ROCKETLINX ES7528

Industrial Managed PoE Plus Switch

Industrial Rack Mount
Managed PoE Switch

24 - 10/100BASE-TX PoE/PoE Plus Ports
4 - Gigabit RJ45/SFP Ports

User Guide

COMTROL®

Copyright Notice

Second Edition, June 18, 2013

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Document Number: 2000509 Rev B

Table of Contents

Introduction

The ES7528 is a rack mount high-port density managed PoE switch designed exclusively for highly critical PoE applications such as real-time IP video surveillance with high-resolution quality and evolving wireless communication systems such as Wimax and IEEE 802.11 a/b/g/n access points.

The ES7528 provides a total of 28-ports:

- 24 Fast Ethernet PoE injector ports that can deliver 15.4 Watts (IEEE 802.3af) or 32 Watts (high power PoE IEEE 802.3at)
- 4 Gigabit copper/SFP Combo uplink Ethernet ports

With network redundancy technology, the ES7528 can aggregate up to twelve Fast Ethernet and two Gigabit rings while providing high-quality data transmission with less than 5ms network recovery time. To ensure traffic switching without data loss and blocking, the ES7528 provides a 12.8G backplane with an integrated non-blocking switching function. The ES7528 incorporates LLDP functionality and works with NetVision to allow administrators to automatically discover devices and efficiently manage the industrial network performance in large-scale surveillance networks. The ES7528 supports AC and dual 53VDC power inputs that can be aggregated to provide redundancy. The ES7528 also provides alarm relay output signaling functionality.

The ES7528 provides advanced Layer 2 management features including IGMP Query/Snooping, DHCP, 256 VLAN, QoS, LACP, LPLD, and the corrosion resistant robust design, the ES7528 is a revolutionary solution for industrial surveillance applications.

Detailed specifications are available for the ES7528.

You can refer to *Feature Overview* on Page 28 for web user interface features.

Hardware Installation

You can use the following subsections to install the RocketLinx ES7528:

Connect the Power and Ground

You can use the following procedure to connect power and the ground to the ES7528. The ES7528 is equipped with both AC and DC1/DC2 power inputs.

1. Connect the power cord to the AC power input connector.

   Note: *To reach the maximum total power budget, power inputs must be aggregated. Refer to the following table for detailed information.*

2. Connect the DC power inputs.

   a. Insert positive and negative wires (12-24AWG) into the V+ and V- contacts.

   Note: *Power should be disconnected from the power supply before connecting it to the switch. Otherwise, your screw driver blade can inadvertently short your terminal connections to the grounded enclosure.*

   b. Tighten the wire-clamp screws to prevent the wires from coming loose.

Wire: 12 to 22 AWG
DC Input: 53VDC

Electrical Specifications	Value	
Power Input Voltage DC1/DC2	IEEE 802.3af	48VDC (46-57VDC)
	IEEE 802.3at	53VDC (50-57VDC)
	AC and DC1/DC2 aggregated	53VDC 8.2A (maximum)
	DC1/DC2 aggregated	DC1=DC2†
Power Input Voltage	PSU/AC power	100-250VAC 47~63Hz 4A
PoE Output Voltage	IEEE 802.3af	44-57VDC
	IEEE 802.3at	50-57VDC
PoE Power/Port (Maximum)	IEEE 802.3af	15.4W
	IEEE 802.3at	32W

Electrical Specifications	Value	
Power Budget	DC1	400W
	DC2	400W
	PSU/AC Power	300W
Total Power Budget	Minimum	Up to 568W
	Maximum	Up to 720W
Power Consumption	Maximum	28W without PD load

† *The ES7528 provides redundant or aggregated power inputs, depending on the voltage of the power input. If there are more than two power inputs connected with different voltages, the ES7528 is powered from the highest connected voltage (redundant power). If the voltages of power inputs are the same, the total power output is aggregated*.

For example, to reach 700W, you can aggregate the power inputs accordingly:

- AC = 300W and DC1/2=400W
- DC1 = 350W and DC2/ = 350W

- PWR1 and PWR2 support power redundancy and reverse polarity protection.
- If both power inputs are connected, the ES7528 is powered from the highest connected voltage.
- The ES7528 can emit an alarm if PWR1 or PWR2 are no longer receiving power.

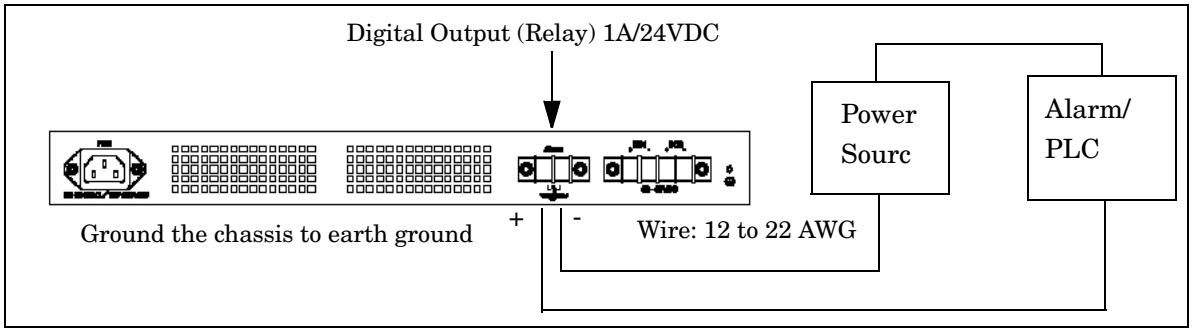
3. Connect a ground wire between the chassis and earth ground using 12-24AWG wire to ensure that the ES7528 is not damaged by noise or electrical shock.
   a. Loosen the earth ground screw on the back of the ES7528.
   b. Insert the ground wire.
   c. Tighten the ground screw after the earth ground wire is connected.

Connect the Digital Inputs or Relay Output

If desired, connect the Digital or Relay Output. The relay contacts are energized, (open) for normal operation and close for fault conditions. The fault conditions include:

- Dry output
- Power failure
- Ethernet port link break
- Ping failure
- Super ring failure

You can configure the fault relay settings in the ES7528 web user interface (*Fault Relay* on Page 117) or through the Command Line Interface (*Global Configuration Mode* on Page 142).



1. Insert the positive and negative wires (12-24 AWG) into V+ and V-.
2. Tighten the wire-clamp screws to prevent the wires from coming loose.

Mount the ES7528

You can use the following procedure to mount the ES7528 into a rack.

1. Attach the brackets to the ES7528 by using the screws provided in the rack mounting kit.
2. Mount the ES7528 in a 19-inch rack by using the four rack-mounting screws provided in the kit.

> **Temperature**: Verify that the rack environment temperature conforms to the specified operating temperature range. If necessary, refer to the Comtrol web site for operating temperature ranges.
>
> **Mechanical Loading**: Do not place any equipment on top of the switch. In a high vibration environment, additional rack mounting protection is necessary.
>
> **Grounding**: Rack-mounted equipment should be properly grounded. On the back panel of the ES7528, there is one earth ground screw. Loosen the earth ground screw

Note: *When installing multiple switches in high temperature environments, reserve 0.5U-1U of free space between the switches. It is important to disperse the heat generated by the ES7528.*

Connect the Ethernet Ports

You can use the following information to connect standard Ethernet cables between the ES7528 Ethernet ports and the network nodes.

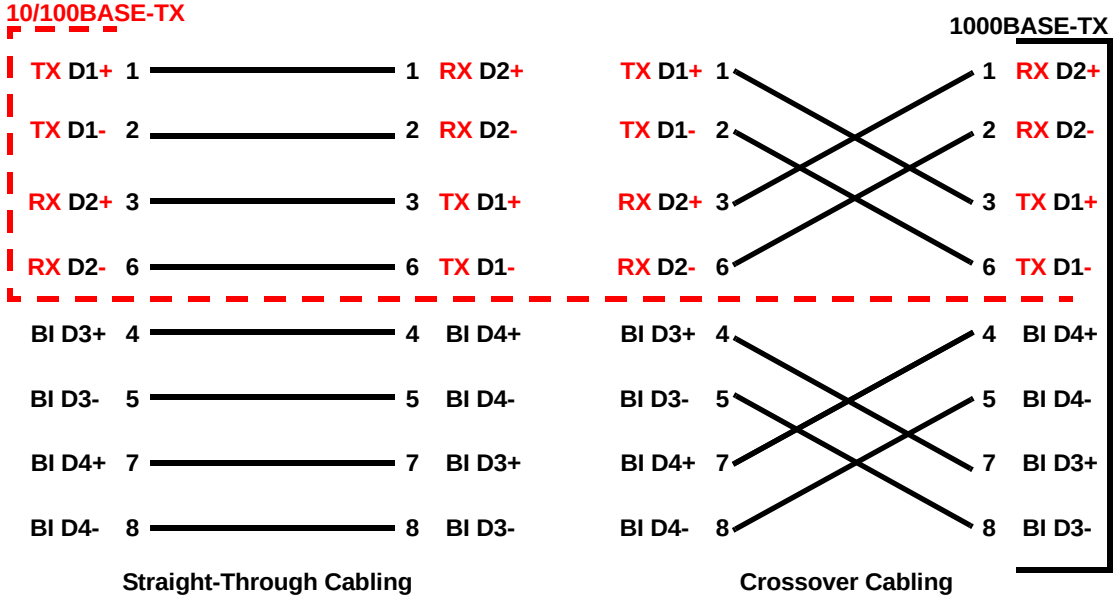
- Ports 1-24 are Fast Ethernet (10/100BASE-TX) PoE ports that are IEEE 802.3af (PoE) and IEEE 802.3at (PoE Plus) compliant. The ports provide 48VDC at 350mA (maximum 15.4W/port) or provide 53VDC at 606mA (maximum 32W/port). The following table shows the RJ45 PoE pin-out assignment.
- Ports 25-28 are RJ45/SFP Combo Gigabit ports that support Gigabit/1000BASE-SX/LX/LHX/ZD/ZX.

See *Connect SFP Transceivers (Combo Ports 25-28)* on Page 13 for information about SFP installation.

The following table shows the RJ45 PoE pin-out assignment.

Pin	10/100BASE-TX PoE (Alternative A)	1000BASE-TX
1	RX + and Vport -	BI_DA+
2	RX - and Vport -	BI_DA-
3	TX + and Vport +	BI_DB+
4	NC	BI_DC+
5	NC	BI_DC-
6	TX - and Vport +	BI_DB-
7	NC	BI_DD+
8	NC	BI_DD-

All of the Ethernet ports automatically detect the signal from the connected devices to negotiate the link speed and duplex mode (half- or full-duplex). Auto MDI/MDIX allows you to connect another switch, hub, or workstation without changing straight-through or crossover cables. Crossover cables cross-connect the transmit lines at each end to the received lines at the opposite end.



Connect one side of an Ethernet cable into any switch port and connect the other side to your attached device.

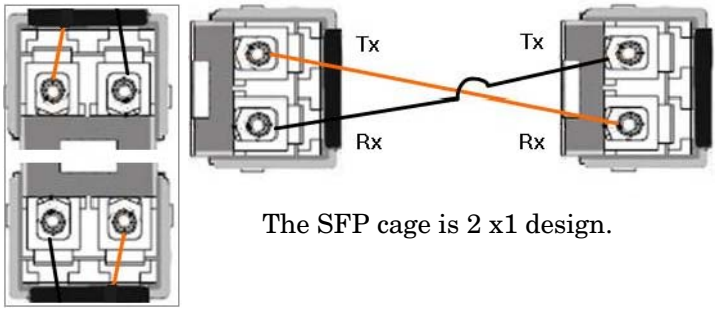
The **LNK/ACT** LED is lit when the cable is correctly connected. Always make sure that the cables between the switches and attached devices (for example, switch, hub, or workstation) are less than 100 meters (328 feet) and meet these requirements.

- **10BASE-T**: 2-pair UTP/STP Category 3, 4, 5 cable, EIA/TIA-568 100-ohm
- **100BASE-TX**: 2-pair UTP/STP Category 5, 5e cable, EIA/TIA-568 100-ohm
- **1000BASE-TX**: 4-pair UTP/STP Category 5 cable, EIA/TIA-568 100-ohm
- **IEEE 802.3af**: 4-pair UTP/STP Category 5 cable, EIA/TIA-568 100-ohm
- **IEEE 802.3at**: 4-pair UTP/STP Category 5e / 6 cable, EIA/TIA-568 100-ohm

Connect SFP Transceivers (Combo Ports 25-28)

The ES7528 equips four Gigabit SFP ports combined with RJ45 Gigabit Ethernet ports (Ports 25-28). The SFP ports accept standard mini GBIC SFP transceivers that support 1000BASE-X (1000BASE-SX/LX/LHX/XD/ZX).

To ensure system reliability, Comtrol recommends using Comtrol certified SFP Transceivers.



The SFP cage is 2 x1 design.

1. Plug the SFP transceiver into the SFP fiber transceiver.
2. Connect the transmit channel to the receive channel at each end.
3. Check the direction/angle of the fiber transceiver and the fiber cable.

   Note: *This is a Class 1 Laser/LED product. Do not stare at the Laser/LED Beam.*

The SFP port does not function until the fiber cable is linked to another active device. The SFP and corresponding RJ45 ports work in an exclusive mode. Traffic sent or received through the SFP module has priority thus no traffic is sent or received over the corresponding RJ45 connection. To use the RJ45 connection, remove the corresponding SFP.

Multi-Mode cables should not exceed 2KM and Single-Mode cables should not exceed 30km.

LED Descriptions

This subsection provides information about the ES7528 LEDs. You can also refer to *Device Front Panel* on Page 130 for information about using the web user interface to remotely view LED information.

LED Name	LED On	LED Blinking	LED Off
DC1 (Power) DC2 (Power)	Power available	Power not available	Power is off
PSU (AC power)	Power available	Power not available	Power is off
Alarm	Alarm activated		Alarm not activated
R.S. (Super-Ring Redundancy Manager)	Green: Normal Ring state Amber: Abnormal Ring state	Green Flashing: Incorrect configuration Amber Flashing: The break has been detected to be local to one of the ports	Super-Ring not active
Sys (System)	System ready	System is uploading firmware or the system is rebooting	System not ready
LEDs 1-24 Link/Act Duplex	 Green: 100M Yellow: 10M Green: Full-Duplex	 Green (802.3af): 1000M Blue (802.3at): 1000M Yellow: 10M	 Not connected Half-Duplex
LEDs G1-G4 Link/Act Duplex	 Duplex: Full-Duplex	Link/Act: Green: 1000M Yellow: 10M or 100M	Link/Act: Not connected Duplex: Half-Duplex

Initial Configuration Using NetVision

NetVision is a management utility for the RocketLinx family of switches. This section discusses the following procedures:

- *Setting Up NetVision*
- *NetVision Overview* on Page 16
- *Programming Network Information* on Page 18
- *Creating a Backup Configuration File* on Page 19
- *Uploading a Configuration File* on Page 20
- *Upgrading Firmware* on Page 21
- *Upgrading the Bootloader* on Page 22

Optionally, you can use the web user interface or the CLI to perform these tasks on the ES7528:

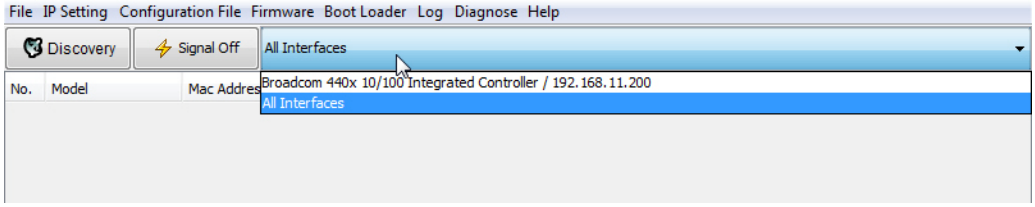
- *IP Configuration* on Page 40
- *Firmware Upgrade* on Page 58
- *Basic Settings (CLI)* on Page 148

Setting Up NetVision

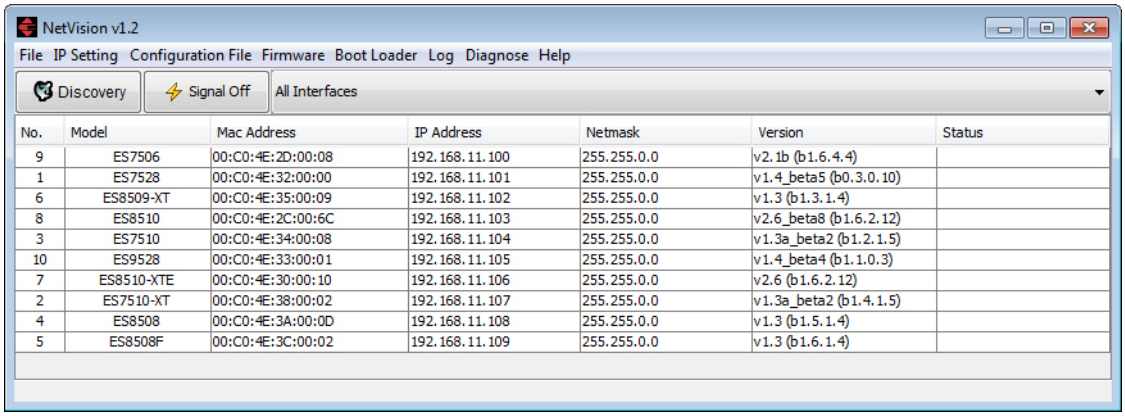
Use the following procedure to set up NetVision.

1. If necessary, install the latest version of the Java Runtime Environment.
2. Copy NetVision into a host system with a Windows operating system. Make sure that you note the file location because NetVision is an executable and it is not available through the Start button. For your convenience, you may want create a NetVision shortcut on your desktop.

   NetVision is available on the *RocketLinx Software and Documentation* CD or you can download NetVision from the ES7528 **Software** page on the Comtrol FTP site.
3. Start NetVision.
4. To locate RocketLinx switches connected to a specific interface, select the interface from the drop list or select **All Interfaces** to locate all RocketLinx managed devices on the network.



5. Click the **Discovery** button. After five seconds the ES7528 and any other managed RocketLinx models should display.



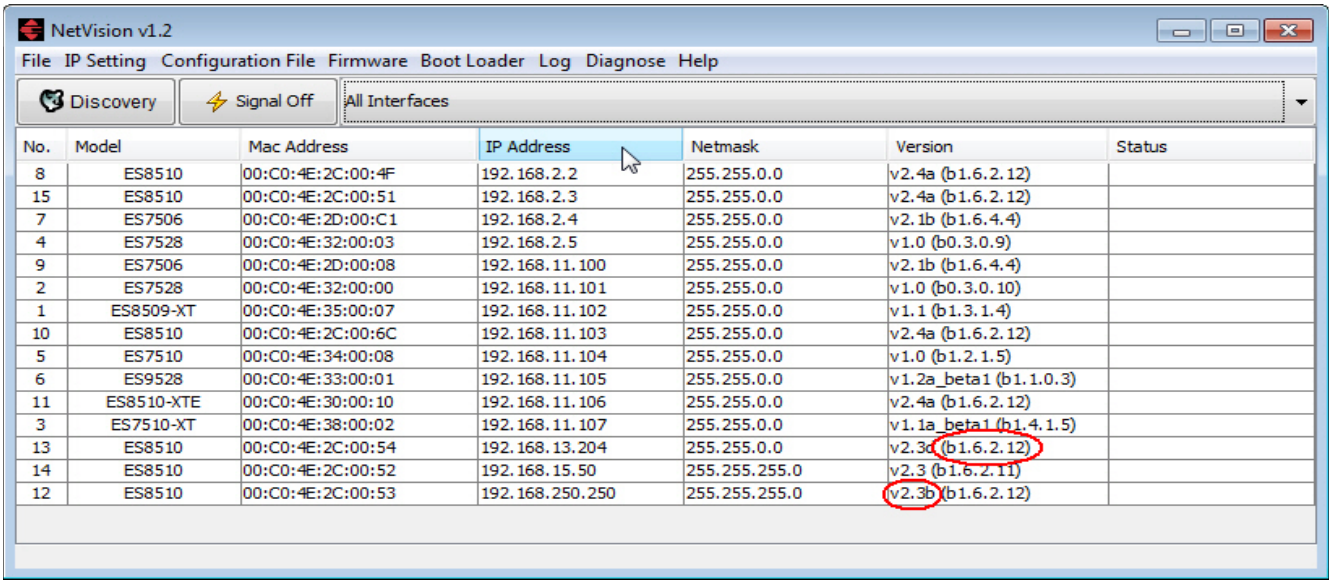
No.	Model	Mac Address	IP Address	Netmask	Version	Status
9	ES7506	00:C0:4E:2D:00:08	192.168.11.100	255.255.0.0	v2.1b (b1.6.4.4)	
1	ES7528	00:C0:4E:32:00:00	192.168.11.101	255.255.0.0	v1.4_beta5 (b0.3.0.10)	
6	ES8509-XT	00:C0:4E:35:00:09	192.168.11.102	255.255.0.0	v1.3 (b1.3.1.4)	
8	ES8510	00:C0:4E:2C:00:6C	192.168.11.103	255.255.0.0	v2.6_beta8 (b1.6.2.12)	
3	ES7510	00:C0:4E:34:00:08	192.168.11.104	255.255.0.0	v1.3a_beta2 (b1.2.1.5)	
10	ES9528	00:C0:4E:33:00:01	192.168.11.105	255.255.0.0	v1.4_beta4 (b1.1.0.3)	
7	ES8510-XTE	00:C0:4E:30:00:10	192.168.11.106	255.255.0.0	v2.6 (b1.6.2.12)	
2	ES7510-XT	00:C0:4E:38:00:02	192.168.11.107	255.255.0.0	v1.3a_beta2 (b1.4.1.5)	
4	ES8508	00:C0:4E:3A:00:0D	192.168.11.108	255.255.0.0	v1.3 (b1.5.1.4)	
5	ES8508F	00:C0:4E:3C:00:02	192.168.11.109	255.255.0.0	v1.3 (b1.6.1.4)	

Go to the *Programming Network Information* subsection on Page 18 to program the network information.

NetVision Overview

This subsection provides an overview of NetVision and NetVision menus.

You ca n change the order of any column by clicking the column heading. The following graph shows displaying the RocketLinx switches by IP address.

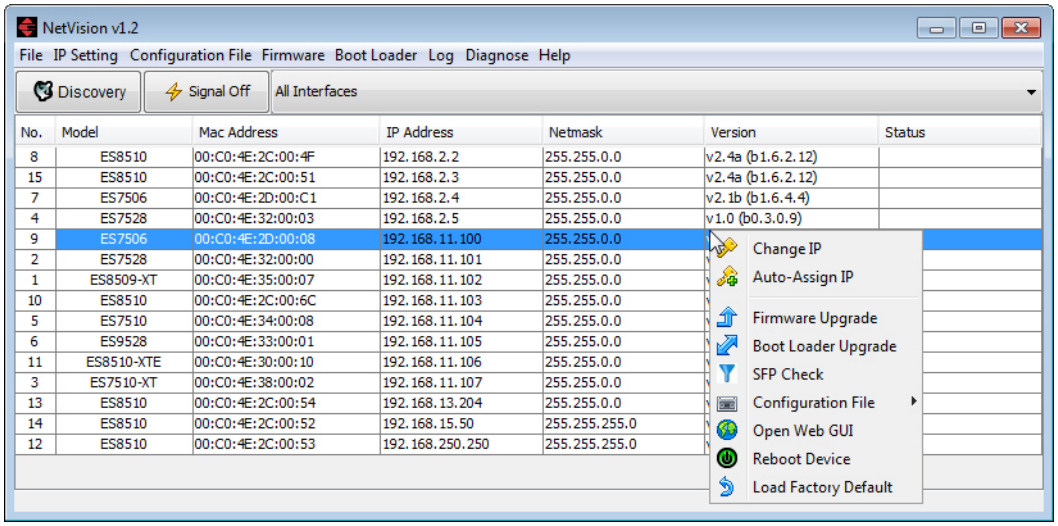


No.	Model	Mac Address	IP Address	Netmask	Version	Status
8	ES8510	00:C0:4E:2C:00:4F	192.168.2.2	255.255.0.0	v2.4a (b1.6.2.12)	
15	ES8510	00:C0:4E:2C:00:51	192.168.2.3	255.255.0.0	v2.4a (b1.6.2.12)	
7	ES7506	00:C0:4E:2D:00:C1	192.168.2.4	255.255.0.0	v2.1b (b1.6.4.4)	
4	ES7528	00:C0:4E:32:00:03	192.168.2.5	255.255.0.0	v1.0 (b0.3.0.9)	
9	ES7506	00:C0:4E:2D:00:08	192.168.11.100	255.255.0.0	v2.1b (b1.6.4.4)	
2	ES7528	00:C0:4E:32:00:00	192.168.11.101	255.255.0.0	v1.0 (b0.3.0.10)	
1	ES8509-XT	00:C0:4E:35:00:07	192.168.11.102	255.255.0.0	v1.1 (b1.3.1.4)	
10	ES8510	00:C0:4E:2C:00:6C	192.168.11.103	255.255.0.0	v2.4a (b1.6.2.12)	
5	ES7510	00:C0:4E:34:00:08	192.168.11.104	255.255.0.0	v1.0 (b1.2.1.5)	
6	ES9528	00:C0:4E:33:00:01	192.168.11.105	255.255.0.0	v1.2a_beta1 (b1.1.0.3)	
11	ES8510-XTE	00:C0:4E:30:00:10	192.168.11.106	255.255.0.0	v2.4a (b1.6.2.12)	
3	ES7510-XT	00:C0:4E:38:00:02	192.168.11.107	255.255.0.0	v1.1a_beta1 (b1.4.1.5)	
13	ES8510	00:C0:4E:2C:00:54	192.168.13.204	255.255.0.0	v2.3c (b1.6.2.12)	
14	ES8510	00:C0:4E:2C:00:52	192.168.15.50	255.255.255.0	v2.3 (b1.6.2.11)	
12	ES8510	00:C0:4E:2C:00:53	192.168.250.250	255.255.255.0	v2.3b (b1.6.2.12)	

v2.3b is the firmware version.
b1.6.2.12 is the Bootloader version.

You can highlight a RocketLinx and use the menus in the table below to perform the following tasks.

Optionally, highlight a RocketLinxor multiple RocketLinx switches, right-click, and use the pop-up menu.



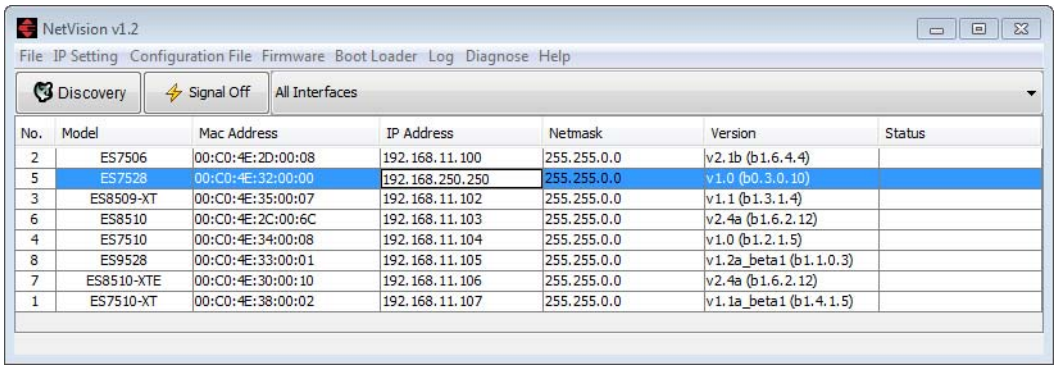
Menu	Option	Description
File	Discovery	Locates all RocketLinx managed switches on the network interface.
	LED Signal	Turns on or off the LEDs on a RocketLinx so that you can locate a specific RocketLinx without verifying the IP or MAC addresses.
	Open Web User Interface	Opens the web user interface for configuration automatically.
	Reboot Device	Reboots the RocketLinx. You can shift-click to reboot multiple RocketLinx switches.
	Load Factory Defaults	Reloads the factory defaults, including, the IP address and subnet mask. See *Factory Defaults* on Page 60 to reload the factory defaults without resetting the IP address and subnet mask.
	Preference	Sets the **Discovery** option for manual update (click the Discovery button) or automatically update every *xx* seconds.
	Exit	Exits NetVision.
IP Setting	Modify IP	Executes the IP address or netmask changes on the RocketLinx. See *Programming Network Information* on Page 18 for more information.
	Auto-Assign IP	Assigns a range of IP addresses to multiple RocketLinx switches.
Configuration File	Backup	Creates a backup file for the specified RocketLinx switch.
	Restore	Restores from a selected backup file.
	Load Default	Restores the RocketLinx with the default configuration file.
Firmware	Upgrade	Uploads the firmware that you have selected. The latest firmware file is available on the Comtrol FTP site. New firmware versions may include bug fixes or new features.
Boot Loader	Upgrade	Uploads the Bootloader file that you have selected. The latest Bootloader file is available on the Comtrol FTP site. A new Bootloader version may include bug fixes or new features.
Log	Show Panel	Opens a window in the bottom of the NetVision pane.
	Log Window	Opens a separate window that you can save, if necessary.
Diagnose	SFP Check	Verifies SFP operation.
	Self Test	Performs a self test RocketLinx. You can review the results in the log file.

Programming Network Information

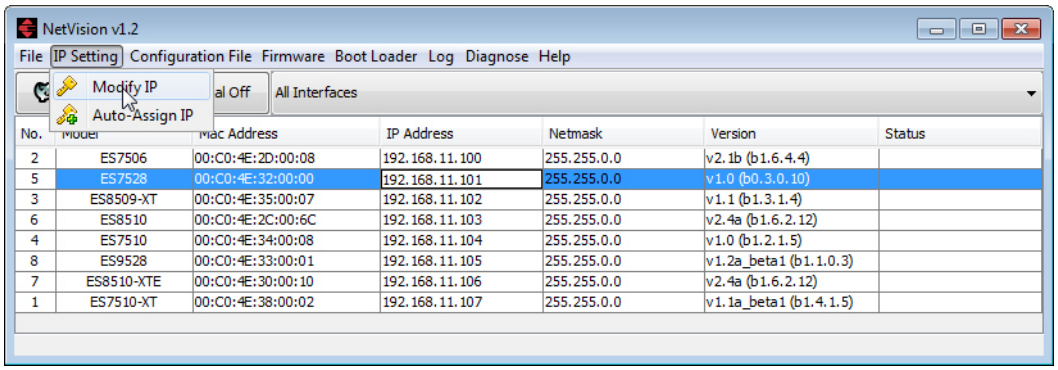
You can use the following procedure to program the network information into the ES7528.

Note: *If you have multiple RocketLinx managed switches that you want to program sequentially, you can use the following procedure and shift-click to highlight multiple switches. Enter an appropriate IP address range, subnet mask, and click Apply.*

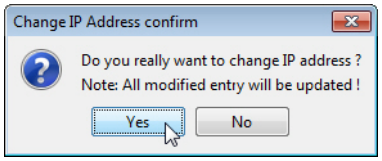
1. If you have not done so, start NetVision.
2. Click the **Discovery** button, after five seconds the ES7528 should be listed.
3. Highlight the ES7528, double-click the **IP Address** field and enter a desired IP address.



4. Double-click the **Netmask** field and enter a desired subnet mask.
5. Select the **IP Settings --> Modify IP** menu item to apply the IP address and Netmask changes to the ES7528. Optionally, you can right-click and click **Change IP**.



6. Click **Yes**.



Note: *Most menu items are available by right-clicking your mouse.Many of these functions can also be done using the web user interface or through the Command Line Interface.*

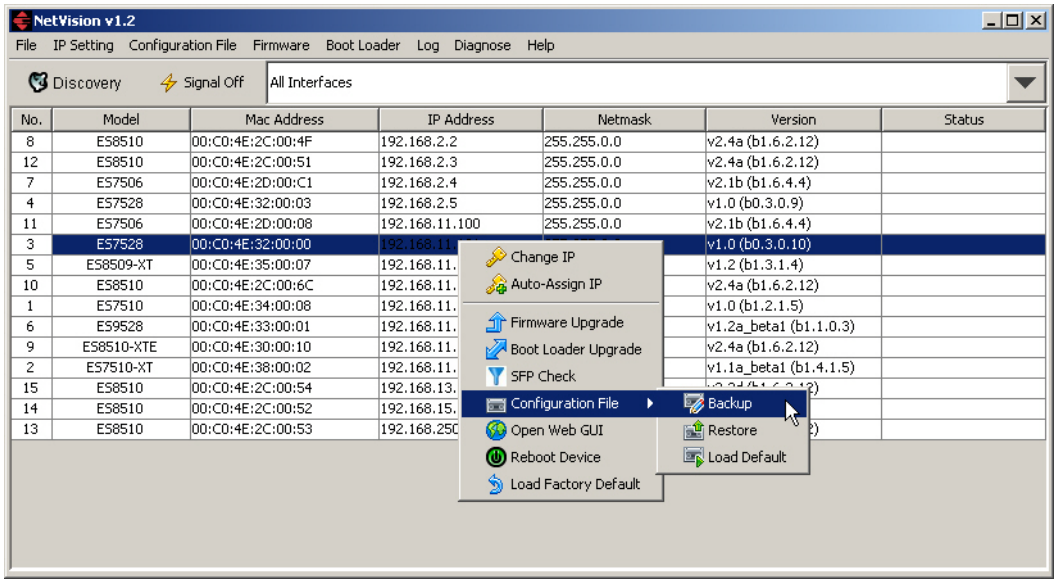
Creating a Backup Configuration File

You can use NetVision to save the current configuration stored in the ES7528 flash using a Windows XP system.

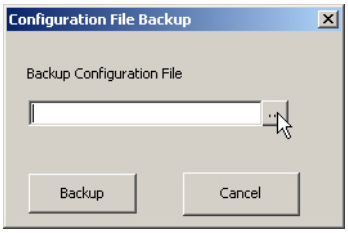
Note: *For operating systems newer than Windows XP, use TFTP with the web user interface (Backup the Configuration - TFTP Server Method on Page 54) or the CLI (Backup and Restore on Page 152).*

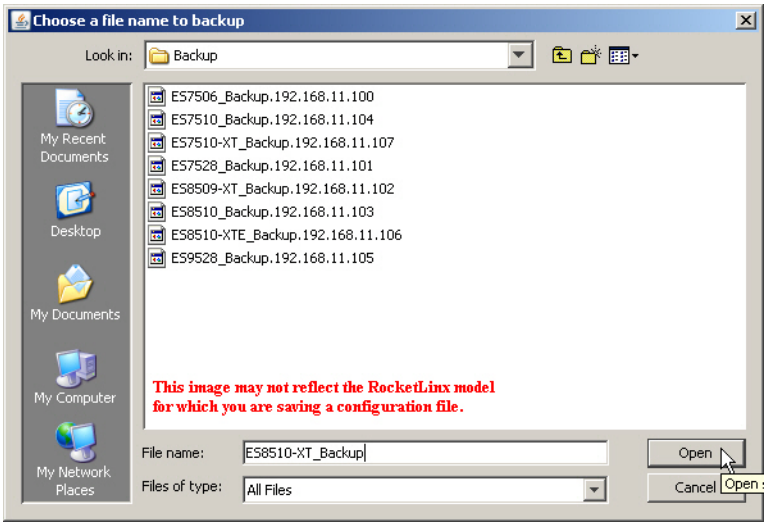
The configuration file can be reloaded on the ES7528 or used load the same settings onto another ES7528. The ES7528configuration file is a standard text file. You can open the file with Word or Notepad. You can also modify the file, add/remove the configuration settings, and then restore the file back to the ES7528.

1. Highlight the ES7528 for which you want to create a backup file.
2. Right-click and select **Backup**.

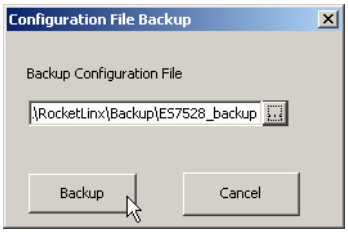


3. Click the **Browse** button and navigate to the location where you want to save the configuration file.
4. Enter the backup file name and click **Open**.





5. Click the **Backup** button.



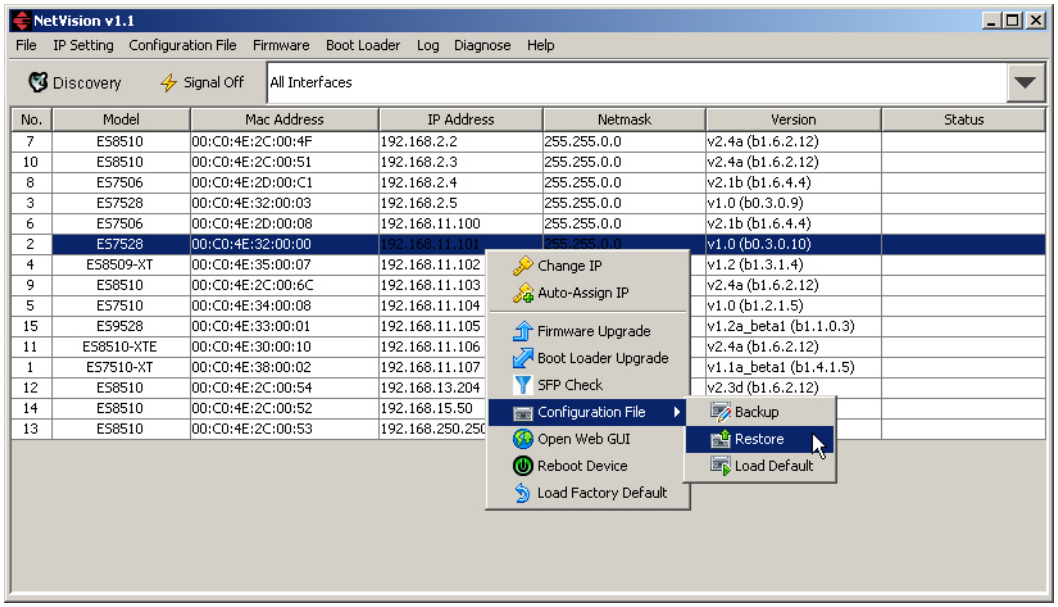
Uploading a Configuration File

Before you can restore a configuration file, you must have saved the backup configuration file using Windows XP. To restore a configuration file on an operating system later than Windows XP, go to *Restore the Configuration - TFTP Server Method* on Page 57 or *Backup and Restore* on Page 152.

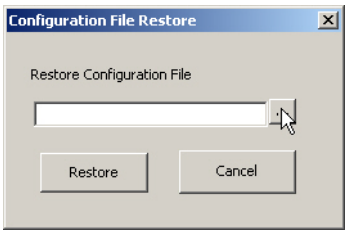
Note: *If you are using an operating system later than Windows XP you must have created a backup file using TFTP with the web user interface (Backup the Configuration - TFTP Server Method on Page 54) or the CLI (Backup and Restore on Page 152.).*

The ES7528configuration file is a standard text file. You can open the file with Word or Notepad. You can also modify the file, add/remove the configuration settings, and then restore the file back to the ES7528. You can only load configuration files from the same RocketLinx model.

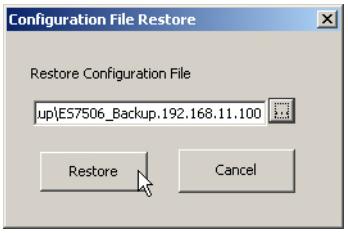
1. Highlight the ES7528 on to which you want to load the configuration file, right-click, and select **Restore**.



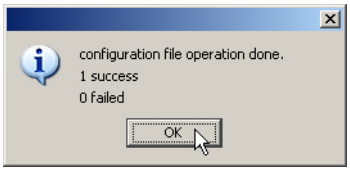
2. Click the **Browse** button to locate the backup file.

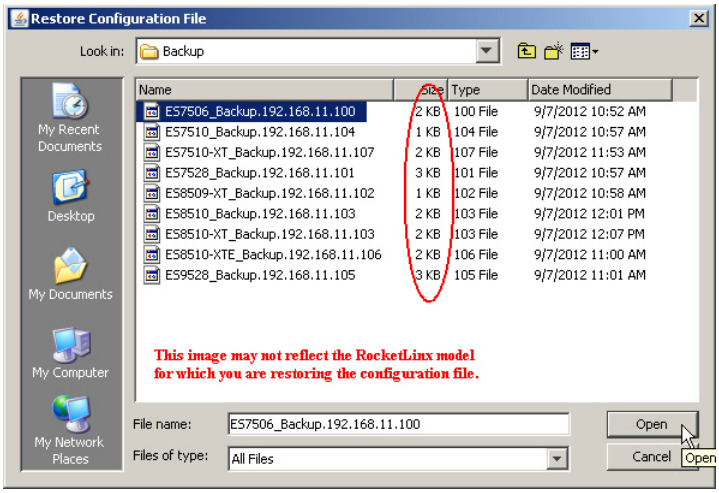


3. Highlight the appropriate backup file, and click **Open**.
4. Click the **Restore** button.



5. Click the **Ok** button to the *Success* message.



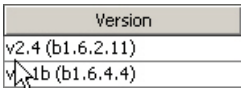


Upgrading Firmware

There are several methods that you can use to upload the latest firmware into the ES7528. Optionally, you can use the web user interface (*Firmware Upgrade* on Page 58) or the CLI (*Firmware Upgrade* on Page 153).

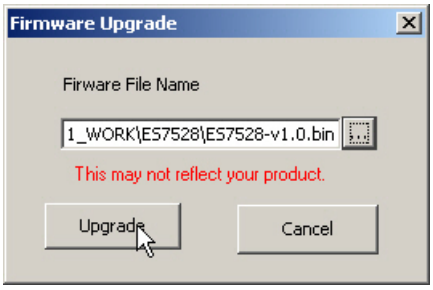
Use this procedure to upload the latest ES7528 firmware into the RocketLinx using NetVision.

1. Locate and download the firmware by selecting the **Software** page that corresponds to your RocketLinx switch by accessing the Comtrol FTP site.
2. Highlight the ES7528 (or several ES7528 switches) and note the firmware version.
3. Right-click and select **Firmware Upgrade**.



4. Browse to the location of the firmware file, select the file, and click **Upgrade**.

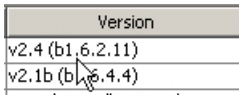
   Status first displays *Firmware uploading* and then displays *Firmware Burning* in the **Status** field.
5. Verify that when the **Status** field is empty, that the version number matches the new version number.
6. Click **Discovery** to update the display.

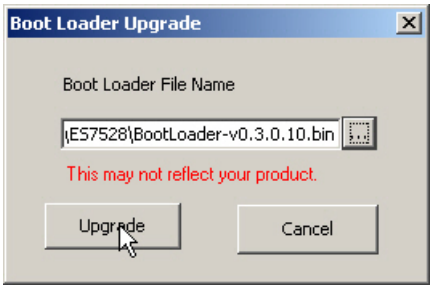


Upgrading the Bootloader

Use the following procedure to upload the latest ES7528 Bootloader into the RocketLinx. You cannot use the web user interface or CLI to upload the Bootloader.

1. Locate and download the Bootloader by selecting the **Software** page that corresponds to your RocketLinx switch by accessing the Comtrol FTP site.
2. Highlight the ES7528 switch (or several ES7528 switches) and note the version, which is displayed in parenthesis.
3. Right-click and select **Boot Loader Upgrade**.
4. Browse to the location of the firmware file, select the file, and click **Upgrade**.
5. Click **Discovery** to update the display.
6. Verify that when the **Status** field is empty, that the version number matches the new version number.





Configuration Using the Web User Interface

The ES7528 provides in-band and out-band configuration methods:

- Out-band management means that you configure the ES7528 using the RS-232 console cable and the Command Line Interface (CLI) to access the ES7528 without attaching an admin PC to the network. You can use out-band management if you lose the network connection to the ES7528. The CLI and Telnet are discussed in *Configuration Using the Command Line Interface (CLI)* on Page 133.
- In-band management means that you connect remotely using the ES7528 IP address through the network. You can remotely connect with the ES7528 embedded Java applet web user interface or a Telnet console and the CLI. The ES7528 provides HTTP web user interface (Page 24) and secure HTTPS web user interface (Page 26) for web management.

Configuration Overview

This subsection discusses a minimum level of configuration required to operate the ES7528.

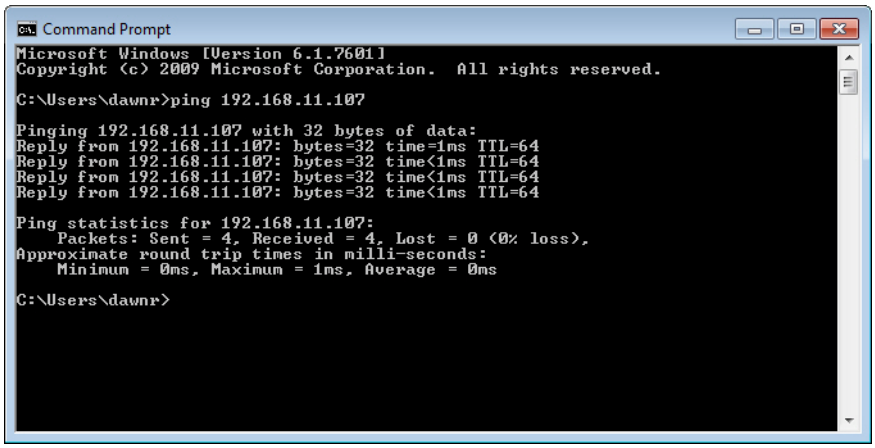
1. If you have not done so, install the hardware, see *Hardware Installation* on Page 9.
2. If you are planning on using in-band management, you need to program the ES7528 IP address to meet your network requirements. The easiest way to configure the IP address is using a Windows system and NetVision, see *Programming Network Information* on Page 18.
3. If you are planning on connecting PDs, configure the PoE port characteristics, see *PoE Control* on Page 70.
4. Configure other features as desired. You can refer to the *Feature Overview* on Page 28 to locate configuration information or use these links:
   - *Basic Settings* on Page 38
   - *Port Configuration* on Page 61
   - *Power over Ethernet* on Page 70
   - *Network Redundancy* on Page 74
   - *VLAN* on Page 86
   - *Private VLAN* on Page 94
   - *Traffic Prioritization* on Page 97
   - *Multicast Filtering* on Page 100
   - *SNMP* on Page 104
   - *Security* on Page 107
   - *Warning* on Page 117
   - *Monitor and Diag* on Page 123
   - *Device Front Panel* on Page 130
   - *Save to Flash* on Page 131
   - *Logout* on Page 131

Web User Interface

The ES7528 web management page was developed with Java. You can use any standard web browser, which is compatible with Java Runtime to configure and communicate with the ES7528 from anywhere on the network.

