

TAP-125-u-w-x-z (yyyyyyyyy) User's Manual

Edition 1.0, August 2019

www.moxa.com/product



© 2019 Moxa Inc. All rights reserved.

TAP-125-u-w-x-z (yyyyyyyyy) 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

© 2019 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.....	1-1
Overview	1-2
Package Checklist	1-2
Product Features	1-2
Product Specifications	1-2
Functional Design	1-4
LAN Port	1-4
LED Indicators	1-5
2. Getting Started.....	2-1
First-time Installation and Configuration	2-2
Communication Testing	2-3
Function Map	2-3
3. Web Console Configuration	3-1
Web Browser Configuration	3-2
Overview	3-3
Basic Settings	3-4
System Info Settings	3-4
Network Settings.....	3-5
Time Settings	3-6
Wireless Settings	3-7
Basic Wireless Settings.....	3-8
WLAN Security Settings.....	3-10
Advanced Wireless Settings	3-14
Advanced Settings	3-15
Using Virtual LAN	3-15
Configuring Virtual LAN	3-16
DHCP Server (for AP mode only)	3-17
Packet Filters	3-18
SNMP Agent.....	3-20
Auto Warning Settings.....	3-22
System Log	3-23
Syslog	3-23
E-mail.....	3-24
Trap	3-25
Status	3-27
System Status	3-27
Wireless Status	3-27
Associated Client List (for AP mode only).....	3-28
DHCP Client List (for AP mode only).....	3-28
System Log	3-29
Maintenance	3-29
Console Settings	3-29
Ping.....	3-30
Firmware Upgrade.....	3-30
Config Import Export	3-31
Load Factory Default.....	3-31
Password.....	3-31
Save Configuration	3-32
Restart.....	3-32
Logout.....	3-33
4. Other Console Considerations	4-1
Configuration by Telnet and SSH Consoles	4-2
Configuration by Web Browser with HTTPS/SSL.....	4-2
Disabling Telnet and Browser Access	4-3
A. References	A-1
Beacon	A-2
DTIM.....	A-2

Introduction

The TAP-125 industrial IEEE a/b/g/n/ac wave2 wireless AP/bridge/ client is an ideal wireless solution for applications such as onboard passenger infotainment systems and inter-carriage wireless backbone networks. The TAP-125 provides a faster data rate, wider range, and noticeably stronger signal at the same distance compared with 802.11ac Wave 2 models. The TAP-125 is compliant with EN 50155, covering operating temperature, power input voltage, surge, ESD, and vibration.

The following topics are covered in this chapter:

- ❑ **Overview**
- ❑ **Package Checklist**
- ❑ **Product Features**
- ❑ **Product Specifications**
- ❑ **Functional Design**
 - LAN Port
 - LED Indicators

Overview

The TAP-125-U-W-X-Z (YYYYYYYY) is 802.11ac Wave 2 compliant to deliver speed, range, and reliability to support even the most bandwidth-intensive applications. The 802.11ac Wave 2 standard incorporates multiple technologies, including Spatial Multiplexing MIMO (Multi-In, Multi-Out), 20, 40, and 80 MHz channels, and dual bands (2.4 GHz and 5 GHz) to generate lightning speeds, while still being able to communicate with legacy 802.11a/b/g devices.

The TAP-125-U-W-X-Z (YYYYYYYY) is compliant with EN 50155, covering operating temperature, power input voltage, surge, ESD, and vibration. The wide operating temperature range and IP30-rated housing with LED indicators make the TAP-125-U-W-X-Z (YYYYYYYY) a convenient yet reliable solution for all types of industrial wireless applications.

Package Checklist

Moxa's TAP-125-U-W-X-Z (YYYYYYYY) is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- 1 TAP-125-U-W-X-Z (YYYYYYYY)
- 2 plastic RJ45 protective caps for console port
- Warranty card

NOTE Antennas are not included and should be purchased separately.

Product Features

- Designed specifically for rail passenger infotainment systems
- Compliant with EN 50155
- IEEE802.11a/b/g/n/ac wave 2 compliant
- Three-in-one design (AP/Client)
- Long-distance transmission support
- Wide -40 to 75°C operating temperature range (-T model)
- Wall or rack mounting
- IP30 protected high-strength metal housing

Product Specifications

WLAN Interface

Standards:

IEEE 802.11a/b/g/n/ac wave 2 for Wireless LAN
IEEE 802.11i for Wireless Security
IEEE 802.3 for 10BaseT
IEEE 802.3u for 100BaseTX
IEEE 802.3ab for 1000BaseT
IEEE 802.1D for Spanning Tree Protocol
IEEE 802.1w for Rapid STP
IEEE 802.1Q VLAN

Spread Spectrum and Modulation (typical):

- DSSS with DBPSK, DQPSK, CCK
- OFDM with BPSK, QPSK, 16QAM, 64QAM
- 802.11b: CCK @ 11/5.5 Mbps, DQPSK @ 2 Mbps, DBPSK @ 11 Mbps
- 802.11a/g: 64QAM @ 54/48 Mbps, 16QAM @ 36/24 Mbps, QPSK @ 18/12 Mbps, BPSK @ 9/6 Mbps
- 802.11ac Wave 2: 64QAM @ 300 Mbps to BPSK @ 6.5 Mbps (multiple rates supported)
- 802.11ac: 256QAM @ 1,733 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 (4 channels)
 5.260 to 5.320 (4 channels)*
 5.500 to 5.700 GHz (11 channel)*
 5.745 to 5.825 GHz (5 channels)

EU:

2.412 to 2.472 GHz (13 channels)
 5.180 to 5.240 (4 channels)
 5.260 to 5.320 (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 (4 channels)
 5.260 to 5.320 (4 channels)*
 5.500 to 5.700 GHz (11 channels)*

*These channels will be opened when DFS certification is obtained. Please check Moxa's website for the most up-to-date certification status.

