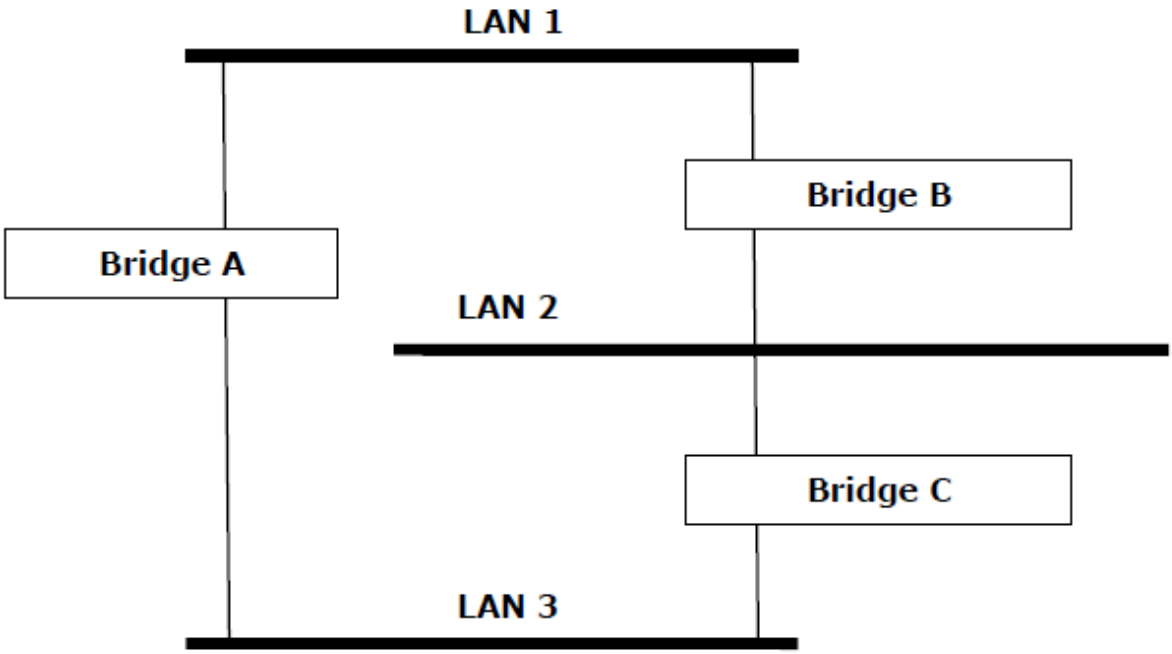
NOTE The STP protocol is part of the IEEE Std. 802.1D, 2004 Edition bridge specification. The following explanation uses "bridge" instead of "switch."

What is STP?

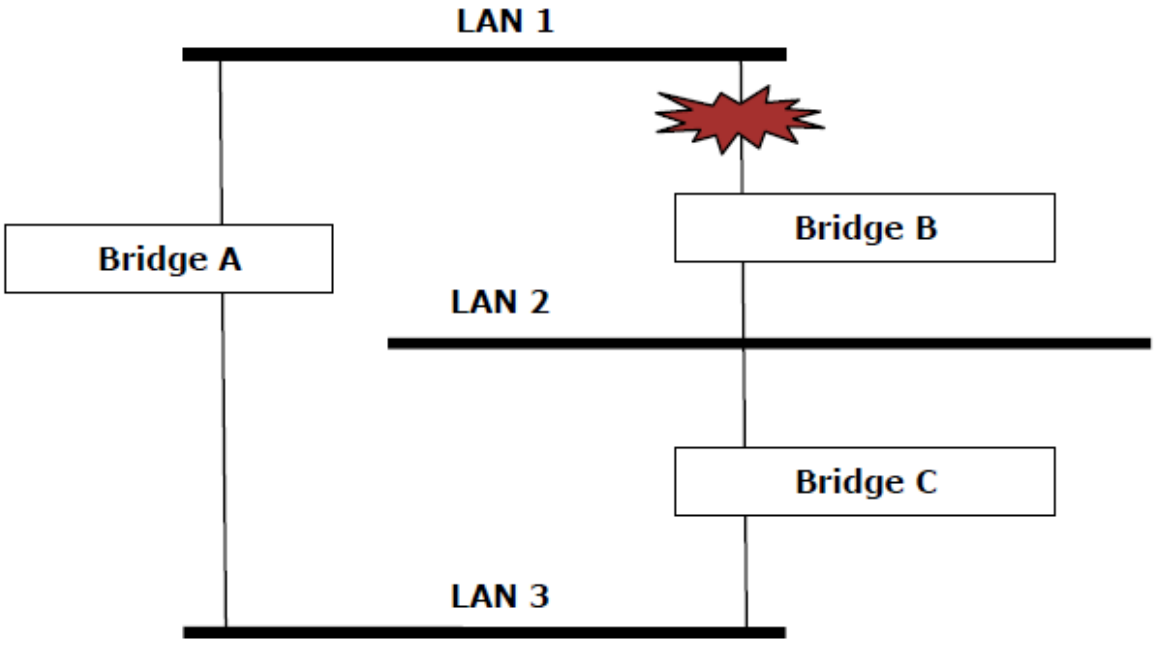
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- Locate and then disable less efficient paths (i.e., paths that have a lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

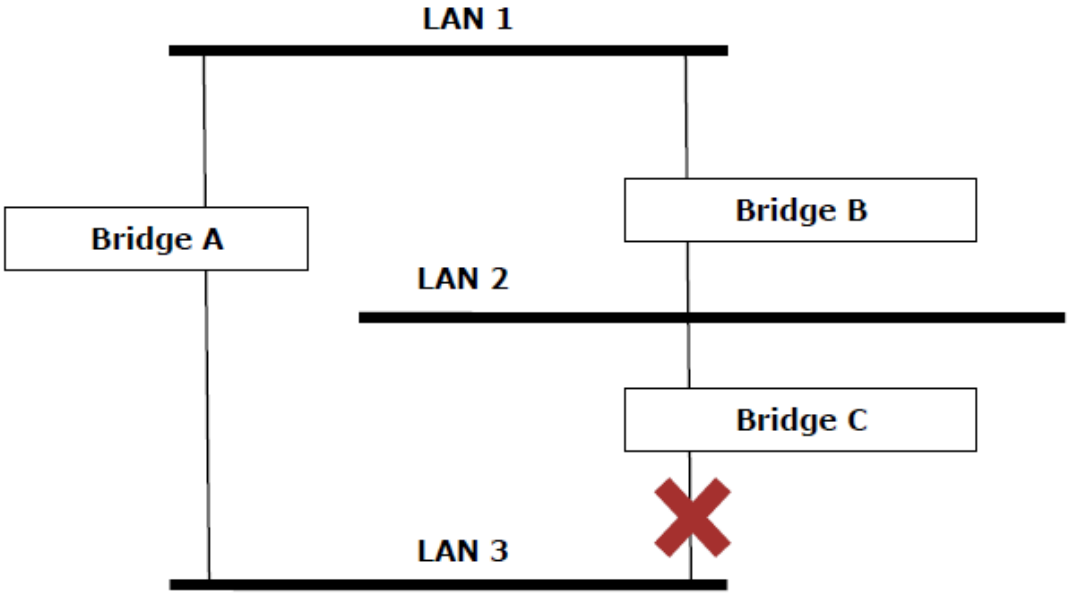
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or block, one of the paths from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through bridges C and A since this path has a greater bandwidth and is therefore more efficient.



What happens if a link failure is detected? As shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through bridge B.



STP will determine which path between each bridged segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous 3 figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

STP Requirements

Before STP can configure the network, the system must satisfy the following requirements:

- All bridges must be able to communicate with each other. The communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. For example, the default priority setting of Moxa switches is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficiency cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost.

STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- Which bridge should be the Root Bridge? The Root Bridge is the central reference point from which the network is configured.
- The Root Path Costs for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's Root Port. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path. In other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the Designated Bridge for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the Designated Bridge Port.

STP Configuration

After all of the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

STP Reconfiguration

Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has ceased to function. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, the first bridge to detect the change will send out an SNMP trap when the topology of your network changes.

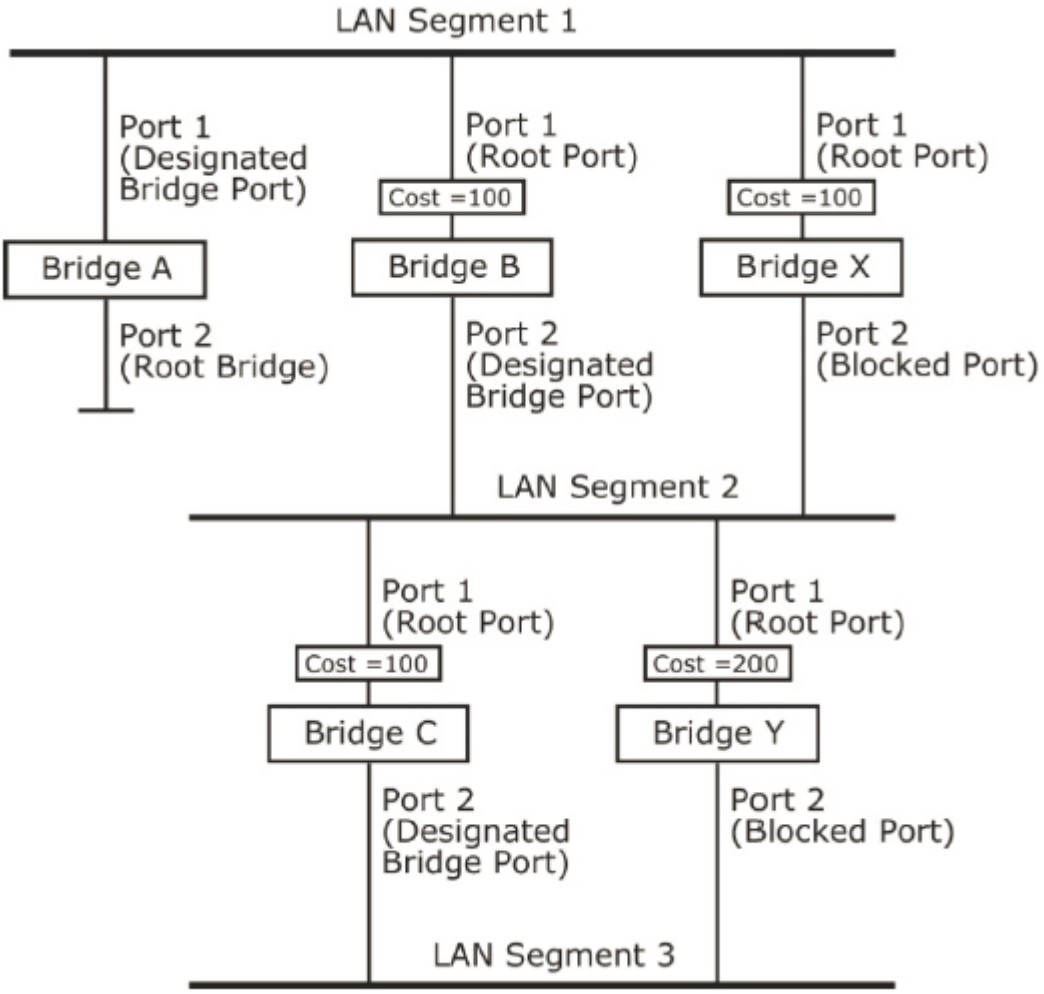
Differences between STP and RSTP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

STP and RSTP spanning tree protocols operate without regard to a network's VLAN configuration, and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology.

STP Example

The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.



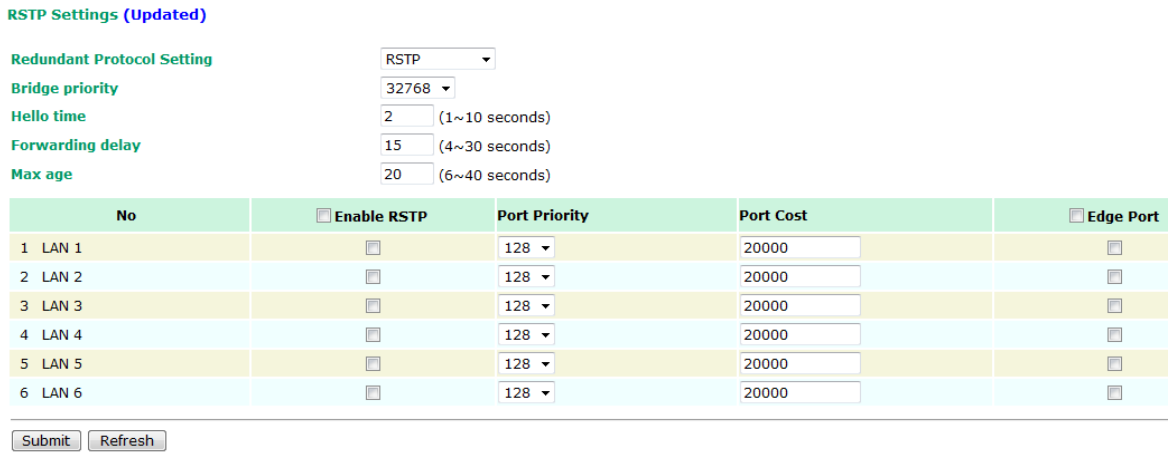
- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
  - The route through bridges C and B costs 200 (C to B=100, B to A=100)
  - The route through bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is port 2 on bridge C.

RSTP/Turbo Chain Settings (For Master or Slave Mode Only)

The TAP-323 supports IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid STP standards. In addition to eliminating unexpected path looping, STP/RSTP can provide a backup recovery path if a wired/wireless path fails accidentally. This fail-over function can increase the reliability and availability of the network. The TAP-323 also supports Turbo Chain on its fiber interfaces.

The TAP-323's STP/RSTP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every TAP-323 connected to your network.

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter is given below the figure.



Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time

Setting	Description	Factory Default
Numerical value input by user (1 to 10 seconds)	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2 (seconds)

Forwarding delay

Setting	Description	Factory Default
Numerical value input by user (4 to 30 seconds)	The amount of time this device waits before checking to see if it should change to a different state.	15 (seconds)

Max. age

Setting	Description	Factory Default
Numerical value input by user (6 to 40 seconds)	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new Spanning Tree topology.	20 (seconds)

Enable RSTP

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disable

Port priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by inputting a lower number.	128

Port cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology	20000

Edge port

Setting	Description	Factory Default
Checked/unchecked	Sets a port, which no BPDU is expected to go through, as an edge port	unchecked, except ***WLAN1/2*** ports

NOTE We recommend that you use the edge port setting for ports that are only connected to non-STP/RSTP sub-networks or end devices (PLCs, RTUs, etc.) as opposed to network equipment. This can prevent unnecessary waiting and negotiation for the STP/RSTP protocol, and accelerate system initialization. When an edge port receives BPDUs, it can still function as an STP/RSTP port and start negotiation. Setting an edge port is different from disabling STP/RSTP on a port. If you disable STP/RSTP, a port will not deal with STP/RSTP BPDUs at all.

Port Status

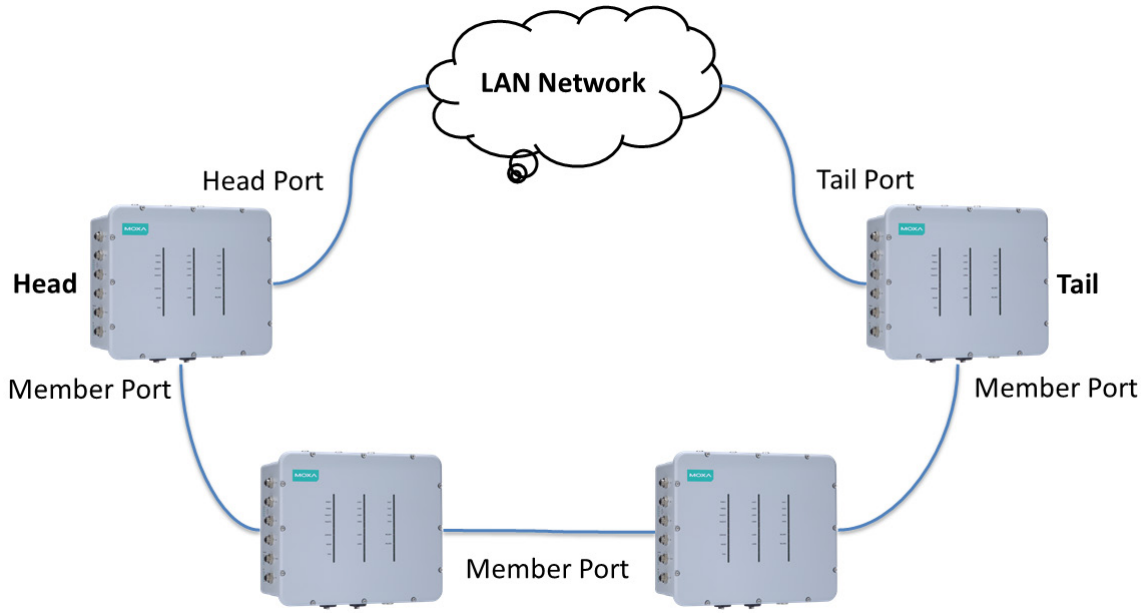
Port Status indicates the current Spanning Tree status of this port. Use **Forwarding** for normal transmission, or **Blocking** to block transmission.

