



Industrial 2-Channel 4 Ports MACsec Gigabit Switch

User Manual

Firmware Version A1.0.11

Models Covered by This Manual: RPT-E2004G/E2004G-2F/E2004G-F-T-X2

Subject Link Inc

www.sbjlink.com

sales@sbjlink.com

Content

Overview	3
Basic Settings	
System	6
IPv4 Settings	7
System Time	9
Speed Configuration	11
Security	
Service Control	12
MACSec Configuration.....	14
SSH.....	22
Diagnostics	
Ping.....	24
Monitoring	
System Warning	26
Maintenance	
Authorization.....	29
Firmware Upgrade.....	31
Config Backup.....	34
Config Restore	35
Command Line Interface	
Connect to CLI via Console Port.....	36
Connect to CLI via Telnet	37
Command Groups.....	43

Overview

CONFIGURATION VIA WEB CONSOLE

1. Open the web browser. We recommend using "Google Chrome".

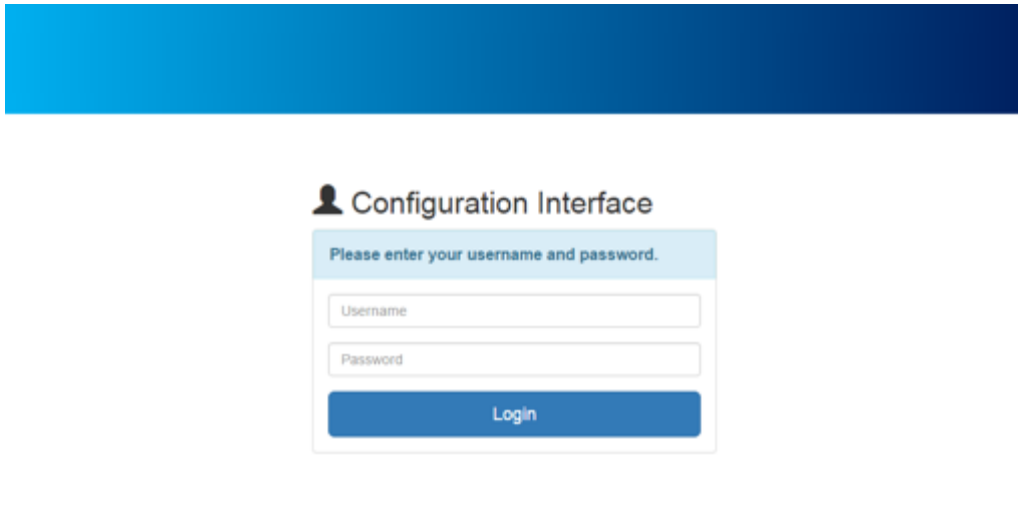
Note: If IE is used, make sure the version is more than **IE 11**.

2. Enter the **IP Address** in the **URL** field to connect to the switch and click "Enter" key.

Note: The default IP Address is "**192.168.10.1**" and the HTTP Service is default disabled. Please use **HTTPS** to connect to the WEB GUI before enabling HTTP Service.



The **Login Page** is displayed.




3. Enter the **Username** and **Password**, and click "**Login**" Button to login to the system.

Note: The default Username and Password is **admin / admin**.




If users use the **default password** to log in the system, the system will redirect to the Update Authorization page to remind users to change password for security purpose.


Update Authorization




Basic Settings

 **Admin**

Please Change the Default Password to Improve the System Security.

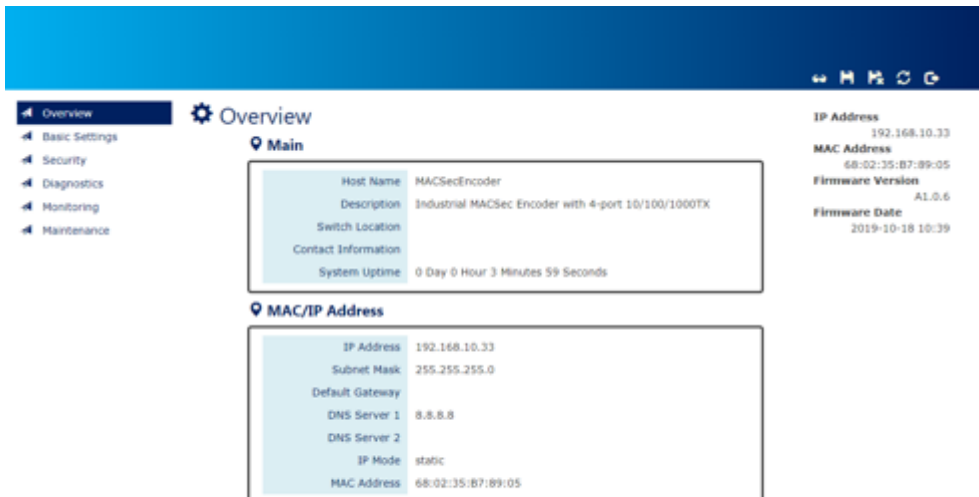
Username	<input type="text" value="admin"/>	
Password	<input type="password"/>	
Confirm Password	<input type="password"/>	

 **Read-only**

Username	<input type="text"/>	
Password	<input type="password"/>	
Confirm Password	<input type="password"/>	

[Apply](#)

After logging into the system with modified password, the "**Overview**" page is displayed.



The screenshot shows the "Overview" page of the system. The page has a dark blue header with navigation icons. On the left, there is a sidebar menu with options: Overview (selected), Basic Settings, Security, Diagnostics, Monitoring, and Maintenance. The main content area is titled "Overview" and contains two sections:

- Main**: A box containing system information:

Host Name	MACSecEncoder
Description	Industrial MACSec Encoder with 4-port 10/100/1000TX
Switch Location	
Contact Information	
System Uptime	0 Day 0 Hour 3 Minutes 59 Seconds
- MAC/IP Address**: A box containing network configuration:

IP Address	192.168.10.33
Subnet Mask	255.255.255.0
Default Gateway	
DNS Server 1	8.8.8.8
DNS Server 2	
IP Mode	static
MAC Address	68:02:35:B7:89:05

On the right side of the page, there is a summary of key information:

- IP Address**: 192.168.10.33
- MAC Address**: 68:02:35:B7:89:05
- Firmware Version**: A1.0.6
- Firmware Date**: 2019-10-18 10:39

GLOBAL FUNCTIONS

Five global functions are provided in the header field.

1.  [Hide/Show Model Information](#)

When a low-resolution environment is used to configure the system via the web console, the "Model Information" field can be hidden to have a better view.

2.  [Save Configuration](#)

After configuring, click the icon to save the configurations to the "**startup-config**" file. The configurations are retained in the system until a factory reset default is done.

3.  [Restore Factory Default](#)

Removes the configurations saved in the system. After restoring factory default, all the settings will be set to default values.

4.  [Reboot System](#)

Reboots the device and restarts the system.

5.  [System Logout](#)

This option enables you to sign out from the system. Users have to login again if they want to configure the settings.





The system will **auto-logout** after the "timeout" timer expires. The "timeout" timer is configured in the CLI mode by using the "exec-timeout" command.

The maximum value of the timer in the web console is **30 mins**.

System

CONFIGURE SYSTEM INFORMATION

System Information

System Name	<input type="text" value="Switch"/>	
System Description	<input type="text" value="Industrial Ethernet Switch with 8-port 10/"/>	
System Location	<input type="text"/>	
System Contact	<input type="text"/>	

Apply

For more information, hover the mouse over the  icon in the system.

- **Host Name**
It is useful to identify the difference between the switches, for example: CoreSwitch01.
The **max. length** for the Host Name is **32 characters**.
Note: #, \, ', ", ? are **invalid** characters.
- **System Description**
The System Description is default defined by the system.
It contains the copper port number, fiber port number, and PoE information (if supported).
The **max. length** for the System Description is **68 characters**.
Note: #, \, ', ", ? are **invalid** characters.
- **Switch Location**
It is useful to find the location of the switches, for example: Area01.
The **max. length** for the Switch Location is **32 characters**.
Note: #, \, ', ", ? are **invalid** characters.
- **Contact Information**
Records the information of the person responsible for this device and also the contact details.
Note: #, \, ', ", ? are **invalid** characters.
- **Apply** (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

IPv4 Settings

Internet Protocol Version 4 (IPv4) is the fourth version of the Internet Protocol. It is used on the packet-switched networks and with connectionless communication. IPv4 has four bytes (32 bits) address and the address space is limited to 4,294,967,296 (2^{32}) unique addresses. On the local area network (LAN), the “Private Network” is used. It starts from **192.168.0.0** and the address space contains 65,025 (2^{16}) IP addresses. The frames can only be sent to the host in the same subnet. For example, the default IP Address of the switch is “192.168.10.1”. When the users want to connect to the web console of the switch, an IP address from “192.168.10.2” to “192.168.10.254” must be assigned to the host.