Security:

- SSID broadcast enable/disable
- 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: up to 800 Mbps
 802.11ac: up to 1,733 Mbps

Protocol Support

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

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

Interface

Connector for External Antennas: TAP-125-U-W-X-Z (YYYYYYY): QMA (female)

M12 Ports: LAN1, 10/100/1000/2500/5000BaseT(X) auto negotiation speed, F/H

Console Port: RS-232 (RJ45-type)

LED Indicators: PWR, FAULT, STATE, WLAN, LAN 5G/2.5G, LAN 10/100/1G, TRAFFIC, ACC (reserved)

Physical Characteristics

Housing: Metal, IP30 protection

Weight: 3000 g (6.61 lb)

Dimensions: 220 x 44 x 250 mm (8.66 x 1.73 x 9.84 in)

Installation: Wall mounting (optional), rack 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 95% (non-condensing)

Power Requirements

Input Voltage: 24 to 110 VDC

Power Consumption: 36 W (0.327 A @ 110 VDC; 1.5 A @ 24 VDC)

Standards and Certifications

Safety: UL 60950-1, EN 60950-1

EMC: EN 301 489-1/17

Radio: EN 300 328, EN 301 893

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

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

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty



ATTENTION

- The TAP-125-U-W-X-Z (YYYYYYYY) is NOT a portable mobile device and should be located at least 60 cm away from the human body.
- The TAP-125-U-W-X-Z (YYYYYYYY) is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of TAP-125-U-W-X-Z (YYYYYYYY) units, and to establish

Functional Design

LAN Port

The TAP-125-U-W-X-Z (YYYYYYYY) comes standard with 1 M12 multi-gigabit port. The LAN LED will light up when the LAN cable is inserted.



M12 Ethernet Port

LED Indicators

The LEDs on the front panel of the TAP-125-U-W-X-Z (YYYYYYY) provide a quick and easy means of determining the current operational status and wireless settings.

The **FAULT** LED is used to indicate system failures. If the TAP-125-U-W-X-Z (YYYYYYY) cannot initialize the wireless module (5/2.4 GHz), the **FAULT** LED will blink at one second intervals. If the TAP-125-U-W-X-Z (YYYYYYY) cannot boot correctly or there are some system errors, the **FAULT** LED will be steady on.

LED	Color	State	Description
PWR	Green	ON	Power is being supplied
		OFF	No power supply
FAULT	Green	ON	Reserved
		Blinking	Reserved
		OFF	Reserved
	Red	ON	Device is booting up, system configuration error, or system boot-up error
		Blinking (slow at 1-sec intervals)	Cannot get an IP address from the DHCP server
		Blinking (fast at 0.5-sec intervals)	IP address conflict
		OFF	There are no error conditions
STATE	Green	ON	Software is ready
		Blinking	Reserved
		OFF	The TAP-125 is running normally
	Red	ON	The device is booting up or there is an error condition
		Blinking	Wi-Fi module initialization error (OS and file system boot-up is OK)
		OFF	N/A
WLAN	Green	ON	Reserved
		Blinking at 1-sec intervals	Data transmitted at 5 GHz
		OFF	No data transmitted at 5 GHz
	Amber	Amber ON	Reserved
		Blinking	Data transmitted at 2.4 GHz
		OFF	Reserved
5 G/2.5 G	Green	ON	5 G Ethernet is connected
		Blinking	N/A
		OFF	5 G Ethernet is not connected
	Amber	ON	2.5 G Ethernet is connected
		Blinking	N/A
		OFF	2.5 G Ethernet is not connected
1G/100M /10M	Green	ON	10/100/1000 Mbps Ethernet is connected
		Blinking	N/A
		OFF	Reserved
	Amber	ON	Reserved
		Blinking	N/A
		OFF	Reserved
TRAFFIC	Green	ON	Reserved
		Blinking	Ethernet traffic present
		OFF	Reserved
	Amber	ON	Reserved
		Blinking	Reserved
		OFF	Reserved

Getting Started

This chapter explains how to install Moxa's TAP-125-U-W-X-Z (YYYYYYYY) for the first time, and quickly set up your wireless network and test whether the connection is running well. The Function Map discussed in the third section provides a convenient means of determining which functions 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-125-U-W-X-Z (YYYYYYYY), make sure that all items in the Package Checklist are in the box. You will need access to a notebook computer or PC equipped with an Ethernet port. The TAP-125-U-W-X-Z (YYYYYYYY) has a default IP address that must be used when connecting to the device for the first time.

- **Step 1: Power on the device.**

The TAP-125-U-W-X-Z (YYYYYYYY) can be powered by a DC power input.

- **Step 2: Connect the TAP-125-U-W-X-Z (YYYYYYYY) to a notebook or PC.**

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

Choose an IP address on the same subnet as the TAP-125-U-W-X-Z (YYYYYYYY). Since the TAP-125-U-W-X-Z (YYYYYYYY)'s default IP address is **192.168.127.253**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

- **Step 4: Use the web-based manager to configure the TAP-125-U-W-X-Z (YYYYYYYY)**

Open your computer's web browser and type **http://192.168.127.253** in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on the **Login** button:



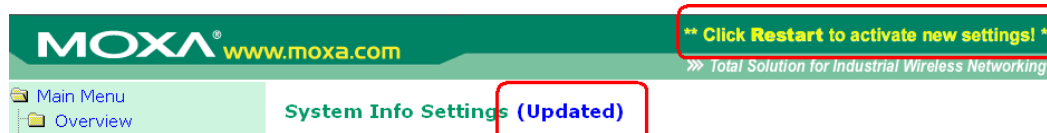
NOTE Default user name and password:

User Name: **admin**

Password: **moxa**

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

NOTE After you click **Submit** to apply changes the web page will refresh (**Updated**) will appear on the page and a blinking reminder will be shown on the upper-right corner of the web page:



To activate the changes click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the TAP-125-U-W-X-Z (YYYYYYYY) to complete the reboot procedure.

- **Step 5: Select the TAP-125-U-W-X-Z (YYYYYYYY) operation mode.**

By default, the TAP-125-U-W-X-Z (YYYYYYYY)'s operation mode is set to AP. You can change to Client mode in

Wireless Settings → **Basic Wireless Settings**. Detailed information about configuring the TAP-125-U-W-X-Z (YYYYYYYY)'s operation can be found in Chapter 3.