The Turbo Chain Concept

Moxa's Turbo Chain is an advanced software-technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the "chain" concept, you first connect the APs in a chain and then simply link the two ends of the chain to an Ethernet network, as illustrated in the following figure.

Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses a multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

Setting Up a Turbo Chain



1. Select the Head AP, Tail AP, and Member AP.
2. Configure one port as the Head port and one port as the Member port in the Head AP, configure one port as the Tail port and one port as the Member port in the Tail AP, and configure two ports as Member ports in each of the Member switches.
3. Connect the Head AP, Tail AP, and Member APs as shown in the above diagram.

The path connecting to the Head port is the main path, and the path connecting to the Tail port is the backup path of the Turbo Chain. Under normal conditions, packets are transmitted through the Head Port to the LAN network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.

Configuring "Turbo Chain"

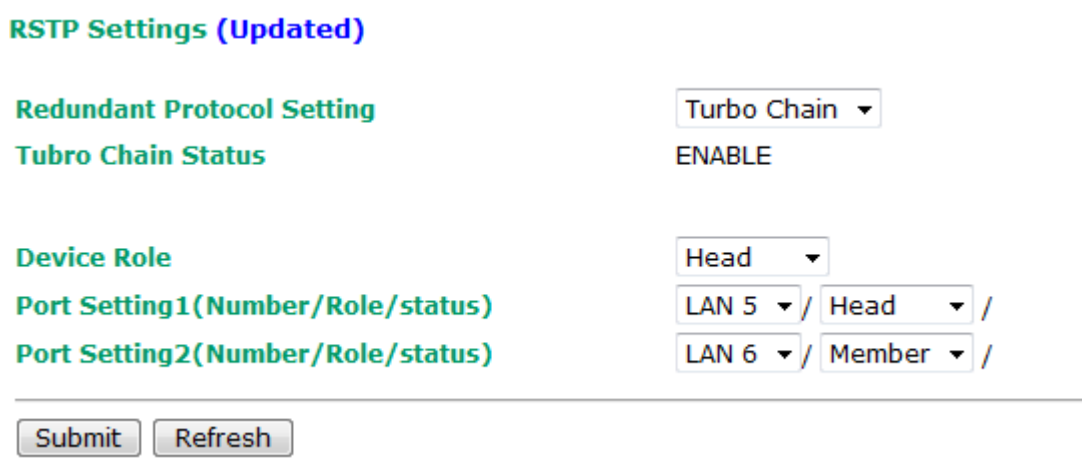
Use the scrollbar at the top of the **Redundancy Protocol** page to select **Turbo Chain** and **RSTP**.
Note that the configuration pages for these two protocols are different.

Protocol

Setting	Description	Factory Default
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	None
RSTP (IEEE 802.1D-2004)	Select this item to change to the RSTP configuration page.	

The following figures indicate which Turbo Chain parameters can be configured. A more detailed explanation of each parameter follows.

Head TAP Configuration



Member TAP Configuration

Tail TAP Configuration

Turbo Chain Status

Indicates whether Turbo Chain is enabled or disabled on the TAP-323.

Device Role

Setting	Description	Factory Default
Head, Member, or Tail	Select this AP as Head, member, or Tail AP	Head

Port Setting

Setting	Description	Factory Default
Port Number / Role / Status	Configure the LAN port and define its role in the Turbo Chain topology.	LAN5 as Head LAN6 as Member

SNMP Agent

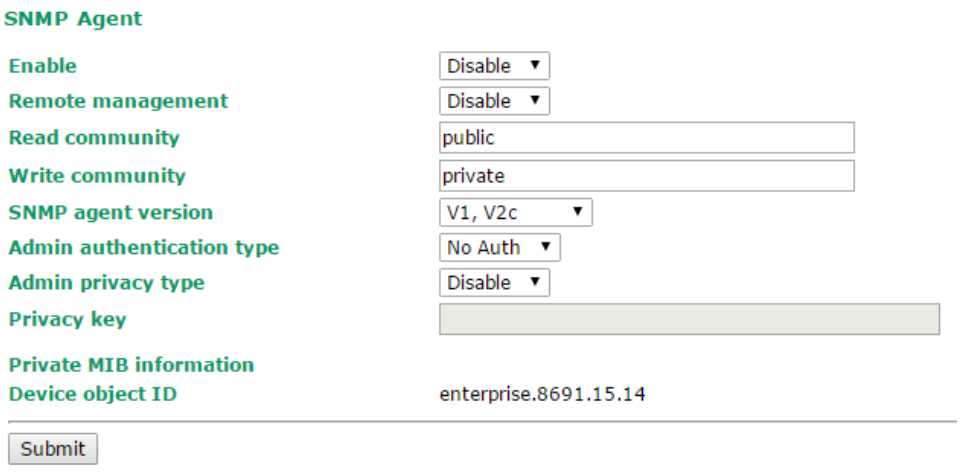
The TAP-323 supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

The TAP-323's MIB can be found in the software CD and supports reading the attributes via SNMP. (Only ***get*** method is supported.)

SNMP security modes and security levels supported by the TAP-323 are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	None	No	Use admin or user account to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

The following parameters can be configured on the **SNMP Agent** page. A more detailed explanation of each parameter is given below the following figure.



Enable

Setting	Description	Factory Default
Enable	Enables SNMP Agent	Disable
Disable	Disables SNMP Agent	

Remote Management

Setting	Description	Factory Default
Enable	Allow remote management via SNMP agent	Disable
Disable	Disallow remote management via SNMP agent	

Read community (for V1, V2c, V3 or V1, V2c)

Setting	Description	Factory Default
Read Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can access all objects with read-only permissions using this community string.	public

Write community (for V1, V2c, V3 or V1, V2c)

Setting	Description	Factory Default
Read/Write Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can access all objects with read/write permissions using this community string.	private

SNMP agent version

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Select the SNMP protocol version used to manage the switch.	V1, V2c

Admin auth type (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
No Auth	Use **admin** account to access objects. No authentication	No Auth
MD5	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	
SHA	Provides authentication based on HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	

Admin private key (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Disable	No data encryption	Disable
DES	DES-based data encryption	
AES	AES-based data encryption	

Private Key

A data encryption key is the minimum requirement for data encryption (maximum of 63 characters).

Private MIB Information Device Object ID

Also known as an ***OID***. This is the TAP-323's enterprise value and is a fixed value.

PoE Settings

The TAP-323 has 4 PSE ports that can supply PoE power to PD devices, such as video cameras, on the trackside.

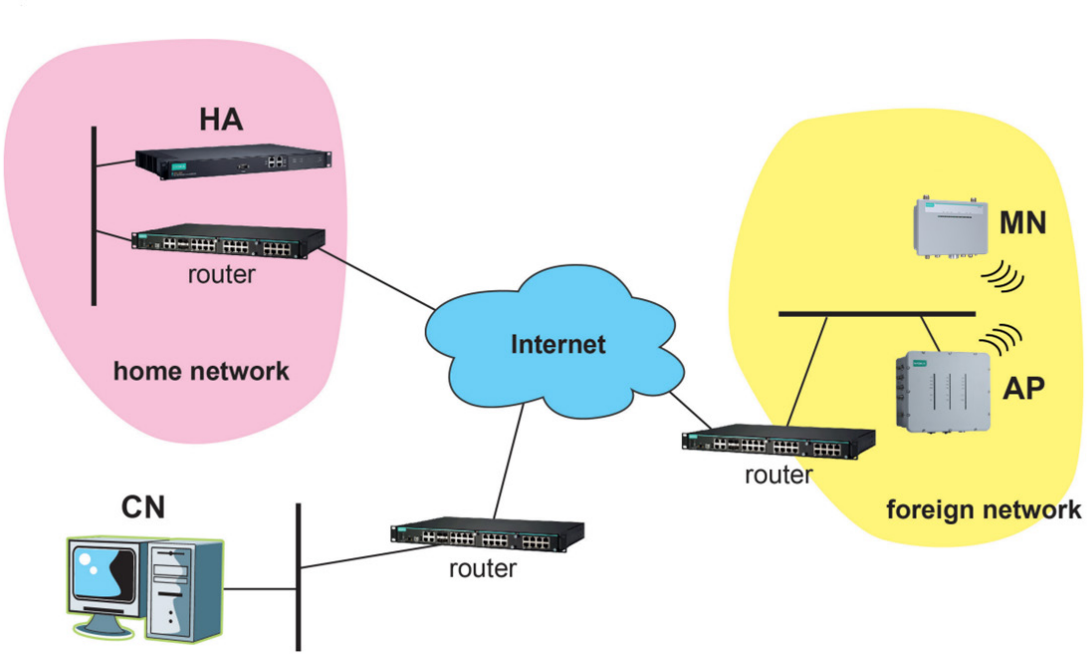
PoE Enable

Setting	Description	Factory Default
Enable/Disable	Enable or disable the LAN port (LAN1 to LAN4) for PoE	Enable

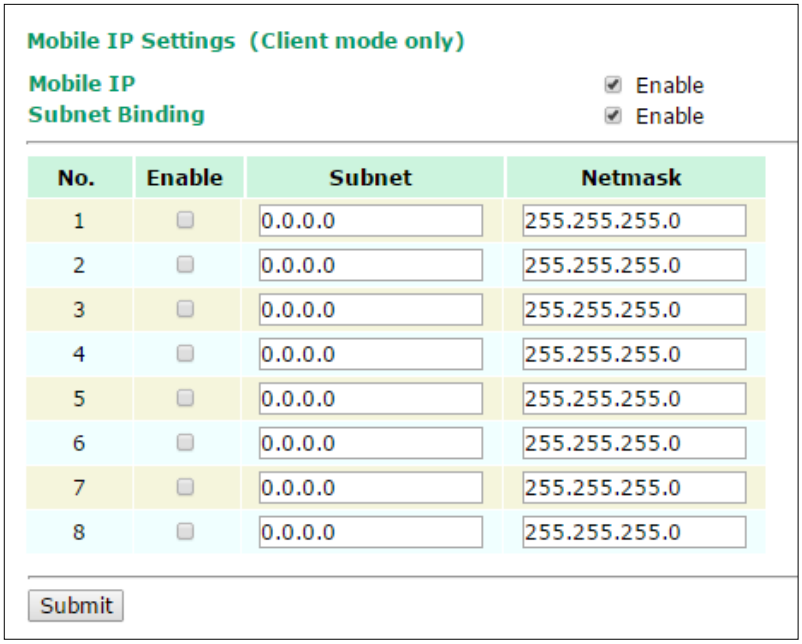
Mobile IP Settings

The mobile IP technology enables the TAP-323 to roam between Layer 3 networks with a roaming break time less than 50 ms. When the TAP-323 is in client/client router mode, it is a mobile node (MN) that is able to roam across different subnets without changing its IP address.

Mobile IP Topology Example:



Terminology	Description
Mobile Node (MN)	A host or router that changes its location from one network to another.
Home network	The network within which the MN receives its identifying IP address (home address)
Home address	The IP address assigned to the MN within its home network
Foreign network	The network in which an MN is operating when away from its home network
Home agent (HA)	A router on the home network that provides services to the MN. The home agent intercepts packets sent to the MN within the home network, encapsulates them, and then tunnels them to the MN.
Correspondent Node (CN)	A peer with which a mobile node is communicating
Co-located Care-of Address (CCoA)	The new IP address of the MN when operating on a foreign network.
Binding	The association of the home address with a CCoA



Setting	Description	Factory Default
Mobile IP	Enable/disable mobile IP capability of the client (mobile node) for L3 controller based roaming	Disable
Subnet Binding	Define a subnet of devices connected behind the client (MN) so that data will be forwarded to the corresponding device subnets. Proper IP planning is required to avoid configuring the subnet binding IP to limit access to the TAP.	Disable

Note that when the Mobile IP is enabled, the corresponding AP and WAC (HA) controller will also need to be configured properly (with 50 ms roaming enabled) to ensure correct operation of the L3 roaming network.

Auto Warning Settings

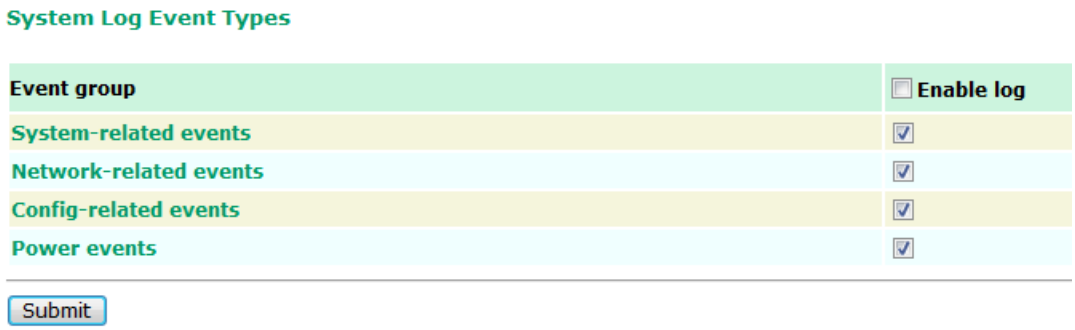
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. This way even when system administrators are out of the control room for an extended period, they can still be informed of the status of devices almost instantaneously when exceptions occur.

In addition to logging these events, the TAP-323 supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Log

System Log Event Types

Detailed information for grouped events is shown in the following table. You can check the **Enable log** box to enable event groups. By default all the values are enabled (checked). The log for system events can be seen in **Status → System Log**.



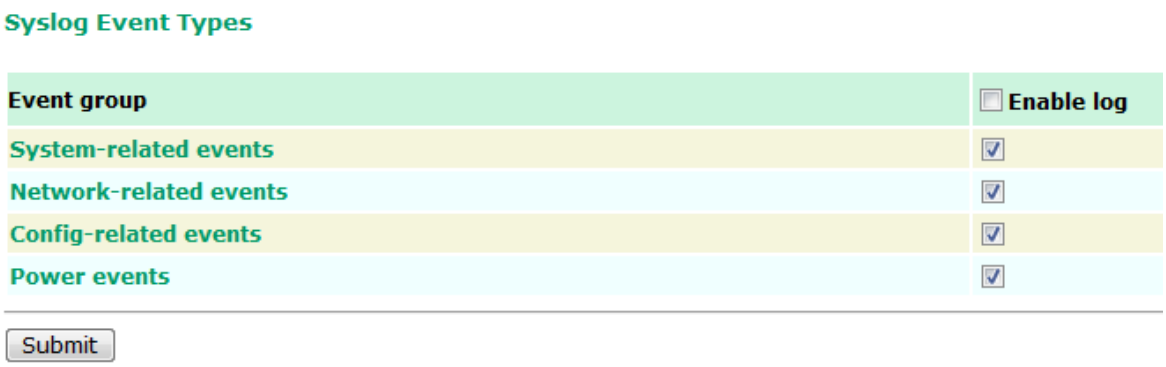
System-related events	**Event triggers when...**
System restart (warm start)	The TAP-323 is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
Network-related events	**Event triggers when...**
LAN 1 or LAN 2 link on	The LAN port is connected to a device or network.
LAN 1 or LAN 2 link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Client joined/ left for WLAN 1 or WLAN 2 (for AP or Master mode)	A wireless client is associated or disassociated.
WLAN 1 or WLAN 2 connected to AP (for Slave mode)	The TAP-323 is associated with an AP.
WLAN 1 or WLAN 2 disconnected (for Slave mode)	The TAP-323 is disassociated from an AP.
Config-related events	**Event triggers when...**
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the TAP-323.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The TAP-323's firmware is updated.
Power events	**Event triggers when...**
Power 1/2 transition (On → Off)	The TAP-323 is powered down in PWR1/2.
PoE transition (On → Off)	The TAP-323 is powered down in PoE.
Power 1/2 transition (Off → On)	The TAP-323 is powered via PWR1/2.
PoE transition (Off → On)	The TAP-323 is powered via PoE.

Syslog

This function provides the event logs for the Syslog server. The function supports up to three configurable Syslog servers and Syslog server UDP port numbers. When an event occurs, the event will be sent as a Syslog UDP packet to the specified Syslog servers.

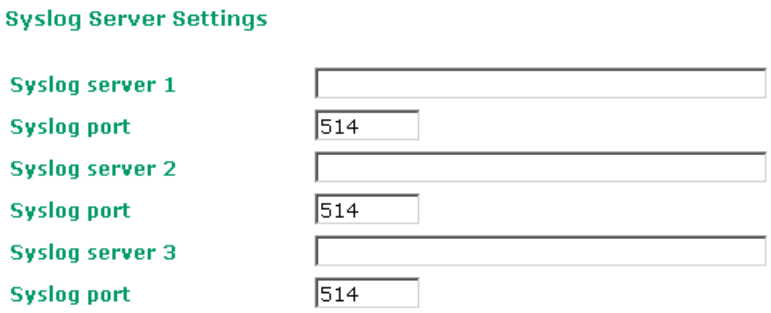
Syslog Event Types

Detailed information for the grouped events is shown in the following table. You can check the **Enable log** box to enable event groups. By default all values are enabled (checked). Details for each event group can be found on the "System log Event Types" table on page 3-31.



Syslog Server Settings

You can configure the parameters for your Syslog servers on this page.



