Moxa Tough AP TAP-6226 User's Manual

Edition 3.0, September 2017

www.moxa.com/product

Moxa Tough AP TAP-6226 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 AirWorks TAP-6226 with dual-RF wireless capability allows wireless users to access network resources more reliably. The TAP-6226 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-6226 outdoor dual-RF track-side wireless AP provides a complete and flexible solution for railway train-to-ground applications in demanding environments. The TAP-6226 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-6226 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-6226 has two AC power inputs for redundancy to increase the reliability of the power supply, and can be powered via PoE. The TAP-6226 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 CBTC and CCTV.

Package Checklist

Moxa's TAP-6226 ships with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- TAP-6226 with protective caps for LAN/fiber/console ports
- Accessory pack, including wall-mounting kit and fiber panel mounting kit
- Quick installation guide (printed)
- Warranty card

NOTE The items above come with the standard TAP-6226. The package contents may vary for customized versions.

Product Features

- EN 50121-4 railway certified
- Controller-based Turbo Roaming (AP)
- Dual-RF design
- Advanced wireless security
  - 64-bit and 128-bit WEP/WPA/WPA2
  - SSID Hiding / IEEE 802.1x / RADIUS
  - Packet access control and filtering
- Turbo Chain* supported on fiber ports
- Diverse selection of antennas
- RS-232 console port
- -40 to 75°C operating temperature range
- 110 VAC power input
- Wall mountable
- IP68 protected high-strength metal housing

***100 ms recovery time**

Product Specifications

WLAN Interface

Standards:

IEEE 802.11a/b/g for Wireless LAN
IEEE 802.11i for Wireless Security
IEEE 802.3 for 10BaseT
IEEE 802.3u for 100BaseTX
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 (802.11abg, 11 channels)
5.18 to 5.24 GHz (802.11a, 4 channels)
5.26 to 5.825 GHz (optional)
EU:
2.412 to 2.472 GHz (802.11abg, 13 channels)
5.18 to 5.24 GHz (802.11a, 4 channels)
5.26 to 5.825 GHz (optional)
*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

TX Transmit Power:

802.11b:
Typ. 26±1.5 dBm @ 1 to 11 Mbps
802.11g:
Typ. 26±1.5 dBm @ 6 to 24 Mbps, Typ. 25±1.5 dBm @ 36 Mbps, Typ. 24±1.5 dBm @ 48 Mbps, Typ. 23±1.5 dBm @ 54 Mbps
802.11a:
Typ. 26±1.5 dBm @ 6 to Mbps, Typ. 25±1.5 dBm @ 36Mbps, Typ. 24±1.5 dBm @ 48 Mbps, Typ. 23±1.5 dBm @ 54 Mbps

RX Sensitivity:

802.11b:
-97 dBm @ 1 Mbps, -94 dBm @ 2 Mbps, -92 dBm @ 5.5 Mbps, -90 dBm @ 11 Mbps
802.11g:
-93 dBm @ 6 Mbps, -91 dBm @ 9 Mbps, -90 dBm @ 12 Mbps, -88 dBm @ 18 Mbps, -84 dBm @ 24 Mbps, -80 dBm @ 36 Mbps, -76 dBm @ 48 Mbps, -74 dBm @ 54 Mbps
802.11a:
-90 dBm @ 6 Mbps, -89 dBm @ 9 Mbps, -89 dBm @ 12 Mbps, -85 dBm @ 18 Mbps, -83 dBm @ 24 Mbps, -79 dBm @ 36 Mbps, -75 dBm @ 48 Mbps, -74 dBm @ 54 Mbps

Protocol Support

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

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 A-coded 5-pin male connector

Fiber Ports: 2, 100BaseSFP slot

Fiber Module: 100Base multi-mode 1300 nm wavelength with LC connector for 4 km transmission (50/125 µm or 62.5/125 µm 800 MHz-km @ 1300 nm wavelength)

LED Indicators: PWR1, PWR2, PoE1-4, FAULT, STATE, HEAD, TAIL, LAN1-6, WLAN1, WLAN2

Physical Characteristics

Housing: Metal, IP68 protection

Weight: 10 kg

Dimensions: 322 x 282 x 159 mm

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

Power Consumption:

AC input: 110 to 220 VAC, 50 to 60 Hz, 0.68 A (max.)

DC input: 110 to 220 VDC, 0.68 A (max.)

Maximum 74.8 watts

Reverse Polarity Protection: Present

Overload Current Protection: Present

Standards and Certifications

Safety: UL 60950-1, EN 60950-1

EMC: EN 301 489-1/17; FCC Part 15, Subpart B; EN 55032/55024

Radio: EN 300 328, EN 301 893

Rail Traffic: EN 50155*, EN 50121-1/4

*Complies with a portion of EN 50155 specifications. Please contact Moxa or a Moxa distributor for details.

Note: Please check Moxa's website for the most up-to-date certification status.

Reliability

MTBF (mean time between failures):

TAP-6226-TC: 382,735 hrs

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty

ATTENTION

The TAP-6226 is NOT a portable mobile device and should be located at least 20 cm away from the human body. The TAP-6226 is NOT designed for the general consumer. A well-trained technician is required to safely deploy TAP-6226 units and establish a wireless network.

Patent http://www.moxa.com/doc/operations/Moxa_Patent_Marking.pdf

Functions

LED Indicators

The LEDs on the front panel of TAP-6226 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-6226 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-6226 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.
FAULT	Red	On	Relay is event-triggered.
		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
STATE	Green/Red	Green	System startup is complete and the system is in operation.
		Green (blinking at 1-second intervals)	The AWK Search Utility has located the AWK.
		Red	Booting or error condition.
HEAD	Green	On	TAP is set as HEAD TAP in Turbo Chain.
		Blinking	TAP head port link is broken.
		Off	TAP is not set as HEAD TAP in Turbo Chain.
TAIL	Green	On	TAP is set as TAIL TAP in Turbo Chain.
		Blinking	TAP TAIL port link is broken or is in blocking state
		Off	TAP is not set as TAIL TAP in Turbo Chain
WLAN 1	Green/Amber	Green On	WLAN is functioning in **Slave** mode.
		Green, blinking	WLAN is transmitting data in **Slave** mode.
		Amber On	WLAN is functioning in **AP/Bridge/Master** mode.
		Amber, blinking	WLAN is transmitting data in **AP/Bridge/Master** mode.
		Off	WLAN is not in use or is not working properly.
WLAN 2	Green/Amber	Green On	WLAN is functioning in **Slave** mode.
		Green, blinking	WLAN is transmitting data in **Slave** mode.
		Amber On	WLAN is functioning in **AP/Bridge/Master** mode.
		Amber, blinking	WLAN is transmitting data in **AP/Bridge/Master** mode.
		Off	WLAN is not in use or is not working properly.
LAN 1-6	Yellow/Green	Yellow, on	LAN port's 10 Mbps link is active.
		Yellow, blinking	Data is being transmitted at 10 Mbps.
		Yellow, off	LAN port's 10 Mbps link is inactive.
		Green, on	LAN port's 100 Mbps link is active.
		Green, blinking	Data is being transmitted at 100 Mbps.
		Green, off	LAN port's 100 Mbps link is inactive.
PoE1-4	Green	On	PSE port is supplying power to PD.
		Off	PSE port is not supplying power.

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 6.

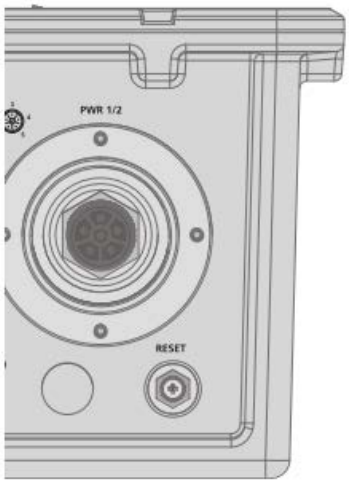
Reset Button

The **RESET** button is located on the bottom panel of the TAP-6226. You can reboot the TAP-6226 or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

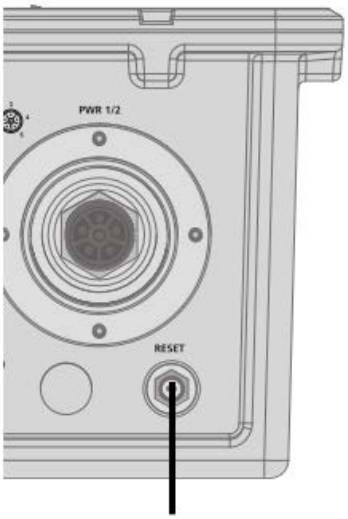
- **System reboot:** Hold the **RESET** button down for less than 5 seconds and then release.
- **Reset to factory default:** Hold the **RESET** button down for over 5 seconds until the **STATE** LED starts blinking green. Release the button to reset the TAP-6226.

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 AirWorks TAP-6226 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**
- **Function Guide Map**

First-time Installation and Configuration

Before installing the TAP-6226, make sure that all items in the Package Checklist are in the box. In addition, you will need access to a notebook computer or PC equipped with an Ethernet port. The TAP-6226 has a default IP address that you must use when connecting to the device for the first time.

Step 1: Connect to a power source.

The TAP-6226 can be powered through the 110/220 VAC power input using an M23 power cable (must be purchased separately).

Step 2: Connect the TAP-6226 to a notebook or PC.

Since the TAP-6226 supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the TAP-6226 to a computer. If the LED indicator on TAP-6226's LAN port lights up, it means the connection is established.

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

Set an IP address on the same subnet as the TAP-6226. Since the TAP-6226's default IP address is **192.168.127.253**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

NOTE After you select **Maintenance → Load Factory Default** and click the **Submit** button, the TAP-6226 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-6226

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 Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on the **Login** button:

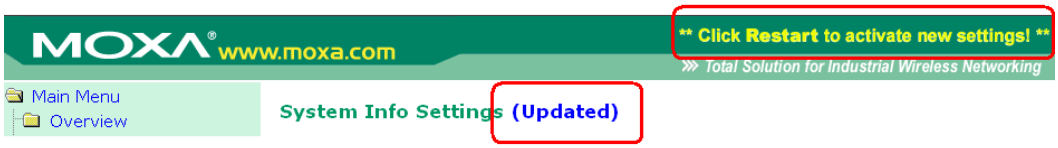
NOTE Default user name and password:

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. (Firmware Version 1.6 password: moxa; Firmware Versions 1.0 to 1.5 password: root)

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.



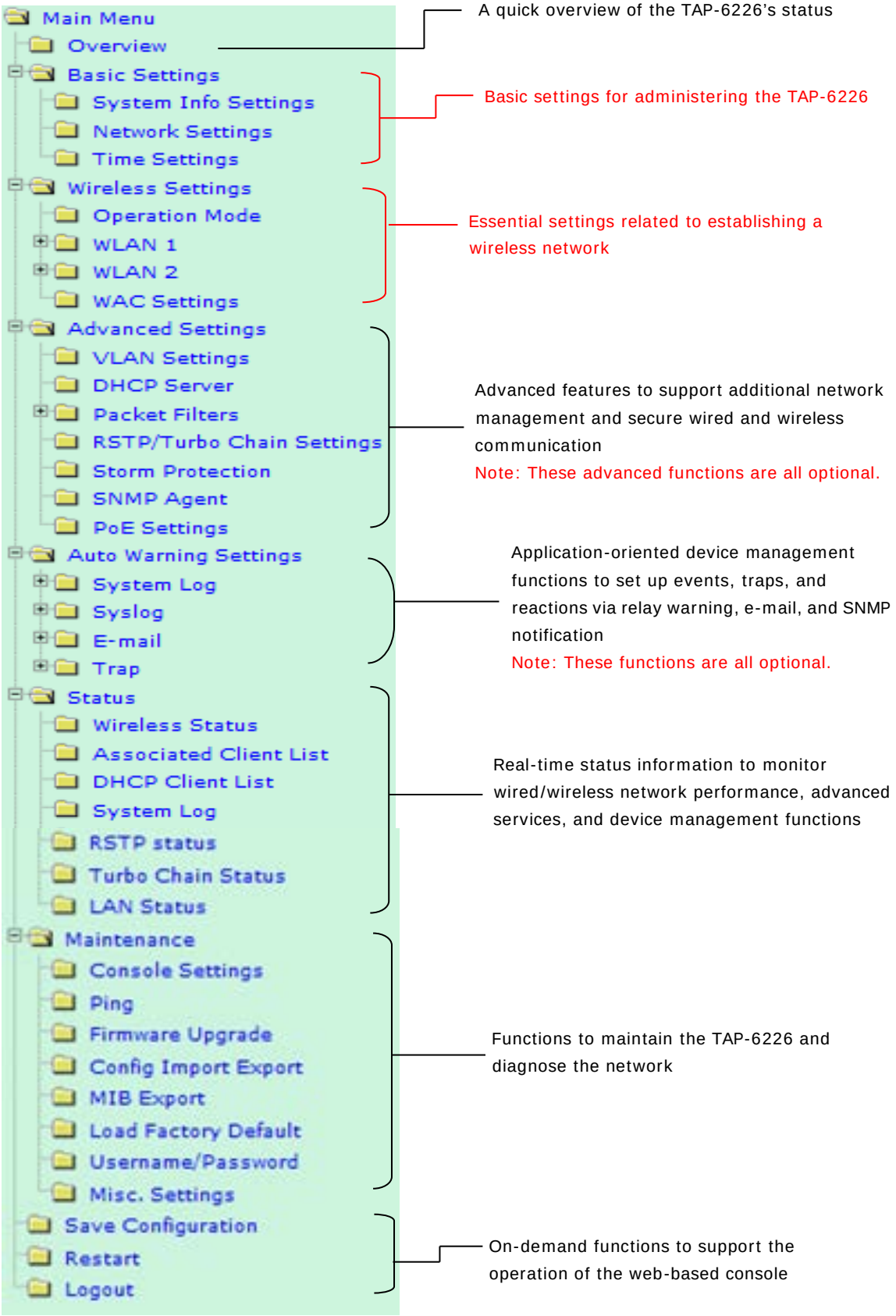
To make the changes effective, click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the TAP-6226 to complete its restart process.

Step 5: Select the operation mode

By default, the TAP-6226'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-6226's operation mode can be found in Chapter 3.

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-6226, 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
- **Advanced Settings**
  - Using Virtual LAN
  - DHCP Server (for AP operation mode's AP mode only)
  - Packet Filters
  - RSTP/Turbo Chain Settings (for Master or Slave mode only)
  - Storm Protection
  - 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
  - Misc. Settings
- **Save Configuration**
- **Restart**
- **Logout**

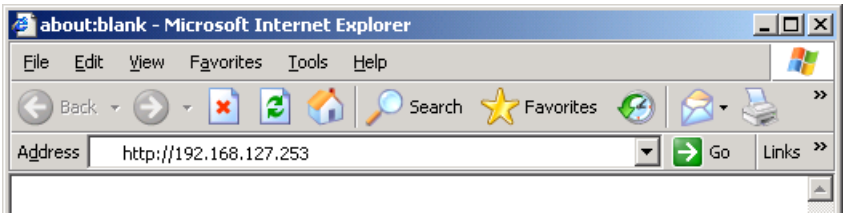
Configuration by Web Browser

Moxa TAP-6226'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-6226's management and monitoring functions from a PC host connected to the same LAN as the TAP-6226, you must make sure that the PC host and TAP-6226 are on the same logical subnet. Similarly, if the TAP-6226 is configured for other VLAN settings, you must make sure your PC host is on the management VLAN. The Moxa TAP-6226's default IP is **192.168.127.253**.

Follow the steps below to access the TAP-6226's web-based console management.

1. Open your web browser (e.g., Internet Explorer) and type the TAP-6226's IP address in the address field. Press **Enter** to establish the connection.

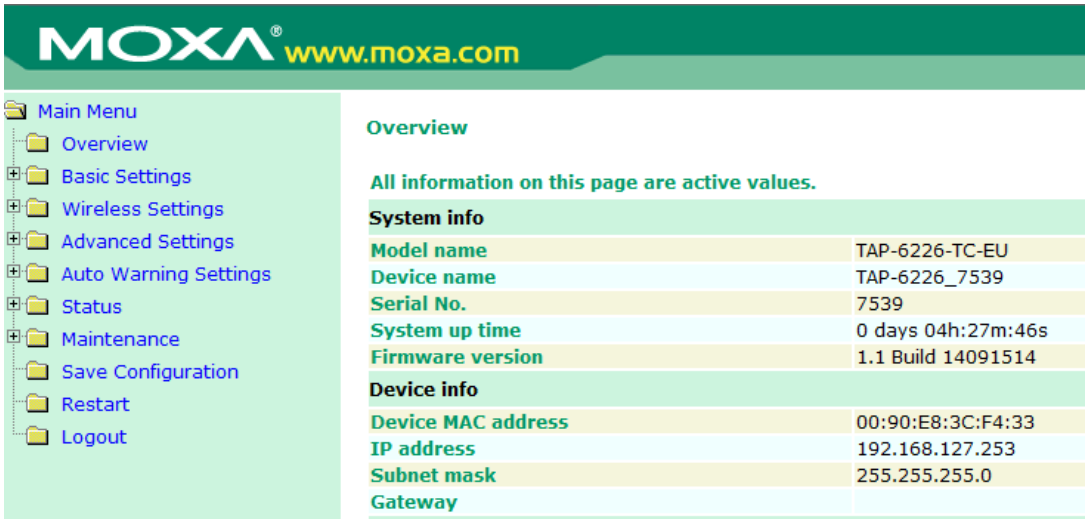


2. The Web Console Login page will open. Enter the password (User Name is set as **admin**; the default password is **moxa** if a new password has not been set.) and then click **Login** to continue.

NOTE Firmware Version 1.6 password: moxa
Firmware Versions 1.0 to 1.5 password: root

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-6226 are both displayed in the web page title. This information can help you identify multiple TAP-6226 units.

You can use the menu tree on the left side of the window to open the function pages to access each of TAP-6226's functions.



In the following sections, we will review each of the TAP-6226'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-6226 is shown as TAP-6226-XX where XX indicates the country code. The country code represents the TAP-6226 version and which bandwidth it uses. We use **TAP-6226-TC** 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-6226.

ATTENTION

For security reasons, you will need to log back into the TAP-6226 after a 3-minute time-out.

Overview

The **Overview** page summarizes the TAP-6226's current status. The information is categorized into the groups: **System info**, **Device info**, and **802.11 info**.

Overview

All information on this page are active values.

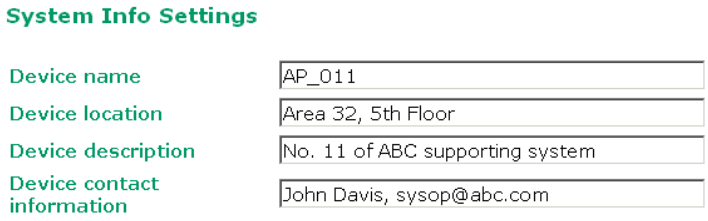
System info		
Model name	TAP-6226-TC-EU	
Device name	TAP-6226_7539	
Serial No.	7539	
System up time	0 days 04h:27m:46s	
Firmware version	1.1 Build 14091514	
Device info		
Device MAC address	00:90:E8:3C:F4:33	
IP address	192.168.127.253	
Subnet mask	255.255.255.0	
Gateway		
802.11 info		
Country code	EU	
Operation mode	AP-Client - AP (WLAN 1)	AP-Client - AP (WLAN 2)
Channel	6	11
RF type	B/G Mixed	B/G Mixed
SSID	MOXA_1	MOXA_2

Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the TAP-6226.