If you did not program the IP address for your network using NetVision (*Programming Network Information* on Page 18), you need to change your computer IP address to **192.168.250.x** (Network Mask: 255.255.0.0). The default IP address for the ES7528 is *192.168.250.250*.

1. Open a command prompt window and ping the IP address for the ES7528 to verify a normal response time.



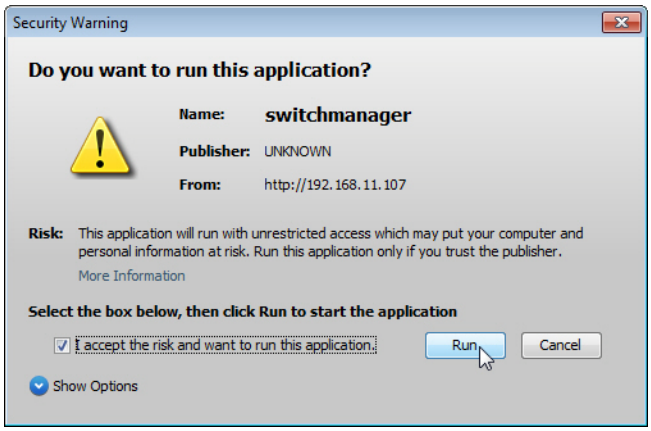
2. Launch the web browser on the PC using one of these methods:
   - Right-click the ES7528 in NetVision and click **Open Web GUI**.
   - Type **http://192.168.250.250** (or the IP address of the switch), and then press **Enter**.

Windows XP - Windows Server 2003

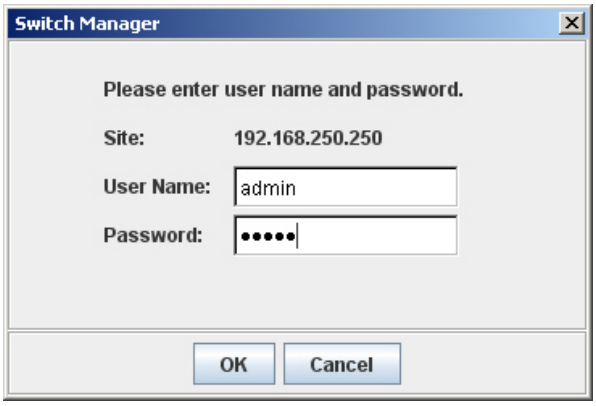
If a *Warning - Security* message appears, click **Always trust content from this publisher** and then **Run** when requested to run the application (IP address).

Windows Vista - Windows 7

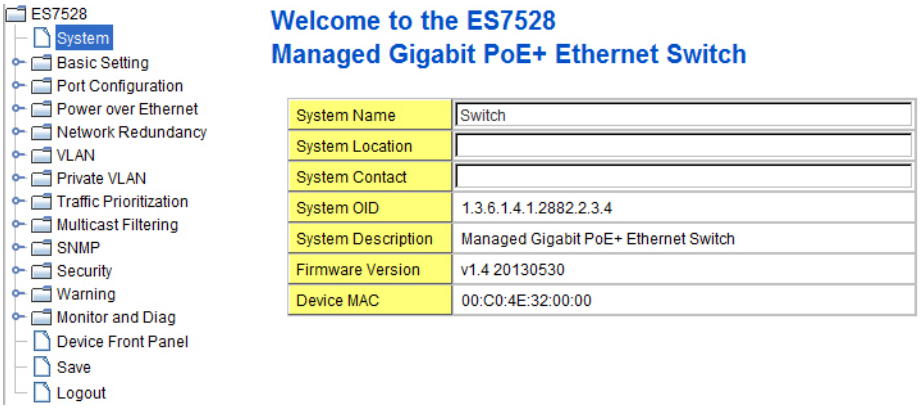
If necessary, click **I accept the risk and want to run this application**, and then **Run** if a security warning popup message appears.



3. Enter the user name, the password, and click **OK**. The default user name and password are both **admin**.



The *Welcome* page of the web management interface then appears.



4. If you have not done so, you can change the ES7528 IP address to meet your network environment.
   a. Double-click **Basic Setting**.
   b. Click **IP Configuration**.
      To use static addressing, enter a valid IP add dress, subnet mask and default gateway.
      To use DHCP, click **Enable** in the **DHCP Client** drop list.
   c. Click **Apply**.
5. If you are planning on connecting PDs, configure the PoE port characteristics, see *PoE Control* on Page 70.

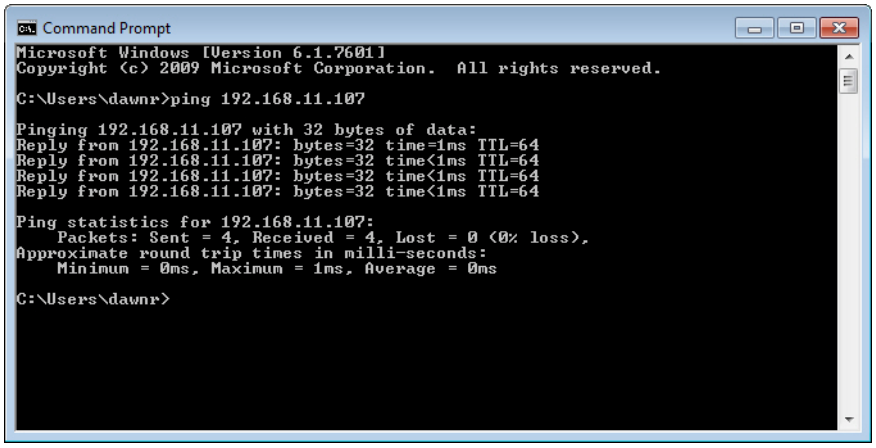
You can use the *Feature Overview* on Page 28 to locate other features that you may want to configure.

Secure Web User Interface

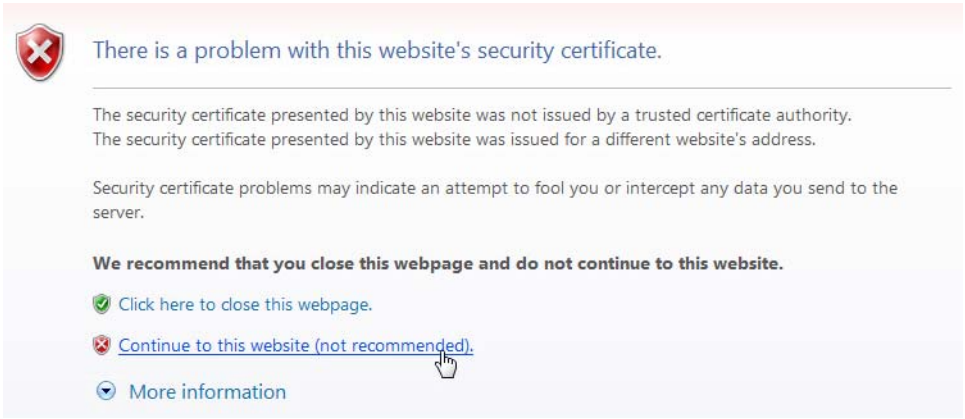
The ES7528 web user interface also provides secured management through an HTTPS login so that all of the configuration commands are secure.

If you did not program the IP address for your network using NetVision (*Programming Network Information* on Page 18), you need to change your computer IP address to **192.168.250.x** (Network Mask: 255.255.0.0). The default IP address for the ES7528 is *192.168.250.250*.

1. Open a command prompt window and ping the IP address for the ES7528 to verify a normal response time.

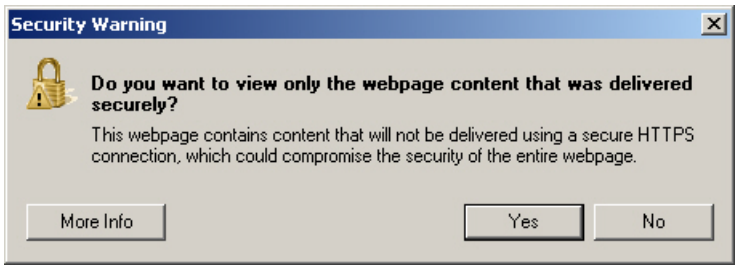


2. Launch the web browser and type **https://192.168.250.250** (or the IP address of the ES7528).and then press **Enter**.
3. Click **Continue to the web site (not recommended)**.



Windows XP and Windows Server 2003

a. Click **No** when the popup screen appears and requests you to trust the secured HTTPS connection distributed by the ES7528.

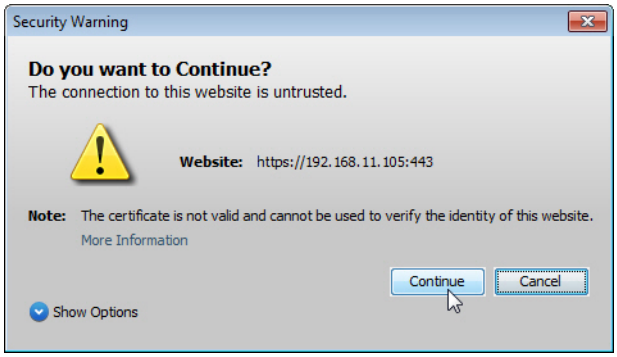


b. Click **Always trust content from this publisher** and then **Run** when requested to run the application (IP address) in the *Warning - Security* message.

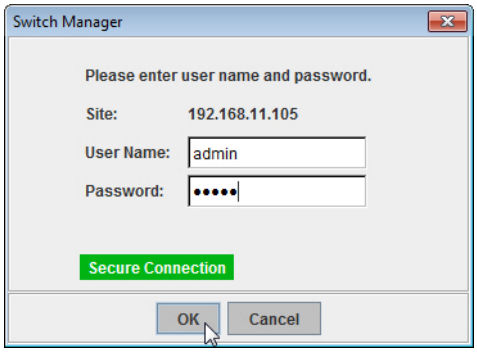
Windows Vista - Windows 7

a. Click the **Continue** button.

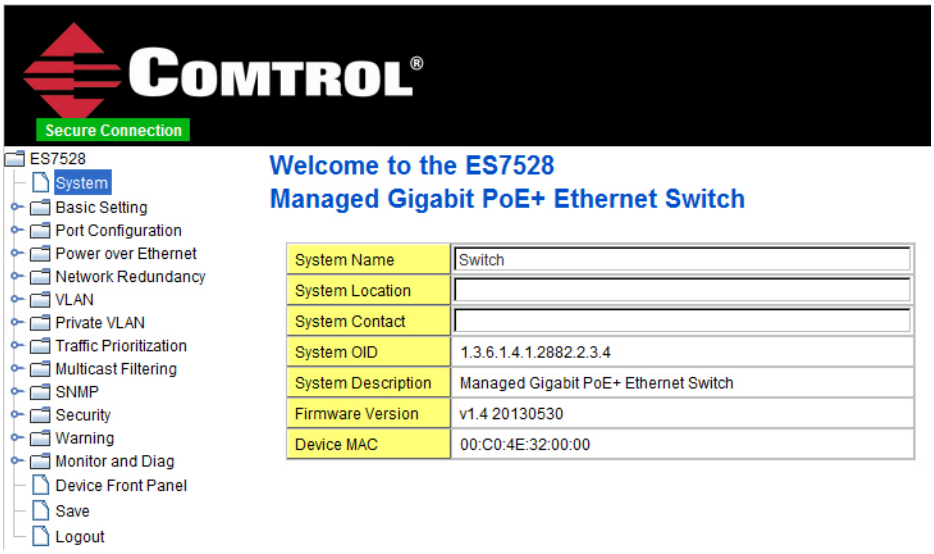
b. If necessary, click **I accept the risk and want to run this application** and then **Run** if a security warning popup message appears.



4. Enter the user name and the password and click **OK**. The default user name and password are both **admin**.



The *Welcome* page of the web management interface then appears.



5. If you have not done so, you can change the ES7528 IP address to meet your network environment.
   a. Double-click **Basic Setting**.
   b. Click **IP Configuration**.
      To use static addressing, enter a valid IP address, subnet mask and default gateway.
      To use DHCP, click **Enable** in the **DHCP Client** drop list.
   c. Click **Apply**.
6. If you are planning on connecting PDs, configure the PoE port characteristics, see *PoE Control* on Page 70.

Feature Overview

The following table provides detailed information about ES7528 features and provides the location of the configuration information in the web user interface.

Type	Category	Details
802.1x Port-Based Network Access Control Configuration	*802.1x Configuration* on Page 113	• System Authentication Control - Enable/Disable • Authentication Method - RADIUS or Local • RADIUS Server - IP Address, Shared Key, Server Port, and Accounting Port • Local RADIUS User - User Name, Password, and VID • Secondary RADIUS Server - IP Address, Shared Key, Server Port, and Accounting Port • Local RADIUS User List

Type	Category	Details
802.1x Port-Based Network Access Control Port Configuration	*802.1x Port Configuration* on Page 114	Port Configuration • Port Control - Auto, Forced Authorized, or Force Unauthorized • Re-authentication - Enable/Disable • Maximum Request • Guest VLAN • Host Mode - Single/Multi • Admin Control Direction - Both or In Timeout Configuration • Port by Port • Re-Authentication Periods • Quiet Period • Tx Period • Supplicant Timeouts • Server Timeouts
802.1x Port-Based Network Access Control Port Status	*802.1x Port Status* on Page 116	• Port by Port • Port Control • Authorize Status • Authorized Supplicant • Oper Control Direction
Admin Password	*Admin Password* on Page 39	• Admin
Backup and Restore	*Backup and Restore* on Page 51	Local or TFTP
CoS-Queuing Mapping	*CoS-Queue Mapping* on Page 98	• CoS 0 through 7 • Queue 0 through 7 • Queue 7 highest priority
DHCP Server Configuration	*DHCP Server Configuration* on Page 46 *DHCP Leased Entries* on Page 48 *DHCP Relay Agent* on Page 49	• DHCP Server Configuration - Excluded Addresses and Manual Binding - Port and IP Address - Option 82 • DHCP Leased Entries • DHCP Relay Agent - Helper Address 1-4 - DHCP Option82 Relay Agent (Circuit ID/Remote ID)
DSCP-Queuing Mapping	*DSCP-Queue Mapping* on Page 99	• DSCP 0 through 7 • Queue 0 through 7 • Queue 7 highest priority

Type	Category	Details
Event Selection	*Event Selection* on Page 120	• Device Cold Start • Device Warm Start • Authentication Failure • Time Synchronization Failure • Power 1 Failure • Power 2 Failure • AC Failure • Fault Relay • Super Ring Topology Change • SFP Failure • Port by Port Event Selection
Fault Relay	*Warning* on Page 117	Relay 1- Multi-event • Power • Port Link (Port or Ports) • Ring Failure • Ping Failure - IP Address • Ping Reset, IP Address, Reset Time (Sec), and Hold Time (Sec) • Dry Output - On Period (Sec) and Off Period (Sec)
Filter Set/Attach	*Security* on Page 107	• Packet Filtering by MAC or IP • IP Filter ID/Name • Ingress Ports
GMRP Configuration	*Multicast Filtering* on Page 100	• Enable/Disable • Port by Port Basis
GVRP Configuration	*GVRP Configuration* on Page 92	• 2K Entries • Enable/Disable GVRP Protocol • State - Enable/Disable • Join Timer • Leave Timer • Leave All Timer
IGMP Query	*IGMP Query* on Page 102	• Version - Version 1, Version 2, or Disable • Query Intervals • Query Maximum Response Time
IGMP Snooping	*IGMP Snooping* on Page 101	• Enable/Disable • VID • Port by Port IGMP Snooping Table - IP Address - VID

Type	Category	Details
IP Configuration	*Basic Settings* on Page 38	• IPv4 and IPv6 support • DHCP • DNS1 and DNS2
Jumbo Frame	*Basic Settings* on Page 38	• System MTU 1518 (Range 64-9216)
MAC Address Table (8K)	*MAC Address Table* on Page 123	• Aging Time (Sec) • Static Unicast MAC Address - MAC Address, VID, and Port • Port by Port MAC Address Table View - Static Unicast - Dynamic Unicast - Static Multicast - Dynamic Multicast
MSTP Configuration	*MSTP Configuration* on Page 79	• MSTP Region Configuration - Name and Revision • New MST Instance - Instance ID, VLAN Group, and Instance Priority • Current MST Instance Configuration - Instance ID, VLAN Group, and Instance Priority
MSTP Information	*MSTP Information* on Page 82	• Instance ID • Root Information - Root Address - Root Priority - Root Port - Root Path Cost - Maximum Age - Hello Time - Forward Delay • Port Information - Role - Port State - Path Cost - Port Priority - Link Type - Edge Port
MSTP Port Configuration	*MSTP Port Configuration* on Page 81	Instance ID • Port • Path Cost • Priority • Link Type • Edge Port
Ping Utility	*Ping Utility* on Page 129	Target IP Address

Type	Category	Details
PoE Control	*PoE Control* on Page 70	• PoE System - Enable/Disable • DC1 and DC2 Power Budget - Watts, Voltage, and Power Budget Warning Level • Port by Port - PoE - Enable/Disable - Powering Mode - 802.3af, 802.3at (LLDP), 802.3af (2-event) or Force - Power Budget (W) - Power Priority - Critical, High, Or Low • PD Status Detection - Enable/Disable - PD IP Address - Cycle Time
PoE Scheduling	*PoE Scheduling* on Page 72	PoE Ports On/Off on an hourly/daily basis.
PoE Status	*PoE Status* on Page 73	Displays: • DC1/2 Power (V and W) • AC Power (V and W) • Primary/Secondary Power • Tertiary Power • Total Power Budget • Total Output Power • Power Budget Warning Level • Utilization • Event Port by Port: • PoE Mode • Operation Status • PD Class • Consumption(W) • Voltage(V) • Current(mA)
Port Control	*Port Control* on Page 61	• Enable/Disable Port State • Speed/Duplex - Auto-Negotiation, 10 Full/Half, 100 Full/Half, and 1000 Full (Ports 25-28) • Flow control - Disable/Symmetric • User-Defined Description
Port Mirror Mode	*Port Mirroring* on Page 126	• Port Mirror Mode - Enable/Disable • Port by Port - Source Port - Rx and Tx - Destination Port - Rx and Tx

Type	Category	Details
Port Statistics	*Port Statistics* on Page 125	Port by Port • Type • Link • State • Rx and Tx Good • Rx and Tx Bad • Rx Abort • Collision
Port Status	*Port Status* on Page 63	• Port Type • Link - Up/Down • State - Enable/Disable • Speed/Duplex • Flow Control • SFP Vendor, Wavelength, and Distance • SFP DDM - Temperature, Tx Power, and Rx Power
Port Trunk	*Aggregation Setting* on Page 67 *Aggregation Status* on Page 69	Aggregation Settings • Group ID - Trunk 1-8 • Trunk Type - Static or 802.3ad LACP • Load Balance - MAC hash or IP hash Aggregation Status by Trunk • Type • Aggregated Ports • Individual Ports • Link down Ports
PVLAN Configuration	*PVLAN Configuration* on Page 94	• VLAN ID • PVLAN Type - None, Primary, Isolated, and Community
PVLAN Information	*PVLAN Information* on Page 96	• Primary VLAN • Secondary VLAN • Secondary VLAN Type • Ports
PVLAN Port Configuration	*PVLAN Port Configuration* on Page 95	Port Configuration • PVLAN Port Type - Normal, Host, or Promiscuous • VLAN ID PVLAN Association • Secondary VLAN • Primary VLAN

Type	Category	Details
QoS Setting	*QoS Setting* on Page 97	Queue scheduling • Use a Round Robin Scheme • Use Weighted Round Robin Scheme • Use A Strict Priority Scheme •
Rate Control	*Rate Control* on Page 65	• Ingress Rate (1 Mbps to 100Mbps) • Egress Rate (1 Mbps to 100Mbps)
Redundant Ring	*Redundant Ring* on Page 84	• Ring ID and Name • Ring Configuration - ID - Name - Version (Super Ring and Rapid Super Ring) - Device Priority - Ring Port - Path Cost - Ring Port2 - Path Cost - Rapid Dual Homing - Ring Status
Redundant Ring Information	*Redundant Ring Information* on Page 85	• 32 Ring ID Maximum • Supports Up To 12 x 100M Rings Plus 2 Gigabit Rings Aggregation Capability • Version • Role • Status • RM MAC • Blocking Port • Role Transition Count • Ring State Transition Count
Reset/Reboot	*Factory Defaults* on Page 60 *System Reboot* on Page 60	• Reset to Factory Default Values • Reboot from Interface
SNMP Configuration	*SNMP Configuration* on Page 104	• V1/V2c Community • Public - Read Only or Read and Write • Private - Read Only or Read and Write
SNMP Traps	*SNMP Traps* on Page 106	• Enable/Disable • Trap Server - Server IP Address, Community, and Version (V1 or V2c) • Trap Server Profile - Displays Server IP, Community, and Version

Type	Category	Details
SNMP V3 Profile	*SNMP V3 Profile* on Page 105	SNMP V3 • User Name • Security Level • Authentication Level • Authentication Password • DES Password SNMP V3 Users - Displays Profile Information
Storm Control	*Storm Control* on Page 66	Rate Control • Broadcast Rate (0-262143 Kbits) • Destination Lookup Failure (DLF) Rate (0-1000000 Kbits) • Multicast Rate (0-262143 Kbits) Port Configuration • Ports 1-28 (Enable/Disable) • Broadcast Rate • DLF Rate • Multicast Rate
STP Configuration	*STP Configuration* on Page 75	• STP, RSTP, MSTP, or Disable • Bridge Address • Bridge Priority • Maximum Age • Hello Time • Forward Delay
STP Information	*STP Information* on Page 77	• Root Information - Root Address - Root Priority - Root Port - Root Path Cost - Maximum Age - Hello Time - Forward Delay • Port Information - Role - Port State - Path Cost - Port Priority - Link Type - Edge Port - Aggregated (D/Type)

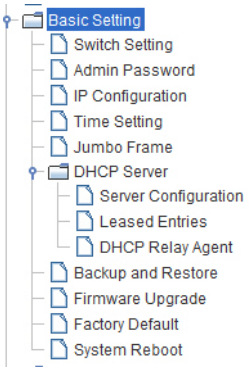
Type	Category	Details
STP Port Configuration	*STP Port Configuration* on Page 76	Port by Port • STP State • Path Cost • Priority • Link Type • Edge Port
SYSLOG Mode	*SysLog Configuration* on Page 121	• Disable, Local, Remote, or Both • Remote IP Address
System Event Logs	*Event Log* on Page 127	• Index • Date • Time • Event Log
Time Setting	*Time Setting* on Page 42	• IEEE 1588 • Manual or NTP Client • Time Zone Setting • Daylight Savings Time
Topology Discovery	*Topology Discovery (LLDP)* on Page 128	• LLDP - Enable/Disable • LLDP Configuration - Timer and Hold Time • LLDP Port State - Local Port, Neighbor ID, Neighbor IP, and Neighbor VID
Unknown Multicast	*Unknown Multicast* on Page 102	• Send to Query Ports • Send to All Ports • Discard
Upgrade Firmware	*Firmware Upgrade* on Page 58	Local or TFTP
VLAN Configuration	*VLAN Configuration* on Page 89	• Tunneling support for 256 • Management VLAN ID • Static VLAN - ID and Name • Static VLAN Configuration - VLAN ID, Name, and Ports (Options: No VLAN, Trunk Link, or Access Link)
VLAN Port Configuration	*VLAN Port Configuration* on Page 86	• PVID • Tunnel Mode • EtherType • Accept Frame Type • Ingress Filtering

Type	Category	Details
VLAN Table	*VLAN Table* on Page 93	• VLAN ID • Name • Status • Port by Port
Warning - SMTP Configuration	*SMTP Configuration* on Page 122	• Email Alert - Enable/Disable • SMTP Server IP • Mail Account • Authentication • User Name • Password • Recipient Email Address 1-4

Basic Settings

The *Basic Setting* group allows you the ability to configure switch information, IP address, User name/ Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

The following web pages are included in this group:

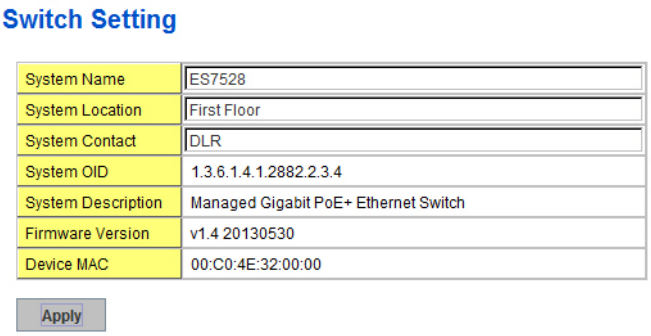


- *Switch Setting* on Page 38
- *Admin Password* on Page 39
- *IP Configuration* on Page 40
- *Time Setting* on Page 42
- *Jumbo Frame* on Page 45
- *DHCP Server Configuration* on Page 46
- *Backup and Restore* on Page 51
- *Firmware Upgrade* on Page 58
- *Factory Defaults* on Page 60
- *System Reboot* on Page 60

Optionally, you can use the CLI for configuration, see *Basic Settings (CLI)* on Page 148.

Switch Setting

You can assign the **System Name**, **Location**, **Contact** and view ES7528 information.

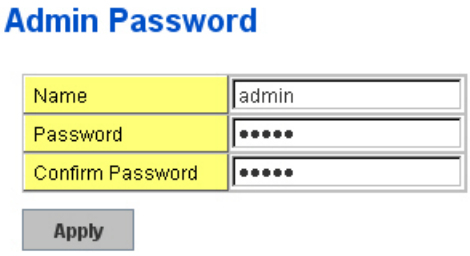


Switch Setting Page	
System Name	You can assign a name to the ES7528. You can input up to 64 characters. After you configure the name, The CLI system selects the first 12 characters as the name in CLI system.
System Location	You can specify the ES7528 physical location with up to 64 characters.
System Contact	You can specify contact people with up to 64 characters by typing the Administer's name, mail address or other information.
System OID	The SNMP Object ID of the ES7528. You can follow the path to find its private MIB in an MIB browser. ***Note:*** *When you attempt to view private MIB, you should first compile private MIB files into your MIB browser.*
System Description	Managed Gigabit PoE + Ethernet Switch.
Firmware Version	Displays the firmware version installed in this ES7528.
Device MAC	Displays a unique hardware address (MAC address) assigned in the factory.

Switch Setting Page (Continued)	
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Admin Password

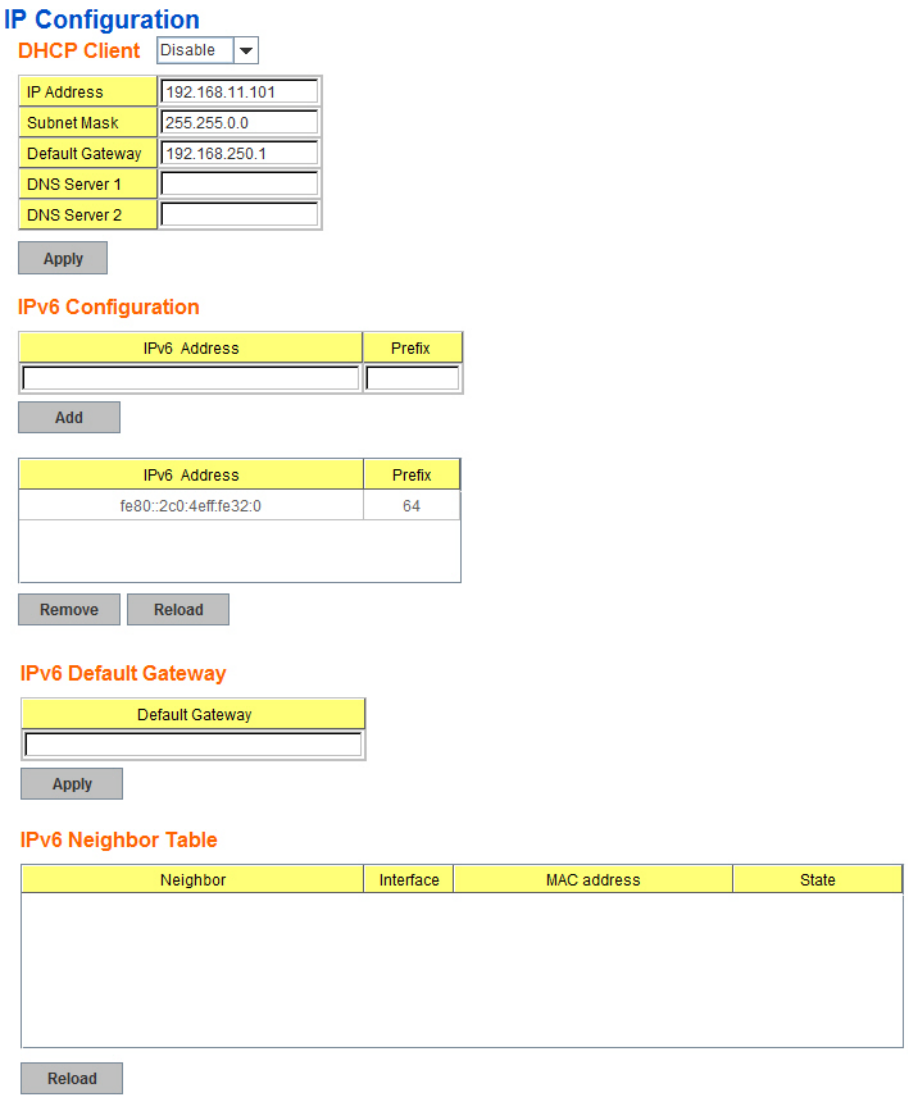
You can change the user name and the password here to enhance security.



Admin Password	Description
User name	You can enter a new user name here. The default name is **admin**.
Password	You can enter a new password here. The default password is **admin**.
Confirm Password	You need to type the new password again to confirm it.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

IP Configuration

This function allows you to configure the ES7528's IP address settings.

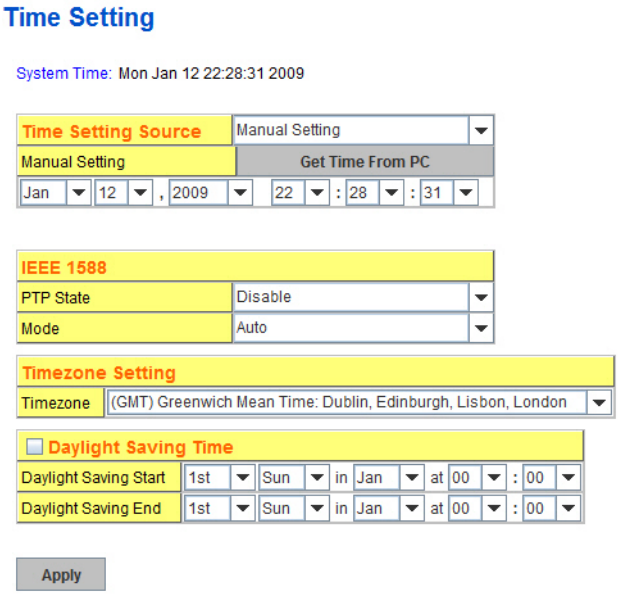


IP Configuration Page	
DHCP Client	You can select to **Enable** or **Disable** the DHCP Client function. When the DHCP Client function is enabled, an IP address is assigned to the switch from the network's DHCP server. In this mode, the default IP address is replaced by the one assigned by DHCP server. If DHCP Client is disabled, then the IP address that you specified is used.
IP Address	You can assign the IP address reserved by your network for the ES7528. If the DHCP Client function is enabled, you do not need to assign an IP address to the ES7528, because it is overwritten by the DHCP server and displays here. The default IP Address is 192.168.250.250.

IP Configuration Page (Continued)	
Subnet Mask	You can assign the subnet mask for the IP address here. If the DHCP Client function is enabled, you do not need to assign the subnet mask. The default Subnet Mask is 255.255.255.0. ***Note:*** *In the CLI, the enabled bit of the subnet mask is used to represent the number displayed in the web management interface. For example, 8 represents: 255.0.0.0,16 represents: 255.255.0.0, 24 represents: 255.255.255.0.*
Default Gateway	You can assign the gateway for the switch here. The default gateway is 192.168.250.1. ***Note:*** *In the CLI, use 0.0.0.0/0 to represent the default gateway.*
DNS Server 1/2	The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.
IPv6 Address	You can enter an IPv6 address for the ES7528. An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:), and the length of IPv6 address is 128bits. The 64-bit interface identifier is automatically generated from the MAC address for the ES7528 using the modified EUI-64 format.
Prefix	This IPv6 prefix specifies the size of a network or subnet. The default is 64.
IPv6 Default Gateway	The IPv6 default gateway IP address identifies the gateway (for example, a router) that receives and forwards those packets whose addresses are unknown to the local network. The agent uses the default gateway address when sending alert packets to the management workstation on a network other than the local network.
IPv6 Neighbor Table	
Neighbor	The *IPv6 Neighbor Table* lists neighbors of the ES7528.
Interface	The interface connected to the neighbor.
MAC address	This is the MAC address of the neighbor.
State	This displays the Neighbor Unreachability Detection (NUD) state of the neighbor entry.
Remove	Click the **Remove** button to remove an IPv6 configuration or IPv6 Neighbor Table entry.
Reload	Click the **Reload** button to reload IPv6 configuration.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Time Setting

Time Setting allows you to set the time manually or through a Network Time Protocol (NTP) server. NTP is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network. The ES7528 also provides Daylight Saving functionality.



Time Setting Page	
Time Setting Source	**Manual Setting**: Click **Manual Setting** to change time as needed. You can also click the **Get Time from PC** button to get PC's time setting for the ES7528. **NTP client**: Click **Time Setting Source** if you want the NTP client to permit the ES7528 to enable the NTP client service. NTP client is automatically enabled if you change the Time Setting Source to NTP Client. The system sends a request packet to acquire current time from the NTP server you assign.
IEEE 1588	The IEEE 1588 PTP (Precision Time Protocol) supports very precise time synchronization in an Ethernet network. There are two clocks, master and slave. The master device periodically launches an exchange of messages with slave devices to help each slave clock re-compute the offset between its clock and the master's clock. To enable IEEE 1588, select **Enable** in the **PTP State** and choose **Auto, Master** or **Slave** Mode. After the time is synchronized, the system time displays the correct time from the PTP server.
Timezone Setting	Select the time zone where the ES7528 is located. The following table lists the time zones for different locations for your reference. The default time zone is (GMT) Greenwich Mean Time.
Daylight Saving Time	Click the **Daylight Saving Time** check box and then set the **Daylight Saving Time Start** and **End** times. During Daylight Saving Time, the ES7528 time is one hour earlier than the actual time.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

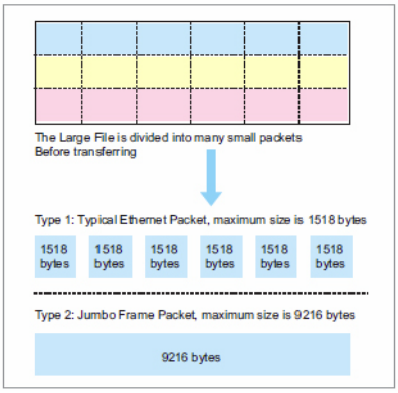
```
Switch(config)# clock timezone
  01  (GMT-12:00) Eniwetok, Kwajalein
  02  (GMT-11:00) Midway Island, Samoa
  03  (GMT-10:00) Hawaii
  04  (GMT-09:00) Alaska
  05  (GMT-08:00) Pacific Time (US & Canada), Tijuana
  06  (GMT-07:00) Arizona
  07  (GMT-07:00) Mountain Time (US & Canada)
  08  (GMT-06:00) Central America
  09  (GMT-06:00) Central Time (US & Canada)
  10  (GMT-06:00) Mexico City
  11  (GMT-06:00) Saskatchewan
  12  (GMT-05:00) Bogota, Lima, Quito
  13  (GMT-05:00) Eastern Time (US & Canada)
  14  (GMT-05:00) Indiana (East)
  15  (GMT-04:00) Atlantic Time (Canada)
  16  (GMT-04:00) Caracas, La Paz
  17  (GMT-04:00) Santiago
  18  (GMT-03:00) NewFoundland
  19  (GMT-03:00) Brasilia
  20  (GMT-03:00) Buenos Aires, Georgetown
  21  (GMT-03:00) Greenland
  22  (GMT-02:00) Mid-Atlantic
  23  (GMT-01:00) Azores
  24  (GMT-01:00) Cape Verde Is.
  25  (GMT) Casablanca, Monrovia
  26  (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
  27  (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
  28  (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
  29  (GMT+01:00) Brussels, Copenhagen, Madrid, Paris
  30  (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
  31  (GMT+01:00) West Central Africa
  32  (GMT+02:00) Athens, Istanbul, Minsk
  33  (GMT+02:00) Bucharest
  34  (GMT+02:00) Cairo
  35  (GMT+02:00) Harare, Pretoria
  36  (GMT+02:00) Helsinki, Riga, Tallinn
  37  (GMT+02:00) Jerusalem
  38  (GMT+03:00) Baghdad
  39  (GMT+03:00) Kuwait, Riyadh
  40  (GMT+03:00) Moscow, St. Petersburg, Volgograd
  41  (GMT+03:00) Nairobi
  42  (GMT+03:30) Tehran
  43  (GMT+04:00) Abu Dhabi, Muscat
  44  (GMT+04:00) Baku, Tbilisi, Yerevan
  45  (GMT+04:30) Kabul
  46  (GMT+05:00) Ekaterinburg
  47  (GMT+05:00) Islamabad, Karachi, Tashkent
  48  (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi
```

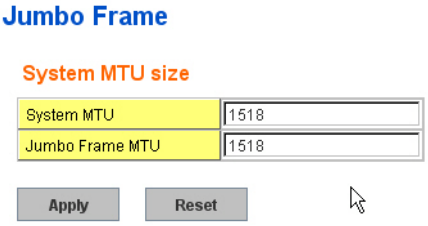
```
49  (GMT+05:45) Kathmandu
50  (GMT+06:00) Almaty, Novosibirsk
51  (GMT+06:00) Astana, Dhaka
52  (GMT+06:00) Sri Jayawardenepura
53  (GMT+06:30) Rangoon
54  (GMT+07:00) Bangkok, Hanoi, Jakarta
55  (GMT+07:00) Krasnoyarsk
56  (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
57  (GMT+08:00) Irkutsk, Ulaan Bataar
58  (GMT+08:00) Kuala Lumpur, Singapore
59  (GMT+08:00) Perth
60  (GMT+08:00) Taipei
61  (GMT+09:00) Osaka, Sapporo, Tokyo
62  (GMT+09:00) Seoul
63  (GMT+09:00) Yakutsk
64  (GMT+09:30) Adelaide
65  (GMT+09:30) Darwin
66  (GMT+10:00) Brisbane
67  (GMT+10:00) Canberra, Melbourne, Sydney
68  (GMT+10:00) Guam, Port Moresby
69  (GMT+10:00) Hobart
70  (GMT+10:00) Vladivostok
71  (GMT+11:00) Magadan, Solomon Is., New Caledonia
72  (GMT+12:00) Auckland, Wellington
73  (GMT+12:00) Fiji, Kamchatka, Marshall Is.
74  (GMT+13:00) Nuku'alofa
```

Jumbo Frame

The typical Ethernet frame range is from 64 to 1,518 bytes. This is sufficient for general usages. However, when users want to transmit large files, the files may be divided into many small size packets. When the transmission speed becomes slow, long size Jumbo frame may solve the issue.

The ES7528 allows you configure the size of the Maximum Transmission Unit (MTU). The default value is 1,518 bytes. You can increase the MTU size to support jumbo frames on all interfaces by setting the Jumbo Frame MTU. The maximum Jumbo Frame size is 9,216 bytes. You can freely change the available packet size.

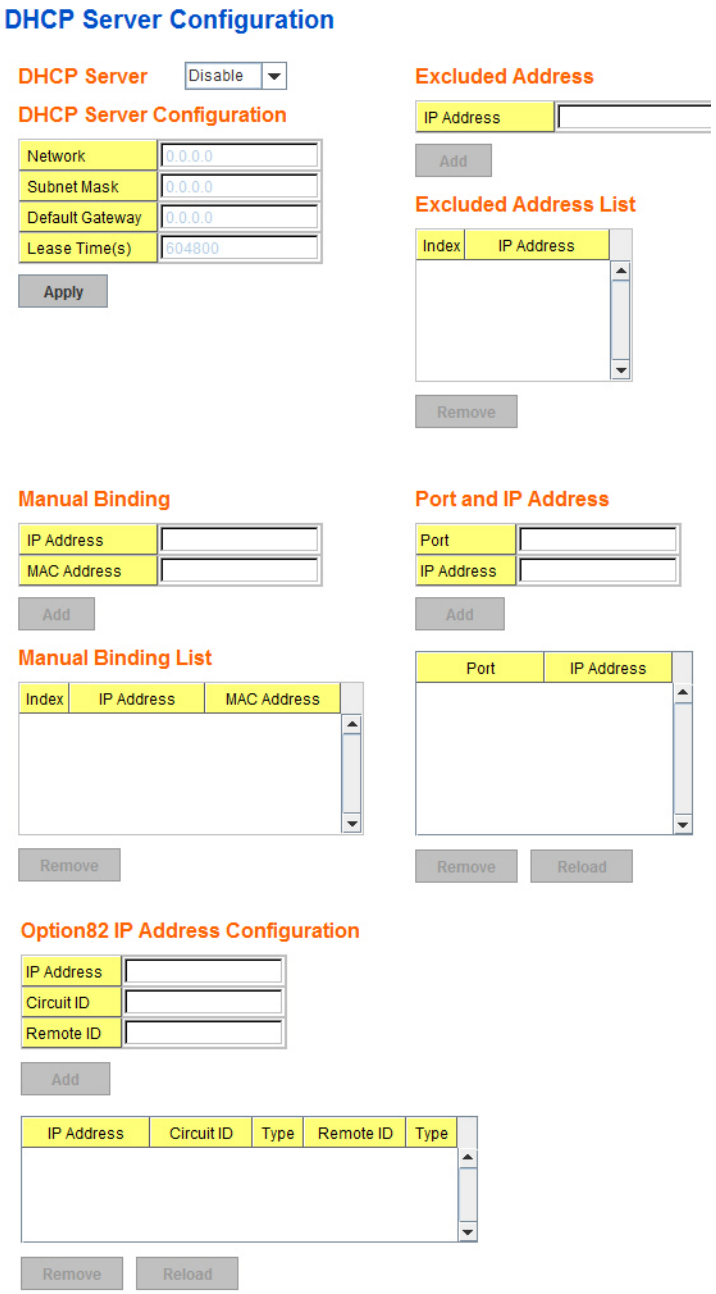




Jumbo Frame	Description
System MTU	Change the MTU size for all Fast Ethernet interfaces on the switch stack. The range is 1500 to 1546 bytes; the default is 1518 bytes.
Jumbo Frame MTU	Change the MTU size for all gigabit Ethernet interfaces on the switch stack. The range is 1500 to 9216 bytes; the default is 1518 bytes.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*
Reset	Click to reset the MTU to the default value.

DHCP Server Configuration

Use this page to configure DHCP server services.

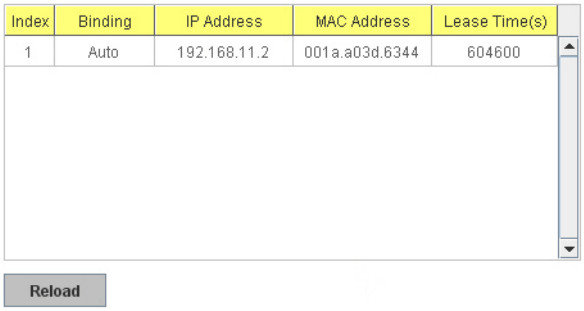


DHCP Server Configuration Page	
DHCP Server	You can select to **Enable** or **Disable** the DHCP Server function. The ES7528 assigns a new IP address to link partners.
DHCP Server Configuration	
Network	Enter the IPv4 address for the DHCP server.
Subnet Mask	Enter the subnet mask for the DHCP server.
Default Gateway	Enter the IP gateway address for the DHCP server.
Lease Time	Enter the Lease Time in seconds for the client.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*
Excluded Address	
IP Address	You can type a specific address into the **IP Address field** for the DHCP server reserved IP address. The IP address that is listed in the **Excluded Address List Table** is not assigned to the network device. Add or remove an IP address from the **Excluded Address List** by clicking **Add** or **Remove**.
Manual Binding	
IP Address	The ES7528 provides an IP address binding and removing function. Enter the specified IP address, and then click **Add** to add a new IP address binding rule for a specified link partner, like a PLC, or any device without **DHCP client** function. To remove an IP address from the Manual Binding List, highlight the rule and click **Remove**.
MAC Address	The ES7528 provides a MAC address binding and removing function. Enter the specified MAC address, and then click **Add** to add a new MAC address binding rule for a specified link partner, like a PLC, or any device without **DHCP client** function. The MAC address format is **xxxx.xxxx.xxxx**; for example, 00C0.4E32.0001. To remove a MAC address from the Manual Binding List, highlight the rule and click **Remove**.
Port and IP Address	
Port	Enter the client port number for the DHCP server.
IP Address	Enter the client IP address for the DHCP server. After entering the port number and IP address, click **Add**. To remove a port and associated IP address, click **Remove**. Click Reload to reload selected port and IP address entries.
Option82 IP Address Configuration	
IP Address	Option 82 IP Address Configuration: fully supports DHCP relay function. The IP address of the Option82 IP address configuration.
Circuit ID	The Circuit ID of the Option82 IP address configuration.