CONFIGURE IPv4 INFORMATION

IPv4 Settings

IPv4 Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP Client
IP Address	<input type="text" value="192.168.10.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>
DNS Server	<input type="text" value="8.8.8.8"/>

[Apply](#)

- **IPv4 Mode**
There are 2 ways to configure IPv4 address - one is to configure a **static** IP address manually and another one is to get an IP address by **DHCP**.
If the IPv4 mode is "**DHCP Client**", IPv4 information fields will be set to "**Disabled**".
- **IP Address**
Assigns a unique static IP Address in the subnet to access the system.
The default IP Address is "**192.168.10.1**".
- **Subnet Mask**
Defines the type of network, to which this device is connected to.
The default Subnet Mask is "**255.255.255.0**".

- [Default Gateway](#)

The IP address of the router used to connect a LAN to a WAN.

- [DNS Server](#)

Specifies the IP address of the DNS Server so that the users can connect to another device based on the **URL** instead of the IP address.

The default DNS Server is "**8.8.8.8**". It is provided by Google.

-  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

System Time

The **System Time** represents the date and time. The system uptime defines the passing time after the system boots up. There is no battery on the switch and hence the system time cannot be saved in the system. Users can configure the time zone and system time manually by synchronizing the time with the browser or by enabling the “**NTP**” service to get the time from a **NTP Server**.

NTP

Network Time Protocol (NTP) is a clock synchronization protocol, which is used to synchronize the system time with the NTP server. NTP is one of the oldest Internet Protocols in use from 1985 until now. It works based on a client-server model, but it can also be used in peer-to-peer relationships. The NTP application on the switch follows the client-server model and the switch plays a role in the NTP Client.

CONFIGURE SYSTEM TIME INFORMATION

System Time

System Time Information

Current Time	1970/01/01 00:05:52
System Uptime	0 Day 0 Hour 5 Minutes 47 Seconds


NTP Settings

NTP Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
NTP Server	<input type="text" value="2.pool.ntp.org"/>

Manual Time Settings

Time Zone	Europe <input type="text" value="Europe"/> <input type="text" value="London"/>
Date Selector	<input type="text" value="1970/01/01"/>
Time Setting	<input type="text" value="00"/> : <input type="text" value="05"/> : <input type="text" value="47"/>
Sync with Browser	<input type="checkbox"/> 2016/11/9 18:27:47

Apply

- **System Time Information**
 - Current Time: The current date time of the system.
 - System Uptime: The system boot up duration.
- **NTP Settings**
 - NTP Mode
"Enable" or "Disable" NTP Service. If NTP Mode is enabled, the system will sync time with NTP Server on an hourly basis.
 - NTP Server
This field displays the URL or the IP address of the host that provides the NTP Service.
- **Manual Time Settings**
 - Time Zone
Select the Time Zone to define the local time offset from GMT.
 - Date Selector
Select the system date manually. The format is "**year/month/day**".
 - Time Setting
Define the system time manually. The format is "**hour:minute:second**".
 - Sync with Browser
Select the checkbox to synchronize the system time with the **browser time**.
-  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

Speed Configuration

CONFIGURE SPEED

Speed Configuration

No.	Speed
Channel 1	1000M ▼
Channel 2	1000M ▼

Apply

- **No.**
There are 2 channels on the MACSec device and there are 2 ports in each channel, one is for encryption and the other is for decryption.
- **Speed**
The speed field is to configure the speed for each channel. The ports in the same channel must work with the same speed.
For the **RPT-E2004G**, there is **10/100/1000M** supported.
For the **RPT-E2004G-2F** and **RPT-E2004G-4F**, there is only **100/1000M** supported because of the fiber interface.
Note: The **Auto** mode must be enabled on the 1000M speed if users connect the MACSec device to another device that support configuring **negotiation** mode.

Service Control

We provide 5 types of interface which are **HTTP**, **HTTPS**, **SSH**, **Telnet**, and **Console Port** to access the management interface of the switch. Users can configure the authority for each type of service to be enabled or disabled. The HTTP and Telnet services are default disabled for security. Other services are enabled by default and users can disable unused service to make the system more secure.

CONFIGURE SERVICE CONTROL INFORMATION

Service Control

HTTP	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
HTTPS	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
SSH	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Telnet	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Console	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

[Apply](#)

- [HTTP](#)
Enable or Disable to access management interface by **HTTP** which is the foundation of data communication for the **World Wide Web (WWW)**.
- [HTTPS](#)
Enable or Disable to access management interface by **HTTPS** which is an adaptation of HTTP for security. The communication will be **encrypted** in HTTPS.
- [SSH](#)
Enable or Disable to access management interface by **SSH**, which is a **cryptographic network** protocol. SSH provides a **secure channel** over an unsecured network in the client-server architecture. The switch plays the role of SSH server and hosts plays the role of SSH client.
- [Telnet](#)
Enable or Disable to access management interface by **Telnet** which is a **text-oriented** virtual terminal connection. It's less secure than SSH because it doesn't encrypt any data even password when the data is transmitting.
- [Console](#)
Enable or Disable to access management interface by **Serial Console Port**. Disable the Console Port can avoid the misconfiguration by someone who can access the device on-site.

-  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

MACSec Configuration



Media Access Control Security (MACSec) is an IEEE standard known as IEEE802.1AE. Devices with MACSec function provide traffic encryption with high throughput on Ethernet links and ensure the point-to-point security between directly connected nodes.

There are 2 terms defined by MACSec, which are secure channel and connectivity association. The secure channel is bidirectional for transmitting or receiving data. We called the transmitting channel as **outbound traffic** and the receiving channel as **inbound traffic**.

WE SUPPORT STATIC ASSOCIATION KEY (SAK) SECURITY MODE FOR ENCRYPTION. THE BOTH SIDE OF THE CONNECTION USE THE SAME KEY WHICH IS MANUALLY CONFIGURED BY USERS TO ENCRYPT THE TRAFFIC. IT IS RECOMMENDED TO CHANGE THE STATIC KEY PERIODICALLY TO PREVENT THE KEY FROM BRUTE-FORCE ATTACK. THIS IS IN LINE WITH CURRENT GOOD SECURITY PRACTICE.

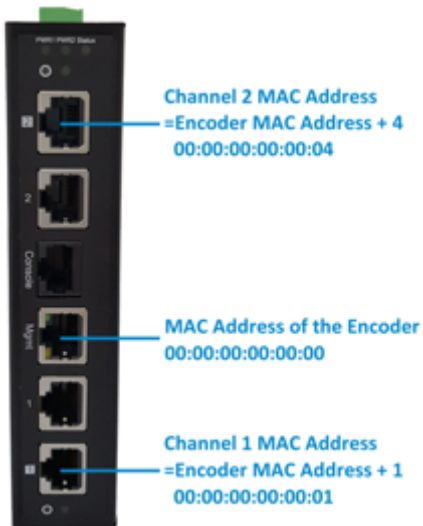
CONFIGURE MACSEC

MACSec Configuration

Channel	Enabled	Peer MAC Address 	SAK 
1	<input type="checkbox"/> Enable	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/> Enable	<input type="text"/>	<input type="text"/>

For more information, hover the mouse over the  icon in the system.

- **Channel**
There are 2 security channels supported.
- **Enabled**
“Enable” or “Disable” MACSec function on the specific channel.
- **Peer MAC Address**
The MAC Address of the connected device is the identifier of this link. For this device, users have to fill in the MAC Address of the connected port on the other side. For the device on the other side, users have to fill in the MAC Address of this port.
The MAC Address of the switch is displayed **on the right side of the WEB GUI**, and the MAC Address of the encryption port of each channel is shown as the following table.
For counting the MAC Addresses of each encryption port, please refer to the following table.



Item	MAC Address	Description
MACSec Encoder	00:00:00:00:00:00 0	
Channel 1 Encryption Port	00:00:00:00:00:00 1	MAC Address of Switch + 1
Channel 2 Encryption Port	00:00:00:00:00:00 4	MAC Address of Switch + 4

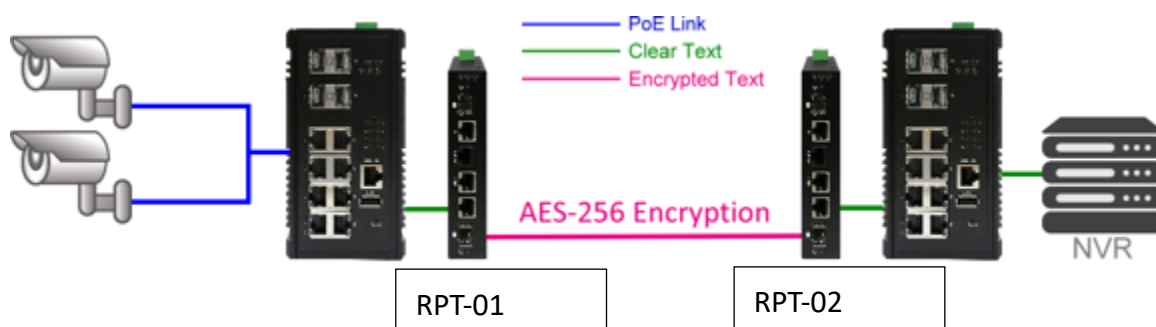
- **SAK (Secure Association Key)**

The SAK is a manually configured key and the SAK for both connected sides must be configured to the same one.