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-6226s 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-6226 units.	TAP-6226_<Serial No. of this TAP-6226>

Device location

Setting	Description	Factory Default
Max. 31 Characters	To specify the location of different TAP-6226 units.	None

Device description

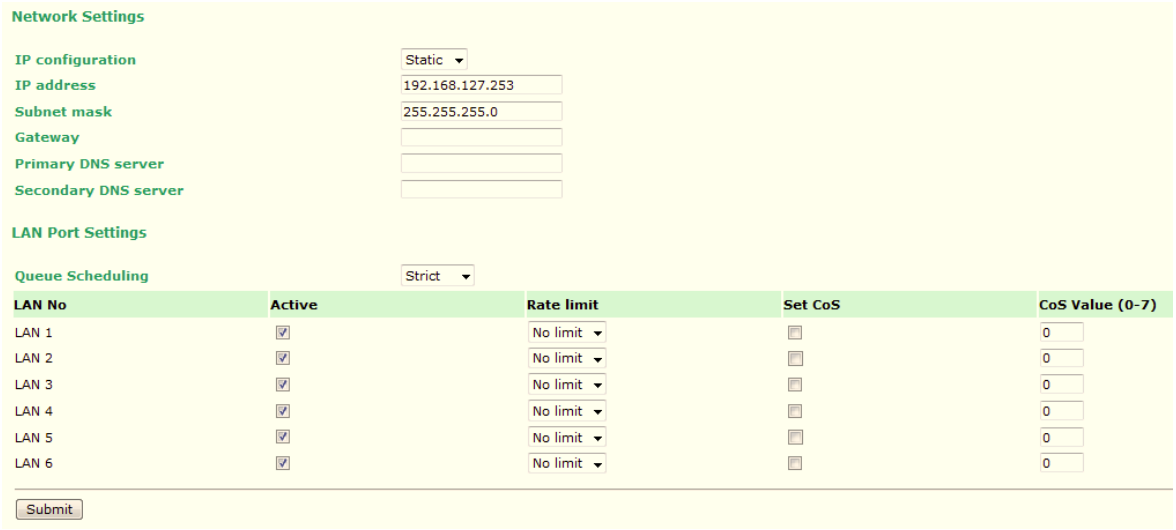
Setting	Description	Factory Default
Max. 31 Characters	Use this space to record a more detailed description of the TAP-6226	None

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-6226.	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-6226'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-6226's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the TAP-6226's IP address manually.	

IP address

Setting	Description	Factory Default
TAP-6226's IP address	Identifies the TAP-6226 on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
TAP-6226's subnet mask	Identifies the type of network to which the TAP-6226 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-6226's default gateway	The IP address of the router that connects the LAN to an outside network.	None

Primary/ Secondary DNS server

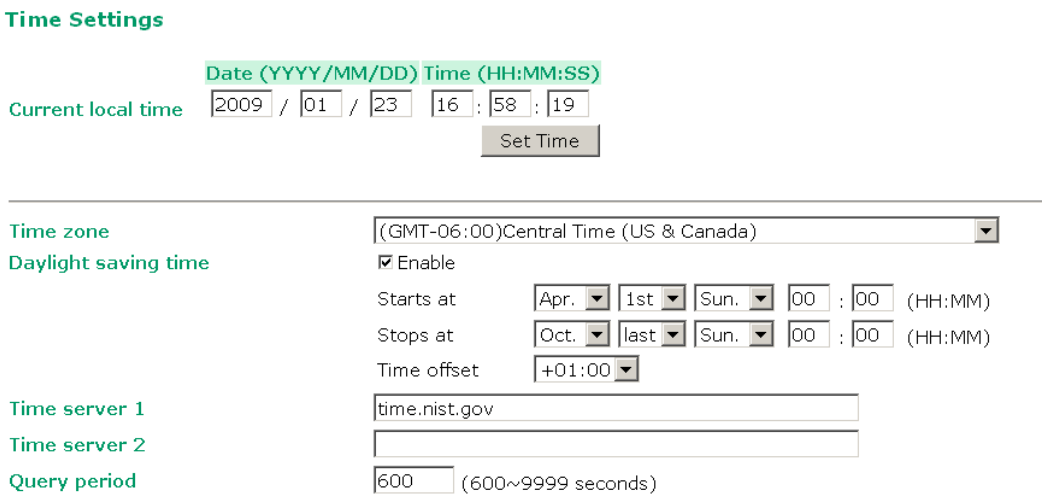
Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the TAP-6226's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. 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
Active	This setting activates or deactivates the LAN port for queue scheduling.	active
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	Enable or disable CoS mapping	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

Time Settings

The TAP-6226 has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as Auto warning can add real-time information to the message.



Current local time shows the TAP-6226's system time when you open this web page. You can click on the **Set Time** button to activate the update after adjusting the date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local time settings will be immediately activated in the system without running Save and Restart.

NOTE The TAP-6226 has a real time clock (RTC). Users are strongly recommended to update the **Local time** for the TAP-6226 after initial setup or long-term shutdown, especially when the network does not have an Internet connection for accessing the 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.	None (yyyy/mm/dd hh:mm:ss format; 24-hour format.)

Time zone

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

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.	None

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

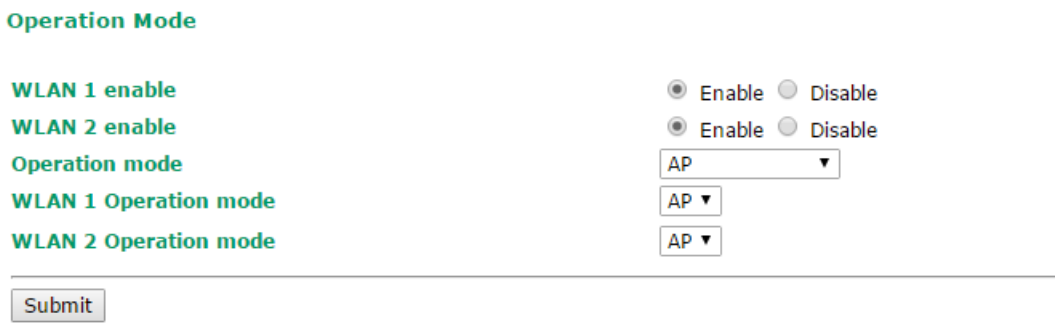
The essential settings for wireless networks are presented in this function group. You must configure the settings correctly before establishing your wireless network.

Operation Mode

The TAP-6226 supports two operation modes that are used for different wireless network applications.

AP

AP mode provides a more flexible topology to allow the user to configure the 2 RF modules for an AP.



Matching Table for AP's WLANs:

WLAN 1	WLAN 2	Allowable Setting
AP	AP	Allow

NOTE TAP-6226 units are meant to be used as trackside access points and hence starting with the firmware version 1.5 the client operation mode has been removed.

Wireless Bridge

A bridge is a network component that connects two networks. The TAP-6226'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-6226's dual RF bridge concept is different from using a single RF, because the TAP-6226 has dual RFs that offer users a cascade link to bridge the two ends without narrowing down the throughput.

WLAN 1/WLAN 2 Enable

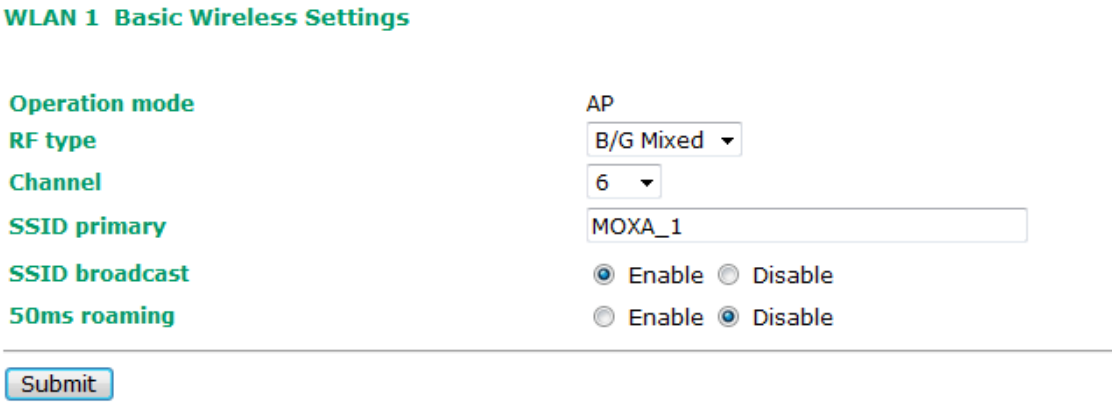
Setting	Description	Factory Default
WLAN1 enable	Turn on/off the WLAN 1 radio by selecting Enable or Disable	Enable
WLAN2 enable	Turn on/off the WLAN 2 radio by selecting Enable or Disable	

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.	

Basic Wireless Settings

The following figure shows the Basic Wireless Settings page. The parameters and options are described below:



RF type

Setting	Description	Factory Default
A	Supports IEEE 802.11a standard only	B/G Mixed
B	Supports IEEE 802.11b standard only	
G	Supports IEEE 802.11g standard only	
B/G Mixed	Supports both IEEE 802.11b/g standards, but 802.11g's throughput may suffer when 802.11b clients are on the network	

Channel (for AP, or Master Mode only)

Setting	Description	Factory Default
Available channels vary with RF type	TAP-6226 plays the role of wireless AP	6 (in B/G Mixed mode)

SSID Primary

Setting	Description	Factory Default
Max. 31 Characters	The SSID of a client and the SSID of the AP must be identical for them to communicate with each other.	MOXA_1 for WLAN1, MOXA_2 for WLAN2

SSID broadcast (for AP, or Master Mode only)

Setting	Description	Factory Default
Enable/Disable	Determines whether or not the SSID will be broadcast.	Enable

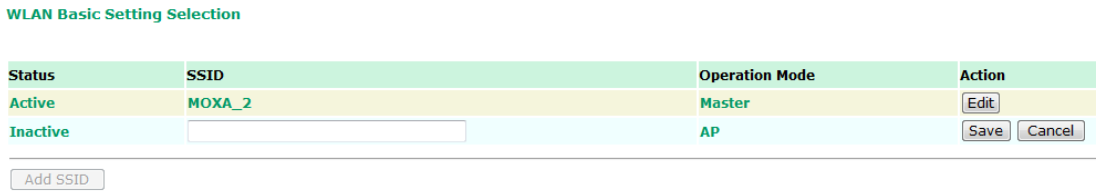
50ms roaming (WAC-1001 and/or WAC-2004 required as controller)

Setting	Description	Factory Default
Enable/Disable	Determines whether or not this AP interface is activated for controller based Turbo Roaming.	Disable

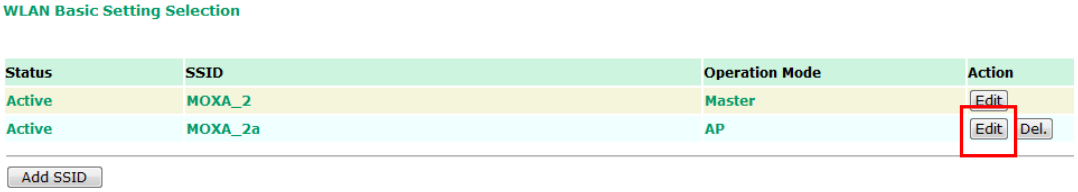
Wireless Bridge Mode's Master

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-6226 provides four standardized wireless security modes: Open, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2. The TAP-6226 supports several security modes with different encryption types:

- **Open:** No authentication, no data encryption.
- **WEP**: Static WEP (Wired Equivalent Privacy) keys must be manually configured.
- **WPA/WPA2-Personal**: Also known as WPA/WPA2-PSK. You 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 IEEE802.1X. The TAP-6226 can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.

The following figure shows the WLAN1/2 Security Settings page. The parameters and options are described below:

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

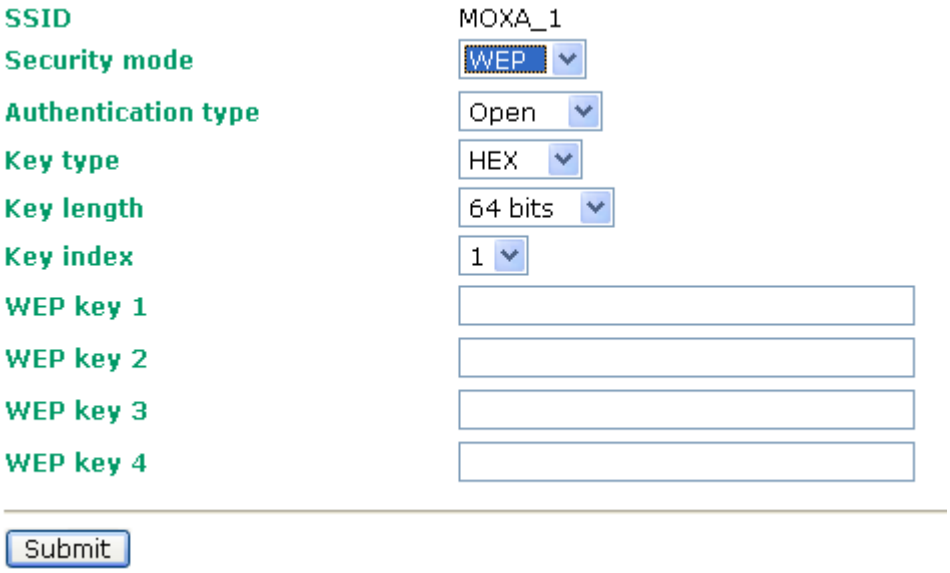
For security reasons, it is highly recommended that the security mode should be set to an option other than Open System. When the security mode is set to Open System, no authentication or data encryption will be performed.

WEP

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption (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 often 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-6226 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 one of two ***Key types***, HEX or 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

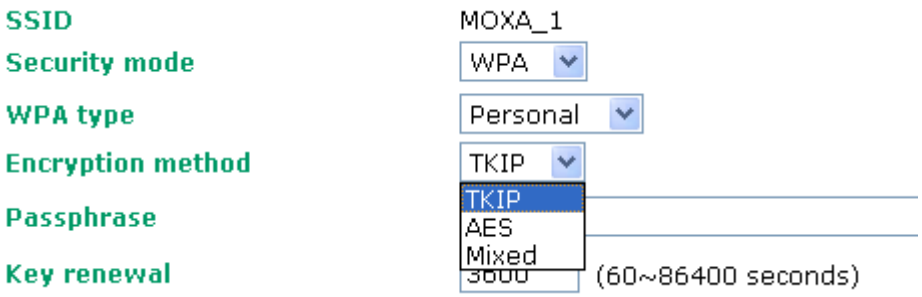
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13 chars **HEX type:** 64 bits: 10 HEX chars 128 bits: 26 HEX chars	A string that can be used as a WEP seed for an RC4 encryption engine.	None

WPA / WPA2-Personal

WPA (Wi-Fi Protected Access) and WPA2 are significantly improved encryption methods over WEP. 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 changes regularly so that the 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-6226 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 complex and as long as possible. The number of ASCII characters of the Passphrase must be at least 8 and can go up to 63. For security reasons, you should only disclose this passphrase to users who need to know 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	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. Note: This option is available in AP or Master mode only, and cannot support AES-enabled clients.	

Passphrase

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

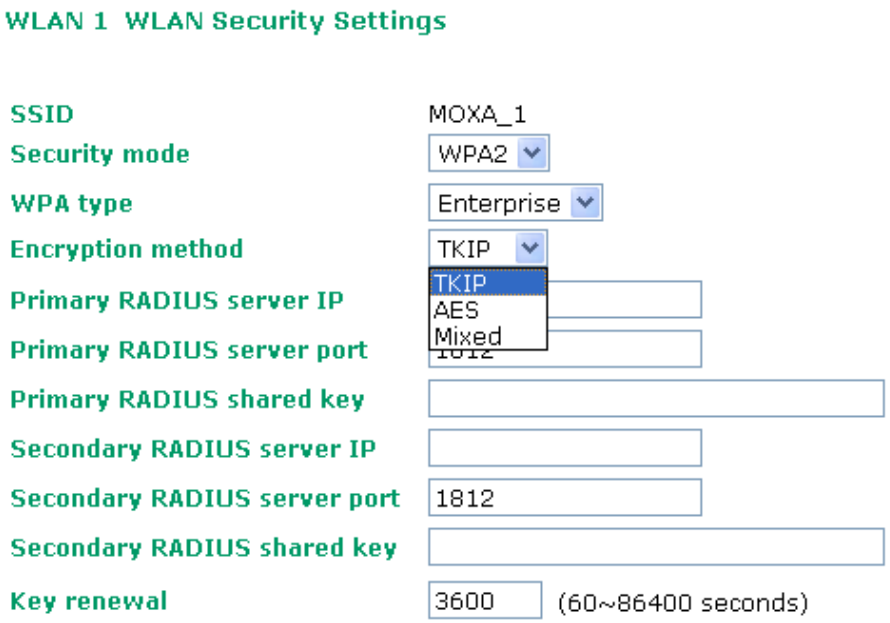
Key renewal (for AP or Master Mode only)

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 tells the wireless AP how often it should change the encryption keys. Generally speaking, the security level will be higher if you set this value to a smaller value, since the encryption keys will be changed more frequently. The default value is 3600 seconds (60 minutes). You can consider using a longer time period if traffic is low.

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 in AP or Master mode only, and cannot support AES-enabled clients.

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

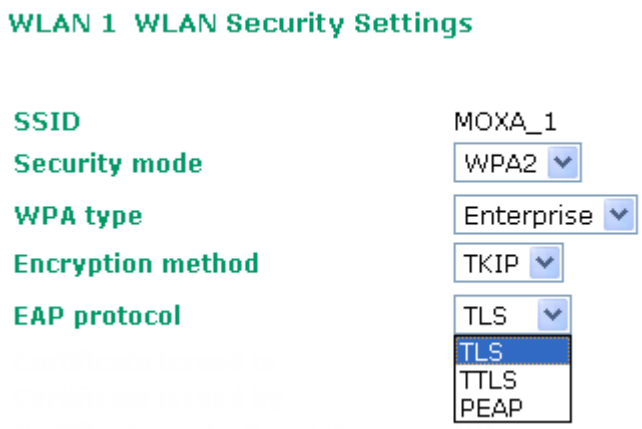
Setting	Description	Factory Default
Max. 31 characters	The secret key shared between AP and RADIUS server	None

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-6226 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	

EAP Protocol

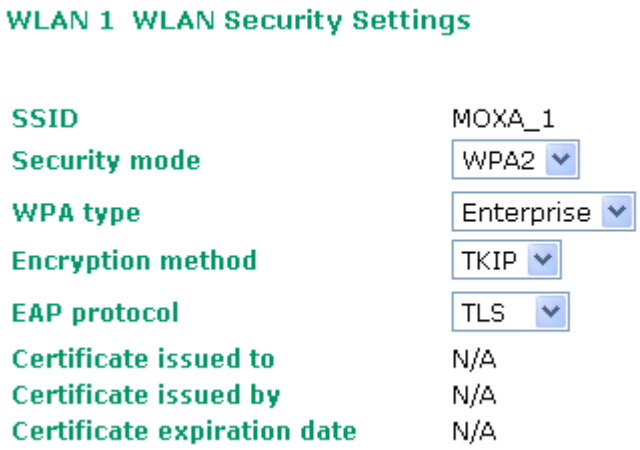
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

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 becomes invalid.