DHCP Server Configuration Page (Continued)	
Remote ID	The Remote ID of the Option82 IP address configuration. After entering the IP Address, Circuit ID, and Remote ID, click **Add**. Click the **Remove** button to remove selected Option82 IP Address table entries. Click the **Reload** button to reload selected Option82 IP Address table entries.
Type	This displays string or hex, depending on the type.

DHCP Leased Entries

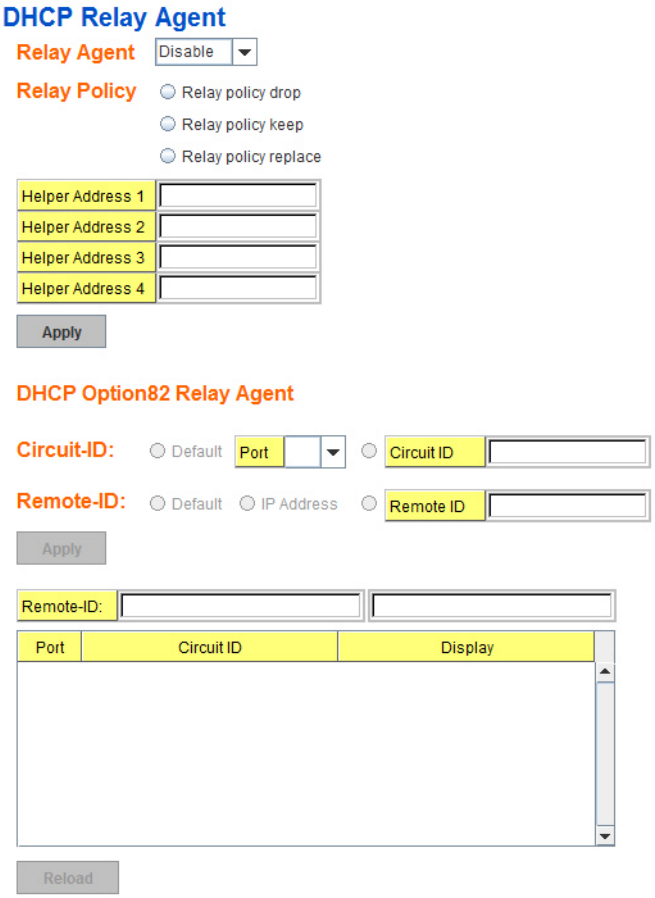
The ES7528 provides an assigned IP address.



DHCP Leased Entries Page	
Index	Index of DHCP leased entries.
Binding	Manual or auto binding IP addresses and MAC addresses.
IP Address	The IP address of the leased entry.
MAC Address	The MAC Address of the leased entry.
Lease Time(s)	The lease time of the leased entry (in seconds).
Reload	Click to reload DHCP leased entries.

DHCP Relay Agent

This subsection discusses the DHCP Relay Agent.



DHCP Server Configuration Page	
DHCP Server	You can select to **Enable** or **Disable** the DHCP Server function. The ES7528 assigns a new IP address to link partners.
DHCP Server Configuration	
Network	Enter the IPv4 address for the DHCP server.
Subnet Mask	Enter the subnet mask for the DHCP server.
Default Gateway	Enter the IP gateway address for the DHCP server.
Lease Time	Enter the Lease Time in seconds for the client.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*
Excluded Address	
IP Address	You can type a specific address into the **IP Address field** for the DHCP server reserved IP address. The IP address that is listed in the **Excluded Address List Table** is not assigned to the network device. Add or remove an IP address from the **Excluded Address List** by clicking **Add** or **Remove**.
Manual Binding	
IP Address	The ES7528 provides an IP address binding and removing function. Enter the specified IP address, and then click **Add** to add a new IP address binding rule for a specified link partner, like a PLC, or any device without **DHCP client** function. To remove an IP address from the Manual Binding List, highlight the rule and click **Remove**.
MAC Address	The ES7528 provides a MAC address binding and removing function. Enter the specified MAC address, and then click **Add** to add a new MAC address binding rule for a specified link partner, like a PLC, or any device without **DHCP client** function. The MAC address format is **xxxx.xxxx.xxxx**; for example, 00C0.4E32.0001. To remove a MAC address from the Manual Binding List, highlight the rule and click **Remove**.
Port and IP Address	
Port	Enter the client port number for the DHCP server.
IP Address	Enter the client IP address for the DHCP server. After entering the port number and IP address, click **Add**. To remove a port and associated IP address, click **Remove**. Click Reload to reload selected port and IP address entries.
Option82 IP Address Configuration	
IP Address	Option 82 IP Address Configuration: fully supports DHCP relay function. The IP address of the Option82 IP address configuration.
Circuit ID	The Circuit ID of the Option82 IP address configuration.

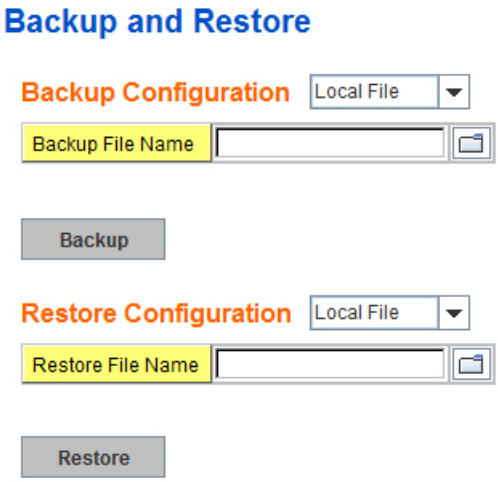
DHCP Server Configuration Page (Continued)	
Remote ID	The Remote ID of the Option82 IP address configuration. After entering the IP Address, Circuit ID, and Remote ID, click **Add**. Click the **Remove** button to remove selected Option82 IP Address table entries. Click the **Reload** button to reload selected Option82 IP Address table entries.
Type	This displays string or hex, depending on the type.

Backup and Restore

Use the **Backup** option to save the current configuration saved in the ES7528 flash to a PC/laptop or a TFTP server.

This allows you to use the **Restore** option to restore a configuration file back to the ES7528 or load the same settings to another ES7528. Before you can restore a configuration file, you must save the backup configuration file in the PC or TFTP server. The ES7528 then downloads this file back into the flash.

The ES7528configuration file is a standard text file. You can open the file with Word or Notepad. You can also modify the file, add/remove the configuration settings, and then restore the file back to the ES7528.



There are two modes to backup and restore the configuration file:

- Local File
  - *Backup the Configuration - Local File Method* on Page 52
  - *Restore the Configuration - Local Method* on Page 53
- *TFTP Server*
  - *Backup the Configuration - TFTP Server Method* on Page 54
  - *Restore the Configuration - TFTP Server Method* on Page 57

You can use the **Local File** method if you have a Windows XP system.

If you have Windows Server 2003 through Windows 7, you must use the **TFTP Server** method to backup or restore configuration files.

Backup & Restore Page	
Backup Configuration	• **Local File**: The ES7528 acts as the file server in Windows XP. Other Windows operating systems must use the TFTP method. This mode is only provided by the web user interface as the backup and restore functions are not supported by the CLI. For procedures, see *Backup the Configuration - Local File Method* on Page 52. • **TFTP Server**: The ES7528 acts as a TFTP client. This mode can be used in both the CLI and web user interface. For procedures, see *Backup the Configuration - TFTP Server Method* on Page 54. ***Note:*** *Pointing to the wrong file causes the entire configuration to be skipped.*
Backup	**Backup** can only backup the configuration file to your PC or a TFTP server.
Restore Configuration	You can select local file in Windows XP or TFTP server in all Windows operating systems to restore the startup configuration. For procedures, see *Restore the Configuration - Local Method* on Page 53 or *Restore the Configuration - TFTP Server Method* on Page 57.
Restore	Click to restore ES7528 startup configurations to the ES7528.

Backup & Restore Page (Continued)	
Backup Configuration	• **Local File**: The ES9528 acts as the file server in Windows XP. Other Windows operating systems must use the TFTP method. This mode is only provided by the web user interface as the backup and restore functions are not supported by the CLI. For procedures, see *Backup the Configuration - Local File Method*. • **TFTP Server**: The ES9528 acts as a TFTP client. This mode can be used in both the CLI and web user interface. For procedures, see *Backup the Configuration - TFTP Server Method*. ***Note:*** *Pointing to the wrong file causes the entire configuration to be skipped.*
• The ES7528 provides a default configuration file in the ES7528. To load the default configuration file, you can use the **Reset** on the *Factory Defaults* page on Page 60or the **Reload** command in the CLI (Page 152). • You can use the CLI to view the latest settings running in the ES7528. The information are the settings you have configured but have not yet saved to the flash. The settings must be saved to the flash in order to work after a power recycle. Use the **running-config** command to view the configuration file, see *Show Running Configuration* on Page 152. • After you save the **running-config** to flash, the new settings are kept and work after the power is cycled. Use the **show startup-config** to view it in the CLI. The **Backup** command can only backup the configuration file to your PC or TFTP server.	

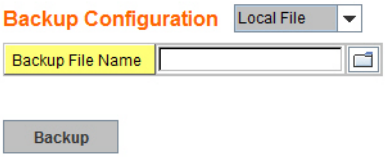
Backup the Configuration - Local File Method

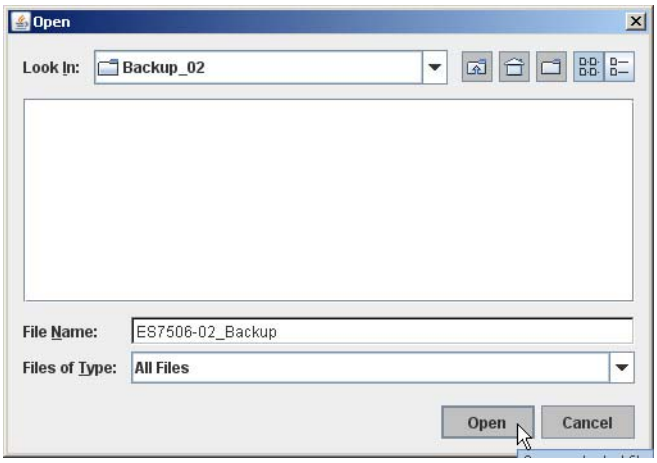
You can use **Local File** method to backup (or restore) with a Windows XP system.

Note: *If you have a Windows Server 2003 through Windows 7operating system, you must use the TFTP server method (Page 54).*

1. Open the web user interface for the ES7528 and open the **Backup and Restore** page under *Basic Settings*.
2. Select **Local File** for **Backup Configuration**.
3. Click the **Folder** icon, browse to the location that you want to store the backup configuration file, enter a file name, and click **Open**.

   Note: *You cannot use spaces in the path to the target file.*





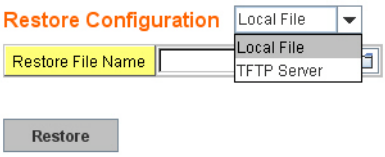
4. Click the **Backup** button and then click **Ok** when the *Success Message* appears. .

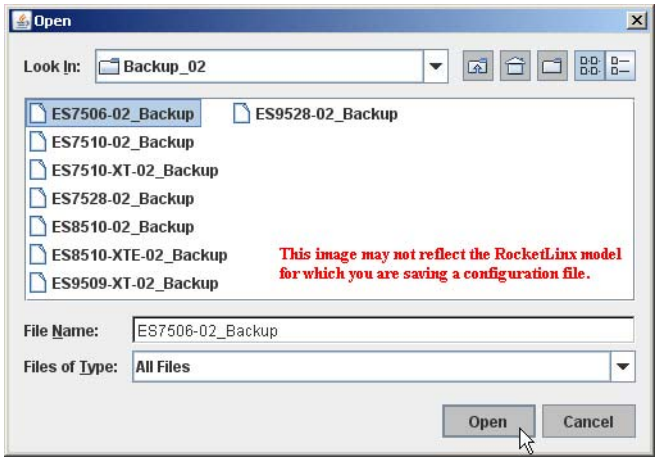
Restore the Configuration - Local Method

You can use **Local File** method to restore with a Windows XP system.

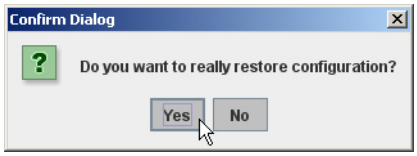
Note: *If you have a Windows Server 2003 through Windows 7operating system, you must use the TFTP server method (Page 57).*

1. Open the web user interface for the ES7528 and open the **Backup and Restore** page under *Basic Settings*.
2. Select **Local File** as the **Restore Configuration**.
3. Click the **Folder** icon, browse to the location where the backup configuration file is located., highlight the file, and click **Open**.

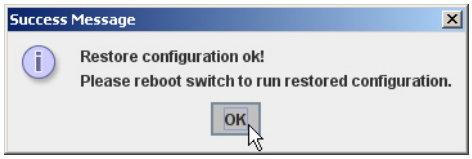




4. Click the **Restore** button.
5. Click **Yes** to the *Confirm Dialog*.



6. Click **Ok** to the *Success Message*.



Backup the Configuration - TFTP Server Method

You must use a TFTP server to create or load backup files if you are using the following operating systems:

- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

If you do not have a TFTP server, you can download one from Comtrol using the *Start the TFTP Server* subsection. You need to disable the Windows firewall, you can use the procedures in *Disable the Windows Firewall* on Page 55. After opening a TFTP server and disabling you can do the following:

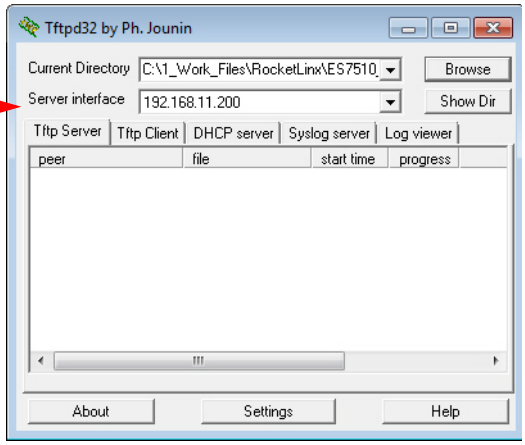
- *Backup the Configuration - TFTP Server Method* on Page 54
- *Restore the Configuration - TFTP Server Method* on Page 57

Start the TFTP Server

Use this procedure to download either the 32-bit or the 64-bit version from Comtrol.

1. If necessary, download the appropriate **.zip** file for your operating system from: ftp://ftp.comtrol.com/contribs/free_3rd_party_utils/tftp_server/ to your system and unzip the file.
2. Execute the TFTP server application, click **Allow access**, and the TFTP server opens.
3. Leave the TFTP server open and go to the next subsection to temporarily disable the firewall.

TFTP Server IP Address

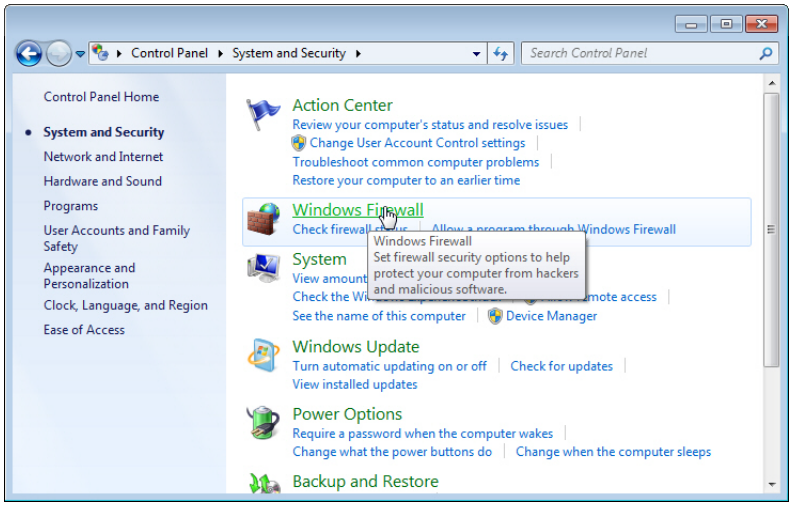


Disable the Windows Firewall

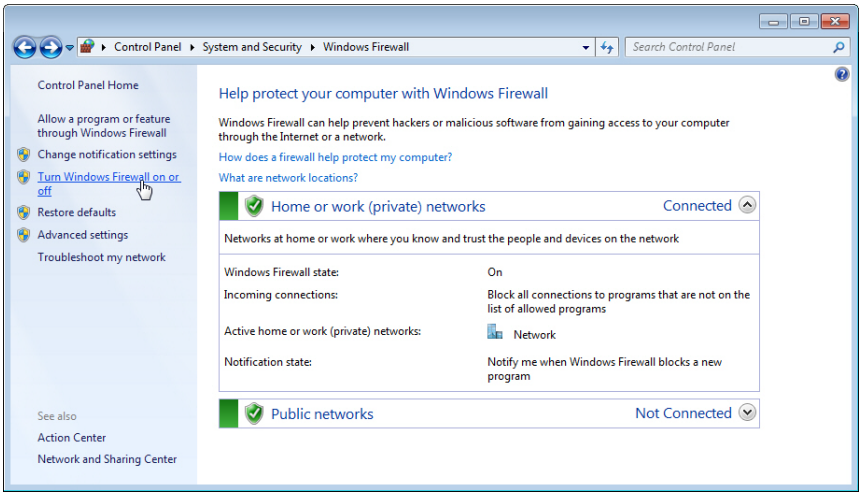
Use the following procedure to temporarily disable the system firewall.This example uses Windows 7.

1. From the **Start** button, click **Control Panel**, and click **System and Security**.

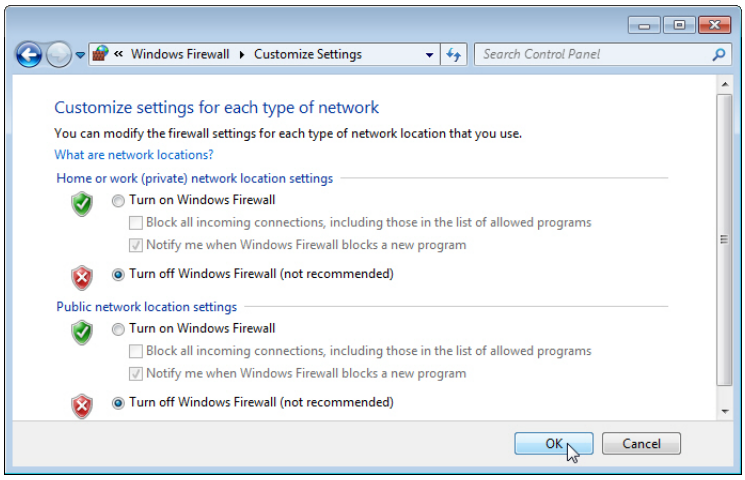
2. Click **Windows Firewall**.



3. Click **Turn Windows Firewall on or off**.



4. Click **Turn off Windows Firewall (not recommended)** for private and public networks and **Ok**.



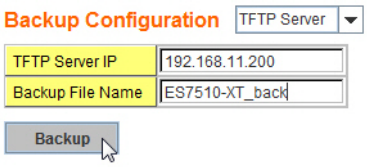
5. Minimize the **Control Panel** and go to the appropriate procedure, *Create a Backup File* on Page 56 or *Restore the Configuration - TFTP Server Method* on Page 57.

Create a Backup File

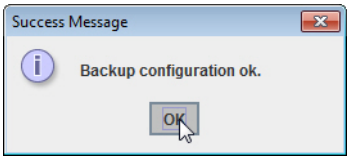
You must have a TFTP server open and disabled the Windows firewall for this following procedure to work.

1. Open the web user interface for the ES7528 and open the **Backup and Restore** page under *Basic Settings*.
2. Select **TFTP Server** for the **Backup Configuration**, enter the IP address of the TFTP server, enter a **Backup File Name**, and click the **Backup** button.

   Note: *You cannot use spaces in the path to the target file.*



3. Click **Ok** to close the popup message.



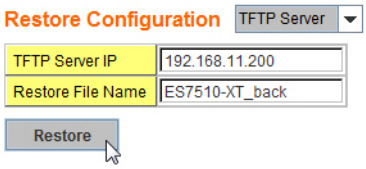
Note: *Make sure that you enable your Windows firewall when you have completed these tasks.*

The backup file is located in the same directory that the TFTP server resides.

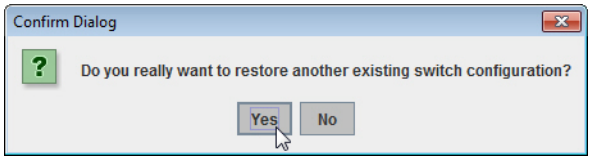
Restore the Configuration - TFTP Server Method

To restore a configuration file, you must open a TFTP server and disable the Windows firewall. If necessary, use *Start the TFTP Server* on Page 54 and *Disable the Windows Firewall* on Page 55.

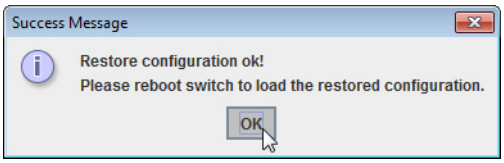
The backup file must be located in the same directory that the TFTP server resides for this procedure to work.



1. Open the web user interface for the ES7528, open the **Backup and Restore** page under *Basic Settings*.
2. Select **TFTP Server** for the **Restore Configuration**, enter the IP address of the TFTP server, enter the **Backup File Name**, and click the **Restore** button.
3. Click **Yes** to the *Confirm Dialog* message.



4. Click **Ok** to the *Success Message*.



Note: *Make sure that you enable your Windows firewall when you have completed these tasks.*

Firmware Upgrade

Use this section to update the ES7528 with the latest firmware. Comtrol provides the latest firmware on the Comtrol FTP site. The new firmware may include new features, bug fixes, or other software changes. Comtrol Technical Support suggests you use the latest firmware before installing the ES7528 at a customer site.

Note: *Optionally, you can use NetVision to upload the latest firmware. If you need to upload a new version of the Bootloader, you must use NetVision. You cannot use the web user interface or CLI to upload the Bootloader.*

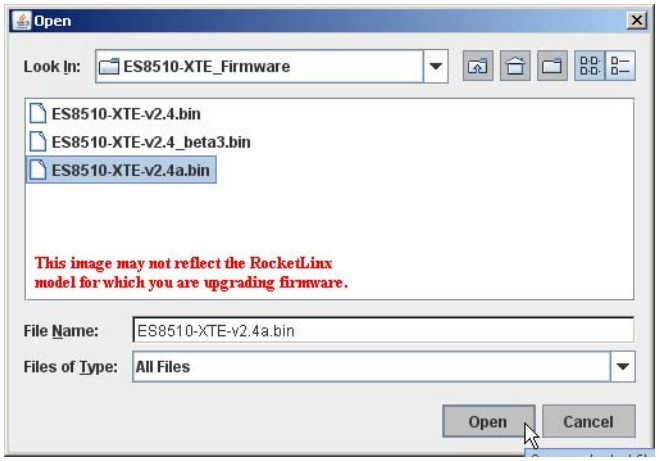
Firmware Upgrade Page	
System Firmware Version	The firmware version on the ES7528. You should check the version number after the switch reboots.
System Firmware Date	The build date of the firmware on the ES7528.
Firmware Upgrade	• **Local File (Windows XP) - see** *Upgrading Firmware (Local File)* on Page 58 • **TFTP Server** (Window Server 2003 - Windows 7) - see *Upgrading Firmware (TFTP Server)* on Page 59

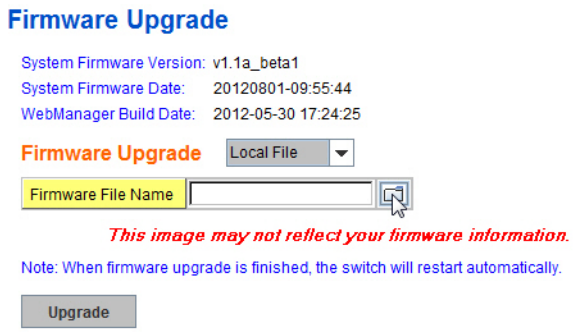
Note: *The system is automatically rebooted after you finish upgrading firmware. You should alert the attached users before updating the firmware that network interruption may occur.*

Upgrading Firmware (Local File)

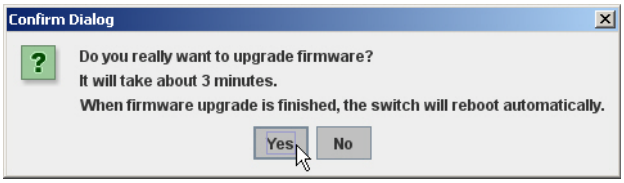
You can use this procedure to upgrade the firmware (not Bootloader) using Windows XP.

1. Open the web user interface for the ES7528, open the **Firmware Upgrade** page under *Basic Settings*.
2. Select **Local** in the **Firmware Upgrade** drop list.
3. Click the **folder** icon, browse to the firmware location, highlight the **.bin** file, and click **Open**.



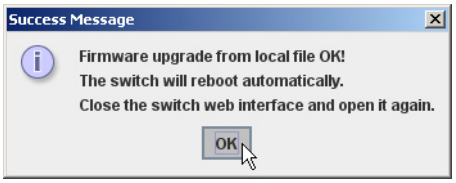


4. Click the **Upgrade** button.
5. Click **Yes** to the *Confirm Dialog* message.



6. Click **Ok** to the *Warning Message*.

7. Click **Ok** to close the *Success Message*.

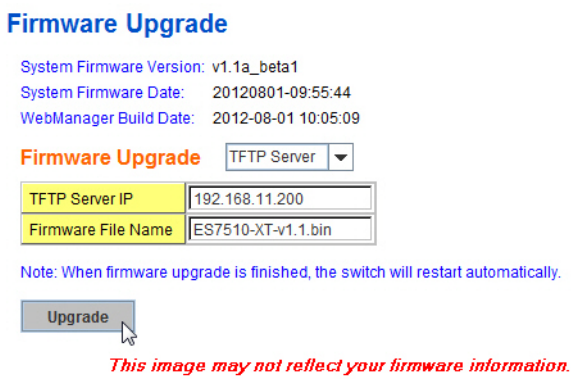


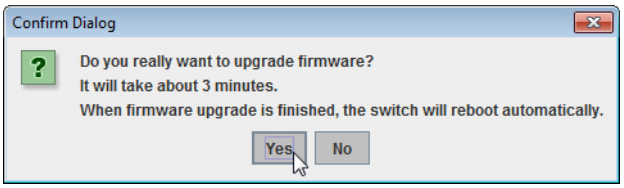
Note: *After the firmware has successfully uploaded, you should close and re-open the browser to clear the Java Virtual Machine cache.*

Upgrading Firmware (TFTP Server)

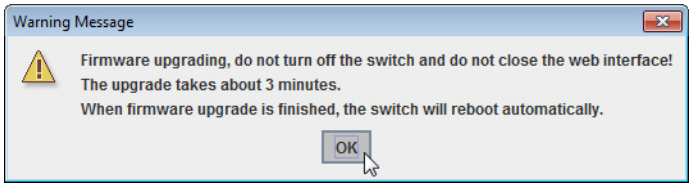
You can use this procedure to upgrade the firmware (not Bootloader) using Windows operating systems.

1. Open a TFTP server, if necessary, see *Start the TFTP Server* on Page 54.
2. Place the ES7528 **.bin** file in the same directory where the TFTP server resides.
3. Disable the Windows firewall, if necessary, see *Disable the Windows Firewall* on Page 55.
4. If necessary, open the web user interface, open the **Firmware Upgrade** page in the *Basic Settings* group.
5. Select **TFTP Server** in the **Firmware Upgrade** drop list.
6. Enter the IP address of the TFTP server, enter the firmware file name, and click the **Upgrade** button.
7. Click **Yes** to the *Confirm Dialog* message.



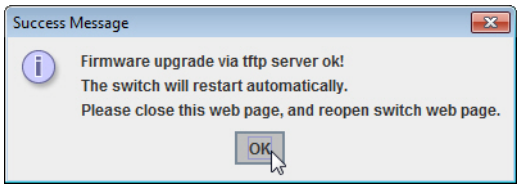


8. Click **Ok** to the *Warning Message*.



9. Click **Ok** to close the *Success Message*.
10. Enable the Windows firewall.

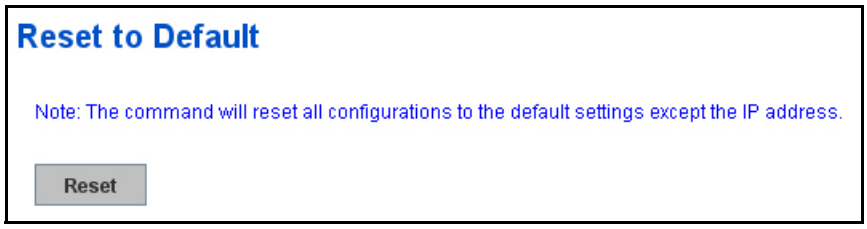
Note: *After the firmware has successfully uploaded, you should close and re-open the browser to clear the Java Virtual Machine cache.*



Factory Defaults

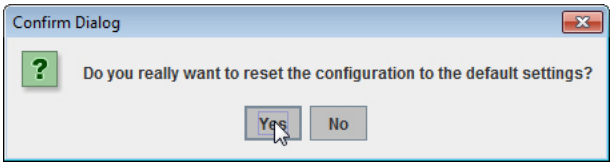
You can reset all the configurations of the switch to default settings.

Click **Reset**, if you want the ES7528 to reset all configurations to factory default settings.

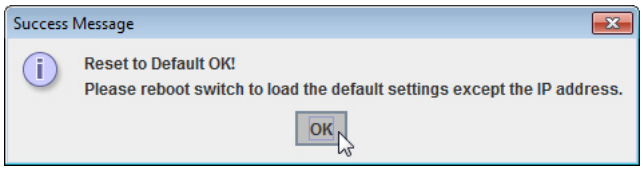


The system displays a popup message window after finishing. The default settings work after rebooting the ES7528.

Click **Yes** in the popup alert screen to reset the configuration to the factory defaults.



The following popup message screen shows you that the ES7528 has been reset to factory defaults. Click **OK** to close the screen and then go to the **Reboot** page to reboot the switch.



Click **OK.** The system automatically reboots the ES7528.

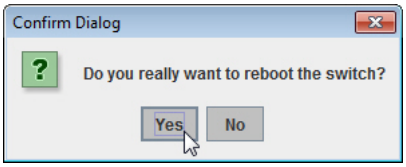
Note: *If you have already configured the IP of the ES7528 to another IP address, when you use this procedure, the software does not reset the IP address to the default IP address. The ES7528 IP address does not change so that you can still connect the switch through the network.*

System Reboot

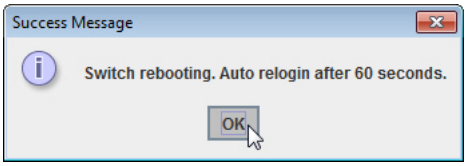
System Reboot allows you to reboot the device. Some of the feature changes require you to reboot the system. Click **Reboot** to reboot your ES7528.

Note: *Before rebooting, remember to click **Save** to save your settings. Otherwise, the settings you are lost when the ES7528 is powered off.*

Click **Yes**. The switch reboots immediately.



Click **Ok** so that the ES7528 reboots.



Port Configuration

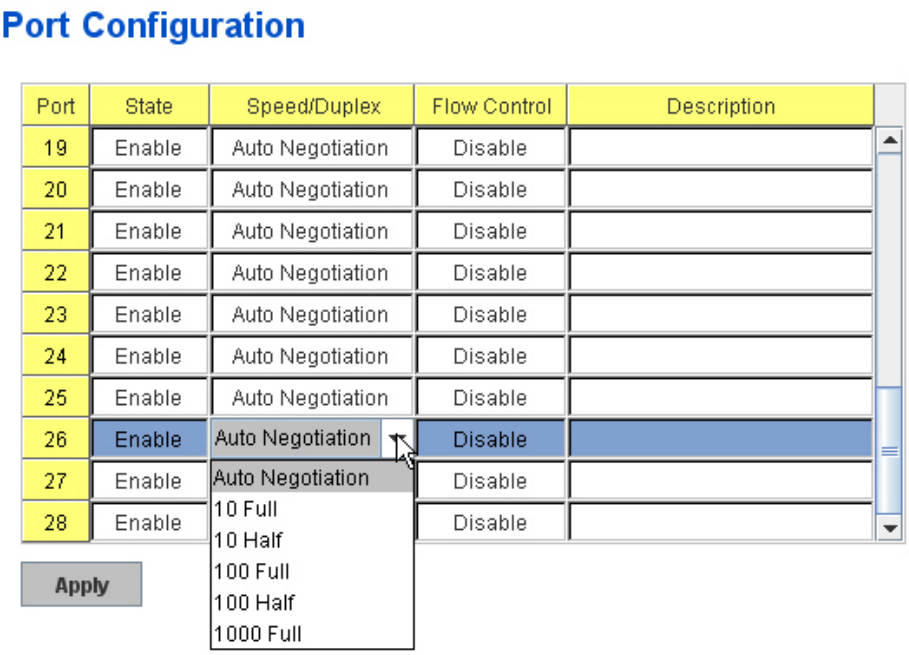
The *Port Configuration* group allows you to enable/disable port state, or configure port auto-negotiation, speed, duplex, flow control, port aggregation settings (port trunking), and rate limit control. It also allows you to view port status and aggregation information. The following pages are included in this group:

- *Port Control*
- *Port Status* on Page 63
- *Rate Control* on Page 65
- *Storm Control* on Page 66
- *Port Trunking* on Page 67

Optionally, you can use the CLI for configuration, see *Port Configuration (CLI)* on Page 154.

Port Control

Port Control page allows you to enable/disable port state, or configure the port auto-negotiation, speed, duplex, and flow control.



Select the port you want to configure and make changes to the port. The following table provides information about the different port control options.

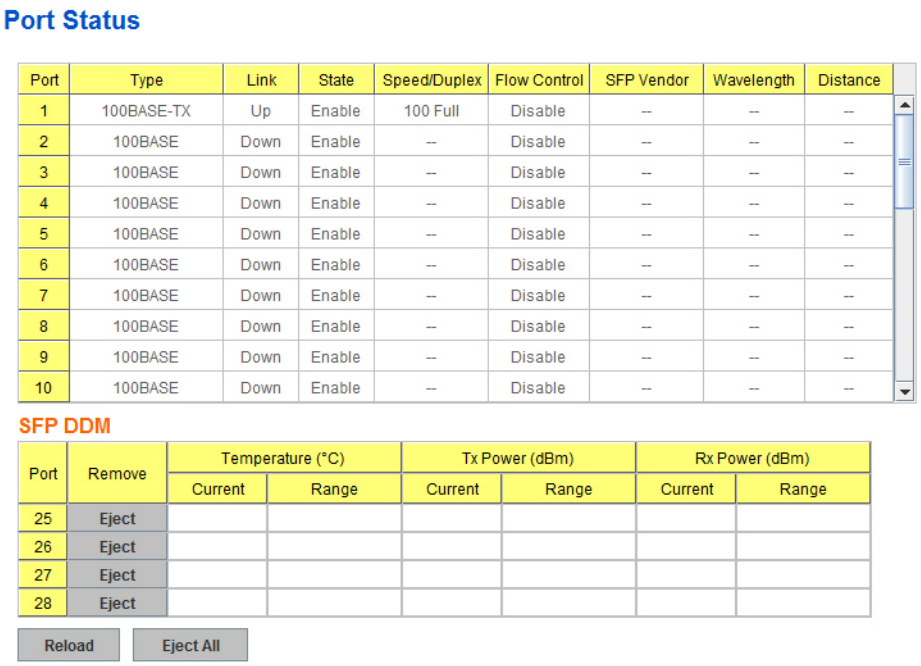
Port Configuration Page	
State	You can enable or disable the state of this port. Once you click **Disable**, the port stops to link to the other end and stops to forward any traffic. The default setting is **Enable** which means all the ports are workable when you receive the ES7528.
Speed/Duplex	You can configure port speed and duplex mode of each port. Below are the selections you can choose: • Fast Ethernet Ports 1~ 24 (fa1~fa24) - Auto Negotiation (default) - 10M full-duplex (10 Full) - 10M half-duplex (10 Half) - 100M full-duplex (100 Full) - 100M half-duplex (100 Half) • Gigabit Ethernet Port 25~28: (gi25~gi28) - Auto Negotiation (default) - 10M full-duplex (10 Full) - 10M half-duplex (10 Half) - 100M full-duplex (100 Full) - 100M half-duplex (100 Half) - 1000M full-duplex (1000 Full)
Flow Control	**Symmetric** means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch to work. **Disable** (default) means that you do not need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch works.
Description	Click this field if you want to enter a port description.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Technical Tip:

If both ends are not at the same speed, they cannot link with each other. If both ends are not in the same duplex mode, they are connected by half-duplex mode.

Port Status

The Port Status page displays the current port status, including Small Form Factory (SFP) fiber transceiver with Digital Diagnostic Monitoring (DDM) function that provides real time information of SFP transceiver and allows you to diagnostic the optical fiber signal received and launched.



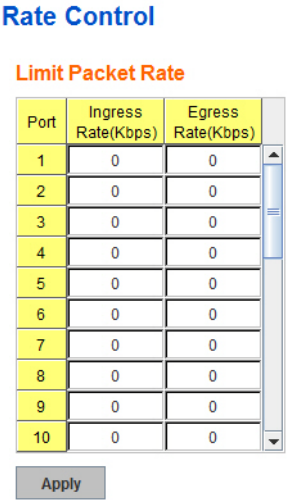
Port Status Page	
Type	100BASE-TX displays for Fast Ethernet copper ports 100BASE-FX displays for 100BASE-FX Fiber ports 1000BASE-TX displays for Gigabit Ethernet Copper ports 1000BASE-X displays for Gigabit Fiber Ports
Link	Shows link status; Up means the link is up and Down means that the link is down.
State	Shows the port state. If the state is enabled it displays **Enable**. If the port is disabled or shutdown, it displays **Disable**.
Speed/Duplex	Current working status of the port.
Flow Control	The state of the flow control.
SFP Vendor	Vendor name of the SFP transceiver that is plugged into the SFP port or ports.
Wavelength	The wave length of the SFP transceiver that is plugged into the SFP port or ports.
Distance	The distance of the SFP transceiver that is plugged into the SFP port or ports.
Temperature	Displays the current temperature detected and acceptable temperature range for the DDM SFP transceiver.
Tx Power (dBm)	Displays the current transmit power detected and acceptable Tx power range for the DDM SFP transceiver.
Rx Power (dBm)	Displays the current received power and acceptable Rx power range for the DDM SFP transceiver.
Scan All	Click the **Scan All** button to scan for all SFPs.
Eject All	You can eject one or all of the DDM SFP transceivers. To eject all of the SFPs, click **Eject All**.

Note: *Most of the SFP transceivers provide vendor information which allows the ES7528 to read it. The user interface can display vendor name, wave length, and distance of all Comtrol SFP transceiver models. If you see Unknown info, it may mean that the vendor does not provide their information or that the information of their transceiver cannot be read.*

If the plugged DDM SFP transceiver is not certified by Comtrol, the DDM function is not supported, but the communication is not disabled.

Rate Control

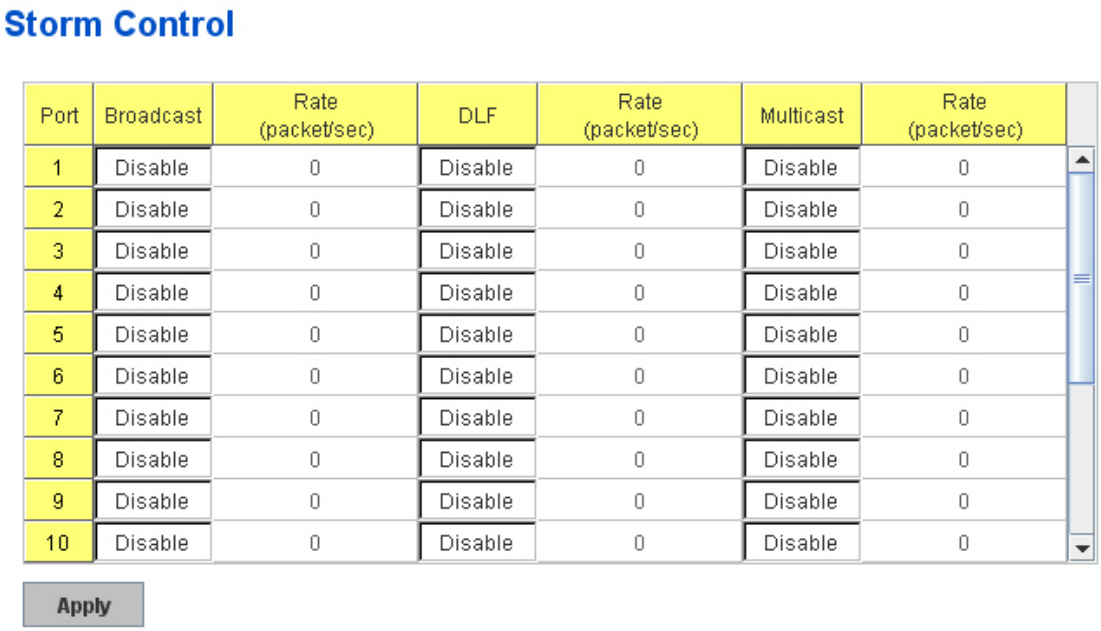
Rate limiting is a form of flow control used to enforce a strict bandwidth limit at a port. You can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types as described below. You can increment the volume step by 64Kbps in the blank.



Rate Control Page	
Bandwidth	The ports support port Ingress and Egress rate control. For example, assume that Port 1 is 10000 Kbps, you can set it's effective Egress rate at 2000 Kbps, Ingress rate is 1000 Kbps. The ES7528 performs the Ingress rate by packet counter to meet the specified rate. • Ingress Ingress rate in Kbps, the rate range is from 1000 Kbps to 1000000 Kbps and zero means no limit. The default value is no-limit. • Egress Egress rate in Kbps, the rate range is from 1000 Kbps to 1000000 Kbps and zero means no limit. The default value is no-limit. Egress rate limiting has an effect on all types of packet types, including Unknown Unicast, Multicast, and Broadcast.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Storm Control

The Storm Control is similar to Rate Control. Rate Control filters all the traffic over the threshold you input by the user interface. Storm Control allows you to define the rate for specific Packet Types.



Storm Control Page	
Broadcast	To enable or disable broadcast storm control on the corresponding port.
DLF	To enable or disable destination lookup failure storm control on this port.
Multicast	To enable or disable multicast storm control on this port.
Rate	Broadcast rate limit range from 0 to 262143 packet/sec (fast Ethernet maximum is 148810 packet/sec).
Rate (packet/ sec)	These columns allow you to manually assign the limit rate of the port. The unit is packets per second. The limit range is from 1 to 262143 packet/sec, zero means no limit. The maximum available value of Fast Ethernet interface is 148810, this is the maximum packet number of the 100M throughput.
Apply	Click **Apply** to apply the settings. It may take some time and the web user interface may become slow, this is normal condition. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Port Trunking

Port Trunking allows you to group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as a physical port that has a bandwidth equal to the combined bandwidth of each trunked port.The member ports of the same trunk group can balance the loading and backup for each other. The Port Trunking feature is usually used when you need higher bandwidth for the network backbone. This is an inexpensive way for you to transfer more data.

The aggregated ports can interconnect to the another switch that also supports Port Trunking. Comtrol supports two types of port trunking:

- Static Trunk
- IEEE 802.3ad

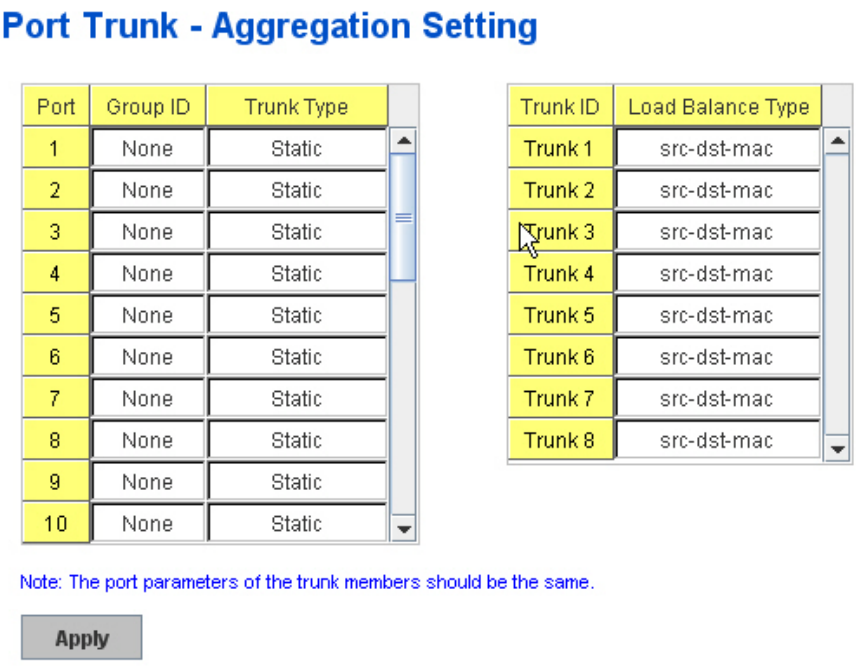
There are some different descriptions for the port trunking. Different manufacturers may use different descriptions for their products, like Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, or Ether Channel.

