Moxa Tough AP TAP-213 User's Manual

Edition 1.0, April 2016

www.moxa.com/product

© 2016 Moxa Inc. All rights reserved.

Moxa Tough AP TAP-213 User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2016 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

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 Europe

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

Moxa India

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

Moxa China (Shanghai office)

Toll-free:	800-820-5036
Tel:	+86-21-5258-9955
Fax:	+86-21-5258-5505

Moxa Asia-Pacific

Tel:	+886-2-8919-1230
Fax:	+886-2-8919-1231

Table of Contents

1

Introduction

The TAP-213 outdoor wireless AP/client is the ideal ruggedized wireless solution [illegible] train-to-ground applications such as CCTV and CBTC communications. It can prov[illegible] ith IEEE 802.11n technology. The TAP-213's dust-tight/weatherproof design is IP68-rated, and it can operate at temperatures ranging from -40 to 75°C, allowing you to extend wireless networks to outdoor locations and critical environments.

Cecilia_Fernandes
2016-04-21 09:00:22

I suggest:
It can provide speeds of up to 300 Mbps...

The following topics are covered in this chapter:

- ❒ **Overview**
- ❒ **Package Checklist**
- ❒ **Product Features**
- ❒ **Product Specifications**
- ❒ **Functional Design**
  - ➢ LAN Port
  - ➢ LED Indicators
  - ➢ Beeper
  - ➢ Reset Button

Overview

The TAP-213 is 802.11n compliant to deliver speed, range, and reliability to support even the most bandwidth-intensive applications. The 802.11n standard incorporates multiple technologies, including MIMO (Multi-In, Multi-Out) Spatial Multiplexing, multiple channels (5, 10, 20 and 40 MHz), and dual bands (2.4 GHz and 5 GHz) to achieve high speeds, while still being able to communicate with legacy 802.11a/b/g devices.

The TAP-213 is compliant with the EN 50155 standard that covers operating temperature range, power input voltage, surge, ESD, and vibration. The TAP can be easily mounted on to a DIN rail or in distribution boxes. Its wide operating temperature range, IP68-rated housing with LED indicators, and the DIN-rail mounting capability make the TAP-213 a convenient yet reliable solution for all types of industrial wireless applications.

Package Checklist

Moxa's TAP-213 is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

Cecilia_Fernandes
2016-04-21 09:02:02

The preliminary datasheet has the following items listed:
• TAP-213
• Wall mounting kit (includes 2 supports)
• Metal cap to cover M12-female connector

- 1 TAP-213
- 1 Wall mounting kit
- 1 plastic protective caps for LAN-1 X-coded port
- 3 metal protective caps for LAN-2 fiber port, USB console port and ABC-02 USB storage port
- DIN-rail mounting kit
- Quick Installation Guide (printed)
- Product Warranty Card

NOTE *We support WiFi client mode, one-to-many Access Point mode, and one-to-one Wireless Bridge mode.*

For devices, depending on the type of antenna used (point-to-point or point-to-multipoint), the target power is fixed by the manufacturer prior to shipment, the antenna is delivered with the device and is configured by a professional installer, so that the radio does not exceed the EIRP allowed per regulatory domain.

Antenna List:

Point to Multipoint:

No.	Manufacturer	Part No.	Antenna Type	MAX Gain
1	KINSUN	ANT-WDB-O-2 BK	Dipole	2.9dBi for 2.4 GHz 2.34dBi for 5GHz
2	KINSUN	ANT-WDB-ANM-0502	Dipole	4.62dBi for 2.4 GHz 1.41dBi for 5GHz

- Point to Point:

No.	Manufacturer	Part No.	Antenna Type	MAX Gain
1	MOXA	ANT-WDB-PNF-1518	Directional panel	15dBi for 2.4 GHz 18dBi for 5GHz

Product Features

- Designed specifically for the wireless communication requirements in rail onboard CCTV and CBTC systems
- Compliant with EN 50155
- IEEE802.11a/b/g/n compliant
- Three-in-one design (AP/Bridge/Client)
- Advanced wireless security
  - 64-bit and 128-bit WEP/WPA/WPA2
  - SSID Hiding/IEEE 802.1X/RADIUS
  - Packet access control & filtering
- STP/RSTP support for network system redundancy
- Long-distance transmission support
- Turbo Roaming enables rapid handover (Client mode)
- ABC-02 for configuration import/export
- RS-232 console management
- Wide -40 to 75°C operating temperature range
- Redundant 24 VDC power inputs or IEEE802.3af Power over Ethernet
- DIN-rail mounting or wall mounting
- IP68-rated high-strength metal housing

Cecilia_Fernandes
2016-04-21 09:04:22

The preliminary datasheet has the following information: 24 to 110 VDC, redundant dual DC power inputs or 48 VDC Power-over-Ethernet (IEEE 802.3af compliant)

Product Specifications

WLAN Interface

Standards:

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

Spread Spectrum and Modulation (typical):

- DSSS with DBPSK, DQPSK, CCK
- OFDM with BPSK, QPSK, 16QAM, 64QAM
- 802.11b: CCK @ 11/5.5 Mbps, DQPSK @ 2 Mbps, DBPSK @ 1 Mbps
- 802.11a/g: 64QAM @ 54/48 Mbps, 16QAM @ 36/24 Mbps, QPSK @ 18/12 Mbps, BPSK @ 9/6 Mbps
- 802.11n: 64QAM @ 300 Mbps to BPSK @ 6.5 Mbps (multiple rates supported)

Operating Channels (central frequency):

- US:
  2.412 to 2.462 GHz (11 channels)
  5.180 to 5.240 GHz (4 channels)
  5.260 to 5.320 GHz (4 channels)*
  5.500 to 5.700 GHz (8 channels; excludes 5.600 to 5.640 GHz)*
  5.745 to 5.825 GHz (5 channels)
- EU:
  2.412 to 2.472 GHz (13 channels)
  5.180 to 5.240 GHz (4 channels)
  5.260 to 5.320 GHz (4 channels)*
  5.500 to 5.700 GHz (11 channels)*
- JP:
  2.412 to 2.484 GHz (14 channels, DSSS)
  5.180 to 5.240 GHz (4 channels)
  5.260 to 5.320 GHz (4 channels)*
  5.500 to 5.700 GHz (11 channels)*

*Special frequency bands (up to 6.0 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
- 802.11n: 6.5 to 300 Mbps (multiple rates supported)

TX Transmit Power:

- 2.4 GHz
  802.11b:
  Typ. 26±1.5 dBm @ 1 to 11 Mbps
  802.11g:
  Typ. 25±1.5 dBm @ 6 to 24 Mbps, Typ. 23±1.5 dBm @ 36 Mbps,
  Typ. 20±1.5 dBm @ 48 Mbps, Typ. 20±1.5 dBm @ 54 Mbps
  802.11n (20 MHz):
  MCS0, 8@20 MHz: Typ. 23 dBm (±1.5 dBm); MCS7, 15@20 MHz:
  Typ. 17 dBm (±1.5 dBm); MCS0, 8@40 MHz: Typ. 23 dBm (±1.5 dBm);
  MCS7, 15@40 MHz: Typ. 17 dBm (±1.5 dBm)
- 5 GHz
  802.11a:
  Typ. 23±1.5 dBm @ 6 to 24 Mbps, Typ. 21±1.5 dBm @ 36 Mbps,
  Typ. 20±1.5 dBm @ 48 Mbps, Typ. 18±1.5 dBm @ 54 Mbps
  802.11n (20/40 MHz):
  MCS0, 8@20 MHz: Typ. 23 dBm (±1.5 dBm); MCS7, 15@20 MHz:
  Typ. 18 dBm (±1.5 dBm); MCS0, 8@40 MHz: Typ. 23 dBm (±1.5 dBm);
  MCS7, 15@40 MHz: Typ. 18 dBm (±1.5 dBm)

RX Sensitivity:

- 2.4 GHz
  802.11b:
  -93 dBm @ 1 Mbps, -93 dBm @ 2 Mbps,
  -93 dBm @ 5.5 Mbps, -88 dBm @ 11 Mbps
  802.11g:
  -88 dBm @ 6 Mbps, -86 dBm @ 9 Mbps, -85 dBm @ 12 Mbps,
  -86 dBm @ 18 Mbps, -85 dBm @ 24 Mbps, -82 dBm @ 36 Mbps,
  -78 dBm @ 48 Mbps, -74 dBm @ 54 Mbps
  802.11n:
  -67 dBm @ MCS15 40 MHz, -69 dBm @ MCS15 20 MHz,
  -67 dBm @ MCS7 40 MHz, -70 dBm @ MCS7 20 MHz
- 5 GHz
  802.11a:
  -90 dBm @ 6 Mbps, -88 dBm @ 9 Mbps, -88 dBm @ 12 Mbps,
  -85 dBm @ 18 Mbps, -81 dBm @ 24 Mbps, -78 dBm @ 36 Mbps,
  -74 dBm @ 48 Mbps, -74 dBm @ 54 Mbps
  802.11n:
  -68 dBm @ MCS15 40 MHz, -71 dBm @ MCS15 20 MHz,
  -63 dBm @ MCS7 40 MHz, -69 dBm @ MCS7 20 MHz

Protocol Support

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

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

Interface

Connector for External Antennas: N-type (female)

Fiber Ports: 1000Base SFP slot

M12 Ports: 1, M12-type, 8-pin X-coding (female), 10/100/1000BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection

Console Port: USB Console (M12 5-pin A-coded connector female)

USB Port: M12 B-coded connector for ABC-02

Reset: Present

LED Indicators: PWR, FAULT, STATE, WLAN, LAN 1, LAN 2

Physical Characteristics

Housing: Metal, IP68 protection

Weight: 1.5 kg

Dimensions: 220 x 150 x 55 mm (8.66 x 5.90 x 2.16 in)

Installation: Wall mounting (standard), DIN-rail mounting (optional)

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 100% (non-condensing)

Power Requirements

Input Voltage: 24 to 110 VDC, redundant dual DC power inputs or 48 VDC Power-over-Ethernet (IEEE 802.3af compliant)

Input Current: 24 to 110 VDC, 15 W (max.)

Connector: M12 male connector

Reverse Polarity Protection: Present

Standards and Certifications

Safety: UL 60950-1, IEC 60950-1(CB)

EMC: EN 61000-6-2/6-4, EN 61000-6-1/6-3

EMI: FCC Part 15B Class A

EMS:

IEC 61000-4-2 ESD: Contact: 6 kV; Air: 8 kV

IEC 61000-4-3 RS: 80 MHz to 1 GHz: 20 V/m

IEC 61000-4-4 EFT: Power: 2 kV; Signal: 2 kV

IEC 61000-4-5 Surge: Power: 2 kV; Signal: 2 kV

IEC 61000-4-6 CS: 10 V

IEC 61000-4-8

Radio: EN 301 489-1/17, EN 300 328, EN 301 893, DFS, TELEC

Rail Traffic: EN 50155 (essential compliance*), EN 50121-4

*Moxa defines "essential compliance" to include those EN 50155 requirements that make products more suitable for rolling stock railway applications.

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

Fire and Smoke: EN 45545

MTBF (mean time between failures)

Time: 400,000 hrs

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty

ATTENTION

- The TAP-213 is NOT a portable mobile device and should be located at least 20 cm away from the human body.
- The TAP-213 is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of TAP-213 units, and to establish a wireless network.

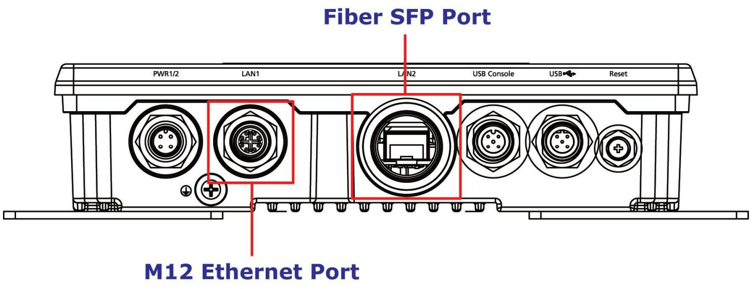
Functional Design

LAN Port

The standard model of the TAP-213 is provided with one M12 X code Gigabit port. The LAN LED will light up when the LAN-1 cable is inserted.

Cecilia_Fernandes
2016-04-21 09:06:09

The label on the product is "LAN1" I suggest:
The LAN LED will light up when you insert the cable in the LAN1 port and a connection is established.



ATTENTION

Do not use a PoE (Power over Ethernet) Injector for the PoE device(s). Instead, use an IEEE 802.3af or IEEE 802.3at compliant PSE (Power Sourcing Equipment).

Cecilia_Fernandes
2016-04-21 09:06:35

Content modified, please check

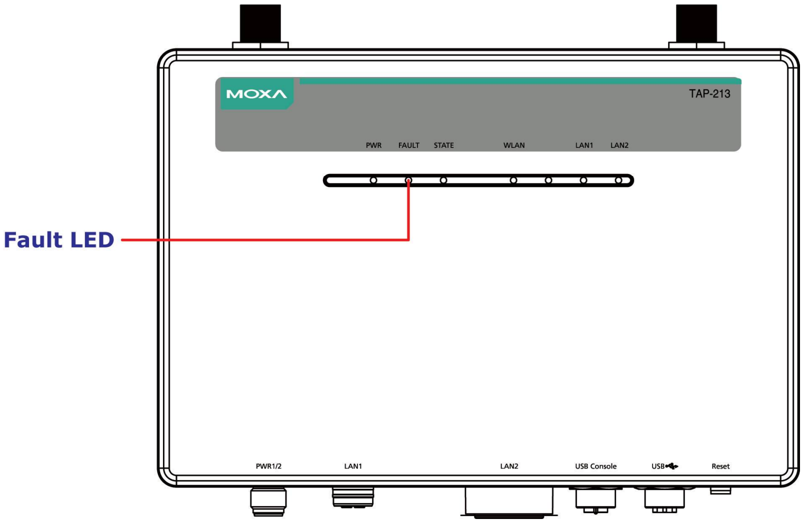
LED Indicators

The LEDs on the front panel provide a quick and easy means of determining the current operational status and wireless settings of the TAP-213.

The **FAULT** LED indicates system failures and user-configured events. If the TAP-213 fails to receive the IP address from a DHCP server, the **FAULT** LED will blink at one-second intervals.

Cecilia_Fernandes
2016-04-21 09:07:36

What does the fault LED indicate about user-configured events. We need to explain this as it is not clear.



The following table summarizes how to read the device’s wireless settings based on the LED displays. More information is available in Chapter 3 in the “Basic Wireless Settings” section.

LED	Color	State	Description
PWR	Green	On	Power is being supplied (from powe
		Off	Power is **not** being supplied.
FAULT	Red	On	System is booting up, or a system c
		Blinking (fast at 0.5-second intervals)	Cannot get an IP address from the
		Blinking (slow at 1-second intervals)	IP address conflict
		Off	Error condition does not exist.
STATE	Green	On	System startup is complete and the system is in operation.
		Blinking (fast at 0.5-second intervals)	AeroLink Protection is enabled and is currently in “Backup” state.
		Blinking (slow at 1-second intervals)	Device has been located by Wireless Utility
	Red	On	System is booting up.
WLAN	Green	On	WLAN is functioning in **Client/Slave** mode.
		Blinking	WLAN is transmitting data in **Client/Slave** mode.
		Off	WLAN is not in **Client/Slave/Client-Router** mode or has not established a link with an AP.
	Amber	On	WLAN is in **AP/Master** mode.
		Blinking	WLAN is transmitting data in **AP/Master** mode.
		Off	WLAN is not in use or is not working properly.
LAN1/LAN2	Green	On	LAN port’s 1000 Mbps link is **active**.
		Blinking	Data is being transmitted at 1000 Mbps.
		Off	LAN port’s 1000 Mbps link is **inactive**.
	Amber	On	LAN port’s 10/100 Mbps link is **active**.
		Blinking	Data is being transmitted at 10/100 Mbps.
		Off	LAN port’s 10/100 Mbps link is **inactive**.

Cecilia_Fernandes
2016-04-21 09:08:35

Cecilia_Fernandes
2016-04-21 09:08:54
Power is on (supplied from power input 1)

I suggest removing this. If we must mention it then I suggest "...or a system configuration error exists."

Cecilia_Fernandes
2016-04-21 09:09:24

I suggest:
No error condition exists.

ATTENTION

When the system fails to boot, the LEDs for **STATE** (Green), **FAULT**, and **WLA** simultaneously and blink at one-second intervals. This may be due to improper issues, such as an unexpected shutdown while updating the firmware. To recover the firmware, refer to the “Firmware Recovery” section in Chapter 6.

Cecilia_Fernandes
2016-04-21 09:09:46

I suggest removing this content.

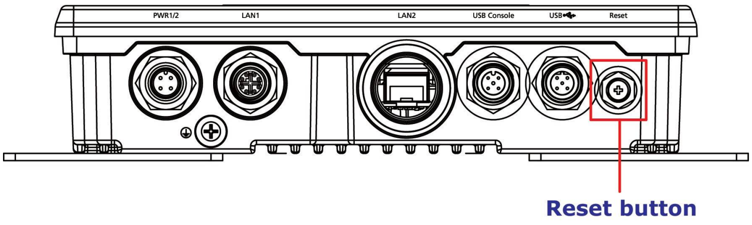
Beeper

The beeper emits two short beeps when the system is ready.

Reset Button

The **Reset** button is located on the top panel of the TAP-213. You can reboot the TAP-213 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 **under 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 light. Release the button to reset the TAP-213.



2

Getting Started

This chapter explains how to install Moxa's AirWorks TAP-213 for the first time to quickly set up your wireless network and how to test whether the connection is working well. The function map provided in Chapter 3 is a convenient reference to the various functions available on the TAP-213 and to determine the functions that you need to use.

The following topics are covered in this chapter:

❒ **First-Time Installation and Configuration**

❒ **Communication Testing**

❒ **Function Map**

First-Time Installation and Configuration

Before installing the TAP-213, make sure that all items mentioned in the package checklist are in the box. You will also need access to a notebook computer or PC equipped with an Ethernet port. The TAP-213 has a default IP address that you must use when connecting to the device for the first time.

- **Step 1: Select the power source.**
  The TAP-213 can be powered by a DC power input or PoE (Power over Ethernet).
- **Step 2: Connect the TAP-213 to a notebook or PC.**
  Since the TAP-213 is provided with the MDI/MDI-X auto-sensing capability, you can use either a straight-through cable or crossover cable to connect it to a computer. When the connection between the TAP-213 and the computer is established, the LED indicator on the TAP-213's LAN port lights up.
- **Step 3: Set up the computer's IP address.**
  Set an IP address for the computer so that it is on the same subnet as that of the TAP-213. Since the TAP-213's default IP address is **192.168.127.253**, and the subnet mask is **255.255.255.0**, set the IP address of the computer in the **192.168.127.xxx** IP range and subnet mas

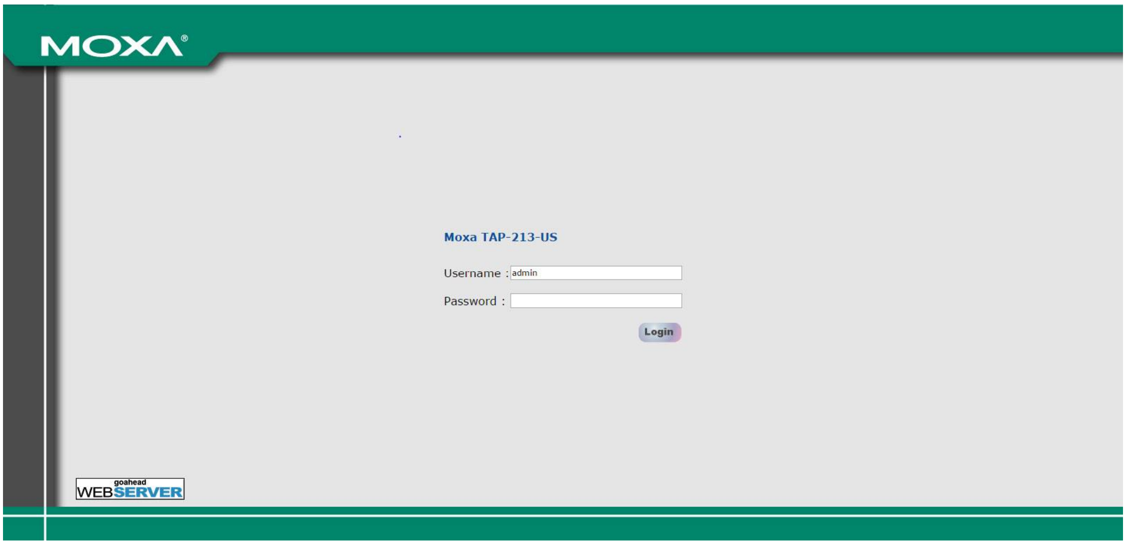
NOTE After you select **Maintenance → Load Factory Default** and click the **Submit** button, the TAP-213 will be reset to factory default settings and the IP address will be reset to **192.168.127.253**.

Cecilia_Fernandes
2016-04-21 09:14:43

If we mention this here, if sounds like we also have to set the default IP address of the TAP.
Load Factory Default is covered on page 59 (3-42) and used only in exceptional cases as per my understanding.

- **Step 4: Use the web-based manager to configure the TAP-213**
  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 following default user name and password and click on the **Login** button:

User Name:	**admin**
Password:	**root**

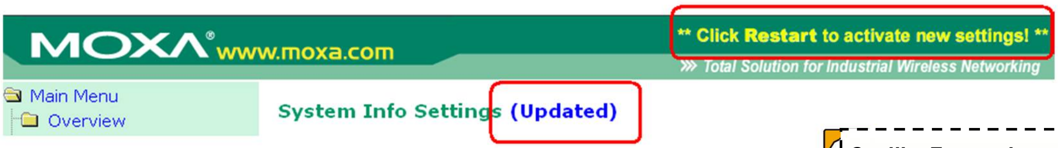

Moxa TAP-213-US

Username : admin

Password :

NOTE For security reasons, we strongly recommend changing the default password. To change the password, select **Maintenance → Password** and follow the instructions on the screen.

NOTE After you click **Submit** to apply changes, the web page is refreshed and an **(Updated)** indicator is displayed next to the page heading along with a blinking reminder to restart the device.


MOXA www.moxa.com
** Click Restart to activate new settings! **
Total Solution for Industrial Wireless Networking
Main Menu
Overview
System Info Settings (Updated)

To activate the changes, click **Restart** and then click **Save and Restart** after y[illegible] The TAP-213 will take about 30 seconds to complete the reboot process.

Cecilia_Fernandes
2016-04-21 09:16:09

Can you please confirm this.
When we click on Restart, doesn't the TAP reboot?

- **Step 5: Select the operation mode for the TAP-213.**
  By default, the operation mode of the TAP-213 is set to **AP**. You can change this setting to **Client** mode at **Wireless Settings → Basic Wireless Settings**. Detailed information about configuring the TAP-213 is available in Chapter 3.

- **Step 6: Test the network connection.**
  In the following sections we describe two methods that you can use to test that a network connection has been established.

Communication Testing

After installing the TAP-213 you can run a sample test to make sure the wireless connection on the TAP-213 is functioning normally. Two testing methods are described below. Use the first method if you are using only one TAP-213 device, and the second method if you are using two or more TAP-213 units.

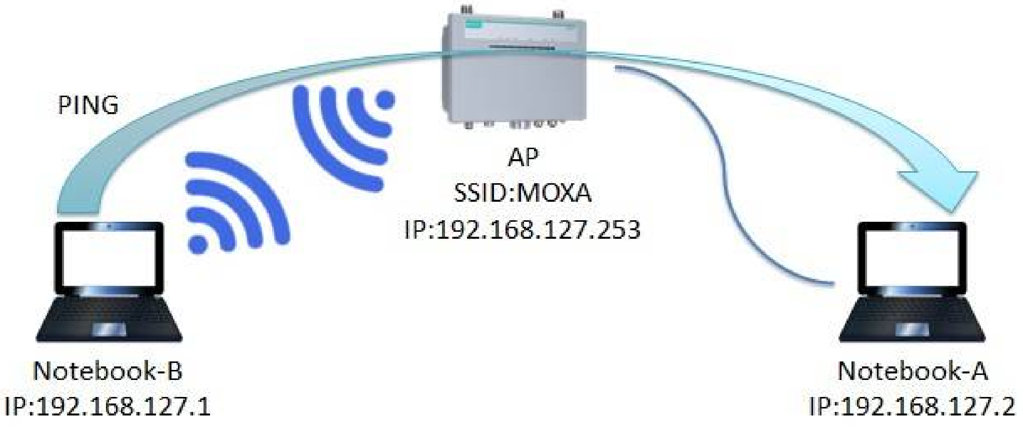
How to Test One TAP-213

If you are only using one TAP-213, you will need one additional notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the TAP-213 (NOTE: the default SSID is **MOXA**), and change the IP address of the second notebook (Notebook B) so that it is on the same subnet as the first notebook (Notebook A), which is connected to the TAP-213.

After configuring the WLAN card, establish a wireless connection with the TAP-213 and open a DOS window on Notebook B. At the prompt, type the following:

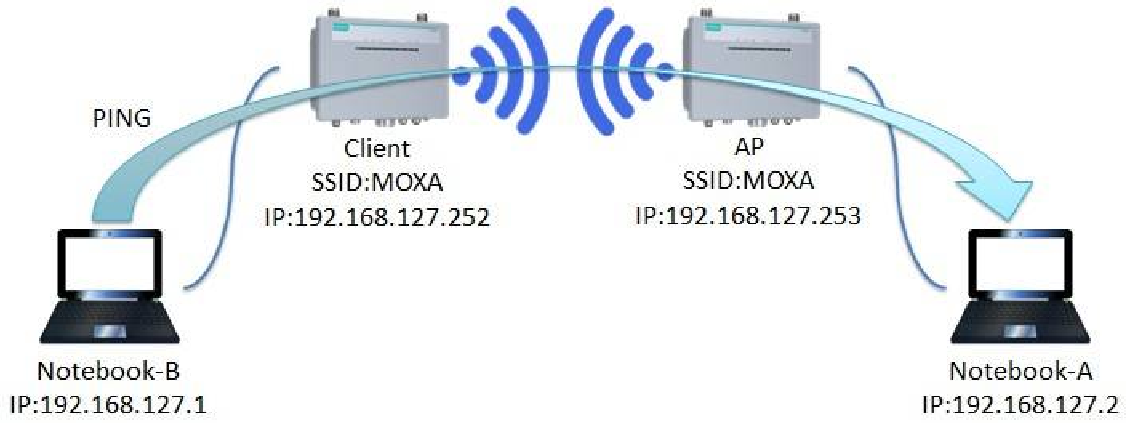
ping *<IP address of notebook A>*

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



How to Test Two or More TAP-213 Units

If you have two or more TAP-213 units, you will need a second notebook computer (Notebook B) equipped with an Ethernet port. Use the default settings for the first TAP-213 connected to notebook A and change the second or third TAP-213 connected to notebook B to Client mode, and then configure the notebooks and TAP-213 units properly.