EAP-TTLS

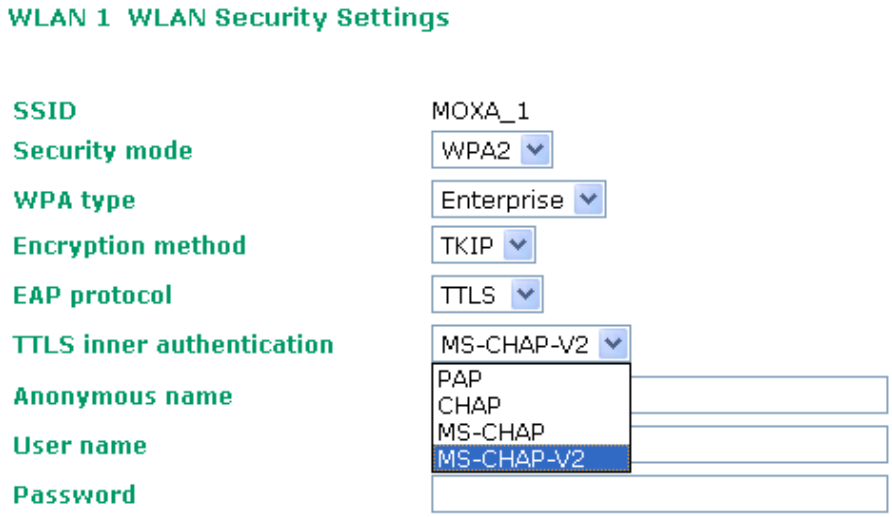
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than create a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called “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-6226 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

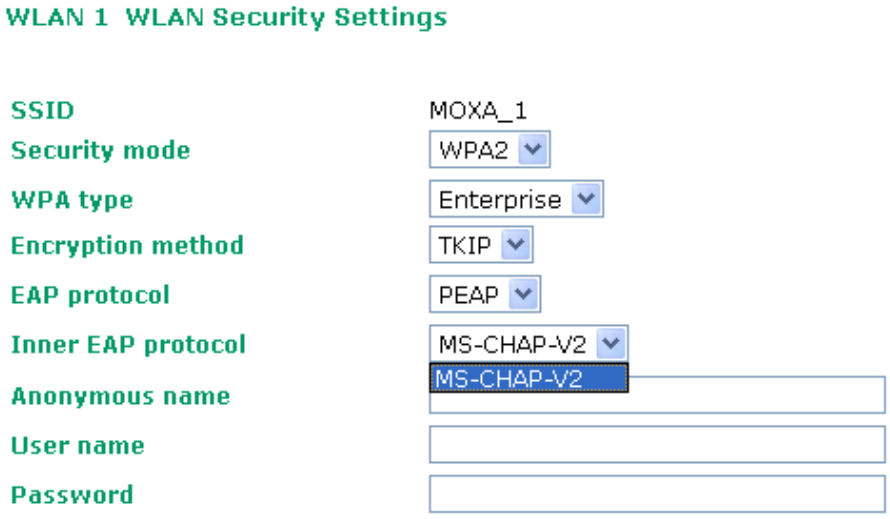
Setting	Description	Factory Default
Max. 31 characters	A distinct name used for outer authentication	None

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-6226 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

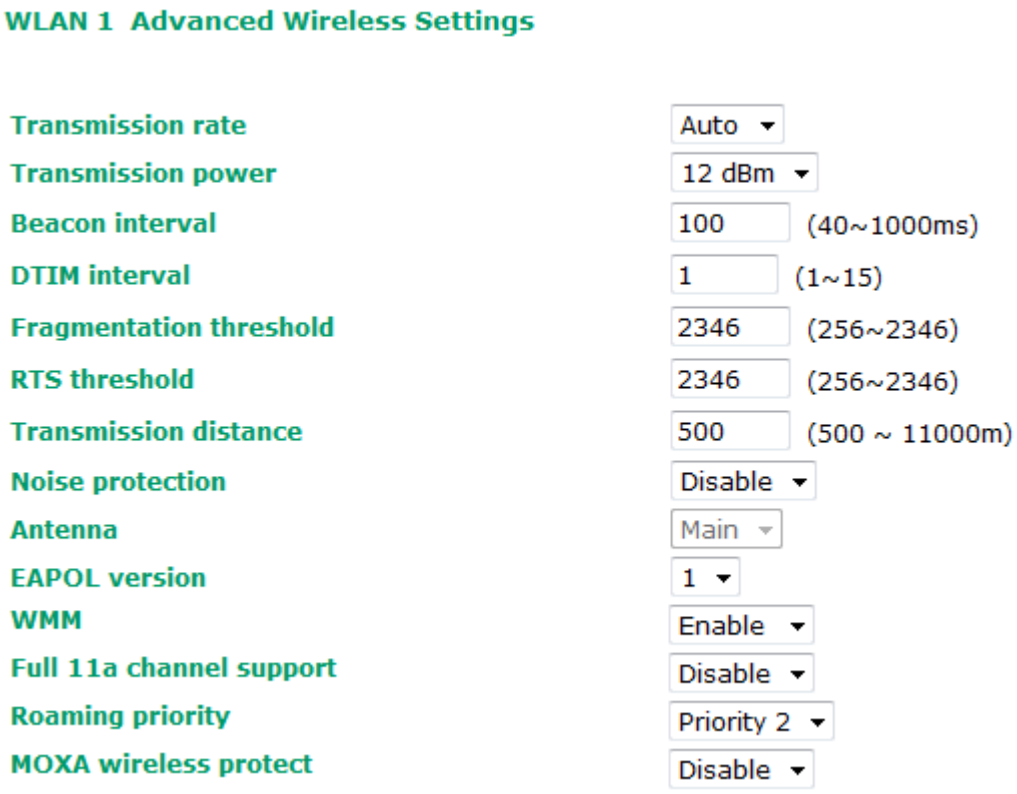
Setting	Description	Factory Default
Max. 31 characters	A distinct name used for outer authentication	None

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

Setting	Description	Factory Default
Auto	The TAP-6226 will sense and adjust the data rate automatically	Auto
Available rates	Users can manually select a target transmission data rate	

Transmission Power

Setting	Description	Factory Default
0 to 20 dBm	Maximum allowable transmission power output from the radio	12 dBm

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 16384)	This value indicates how often the TAP-6226 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)	This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication	2346

NOTE Refer to the relevant glossaries in Chapter 5 for more detailed information about the above-mentioned settings. By setting these parameters properly, you can better tune the performance of your wireless network.

Transmission distance

Setting	Description	Factory Default
Distance or max. range for transmission (500 to 11000 m)	The distance specifies the transmission distance or max. range between two AWK devices. This parameter should be set properly, especially for long-distance communication.	500

Noise protection

Setting	Description	Factory Default
Enable/Disable	The setting enhances the ability of the TAP-6226 to filter wireless interference. You should enable this option for communication distances of under 500 meters and disable it for communication distances of over 500 meters.	Enable

WMM

Setting	Description	Factory Default
Enable/Disable	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.	Disable

802.1p Priority	WMM Access Category
1	Background
2	
0	Best effort
3	
4	Video
5	
6	Video
7	

NOTE Make sure the same **Transmission distance** parameters are set in both the **AP** and **Client** sides, and both **Master and Slave**. When this parameter is more than 500, an optimal algorithm will be enabled to support long-distance transmission.

EAPOL Version

Setting	Description	Factory Default
1	EAPOL version 1, as specified in the 2001 version of 802.1X, is implemented more often.	1
2	EAPOL version 2 is specified in 802.1X-2004.	

Roaming Priority (only for AP mode)

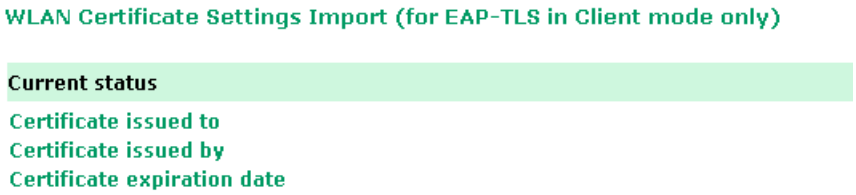
Setting	Description	Factory Default
Priority 1/2	The roaming priority should be set according to the radio deployment method along the trackside. Priority 1: radios along the trackside are deployed with leaky feeder-like coverage patterns. Priority 2: radios along the trackside are deployed with open 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

MOXA wireless protect

Setting	Description	Factory Default
Enable/Disable	Enables Moxa's Wireless Protect to protect your wireless network from Denial-of-Service attacks. This function only works between Moxa's AWK-RTG series.	Disable

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-6226 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.

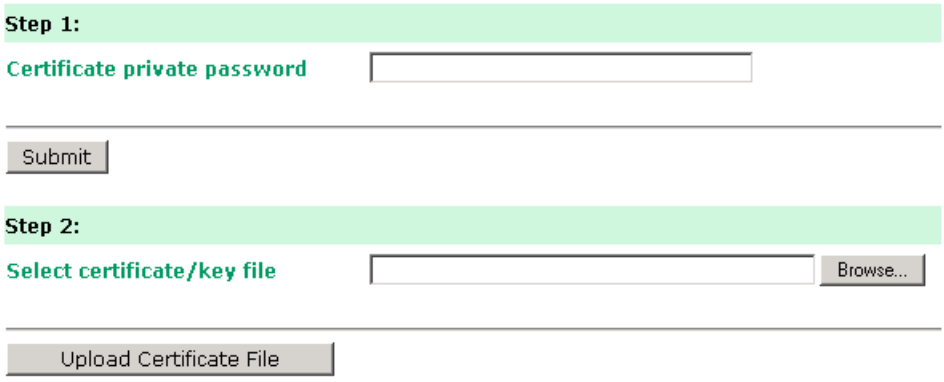


Current Status displays information for the current WLAN certificate imported into the TAP-6226. Nothing will be displayed if no certificate is available.

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:

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 is successful, the information uploaded will be displayed in ***Current Certificate***. If the import 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-6226 reboots. Even though it is expired, it can still be seen on Current Certificate.

WAC Settings

When < 50 ms Turbo Roaming is enabled, **Primary WAC IP address**, **Backup WAC IP address**, and **Roaming domain** will be shown as below.

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-6226 and wireless network system. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the TAP-6226 can support the STP/RSTP protocols to increase reliability across the entire network. In addition, SNMP support can ease the network management via SNMP protocols.

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

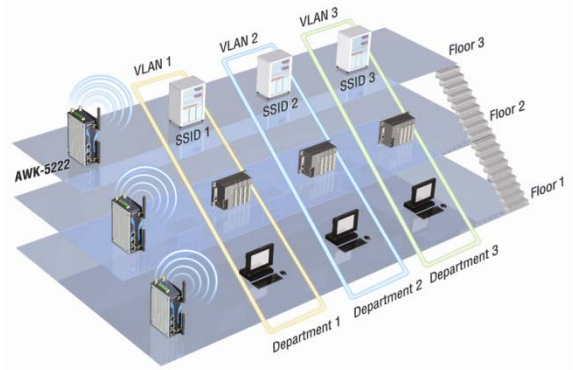
The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

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.

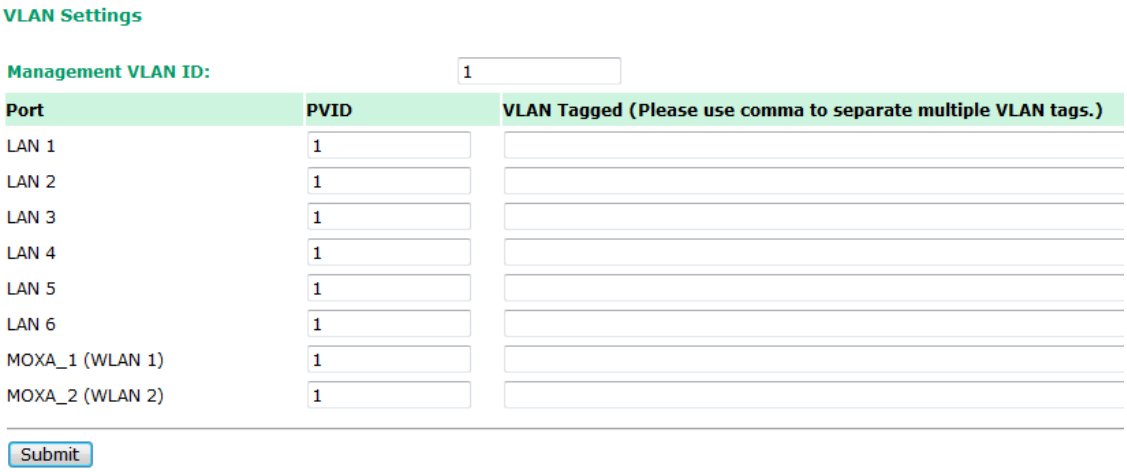
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resources department could be restricted to a gateway that allowed access to only the Internet. A member of the human resources 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.

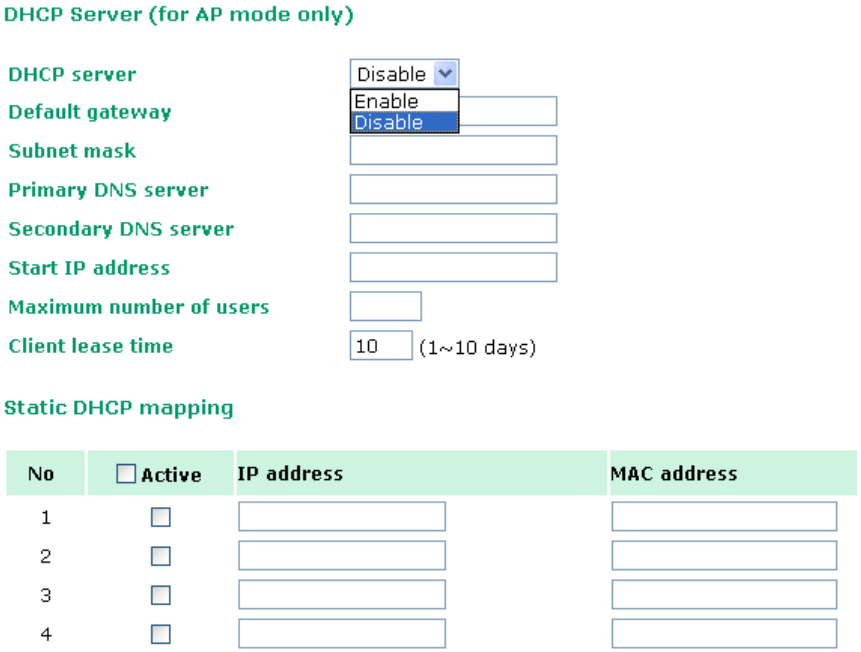
DHCP Server (for AP operation mode's AP mode only)

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-6226 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-6226 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 the DHCP server function	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-6226 can assign.	None

Maximum number of users

Setting	Description	Factory Default
1 to 999	Specifies how many IP addresses can be assigned continuously	None

Client lease time

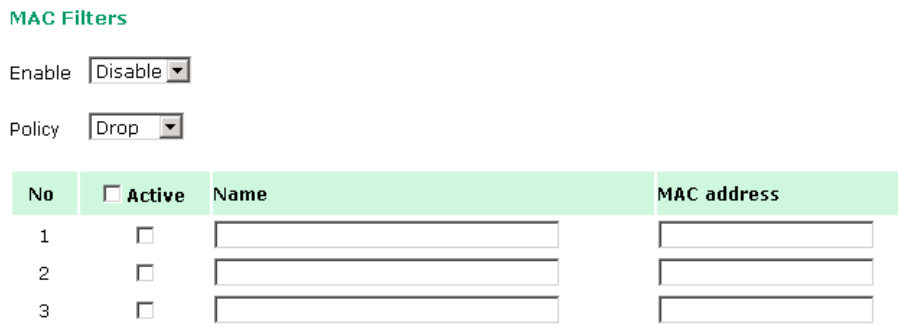
Setting	Description	Factory Default
1 to 10 days	The lease time for which an IP address is assigned. The IP address may expire after the lease time is reached.	10 (days)

Packet Filters

The TAP-6226 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-6226's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The TAP-6226 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.	

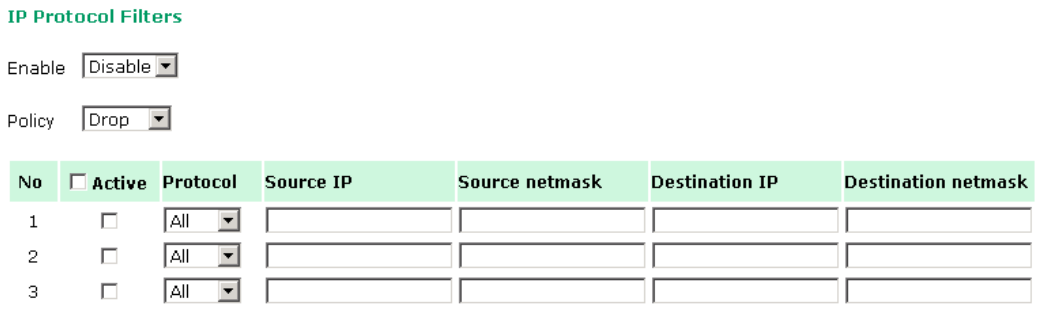
ATTENTION

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-6226'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-6226 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

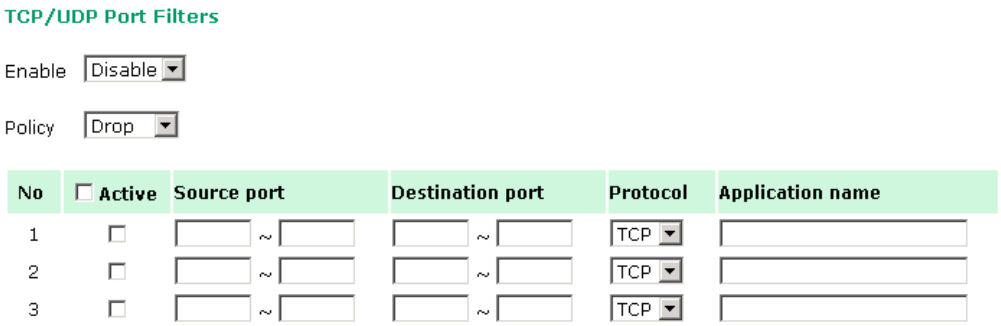
Be careful when you enable the filter function:
Drop + "**no** entity on list is activated" = all packets are **allowed** (i.e., drop nothing)
Accept + "**no** entity on list is activated" = all packets are **denied** (i.e., accept nothing)

TCP/UDP Port Filter

The TAP-6226'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-6226 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

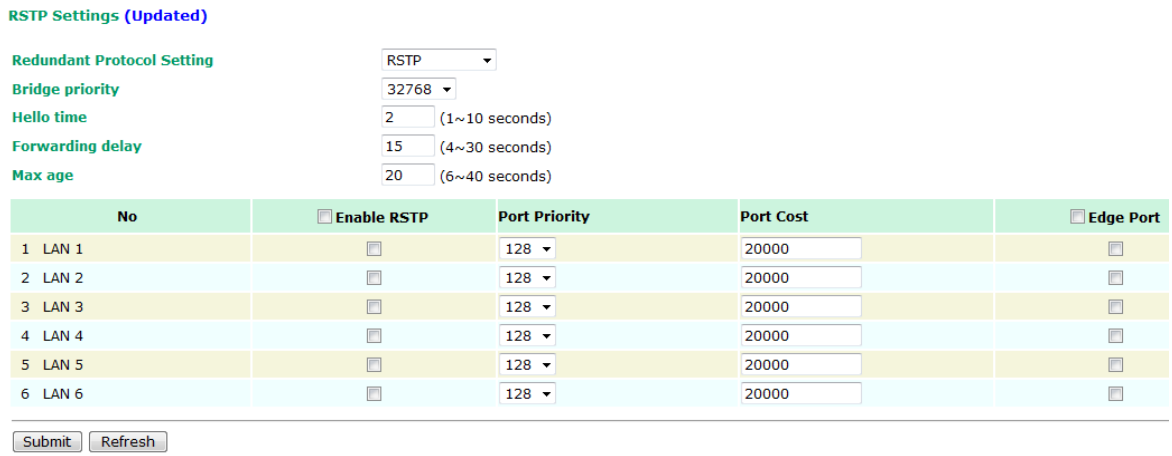
Be careful when you enable the filter function:
Drop + "**no** entity on list is activated" = all packets are **allowed** (i.e., drop nothing)
Accept + "**no** entity on list is activated" = all packets are **denied** (i.e., accept nothing)

RSTP / Turbo Chain Settings (for Master or Slave mode only)

The TAP-6226 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-6226 also supports Turbo Chain on its fiber interfaces.

