

Barox

Industrial Managed Ethernet Switch

Software User Manual

Last Update: September 10, 2015

Version 2.4.0

Contents

Introduction	1
Web Console Configuration	4
Basic Settings	6
Port Management	10
PoE	12
ERPS	15
Spanning Tree.....	22
IGMP Snooping	27
802.1Q VLAN.....	29
QoS	31
Port Trunk	34
Port Mirroring	36
SNMP	37
DHCP Server / Relay	40
802.1X.....	44
UPnP	47
Modbus.....	48
System Warning	55
MAC Table	60
Maintenance	62
Configuration	64
Logout.....	67
Command Line Interface	68
Connect by RS-232 Serial Console	68
Connect by Telnet.....	69
Introduce CLI and Tips	69
Save Configuration File to USB	72
Load Configuration File from USB.....	73
Upgrade Firmware from USB.....	73
Upgrade Firmware by TFTP	74
Commands	75

Introduction

This managed industrial switch supports a variety of layer 2 Network features, such as Network Redundancy (ERPS, RSTP, MSTP), IGMP Snooping, Quality of Service (QoS), 802.1Q VLAN, and SNMP. We also support System Warning mechanism for automatic warnings sent through e-mail or syslog on the switch.

To access and configure this switch, we provide Web GUI and CLI commands. It's easy to configure through Web GUI for a non-engineer manager because of this user-friendly designs for HTML web console interfaces. The **“Web Console Configuration”** section is a good consultation for users. Users can complete configurations by following the manual step by step. Further configurations can be done by CLI commands. We also support 2 ways to connect to CLI: one is through our **“Serial Console Port”**, and another is connecting by **“Telnet”**. We will introduce how to connect to CLI in the **“Command Line Interface”** Section.

Web Console

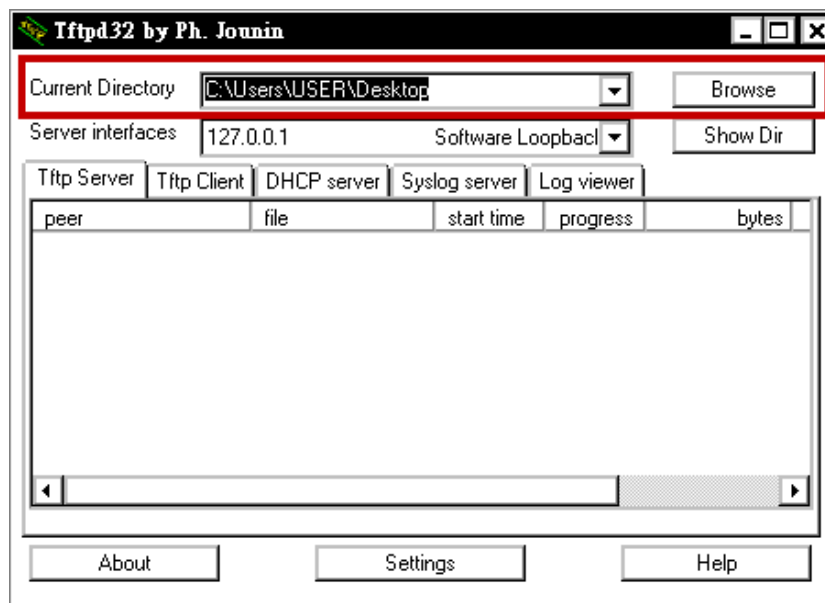
We build a connection between our switch and PC via a web browser. We provide a user-friendly Web GUI for our users. When users link to our web console, it looks like they are browsing an interactive web site. Users can pass commands to the switch by selecting the dropdown menu, typing in a string, checking the checkboxes, and clicking the **“Apply”** button on the browser with graphic interface. It is easy for all users. All they need is any kind of web browser like IE, Chrome, Firefox, Opera. For more detailed information, please see the **“Web Console Configuration”** section.

Command Line Interface

It is another way to configure our switch and it is more difficult than using Web Console. We design our CLI as a Cisco-like interface. Cisco is the most famous international commercial switch vendor, so if users are used Cisco's switch, it would be easier for them to use this switch. On Command Line Interface, we issue commands to set our switch. We list all of the commands in the “

1. Upgrade Firmware by TFTP

Step 1 Open TFTP and configure the file path. Ensure TFTP is ready.

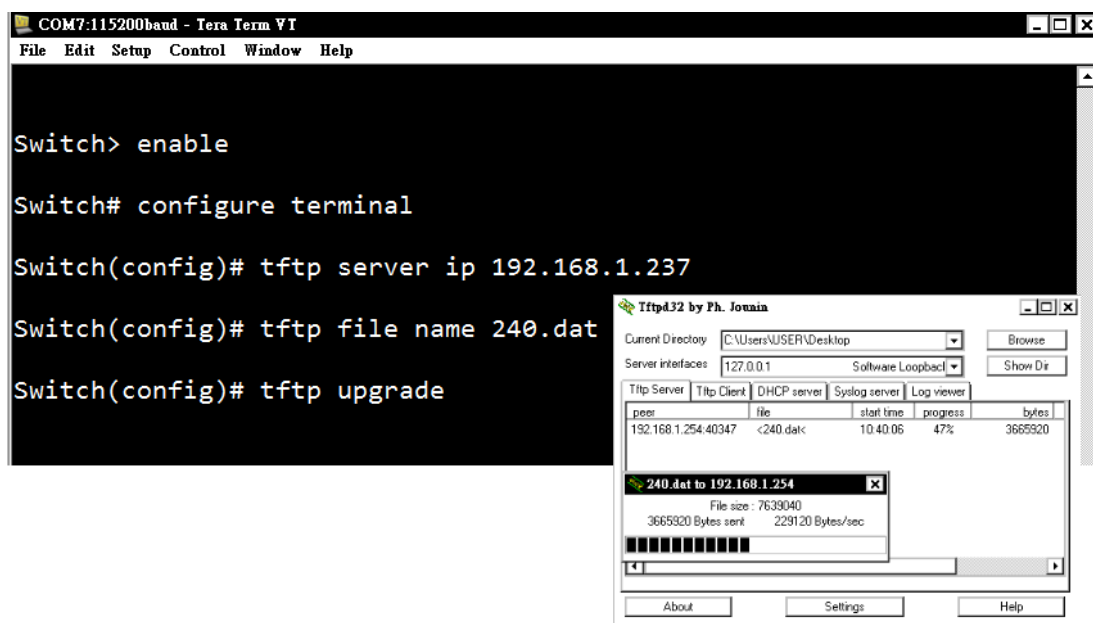


Step 2 Enter “Global Configuration Mode”.

Step 3 Set TFTP Server IP address. Issue the command “tftp server ip [IP_ADDRESS]”.
[IP_ADDRESS] is the IP address where your firmware file located.

Step 4 Set firmware upgrade file name. Issue the command “tftp file name [UPGRADE_FILE_NAME]”. Please make sure the file name of upgrade firmware file.

Step 5 Issue “tftp upgrade” to start upgrading firmware.



Step 6 It will reboot after finishing upgrading the firmware.

Commands” part. We can issue some further features only on CLI mode such as “SNMP Trap

v3". So, you can attempt to find the commands that you couldn't find on Web Console on CLI. You can find more directions for use in the "**Command Line Interface**" section.

Web Console Configuration

Our user-friendly designs for HTML web console interfaces are set in all our industrial managed switches. With a flash memory on the CPU bard and sophisticated management features, users are able to manage the switch through any Internet browser anywhere on the network.

Web Console Configuration Information

Default IP Address: **192.168.1.254**

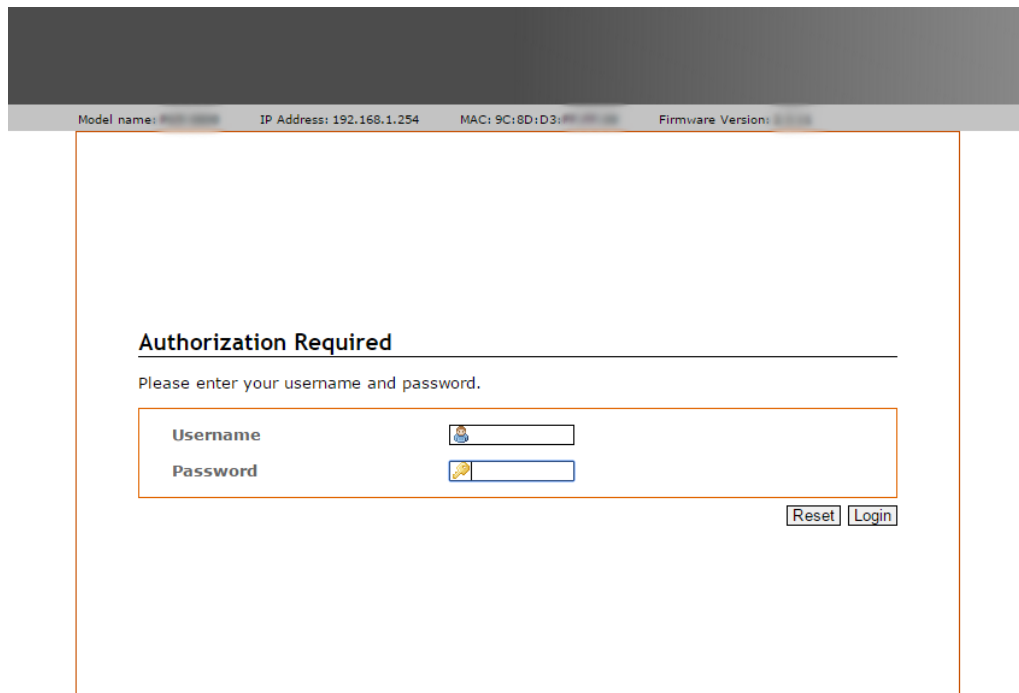
Default Login Account: **admin**

Default Login Password: **admin**

Login Web Site

Step 1 Open a browser (IE, Chrome, Firefox, Opera...)

Step 2 Type switch's IP address, default value is "**192.168.1.254**", in the url field, and then press "Enter" key.



Model name: [redacted] IP Address: 192.168.1.254 MAC: 9C:8D:D3:[redacted] Firmware Version: [redacted]

Authorization Required

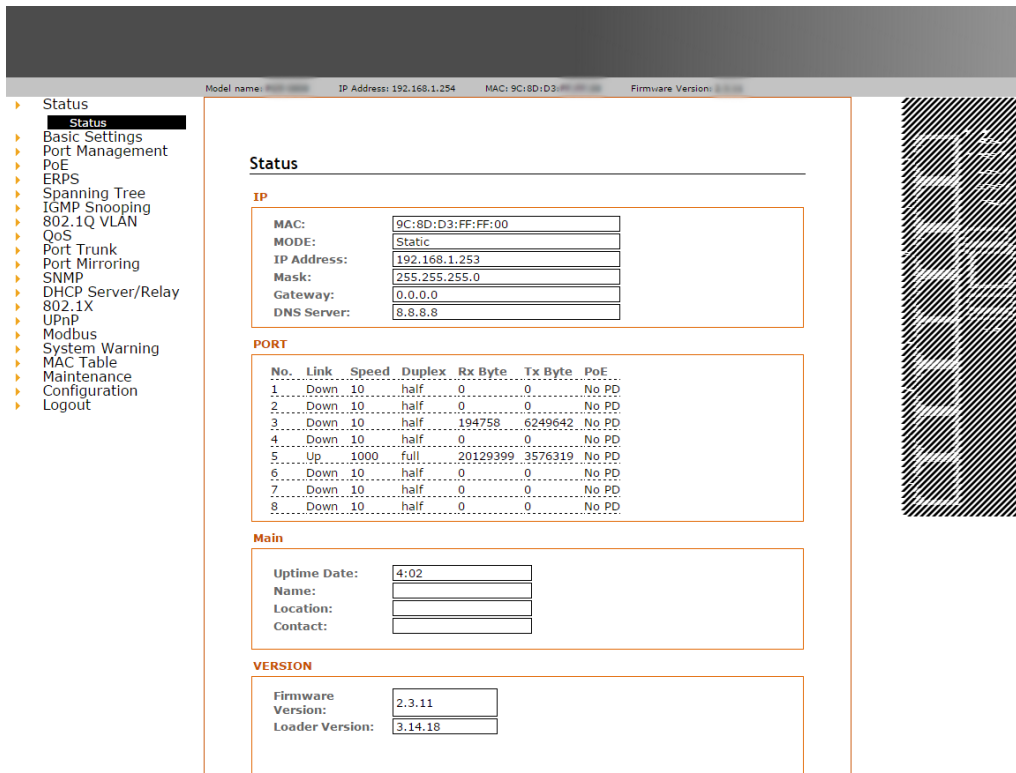
Please enter your username and password.

Username

Password

Figure 1: Login Page on the switch's web console.

Step 3 Login with username and password, default value is **admin / admin**. And then Click “Login” button to login the system.



Model name: **9C18D3** IP Address: 192.168.1.254 MAC: 9C18D3:FF:FF:00 Firmware Version: 2.3.11

▶ Status
 ▶ Status
 ▶ Basic Settings
 ▶ Port Management
 ▶ PoE
 ▶ ERPS
 ▶ Spanning Tree
 ▶ IGMP Snooping
 ▶ 802.1Q VLAN
 ▶ QoS
 ▶ Port Trunk
 ▶ Port Mirroring
 ▶ SNMP
 ▶ DHCP Server/Relay
 ▶ 802.1X
 ▶ UPnP
 ▶ Modbus
 ▶ System Warning
 ▶ MAC Table
 ▶ Maintenance
 ▶ Configuration
 ▶ Logout

Status

IP

MAC:	9C:8D:D3:FF:FF:00
MODE:	Static
IP Address:	192.168.1.253
Mask:	255.255.255.0
Gateway:	0.0.0.0
DNS Server:	8.8.8.8

PORT

No.	Link	Speed	Duplex	Rx Byte	Tx Byte	PoE
1	Down	10	half	0	0	No PD
2	Down	10	half	0	0	No PD
3	Down	10	half	194758	6249642	No PD
4	Down	10	half	0	0	No PD
5	Up	1000	full	20129399	3576319	No PD
6	Down	10	half	0	0	No PD
7	Down	10	half	0	0	No PD
8	Down	10	half	0	0	No PD

Main

Uptime Date:	4:02
Name:	
Location:	
Contact:	

VERSION

Firmware Version:	2.3.11
Loader Version:	3.14.18

Figure 2: Index Page after Login

Basic Settings Configuration Terms

[Web User Interface – System]

System

SWITCH SETTING

System Name:	<input type="text" value="Switch"/>
System Description:	<input type="text" value="8 port Industrial Managed Ethernet Switch"/>
System Location:	<input type="text"/>
System Contact:	<input type="text"/>

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
System Name	The name of this switch. Alphabet (A-Z & a-z), digits (0-9), and minus (-) are allowed. The default system name is "Switch".
System Description	Users can describe about the switch on this field. The default system description is "n port Industrial Managed (PoE) Ethernet Switch".
System Location	Where the switch is located in. The length of system location is 0 to 255. ASCII codes from 32 to 126 are allowed. The default system location is blank.
System Contact	Record the administrator and his/her contact information in this field. The length of system contact is 0 to 255. ASCII codes from 32 to 126 are allowed. The default system contact is blank.

[Web User Interface – Admin Password]

Admin Password

ADMINISTRATIVE ACCOUNT

New Password:	<input type="password"/>
Confirmation:	<input type="password"/>

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
New Password	Set a new login password. The length of new password should be 1 to 31.
Confirmation	Enter again the new password.

[Web User Interface – IP Setting]

IPv4 Setting

IPv4 CONFIGURATION

DHCP Client:	<input type="checkbox"/>
IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text"/>
DNS:	<input type="text"/>

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
DHCP Client	“Enable” or “Disable” DHCP Client.
IP Address	Static IP address setting. Assign the IP address that the network is using.
Subnet Mask	Assign the subnet mask of the IP address.
Gateway	The IP address that connects the LAN to the Internet.
DNS	The IP address of DNS.