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

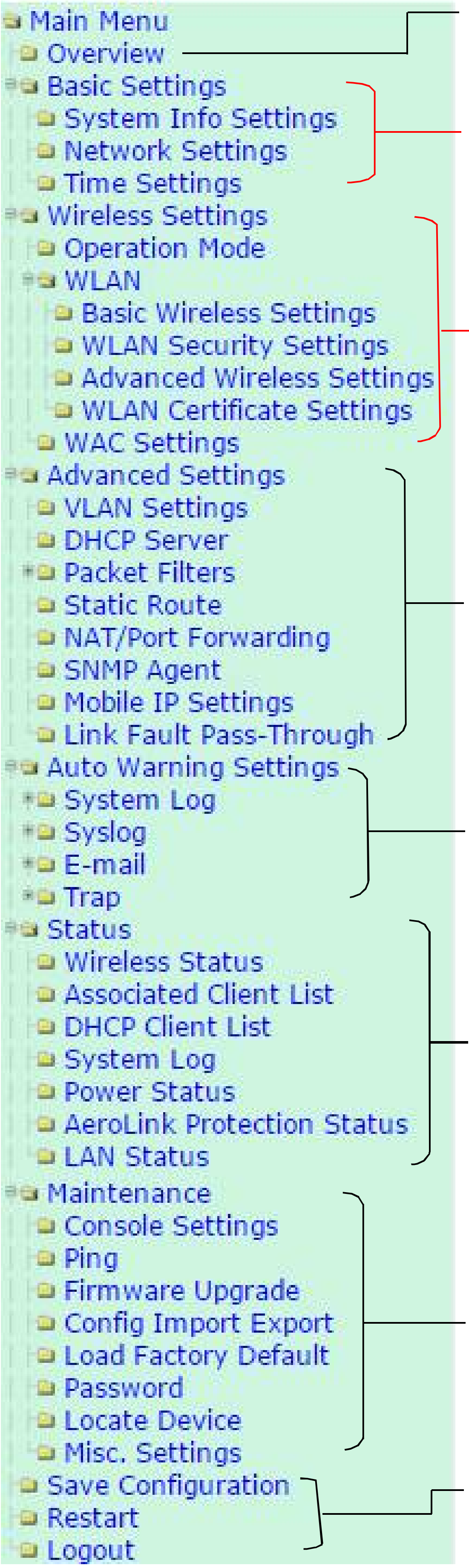
ping *<IP address of notebook A>*

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

Cecilia_Fernandes
2016-04-21 09:16:55

Are we talking about the physical connections or the settings in the web manager?

Function Map



Quick overview of the TAP-213's status

Basic settings for administering the TAP-213

Essential settings related to establishing a wireless network

Advanced features to support additional network management and secure wired and wireless communication

Note: These advanced functions are all optional

Application-oriented device management functions to set up events, traps, and reactions via relay warning, e-mail, and SNMP notification

Note: These functions are all optional

Current status information for monitoring wired/wireless network performance, advanced services, and device management functions

Functions for maintaining the TAP-213, and for diagnosing the network

On-demand functions to support the web-based console management operation

3

Web Console Configuration

In this chapter, we explain all aspects of web-based console configuration. Moxa's easy-to-use management functions help you set up your TAP-213 and make it easy to establish and maintain your wireless network.

The following topics are covered in this chapter:

Web Browser Configuration

The web interface provides a convenient way to modify the configuration of the TAP-213 and access its built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the management and monitoring functions of the TAP-213 from a PC host connected to the same LAN as the TAP-213, you must make sure that the PC host and the TAP-213 are on [illegible] Similarly, if the TAP-213 is configured for other VLAN settings, you must make [illegible] on the management VLAN.

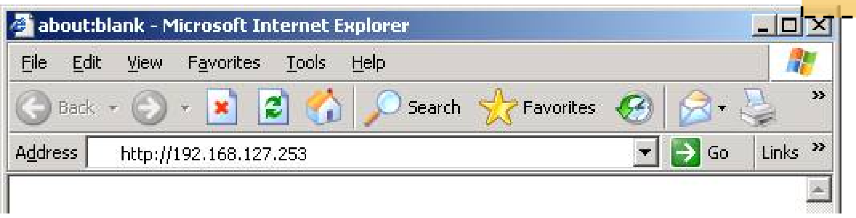
The default IP address of the TAP is **192.168.127.253**.

Cecilia_Fernandes
2016-04-21 09:17:45

What other VLAN settings? Please help clarify this content.

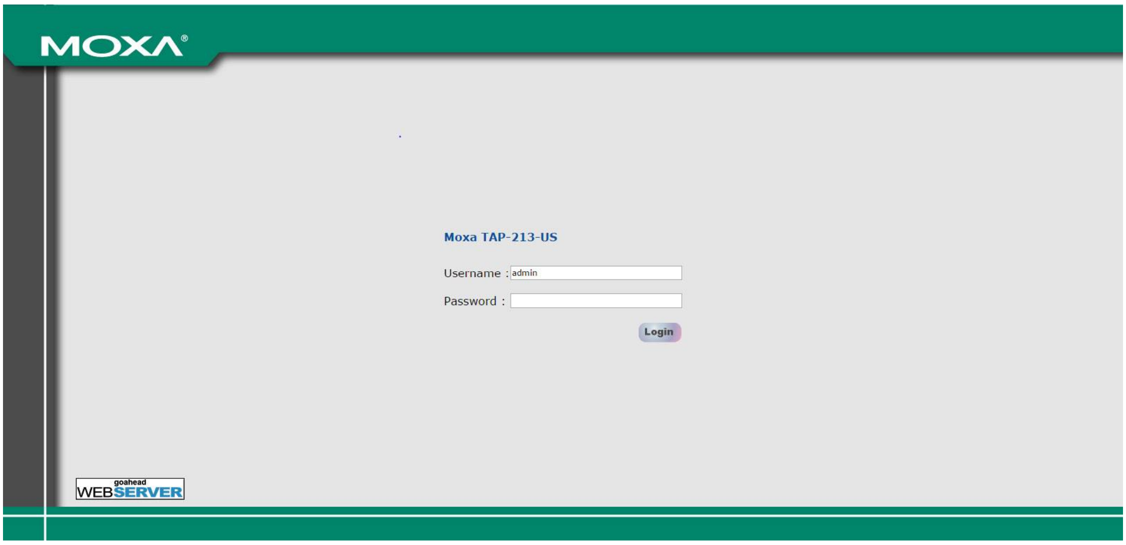
To access the web interface of the TAP-213, do the following:

1. Open a web browser (e.g., Internet Explorer), type in the default IP address of the TAP-213 in the address field, and press **Enter**.


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links

http://192.168.127.253

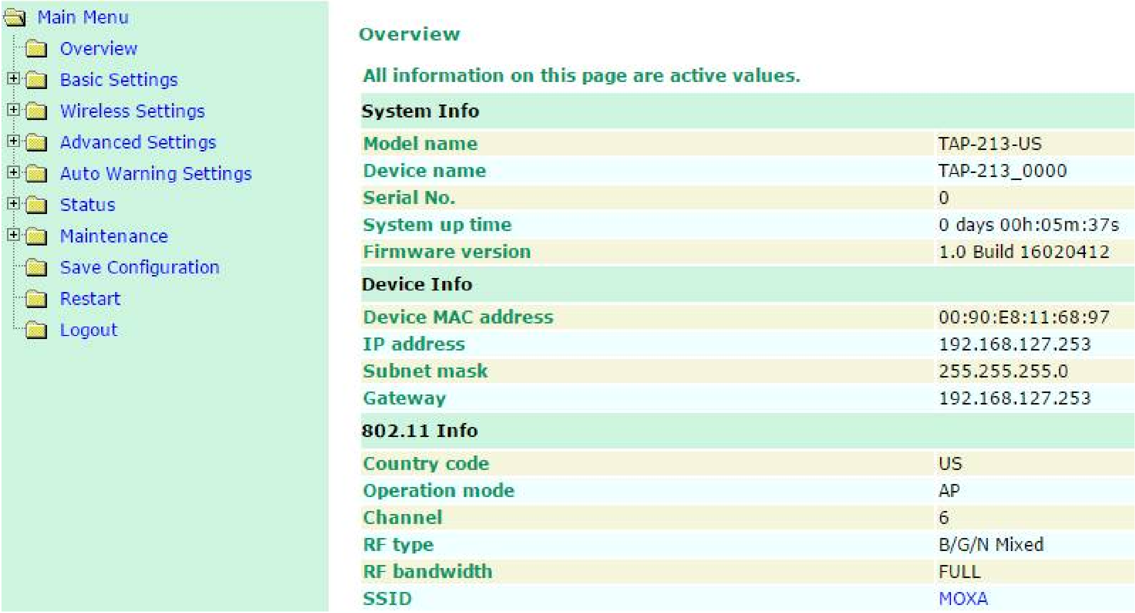
2. In the login page that is displayed, enter the **Username** and **Password** (default Username = **admin**; default Password = **root**) and click **Login** to continue.



Username : admin
Password :

You may need to wait a few moments for the main page to download to your computer. Note that the model name and IP address of the TAP-213 are both shown in the title bar of the web page. You can identify the web interfaces of multiple TAP-213 units using this information.

3. Use the menu tree on the left side of the window to open the configuration pages for the TAP-213's functions.



Overview

All information on this page are active values.

System Info	
Model name	TAP-213-US
Device name	TAP-213_0000
Serial No.	0
System up time	0 days 00h:05m:37s
Firmware version	1.0 Build 16020412
Device Info	
Device MAC address	00:90:E8:11:68:97
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	192.168.127.253
802.11 Info	
Country code	US
Operation mode	AP
Channel	6
RF type	B/G/N Mixed
RF bandwidth	FULL
SSID	MOXA

In the following paragraphs, we describe each TAP-213 management function in detail. An overview of all the functions is available in the "Function Map" section of this manual.

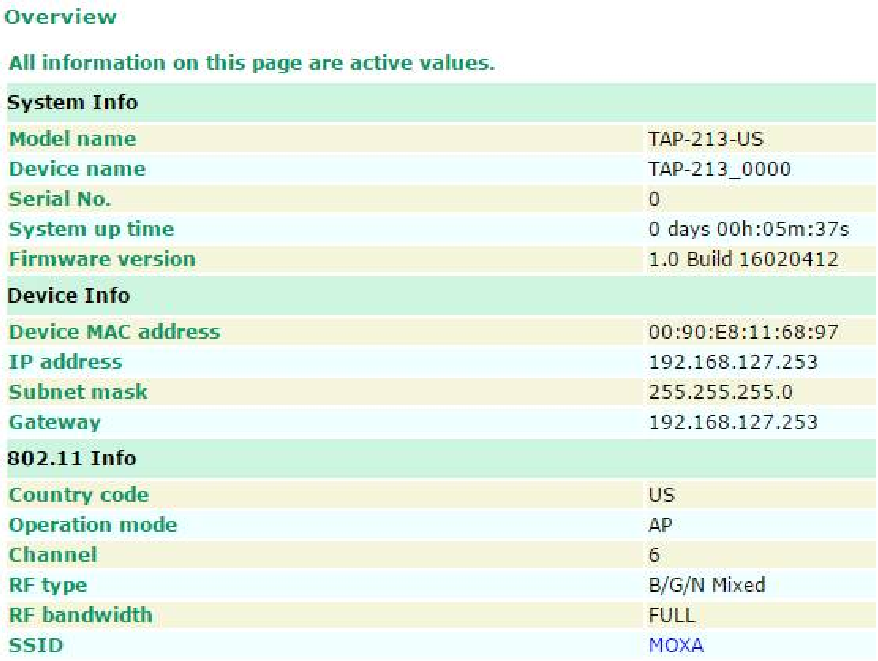
NOTE The model name of the TAP-213 is shown as TAP-213-XX, where XX indicates the country code. The country code indicates the TAP-213 version and the bandwidth it uses. We use **TAP-213-US** in the following figures. (The country code and model name that appears on your computer screen may be different than the one shown here.)

Cecilia_Fernandes
2016-04-21 09:19:21

The country code does not indicate the TAP-213 version or does it? I suggest removing this part.

Overview

The **Overview** page summarizes the TAP-213's current status. The information is categorized into the following groups: **System Info**, **Device Info**, and **802.11 Info**.

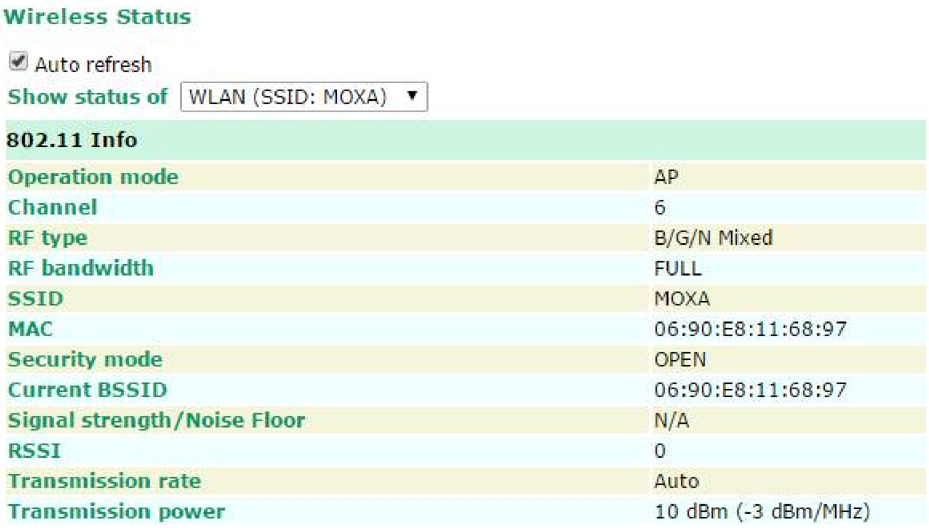


Overview

All information on this page are active values.

System Info	
Model name	TAP-213-US
Device name	TAP-213_0000
Serial No.	0
System up time	0 days 00h:05m:37s
Firmware version	1.0 Build 16020412
Device Info	
Device MAC address	00:90:E8:11:68:97
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	192.168.127.253
802.11 Info	
Country code	US
Operation mode	AP
Channel	6
RF type	B/G/N Mixed
RF bandwidth	FULL
SSID	MOXA

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



Wireless Status

☑ Auto refresh

Show status of WLAN (SSID: MOXA) ▼

802.11 Info	
Operation mode	AP
Channel	6
RF type	B/G/N Mixed
RF bandwidth	FULL
SSID	MOXA
MAC	06:90:E8:11:68:97
Security mode	OPEN
Current BSSID	06:90:E8:11:68:97
Signal strength/Noise Floor	N/A
RSSI	0
Transmission rate	Auto
Transmission power	10 dBm (-3 dBm/MHz)

NOTE The **802.11 Info** that is displayed may differ based on the operation mode selected. For example, **Current BSSID** is not available in **Client** mode, and **Signal strength/Noise Floor** is not available in **AP** mode.

Basic Settings

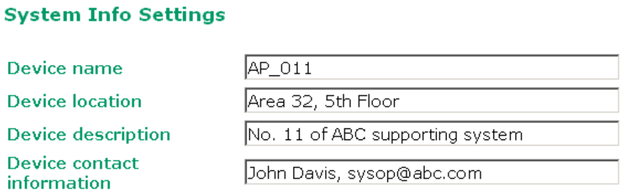
The **Basic Settings** group includes the most commonly used settings required by administrators to maintain and control the TAP-213.

System Info Settings

The **System Info** related settings that you configure here, especially the **Devic** **description**, are displayed on the **Overview** page. They are also included in the emails. Configuring the **System Info** settings for each TAP-213 makes it easier TAP-213 units connected to your network.

Cecilia_Fernandes
2016-04-21 09:20:05

I suggest:
alert or warning



System Info Settings

Device name	AP_011
Device location	Area 32, 5th Floor
Device description	No. 11 of ABC supporting system
Device contact information	John Davis, sysop@abc.com

Device name

Setting	Description
Maximum of 31 characters	Specifies the role or application of this TAP-213 unit.

Cecilia_Fernandes
2016-04-21 09:20:29

I
suggest:

Device location

Setting	Description
Maximum. of 31 characters	Specifies the location of this TAP-213 unit.

Cecilia_Fernandes
2016-04-21 09:20:35

I
suggest:

Device description

Setting	Description
Maximum of 31 characters	You can use this space to record a more detailed description of this TAP-213

Cecilia_Fernandes
2016-04-21 09:20:41

I
suggest:
Format

Device contact information

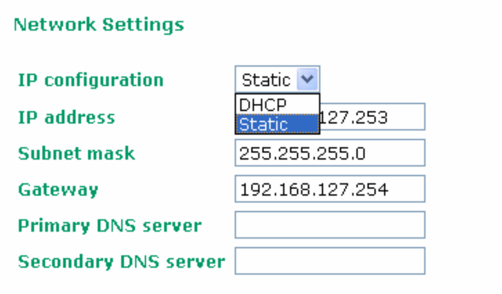
Setting	Description	Factory Default
Maximum of 31 characters	You can use this space to record the contact information of the person responsible for maintaining this TAP-213.	None

Cecilia_Fernandes
2016-04-21 09:20:48

suggest:
Format

Network Settings

The **Network Settings** configuration panel allows you to modify the TCP/IP parameters of the network. An explanation of each configuration item is given below:



Network Settings

IP configuration: Static (DHCP / Static)
IP address: 127.253
Subnet mask: 255.255.255.0
Gateway: 192.168.127.254
Primary DNS server:
Secondary DNS server:

IP configuration

Setting	Description	Factory Default
DHCP	Select this option if you want the TAP-213's IP address to be assigned automatically.	Static
Static	Select this option if you want to manually set the IP address of the TAP-213.	

IP address

Setting	Description	Factory Default
TAP-213's IP address	Identifies the TAP-213 on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
TAP-213's subnet mask	Identifies the type of network to which the TAP-213 is connected (e.g., 255.255.0.0 for a Class B network and 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

Setting	Description	Factory Default
TAP-213'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 the primary/secondary DNS server	The IP address of the DNS server used by your network. After you have entering the DNS server's IP address here, you can use the URL of the TAP-213 (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

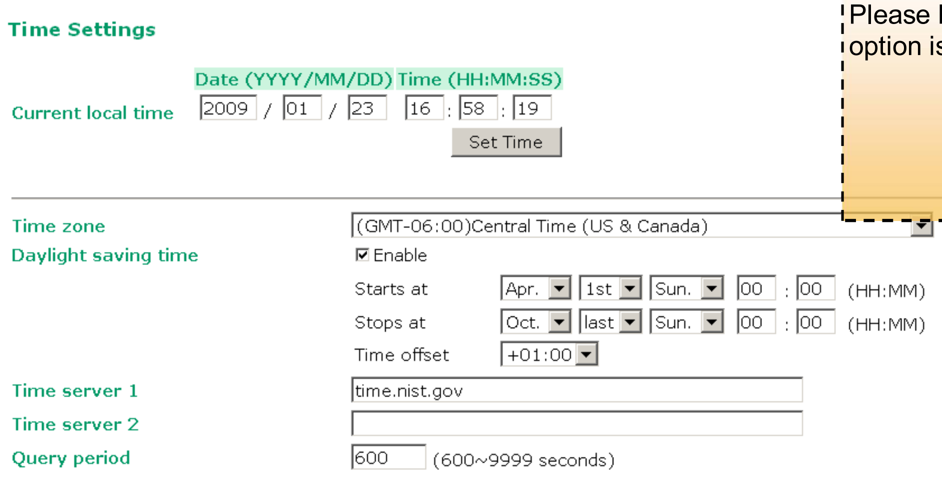
NOTE In the **Client-Router** mode, the WAN (wireless interface) and LAN (wired interface) are configured separately.

Time Settings

The TAP-213 has a time calibration function that can update the date and time information based on an NTP server or the date and time information specified by the user. Functions such as information to the message.

Cecilia_Fernandes
2016-04-21 09:21:52

Please help clarify. The Auto warning option is not available on this screen.



Time Settings

	Date (YYYY/MM/DD)	Time (HH:MM:SS)
Current local time	2009 / 01 / 23	16 : 58 : 19

Time zone	(GMT-06:00)Central Time (US & Canada)
Daylight saving time	☑ Enable
Starts at	Apr. 1st Sun. 00 : 00 (HH:MM)
Stops at	Oct. last Sun. 00 : 00 (HH:MM)
Time offset	+01:00
Time server 1	time.nist.gov
Time server 2	
Query period	600 (600~9999 seconds)

The **Current local time** shows the TAP-213's system time when you open this web page. After you update the date and time setting, click on the **Set Time** button to activate the new date a is displayed next to the date and time fields to indicate that the change is comp immediately activated in the system without running Save and Restart.

Cecilia_Fernandes
2016-04-21 09:23:17

Cecilia_Fernandes
2016-04-21 09:24:47

We should say why it is important to sync the time setting with the built-in RTC.

Current local time

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

Time zone

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

ATTENTION

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

Daylight saving time

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

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

- **Starts at:** The date that daylight saving time begins.
- **Stops at:** The date that daylight saving time ends.

- **Time offset:** Indicates the number of hours the clock should be advanced.

Time server 1/2

Setting	Description	Factory Default
IP address of the name of the **Time Server 1/2**	IP address or domain name of the NTP time server. The second NTP server will be used if the first NTP server fails to connect.	time.nist.gov

Query period

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

Wireless Settings

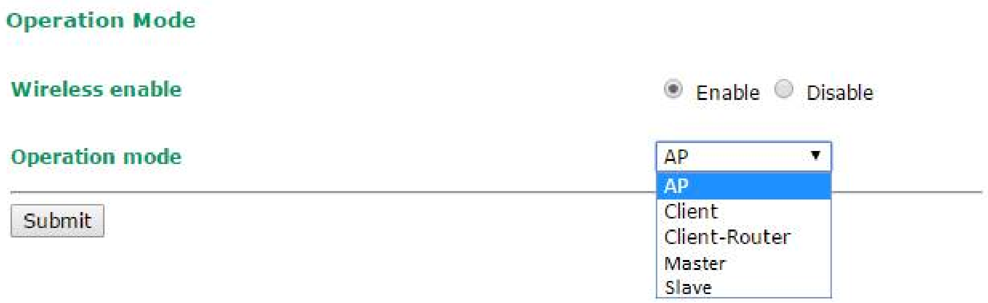
The essential settings for wireless networks are presented in the wireless settings function group. You must configure these settings correctly before you establish your wireless network. Familiarize yourself with the following terms before starting the configuration process:

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

Client: When the TAP-213 is configured for **Client** mode, it can be used as an Ethernet-to-wireless (or LAN-to-WLAN) network adapter. For example, a notebook computer equipped with an Ethernet adaptor but no wireless card can be connected to this device with an Ethernet cable to provide wireless connectivity to another AP.

Operation Mode

The TAP-213 supports five main operation modes—AP, Client, Master, Slave, and ACC—each of which plays a distinct role on the wireless network.



Operation Mode

Wireless enable ● Enable ○ Disable

Operation mode AP

Wireless Enable

Setting	Description	Factory Default
Enable/Disable	Use this function to turn the RF (Radio Frequency) module on or off manually. **NOTE**: This function is available in AP operation mode only.	Enable

Operation Mode

Setting	Description
AP	The TAP-213 plays the role of a wireless AP
Client	The TAP-213 plays the role of a wireless AP Client
Master	This mode collocates with TAP-5232/6232's Wireless b mode. The TAP-213 plays the role of a wireless maste
Slave	This mode collocates with TAP-5232/6232's Wireless b mode. The TAP-213 plays the role of a wireless slave.

Cecilia_Fernandes
2016-04-21 09:25:49

We do not describe the Client-Router
Cecilia_Fernandes

Cecilia_Fernandes
2016-04-21 09:26:41

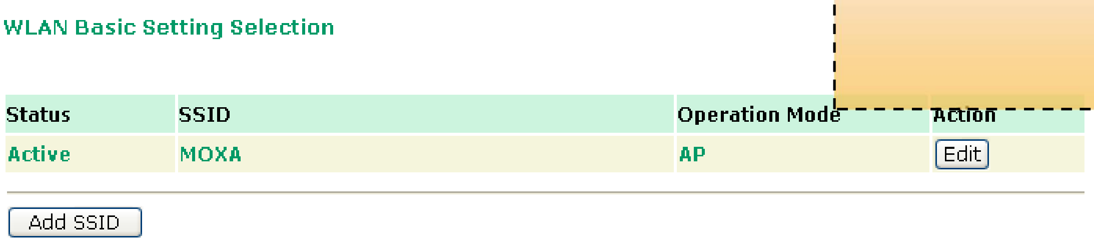
Please help clarify this content.

Basic Wireless Settings

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

Cecilia_Fernandes
2016-04-21 09:27:20

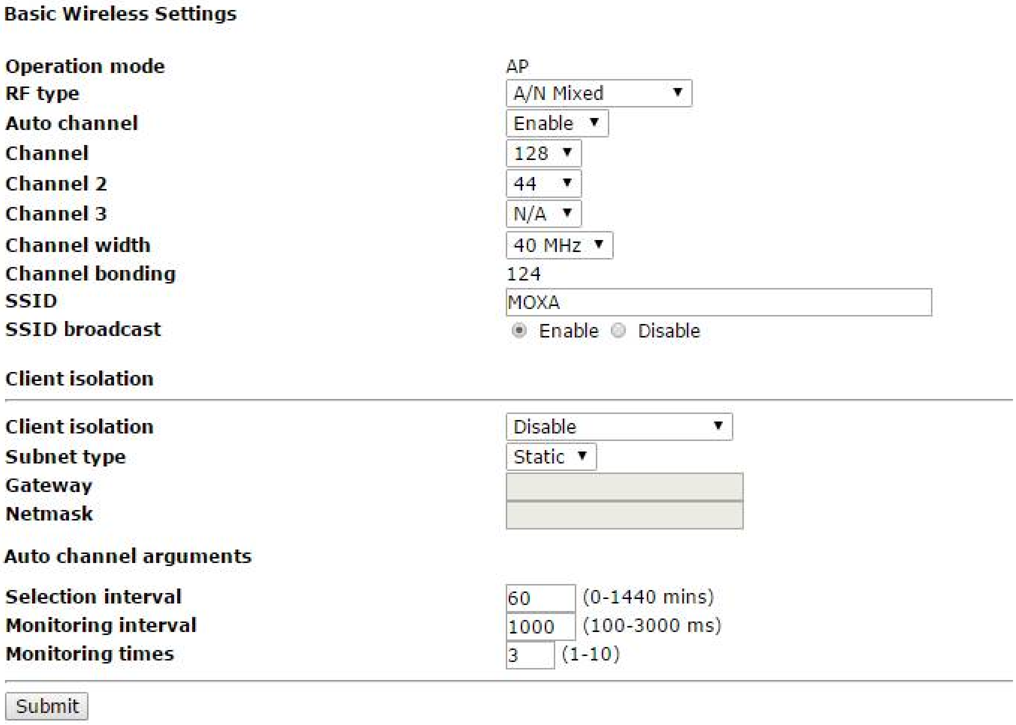
I suggest:
with different modes of operation.