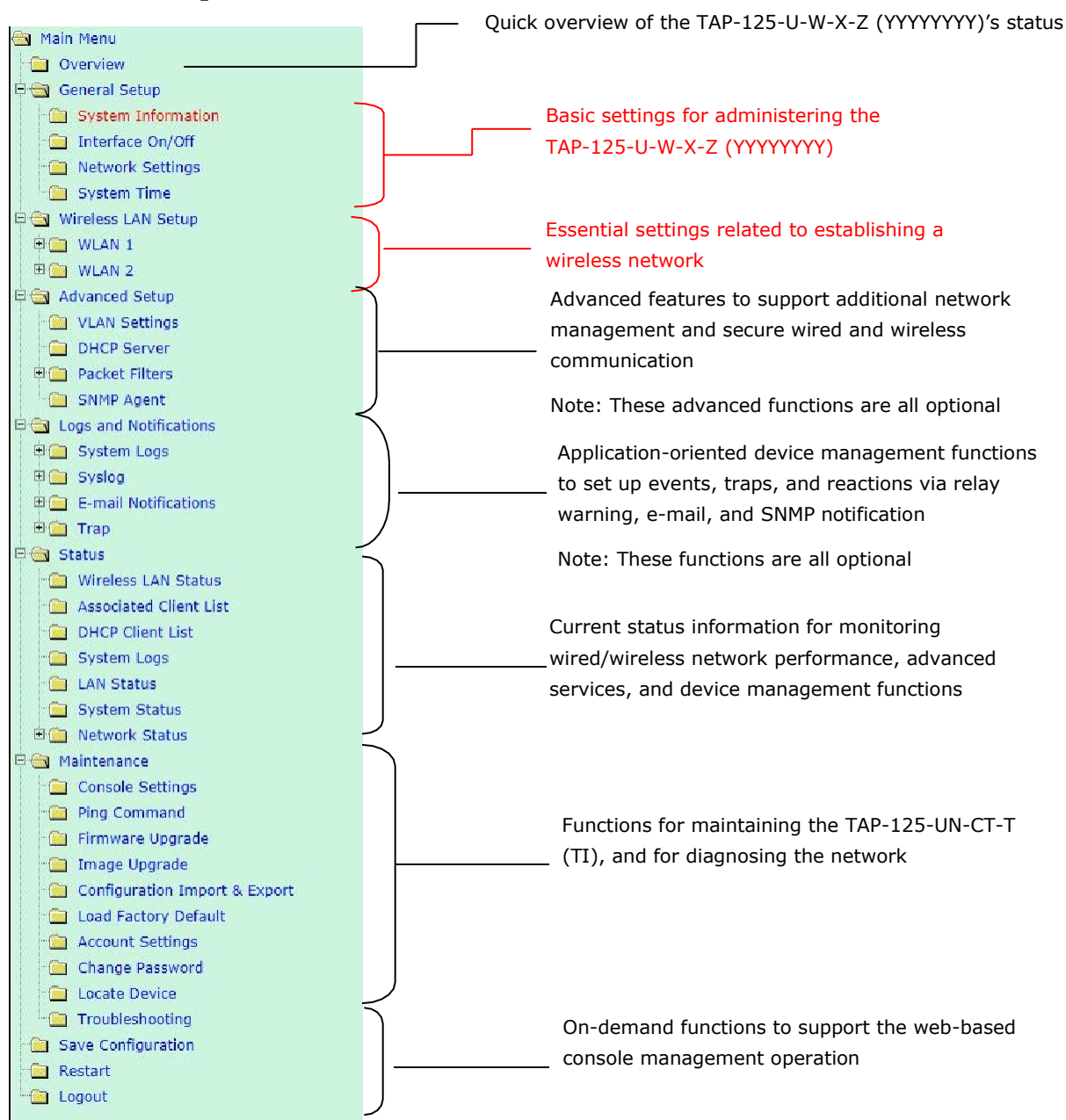
- **Step 6: Test communications.**

In the following sections we describe two test methods that can be used to ensure that a network connection has been established.

Communication Testing

After installing the TAP-125-U-W-X-Z (YYYYYYYY) you can run a sample test to make sure the TAP-125-U-W-X-Z (YYYYYYYY) and wireless connection are functioning normally. Two testing methods are described below. Use the first method if you are using only one TAP-125-U-W-X-Z (YYYYYYYY) device, and use the second method if you are using two or more TAP-125-U-W-X-Z (YYYYYYYY) units.

Function Map



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-125-U-W-X-Z (YYYYYYY) and make it easy to establish and maintain your wireless network.

The following topics are covered in this chapter:

- ❑ **Web Browser Configuration**
- ❑ **Overview**
- ❑ **Basic Settings**
 - System Info Settings
 - Network Settings
 - Time Settings
- ❑ **Wireless Settings**
- ❑ **Basic Wireless Settings**
 - WLAN Security Settings
 - Advanced Wireless Settings
- ❑ **Advanced Settings**
 - Using Virtual LAN
 - Configuring Virtual LAN
 - DHCP Server (for AP mode only)
 - Packet Filters
 - SNMP Agent
- ❑ **Auto Warning Settings**
 - System Log
 - Syslog
 - E-mail
 - Trap
- ❑ **Status**
 - System Status
 - Wireless Status
 - Associated Client List (for AP mode only)
 - DHCP Client List (for AP mode only)
 - System Log
- ❑ **Maintenance**
 - Console Settings
 - Ping
 - Firmware Upgrade
 - Config Import Export
 - Load Factory Default
 - Password
- ❑ **Save Configuration**
- ❑ **Restart**
- ❑ **Logout**

Web Browser Configuration

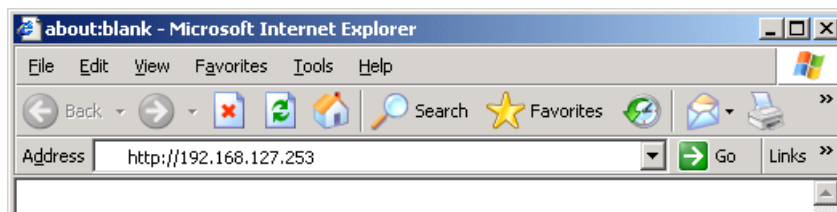
Moxa TAP-125-U-W-X-Z (YYYYYYYY)'s web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the TAP-125-U-W-X-Z (YYYYYYYY)'s management and monitoring functions from a PC host connected to the same LAN as the TAP-125-U-W-X-Z (YYYYYYYY), you must make sure that the PC host and the TAP-125-U-W-X-Z (YYYYYYYY) are on the same logical subnet. Similarly, if the TAP-125-U-W-X-Z (YYYYYYYY) is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

The Moxa TAP-125-U-W-X-Z (YYYYYYYY)'s default IP is **192.168.127.253**.

Follow these steps to access the TAP-125-U-W-X-Z (YYYYYYYY)'s web-based console management interface.

1. Open your web browser (e.g., Internet Explorer) and type the TAP-125-U-W-X-Z (YYYYYYYY)'s IP address in the address field. Press **Enter** to establish the connection.