[Web User Interface – IPv6 Neighbor Cache]

IPv6 Neighbor Cache shows the neighbors that this switch discovered. This table shows neighbor's IPv6 Address, MAC Address and it's state(Delay, REACHABLE, STALE, FAILED, PROBE).

IPv6 Neighbor Cache

IPv6 NEIGHBOR CACHE

IPv6 Address	Link Layer(MAC) Address	State
fe80::7941:e3ea:d701:a7cd	c4:6e:1f:03:1e:5a	REACHABLE

[Web User Interface – IPv6 Setting]

IPv6 Address

IPv6 ENABLE

IPv6 Enable: ☒

IPv6 CONFIGURATION

IPv6 Address	IPv6 Length Prefix
<input type="text"/>	<input type="text"/>
<input type="button" value="Delete"/>	
<input type="button" value="Add"/>	

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
IPv6 Enable	"Enable" or "Disable" using IPv6.
IPv6 Address	Static IPv6 address setting. Assign one or more IPv6 address(es) that the network is using. Default IPv6 Address is generated from MAC Address.
IPv6 Length Prefix	Enter the prefix of this IPv6 Address. Default IPv6 Address is set to "64".

[Web User Interface – System Time]

System Time

NTP

Local Time:	Thu Jan 1 00:34:33 1970 Sync with browser
Select Your Time Zone:	UTC ▼
Enable NTP Client:	<input type="checkbox"/>
Time Server:	2.pool.ntp.org

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Local Time	The system local time. Click “Sync with browser” to synchronize system local time with the browser
Select Your Time Zone	Select the time zone for the switch with the dropdown menu.
Enable NTP Client	Check the ckeckbox to enable NTP Client to synchronize the time with time server.
Time Server	Enter the IP address/name server of time server that used when NTP Client is enabled.

Overview

With the Port Configuration function, users are able to:

- Assign a “value/label” for each port
- Enable/disable port functions of each port
- Choose the speed/duplex of each port
- Enable/disable the flow of control of each port

Port Management Configuration Terms

[Web User Interface – Port Status]

The following picture shows the information of port status on the Web Console. There are 7 columns that show the port list, link status (Up or Down), speed, duplex mode, receive bytes, transmit bytes, and PoE status.

Status

PORT

No.	Link	Speed	Duplex	Rx Byte	Tx Byte	PoE
1	Down	10	half	0	0	No PD
2	Down	10	half	0	0	No PD
3	Up	100	full	151815	2677412	No PD
4	Down	10	half	0	0	No PD
5	Up	1000	full	3043222	939788	No PD
6	Down	10	half	0	0	No PD
	Down	10	half	0	0	No PD

[Web User Interface – Port Configuration]

Port Configuration

PORT

No.	Link	Port name:	Status	Speed/Duplex	Flow control
1	Down	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>
2	Down	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>
3	Down	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>
4	Down	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>
5	Up	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>
6	Down	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>
7	Down	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>
8	Down	<input type="text"/>	Enable ▾	Auto ▾	<input type="checkbox"/>

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
No.	The number of the port. From 1 to N, N depends on models.
Link	The port's link is Up or Down.
Port Name	User can assign a name to each port.
Status	"Enable" or "Disable" traffic/link of the port.
Speed/Duplex	Configure the bandwidth of each port. Default value is "Auto", means auto negotiation. Users can force it to 10Mbps with full/half duplex or 100Mbps with full/half duplex manually.
Flow Control	Use to avoid frame loss when traffic is congestion.

Overview

All our industrial PoE+ managed switches' name start with "P". All series of PoE switches are backward-compatible with IEEE802.3af to support any standard PoE Powered Devices (PD). Not only that, it also has four built-in IEEE802.3at-compliant ports that are able to support PoE output power up to 30W per port.

Ping Alarm

This function uses the ping command to enable or disable any PoE power output port. It enables users to time PoE ports by inserting any powered device's IP address and setting the interval time for a power recycle.

PoE Schedule

The PoE Schedule Interface enables users to set specific dates and times for each port to turn on or off for energy-saving or power-recycle powered devices.

PoE Configuration Terms

[Web User Interface – PoE Configuration]

POE Configuration

PoE PORT

No.	Status	Mode	Consumption
1	No PD Detected	Enable ▼	0.00W
2	No PD Detected	Enable ▼	0.00W
3	No PD Detected	Enable ▼	0.00W
4	No PD Detected	Enable ▼	0.00W
5	No PD Detected	Enable ▼	0.00W
	No PD Detected	Enable ▼	0.00W
	No PD Detected	Enable ▼	0.00W
	No PD Detected	Enable ▼	0.00W

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
No.	Mapping to port number
Status	"No PD Detected", "Supply", and "Disable"
Mode	"Enable" or "Disable" PoE
Consumption	Watts that switch supplied to PD

[Web User Interface – Ping Alarm]

Power over Ethernet

PING ALARM

PD	IP Address	Cycle Time(s)
1		
2		
3		
4		
5		

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
PD	Mapping to port number
IP Address	IP address of the PD
Cycle Time(s)	How long will switch ping the PD

[Web User Interface – Ping Alarm]

The following table is to describe the field of “Ping Alarm” on WEB UI.

Terms	Value Description
Monday~Sunday Enable	Enable PoE when today is the set day
Start time(hour)	When will PoE start providing power to PD
End time(hour)	When will PoE turn off. PoE only works during start time and end time.

The graph below is the WEB User Interface of “Ping Alarm” feature.

Power over Ethernet

PoE SCHEDULE

Port1	Port2	Port3	Port4	Port5	Port6	...
Monday Enable <input type="checkbox"/>						
Start time(hour):				Disable ▼		
End time(hour):				Disable ▼		
Tuesday Enable <input type="checkbox"/>						
Start time(hour):				Disable ▼		
End time(hour):				Disable ▼		
Wednesday Enable <input type="checkbox"/>						
Start time(hour):				Disable ▼		
End time(hour):				Disable ▼		
Thursday Enable <input type="checkbox"/>						
Start time(hour):				Disable ▼		
End time(hour):				Disable ▼		
Friday Enable <input type="checkbox"/>						
Start time(hour):				Disable ▼		
End time(hour):				Disable ▼		
Saturday Enable <input type="checkbox"/>						
Start time(hour):				Disable ▼		
End time(hour):				Disable ▼		
Sunday Enable <input type="checkbox"/>						
Start time(hour):				Disable ▼		
End time(hour):				Disable ▼		

Apply

Overview

Ethernet Ring Protection Switch (ERPS) is an Ethernet ring protection protocol that is used to prevent forming the loop in LAN, thus avoiding the Broadcast Storm Problem. The loop avoidance mechanism ensures that traffic flows on all but the RPL ring link. To achieve the loop-avoidance mechanism, ITU-T G.8032 defines three roles in ERPS, which are RPL Owner Node, RPL Neighbor Node and “None” Node. For the sake of simplicity, we use two scenarios to describe how to configure the ERPS in our device. You can choose to configure it as RPL-configured architecture as Figure 4 or Non-configure architecture as Figure 8.

Before Configuring ERPS

Before configuring ERPS, you need to disable spanning tree protocol (STP) because these two protocols run exclusively in a switch. The steps of disabling MSTP or RSPT protocol are as follows:

- Step 1 Open a web browser (IE, Chrome, Firefox, Opera...) and connect to a switch you want to configure.
- Step 2 Open the “RSTP Configuration” page.
- Step 3 Select “Mode” to “Disable”, and click “Apply” button.

- ▶ Status
- ▶ Basic Settings
- ▶ Port Management
- ▶ PoE
- ▶ ERPS
- ▶ Spanning Tree
 - ▶ RSTP Status
 - ▶ RSTP Configuration**
 - ▶ MSTI Status
 - ▶ MSTI Configuration
 - ▶ MSTI Port Configuration
- ▶ IGMP Snooping
- ▶ 802.1Q VLAN
- ▶ QoS
- ▶ Port Trunk
- ▶ Port Mirroring
- ▶ SNMP
- ▶ DHCP Server/Relay
- ▶ 802.1X
- ▶ UPnP
- ▶ Modbus
- ▶ System Warning
- ▶ MAC Table
- ▶ Maintenance
- ▶ Configuration
- ▶ Logout

RSTP/CIST Configuration

RSTP/CIST
Mode: Disable ▼
Root Priority: 32768 ▼
Root Hello Time: 2
Root Forward Delay: 15
Root Maximum Age: 20

RSTP/CIST PORT

No.	Path Cost(0:Auto,1-2000000000)	Priority	Admin	P2P	Edge	Admin Non STP
Port1	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼
Port2	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼
Port3	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼
Port4	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼
Port5	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼
Port6	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼
Port7	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼
Port8	0	128 ▼	True ▼	Auto ▼	False ▼	False ▼

Apply

Figure 3: Disable “RSTP” before enabling “ERPS”

ERPS Configuration Terms

[Web User Interface –ERPS configuration]

ERPS STATUS

ERPS Status

Protocol:	Disable
Ring ID:	1
Ring State:	Normal
Node State:	INITIAL
APS Channel:	1000
Revertive:	Enable

[Web User Interface –ERPS configuration]

ERPS Configuration

ERPS CONFIGURE

Protocol:	<input type="text" value="Disable"/>
Ring Port 0:	<input type="text" value="Port1"/>
Role:	<input type="text" value="None"/>
Ring Port 1:	<input type="text" value="Port2"/>
Role:	<input type="text" value="None"/>
Ring ID:	<input type="text" value="1"/>
APS Channel:	<input type="text" value="1000"/>
Revertive:	<input type="text" value="Yes"/>

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Protocol	“Enable” or “Disable” ERPS protocol
Ring Port 0	ERPS ring port 0, it could be map to real switch port 1 – port N, N depends on models. Do not set same as Ring port 1.
Ring Port 1	ERPS ring port 1, it could be map to real switch port 1 – port N, N depends on models. Do not set same as Ring port 0.

Continuing description of ERPS

Terms	Value Description
Role	<p>Set the ERPS role as Owner, Neighbor or “None”.</p> <p>“Owner” In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.</p> <p>“Neighbor” In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.</p> <p>“None” Besides Owner and Neighbor node, the rest of nodes are defined as “None” node.</p> <p>All node roles have the ability to block the port if the link attach to the port is failed and disconnected.</p>
Ring ID	ERPS ring ID. The range is from 1 to 239. Ring ID distinguishes different Ring topology.
Channel	ERPS APS Channel ID. The range is from 1 to 4094. It’s a channel to send PDUs of ERPS. It cannot be the same as existed VLAN ID.
RPL link	Ring Protection Link is a link as Figure 4 shows that the ring link is responsible for protecting the whole ring. Any traffic will not go through the protected RPL link because it is blocked by the Owner and Neighbor Nodes. By this blocking mechanism, the ring will not form a loop.
Revertive	<p>Set to Revertive (yes) or Non-revertive (no). The revertive mode works only under the scenario A at the RPL Owner node.</p> <p>[Revertive] While the revertive mode is set, the RPL link will be blocked in 5 minutes after recovery form link failure situation. Otherwise, it will remain unchanged of the blocking state. That is, the failed link port will block permanently until the next event happen.</p> <p>[Non-Revertive] The failed ring link the port attached to it will remain blocked even the situation is eliminated.</p>

Scenario A – RPL configured Architecture

There are three roles we need to configure in this scenario. The following will describe how to configure the three roles in our device.

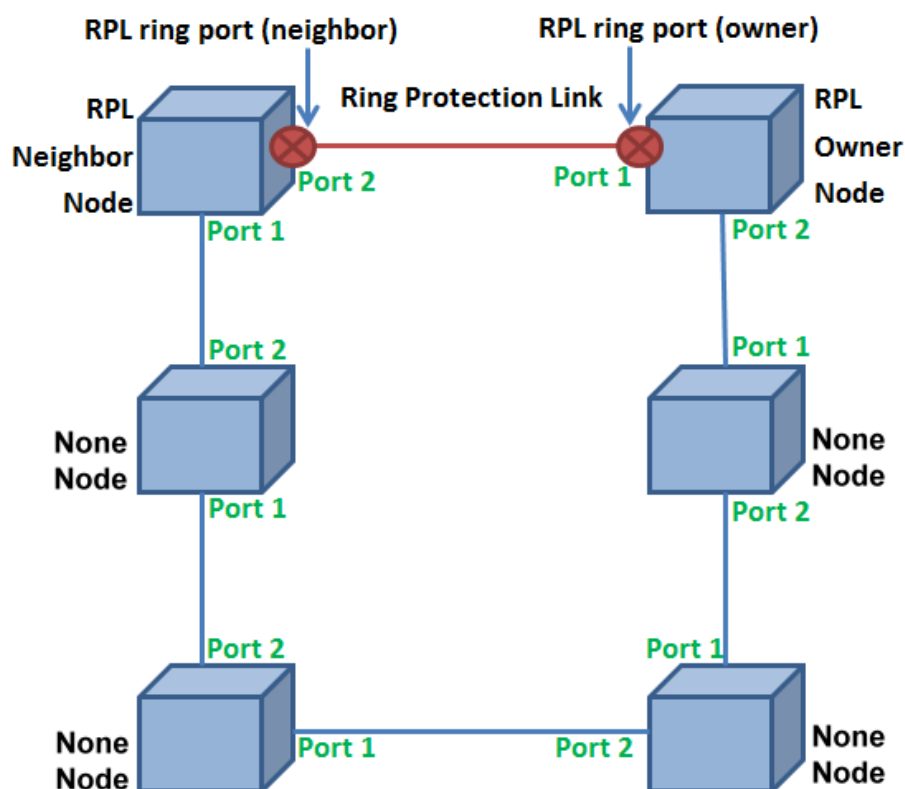


Figure 4: RPL-configured Architecture

Caution: Before enabling any ERPS protocols on any of the Ring Nodes, cautions must be taken not to forming a loop. You should leave at least one ring port unplugged until all nodes in the topology are ready.

[RPL Owner Node]

There is only one RPL Owner Node that could be set in a ring, so we choose one node as RPL owner node. Now we have to map the ERPS ring port to the real switch port. For example, we map the ERPS ring port to the switch port 1, and we set the port as RPL owner role. Then we map ERPS port 1 to switch port 2 and the role is set to None. The configurations are as the graph below.

The difference between to set and not to set the revertive mode is that if the revertive mode is set to “yes”, the ring will recover as same as Figure 4 after the ring state from ABNORMAL to NONE in 5 minutes. Otherwise, the blocked port will remain blocked permanently unless we reconfigure it. After the configurations, don’t forget to press the “Apply” button on the bottom right corner.

ERPS Configuration

ERPS CONFIGURE

Protocol:	Enable ▼
Ring Port 0:	Port1 ▼
Role:	Owner ▼
Ring Port 1:	Port2 ▼
Role:	None ▼
Ring ID:	1
APS Channel:	1000
Revertive:	Yes ▼

Apply

Figure 5: Configure Owner Node

[RPL Neighbor Node]

On RPL Neighbor Node, the real switch port set to be a neighbor port (0 or 1) must map to the owner port. So the link between neighbor port and owner port forms the Ring Protection Link (RPL). After the configurations, don't forget to press the "Apply" button on the bottom right corner. The configurations are as the graph (Figure 6) below.

ERPS Configuration

ERPS CONFIGURE

Protocol:	Enable ▼
Ring Port 0:	Port1 ▼
Role:	None ▼
Ring Port 1:	Port2 ▼
Role:	Neighbor ▼
Ring ID:	1
APS Channel:	1000
Revertive:	Yes ▼

Apply

Figure 6: Configure Neighbor Node

[None Node]

The configurations are as followed graph. We need to map the ERPS ring ports to real switch ports. Do not set ERPS ring port both to the same switch port, cause the incorrect configurations may lead to unexpected errors. The configurations are as the graph below.