The TAP-6226's STP/RSTP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every TAP-6226 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
User-selected numerical value	You can increase the bridge priority by selecting a lower number. Units with higher bridge priority are more likely to be chosen as the root of the Spanning Tree topology.	32768

Hello time

Setting	Description	Factory Default
User-selected numerical value (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. ***Hello time*** indicates how often the root sends hello messages.	2 (seconds)

Forwarding delay

Setting	Description	Factory Default
User-selected numerical value (4 to 30 seconds)	The amount of time this device waits before checking to see if it should change to a different topology.	15 (seconds)

Max. age

Setting	Description	Factory Default
User-selected numerical value (6 to 40 seconds)	As a non-root role, if the device has not received a hello message from the root longer than ***Max. age***, it will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20 (seconds)

Enable RSTP

Setting	Description	Factory Default
Enable/disable	Enables or disables the port as a node on the Spanning Tree topology.	Disable (unchecked)

Port priority

Setting	Description	Factory Default
User-selected numerical value	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
Enable/Disable	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology	2000000

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.

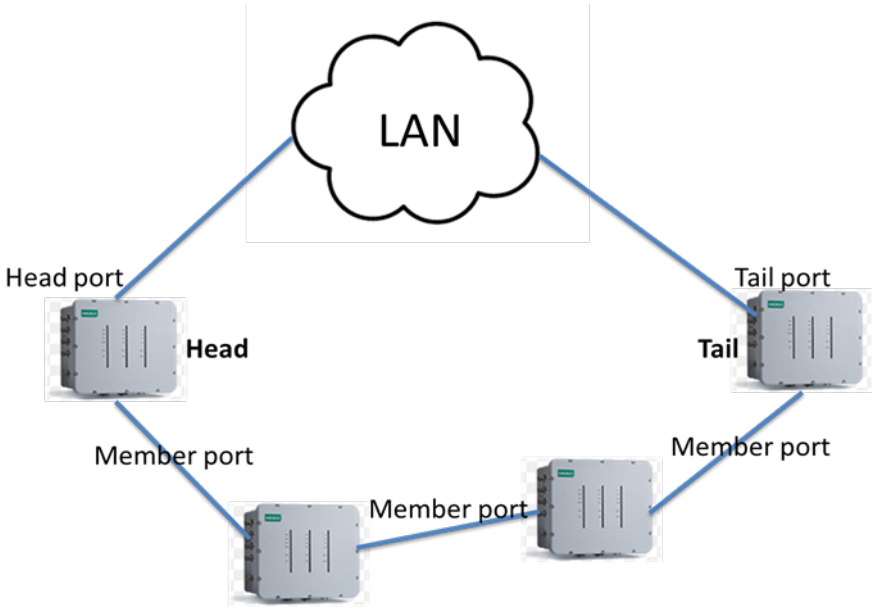
Port Status

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

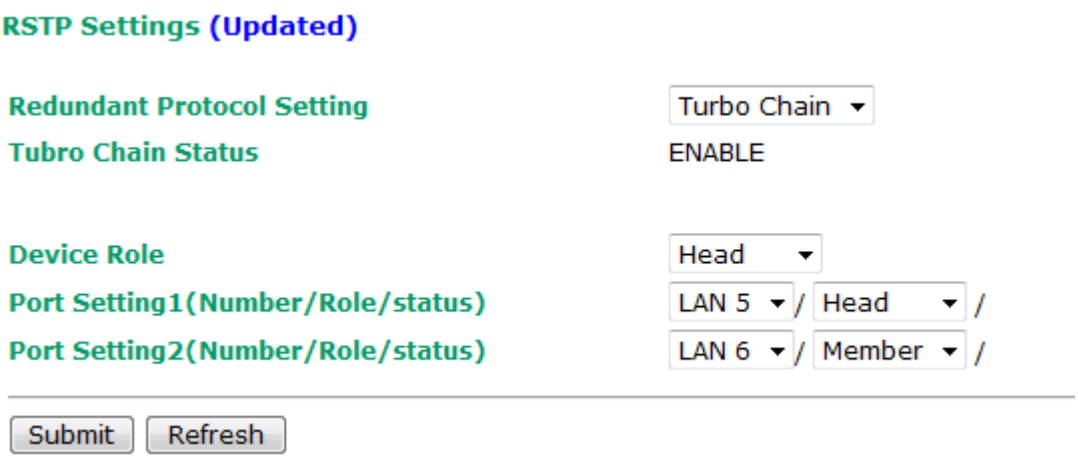
Moxa's Turbo Chain is an advanced software-technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the "chain" concept, you first connect the APs in a chain and then simply link the two ends of the chain to an Ethernet network, as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



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.



Turbo Chain Status

Indicates whether Turbo Chain is enabled or disabled on the TAP-6226.

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

Storm Protection

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called “broadcast storms” could be caused by an incorrectly configured topology or a malfunctioning device.

Storm Protection

Setting	Description	Factory Default
Enable/Disable	Enable or disable Broadcast Storm Protection globally for multicast packets	Enable

Multicast and flooding

Setting	Description	Factory Default
Enable/Disable	If you enable Storm Protection, the Multicast and flooding option will show up. You can Enable or Disable Broadcast Storm Protection globally for unknown multicast and unknown unicast packets.	Disable

SNMP Agent

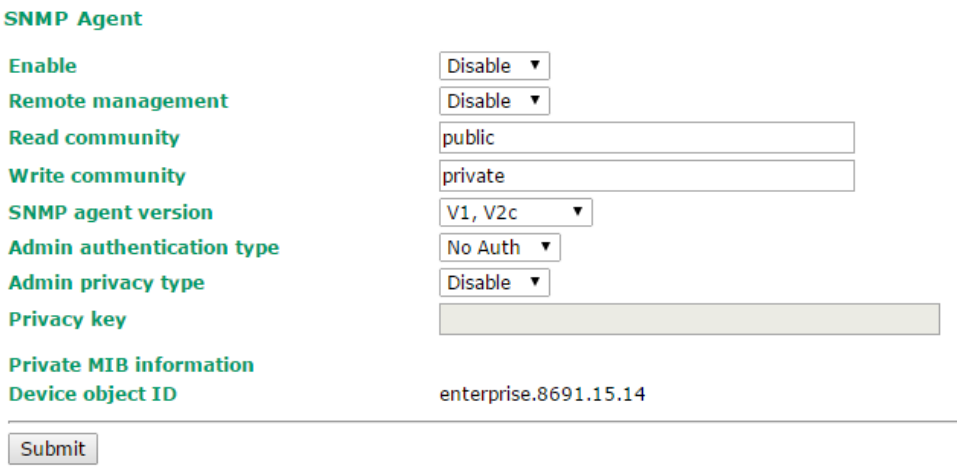
The TAP-6226 supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

The TAP-6226'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-6226 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	

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-6226's enterprise value. It is fixed.

PoE Settings

The TAP-6226 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

Auto Warning Settings

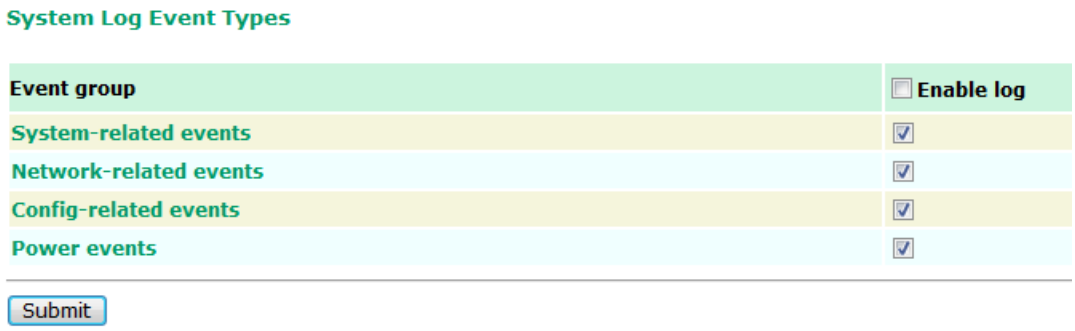
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. This way even 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-6226 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**.



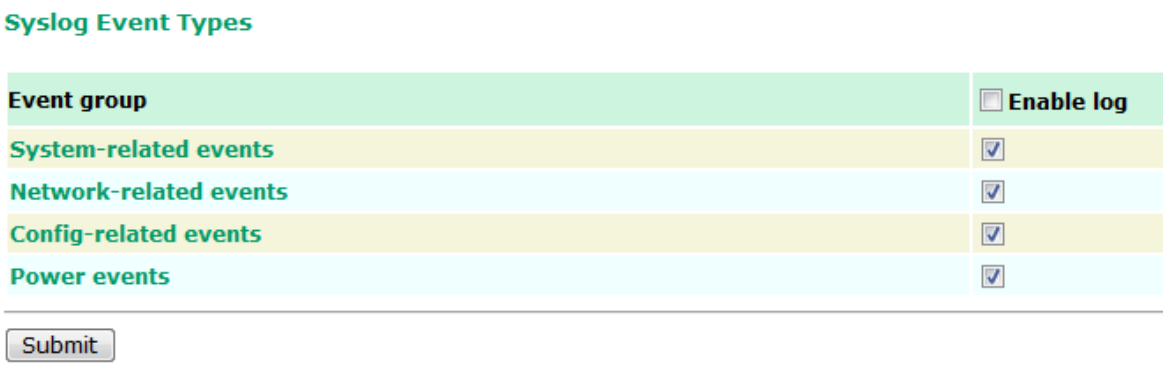
System-related events	**Event triggers when…**
System restart (warm start)	The TAP-6226 is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
Network-related events	**Event triggers when…**
LAN 1 or LAN 2 link on	The LAN port is connected to a device or network.
LAN 1 or 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-6226 is associated with an AP.
WLAN 1 or WLAN 2 disconnected (for Slave mode)	The TAP-6226 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-6226.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The TAP-6226's firmware is updated.
Power events	**Event triggers when…**
Power 1/2 transition (On → Off)	The TAP-6226 is powered down in PWR1/2.
PoE transition (On → Off)	The TAP-6226 is powered down in PoE.
Power 1/2 transition (Off → On)	The TAP-6226 is powered via PWR1/2.
PoE transition (Off → On)	The TAP-6226 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.

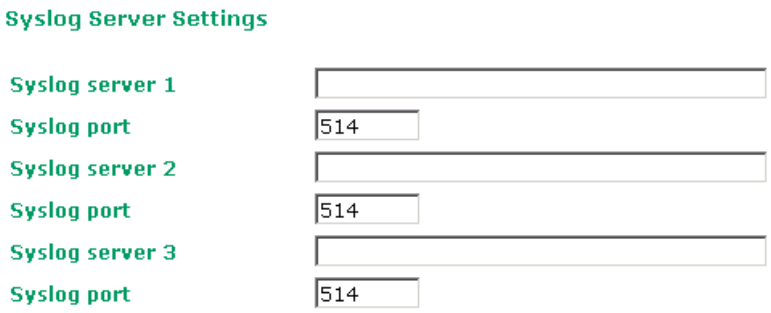
Syslog Event Types

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

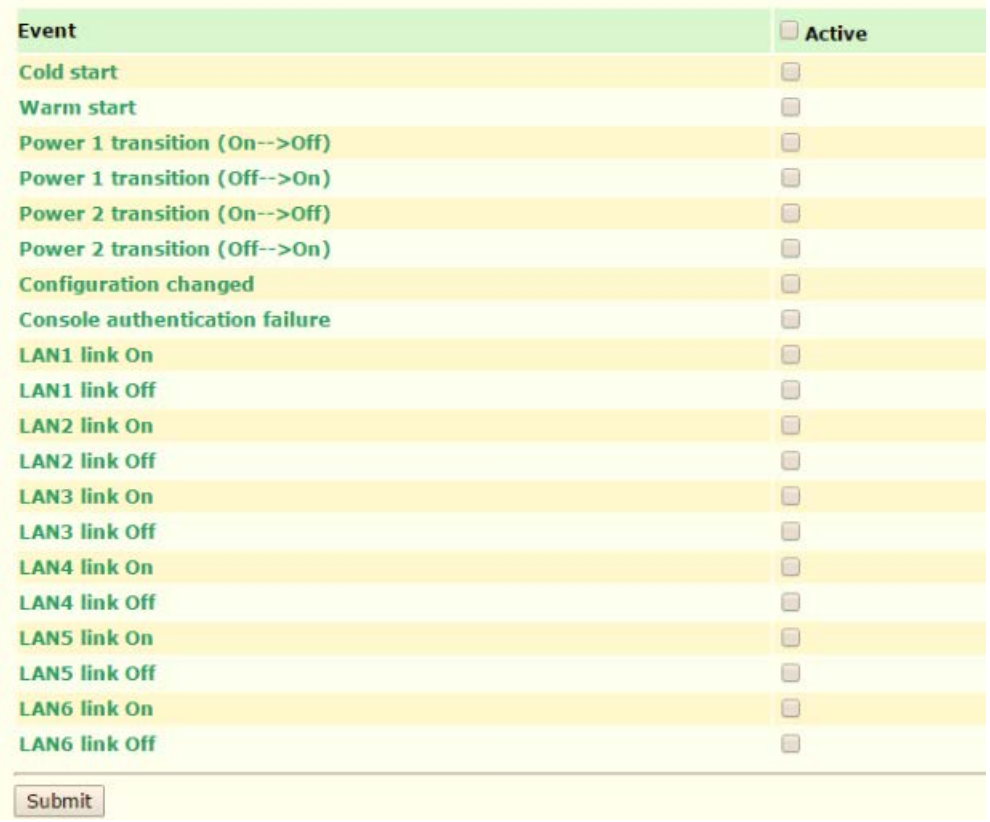
Syslog port

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-6226. 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

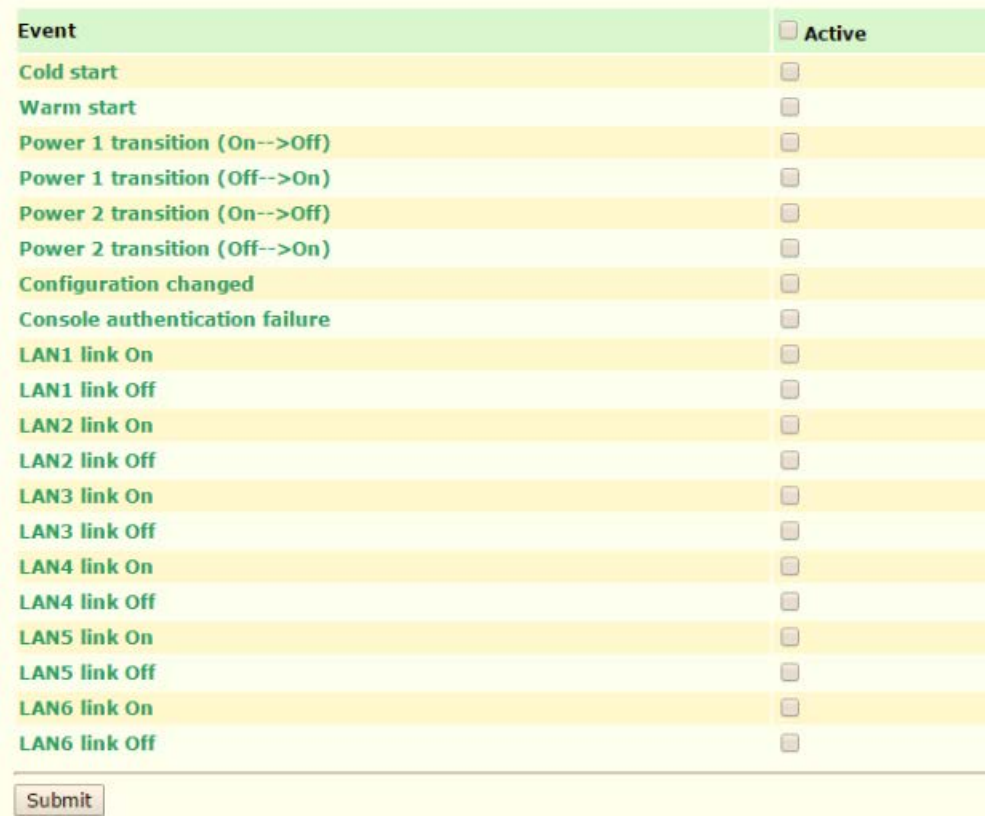
Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' email addresses.	None

Trap

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

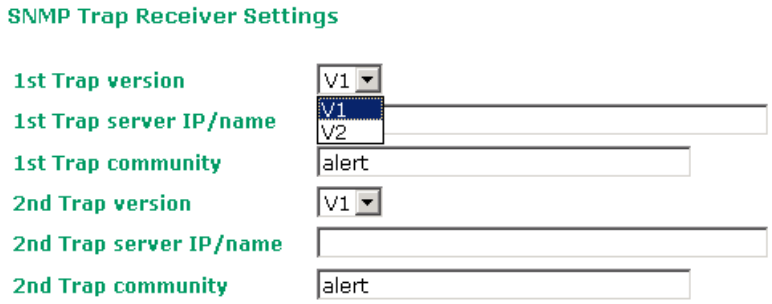
Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overwhelming for the management station to poll or send requests to query every object on every device. It would be more effective for the managed device agent to notify the management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

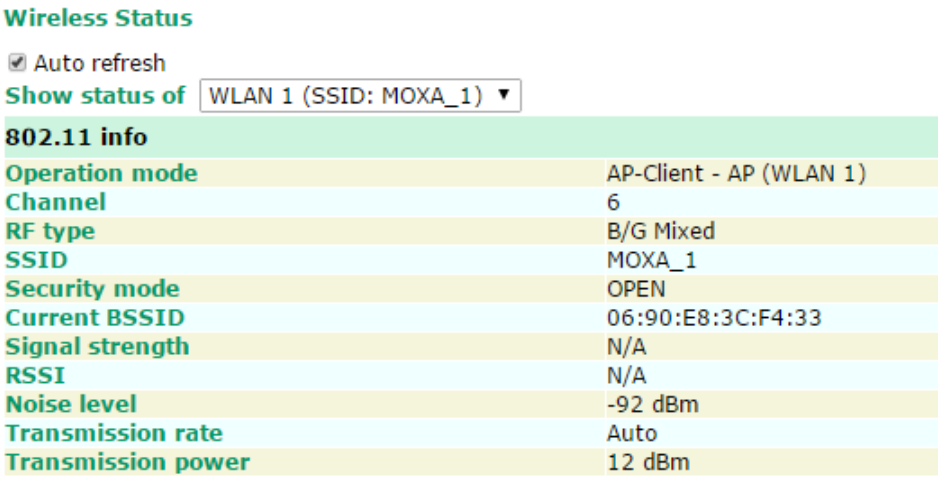
Status

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.