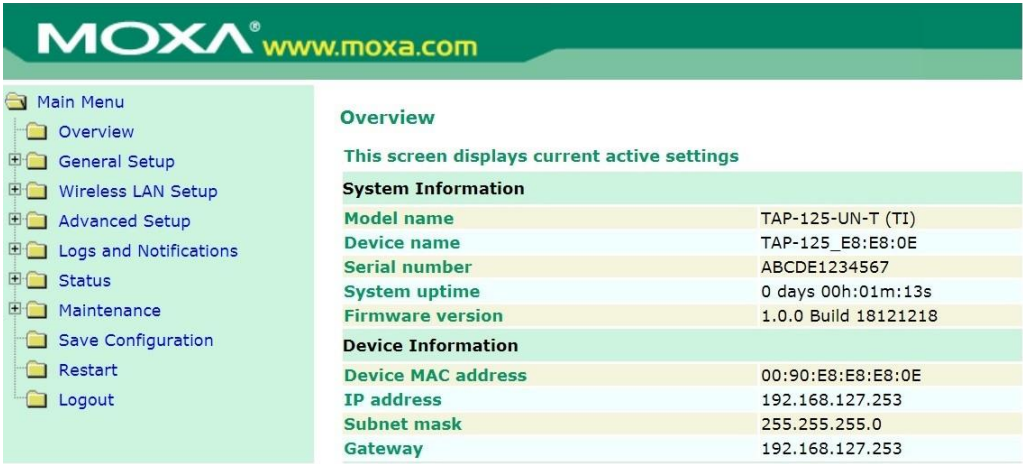


2. The Web Console Login page will open. Enter the password
(Default Username = **admin**; default Password = **moxa**), and then click **Login** to continue.



3. You may need to wait a few moments for the web page to download to your computer. Note that the Model name and IP address of your TAP-125-U-W-X-Z (YYYYYYYY) are both shown in the title bar of the web page. This information can be used to help you identify multiple TAP-125-U-W-X-Z (YYYYYYYY) units.

4. Use the menu tree on the left side of the window to open the function pages to access each of the TAP-125-U-W-X-Z (YYYYYYYY)'s functions.



In the following paragraphs, we describe each TAP-125-U-W-X-Z (YYYYYYYY) management function in detail. A quick overview is available in this manual in the “Function Map” section of Chapter 2.

Overview

The **Overview** page summarizes the TAP-125-U-W-X-Z (YYYYYYYY)'s current status. The information is categorized into several groups: **System info**, **Device info**, and **802.11 info**.

Overview (Warn: Change the default password to ensure a higher level of security)

This screen displays current active settings

System Information			
Model name	TAP-125-UN-T (TI)		
Device name	TAP-125_E8:E8:0E		
Serial number	ABCDE1234567		
System uptime	0 days 00h:02m:10s		
Firmware version	1.0.0 Build 18121218		
Device Information			
Device MAC address	00:90:E8:E8:E8:0E		
IP address	192.168.127.253		
Subnet mask	255.255.255.0		
Gateway	192.168.127.253		
802.11 Information			
Country code	UN		
Operation mode	AP		
Channel	6		48
RF type	B/G/N Mixed		A/N Mixed
Channel width	20MHz		20MHz
SSID	MOXA		MOXA_2

Click on **SSID** for more detailed 802.11 information, as shown in the following figure.

Wireless LAN Status

☒ Auto Update

Show status of WLAN (SSID: MOXA) ▼

802.11 Information	
Operation mode	AP
Channel	6
Channel width	20MHz
RF type	B/G/N Mixed
SSID	MOXA
MAC	06:90:e8:e8:e8:0e
Security mode	OPEN
Current BSSID	06:90:e8:e8:e8:0e
Signal strength	N/A
Signal strength (dBm)	N/A dBm
Noise floor	-105 dBm
SNR	N/A
Transmission Information	
Rate	Auto
Power	12 dBm
Outgoing Packets	
Total sent	239
Packets with error	0
Packets dropped	0
Incoming Packets	
Total received	0
Packets with error	0
Packets dropped	0

NOTE The **802.11 info** that is displayed may be different for different operation modes. For example, "Current BSSID" is not available in Client mode, and "Signal strength" 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-125-U-W-X-Z (YYYYYYYY).

System Info Settings

The **System Info** items, especially **Device name** and **Device description**, are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Info** items makes it easier to identify the different TAP-125-U-W-X-Z (YYYYYYYY) units connected to your network.

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	Factory Default
Max. 31 of characters	This option is useful for specifying the role or application of different TAP-125-U-W-X-Z (YYYYYYYY) units.	TAP-125-UN-CT-T (TI)_<Serial No. of this TAP-125-UN-CT-T (TI)>

Device location

Setting	Description	Factory Default
Max. of 31 characters	Specifies the location of different TAP-125-U-W-X-Z (YYYYYYYY) units.	None

Device description

Setting	Description	Factory Default
Max. of 31 characters	Use this space to record a more detailed description of the TAP-125-U-W-X-Z (YYYYYYYY)	None

Device contact information

Setting	Description	Factory Default
Max. of 31 characters	Provides information about whom to contact in order to resolve problems. Use this space to record contact information of the person responsible for maintaining this TAP-125-U-W-X-Z (YYYYYYYY).	None

Network Settings

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

Network Settings

IP configuration	Static ▼
IP address	DHCP Static 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	The TAP-125-U-W-X-Z (YYYYYYYY)'s IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the TAP-125-U-W-X-Z (YYYYYYYY)'s IP address manually.	

IP address

Setting	Description	Factory Default
TAP-125-UN-CT-T (TI)'s IP address	Identifies the TAP-125-U-W-X-Z (YYYYYYYY) on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
TAP-125-UN-CT-T (TI)'s subnet mask	Identifies the type of network to which the TAP-125-U-W-X-Z (YYYYYYYY) is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Gateway

Setting	Description	Factory Default
TAP-125-UN-CT-T (TI)'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 entering the DNS Server's IP address, you can input the TAP-125-U-W-X-Z (YYYYYYYY)'s URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Time Settings

The TAP-125-U-W-X-Z (YYYYYYYY) has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as Auto warning can add real-time information to the message.

System Time (Updated)

	<div> <div>Date (YYYY/MM/DD)</div> <div>Time (HH:MM:SS)</div> </div>
Current local time	<div> <div>2018 / 12 / 24</div> <div>11 : 11 : 11</div> </div> <div>Set Time</div>
Time protocol	SNTP ▼
Time zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
Daylight saving time	<input type="checkbox"/> Enable
Time server 1	time.nist.gov
Time server 2	
Time sync interval	600 (600~9999 seconds)
	Submit

The **Current local time** shows the TAP-125-U-W-X-Z (YYYYYYYY)'s system time when you open this web page. You can click on the **Set Time** button to activate the updated date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local time settings will be immediately activated in the system without running Save and Restart.