ERPS Configuration

ERPS CONFIGURE

Protocol:	<input type="text" value="Enable"/>
Ring Port 0:	<input type="text" value="Port1"/>
Role:	<input type="text" value="None"/>
Ring Port 1:	<input type="text" value="Port2"/>
Role:	<input type="text" value="None"/>
Ring ID:	<input type="text" value="1"/>
APS Channel:	<input type="text" value="1000"/>
Revertive:	<input type="text" value="Yes"/>

Figure 7: Configure None Node

Scenario B – Non-configured Architecture

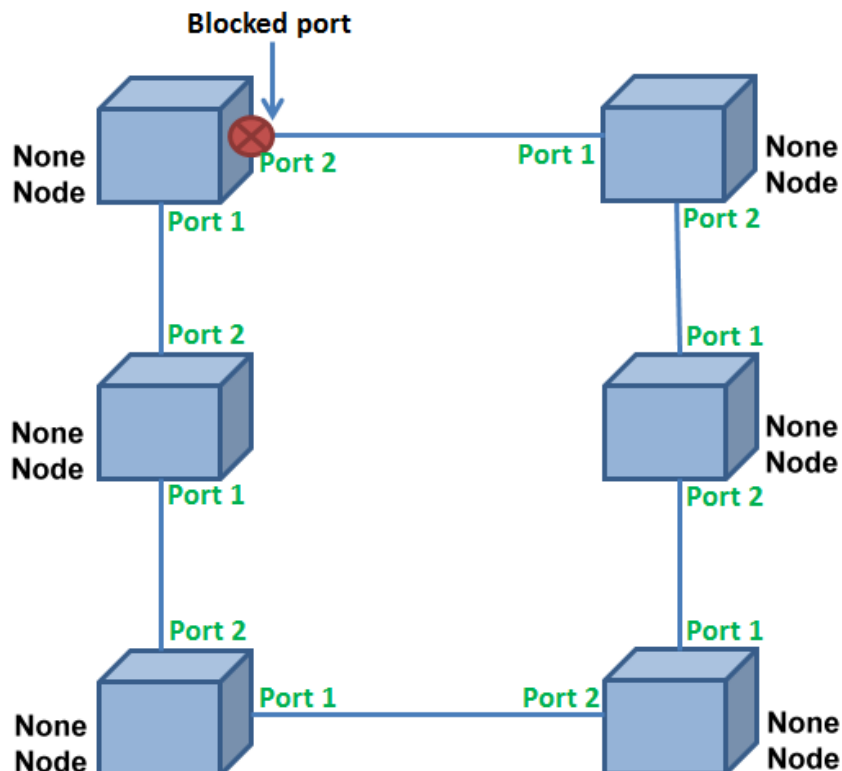


Figure 8: Non-configured Architecture

Caution: Before enabling any ERPS protocols on any of the Ring Nodes, cautions must be taken to not form a loop. You should leave at least one ring port unplugged until all nodes in the topology are ready.

If you do not want to configure RPL owner and neighbor node, the ERPS could still work well under the mechanism by blocking one of the ring ports in the ERPS ring topology. As Figure 8 shows, the ERPS is blocked at one of the ring node ring port. The blocked port is chosen by an election mechanism that is decided by the MAC address. Because the MAC address is unique, it just chooses the biggest MAC as the blocking node.

However, we still have to configure the port, let the ERPS ring port map to the real switch port. For instance, we map the ERPS port 0 to switch port 1 and ERPS port 1 to switch port 2. Of course, the protocol must be enabled if you want to. And the revertive mode has no effect in this scenario. After the configurations, press the “apply” button on the bottom right corner. The configurations are as followed (Figure 9) graph.

ERPS Configuration

ERPS CONFIGURE

Protocol:	Enable ▼
Ring Port 0:	Port1 ▼
Role:	None ▼
Ring Port 1:	Port2 ▼
Role:	None ▼
Ring ID:	1
APS Channel:	1000
Revertive:	Yes ▼

Apply

Figure 9: Configure Non-RPL Topology

Overview

Defined in the IEEE Standard 802.1d, the Spanning Tree Protocol (STP) can be created in an interconnected network of layer-2 switches. There are 2 additional branches of STP: RSTP and MSTP.

Rapid Spanning Tree Protocol (RSTP)

Containing most of STP's fundamental operation features, the Rapid Spanning Tree Protocol (RSTP), defined in the IEEE 802.1w, is an elevated solution of STP. In essence, RSTP generates a waterfall effect away from the root bridge. Each designated bridge then proposes to its neighbors to determine whether or not it can make a swift transition.

Multiple Spanning Tree Protocol (MSTP)

The Multiple Spanning Tree Protocol (MSTP), defined in the IEEE 802.1s, creates opportunities for different VLANs to move along independent instances of spanning tree. It can be more useful than the standard STP in a large networking setting that uses many VLANs because MSTP removes the need of having different STP for each VLAN.

MSTP has the ability to systemize a group of VLANs into a single Multiple Spanning Tree Instance (MSTI). As a matter of fact, different root switches and STP parameters are individually configurable for each specific MSTI. Generally, two MSTIs are used in a network for ease of implementation. Thus, individual links can be active for each MSTI, enabling a degree of load-balancing.

Spanning Tree Configuration Terms

[Web User Interface – RSTP Status]

RSTP/CIST Status

ROOT STATUS

Bridge ID:	8.000.9C:8D:D3:FF:FF:00
Root Priority:	32768
Root Port:	none
Root Path Cost:	0
Hello Time:	2
Forward Delay:	15
Max Age:	20

RSTP/CIST PORT STATUS

No.	Role	Path State	Port Cost	Port Priority	Oper P2P	Oper Edge
Port1	Disabled	Discarding	2000000000	128	Shared	Non-Edge
Port2	Disabled	Discarding	2000000000	128	Shared	Non-Edge
Port3	Disabled	Discarding	2000000000	128	Shared	Non-Edge
Port4	Designated	Forwarding	200000	128	Shared	Edge
Port5	Disabled	Discarding	2000000000	128	Shared	Non-Edge
Port6	Disabled	Discarding	2000000000	128	Shared	Non-Edge
	Disabled	Discarding	2000000000	128	Shared	Non-Edge

[Web User Interface – RSTP Configuration]

RSTP/CIST Configuration

RSTP/CIST

Mode:	<input type="text" value="RSTP"/>
Root Priority:	<input type="text" value="32768"/>
Root Hello Time:	<input type="text" value="2"/>
Root Forward Delay:	<input type="text" value="15"/>
Root Maximum Age:	<input type="text" value="20"/>

RSTP/CIST PORT

No.	Path Cost(0:Auto,1-2000000000)	Priority	Admin P2P	Edge	Admin Non STP
Port1	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="True"/>	<input type="text" value="Auto"/>	<input type="text" value="False"/>
Port2	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="True"/>	<input type="text" value="Auto"/>	<input type="text" value="False"/>
Port3	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="True"/>	<input type="text" value="Auto"/>	<input type="text" value="False"/>
Port4	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="True"/>	<input type="text" value="Auto"/>	<input type="text" value="False"/>
Port5	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="True"/>	<input type="text" value="Auto"/>	<input type="text" value="False"/>
Port6	<input type="text" value="0"/>	<input type="text" value="128"/>	<input type="text" value="True"/>	<input type="text" value="Auto"/>	<input type="text" value="False"/>

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

RSTP / CIST

Terms	Value Description
Mode	“RSTP”: enable RSTP; “MSTP”: enable MSTP “Disable”: disable Spanning Tree Protocol
Root Priority	The range is 0 to 61440. Use to decide the “Root Bridge”. It will choose the bridge with the lowest value of Root Priority as the Root Bridge in the topology. The default value is 32768, and has to be the multiple of 4096.
Root Hello Time	The range is 1 to 10. Use to control the time of sending BPDU packet to check RSTP current status.
Root Forward Delay	The range is 4 to 30. Before changing RSTP state from learning/listening to forwarding, a port has to wait for “Root Forward Delay” seconds.
Root Maximum Age	The range is 6 to 40. A bridge will wait “Root Maximum Age” seconds for STP configuration message. After “Root Maximum Age”, it will try to reconfigure.

RSTP / CIST Port

Terms	Value Description
Path Cost	The range is 1 to 200000000. It defines the transmitting cost from this port to another switch. Set it to 0 means automatic decision.
Priority	The range is 0 to 240. Priority has to be the multiple of 16. It is used to decide which port to block to avoid loop in the ring topology.
Admin P2P	Decide the LAN segment is Point-to-point or shared medium. "True" to enable P2P, "False" to disable P2P.
Edge	Manually decide the port is an edge port or not. Set it to "True" means the port is an edge port, and set it to "False" means the port is never an edge port. Or set it to "Auto", system will decide it automatically.
Admin Non STP	"True" means the port is not in the Spanning-Tree topology. And "False" means the port is attending in the Spanning-Tree topology.

[Web User Interface – MSTI Status]

MSTI Status

Instance ID:

ROOT STATUS

Root Address:	8.001.00:11:22:33:44:55
Root Priority:	32768
Root Port:	none
Root Path Cost:	0

MSTI PORT STATUS

No.	Role	Path State	Port Cost	Port Priority
Port1	Disabled	Discarding	200000000	128
Port2	Disabled	Discarding	200000000	128
Port3	Disabled	Discarding	200000000	128
Port4	Designated	Forwarding	200000	128
Port5	Disabled	Discarding	200000000	128
Port6	Disabled	Discarding	200000000	128
	Disabled	Discarding	200000000	128

[Web User Interface – MSTI Configuration]

MSTI Configuration

MSTI CONFIGURATION

Name:	<input type="text" value="9C:8D:D3:FF:FF:00"/>
Revision(0-65535):	<input type="text" value="0"/>

MSTI INSTANCE

Instance.	Vlan group	Priority
1	<input type="text"/>	32768 ▼
2	<input type="text"/>	32768 ▼
3	<input type="text"/>	32768 ▼
4	<input type="text"/>	32768 ▼
5	<input type="text"/>	32768 ▼
6	<input type="text"/>	32768 ▼
7	<input type="text"/>	32768 ▼
8	<input type="text"/>	32768 ▼
9	<input type="text"/>	32768 ▼
10	<input type="text"/>	32768 ▼
11	<input type="text"/>	32768 ▼
12	<input type="text"/>	32768 ▼
13	<input type="text"/>	32768 ▼
14	<input type="text"/>	32768 ▼
15	<input type="text"/>	32768 ▼

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

MSTI Configuration

Terms	Value Description
Name	Name of the MSTP.
Revision	The range is 0 to 65535. MSTP topology change only impacts the members with the same revision.

MSTI Instance

Terms	Value Description
Instance	We provide 15 instances, from 1 to 15.
VLAN Group	Enter 1 or more VLAN ID to group them in the same instance.
Priority	The range is 0 to 61440. Use to decide the “Root Bridge”. It will choose the bridge with the lowest value of Root Priority as the Root Bridge in the topology. The default value is 32768, and has to be the multiple of 4096.

[Web User Interface – MSTI Port Configuration]

MSTP Configuration

MSTI PORT

Instance1
Instance2
Instance3
Instance4
Instance5
Instance6
Instance7
Instance8
Instance9
Instance10
Instance11
Instance12
Instance13
Instance14
Instance15

Cost:
Port1
Port2
Port3
Port4
Port5
Port6

Priority:
Port1
Port2
Port3
Port4
Port5
Port6

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Instance 1 ~ 15	Select instance 1 to 15 to configure their port cost and priority.
Cost	The range is 1 to 200000000. It defines the transmitting cost from this port to another switch port.
Priority	The range is 0 to 240. Priority is used to decide which port to block to avoid loop in the instance.

Overview

The Internet Group Management Protocol (IGMP) is a communications protocol used by Internet Protocol multicast groups (IP hosts and adjacent multicast routers) to establish group memberships. It is an essential part of IP multicast. There are 3 versions of IGMP: IGMP v1, v2, and v3. It also supports query group up to 256 groups.

Enabling IGMP Snooping kick-starts an analyzation of IGMP packets between hosts and multicast routers. The analyzation proceeds as follows: the switch receives an IGMP report from a host about a specific multicast group and adds the host's port number to that group's multicast list. Likewise, the switch removes the host's port from the table entry when an IGMP leaves.

An important feature of IGMP Snooping is its ability to effectively streamline multicast traffic from bandwidth intensive IP applications, meaning that the switch will only direct multicast traffic to the hosts in that traffic. Although this reduction requires additional memory to handle the multicast tables, it also reduces the packet processing at the switch while decreasing the workload at the end hosts (since their network cards will not receive and filter all the multicast traffic generated in the network).

IGMP Snooping Configuration Terms

[Web User Interface – IGMP Snooping Stream Table]

IGMP Snooping Stream Table shows the information of IGMP Snooping results, including multicast group and member ports. With this table, the switch can forward multicast only to the mapping ports and avoid redundant broadcast traffic.

IGMP Snooping Table

IGMP SNOOPING TABLE

Group	Port
224.0.1.60	5
239.255.255.250	2,5

[Web User Interface – IGMP Snooping Configuration]

IGMP Snooping Configuration

IGMP SNOOPING

IGMP Snooping Enable: ☒

IGMP QUERIER

Querier Enable: ☐

Query Interval(s)

Query Max Response Time(s)

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

IGMP Snooping

Terms	Value Description
IGMP Snooping Enable	Check the checkbox to enable IGMP Snooping Function. IGMP Snooping is enabled by default.

IGMP Querier

Terms	Value Description
Querier Enable	Check the checkbox to enable IGMP Querier. When Querier is enabled, switch will send IGMP query periodically.
Querier Interval(s)	How long will the IGMP query sent. The first query will be sent in 1/3 querier interval time.
Querier Max Response Time(s)	Wait for the report. If there is no report of a group after “Querier Max Response Time”, switch will remove the group’s information.

Overview

A Virtual LAN (VLAN) enables users to segregate network traffic (as it is a network grouping that restricts the broadcast domain), meaning that only the members of the VLAN are able to receive traffic from that VLAN. Even though all the network devices are still plugged into the same switch, creating a VLAN from a switch is essentially reconnecting a group of network devices to another Layer 2 switch.

802.1Q VLAN is a tagged-based VLAN that meets the IEEE 802.1Q specification standard, making it feasible to generate a VLAN across devices from various switch suppliers. IEEE 802.1Q VLAN inserts a “tag” containing a VLAN Identifier (VID) that specifies VLAN numbers into the Ethernet frames.

[Vitess not ready!] This VLAN is supported by us. As well, user defined management VLAN is available, enabling users to connect our switch to other “commercial” products that have set a non VLAN 1 management VLAN.

802.1Q VLAN Configuration Terms

Our industrial managed switches allow users to generate VLAN Group names and choose “Tag” or “Untag” for each port. This is enabled through the VLAN setting interface (default VLAN 1 setting is “Untag” for each port).

[Web User Interface – 802.1Q VLAN Configuration]

802.1Q VLAN

The screenshot displays the '802.1Q VLAN' configuration page. It features a table with the following structure:

ID	name	1	2	3	4	5	6
1		Untag	Untag	Untag	Untag	Untag	Untag

Below the table, there is an 'Add' button on the left and a 'Delete' button on the right. An 'Apply' button is positioned at the bottom right of the interface.

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Management VLAN ID	Set the VLAN ID of management VLAN. Users have to configure other settings done, and configure this field finally.
802.1Q VLAN ID	The ID of this VLAN. VLANs that have the same ID will consider to be the same group.

802.1Q VLAN Name	The name of this VLAN. The same VLAN in the different switches can have different name.
------------------	---

[Web User Interface – 802.1Q VLAN Port Configuration]

802.1Q VLAN Port

802.1Q VLAN PVID

Port	PVID
1	1
2	1
3	1
4	1
5	1
6	1

802.1Q VLAN FILTER

Port	Filter
1	None
2	None
3	None
4	None
5	None
6	None

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
802.1Q VLAN PVID	When a frame comes into the port, it will be tagged with the PVID if the frame is without VLAN tag.
802.1Q VLAN Filter	<p>An incoming frame will be dropped or kept forwarding according to the filter.</p> <ul style="list-style-type: none"> • None: All frames can keep forwarding. • Tagged: Only the frames with 802.1Q tag can keep forwarding, untagged frames will be dropped. • Untagged: Only the frames without 802.1Q tag can keep forwarding, tagged frames will be dropped.