WLAN Basic Setting Selection

Status	SSID	Operation Mode	Action
Active	MOXA	AP	Edit

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



Basic Wireless Settings

Operation mode	AP
RF type	A/N Mixed
Auto channel	Enable
Channel	128
Channel 2	44
Channel 3	N/A
Channel width	40 MHz
Channel bonding	124
SSID	MOXA
SSID broadcast	● Enable ○ Disable

Client isolation

Client isolation	Disable
Subnet type	Static
Gateway	
Netmask	

Auto channel arguments

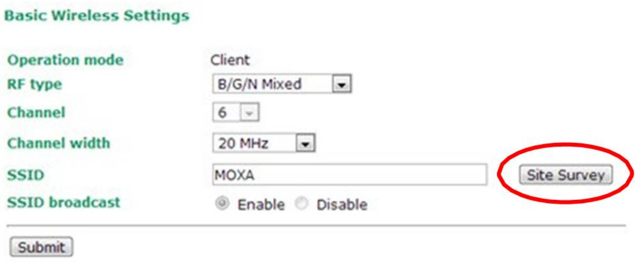
Selection interval	60 (0-1440 mins)
Monitoring interval	1000 (100-3000 ms)
Monitoring times	3 (1-10)

NOTE When you switch to **Client** mode, a **Site Survey** button will be available on the **Basic Wireless Settings** panel. Use the **Site Survey** function to view information about available APs, as s You can click on the SSID of an entity and bring the value of its SSID onto the S Settings page. Click the **Refresh** button to update the site survey table.

Cecilia_Fernandes
2016-04-21 09:27:42

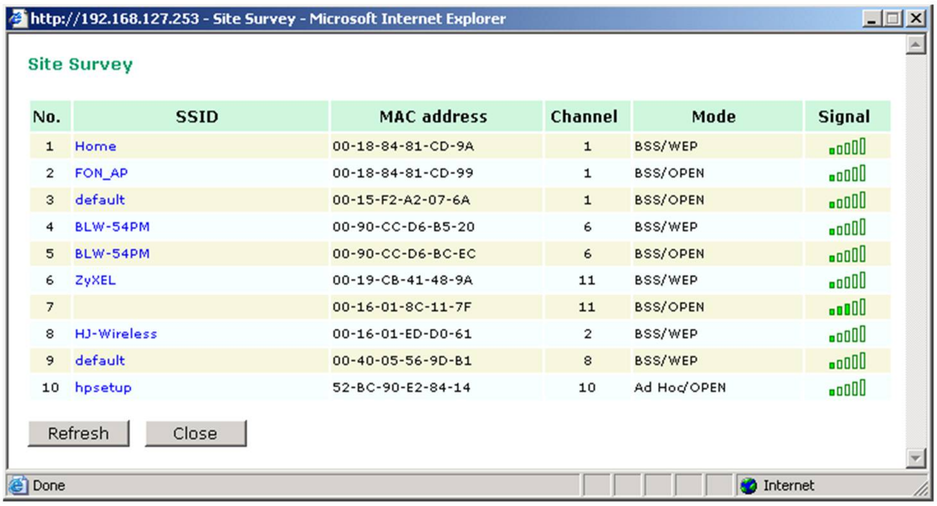
Can you please help clarify this content

If this client is connecting to an AP, a brief disconnection will occur when you click on **Site Survey**.



Basic Wireless Settings

Operation mode	Client
RF type	B/G/N Mixed
Channel	6
Channel width	20 MHz
SSID	MOXA
SSID broadcast	● Enable ○ Disable



http://192.168.127.253 - Site Survey - Microsoft Internet Explorer

Site Survey

No.	SSID	MAC address	Channel	Mode	Signal
1	Home	00-18-84-81-CD-9A	1	BSS/WEP	▮▯▯▯
2	FON_AP	00-18-84-81-CD-99	1	BSS/OPEN	▮▯▯▯
3	default	00-15-F2-A2-07-6A	1	BSS/OPEN	▮▯▯▯
4	BLW-54PM	00-90-CC-D6-B5-20	6	BSS/WEP	▮▯▯▯
5	BLW-54PM	00-90-CC-D6-BC-EC	6	BSS/OPEN	▮▯▯▯
6	ZyXEL	00-19-CB-41-48-9A	11	BSS/WEP	▮▯▯▯
7		00-16-01-8C-11-7F	11	BSS/OPEN	▮▮▯▯
8	HJ-Wireless	00-16-01-ED-D0-61	2	BSS/WEP	▮▯▯▯
9	default	00-40-05-56-9D-B1	8	BSS/WEP	▮▯▯▯
10	hpsetup	52-BC-90-E2-84-14	10	Ad Hoc/OPEN	▮▯▯▯

RF type

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

Cecilia_Fernandes
2016-04-21 09:28:16

We should specify the factory default or say "None".

Auto Channel

Setting	Description	Factory Default
Enable	Enable this function to set the TAP to scan the 3 predefined channels for the "least crowded" channel and use it as the operating channel.	Disable
Disable		

Channel (for AP/Master mode only)

Setting	Description	Factory Default
The available channels vary with the RF type setting	The channel on which the TAP should operate. The TAP-213 plays the role of a wireless AP or Master here.	6 (in B/G/N Mixed mode)

Channel 2, 3

Setting	Description	Factory Default
The available channels vary with RF type	These channels are candidate channels for auto channel selection.	N/A

Channel Width (for any 11N RF type only)

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

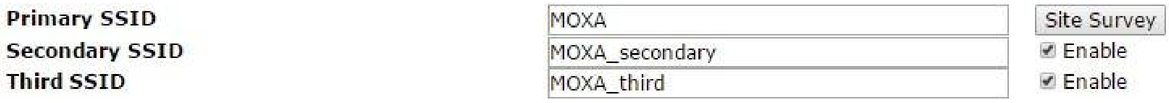
Channel bonding

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

SSID

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

Primary/Secondary/Third SSID (Client or Client-Router mode only)



Primary SSID	MOXA	Site Survey
Secondary SSID	MOXA_secondary	☑ Enable
Third SSID	MOXA_third	☑ Enable

Setting	Description	Factory Default
The name of the primary, secondary, and tertiary SSID	This is the profile setting that allows multiple SSID profiles to be stored on the TAP client so that the TAP can connect to any of the predefined SSID in order of priority (Primary > Secondary > Third)	MOXA MOXA_secondary MOXA_third

SSID broadcast (for AP/Master mode only)

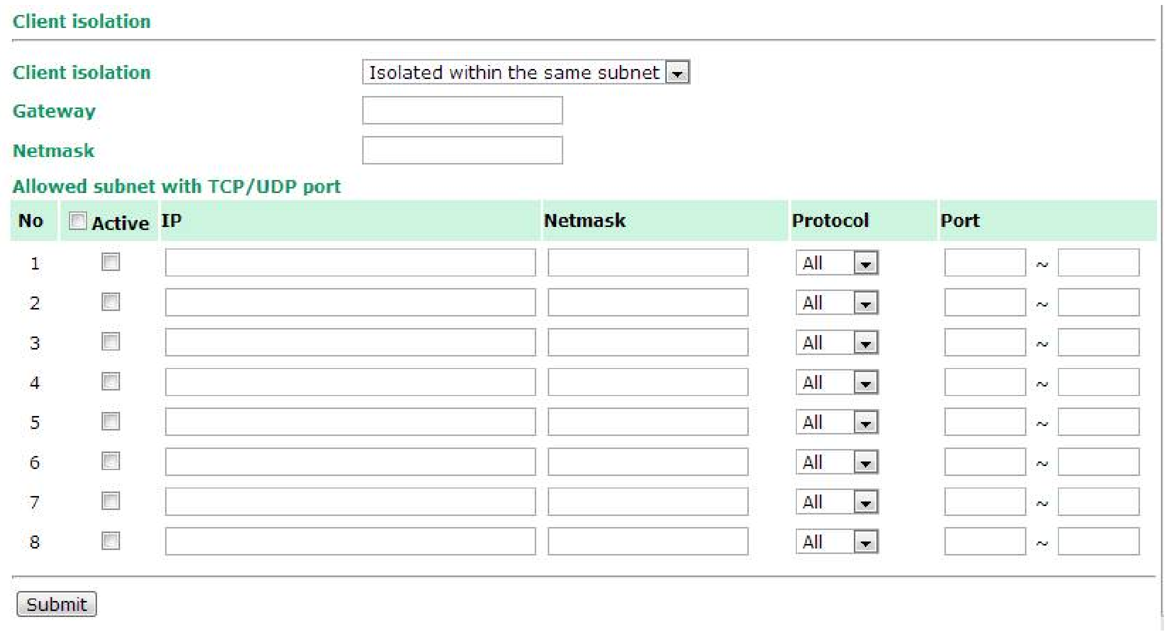
Setting	Description	Factory Default
Enable/ Disable	Use this setting to specify if the SSID can be broadcast or not	Enable

Client Isolation (for AP mode only)

Client isolation is used to isolate the associated wireless clients in one or more APs. Isolated clients cannot communicate with each other, so the level of security is increased. Depending on the type of client isolation you may also define the exception clients inside the isolation network. It can be

Cecilia_Fernandes
2016-04-21 09:28:46

Can you please help clarify this content?



Client isolation

Client isolation	Isolated within the same subnet
Gateway	
Netmask	

Allowed subnet with TCP/UDP port

No	□ Active	IP	Netmask	Protocol	Port
1	□			All	~
2	□			All	~
3	□			All	~
4	□			All	~
5	□			All	~
6	□			All	~
7	□			All	~
8	□			All	~

Client Isolation

Setting	Description	Factory Default
No isolation	No isolation is applied.	No isolation
Isolated within the same AP	All clients associated with this AP will be isolated from each other.	
Isolated within the same subnet	All clients in the specified subnet will be isolated from each other. The subnet is defined by the following two parameters: **Gateway** and **Netmask**.	

Gateway

Setting	Description	Factory Default
Gateway for client isolation function	This setting is used when you have selected the client isolation option, **Isolated within the same subnet**.	None

Netmask

Setting	Description	Factory Default
Netmask for client isolation function	This setting is used when you have selected the client isolation option, I**solated within the same subnet.**	None

Allowed subnet with TCP/UDP port

The **Allowed subnet with TCP/UDP port** setting is used to define the subnets (or hosts) that are excluded when the **Isolated within the same subnet** option is selected. You can define up to eight subnets or hosts.

Active

Setting	Description	Factory Default
Enable/Disable the subnet rule	This checkbox enables or disables a rule for **Allowed subnet with TCP/UDP port.**	Disable

IP

Setting	Description	Factory Default
The IP address of the allowed subnet	The IP address for the allowed subnet definition. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet.	None

Netmask

Setting	Description	Factory Default
The netmask for allowed subnet definition	The netmask of the subnet definition. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet. You can also define the exception host by entering 255.255.255.255 in this field.	None

Protocol

Setting	Description	Factory Default
The protocol for allowed subnet definition	The protocol of the subnet definition. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet.	All

Port

Setting	Description	Factory Default
The range of ports for the allowed subnet definition	The port range of the subnet definition. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet.	None

NOTE The TAP-213-EU (for European frequency bands) only connects SSID-hidden APs for IEEE 802.11b/g/n channels.

Auto Channel arguments

You can configure the following parameters to set the scan timing intervals for the auto channel selection process. Use the default values unless specific channel selection intervals are required.

Selection Interval

Setting	Description	Factory Default
0-1440 mins	The time between each channel re-selection. For example, if you set this field to 60 minutes, the AP scans for the least crossed channel every 60 minutes.	60

Monitoring Interval

Setting	Description	Factory Default
100-3000 ms	The channel scanning duration.	1000

Monitoring times

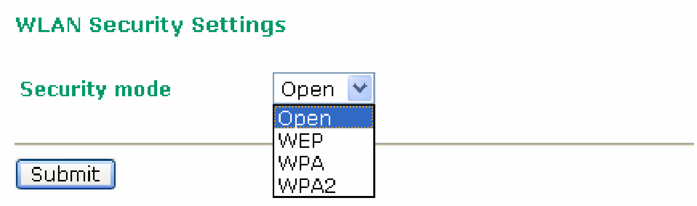
Setting	Description	Factory Default
1-10	The number of times the AP performs the channel scanning before selecting a “clear” channel to use.	3

WLAN Security Settings

The TAP-213 provides four standardized wireless security modes: **Open**, **WEP** (Wired Equivalent Privacy), **WPA** (Wi-Fi Protected Access), and **WPA2**. Several security modes are available in the TAP-213 by selecting ***Security mode*** and ***WPA type***:

- **Open:** No authentication, no data encryption.
- **WEP:** Static WEP (Wired Equivalent Privacy) keys must be configured manually.
- **WPA/WPA2-Personal:** Also known as WPA/WPA2-PSK. You will need to specify the Pre-Shared Key in the ***Passphrase*** field, which will be used by the TKIP or AES engine as a master key to generate keys that actually encrypt outgoing packets and decrypt incoming packets.
- **WPA/WPA2-Enterprise:** Also called WPA/WPA2-EAP (Extensible Authentication Protocol). In addition to device-based authentication, WPA/WPA2-Enterprise enables user-based authentication via IEEE802.1X.

The TAP-213 can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.



WLAN Security Settings

Security mode: Open

Security mode

Setting	Description	Factory Default
Open	No authentication	Open
WEP	Static WEP is used	
WPA*	WPA is used	
WPA2*	Fully supports IEEE802.11i with "TKIP/AES + 802.1X"	

Open

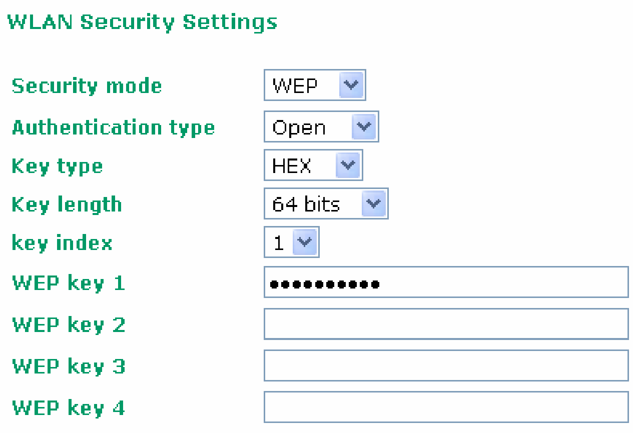
For security reasons, you should **NOT** set security mode to Open System, since authentication and data encryption are **NOT** performed in Open System mode.

WEP

According to the IEEE802.11 standard, WEP can be used for authentication and data encryption to maintain confidentiality. **Shared** (or **Shared Key**) authentication type is used if WEP authentication and data encryption are both needed. Normally, **Open** (or **Open System**) authentication type is used when WEP data encryption is run with authentication.

When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The TAP-213 provides 4 entities of WEP key settings that can be selected to use with ***Key index***. The selected key setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

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



WLAN Security Settings

Security mode	WEP
Authentication type	Open
Key type	HEX
Key length	64 bits
key index	1
WEP key 1	••••••••••
WEP key 2	
WEP key 3	
WEP key 4	

Authentication type

Setting	Description	Factory Default
Open	Data encryption is enabled, but without 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

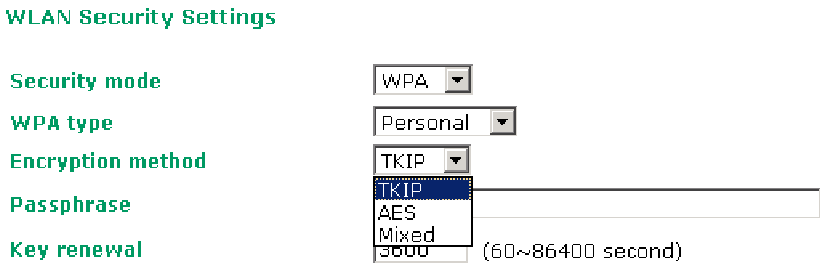
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13chars HEX type: 64 bits: 10 hex chars 128 bits: 26 hex chars	A string that can be used as a WEP seed for the RC4 encryption engine.	None

WPA/WPA2-Personal

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

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The TAP-213 also supports AES algorithms in WPA and WPA2 for better compatibility.

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



WLAN Security Settings

Security mode	WPA
WPA type	Personal
Encryption method	TKIP
Passphrase	
Key renewal	3600 (60~86400 second)

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/Master mode only, and does not support AES-enabled clients.*

Passphrase

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

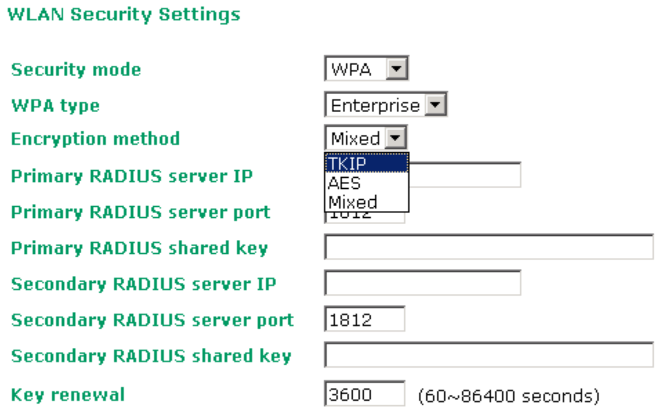
Key renewal (for AP/Master mode only)

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

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

WPA/WPA2-Enterprise (for AP/Master mode)

By setting ***WPA type*** to **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 an efficient connection authentication on a large-scale network. It is not necessary to exchange keys or passphrases.



WLAN Security Settings

Security mode	WPA
WPA type	Enterprise
Encryption method	Mixed
Primary RADIUS server IP	
Primary RADIUS server port	1812
Primary RADIUS shared key	
Secondary RADIUS server IP	
Secondary RADIUS server port	1812
Secondary RADIUS shared key	
Key renewal	3600 (60~86400 seconds)

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/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

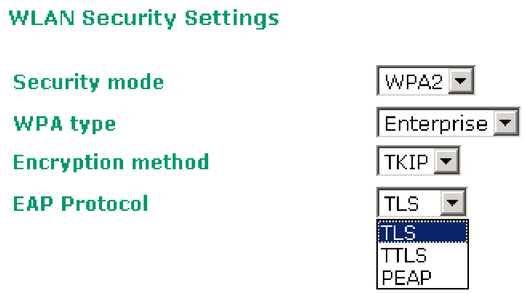
Setting	Description	Factory Default
Max. of 31 characters	The secret key shared between AP and RADIUS server	None

Key renewal

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

WPA/WPA2-Enterprise (for Client/Slave mode)

When used as a client, the TAP-213 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.



WLAN Security Settings

Security mode: WPA2

WPA type: Enterprise

Encryption method: TKIP

EAP Protocol: TLS

Encryption method

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

EAP Protocol

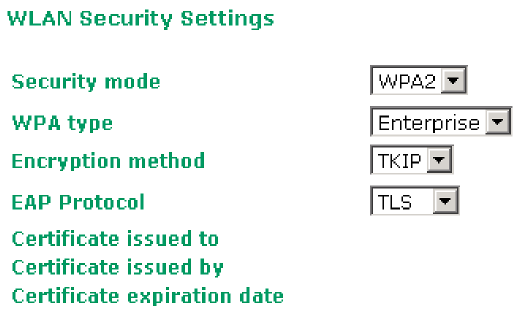
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

Before choosing the EAP protocol for your WPA/WPA2-Enterpise 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 **Basic Wireless Settings → WLAN Certificate Settings** to import your WLAN certificate and enable EAP-TLS on the client end.



WLAN Security Settings

Security mode: WPA2

WPA type: Enterprise

Encryption method: TKIP

EAP Protocol: TLS

Certificate issued to

Certificate issued by

Certificate expiration date

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 has expired

EAP-TTLS

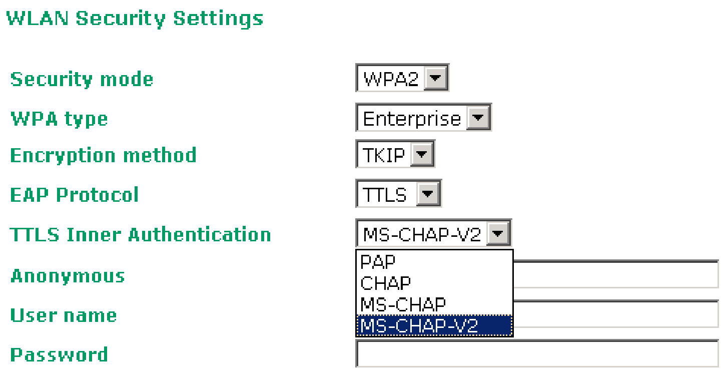
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called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

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

As you can see, digital certificates are still needed for 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-213 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 and 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, with the true user name only shown through the encrypted channel. Keep in mind that not all client software supports anonymous alteration. Confirm this with the network administrator before you enable identity hiding in TTLS and PEAP.



WLAN Security Settings

Security mode	WPA2
WPA type	Enterprise
Encryption method	TKIP
EAP Protocol	TTLS
TTLS Inner Authentication	MS-CHAP-V2
Anonymous	
User name	
Password	

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

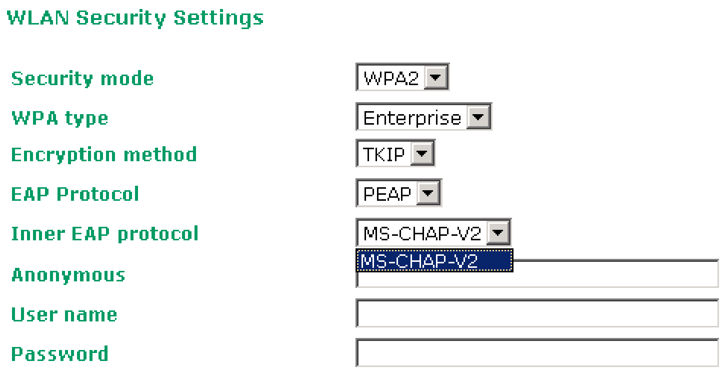
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

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

PEAP

There are a few differences in the TTLS and PEAP inner authentication procedures. 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-213 provides **MS-CHAP-V2** merely as an EAP method for inner authentication.



WLAN Security Settings

Security mode	WPA2
WPA type	Enterprise
Encryption method	TKIP
EAP Protocol	PEAP
Inner EAP protocol	MS-CHAP-V2
Anonymous	
User name	
Password	

Inner EAP protocol

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

Anonymous

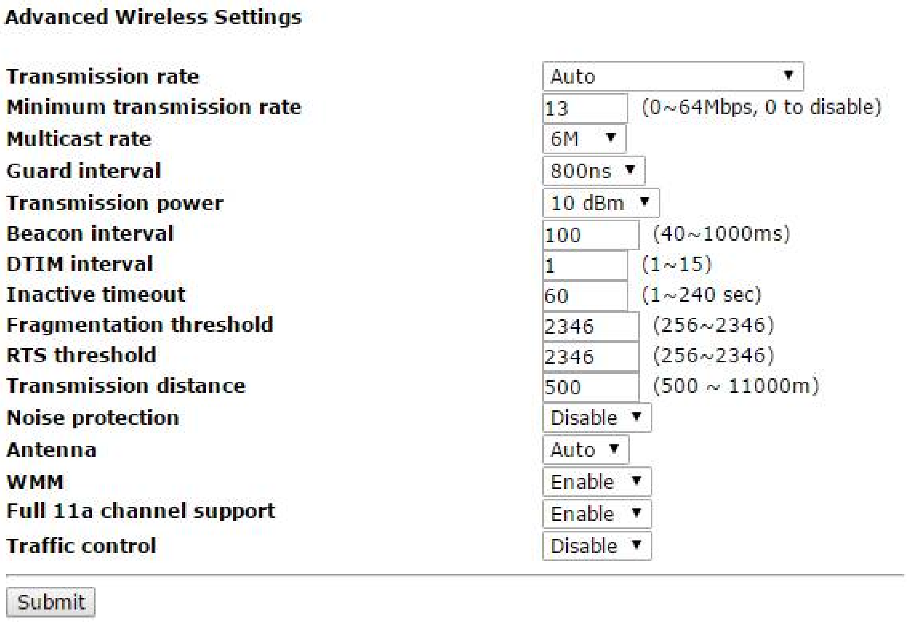
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

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.



Advanced Wireless Settings

Transmission rate	Auto
Minimum transmission rate	13 (0~64Mbps, 0 to disable)
Multicast rate	6M
Guard interval	800ns
Transmission power	10 dBm
Beacon interval	100 (40~1000ms)
DTIM interval	1 (1~15)
Inactive timeout	60 (1~240 sec)
Fragmentation threshold	2346 (256~2346)
RTS threshold	2346 (256~2346)
Transmission distance	500 (500 ~ 11000m)
Noise protection	Disable
Antenna	Auto
WMM	Enable
Full 11a channel support	Enable
Traffic control	Disable

Transmission Rate

Setting	Description	Factory Default

Auto	The TAP-213 senses and adjusts the data rate automatically	Auto
Available rates	Users can manually select a target transmission data rate	

Multicast Rate (for AP/Master mode only)

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

Guarding Interval

Setting	Description	Factory Default
Guarding Interval	Guarding interval is used to ensure that distinct transmissions do not interfere with one another. You can select the guarding interval manually for Wireless-N connections. The two options are Short (400ns) and Long (800ns).	800ns.

Transmission Power for 2.4 GHz

Setting	Description	Factory Default
Transmission Power	Specifies transmission power for the radio in the unit of dBm.	10dBm

Transmission Power for 5 GHz

Setting	Description	Factory Default
Auto	Specifies transmission power for the radio in the unit of dBm.	10dBm

Beacon Interval (for AP/Master mode only)

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

DTIM Interval (for AP/Master mode only)

Setting	Description	Factory Default
Data Beacon Rate (1 to 15)	Indicates how often the TAP-213 sends out a Delivery Traffic Indication Message	1

Fragmentation threshold

Setting	Description	Factory Default
Fragment Length (256 to 2346)	Specifies the maximum size a data packet before splitting and creating another new packet	2346

RTS threshold

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

NOTE Transmission power indicates the maximum value of transmission power which the user plans. However, the real transmitted power depends on the radio module and some facts, such as country, regulatory limitations and data rate. Please check the Transmission power in Status > Wireless Status for a real and updated value of transmission power, which the TAP is currently using.

You can refer to the related glossaries in the reference section for detailed information about the above-mentioned settings. By setting these parameters properly, you can better tune the performance of your wireless network.