Current local time

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

Time zone

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

**ATTENTION**

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

Daylight saving time

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

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

- **Starts at:** The date that daylight saving time begins.
- **Stops at:** The date that daylight saving time ends.
- **Time offset:** Indicates how many hours forward the clock should be advanced.

Time server 1/2

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

Time sync interval

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

Wireless Settings

The essential settings for wireless networks are presented in this function group. Settings must be properly set before establishing 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-125-U-W-X-Z (YYYYYYY) is configured for **Client** mode, it can be used as an Ethernet-to-wireless (or LAN-to-WLAN) network adaptor. 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.

Basic Wireless Settings

The “WLAN Basic Setting Selection” panel is used to add and edit SSIDs. An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. You can configure your TAP to use up to 9 SSIDs, and configure each SSID differently. All of the SSIDs are active at the same time; that is, client devices can use any of the SSIDs to associate with the access point.

WLAN Basic Setting Selection

Status	SSID	Operation Mode	Action
Active	MOXA	AP	Edit

[Add SSID](#)

Click on **Add SSID** to create more SSIDs.

Click on **Edit** to assign different configuration settings to each SSID. The configuration panel appears as follows:

WLAN 1 Basic WLAN Setup

Operation mode

AP

RF type

B/G/N Mixed ▼

Channel width

20 MHz ▼

Channel

6 ▼

SSID

MOXA

SSID broadcast

☒ Enable ☐ Disable

Client isolation

Client isolation

No isolation ▼

[Submit](#)

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 may operate at a slower speed if when 802.11b clients are on the network	
G/N Mixed	Supports IEEE 802.11g/n standards, but 802.11ac Wave 2 may 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 may operate at a slower speed if 802.11b clients are on the network	
N Only (2.4GHz)	Only supports the 2.4 GHz IEEE 802.11ac Wave 2 standard	
5 GHz		
A	Only supports the IEEE 802.11a standard	
A/N Mixed	Supports IEEE 802.11a/n standards, but 802.11ac Wave 2 may operate at a slower speed if 802.11a clients are on the network	
N Only (5GHz)	Only supports the 5 GHz IEEE 802.11ac Wave 2 standard	
AC	Only supports the 5 GHz IEEE 802.11ac standard	

Channel (for AP mode only)

Setting	Description	Factory Default
Available channels vary with RF type	The TAP-125-U-W-X-Z (YYYYYYY) plays the role of wireless AP.	6 (in B/G/N Mixed mode)

Channel Width (for any 11N RF type only)

Setting	Description	Factory Default
20 MHz	Select your channel width, If you are not sure which option to use, select 20/ 40MHz (Auto)	20 MHz
20/40/80 MHz		

Channel bonding

If 20/40 MHz only is the Channel Width setting, this channel bonding will auto set the channel based on your channel setting.

SSID

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

SSID broadcast

Setting	Description	Factory Default
Enable/ Disable	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 used in server access.

Client isolation**Client isolation**

Isolated within the same subnet ▼

Gateway**Netmask****Allowed subnet with TCP/UDP port**

No	<input type="checkbox"/> Active	IP	Netmask	Protocol	Port
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	All ▼	<input type="text"/> ~ <input type="text"/>

Client Isolation

Setting	Description	Factory Default
No isolation	No isolation is applied.	No isolation
Isolated within the same VAP	All clients associated to this Virtual AP (VAP) 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 "Isolated within the same subnet" is selected. Gateway and netmask are used to define the network in which wireless clients will be isolated from each other.	None

Netmask

Setting	Description	Factory Default
Netmask for client isolation function	This setting is used when "Isolated within the same subnet" is selected. Gateway and netmask are used to define the network in which wireless clients will be isolated from each other.	None

"Allowed subnet with TCP/UDP port" settings are used to define the exception subnets (or hosts) when "Isolated within the same subnet" is selected. Up to eight subnets or hosts can be defined.

Active

Setting	Description	Factory Default
Enable/Disable	This checkbox enables or disables the rule for allowed subnet settings.	Disable

IP

Setting	Description	Factory Default
IP address for allowed subnet definition	The IP address of the 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
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
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
Port for 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

WLAN Security Settings

The TAP-125-U-W-X-Z (YYYYYYY) 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-125-U-W-X-Z (YYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) 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

TKIP

AES

Mixed

3000

Key renewal

(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.	

Passphrase

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

Key renewal

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

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

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 type
 Encryption method
 Primary RADIUS server IP
 Primary RADIUS server port
 Primary RADIUS shared key
 Secondary RADIUS server IP
 Secondary RADIUS server port
 Secondary RADIUS shared key
 Key renewal (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.	

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)

Advanced Wireless Settings

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

Advanced WLAN Settings

Guard interval	800ns ▼
Maximum transmission power	12 dBm (-1 dBm/MHz) ▼
Beacon interval	100 (40~1000ms)
DTIM interval	1 (1~15)
RTS threshold	2346 (256~2346)
Antenna	4x4 ABCD ▼
WMM	Enable ▼

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.

Beacon Interval

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

DTIM Interval

Setting	Description	Factory Default
Data Beacon Rate (1 to 15)	Indicates how often the TAP-125-U-W-X-Z (YYYYYYYY) sends out a Delivery Traffic Indication Message	1

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

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

Advanced Settings

Several advanced functions are available to increase the functionality of your TAP-125-U-W-X-Z (YYYYYYYY) 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.

Using Virtual LAN

Setting up Virtual LANs (VLANs) on your device 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

Management VLAN ID:

Port	PVID	VLAN Tagged (Use commas to separate VLAN tags)
LAN	<input type="text" value="1"/>	<input type="text"/>
MOXA (WLAN 1)	<input type="text" value="1"/>	<input type="text"/>
MOXA_2 (WLAN 2)	<input type="text" value="1"/>	<input type="text"/>

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-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) 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	<input type="text"/>
Subnet mask	<input type="text"/>
Primary DNS server	<input type="text"/>
Secondary DNS server	<input type="text"/>
Start IP address	<input type="text"/>
Maximum number of users	<input type="text"/>
Client lease time	10 (1~10 days)

Static DHCP mapping

No	<input type="checkbox"/> Active	IP Address	MAC Address
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

DHCP server

Setting	Description	Factory Default
Enable	Enables TAP-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY)'s MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The TAP-125-U-W-X-Z (YYYYYYYY) provides 8 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the

MAC Filters

Enable

Policy

No	<input type="checkbox"/> Active	Name	MAC address
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

setting.