Overview

Quality of Service (QoS) is used to ensure the priority of network traffic receiving correct treatments based on specific criteria. This eliminates the unpredictability issue of network traffic.

There are 3 types of Traffic Prioritization: port base, 802.1p/COS and TOS/DSCP. With this function, the traffic is classifiable as 4 classes for differential network application, of which our industrial managed switches support 4 priority queues.

Type-of-service (ToS)

Type of Service, or ToS, is applied as the IPv4 ToS priority. Fully decoded into 64 possibilities, the most significant 6 bits of the ToS field used results in a singular code that is then compared with the matching bit in the IPv4 ToS priority control bit (0~63). The priority from the 6-bit ToS field in the IP header is determined this way.

QoS Configuration Terms

[Web User Interface – QoS Classification]

Qos Classification

QoS CLASSIFICATION

Queue Scheduling	Weighted ▼
Trust Mode:	
Port 1	DSCP ▼
Port 2	DSCP ▼
Port 3	DSCP ▼
Port 4	DSCP ▼
Port 5	DSCP ▼
Port 6	DSCP ▼
DSCP ▼	
Default Cos:	
Port 1	0 ▼
Port 2	0 ▼
Port 3	0 ▼
Port 4	0 ▼
Port 5	0 ▼
Port 6	0 ▼
0 ▼	

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Queue Scheduling	<p>“Weighted” means “Weighted Round Robin”. All traffic can be forwarded by a fix percentage.</p> <p>“Strict” means “Strict Priority Queuing”. Traffic is forwarded sequentially according to the priority, the highest priority port transmit first.</p>
Trust Mode	<p>“DSCP” refers to ToS mapping.</p> <p>“CoS” refers to CoS mapping.</p>
Default CoS	If “Trust Mode” is set to “CoS” and the incoming packet is without priority tag, system will use “Default CoS” priority to forward it.

[Web User Interface – CoS Mapping]

CoS Mapping

CoS MAPPING

CoS	Priority
0	2
1	1(Lowest)
2	3
3	4
4	5
5	6
6	7
7	8(Highest)

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
CoS	There are 8 classes, from 0 to 7.
Priority	<p>Map a class to a priority queue.</p> <p>We provide 8 queues from 1 to 8. The highest priority queue is 8, and the lowest priority queue is 1.</p> <p>* 5/6-port models provide only 4 queues from 1 to 4.</p>

[Web User Interface – ToS Mapping]

ToS Mapping

ToS MAPPING

ToS	Priority	ToS	Priority	ToS	Priority	ToS	Priority
0x00(0)	1(Lowe ▼)	0x40(16)	3 ▼	0x80(32)	5 ▼	0xC0(48)	7 ▼
0x04(1)	1(Lowe ▼)	0x44(17)	3 ▼	0x84(33)	5 ▼	0xC4(49)	7 ▼
0x08(2)	1(Lowe ▼)	0x48(18)	3 ▼	0x88(34)	5 ▼	0xC8(50)	7 ▼
0x0C(3)	1(Lowe ▼)	0x4C(19)	3 ▼	0x8C(35)	5 ▼	0xCC(51)	7 ▼
0x10(4)	1(Lowe ▼)	0x50(20)	3 ▼	0x90(36)	5 ▼	0xD0(52)	7 ▼
0x14(5)	1(Lowe ▼)	0x54(21)	3 ▼	0x94(37)	5 ▼	0xD4(53)	7 ▼
0x18(6)	1(Lowe ▼)	0x58(22)	3 ▼	0x98(38)	5 ▼	0xD8(54)	7 ▼
0x1C(7)	1(Lowe ▼)	0x5C(23)	3 ▼	0x9C(39)	5 ▼	0xDC(55)	7 ▼
0x20(8)	2 ▼	0x60(24)	4 ▼	0xA0(40)	6 ▼	0xE0(56)	8(Highe ▼
0x24(9)	2 ▼	0x64(25)	4 ▼	0xA4(41)	6 ▼	0xE4(57)	8(Highe ▼
0x28(10)	2 ▼	0x68(26)	4 ▼	0xA8(42)	6 ▼	0xE8(58)	8(Highe ▼
0x2C(11)	2 ▼	0x6C(27)	4 ▼	0xAC(43)	6 ▼	0xEC(59)	8(Highe ▼
0x30(12)	2 ▼	0x70(28)	4 ▼	0xB0(44)	6 ▼	0xF0(60)	8(Highe ▼
0x34(13)	2 ▼	0x74(29)	4 ▼	0xB4(45)	6 ▼	0xF4(61)	8(Highe ▼
0x38(14)	2 ▼	0x78(30)	4 ▼	0xB8(46)	6 ▼	0xF8(62)	8(Highe ▼
0x3C(15)	2 ▼	0x7C(31)	4 ▼	0xBC(47)	6 ▼	0xFC(63)	8(Highe ▼

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
ToS	There are 64 types, from 0 to 63. It represents the 6-bit tag called DSCP in the ToS tag.
Priority	<p>Map a type to a priority queue.</p> <p>We provide 8 queues from 1 to 8. The highest priority queue is 8, and the lowest priority queue is 1.</p> <p>* 5/6-port models provide only 4 queues from 1 to 4.</p>

Overview

Port Trunk, also called “Link Aggregation”, is a method of combining multiple network connections in parallel. It is to increase throughput beyond what a single connection could sustain. For example, if we need a 5G link but we only have 1G port, we can use port trunk and link 5 1G port to obtain a 5G trunk.

We support 2 types of Port Trunk. One is LACP (dynamic) and the other is Static. LACP mode is more flexible, and it can change mode to use trunk or single port. Dynamic Port Trunk also provides a redundancy in case one of the links should fail. If one of the trunk members is failed, it will work well in LACP mode, but it will link down if using static mode. Static mode is still necessary, because some devices only support static trunk.

Port Trunk Configuration Terms

[Web User Interface – Trunk Status]

In the “Trunk Status” page, we can see the trunk members and trunk mode. It’s easy to manage the mapping of ports and trunks with this table.

Trunk Status

AGGREGATION

Group	Type	Port
1	-	-
2	lacp	1,2
3	-	-
4	-	-
5	lacp	5,6
6	-	-
7	-	-
8	-	-

[Web User Interface – Trunk Configuration]

Trunk Configuration

AGGREGATION GROUP TYPE

Group ID	Trunk Type
Trunk1	LACP ▼
Trunk2	LACP ▼
Trunk3	LACP ▼
Trunk4	LACP ▼
Trunk5	LACP ▼
Trunk6	LACP ▼
Trunk7	LACP ▼
Trunk8	LACP ▼

AGGREGATION GROUP MEMBER

PORT NO.	Group ID
Port1	None ▼
Port2	None ▼
Port3	None ▼
Port4	None ▼
Port5	None ▼
Port6	None ▼
	None ▼

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Aggregation	Show the status of Port Trunk. List all Trunks and show their type and members.

Overview

Port Mirroring feature can capture the traffic of other specified ports. We can use it to observe the network traffic and analysis the packets to resolve problems.

Port Mirroring Configuration Terms

[Web User Interface –Port Mirroring]

Port Mirroring

PORT MIRRORING

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Port Mirror Mode	Check the checkbox to enable Port Mirroring.
Go to Interface	Configure the mirroring destination port.
Monitor Direction	<p>“Tx” means only mirroring transmitting traffic.</p> <p>“Rx” means only mirroring receiving traffic.</p> <p>“Both” means mirroring both transmitting and receiving traffic.</p>
Source Port	Select the mirroring source ports. Users can select one or more ports to monitor, but the destination port is disabled to select as source port.

Overview

Simple Network Management Protocol (SNMP) is used for collecting information from various network devices, such as servers, switches, hubs and routers, on an IP network. Management systems discover problems by interpreting traps or change notices from network devices implementing SNMP. This collection of information allows network administrators to manage network performance, solve issues, and plan for future growth.

SNMP Configuration Terms



[Web User Interface – SNMP Agent]

SNMP Agent

SNMP GENERAL

SNMP Version:	v1 , v2c , v3 ▼
Read-Only Community	public
Read and Write Community	private

SNMP v3

Admin Auth level:	Auth-only ▼
Admin Auth Type:	SHA ▼
Auth Passphrase 
Admin Data Encrypt Type:	AES ▼
Encrypt Passphrase 
User Auth level:	Auth-only ▼
User Auth Type:	SHA ▼
Auth Passphrase 
User Data Encrypt Type:	AES ▼
Encrypt Passphrase 

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

SNMP General

Terms	Value Description
SNMP Version	Switches support SNMP v1, v2c, and v3 server. Users can enable all SNMP server v1, v2c and v3, or enable only v1 and v2c, or enable only enable v3. Default SNMP server is enabled, set version to "None" to disable it.
Read-Only Community	Using "Read-Only Community" on the SNMP MIB walk utility can only read information.
Read and Write Community	Using "Read and write Community" on the SNMP MIB walk utility not only can read information, but can write/edit part of information.

SNMP V3

There are 2 accounts using SNMP v3 authentication. These 2 accounts are "admin" and "user". In this section, it introduces the authentication settings and encryption information.

Terms	Value Description
Admin Auth level	"Auth-only" means only do authentication but not encrypt data. "Both" means both do authentication and encrypt data. "None" means not do authentication and not encrypt data.
Admin Auth Type	The method used to encrypt the passphrase
Auth Passphrase	"Auth Passphrase" is a string used to authenticate (Admin).
Admin Data Encrypt Type	The method used to encrypt the data.
Encrypt Passphrase	"Encrypt Passphrase" is a string used to encrypt data (Admin).
User Auth level	"Auth-only" means only do authentication but not encrypt data. "Both" means both do authentication and encrypt data. "None" means not do authentication and not encrypt data.
User Auth Type	The method used to encrypt the passphrase
Auth Passphrase	"Auth Passphrase" is a string used to authenticate (User).
User Data Encrypt Type	The method used to encrypt the data.
Encrypt Passphrase	"Encrypt Passphrase" is a string used to encrypt data (User).

[Web User Interface – SNMP Trap]

Trap Setting

SNMP

Trap Mode:	<input type="text" value="None"/>
Inform Retry:	<input type="text" value="10"/>
Inform Timeout:	<input type="text" value="30"/>
Trap Destination IP:	<input type="text"/>
Community:	<input type="text" value="public"/>

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Trap Mode	SNMP Trap is disabled (set to “None”) by default. Users can set it to “Trap v1”, “Trap v2c”, or “Inform (v2c)”. If users set it to “Trap”, the trap message will only send once, but if set the mode to “Inform”, the trap message will send “Inform Retry” times.
Inform Retry	The trap message will be sent “Inform Retry” times. This field works only when “Trap Mode” is set to “Inform”.
Inform Timeout	The trap message will be sent after “Inform Timeout” expired. This field works only when “Trap Mode” is set to “Inform”.
Trap Destination IP	The Destination IP that trap message will be sent to.
Community	“Community” is a string that will show in the trap message.

Overview

DHCP Client & Server

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol. It is used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters. For example, devices can request IP addresses for interfaces from a DHCP server. Using DHCP can also reduce the need for a network administrator or a user to configure these settings manually.

The protocol operates based on the client-server model. When DHCP Clients connect to a network, they will send a broadcast query to request necessary information from a DHCP server. DHCP Servers manage a pool of IP address and network configuration information. If they get queries from DHCP Clients, they will automatically distribute IP address and network parameters to them.

DHCP Relay Agent

DHCP Relay Agents help DHCP Clients forwarding request to DHCP Servers. With DHCP Relay Agents, DHCP Servers and Clients will not know each other. A Relay Agent can connect to more than 1 DHCP Server, so that DHCP Clients will have more resources.

DHCP Relay Option 82

We can also use the information of DHCP Relay Option 82 to distribute IP address. Our option 82 format is cisco-like, it contains Circuit ID and Remote ID. The packets format of Circuit ID and Remote ID are shown as Figure 1 and Figure 2, and the detail of packet fields are in the Table 1 and Table 2. Using DHCP Relay Option 82, the IP addresses will get more controllable.

DHCP Configuration Terms

[Web User Interface – DHCP Client configuration]

IP Setting

IP CONFIGURATION

DHCP Client:	<input type="checkbox"/>
IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text"/>
DNS:	<input type="text"/>

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
DHCP Client	“Enable” or “Disable” DHCP Client.
IP Address	Static IP address setting. Assign the IP address that the network is using.
Subnet Mask	Assign the subnet mask of the IP address.
Gateway	The IP address that connects the LAN to the Internet.
DNS	The IP address of DNS.

[Web User Interface – DHCP Server configuration]

DHCP Server

DHCP SERVER

Server Status:	Down
Enable:	<input type="checkbox"/>
Included Start Address:	<input type="text"/>
Included End Address:	<input type="text"/>
Default Gateway:	<input type="text"/>
Name Server:	<input type="text"/>
Lease Time:	<input type="text" value="60"/>

[Apply](#)



The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Server Status	DHCP Server Status, It shows “Down” when “Disable”, and it shows “Up” when “Enable”.
Enable	“Enable” or “Disable” DHCP Server.
Included Start Address	The start address of the pool that DHCP Server managed.
Included End Address	The end address of the pool that DHCP Server managed.
Default Gateway	The IP address that connects the LAN to the Internet.
Name Server	The IP address of DNS.
Lease Time	A controllable time period that DHCP server will reclaim IP addresses.

[Web User Interface – DHCP Server Binding configuration]

Binding Table Configuration

DHCP SERVER BINDING

ID[01-32]	Binding MAC	Binding IP	
<input type="text"/>	<input type="text"/>	<input type="text"/>	 Delete
 Add			

 Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
ID	“Enable” or “Disable” DHCP Client.
Binding Mac	The MAC address of the device that wishes binding.
Binding IP	The IP address that will assign to the device with the Binding MAC address.

[Web User Interface – DHCP Relay configuration]

DHCP Relay

DHCP RELAY

Enable:	<input type="checkbox"/>
Relay option82:	<input type="checkbox"/>
Relay to server1:	<input type="text"/>
Relay to server2:	<input type="text"/>
Relay to server3:	<input type="text"/>
Relay to server4:	<input type="text"/>

DHCP RELAY UNTRUST

No.	Relay Untrust
1	<input type="text" value="Disable"/>
2	<input type="text" value="Disable"/>
3	<input type="text" value="Disable"/>
4	<input type="text" value="Disable"/>
5	<input type="text" value="Disable"/>
6	<input type="text" value="Disable"/>
	<input type="text" value="Disable"/>

 Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

DHCP RELAY

Terms	Value Description
Enable	“Enable” or “Disable” DHCP Relay Agent
Relay Option 82	“Enable” or “Disable” DHCP Relay Option 82
Relay to server1	The IP address of the first DHCP Server that Relay Agent connect to
Relay to server2	The IP address of the second DHCP Server that Relay Agent connect to
Relay to server3	The IP address of the third DHCP Server that Relay Agent connect to
Relay to server4	The IP address of the fourth DHCP Server that Relay Agent connect to

DHCP RELAY UNTRUST

Terms	Value Description
Relay Untrust	Per-port “Enable” or “Disable” Relay Untrust. DHCP frames can pass that port when it set to “Enable” only.

Overview

802.1X is an IEEE Standard for Port-based Network Access Control. It provides an authentication mechanism to devices that wish to attach to a LAN or WLAN. This port-based network access control protocol contains 3 parts, supplicant, authenticator, and authentication server. With 802.1X authentication, we can link a username with an IP address, MAC address, and port. This provides greater visibility into the network. 802.1X also provides more security because it only allows traffic transmitting on authenticated ports or MAC addresses. Although the IEEE standard defined it as a “Port-based” control, to provide more robust service, we implement our 802.1X to a “MAC-based” access control.

RADIUS

RADIUS is used in the authentication process. Database of authorized users is maintained on a RADIUS server. There is an authenticator, our switch enabling 802.1X, to forward the authentication requests between authentication (RADIUS) server and client. Allowing or denying the requests decides if the client can connect to a LAN/WAN or not.