Noise protection

Setting	Description	Factory Default
Enable/Disable	Adjusts the interference coping capability of the wireless signal. This option should be enabled for communication distance under 500 meters, and should be disabled for communication distances over 500 meters.	Enable

WMM

Setting	Description	Factory Default
Enable/Disable	WMM is a QoS standard for WLAN traffic. Voice and video data will be given priority bandwidth when enabled with WMM supported wireless clients.	Disable

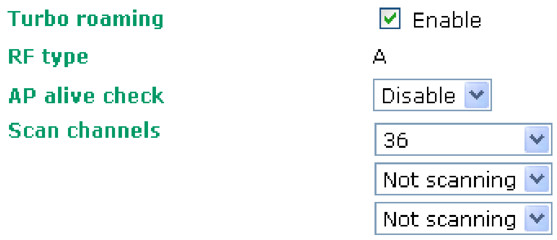
Full 11a channel support

Setting	Description	Factory Default
Enable/Disable	“Full 11a channel support” allows users to select one channel from 802.11a, including channels in licensed and unlicensed bands.	Disable

Turbo Roaming (for Client mode only)

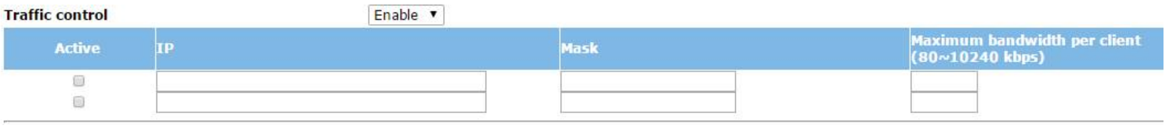
Setting	Description	Factory Default
Enable/ Disable	Moxa’s Turbo Roaming can enable rapid handover when the TAP-213, as a client, roams among a group of APs.	Disable

When Turbo Roaming is enabled, the **RF type**, **AP alive check**, and **Scan channels** parameters will be shown as follows. The **RF type** shows the current RF type that this client is using. The **AP alive check** parameter will check if the AP connection is still available. When this function is enabled, a check will be done every 10 ms. You can set up **Scan channels** for the APs among which this client is going to roam. There are three Scan channels available. Note that the **Scan channels** may need to be modified when the **RF type** is changed. (For example, channel 36 is not available in **B**, **G**, **N** or **B/G/N Mix** mode.)



Turbo roaming	☑ Enable
RF type	A
AP alive check	Disable
Scan channels	36 Not scanning Not scanning

Traffic Control



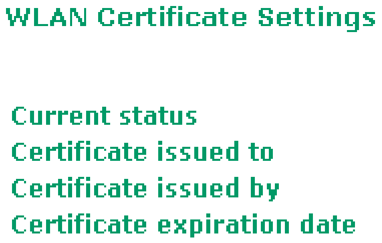
Traffic control Enable

Active	IP	Mask	Maximum bandwidth per client (80~10240 kbps)
□			
□			

Setting	Description	Factory Default
Enable/Disable	Enable this function to limit the bandwidth for a client device with the specified IP address settings. Enter maximum bandwidth (80 to 10240 kbps) to limit the wireless bandwidth allocated to clients to prevent a client from hoarding the wireless bandwidth.	Disable

WLAN Certification Settings (for EAP-TLS in Client/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-213 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.



WLAN Certificate Settings

Current status
Certificate issued to
Certificate issued by
Certificate expiration date

Current Status displays information for the current WLAN certificate, which has been imported into the TAP-213. Nothing will be shown if a certificate is not available.

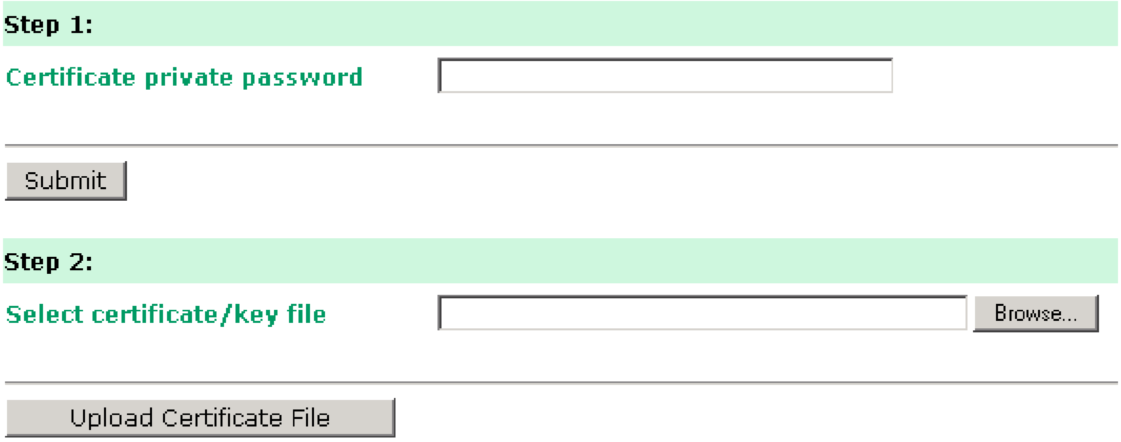
Certificate issued to: Shows the certificate user

Certificate issued by: Shows the certificate issuer

Certificate expiration date: Indicates when the certificate has expired

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

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



Step 1:

Certificate private password

Step 2:

Select certificate/key file

NOTE The WLAN certificate will remain after the TAP-213 reboots. Even though it is expired, it can still be seen on the ***Current Certificate***.

Advanced Settings

Several advanced functions are available to increase the functionality of your TAP-213 and wireless network system. A VLAN is a collection of clients and hosts grouped together as if they were connected to the broadcast domains in a layer 2 network. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the TAP-213 can support STP/RSTP protocol to increase reliability across the entire network, and SNMP support can make network management easier.

Using Virtual LAN

Setting up Virtual LANs (VLANs) on your TAP 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, commonly known as a VLAN, is a group of hosts with a common set of requirements that 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 for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via 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 network restricts members to resources on their own VLAN
- Clients roam without compromising security

VLAN Workgroups and Traffic Management

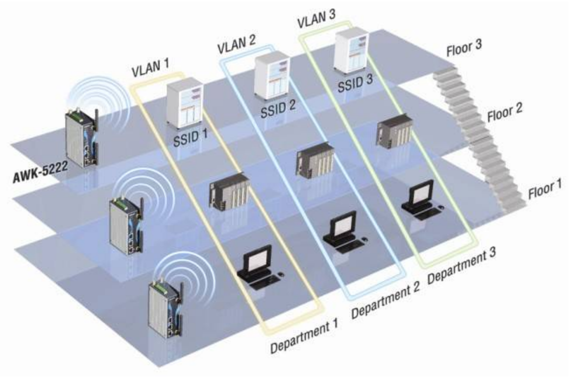
The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

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. This eliminates 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 resource 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 resource, 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.

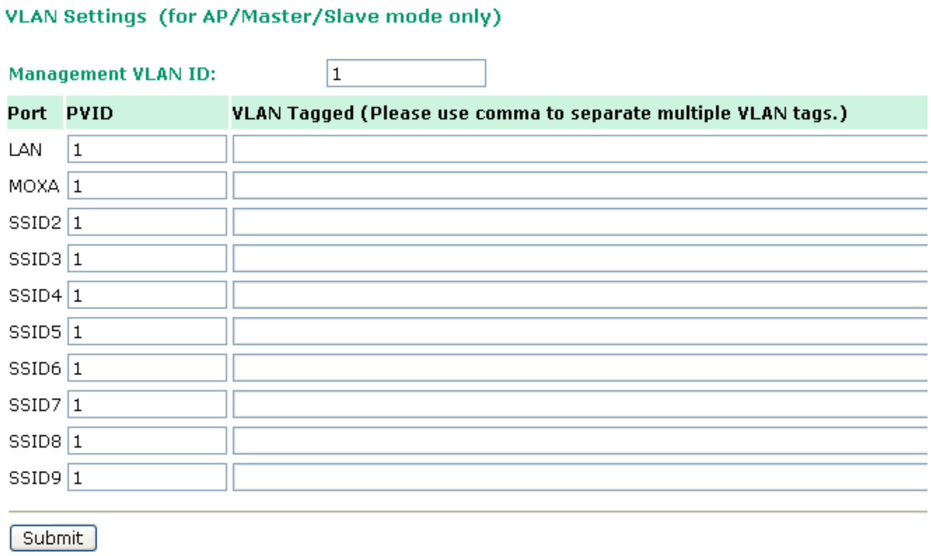
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resource department could be restricted to a gateway that allowed access to only the Internet. A member of the human resource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



Configuring Virtual LAN

VLAN Settings

To configure the TAP's VLAN, use the VLAN Setting page to configure the ports.



VLAN Settings (for AP/Master/Slave mode only)

Management VLAN ID: 1

Port	PVID	VLAN Tagged (Please use comma to separate multiple VLAN tags.)
LAN	1	
MOXA	1	
SSID2	1	
SSID3	1	
SSID4	1	
SSID5	1	
SSID6	1	
SSID7	1	
SSID8	1	
SSID9	1	

Management VLAN ID

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

Port

Type	Description	Trunk Port
LAN	This port is the LAN port on the TAP.	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 of the VLAN IDs range from 1 to 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.

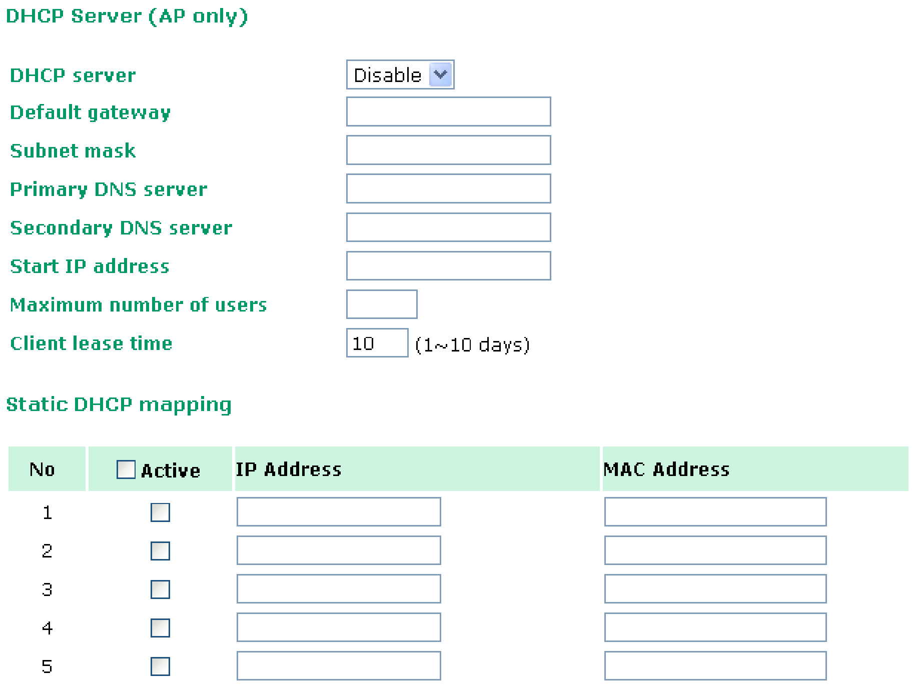
DHCP Server (for AP mode only)

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-213 can act as a simplified DHCP server and easily assign IP addresses to your DHCP 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-213 provides a **Static DHCP mapping** list with up to 16 entities. Be reminded 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)

DHCP server	Disable
Default gateway	
Subnet mask	
Primary DNS server	
Secondary DNS server	
Start IP address	
Maximum number of users	
Client lease time	10 (1~10 days)

Static DHCP mapping

No	□ Active	IP Address	MAC Address
1	□		
2	□		
3	□		
4	□		
5	□		

DHCP server

Setting	Description	Factory Default
Enable	Enables TAP-213 as a DHCP server	Disable
Disable	Disable 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 URL as well. 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 IP address which TAP-213 can start assigning	None

Maximum number of users

Setting	Description	Factory Default
1 – 999	Specifies how many IP address can be assigned continuously	None

Client lease time

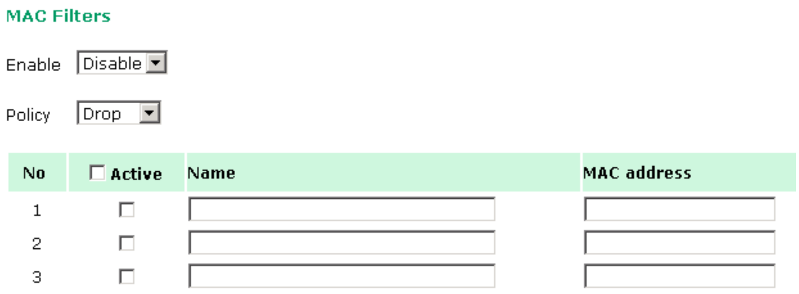
Setting	Description	Factory Default
1 – 10 days	The lease time for which an IP address is assigned. The IP address may go expired after the lease time is reached.	10 (days)

Packet Filters

The TAP-213 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-213's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The TAP-213 provides 8 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.



MAC Filters

Enable: Disable

Policy: Drop

No	□ Active	Name	MAC address
1	□		
2	□		
3	□		

Enable

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

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

Be careful when you enable the filter function:

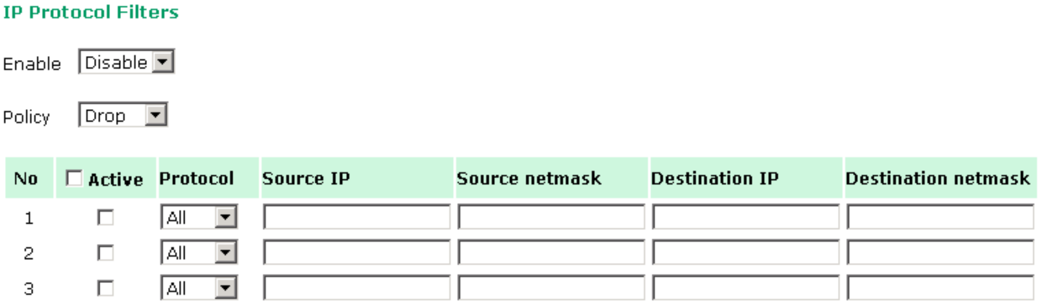
Drop + "no entity on list is activated" = all packets are **allowed**

Accept + "no entity on list is activated" = all packets are **denied**

IP Protocol Filter

The TAP-213'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-213 provides 8 entities 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.



IP Protocol Filters

Enable: Disable

Policy: Drop

No	□ Active	Protocol	Source IP	Source netmask	Destination IP	Destination netmask
1	□	All				
2	□	All				
3	□	All				

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 fitting the entities on the list can be allowed	Drop
Drop	Any packet fitting the entities on the list will be denied	

ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed.**

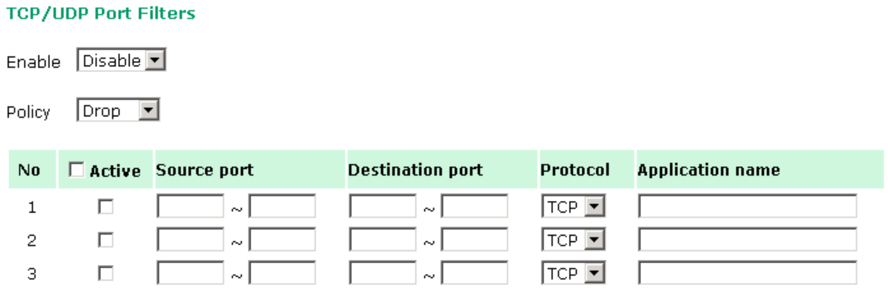
Accept + "no entity on list is activated" = all packets are **denied.**

TCP/UDP Port Filter

The TAP-213'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-213 provides 8 entities 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.



TCP/UDP Port Filters

Enable Disable

Policy Drop

No	□ Active	Source port	Destination port	Protocol	Application name
1	□	~	~	TCP	
2	□	~	~	TCP	
3	□	~	~	TCP	

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 the packets fitting the entities on list can be allowed.	Drop
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed**

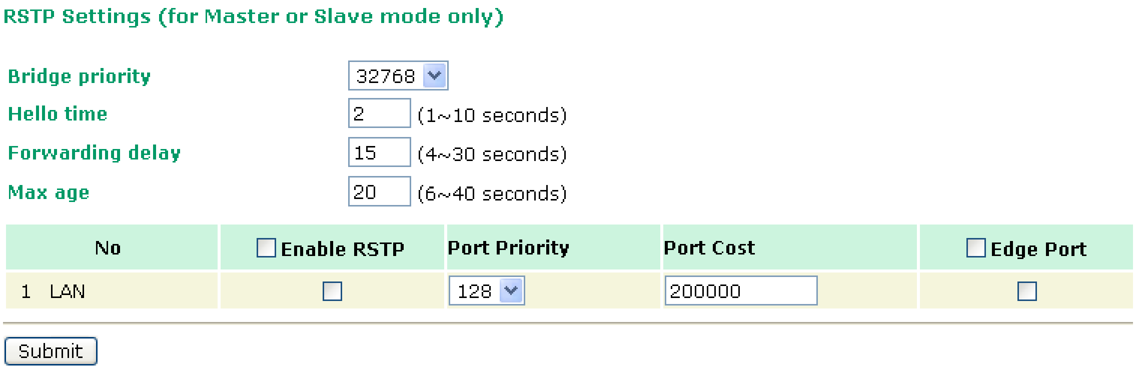
Accept + "no entity on list is activated" = all packets are **denied**

RSTP Settings (for AP/Master mode only)

TAP-213 supports IEEE802.1D Spanning Tree Protocol and IEEE802.1w Rapid STP standards. In addition to eliminating unexpected path looping, STP/RSTP can provide a backup path recovery if a wired/ wireless path fails accidentally. The reliability and availability can increase because this fail-over function.

TAP-213's STP/RSTP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every TAP-213 connected to your network. If TAP-213 plays a **Client** role, which is connected to a device (PLC, RTU, etc.) as opposed to network switch equipment, it is not necessary to enable STP/RSTP. The reason is that it will cause unnecessary negotiation. TAP-213s support STP/RSTP in **AP** mode only.

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



RSTP Settings (for Master or Slave mode only)

Bridge priority	32768
Hello time	2 (1~10 seconds)
Forwarding delay	15 (4~30 seconds)
Max age	20 (6~40 seconds)

No	□ Enable RSTP	Port Priority	Port Cost	□ Edge Port
1 LAN	□	128	200000	□

RSTP status

This field will appear only when selected to operate STP/RSTP. It indicates whether this TAP-213 is the Root of the Spanning Tree (the root is determined automatically) or not.

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	You can increase the bridge priority by selecting a lower number. A higher bridge priority brings a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time

Setting	Description	Factory Default
Numerical value input by user (1 – 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
Numerical value input by user (4 – 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
Numerical value input by user (6 – 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
Numerical value selected by user	Increase this port’s priority as a node on the Spanning Tree topology by inputting a lower number.	128

Port cost

Setting	Description	Factory Default
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 expectedly goes through, as an edge port	unchecked, except AP port

NOTE We recommend you set an edge port for the port, which is connected to a non-STP/RSTP sub-network or an end device (PLC, RTU, etc.) as opposed to network equipment. This can prevent unnecessary waiting and negotiation of 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.

SNMP Agent

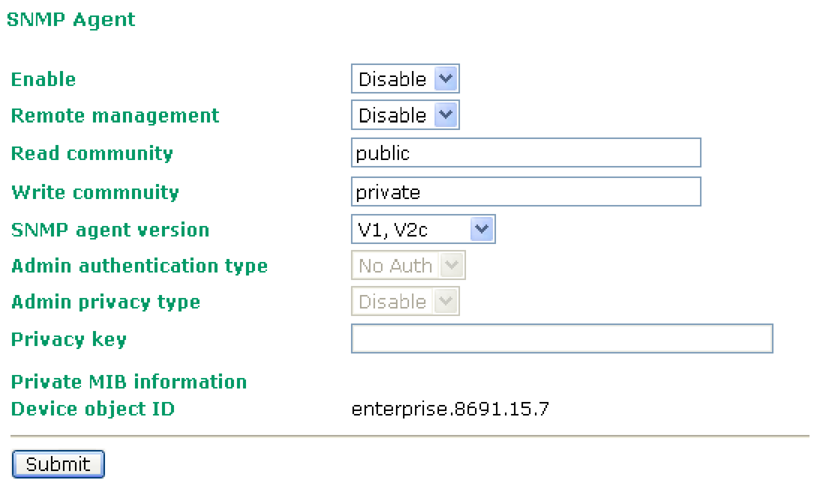
The TAP-213 supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

The TAP-213'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-213 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	No	No	Use account with admin or user 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.



SNMP Agent

Enable	Disable
Remote management	Disable
Read community	public
Write commnuity	private
SNMP agent version	V1, V2c
Admin authentication type	No Auth
Admin privacy type	Disable
Privacy key	
Private MIB information Device object ID	enterprise.8691.15.7

Enable

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

Remote Management

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

Read community (for V1, V2c)

Setting	Description	Factory Default
V1, V2c 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)

Setting	Description	Factory Default
V1, V2c Read /Write Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can accesses 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

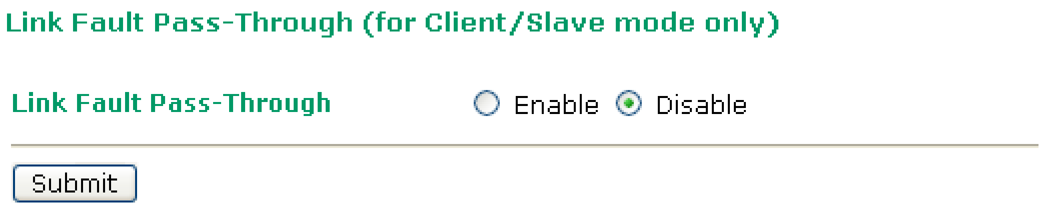
Also known as ***OID***. This is the TAP-213's enterprise value. It is fixed.

Link Fault Pass-Through (for Client/Slave mode only)

This function means if Ethernet port is link down, wireless connection will be forced to disconnect. Once Ethernet link is recovered, TAP will try to connect to AP.

If wireless is disconnected, TAP restarts auto-negotiation on Ethernet port but always stays in the link failure state. Once the wireless connection is recovered, TAP will try to recover the Ethernet link.

System log will indicate the link fault pass through events in addition to the original link up/down events.



Link Fault Pass-Through (for Client/Slave mode only)

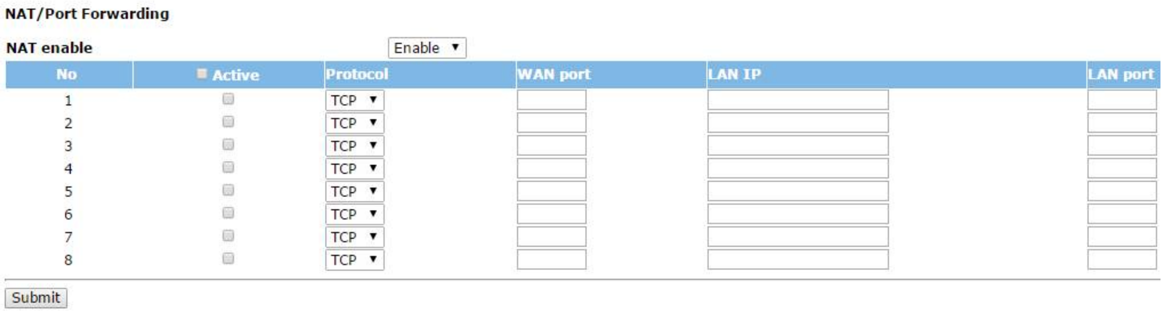
Link Fault Pass-Through ○ Enable ● Disable

Link Fault Pass-Through

Setting	Description	Factory Default
Enable	Enables Link Fault Pass-Through	Disable
Disable	Disables Link Fault Pass-Through	

NAT/Port Forwarding

Set the NAT/Port Forwarding settings to allow the TAP to route specified outgoing and incoming traffic to other subnets. You can select the port forwarding protocol and enter the WAN port whose traffic the TAP forwards to a device with the defined LAN port and IP address.



NAT/Port Forwarding

NAT enable: Enable ▾

No	☐ Active	Protocol	WAN port	LAN IP	LAN port
1	☐	TCP ▾			
2	☐	TCP ▾			
3	☐	TCP ▾			
4	☐	TCP ▾			
5	☐	TCP ▾			
6	☐	TCP ▾			
7	☐	TCP ▾			
8	☐	TCP ▾			

Auto Warning Settings

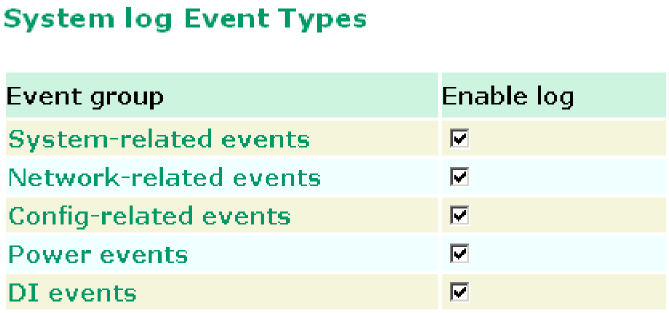
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system 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-213 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

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



System log Event Types

Event group	Enable log
System-related events	☑
Network-related events	☑
Config-related events	☑
Power events	☑
DI events	☑

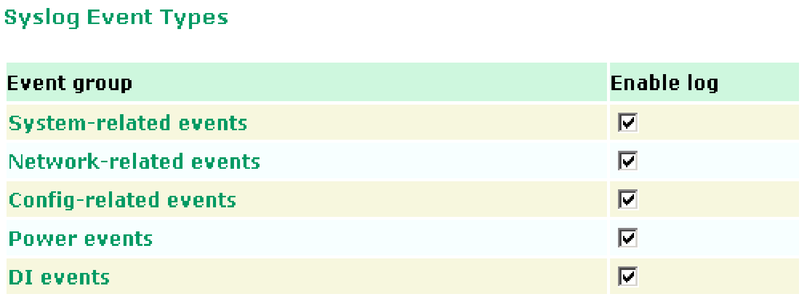
System-related events	**Event is triggered when…**
System restart (warm start)	The TAP-213 is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
Network-related events	**Event is triggered when…**
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Client joined/ left (for AP/Master mode)	A wireless client is associated or disassociated.
WLAN connected to AP (for Client/Slave mode)	The TAP-213 is associated with an AP.
WLAN disconnected (for Client/Slave mode)	The TAP-213 is disassociated from an AP.
Config-related events	**Event is triggered when…**
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the TAP-213.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The TAP-213's firmware is updated.
Power events	**Event is triggered when…**
Power 1/2 transition (On -> Off)	The TAP-213 is powered down in PWR1/2.
PoE transition (On -> Off)	The TAP-213 is powered down in PoE.
Power 1/2 transition (Off -> On)	The TAP-213 is powered via PWR1/2.
PoE transition (Off -> On)	The TAP-213 is powered via PoE.
DI events	**Event is triggered when…**
DI1/2 transition (On -> Off)	Digital Input 1/2 is triggered by on to off transition
DI1/2 transition (Off -> On)	Digital Input 1/2 is triggered by off to on transition

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

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

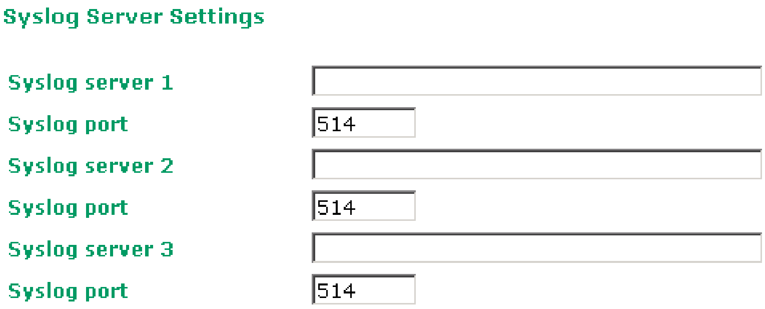


Syslog Event Types

Event group	Enable log
System-related events	☑
Network-related events	☑
Config-related events	☑
Power events	☑
DI events	☑

Syslog Server Settings

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



Syslog Server Settings

Syslog server 1	
Syslog port	514
Syslog server 2	
Syslog port	514
Syslog server 3	
Syslog port	514

Syslog server 1/ 2/ 3

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

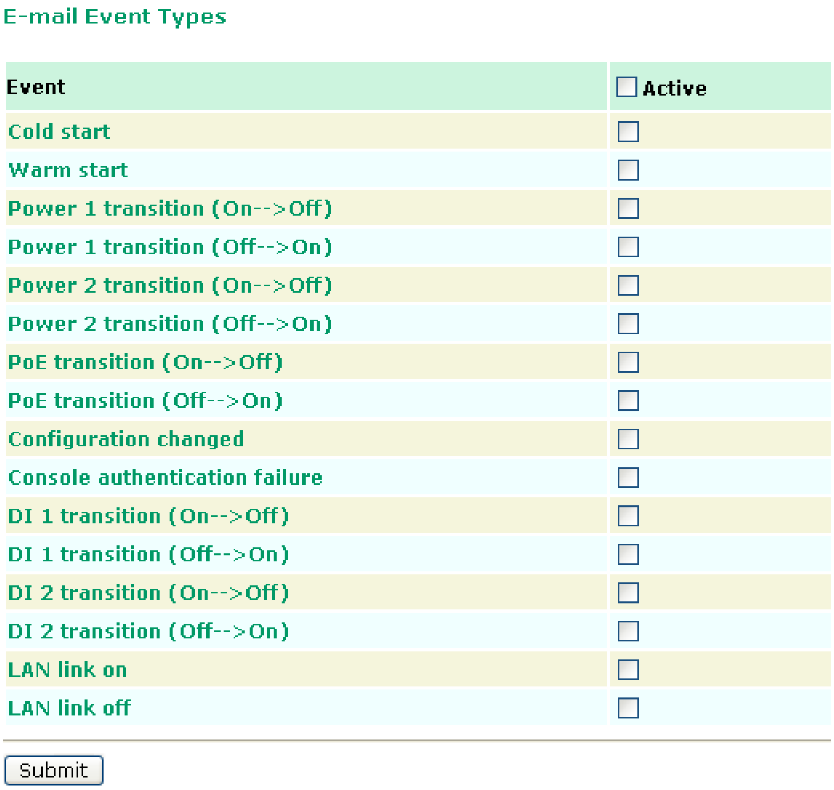
Syslog port

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 box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found on the "System log Event Types" table on page 3-31.