When the other end uses IEEE 802.3ad LACP, you should assign IEEE 802.3ad LACP to the trunk. When the other end uses non-802.3ad, you can then use Static Trunk.

There are two pages for port trunking, *Aggregation Setting* on Page 67 and *Aggregation Status* on Page 69.

Aggregation Setting

Use the *Port Trunk - Aggregation Setting* page to set up port trunking.

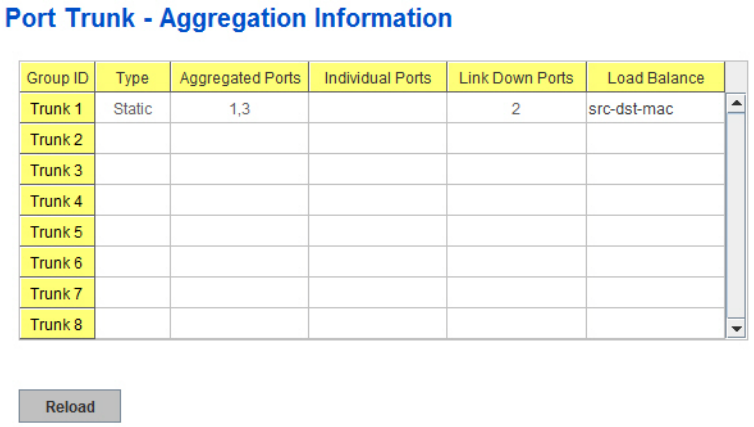


Aggregation Setting Page	
Trunk Size	The ES7528 can support up to 8 trunk groups. Each trunk group can aggregate up to 8 members. The ports should use the same speed and duplex. The maximum trunk size is decided by port volume.
Group ID	**Group ID** is the ID for the port trunking group. Ports with same group ID are in the same group.
Trunk Type	**Static** or **802.3ad LACP**. Each trunk group can only support **Static** or **802.3ad LACP**. Non-active ports cannot be setup here.

Aggregation Setting Page (Continued)	
Load Balance Type	There are several load balance types based on dst-ip (Destination IP), dst-mac (Destination MAC), src-dst-ip (Source and Destination IP), src-dst-mac (Source and Destination MAC), src-ip (Source IP), src-mac (Source MAC).
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Aggregation Status

The *Port Trunk - Aggregation Information* page shows the status of port aggregation. Once the aggregation ports are negotiated, you see the following status.



Aggregation Status Page	
Group ID	Displays Trunk 1 to Trunk 8 set up.
Type	The Type is **Static** or **LACP**. Static means that LACP is disabled and configured statically by the Administrator.
Aggregated Ports	When LACP links, you can see the member ports in the **Aggregated** column.
Individual Ports	When **LACP** is enabled, member ports of LACP group that are not connected to the correct LACP member ports are displayed in the **Individual** column.
Link Down Ports	When **LACP** is enabled, member ports of LACP group that are not linked up are displayed in the **Link Down** column.
Load Balance	There are several load balance types based on dst-ip (Destination IP), dst-mac (Destination MAC), src-dst-ip (Source and Destination IP), src-dst-mac (Source and Destination MAC), src-ip (Source IP), src-mac (Source MAC).
Reload	Click **Reload** to reload aggregation settings.

Power over Ethernet

Power over Ethernet is one of the key features of the ES7528. The ES7528 is IEEE 802.3af and IEEE 802.3at compliant. The ES7528 supports up to 24 PoE injectors ports, each port with the ability to deliver 606 mA current.

The following pages are included in this section:

PoE Control

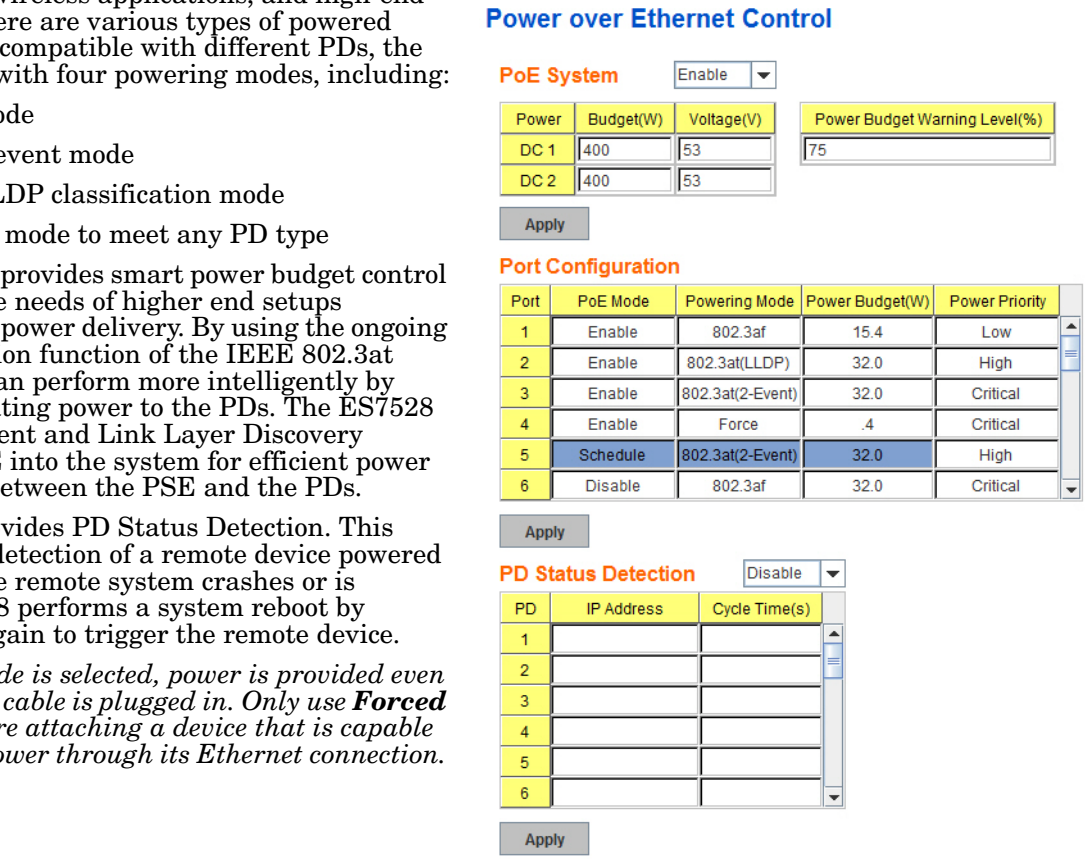
In WiMax systems, wireless applications, and high-end PoE applications, there are various types of powered devices (PDs). To be compatible with different PDs, the ES7528 is designed with four powering modes, including:

- IEEE 802.3af mode
- IEEE 802.3at 2-event mode
- IEEE 802.3at LLDP classification mode
- Forced powering mode to meet any PD type

IEEE 802.3at LLDP provides smart power budget control behavior to fulfill the needs of higher end setups requiring exact high power delivery. By using the ongoing dynamic re-negotiation function of the IEEE 802.3at LLDP, the ES7528 can perform more intelligently by dynamically reallocating power to the PDs. The ES7528 implements the 2 event and Link Layer Discovery Protocol (LLDP) PoE into the system for efficient power budget negotiation between the PSE and the PDs.

The ES7528 also provides PD Status Detection. This provides automatic detection of a remote device powered by the ES7528. If the remote system crashes or is unstable, the ES7528 performs a system reboot by turning off and on again to trigger the remote device.

Note: *If **Forced** mode is selected, power is provided even if no Ethernet cable is plugged in. Only use **Forced** mode if you are attaching a device that is capable of receiving power through its Ethernet connection.*



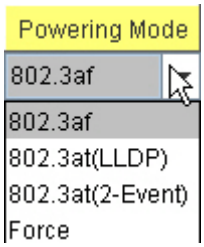
DO NOT TOUCH THE DEVICE SURFACE DURING PoE OPERATION - HIGH POWER FEEDING.

You can use these steps to configure PoE settings. Refer to the following table if you need more detailed information.

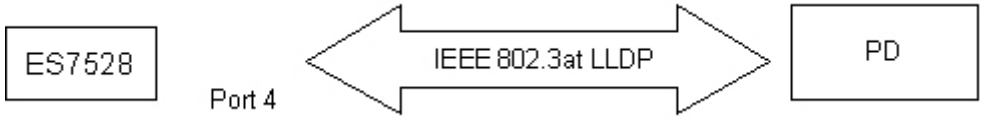
1. Select **Enable** in the **PoE System** drop list.
2. Enter appropriate values for the **DC1** and/or **DC2** power budgets.
3. Optionally, set a **Power Budget Warning Level** so that the ES7528 sends a warning event. See *SysLog Configuration* on Page 121 or *SMTP Configuration* on Page 122 for more information.
4. Click **Apply**.

5. Select **Enable** for the port or ports that you want to use as PoE ports.
6. Select the appropriate **PoE Mode** (**Enable**, **Disable**, or **Schedule**) for the corresponding port.

   Note: *If you select* ***Schedule****, you must also configure the port or ports using PoE Scheduling on Page 72.*
7. Select the appropriate **Powering Mode** (**802.3af**, **802.3at(LLDP)**, **802.3at(2 event)**, or **Force** for the PD that you plan on attaching to the corresponding port.
8. Enter a valid **Power Budget** based on the attached power supply.
9. Select an appropriate **Power Priority** (**Critical**, **High**, or **Low**).
10. Click **Apply**.
11. If desired, set up **PD Status Detection**.
12. You must **Save** the settings (Page 131), if you want maintain these settings if the ES7528 is powered off.

PoE Control	Description
PoE System	You can **Enable/Disable** ports, or set it to scheduling control mode.
DC1/DC2 Power Budget (W)	The output power range is 1-480W.
Port Configuration	
PoE Mode	You can select **Disable**, **Enable**, or **Schedule** for PoE mode for each port. Select **Schedule** to enable the port in the *PoE Schedule* page (Page 72).
Powering Mode	Use this mode to change the **Powering Mode** to one of the following: • **802.3af** If the PD follows IEEE 802.3af, then the ES7528 delivers power. • **802.3at(LLDP)** Delivers power to a PD that supports IEEE 802.3at LLDP. • **802.3at(2-Event)** Delivers power to a PD that supports 2-Event. • **Force** If Force is enabled, the port directly delivers the power even if there is no Ethernet cable connected.  ***Note:*** *Use caution when using* ***Force*** *mode. Do not connect a standard Ethernet device if using* ***Force*** *mode, it will damage the device.*
Power Priority	Power Priority lets the PoE port with higher priority to deploy power under the limit power budget. There are three priorities (**Critical**, **High** and **Low**).
PD Status Detection	
PD Status Detection	**Enable/Disable** the PD Status Detection function.
IP Address	Type in the IP address that you want to detect.
Cycle Time(s)	This is the gap per detection in seconds.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must* ***Save*** *the settings (Page 131), if you want maintain these settings if the ES7528 is powered off.*

The following illustrates how to configure IEEE 802.3at LLDP. Assume the PD is ready for the configuration for IEEE 802.3at LLDP, you only need to confirm the ES7528 configuration.



For example, connect the port of the ES7528 to the PD (Port 4), set **PoE Mode** is **Enable** and **Powering Mode** is **802.3at(LLDP)**. When the ES7528 and the PD are ready to IEEE 802.3at LLDP, IEEE 802.3at

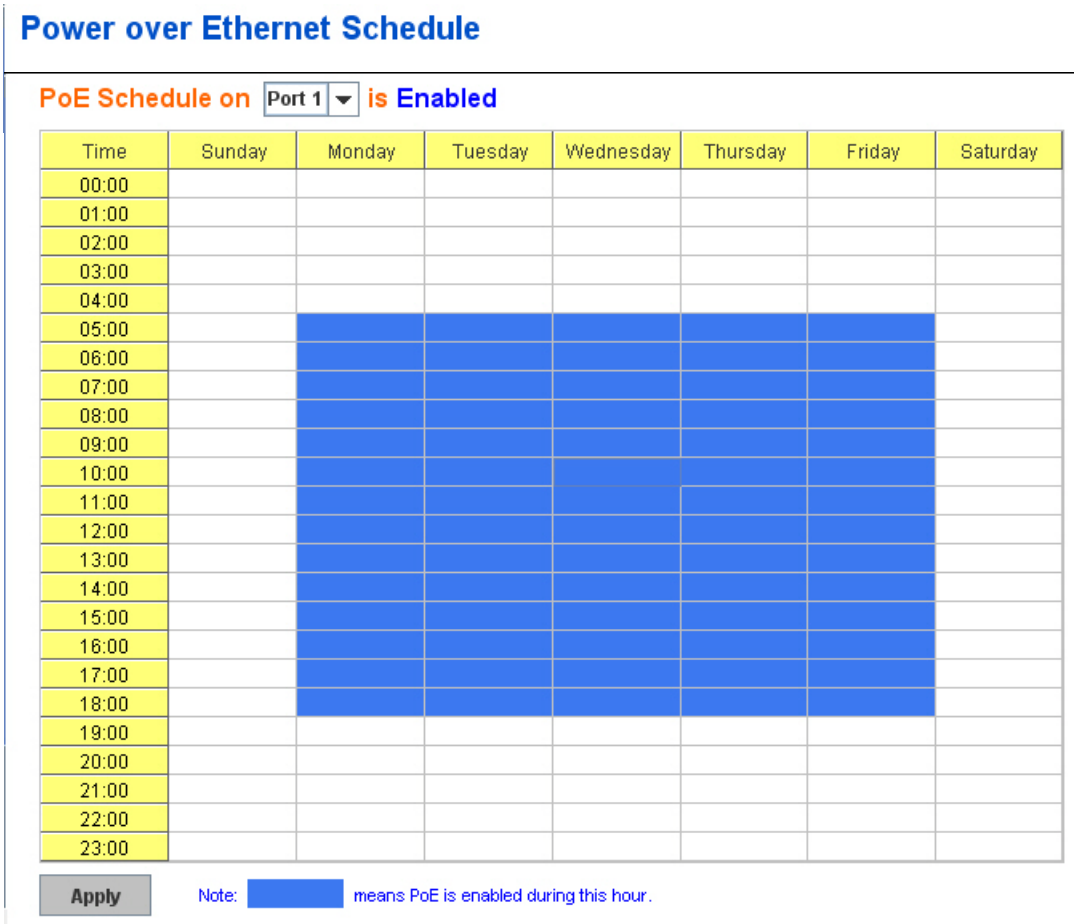
LLDP starts operation. Refer to *PoE Status* on Page 73, to see the **PoE Status** page.

PoE Scheduling

The PoE Scheduling control is a powerful function to help you save power and money.

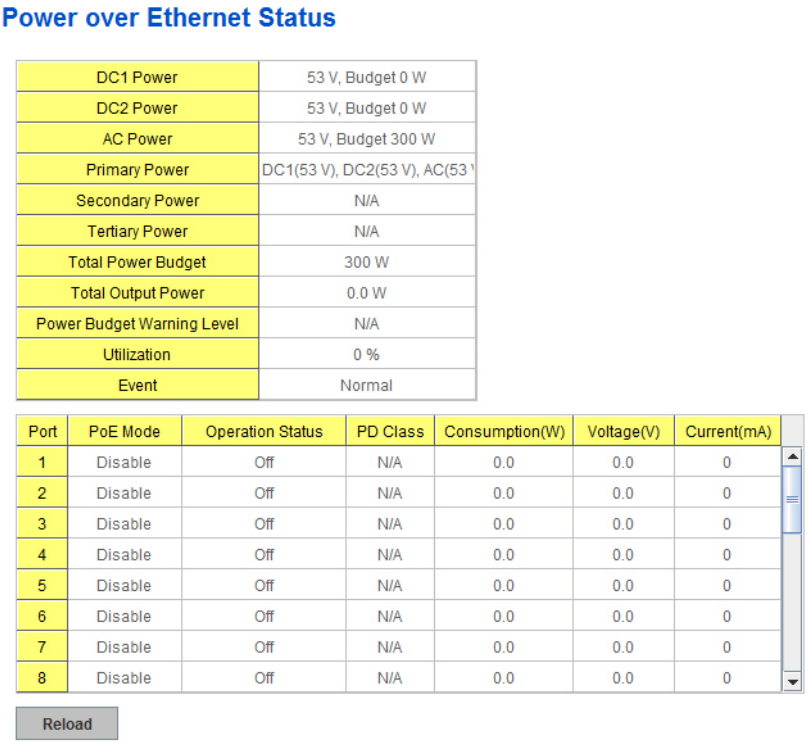
You can schedule a PoE port after the **PoE Mode** has been set to **Schedule** in the *PoE Control* page.

Select the port in the **PoE Schedule** on drop list. Click time blocks that you want to enable the PoE port and click.**Apply**.



PoE Status

The *PoE Status* page shows the operating status of each PoE port. You can use the *PoE Control* page (Page 70) if you need to make any changes.



Network Redundancy

It is critical for industrial applications that the network remains running at all times. The ES7528 supports:

- Standard Rapid Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP)

  The ES7528 supports RSTP versions IEEE 802.1D-2004, IEEE 802.1D-1998 STP, and IEEE 802.1w RSTP.

- Multiple Spanning Tree Protocol (MSTP)

  MSTP implements IEEE 802.1s, which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs. MSTP was originally defined in the IEEE 802.1s and later merged into the IEEE 802.1Q-2003 specification.

- Redundant Ring

  The Redundant Ring features 0 ms for restore and less than 5 ms for fail over for copper.

- Rapid Dual Homing (RDH)

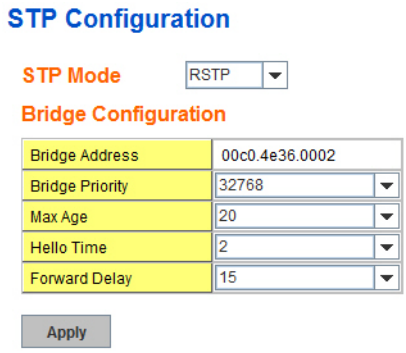
  Advanced RDH technology allows the ES7528 to connect with a core managed switch easily. With RDH technology, you can also couple several Rapid Super Rings or RSTP groups together, which is also known as Auto Ring Coupling.

The following pages are included in this group:

- *STP Configuration* on Page 75
- *STP Port Configuration* on Page 76
- *STP Information* on Page 77
- *MSTP Configuration* on Page 79
- *MSTP Port Configuration* on Page 81
- *MSTP Information* on Page 82
- *Redundant Ring* on Page 84
- *Redundant Ring Information* on Page 85

Optionally, you can use the CLI to configure these features, see *Network Redundancy (CLI)* on Page 166.

STP Configuration



This page allows you to select the STP mode and configure the global STP/RSTP bridge configuration. Spanning Tree Protocol (STP; IEEE 802.1D) provides a loop-free topology for any LAN or bridged network.

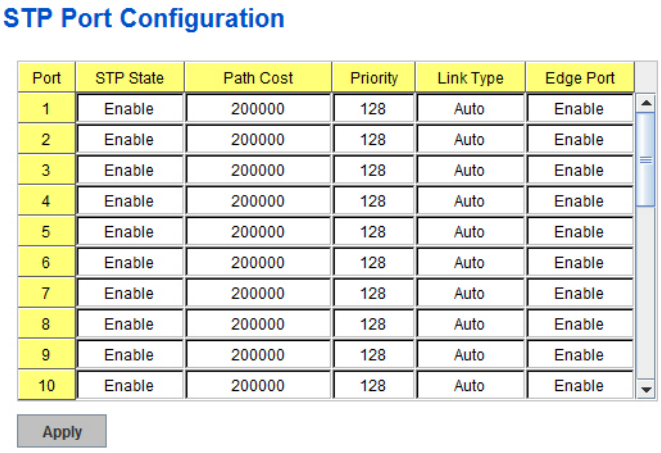
Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) is an evolution of the Spanning Tree Protocol (STP), and was introduced with the IEEE 802.1w standard, and provides faster spanning tree convergence after a topology change. In most cases, IEEE 802.1w can also revert back to IEEE 802.1D in order to interoperate with legacy bridges on a per-port basis. The new edition of the IEEE 802.1D standard, IEEE 802.1D-2004, incorporates the IEEE 802.1t-2001 and IEEE 802.1w standards.

Multiple Spanning Tree Protocol (MSTP; IEEE 802.1s) which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides a loop-free topology with load balancing while reducing the number of spanning-tree instances required to support a large number of VLANs. MSTP was originally defined in the IEEE 802.1s and later merged into the IEEE 802.1Q-2003 specification.

STP Configuration Page	
STP Mode	Select STP running protocol STP, RSTP or MSTP or disable STP.
Bridge Configuration	
Bridge Address	A value used to identify the bridge. This item cannot be modified.
Bridge Priority	A value used to identify the bridge. The bridge with the lowest value has the highest priority and is selected as the root. Enter a number 0 through 61440 in increments of 4096.
Max Age	The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting to reconfigure. Enter a number of 6 through 40. ***Note:*** *2*(Forward Delay Time-1) should be greater than or equal to the Max Age. The Max Age should be greater than or equal to 2*(Hello Time + 1).*
Hello Time	The number of seconds between the transmissions of Spanning-Tree Protocol configuration messages. Enter a number of 1 through 10. ***Note:*** *2*(Forward Delay Time-1) should be greater than or equal to the Max Age. The Max Age should be greater than or equal to 2*(Hello Time + 1).*
Forward Delay	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 through 30. ***Note:*** *2*(Forward Delay Time-1) should be greater than or equal to the Max Age. The Max Age should be greater than or equal to 2*(Hello Time + 1).*
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

STP Port Configuration

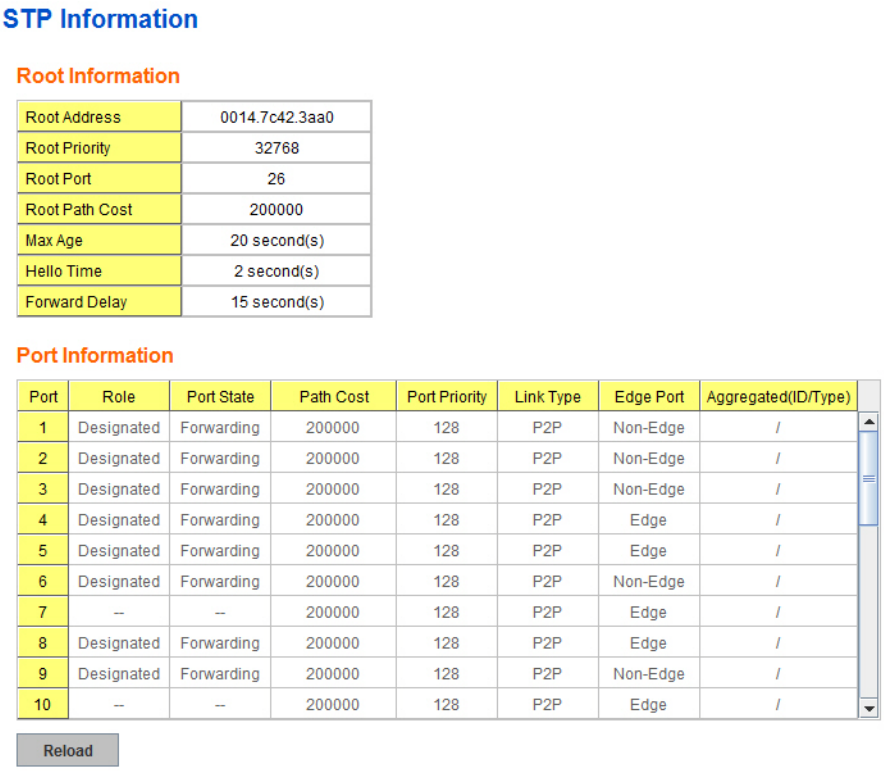
This page allows you to configure the port parameter after you have enabled STP, RSTP, or MSTP.



STP Port Configuration Page	
STP State	You can enable/disable STP/RSTP/MSTP on a port by port basis. You can disable the STP state when connecting a device in order to avoid STP waiting periods.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number from 1 through 200000000.
Priority	Decide which port should be blocked by priority on your LAN. Enter a number from 0 through 240 in increments of 16.
Link Type	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port in question is connected to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or if it is connected to two or more bridges (that is., it is served by a shared medium LAN segment). This configuration allows the p2p status of the link to be controlled by an administrator.
Edge Port	Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, and skipping the listening and learning stages. When a non-bridge device connects an edge port, this port is in a blocking state and turn to forwarding state in 2*Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

STP Information

The *STP Information* page allows you to see the ES7528 root information and port status.



STP Information Page	
Root Information	
Root Address	Root bridge address, which is the bridge with the smallest (lowest) bridge ID.
Root Priority	Root bridge priority, the bridge with the lowest value has the highest priority and is selected as the root.
Root Port	Root port of this bridge.
Root Path Cost	Root path cost.
Max Age	The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting to reconfigure.
Hello Time	The number of seconds between the transmissions of Spanning-Tree Protocol configuration messages.
Forward Delay	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state.

STP Information Page (Continued)	
Port Information	
Port Role	Descriptive information about the STP/RSTP switch port role. Role: Root, Designated, Alternate, Backup, Disabled, Unknown.
Port State	Descriptive information about the STP/RSTP switch port state. State: Blocking, Listening, Learning, Forwarding, Disabled, Unknown.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Path cost range is 1 through 200000000.
Port Priority	Decide which port should be blocked by priority in your LAN. Range is 0 through 240 in increments of 16.
Link Type	Operational link type. Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port in question can be concerned to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or can be connected to two or more bridges (that is, it is served by a shared medium LAN segment).
Edge Port	Operational edge port state. Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages. When the non-bridge device connects an edge port, this port is in blocking state and turn to forwarding state in 2*Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Reload	Click the **Reload** button to reload STP information.

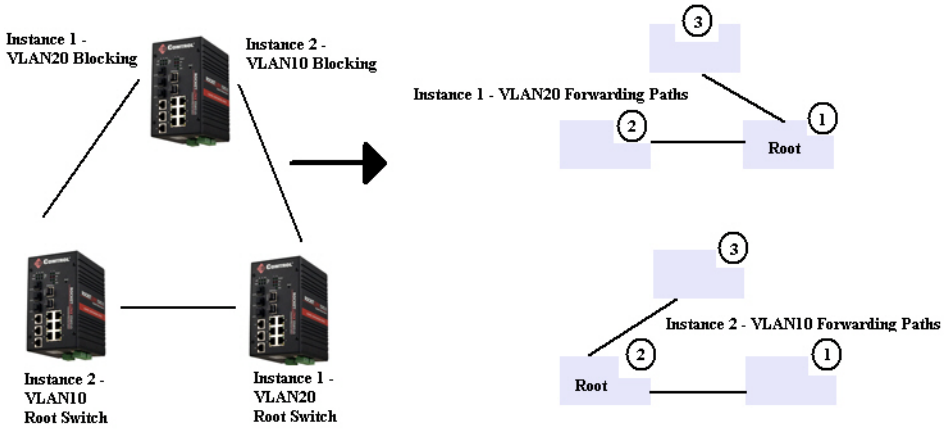
MSTP Configuration

Multiple Spanning Tree Protocol (MSTP) is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, creates a faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

While using MSTP, there are some new concepts of network architecture. A switch may belong to different groups, act as root or designate switch, or generate BPDU packets for the network to maintain the forwarding table of the spanning tree. MSTP can also provide load balancing between switches.

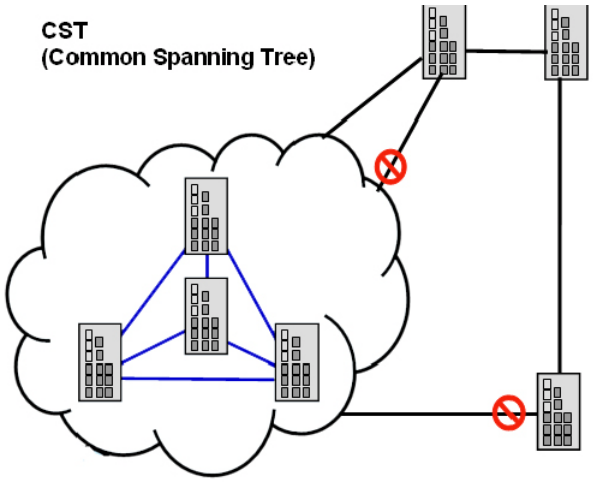
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). The maximum number of instances that the ES7528 supports is 16, with a range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP instances.

The following figure shows a MSTP instance with two VLANs. Each instance has a root node and forwarding paths.

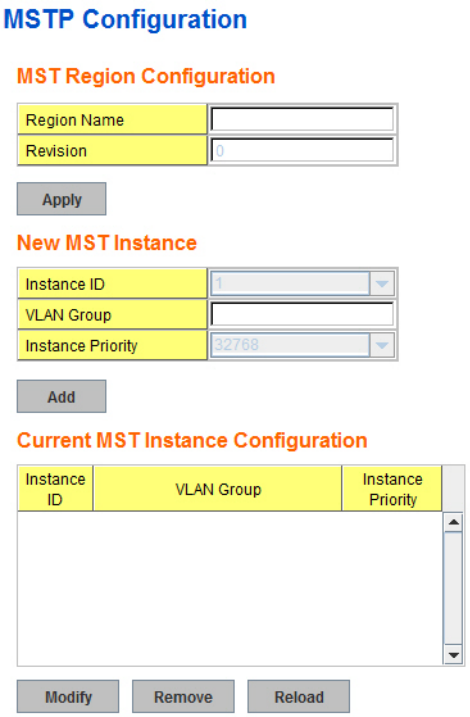


A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, or MSTP protocols.

The following diagram shows a CST attached to a larger network. In this network, a Region may have different instances and its own forwarding path and table, however, the CST acts as a single bridge.



This is the *MSTP Configuration* page.

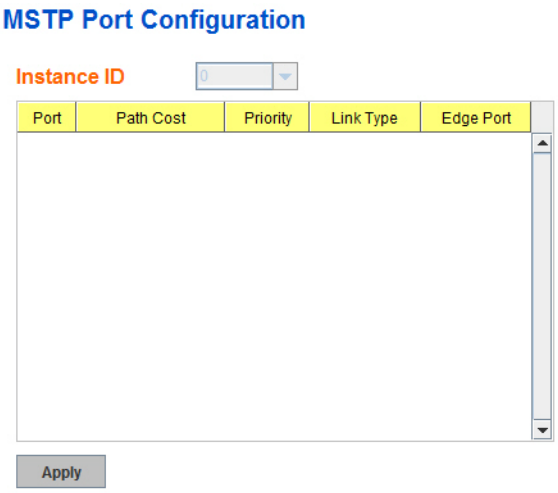


MSTP Configuration Page	
MST Region Configuration	
Region Name	A name used to identify the MST Region.
Revision	A value used to identify the MST Region.
Apply	Click the **Apply** button to apply the MST Region Configuration.
New MST Instance	
Instance ID	A value used to identify the MST instance, valid value are 1 through 15. Instance 0 (CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).
VLAN Group	Give a VLAN group to map this MST instance. Use a VLAN number (for example, 10), range (for example:1-10) or mixing format (for example: 2,4,6,4-7,10).
Instance Priority	A value used to identify the MST instance. The MST instance with the lowest value has the highest priority and is selected as the root. Enter a number 0 through 61440 in increments of 4096.
Add	Click the **Add** button to add the New MST Instance.

MSTP Configuration Page (Continued)	
Current MST Instance Configuration	
Instance ID	A value used to identify the MST instance. Instance 0 (CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).
VLAN Group	Provide a VLAN group to map this MST instance. Use the VLAN number, for example: 10. You can set a range, for example: 1-10) or set specific VLANs, for example: 2,4,6,4-7.
Instance Priority	A value used to identify the MST instance. The MST instance with the lowest value has the highest priority and is selected as the root. Enter a number 0 through 61440 in increments of 4096.
Modify	Click the **Modify** button to apply the current MST instance configuration. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

MSTP Port Configuration

This page allows you to configure the port settings. Choose the Instance ID that you want to configure.

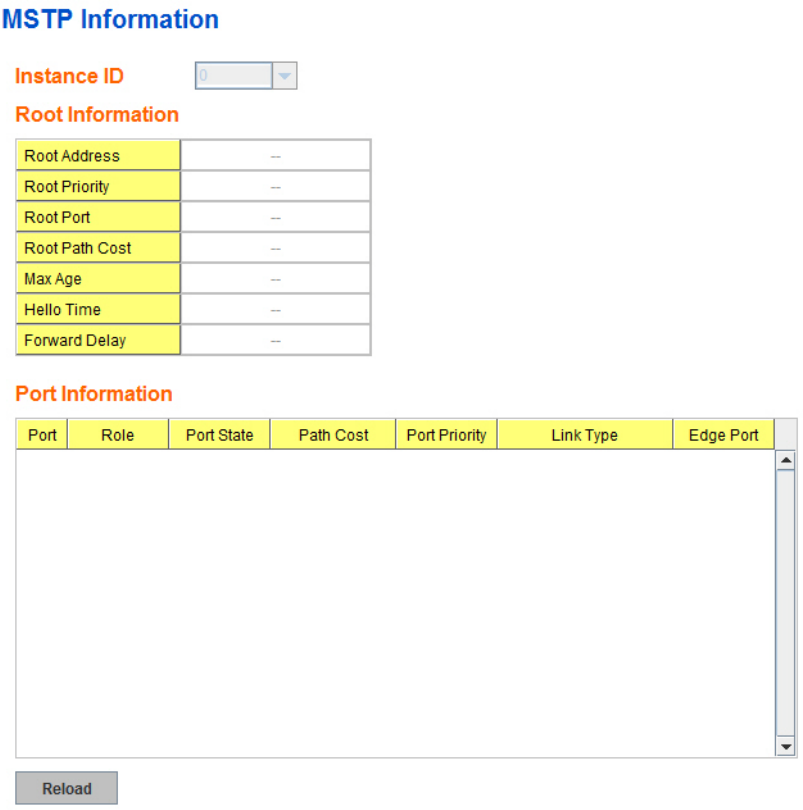


MSTP Port Configuration Page	
Instance ID	Select an Instance ID to display and modify MSTP instance setting.
Port Configuration	
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number from 1 through 200000000.
Priority	Decide which port should be blocked by priority on your LAN. Enter a number from 0 through 240 in increments of 16.
Link Type	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port in question is connected to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or if it's connected to two or more bridges (that is, it is served by a shared medium LAN segment). This configuration allows the p2p status of the link to be controlled by an administrator.

MSTP Port Configuration Page (Continued)	
Edge Port	Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, and skipping the listening and learning stages. When the non-bridge device connects an edge port, this port is in a blocking state and turn to forwarding state in 2*Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Apply	Click the **Apply** button to apply the configuration. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

MSTP Information

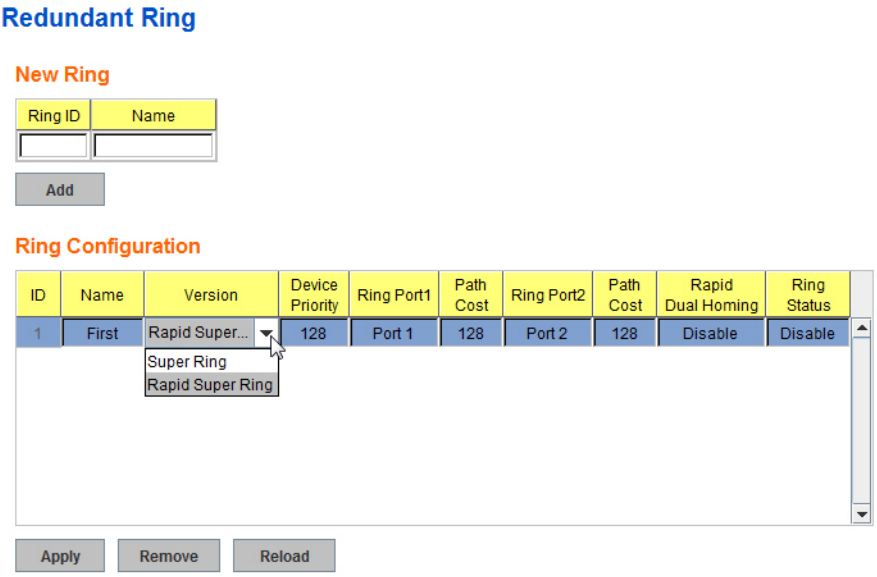
This page allows you to see the current MSTP information. Choose the Instance ID first. If the instance is not added, the information remains blank.



MSTP Information Page	
Instance ID	Select an instance ID to display MSTP instance information. Instance 0 (CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).
Root Information	
Root Address	Root bridge address, which is the bridge with the smallest (lowest) bridge ID.
Root Priority	Root bridge priority, the bridge with the lowest value has the highest priority and is selected as the root.
Root Port	Root port of this bridge.
Root Path Cost	Root path cost.
Max Age	The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting to reconfigure.
Hello Time	The number of seconds between the transmissions of Spanning-Tree Protocol configuration messages.
Forward Delay	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state.
Port Information	
Port Role	Descriptive information about the MSTP switch port role. Role: Master, Root, Designated, Alternate, Backup, Boundary, Disabled, Unknown.
Port State	Descriptive information about the MSTP switch port state. State: Blocking, Listening, Learning, Forwarding, Disabled, Unknown.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Path cost range is 1 through 200000000.
Port Priority	Decide which port should be blocked by priority in your LAN. The range is 0 through 240 in increments of 16.
Link Type	Operational link type. Some of the rapid state transactions that are possible within MSTP are dependent upon whether the port in question can be concerned to exactly one other bridge (that is, it is served by a point-to-point LAN segment), or can be connected to two or more bridges (that is, it is served by a shared medium LAN segment).
Edge Port	Operational edge port state. Present in implementations that support the identification of edge ports. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages. When the non-bridge device connects an edge port, this port is in blocking state and turn to forwarding state in 2*Hello Time seconds. When the bridge device connects an edge port, this port is a non-edge port automatic.
Reload	Click the **Reload** button to reload MSTP instance information.

Redundant Ring

The most common industrial network redundancy is to form a ring or loop. Typically, managed switches are connected in series and the last switch is connected back to the first one. In such connection, you can implement Redundant Ring technology.

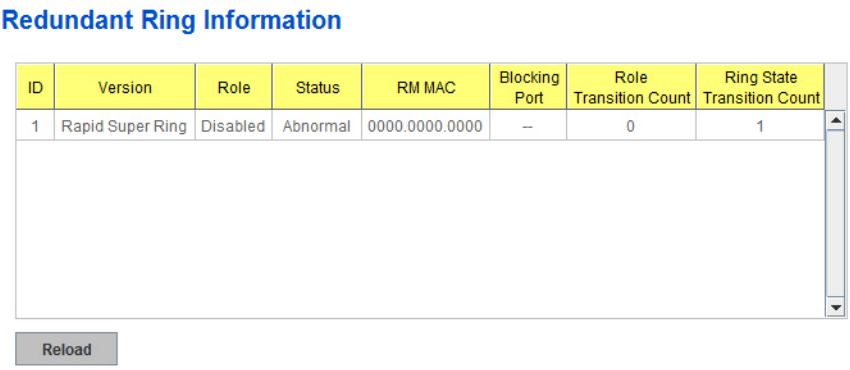


Redundant Ring Page	
New Ring (Ring ID/Name)	To create a Redundant Ring enter the Ring ID, which has range from 0 to 31. If the name field is left blank, the name of this ring is automatically named with the Ring ID. The maximum number of rings is 32. ***Note:*** *Once a ring is created, you cannot change it.*
Ring Configuration	
ID	Once a Ring is created, the Ring ID appears, and cannot be changed. In multiple ring environments, the traffic can only be forwarded under the same Ring ID. Remember to check the Ring ID when there are more than one ring in existence.
Name	This field shows the name of the Ring. If it is not entered when creating, it is automatically named by the rule *RingID*.
Version	The version of Ring can be changed here, the choices are **Rapid Super Ring** or **Super Ring**.
Device Priority	The switch with highest priority (highest value) is automatically selected as the **Ring Master** (RM). When one of the ring ports on this switch becomes a forwarding port and the other one becomes a blocking port. If all of the switches have the same priority, the switch with the highest MAC address is selected as the Ring Master.
Ring Port1	In a **Rapid Super Ring** environment, you should have two Ring ports. Whether this switch is a Ring Master or not. When configuring **Rapid Super Rings**, two ports should be selected to be Ring ports. For a Ring Master, one of the Ring Ports becomes the forwarding port and the other one becomes the blocking port.
Path Cost	Change the Path Cost of Ring Port1, if this switch is the Ring Master of a Ring, then it determines the blocking port. The port with higher Path Cost in the two Ring Ports becomes the blocking port, If the Path Cost is the same, the port with larger port number becomes the blocking port.
Ring Port2	Assign another port for ring connection.
Path Cost	Change the Path Cost of Ring Port2.

Redundant Ring Page (Continued)	
Rapid Dual Homing	Rapid Dual Homing is an important feature of Rapid Super Ring redundancy technology. When you want to connect multiple RSR or form redundant topology with other vendors, RDH allows you to have a maximum of seven multiple links for redundancy without any problem. In RDH, you do not need to configure a specific port to connect to other protocol. The RDH selects the fastest link for the primary link and blocks all the other links to avoid a loop. If the primary link failed, RDH automatically forwards the secondary link for a network redundant. If there are more connections, they are standby links and are recovered if both primary and secondary links are broken.
Ring status	To **Enable/Disable** the Ring, remember to enable the Ring after you add it.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Redundant Ring Information

This page shows Redundant Ring information.



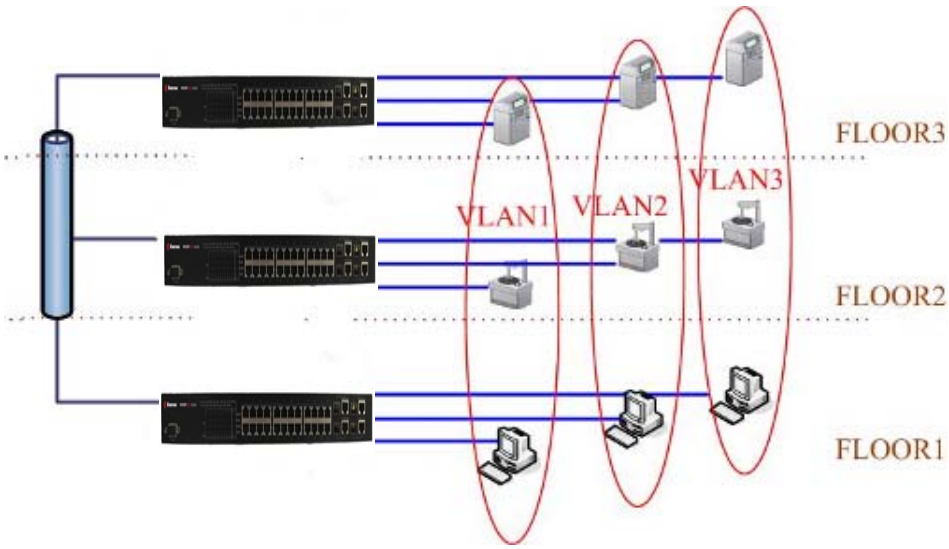
Redundant Ring Information Page	
ID	The Ring ID.
Version	Displays the ring version, this field could be Super Ring or Rapid Super Ring.
Role	This ES7528 is the RM (Ring Master) or nonRM (non-ring master).
Status	If this field is **Normal** it means the redundancy is approved. If any one of the link in this Ring is broken, then the status is **Abnormal**.
RM MAC	The MAC address of Ring Master of this Ring. It helps to find the redundant path.
Blocking Port	Shows which is blocked port of RM.
Role Transition Count	Shows how many times this ES7528 has changed its Role from nonRM to RM or from RM to nonRM.
Role state Transition Count	Shows how many times the Ring status has been transformed between **Normal** and **Abnormal** state.
Reload	Click to reload redundant ring information.

VLAN

A Virtual LAN (VLAN) is a logical grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members. The VLAN allows you to isolate network traffic so that only members of the VLAN could receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is the logical equivalent of physically reconnecting a group of network devices to another Layer 2 switch, without actually disconnecting these devices from their original switches.

The ES7528 supports IEEE 802.1Q VLAN, which is also known as Tag-Based VLAN. This Tag-Based VLAN allows a VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, this saves a lot of computing resources within the ES7528.

The following figure displays an IEEE 802.1Q VLAN.



The ES7528 supports VLAN tunneling (QinQ), which expands the number of VLANs by adding a tag to the 802.1Q packets. The original VLAN is usually identified as Customer VLAN (C-VLAN) and the new VLAN is Service VLAN(S-VLAN). By adding the additional tag, QinQ increases the possible number of VLANs. After QinQ is enabled, the ES7528 can reach up to 256x256 VLANs. With different standard tags, it also improves network security.

VLAN Configuration pages allow you to add and remove a VLAN, configure port Ingress/Egress parameters, and view the VLAN table. The following pages are included in this group:

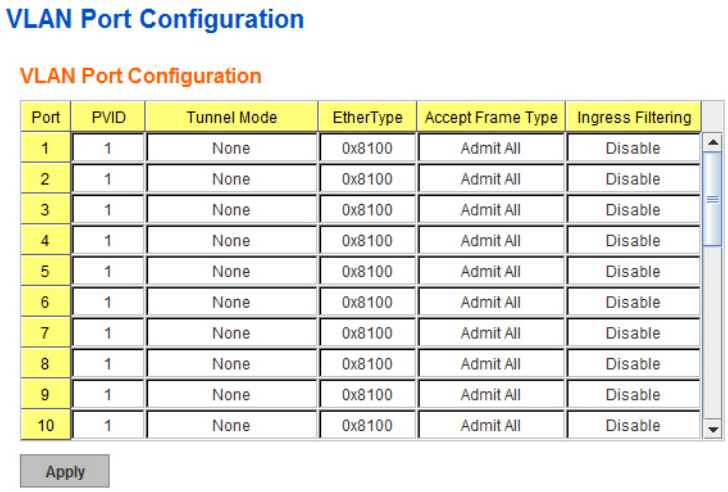
- *VLAN Port Configuration* on Page 86
- *VLAN Configuration* on Page 89
- *GVRP Configuration* on Page 92
- *VLAN Table* on Page 93

Optionally, you can use the CLI for configuration, see *VLAN (CLI)* on Page 175.