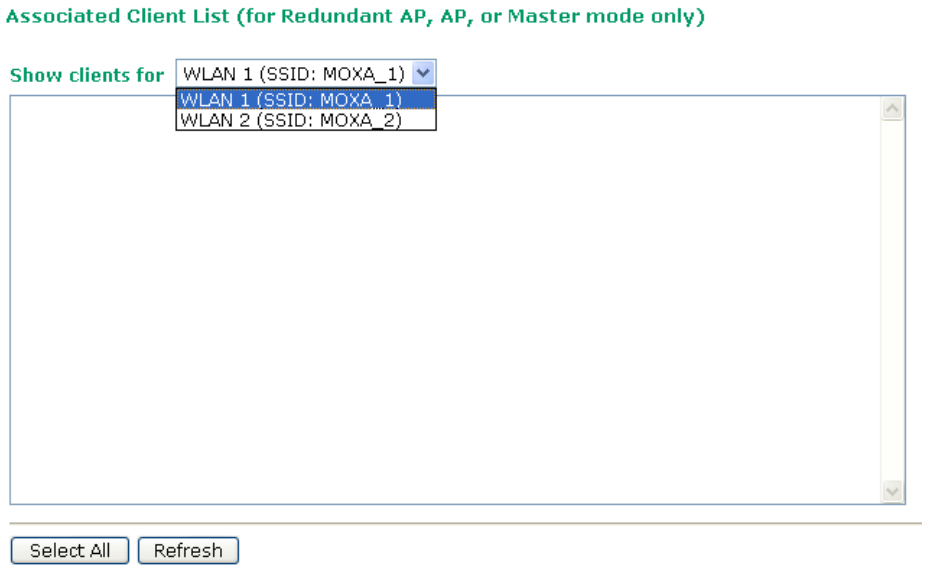
Certain **802.11 info** values may not appear in certain operation modes. For example, **Current BSSID** and **RSSI** are not available in AP or Master modes.

It is helpful to use the continuously updated information option on this page, such as RSSI, to monitor the signal strength of the TAP-6226 in Slave modes.



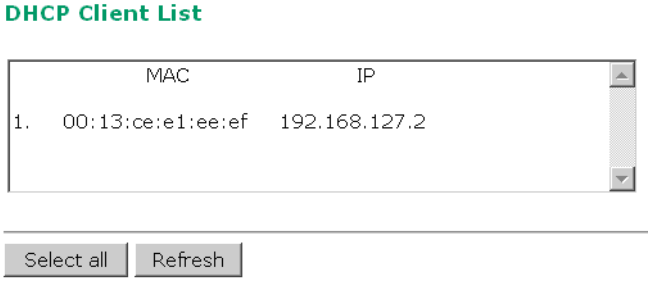
Associated Client List (for AP or Master Mode only)

Associated Client List shows all the clients that are currently associated with a particular TAP-6226. Click **Select all** to select all the content in the list for further editing. Click **Refresh** to refresh the list.

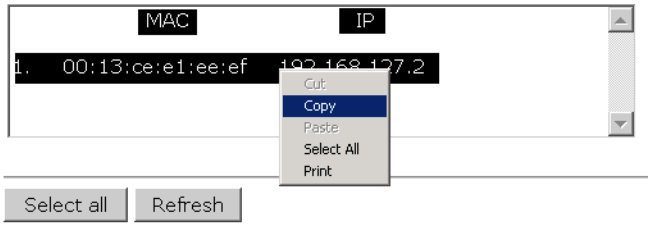


DHCP Client List (for AP mode only)

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.

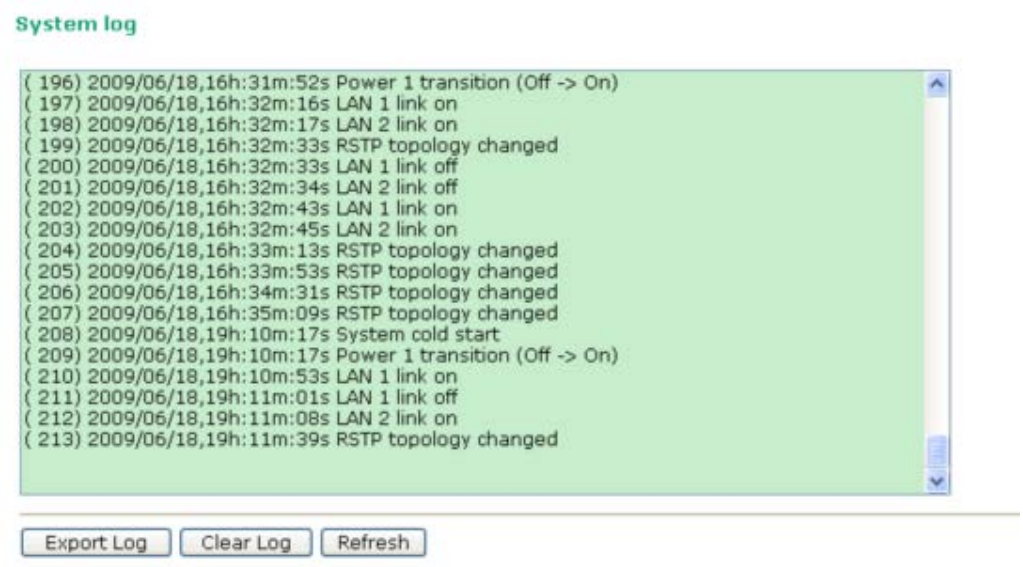


Click **Select all** to select all content in the list for further editing.



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.

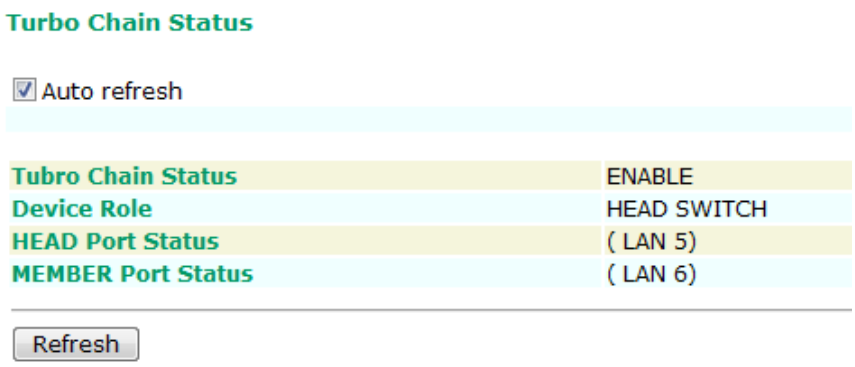


RSTP Status

This status field will appear only when STP/RSTP is enabled. It indicates whether or not this TAP-6226 is the Root of the Spanning Tree (the root is determined automatically) and the status of each port.

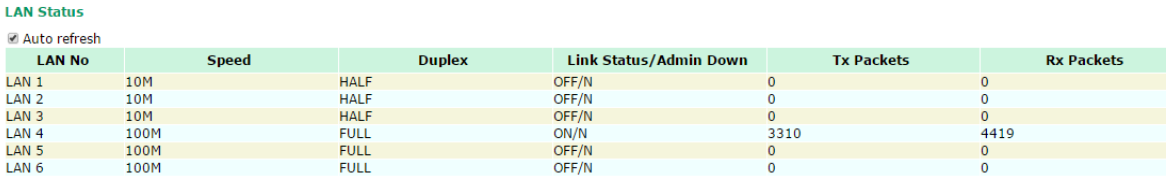
Turbo Chain Status

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.

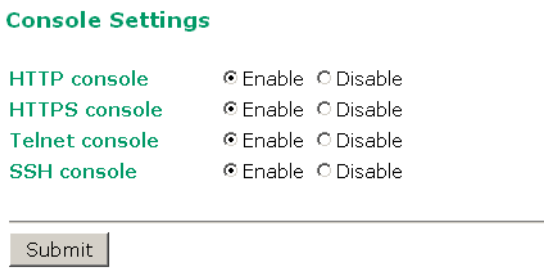


Maintenance

Maintenance functions provide the administrator with tools to manage the TAP-6226 and wired/wireless networks.

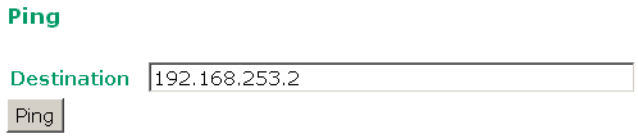
Console Settings

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.

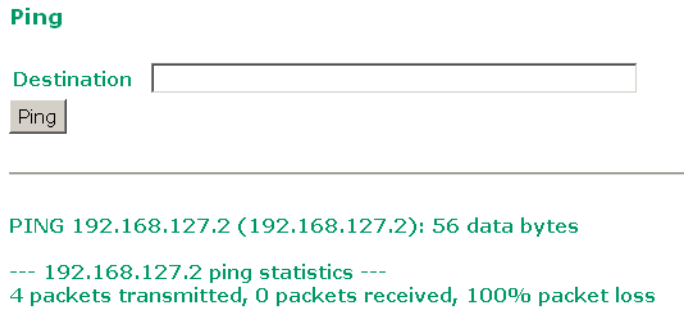


Ping

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-6226 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-6226 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-6226 will reboot itself.

When upgrading your firmware, the TAP-6226's other functions are deactivated.

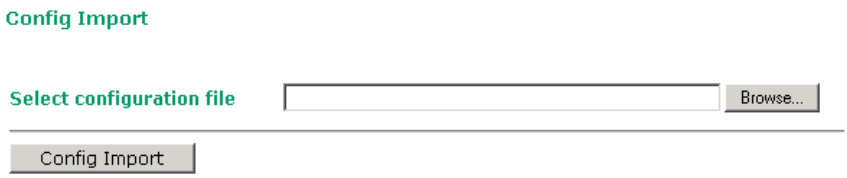
ATTENTION

Make sure the power source is stable when you upgrade your firmware. An unexpected power interruption may damage your TAP-6226.

Config Import Export

You can back up or restore the TAP-6226's configuration with **Config Import Export**.

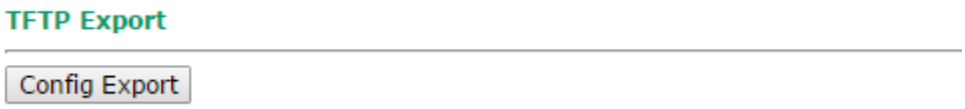
In the **Config Import** section, click **Browse** to specify the configuration file and click the **Config Import** button to begin importing the configuration.



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.

In the TFTP import section, you can specify a configuration to be imported into the TAP-6226 from a remote TFTP server. Specify the IP, configuration path, and the file name of the configuration file to tell the TAP-6226 to import the file from that specific location.

A configuration file can also be exported to the TFTP server to create a copy of the TFTP's current configuration.

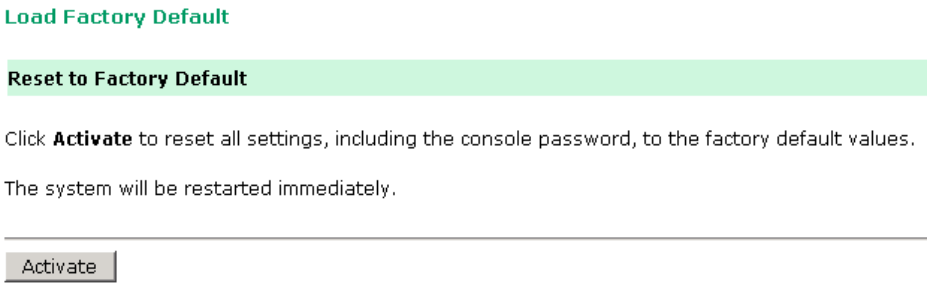


MIB Export

The MIB file of the TAP-6226 can be exported from the TAP-6226 for SNMP configuration purposes.

Load Factory Default

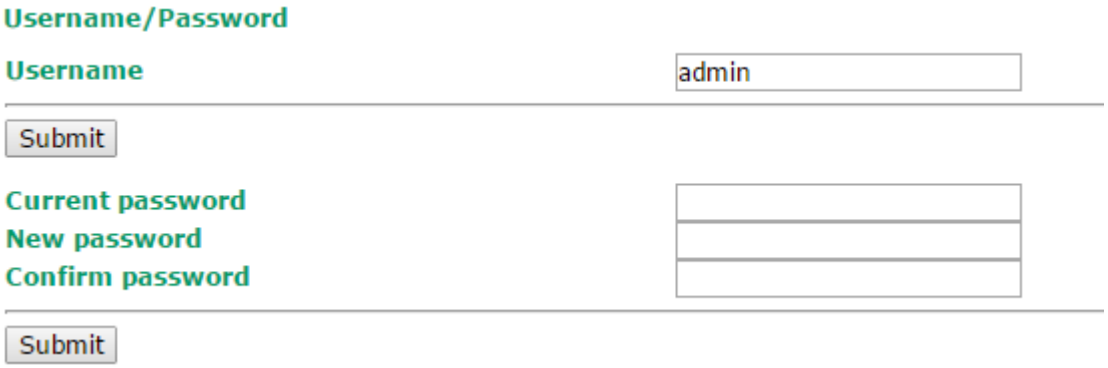
Use this function to reset the TAP-6226 and roll all settings back to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the TAP-6226.



Username/Password

You can change the administration username/password for each of the TAP-6226'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 security reasons, do not use the default password ***moxa***, and remember to change the administration password regularly.

NOTE Firmware Version 1.6 password: moxa
Firmware Versions 1.0 to 1.5 password: root



Misc. Settings

Additional settings to help you manage your TAP-6226, are available on this page.

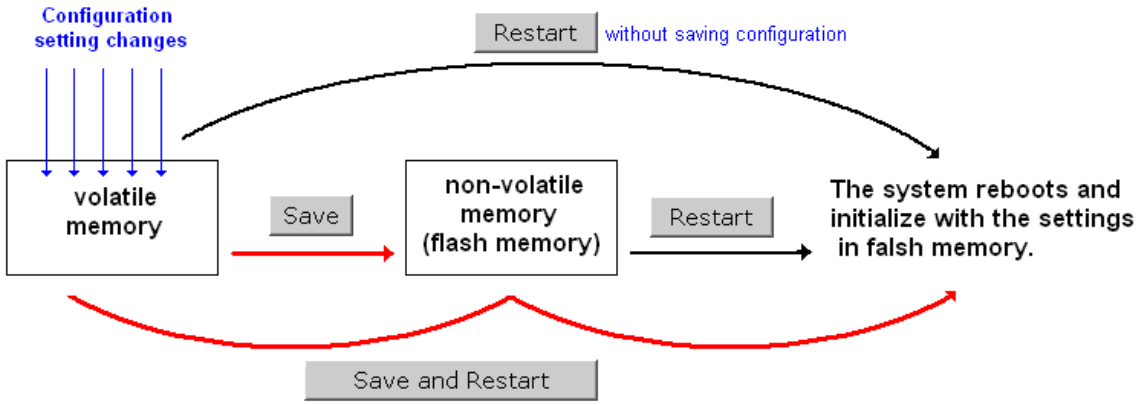
Reset button

Setting	Description	Factory Default
Always enable	The TAP-6226's Reset button works normally.	Always enable
Disable after 60 sec	The TAP-6226's Reset button will become invalid 60 seconds after the TAP-6226 completes booting.	

Save Configuration

The following figure shows how the TAP-6226 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-6226 is shut down or rebooted. Because the TAP-6226 starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the TAP-6226.

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

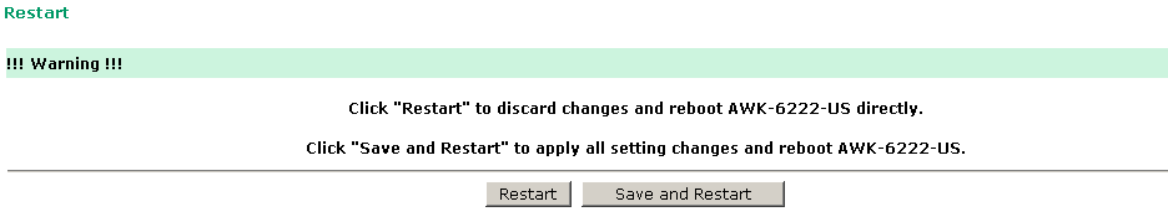


After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However, 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-6226 directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the TAP-6226.

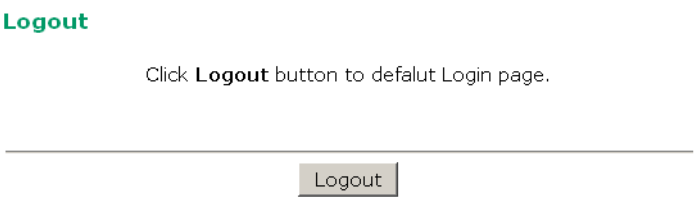


If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.