Syslog server 1/2/3

Setting	Description	Factory Default
IP address	Enter the IP address of the 1st/ 2nd/ 3rd Syslog Server	None

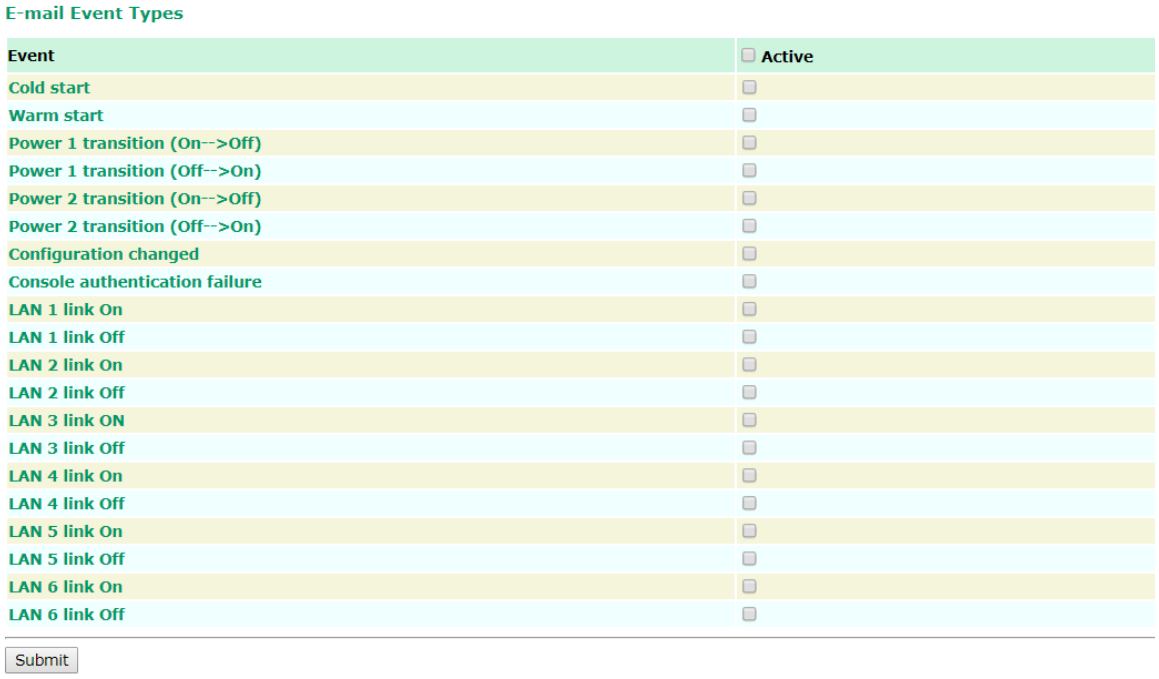
Syslog port

Setting	Description	Factory Default
Port destination (1 to 65535)	Enter the UDP port of the corresponding Syslog server	514

E-mail

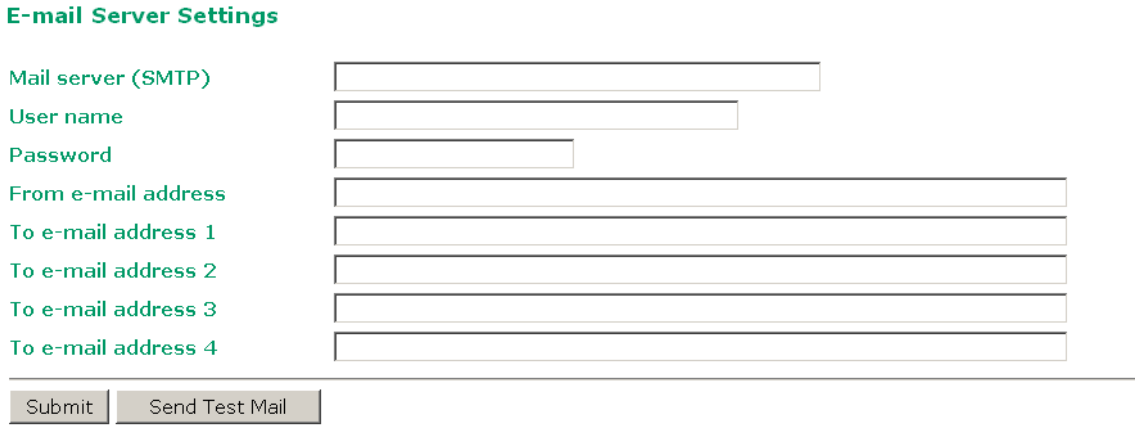
E-mail Event Types

Check the **Active** box to enable the event items. By default all values are deactivated (unchecked). Details for each event item can be found on the "System log Event Types" table on page 3-24.



E-mail Server Settings

You can set up to four email addresses to receive alarm emails from the TAP-323. The following parameters can be configured on the **E-mail Server Settings** page. In addition, a **Send Test Mail** button can be used to test whether the Mail server and email addresses are working. More detailed explanations about these parameters are given after the following figure.



Mail server (SMTP)

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

User name & Password

Setting	Description	Factory Default
	User name and password used in the SMTP server	None

From e-mail address

Setting	Description	Factory Default
Max. 63 characters	Enter the administrator's email address, which will be shown in the "From" field of a warning email.	None

To E-mail address 1/ 2/ 3/ 4

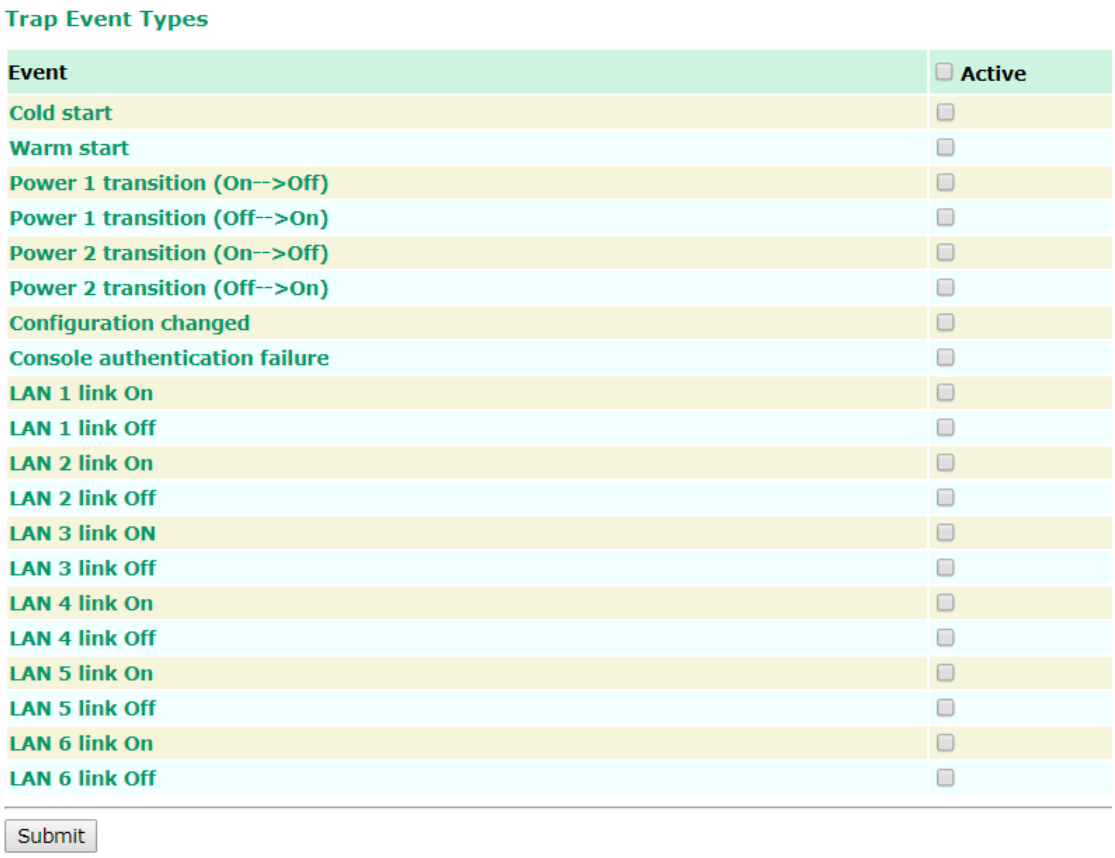
Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' email addresses.	None

Trap

Traps can be used to signal abnormal conditions (notifications) to a management station. This trap-driven notification can make your network more efficient.

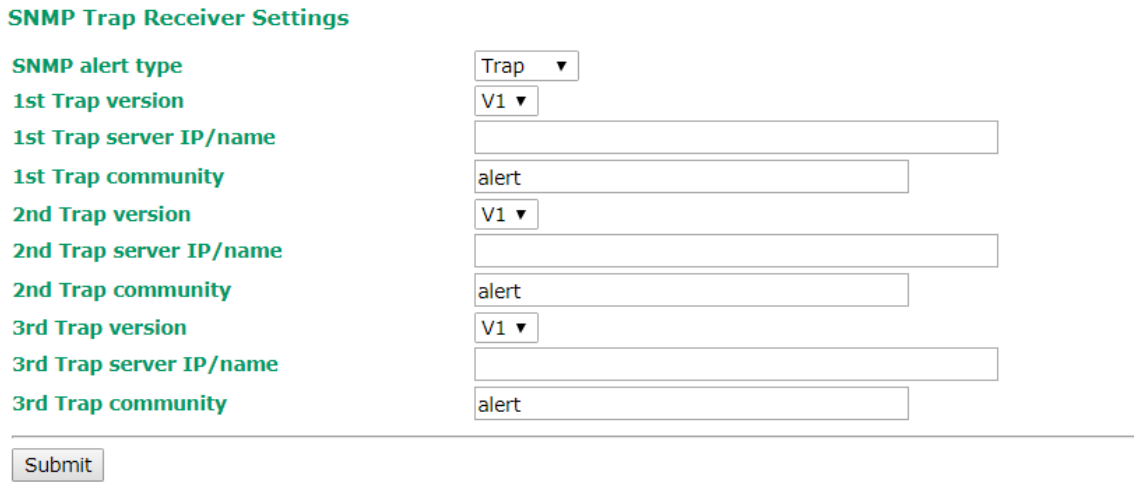
Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overwhelming for the management station to poll or send requests to query every object on every device. It would be more effective for the managed device agent to notify the management station when necessary by sending a message known as a trap.

Trap Event Types



SNMP Trap Receiver Settings

SNMP traps are defined in SMIv1 MIBs (SNMPv1) and SMIv2 MIBs (SNMPv2c). The two styles are basically equivalent, and it is possible to convert between the two. You can set the parameters for SNMP trap receivers through the web page.



1st / 2nd Trap version

Setting	Description	Factory Default
V1	SNMP trap defined in SNMPv1	V1
V2	SNMP trap defined in SNMPv2	

1st / 2nd Trap server IP/name

Setting	Description	Factory Default
IP address or host name	Enter the IP address or name of the trap server used by your network.	None

1st / 2nd Trap community

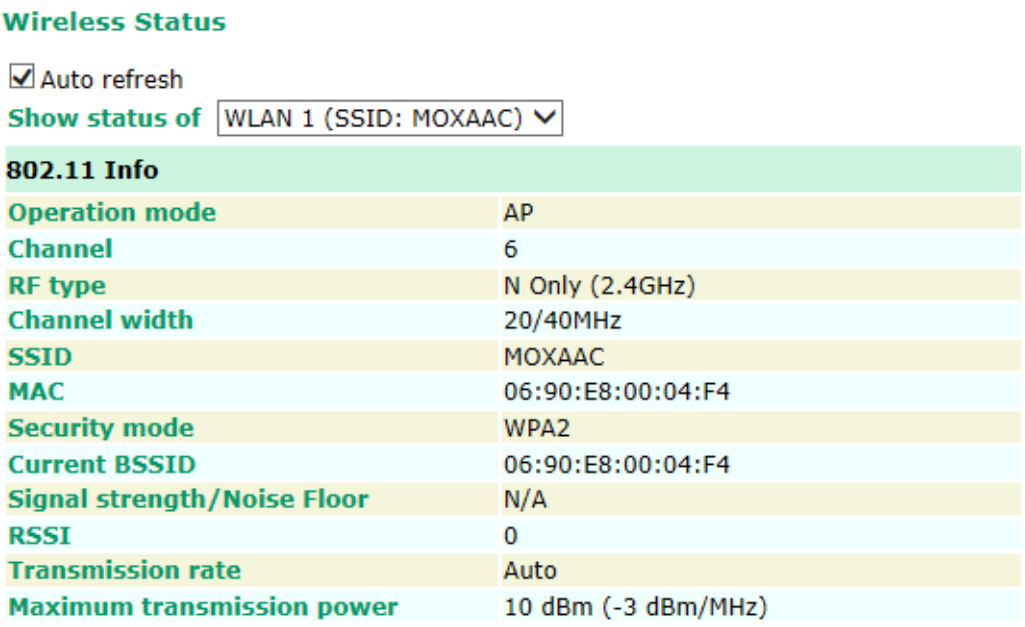
Setting	Description	Factory Default
Max. 31 characters	Use a community string match with a maximum of 31 characters for authentication.	alert

Status

Wireless Status

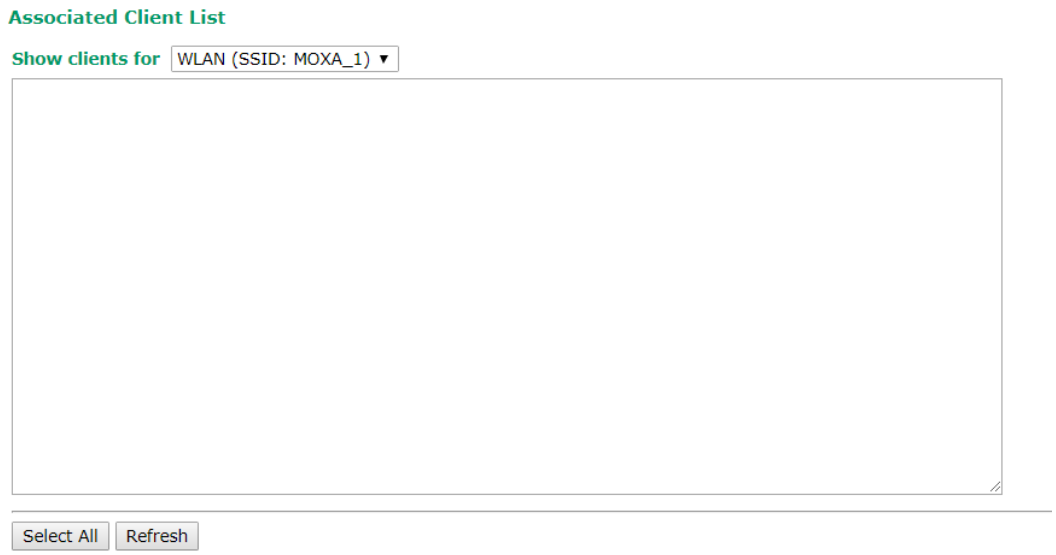
The status for **802.11 info** parameters, such as Operation mode and Channel, are shown on the **Wireless Status** page. The status will refresh every 5 seconds if the **Auto refresh** box is checked. Depending on the operation mode, certain **802.11 info** values may not be displayed. For example, the **Current BSSID** and **Signal strength** parameters are not available in the **AP** mode.

It is helpful to use the continuously updated information option on this page, such as Signal strength, to monitor the signal strength of the TAP-323 in Slave mode. The transmission power indicated is the current transmission power being updated periodically.



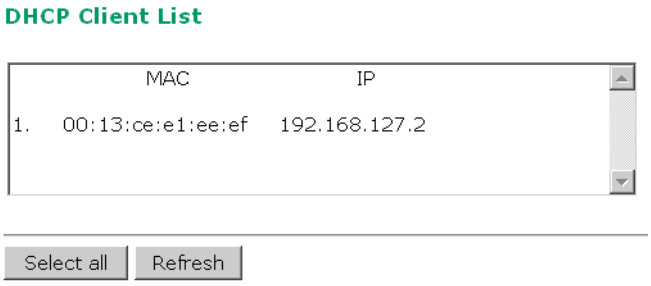
Associated Client List (for AP or Master Mode only)

Associated Client List shows all the clients that are currently associated with a particular TAP-323. Click **Select all** to select all the content in the list for further editing. Click **Refresh** to refresh the list.

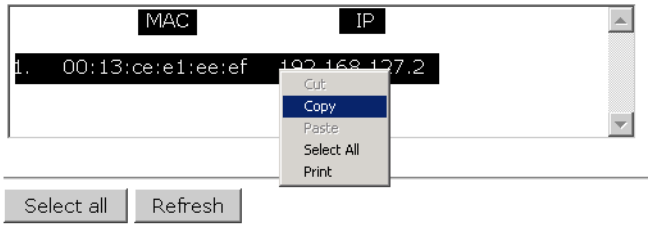


DHCP Client List (for AP mode only)

When you enable the DHCP server, the DHCP Client List shows all the clients that require and have successfully received IP assignments. Click the **Refresh** button to refresh the list.