VLAN Port Configuration

The *VLAN Port Configuration* page allows you to configure VLAN port parameters on a specific port. These

parameters include the port VLAN ID (PVID), Tunnel Mode, Accept Frame Type and Ingress Filtering

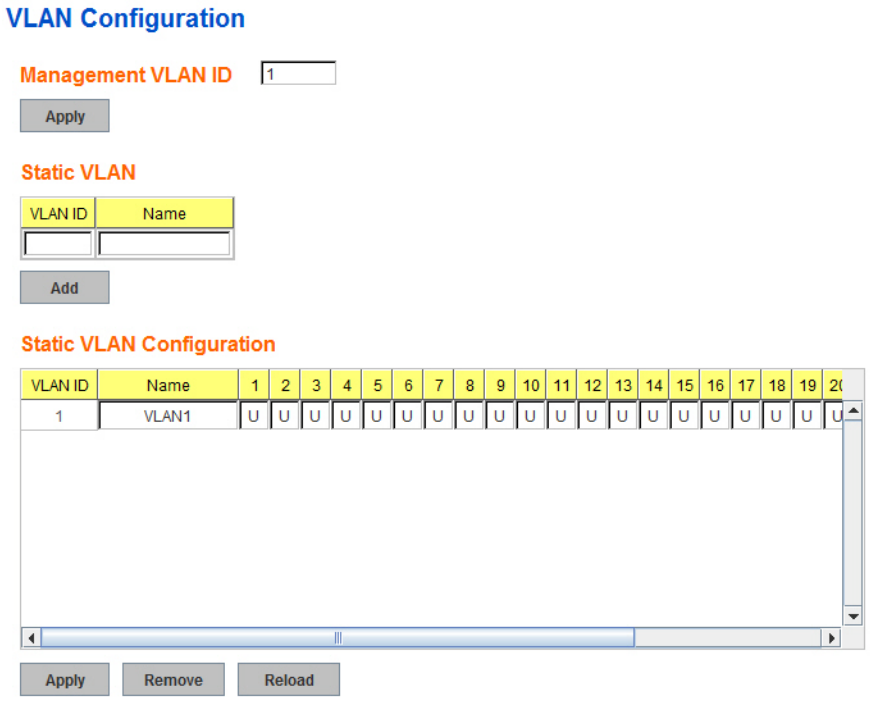


VLAN Port Configuration Page	
PVID	Enter the port VLAN ID (PVID). The PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 0 to 4,095 (0 and 4,095 are reserved), 1 is the default value; 2 to 4,094 are valid and available in this column. Enter the PVID you want to configure.
Tunnel Mode	**None** - IEEE 802.1Q tunnel mode is disabled. **802.1Q Tunnel**: QinQ is applied to the ports which connect to the C-VLAN. The port receives a tagged frame from the C-VLAN. You need to add a new tag (Port VID) as an S-VLAN VID. When the packets are forwarded to the C-VLAN, the S-VLAN tag is removed. After **802.1Q Tunnel** mode is assigned to a port, the egress setting of the port should be *Untag*, it indicates that the egress packet is always untagged. This is configured in the Static VLAN Configuration table (Page 89). **802.1Q Tunnel Uplink**: QinQ is applied to the ports which connect to the S-VLAN. The port receives a tagged frame from the S-VLAN. When the packets are forwarded to the S-VLAN, the S-VLAN tag is kept. After **802.1Q Tunnel Uplink** mode is assigned to a port, the egress setting of the port should be *Tag*, it indicates that the egress packet is always tagged. This is configured in the Static VLAN Configuration table (Page 89). For example, if the VID of S-VLAN/Tunnel Uplink is 10, the VID of C-VLAN/Tunnel is 5. The 802.1Q Tunnel port receives Tag 5 from C-VLAN and adds Tag 10 to the packet. When the packets are forwarded to S-VLAN, Tag 10 is kept.
EtherType	This allows you to define the EtherType manually. This is an advanced QinQ parameter that allows you to define the transmission packet type.
Accept Frame Type	This defines the accepted frame type of the port. There are two modes you can select: • **Admit All** mode means that the port can accept both tagged and untagged packets. When you select **Admit All**, untagged frames or Priority-Tagged only frames received on this port are accepted and assigned to the PVID for this frame. This control does not affect VLAN independent BPDU frames, such as Super Ring, STP, GVRP and LACP. It does affect VLAN dependent BPDU frames, such as GMRP. • **Tag Only** mode means that the port can only accept tagged packets.When you select **Tag Only** the ES7528 discards untagged frames or Priority-Tagged only frames received on this port.

VLAN Port Configuration Page (Continued)	
Ingress Filtering	Ingress filtering instructs the VLAN engine to filter out undesired traffic on a port. • When you **Enable Ingress Filtering**, the port checks whether the incoming frames belong to the VLAN they claimed or not. The port then determines if the frames can be processed or not. For example, if a tagged frame from *TEST VLAN* is received, and Ingress Filtering is enabled, the ES7528 determines if the port is on the *TEST VLAN*'s Egress list. If it is, the frame can be processed. If it is not, the frame is dropped. • When you select **Disable**, the port accepts all incoming frames regardless of its VLAN classification. This control does not affect VLAN independent BPDU frames, such as Super Ring, STP, GVRP and LACP. It does affect VLAN dependent BPDU frames, such as GMRP.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

VLAN Configuration

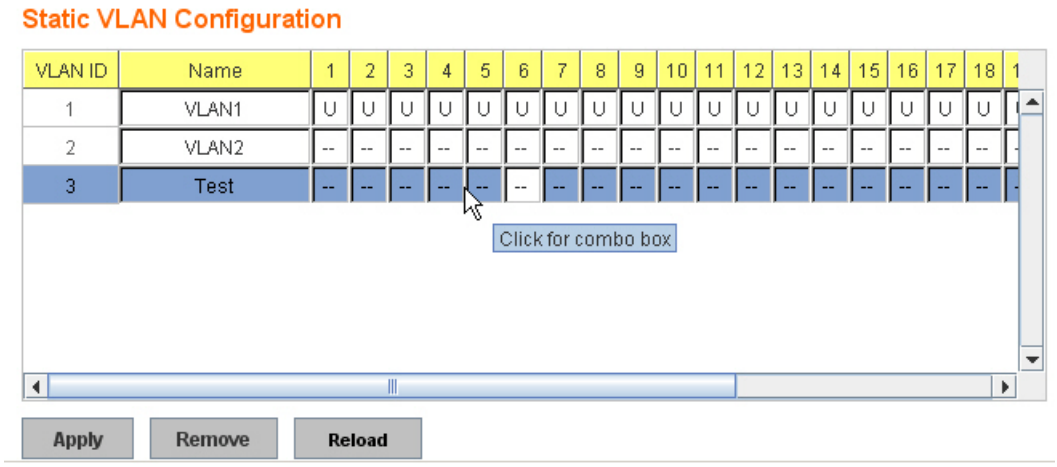
Use this page to assign the Management VLAN, create the static VLAN, and assign the Egress rule for the member ports of the VLAN.



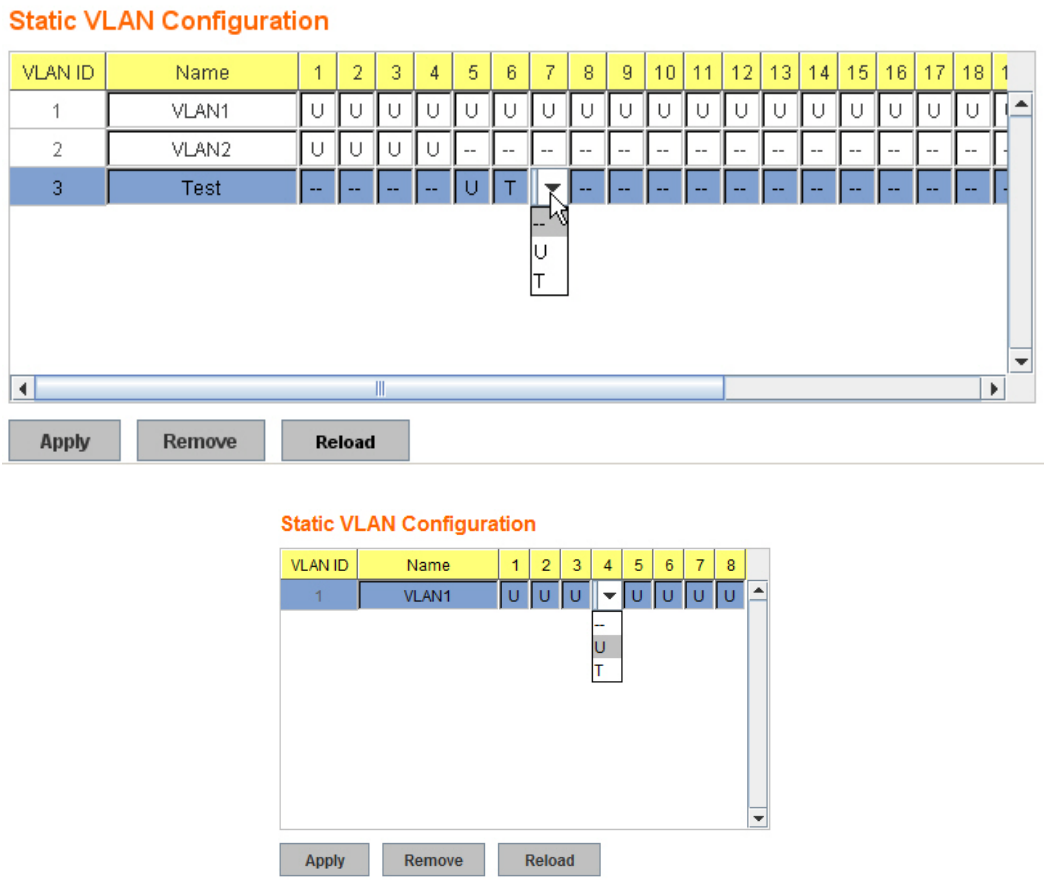
VLAN Configuration Page	
Management VLAN ID	The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch. The default management VLAN ID is **1**. Click **Apply** after you enter the VLAN ID.
Static VLAN	You can assign a VLAN ID and VLAN Name for the new static VLAN. • **VLAN ID**: This is used by the switch to identify different VLANs. A valid VLAN ID is between 1 and 4,094, 1 is the default VLAN. • **VLAN Name**: This is a reference for the network administrator to identify different VLANs. The VLAN name may up to 12 characters in length. If you do not provide a VLAN name, the system automatically assigns a VLAN name • . The rule is VLAN (VLAN ID). Click **Add** to create a new VLAN. The new VLAN displays in the Static VLAN Configuration table. After creating the VLAN, the status of the VLAN remains Unused, until you add ports to the VLAN. ***Note:*** *Before changing the management VLAN ID by web or Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator cannot access the switch through the network. The ES7528 supports a maximum of 256 VLANs.*

Static VLAN Configuration	• **VLAN ID**: The VLAN identifier for this VLAN.
	• **Name**: The name of the VLAN.
	• 1 - 28: The corresponding port number on the VLAN.
	  • **--** Not available
	  • **U** Untag, indicates that egress/outgoing frames are not VLAN tagged.
	  • **T** Tag, indicates that egress/outgoing frames are
	  • LAN tagged.
	• Click **Apply** to apply the settings.
	Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*
	• Click **Remove** to remove the selected static VLAN.
	• Click **Reload** to reload static VLAN configuration.

The following figure shows a static VLAN configuration table. The new VLAN 3 was created and the VLAN name is test. Egress rules of the ports are not configured.



This figure displays how to configure the Egress rule of the ports.



Use the following steps to configure Egress rules:

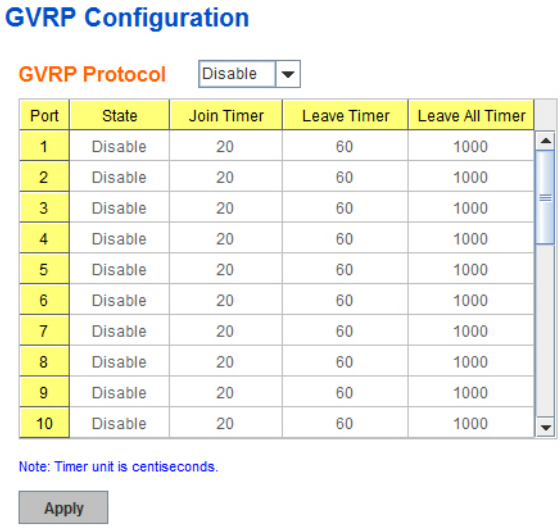
1. Select the VLAN ID. The entry of the selected VLAN turns to light blue.
2. Assign Egress rule of the ports to **U** or **T**.
3. Press **Apply** to apply the setting.

If you want to remove one VLAN, select the VLAN entry and then click the **Remove** button.

GVRP Configuration

GARP VLAN Registration Protocol (GVRP) allows you to set-up VLANs automatically rather than manual configuration on every port on every switch in the network. GVRP conforms to the IEEE 802.1Q specification. This defines a method of tagging frames with VLAN configuration data that allows network devices to dynamically exchange VLAN configuration information with other devices.

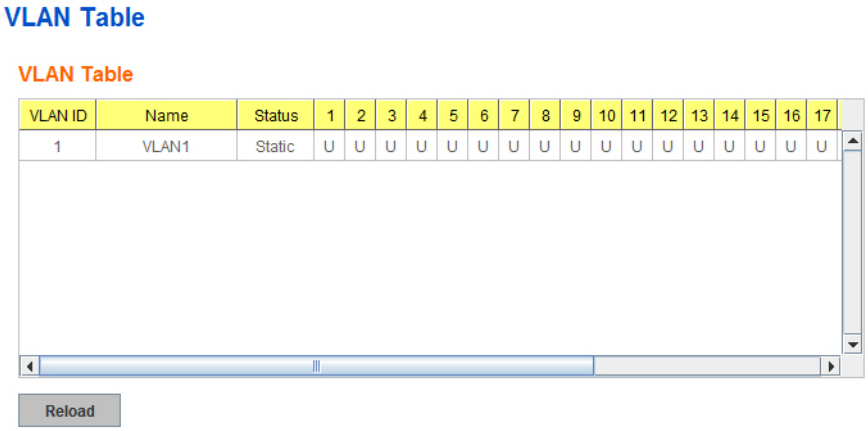
GARP (Generic Attribute Registration Protocol), a protocol that defines procedures by which end stations and switches in a local area network (LAN) can register and de-register attributes, such as identifiers or addresses, with each other. Every end station and switch thus has a current record of all the other end stations and switches that can be reached. GVRP, like GARP, eliminates unnecessary network traffic by preventing attempts to transmit information to unregistered users. In addition, it is necessary to manually configure only one switch and all the other switches are configured accordingly.



GVRP Configuration Page	
GVRP Protocol	Allows you to **Enable/Disable** GVRP globally.
State	After enabling GVRP globally, you can still **Enable/Disable** GVRP by port.
Join Timer	Controls the interval of sending the GVRP Join BPDU (Bridge Protocol Data Unit). An instance of this timer is required on a per-port, per-GARP participant basis.
Leave Timer	Controls the time to release the GVRP reservation after having received the GVRP Leave BPDU. An instance of the timer is required for each state machine that is in the LV state.
Leave All Timer	Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-port, per-GARP participant basis.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

VLAN Table

This table displays the current settings of your VLAN table, including VLAN ID, Name, Status, and Egress rule of the ports.



VLAN Table Page	
VLAN ID	The ID of the VLAN.
Name	The name of the VLAN.
Status	**Static** means that this is a manually configured static VLAN. **Unused** means this VLAN is created by web user interface/CLI and has no member ports and the VLAN is not workable yet. **Dynamic** means this VLAN was learnt by GVRP. • **--** No VLAN setting. • **T** A Trunk Link is a LAN segment used for multiplexing VLANs between VLAN bridges. All the devices that connect to a Trunk Link must be IEEE 802.1Q VLAN-aware, which sends and receives frames with IEEE 802.1Q tags. • **U** An Access Link is a LAN segment used to multiplex one or more IEEE 802.1Q VLAN-unaware devices into a Port of a VLAN Bridge. Devices that are connected to an Access Link sends and receives frames without IEEE 802.1Q tagging, which is the identification of the VLAN it belongs to.

After creating the VLAN, the status of this VLAN remains in **Unused** status until you add ports to the VLAN.

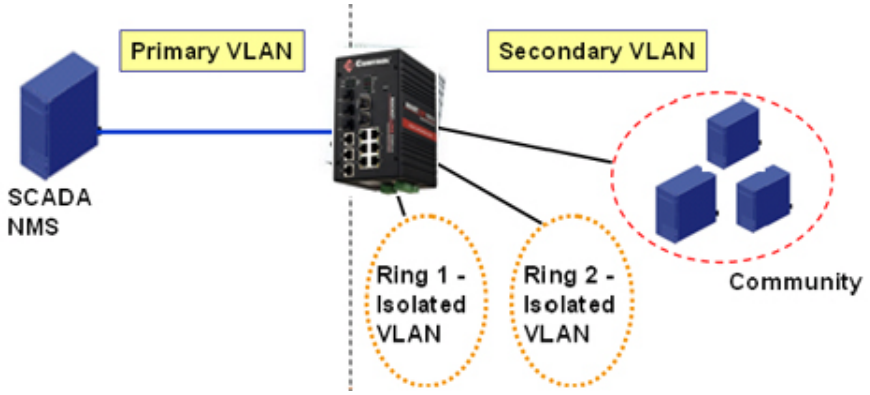
Private VLAN

A private VLAN helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. The private VLAN features provides primary and secondary VLANs within a single switch.

Primary VLAN: The uplink port is usually a member of the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with Secondary VLANs.

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated and Community VLANs. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other, however, the isolated VLAN ports cannot.

This figure shows a typical private VLAN network. A SCADA/Public Server or NMS workstation is usually located in a primary VLAN. Client PCs and rings are usually located within the secondary VLAN.



The following web pages are in this group:

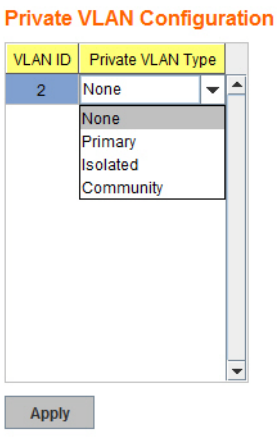
- *PVLAN Configuration* on Page 94
- *PVLAN Port Configuration* on Page 95
- *PVLAN Information* on Page 96

Optionally, you can use the CLI for configuration, see *Private VLAN (CLI)* on Page 178.

PVLAN Configuration

PVLAN Configuration allows you to assign a private VLAN type. Choose the private VLAN types for each VLAN you want configure.

Note: *You must have previously configured a VLAN in the VLAN Configuration screen. Refer to VLAN Configuration on Page 89 for information.*

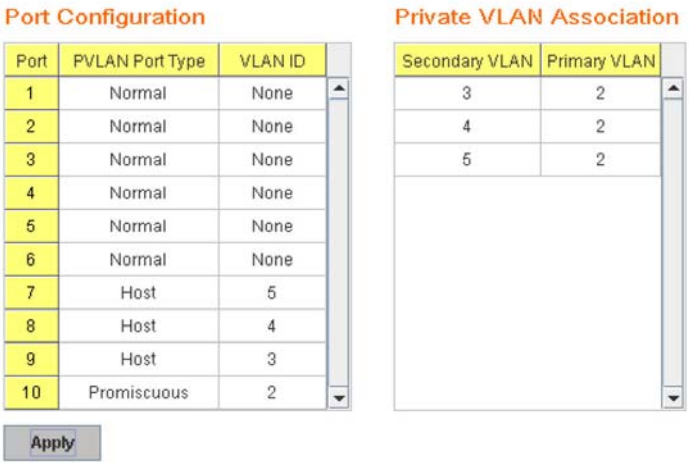


Private VLAN Configuration Page	
VLAN ID	• *Primary VLAN* - The uplink port is usually the primary VLAN. Ports within a primary VLAN can communicate with ports in a secondary VLAN • *Secondary VLAN* - The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLANs. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other. However, the isolated VLAN ports cannot.

Private VLAN Configuration Page (Continued)	
Private VLAN Type	• **None**: The VLAN is not included in private VLAN. • Primary: A primary VLAN contains promiscuous ports that can communicate with the secondary VLANs. • **Isolated**: The member ports of the VLAN are isolated. • **Community**: The member ports of the VLAN can communicate with each other.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

PVLAN Port Configuration

The *PVLAN Port Configuration* page allows you to configure the port configuration and private VLAN associations.



Private VLAN Port Configuration Page	
PVLAN Port Type	The following options are available: **Normal**: Normal ports remain in their original VLAN configuration. **Host**: Host ports can be mapped to the secondary VLAN. **Promiscuous**: Promiscuous ports can be associated to the primary VLAN.
VLAN ID	After assigning the port type, this displays the available VLAN ID for which the port can associate.
Private VLAN Association	
Secondary VLAN	After the isolated and community VLANs are configured in the *Private VLAN Configuration* page, the VLANs belonging to the second VLAN are displayed.
Primary VLAN	After the Primary VLAN Type is assigned in *Private VLAN Configuration* page, the secondary VLAN can associate to the primary VLAN ID. ***Note:*** *Before configuring PVLAN port type, the private VLAN Association should be done first.*

For example:

1. **VLAN Create**: VLANs 2-5 are created in the *VLAN Configuration* page.
2. **Private VLAN Type**: VLANs 2-5 has their own Private VLAN Type configured in the *Private VLAN Configuration* page.

   VLAN 2 belongs to the Primary VLAN.

   VLANs 3-5 belong to the secondary VLAN (Isolated or Community).
3. **Private VLAN Association**: Associate VLANs 3-5 to VLAN 2 in the Private VLAN Association first.
4. **Private VLAN Port Configuration**

   VLAN 2 – Primary -> The member port of VLAN 2 is a promiscuous port.

   VLAN 3 – Isolated -> The Host port can be mapped to VLAN 3.

   VLAN 4 – Community -> The Host port can be mapped to VLAN 3.

   VLAN 5 – Community -> The Host port can be mapped to VLAN 3.
5. **Result**:

   VLAN 2 -> VLANs 3, 4, 5; member ports can communicate with the ports in secondary VLAN.

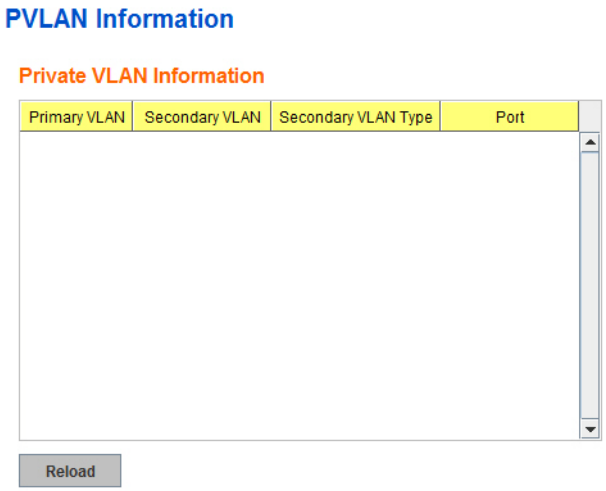
   VLAN 3 -> VLAN 2, member ports are isolated, but it can communicate with the member ports of VLAN 2.

   VLAN 4 -> VLAN 2, member ports within the community can communicate with each other and communicate with member ports of VLAN 2.

   VLAN 5 -> VLAN 2, member ports within the community can communicate with each other and communicate with member ports of VLAN 2.

PVLAN Information

The *PVLAN Information* page allows you to see the private VLAN information. Click **Reload** to refresh the page contents..



Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization mechanism which allows you to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port with regard to setting priorities.

The ES7528 QoS supports four physical queues, weighted fair queuing (WRR) and Strict Priority scheme, that follows the IEEE 802.1p CoS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

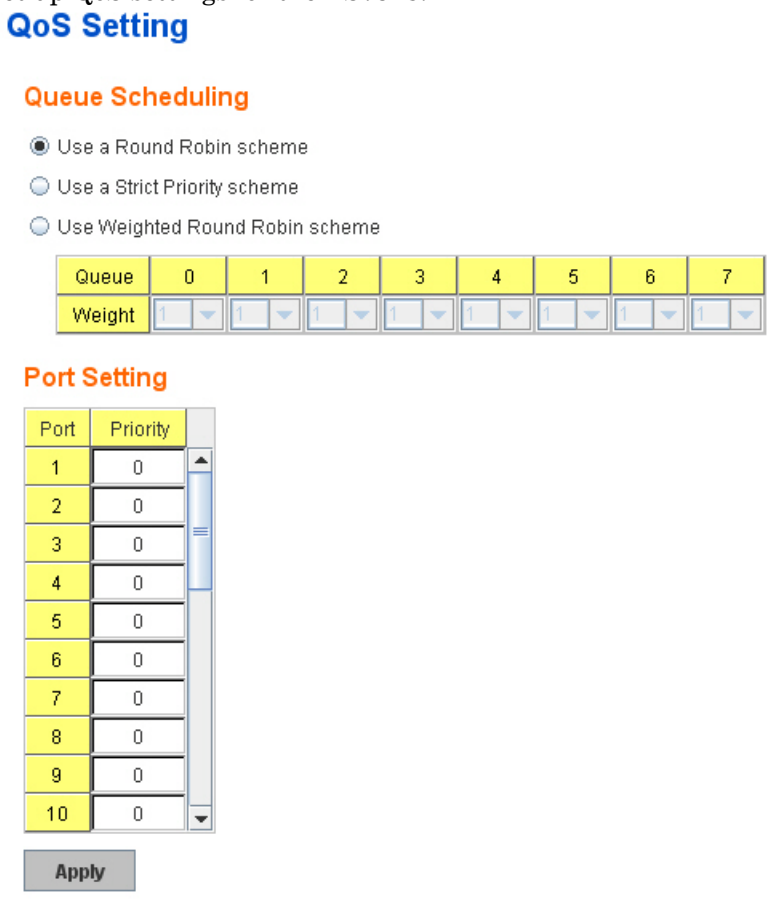
The following web pages are included in this group:

- *QoS Setting*
- *CoS-Queue Mapping* on Page 98
- *DSCP-Queue Mapping* on Page 99

Optionally, you can use the CLI for configuration, see *Traffic Prioritization (CLI)* on Page 182.

QoS Setting

Use this subsection to set up QoS settings for the ES7528.



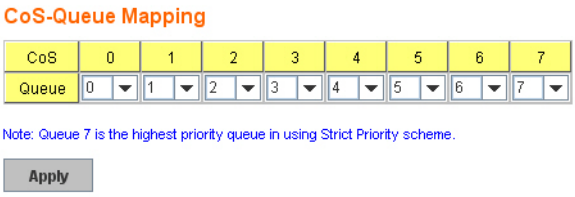
QoS Setting Page	
Queue Scheduling	
Use a Round Robin scheme	The Round Robin scheme means all the priority has the same privilege, the traffic is forward cyclic from highest to lowest.

QoS Setting Page (Continued)	
Use a strict priority scheme	Packets with higher priority in the queue are always processed first, except that there is no packet with higher priority.
Use Weighted Round Robin scheme	This scheme allows you to assign new weight ratio for each class. The 10 is the highest ratio. The ratio of each class is: `Wx / W0 + W1 + W2 + W3 + W4 + W5 + W6 + W7 (Total volume of Queue 0-7)`
Port Setting	
Priority	Indicates the default port priority value for untagged or priority-tagged frames. When the ES7528 receives the frames, the ES7528 attaches the value to the CoS field of the incoming VLAN-tagged packets. You can enable 0,1,2,3,4,5,6 or 7 to the port. Default priority type is **COS**. The system provides default CoS-Queue table to which you can refer for the next command.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

CoS-Queue Mapping

Use this page to change the CoS values into a Physical Queue mapping table. Since the switch fabric of the ES7528 supports eight queues, Lowest, Low, Middle and High. You should therefore assign how to map CoS value to the level of the physical queue.

Class of service (CoS) is a 3 bit field within a layer two Ethernet frame header defined by IEEE 802.1p when



using IEEE 802.1Q tagging. The field specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic.

While CoS operates only on Ethernet at the data link layer, other QoS mechanisms (such as DiffServ) operate at the network layer and higher. Others operate on other physical layers. Although IEEE 802.1Q tagging must be enabled to communicate priority information from switch to switch, some switches use CoS to internally classify traffic for QoS purposes.

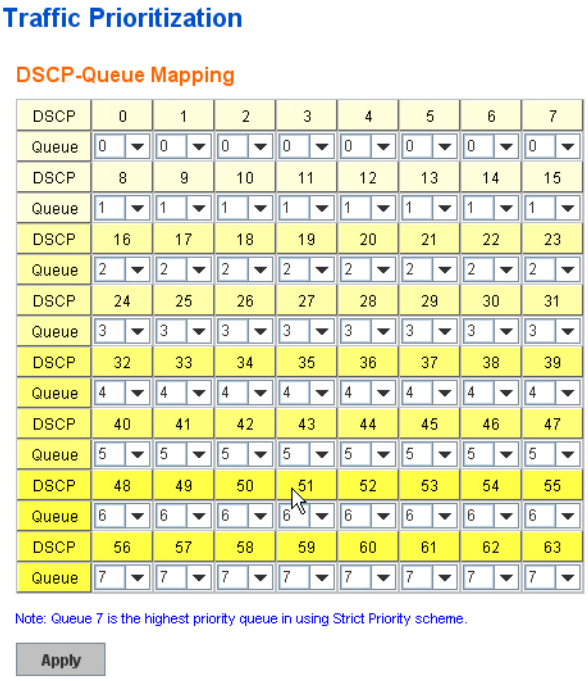
Differentiated Services (DiffServ) is a model where traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field. Defined in RFC2474 and RFC2475, the DiffServ standard supersedes the original specification for defining packet priority described in RFC791. DiffServ increases the number of definable priority levels by reallocating bits of an IP packet for priority marking. The DiffServ architecture defines the DiffServ field, which supersedes the ToS field in IPv4 to make per-hop behavior (PHB) decisions about packet classification and traffic conditioning functions, such as; metering, marking, shaping, and policing.

After configuration, press **Apply** to enable the settings.

Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

DSCP-Queue Mapping

Use this page to change DSCP values to Physical Queue mapping table. Since the switch fabric of the ES7528 only supports eight queues. You can change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.



After configuration, press **Apply** to enable the settings.

Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Multicast Filtering

For multicast filtering, the ES7528 uses IGMP (Internet Group Management Protocol) Snooping technology. IGMP is an internet protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computer's data.

Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership.

In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown in the following table.

Messages	
Query	A message sent from the querier (an IGMP router or a switch) that asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable **IGMP Snooping** and **IGMP Query** functions. This section illustrates the information of the IGMP Snooping function, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

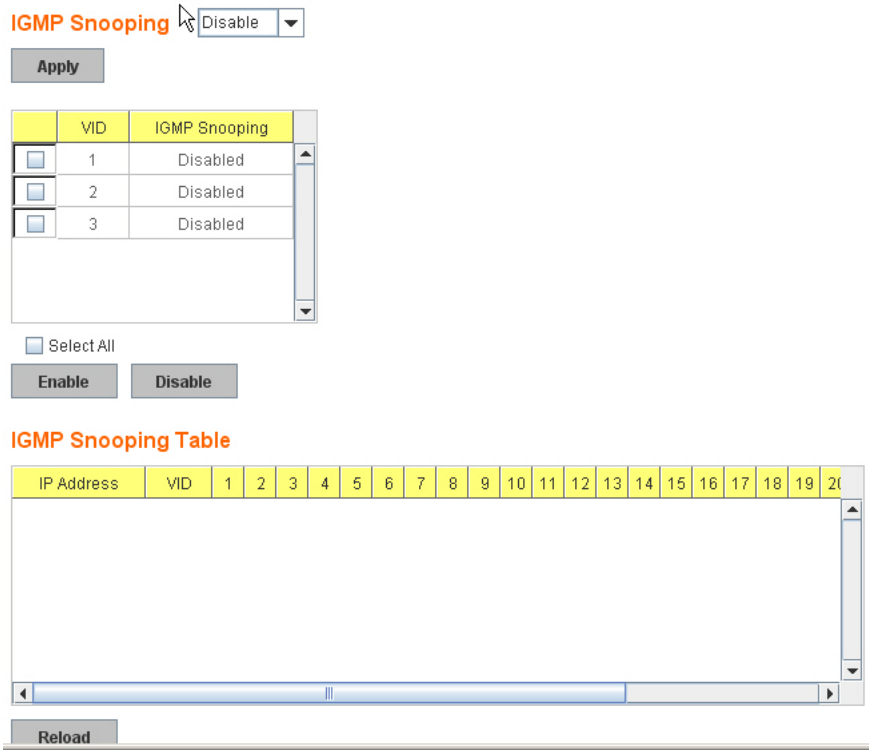
The following web pages are included in this group:

- *IGMP Snooping* on Page 101
- *IGMP Query* on Page 102
- *Unknown Multicast* on Page 102
- *GMRP Configuration* on Page 103

Optionally, you can use the CLI for configuration, see *Multicast Filtering (CLI)* on Page 185.

IGMP Snooping

Use this page to enable the IGMP Snooping feature, assign IGMP Snooping for specific VLANs, and view the IGMP Snooping table from a dynamic learnt or static that you provide.



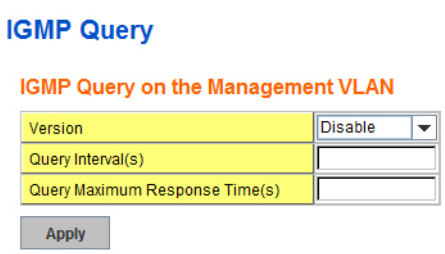
IGMP Snooping Page	
IGMP Snooping	You can select **Enable** or **Disable**. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN. You can **Enable** IGMP Snooping for some VLANs so that some of the VLANs support IGMP Snooping and others do not. To assign IGMP Snooping to VLAN, click the check box of the VLAN ID or click the **Select All** check box for all VLANs and then click **Enable**. You can also **Disable** IGMP Snooping for certain VLANs using the same method.
IGMP Snooping Table	This table displays the multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. The ES7528 supports 256 multicast groups. Click **Reload** to refresh the table.

Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

IGMP Query

Use this page to configure the IGMP Query feature. Since the ES7528 can only be configured by member ports of the management VLAN, the IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, first check to see whether each VLAN has its own IGMP Querier.

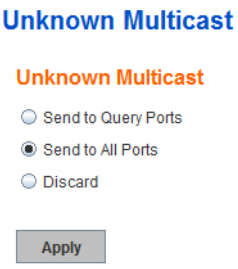
The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.



IGMP Query Page	
Version	Select **Version 1**, **Version 2** or **Disable**. • **Version 1** means IGMP V1 General Query • **Version 2** means IGMP V2 General Query. The query is forwarded to all multicast groups in the VLAN. • **Disable** allows you to disable IGMP Query.
Query Interval(s)	The period of query (seconds) sent by querier. Enter a number between 1 and 65,535.
Query Maximum Response Time	The span querier detect (seconds) to confirm there are no more directly connected group members on a LAN. Enter a number between 1 and 25.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Unknown Multicast

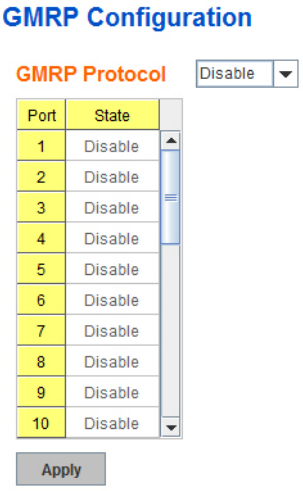
This page allows you to decide how to forward the unknown multicast traffic. After enabling IGMP Snooping, the known multicast can be filtered by IGMP Snooping mechanism and forwarded to the member ports of known multicast groups. The other multicast streams that are not learned are-called unknown multicasts, the ES7528 decides how to forward them based on the setting on this page.



UnKnown Multicast Page	
Send to Query Ports	The unknown multicast is sent to the Query ports. The Query port means the port received the IGMP Query packets. It is usually the uplink port of the switch.
Send to All Ports	The unknown multicast is flooded on all ports even if they are not member ports of the groups.
Discard	The unknown multicast is discarded. Non-member ports do not receive the unknown multicast streams.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

GMRP Configuration

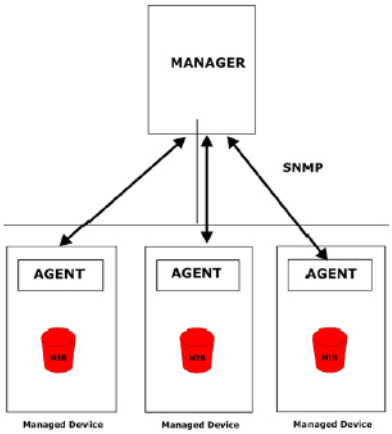
GARP Multicast Registration Protocol (GMRP) is a Generic Registration Protocol (GARP) application that provides a multicast traffic management facility at Layer 2 similar to what IGMP provides at Layer 3. GMRP and GARP are industry-standard protocols first introduced as part of IEEE 802.1D.



GMRP Configuration	Description
GMRP Protocol	**Enable/Disable** GMRP protocol.
State	The state of the GMRP operation on this port. The value enabled indicates that the GMRP is enabled on this port as long as the GMRP protocol is also enabled for this device. When disabled, but the GMRP protocol is still enable for the device, GMRP is disabled on this port.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

SNMP

Simple Network Management Protocol (SNMP) is a protocol to exchange management information between network devices. SNMP is a member of the TCP/IP protocol suite. The ES7528 supports SNMP v1 and v2c and v3.



An SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

The following web pages are included in this group:

- *SNMP Configuration*
- *SNMP V3 Profile* on Page 105
- *SNMP Traps* on Page 106

Optionally, you can use the CLI for configuration, see *SNMP (CLI)* on Page 190.

SNMP Configuration

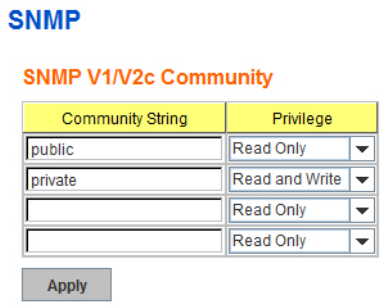
Use this page to configure the SNMP v1/v2c Community. The community string can be viewed as the password because SNMP v1/v2c does not request you to enter a password before you try to access the SNMP agent.

The community includes two privileges:

- **Read Only** privilege, you only have the ability to read the values of MIB tables. The default community string is **public**.
- **Read and Write** privilege, you have the ability to read and set the values of MIB tables. The default community string is **private**.

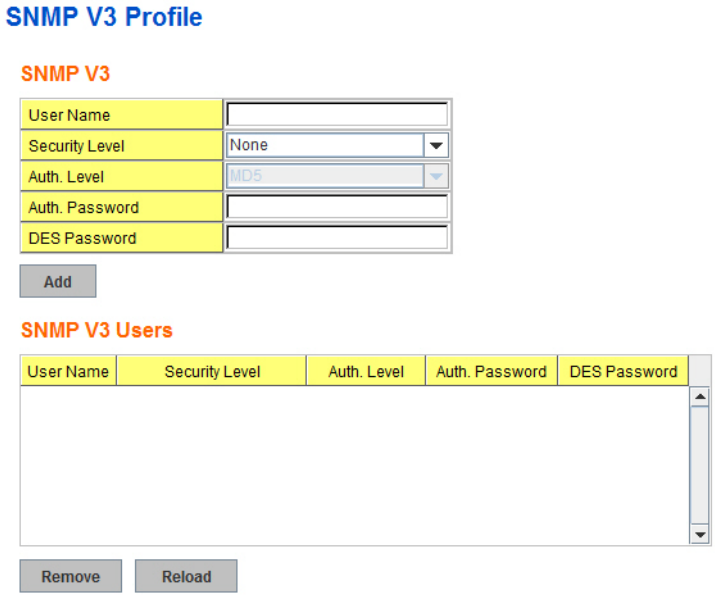
The ES7528 allows you to assign four community strings. Type the community string, select the privilege, and then click **Apply**.

Note: *When you first install the device in your network, we recommend that you change the community string. Most SNMP management applications use public and private as the default community name, this could be a network security leak.*



SNMP V3 Profile

SNMP v3 can provide more security functions when you perform remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between the ES7528 and the administrator are encrypted to ensure secure communication.

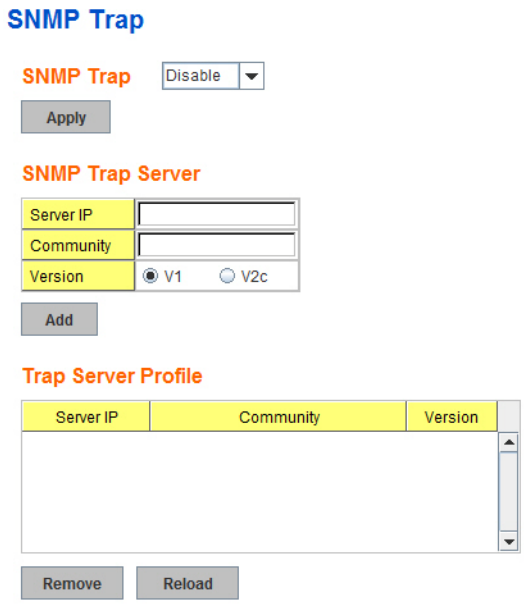


SNMP V3 Profile Page	
User Name	SNMP v3 user name.
Security Level	Select the following levels of security: **None**, **Authentication**, and **Authentication and Privacy**.
Auth Level	Select either **MD5** (Message-Digest algorithm 5) or **SHA** (Secure Hash Algorithm). • **MD5** is a widely used cryptographic hash function with a 128-bit hash value. • **SHA** functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. The ES7528 provides two user authentication protocols in MD5 and SHA. You need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.
Auth Password	Enter the SNMP v3 user authentication password.
DES Password	Enter the password for SNMP v3 user DES Encryption.
Add	Click to add an SNMP v3 user.
SNMP V3 Users	This table provides SNMP v3 user information. Click **Remove** to remove a selected SNMP v3 user. Click **Reload** to reload SNMP v3 user information.

Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

SNMP Traps

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap information. So you do not need to install new applications to read the notification information.



SNMP Trap Page	
SNMP Trap	Click Enable or Disable SNMP trap functionality.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*
SNMP Trap Server	
Server IP	The SNMP trap server IP address.
Community	The SNMP trap server community string.
Version	The SNMP trap version, V1 or V2c.
Add	Click the **Add** button to add a SNMP server.
Trap Server Profile	
Server IP	The SNMP trap server IP address
Community	The SNMP trap server community string.
Version	The SNMP trap version, V1 or V2c.
Remove	Click the **Remove** button to remove selected SNMP server.
Reload	Click the **Reload** button to reload SNMP server information.

You can see the change of the SNMP pre-defined standard traps and Comtrol pre-defined traps. The pre-defined traps can be found in the Comtrol private MIB.

Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Security

The ES7528 provides several security features for you to secure your connection. The following pages are included in this group:

- *Filter Set (Access Control List)*
  - *MAC Filter (Port Security)* on Page 108
  - *IP Filter* on Page 110
  - *Filter Attach* on Page 112
- *802.1x Configuration* on Page 113
- *802.1x Port Configuration* on Page 114
- *802.1x Port Status* on Page 116

Optionally, you can use the CLI for configuration, see *Security (CLI)* on Page 191.

Filter Set (Access Control List)

The Filter Set is known as Access Control List (ACL) feature. There are two major types:

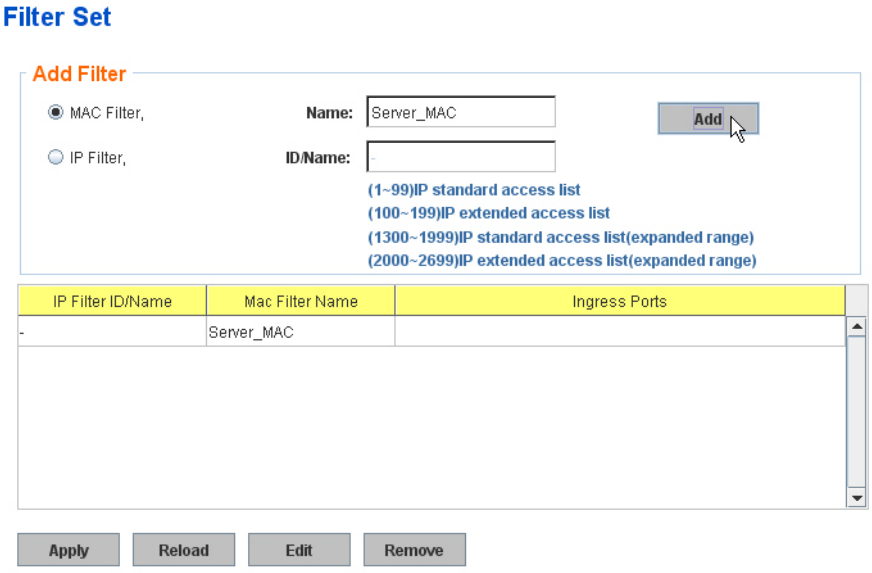
- *MAC Filter (Port Security)* on Page 108, which is called Port Security in other RocketLinx switches. It allows you to define the access rule based on the MAC address.
- *IP Filter* on Page 110, which is called IP security in other RocketLinx models and supports the IP Standard access list, and advanced IP based access lists.