You will not be able to run any of the TAP-6226'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**
- **AWK Search Utility**
  - Installing AWK Search Utility
  - Configuring AWK Search Utility

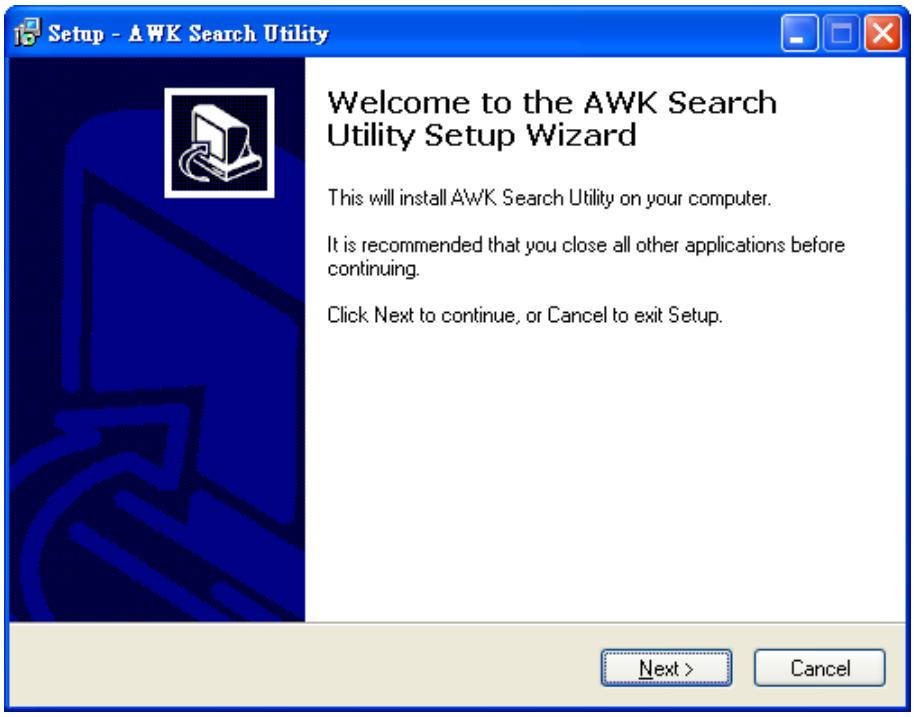
Overview

The Documentation & Software CD included with your TAP-6226 is designed to make the installation and configuration procedure easy and straightforward. This auto-run CD includes AWK Search Utility (to broadcast search for all AWK's accessible over the network), the TAP-6226 User's Manual, and Quick Installation Guide.

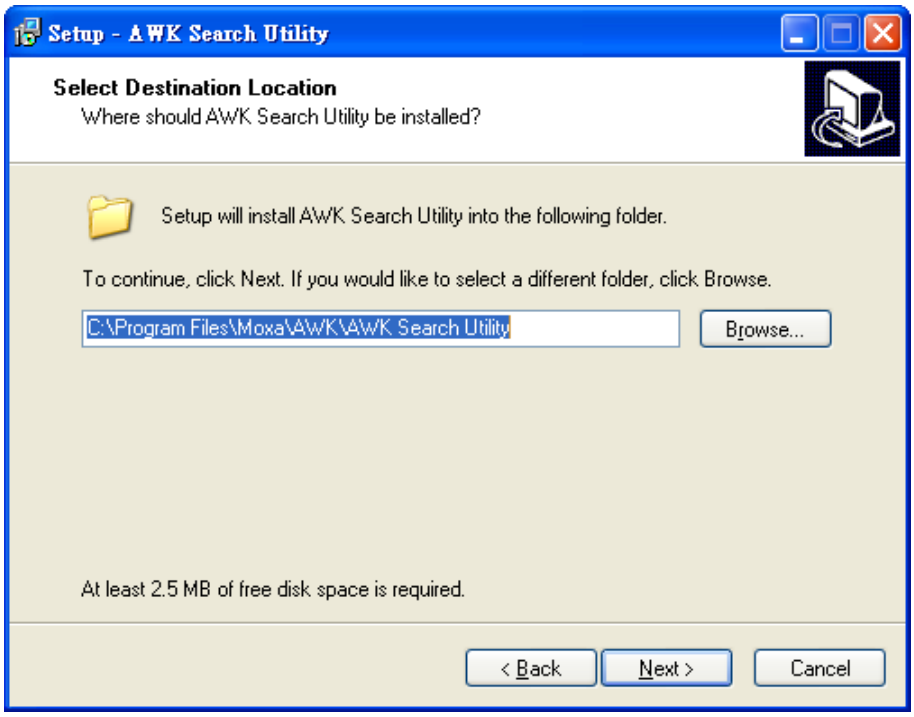
AWK Search Utility

Installing AWK Search Utility

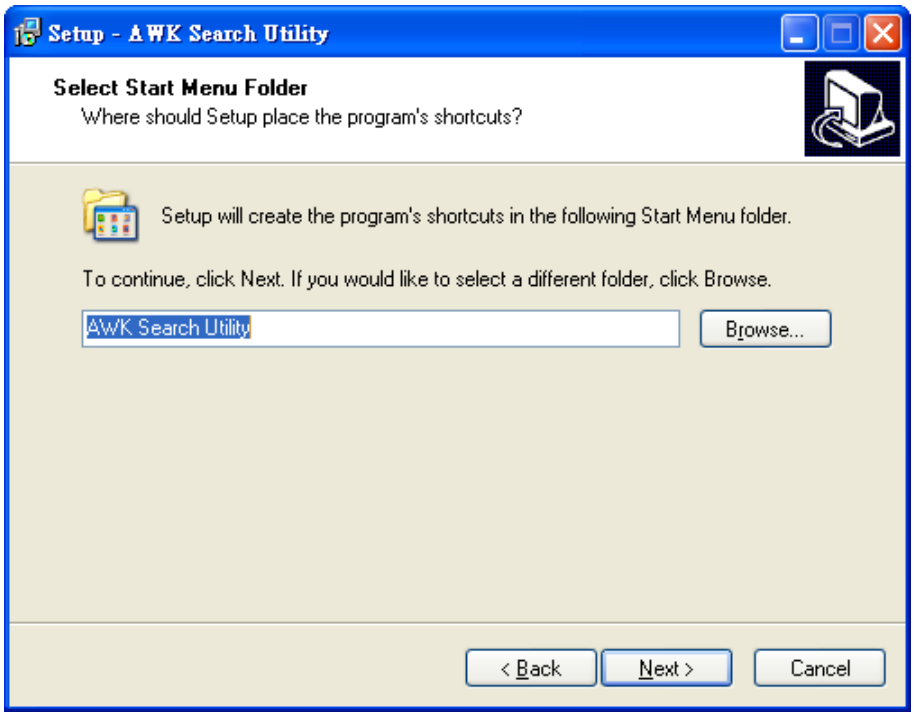
1. Click the **INSTALL UTILITY** button in the AWK Installation CD auto-run window to install AWK Search Utility. Once the program starts running, click **Yes** to proceed.
2. Click **Next** when the Welcome screen opens to proceed with the installation.



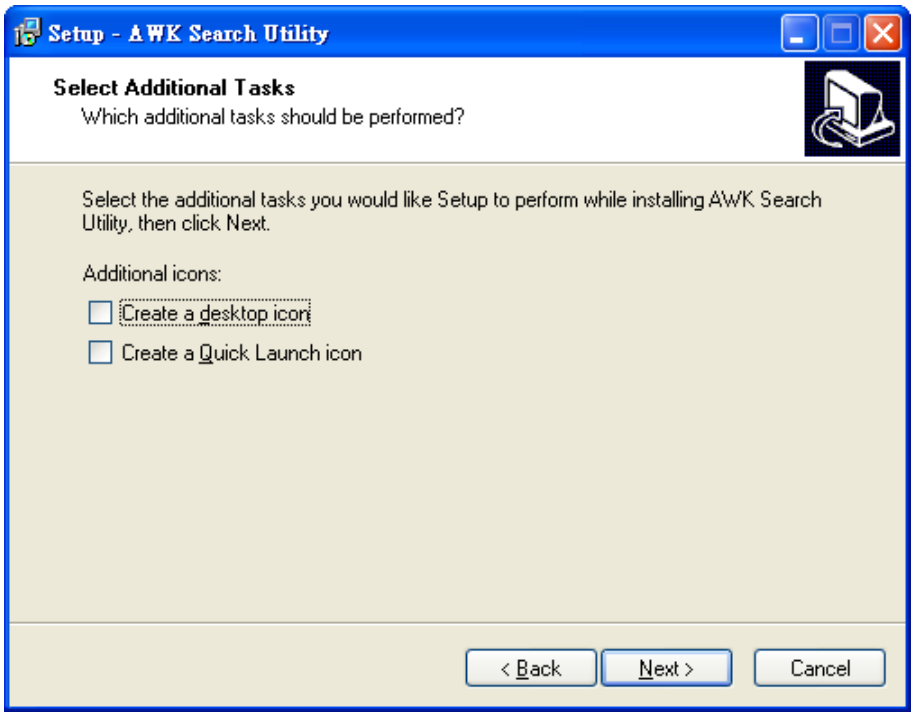
3. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



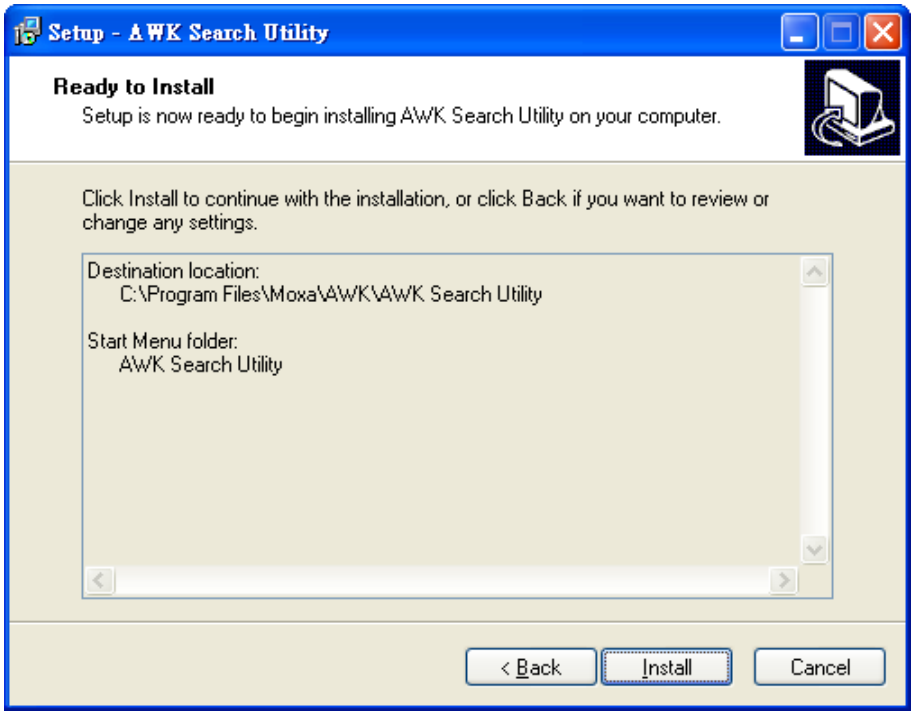
4. Click **Next** to create the program's shortcut files in the default directory, or click **Browse** to select an alternate location.



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

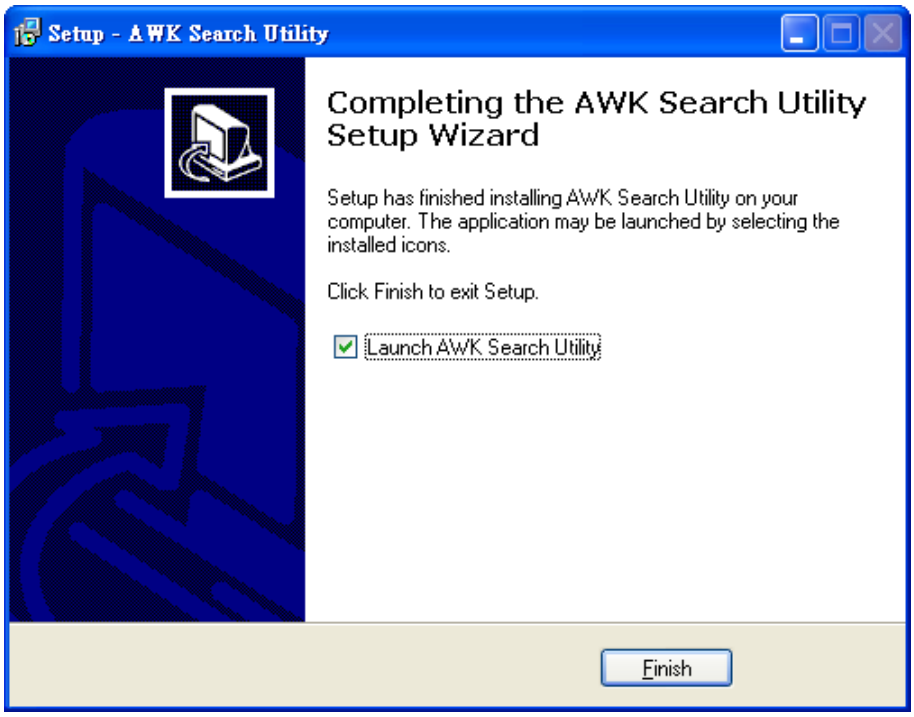


6. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.



7. 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.

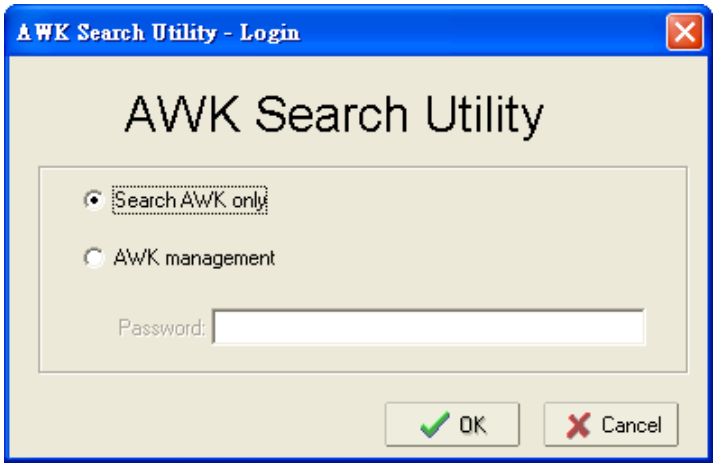
8. Click **Finish** to complete the installation of AWK Search Utility.



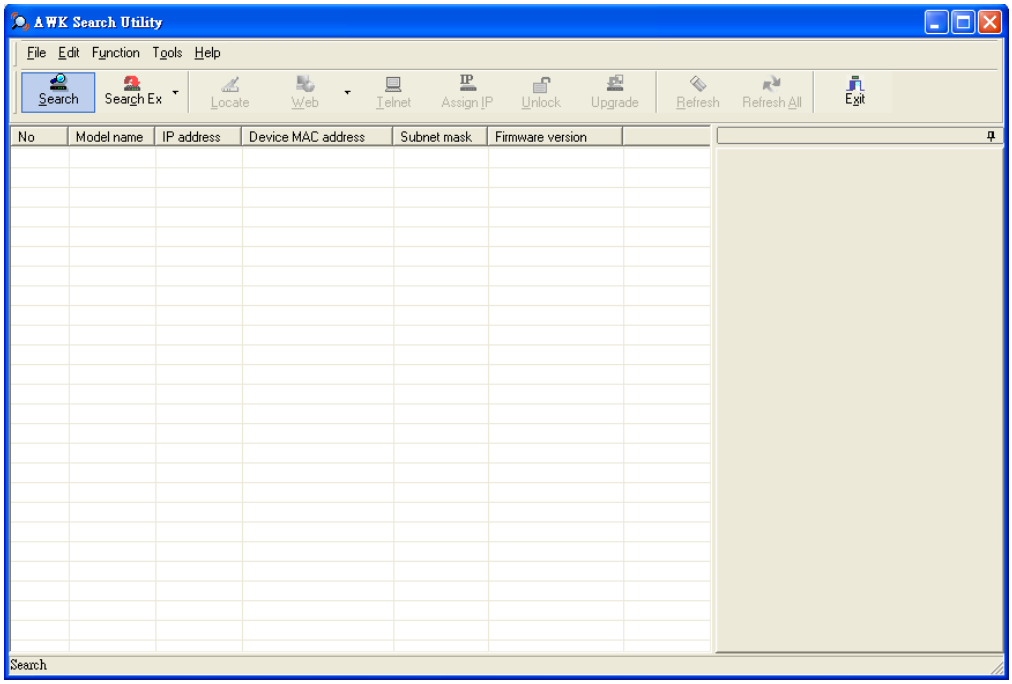
Configuring AWK Search Utility

The Broadcast Search function is used to locate all TAP-6226 APs that are connected to the same LAN as your computer. After locating a TAP-6226, you will be able to change its IP address. Since the Broadcast Search function searches by TCP packet and not IP address, it doesn't matter if the TAP-6226 is configured as an AP. 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 **AWK Search Utility**. When the Login page appears, select the "Search AWK only" option to search for AWKs and to view each AWK's configuration. Select the "AWK management" option to assign IPs, upgrade firmware, and locate devices.

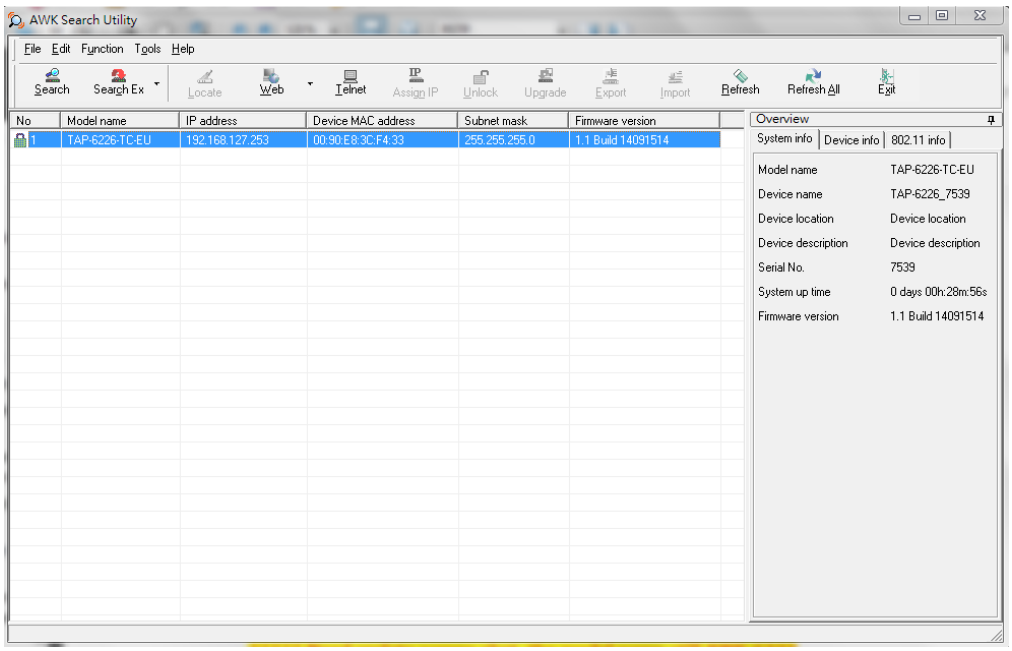


2. Open AWK Search Utility and then click the **Search** icon.

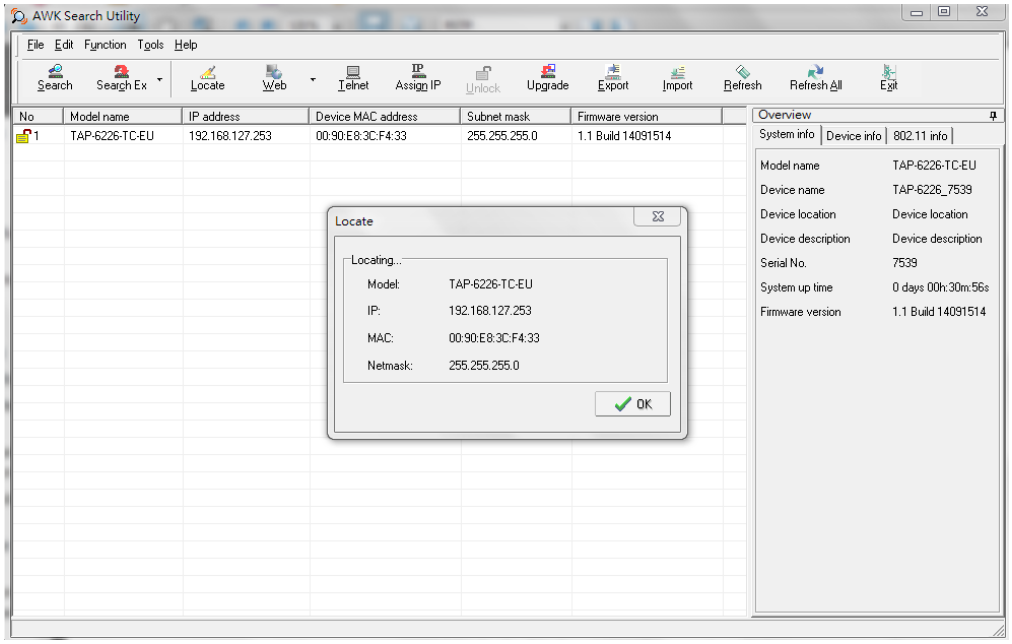


The “Searching” window indicates the progress of the search.