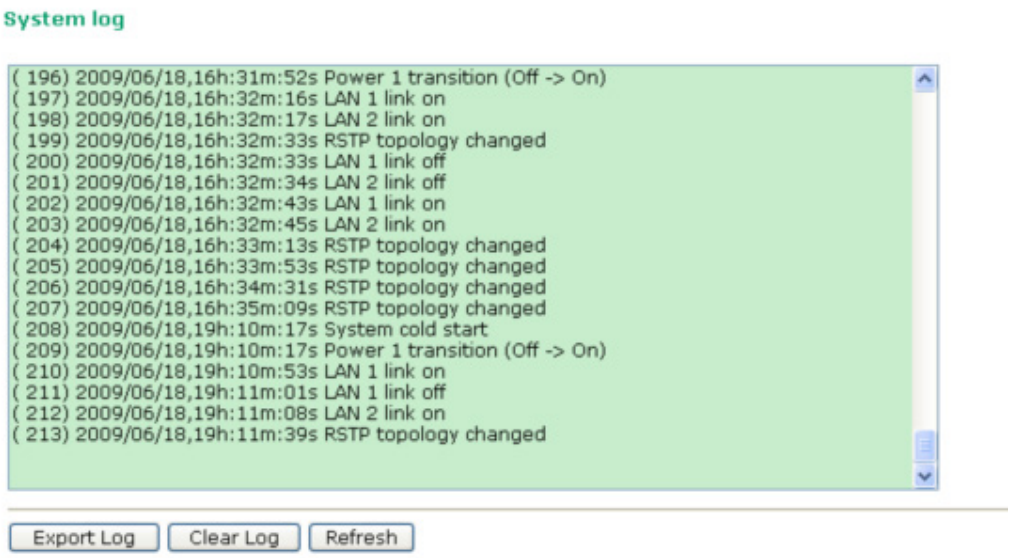


Click **Select all** to select all content in the list for further editing.



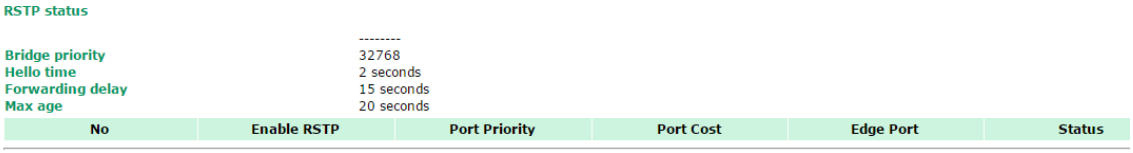
System Log

Triggered events are recorded in the System Log. You can export the log contents to an available viewer by clicking **Export Log**. You can use the **Clear Log** button to clear the log contents and the **Refresh** button to refresh the log.



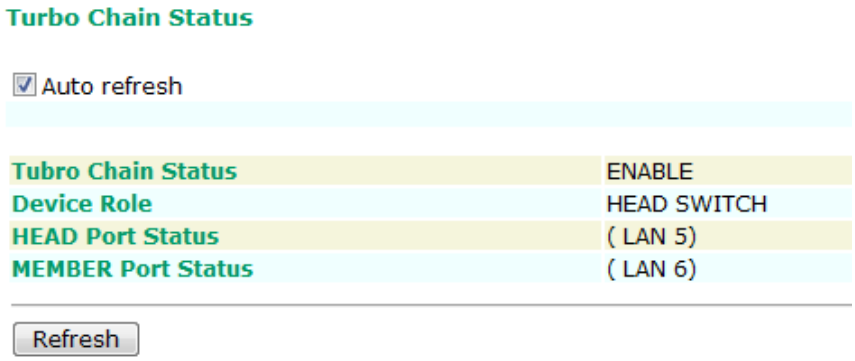
RSTP Status

This status field will appear only when STP/RSTP is enabled. It indicates whether or not this TAP-323 is the Root of the Spanning Tree (the root is determined automatically) and the status of each port.



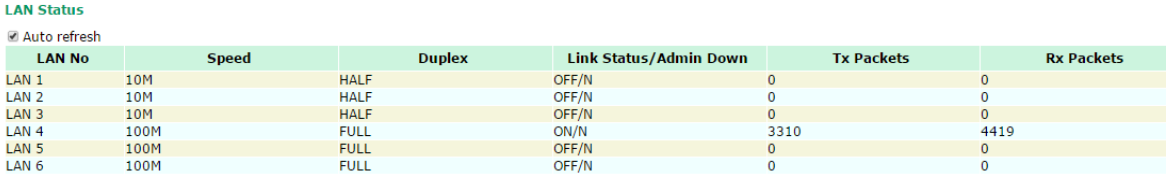
Turbo Chain Status

The status and configuration of the Turbo Chain ports can be monitored on this status page.



LAN Status

Each LAN port's status can be monitored on this page. Parameters include LAN speed, half/full duplex, link status, and number of Tx and Rx packets.

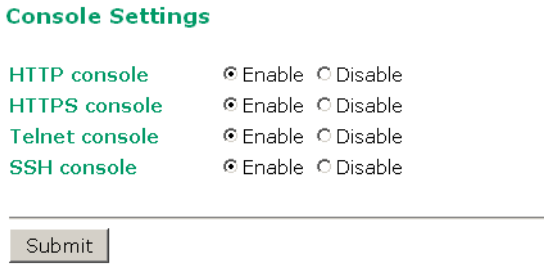


Maintenance

Maintenance functions provide the administrator with tools to manage the TAP-323 and wired/wireless networks.

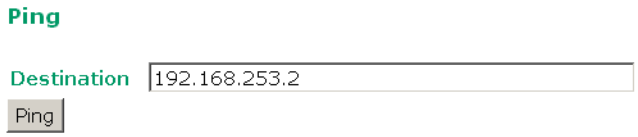
Console Settings

You can enable or disable access permission for the following consoles: HTTP, HTTPS, Telnet, and SSH connections. For more security, we recommend that you only allow access to the two secure consoles, HTTPS and SSH.

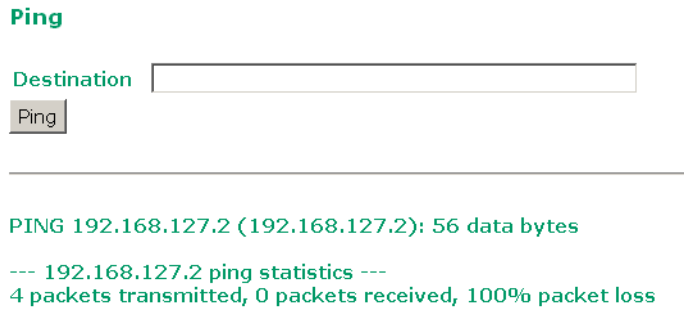


Ping

Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and discover whether or not the access path is available.



If the node and access path are available, you will see that all packets were successfully transmitted with no loss. Otherwise, some, or even all, packets may be lost, as shown in the following figure.



Firmware Upgrade

The TAP-323 can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available from Moxa's download center.

Before running a firmware upgrade, make sure the TAP-323 is off-line. Click the **Browse** button to specify the firmware image file and click **Firmware Upgrade and Restart** to start the firmware upgrade. After the progress bar reaches 100%, the TAP-323 will reboot itself.

When upgrading your firmware, the TAP-323's other functions are deactivated.

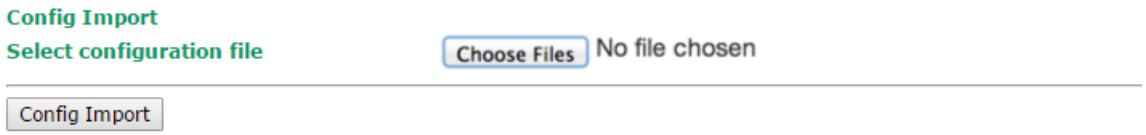
ATTENTION

Make sure the power source is stable when you upgrade your firmware. An unexpected power interruption may damage your TAP-323.

Config Import Export

You can back up or restore the TAP-323's configuration with **Config Import Export**.

In the **Config Import** section, click **Browse** to specify the configuration file and click the **Config Import** button to begin importing the configuration.



In the **Config Export** section, click the **Config Export** button and save the configuration file onto your local storage media. The configuration file is a text file and you can view and edit it with a general text editor.

Downloading the Configuration from a TFTP Server

You can download a configuration file from a TFTP server on to your TAP-323 as follows:

1. Start your TFTP server.
2. Copy the TAP-323 configuration file to a folder on the TFTP server.
3. On the TAP-323 Config Import page, input your TFTP server IP and Configuration path.

Note. The configuration path is the path of the configuration file, which is a relative path. If your configuration file is already available in a folder on the TFTP server, you can leave this field blank.

4. Input your configuration File name with the filename extension or click on the Config Import button to browse to the file. Once the configuration downloads successful, you will see "TFTP import success" information on the web page.
5. Click Save and then Restart on the top-right side.

To download the configuration to the TAP:

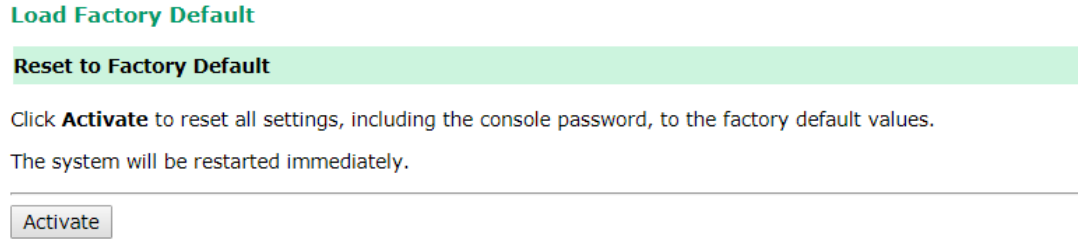
1. Turn off the TAP.
2. Plug in the ABC-02 to the TAP's USB port.
3. Turn on TAP
4. TAP will detect ABC-02 during the boot up process, and download the configuration from the ABC-02 to the TAP automatically. Once the configuration downloads and if configuration format is correct, the TAP will emit three short beeps, and then continue the boot up.
5. Once the TAP has booted up successfully, it will emit the normal two beeps, and the ready LED will turn to solid green.

MIB Export

The SNMP MIB file for TAP-323 is embedded in the device. To export the MIB file, simply click on the "MIB Export" button and save it to your local drive.

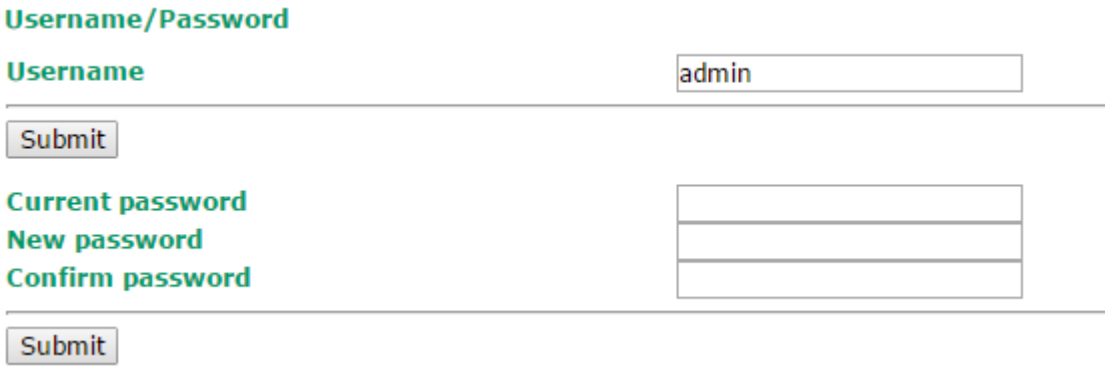
Load Factory Default

Use this function to reset the TAP-323 and roll all settings back to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the TAP-323.



Username/Password

You can change the administration username and password for each of the TAP-323's console managers by using the **Username/Password** function. Before you set up a new password, you must input the current password and reenter the new password for confirmation. For your security, do not use the default password moxa, and remember to change the administration password regularly.

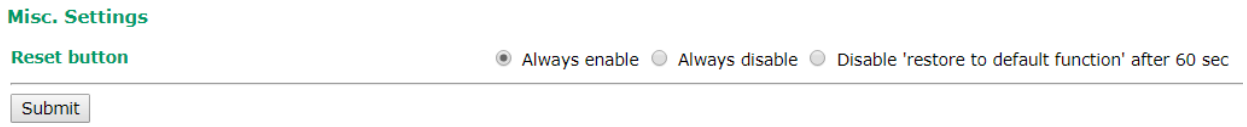


Locate Device

The AP can be identified by a beeping sound and flashing LED when clicking on the "start to locate" button. To stop the beeping, click on the "stop locating" button.

Misc. Settings

Additional settings that can help you manage your TAP-323 are available on this page.



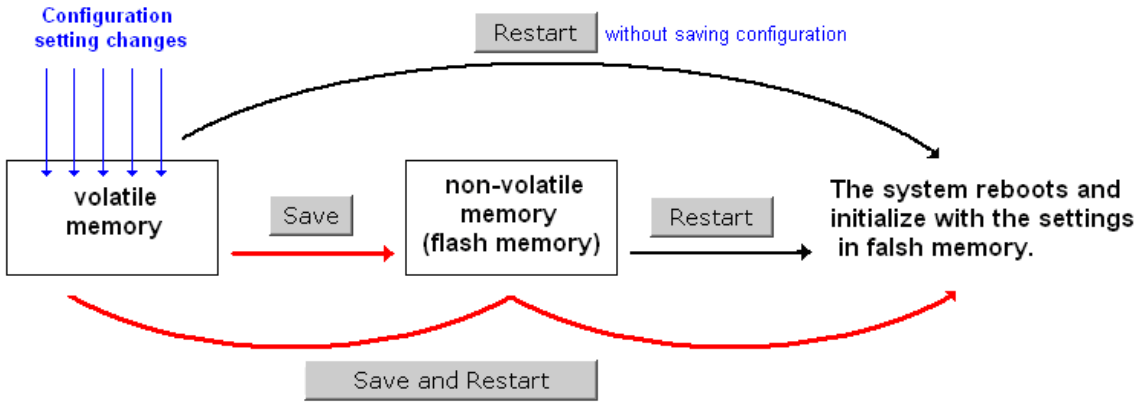
Reset button

Setting	Description	Factory Default
Always enable	The TAP-323's reset button works normally	Always enable
Always disable	The TAP-323's reset button will not work	
Disable the "restore to default" function after 60 seconds	The TAP-323's reset to default function will be inactive 60 seconds after the TAP-323 completes the boot-up process.	

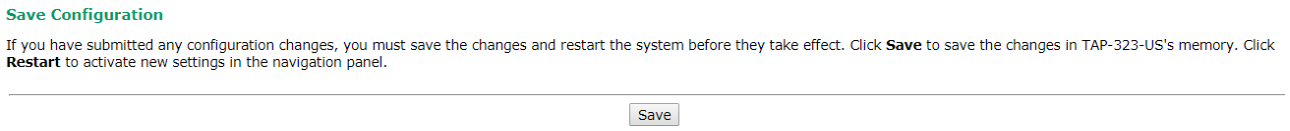
Save Configuration

The following figure shows how the TAP-323 stores the setting changes into volatile and non-volatile memory. Unless it is saved, all data stored in volatile memory will disappear when the TAP-323 is shut down or rebooted. Because the TAP-323 starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the TAP-323.

This also means the new changes will not work unless you run either the **Save Configuration** function or the **Restart** function.



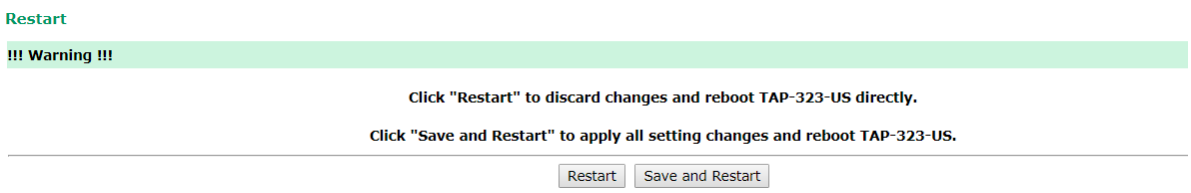
After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However, the new setting changes will remain in the non-volatile memory until you save the configurations.



Restart

If you submitted configuration changes, you will see blinking text in the upper right corner of the screen. After making all your changes, click the **Restart** function in the left menu box. One of two different screens will appear.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the TAP-323 directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the TAP-323.

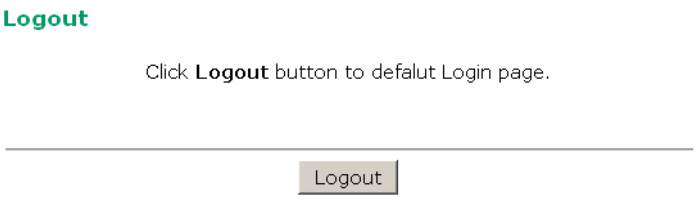


If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.

You will not be able to run any of the TAP-323's functions while the system is rebooting.

Logout

Logout helps users disconnect the current HTTP or HTTPS session and go to the Login page. For security reasons, we recommend that you log out before quitting console manager.