802.1X Configuration Terms

[Web User Interface – 802.1X]

802.1X

802.1X

802.1X Enable:

☐

Server Type:

802.1X PORT

No.	Enable Port	Re-Auth	Re-Auth Period(Sec.)
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3600

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

802.1X

Terms	Value Description
802.1X Enable	Check the checkbox to enable "802.1X" protocol.
Server Type	"Local" for authenticating with local server setting on the "Local Database" page. "RADIUS" for authenticating with remote RADIUS server setting on the "RADIUS Server" page.

802.1X Port

Terms	Value Description
No.	The number of ports, from 1 to N, N depends on models.
Enable Port	Check the checkbox(es) to enable authentication before connecting to a LAN or WAN.
Re-Auth	"Re-Auth" means re-authenticate, it is enabled by default. Check the checkbox(es) to enable re-authentication after "Re-Auth Period" seconds.
Re-Auth Period(Sec.)	"Re-Auth Period" default value is 3600 seconds (60 minutes). Switch will ask the client for re-authentication every "Re-Auth Period" seconds.

[Web User Interface – Local Database]

Local Database

LOCAL DATABASE

User Nmae

Password

Confirm Password

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.



Terms	Value Description
User Name	The user name use to authenticate in 802.1X when server set to "Local".
Password	The password use to authenticate in 802.1X when server set to "Local".
Confirm Password	Fill in the password again.

[Web User Interface – RADIUS Server]


Users can set 2 RADIUS server information that will try to authenticate the second server is authentication with the first server is failed.

Radius Server

RADIUS SERVER

1st Server IP	<input type="text"/>
1st Server Port	<input type="text" value="1812"/>
1st Server Shared Key	<input type="text"/> 
2nd Server IP	<input type="text"/>
2nd Server Port	<input type="text" value="1812"/>
2nd Server Shared Key	<input type="text"/> 

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Server IP	IP Address of RADIUS server
Server Port	"Server Port" default value is 1812. Switch will communicate with RADIUS server via this port.
Server Shared Key	Shared key is used to authenticate authenticator (switch) and authentication (RADIUS) server. Click "  " icon to show the shared key.

Overview

Universal Plug and Play (UPnP) is a set of networking protocols that is promoted by the UPnP Forum. UPnP Protocol permits networked devices to discover each other's presence on the network and seamlessly establish functional network services for data sharing, communications, and entertainment.

The concept of UPnP is an extension of plug-and-play, a technology for dynamically attaching devices directly to a computer. But UPnP is not directly related to the earlier plug-and-play technology any more. UPnP devices are "plug-and-play" in that when connected to a network they automatically establish working configurations with other devices.

UPnP Configuration Terms

[Web User Interface – UPnP configuration]

UPnP

UPnP

UPnP Enable: ☐

UPnP Advertisement Interval (sec):

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
UPnP Enable	"Enable" or "Disable" UPnP protocol
UPnP Interval	UPnP Interval is the setting of Advertisement interval. It controls the time of sending advertisement.

Overview

Modbus is a serial communications protocol that is used with programmable logic controllers (PLCs). It is a commonly, simple, and robust available method of connecting industrial devices. Modbus TCP, or Modbus Messaging on TCP/IP, is Modbus RTU with TCP interface and can run on Ethernet. It can carry data of Modbus message structure between connecting devices running Modbus. According to the standard, Modbus encapsulates the message with an Ethernet TCP/IP wrapper. Enable Modbus TCP, we only obtain the encapsulated data, and with other utilities, we can understand the real meaning.

MODBUS Data Map and Information

The data map addresses of Barox switches shown in the following table for **Function Code 6**

System Information

Address Offset	Data Type	Interpretation	Description
0x0000 to 0x0005	1 word	HEX	Port 1 to 6 Status 0x0000 : Link down 0x0001 : Enable 0x0002 : Disable Port 1 to 6 Status Configuration 0x0001 : Enable 0x0002 : Disable

The data map addresses of Barox switches shown in the following table start from MODBUS for **Function Code 4**. For example, the address offset 0x0000 (hex) equals MODBUS address 30001, and the address offset 0x0015 (hex) equals MODBUS address 30022. Note that all the information read from Barox switches are in hex mode. To interpret the information, refer to the ASCII table for the translation (e.g. 0x4C = 'L', 0x6E = 'n').

System Information

Address Offset	Data Type	Interpretation	Description
0x0000	1 word	HEX	Vendor ID = 0x0000
0x0001	1 word		Unit ID (Ethernet = 1)
0x0002	1 word	HEX	Product Code = 0x0000

Address Offset	Data Type	Interpretation	Description
0x0030	20 words	ASCII	Product Name = “PG5-1002-SFP” Word 0 Hi byte = ‘P’ Word 0 Lo byte = ‘G’ Word 1 Hi byte = ‘5’ Word 1 Lo byte = ‘-’ Word 2 Hi byte = ‘1’ Word 2 Lo byte = ‘0’ Word 3 Hi byte = ‘0’ Word 3 Lo byte = ‘2’ Word 4 Hi byte = ‘-’ Word 4 Lo byte = ‘S’ Word 5 Hi byte = ‘F’ Word 5 Lo byte = ‘P’
0x0050	1 word		Product Serial Number
0x0051	2 words	HEX	Firmware Version For example : Word 0 = 0x0203 Word 1 = 0x0300 Firmware Version was 2.3.3
0x0053	2 words	HEX	Firmware Release Date For example : Word 0 = 0x2319 Word 1 = 0x1501 Firmware was released on 2015-01-23 at 19:00
0x0055	3 words	HEX	Ethernet MAC Address Ex : MAC = 9C:8D:D3:FF:FF:00 Word 0 Hi byte = 0x9C Word 0 Lo byte = 0x8D Word 1 Hi byte = 0xD3 Word 1 Lo byte = 0xFF Word 2 Hi byte = 0xFF Word 2 Lo byte = 0x00
0x0058	1 word	HEX	Power 1 Status 0x0000 : Off 0x0001 : On

Address Offset	Data Type	Interpretation	Description
0x0059	1 word	HEX	Power 2 Status 0x0000 : Off 0x0001 : On
0x005A	1 word	HEX	Fault LED Status 0x0000 : Boot error 0x0001 : Normal 0x0002 : Fault
0x0082	1 word	HEX	DO1 Status 0x0001 : Normal 0x0002 : Fault

Port Information

Address Offset	Data Type	Interpretation	Description (N depends on models)
0x1000 to 0x1005	1 word	HEX	Port 1 to Port N Status 0x0000 : Link down 0x0001 : Link up 0x0002 : Disable 0xFFFF : No port
0x1100 to 0x1105	1 word	HEX	Port 1 to Port N Speed 0x0000 : 10M-Half 0x0001 : 10M-Full 0x0002 : 100M-Half 0x0003 : 100M-Full 0x0005 : 1000M-Full 0xFFFF : No port
0x1200 to 0x1205	1 word	HEX	Port 1 to Port N Flow Ctrl 0x0000 : Off 0x0001 : On 0xFFFF : No port
0x1300 to 0x1305	1 word	HEX	Port 1 to Port N MDI/MDIX 0x0000: MDI 0x0001: MDIX 0xFFFF: No port

Address Offset	Data Type	Interpretation	Description
0x1400 to 0x1413 (Port 1) 0x1414 to 0x1427 (Port 2) ...	20 words	ASCII	Port 1 to Port N Name Port Name = "100FDX,RJ45." Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '0' Word 1 Lo byte = 'F' ... Word 5 Hi byte = '5' Word 5 Lo byte = '

Packets Information

Address Offset	Data Type	Interpretation	Description (N depends on models)
0x2000 to 0x200B	2 words	HEX	Port 1 to Port N Tx Packets Ex : Port1 Tx Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0x1324 Word 1 = 0x4800
0x2080 to 0x208B	2 words	HEX	Port 1 to Port N Tx Bytes Ex : Port1 Tx Bytes Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0x1324 Word 1 = 0x4800
0x2100 to 0x210B	2 words	HEX	Port 1 to Port N Rx Packets Ex : Port1 Rx Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0x1324 Word 1 = 0x4800
0x2180 to 0x218B	2 words	HEX	Port 1 to Port N Rx Bytes Ex : Port1 Rx Bytes Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0x1324 Word 1 = 0x4800

Address Offset	Data Type	Interpretation	Description
0x2200 to 0x220B	2 words	HEX	Port 1 to Port N Tx Error Packets Ex : Port 1 Tx Error Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0x1324 Word 1 = 0x4800
0x2300 to 0x230B	2 words	HEX	Port 1 to Port N Rx Error Packets Ex : Port1 Rx Error Packet Amount = 13244800 Received MODBUS response : 0x13244800 Word 0 = 0x1324 Word 1 = 0x4800

Redundancy Information

Address Offset	Data Type	Interpretation	Description (N depends on models)
0x3000	1 word	HEX	Redundancy Protocol 0x0000 : None 0x0001 : RSTP 0x0002 : MSTP 0x0003 : ERPS
0x3100	1 word	HEX	RSTP Root 0xFFFF : None 0x0001 : Root 0x0002 : Not root
0x3200 to 0x3205	1 word	HEX	RSTP Port 1 to Port N Status 0xFFFF : Spanning tree not enable 0x0000 : Disable 0x0001 : Not spanning tree port 0x0002 : Link down 0x0003 : Blocked 0x0004 : Learning 0x0005 : Forwarding
0x3300	1 word	HEX	ERPS Port0 Role 0xFFFF : ERPS not enable 0x0000 : Normal 0x0001 : Neighbor 0x0002 : RPL Owner

Address Offset	Data Type	Interpretation	Description
0x3301	1 word	HEX	ERPS Port1 Role 0xFFFF : ERPS not enable 0x0000 : Normal 0x0001 : Neighbor 0x0002 : RPL Owner
0x3302	1 word	HEX	ERPS Port0 Status 0x0000 : Disable 0x0001 : ERPS not enable 0x0002 : Link down 0x0003 : Forwarding 0x0004 : Learning 0x0005 : Blocking
0x3303	1 word	HEX	ERPS Port1 Status 0x0000 : Disable 0x0001 : ERPS not enable 0x0002 : Link down 0x0003 : Forwarding 0x0004 : Learning 0x0005 : Blocking
0x3304	1 word	HEX	ERPS Port0 Port Ex : ERPS Port0 is Port1 Word 0 = 0x0001
0x3305	1 word	HEX	ERPS Port1 Port Ex : ERPS Port1 is Port2 Word 0 = 0x0002

Modbus Configuration Terms

[Web User Interface – Modbus]

Modbus

Modbus

Modbus Tcp Enable:

☐

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Modbus TCP Enable	Check the checkbox to enable Modbus TCP.

Overview

System Warning is integral when it comes to managing a switch. Many programs are available for users, including “Syslog”, “System Event Log”, “Email Server” setup (for Advanced Notice in any event type), “Event Type Selection”, and “Fault Alarm” setting. When an event occurs, users will receive an advanced warning message through email, bettering the flexibility for the user to monitor the remote site network and device statuses.

System Warning Configuration Terms

[Web User Interface – Syslog Setting]

Syslog Setting

SYSLOG

SYSLOG Mode:

SYSLOG Server IP Address:

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
SYSLOG Mode	<p>“Enable” (Local, Remote, USB, All) or “Disable” Syslog.</p> <p>Enable “Local Only”, the system log will show on “System Event Log” page.</p> <p>Enable “Remote Only”, the system log will show on Remote Host, users can use utilities such as “TFTP” to get the messages.</p> <p>Enable “USB Only”, the system log will save to USB, and the file is named “message”.</p> <p>* USB mode is provided in 5/6-port models</p>
SYSLOG Server IP Address	If the SYSLOG Mode is set to “Remote Only” or “All”, users have to configure a IP address to receive system log.

Clicking the “Apply” button on the bottom right corner of the interface opens the System Event Log. Within is the SYSLOG LIST window. The LIST contains up to 5 pages of information that is updated when users click the “Refresh” button.


SYSLOG LIST

Apply


[Web User Interface – SMTP Setting]

SMTP Setting

SMTP

E-mail Alert:	<input type="text" value="Disable"/>
SMTP Server Address:	<input type="text"/>
Sender E-mail Address:	<input type="text"/>
Mail Subject:	<input type="text"/>
Authentication:	<input type="checkbox"/>
Username:	<input type="text"/>
Password:	<input type="password"/> 
Recipient E-mail Address 1:	<input type="text"/>
Recipient E-mail Address 2:	<input type="text"/>
Recipient E-mail Address 3:	<input type="text"/>
Recipient E-mail Address 4:	<input type="text"/>

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
E-mail Alert	“Enable” or “Disable” send an e-mail when event occurred.
SMTP Server Address	The IP address/name server of SMTP server
Sender E-mail Address	The E-mail address of system event message sender.
Mail Subject	The subject that will show on the e-mail.
Authentication	Check the checkbox to enable authentication.
Username	The username used to do authentication.
Password	The password used to do authentication. Click “  ” icon to show the password.
Recipient E-mail Address 1~4	The E-mail address of system event message receiver. When event occurred, an e-mail will send to these e-mail addresses.

[Web User Interface – Event Selection]

The “Event Selection” interface allows users to select any event, including “System Cold Start”, and any ports, such as “Link Up”, “Link Down” and “Link Up & Link Down”, and send system warning messages to SYSLOG and/or SMTP. To save, just click the “Apply” button.

Event Selection

EVENT SELECTION

Event	SYSLOG	SMTP
System Cold Start:	<input type="checkbox"/>	<input type="checkbox"/>

EVENT SELECTION PORT

Port No.	SYSLOG	SMTP
1	Disable	Disable
2	Disable	Disable
3	Disable	Disable
4	Disable	Disable
5	Disable	Disable
6	Disable	Disable
	Disable	Disable

Apply

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Event Selection

Terms	Value Description
System Cold Start	Check the checkbox under “SYSLOG” to enable sending system log (if SYSLOG Mode is enabled) when system cold start. Check the checkbox under “SMTP” to enable sending an e-mail (if SMTP is enabled and well set) when system cold start.

Event Selection Port

Terms	Value Description
Port No.	The ports of this switch, from 1 to N, N depends on models.
SYSLOG	“Enable” (Link Up, Link Down, Link Up & Link Down) or “Disable” sending system log when event occurred.
SMTP	“Enable” (Link Up, Link Down, Link Up & Link Down) or “Disable” sending an e-mail to receivers with system log information when event occurred.

[Web User Interface – Fault Alarm]

To enable this function, users choose the checkboxes of the “Fault Alarm” type they want to receive warnings to, such as power failure or port link down/broken. Thus, if a selected event occurs, the fault LED of the switch’s front panel will change to red.

Fault Alarm

FAULT ALARM

Power1 Failure: ☐

Power2 Failure: ☐

Port1 Link Down/Broken: ☐

Port2 Link Down/Broken: ☐

Port3 Link Down/Broken: ☐

Port4 Link Down/Broken: ☐

Port5 Link Down/Broken: ☐

Port6 Link Down/Broken: ☐

Link Down/Broken: ☐

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Power 1&2 Failure	Check the checkbox(es) to enable “Fault Alarm” when the status of Power 1 or Power 2 become failure.
Port 1 ~ N Link Down/Broken	Check the checkbox(es) to enable “Fault Alarm” when the link of selected port is down or broken. N depends on models

Overview

Supporting queries by the forwarding process, the MAC Address table is a filtering database. The forwarding process determines the selective forwarding of a frame received by a given port with a given destination MAC address through a given potential transmission port.

MAC Table Configuration Terms

[Web User Interface – MAC Address Table]

MAC Address Table lists the information of dynamic learning or static writing MAC addresses. This table also shows the mapping ports and VLAN ID to each MAC address. It is useful to forward traffic to the correct way.