You can use Access Control Entry (ACE) to define a Permit or Deny rule for specific IP or MAC address, or IP groups by network mask in each ACE. One ACL may include several ACEs. The system checks the ACEs one after another and forwards the data based on the result.

If the rules conflict, the oldest entry is selected.

To define rules using the MAC Filter, click **MAC Filter**, and type the **Name.** To define rules using the IP Filter, click **IP Filter**, and type the **ID/Name**. The ID for the IP access list is listed as below of the field.

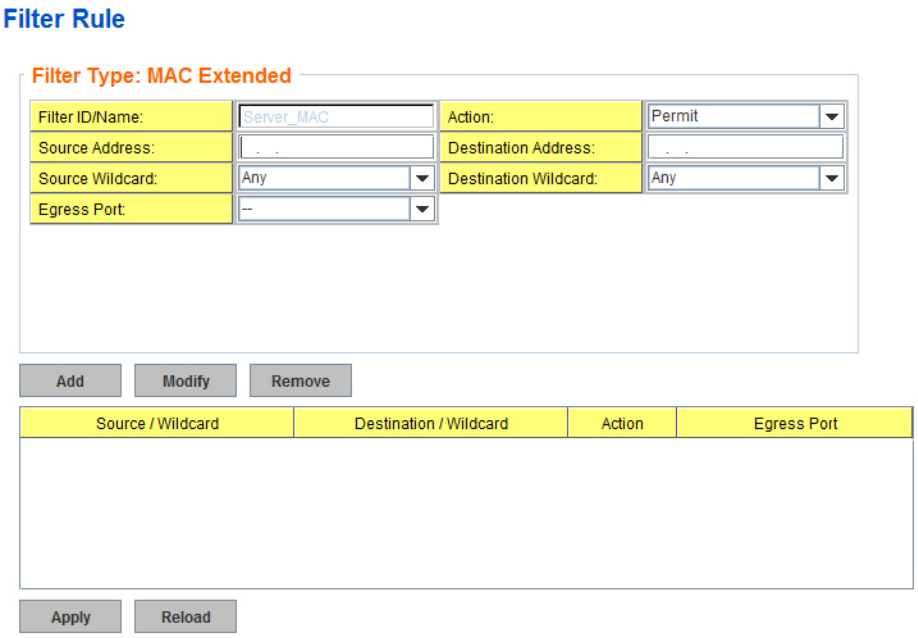
Click **Add** to add the rule. Click **Edit** to edit the contents of the rule. After configuring the rules, click **Apply** to apply all the rules. Click **Reload** to reload setting and **Remove** to remove one of the entries.

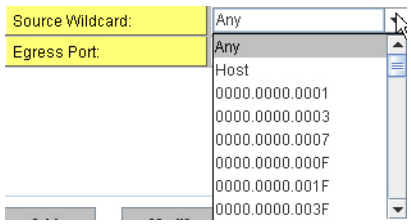
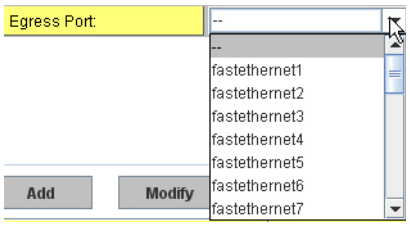


MAC Filter (Port Security)

The MAC Filter allows you to define the Access Control List for a specific MAC address or a group of MAC addresses.

To access the options in the following web page, you must first enter the name of the MAC filter in the Name text box in the Filter Set web page, highlight the MAC filter name, click **Edit**, and then this page appears.



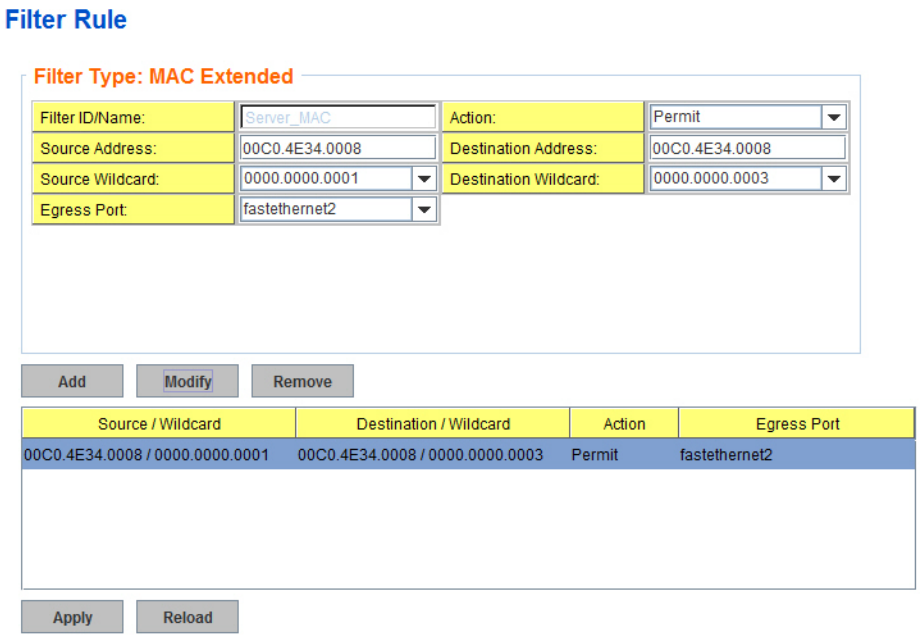
Filter Type: MAC Standard/ Extended	Description
Filter ID/Name	The name for this MAC Filter entry.
Action	Select **Permit** to permit traffic from specified sources or Deny to deny traffic from those sources.
Source/ Destination Address	Type the MAC address that you want to configure. The format is AABB.CCDD.EEFF. For example: The Source to Destination is 00c0.4e32.0001 to 00c0.4e32.0022.
Source/ Destination Wildcard	You can define a single host or a group of hosts based on the wildcard. Some of the allowance examples are shown in the following table. 
Egress Port	Bind the MAC Filter rule to specific port. 

Wildcard	Bit	Number of Allowances	Note
Any	1111.1111.1111	All	
Host		1	Only the source or destination
0000.0000.0003	0000.0000.000(00000011)	3	
0000.0000.0007	0000.0000.000(00000111)	7	
0000.0000.000F	0000.0000.000(11111111)	15	
....			

Once you finish configuring the MAC settings, click **Add** to apply your configuration.

The following example shows:

- Permit Source MAC address from 00c0.4e32.0000 to Destination MAC 00c0.4e32.0002.
- The Permit rule is egress rule and it is bound to fastethernet Port 2.

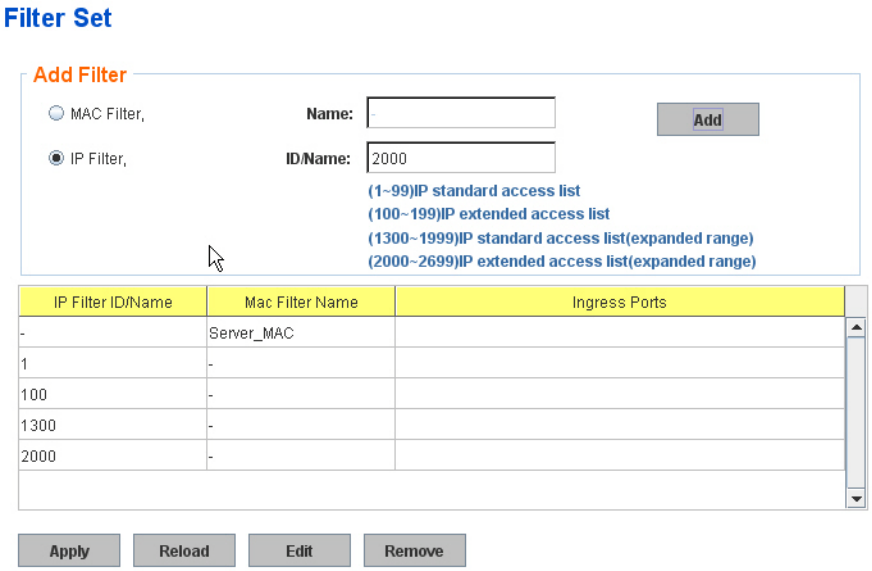


Once you finish configuring the settings, click **Apply** to apply your configuration.

Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

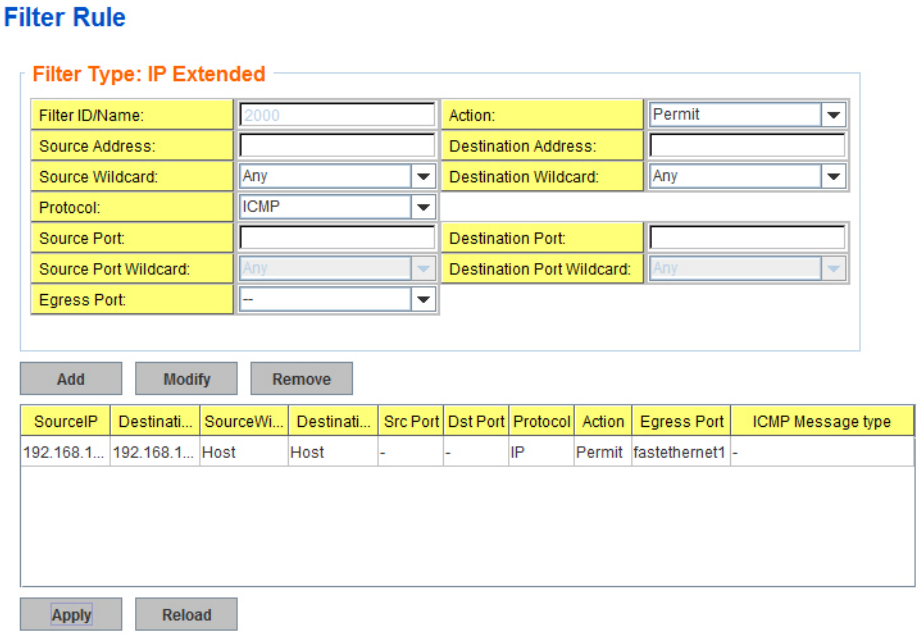
IP Filter

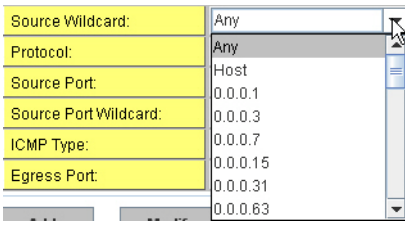
Click **IP Filter** and type **ID/Name** to configure security using IP addresses. Click **Reload** to reload setting and **Remove** to remove one of the entries.



IP Filter Set	Description
ID/Name	You can enter an ID for the IP access list or you can enter an ACL name ID/Name field. If you enter an ACL name, the entry uses IP Extended mode and supports IP Standard and IP Extended.
IP Standard Access List	This type of ACL allows you to define filter rules according to the source IP address.
IP Extended Access List	This type of ACL allows you to define filter rules according to the source IP address, destination IP address, Source TCP/UDP port, destination TCP/UDP port and ICMP type and code.

Highlight an IP Filter ID/Name and click **Edit** to configure the IP Filter Rules.



Filter Type: IP Standard/ Extended	Description
Filter ID/Name	The ID or the name for this IP Filter entry.
Action	Select **Permit** to permit traffic from specified sources and Deny to deny traffic from those sources.
Source/Destination Address	Type the source/destination IP address you want configured.
Source/Destination Wildcard	You can define a single host or a group of hosts based on the wildcard. Some of the allowance examples are shown in the following table. 
Protocol	Select a protocol that you want associate with the filter. The field includes IP, TCP, UDP or ICMP type.
Destination Port	TCP/UDP port of the Destination Port field.
ICMP Type	The ICMP Protocol Type range from 1 ~ 255.
ICMP Code	The ICMP Protocol Code range from 1 ~ 255.
Egress Port	Bind this Filter to selected egress port.
Add	Adds the rule to the Filter.
Remove	Removes the selected rule from the Filter.
Modify	Allows you to edit the rule which you selected.
Reload	Reloads the rule table.

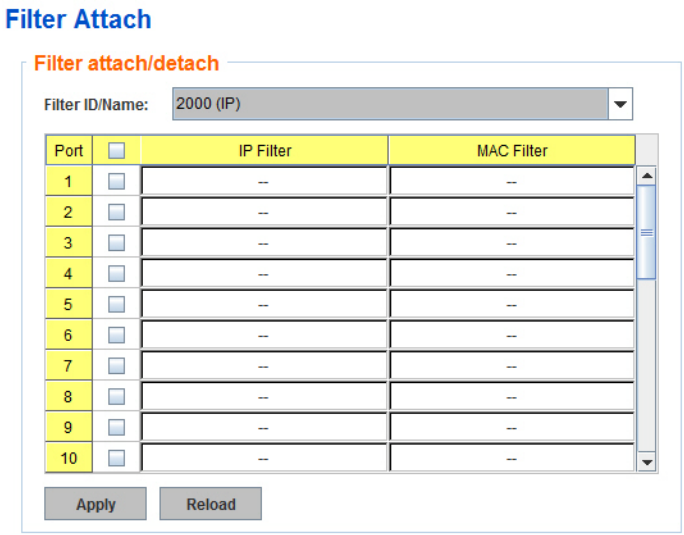
Wildcard	Bit	Number of Allowances	Note
Any	11111111.11111111	All	All IP addresses or a mask 255.255.255.255
Host	0.0.0.0	1	Only the source or destination
0.0.0.3	0.0.0.0.(00000011)	3	
0.0.0.7	0.0.0.0.(00000111)	7	
0000.0000.000F	0.0.0.0.(11111111)	15	
....			

Note: *The mask is a wildcard mask: the high-order bits of the mask that are binary zeros determine how many corresponding high-order bits in the IP address are significant. The selected action applies to any source address with these high-order bits.*

Filter Attach

Initially, the interfaces associated with the selected device have no Filter attached to them. To attach or detach a Filter: select the row for the interface to which you want to attach a Filter or from which you want to detach a Filter.

Click **Reload** to reload the filter table.

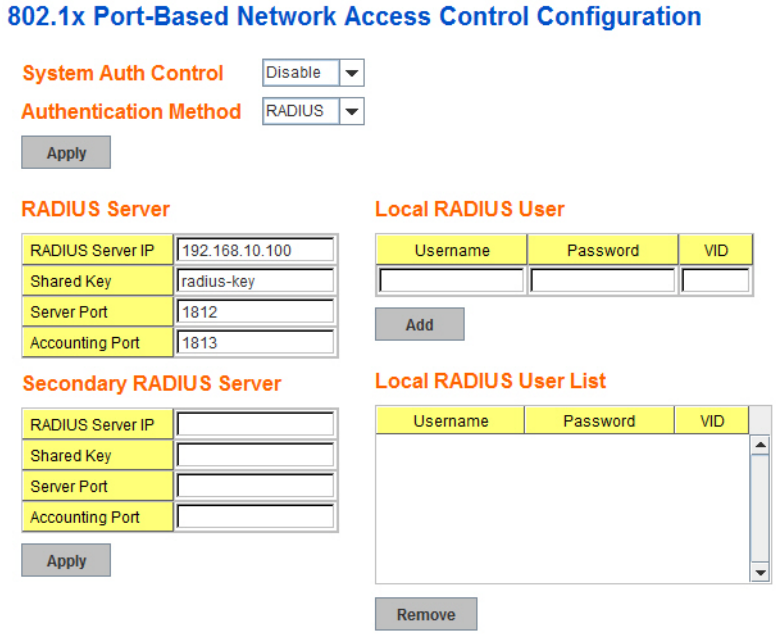


Click the **Apply** button to apply the Filter configurations.

Note: *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

802.1x Configuration

IEEE 802.1x is the protocol that performs authentication to obtain access to IEEE 802 LANs. It is port-base network access control. With the function, the ES7528 could control which connection is available or not.

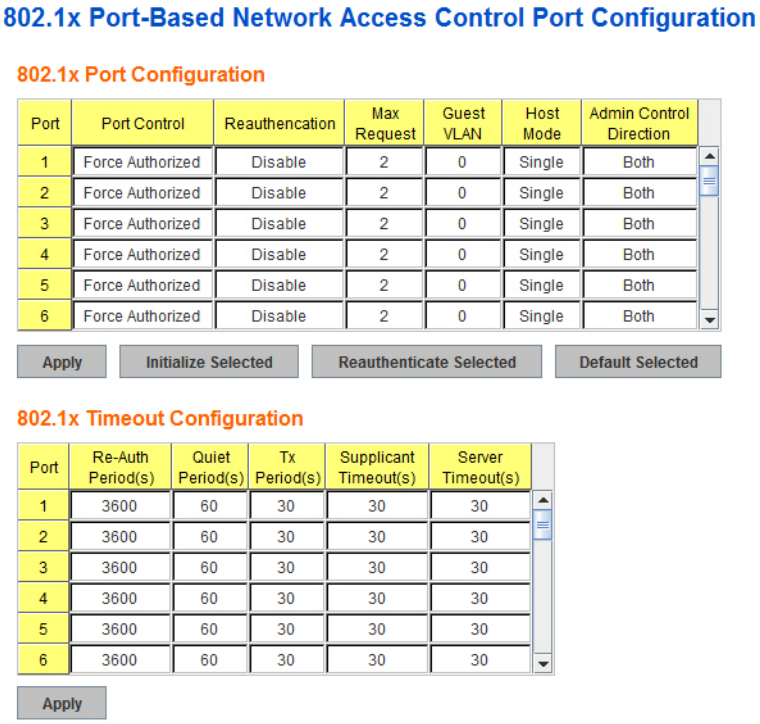


IEEE 802.1x Page	
System Auth Control	**Enable** or **Disable** the IEEE 802.1x authentication.
Authentication Method	**RADIUS** is an authentication server that provides a key for authentication. When you use this method, you must connect the switch to the server. If you select **Local** for the authentication method, the switch uses the local user database that can be created in this page for authentication.
RADIUS Server	
RADIUS Server IP	The IP address of the RADIUS server.
Shared Key	The password used to communicate between the ES7528 and the RADIUS Server.
Server Port	The UDP port of the RADIUS server.
Accounting Port	The port for packets that contains the account login or logout information.
Secondary RADIUS Server	
RADIUS Server IP	You can set a Secondary RADIUS Server, if the primary RADIUS server goes down.
Shared Key	The password used to communicate between the ES7528 and the secondary RADIUS Server.
Server Port	The UDP port of the secondary RADIUS server.
Accounting Port	The port for packets that contains the account login or logout information for the secondary server.

IEEE 802.1x Page (Continued)	
Local RADIUS User	You can add an Account/Password for local authentication. • User name: The user name of the local RADIUS user. • Password: The password of the local RADIUS user. • VID: The VLAN ID (VID) of the local RADIUS user. Click the **Add** button to add a local RADIUS user.
Local RADIUS User List	Shows the account information, select **Remove** to remove a selected account. • User name: The user name of the local RADIUS user. • Password: The password of the local RADIUS user. • VID: The VLAN ID (VID) of the local RADIUS user.

802.1x Port Configuration

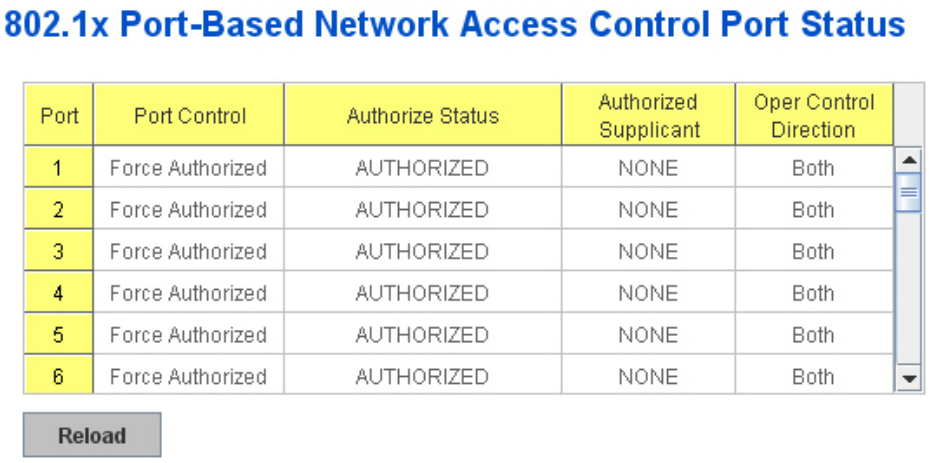
After configuring the RADIUS Server or Local user list, you also need to configure the authentication mode, authentication behavior, applied VLAN for each port, and permitted communications.



802.1x Port Configuration Page	
Port control	**Force Authorized** means that this port is authorized; the data is free to move in/out. **Force unauthorized** is just the opposite, the port is blocked. To control this port with a RADIUS server, select **Auto** for port control.
Reauthentication	If this field is enabled, the ES7528 requests the client to re-authenticate. The default time interval is 3600 seconds.
Max Request	This is the maximum times that the ES7528 allows a client request.
Guest VLAN	The permitted range for this field is 0 to 4094. If this field is set to 0, that means the port is blocked after an authentication failure. Otherwise, the port is set to Guest VLAN.
Host Mode	If there is more than one device connected to this port, set the Host Mode to **Single**, which means only the first PC to authenticate successfully can access this port. If this port is set to **Multi**, all of the devices can access this port once any one of them passes the authentication.
Admin Control Direction	Use this to determine which devices can only send data or both send and receive data.
Apply	Click **Apply** to apply the settings.
Initialize Selected	Click to set the authorization state of the selected port to initialize status.
Reauthenticate Selected	Click to send an EAP Request to the requestor to request reauthentication.
Default Selected	Click to reset the configurable IEEE 802.1x parameters of selected port to the default values.
802.1x Timeout Configuration	
Re-Auth Period(s)	Controls the re-authentication time interval (seconds), you can enter a range of 1 - 65535.
Quiet Period(s)	When authentication fails, the ES7528 waits for a period and then tries to communicate with the RADIUS server again.
Tx Period(s)	The time interval of the authentication request.
Supplicant Timeout(s)	The timeout for the client authentication.
Sever Timeout(s)	The timeout for the server response for authentication.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

802.1x Port Status

Use the 802.1x Port Status page to observe the port status for Port Control Status, Authorize Status, Authorized Supplicant, and Oper Control Direction for each port.



Warning

The ES7528 provides several types of warning features for you to remotely monitor the status of the attached devices or changes in your network. The features include Fault Relay, System Log, and SMTP Email Alert.

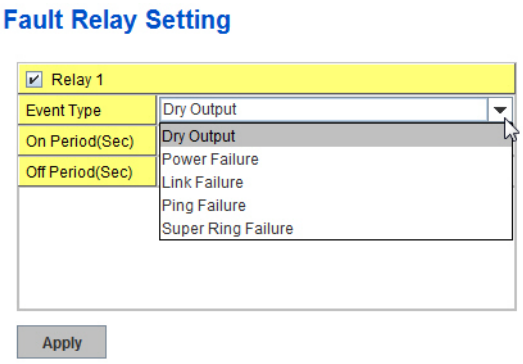
The following web pages are included in this group:

- *Fault Relay*
- *Event Selection* on Page 120
- *SysLog Configuration* on Page 121
- *SMTP Configuration* on Page 122

Optionally, you can use the CLI for configuration, see *Warnings (CLI)* on Page 193.

Fault Relay

The ES7528 provides one digital output (Relay Output). The relay contacts are energized (open) for normal operation and close under fault conditions: Fault conditions include Power Failure, Ethernet port Link Failure, Ping Failure, and Super Ring Topology changes. Each Relay can be assigned 1 fault condition.



***Relay 1*:** Click the **Relay 1** check box and then select the Event Type and its parameters.

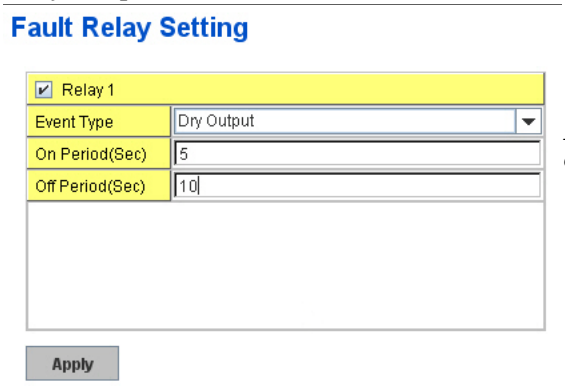
***Event Type*:** Dry Output, Power Failure, Link Failure, Ping Failure, and Super Ring Failure. Each event type has its own parameters. You can configure each Event Type. Each Relay has one event type.

***Event Type*: Dry Output**

***On Period (Sec)*:** Type the period time to turn on Relay Output. The available time period range is 0 - 4294967295 seconds.

Off Period (Sec): Type the period time to turn off Relay Output. The available time period range is 0 - 4294967295 seconds.

How to Configure: Enter turn-on and turn-off periods, when the time is reached, the system turns on or turns off the Relay Output.

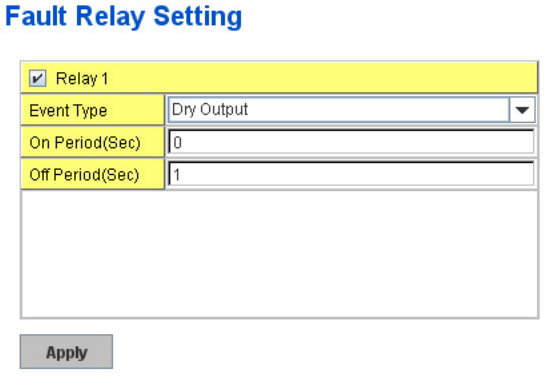


Relay turned on for 5 seconds then off for 10 seconds.

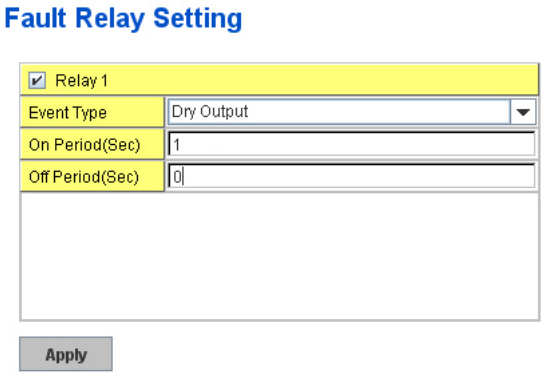
How to Turn On/Off the Other Device: Type **1** into the **On period** field and **0** into **Off Period** fields, and apply the setting, then it is triggered to form as a closed circuit.

To turn off the relay, just type **0** into the **On period** field and **1** into **Off Period** field and apply the setting, the relay is triggered to form as a open circuit.

This function is also available in the CLI SNMP management interface.



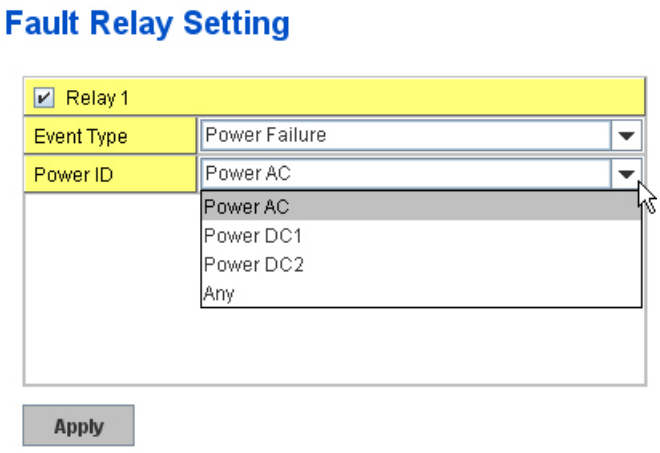
Turn on fault relay.



Turn off fault relay.

Event Type: Power Failure

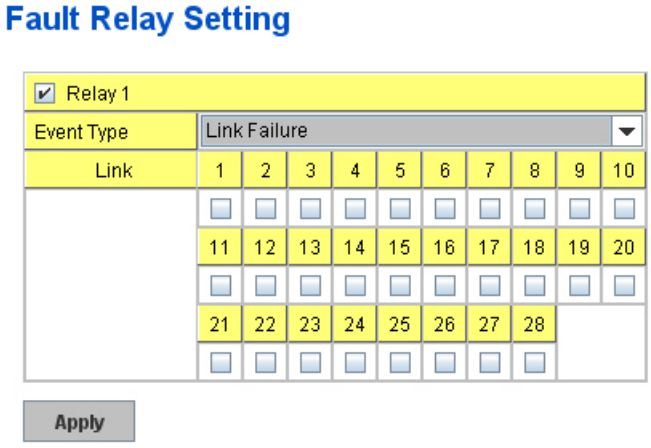
***Power ID*:** Select Power AC, Power DC1, Power DC2 or Any you want to monitor power failures. When the power is shut down or broken, the system shorts the Relay Out and light the Alarm LED.



Event Type: Link Failure

***Link*:** Select the port ID that you want to monitor.

How to Configure: Select the check boxes of the Ethernet ports you want to monitor. You can select one or multiple ports. When the selected ports are linked down or broken, the system shorts the Relay Output and light the Alarm LED.



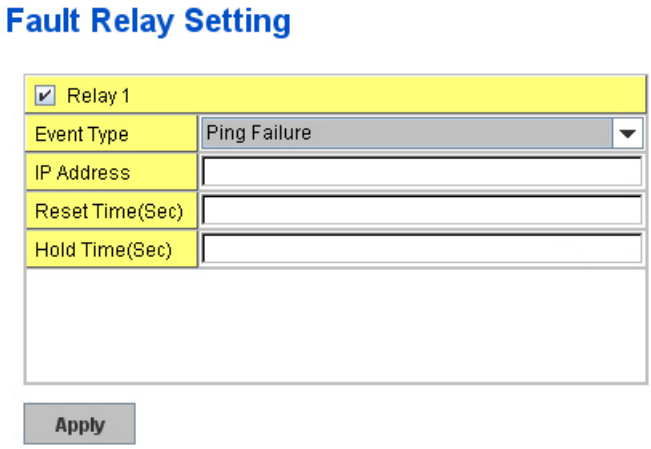
Event Type: Ping Failure

***IP Address*:** The IP address of the target device you want to ping.

***Reset Time (Sec)*:** Waiting time to short the relay output.

***Hold Time (Sec)*:** Waiting time to ping the target device for the duration of remote device boot.

How to Configure: After selecting the **Ping Failure** event type, the system turns Relay Output to the short state and continuously ping the target device. When the ping failure occurs, the switch turns the Relay Output to the open state for a period of **Reset Time**.

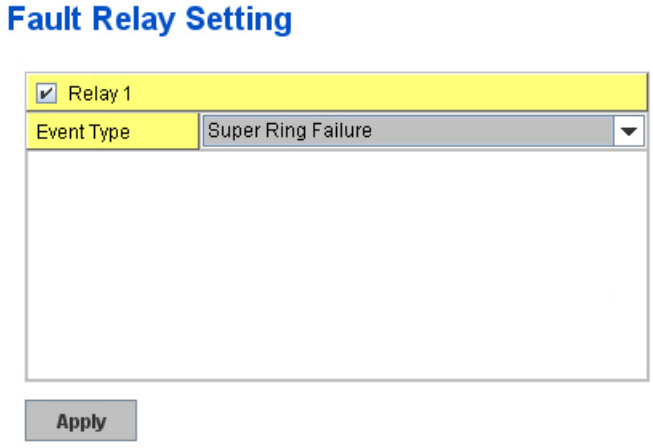


After the **Reset Time** timeout, the system turns the Relay Output to close state. After the **Hold Time** timer is timeout, the switch system starts pinging the target device. For example: Reset Time is 5 sec, Hold Time is 50 sec.

If a ping failure occurs, the ES7528 turns Relay output to the open state to emulate the power switch off for 5 second periods. After the **Reset Time** timeout, the ES7528 starts pinging the target device after 50 second periods. The period time is fora target device system to reboot. During the period, the ES7528 does not ping the target device until the **Hold Time** times out.

Event Type: Super Ring Failure

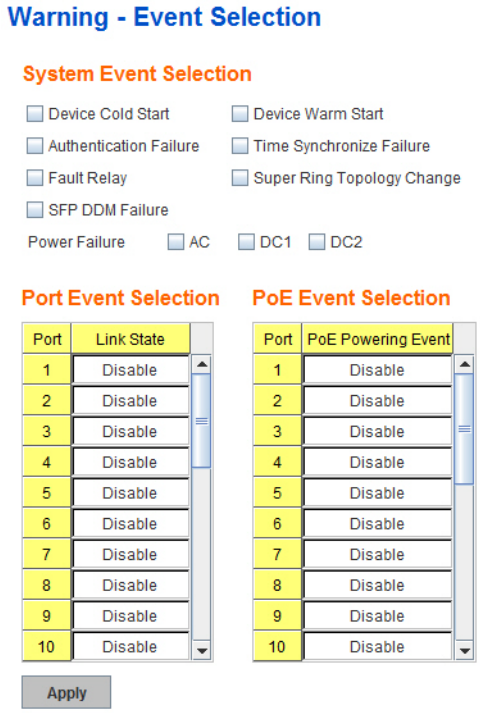
Select **Super Ring Failure** to receive notification when the Redundant Ring topology has changed. The system shorts the Relay Out and lengthen the Alarm LED.



Once you finish configuring the settings, click **Apply** to apply your configuration.

Event Selection

Event Types can be divided into three basic groups: System Events, PoE Events, and Port Events. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of specific ports.

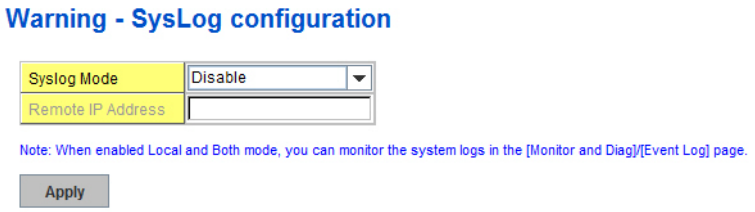


System Event	Warning is sent when….
Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or web user interface.
Authentication failure	An incorrect password or SNMP Community String is entered.
Time Synchronize Failure	Accessing the NTP Server is failing.
Fault Relay	The DO/Fault Relay is on.
Super Ring Topology Changes	Master of Super Ring has changed or backup path is activated.
SFP DDM Failure	The information read from the DDM SFP transceiver is over temperature or out the range of TX/RX power.
Power Failure	Power (AC, DC1, DC2 or Any) is failure.
Port Event	**Warning is sent when…..**
Link-Up	The port is connected to another device.
Link-Down	The port is disconnected. For example, the cable is pulled out or the opposing devices is down.
Both	The link status changed.

PoE Powering Event	Warning is sent when…..
Enable	The PoE port is powering.
Disable	The PoE port is not powering.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

SysLog Configuration

The System Log provides the system administrator ES7528 events history. There are two System Log modes provided by the ES7528, **Local** mode and **Remote** mode.



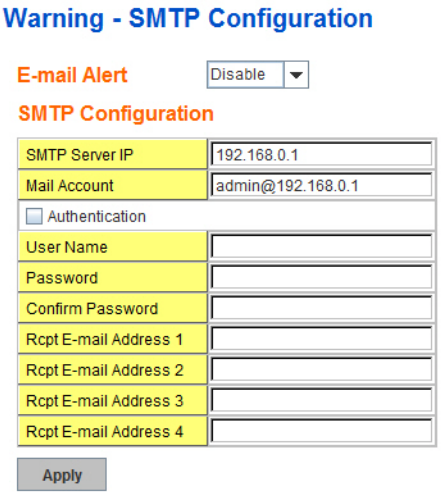
Warning - SysLog Configuration Page	
Syslog Mode	There are two system logs available: • **Local Mode**: The ES7528 prints the events that have been selected in the Event Selection page to the System Log table of the ES7528. You can monitor the system logs in the *Monitor and Diag /Event Log* page. • **Remote Mode**: Assign the IP address of the System Log server. The ES7528 sends the events that occurred in the selected in *Event Selection* page to System Log server that you assign. • **Both**: This enables both **Local** and **Remote** modes.
Remote IP Address	The IP address of the System log server.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

When enabling **Local** or **Both** modes, you can monitor the system logs in the *Monitor and Diag /Event Log* page.

SMTP Configuration

The ES7528 supports an Email Alert feature. The ES7528 sends the events that have occurred to a remote email server. The email warning conforms to the SMTP standard.

The E-mail Alert page allows you to assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If the SMTP server requests authentication, you can set up the user name and password.



SMTP Configuration Page	
SMTP Server IP Address	Enter the IP address of the email server.
Mail Account	The mail account for the SMTP server.
Authentication	Click the check box to enable password.
User Name	Enter an email account name (maximum 40 characters).
Password	Enter the password of the email account.
Confirm Password	Re-type the password of the email account.
You can set up to 4 email addresses to receive email alarm from the ES7528.	
Rcpt E-mail Address 1	The first email address to receive an email alert from the ES7528 (maximum 40 characters).
Rcpt E-mail Address 2	The second email address to receive an email alert from the ES7528 (maximum 40 characters).
Rcpt E-mail Address 3	The third email address to receive an email alert from the ES7528 (maximum 40 characters).
Rcpt E-mail Address 4	The fourth email address to receive an email alert from the ES7528 (maximum 40 characters)
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Monitor and Diag

The ES7528 provides several web user interface pages for you to monitor the status of the switch or diagnostics when encountering problems related to the ES7528. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log, and Ping.

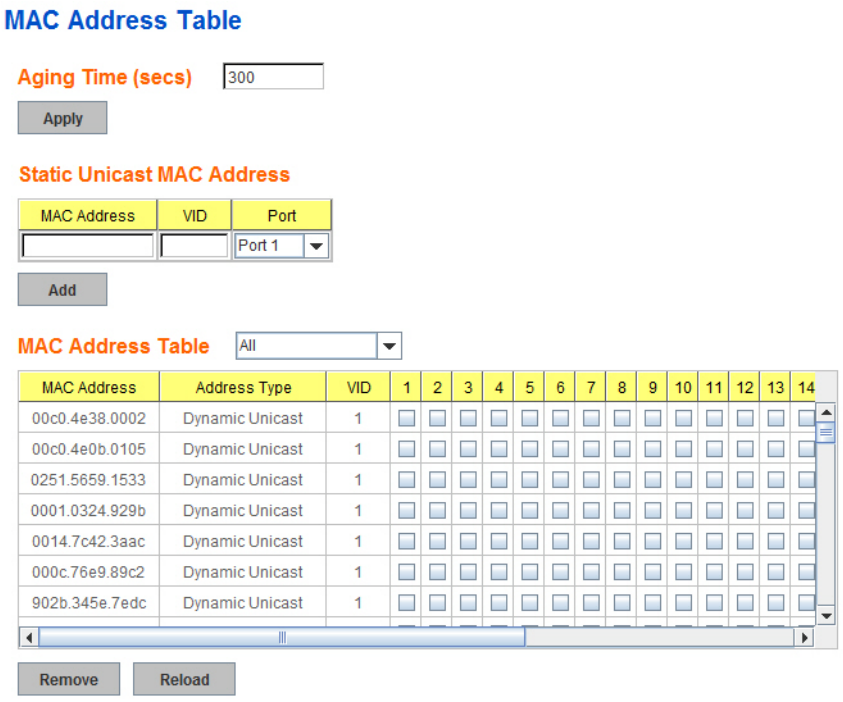
The following web pages are included in this group:

- *MAC Address Table*
- *Port Statistics* on Page 125
- *Port Mirroring* on Page 126
- *Event Log* on Page 127
- *Topology Discovery (LLDP)* on Page 128
- *Ping Utility* on Page 129

Optionally, you can use the CLI for configuration, see *Monitor and Diag (CLI)* on Page 196.

MAC Address Table

The ES7528 provides 16K entries in the MAC Address Table.You can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports.



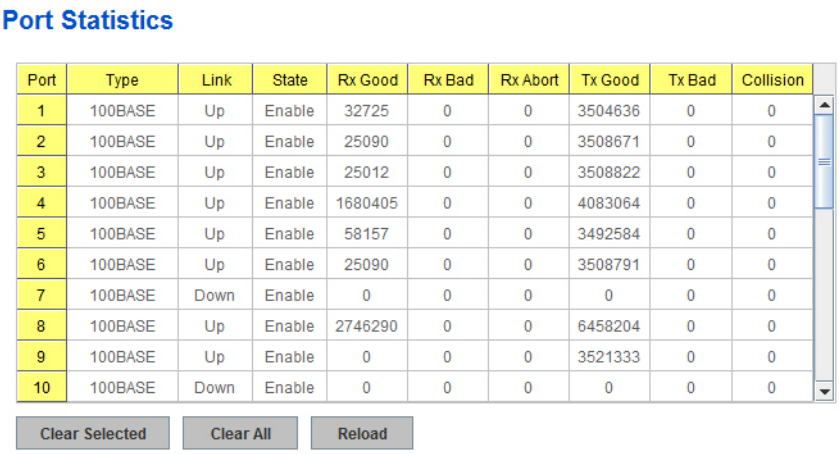
MAC Address Table Page	
Aging Time (Sec)	Each switch fabric has a size limit to write the learnt MAC address. To save more entries for a new MAC address, the switch fabric ages out a non-used MAC address entry per the Aging Time timeout. This value determines the interval that an automatically learnt MAC address entry remains valid in the forwarding database, since its last access as a source address, before being purged. The value should be increments of 15 in seconds. The minimum age time is 15 seconds. The maximum age time is 3825 seconds or almost 64 minutes. The default Aging Time is 300 seconds. If the value is set to 0, the aging function is disabled and all learned addresses remain in the database forever.
Static Unicast MAC Address	Some applications may require that you type in the static Unicast MAC address to its MAC address table. Type the MAC address (format: xxxx.xxxx.xxxx), select its VID, and Port ID, and then click **Add** to add it to MAC Address Table.
MAC Address Table	This displays all the MAC addresses learnt by the switch fabric. The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast, and Dynamic Multicast. The table allows you to sort the address by the packet types and port.
Address Types	• **Management Unicast** means the MAC address of the switch. It belongs only to the CPU port. • **Static Unicast** MAC addresses can be added and deleted. • **Dynamic Unicast MAC** is a MAC address learnt by the switch Fabric. • **Static Multicast** can be added by the CLI and can be deleted using the web user interface and CLI. • **Dynamic Multicast** appears after you enabled IGMP and the switch learnt IGMP report. • **Management Multicast** - multicast address that is configured for management purposes, such as GVRP and so on. Management entries are read-only. Dynamic and static entries can be removed.
Remove	Click to remove the static Unicast/Multicast MAC address.
Reload	Click to reload to refresh the table. The new learnt Unicast/Multicast MAC address are updated in the MAC Address Table.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Port Statistics

Use this page to view operation statistics for each port. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collisions.

Note: *If you see an increase of Bad, Abort or Collision counts, that may mean the network cable is not properly connected or the network performance of the port is poor. Check your network cable, the network interface card of the connected device, the network application, or reallocate the network traffic.*

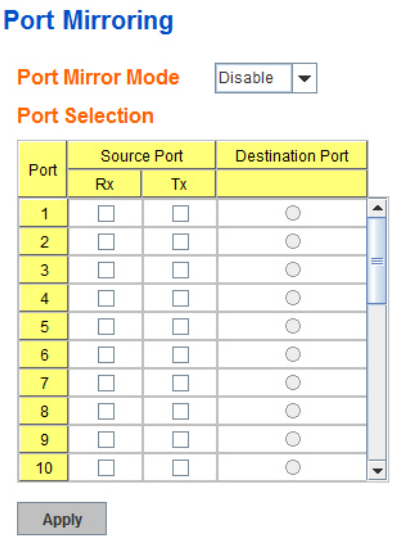
The following information provides a view of the current port statistic information.



Port Statistics Page	
Type	Indicates the port type.
Link	Indicates the link status; **Up** or **Down**.
State	Indicates the link state; **Enable** or **Disable**.
RX Good	The count of good frames received, which is the total number of received unicast, broadcast, multicast, and pause frames.
RX Bad	The count of bad frames received, which is the total number of undersize, fragment, oversize, jabber, receive errors (RxErr), and frame check sequence errors (FCSErr) frames.
RX Abort	The count of abort frames received, which is the total number of discarded and filtered frames.
TX Good	The count of good frames transmitted, which is the total number of transmitted unicast, broadcast, multicast and pause frames.
TX Bad	The count of FCSErr frames transmitted.
Collision	The count of collision frames, including single, multiple, excessive, and late collisions frames.
Clear Selected	Click to clear selected port counts.
Clear All	Click to clear all counts.
Reload	Click to reload all counts.