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-125-U-W-X-Z (YYYYYYYY)'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-125-U-W-X-Z (YYYYYYYY) 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

Policy

No	<input type="checkbox"/> Active	Protocol	Source IP	Source netmask	Destination IP	Destination netmask
1	<input type="checkbox"/>	All	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	All	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	All	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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-125-U-W-X-Z (YYYYYYYY)'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-125-U-W-X-Z (YYYYYYY) 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

Policy

No	<input type="checkbox"/> Active	Source port	Destination port	Protocol	Application name
1	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>

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**

SNMP Agent

The TAP-125-U-W-X-Z (YYYYYYY) 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-125-U-W-X-Z (YYYYYYY)’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-125-U-W-X-Z (YYYYYYY) 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

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
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

SNMP agent

Remote management

Read community

Write community

SNMP agent version

Admin authentication type

Authentication username

Admin encryption method

Private key

Private MIB information

Device object ID

SNMP agent

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 access all objects with read/write permissions using this community string.	private

SNMP agent version

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

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

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

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

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

Private key

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

Private MIB Information Device Object ID

Also known as **OID**. This is the TAP-125-U-W-X-Z (YYYYYYYY)'s enterprise value. It is fixed.

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-125-U-W-X-Z (YYYYYYYY) 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 logging** to enable the grouped events. All default values are enabled (checked). The log for system events can be seen in **Status** → **System Logs**.

System Log Event Types

Event Type	<input type="checkbox"/> Enable Logging
System-related events	<input checked="" type="checkbox"/> Active
Network-related events	<input checked="" type="checkbox"/> Active
Configuration-related events	<input checked="" type="checkbox"/> Active

System-related events	Event is triggered when...
System restart (warm start)	The TAP-125-U-W-X-Z (YYYYYYYY) 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	A wireless client is associated or disassociated.
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-125-U-W-X-Z (YYYYYYYY).
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The TAP-125-U-W-X-Z (YYYYYYYY)'s firmware is updated.

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 Type	<input type="checkbox"/> Enable Logging
System-related events	<input checked="" type="checkbox"/> Active
Network-related events	<input checked="" type="checkbox"/> Active
Configuration-related events	<input checked="" type="checkbox"/> Active

Syslog Server Settings

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

Syslog Server Settings

Syslog server 1	<input type="text"/>
Syslog port	<input type="text" value="514"/>
Syslog server 2	<input type="text"/>
Syslog port	<input type="text" value="514"/>
Syslog server 3	<input type="text"/>
Syslog port	<input type="text" value="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 **Enable Notification** 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.

Notification Event Types

Event Type	<input type="checkbox"/> Enable Notification
Cold start	<input type="checkbox"/> Active
Warm start	<input type="checkbox"/> Active
Power 1 transition (On-->Off)	<input type="checkbox"/> Active
Power 1 transition (Off-->On)	<input type="checkbox"/> Active
Configuration changed	<input type="checkbox"/> Active
Console authentication failure	<input type="checkbox"/> Active
LAN link on	<input type="checkbox"/> Active
LAN link off	<input type="checkbox"/> Active

E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the TAP-125-U-W-X-Z (YYYYYYYY). 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)	<input type="text"/>
User name	<input type="text"/>
Password	<input type="password"/>
From e-mail address	<input type="text"/>
To e-mail address 1	<input type="text"/>
To e-mail address 2	<input type="text"/>
To e-mail address 3	<input type="text"/>
To e-mail address 4	<input type="text"/>

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

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 Type	<input type="checkbox"/> Enable Notification
Cold start	<input type="checkbox"/> Active
Warm start	<input type="checkbox"/> Active
Power 1 transition (On-->Off)	<input type="checkbox"/> Active
Power 1 transition (Off-->On)	<input type="checkbox"/> Active
Configuration changed	<input type="checkbox"/> Active
Console authentication failure	<input type="checkbox"/> Active
LAN link on	<input type="checkbox"/> Active
LAN link off	<input type="checkbox"/> Active

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	<input type="button" value="V1"/>
1st Trap server IP/name	<input type="button" value="V1"/> <input type="button" value="V2"/>
1st Trap community	<input type="text" value="alert"/>
2nd Trap version	<input type="button" value="V1"/>
2nd Trap server IP/name	<input type="text"/>
2nd Trap community	<input type="text" value="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

System Status

The system status page displays the device information of the TAP. The system displays the CPU utilization information in real-time to monitor the usage of the system processor.

System Status

Memory Info	
Total (kB)	898540
Used (kB)	117288
Free (kB)	616568
CPU Info	
Usage (%)	1.74

Refresh

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.

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 mode only)

Associated Client List shows all the clients that are currently associated to a particular TAP-125-U-W-X-Z (YYYYYYYY). 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>
----	---------------------

[Select all](#)[Refresh](#)

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

[Select all](#)[Refresh](#)

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

[Cut](#)
[Copy](#)
[Paste](#)
[Select All](#)
[Print](#)

[Select all](#)[Refresh](#)