3. When the search is complete, all AWKs that were located will be displayed in the AWK Search Utility window.

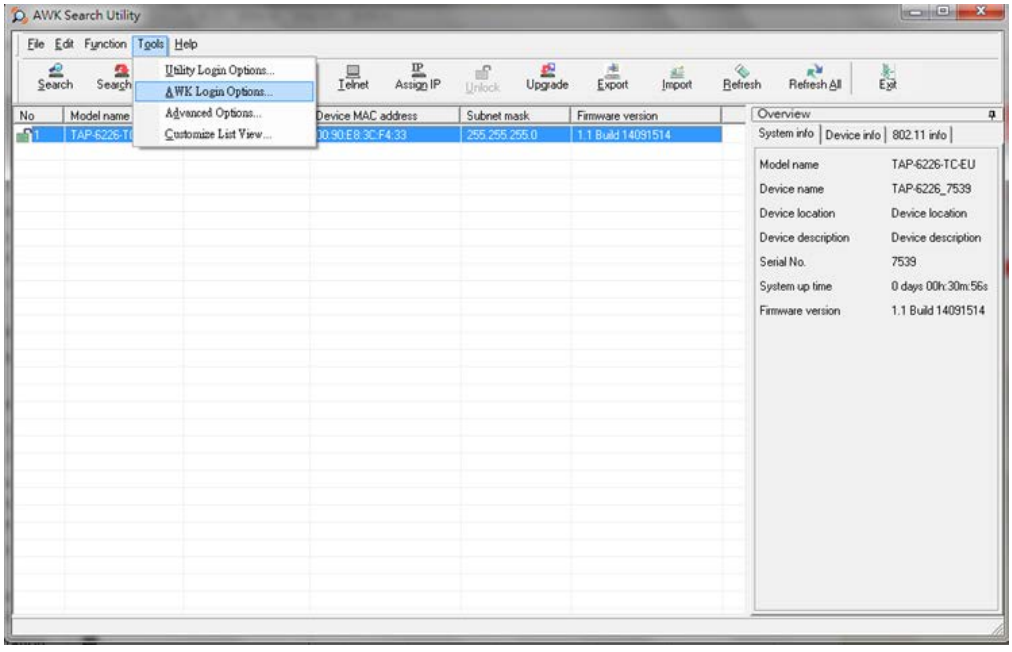


Click **Locate** to cause the selected device to beep.



Make sure your AWK is **unlocked** before using the search utility's icons setting. The AWK will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.

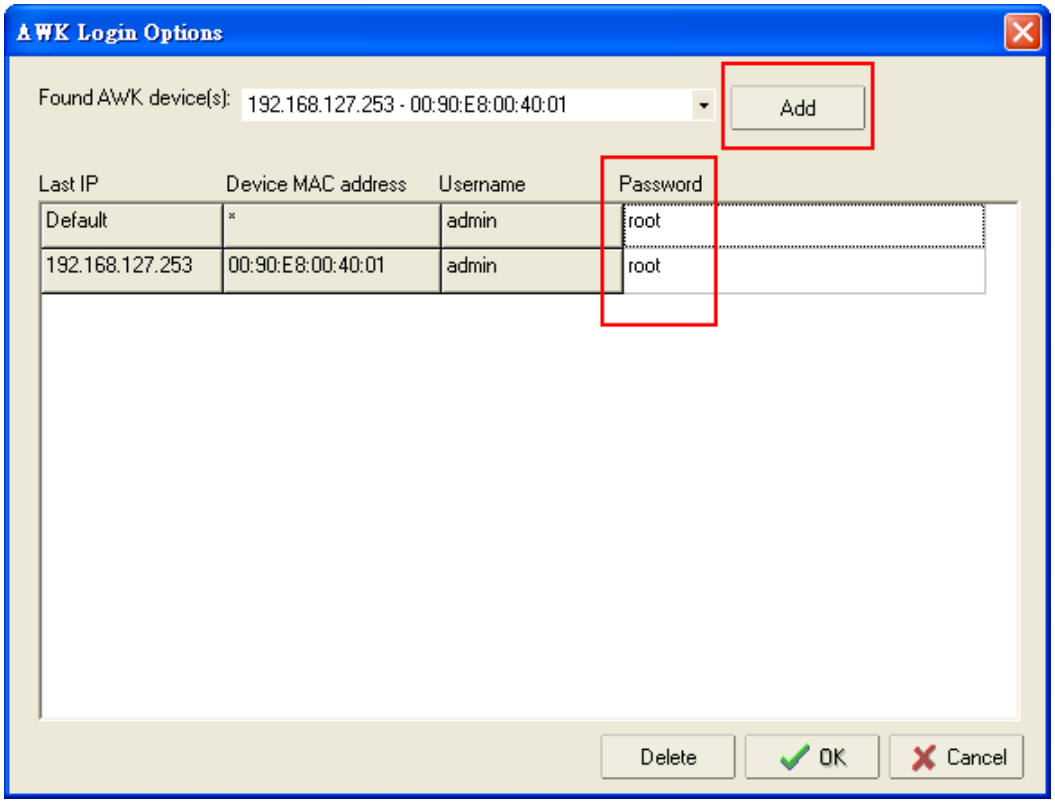
Go to **Tools → AWK login Options** to manage and unlock additional AWKs.



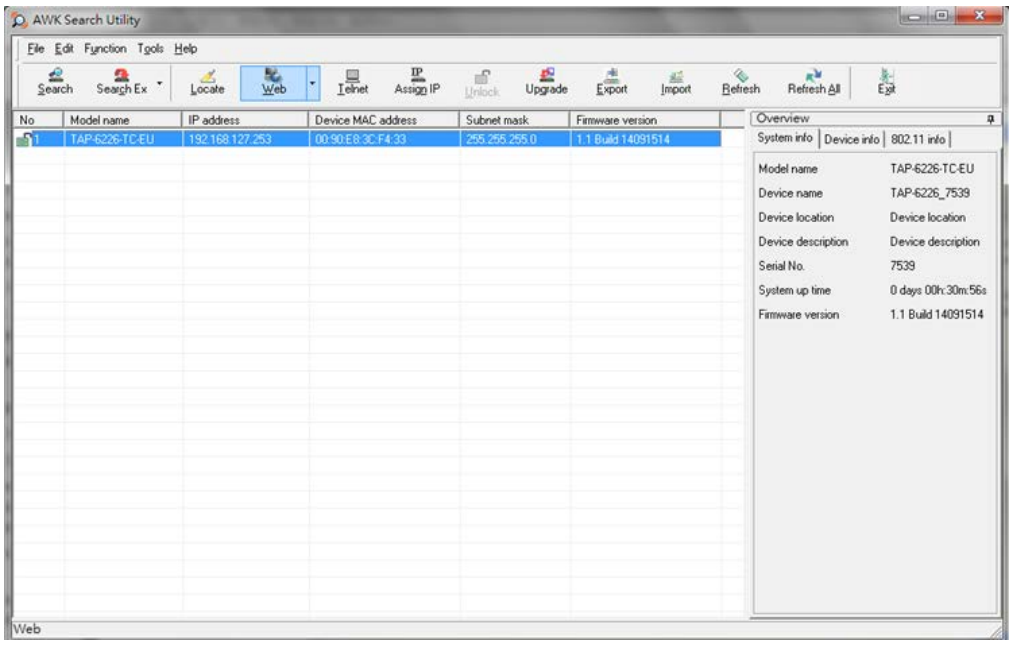
Use the scroll down list to select the MAC addresses of those AWKs you would like to manage, and then click **Add**. Key in the password for the AWK device and then click **OK** to save. If you return to the search page and search for the AWK again, you will find that the AWK will unlock automatically.

ATTENTION

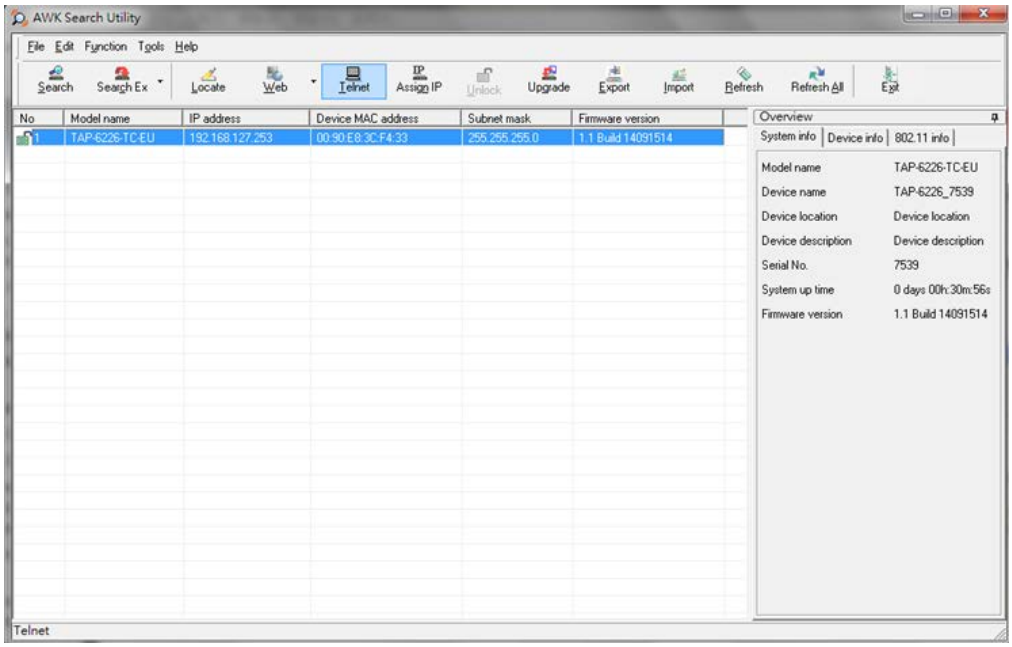
For security purposes, we suggest that you can change the AWK search utility login password instead of using the default.



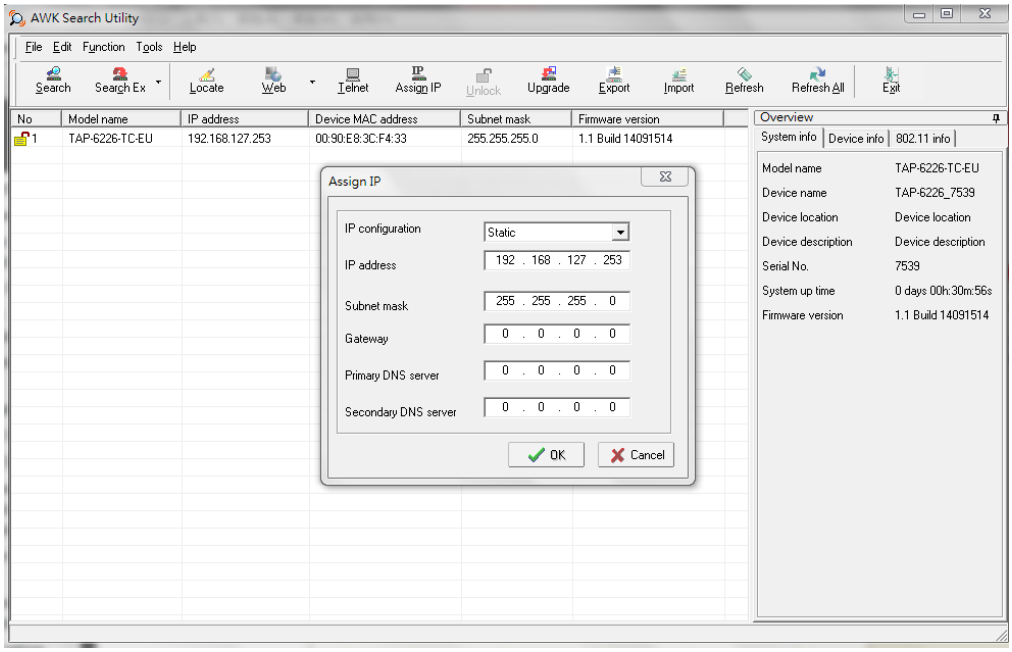
To modify the configuration of the highlighted AWK, click on the Web icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.



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



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

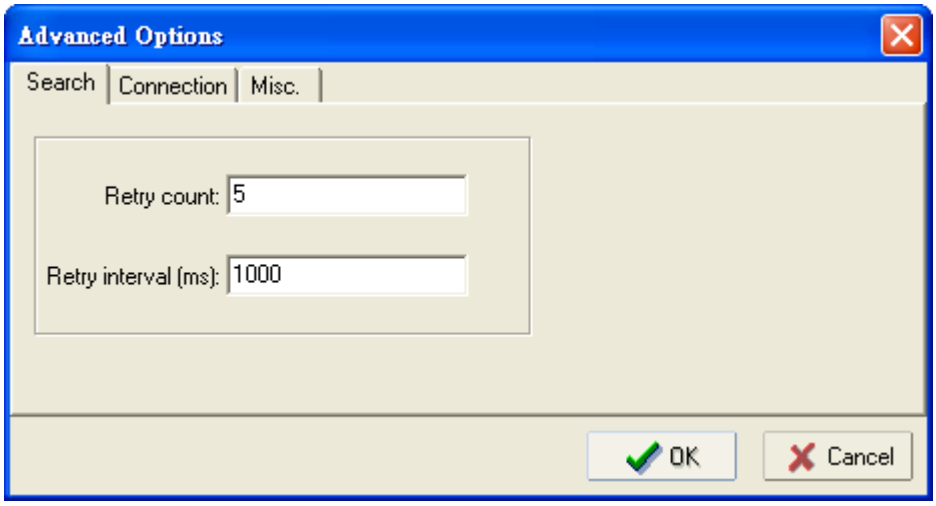


The three advanced options—**Search**, **Connection**, and **Miscellaneous**—are explained below:

Search

Retry count (default=5): Indicates how many times the search will retry automatically.

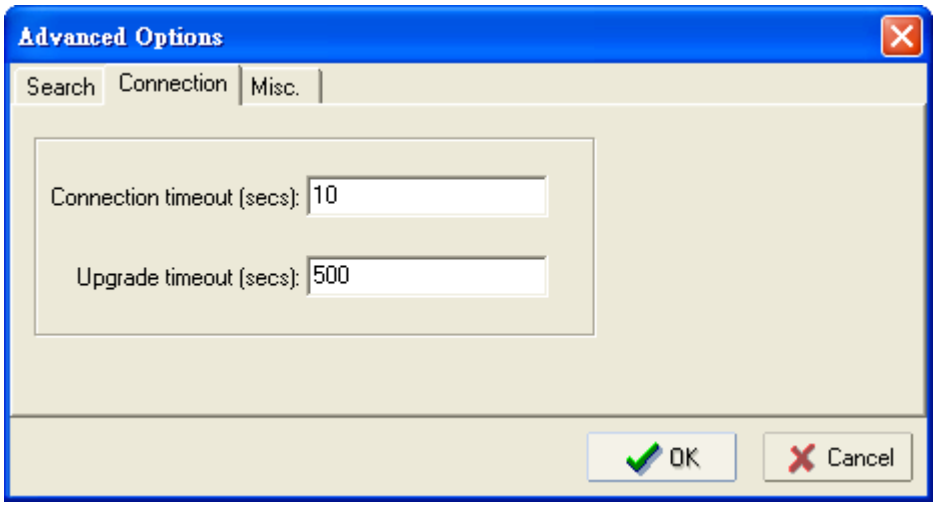
Retry interval (ms): The time interval between retries.



Connection

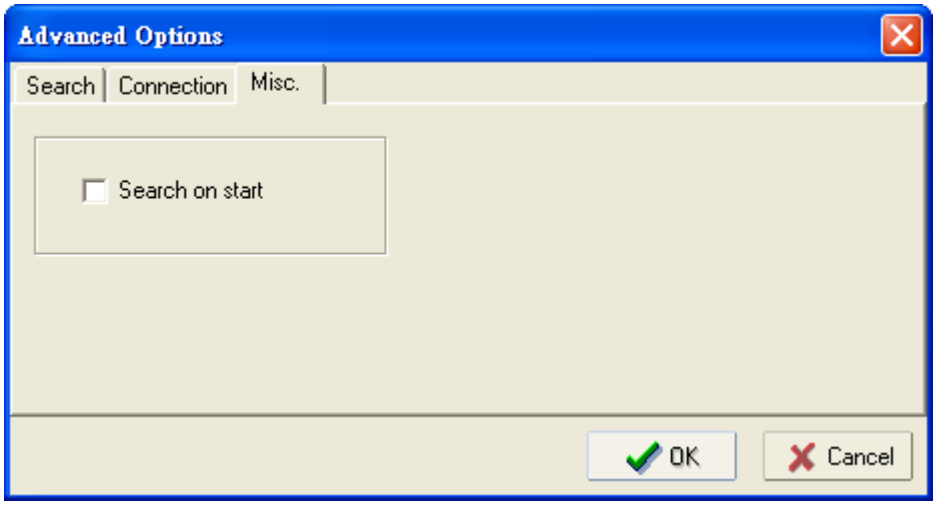
Connection timeout (secs): Use this option to set the time of inactivity during the Default Login, Locate, Assign IP, Upload Firmware, and Unlock functions before the connection times out.