4

Software Installation/Configuration

The following topics are covered in this chapter:

- **Overview**
- **Wireless Search Utility**
  - Configuring Wireless Search Utility

Overview

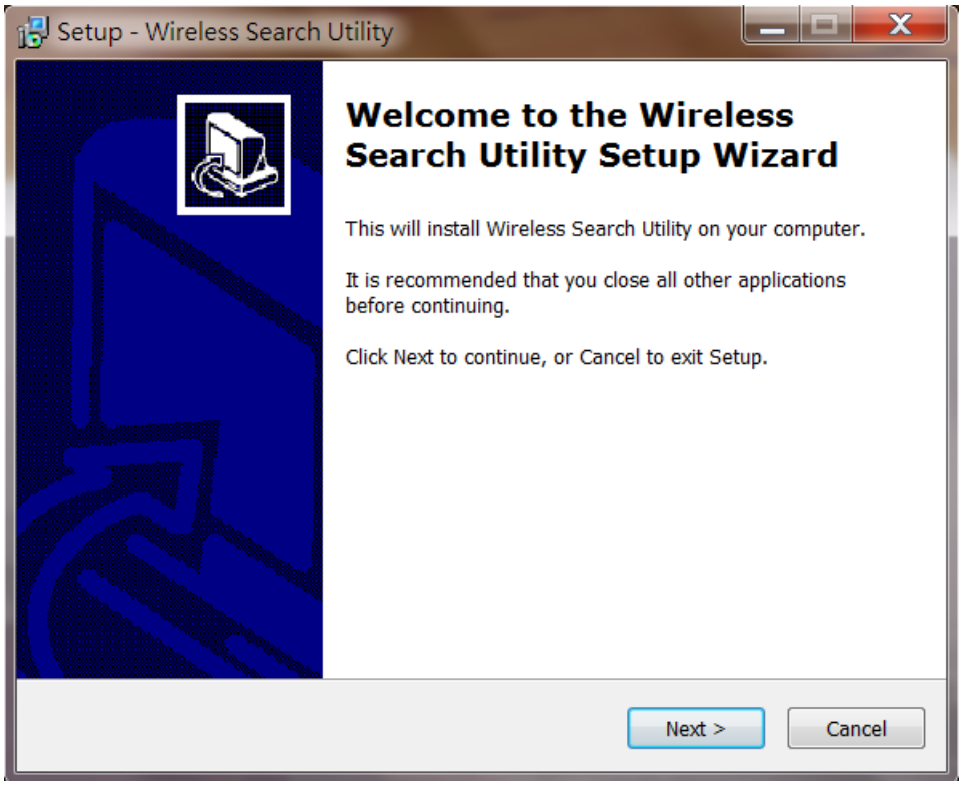
The Wireless Search Utility can be downloaded from the Moxa website at www.moxa.com.

Wireless Search Utility

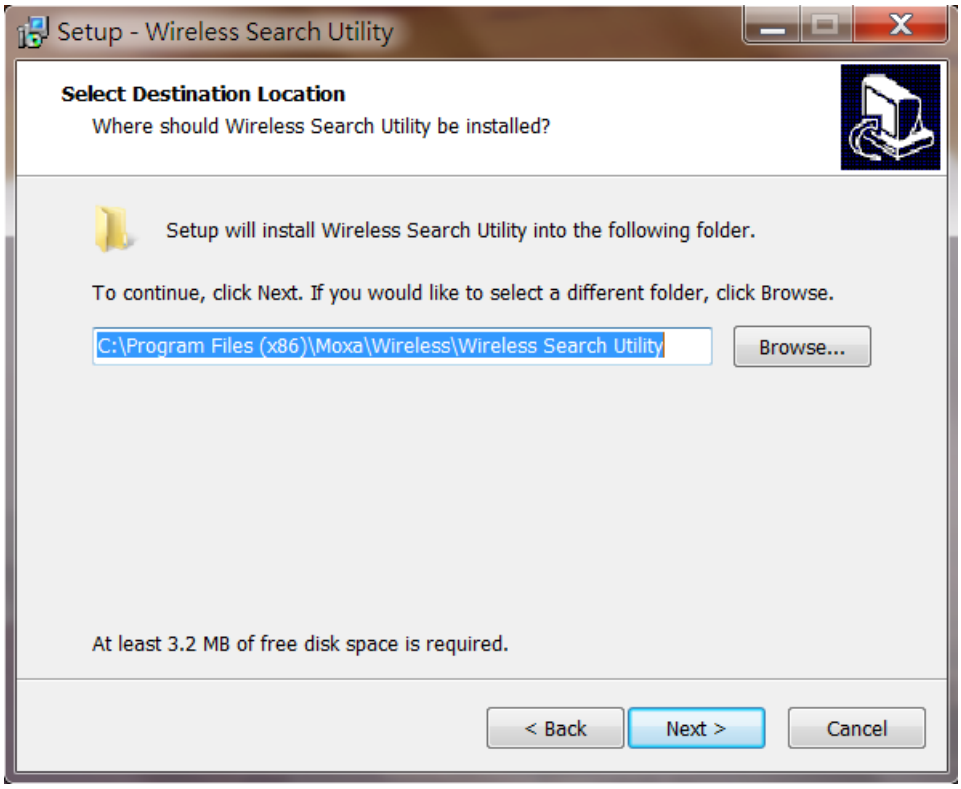
Installing Wireless Search Utility

Once the Wireless Search Utility is downloaded, run the setup executable to start the installation.

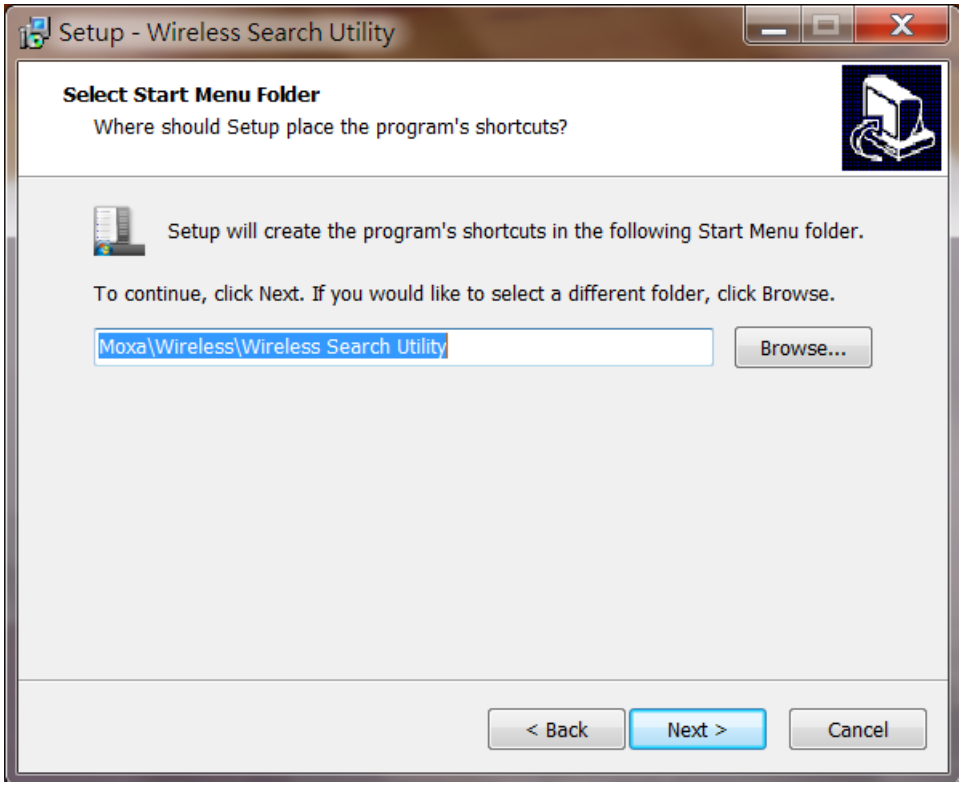
1. Click **Next** in the **Welcome** screen to proceed with the installation.



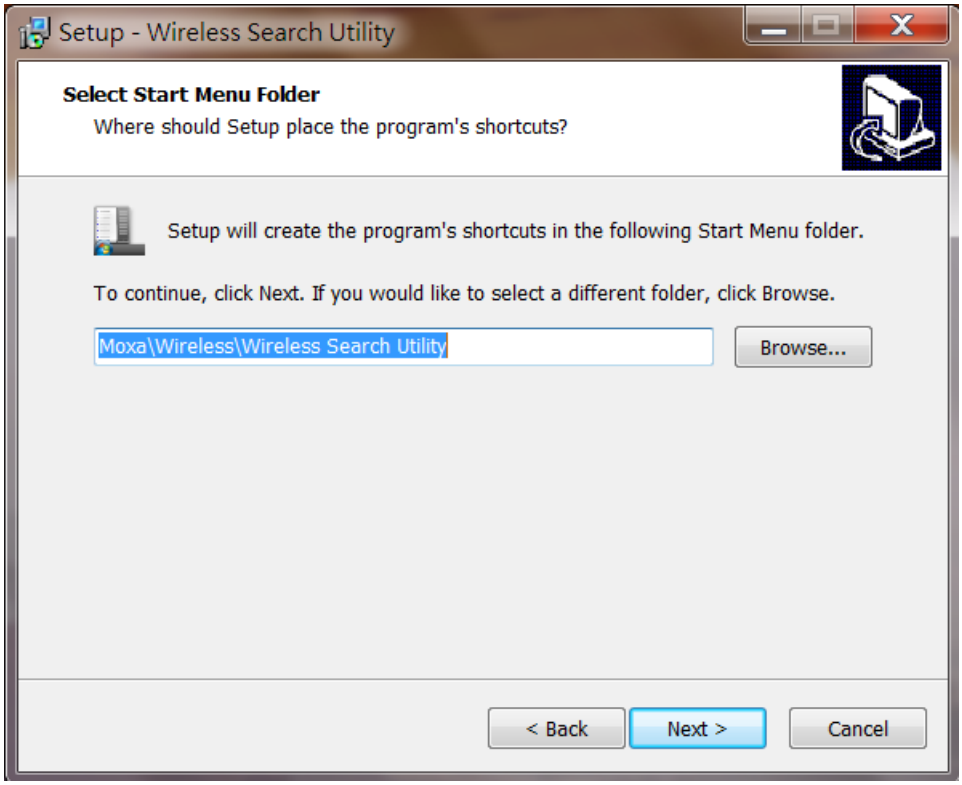
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



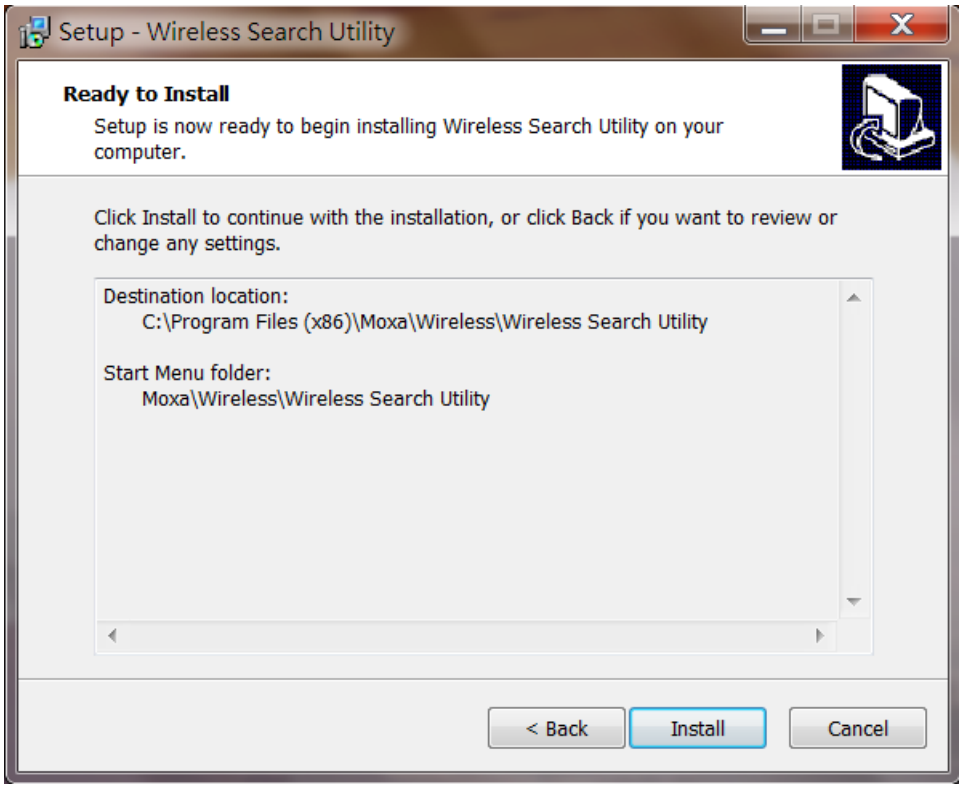
3. Click **Next** to install the program's shortcut files in the default directory, or click **Browse** to select an alternate location.



4. Click **Next** to select additional tasks.

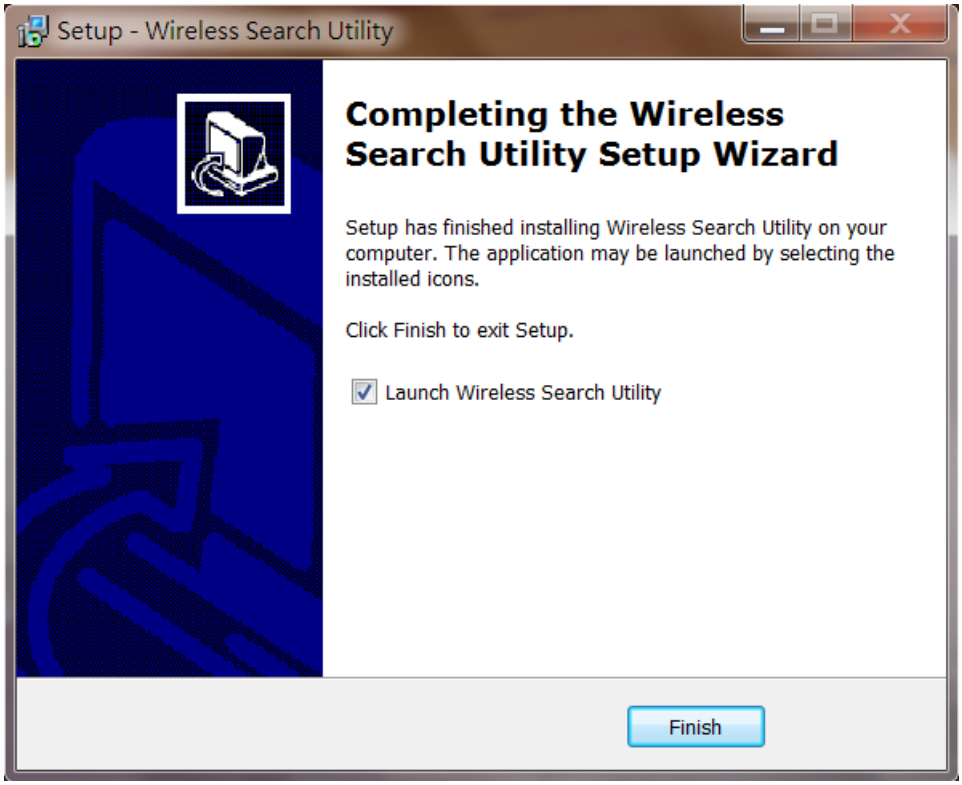


5. Click **Install** to proceed with the installation. The installer then displays a summary of the installation options.



6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.

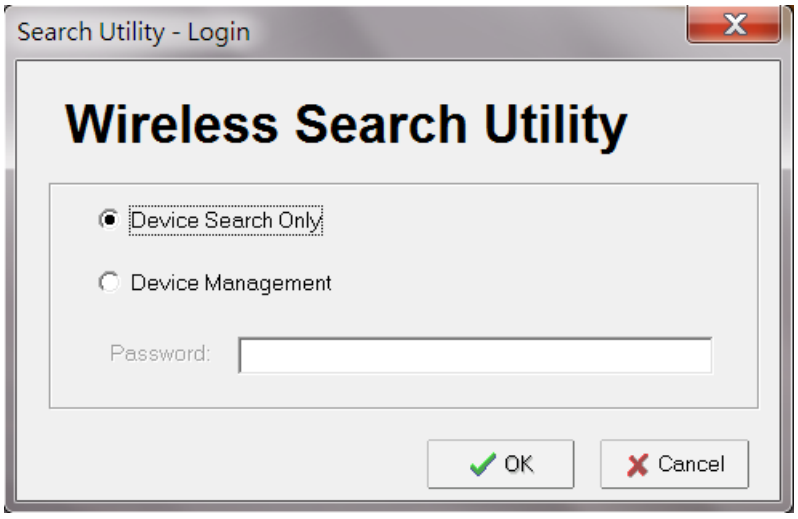
7. Click **Finish** to complete the installation of Wireless Search Utility.