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
```

[Export Log](#)
[Clear Log](#)
[Refresh](#)

Maintenance

Maintenance functions provide the administrator with tools to manage the TAP-125-U-W-X-Z (YYYYYYYY) 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

Auto logout period (1~60 minutes)

Accessible Interfaces

Interface	HTTP	HTTPS	Telnet	SSH	SNMP	Moxa Service
Enable services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ethernet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

* If you disable all access portals, you will not be able to remotely access this device.

* If you disable HTTPS, some Moxa service features will be disabled.

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

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-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) 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-125-U-W-X-Z (YYYYYYYY) will reboot itself.

When upgrading your firmware, the TAP-125-U-W-X-Z (YYYYYYYY)'s other functions are forbidden.

Firmware Upgrade

Select update image



ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your TAP-125-U-W-X-Z (YYYYYYYY).

Config Import Export

You can back up or restore the TAP-125-U-W-X-Z (YYYYYYYY)'s configuration with **Config Import Export**.

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

Configuration Export

Export Configuration

SNMP MIB file for TAP-125-U-W-X-Z (YYYYYYYY) is embedded in the device. To export the MIB file, simply click on the "MIB Export" button and save it to your local drive.

SNMP MIB file Export

MIB Export

Load Factory Default

Use this function to reset the TAP-125-U-W-X-Z (YYYYYYYY) and roll all settings back to the factory or customized default values.

Load Factory Default

Reset to Factory Default Values

Click "**System Reset**" to reset all system settings, including the console password, to factory default values.

The system will be restarted immediately after the reset to factory default values.

System Reset

Password

You can change the administration password for each of the TAP-125-U-W-X-Z (YYYYYYYY)'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 **moxa**, and remember to change the administration password regularly.

NOTE The default password is `root`.

Password

Current password

....

New password

.....

Confirm password

.....

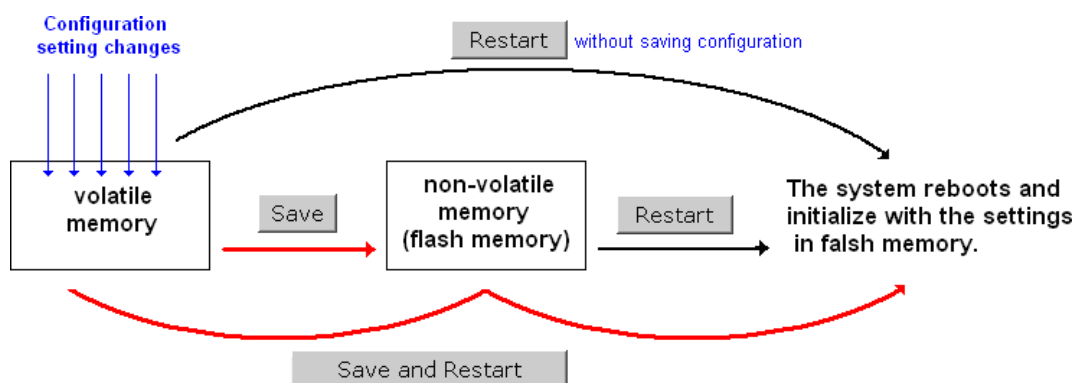
Submit

Save Configuration

The following figure shows how the TAP-125-U-W-X-Z (YYYYYYYY) stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the TAP-125-U-W-X-Z (YYYYYYYY) is

shutdown or rebooted unless they are **y**. Because the TAP-125-U-W-X-Z (YYYYYYYY) starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the TAP-125-U-W-X-Z (YYYYYYYY).

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



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

Save Configuration (All Configuration Settings Saved)

You must save the changes and restart the system for configuration changes to take effect. Click **Save** to save configuration changes to the system memory.

Save

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-125-U-W-X-Z (YYYYYYYY) directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the TAP-125-U-W-X-Z (YYYYYYYY).

Restart

!!! Warning !!!

Click **Restart** to discard configuration changes and restart the system.

Click **Save and Restart** to save configuration changes and restart the system.

Restart

Save and Restart

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.

Restart

!!! Warning !!!

The system will restart immediately after you click Restart. All Ethernet connections will be disconnected.

Restart

You will not be able to run any of the TAP-125-U-W-X-Z (YYYYYYY)'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.

Logout

Other Console Considerations

This chapter explains how to access the TAP-125-U-W-X-Z (YYYYYYYY) for the first time. In addition to HTTP access, there are four ways to access TAP-125-U-W-X-Z (YYYYYYYY): 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-125-U-W-X-Z (YYYYYYYY) to a PC's COM port, can be used if you do not know the TAP-125-U-W-X-Z (YYYYYYYY)'s IP address. The other consoles can be used to access the TAP-125-U-W-X-Z (YYYYYYYY) over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

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

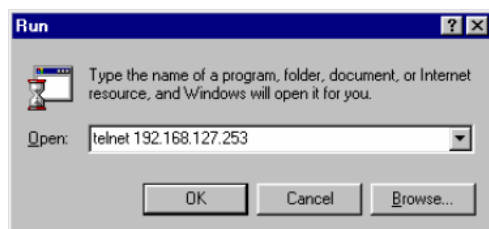
Configuration by Telnet and SSH Consoles

You may use Telnet or SSH client to access the TAP-125-U-W-X-Z (YYYYYYYY) and manage the console over a network. To access the TAP-125-U-W-X-Z (YYYYYYYY)'s functions over the network from a PC host that is connected to the same LAN as the TAP-125-U-W-X-Z (YYYYYYYY), you need to make sure that the PC host and the TAP-125-U-W-X-Z (YYYYYYYY) are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

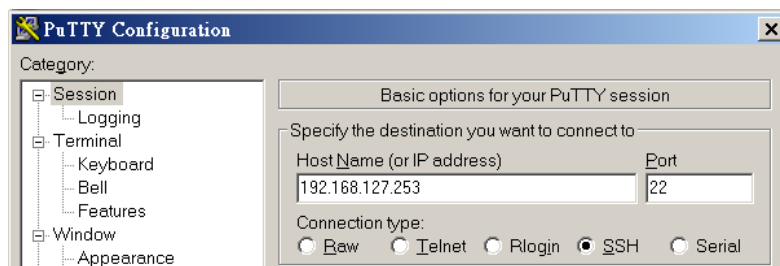