Note: SAK is a **32-digit hexadecimal** number. The remaining digits of SAK will be configured to 0 if the SAK is configured less than 32-digit.

The default SAK is **blank**.

MACSEC EXAMPLE – BASIC APPLICATION



Item	Value
MAC Address of RPT-01	68:02:35:FF:FE:FF
MAC Address of port 1 on RPT-01	68:02:35:FF:FF:00
MAC Address of RPT-02	68:02:35:FF:FF:09
MAC Address of port 1 on RPT-02	68:02:35:FF:FF:10
Configuration for RPT-01	
Peer MAC Address	68:02:35:FF:FF:10
SAK	98959578066987793539674551386204
Configuration for RPT-02	
Peer MAC Address	68:02:35:FF:FF:00
SAK	98959578066987793539674551386204

⚙️ MACSec Configuration

Channel	Enabled	Peer MAC Address ?	SAK ?
1	<input checked="" type="checkbox"/> Enable	68:02:35:FF:FF:10	98959578066987793539674551:
2	<input type="checkbox"/> Enable		

Apply

Configuration for RPT-01

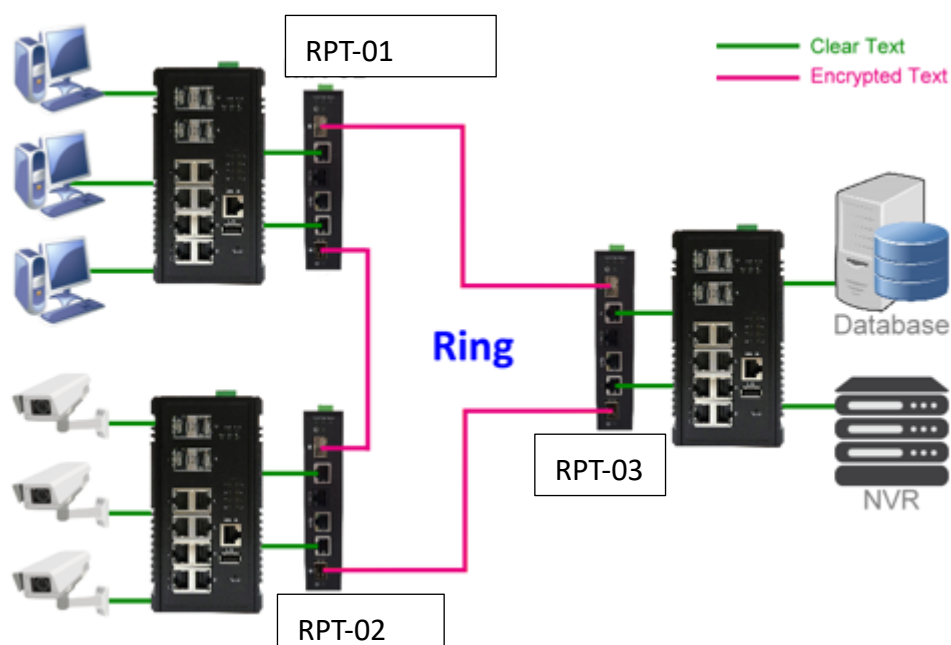
⚙️ MACSec Configuration

Channel	Enabled	Peer MAC Address ?	SAK ?
1	<input checked="" type="checkbox"/> Enable	68:02:35:FF:FF:00	98959578066987793539674551:
2	<input type="checkbox"/> Enable		

Apply

Configuration for RPT-02



MACSEC EXAMPLE – RING TOPOLOGY



Item	Value
MAC Address of RPT-01	68:02:35:FF:AA:00
MAC Address of port 1 on RPT-01	68:02:35:FF:AA:01
MAC Address of port 2 on RPT-01	68:02:35:FF:AA:04
MAC Address of RPT-02	68:02:35:FF:BB:00
MAC Address of port 1 on RPT-02	68:02:35:FF:BB:01
MAC Address of port 2 on RPT-02	68:02:35:FF:BB:04
MAC Address of RPT-03	68:02:35:FF:CC:00
MAC Address of port 1 on RPT-03	68:02:35:FF:CC:01
MAC Address of port 2 on RPT-03	68:02:35:FF:CC:04
Configuration for RPT-01	
Peer MAC Address (CH1)	68:02:35:FF:BB:04
SAK (CH1)	ABCDEF0123456789ABCDEF0123456789
Peer MAC Address (CH2)	68:02:35:FF:CC:04
SAK (CH2)	9876543210FEDCBA9876543210FEDCBA
Configuration for RPT-02	
Peer MAC Address (CH1)	68:02:35:FF:CC:01
SAK (CH1)	F01A23B45C67D89EF01A23B45C67D89E
Peer MAC Address (CH2)	68:02:35:FF:AA:01
SAK (CH2)	ABCDEF0123456789ABCDEF0123456789
Configuration for RPT-03	
Peer MAC Address (CH1)	68:02:35:FF:BB:01

SAK (CH1)	F01A23B45C67D89EF01A23B45C67D89E
Peer MAC Address (CH2)	68:02:35:FF:AA:04
SAK (CH2)	9876543210FEDCBA9876543210FEDCBA



MACSec Configuration

Channel	Enabled	Peer MAC Address 	SAK 
1	<input checked="" type="checkbox"/> Enable	68:02:35:FF:BB:04	ABCDEF0123456789ABCDEF0123
2	<input checked="" type="checkbox"/> Enable	68:02:35:FF:CC:04	9876543210FEDCBA9876543210

Apply

Configuration for RPT-01



MACSec Configuration

Channel	Enabled	Peer MAC Address 	SAK 
1	<input checked="" type="checkbox"/> Enable	68:02:35:FF:CC:01	F01A23B45C67D89EF01A23B45C
2	<input checked="" type="checkbox"/> Enable	68:02:35:FF:AA:01	ABCDEF0123456789ABCDEF0123

Apply

Configuration for RPT-02

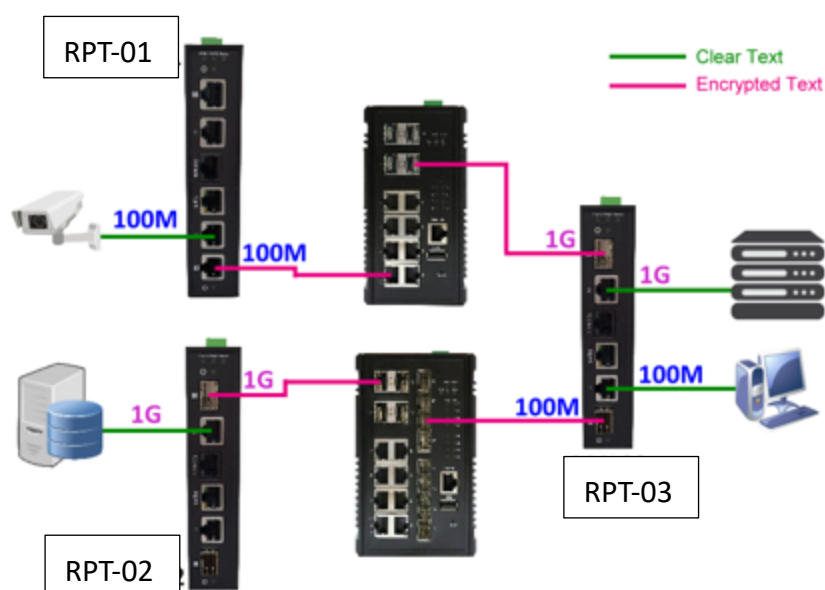
MACSec Configuration

Channel	Enabled	Peer MAC Address 	SAK 
1	<input checked="" type="checkbox"/> Enable	68:02:35:FF:BB:01	F01A23B45C67D89EF01A23B45C
2	<input checked="" type="checkbox"/> Enable	68:02:35:FF:AA:04	9876543210FEDCBA9876543210