MAC Address Table

MAC ADDRESS TABLE

VID	Mac	Type	Port
1	00:19:70:86:8c:f5	learning	5
1	00:20:4a:ea:70:d3	learning	5
1	00:30:ab:26:cb:04	learning	5
1	00:50:7f:47:22:8a	learning	5
1	01:00:5e:7f:ff:fa	static	5
1	08:00:27:33:7e:42	learning	5
1	08:60:6e:46:3c:3a	learning	5
1	10:bf:48:5a:b4:0d	learning	5
1	10:c3:7b:27:54:db	learning	5
1	10:c3:7b:46:22:af	learning	5
1	10:c3:7b:b6:4f:9a	learning	5
1	1c:4b:d6:fd:c8:a6	learning	5
1	30:85:a9:a7:9d:63	learning	5
1	30:85:a9:a8:05:bb	learning	5
1	38:2c:4a:82:07:d2	learning	5
1	48:5b:39:d1:1f:06	learning	5
1	54:27:1e:a0:74:ad	learning	5
1	54:53:ed:af:5c:bd	learning	5
1	54:a0:50:ad:0c:13	learning	5
1	5c:93:a2:d1:72:43	learning	5
1	5c:93:a2:eb:53:f5	learning	5
1	60:a4:4c:e9:c1:00	learning	5
1	74:d4:35:f1:2d:e9	learning	5
1	74:e5:43:09:e5:8f	learning	5
1	d0:bf:9c:34:a2:9f	learning	5
1	d8:fc:93:44:8b:8f	learning	5
1	e0:3f:49:e7:44:c2	learning	5
1	ec:43:f6:6f:90:fd	learning	5
1	f0:79:59:6c:a5:dd	learning	5
1	f0:bf:97:d2:a5:e1	learning	5

[Web User Interface – MAC Table Configuration]

MAC Table Configuration

MAC TABLE CONFIGURATION

VID	Mac	1	2	3	4	5	6	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="button" value="Delete"/>
<input type="button" value="Add"/>								

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
VID	VLAN ID, users have to configure the mapping VLAN and members.
MAC	MAC address of this VID. If the member of this VLAN is more than 1, users have to set a multicast MAC address (the lowest bit of the first byte must be “1”) to this VID.
1 ~ N	1 to N represents port 1 to port N, N depends on models. Check the checkbox(es) of the port to include them into the group. If users check more than 1 port, they have to set a multicast MAC address (the lowest bit of the first byte must be “1”) in the “MAC” field.

Overview

Users are able to implement firmware upgrade, system reboot and reset in the maintenance section.

Upgrade

Barox is constantly revising, updating, and developing new features for specific application requirements for industrial managed switches. To access and download the latest firmware, visit this website. Users can store it in their PC, server, or USB and use it to upgrade the system to the newest version.

Maintenance Configuration Terms

[Web User Interface – Upgrade]

Upgrade

FIRMWARE UPGRADE

Image: No file chosen

USB FIRMWARE UPGRADE

* Image:

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Firmware Upgrade

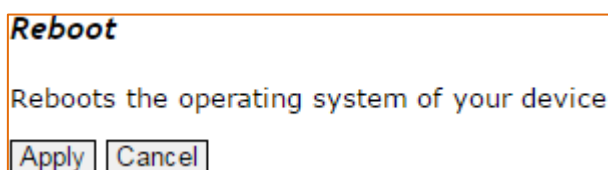
Terms	Value Description
Choose File	Click “Choose File” button to select firmware upgrade file. Please ensure that correct upgrade file is selected.
Upgrade	After firmware upgrade file is selected, click “Upgrade” button to upload the firmware upgrade file and upgrade the system.

***This part is only for 5/6-port models**

USB Firmware Upgrade (**This feature is only for 5/6-port models.**)

Terms	Value Description
Text Field	Enter path or file name, such as upgrade.dat, v2_4_0.rar, or folder/upgrade.dat, of firmware upgrade file in the USB storage.
Upgrade	After firmware upgrade file is selected, click “Upgrade” button to upload the firmware upgrade file and upgrade the system.

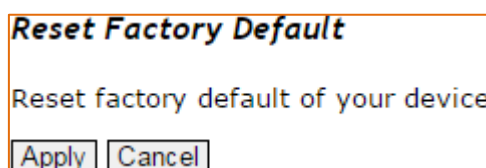
[Web User Interface – Reboot]



The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Apply	Click “Apply” button to reboot the switch.

[Web User Interface – Default]



The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Apply	Click “Apply” button to reset the switch to factory default settings.

Overview

Users are able to save all the configured settings that are backed-up and stored in a PC, server, or USB through the built-in USB port in the “Configuration” section.

The USB port enables the “Auto Load” function, which boots the switch’s saved configuration in the storage device. Users can also use this function to “Auto Load” the configuration to other switches.

The USB device can remain plugged into the switch to enable “Auto Backup”, which automatically backs up configuration settings whenever users save changes

Configuration Terms

[Web User Interface – Save]

Save

SAVE CONFIGURATION

Save Configuration:

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
Save	Click “Save” button to save running-config into startup-config.

[Web User Interface – Backup & Restore]

Backup & Restore

CONFIGURATION MANAGEMENT

Backup Configuration:

Upload Configuration: No file chosen

USB MANAGEMENT

*

Save Running Config To USB:

Save Startup Config To USB:

Upload Config From USB:

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

***This part is only for 5/6-port models**

Configuration Management

Terms	Value Description
Backup Configuration	Click “Backup” button to save startup-config to local host (PC).
Upload Configuration	Click “Choose File” button to select a configuration file. After the configuration file is selected, click “Upload” button to upload the selected file. It will reboot system after finishing loading the file.

USB Management

Terms	Value Description
Save Running Config To USB	Enter path or file name, such as switch-config.cfg, config, or folder/switch.cfg, of running-config file. And then click “Backup” button, the running-config will be saved to USB. *For 8/10/12-port models, the file name is fixed as following: 8-port: SWITCH08.TXT 10-port: SWITCHS.TXT 12-port: SWITCH12.TXT
Save Running Config To USB	Enter path or file name, such as switch-config.cfg, config, or folder/switch.cfg, of startup-config file. And then click “Backup” button, the startup-config will be saved to USB. *For 8/10/12-port models, the file name is fixed as following: 8-port: SWITCH08.TXT 10-port: SWITCHS.TXT 12-port: SWITCH12.TXT
Upload Config From USB	Enter path or file name, such as switch-config.cfg, config, or folder/switch.cfg, of configuration file. And then click “Upload” button, the configuration file will be uploaded from USB to switch. *For 8/10/12-port models, the file name is fixed as following: 8-port: SWITCH08.TXT 10-port: SWITCHS.TXT 12-port: SWITCH12.TXT

[Web User Interface – Auto Load & Backup]

USB Auto Load and Backup

AUTO LOAD AND BACKUP

USB Auto Load:	<input checked="" type="checkbox"/>
USB Auto Backup:	<input type="checkbox"/>

[Apply](#)

The graph above is the WEB User Interface. And the table below is to describe the field of the WEB UI.

Terms	Value Description
USB Auto Load	<p>“USB Auto Load” is enabled by default.</p> <p>Check the checkbox to enable “USB Auto Load”. System will auto load startup-config file from USB to switch when rebooting if USB stick is plugged. Please make sure the startup file name is “switch-[MAC ADDRESS].cfg”, if the file didn’t exist, it will try to find “switch-config.cfg”. If all of them don’t exist, it does not work.</p> <p>*For 8/10/12-port models, the auto-load file name is fixed as following:</p> <p>8-port: SWITCH08.TXT 10-port: SWITCHS.TXT 12-port: SWITCH12.TXT</p>
USB Auto Backup	<p>Check the checkbox to enable “USB Auto Backup”. System will auto backup running-config file to USB storage. The saved running-config file name is “switch-[MAC ADDRESS]-[yyyymmddhhmmss].cfg”.</p> <p>*For 8/10/12-port models, the auto-backup file name is fixed as following:</p> <p>8-port: SWITCH08.TXT 10-port: SWITCHS.TXT 12-port: SWITCH12.TXT</p>

Overview

To ensure the security of system, please logout when there is no need to use web console.
Click “Logout” button on the left side menu to logout the system.

Command Line Interface

2. Connect by RS-232 Serial Console

We assume that the operating system is Windows7, and connection utility is “Tera Term”.

Step 1 Click “Windows” button, and click “Tera Term”, shown as Figure 10.

Step 2 Click “Setup” on the tool list, and click “Serial port”, shown as Figure 11.

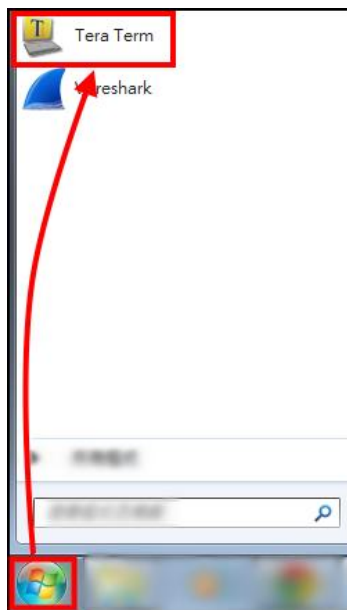


Figure 10: Open Tera Term

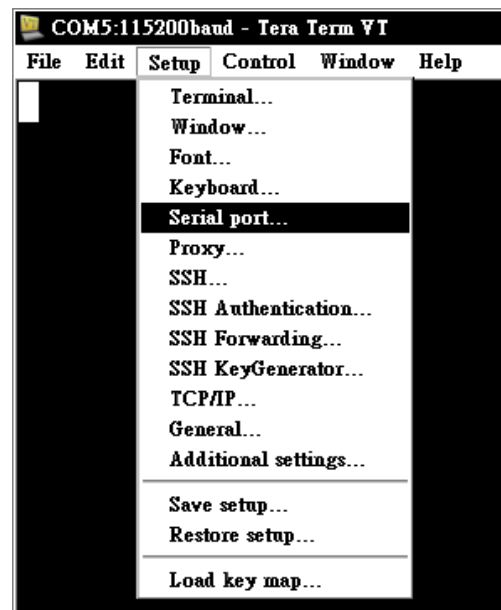


Figure 11: Configure Serial Port

Step 3 Select the Com port, and set parameters: **115200 / 8 / none / 1 / none**

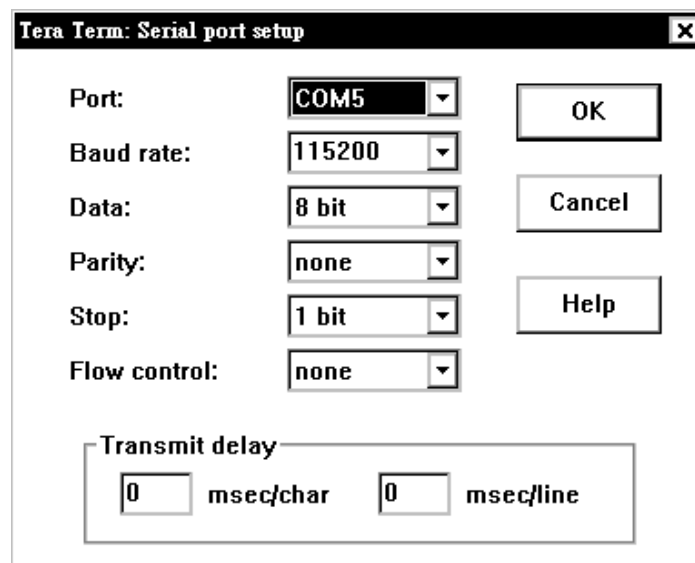


Figure 12: Configure Serial Port

Step 4 Login with username and password, default value is admin / admin



Figure 13: Login CLI by Serial Console

3. Connect by Telnet

We assume that the operating system is Windows7

Step 1 Click “Windows” button, and type “telnet 192.168.1.254” in the “Search” box.

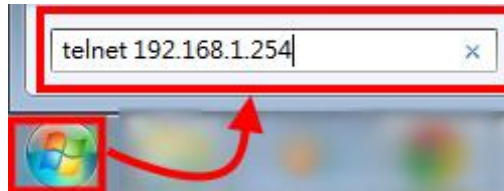


Figure 14: Connect to Switch by Telnet

Step 2 Login with username and password, default value is admin / admin



Figure 15: Login CLI by Telnet

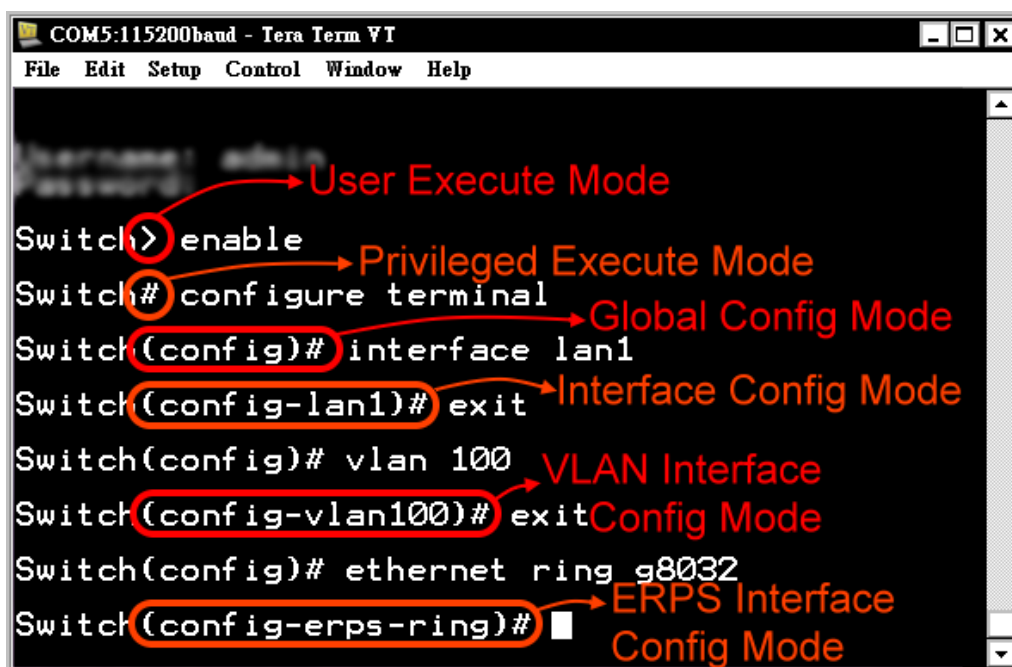
4. Introduce CLI and Tips

Our system is a cisco-like command line interface. This user interface allows us to directly and simply execute commands to configure, monitor and maintain switches. To aid in the

configuration of switches, our command-line interface is divided into different command modes. Each command mode has its own set of commands available. The standard order that users would access the modes is as follows: **User EXEC mode**; **Privileged EXEC mode**; **Global configuration mode**; and other **Interface configuration mode**. Figure 16 shows the different modes on the CLI.

Beginner's Guide

There are two important and helpful commands, “?” and “help”. These two commands will list all commands in the current mode. The difference between “?” and “help” is that “help” is more detailed and users will see all commands including entire usages in that mode, while “?” shows the major commands in that mode. Figure 17 shows the difference. The top part is the demo of “?”, and it lists all major commands in this mode. The following part is the demo of “help”, and it lists all commands available containing usages.



```
COM5:115200baud - Tera Term VT
File Edit Setup Control Window Help

Switch> enable
Switch# configure terminal
Switch(config)# interface lan1
Switch(config-lan1)# exit
Switch(config)# vlan 100
Switch(config-vlan100)# exit
Switch(config)# ethernet ring g8032
Switch(config-erps-ring)#
```

The screenshot shows a Tera Term window with a menu bar (File, Edit, Setup, Control, Window, Help) and a terminal window. The terminal displays a sequence of commands and mode transitions. Red circles and arrows are used to highlight and label the modes:

- User Execute Mode**: Points to the initial `Switch>` prompt.
- Privileged Execute Mode**: Points to the `Switch#` prompt after the `enable` command.
- Global Config Mode**: Points to the `Switch(config)#` prompt after the `configure terminal` command.
- Interface Config Mode**: Points to the `Switch(config-lan1)#` prompt after the `interface lan1` command.
- VLAN Interface Config Mode**: Points to the `Switch(config-vlan100)#` prompt after the `vlan 100` command.
- ERPS Interface Config Mode**: Points to the `Switch(config-erps-ring)#` prompt after the `ethernet ring g8032` command.