Port Mirroring

Port mirroring (also called *port spanning*) is a tool that allows you to mirror the traffic from one or more ports onto another port, without disrupting the flow of traffic on the original port. Any traffic that goes into or out of the **Source Ports** is duplicated at the **Destination Ports**. This traffic can then be analyzed at the Destination Port using a monitoring device or application. The network administrator typically utilizes this tool for diagnostics, debugging, or fending off attacks

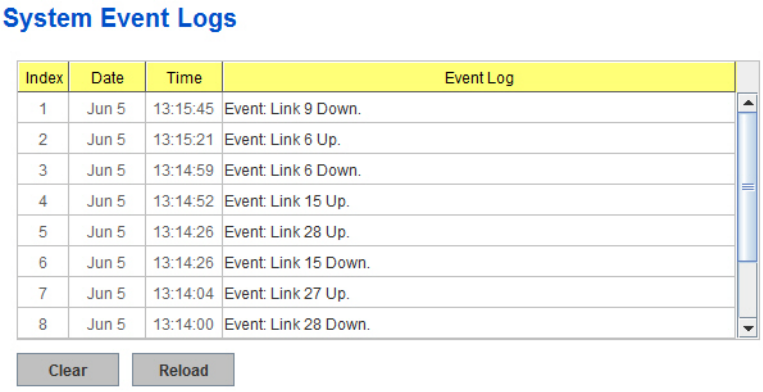


Port Mirroring Mode Page	
Port Mirror Mode	Select **Enable** or **Disable** to enable/disable port mirroring.
Source Port	This is also known as *Monitor Port*. These are the ports that you want to monitor. The traffic of all source/monitor ports is copied to destination/analysis ports. You can choose a single port, or any combination of ports, but you can only monitor them in Rx or TX only. Click the check box of the Port ID, RX, Tx or both to select the source ports.
Destination Port	This is also known as *Analysis Port*. You can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port or ports being monitored. Only one RX/TX of the destination port can be selected. The network administrator typically connects a LAN analyzer or Netxray device to this port.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Event Log

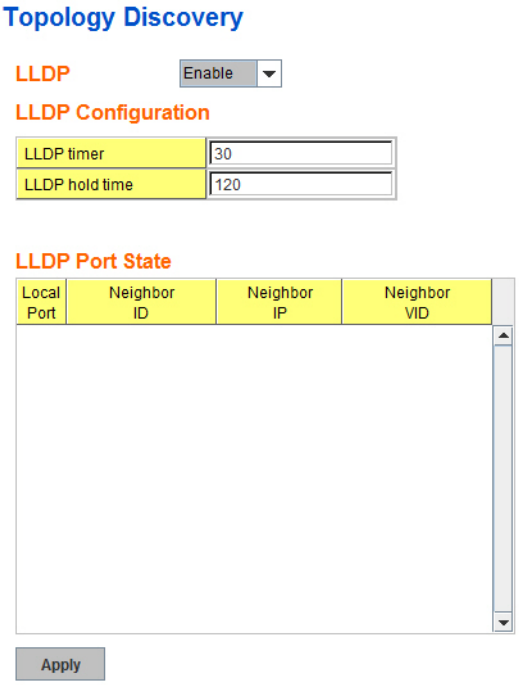
The System Log feature was introduced in *SysLog Configuration* on Page 121. When **System Log Local** mode is selected, the ES7528 records events that occurred in the local log table. This page shows this log table. The entry includes the index, occurred data and time, and content of the events.

Click **Clear** to clear the entries. Click **Reload** to refresh the table.



Topology Discovery (LLDP)

The ES7528 supports topology discovery or LLDP (IEEE 802.1AB Link Layer Discovery Protocol) functionality that can help to discovery multi-vendor's network devices on the same segment by a network monitoring system (NMS) that supports LLDP functionality.



With LLDP functionality, NMS can easily maintain the topology map, display port ID, port description, system description, and VLAN ID. Once a link failure occurs, the topology changes the events that can be updated to the NMS as well. The LLDP Port State can display the neighbor ID and IP learnt from the connected devices.

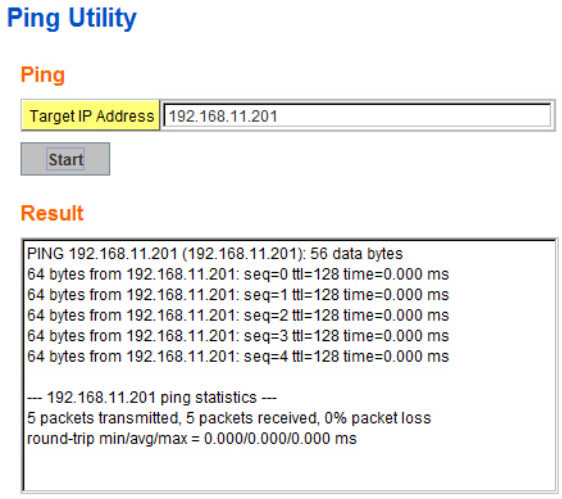
Topology Discovery Page	
LLDP	Select **Enable/Disable** to enable/disable LLDP function.
LLDP Configuration	
LLDP timer	This is the interval time of each LLDP in seconds; valid values are from 5 to 254. The default is 30 seconds.
LLDP hold time	The Time to Live (TTL) timer. The LLDP state expires when the LLDP is not received by the hold time. The default is 120 seconds. and the range is from 10 to 255.
LLDP Port State	
Local Port	The current port number that linked with network device.
Neighbor ID	The MAC address of the peer device on the same network segment.
Neighbor IP	The IP address of the peer device on the same network segment.
Neighbor VID	The VLAN ID of the peer device on the same network segment.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 131), if you want to maintain these settings if the ES7528 is powered off.*

Ping Utility

This page provides a **Ping Utility** to ping a remote device and check whether the device is alive or not.

Type the **Target IP** address of the target device and click **Start** to start the ping.

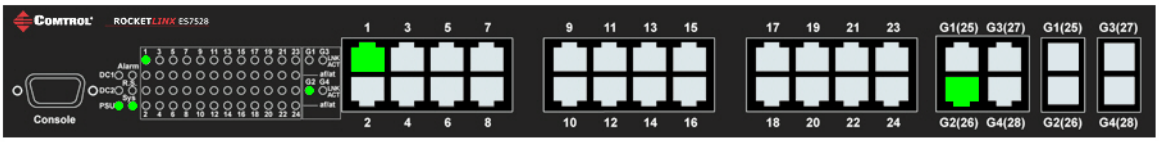
After few seconds, you can see the result in the **Result** field.



Device Front Panel

The **Device Front Panel** allows you to see the LED status of the ES7528.

Device Front Panel



LED Name	LED On/Link Up	LED Off/Link Down
DC1 (Power) DC2 (Power)	Green: Power Green: Power	Black: No power
PSU (AC power)	Green: Power	Black: No power
Alarm	Green: Alarm activated	Black: Not activated
R.S. (Super-Ring Redundancy Manager)	Green: Ring state is normal	Black: Ring feature not enabled
Sys (System)	Green	Black: System not ready
LEDs 1-24	Green: Link active	Black: Not connected
LEDs G1-G4	Green	Black: Not connected

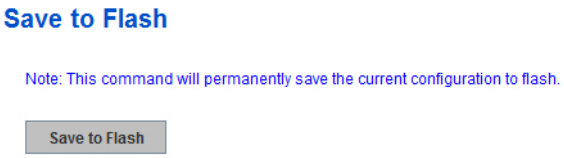
Note: *There is not a CLI command for this feature. If you can view the physical LEDs, you can use the* *LED Descriptions on Page 14**, which provide detailed LED information.*

Save to Flash

The **Save Configuration** pages allows you to save any configuration you made to the flash.

Powering off the switch without clicking **Save Configuration** causes loss of the new settings. Applying changes on web user interface pages do not save the changes to the flash.

After selecting **Save Configuration**, click **Save to Flash** to save your new configuration.

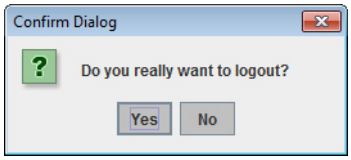


Optionally, you can use the CLI, see *Saving to Flash (CLI)* on Page 199.

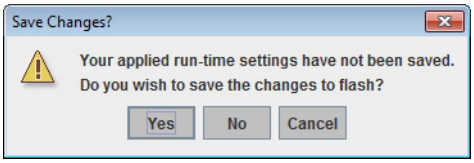
Logout

Click the **Logout** option in the web user interface to manually logout the web connection.

If you have saved your changes, click **Yes** to logout, **No** to remain the web user interface.



If you did not save your changes, you can save your changes when you logout.



Configuration Using the Command Line Interface (CLI)

Overview

The ES7528 provides in-band and out-band configuration methods:

- Out-band management means that you configure the ES7528 using the RS-232 console cable and the Command Line Interface (CLI) to access the ES7528 without attaching an admin PC to the network. You can use out-band management if you lose the network connection to the ES7528.
- In-band management means that you connect remotely using the ES7528 IP address through the network. You can remotely connect with the ES7528 embedded Java applet web user interface or a Telnet console and the CLI.

If you are planning on using in-band management, you need to program the ES7528 IP address to meet your network requirements. The easiest way to configure the IP address is using a Windows system and NetVision, which is discussed in *Programming Network Information* on Page 18.

If you want to use the web user interface for configuration, see *Configuration Using the Web User Interface* on Page 23.

Use the following procedures to access the ES7528 using the CLI:

- *Using the Serial Console*
- *Using a Telnet Console*

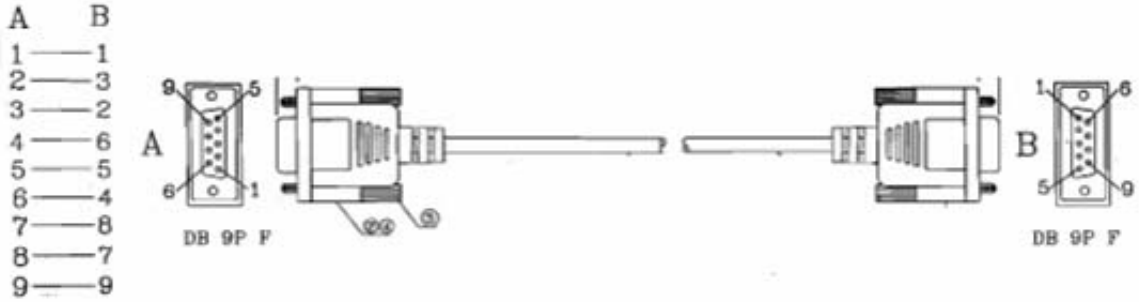
This section contains information about the following groups of commands:

Using the Serial Console

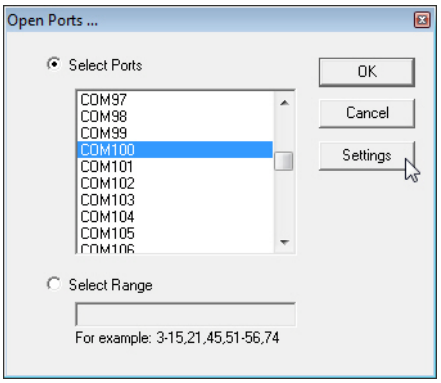
Comtrol provides one RS-232 DB9 console cable with the ES7528.

Note: *A system COM port is required to use a serial console connection. If you do not have an available COM port, use the Using a Telnet Console procedure on Page 135.*

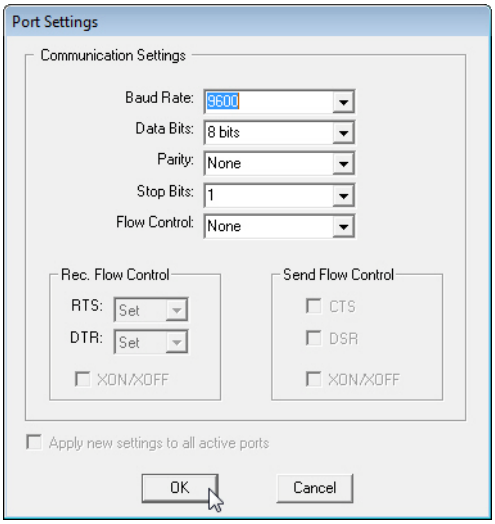
1. Attach one end of the RS-232 DB9 connector to your PC COM port and connect the other end to the **Console** port of the ES7528. If you misplace the cable, you can use this console cable pin assignment or purchase a null-modem cable.



2. Start a terminal program such as HyperTerminal or the Comtrol Test Terminal program. You can download Test Terminal from the FTP site.



   - Test Terminal - WCom2 (Windows XP through Windows 7)
     - Unzip Test Terminal and place it in a location that you can execute an application.
     - Execute **Wcom2.exe**.
     - Click the **File** menu, the **Open Port** option and then click the appropriate COM port number.
     - Click **Settings**, use the values in the following table, and then click **Ok**.



Serial Settings	Value
Baud Rate	9600
Data bits	8
Parity	None
Stop Bit	1
Flow Control	None

     - Click **Ok**.
     - Press the cursor in the Terminal window and press the **Enter** key.

- HyperTerminal (Windows XP, *unless installed manually*)
  - *Windows XP*: Go to **Start -> Program -> Accessories -> Communications -> HyperTerminal**
  - Enter a name for the new console connection and click **OK**.
  - Enter the IP address in the **Host Address** text box.
  - Select **TCP/IP (Winsock)** in the **Connect using** drop-list and click **Ok**.
  - Set the serial settings using the *Serial Settings* table (above).
  - Press the **Enter** key in the Terminal window.
  - After it is connected, you can see the *Switch login* request, go to Step 3.

3. Log in to the switch. The default user name is **admin**, password, **admin**.

```
Switch login: admin
Password:


Switch (version 1.0-20110126-11:38:53).


Switch>
```

```
Switch login: admin
Password:


Switch (version 1.3-20121211-16:25:00).


Switch>
```

4. If necessary, configure the IP address for your network. The following example shows how to program an IP address of 192.168.11.252 with a Class B subnet mask (255.255.0.0).

```
Switch> enable
Switch# configure terminal
Switch(config)# int vlan1
Switch(config-if)# ip address 192.168.11.252/16
```

Using a Telnet Console

The ES7528 supports a Telnet console or SSH console with the Command Line Interface (CLI), which is the same as what you see using the RS-232 console port. The SSH connection can secure all the configuration commands you send to the ES7528.

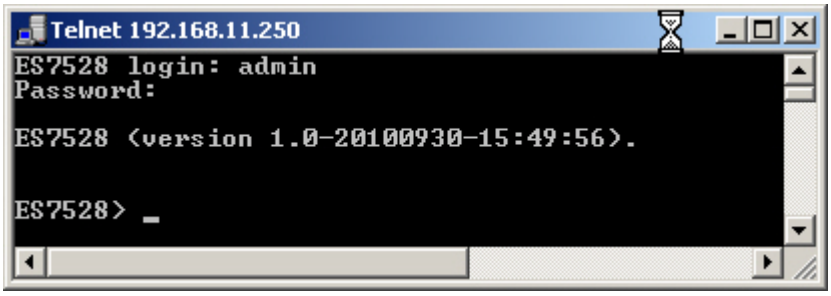
SSH is a client/server architecture while the ES7528 is the SSH server. When you want to make SSH connection with the ES7528, you may need to download an SSH client tool.

The following subsections provide information for *Telnet* or an *SSH Client*.

Telnet

The following shows how to open a Telnet connection to the ES7528 using Windows XP.

1. Go to **Start -> Run -> cmd** and then press **Enter**.
2. Type **Telnet 192.168.250.250** (or the IP address of the ES7528) and then press **Enter**.
3. Enter the *Login Name* and *Password*. The default login name and password are **admin.**



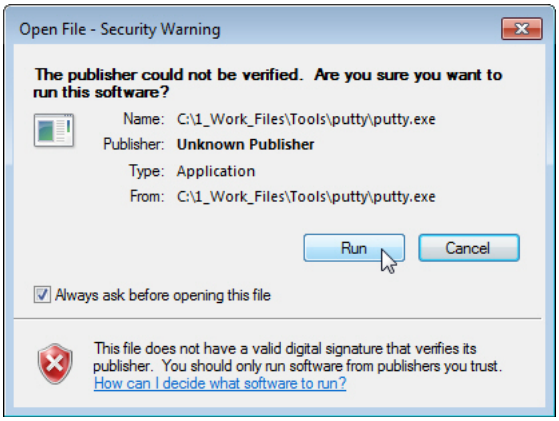
All the commands you see in SSH are the same as the CLI commands you see through the RS-232 console.

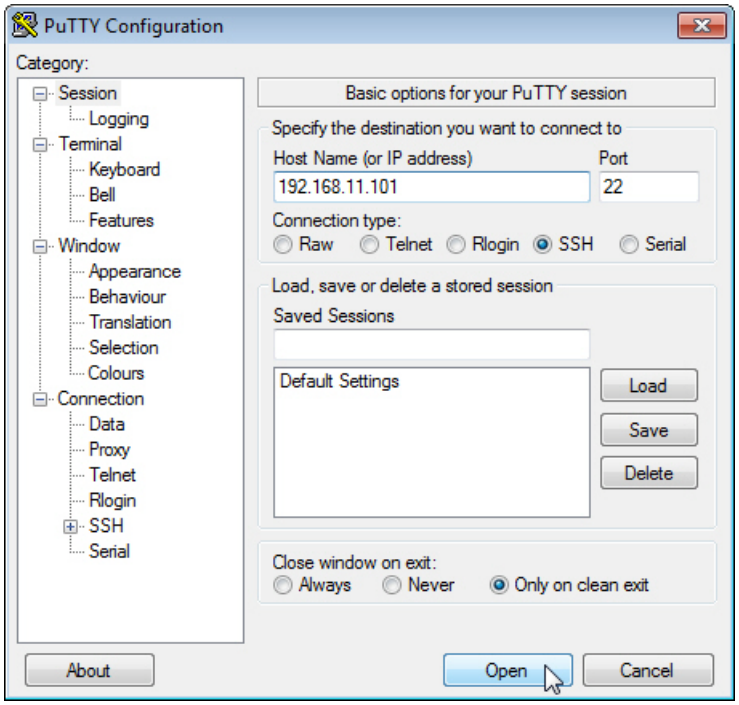
SSH Client

There are many free, sharewares, trials or charged SSH clients you can find on the internet. For example, PuTTY is a free and popular Telnet/SSH client. The following procedures shows how to login with SSH and PuTTY.

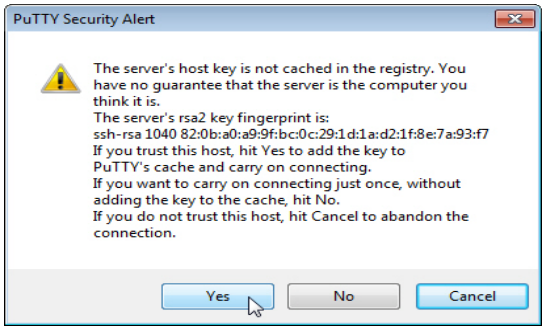
1. Download PuTTY (the Telnet and SSH client itself) from:

   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
2. Click **Run** to start PuTTY.
3. In the **Session** configuration, enter the **Host Name** (IP address of the ES7528), **Port number** (default = 22), click **SSH** for the protocol, and then click **Open** to start the SSH session console.



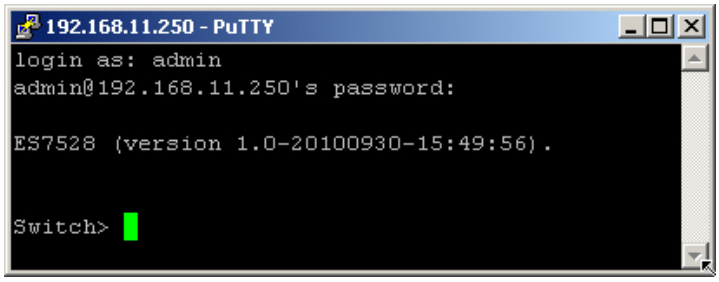


4. After click **Open**, you the cipher information displays in the popup screen. Click **Yes** to accept the Security Alert.



   After few seconds, the SSH connection to the ES7528 opens.

5. Enter the *Login Name* and *Password*. The default login name and password are **admin**.



All the commands you see in SSH are the same as the CLI commands you see through the RS-232 console.

Command Line Interface Introduction

The Command Line Interface (CLI) is the user interface to the ES7528 embedded software. You can view the system information, show the status, configure the switch, and receive a response back from the system by keying in a command.

There are several different command modes. Each command mode has its own access ability, available command lines and uses different command lines to enter and exit. These modes are:

- *User EXEC Mode* on Page 138, which includes commands to ping or telnet to a remote device, and show some basic information and to access *Privileged EXEC* mode
- *Privileged EXEC Mode* on Page 141, which provides a view current configuration, reset default, reload switch, show system information, save configuration, and access *Global Configuration* mode
- *Global Configuration Mode* on Page 142, which you can use configure all ES7528 features and access to one of the *Interface Configuration* modes
- *(Port) Interface Configuration* on Page 143, which can be used to configure port settings
- *(VLAN) Interface Configuration* on Page 144, which can be used to configure the settings for a specific VLAN

Refer to *Configuration Using the Command Line Interface (CLI)* on Page 133 to access the CLI.

User EXEC Mode

When you login to the ES7528 with the CLI, you are in *User EXEC* mode.

In User EXEC Mode, you can ping, telnet to a remote device, and show some basic information.

Type the command and press **Enter**:

- **enable** to access *Privileged EXEC* mode (*Privileged EXEC Mode* on Page 141).
- **exit** to logout.
- **?** to see the command list.

```
Switch>
  enable       Turn on privileged mode command
  exit         Exit current mode and down to previous mode
  list         Print command list
  ping         Send echo messages
  quit         Exit current mode and down to previous mode
  show         Show running system information
  telnet       Open a telnet connection
  traceroute   Trace route to destination
```

- **list** to review the *User EXEC* mode commands and corresponding options.

For the complete list of commands with options, refer to *User EXEC Mode* on Page 201.

Accessing the Options for a Command

The following example illustrates how to view the description and options for a command. This example illustrates the **show** command and the firmware version displayed may not reflect your firmware version.

Note: *The* ***?*** *does not appear on the screen.*

1. If you type **show?** (without a space between **show** and the **?**; do not press the **Enter** key) the ES7528 provides a basic description of that command.

```
Switch login: admin
Password:

Switch  (version 2.7 -20130314 - 15:23:41)
switch> show
  show  Show running system information
```

2. If you type **show ?** (with a space between **show** and the **?**; do not press the **Enter** key) the ES7528 provides information about the options for that command.

```
Switch> show
  gvrp           GARP VLAN Registration Protocol
  ip             IP information
  version        Displays ISS version
Switch> show
```

3. Type **show ip ?** (with a space between **show** and the **?**, do not press the **Enter** key) to review the options for **ip**.

```
Switch> show ip
  forwarding  IP forwarding status
  route       IP routing table
```

4. Type **show ip route** and press the **Enter** key to view the IP routing tables for the ES7528.

```
Switch> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.250.1, vlan1
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.168.0.0/16 is directly connected, vlan1
```

5. If you type **list** and press **Enter**, the ES7528 provides you information about all of the commands and options for a mode. The following example shows the available commands and their options for *User EXEC* mode.

```
ES7528> list
  enable
  exit
  list
  ping A.B.C.D
  ping WORD
  ping X:X::X:X
  quit
  show gvrp statistics [IFNAME]
  show ip forwarding
  show ip route
  show ip route A.B.C.D
  show ip route A.B.C.D/M
  show ip route supernets-only
  show version
  telnet WORD
  telnet WORD PORT
  traceroute WORD
```

Privileged EXEC Mode

If you type **enable** in *User EXEC* mode, you can access *Privileged EXEC* mode. In this mode, the ES7528 allows you to view current configuration, reset default, reload switch, show system information, save configuration, and enter *Global Configuration* mode.

Type the following commands and press the **Enter** key:

- **configure terminal** to access *Global Configuration* mode (*Global Configuration Mode* on Page 142).
- **exit** to close the CLI.
- **?** to see the command list.
- **list** to review the *Privileged EXEC* mode commands and corresponding options.

For the complete list of commands and options, refer to *Privileged EXEC Mode* on Page 202.

```
Switch>enable
Switch#
  archive      manage archive files
  clear        Reset functions
  clock        Configure time-of-day clock
  configure    Configuration from vty interface
  copy         Copy from one file to another
  debug        Debugging functions
  disable      Turn off privileged mode command
  dot1x        IEEE 802.1x standard access security control
  end          End current mode and change to enable mode
  exit         Exit current mode and down to previous mode
  list         Print command list
  mac          MAC interface commands
  no           Negate a command or set its defaults
  pager        Terminal pager
  ping         Send echo messages
  quit         Exit current mode and down to previous mode
  reboot       Reboot system
  reload       copy a default-config file to replace the current one
  show         Show running system information
  telnet       Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
  write        Write running configuration to memory, network, or terminal
```

Global Configuration Mode

If you type **configure terminal** in *Privileged EXEC* mode, you can then access *Global Configuration* mode. In *Global Configuration* mode, you can configure all ES7528 features. Type the following commands and press the **Enter** key:

- **interface *IFNAME/VLAN***, to access the corresponding *Interface Configuration* mode.
- **exit** to return to *Privileged EXEC* mode.
- **?** to see the command list.
- **list** to review the *Global Configuration* mode commands and corresponding options.

The following is a list of available command lists of *Global Configuration* mode. For the complete list of commands and options, refer to *Global Configuration Mode* on Page 207..

```
Switch# configure terminal
Switch(config)#
  access-list         Add an access list entry
  administrator       Administrator account setting
  clock               Configure time-of-day clock
  default             Set a command to its defaults
  dot1x               IEEE 802.1x standard access security control
  end                 End current mode and change to enable mode
  exit                Exit current mode and down to previous mode
  gmrp                GMRP protocol
  gvrp                GARP VLAN Registration Protocol
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  IP information
  ipv6                IP information
  lacp                Link Aggregation Control Protocol
  list                Print command list
  lldp                Link Layer Discovery Protocol
  log                 Logging control
  mac                 Global MAC configuration subcommands
  mac-address-table   Mac address table
  mirror              Port mirroring
  modbus              Modbus TCP slave
  nameserver          DNS Server
  netvision           NetVision protocol
  no                  Negate a command or set its defaults
  ntp                 Configure NTP
  poe                 Configure Power over Ethernet
  ptpd                IEEE1588 Precision Time Protocol
  qos                 Quality of Service (QoS)
  redundant-ring      Configure redundant ring
  relay               relay output type information
  router              Enable a routing process
  service             System service
  sfp                 Small form-factor pluggable
  smtp-server         SMTP server configuration
  snmp-server         SNMP server
  spanning-tree       spanning tree algorithm
  system              System setting
  trunk               Trunk group configuration
  vlan                Virtual LAN
  warning-event       Warning event selection
  write-config        Specify config files to write to
```

(Port) Interface Configuration

When you type **interface *IFNAME*** in *Global Configuration* mode, you can access *Interface Configuration* mode. In this mode you can configure port settings.

The port interface names for the Fast Ethernet ports are fa1 through fa24. The port interface names for Gigabit Ethernet port are gi25 through gi28.

Type the interface name, for example fa1, when you want to enter certain interface configuration mode. Type the following commands and press the **Enter** key:

- **exit** to return to *Privileged EXEC* mode.
- **?** to see the command list.
- **list** to review the *Interface Configuration* mode commands and corresponding options. The following list is the available commands for the *Port Interface Configuration* mode.

For the complete list of commands and options, refer to *Port Interface Configuration Mode* on Page 212**.**

```
Switch(config)# interface fa1
Switch(config-if)#
  acceptable         Configure 802.1Q acceptable frame types of a port
  auto-negotiation   Enable auto-negotiation state of a given port
  description        Interface specific description
  dot1x              IEEE 802.1x standard access security control
  duplex             Specify duplex mode of operation for a port
  end                End current mode and change to enable mode
  ethertype          Ethertype
  exit               Exit current mode and down to previous mode
  flowcontrol        Set flow-control value for an interface
  garp               General Attribute Registration Protocol
  ingress            IEEE 802.1Q ingress filtering features
  ip                 Interface Internet Protocol config commands
  lacp               Link Aggregation Control Protocol
  list               Print command list
  loopback           Specify loopback mode of operation for a port
  mac                MAC interface commands
  mdix               Enable mdix state of a given port
  no                 Negate a command or set its defaults
  poe                Configure Power over Ethernet
  qos                Quality of Service (QoS)
  quit               Exit current mode and down to previous mode
  rate-limit         Rate limit configuration
  sfp                Small form-factor pluggable
  shutdown           Shutdown the selected interface
  spanning-tree      spanning-tree protocol
  speed              Specify the speed of a Fast Ethernet port or a
                      Gigabit Ethernet port
  storm-control      Enables packet flooding rate limiting features
  switchport         Set switching mode characteristics
```

(VLAN) Interface Configuration

If you type **interface VLAN *VLAN-ID*** in *Global Configuration* mode, you can access *VLAN Interface Configuration* mode. In this mode, you can configure the settings for the specific VLAN.

The VLAN interface name of VLAN 1 is VLAN 1, VLAN 2 is VLAN 2.

Type **exit** to return to the previous mode. Type **?** to see the available command list.

For the complete list of commands and options, refer to *VLAN Interface Configuration Mode* on Page 214.

```
Switch(config)# interface vlan 1
Switch(config-if)#
  description  Interface specific description
  end          End current mode and change to enable mode
  exit         Exit current mode and down to previous mode
  ip           Interface Internet Protocol config commands
  ipv6         Interface Internet Protocol config commands
  list         Print command list
  no           Negate a command or set its defaults
  quit         Exit current mode and down to previous mode
  shutdown     Shutdown the selected interface
```

Command Mode Summary

This table is a summary of the five command modes.

Mode: Main Function	Access and Exit Mode	Prompt
User EXEC: This is the first level of access. You can ping, telnet a remote device, and show some basic information.	• Access *User EXEC* mode: Login successfully. • Exit: **exit** to logout. • Next mode: Type **enable** to enter *Privileged EXEC* mode.	`Switch>`
Privileged EXEC: Allows you to view current configuration, reset the default values, reload the switch, show system information, save configuration and enter *Global Configuration* mode.	• Access *Privileged EXEC* mode: Type **enable** in *User EXEC* mode. • Exec: Type **disable** to exit to *User EXEC* mode. • Type **exit** to logout. • Next mode: Type **configure terminal** to enter *Global Configuration* mode.	`Switch#`
Global Configuration: Configure all of the features that the ES7528 provides.	• Access *Global Configuration* mode: Type **configure terminal** in *Privileged EXEC* mode. • Exit: Type **exit** or **end** or press **Ctrl-Z** to exit. • Next mode: Type **interface IFNAME/ VLAN *VID*** to enter *Interface Configuration* mode.	`Switch(config)#`
Port Interface Configuration: Configure port related settings.	• Access *Port Interface Configuration* mode: Type **interface *IFNAME*** in global configuration mode. • Exit: Type **exit** or **Ctrl+Z** to *Global Configuration* mode. • Type **end** to return to *Privileged EXEC* mode.	`Switch(config-if)#`

Mode: Main Function	Access and Exit Mode	Prompt
VLAN Interface Configuration: Configure settings for a specific VLAN.	• Access *VLAN Interface Configuration* mode: Type **interface VLAN *VID*** in *Global Configuration* mode. • Exit: Type **exit** or **Ctrl+Z** to return to *Global Configuration* mode. • Type **end** to return to *Privileged EXEC* mode.	`Switch(config-vlan)#`

The following are useful commands to save you typing time and to avoid typing errors.

Press **?** to see all of the available commands in a mode. It helps you to see the next command you can type.

```
Switch(config)# interface (?)
  IFNAME    Interface's name
  vlan      Select a vlan to configure
```

Type a *Character***?** (shown below) to see all of the available commands starting with this character.

```
Switch(config)# a?
  access-list     Add an access list entry
  administrator   Administrator account setting
```

Press the Tab key, which helps you to input the command quicker. If there is only one available command in the next, click the **Tab** key to help finish the typing.

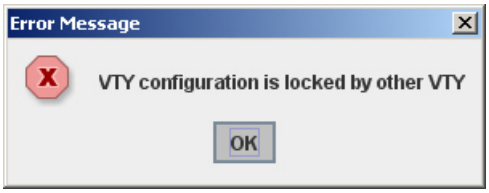
```
Switch# co (tab) (tab)
Switch# configure terminal

Switch(config)# ad (tab)
Switch(config)# administrator
```

Key Combination	Function
Ctrl+C	To stop executing the unfinished command.
Ctrl+S	To lock the screen of the terminal - you cannot input any command.
Ctrl+Q	To unlock the screen which is locked by **Ctrl+S**.
Ctrl+Z	To exit *Configuration* mode.

VTY Configuration Locked (Error Message)

An alert message appears when multiple users are attempting to configure the ES7528. If the administrator is in *Configuration* mode, then the web users cannot change settings. The ES7528 allows only one administrator to configure the switch at a time.



Basic Settings (CLI)

The Basic Setting group provides you with the ability to configure switch information, IP address, User name/ Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

Optionally, you can use the web user interface for configuration, see *Basic Settings* on Page 38.

This table provides detailed information about the CLI commands for basic settings.

Switch Setting	

System Name	`Switch(config)# hostname`
	`  DWORD  Network name of this system`
	`Switch(config)# hostname ES7528`
	`Switch(config)#`

System Location	`Switch(config)# snmp-server location Minnesota`
System Contact	`Switch(config)# snmp-server contact support@comtrol.com`

Display	`Switch# show snmp-server name`
	`ES7528`
	`Switch# show snmp-server location`
	`Minnesota`
	`Switch# show snmp-server contact`
	`support@comtrol.com`
	`Switch> show version`
	`Loader Version : 0.3.0.9`
	`Firmware Version : 1.0-20100930-15:49:56`
	`Hardware Version : 0.1`
	`CPLD Version : 0.1`
	`Switch# show hardware mac`
	`MAC Address: 00C04E320001`

Admin Password	

User Name and Password	`Switch(config)# administrator`
	`  NAME  Administrator account name`
	`Switch(config)# administrator admin`
	`  PASSWORD  Administrator account password`
	`Switch(config)# administrator admin admin`
	`Change administrator account admin and password admin success.`

Display	`Switch# show administrator`
	`Administrator account information`
	`name: admin`
	`password: admin`

IP Configuration	
IP Address/Mask (192.168.250.250, 255.255.255.0 The enabled bit of the subnet mask is used to represent the number displayed in the web user interface. For example, 8 represents: 255.0.0.0, 16 represents: 255.255.0.0, 24 represents:255.255.255.0.	Switch(config)# int vlan 1 Switch(config-if)# ip address dhcp Switch(config-if)# ip address 192.168.250.8/24 Switch(config-if)# ip dhcp client Switch(config-if)# ip dhcp client renew
Gateway	Switch(config)# ip route 0.0.0.0/0 192.168.250.254/24
Remove Gateway	Switch(config)# no ip route 0.0.0.0/0 192.168.250.254/24
Display	Switch# show running-config …… ! interface vlan1 ip address 192.168.250.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.250.254/24 !
Time Setting	
NTP Server	Switch(config)# ntp peer enable disable primary secondary Switch(config)# ntp peer primary IPADDR Switch(config)# ntp peer primary 192.168.250.250
Time Zone	Switch(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ***Note:*** *By typing clock timezone?, you can see the timezone list. Then choose the number of the timezone you want to select.*
IEEE 1588	Switch(config)# ptpd run <cr> preferred-clock Preferred Clock slave Run as slave

Time Setting (Continued)	

Display	Switch # sh ntp associations
	Network time protocol
	  Status: Disabled
	  Primary peer: N/A
	  Secondary peer: N/A
	Switch # show clock
	Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
	
	Switch # show clock timezone
	clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
	
	Switch# show ptpd
	PTPd is enabled
	Mode: Slave

Jumbo Frame	
Jumbo Frame	Switch(config)# system mtu jumbo <1500-9216> Switch(config)# system mtu jumbo 9000
DHCP Server	
DHCP Server configuration	Enable DHCP Server on ES7528 Switch Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Configure DHCP network address pool Switch(config-dhcp)#network 50.50.50.0/4 -(network/mask) Switch(config-dhcp)#default-router 50.50.50.1
Lease time configure	Switch(config-dhcp)#lease 300 (300 sec)
DHCP Relay Agent	Enable DHCP Relay Agent Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option Enable DHCP Relay policy Switch(config-dhcp)# ip dhcp relay information policy replace drop Relay Policy keep Drop/Keep/Replace option 82 field replace

DHCP Server (cont.)	
Show DHCP server information	Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.17.0/24 default-router:192.168.17.254 lease time:300 Excluded Address List IP Address --------------- (list excluded address) Manual Binding List IP Address MAC Address --------------- --------------- (list IP & MAC binding entry) Leased Address List IP Address MAC Address Leased Time Remains --------------- --------------- -------------------- (list leased Time remain information for each entry)
DHCP Commands	Switch(config)# router dhcp Switch(config-dhcp)# default-router DHCP Default Router end Exit current mode and down to previous enable mode exit Exit current mode and down to previous mode ip IP protocol lease DHCP Lease Time list Print command list network dhcp network no Remove quit Exit current mode and down to previous mode service Enable service
DHCP Server Enable	Switch(config-dhcp)# service dhcp <cr>
DHCP Server IP Pool (Network/Mask)	Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME second Switch(config-dhcp)# lease 1000 (1000 second)
DHCP Server – Excluded Address	Switch(config-dhcp)# ip dhcp excluded-address A.B.C.D IP address Switch(config-dhcp)# ip dhcp excluded-address 192.168.10.123 <cr>

DHCP Server (cont.)	

DHCP Server – Static IP and MAC binding	`Switch(config-dhcp)# ip dhcp static`
	`  MACADDR  MAC address`
	`Switch(config-dhcp)# ip dhcp static 00C0.4E32.0001`
	`  A.B.C.D  leased IP address`
	`Switch(config-dhcp)# ip dhcp static 00C0.4E32.0001 192.168.10.99`

DHCP Relay – Enable DHCP Relay	`Switch(config-dhcp)# ip dhcp relay information`
	`  option  Option82`
	`  policy  Option82`
	`Switch(config-dhcp)# ip dhcp relay information option`

DHCP Relay – DHCP policy	`Switch(config-dhcp)# ip dhcp relay information policy`
	`  drop  Relay Policy`
	`  keep  Drop/Keep/Replace option82 field`
	`  replace`
	`Switch(config-dhcp)# ip dhcp relay information policy drop`
	`  <cr>`
	`Switch(config-dhcp)# ip dhcp relay information policy keep`
	`  <cr>`
	`Switch(config-dhcp)# ip dhcp relay information policy replace`
	`  <cr>`

DHCP Relay – IP Helper Address	`Switch(config-dhcp)# ip dhcp helper-address`
	`  A.B.C.D`
	`Switch(config-dhcp)# ip dhcp helper-address 192.168.10.200`

Reset DHCP Settings	`Switch(config-dhcp)# ip dhcp reset` `  <cr>`
Backup and Restore	

Backup Startup Configuration File	`Switch# copy startup-config tftp: 192.168.250.33/default.conf`
	`Writing Configuration [OK]`
	Note: *To backup the latest startup configuration file, you should save current settings to flash first. You can refer to Save to Flash on Page 131 to see how to save settings to the flash.*
	In the example above, 192.168.250.33 is the TFTP server's IP and default.conf is name of the configuration file. Your environment may use different IP addresses or different file name. Type target TFTP server IP or file name in this command.

Restore Configuration	`Switch# copy tftp: 192.168.250.33/default.conf startup-config`
Show Startup Configuration	`Switch# show startup-config`
Show Running Configuration	`Switch# show running-config`

Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.11.33 ES7528.bin Firmware upgrading, don't turn off the switch! Tftping file ES7528.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Factory Default	
Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

Port Configuration (CLI)

The Port Configuration group allows you to enable/disable port state, or configure port auto-negotiation, speed, duplex, flow control, rate limit control, and port aggregation settings. It also allows you to view port status and aggregation information.

Optionally, you can use the web user interface for configuration, see *Port Configuration* on Page 61.

This table provides detailed information about the CLI commands for port configuration.

Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to DOWN Port1 Link Change to UP interface fastethernet1 is up now. Switch(config-if)# Port1 Link Change to UP Switch(config)# sfp ddm Digital diagnostic and monitoring Switch(config)# sfp ddm Eject Reject DDM SFP Switch(config)# sfp ddm eject → eject SFP DDM transceiver all All DDM interface Example: Switch(config)# sfp ddm eject all DDM SFP on Port 9 normally ejected. DDM SFP on Port 9 normally ejected. All DDM SFP normally ejected. Switch(config)# interface gigabitethernet10 → eject port 10 SFP DDM transceiver. Switch(config-if)# sfp ddm eject DDM SFP on Port 9 normally ejected.
Port Control – Auto Negotiation	Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/ Duplex	Switch(config-if)# speed 100 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full set the duplex mode ok!

Port Control (continued)	
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!
Port Status	

Port Status	Switch# show interface
	Interface fastethernet1
	  Administrative Status : Enable
	  Operating Status : Connected
	  Duplex : Full
	  Speed : 100
	  Flow Control :off
	  Default Port VLAN ID: 1
	  Ingress Filtering : Disabled
	  Acceptable Frame Type : All
	  Port Security : Disabled
	  Auto Negotiation : Disable
	  Loopback Mode : None
	  STP Status: forwarding
	  Default CoS Value for untagged packets is 0.
	  Mdix mode is Disable.
	  Medium mode is Copper.
	
	Switch# show sfp ddm →show SFP DDM information
	Port 8
	  Temperature:N/A
	  Tx power:N/A
	  Rx power:N/A
	Port 9
	  Temperature:64.00 C <range :0.0-80.00>
	  Tx power:-6.0 dBm <range : -9.0 - -4.0>
	  Rx power:-30.0 dBm <range: -30.0 - -4.0>
	Port 10
	  Temperature:67.00 C <range :0.0-80.00>
	  Tx power:-6.0 dBm <range : -9.0 - -4.0>
	  Rx power:-2.0 dBm <range: -30.0 - -4.0>
	
	Note: *Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port.*

Rate Control	

Rate Control – Ingress or Egress	`Switch(config-if)# rate-limit`
	`  egress  Outgoing packets`
	`  ingress  Incoming packets`
	Note: *To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.*

Rate Control – Filter Packet Type	`Switch(config-if)# rate-limit ingress mode`
	`  all  Limit all frames`
	`  broadcast  Limit Broadcast frames`
	`  flooded-unicast  Limit Broadcast, Multicast and flooded unicast frames`
	`  multicast  Limit Broadcast and Multicast frames`
	`Switch(config-if)# rate-limit ingress mode broadcast`
	`Set the ingress limit mode broadcast ok.`

Rate Control – Bandwidth	`Switch(config-if)# rate-limit ingress bandwidth`
	`  <0-100>  Limit in megabits per second (0 is no limit)`
	`Switch(config-if)# rate-limit ingress bandwidth 8`
	`Set the ingress rate limit 8Mbps for Port 1.`

Storm Control	

Storm Control – Packet Type	`Switch(config-if)# storm-control`
	`broadcast :Broadcast packets`
	`dlf :Destination Lookup Failure`
	`multicast :Multicast packets`

Storm Control - Rate	`Switch(config)# storm-control broadcast`
	`<0-100000> Rate limit value 0~262143 packet/sec`
	`Switch(config)# storm-control broadcast 10000`
	`limit_rate = 10000 packets/sec`
	`Set rate limit for Broadcast packets.`
	`Switch(config)# storm-control multicast 10000`
	`limit_rate = 10000 packets/sec`
	`Set rate limit for Multicast packets.`
	`Switch(config)# storm-control dlf 10000`
	`limit_rate = 10000 packets/sec`
	`Set rate limit for Destination Lookup Failure packets.`

Port Trunking	

LACP	`Switch(config)# lacp group 1 25-28`
	`Group 1 based on LACP(IEEE 802.3ad) is enabled!`
	Note: *The interface list is gi25-28. Ports with a different speeds cannot be aggregated together.*

Static Trunk	`Switch(config)# trunk group 2 fa6-7gi25-28` `Trunk group 2 enable ok!`

Port Trunking (cont.)

Display – LACP

```
Switch# show lacp internal
LACP group 1 internal information:
      LACP Port   Admin    Oper     Port
Port  Priority    Key      Key      State
----- ---------- -------- -------- -------
   8           1        8        8    0x45
   9           1        9        9    0x45
  10           1       10       10    0x45

LACP group 2 is inactive
LACP group 3 is inactive
LACP group 4 is inactive
```

Display – Trunk

```
Switch# show trunk group 1
FLAGS:     I -> Individual         P -> In channel
           D -> Port Down

Trunk Group
GroupID  Protocol  Ports
--------+---------+-----------------------------------
 1        LACP      8(D) 9(D) 10(D)
Switch# show trunk group 2
FLAGS:     I -> Individual         P -> In channel
           D -> Port Down

Trunk Group
GroupID  Protocol  Ports
--------+---------+-----------------------------------
 2        Static    6(D) 7(P)
Switch#
```

Power over Ethernet (CLI)

Power over Ethernet is one of the key features of ES7528. It is fully IEEE 802.3af compliant, and supports IEEE 802.3at, including two-event and LLDP classification. The ES7528 supports up to 24-Port PoE injectors in Port 1 to Port 24, each port with the ability to deliver 606 mA current.

For more information or to use the web user interface, see *Power over Ethernet* on Page 70.

This table provides detailed information about the CLI commands for PoE control.