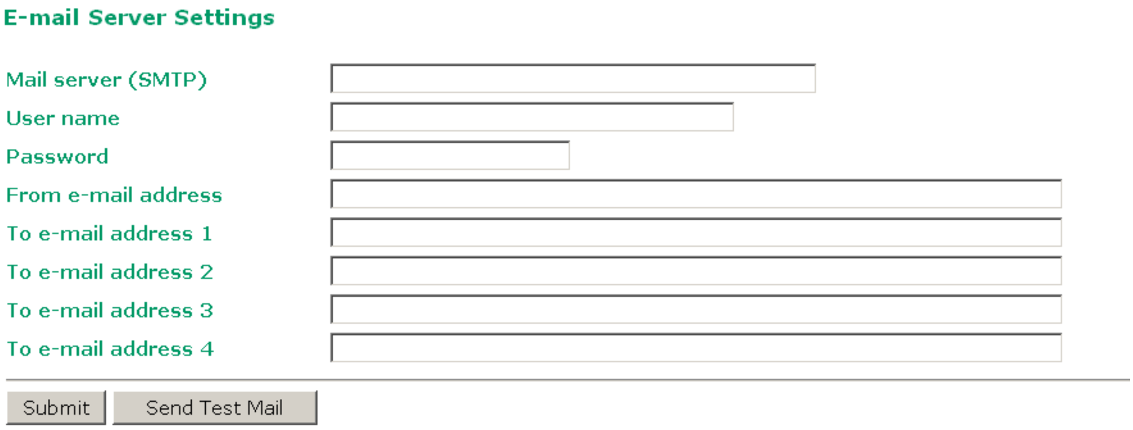


E-mail Event Types

Event	□ Active
Cold start	□
Warm start	□
Power 1 transition (On-->Off)	□
Power 1 transition (Off-->On)	□
Power 2 transition (On-->Off)	□
Power 2 transition (Off-->On)	□
PoE transition (On-->Off)	□
PoE transition (Off-->On)	□
Configuration changed	□
Console authentication failure	□
DI 1 transition (On-->Off)	□
DI 1 transition (Off-->On)	□
DI 2 transition (On-->Off)	□
DI 2 transition (Off-->On)	□
LAN link on	□
LAN link off	□

E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the TAP-213. 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 e-mail addresses work well. More detailed explanations about these parameters are given after the following figure.



E-mail Server Settings

Mail server (SMTP)	
User name	
Password	
From e-mail address	
To e-mail address 1	
To e-mail address 2	
To e-mail address 3	
To e-mail address 4	

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 e-mail address which will be shown in the "From" field of a warning e-mail.	None

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

Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' e-mail addresses.	None

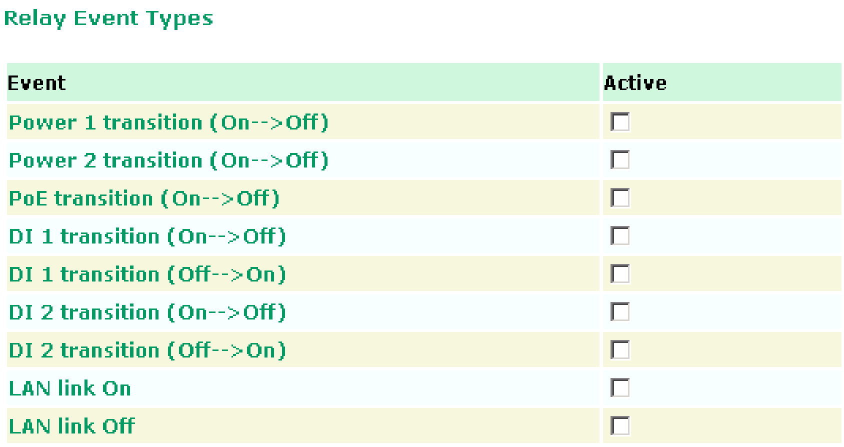
Relay

The TAP-213 has one relay output, which consists of 2 terminal block contacts on the TAP-213's top panel. These relay contacts are used to indicate user-configured events and system failure.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the TAP-213 is not powered.

Relay Event Types

You can check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found in the "System log Event Types" table on page 3-31.



Relay Event Types

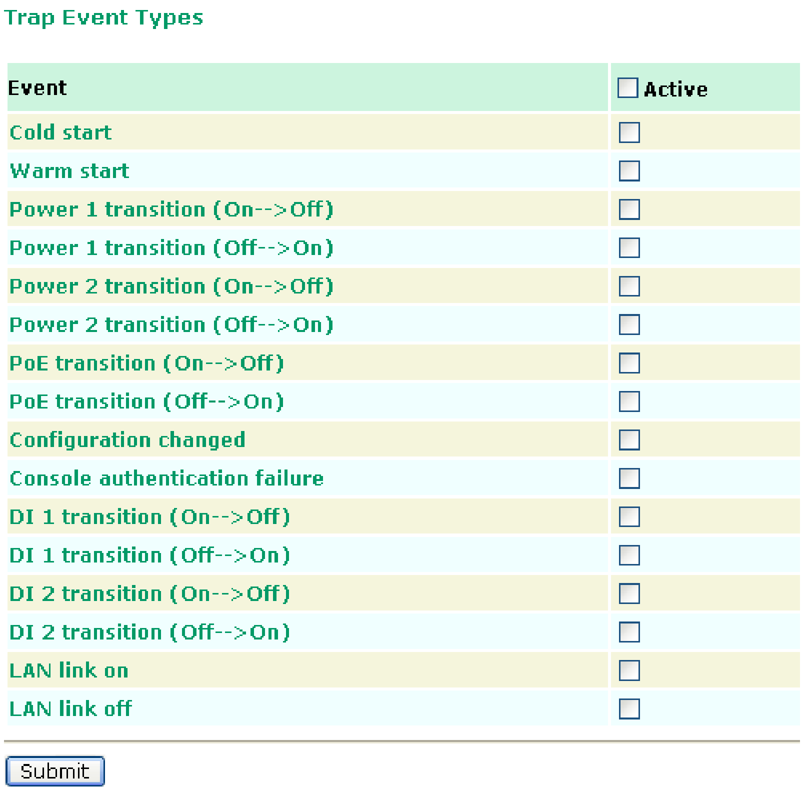
Event	Active
Power 1 transition (On-->Off)	□
Power 2 transition (On-->Off)	□
PoE transition (On-->Off)	□
DI 1 transition (On-->Off)	□
DI 1 transition (Off-->On)	□
DI 2 transition (On-->Off)	□
DI 2 transition (Off-->On)	□
LAN link On	□
LAN link Off	□

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 overloading for the management station to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management station by sending a message known as a trap for the event.

Trap Event Types

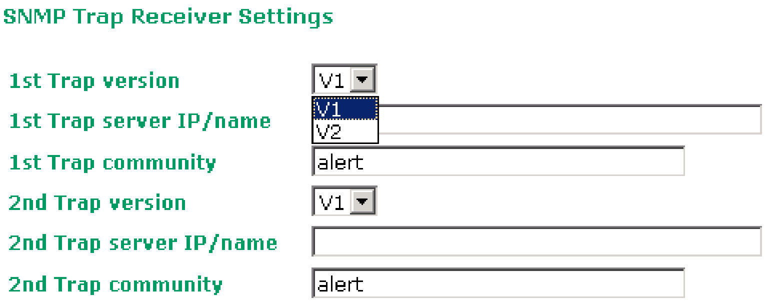


Trap Event Types

Event	□ Active
Cold start	□
Warm start	□
Power 1 transition (On-->Off)	□
Power 1 transition (Off-->On)	□
Power 2 transition (On-->Off)	□
Power 2 transition (Off-->On)	□
PoE transition (On-->Off)	□
PoE transition (Off-->On)	□
Configuration changed	□
Console authentication failure	□
DI 1 transition (On-->Off)	□
DI 1 transition (Off-->On)	□
DI 2 transition (On-->Off)	□
DI 2 transition (Off-->On)	□
LAN link on	□
LAN link off	□

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.



SNMP Trap Receiver Settings

1st Trap version	V1
1st Trap server IP/name	
1st Trap community	alert
2nd Trap version	V1
2nd Trap server IP/name	
2nd Trap community	alert

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. of 31 characters	Use a community string match with a maximum of 31 characters for authentication.	alert

Status

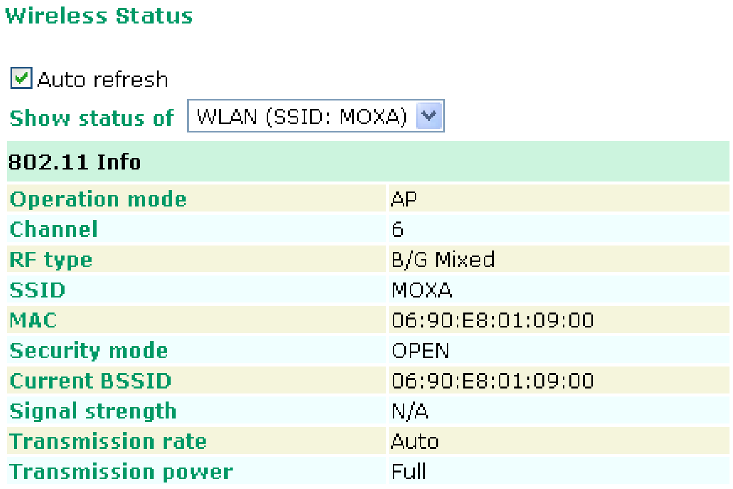
Wireless Status

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 values for **802.11 info** may not show up due to different operation modes. As a result, **Current BSSID** and **Signal strength** are not available in AP mode.

It is helpful to use the continuously updated information on this page, such as **Signal strength**, to monitor the signal strength of the TAP-213 in Client, Slave, or ACC mode.

The transmission power indicated is the current transmission power being updated periodically.



Wireless Status

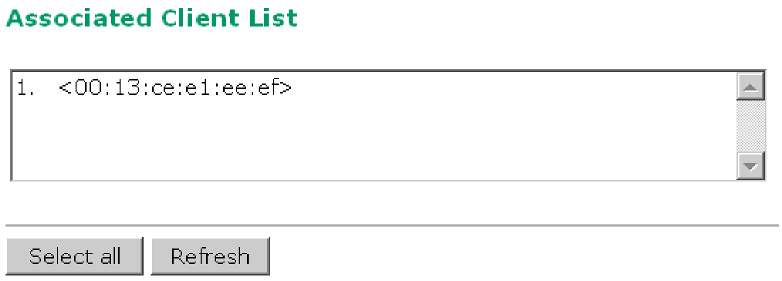
☑ Auto refresh

Show status of WLAN (SSID: MOXA)

802.11 Info	
Operation mode	AP
Channel	6
RF type	B/G Mixed
SSID	MOXA
MAC	06:90:E8:01:09:00
Security mode	OPEN
Current BSSID	06:90:E8:01:09:00
Signal strength	N/A
Transmission rate	Auto
Transmission power	Full

Associated Client List (for AP/Master mode only)

Associated Client List shows all the clients that are currently associated to a particular TAP-213. You can click **Select all** to select all the content in the list for further editing. You can click **Refresh** to refresh the list.

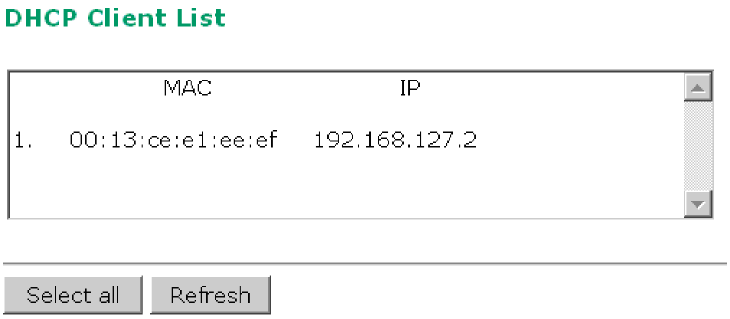


Associated Client List

1. <00:13:ce:e1:ee:ef>

DHCP Client List (for AP mode only)

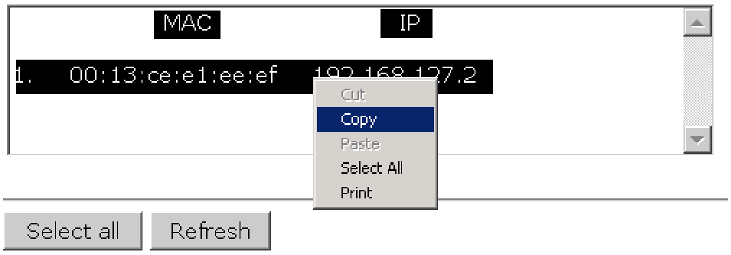
The DHCP Client List shows all the clients that require and have successfully received IP assignments. You can click the **Refresh** button to refresh the list.



DHCP Client List

```
                 MAC                    IP

1.    00:13:ce:e1:ee:ef    192.168.127.2
```

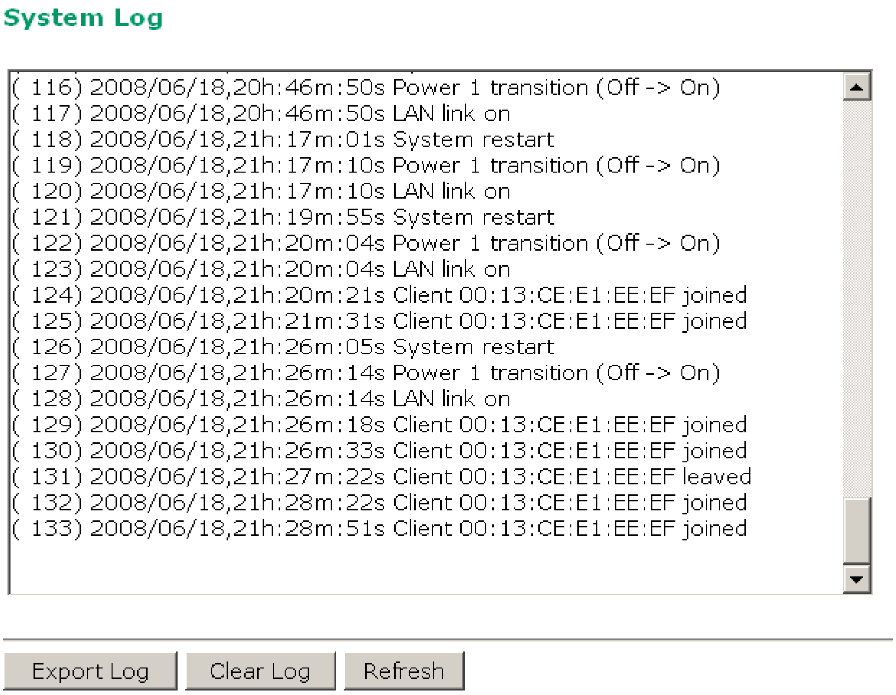
You can press **Select all** button to select all content in the list for further editing.



```
                 MAC                    IP

1.    00:13:ce:e1:ee:ef    192.168.127.2
```

System Log

Triggered events are recorded in 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.



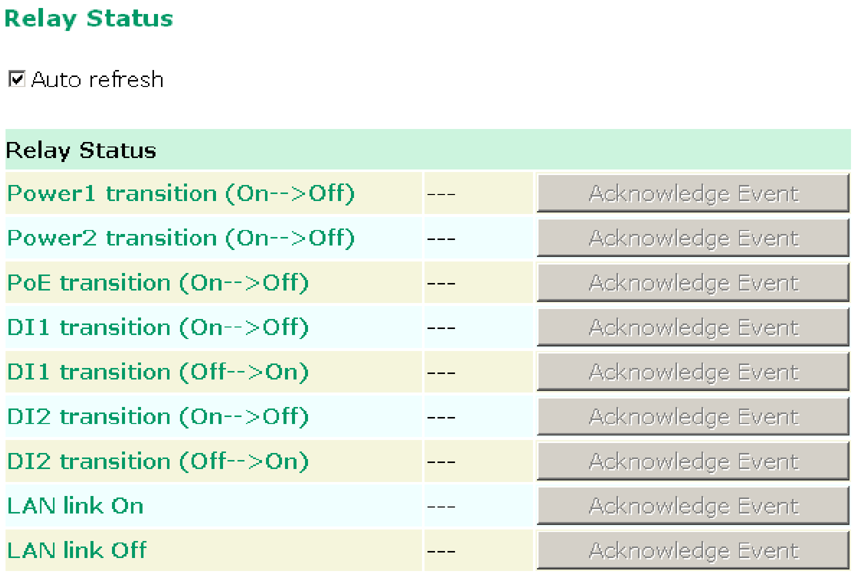
System Log

```
( 116) 2008/06/18,20h:46m:50s Power 1 transition (Off -> On)
( 117) 2008/06/18,20h:46m:50s LAN link on
( 118) 2008/06/18,21h:17m:01s System restart
( 119) 2008/06/18,21h:17m:10s Power 1 transition (Off -> On)
( 120) 2008/06/18,21h:17m:10s LAN link on
( 121) 2008/06/18,21h:19m:55s System restart
( 122) 2008/06/18,21h:20m:04s Power 1 transition (Off -> On)
( 123) 2008/06/18,21h:20m:04s LAN link on
( 124) 2008/06/18,21h:20m:21s Client 00:13:CE:E1:EE:EF joined
( 125) 2008/06/18,21h:21m:31s Client 00:13:CE:E1:EE:EF joined
( 126) 2008/06/18,21h:26m:05s System restart
( 127) 2008/06/18,21h:26m:14s Power 1 transition (Off -> On)
( 128) 2008/06/18,21h:26m:14s LAN link on
( 129) 2008/06/18,21h:26m:18s Client 00:13:CE:E1:EE:EF joined
( 130) 2008/06/18,21h:26m:33s Client 00:13:CE:E1:EE:EF joined
( 131) 2008/06/18,21h:27m:22s Client 00:13:CE:E1:EE:EF leaved
( 132) 2008/06/18,21h:28m:22s Client 00:13:CE:E1:EE:EF joined
( 133) 2008/06/18,21h:28m:51s Client 00:13:CE:E1:EE:EF joined
```

Relay Status

The status of user-configurable events can be found under **Relay Status**. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

If an event is triggered, it will be noted on this list. System administrators can click **Acknowledge Event** when he has acknowledged the event and addressed it.



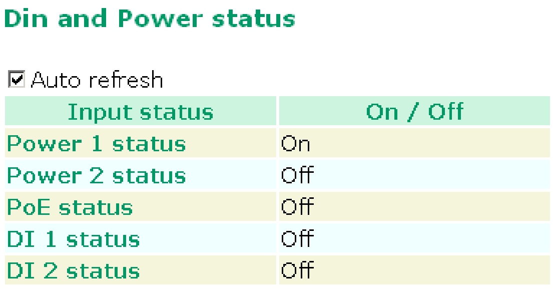
Relay Status

☑ Auto refresh

Relay Status		
Power1 transition (On-->Off)	---	Acknowledge Event
Power2 transition (On-->Off)	---	Acknowledge Event
PoE transition (On-->Off)	---	Acknowledge Event
DI1 transition (On-->Off)	---	Acknowledge Event
DI1 transition (Off-->On)	---	Acknowledge Event
DI2 transition (On-->Off)	---	Acknowledge Event
DI2 transition (Off-->On)	---	Acknowledge Event
LAN link On	---	Acknowledge Event
LAN link Off	---	Acknowledge Event

DI and Power Status

The status of power inputs and digital inputs is shown on this web page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.



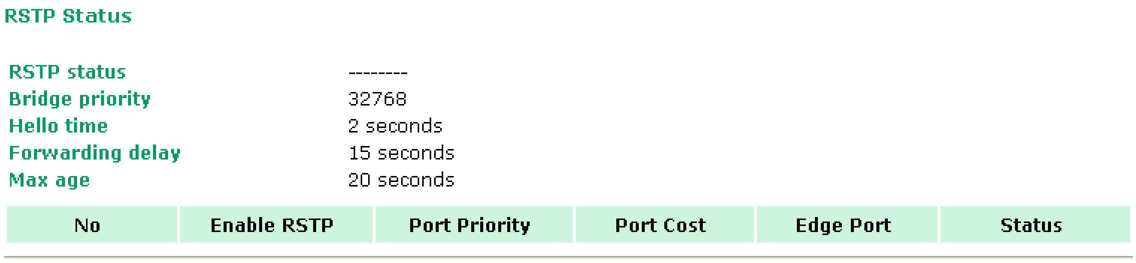
Din and Power status

☑ Auto refresh

Input status	On / Off
Power 1 status	On
Power 2 status	Off
PoE status	Off
DI 1 status	Off
DI 2 status	Off

RSTP Status

The following figures indicate the status which Spanning Tree Protocol parameters have been configured.



RSTP Status

RSTP status	--------
Bridge priority	32768
Hello time	2 seconds
Forwarding delay	15 seconds
Max age	20 seconds

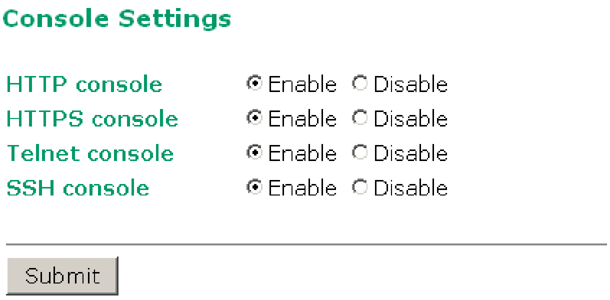
No	Enable RSTP	Port Priority	Port Cost	Edge Port	Status

Maintenance

Maintenance functions provide the administrator with tools to manage the TAP-213 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 you only allow access to the two secured consoles, HTTPS and SSH.

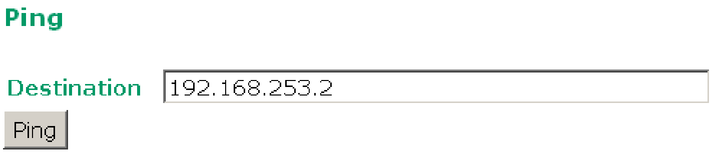


Console Settings

HTTP console	● Enable ○ Disable
HTTPS console	● Enable ○ Disable
Telnet console	● Enable ○ Disable
SSH console	● Enable ○ Disable

Ping

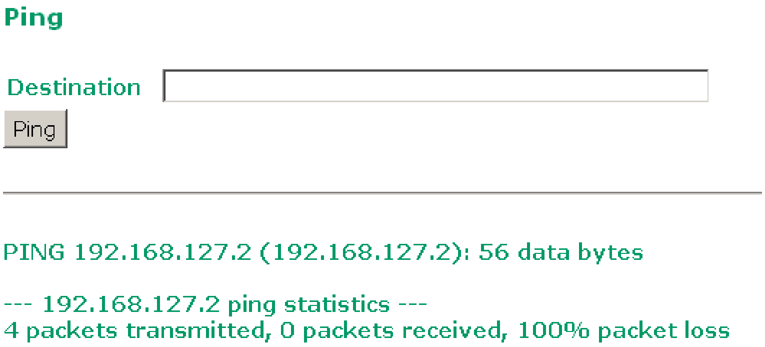
Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and whether or not the access path is available.



Ping

Destination: 192.168.253.2

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 get lost, as shown in the following figure.