Apply

Configuration for RPT-03

MACSEC EXAMPLE – DIFFERENT SPEEDS ON A MACSEC DEVICE



Item	Value
MAC Address of RPT-01	68:02:35:FF:AA:00
MAC Address of port 1 on RPT-01	68:02:35:FF:AA:01
MAC Address of RPT-02	68:02:35:FF:BB:00
MAC Address of port 2 on RPT-02	68:02:35:FF:BB:04
MAC Address of RPT-03	68:02:35:FF:CC:00
MAC Address of port 1 on RPT-03	68:02:35:FF:CC:01
MAC Address of port 2 on RPT-03	68:02:35:FF:CC:04
Configuration for RPT-01	
Peer MAC Address (CH1)	68:02:35:FF:CC:04
SAK (CH1)	12345678901234567890123456789012
Speed (CH1)	100M
Configuration for RPT-02	
Peer MAC Address (CH2)	68:02:35:FF:CC:01
SAK (CH2)	21098765432109876543210987654321
Speed (CH2)	1000M (default)
Configuration for RPT-03	
Peer MAC Address (CH1)	68:02:35:FF:BB:04
SAK (CH1)	21098765432109876543210987654321
Speed (CH1)	100M
Peer MAC Address (CH2)	68:02:35:FF:AA:01
SAK (CH2)	12345678901234567890123456789012
Speed (CH2)	1000M (default)

⚙️ MACSec Configuration

Channel	Enabled	Peer MAC Address ?	SAK ?
1	<input checked="" type="checkbox"/> Enable	68:02:35:FF:CC:04	12345678901234567890123456
2	<input type="checkbox"/> Enable		

Apply

⚙️ Speed Configuration

No.	Speed
Channel 1	100M
Channel 2	1000M

Apply

Configuration for RPT-01

⚙️ MACSec Configuration

Channel	Enabled	Peer MAC Address ?	SAK ?
1	<input type="checkbox"/> Enable		
2	<input checked="" type="checkbox"/> Enable	68:02:35:FF:CC:01	21098765432109876543210987

Apply

⚙️ Speed Configuration

No.	Speed
Channel 1	1000M
Channel 2	1000M

Apply

Configuration for RPT-02

⚙️ MACSec Configuration

Channel	Enabled	Peer MAC Address ?	SAK ?
1	<input checked="" type="checkbox"/> Enable	68:02:35:FF:BB:04	210987654321098765432109876
2	<input checked="" type="checkbox"/> Enable	68:02:35:FF:AA:01	123456789012345678901234567

Apply

⚙️ Speed Configuration

No.	Speed
Channel 1	100M
Channel 2	1000M

Apply

Configuration for RPT-03

SSH

To reduce the steps for login the system via **SSH** connection, the **public/private key** pair is a good choice for users. The pair of keys is created on the local device and users have to provide the public key to the target device, for example, the Ethernet switch. When users connect to the target device, the system creates a safe connection by SSH. The localhost and target device **authenticates** each other with the public and private keys to make sure the security.

BACKUP HOST KEY FILE

Host Key Backup

Backup to Localhost

File Name

Save

- [Backup to Localhost](#)

- [File Name](#)

Specify the File Name for the **SSH Host Key** file, which will be saved to the localhost.

-  (Save Button)

Click the "Save" button to save the configuration file to the **Localhost** or **USB**.

RESTORE HOST KEY FILE

Host Key Restore

Restore from Localhost

File Name

+ Select File

Restore

- [Restore from Localhost](#)

- [File Name](#)

Select the **SSH Host Key** file, which is saved in the Localhost.

-  (Restore Button)

Click the "Restore" button to restore the **SSH Host Key** from the **Localhost** or **USB**.

SSH STATUS

SSH Status

SSH Version	SSH-2
SSH Key Size	256

- [SSH Version](#)
The version of SSH that system accepts.
- [SSH Key Size](#)
The length (bits) of SSH that the Host Key should be.

HOST KEY INFORMATION

The current **SSH Host Key** is displayed in the “[SSH Host Key](#)” page. The system only accept one SSH Host Key, once users restore another Host Key, the current Host Key will be replaced.

SSH Host Key

```
AAAAB3NzaC1yc2EAAAADAQABAAQCAQIINLLQMBzd+BcavrgDWypnd3
1h5/lwimsRWAnEMFuLwdP3L0PIIK05HLnoprQjyWiJyZmQ9wgucZ1dXUtpne
1yfgxTi8CQayACHMj3gTVzWAAPNhS8Ouq7LRMThucySBQouiQHKPlbi2KZm6+IX
DHAmAG1cOM9vnRuiymDkmWBI/xVk4i0Vx+q2rAUcUOKBNm2Ydr/rz4MxoAeQRCJ
UhjeH0yIbHctM8+stM1/3k54Kn4Ivt9OqDCnLGjC3hwKxLDn1UxPDp46+oKbTls
8OLAcA285mTTKMj8g9XTIGsRD259bsajaj65e7GA16ovnlWqew4f4jG000OVdh
```

Ping

Ping is a tool used to test the reachability of a device on the IP network. Ping is enabled by sending **Internet Control Message Protocol (ICMP)** request to the target device and waits for the response packet from the target device to check the connection.

PING ANOTHER DEVICE WITH IPV4

Ping

Start
Stop
Clear
Reset

Type	<input checked="" type="radio"/> IPv4
IP Address	<input style="width: 90%;" type="text" value="192.168.10.88"/> ✓
Count	<input style="width: 90%;" type="text" value="3"/> ✓ ?
Result	<pre> ----- Start Ping 192.168.10.88 ----- 64 bytes from 192.168.10.88: ttl=128 time=6.751 ms (1) 64 bytes from 192.168.10.88: ttl=128 time=11.794 ms (2) 64 bytes from 192.168.10.88: ttl=128 time=10.892 ms (3) ----- Ping Statistics ----- Transmitted: 3 packets, Received: 3 packets, Loss: 0.00% ----- End (Count=3) ----- </pre>

For more information, hover the mouse over the  icon in the system.

- **Type**
Ping a connected device with “**IPv4**” protocol.
- **IP Address**
The IP address of the connected device is verified based on the type.
- **Count**
Sets the count times. The system will send “Count” number ICMP packets to the specific IP address and wait for the response.
The range of the Count is **from 3 to 50**.
The default Count is **3**.
- **Result**
The result of the ping shows the response from the specific IP address. If the specific IP address does not respond, it displays No Response.
- **“Start” Button**
Click the “Start” Button to start the ping to the IP address.


- **“Stop” Button**
Click the “Stop” Button to stop the ping to the IP address before the count is completed.
- **“Clear” Button**
Click the “Clear” Button to clear the “Result”.
- **“Reset” Button**
Click the “Reset” Button to clear the “Result” and reset the “IP Address” and “Count” number.

System Warning

System Warning provides “System Event Log” for different types of services. These logs are very useful for the administrator to manage and debug the system. When the system is powered off or when someone tries to login the system or the system reboots abnormally, or when some of the interfaces are linked down, the system sends log messages to notify specific users and record the events on the server or assigned platform.


CONFIGURE SYSTEM WARNING INFORMATION

System Log Settings

System Log Mode	<input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote
Remote Server IP Address	<input style="width: 100%;" type="text"/>
Service Port	<input style="width: 80%;" type="text" value="514"/> 

[Apply](#)

For more information, hover the mouse over the  icon in the system.

- [System Log Mode](#)
Select the checkbox to send system log to Local (Switch) or Remote when events happened.
- [Remote Server IP Address](#)
The field contains the IP Address of the remote server. If the “**Remote**” mode is enabled, users have to assign this IP Address to receive the system logs.
- [Service Port](#)
The port is used to listen to the system log packets on the remote server.
The range of the Service Port is **from 1 to 65535**.
The default Service Port is **514**.
-  (Apply Button)
After configuring above fields, click "**Apply**" button to make the changes effective.

SYSTEM EVENT LOG

System Event Log

Jan 1 00:38:43 buildroot user.warn emonitor: [EVENT] Authentication Fail (Auth IP: 192.168.10.88)

- [Log Text Area](#)
The system event information displays if the “**Local**” system log mode is enabled and the configured events are triggered.
- (Clear Button)
Click the “Clear” button to clear the system event log in the text area.
- (Refresh Button)
Click the “Refresh” button to refresh the system event log in the text area.

CONFIGURE SYSTEM EVENT SELECTION

System Event Selection

Event	System Log
Authentication Failure	<input type="text" value="Disable"/>

- [Event](#)
We only provide **Authentication Failure** Event on the MACSec Encoder.

Authentication Failure: Login failed on the web console or CLI. It may be caused due to incorrect username or password.