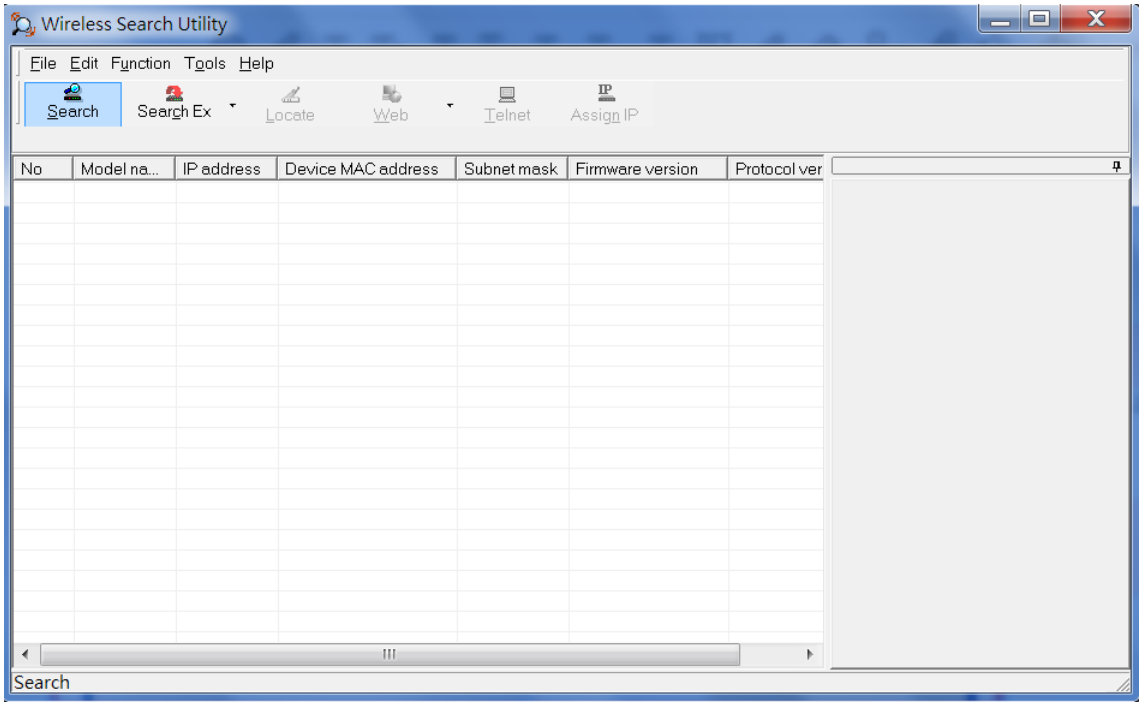
Configuring Wireless Search Utility

The Broadcast Search function is used to locate all TAP-323 APs that are connected to the same LAN as your computer. After locating a TAP-323, you will be able to change its IP address. Since the Broadcast Search function searches by UDP packets and not IP address, it doesn't matter if the TAP-323 is configured as an AP or Client. In either case, APs and Clients connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

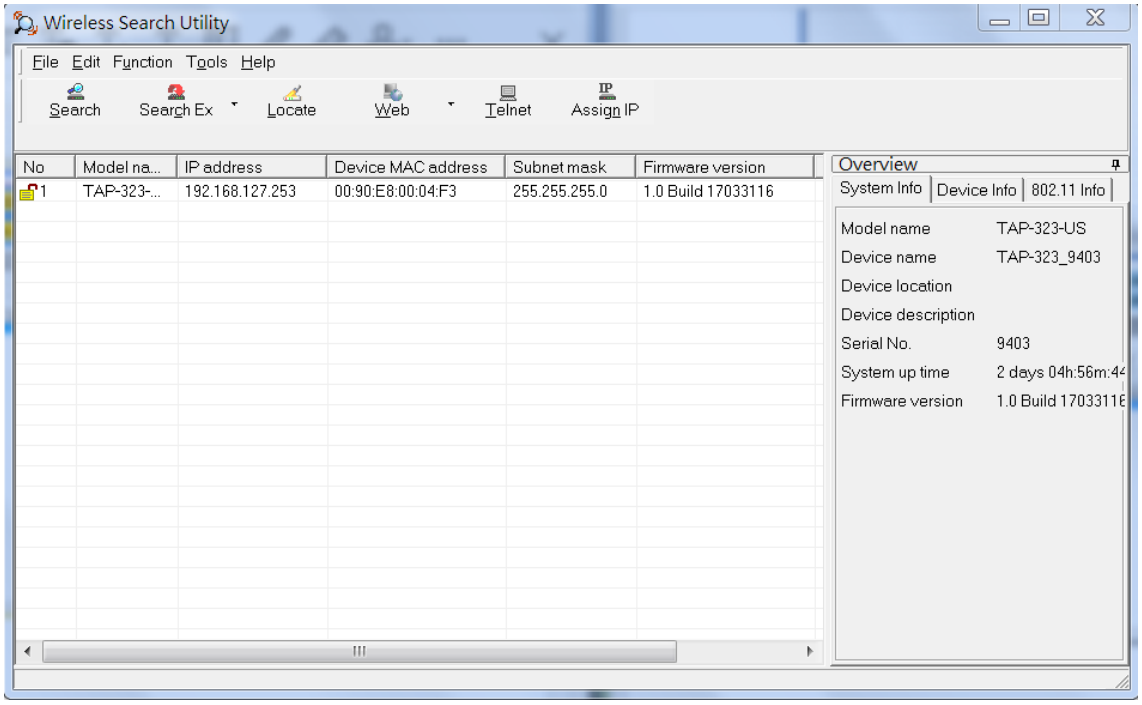
1. Start the **Wireless Search Utility** program. When the Login page appears, select the "Device Search only" option to search for TAPs and to view each TAP's configuration. Select the "Device management" option to assign IPs, upgrade firmware, and locate devices.



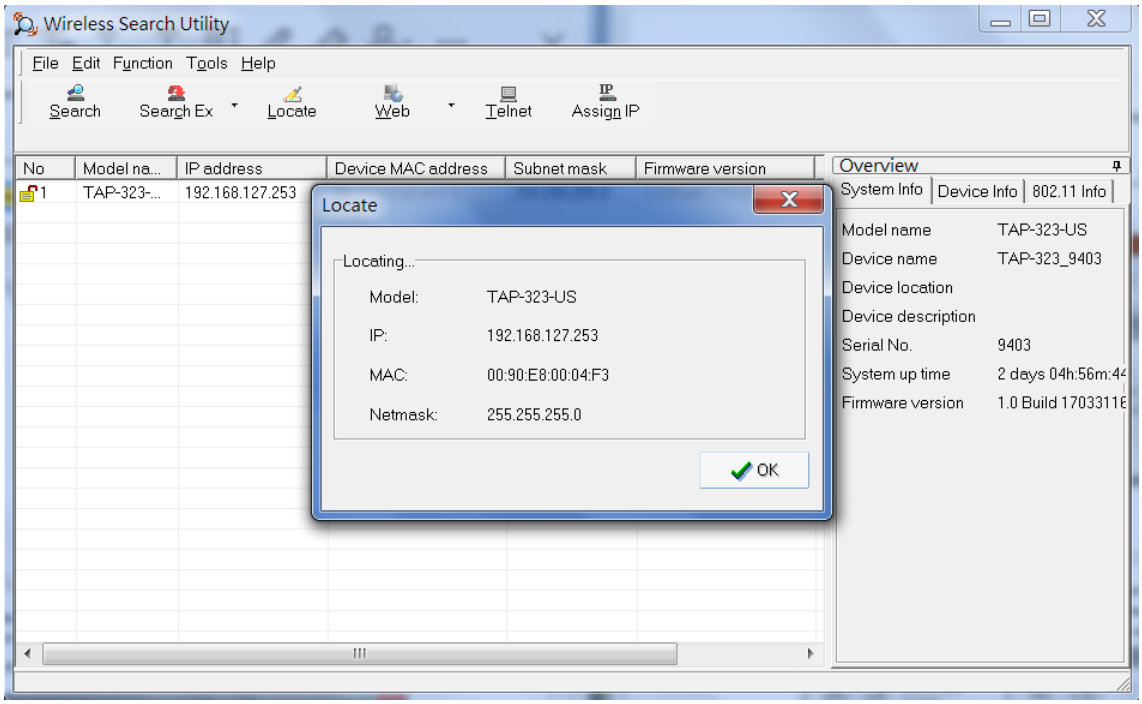
2. Open the Wireless Search Utility and then click the **Search** icon.



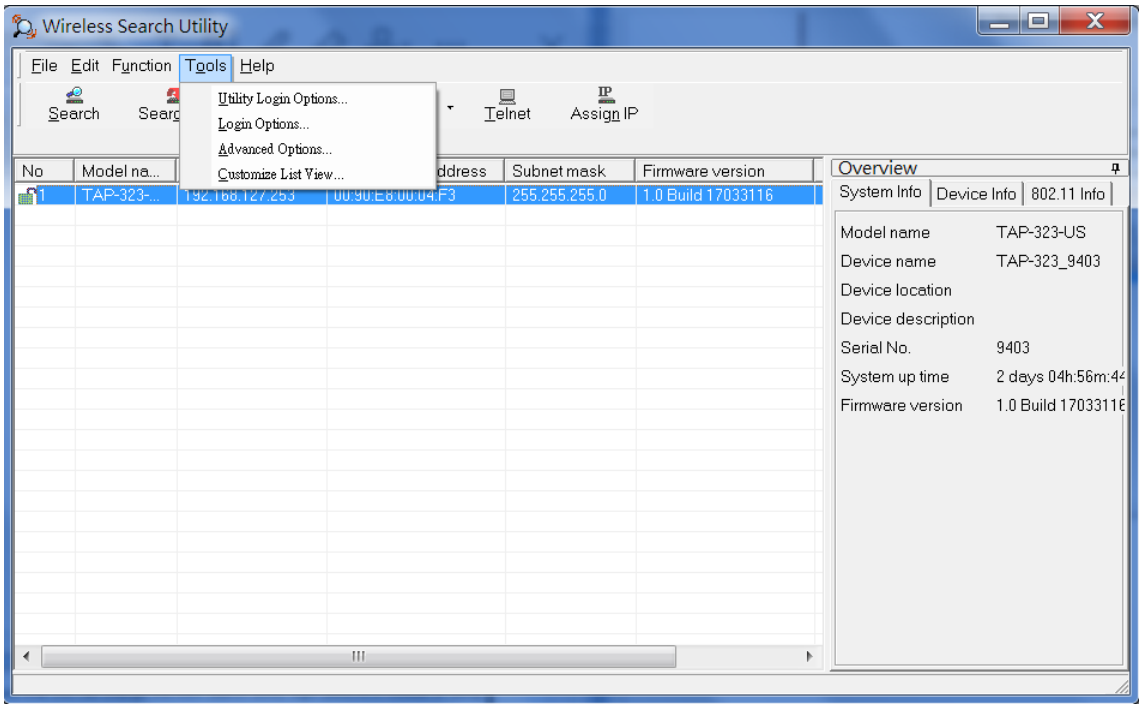
3. The "Searching" window indicates the progress of the search. When the search is complete, all TAPs that were located will be displayed in the Wireless Search Utility window.



4. Click **Locate** to cause the selected device to beep.



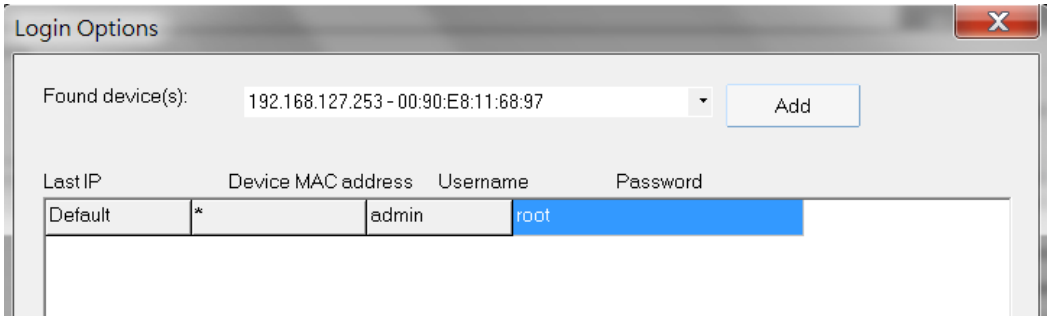
5. Make sure your TAP is **unlocked** before using the search utility's icons setting. The TAP will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.
6. Go to **Tools → Login Options** to manage and unlock additional TAPs.



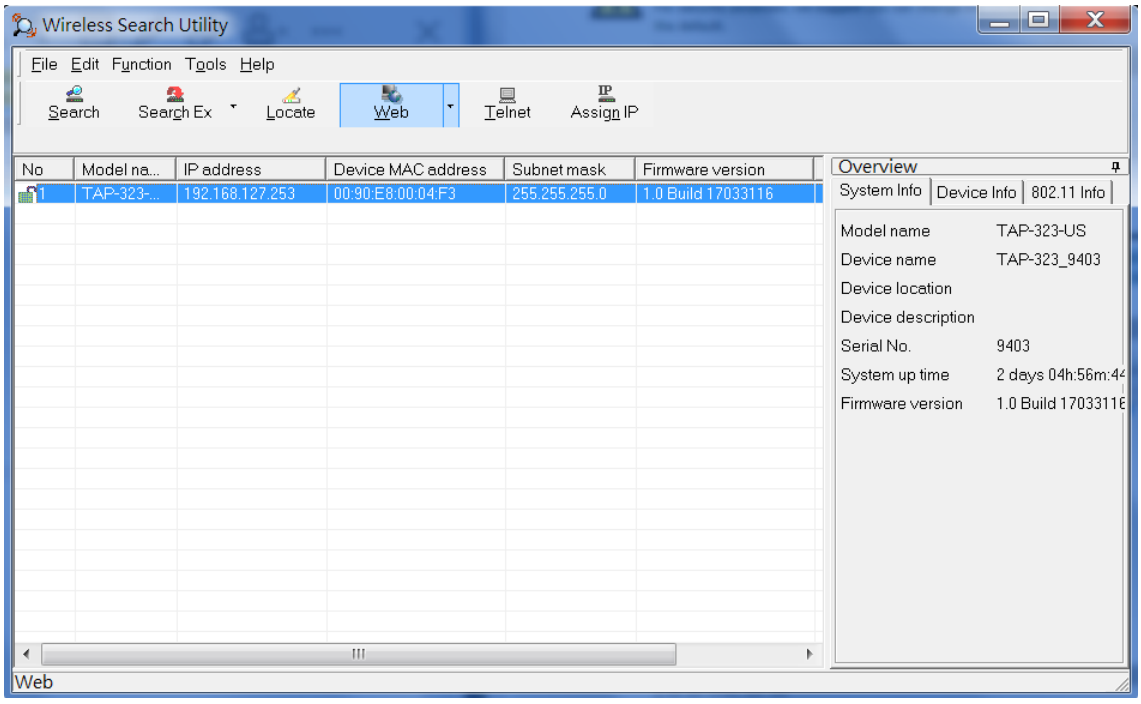
7. Use the scroll down list to select the MAC addresses of those TAPs you would like to manage, and then click **Add**. Key in the password for the TAP device and then click **OK** to save. If you return to the search page and search for the TAP again, you will find that the TAP will unlock automatically.

ATTENTION

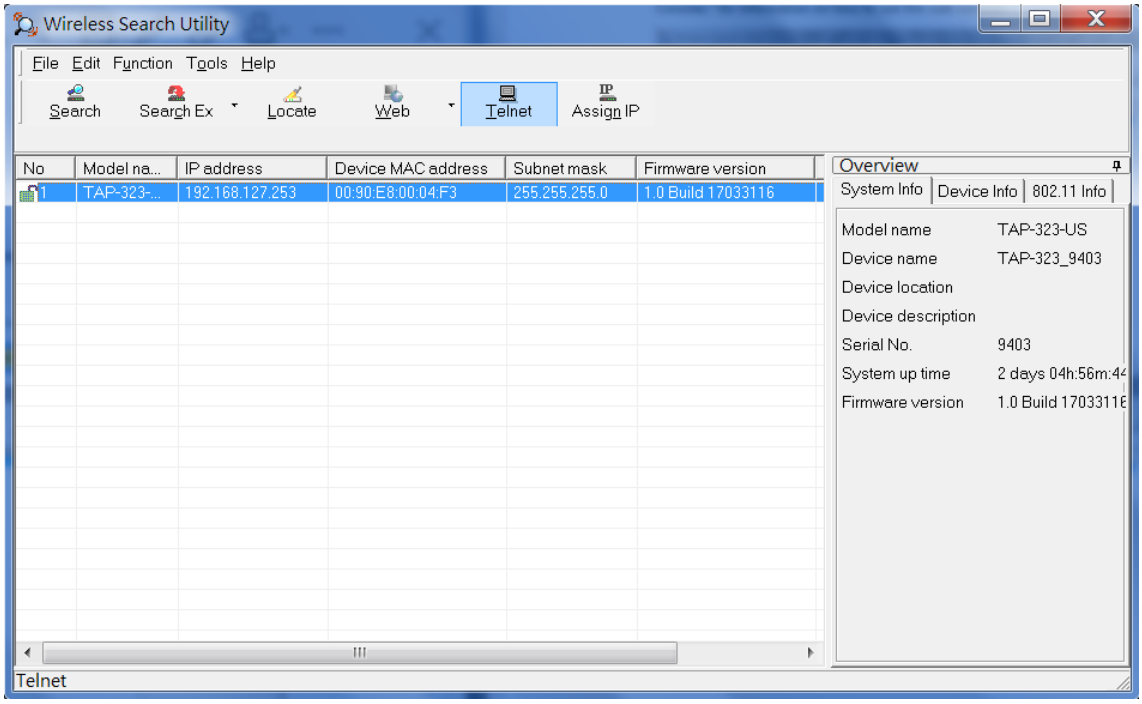
For security purposes, we suggest you can change the wireless search utility login password instead of using the default.