Ping

Destination:

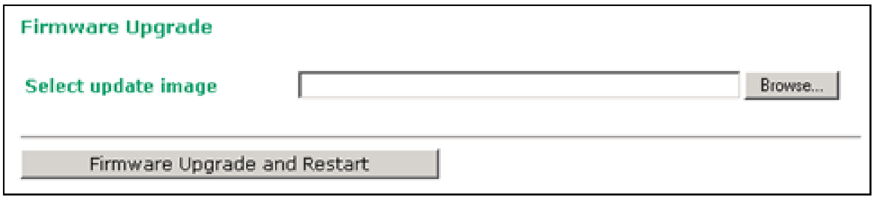
```
PING 192.168.127.2 (192.168.127.2): 56 data bytes

--- 192.168.127.2 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

Firmware Upgrade

The TAP-213 can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available at Moxa's download center.

Before running a firmware upgrade, make sure the TAP-213 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-213 will reboot itself.

When upgrading your firmware, the TAP-213's other functions are forbidden.



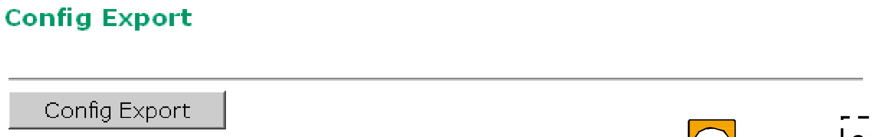
ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your TAP-213.

Config Import/Export

You can back up and restore the TAP-213's configuration with **Config Import and Config Export** functions.

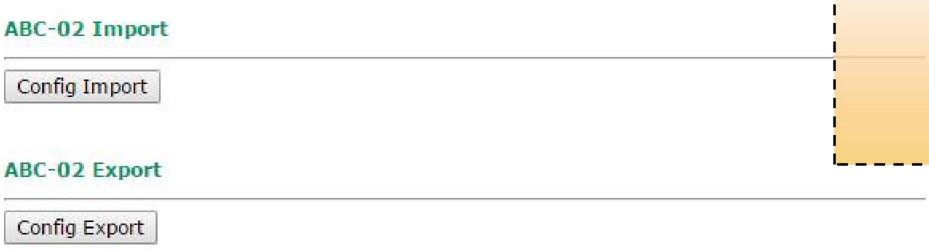
In the **Config Import** section, click **Browse** to specify the configuration file and click on the **Config Import** button to begin importing the configuration.



You can also back up or restore the ABC-02 (HW Rev. 1.1 support only) configuration with **Config Import** [illegible] **Export**.

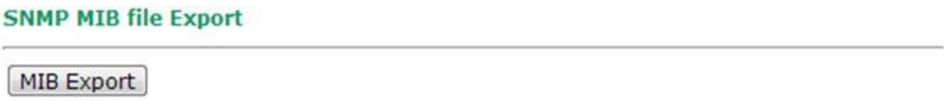
Cecilia_Fernandes
2016-04-21 09:30:26

Is this the latest information?



To download the configuration to the TAP:

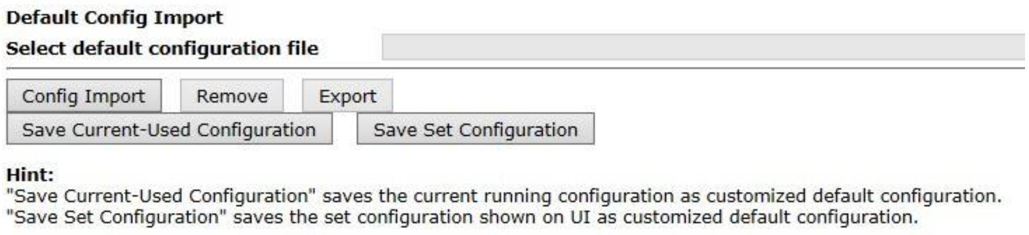
1. Turn off the TAP.
2. Plug in the ABC-02 to the TAP's RS-232 console.
3. Turn on TAP.
4. TAP will detect ABC-02 during the boot up process, and download the configuration from the ABC-01 to the TAP automatically. Once the configuration downloads and if configuration format is correct, the TAP will emit three short beeps, then continue the boot up.
5. Once the TAP has booted up successfully, it will emit the normal two beeps, and the ready LED will turn to solid green.



SNMP MIB file for TAP-213 is embedded in the device. To export the MIB file, simply click on the "MIB Export" button and save it to your local drive.

Default Config Import

You can use the **Default Config Import** screen to import a default configuration file on the TAP. This default configuration file is used when you reset the TAP to the defaults.



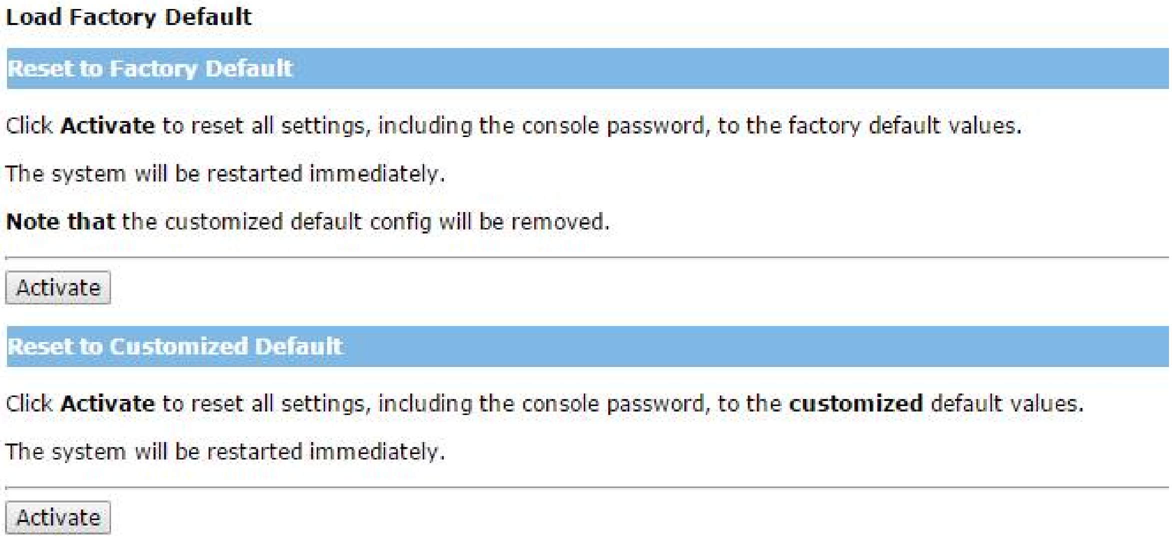
Default Config Import

Select default configuration file

Hint:
"Save Current-Used Configuration" saves the current running configuration as customized default configuration.
"Save Set Configuration" saves the set configuration shown on UI as customized default configuration.

Load Factory Default

Use this function to reset the TAP-213 and roll all settings back to the factory or customized (using imported configuration file in the **Default Config Import** screen) default values. You can also reset the hardware by pressing the reset button on the top panel of the TAP-213.



Load Factory Default

Reset to Factory Default

Click **Activate** to reset all settings, including the console password, to the factory default values.

The system will be restarted immediately.

Note that the customized default config will be removed.

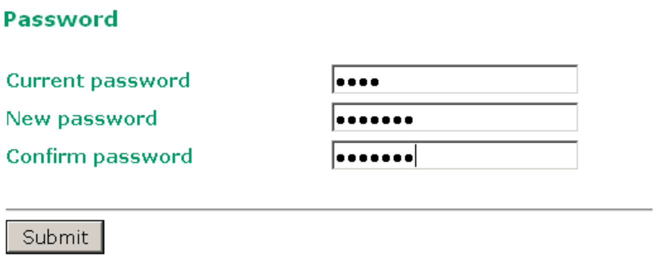
Reset to Customized Default

Click **Activate** to reset all settings, including the console password, to the **customized** default values.

The system will be restarted immediately.

Password

You can change the administration password for each of the TAP-213's console managers by using the **Password** function. Before you set up a new password, you must input the current password and reenter the new password for confirmation. For your security, do not use the default password ***root***, and remember to change the administration password regularly.

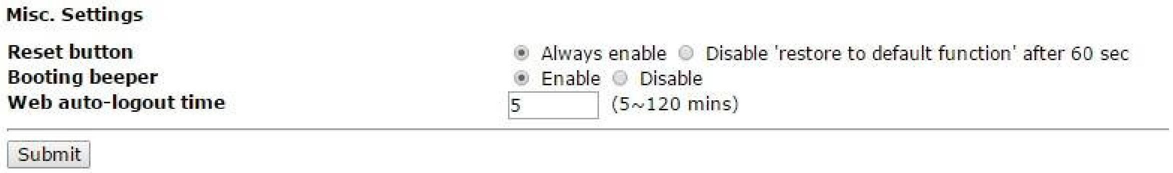


Password

Current password	••••
New password	•••••••
Confirm password	•••••••

Misc. Settings

Additional settings to help you manage your TAP-213, are available on this page.



Misc. Settings

Reset button ● Always enable ○ Disable 'restore to default function' after 60 sec

Booting beeper ● Enable ○ Disable

Web auto-logout time 5 (5~120 mins)

Reset button

Setting	Description	Factory Default
Always enable	The TAP-213's Reset button works normally.	Always enable
Disable 'restore to default function' after 60 sec	The TAP-213's reset to default function will be inactive 60 seconds after the TAP-213 finishes booting up.	

Booting beeper

Setting	Description	Factory Default
Enable/Disable	Disable this function to turn off the beeper when the TAP is booting up.	Enable

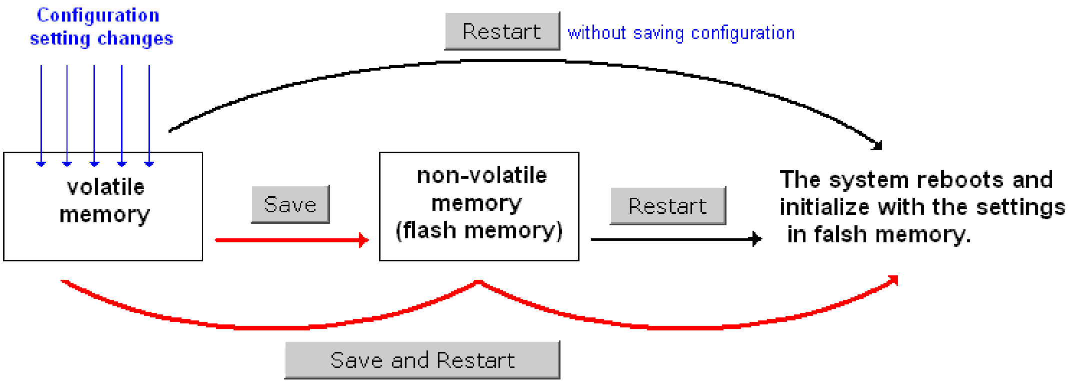
Web auto-logout time

Setting	Description	Factory Default
5 to 120 min.	This sets the inactivity timeout. When the web console is idle for the specified time, the system automatically logs out the user.	5

Save Configuration

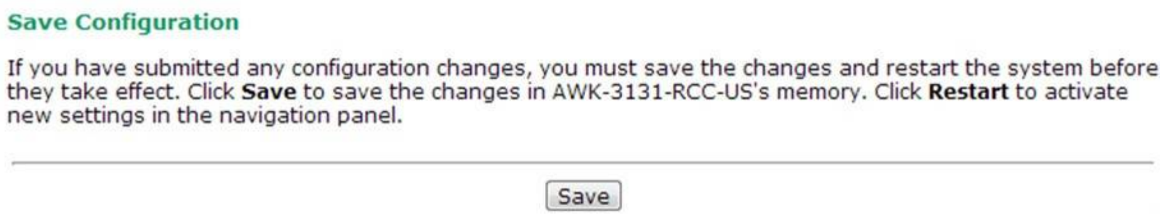
The following figure shows how the TAP-213 stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the TAP-213 is shutdown or rebooted unless they are **y**. Because the TAP-213 starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the TAP-213.

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



Configuration setting changes
Restart
without saving configuration
volatile memory
Save
non-volatile memory (flash memory)
Restart
The system reboots and initialize with the settings in falsh memory.
Save and Restart

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.



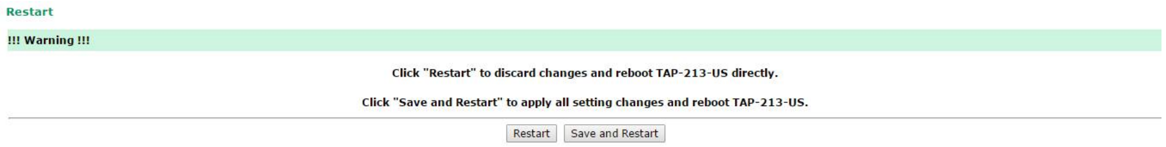
Save Configuration

If you have submitted any configuration changes, you must save the changes and restart the system before they take effect. Click **Save** to save the changes in AWK-3131-RCC-US's memory. Click **Restart** to activate new settings in the navigation panel.

Restart

If you submitted configuration changes, you will find a blinking string 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-213 directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the TAP-213.



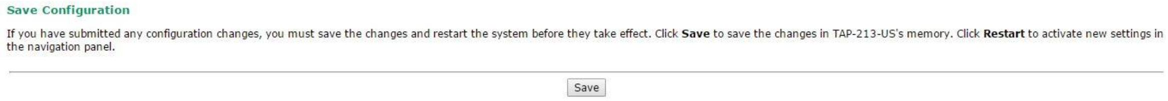
Restart

!!! Warning !!!

Click "Restart" to discard changes and reboot TAP-213-US directly.

Click "Save and Restart" to apply all setting changes and reboot TAP-213-US.

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.



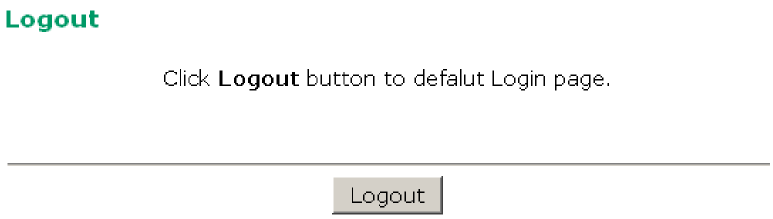
Save Configuration

If you have submitted any configuration changes, you must save the changes and restart the system before they take effect. Click **Save** to save the changes in TAP-213-US's memory. Click **Restart** to activate new settings in the navigation panel.

You will not be able to run any of the TAP-213'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 you logout before quitting the console manager.



Logout

Click **Logout** button to defalut Login page.

4

Software Installation and Configuration

The following topics are covered in this chapter:

- ❒ **Overview**
- ❒ **Wireless Search Utility**
  - ➢ Installing Wireless Search Utility
  - ➢ Configuring Wireless Search Utility

Overview

The Documentation & Software CD included with your TAP-213 is designed to make the installation and configuration procedure easy and straightforward. This auto-run CD includes TAP Search Utility (to broadcast search for all TAP's accessible over the network), the TAP-213 User's Manual, and Quick Installation Guide.

Cecilia_Fernandes
2016-04-21 09:31:15

Please confirm if we have removed the software CD. If yes, then I need to rewrite this content.

Wireless Search Utility

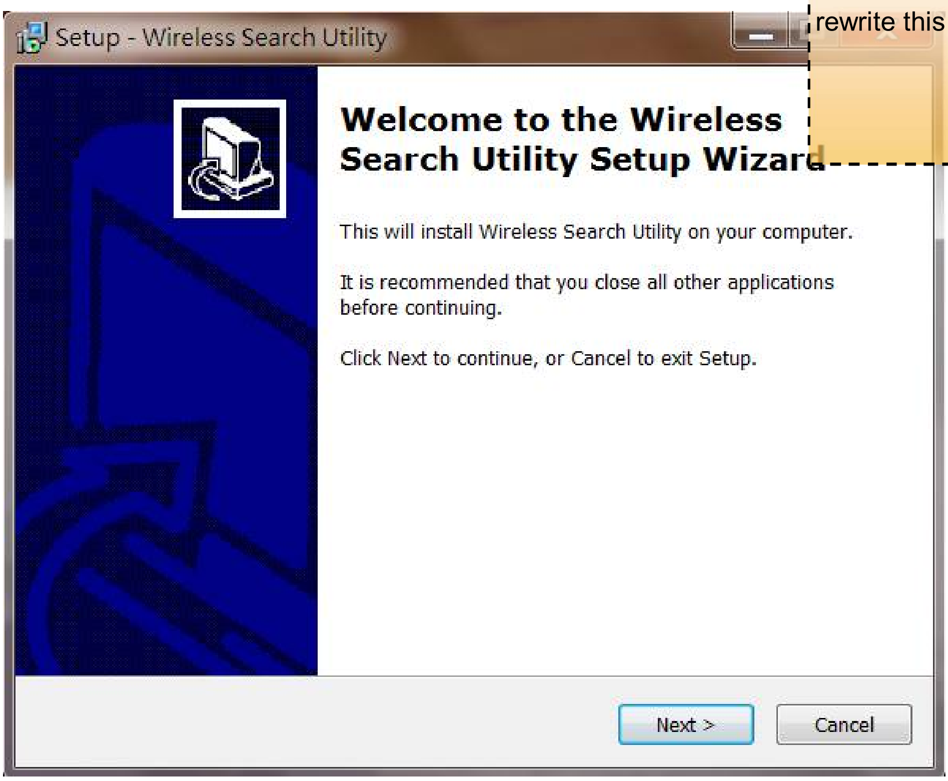
Installing Wireless Search Utility

Click the **INSTALL UTILITY** button in the TAP Installation CD auto-run window [illegible] Search Utility. Once the program starts running, click **Yes** to proceed.

Cecilia_Fernandes
2016-04-21 09:31:20

Please confirm if we have removed the software CD. If yes, then I need to rewrite this content.

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



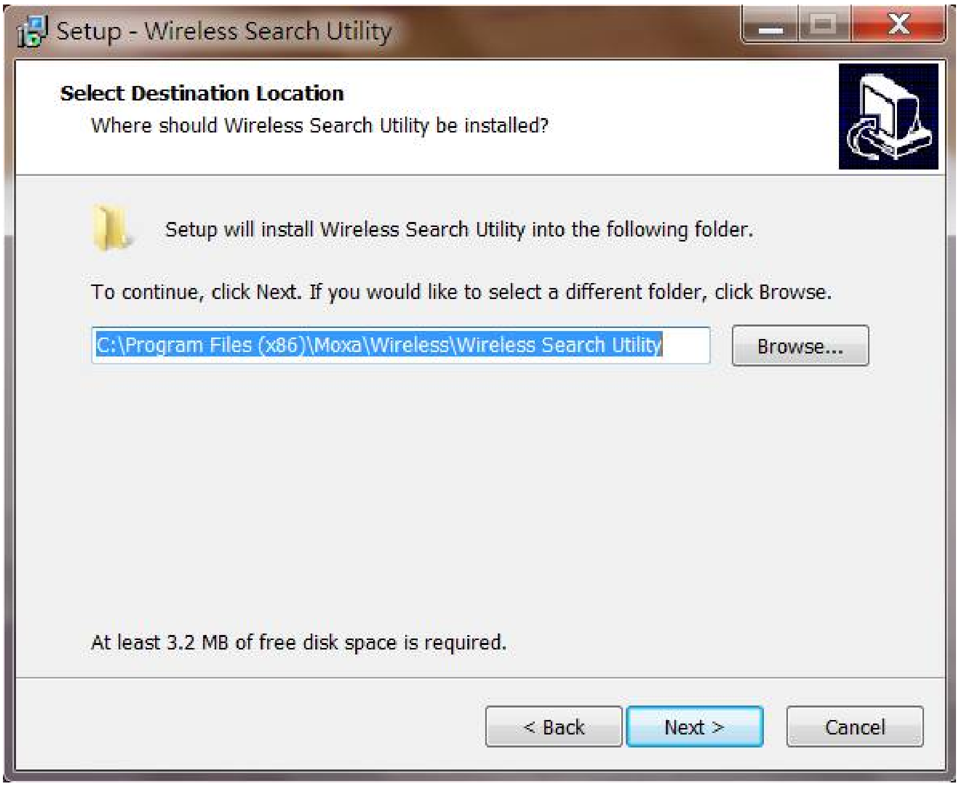
Welcome to the Wireless Search Utility Setup Wizard

This will install Wireless Search Utility on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

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



Select Destination Location

Where should Wireless Search Utility be installed?

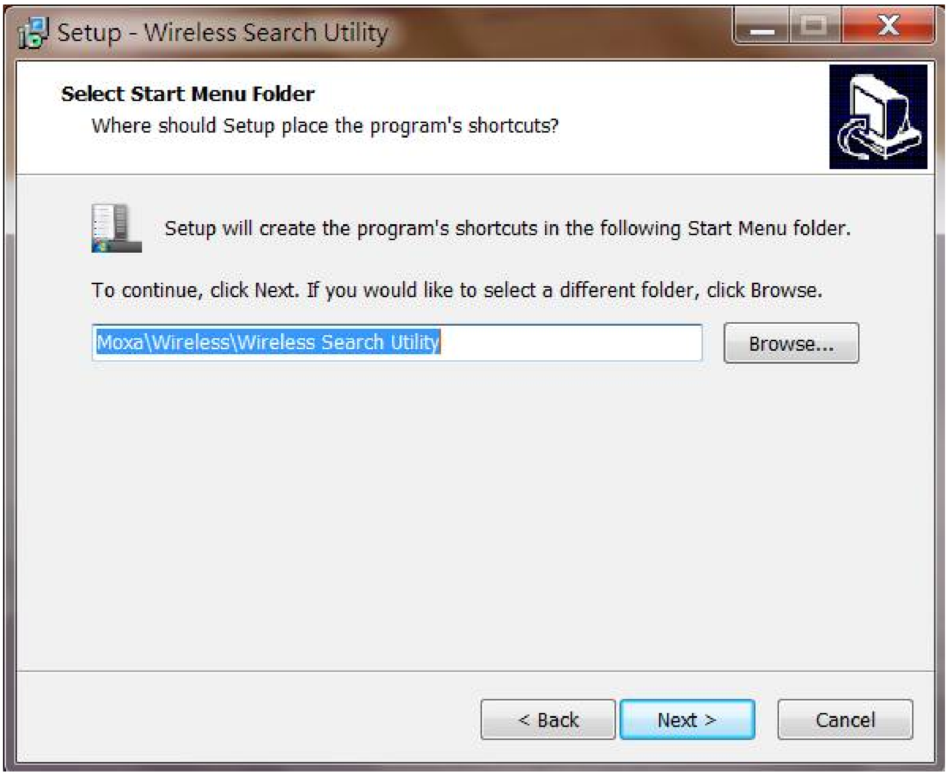
Setup will install Wireless Search Utility into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\Moxa\Wireless\Wireless Search Utility

At least 3.2 MB of free disk space is required.