-  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

Authorization

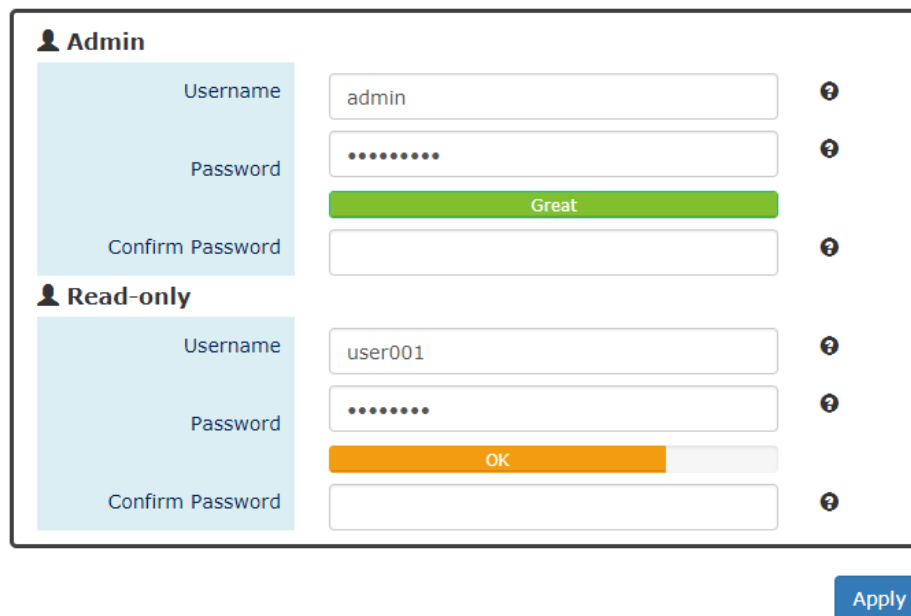
The "**Username**" and "**Password**" are very important information both in the "**Command Line Interface**" or "**Web Console**". Users have to login into the system before doing any configuration. We strongly suggest the users to change at least the password **for security** when they are going to use this device.

CONFIGURE LOGIN INFORMATION

Currently we support two-level users – **Admin** and **Read-only** user. The Admin can access any page and configure the system but the read-only user can only access status pages.

Update Authorization

Basic Settings



User Type	Username	Password	Confirm Password	Password Strength
Admin	admin		Great
Read-only	user001		OK

[Apply](#)

For more information, hover the mouse over the  icon in the system.

- Username**

The account used to login to the system.

The maximum length of the Username is **32** characters

Only **alphabet** (A-Z, a-z) and **numbers** (0-9) are allowed.

The default Username is **admin**.
- Password**

The password used to login to the system. We provide **password strength** bar for reference.

There are 3 levels - **Weak**, **OK**, and **Great**. We strongly recommend users configuring the password to "**Great**" level for security.

The maximum length of the Password is **32** characters.

Only **alphabet** (A-Z, a-z), **numbers** (0-9), and **chars** (!,@,%^*,(,)) are allowed.

The default Password is **admin**.

- **Confirm Password**

It is used to confirm the value specified by the users in the "Password" field. The value of the field must be the same as "Password".

-  (Apply Button)

After configuring above fields, click "**Apply**" button to make the changes effective.

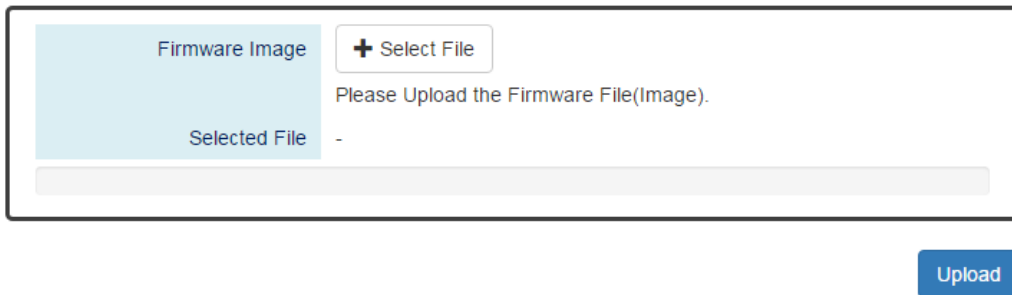
Firmware Upgrade

For a better performance and wider industrial applications, we constantly develop new features and revise the issues from the users. We suggest the users to upgrade the system to the newest firmware version to have a better user experience.


UPGRADE FIRMWARE VERSION

Firmware Upgrade

Upload Firmware File



The screenshot displays a user interface for uploading a firmware file. It features a light blue header area with the text 'Firmware Image' and a '+ Select File' button. Below this, the text 'Selected File' is followed by a hyphen '-'. A message 'Please Upload the Firmware File(Image)' is positioned to the right. At the bottom right of the interface is a blue 'Upload' button.

- [Firmware Image](#)
Click the "**Select File**" button to select the firmware image provided by the sales or support. The **Firmware Version** displayed on the system can be customized by the **file name**. For example, if you want the version to be called as 1.2.3, you only need to modify the file name to **XXX-v1.2.3** (XXX is the original file name).
 - [Selected File](#)
After selecting a firmware image to be uploaded, the **selected file name** will be displayed in this field.
 -  (Upload Button)
After selecting the firmware image, click "Upload" button to upload it.
-

UPGRADE FIRMWARE PROCESS - UPLOADING FIRMWARE FILE

The following steps are performed when the system starts to upgrade after the "Apply" button is clicked:

1. **Uploading** the firmware image

The progress bar displays the uploading percentage.

📍 Upload Firmware File

Uploading... Please Wait.

The screenshot shows a web interface for uploading a firmware file. It features a light blue header with the text "Firmware Image" and a "+ Select File" button. Below this, it says "Please Upload the Firmware File(Image)." and "Selected File WEBFULL-v0.0.14.1214". A green progress bar is filled to 56%. At the bottom right, there is a blue "Upload" button.

2. **Verifying** the uploaded file

When the file is **100%** uploaded, the system starts to **verify** the uploaded file to make sure it is **valid**. By default, the firmware image is encrypted to prevent the attack on man-in-the-middle. Optionally, higher encryption methodology is also provided.

📍 Upload Firmware File

Uploading Finished, Verifying Uploading File...

The screenshot shows the same web interface as before, but the green progress bar is now filled to 100%. The "Upload" button remains at the bottom right.

3. **Installing** the uploaded firmware image

The new firmware will install after the system validates it.

📍 Upload Firmware File

Verifying Finished, Installing Firmware...

The screenshot shows the same web interface as before, with the green progress bar at 100% and the "Upload" button at the bottom right.

4. **Rebooting** the system

The system will reboot automatically if the firmware is upgraded without any issue.
The progress bar displays the rebooting progress.

Device Rebooting... Please Wait...

The Web Page Will Refresh Automatically.



Config Backup

In the normal application, there are several switches in the Network and they might be configured to the same features. To facilitate this, the users can configure one of the switches and save the configuration file to localhost (for example: users' PC) or USB sticks and then restore the configurations on another switch via "**Config Restore**" function. Configuration file in the USB can also have a way to fast replace the device when it is damage.

BACKUP CONFIGURATION FILE

Config Backup

Backup to Localhost

File Name	<input type="text"/>	Save
-----------	----------------------	------

- Backup to Localhost

- File Name

Specify the File Name for the **Startup-config** file, which will be saved to the localhost.

-  (Save Button)

Click the "Save" button to save the configuration file to the **Localhost** or **USB**.

NOTE: If the **File Name** filed is empty, the system assigns the default name: *config-[datetime].cfg*

Config Restore

We suggest users to save/backup the configurations after a series of settings. If another device needs the same configurations, users can use the **Config Restore** function to restore it.

RESTORE CONFIGURATION FILE

Config Restore

Restore from Localhost

- Restore from Localhost

- File Name

Select the configuration file, which is saved in the Localhost.

-  (Restore Button)

Click the "Restore" button to restore the configurations from the **Localhost** or **USB**.

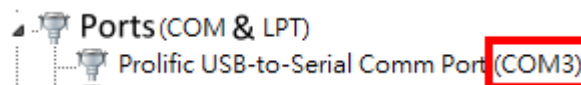
Command Line Interface

Command Line Interface is usually called **CLI**. It allows the users to configure, monitor, and maintain the switch by executing commands directly.

CONNECT TO CLI VIA CONSOLE PORT

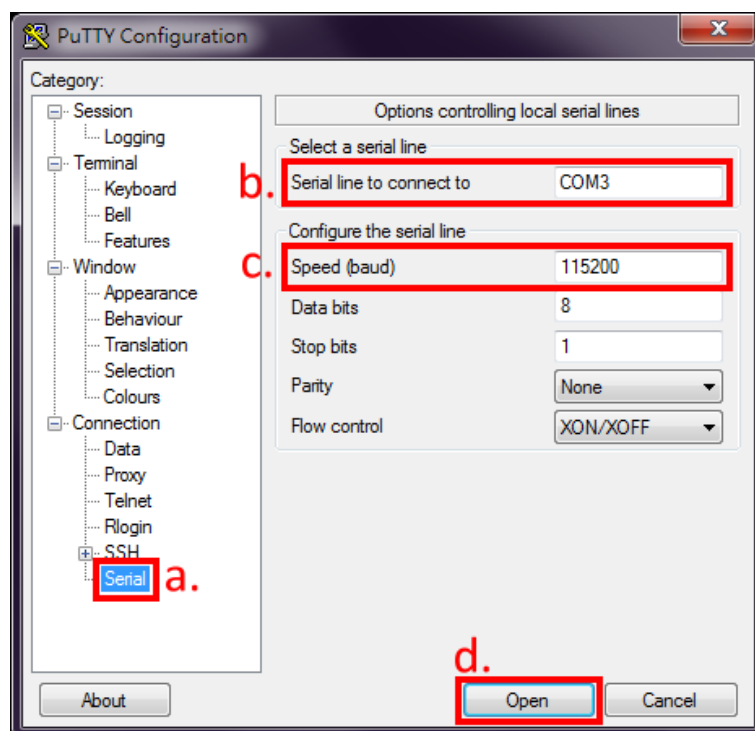
Before starting the connection to the Console Port, ensure that you have a utility (such as “Putty”, “Tera Term”, “HyperTerminal”, “SecureCRT”, etc.) to do that. The following example is operating on **Windows 7** and connected by “**Putty**”.