NOTE The TAP-125-U-W-X-Z (YYYYYYYY)'s default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet 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-125-U-W-X-Z (YYYYYYYY)'s IP address from the Windows Run window (you may also issue the telnet command from the MS-DOS prompt).



2. When using SSH client (ex. PuTTY), please run the client program (ex. putty.exe) and then input the TAP-125-U-W-X-Z (YYYYYYYY)'s IP address, specifying **22** for the SSH connection port.



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

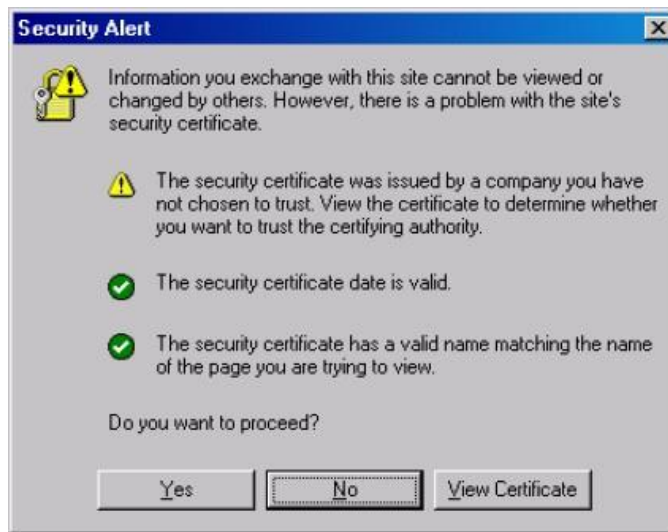
To secure your HTTP access, the TAP-125-U-W-X-Z (YYYYYYYY) supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the TAP-125-U-W-X-Z (YYYYYYYY)'s web browser interface via HTTPS/SSL.

1. Open your web browser and type `https://<TAP-125-U-W-X-Z (YYYYYYYY)'s IP address>` in the address field. Press

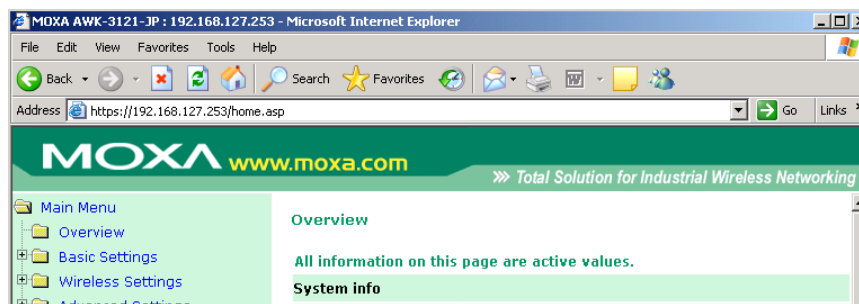
Enter to establish the connection.



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



- Select **Yes** to accept the certificate issued by Moxa IW and then enter the TAP-125-U-W-X-Z (YYYYYYYY)'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-125-U-W-X-Z (YYYYYYYY)'s functions.



Disabling Telnet and Browser Access

If you are connecting the TAP-125-U-W-X-Z (YYYYYYYY) 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

Auto logout period (1~60 minutes)

Accessible Interfaces

Interface	HTTP	HTTPS	Telnet	SSH	SNMP	Moxa Service
Enable services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ethernet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

* If you disable all access portals, you will not be able to remotely access this device.

* If you disable HTTPS, some Moxa service features will be disabled.

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your TAP-125-U-W-X-Z (YYYYYYY) and plan your industrial wireless network better.

The following topics are covered in this appendix:

- ❑ **Beacon**
- ❑ **DTIM**

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.

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 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.

IMPORTANT NOTE:

This device or equipment is restricted to mobile configuration. To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 70 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. This transmitter module must not be co-located or operating in conjunction with any other antenna or transmitter.

This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

The device for operation in the band 5150–5250 MHz is only for indoor use.

External antenna Use only the identical model number antennas that have been approved by the applicant. It should be noted that various model number of antennas cannot be mixed-use. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC/IC limit and is prohibited.

Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

- 1) This device is intended for OEM integrators only.
- 2) Please see the full Grant of Equipment document for other restrictions.

This device or equipment FCC ID: SLE-WAPN010 \ FCCID: SLE-WAPC002 has been approved by FCC to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna List:

No.	Manufacturer	Part No.	Antenna Type	Peak Gain
1	MOXA	MAT-WDB-PA-NF-2-0708	Panel	7.63dBi for 2.4GHz 8.77dBi for 5.15~5.25GHz 8.77dBi for 5.25~5.35GHz 8.50dBi for 5.47~5.725GHz 8.18dBi for 5.725~5.825GHz
2	MOXA	WI25-A1-0810012-RG316	Panel	8.5dBi for 2.4GHz 10.5dBi for 5GHz
3	MOXA	ANT-WSB-PNF-12	Panel	12dBi for 2.4GHz
4	MOXA	ANT-WDB-PNF-1518	Panel	15dBi for 2.4GHz 18dBi for 5GHz
5	MOXA	MI05-A1-XX23037-X0	Panel	23dBi for 5GHz
6	MOXA	MI05-A1-XX16020-X0	Panel	12dBi for 5GHz
7	MOXA	ANT-WSB5-PNF-18	Panel	18dBi for 2.4GHz 18dBi for 5GHz
8	MOXA	ANT-WSB-AHRM-05-1.5m BK	Omni-directional	1.51dBi for 2.4GHz
9	MOXA	ANT-WSB-ANF-09	Omni-directional	9.0dBi for 2.4GHz
10	MOXA	MAT-WDB-CA-RM-2-0205	Omni-directional	2.5dBi for 2.4GHz 5.0dBi for 5.15~5.25GHz 5.7dBi for 5.25~5.35GHz 4.9dBi for 5.47~5.725GHz 5.2dBi for 5.725~5.825GHz
11	MOXA	MAT-WDB-DA-RM-2-0203-1m	Omni-directional	2.43dBi for 2.4GHz 3.80dBi for 5.15~5.25GHz 2.72dBi for 5.25~5.35GHz 2.26dBi for 5.47~5.725GHz 2.34dBi for 5.725~5.825GHz
12	MOXA	ANT-WDB-ANM-0306	Omni-directional	3.8dBi for 2.4GHz 5.7dBi for 5.15~5.25GHz 5.7dBi for 5.25~5.35GHz 6.3dBi for 5.47~5.725GHz 6.3dBi for 5.725~5.825GHz
13	MOXA	ANT-WDB-ARM-0202	Omni-directional	1.8dBi for 2.4GHz 1.8dBi for 5GHz
14	MOXA	ANT-WDB-ARM-02	Omni-directional	2.04dBi for 2.4GHz 0.81dBi for 5GHz
15	MOXA	ANT-WDB-ANM-0502	Omni-directional	4.62dBi for 2.4GHz 2.0dBi for 5GHz
16	MOXA	ANT-WDB-ANM-0407	Omni-directional	4.0dBi for 2.4GHz 7.0dBi for 5GHz
17	MOXA	ANT-WDB-ANF-0609	Omni-directional	6.0dBi for 2.4GHz 9.0dBi for 5GHz
18	MOXA	ANT-WDB-ANM-0609	Omni-directional	6.0dBi for 2.4GHz 9.0dBi for 5GHz
19	MOXA	ANT-WSB5-ANF-12	Omni-directional	12dBi for 5GHz
20	MOXA	MHH-A11-XX110170-X0	Railway	9.0dBi for 2.4GHz 8.0dBi for 5GHz
21	MOXA	WI25-A1-1215053-X0	Sector	12dBi for 2.4GHz 15dBi for 5GHz
22	MOXA	TOP 200 AMR MF-05-4	Patch	8.2dBi for 2.4GHz 8.5dBi for 5GHz