Upgrade timeout (secs): Use this option to set the time of inactivity during a firmware is upgrading before the connection times out, which is the time taken for the firmware to be written to the flash memory.>



Misc.

Search on start: Select this option if you would like the search function to start searching for devices after you log in to the AWK search Utility.



5

Other Console Configurations

In this chapter, we explain how to access the TAP-6226 for the first time. In addition to HTTP access, there are four ways to access the TAP-6226: serial console, Telnet console, SSH console, and HTTPS console. The serial console connection method, which requires using a short serial cable to connect the TAP-6226 to a PC's COM port, can be used if you do not know the TAP-6226's IP address. The other consoles can be used to access the TAP-6226 over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration by Telnet and SSH Consoles**
- **Configuration by Web Browser with HTTPS/SSL**
- **Disabling Telnet and Browser Access**

ATTENTION

1. You **CANNOT** connect to the TAP-6226 with two or more console configurations simultaneously.
2. You *can* connect to the TAP-6226 simultaneously by web browser and serial/Telnet/SSH console. However, we strongly suggest that you do **NOT** use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your TAP-6226.

RS-232 Console Configuration (115200, None, 8, 1, VT100)

The serial console connection method, which requires using a short serial cable to connect the TAP-6226 to a PC's COM port, can be used if you do not know the TAP-6226's IP address. It is also convenient to use serial console configurations when you cannot access the TAP-6226 over an Ethernet LAN, as would be the case if the LAN cable gets disconnected or your network experiences a broadcast storm.

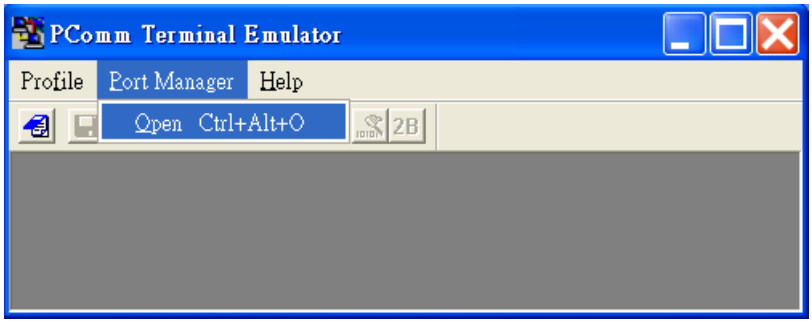
ATTENTION

Do not use the RS-232 console manager when the TAP-6226 is powered in reverse voltage (e.g., -48 VDC), even though reverse voltage protection is supported. If you need to connect the RS-232 console using reverse voltage, Moxa's TCC-82 isolator is your best solution.

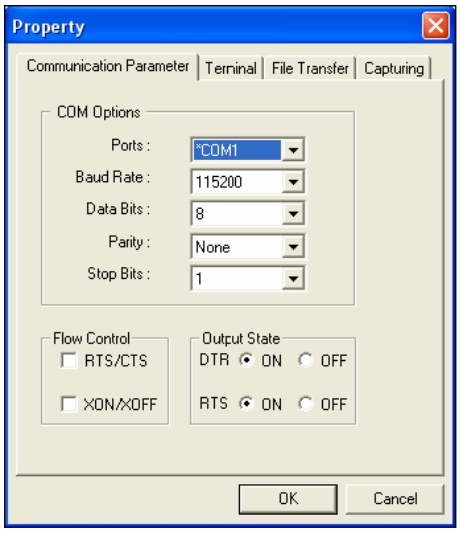
NOTE We recommend using Moxa PComm (Lite) Terminal Emulator, which can be downloaded free of charge from Moxa's website.

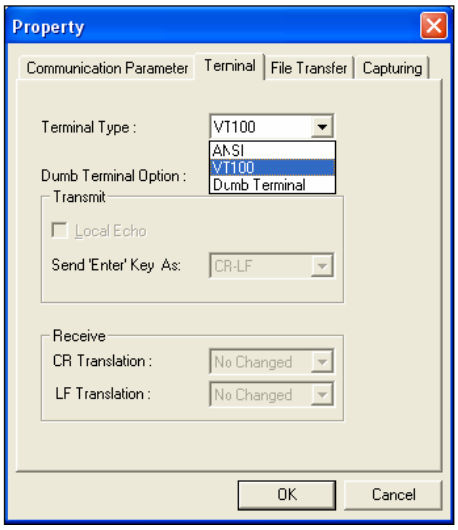
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the TAP-6226's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, take the following steps to access the RS-232 console utility.

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



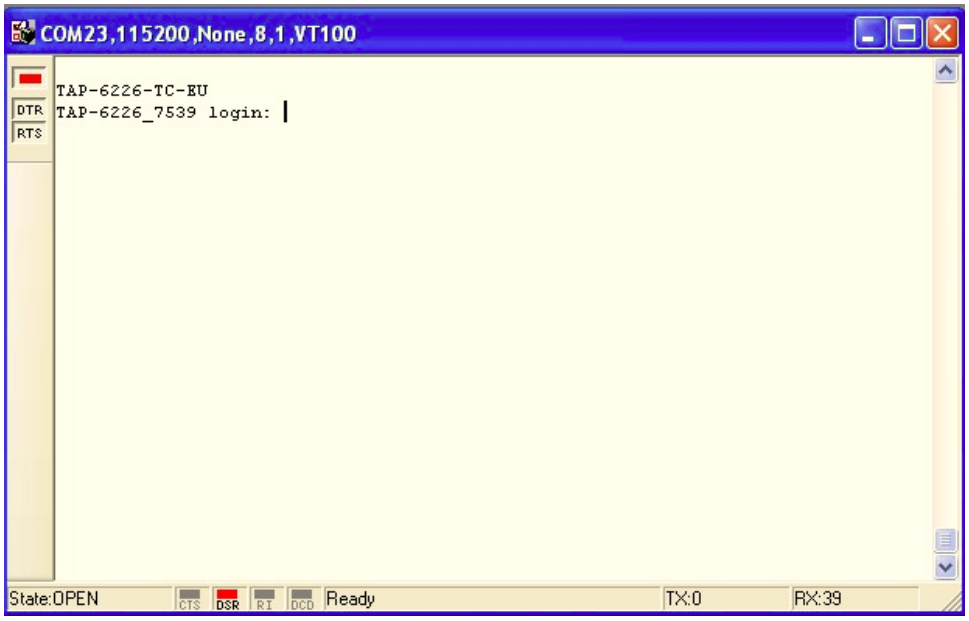
3. The **Communication Parameter** page of the Property window opens. Select the appropriate COM port for Console Connection, **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits.



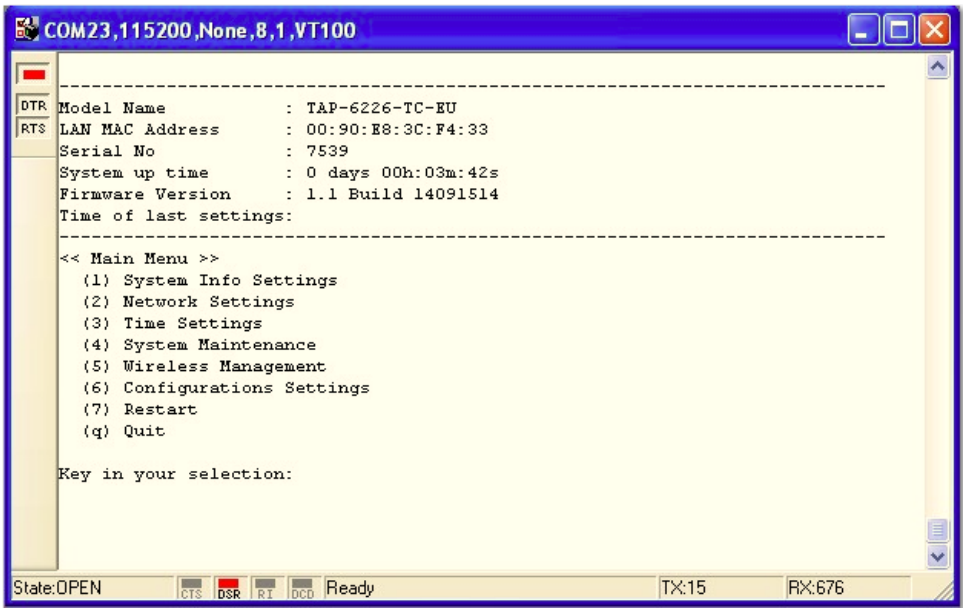


4. Click on the **Terminal** tab, and select **VT100 (or ANSI)** for Terminal Type. Click on **OK** to continue.
5. The Console login screen will appear. Log in to the RS-232 console with the login name (default: **admin**) and password (default: **moxa**, if no new password is set).

NOTE Firmware Version 1.6 password: moxa
Firmware Versions 1.0 to 1.5 password: root



6. The TAP-6226's device information and Main Menu will be displayed. Follow the onscreen instructions 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 RS-232 cable or trigger **DTR**, a disconnection event will be invoked to enforce logout for network security. You will need to log in again to resume operation.

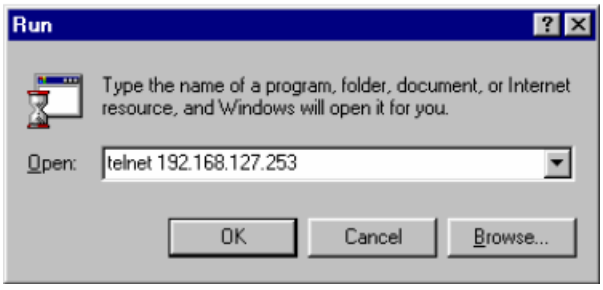
Configuration by Telnet and SSH Consoles

You may use a Telnet or SSH client to access the TAP-6226 and manage the console over a network. To access the TAP-6226's functions over the network from a PC host that is connected to the same LAN as the TAP-6226, you need to make sure that the PC host and the TAP-6226 are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

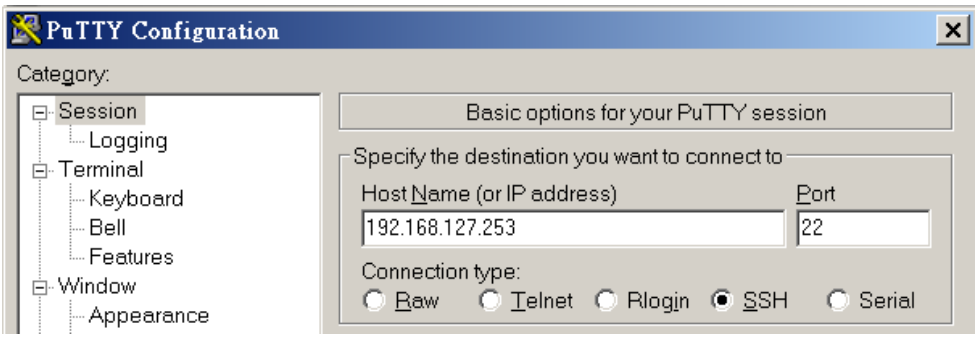
NOTE The TAP-6226's default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

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

1. From Windows Desktop, **Start** and then use Telnet to access the TAP-6226's IP address from the Windows **Run** window. (You may also issue the telnet command from an MS-DOS prompt.)



When using SSH client (e.g., PuTTY), run the client program (e.g., putty.exe) and then input the TAP-6226's IP address, specifying **22** for the SSH connection port.

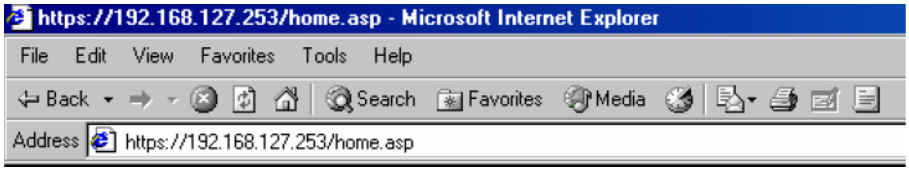


2. The Console login screen will appear. Refer to the previous section, **RS-232 Console Configuration**, for login and administration instructions.

Configuration by Web Browser with HTTPS/SSL

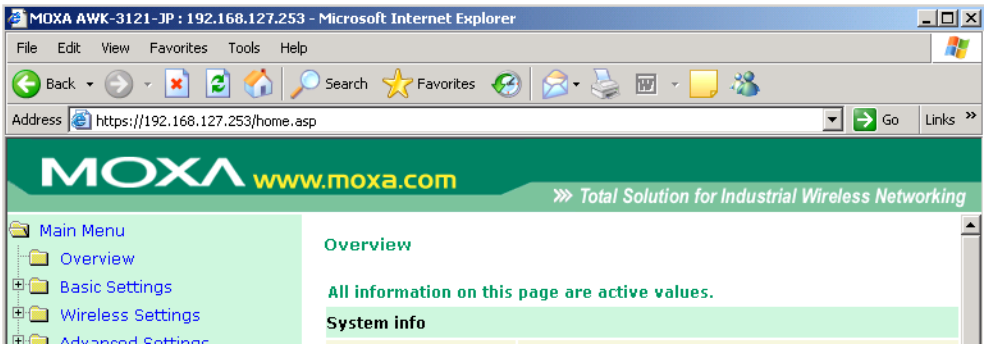
To secure your HTTP access, the TAP-6226 supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the TAP-6226's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://<TAP-6226's IP address> in the address field. Press **Enter** to establish the connection.



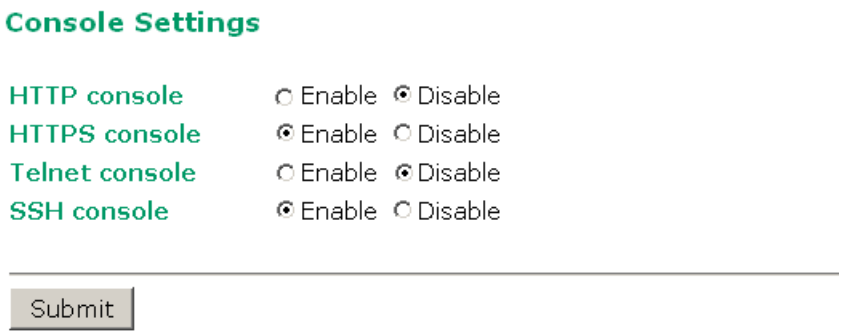
2. Warning messages will pop up to warn users that the security certificate was issued by a company they have not yet chosen to trust.

3. Select **Yes** to accept the certificate issued by Moxa IW and then enter the TAP-6226's web browser interface secured via HTTPS/SSL. (The **https** protocol will be visible at the beginning of the URL.) Use the menu tree on the left side of the window to access the TAP-6226's various functions.



Disabling Telnet and Browser Access

If you are connecting the TAP-6226 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. To do this, access **Maintenance → Console Settings**, as shown in the following figure.



6

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your TAP-6226 units and plan your industrial wireless network.

The following topics are covered in this chapter:

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

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 the AP.

DTIM

Delivery Traffic Indication Map (DTIM) is contained in beacon frames. It indicates 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

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 IEEE 802.1D standard, 1998 Edition bridge specification.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by the IEEE 802.1w-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 (AP and WDS1-WDS8) of the same TAP-6226.

This feature is particularly helpful when the TAP-6226 connects to older equipment, such as legacy switches.

Differences between RSTP and STP

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.

7

Support Information

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

The following topics are covered in this chapter:

- **DoC (Declaration of Conformity)**
  - Federal Communication Commission Interference Statement
  - R&TTE Compliance Statement
- **Firmware Recovery**
- **Technical Support Contact Information**

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 (e.g., use only shielded interface cables when connecting to a 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 transmitter and 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.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

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 followed 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.

Firmware Recovery

When **FAULT** and **STATE** LEDs all light up simultaneously and blink at one-second intervals, it means the system boot has failed. This may result from improper operation or an issue beyond the control of the user, such as an unexpected shutdown during a firmware update. The TAP-6226 is designed to help administrators recover from such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the TAP-6226's RS-232 console with **115200bps and N-8-1**. You will see the following message shown on the terminal emulator every second.

```
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
```

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

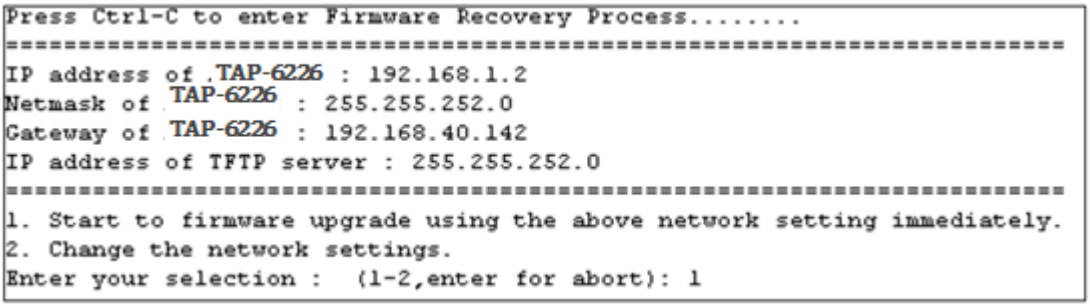
```
Press Ctrl-C to enter Firmware Recovery Process.....
Press Ctrl-C to enter Firmware Recovery Process.....
==========================================================================
IP address of TAP-6226  : 192.168.40.155
Netmask of TAP-6226  : 255.255.252.0
Gateway of TAP-6226  : 192.168.43.254
IP address of TFTP server : 192.168.40.142
==========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort):
```

Enter **2** to change the network setting. Specify the location of the TAP-6226's firmware file on the TFTP server and press **y** to write the settings into flash memory.

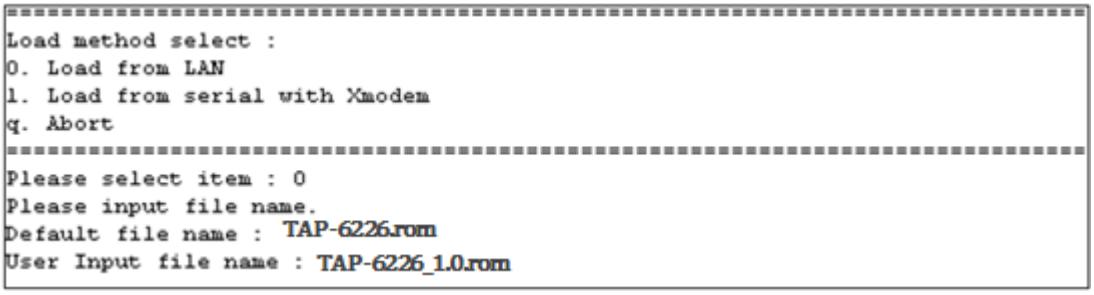
```
==========================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 2

IP address of  TAP-6226 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
Netmask of TAP-6226  : 255.255.252.0
Gateway of TAP-6226  : 192.168.1.254
Update RedBoot non-volatile configuration - continue (y/n)? y
```

The TAP-6226 will restart, 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.



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



Technical Support Contact Information

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Moxa Internet Services has been set up to provide technical support, driver updates, product information, certification status, installation guide and user's manual updates.

The following services are provided:

- Tech support emails:

  support@moxa.com (global)
  support@usa.moxa.com (The Americas)

- Links to Moxa's corporate website for product information:

  http://www.moxa.com