1. Connect the Console Port to your PC or Laptop and check the port number in the “Device Manager” on the PC.

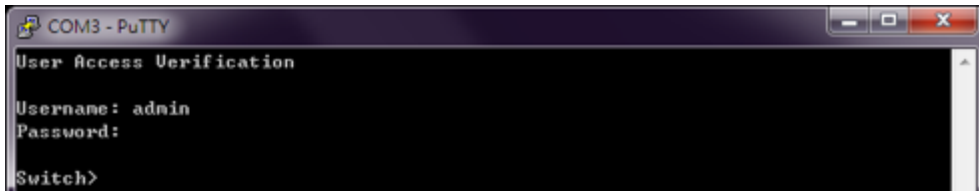


2. Configure the Serial Information with the COM port number and Speed (Baud Rate: **115200**). By default, the Data bits and Parity are **8** and **1**. Then click “Open” to connect to the CLI.

Note: The complete parameters are **COMX/115200/8/1**.



3. Enter the username and password to login to the system. The default username and password is **admin/admin**.

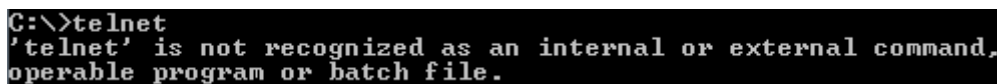


```
COM3 - PuTTY
User Access Verification
Username: admin
Password:
Switch>
```

4. When you see “**Switch>**”, it refers that you have logged in to the system. You can then start to configure the system on the CLI mode.

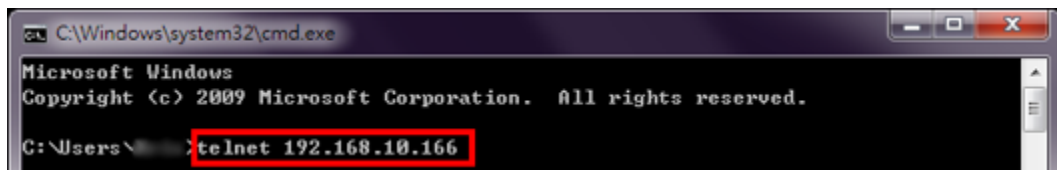
CONNECT TO CLI VIA TELNET

The following example is operating on **Windows 7**. If the system shows the information as the picture below, please enable the “Telnet Client” before using telnet function.



```
C:\>telnet
'telnet' is not recognized as an internal or external command,
operable program or batch file.
```

1. Click Windows “Start” button and enter “cmd” on the search box to open the “Command Prompt”.
2. Enter “**telnet [IP_ADDRESS]**” on the CMD window. For example, the IP address of the switch is “192.168.10.166”, so enter “telnet 192.168.10.166” and then press the “Enter” key.



```
C:\Windows\system32\cmd.exe
Microsoft Windows
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\> telnet 192.168.10.166
```

3. Enter the username and password to login the system. The default username and password is **admin/admin**.



```
Telnet 192.168.10.166
User Access Verification
Username: admin
Password:
Switch>
```

4. When “**Switch>**” is displayed, it refers that you have logged in to the system. You can then start to configure the system on the CLI mode.

CONFIGURE SYSTEM UNDER DIFFERENT MODES

After login to CLI, users have to enter the Privileged Mode for “show” commands. If users want to configure the system via CLI, they have to enter Configuration Mode.

The command to enter Privileged Mode is “**enable**”. After enter Privileged Mode, issue “**configure terminal**” to enter Configuration Mode. When “**Switch(config)#**” is displayed, users can start configuring the system with all commands under Configuration Mode. In the Command Group section, the mode of each command will be marked in the last column of the commands table.

```

Telnet 192.168.10.147
Welcome to Switch.
Username: admin
Password:
Switch> enable Enter Privileged Mode
Switch# configure terminal Enter Configuration Mode
Switch(config)#

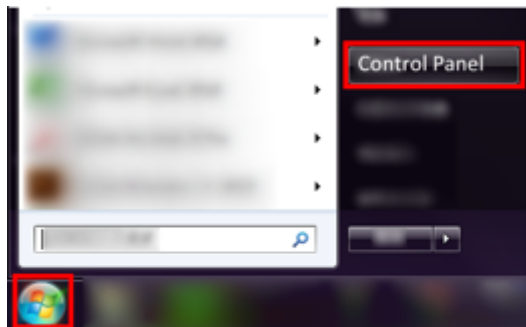
```

The **Interface** Mode is under Configuration Mode. If the command that users are preparing to issue is under this mode, they have to enter it first. Users can issue “**exit**” to leave current mode. In the following table, we list the commands to enter **Interface** Mode.

Mode	Command	Description
Interface	interface lanX	X implies the port number

ENABLE TELNET CLIENT ON WIDOWS 7

1. Click the Windows “Start” button and click “Control Panel” item.



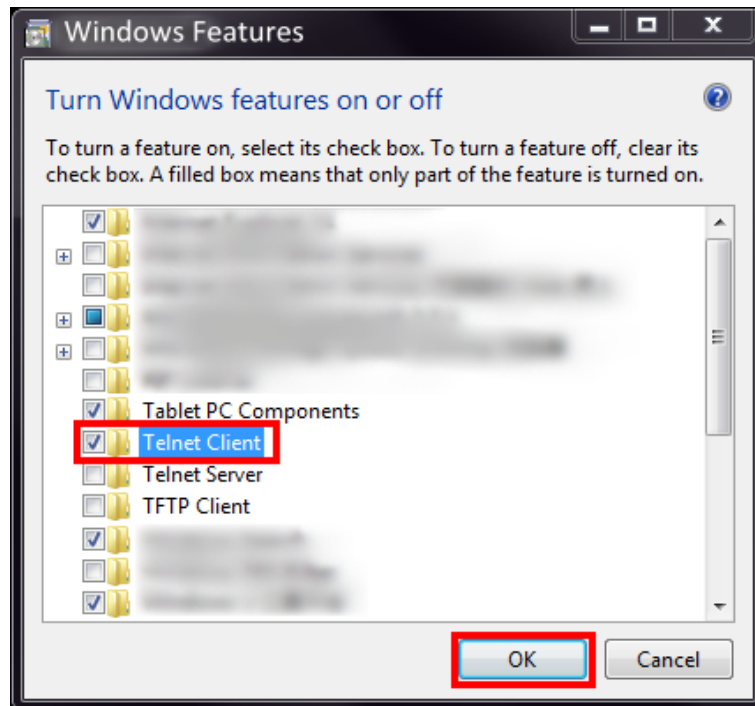
2. Click the “Programs” item.



3. Click the “Turn Windows features on or off” item.



4. Select the checkbox of “Telnet Client” and then click “OK” to enable telnet function.



5. Click Windows “Start” button and enter “cmd” on the search box to open the “Command Prompt” to test the telnet function.

 A screenshot of the Windows Command Prompt window. The title bar shows "C:\Windows\system32\cmd.exe". The window content shows the following text:


```
Microsoft Windows
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ >telnet /?

telnet [-a[-e escape char][-f log file][-l user][-t term][host [port]]
-a Attempt automatic logon. Same as -l option except uses
  the currently logged on user's name.
-e Escape character to enter telnet client prompt.
-f File name for client side logging
-l Specifies the user name to log in with on the remote system.
  Requires that the remote system support the TELNET ENVIRON option.
-t Specifies terminal type.
  Supported term types are vt100, vt52, ansi and vtnt only.
host Specifies the hostname or IP address of the remote computer
  to connect to.
port Specifies a port number or service name.

C:\Users\ >
```

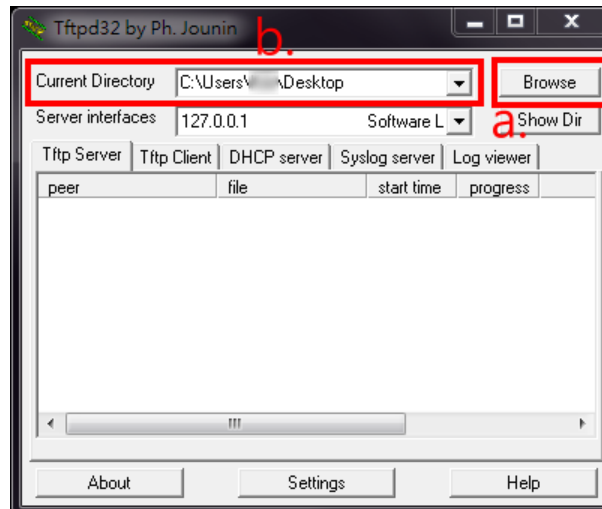
FIRMWARE UPGRADE VIA CLI

Users can upgrade the system with a new firmware on both the web console and CLI mode. To upgrade on the web console, a high interactivity web GUI is provided for the users. Please refer to [Firmware Upgrade](#) section. To upgrade on the CLI mode, there are 3 methods: TFTP, wget (HTTP), and USB. The following sections explain how to upgrade the firmware using the 3 methods.