Figure 16: Configuration Modes on CLI

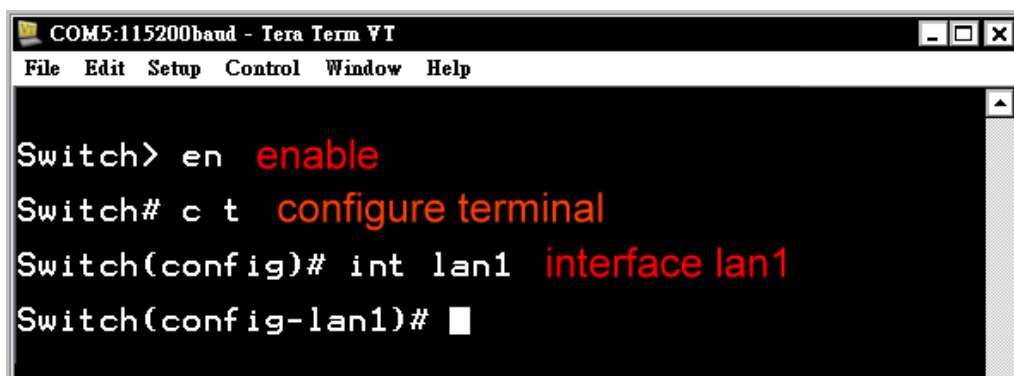

```
Switch#  
help          Show available commands  
quit          Disconnect  
logout        Disconnect  
exit          Exit from current mode  
history       Show a list of previously run commands  
enable        Turn on privileged commands  
disable       Turn off privileged commands  
configure     Enter configuration mode  
show          Display en status or configure  
  
Switch# help  
  
Commands available:  
help          Show available commands  
quit          Disconnect  
:  
show system mac      show the system MAC address  
show system serial-number show the system serial number  
show system version firmware show the system firmware version  
show system version loader show the system loader version  
show boot host dhcp  show DHCP client  
show ip mode         show the IP address mode  
:  
show ntp client sync hour show ntp hour configuration  
show ntp client sync day show ntp day configuration  
show ntp client sync month show ntp month configuration  
show ntp client sync weekly show ntp weekly configuration  
show clock time      show time  
show clock timezone  show timezone  
:  
:
```

Figure 17: The Difference Between “?” and “help”

Useful Tips

In the following, we will introduce 2 tips that are very helpful. The first tip is “shorthand”. Almost all commands can be finished by using shorthand. When we use a shorthand, we have to note if it is unique. For example, when we want to use something to replace “enable”, we have to use “en” instead of “e” because “e” may map to either “exit” or “enable”. Figure 18 shows you some examples.

Another helpful tip is the “Tab” key. Most of commands can be autocompleted by the “Tab” key. For example, you could just type “en”, and hit the “Tab” key to autocomplete “enable”. Notice that if the words we typed are not unique, it will return all the possible commands until the words can match the unique one.



```
COM5:115200baud - Tera Term VT  
File Edit Setup Control Window Help  
  
Switch> en enable  
Switch# c t configure terminal  
Switch(config)# int lan1 interface lan1  
Switch(config-lan1)#
```

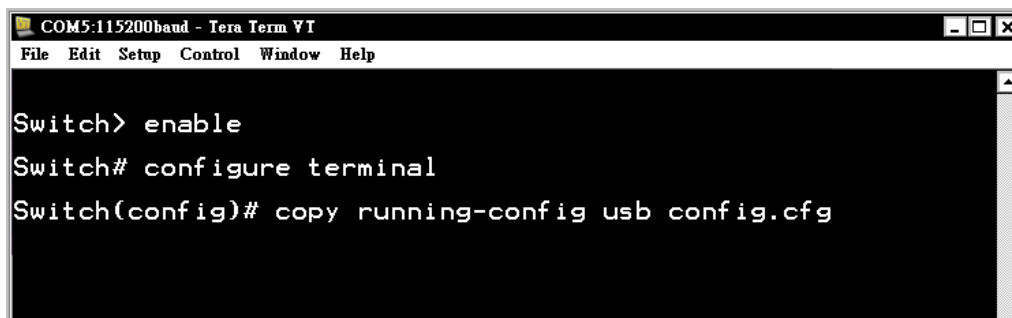
Figure 18: Demo of Shorthand

5. Save Configuration File to USB

Before saving a configuration file to USB, you have to ensure that the USB stick is plugged in.

Save “**running-config**” to USB

- Step 1 Enter “Global Configuration Mode”.
- Step 2 Issue the command: “copy running-config usb [PATH/FILENAME]”. The [PATH/FILENAME] field should be filled in the path or file name of the configuration file.



```
COM5:115200baud - Tera Term VT
File Edit Setup Control Window Help

Switch> enable
Switch# configure terminal
Switch(config)# copy running-config usb config.cfg
```

Figure 19: Enter “Global Configuration Mode” and Issue Save Command

Save “**startup-config**” to USB

- Step 1 Enter “Global Configuration Mode”.
- Step 2 Issue the command: “copy startup-config usb [PATH/FILENAME]”. The [PATH/FILENAME] field should be filled in the path or file name of the configuration file.



```
COM5:115200baud - Tera Term VT
File Edit Setup Control Window Help

Switch> enable
Switch# configure terminal
Switch(config)# copy startup-config usb config.cfg
```

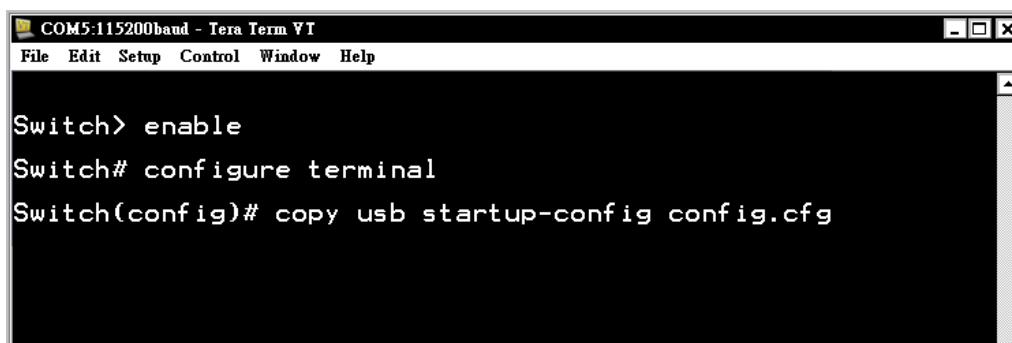
Figure 20: Enter “Global Configuration Mode” and Issue Save Command

6. Load Configuration File from USB

Before load configuration file to USB, you have to ensure that the USB stick is plugged in.

Load “**startup-config**” from USB

- Step 1 Enter “Global Configuration Mode”.
- Step 2 Issue the command: “copy usb startup-config [PATH/FILENAME]”. The [PATH/FILENAME] field should be filled in the path or file name of the configuration file.



```
COM5:115200baud - Tera Term VT
File Edit Setup Control Window Help

Switch> enable
Switch# configure terminal
Switch(config)# copy usb startup-config config.cfg
```

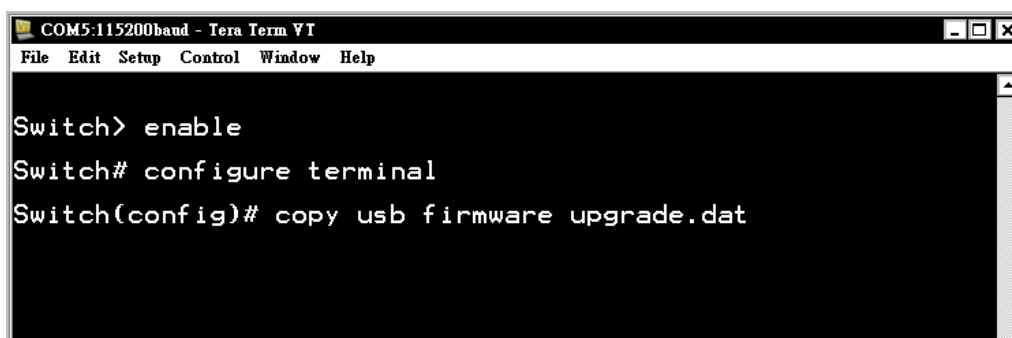
Figure 21: Enter “Global Configuration Mode” and Issue Load Command

7. Upgrade Firmware from USB

This feature is only for 5/6-port models.

Before load configuration file to USB, you have to ensure that the USB stick is plugged.

- Step 1 Enter “Global Configuration Mode”.
- Step 2 Issue the command: “copy usb firmware [PATH/FILENAME]”. The [PATH/FILENAME] field should be filled in the path or file name of the configuration file.



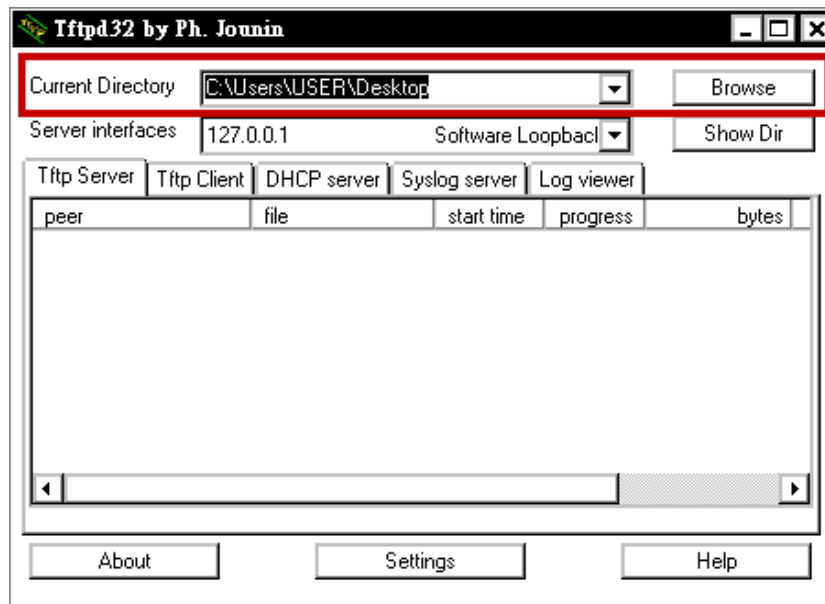
```
COM5:115200baud - Tera Term VT
File Edit Setup Control Window Help

Switch> enable
Switch# configure terminal
Switch(config)# copy usb firmware upgrade.dat
```

Figure 22: Enter “Global Configuration Mode” and Issue Upgrade Command

8. Upgrade Firmware by TFTP

Step 7 Open TFTP and configure the file path. Ensure TFTP is ready.

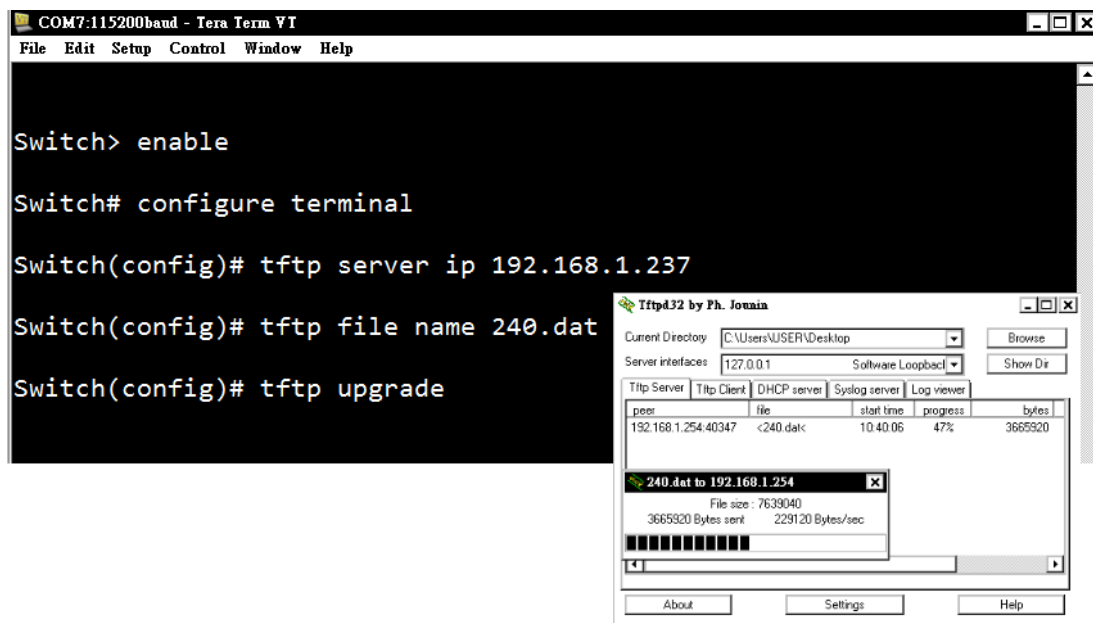


Step 8 Enter “Global Configuration Mode”.

Step 9 Set TFTP Server IP address. Issue the command “tftp server ip [IP_ADDRESS]”.
[IP_ADDRESS] is the IP address where your firmware file located.

Step 10 Set firmware upgrade file name. Issue the command “tftp file name [UPGRADE_FILE_NAME]”. Please make sure the file name of upgrade firmware file.

Step 11 Issue “tftp upgrade” to start upgrading firmware.



Step 12 It will reboot after finishing upgrading the firmware.

9. Commands

• This is only for 8/10/12-port models.

* This is only for 5/6-port models.