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



Select Start Menu Folder

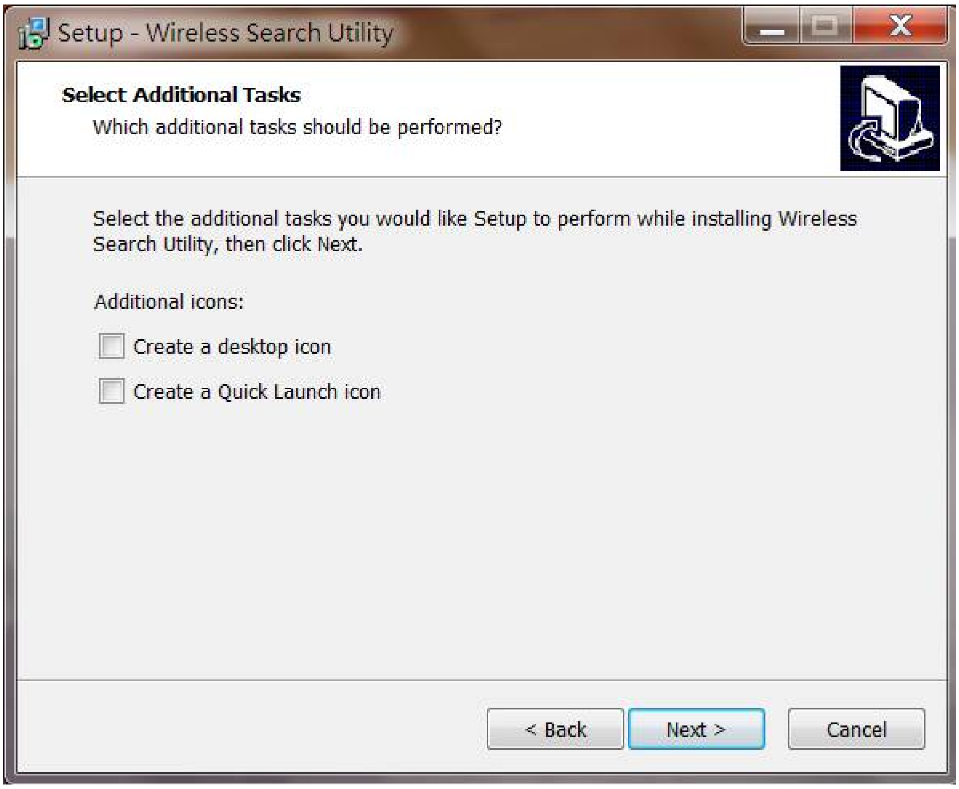
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

Moxa\Wireless\Wireless Search Utility

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



Select Additional Tasks

Which additional tasks should be performed?

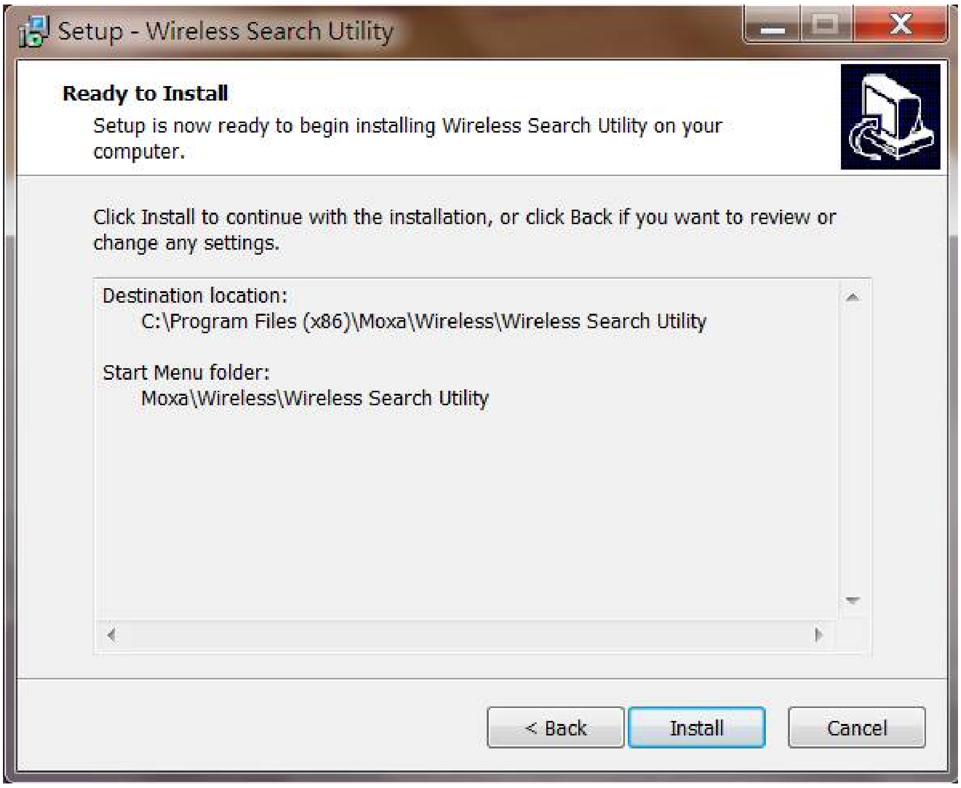
Select the additional tasks you would like Setup to perform while installing Wireless Search Utility, then click Next.

Additional icons:

□ Create a desktop icon

□ Create a Quick Launch icon

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



Ready to Install

Setup is now ready to begin installing Wireless Search Utility on your computer.

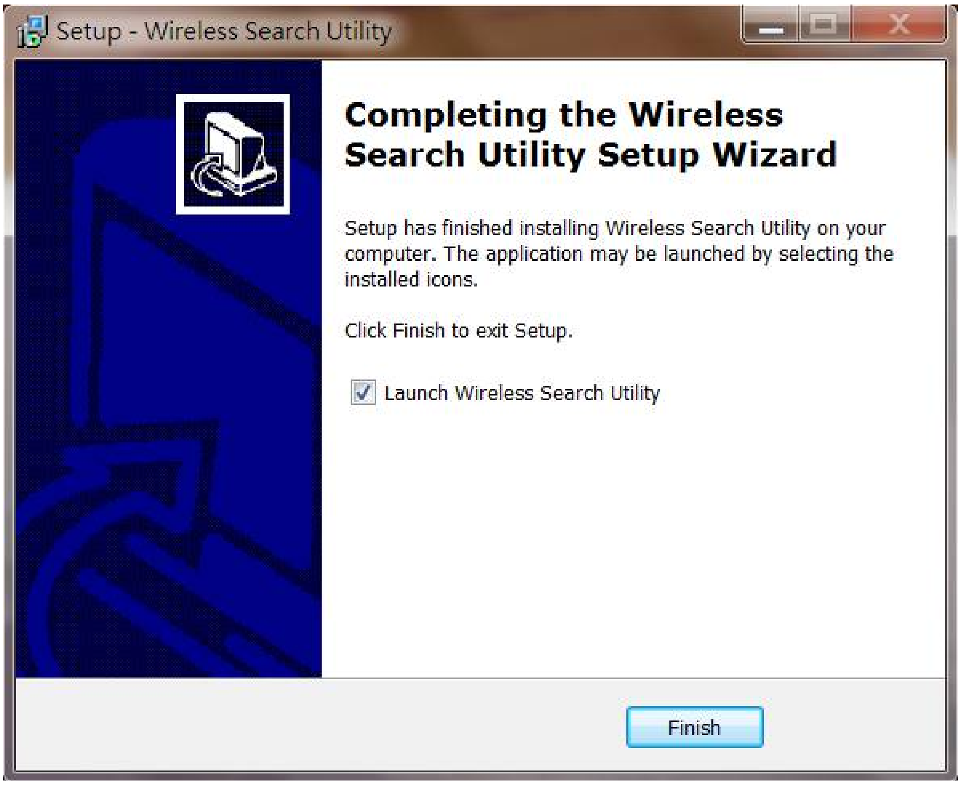
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
    C:\Program Files (x86)\Moxa\Wireless\Wireless Search Utility

Start Menu folder:
    Moxa\Wireless\Wireless Search Utility

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

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



Setup - Wireless Search Utility

Completing the Wireless Search Utility Setup Wizard

Setup has finished installing Wireless Search Utility on your computer. The application may be launched by selecting the installed icons.

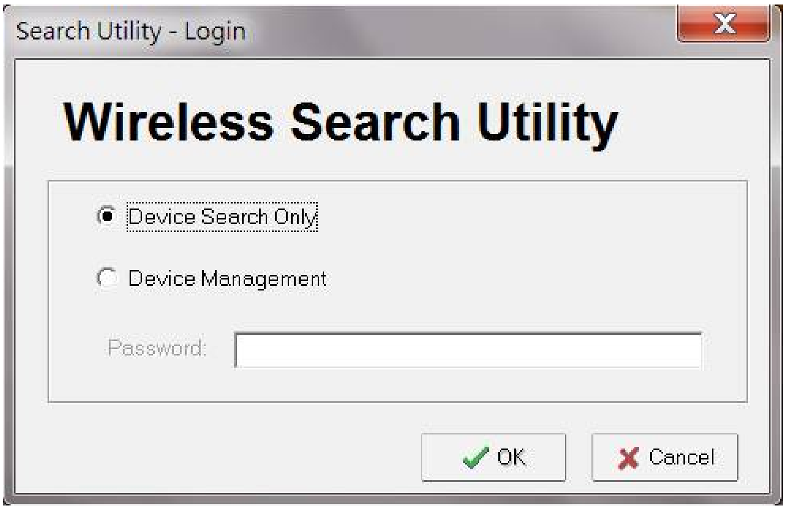
Click Finish to exit Setup.

☑ Launch Wireless Search Utility

Configuring Wireless Search Utility

The Broadcast Search function is used to locate all TAP-213 APs that are connected to the same LAN as your computer. After locating a TAP-213, 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-213 is configured as an AP or Client. In either case, APs and Clients connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

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



Search Utility - Login

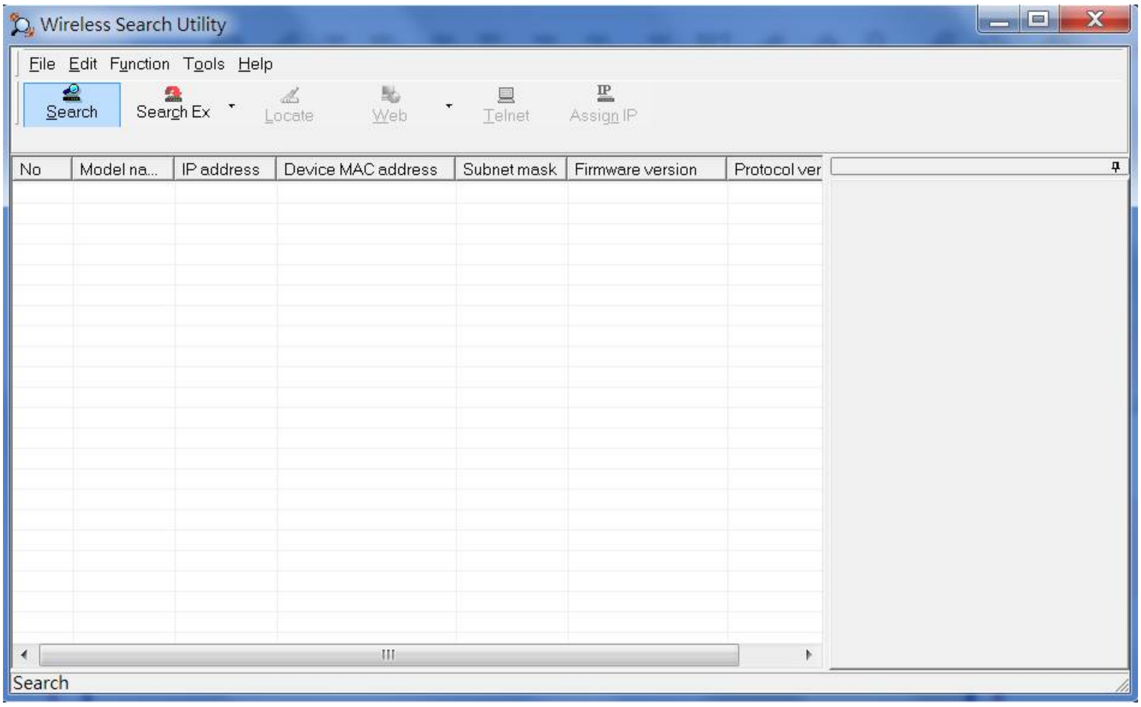
Wireless Search Utility

● Device Search Only

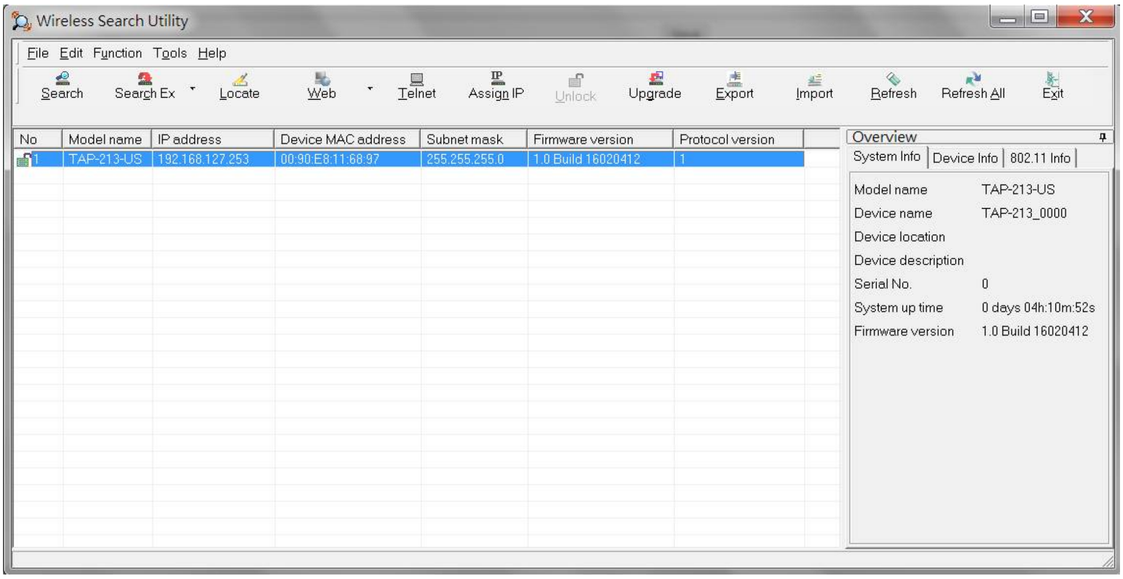
○ Device Management

Password:

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



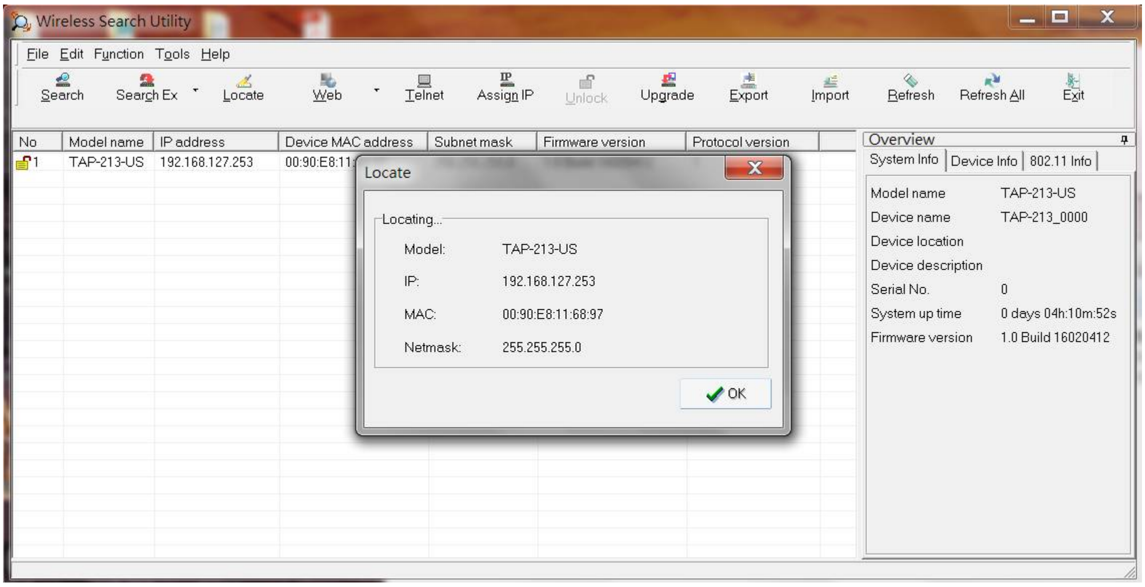
3. The “Searching” window indicates the progress of the search. When the search is complete, all TAPs that were located will be displayed in the Wireless Search Utility window.



No	Model name	IP address	Device MAC address	Subnet mask	Firmware version	Protocol version
1	TAP-213-US	192.168.127.253	00:90:E8:11:68:97	255.255.255.0	1.0 Build 16020412	1

Model name	TAP-213-US
Device name	TAP-213_0000
Device location	
Device description	
Serial No.	0
System up time	0 days 04h:10m:52s
Firmware version	1.0 Build 16020412

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



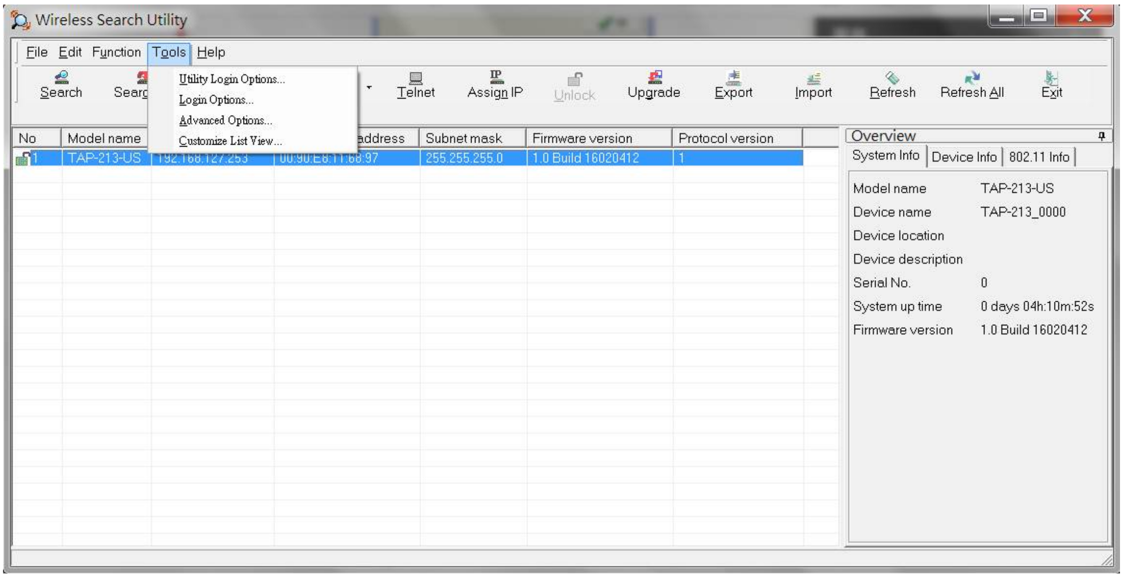
No	Model name	IP address	Device MAC address	Subnet mask	Firmware version	Protocol version
1	TAP-213-US	192.168.127.253	00:90:E8:11			

Locating...

Model:	TAP-213-US
IP:	192.168.127.253
MAC:	00:90:E8:11:68:97
Netmask:	255.255.255.0

Model name	TAP-213-US
Device name	TAP-213_0000
Device location	
Device description	
Serial No.	0
System up time	0 days 04h:10m:52s
Firmware version	1.0 Build 16020412

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



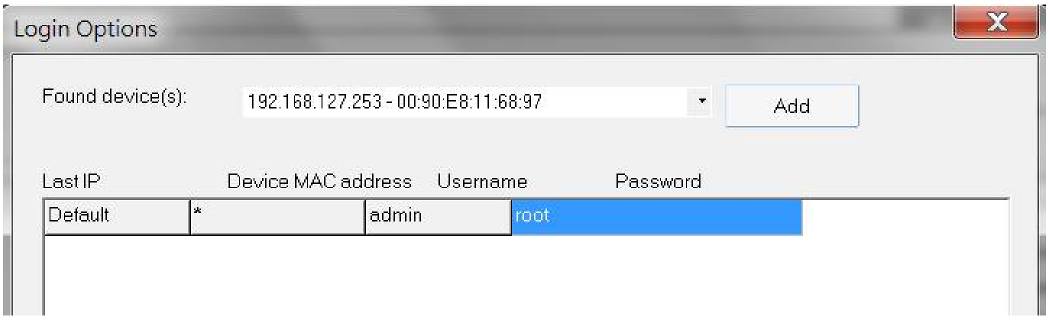
No	Model name	address	Subnet mask	Firmware version	Protocol version
1	TAP-213-US	192.168.127.253 / 00:90:E8:11:68:97	255.255.255.0	1.0 Build 16020412	1

Model name	TAP-213-US
Device name	TAP-213_0000
Device location	
Device description	
Serial No.	0
System up time	0 days 04h:10m:52s
Firmware version	1.0 Build 16020412

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

ATTENTION

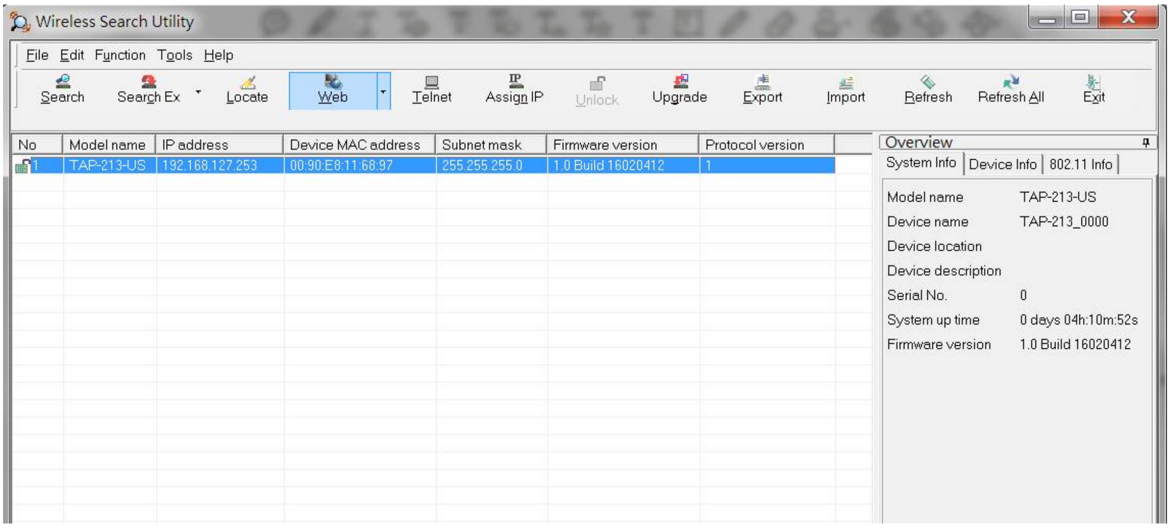
For security purposes, we suggest you can change the wireless search utility login password instead of using the default.



Found device(s): 192.168.127.253 - 00:90:E8:11:68:97

Last IP	Device MAC address	Username	Password
Default	*	admin	root

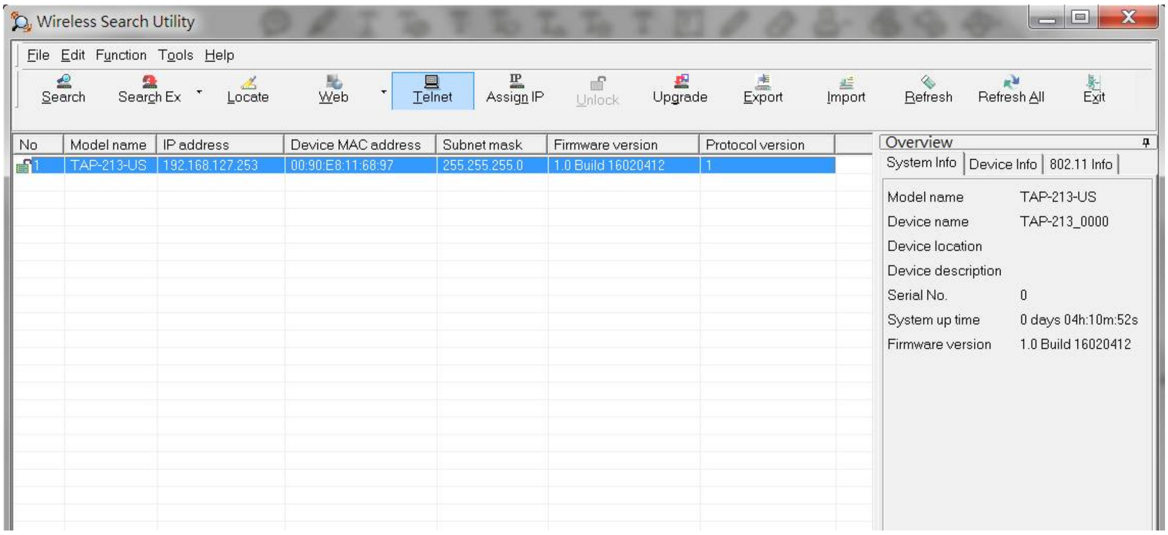
To modify the configuration of the highlighted TAP, click on the Web icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, “Using the Web Console,” for information on how to use the web console.



No	Model name	IP address	Device MAC address	Subnet mask	Firmware version	Protocol version
1	TAP-213-US	192.168.127.253	00:90:E8:11:68:97	255.255.255.0	1.0 Build 16020412	1

Model name	TAP-213-US
Device name	TAP-213_0000
Device location	
Device description	
Serial No.	0
System up time	0 days 04h:10m:52s
Firmware version	1.0 Build 16020412

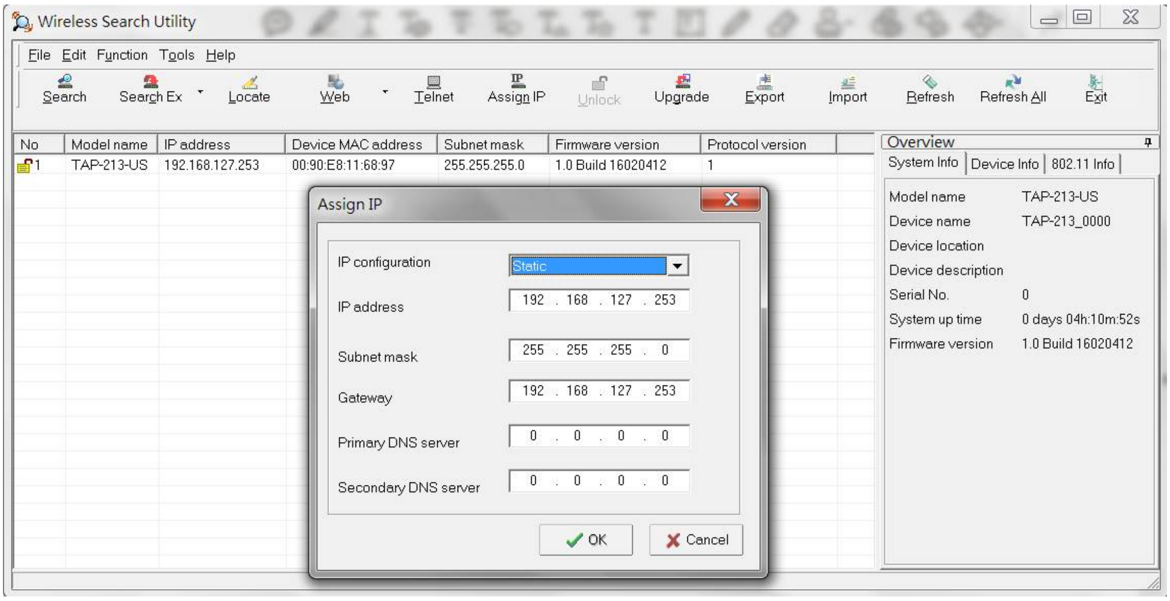
Click on **Telnet** if you would like to use telnet to configure your TAPs.



No	Model name	IP address	Device MAC address	Subnet mask	Firmware version	Protocol version
1	TAP-213-US	192.168.127.253	00:90:E8:11:68:97	255.255.255.0	1.0 Build 16020412	1

Model name	TAP-213-US
Device name	TAP-213_0000
Device location	
Device description	
Serial No.	0
System up time	0 days 04h:10m:52s
Firmware version	1.0 Build 16020412

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



No	Model name	IP address	Device MAC address	Subnet mask	Firmware version	Protocol version
1	TAP-213-US	192.168.127.253	00:90:E8:11:68:97	255.255.255.0	1.0 Build 16020412	1

Assign IP

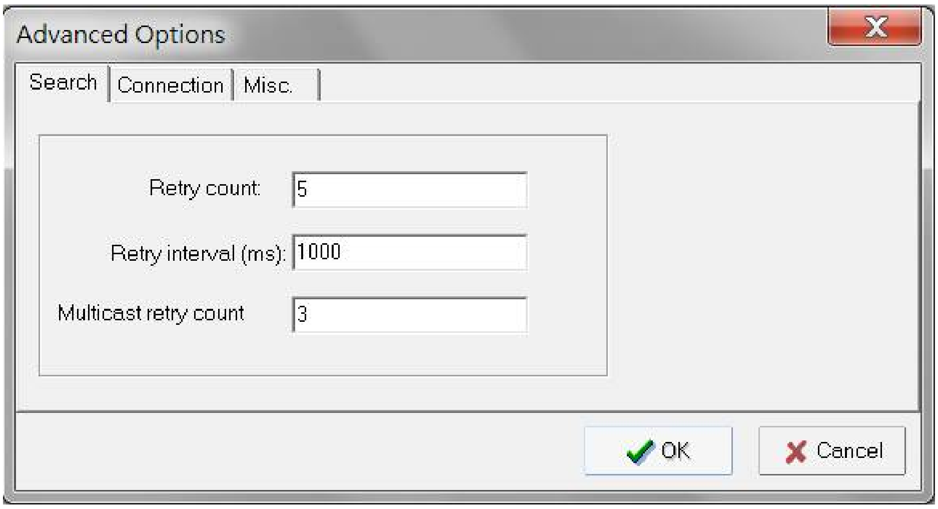
IP configuration	Static
IP address	192 . 168 . 127 . 253
Subnet mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 127 . 253
Primary DNS server	0 . 0 . 0 . 0
Secondary DNS server	0 . 0 . 0 . 0

Model name	TAP-213-US
Device name	TAP-213_0000
Device location	
Device description	
Serial No.	0
System up time	0 days 04h:10m:52s
Firmware version	1.0 Build 16020412

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

Search

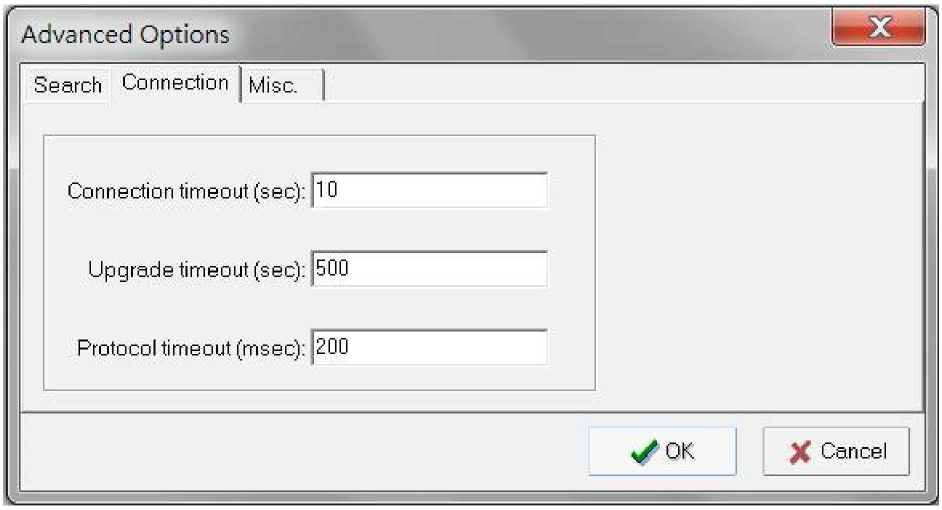
- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time elapsed between retries.



Retry count:	5
Retry interval (ms):	1000
Multicast retry count	3

Connection

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



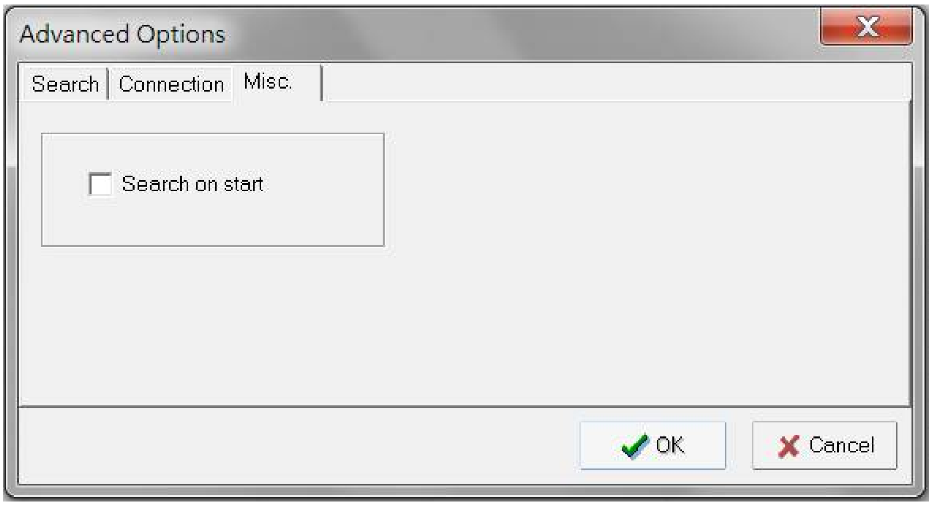
Connection timeout (sec): 10

Upgrade timeout (sec): 500

Protocol timeout (msec): 200

Misc.

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



□ Search on start

5

Other Console Considerations

This chapter explains how to access the TAP-213 for the first time. In addition to HTTP access, there are four ways to access TAP-213: 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-213 to a PC's COM port, can be used if you do not know the TAP-213's IP address. The other consoles can be used to access the TAP-213 over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

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

❒ **Configuration by Telnet and SSH Consoles**

❒ **Configuration by Web Browser with HTTPS/SSL**

❒ **Disabling Telnet and Browser Access**

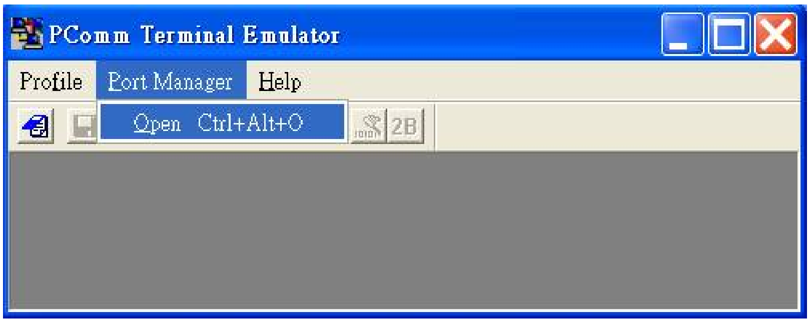
USB Console Configuration (115200, None, 8, 1, VT100)

The serial console connection method, which requires using a short serial cable to connect the TAP-213 to a PC's COM port, can be used if you do not know the TAP-213's IP address. It is also convenient to use serial console configurations when you cannot access the TAP-213 over Ethernet LAN, such as in the case of LAN cable disconnections or broadcast storming over the LAN.

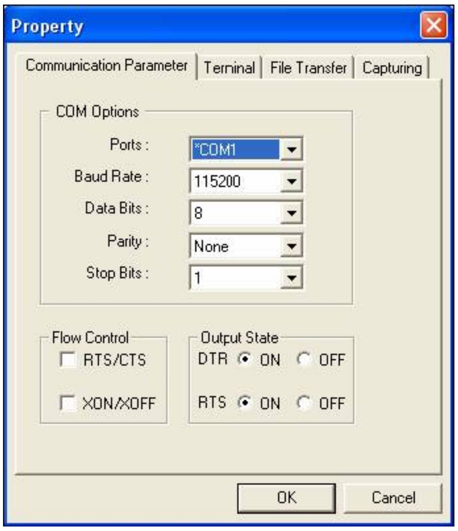
NOTE We recommend using **Moxa PComm (Lite)** Terminal Emulator, which can be downloaded free of charge from Moxa's website.

Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the TAP-213's USB console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, take the following steps to access the RS-232 console utility.

1. From the Windows desktop, open the Start menu and start **PComm Terminal Emulator** in 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. Click on the **Terminal** tab, and select **VT100 (or ANSI)** for Terminal Type. Click on **OK** to continue.



COM Options

Ports : *COM1

Baud Rate : 115200

Data Bits : 8

Parity : None

Stop Bits : 1

Flow Control

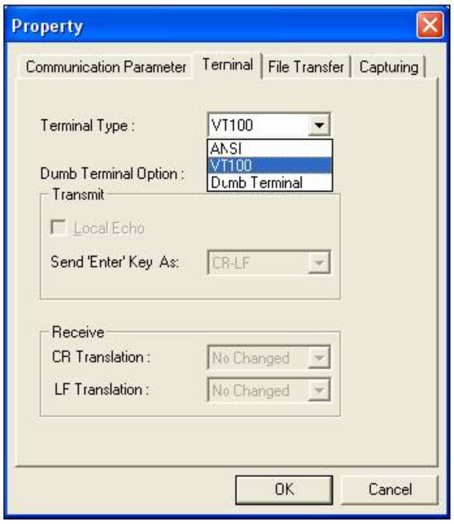
□ RTS/CTS

□ XON/XOFF

Output State

DTR ● ON ○ OFF

RTS ● ON ○ OFF



Terminal Type : VT100

Dumb Terminal Option :

Transmit

□ Local Echo

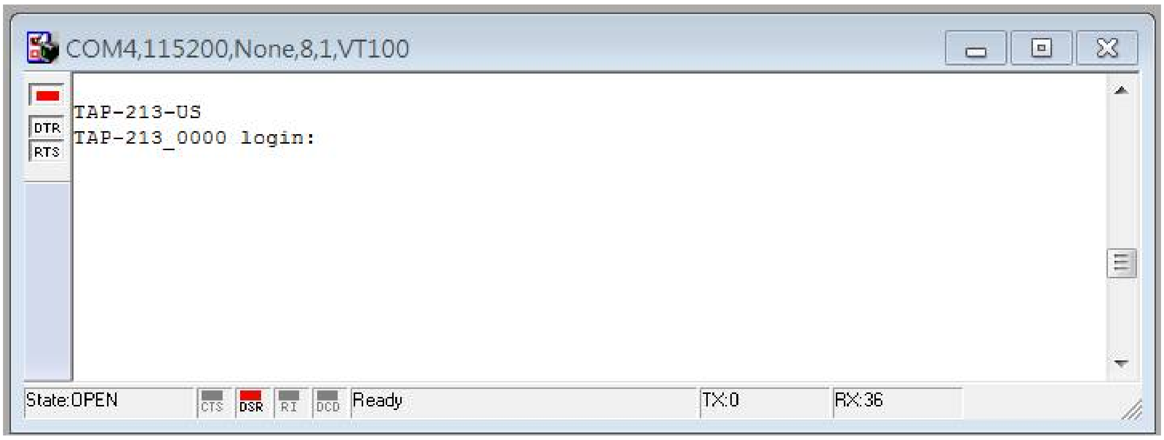
Send 'Enter' Key As: CR-LF

Receive

CR Translation : No Changed

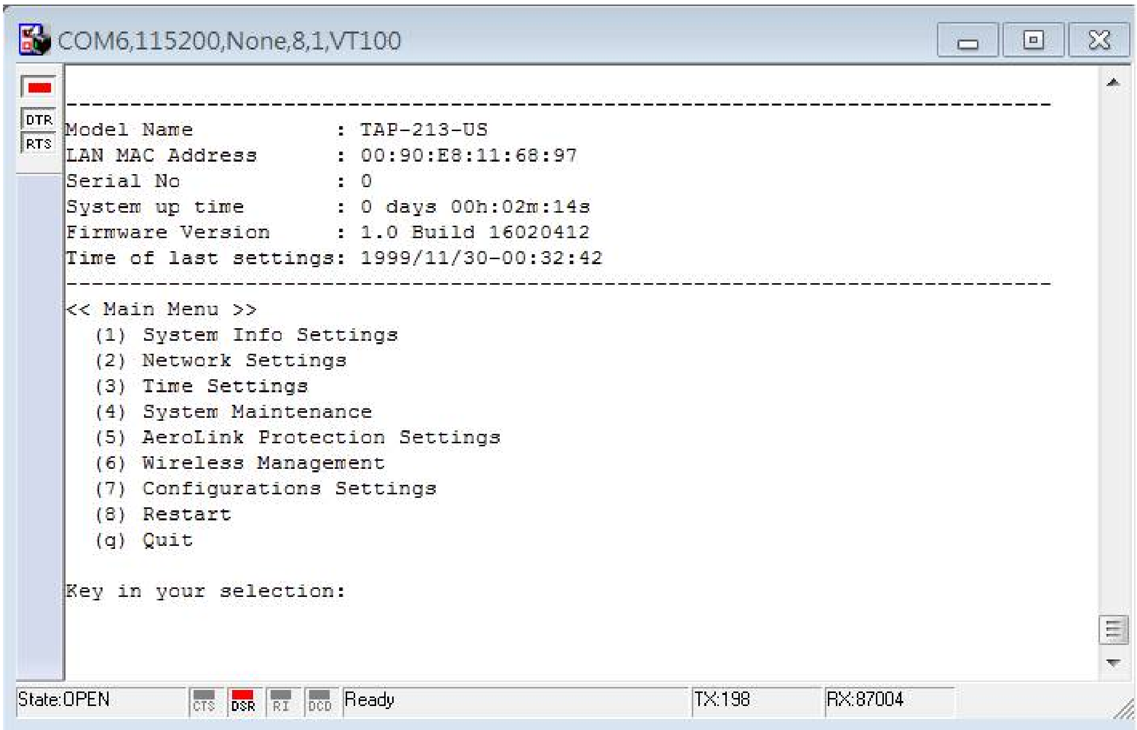
LF Translation : No Changed

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