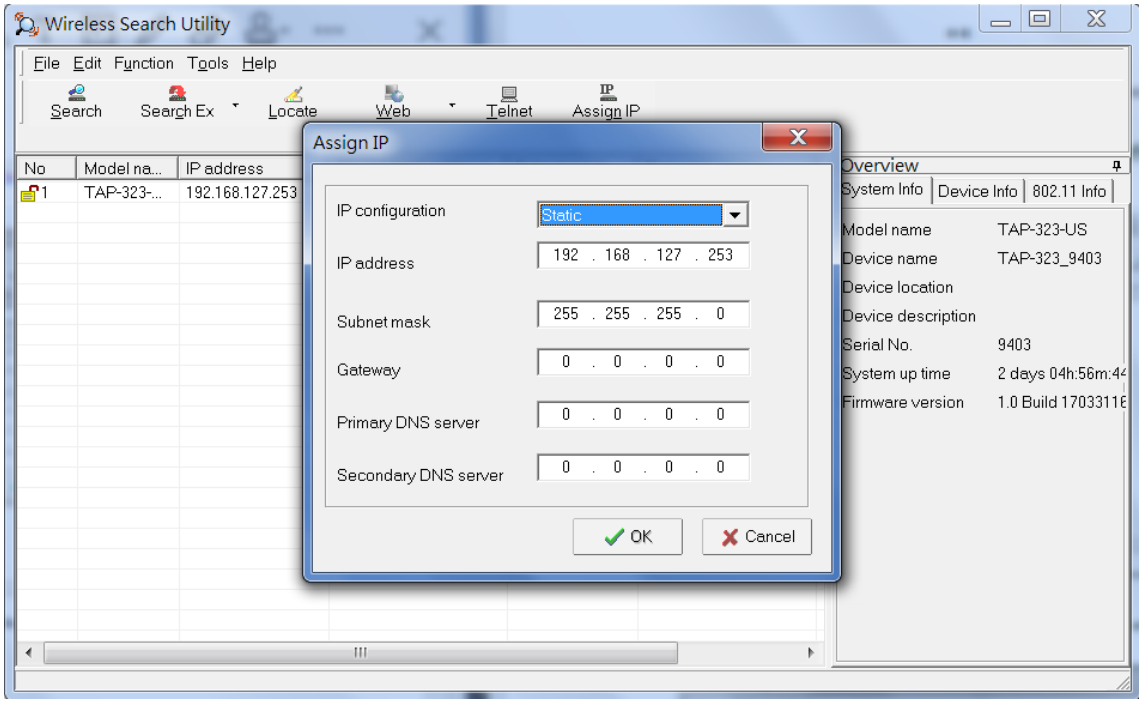
To modify the configuration of the highlighted TAP, click on the Web icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.



Click on **Telnet** if you would like to use telnet to configure your TAPs.



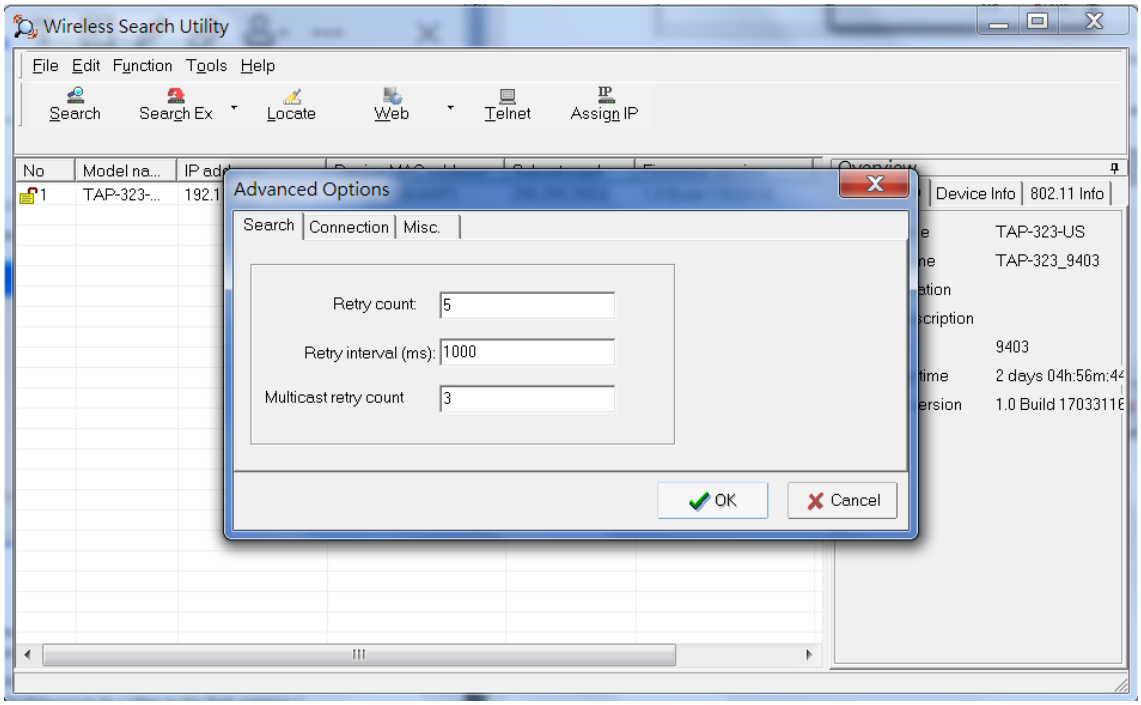
Click **Assign IP** to change the IP setting.



The three advanced options—**Search**, **Connection**, and **Miscellaneous**—are explained below:

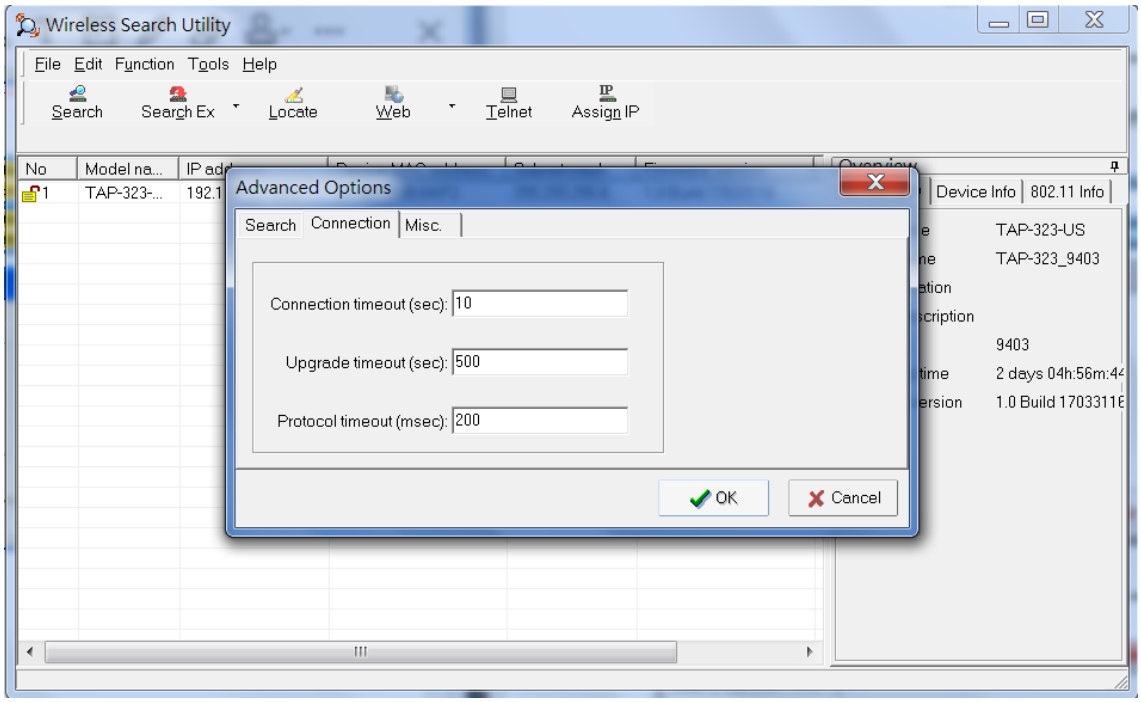
Search

- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time elapsed between retries.



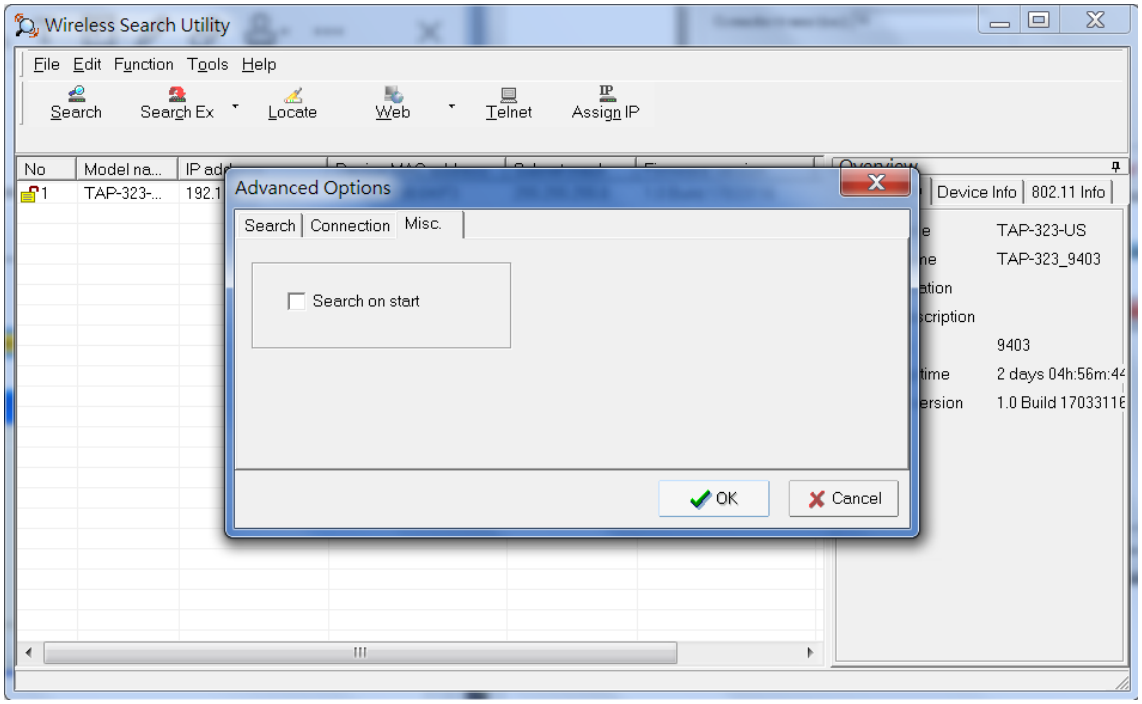
Connection

- **Connection timeout (secs):** Use this option to set the waiting time for the **Default Login**, **Locate**, **Assign IP**, **Upload Firmware**, and **Unlock** to complete.
- **Upgrade timeout (secs):** Use this option to set the waiting time for the connection to disconnect while the firmware is upgrading. Use this option to set the waiting time for the Firmware to write to flash.



Misc.

Search on start: Checkmark this box if you would like the search function to start searching for devices after you log in to the Wireless Search Utility.



5

Using Other Consoles

This chapter explains how to access the TAP-323 for the first time. In addition to HTTP access, there are four ways to access the TAP-323: USB console, Telnet console, SSH console, and HTTPS console. The USB console connection method, which requires using a short USB cable to connect the TAP-323 to a PC's COM port, can be used if you do not know the TAP-323's IP address. The other consoles can be used to access the TAP-323 over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

- **USB Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration via Telnet and SSH Consoles**

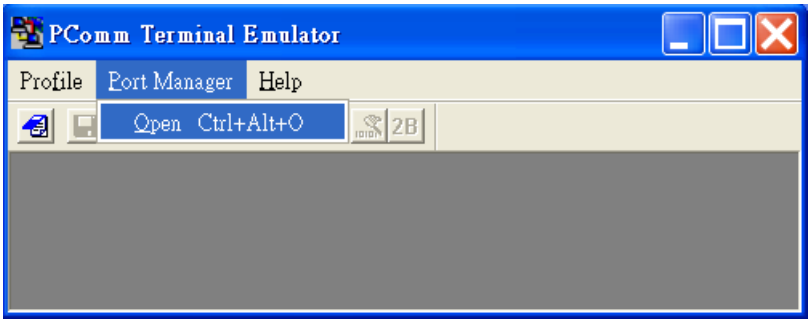
USB Console Configuration (115200, None, 8, 1, VT100)

The USB console connection method, which requires using a short USB cable to connect the TAP-323 to a PC's COM port, can be used if you do not know the TAP-323's IP address. It is also convenient to use USB console configurations when you cannot access the TAP-323 over Ethernet LAN, such as in the case of LAN cable disconnections or broadcast storming over the LAN.

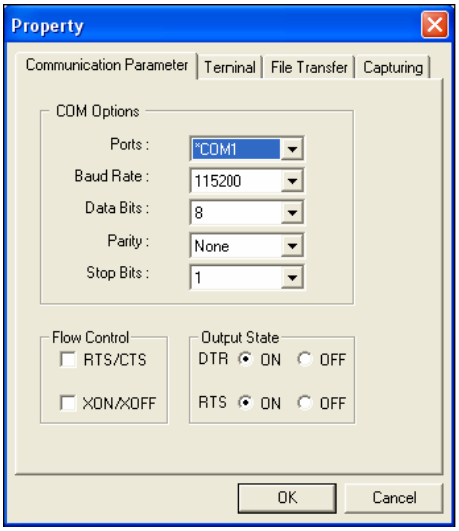
NOTE We recommend using the **Moxa PComm (Lite)** Terminal Emulator, which is available for download at: http://www.moxa.com/product/download_pcommlite_info.htm.

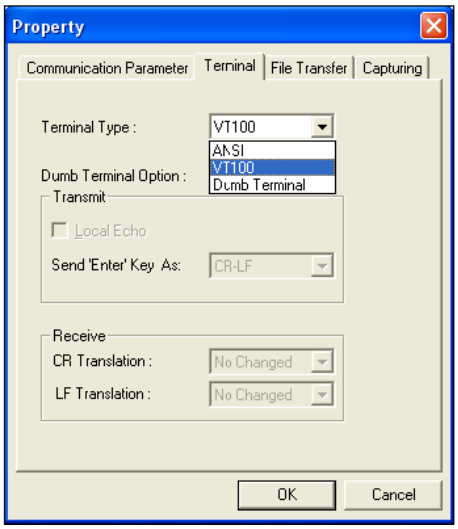
Before running PComm Terminal Emulator, use an M12 5-pin B-coded to USB type A cable to connect the TAP-323's USB console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, take the following steps to access the USB console utility.

1. From the Windows desktop, open the Start menu and run the **PComm Terminal Emulator** from the PComm (Lite) group.
2. In the **Port Manager** menu, select **Open** to open a new connection.



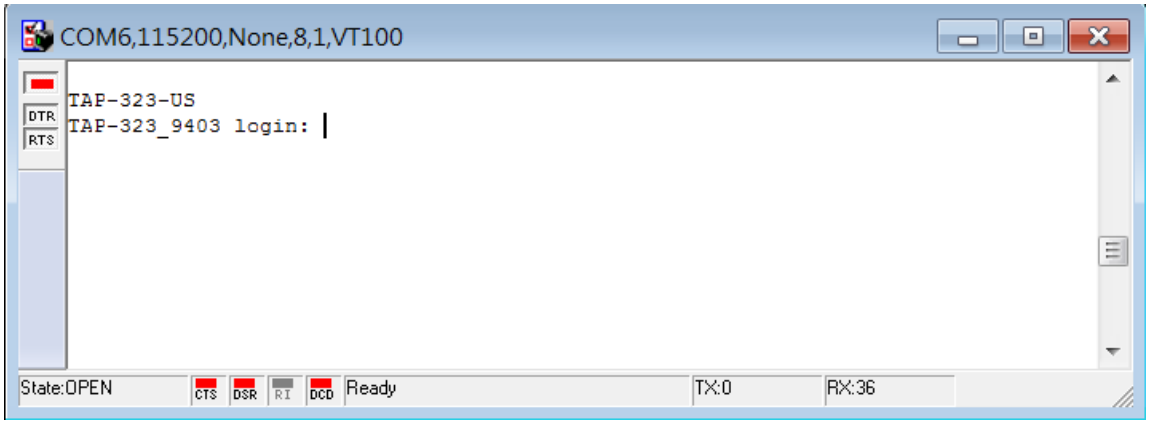
3. The **Communication Parameter** page of the Property window opens. Select the appropriate COM port for Console Connection, **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits. Click on the **Terminal** tab, and select **VT100 (or ANSI)** for Terminal Type. Click on **OK** to continue.