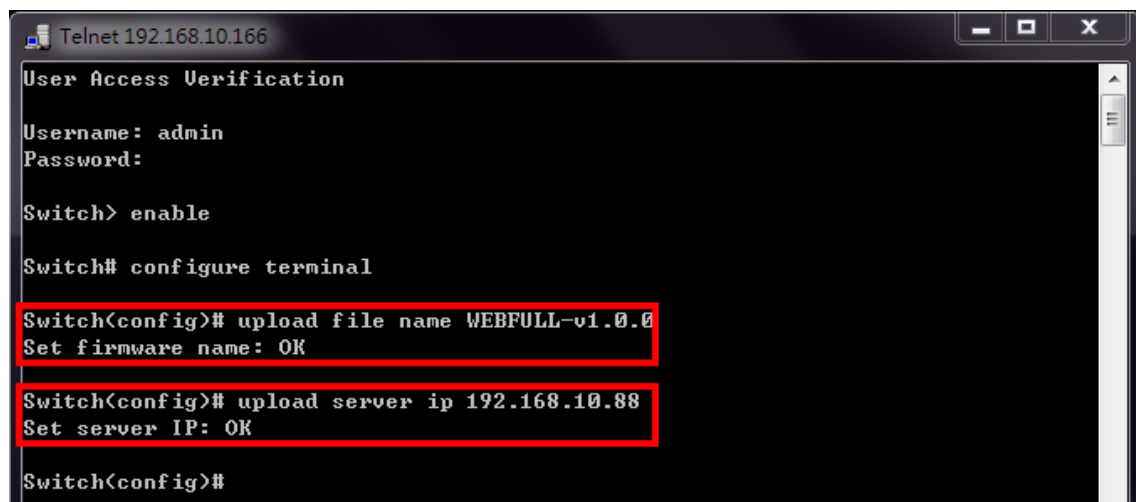
FIRMWARE UPGRADE VIA CLI – TFTP

If the users are planning to upgrade the firmware via CLI mode with TFTP, a **TFTP server** is needed before upgrading. You can download the free TFTP server from [tftpd official website](#).

1. Open the TFTP Server and browser the file directory path. For example, if the firmware file is saved on the desktop, the path to the desktop should be specified in the “**Current Directory**” field.



2. Make sure the link between the switch and the host (PC or laptop) is connected. To verify it, ping the IP address of the switch IP address from the host to check it.
3. Assign the **firmware file name** by issuing the “**upload file name [FILE_NAME]**”. The default file name is “WEBFULL”.
4. Assign the TFTP Server IP address by issuing “**upload server ip [SERVER_IP]**”. The server IP address is the IP address of the host, which is running the TFTP server.
The commands for assigning the filename and server IP are in the **Configure mode**, so before configuring, specify “configure terminal” to enter the **Configure mode**.
If the command is completely configured, the system will display “OK”.



5. Start to upgrade the firmware file by specifying “upload tftp”. The system starts to upload the assigned file by the TFTP. This takes a few minutes.


```

Telnet 192.168.10.166
User Access Verification
Username: admin
Password:

Switch> enable

Switch# configure terminal

Switch(config)# upload file name WEBFULL-v1.0.0
Set firmware name: OK

Switch(config)# upload server ip 192.168.10.88
Set server IP: OK

Switch(config)# upload tftp
CAUTION: DO NOT SHUTDOWN WHEN THE PROCEDURE IS NOT FINISHED
Uploading firmware via 'tftp'

firmware uploading ...
It may take few seconds or minutes to upload, please wait patiently.

```

6. After uploading, the system will **verify** the uploaded file. If the verification passes, the new firmware file will be installed. Ensure the system is **powered on** and the system will **reboot** automatically after the firmware is completely installed.

```

Telnet 192.168.10.166
verifying firmware ...
It may take 5 - 6 seconds to complete, please wait patiently.
verified OK!

decompressing and extracting ...
It may take 10 - 20 seconds to complete, please wait patiently.
decompression OK!

Start Upgrading Kernel ...
Erasing blocks: 97/97 <100%>
Writing data: 6145k/0k <100%>
Verifying data: 6145k/0k <100%>

Start Upgrading Rootfs ...
libscan: scanning eraseblock 839 -- 100 % complete
ubiformat: 839 eraseblocks have valid erase counter, mean value is 58
ubiformat: 1 bad eraseblocks found, numbers: 170
ubiformat: flashing eraseblock 274 -- 100 % complete
9 -- 100 % complete   eraseblock 838 -- 99 % complete

finished!
System is going to reboot ...

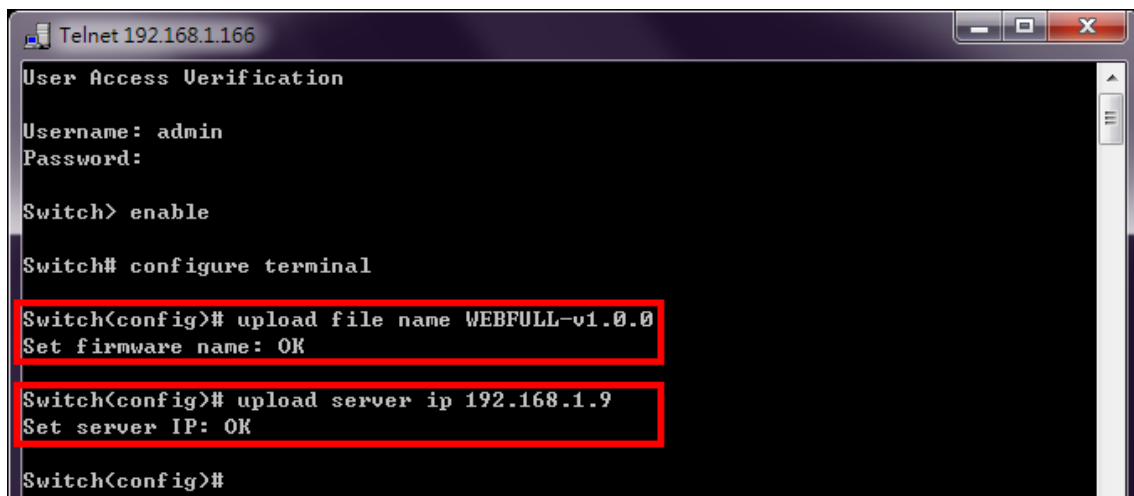
```

FIRMWARE UPGRADE VIA CLI – WGET

“Wget” uses the **HTTP** to transmit the file to the switch. Users have to establish a **HTTP Server** such as “[Apache](#)” and upload the firmware file to the HTTP Server.

1. Assume there is a HTTP Server existed whose IP address is “**192.168.1.9**” and the firmware file named **WEBFULL-v1.0.0** is uploaded.
2. Make sure the link between the switch and the server is connected. We can ping the IP address of the server from the switch by using the command “**ip ping [IP_ADDRESS]**”.
3. Assign the **firmware file name** by using “**upload file name WEBFULL-v1.0.0**”.
4. Assign the **Wget Server IP address** by using “**upload server ip 192.168.1.9**”.

If the command is completely configured, the system will display “**OK**”.