```
TAP-213-US
TAP-213_0000 login:
```

5. The TAP-213's device information and Main Menu will be displayed. Please follow the description on screen and select the administration option you wish to perform.



```
-----------------------------------------------------------------------------
Model Name           : TAP-213-US
LAN MAC Address      : 00:90:E8:11:68:97
Serial No            : 0
System up time       : 0 days 00h:02m:14s
Firmware Version     : 1.0 Build 16020412
Time of last settings: 1999/11/30-00:32:42
-----------------------------------------------------------------------------
<< Main Menu >>
  (1) System Info Settings
  (2) Network Settings
  (3) Time Settings
  (4) System Maintenance
  (5) AeroLink Protection Settings
  (6) Wireless Management
  (7) Configurations Settings
  (8) Restart
  (q) Quit

Key in your selection:
```

ATTENTION

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

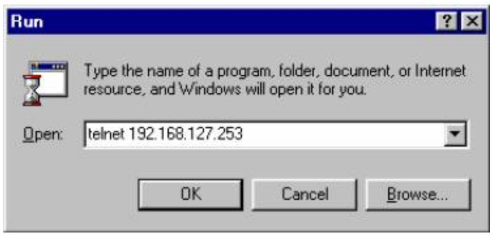
Configuration by Telnet and SSH Consoles

You may use Telnet or SSH client to access the TAP-213 and manage the console over a network. To access the TAP-213's functions over the network from a PC host that is connected to the same LAN as the TAP-213, you need to make sure that the PC host and the TAP-213 are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

NOTE The TAP-213'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, run **Start** → **Run**, and then use Telnet to access the TAP-213's IP address from the Windows Run window (you may also issue the telnet command from the MS-DOS prompt).

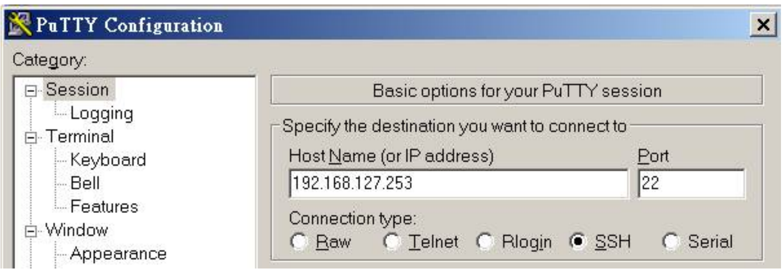


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.127.253

2. When using SSH client (ex. PuTTY), please run the client program (ex. putty.exe) and then input the TAP-213's IP address, specifying **22** for the SSH connection port.



PuTTY Configuration

Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Basic options for your PuTTY session
Specify the destination you want to connect to

Host Name (or IP address): 192.168.127.253

Port: 22

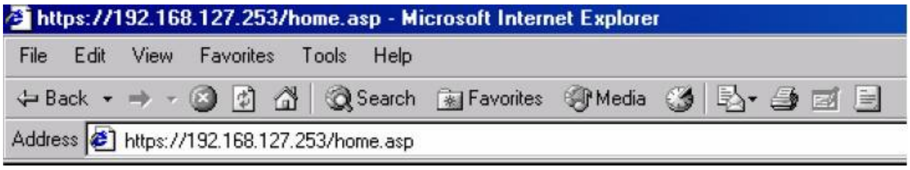
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

3. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.

Configuration by Web Browser with HTTPS/SSL

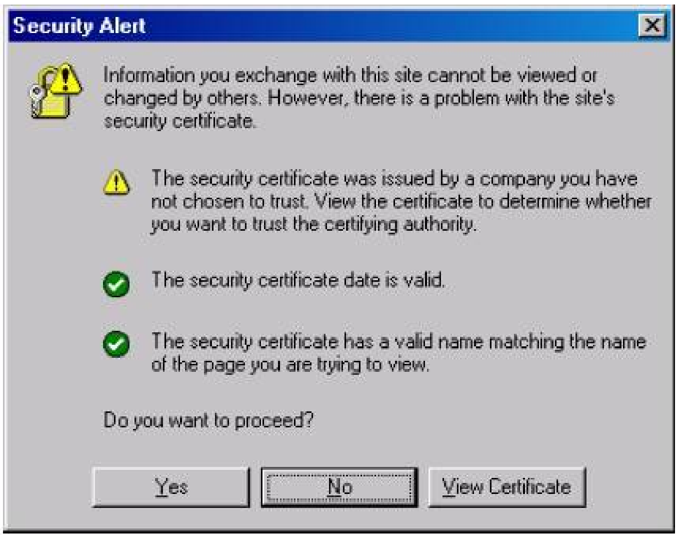
To secure your HTTP access, the TAP-213 supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the TAP-213's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://<TAP-213's IP address> in the address field. Press **Enter** to establish the connection.


https://192.168.127.253/home.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address

https://192.168.127.253/home.asp

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



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

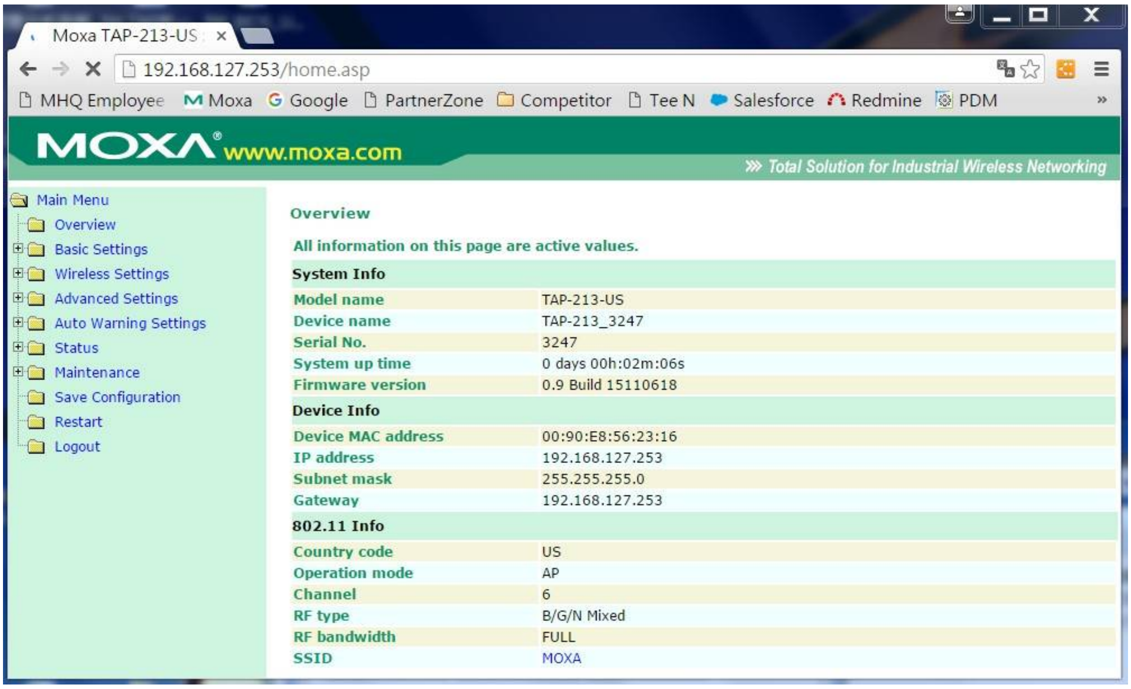
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

3. Select **Yes** to accept the certificate issued by Moxa IW and then enter the TAP-213's web browser interface secured via HTTPS/SSL. (You can see the protocol in URL is **https**.) Then you can use the menu tree on the left side of the window to open the function pages to access each of TAP-213's functions.



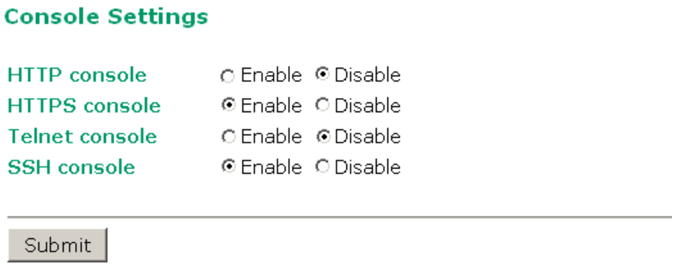
Overview

All information on this page are active values.

System Info	
Model name	TAP-213-US
Device name	TAP-213_3247
Serial No.	3247
System up time	0 days 00h:02m:06s
Firmware version	0.9 Build 15110618
Device Info	
Device MAC address	00:90:E8:56:23:16
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	192.168.127.253
802.11 Info	
Country code	US
Operation mode	AP
Channel	6
RF type	B/G/N Mixed
RF bandwidth	FULL
SSID	MOXA

Disabling Telnet and Browser Access

If you are connecting the TAP-213 to a public network but do not intend to use its management functions over the network, then we suggest disabling both Telnet Console and Web Configuration. Please run **Maintenance** → **Console Settings** to disable them, as shown in the following figure.



Console Settings

HTTP console	○ Enable	● Disable
HTTPS console	● Enable	○ Disable
Telnet console	○ Enable	● Disable
SSH console	● Enable	○ Disable

A

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your TAP-213s and plan your industrial wireless network better.

The following topics are covered in this appendix:

❒ **Beacon**

❒ **DTIM**

❒ **Fragment**

❒ **RTS Threshold**

❒ **STP and RSTP**

- ➢ The STP/RSTP Concept
- ➢ 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 AP.

DTIM

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

Fragment

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

RTS Threshold

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

STP and RSTP

The STP/RSTP Concept

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

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

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:
  - Defaults to sending 802.1D-style BPDUs if packets with this format are received.
  - STP (802.1D) and RSTP (802.1w) can operate on the LAN ports and WLAN ports (AP, Master, Slave, and ACC modes) of the same TAP-213.

This feature is particularly helpful when the TAP-213 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.

B

Supporting Information

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

The following topics are covered in this appendix:

❒ **Firmware Recovery**

❒ **DoC (Declaration of Conformity)**

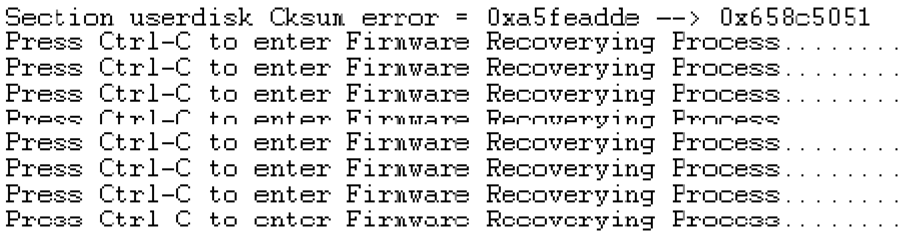
  ➢ Federal Communication Commission Interference Statement

  ➢ R&TTE Compliance Statement

Firmware Recovery

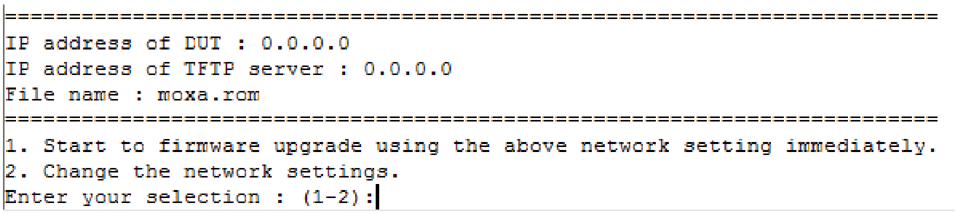
When the LEDs of **FAULT**, **Signal Strength**, **CLIENT**, **BRIDGE** and **WLAN** all light up simultaneously and blink at one-second interval, it means the system booting has failed. It may result from some wrong operation or uncontrollable issues, such as an unexpected shutdown during firmware update. The TAP-213 is designed to help administrators recover such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the TAP-213's ES-232 console with **115200bps and N-8-1**. You will see the following message shown on the terminal emulator every one second.



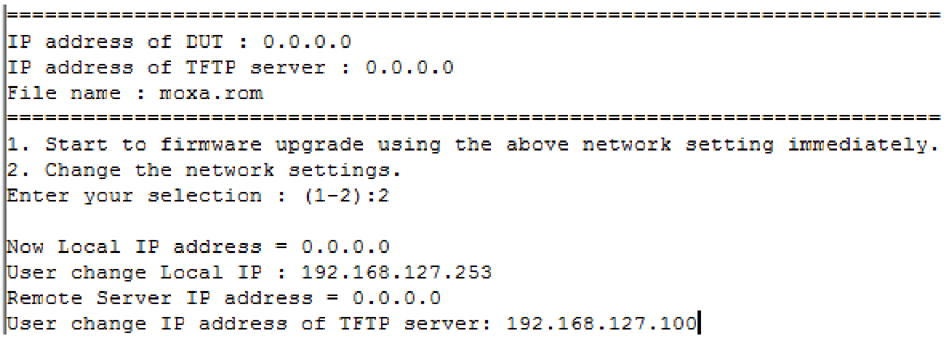
```
Section userdisk Cksum error = 0xa5feadde --> 0x658c5051
Press Ctrl-C to enter Firmware Recoverying Process........
Press Ctrl-C to enter Firmware Recoverying Process........
Press Ctrl-C to enter Firmware Recoverying Process........
Press Ctrl-C to enter Firmware Recoverying Process
Press Ctrl-C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

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



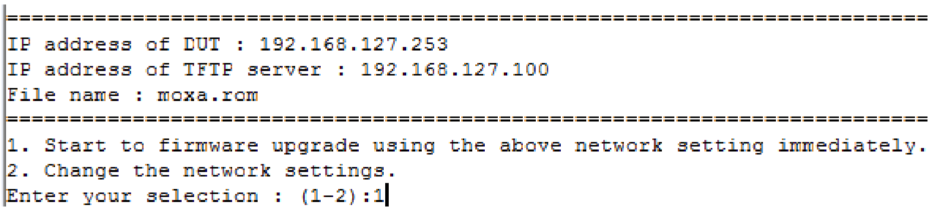
```
========================================================================
IP address of DUT : 0.0.0.0
IP address of TFTP server : 0.0.0.0
File name : moxa.rom
========================================================================
1. Start to firmware upgrade using the above network setting immediately.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

Enter **2** to change the network setting. Specify where the TAP-213's firmware file on the TFTP server and press **y** to write the settings into flash memory.



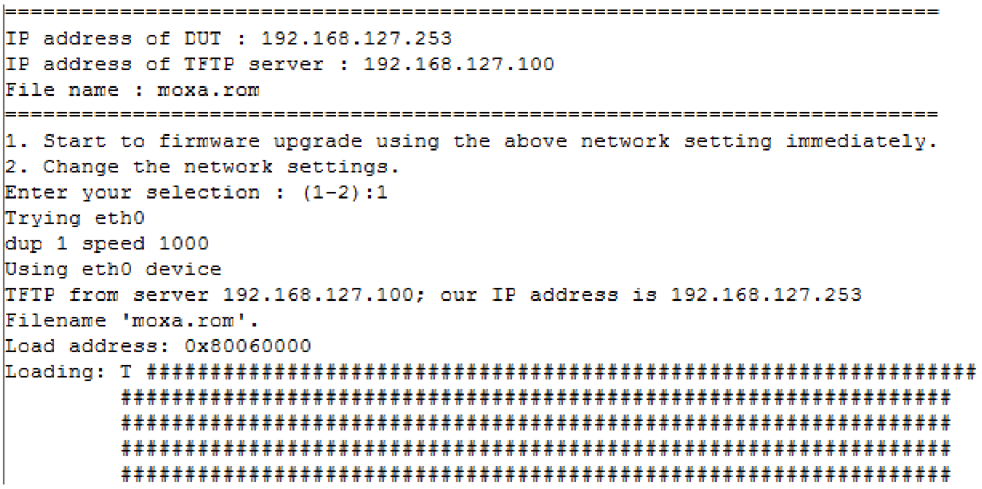
```
========================================================================
IP address of DUT : 0.0.0.0
IP address of TFTP server : 0.0.0.0
File name : moxa.rom
========================================================================
1. Start to firmware upgrade using the above network setting immediately.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

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

TAP-213 restarts, and the "Press Ctrl-C to enter Firmware Recovery Process…" message will reappear. Press **Ctrl-C** to enter the menu and select **1** to start the firmware upgrade process.



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

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



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

DoC (Declaration of Conformity)

Federal Communication Commission Interference Statement

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

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

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

FCC Radiation Exposure Statement

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

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

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

R&TTE Compliance Statement

Moxa declares that the apparatus TAP-213 complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

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 allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

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

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

EU Countries Not Intended for Use

None.

Potential Restrictive Use

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

Cecilia_Fernandes
2016-04-21 09:33:08

I am not sure if this is a stray character of part of the content. please confirm