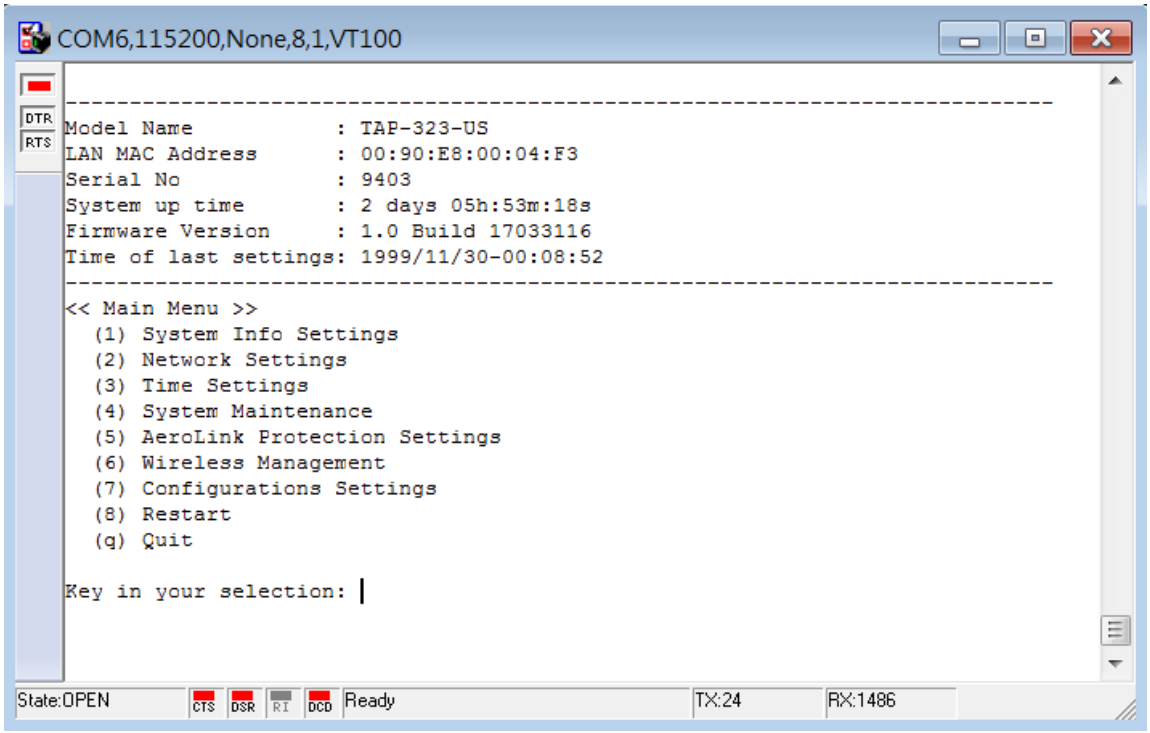


NOTE -The USB driver is available for download at: http://www.moxa.com/product/UPort_2210.htm
-You will see two COM ports. Select the first port (COM1) to connect to the TAP-323 USB console. The COM2 port is reserved for future use.

4. The Console login screen will appear. Log into the USB console with the login name (default: **admin**) and password (default: **moxa**, if no new password is set).



5. The TAP-323's device information and Main Menu will be displayed. Please follow the description on screen and select the administration option you wish to perform.



NOTE To modify the appearance of the PComm Terminal Emulator window, select **Edit → Font** and then choose the desired formatting options.

ATTENTION

If you unplug the USB cable or trigger **DTR**, a disconnection event will be evoked to enforce logout for network security. You will need to log in again to resume operation.

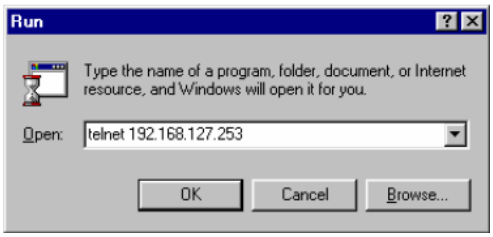
Configuration via Telnet and SSH Consoles

You may use Telnet or SSH client to access the TAP-323 and manage the console over a network. To access the TAP-323's functions over the network from a PC host that is connected to the same LAN as the TAP-323, you need to make sure that the PC host and the TAP-323 are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

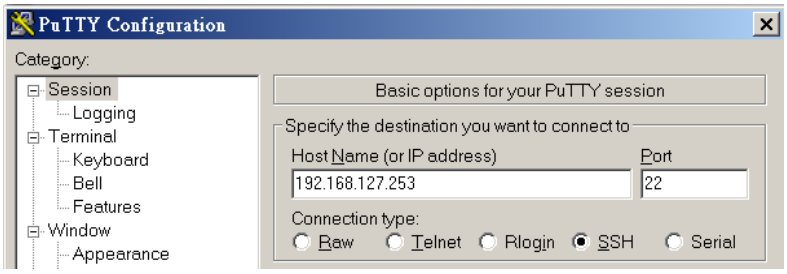
NOTE The TAP-323's default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

Follow the steps below to access the console utility via Telnet or SSH client.

1. From Windows Desktop, go to **Start → Run**, and then use Telnet to access the TAP-323's IP address from the Windows Run window (you may also issue the telnet command from the MS-DOS prompt).

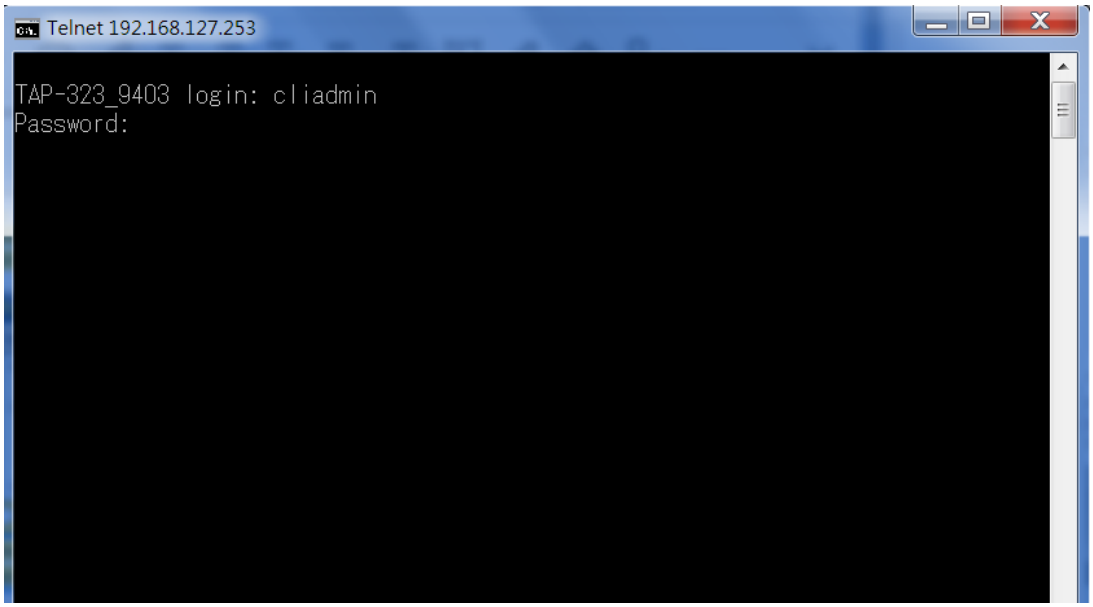


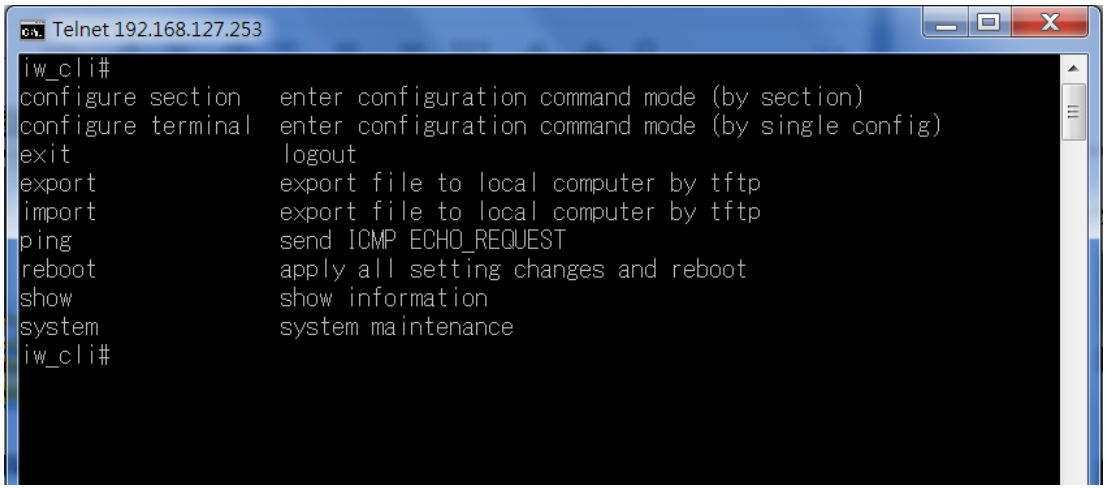
2. When using SSH client (ex. PuTTY), please run the client program (ex. putty.exe) and then input the TAP-323's IP address, specifying **22** for the SSH connection port.



The console login screen is displayed. Refer to the *USB Console Configuration* section for login and administration information.

3. Log in into the command page (default username/password is admin/moxa, if no new password is set). TAP-323 supports the CLI mode. You can use the TAB key to check a related CLI command.



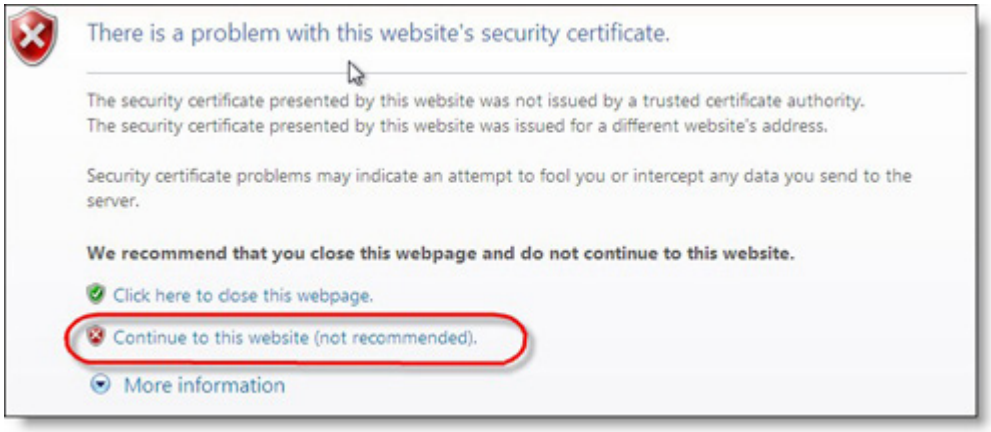


Configuration by Web Browser with HTTPS/SSL

To secure your HTTP access, the TAP-323 supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the TAP-323's web browser interface via HTTPS/SSL.

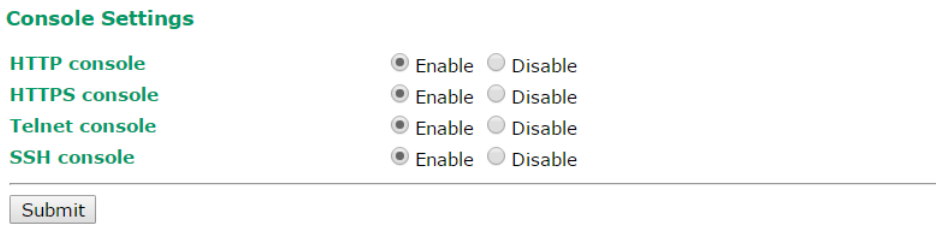
1. Open your web browser and type https://<TAP-323's IP address> in the address field. Press **Enter** to establish the connection.

2. Click on **continue to this website**.
   The protocol in the URL changes to HTTPS. You can now enter your username and password to login into the function page.



Disabling Telnet and Browser Access

If you are connecting the TAP-323 to a public network but do not intend to use its management functions over the network, then we suggest disabling both Telnet Console and Web Configuration. Please run **Maintenance → Console Settings** to disable them, as shown in the following figure.



A

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you manage your TAP-323s and plan your industrial wireless network better.

The following topics are covered in this appendix:

- **Beacon**
- **DTIM**
- **Fragment**
- **RTS Threshold**
- **STP and RSTP**
  - The STP/RSTP Concept

Beacon

A beacon is a packet broadcast by the AP to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination address, a time stamp, Delivery Traffic Indicator Maps (DTIM), and the Traffic Indicator Message (TIM). Beacon Interval indicates the frequency interval of AP.

DTIM

Delivery Traffic Indication Map (DTIM) is contained in beacon frames. It is used to indicate that broadcast and multicast frames buffered by the AP will be delivered shortly. Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power.

Fragment

A lower setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

RTS Threshold

RTS Threshold (256-2346) – This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2,346. When you encounter inconsistent data flow, only minor modifications are recommended.

STP and RSTP

The STP/RSTP Concept

The **Spanning Tree Protocol (STP)** was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. The STP protocol is part of the IEEE802.1D standard, 1998 Edition bridge specification.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE802.1w-2001 standard. RSTP provides the following benefits:

• The topology of a bridged network will be determined much more quickly compared to STP.

• RSTP is backward compatible with STP, making it relatively easy to deploy. For example:

- Defaults to sending 802.1D-style BPDUs if packets with this format are received.
- STP (802.1D) and RSTP (802.1w) can operate on the LAN ports and WLAN ports of the same TAP-323.

This feature is particularly helpful when the TAP-323 connects to older equipment, such as legacy switches.

B

Supporting Information

This chapter presents additional information about this product. You can also learn how to contact Moxa for technical support.

The following topics are covered in this appendix:

- **Firmware Recovery**
  - Federal Communication Commission Interference Statement
  - Canada, Industry Canada (IC) Notices
  - RED Compliance Statement

Firmware Recovery

When the LEDs of **FAULT**, **Signal Strength**, **CLIENT**, **BRIDGE** and **WLAN** all light up simultaneously and blink at one-second interval, it means the system booting has failed. It may result from some wrong operation or uncontrollable issues, such as an unexpected shutdown during firmware update. The TAP-323 is designed to help administrators recover such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the TAP-323's ES-232 console with **115200bps and N-8-1**. You will see the following message shown on the terminal emulator every one second.

```
Section userdisk Cksum error = 0xa5feadde --> 0x658c5051
Press Ctrl-C to enter Firmware Recovering Process.......
Press Ctrl-C to enter Firmware Recovering Process.......
Press Ctrl-C to enter Firmware Recovering Process.......
Press Ctrl-C to enter Firmware Recovering Process
Press Ctrl-C to enter Firmware Recovering Process.......
Press Ctrl-C to enter Firmware Recovering Process.......
Press Ctrl-C to enter Firmware Recovering Process.......
Press Ctrl C to enter Firmware Recovering Process.......
```

Press **Ctrl - C** and the following message will appear.

```
================================================================================
IP address of DUT : 0.0.0.0
IP address of TFTP server : 0.0.0.0
File name : moxa.rom
================================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection : (1-2):
```

Enter **2** to change the network setting. Specify the location of the TAP-323's firmware file on the TFTP server and press **y** to write the settings into flash memory.

```
================================================================================
IP address of DUT : 0.0.0.0
IP address of TFTP server : 0.0.0.0
File name : moxa.rom
================================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection : (1-2):2

Now Local IP address = 0.0.0.0
User change Local IP : 192.168.127.253
Remote Server IP address = 0.0.0.0
User change IP address of TFTP server: 192.168.127.100
```

TAP-323 restarts, and the "Press Ctrl-C to enter Firmware Recovery Process…" message will reappear. Press **Ctrl-C** to enter the menu and select **1** to start the firmware upgrade process.

```
================================================================================
IP address of DUT : 192.168.127.253
IP address of TFTP server : 192.168.127.100
File name : moxa.rom
================================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection : (1-2):1
```

Select **0** in the sub-menu to load the firmware image via LAN, and then enter the file name of the firmware to start the firmware recovery.

```
==========================================================================
IP address of DUT : 192.168.127.253
IP address of TFTP server : 192.168.127.100
File name : moxa.rom
==========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection : (1-2):1
Trying eth0
dup 1 speed 1000
Using eth0 device
TFTP from server 192.168.127.100; our IP address is 192.168.127.253
Filename 'moxa.rom'.
Load address: 0x80060000
Loading: T ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
         ##################################################################
```

DoC (Declaration of Conformity)

Federal Communication Commission Interference Statement

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

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

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC 15.407(e): Within the 5.15-5.25 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

Canada, Industry Canada (IC) Notices

This device complies with Industry Canada's license-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Warning:
Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Canada, avis d'Industry Canada (IC)

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Devraient également être informés les utilisateurs que les radars à haute puissance sont désignés comme utilisateurs principaux (c.-à-utilisateurs prioritaires) des bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient provoquer des interférences et / ou endommager les appareils LE-LAN.

Radio Frequency (RF) Exposure Information

The radiated output power of this wireless device is below the Industry Canada (IC) radio frequency exposure limits. This wireless device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions (i.e., the device antennas are greater than 20 cm from a person's body).

Informations concernant l'exposition aux fréquences radio (RF)

La puissance de sortie émise par l'appareil de sans fil est inférieure à la limite d'exposition aux fréquences radio d'Industry Canada (IC). Utilisez l'appareil de sans fil de façon à minimiser les contacts humains lors du fonctionnement normal.

Ce périphérique a également été évalué et démontré conforme aux limites d'exposition aux RF d'IC dans des conditions d'exposition à des appareils mobiles (antennes sont supérieures à 20 cm à partir du corps d'une personne).

Antenna Gain and RF Radiated Power

The following sections contain the FCC rules regarding adapting the product transmission power based on the antenna used. This radio transmitter FCCID: SLE-WAPN008 has been approved by FCC to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna List

Antenna Part No.	Antenna Type	Maximum Antenna Gain*
ANT-WDB-O-2 BK	Dipole	2.9 dBi for 2.4 GHz 2.34dBi for 5 GHz
ANT-WDB-ANM-0502	Dipole	4.62 dBi for 2.4 GHz 1.41dBi for 5 G

RED Compliance Statement

Moxa declares that the apparatus TAP-323 complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The essential requirements laid down in Directive 1999/5/EC which are relevant to fixed-line terminal equipment, i.e. to ensure the protection of health and safety of persons and of domestic animals and the protection of prop-erty and an adequate level of electromagnetic compatibility, are appropriately covered by Directive 2014/35/EU of the European Parliament and of the Council and Directive 2014/30/EU of the European Parliament and of the Council . This Directive should therefore not apply to fixed-line terminal equipment.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: only channels 10, 11, 12, and 13.