System Group

Command	Mode
hostname [Switch]	configure
no hostname	configure
system location [none]	configure
system contact [none]	configure
no system location	configure
no system contact	configure
show system uptime	configure
show system mac	configure
show system version firmware	configure
show system version loader	configure
username [NAME] password [PASSWD]	configure

IP Group

Command	Mode
boot host dhcp	configure
ip address [ip_addr] [ip_mask]	configure
ip default-gateway [ip_router]	configure
ip name-server [ip_addr_string]	configure
no boot host dhcp	configure
no ip default-gateway	configure
no ip name-server	configure
show boot host dhcp	configure
show ip address	configure
show ip default-gateway	configure
show ip name-server	configure
show ip mode	configure

IPv6 Group

Command	Mode
ipv6 enable	configure
ipv6 address add [IPV6_ADDR</PREFIX_LEN>]	configure
ipv6 neighbor flush	configure
ipv6 ping [IPV6_ADDR] [<size PKG_SIZ> <repeat PKG_CNT>]	configure

no ipv6 enable	configure
no ipv6 address [IPV6_ADDR/PREFIX_LEN]	configure
show ipv6 enable	configure
show ipv6 address	configure
show ipv6 neighbor	configure

Time Group

Command	Mode
ntp time update	configure
ntp client timeserver [ip_addr_string]	configure
clock time [hh:mm:ss] [day] [month] [year]	configure
clock timezone [area] [city]	configure
ntp client sync [minute hour day month year] [NUMBER] •	configure
ntp client sync schedule enable *	configure
ntp client sync minute [time] *	configure
ntp client sync hour [time] *	configure
ntp client sync day [time] *	configure
ntp client sync month [time] *	configure
ntp client sync weekly [time] *	configure
no ntp client timeserver	configure
no clock timezone	configure
no ntp client sync [minute hour day month year] [NUMBER] •	configure
no ntp client sync schedule *	configure
no ntp client sync minute *	configure
no ntp client sync hour *	configure
no ntp client sync day *	configure
no ntp client sync month *	configure
no ntp client sync weekly *	configure
show ntp client timeserver	configure
show clock timezone	configure
show ntp client sync [minute hour day month year] [NUMBER] •	
show ntp client sync schedule *	configure
show ntp client sync minute *	configure
show ntp client sync hour *	configure
show ntp client sync day *	configure
show ntp client sync month *	configure
show ntp client sync weekly *	configure

Port Group

Command	Mode
speed_duplex [10 100] [full half]	interface
flowcontrol <receive> [on off desired]	interface
name [string]	interface
shutdown	interface
no speed_duplex	interface
no flowcontrol	interface
no name	interface
no shutdown	interface
show speed_duplex	interface
show flowcontrol	interface
show name	interface
show link state	interface
show link rx	interface
show link tx	interface
show link summary	interface
show interface transceiver	interface

VLAN Group

Command	Mode
management vlan [vlan_id]	configure
name [vlan_name]	vlan
member [member_portlist] [<untag_portlist>]	vlan
switchport pvid [vlan_id]	interface
switchport filter [tagged untagged]	interface
no name	vlan
no member	vlan
no switchport pvid	interface
no switchport filter	interface
show name	vlan
show member	vlan
show switchport pvid	interface
show switchport filter	interface

ERPS Group

Command	Mode
ethernet ring erps major	configure
enable	ERPS

disable	ERPS
rpl [port0 port1] [owner neighbor]	ERPS
aps-channel [channel ID]	ERPS
revertive	ERPS
clear	ERPS
port0 interface [interface name]	ERPS
port1 interface [interface name]	ERPS
fs [port0 port1]	ERPS
ms [port0 port1]	ERPS
ring-id [erps ring ID]	ERPS
timer hold-off [0~10000]	ERPS
timer guard [10~2000]	ERPS
timer wtr [1~12]	ERPS
no rpl [port0 port1]	ERPS
no aps-channel	ERPS
no revertive	ERPS
no port0	ERPS
no port1	ERPS
no ring-id	ERPS
no timer hold-off	ERPS
no timer guard	ERPS
no timer wtr	ERPS
show status	ERPS
show brief	ERPS
show port status	ERPS
show configuration	ERPS

PoE Group

Command	Mode
power inline never	interface
keepalive ip [IP_Address]	interface
keepalive time [Seconds]	interface
schedule [monday~sunday] enable	interface
schedule [monday~sunday] starttime [Hour]	interface
schedule [monday~sunday] endtime [Hour]	interface
no power inline never	interface
no keepalive ip	interface
no keepalive time	interface

no schedule [Monday~sunday] enable	interface
no schedule [monday~sunday] starttime	interface
no schedule [monday~sunday] endtime	interface
show power inline status	interface
show keepalive ip	configure
show keepalive time	configure
show schedule [Monday~sunday]	configure
show schedule [monday~sunday] starttime	configure
show schedule [monday~sunday] endtime	configure

Spanning-Tree Group

Command	Mode
spanning-tree mode [rstp mst]	configure
spanning-tree priority [priority_value]	configure
spanning-tree forward-time [forward time]	configure
spanning-tree hello-time [hello_time]	configure
spanning-tree max-age [max_age]	configure
spanning-tree cost [link_cost_value]	interface
spanning-tree port-priority [port_priority]	interface
spanning-tree link-type [point-to-point point-to-multiple]	interface
spanning-tree auto-edge off	interface
spanning-tree admin-edge on	interface
spanning-tree stp disable	interface
no spanning-tree mode	configure
no spanning-tree priority	configure
no spanning-tree forward-time	configure
no spanning-tree hello-time	configure
no spanning-tree max-age	configure
no spanning-tree mst [instance_ID] priority	configure
no spanning-tree cost	interface
no spanning-tree port-priority	interface
no spanning-tree link-type	interface
no spanning-tree auto-edge	interface
no spanning-tree admin-edge	interface
no spanning-tree stp	interface
show spanning-tree mode	configure
show spanning-tree priority	configure
show spanning-tree forward-time	configure

show spanning-tree hello-time	configure
show spanning-tree max-age	configure
show spanning-tree cost	interface
show spanning-tree port-priority	interface
show spanning-tree link-type	interface
show spanning-tree auto-edge	interface
show spanning-tree admin-edge	interface
show spanning-tree stp	interface
spanning-tree mst [instance_ID] priority [priority]	configure
spanning-tree mst name [NAME]	configure
spanning-tree mst revision [REVISION]	configure
spanning-tree mst instance [instance_ID] vlan [vlan_grp]	configure
spanning-tree mst [instance_ID] cost [cost_value]	interface
spanning-tree mst [instance_ID] port-priority [priority]	interface
no spanning-tree mst name	configure
no spanning-tree mst revision	configure
no spanning-tree mst instance [instance_ID] vlan	configure
no spanning-tree mst [instance_ID] cost	interface
no spanning-tree mst [instance_ID] port-priority	interface
show spanning-tree mst name	configure
show spanning-tree mst revision	configure
show spanning-tree mst instance [instance_ID] vlan	configure
show spanning-tree mst [instance_ID] priority	configure
show spanning-tree mst [instance_ID] cost	interface
show spanning-tree mst [instance_ID] port-priority	interface

Event Group

Command	Mode
event smtp power1 enable	configure
event smtp power2 enable	configure
event smtp cold-start enable	configure
event smtp warm-start enable	configure
event smtp authentication-failure enable	configure
event smtp erps-change enable	configure
event smtp interface [INTERFACE_NAME] up	configure
event smtp interface [INTERFACE_NAME] down	configure
no event smtp power1	configure
no event smtp power2	configure

no event smtp cold-start	configure
no event smtp warm-start	configure
no event smtp authentication-failure	configure
no event smtp erps-change	configure
no event smtp interface [INTERFACE_NAME] up	configure
no event smtp interface [INTERFACE_NAME] down	configure
show event smtp power1	configure
show event smtp power2	configure
show event smtp cold-start	configure
show event smtp warm-start	configure
show event smtp authentication-failure	configure
show event smtp erps-change	configure
show event smtp interface [INTERFACE_NAME] up	configure
show event smtp interface [INTERFACE_NAME] down	configure
event syslog power1 enable	configure
event syslog power2 enable	configure
event syslog cold-start enable	configure
event syslog warm-start enable	configure
event syslog authentication-failure enable	configure
event syslog erps-change enable	configure
event syslog interface [INTERFACE_NAME] up	configure
event syslog interface [INTERFACE_NAME] down	configure
no event syslog power1	configure
no event syslog power2	configure
no event syslog cold-start	configure
no event syslog warm-start	configure
no event syslog authentication-failure	configure
no event syslog erps-change	configure
no event syslog interface [INTERFACE_NAME] up	configure
no event syslog interface [INTERFACE_NAME] down	configure
show event syslog power1	configure
show event syslog power2	configure
show event syslog cold-start	configure
show event syslog warm-start	configure
show event syslog authentication-failure	configure
show event syslog erps-change	configure
show event syslog interface [INTERFACE_NAME] up	configure

show event syslog interface [INTERFACE_NAME] down	configure
event alarm power1 enable	configure
event alarm power2 enable	configure
event alarm interface [INTERFACE_NAME] down	configure
no event alarm power1	configure
no event alarm power2	configure
no event alarm interface [INTERFACE_NAME] down	configure
show event alarm power1	configure
show event alarm power2	configure
show event alarm interface [INTERFACE_NAME] down	configure
event apply	configure

Syslog Group

Command	Mode
syslog server [IP_address]	configure
syslog mode [all remote local usb *]	configure
no syslog server	configure
no syslog mode	configure
show syslog server	configure
show syslog mode	configure
show syslog log	configure

SMTP Group

Command	Mode
smtp enable	configure
smtp sender [E-MAIL_ADDR]	configure
smtp subject [subject_text]	configure
smtp server address [GMAIL_SMPT_SERVER]	configure
smtp server port [GMAIL_SMPT_SERVER]	configure
smtp authentication enable	configure
smtp authentication username [GMAIL_ACCOUNT]	configure
smtp authentication password [GMAIL_PASS]	configure
smtp receive [1 2 3 4] [e-mail_address]	configure
no smtp enable	configure
no smtp sender	configure
no smtp subject	configure
no smtp server address	configure
no smtp server port	configure
no smtp authentication enable	configure

no smtp authentication username	configure
no smtp authentication password	configure
no smtp receive [1 2 3 4]	configure
show smtp state	configure
show smtp sender	configure
show smtp subject	configure
show smtp server address	configure
show smtp server port	configure
show smtp authentication enable	configure
show smtp authentication username	configure
show smtp receive [1 2 3 4]	configure

SNMP Group

Command	Mode
snmp server enable [<v1-v2c-only v3-only>]	configure
snmp server community [ro rw] [community_name]	configure
snmp server v3 level [admin user] [auth noauth priv]	configure
snmp server v3 auth [admin user] [md5 sha] [PWD]	configure
snmp server v3 encryption [admin user] [des aes] [PWD]	configure
no snmp server enable	configure
no snmp server community [ro rw]	configure
no snmp server v3 level [admin user]	configure
no snmp server v3 auth [admin user]	configure
no snmp server v3 encryption [admin user]	configure
show snmp server enable	configure
show snmp server community [ro rw]	configure
show snmp server v3 level [admin user]	configure
show snmp server v3 auth [admin user]	configure
show snmp server v3 encryption [admin user]	configure
snmp trap enable	configure
snmp trap host [DESTINATION_IP]	configure
snmp trap version [1 2c 3] [traps inform]	configure
snmp trap community [trap_community_name]	configure
snmp trap inform retry [retry_time]	configure
snmp trap inform timeout [retry_interval]	configure
snmp trap v3 user [user_ID]	configure
snmp trap v3 level [auth noauth priv]	configure
snmp trap v3 engine-ID [engineID]	configure

snmp trap v3 auth [md5 sha] [PASSWORD]	configure
snmp trap v3 encryption [des aes] [PASSWORD]	configure
no snmp trap enable	configure
no snmp trap host	configure
no snmp trap version	configure
no snmp trap community	configure
no snmp trap inform retry	configure
no snmp trap inform timeout	configure
no snmp trap v3 user	configure
no snmp trap v3 level	configure
no snmp trap v3 engine-ID	configure
no snmp trap v3 auth	configure
no snmp trap v3 encryption	configure
show snmp trap enable	configure
show snmp trap host	configure
show snmp trap version	configure
show snmp trap community	configure
show snmp trap inform retry	configure
show snmp trap inform timeout	configure
show snmp trap v3 user	configure
show snmp trap v3 level	configure
show snmp trap v3 engine-ID	configure
show snmp trap v3 auth	configure
show snmp trap v3 encryption	configure

Port Trunk Group

Command	Mode
trunk group [group] [static lacp] [interface_list]	configure

Port Mirror Group

Command	Mode
monitor enable	configure
monitor source [rx tx both] [port_list]	configure
monitor destination [dest_port_number]	configure
no monitor enable	configure
no monitor source	configure
no monitor destination	configure
show monitor enable	configure
show monitor source	configure

show monitor destination	configure
--------------------------	-----------

QoS Group

Command	Mode
qos queue-schedule [strict wrr]	configure
qos map cos [priority_type] to tx-queue [queue]	configure
qos map dscp [[priority_type] to tx-queue [[queue]	configure
qos trust [cos dscp]	interface
qos default cos [cos_default_value]	interface
no qos queue-schedule	configure
no qos map cos [priority_type]	configure
no qos map dscp [priority_type]	configure
no qos trust	interface
no qos default cos	interface
show qos queue-schedule	configure
show qos map cos [priority_type]	configure
show qos map dscp [priority_type]	configure
show qos trust	interface
show qos default cos	interface

DHCP Server/Relay

Command	Mode
dhcp service server	configure
dhcp server included-address [IP_START] [IP_END]	configure
dhcp server default-gateway [router_ip]	configure
dhcp server name-server [dns_ip]	configure
dhcp server lease [dhcp_lease_time]	configure
dhcp server binding [bind_num][MAC] [bind_IP]	configure
dhcp server port-binding [Port] [bind_IP]	configure
dhcp service relay	configure
dhcp relay server [server_number] [IP]	configure
dhcp relay information option	configure
dhcp relay information policy [replace keep drop]	configure
dhcp relay untrust	interface
no dhcp service server	configure
no dhcp server included-address	configure
no dhcp server default-gateway	configure
no dhcp server name-server	configure
no dhcp server lease	configure

no dhcp server binding [bind_num]	configure
no dhcp service relay	configure
no dhcp relay server [server_number]	configure
no dhcp relay information option	configure
no dhcp relay information policy [replace keep drop]	configure
no dhcp relay untrust	configure
show dhcp service	interface
show dhcp server status	configure
show dhcp server included-address	configure
show dhcp server default-gateway	configure
show dhcp server name-server	configure
show dhcp server lease	configure
show dhcp server binding [bind_num][MAC] [bind_IP]	configure
show dhcp relay enable	configure
show dhcp relay server [server_number]	configure
show dhcp relay information option	configure
show dhcp relay information policy [replace keep drop]	configure
show dhcp relay untrust	interface

IGMP Snooping

Command	Mode
igmp snooping enable	configure
igmp snooping query max-respond-time [1..12]	configure
igmp snooping query interval [1..3600]	configure
igmp snooping last-member count [2..10]	configure
igmp snooping last-member interval [60..300]	configure
igmp snooping querier enable	configure
igmp snooping fast-leave enable	interface
no igmp snooping enable	configure
no igmp snooping query max-respond-time	configure
no igmp snooping query interval	configure
no igmp snooping last-member count	configure
no igmp snooping last-member interval	configure
no igmp snooping querier	configure
no igmp snooping fast-leave	interface
show igmp snooping mdb	configure
show igmp snooping all	configure
show igmp snooping fast-leave	interface

802.1X Group

Command	Mode
dot1x enable	configure
dot1x authentication server type [local radius]	configure
dot1x authentication server 1 ip [IP]	configure
dot1x authentication server 1 port [PORT]	configure
dot1x authentication server 1 share-key [KEY]	configure
dot1x authentication server 2 ip [IP]	configure
dot1x authentication server 2 port [PORT]	configure
dot1x authentication server 2 share-key [KEY]	configure
dot1x local-db [USER] [PASSWORD]	configure
dot1x authenticator enable	interface
dot1x reauthentication enable	interface
dot1x reauthentication period [SEC]	interface
no dot1x enable	configure
no dot1x authentication server type	configure
no dot1x authentication server 1 ip	configure
no dot1x authentication server 1 port	configure
no dot1x authentication server 1 share-key	configure
no dot1x authentication server 2 ip	configure
no dot1x authentication server 2 port	configure
no dot1x authentication server 2 share-key	configure
no dot1x local-db [USER] [PASSWORD]	configure
no dot1x authenticator enable	interface
no dot1x reauthentication enable	interface
no dot1x reauthentication period	interface
show dot1x enable	configure
show dot1x authentication server type	configure
show dot1x authentication server 1 ip	configure
show dot1x authentication server 1 port	configure
show dot1x authentication server 1 share-key	configure
show dot1x authentication server 2 ip	configure
show dot1x authentication server 2 port	configure
show dot1x authentication server 2 share-key	configure
show dot1x local-db [USER] [PASSWORD]	configure
show dot1x brief	configure

show dot1x server brief	configure
show dot1x brief	interface
show dot1x server brief	interface
show dot1x authenticator enable	interface
show dot1x reauthentication enable	interface
show dot1x reauthentication period	interface

UPnP Group

Command	Mode
upnp enable	configure
upnp advertisement interval [SEC]	configure
no upnp enable	configure
no upnp advertisement interval	configure
show upnp enable	configure
show upnp advertisement interval	configure

Modbus Group

Command	Mode
modbus tcp server	configure
no modbus tcp server	configure
show modbus tcp server	configure

MAC Table Group

Command	Mode
mac set [1-4094] [MAC] [Port]	configure
no mac set [1-4094] [MAC]	configure
show mac set	configure

USB Group

Command	Mode
usb auto-load	configure
usb auto-backup	configure
no usb auto-load	configure
no usb auto-backup	configure
show usb auto-load	configure
show usb auto-backup	configure

File Group

Command	Mode
copy running-config startup-config	configure
copy startup-config running-config	configure

TFTP Group

Command	Mode
tftp upgrade	configure
tftp server ip [IP_ADDRESS]	configure
tftp file name [UPGRADE_FILE_NAME]	configure