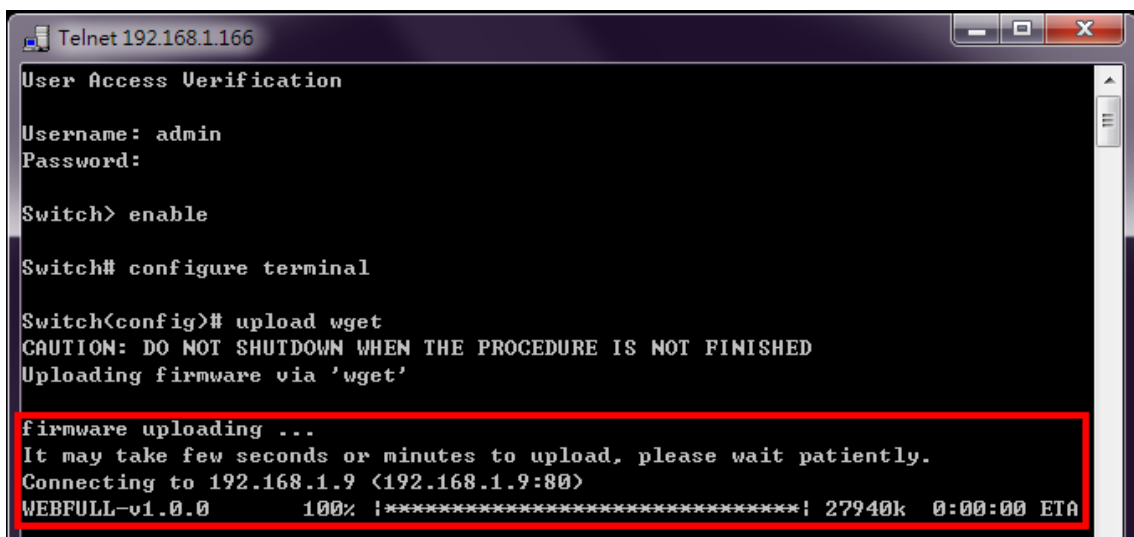


```

Telnet 192.168.1.166
User Access Verification
Username: admin
Password:

Switch> enable
Switch# configure terminal
Switch(config)# upload file name WEBFULL-v1.0.0
Set firmware name: OK
Switch(config)# upload server ip 192.168.1.9
Set server IP: OK
Switch(config)#
  
```

5. Start to upgrade the firmware file by using “**upload wget**”. The system starts to upload the assigned file by HTTP. This takes a few seconds or minutes.



```

Telnet 192.168.1.166
User Access Verification
Username: admin
Password:

Switch> enable
Switch# configure terminal
Switch(config)# upload wget
CAUTION: DO NOT SHUTDOWN WHEN THE PROCEDURE IS NOT FINISHED
Uploading firmware via 'wget'

firmware uploading ...
It may take few seconds or minutes to upload, please wait patiently.
Connecting to 192.168.1.9 (192.168.1.9:80)
WEBFULL-v1.0.0      100% !*****! 27940k  0:00:00 ETA
  
```

6. Once the uploading is complete, the system will **verify** the uploaded file. If the verification passes, the new firmware file will be installed. Ensure to keep the system **powered on** and the system will **reboot** automatically after the firmware is completely installed.

```

Telnet 192.168.1.166
verified firmware ...
It may take 5 - 6 seconds to complete, please wait patiently.
verified OK!

decompressing and extracting ...
It may take 10 - 20 seconds to complete, please wait patiently.
decompression OK!

Start Upgrading Kernel ...
Erasing blocks: 97/97 <100%>
Writing data: 6145k/0k <100%>
Verifying data: 6145k/0k <100%>

Start Upgrading Rootfs ...
libscan: scanning eraseblock 839 -- 100 % complete
ubiformat: 839 eraseblocks have valid erase counter, mean value is 58
ubiformat: 1 bad eraseblocks found, numbers: 170
ubiformat: flashing eraseblock 274 -- 100 % complete
9 -- 100 % complete   eraseblock 838 -- 99 % complete

finished!
System is going to reboot ...

```

COMMAND GROUPS

The following are the commands that the users can use in the CLI mode. Please check if the **mode** is correct before issuing the command.

AUTHENTICATION GROUP

Command	Explanation	Mode
logout	Disconnect	Configure
username [USER_ID] [PASSWORD]	Configure username and password	Configure
username-ro [USER_ID] [PASSWORD]	Configure read only username and password	Configure
show username	Display admin ID	Configure
show username-ro	Display read only user ID	Configure
no username	Default username and password	Configure
no username-ro	Default read only username and password	Configure

SSH GROUP

Command	Explanation	Mode
upload host-key-config wget [file]	Upload SSL host key config from Localhost	Configure
show ssh host-key	Display SSH host key	Configure
show ssh status	Display SSH status	Configure

SYSTEM GROUP

Command	Explanation	Mode
erase startup-config	Reset to factory default and reboot	Configure
erase startup-config keep-ip	Reset to factory default except IP	Configure
erase startup-config keep-ip-user	Reset to factory default except IP and USER	Configure
erase startup-config keep-user	Reset to factory default except USER ID/PASS	Configure
exec-timeout [MINUTE] [SECOND]	Set idle timeout [MINUTE] [SECOND]	Configure
hostname [HOSTNAME]	Set Switch Host Name	Configure
reboot	Reboot the switch	Configure
system contact [CONTACT]	Set system contact	Configure
system description [SYS_DESCRIPTION]	Set device description	Configure
system location [LOCATION]	Set device location	Configure
show exec-timeout	Display idle timeout	Configure
show hostname	Display Switch Host Name	Configure
show system contact	Display system contact	Configure
show system description	Display system description	Configure
show system firmware-date	Display system release time	Configure
show system location	Display system location	Configure
show system mac	Display system MAC address	Configure
show system uptime	Display system uptime	Configure
show system version firmware	Display system version	Configure
no exec-timeout	Default idle timeout	Configure
no hostname	Default Switch Host Name	Configure
no system contact	Clear system contact	Configure
no system description	Clear device description	Configure
no system location	Clear device location	Configure

IPv4 GROUP

Command	Explanation	Mode
ip address [IP_ADDR] [MASK]	Set IPv4 address and netmask	Configure
ip default-gateway [DEFAULT_GATEWAY_ADDR]	Set default gateway address	Configure
ip name-server [NAME_SERVER1_IP] [NAME_SERVER2_IP]	Set Domain Name-Server	Configure
ip ping [IPv4_ADDR] [<size PKG_SIZ> <repeat PKG_CNT>]	Issue an IPv4 ping command	Configure
show ip address	Display Host address of IPv4	Configure
show ip default-gateway	Display default gateway address	Configure
show ip first-nameserver	Display Domain Name-Server-1st	Configure
show ip second-nameserver	Display Domain Name-Server-2nd	Configure

no ip address	Delete IPv4 address	Configure
no ip default-gateway	Clear the default gateway address	Configure
no ip name-server	Clear the domain name-server	Configure

TIME GROUP

Command	Explanation	Mode
clock time [hh:mm:ss] [day] [month] [year]	Configure time	Configure
clock timezone [AREA] [CITY]	Configure time zone	Configure
ntp client sync [minute hour day month year] [NUMBER]	Configure NTP client sync	Configure
ntp client timeserver [SERVER_IP/URL]	Configure NTP client time server	Configure
ntp time update	Configure NTP time update	Configure
show clock time	Show time	Configure
show clock timezone	Show timezone	Configure
show ntp client sync	Show sync time	Configure
show ntp client timeserver	Show NTP server configuration	Configure
no clock timezone	Remove timezone	Configure
no ntp client sync	Remove NTP sync time	Configure
no ntp client timeserver	Remove NTP time server configuration	Configure

SPEED GROUP

Command	Explanation	Mode
speed [10 100]	Configure speed for the designated port (10M is only supported on RPT-E2004G)	Interface
show speed	Display speed for the designated port	Interface
no speed	Default speed to 1000M for the designated port	Interface

MACSEC GROUP

Command	Explanation	Mode
macsec enable	Enable MACSec	Interface
macsec peer_macaddress [MAC_ADDR]	Configure Peer Mac Address for MACSec	Interface
macsec sak [SAK: 32 digit hex]	Configure MACSec SAK key	Interface
show macsec	Display MACSec Status	Interface
show macsec peer_macaddress	Display MACSec Peer's MAC Address	Interface
show macsec sak	Display MACSec SAK key	Interface
no macsec	Disable MACSec function	Interface
no macsec peer_macaddress	Remove MACSec Peer's MAC Address	Interface
no macsec sak	Remove MACSec SAK key	Interface

SERVICE CONTROL GROUP

Command	Explanation	Mode
service [http https ssh telnet console] enable	Enable service http, https, ssh, telnet, or console port	Configure
show service [http https ssh telnet console]	Display service http, https, ssh, telnet, or console port	Configure
no service [http https ssh telnet console]	Disable service http, https, ssh, telnet, or console port	Configure

SYSLOG GROUP

Command	Explanation	Mode
event syslog auth-failure	Register an event of authentication failure	Configure
syslog local enable	Enable logging to local	Configure
syslog log clear	Clear syslog log	Configure
syslog remote enable	Enable logging to remote	Configure
syslog remote port [PORT]	Set syslog remote server port	Configure
syslog remote server [ADDRESS]	Set syslog remote server address	Configure
show event syslog auth-failure	Display authentication failure event registration	Configure
show syslog local	Display local logging state	Configure
show syslog log	Display syslog messages	Configure
show syslog remote	Display remote logging state	Configure
show syslog remote port	Display remote server port	Configure
show syslog remote server	Display remote server IP	Configure
no event syslog auth-failure	Unregister an event of authentication failure	Configure
no syslog local	Disable logging to local	Configure
no syslog remote	Disable logging to remote	Configure
no syslog remote port	Default syslog remote server port	Configure
no syslog remote server	Clear syslog remote server address	Configure