PoE System Status	

Display	Switch> enable
	Switch# show poe system
	PoE System
	  PoE Admin : Enable
	  PoE Hardward : Normal
	  PoE Input Voltage :
	  Vmain 1 : 52.9 V
	  Vmain 2 : 53.0 V
	  Vmain 3 : 53.1 V
	  Output power : 0.0 Watts
	  Temperature 1 : 50 degree
	  Temperature 2 : 53 degree
	  Temperature 3 : 48 degree
	  Power information :
	  Emergency power :
	  Primary : DC1(53 V), DC2(53 V), AC(53 V)
	  Secondary : N/A
	  Tertiary : N/A
	  Budget :
	  DC Power 1 : 400 Watts
	  DC Power 2 : 400 Watts
	  AC Power : 300 Watts (In Use)
	  Total : 300 Watts in Use
	  Warning water level : N/A
	  Utilization : 0 %
	  Event : Normal

PoE Interface Status	

Display	Switch> enable
	Switch# show poe interface
	  [IFNAME] Interface name
	Switch# show poe interface fa1
	Interface fastethernet1 (POE Port 1)
	  Control Mode : User (Disable)
	  Powering Mode : 802.3af
	  Operation Status : Off
	  Detection Status : Valid
	  Classification : N/A
	  Priority : Highest
	  Output Power : 0.0 Watts, Voltage : 0.0 V, Current : 0 mA
	  Power Budget :
	  Budget : 32.0 Watts, effective 0 Watts
	  Power Budget Warning Level : N/A
	  Utilization : 0 %
	  Event : Normal

PoE PD Detection	

Status	Switch# show poe pd-detect
	PD Status Detection
	  Status : Enabled
	  Host 1 :
	  Target IP : 192.168.250.100
	  Cycle Time : 10
	  Host 2 :
	  Target IP : 192.168.250.200
	  Cycle Time : 20
	  Host 3 :
	  Target IP : 192.168.250.15
	  Cycle Time : 30
	  Host 4 :
	  Target IP : 192.168.250.20
	  Cycle Time : 40

PoE Schedule	

Display Status	Switch# show poe schedule
	  [IFNAME] Inteface name
	Switch# show poe schedule fa1
	Interface fastethernet1
	  PoE Schedule
	  Status : Disabled
	  Weekly Schedule :
	  Sunday : All day disable
	  Monday : 6,7,8,9,10,11,12,13,14,15,16,17,18
	  Tuesday : 6,7,8,9,10,11,12,13,14,15,16,17,18
	  Wednesday : 6,7,8,9,10,11,12,13,14,15,16,17,18
	  Thursday : 6,7,8,9,10,11,12,13,14,15,16,17,18
	  Friday : 6,7,8,9,10,11,12,13,14,15,16,17,18
	  Saturday : All day disable

Set PoE Powering Mode	

802.3af	Switch> enable
	Switch# config term
	Switch(config)# interface fa1
	Switch(config-if)# poe
	  budget Configure the power budget of power over ethernet
	  control-mode PoE control mode
	  powering-mode PoE powering mode
	  schedule Configure the schdule of day
	  type String to indicate the type of powered device
	  user Port control in user mode
	Switch(config-if)# poe powering-mode
	  802.3af 802.3af powering mode
	  forced forced powering mode
	  802.3at 802.3at powering mode
	Switch(config)# poe powering-mode 802.3af

Forced Powering Mode	Switch> enable Switch# config term Switch(config)# interface fa1 Switch(config-if)# poe powering-mode forced
802.3at	Switch> enable Switch# config term Switch(config)# interface fa1 Switch(config-if)# poe powering-mode 802.3at

Set Control Mode on Port/Schedule	

Set PoE Port to User Mode	Switch> enable
	Switch# config term
	Switch(config)# interface fa1
	Switch(config-if)# poe control-mode
	  schedule Schedule mode
	  user User mode
	Switch(config-if)# poe control-mode user

Schedule	Switch> enable
	Switch# config term
	Switch(config)# interface fa1
	Switch(config-if)# poe control-mode
	  schedule Schedule mode
	  user User mode
	Switch(config-if)# poe control-mode schedule

Enable/Disable PoE Function in User Mode	

Enable	Switch> enable
	Switch# config term
	Switch(config)# interface fa1
	Switch(config-if)# poe user
	  disable Disables the poe for the port
	  enable Enables the poe for the port
	Switch(config-if)# poe user enable

Disable	Switch(config-if)# poe user disable
Port Type String	
Set	Switch> enable Switch# config term Switch(config)# interface fa1 Switch(config-if)# poe type TYPE Type string, maximum 20 characters Switch> enable Switch# config term Switch(config)# interface fa1 Switch(config-if)# poe type IPCam-1
Set Port Budget	

Set Power Consumption (Max) to 12W	Switch> enable
	Switch# config term
	Switch(config)# interface fa1
	Switch(config-if)# poe budget
	  [POWER] 0.4 - 32 Watts
	  warning Warning water level
	Switch(config-if)# poe budget 12

PoE Budget Warning (%)	
Set	Switch> enable Switch# config term Switch(config)# interface fa1 Switch(config-if)# poe budget warning <0-100> 0 is disable, valid range is 1 to 100 percentage Switch(config-if)# poe budget warning 60
PoE Priority	
Set	Switch> enable Switch# config term Switch(config)# interface fa1 Switch(config-if)# poe priority critical Hightest priority level high High priority level low Low priority level Switch(config-if)# poe priority critical
PoE Schedule Weekday Hour	
Enable Hour 1, 3, 5 and 10 to 23 on Sunday	Switch> enable Switch# config term Switch(config)# interface fa1 Switch(config-if)# poe schedule <0-6> Weekday: valid range 0-6 (0=Sun, 1=Mon..., 6=Sat) Switch(config-if)# poe schedule 0 1,3,5,10-23
Disable Sunday Schedule	Switch(config-if)# no poe schedule 0
PoE Budget DC1/DC2	
Set	Switch(config)# poe disable Disables power over ethernet enable Enables power over ethernet budget Configure the power budget of power over ethernet pd-detect Configure PD status detection Switch(config)# poe budget DC1 Power source : DC 1 DC2 Power source : DC 2 vin Input voltage warning Warning water level Switch(config)# poe budget DC1 [POWER] System budget : 1 - 400 Watts Switch(config)# poe budget DC1 Switch(config)# poe budget DC1 400

PoE PD Detect	

Enable	Switch> enable
	Switch# config term
	Switch(config)# poe
	  disable Disables power over ethernet
	  enable Enables power over ethernet
	  budget Configure the power budget of power over ethernet
	  pd-detect Configure PD status detection
	Switch(config)# poe pd-detect
	  disable Disable PD status detection
	  enable Enable PD status detection
	  A.B.C.D PD IP address
	Switch(config)# poe pd-detect enable

Disable	Switch(config)# poe pd_detect disable
PoE PD Detect Cycle Time	
Ping 20 Sec, Re-enable PoE	Switch(config)# poe pd_detect 192.160.1.2 20

Network Redundancy (CLI)

It is critical for industrial applications that the network remains running at all times. The ES7528 supports:

- Standard Rapid Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP)

  The ES7528 supports RSTP versions IEEE 802.1D-2004, IEEE 802.1D-1998 STP, and IEEE 802.1w RSTP.

- Multiple Spanning Tree Protocol (MSTP)

  MSTP implements IEEE 802.1s, which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs. MSTP was originally defined in the IEEE 802.1s and later merged into the IEEE 802.1Q-2003 specification.

- Redundant Ring

  The Redundant Ring features 0 ms for restore and about 5 ms for fail over for copper.

- Rapid Dual Homing (RDH)

  Advanced RDH technology allows the ES7528 to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP groups together, which is also known as Auto Ring Coupling.

Optionally, you can use the web user interface for configuration, see *Network Redundancy* on Page 74.

This table provides detailed information about the CLI command lines for network redundancy.

GLobal (STP, RSTP, and MSTP)	
Enable	`Switch(config)# spanning-tree enable`
Disable	`Switch(config)# spanning-tree disable`

Mode	`Switch(config)# spanning-tree mode`
	`  rst  the rapid spanning-tree protocol (802.1w)`
	`  stp  the spanning-tree prtotcol (802.1d)`
	`  mst  the multiple spanning-tree protocol (802.1s)`
	
	`Switch(config)# spanning-tree mode`
	`Switch(config)# spanning-tree mode mst`
	`  Spanning-Tree Mode change to be MSTP (802.1s)`
	
	`Switch(config)# spanning-tree mode stp`
	`Spanning-Tree Mode change to be STP(802.1d) .`
	
	`Switch(config)# spanning-tree mode rst`
	`Spanning-Tree Mode change to be RSTP(802.1w) .`
	
	`Switch(config)# spanning-tree mode mst`
	`Spanning-Tree Mode change to be MSTP(802.1s).`

Bridge Priority	`Switch(config)# spanning-tree priority`
	`  <0-61440>  the value of bridge priority in multiple of 4096`
	`Switch(config)# spanning-tree priority 4096`

Bridge Times	`Switch(config)# spanning-tree bridge-times (forward Delay) (max-age) (Hello Time)`
	`Switch(config)# spanning-tree bridge-times 15 20 2`
	
	`This command allows you configure all the timing in one time.`

Forward Delay	`Switch(config)# spanning-tree forward-time`
	`  <4-30>  the value of forward delay time in seconds`
	`Switch(config)# spanning-tree forward-time 15`

Max Age	`Switch(config)# spanning-tree max-age`
	`  <6-40>  the value of message maximum age time in seconds`
	`Switch(config)# spanning-tree max-age 20`

Hello Time	`Switch(config)# spanning-tree hello-time`
	`  <1-10>  the value of hello time in seconds`
	`Switch(config)# spanning-tree hello-time 2`

MSTP	

Enter the MSTP Configuration Tree	Switch(config)# spanning-tree mst
	  MSTMAP the mst instance number or range
	  configuration enter mst configuration mode
	  forward-time the forward delay time
	  hello-time the hello time
	  max-age the message maximum age time
	  max-hops the maximum hops
	  sync sync port state of exist vlan entry
	Switch(config)# spanning-tree mst configuration
	Switch(config)# spanning-tree mst configuration
	Switch(config-mst)#
	  abort exit current mode and discard all changes
	  end exit current mode, change to enable mode and apply all changes
	  exit exit current mode and apply all changes
	  instance the mst instance
	  list Print command list
	  name the name of mst region
	  no Negate a command or set its defaults
	  quit exit current mode and apply all changes
	  revision the revision of mst region
	  show show mst configuration

Region Configuration	Region Name: Switch(config-mst)# name NAME the name string Switch(config-mst)# name comtrol Region Revision: Switch(config-mst)# revision <0-65535> the value of revision Switch(config-mst)# revision 65535
Mapping Instance to VLAN (Ex: Mapping VLAN 2 to Instance 1)	Switch(config-mst)# instance <1-15> target instance number Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(ex.10) or range(ex.1-10) Switch(config-mst)# instance 1 vlan 2

MSTP (Continued)	
Display Current MST Configuration	Switch(config-mst)# show current Current MST configuration Name [comtrol] Revision 65535 Instance Vlans Mapped -------- --------------------------------------- 0 1,4-4094 1 2 2 3 --- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ---
Remove Region Name	Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name
Remove Instance example	Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2
Show Pending MST Configuration	Switch(config-mst)# show pending Pending MST configuration Name [] (->The name is removed by no name) Revision 65535 Instance Vlans Mapped -------- --------------------------------------- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance 2) --- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ---
Apply the setting and go to the configuration mode	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Apply the setting and go to the global mode	Switch(config-mst)# end apply all mst configuration changes Switch#

MSTP (Continued)	
Abort the Setting and go to the configuration mode. Show Pending to see the new settings are not applied.	Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name [comtrol] (->The name is not applied after Abort settings.) Revision 65535 Instance Vlans Mapped -------- ------------------------------------ 0 1,4-4094 1 2 2 3 (-> The instance is not applied after Abort settings.) --- Config HMAC-MD5 Digest: 0xAC36177F50283CD4B83821D8AB26DE62 ---
RSTP	
System RSTP Setting	The mode should be rstp, timings can be configured in the global settings listed in the previous examples.
Port Configuration Mode	
Port Configuration	Switch(config)# interface fa1 Switch(config-if)# spanning-tree bpdufilter a secure BPDU process on edge-port interface bpduguard a secure response to invalid configurations (received BPDU sent by self) cost change an interface's spanning-tree port path cost edge-port interface attached to a LAN segment that is at the end of a bridged LAN or to an end node link-type the link type for the Rapid Spanning Tree mst the multiple spanning-tree port-priority the spanning tree port priority
Port Path Cost	Switch(config-if)# spanning-tree cost <1-200000000> 16-bit based value range from 1-65535, 32-bit based value range from 1-200,000,000 Switch(config-if)# spanning-tree cost 200000
Port Priority	Switch(config-if)# spanning-tree port-priority <0-240> Number from 0 to 240, in multiple of 16 Switch(config-if)# spanning-tree port-priority 128
Link Type - Auto	Switch(config-if)# spanning-tree link-type auto
Link Type - P2P	Switch(config-if)# spanning-tree link-type point-to-point

Port Configuration Mode (Continued)	
Link Type – Share	`Switch(config-if)# spanning-tree link-type shared`
Edge Port	`Switch(config-if)# spanning-tree edge-port enable` `Switch(config-if)# spanning-tree edge-port disable`

MSTP Port Configuration	`Switch(config-if)# spanning-tree mst MSTMAP cost`
	`  <1-200000000>  the value of mst instance port cost`
	`Switch(config-if)# spanning-tree mst MSTMAP port-priority`
	`  <0-240>  the value of mst instance port priority in multiple of 16`

Global Information	

Active Information	`Switch# show spanning-tree active`
	` Spanning-Tree :  Enabled  Protocol :  MSTP`
	` Root Address :  00C0.4E32.0001  Priority :  32768`
	` Root Path Cost : 0  Root Port : N/A`
	` Root Times :  max-age 20, hello-time  2, forward-delay 15`
	` Bridge Address : 00C0.4E32.0001  Priority :  32768`
	` Bridge Times : max-age 20, hello-time  2, forward-delay 15`
	` BPDU transmission-limit : 3`
	
	` Port  Role  State  Cost  Prio.Nbr  Type  Aggregated`
	` ------ ---------- ---------- -------- ---------- ------------ ------------`
	` fa1  Designated Forwarding  200000  128.1  P2P(RSTP)  N/A`
	` fa2  Designated Forwarding  200000  128.2  P2P(RSTP)  N/A`

RSTP Summary	`Switch# show spanning-tree summary`
	` Spanning-Tree :  Enabled  Protocol :  MSTP`
	` Root Address :  00c0.4e32.004f  Priority :  32768`
	` Root Path Cost : 400000  Root Port : 10`
	` Root Times :  max-age 20, hello-time  2, forward-delay 15`
	` Bridge Address  00c0.4e32.0001  Priority :  32768`
	` Bridge Times : max-age 20, hello-time  2, forward-delay 15`
	` BPDU transmission-limit : 3`
	` BPDU Skewing Detection : Disabled`
	` Backbonefast : Disabled`
	` Topology Change Flag :  False  Topology Change Detected Flag : False`
	` Topology Change Count : 571  Last Topology Change from : 0000.0000.0000`
	` Timers: hello 0, topology change 0`
	
	` Summary of connected spanning tree ports :`
	`  Port-State Summary`
	`  Blocking  Listening  Learning  Forwarding  Disabled`
	`  --------  ---------  --------  ----------  --------`
	`  1  0  0  1  8`
	`  Port Link-Type Summary`
	`  AutoDetected  PointToPoint  SharedLink  EdgePort`
	`  ------------  ------------  ----------  --------`
	`  10  0  0  8`

Global Information (Continued)	
Port Info	Switch# show spanning-tree interface fa1 Interface fastethernet1 of Bridge is Alternate Blocking Edge Port : Edge (Non-Edge) BPDU Filter : Disabled Link Type : Auto (Point-to-point) BPDU Guard : Disabled Timers : message-age 4, forward-delay 0 BPDUs : sent 26, received 34037 TCNs : sent 0, received 0 Message Expired Count : 0 Forward Transition Count : 8 Aggregation Group: N/A Type: N/A Aggregated with : N/A Port information port id 128.6 priority 128 cost 200000 Designated root address 00c0.4e32.004f priority 32768 cost 200000 Designated bridge address 00c0.4e32.0007 priority 32768 port id 128.5
MSTP Information	
MSTP Configuration	Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Running) Name [comtrol] Revision 65535 Instance Vlans Mapped -------- ------------------------------------ 0 1,4-4094 1 2 2 3 --- Config HMAC-MD5 Digest: 0xAC36177F50283CD4B83821D8AB26DE62 ---
Display all MST Information	Switch# show spanning-tree mst ###### MST00 vlans mapped: 1,4-4094 Bridge address 00C0.4E32.0001 priority 32768 (sysid 0) Root this switch for CST and IST Configured max-age 2, hello-time 15, forward-delay 20, max-hops 20 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP) ###### MST01 vlans mapped: 2 Bridge address 00C0.4E32.0001 priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)

MSTP Information (Continued)

Display all MST Information

```
Switch# show spanning-tree mst
 ###### MST00   vlans mapped: 1-4094
 Bridge         address 00c0.4e30.0001  priority  32768 (sysid 0)
 Root           address 00c0.4e2c.004f  priority  32768 (sysid 0)
                port    10              path cost 400000
 Regional root  this switch
 Operational    max-age  2, hello-time 15, forward-delay 20
 Configured     max-age  2, hello-time 15, forward-delay 20, max-hops 20

  Port     Role      State      Cost    Prio.Nbr         Type
 ------ ---------- ---------- -------- ---------- ------------------
  fa2   Alternate  Blocking    200000   128.6    P2P Bound(RSTP)
  fa1   Root       Forwarding  200000   128.10   P2P Bound(RSTP)
```

MSTP Root Information

```
Switch# show spanning-tree mst root
   MST    Root         Root    Root  Root   Max  Hello  Fwd
 Instance   Address     Priority  Cost  Port   age         dly
 -------- -------------- -------- ---------- ------ ----- ----- -----
   MST00  00C0.4E32.0001   32768   0   N/A   20   2   15
   MST01  00C0.4E32.0001   32768   0   N/A   20   2   15
   MST02  00C0.4E32.0001   32768   0   N/A   20   2   15
```

MSTP Instance Information

```
Switch# show spanning-tree mst 1
 ###### MST01   vlans mapped: 2
 Bridge         address 00C0.4E32.0001  priority  32768 (sysid 1)
 Root           this switch for MST01

  Port     Role      State      Cost    Prio.Nbr         Type
 ------ ---------- ---------- -------- ---------- ------------------
   fa1  Designated Forwarding   200000   128.1    P2P Internal(MSTP)
   fa2  Designated Forwarding   200000   128.2    P2P Internal(MSTP)
```

MSTP Port Information

```
Switch# show spanning-tree mst interface fa1
 Interface fastethernet1 of MST00 is Designated Forwarding
 Edge Port : Edge (Edge)            BPDU Filter : Disabled
 Link Type : Auto (Point-to-point)  BPDU Guard :  Disabled
 Boundary :  Internal(MSTP)
 BPDUs :  sent 6352, received 0

 Instance    Role      State      Cost    Prio.Nbr      Vlans mapped
 -------- ---------- ---------- -------- ---------- --------------------
     0    Designated Forwarding   200000   128.1    1,4-4094
     1    Designated Forwarding   200000   128.1    2
     2    Designated Forwarding   200000   128.1    3
```

Redundant Ring	

Create or configure a Ring	`Switch(config)# redundant-ring 1`
	`Ring 1 created`
	`Switch(config-redundant-ring)#`
	Note: *1 is the target Ring ID which is going to be created or configured.*

Super Ring Version	`Switch(config-redundant-ring)# version`
	`  default  set default to Redundant ring`
	`  rapid-super-ring  rapid super ring`
	`  super-ring  super ring`
	
	`Switch(config-redundant-ring)# version rapid-super-ring`

Priority	`Switch(config-redundant-ring)# priority`
	`  <0-255>  valid range is 0 to 255`
	`default  set default`
	`Switch(config-redundant-ring)# super-ring priority 100`

Ring Port	`Switch(config-redundant-ring)# port`
	`  IFLIST  Interface list, ex: fa1,fa3-5,gi25-28`
	`  cost  path cost`
	`Switch(config-redundant-ring)# port fa1,fa2`

Ring Info	

Ring Info	`Switch# show redundant-ring [Ring ID]`
	`[Ring1] Ring1`
	`Current Status : Disabled`
	`Role : Disabled`
	`Ring Status : Abnormal`
	`Ring Manager : 0000.0000.0000`
	`Blocking Port : N/A`
	`Giga Copper : N/A`
	`Configuration :`
	`Version : Super Ring`
	`Priority : 128`
	`Ring Port : fa1, fa2`
	`Path Cost : 100, 200`
	`Dual-Homing II : Disabled`
	`Statistics :`
	`Watchdog sent 0, received 0, missed 0`
	`Link Up sent 0, received 0`
	`Link Down sent 0, received 0`
	`Role Transition count 0`
	`Ring State Transition count 1`
	
	Ring ID is optional. If the ring ID is typed, this command only displays the information of the target Ring.

VLAN (CLI)

A Virtual LAN (VLAN) is a logical grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members. The VLAN allows you to isolate network traffic so that only members of the VLAN could receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is the logical equivalent of physically reconnecting a group of network devices to another Layer 2 switch, without actually disconnecting these devices from their original switches.

The ES7528 supports IEEE 802.1Q VLAN, which is also known as Tag-Based VLAN. This Tag-Based VLAN allows a VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

Optionally, you can use the web user interface for configuration, see *VLAN* on Page 86.

The following table provides detailed information about command lines for the VLAN.

VLAN Port Configuration	
VLAN Port PVID	`Switch(config-if)# switchport trunk native vlan 2` `Set port default vlan id to 2 success`

Port Accept Frame Type	`Switch(config)# inter fa1`
	`Switch(config-if)# acceptable frame type all`
	`any kind of frame type is accepted!`
	`Switch(config-if)# acceptable frame type vlantaggedonly`
	`only vlan-tag frame is accepted!`

Ingress Filtering (for Fast Ethernet Port 1)	`Switch(config)# interface fa1`
	`Switch(config-if)# ingress filtering enable`
	`ingress filtering enable`
	`Switch(config-if)# ingress filtering disable`
	`ingress filtering disable`

Egress rule – Untagged (for VLAN 2)	`Switch(config-if)# switchport access vlan 2` `switchport access vlan - success`
Egress rule – Tagged (for VLAN 2)	`Switch(config-if)# switchport trunk allowed vlan add 2`

Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	`Switch# show interface fa1`
	`Interface fastethernet1`
	`  Administrative Status : Enable`
	`  Operating Status : Not Connected`
	`  Duplex : Auto`
	`  Speed : Auto`
	`  Flow Control :off`
	`  Default Port VLAN ID: 2`
	`  Ingress Filtering : Disabled`
	`  Acceptable Frame Type : All`
	`  Port Security : Disabled`
	`  Auto Negotiation : Enable`
	`  Loopback Mode : None`
	`  STP Status: disabled`
	`  Default CoS Value for untagged packets is 0.`
	`  Mdix mode is Auto.`
	`  Medium mode is Copper.`

VLAN Port Configuration (continued)	
Display – Port Egress Rule (Egress rule, IP address, status)	Switch# show running-config …… ! interface fastethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 ……. interface vlan1 ip address 192.168.250.8/24 no shutdown
VLAN Configuration	
Create VLAN (2)	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# ***Note:*** *In the CLI configuration, you should first create a VLAN interface. Then you can start to add/remove ports. The default status of the created VLAN is unused until you add member ports to it.*
Remove VLAN	Switch(config)# no vlan 2 no vlan success ***Note:*** *You can only remove the VLAN when the VLAN is in unused mode.*
VLAN Name	Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name ***Note:*** *Use no name to change the name to default name, VLAN VID.*
VLAN description	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2 Switch(config-if)# no description ->Delete the description.
IP address of the VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.250.18/24 Switch(config-if)# no ip address 192.168.250.8/24 ->Delete the IP address
Create multiple VLANs (VLAN 5-8)	Switch(config)# interface vlan 5-8
Shutdown VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN

VLAN Configuration (continued)	

Display – VLAN table	`Switch# sh vlan`
	`VLAN Name  Status  Trunk Ports  Access Ports`
	`---- ----  ------  ------------  -------------------------`
	`1  VLAN1  Static  -  fa1-7,gi25-28`
	`2  VLAN2  Unused  -  -`
	`3  test  Static  fa4-7,gi25-28  fa1-3,fa7,gi25-28`

Display – VLAN interface information	`Switch# show interface vlan1`
	`interface vlan1 is up, line protocol detection is disabled`
	`index 14 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>`
	`HWaddr: 00:c0:4e:ff:01:b0`
	`inet 192.168.250.100/24 broadcast 192.168.250.255`
	`input packets 639, bytes 38248, dropped 0, multicast packets 0`
	`input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0`
	`output packets 959, bytes 829280, dropped 0`
	`output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0`
	`collisions 0`

GVRP Configuration	

GVRP enable/ disable	`Switch(config)# gvrp mode`
	`disable  Disable GVRP feature globally on the switch`
	`enable  Enable GVRP feature globally on the switch`
	`Switch(config)# gvrp mode enable`
	`Gvrp is enabled on the switch!`

Configure GVRP timer
 	
Join timer /Leave timer/ LeaveAll timer
	`Switch(config)# inter fa1`
	`Switch(config-if)# garp timer`
	`<10-10000>`
	`Switch(config-if)# garp timer 20 60 1000`
	Note: *The unit of this timer is centiseconds.*

Management VLAN	
Management VLAN	`Switch(config)# int vlan 1 (Go to management VLAN)` `Switch(config-if)# no shutdown`

Display	`Switch# show running-config`
	`….`
	`!`
	`interface vlan1`
	`ip address 192.168.250.17/24`
	`ip igmp`
	`no shutdown`
	`!`
	`….`

Private VLAN (CLI)

A private VLAN helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. The Private VLAN features provides primary and secondary VLANs within a single switch.

Primary VLAN: The uplink port is usually a member of the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with Secondary VLANs.

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated and Community VLANs. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other, however, the isolated VLAN ports cannot.

Optionally, you can use the web user interface for configuration, see *Private VLAN* on Page 94.

The following table provides detailed information about command lines for private VLAN port configuration, VLAN configuration, and VLAN table display.

Private VLAN Configuration	

Create VLAN	`Switch(config)# vlan 2`
	`vlan 2 success`
	`Switch(config-vlan)#`
	`  end  End current mode and change to enable mode`
	`  exit  Exit current mode and down to previous mode`
	`  list  Print command list`
	`  name  Assign a name to vlan`
	`  no  no`
	`  private-vlan  Configure a private VLAN`

Private VLAN Type
 	
Choose the Types
 	
Primary Type
 	
Isolated Type
 	
Community Type
	Go to the VLAN you want configure first.
	`Switch(config)# vlan (VID)`
	
	`Switch(config-vlan)# private-vlan`
	`  community  Configure the VLAN as an community private VLAN`
	`  isolated  Configure the VLAN as an isolated private VLAN`
	`  primary  Configure the VLAN as a primary private VLAN`
	
	`Switch(config-vlan)# private-vlan primary`
	`  <cr>`
	
	`Switch(config-vlan)# private-vlan isolated`
	`  <cr>`
	
	`Switch(config-vlan)# private-vlan community`
	`  <cr>`

Private VLAN Port Configuration	
Go to the port configuration	Switch(config)# interface (port_number, ex: fa1) Switch(config-if)# switchport private-vlan host-association Set the private VLAN host association mapping map primary VLAN to secondary VLAN
Private VLAN Port Type Promiscuous Port Type Host Port Type	Switch(config-if)# switchport mode private-vlan Set private-vlan mode Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host promiscuous Set the mode to private-vlan promiscuous Switch(config-if)# switchport mode private-vlan promiscuous <cr> Switch(config-if)# switchport mode private-vlan host <cr>
Private VLAN Port Configuration PVLAN Port Type Host Association primary to secondary (The command is only available for host port.)	Switch(config)# interface fa1 Switch(config-if)# switchport mode private-vlan host Switch(config-if)# switchport private-vlan host-association <2-4094> Primary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 <2-4094> Secondary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 3
Mapping primary to secondary VLANs (This command is only available for promiscuous port)	Switch(config)# interface fa1 Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)# switchport private-vlan mapping 2 add 3 Switch(config-if)# switchport private-vlan mapping 2 add 4 Switch(config-if)# switchport private-vlan mapping 2 add 5
Private VLAN Information	
Private VLAN Information	Switch# show vlan private-vlan FLAGS: I -> Isolated P -> Promiscuous C -> Community Primary Secondary Type Ports ------- --------- ----------------- ---------------------- 2 3 Isolated fa1(P),fa2(I) 2 4 Community fa2(P),fa3(C) 2 5 Community fa2(P),fa1(C),fa3(I) 10 - - -

Private VLAN Information (Continued)	

Running Config Information
 	
Private VLAN Type
 	
Private VLAN Port Information
	Switch# show run
	Building configuration...
	
	Current configuration:
	hostname Switch
	vlan learning independent
	!
	vlan 1
	!
	vlan 2
	 private-vlan primary
	!
	vlan 3
	 private-vlan isolated
	!
	vlan 4
	 private-vlan community
	!
	vlan 5
	 private-vlan community
	!
	……..
	……..
	interface fastethernet7
	  switchport access vlan add 2,5
	  switchport trunk native vlan 5
	 switchport mode private-vlan host
	 switchport private-vlan host-association 2 5
	!
	interface fastethernet
	  switchport access vlan add 2,4
	  switchport trunk native vlan 4
	 switchport mode private-vlan host
	 switchport private-vlan host-association 2 4
	!
	interface gigabitethernet9
	  switchport access vlan add 2,5
	  switchport trunk native vlan 5
	 switchport mode private-vlan host
	 switchport private-vlan host-association 2 3
	!
	interface gigabitethernet10
	  switchport access vlan add 2,5
	  switchport trunk native vlan 2
	 switchport mode private-vlan promiscuous
	 switchport private-vlan mapping 2 add 3-5
	……
	……..

Private VLAN Information (Continued)	
PVLAN Type	Switch# show vlan private-vlan type Vlan Type Ports ---- ---------- ---------- 2 primary fa3 3 isolated fa2 4 community fa1 5 community fa4,fa5 10 primary -
Host List	Switch# show vlan private-vlan port-list Ports Mode Vlan ----- ---------- ---- 1 normal - 2 normal - 3 normal - 4 normal - 5 normal - 6 normal - 7 host 5 8 host 4 9 host 3 10 promiscuous 2

Traffic Prioritization (CLI)

Quality of Service (QoS) provides a traffic prioritization mechanism which allows you to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port with regard to setting priorities.

ES7528 QOS supports four physical queues, weighted fair queuing (WRR) and Strict Priority scheme, that follows the IEEE 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

Optionally, you can use the web user interface for configuration, see *Traffic Prioritization* on Page 97. This table provides detailed information about command lines for traffic prioritization configuration

QoS Setting	

Queue Scheduling – Round Robin	`Switch(config)# qos queue-sched`
	`  rr   Round Robin`
	`  sp   Strict Priority`
	`  wrr  Weighted Round Robin`
	`Switch(config)# qos queue-sched rr`
	`The queue scheduling scheme is setting to Round Robin.`

Queue Scheduling – Strict Priority	`Switch(config)# qos queue-sched sp` `The queue scheduling scheme is setting to Strict Priority.`
Queue Scheduling - WRR	`Switch(config)# qos queue-sched wrr 1 1 1 1 1 1 1 1` `The queue scheduling scheme is setting to Weighted Round Robin.`

Port Setting – Priority	`Switch(config)# interface fa1`
	`Switch(config-if)# qos priority`
	`  DEFAULT-PRIORITY  Assign an priority (7 highest)`
	`Switch(config-if)# qos priority 7`
	`The default port priority value is set 7 ok.`
	Note: *When change the port setting, you should Select the specific port first. Ex: fa1 means Fast Ethernet Port 1.*

Display – Queue Scheduling	`Switch# show qos queue-sched` QoS queue scheduling scheme: Weighted Round Robin (Use an 8,4,2,1 weight)

QoS Setting (Continued)	
Display – Port Setting	Switch# show qos port-priority Port Default Priority : Port Priority -----+---- 1 0 2 0 3 0 4 0 5 0 6 0 7 0 8 0 9 0 10 0 … 26 0 27 0 28 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-7) **Format**: *qos cos-map priority_value queue_value.*
Map CoS 0 to Queue 0	Switch(config)# qos cos-map 0 0 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 1	Switch(config)# qos cos-map 1 1 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 2	Switch(config)# qos cos-map 2 2 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 3	Switch(config)# qos cos-map 3 3 The CoS to queue mapping is set ok.
Map CoS 4 to Queue 4	Switch(config)# qos cos-map 4 4 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 5	Switch(config)# qos cos-map 5 5 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 6	Switch(config)# qos cos-map 6 6 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 7	Switch(config)# qos cos-map 7 7 The CoS to queue mapping is set ok.

CoS-Queue Mapping (Continued)	

Display – CoS-Queue mapping	Switch# sh qos cos-map
	CoS to Queue Mapping :
	CoS Queue
	---- + ------
	  0 0
	  1 1
	  2 2
	  3 3
	  4 4
	  5 5
	  6 6
	  7 7

DSCP-Queue Mapping	

Format	Switch(config)# qos dscp-map
	  PRIORITY Assign an priority (63 highest)
	Switch(config)# qos dscp-map 0
	  QUEUE Assign an queue (0-7)
	Format: **qos dscp-map priority_value queue_value.**

Map DSCP 0 to Queue 1	Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.

Display – DSCO-Queue mapping	Switch# show qos dscp-map
	DSCP to Queue Mapping : (dscp = d1 d2)
	
	  d2| 0 1 2 3 4 5 6 7 8 9
	d1 |
	-----+----------------------
	  0 | 0 0 0 0 0 0 0 0 1 1
	  1 | 1 1 1 1 1 1 2 2 2 2
	  2 | 2 2 2 2 3 3 3 3 3 3
	  3 | 3 3 4 4 4 4 4 4 4 4
	  4 | 5 5 5 5 5 5 5 5 6 6
	  5 | 6 6 6 6 6 6 7 7 7 7
	  6 | 7 7 7 7

Multicast Filtering (CLI)

For multicast filtering, the ES7528 uses IGMP (Internet Group Management Protocol) Snooping technology. IGMP is an internet protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership.

In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown in the following table.

Message	Description
Query	A message sent from the querier (an IGMP router or a switch) that asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable **IGMP Snooping** and **IGMP Query** functions. This section illustrates the information of the IGMP Snooping function, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

Optionally, you can use the web user interface for configuration, see *Multicast Filtering* on Page 100.

The following table provides detailed information about command lines for multicast filtering configuration.

IGMP Snooping	
IGMP Snooping - Global	`Switch(config)# ip igmp snooping` `IGMP snooping is enabled globally. Specify on which vlans IGMP snooping enables`

IGMP Snooping - VLAN	`Switch(config)# ip igmp snooping vlan`
	`  VLANLIST  allowed vlan list`
	`  all       all existed vlan`
	`Switch(config)# ip igmp snooping vlan 1-2`
	`IGMP snooping is enabled on VLAN 1-2.`

Disable IGMP Snooping - Global	`Switch(config)# no ip igmp snooping` `IGMP snooping is disabled globally ok.`
Disable IGMP Snooping - VLAN	`Switch(config)# no ip igmp snooping vlan 3` `IGMP snooping is disabled on VLAN 3.`

IGMP Snooping (Continued)	
Display – IGMP Snooping Setting	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled
Display – IGMP Table	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ---- --------------- ------- ------------------------ 1 239.192.8.0 IGMP fa6, 1 239.255.255.250 IGMP fa6,
IGMP Query	
IGMP Query V1	Switch(config)# int vlan 1 Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 Switch(config-if)# ip igmp
IGMP Query version	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2

IGMP Query Interval	Switch(config)# int vlan 1 (Go to management VLAN)
	Switch(config-if)# ip igmp
	Switch(config-if)# ip igmp query-interval 60 (Change query interval to 60 seconds, default value is 125 seconds)

IGMP Query Max Response Time	Switch(config)# int vlan 1 (Go to management VLAN)
	Switch(config-if)# ip igmp
	Switch(config-if)# ip igmp query-max-response-time 15 (Change query max response time to 15 seconds, default value is 10 seconds)

Disable	Switch(config)# int vlan 1 Switch(config-if)# no ip igmp

IGMP Query (Continued)	
Display	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config …. ! interface vlan1 ip address 192.168.250.17/24 ip igmp no shutdown ! …….
Unknown Multicast	
Send Unknown Multicast to Query Ports	Switch(config)# ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning enabled
Send Unknown Multicast to All Ports	Switch(config)# no ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning disabled Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!
Discard All Unknown Multicast	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!

GMRP Configuration	
Enable GMRP globally	`Switch(config)# gmrp mode enable` `Gmrp is enabled on the switch!`
Disable GMRP globally	`Switch(config)# gmrp mode disable` `Gmrp is disabled on the switch!`
Enable GMRP on a port	`Switch(config)# gmrp mode enable fa1` `Gmrp enabled on port 1 !`
Disable GMRP on a port	`Switch(config)# gmrp mode disable fa2` `Gmrp disabled on port 2 !`

Display	`Switch# sh gmrp`
	`GMRP global enabled`
	`port 1 : enabled`
	`port 2 : enabled`
	`port 3 : disabled`
	`port 4 : disabled`
	`port 5 : disabled`
	`port 6 : disabled`
	`port 7 : disabled`
	`port 8 : disabled`
	`port 9 : disabled`
	`port 10 : disabled`

Force Filtering	
Enable	`Switch(config)# mac-address-table force filtering` `Filtering unknown multicast addresses ok!`
Disable	`Switch(config)# no mac-address-table force filtering` `Flooding unknown multicast addresses ok!`

SNMP (CLI)

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. The ES7528 supports SNMP v1 and v2c and V3.

An SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

Optionally, you can use the web user interface for configuration, see *SNMP* on Page 104.

The following table provides detailed information about command lines for SNMP configuration.

SNMP Community	
Read Only Community	`Switch(config)# snmp-server community public ro` `community string add ok`
Read Write Community	`Switch(config)# snmp-server community private rw` `community string add ok`
SNMP Trap	
Enable Trap	`Switch(config)# snmp-server enable trap` `Set SNMP trap enable ok.`
SNMP Trap Server IP without specific community name	`Switch(config)# snmp-server host 192.168.250.33` `SNMP trap host add OK.`

SNMP Trap Server IP with version 1 and community	`Switch(config)# snmp-server host 192.168.250.33 version 1 private`
	`SNMP trap host add OK.`
	Note: *Private is the community name, version 1 is the SNMP version.*

SNMP Trap Server IP with version 2 and community	`Switch(config)# snmp-server host 192.168.250.33 version 2 private` `SNMP trap host add OK.`
Disable SNMP Trap	`Switch(config)# no snmp-server enable trap` `Set SNMP trap disable ok.`

Display	`Switch# sh snmp-server trap`
	`SNMP trap: Enabled`
	`SNMP trap community: public`
	
	`Switch# show running-config`
	`.......`
	`snmp-server community public ro`
	`snmp-server community private rw`
	`snmp-server enable trap`
	`snmp-server host 192.168.250.33 version 2 admin`
	`snmp-server host 192.168.250.33 version 1 admin`
	`……..`

Security (CLI)

The ES7528 provides several security features for you to secure your connection.
Optionally, you can use the web user interface for configuration, see *Security* on Page 107.
This table provides information about the command lines for security configuration.

Port Security	
Add MAC	`Switch(config)# mac-address-table static 00c0.4e32.0101 vlan 1 interface fa1` `mac-address-table unicast static set ok!`

Port Security	`Switch(config)# interface fa1`
	`Switch(config-if)# switchport port-security`
	`Disables new MAC addresses learning and aging activities!`
	Rule: *Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.*

Disable Port Security	`Switch(config-if)# no switchport port-security` `Enable new MAC addresses learning and aging activities!`

Display	`Switch# show mac-address-table static`
	`Destination Address  Address Type  Vlan  Destination Port`
	`------------------  --------------  -------  -----------------`
	`00c0.4e32.0101  Static  1  fa1`

IP Security	

IP Security	`Switch(config)# ip security`
	`Set ip security enable ok.`
	`Switch(config)# ip security host 192.168.250.33`
	`Add ip security host 192.168.250.33 ok.`

Display	`Switch# show ip security`
	`ip security is enabled`
	`ip security host:`
	`192.168.250.33`

802.1x	
enable disable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#

authentic-method	Switch(config)# dot1x authentic-method
	  local Use the local username database for authentication
	  radius Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication
	Switch(config)# dot1x authentic-method radius
	Switch(config)#

radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.250.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.250.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.250.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.250.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius secondary-server-ip	Switch(config)# dot1x radius secondary-server-ip 192.168.250.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.250.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813
User name/ password for authentication	Switch(config)# dot1x username chris passwd chris vlan 1

Warnings (CLI)

The ES7528 provides several types of warning features for you to remotely monitor the status of the attached devices or changes in your network. The features include Fault Relay, System Log, and SMTP Email Alert.

Optionally, you can use the web user interface for configuration, see *Warning* on Page 117.

This table provides detailed information about the command lines of the warning configuration.

Fault Relay Output	

Relay Output	`Switch(config)# relay 1`
	`  dry  dry output`
	`  ping  ping failure`
	`  port  port link failure`
	`  power  power failure`
	Note: `ring  super ring failure`

Dry Output	`Switch(config)# relay 1 dry`
	`<0-4294967295> turn on period in second`
	`Switch(config)# relay 1 dry 5`
	`<0-4294967295> turn off period in second`
	`Switch(config)# relay 1 dry 5 5`

Ping Failure	`Switch(config)# relay 1 ping 192.168.250.33`
	`  <cr>`
	`  reset  reset a device`
	`Switch(config)# relay 1 ping 192.168.250.33 reset`
	`  <1-65535>  reset time`
	`Switch(config)# relay 1 ping 192.168.250.33 reset 60`
	`  <0-65535>  hold time to retry`
	`Switch(config)# relay 1 ping 192.168.250.33 reset 60 60`

Port Link Failure	`Switch(config)# relay 1 port`
	`  PORTLIST  port list`
	`Switch(config)# relay 1 port fa1-5`

Power Failure	`Switch(config)# relay 1 power`
	`  <1-3>  power id (1: AC, 2: DC1, 3:DC2)`
	`  any  Anyone power failure asserts relay`
	`Switch(config)# relay 1 power 1`
	`Switch(config)# relay 1 power 2`

Super Ring Failure	`Switch(config)# relay 1 ring`

Disable Relay	`Switch(config)# no relay`
	`  1  relay id`
	`Switch(config)# no relay 1` *`(Relay_ID: 1 or 2)`*
	`  <cr>`

Display	`Switch# show relay 1`
	` Relay Output Type : Port Link`
	` Port : 1, 2, 3, 4, 5`

Event Selection	

Event Selection	Switch(config)# warning-event
	  coldstart Switch cold start event
	  warmstart Switch warm start event
	  linkdown Switch link down event
	  linkup Switch link up event
	  authentication Authentication failure event
	  fault-relay Switch fault relay event
	  poe-powering Switch PoE powering or unpowered event
	  power Switch power failure event
	  sfp-ddm Switch SFP DDM abnormal event
	  super-ring Switch super ring topology change event
	  time-sync Switch time synchronize event

Example: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Example: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface list, ex: fa1,fa3-5,gi25-28 Switch(config)# warning-event linkup fa1gi2 Set fa5 link up event enable ok.

Display	Switch# show warning-event
	Warning Event:
	  Cold Start: Enabled
	  Warm Start: Disabled
	  Authentication Failure: Disabled
	  Link Down: fa4-5
	  Link Up: fa4-5
	  Power Failure:
	  Super Ring Topology Change: Disabled
	  Fault Relay: Disabled
	  Time synchronize Failure: Disabled
	  PoE Powering:
	  SFP DDM: Enabled

Syslog Configuration	
Local Mode	`Switch(config)# log syslog local`
Server Mode	`Switch(config)# log syslog remote 192.168.250.33`
Both	`Switch(config)# log syslog local` `Switch(config)# log syslog remote 192.168.250.33`
Disable	`Switch(config)# no log syslog local`
SMTP Configuration	
SMTP Enable	`Switch(config)# smtp-server enable email-alert` `SMTP Email Alert set enable ok.`

Sender mail	`Switch(config)# smtp-server server 192.168.250.100`
	`  ACCOUNT  SMTP server mail account, ex: admin@comtrol.com`
	`Switch(config)# smtp-server server 192.168.250.100 admin@comtrol.com`
	`SMTP Email Alert set Server: 192.168.250.100, Account: admin@comtrol.com ok.`

Receiver mail	`Switch(config)# smtp-server receipt 1 abc@comtrol.com` `SMTP Email Alert set receipt 1: abc@comtrol.com ok.`

Authentication with user name and password	`Switch(config)# smtp-server authentication username admin password admin`
	`SMTP Email Alert set authentication Username: admin, Password: admin`
	Note: *You can assign string to user name and password.*

Disable SMTP	`Switch(config)# no smtp-server enable email-alert` `SMTP Email Alert set disable ok.`
Disable Authentication	`Switch(config)# no smtp-server authentication` `SMTP Email Alert set Authentication disable ok.`

Display	`Switch# sh smtp-server`
	`SMTP Email Alert is Enabled`
	`  Server: 192.168.250.100, Account: admin@comtrol.com`
	`  Authentication: Enabled`
	`  Username: admin, Password: admin`
	`SMTP Email Alert Receipt:`
	`  Receipt 1: abc@comtrol.com`
	`  Receipt 2:`
	`  Receipt 3:`
	`  Receipt 4:`

Monitor and Diag (CLI)

The ES7528 provides several types of features for you to monitor the status of the switch or diagnostic for you to check the problem when encountering problems related to the switch. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log, and Ping.

Optionally, you can use the web user interface for configuration, see *Monitor and Diag* on Page 123.

This table provides detailed information about command lines of the Monitor and Diag configuration.

MAC Address Table	

Aging Time	`Switch(config)# mac-address-table aging-time 350`
	`mac-address-table aging-time set ok!`
	Note: *The default aging timeout value is 300.*

Add Static Unicast MAC address	`Switch(config)# mac-address-table static 00c0.4e32.0101 vlan 1 interface fastethernet5`
	`mac-address-table ucast static set ok!`
	Rule: mac-address-table static MAC_address VLAN VID interface interface_name

Add Multicast MAC address	`Switch(config)# mac-address-table multicast 00c0.4e32.0101 vlan 1 interface fa3-4`
	`Adds an entry in the multicast table ok!`
	Rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range

Show MAC Address Table – All types	`Switch# show mac-address-table`
	
	`***** UNICAST MAC ADDRESS *****`
	`Destination Address  Address Type  Vlan  Destination Port`
	`00c0.4e32.ca3b  Dynamic  1  fa1`
	`00c0.4e32.0386  Dynamic  1  fa2`
	`00c0.4e32.0101  Static  1  fa3`
	`00c0.4e32.0102  Static  1  fa3`
	`00c0.4e32.0100  Management  1`
	`***** MULTICAST MAC ADDRESS *****`
	`Vlan  Mac Address  COS  Status  Ports`
	`1  00c0.4e32.0800  0  fa6`
	`1  00c0.4e32.fffa  0  fa4,fa6`

Show MAC Address Table – Dynamic Learnt MAC addresses	`Switch# show mac-address-table dynamic`
	`Destination Address  Address Type  Vlan  Destination Port`
	`00c0.4e32.ca3b  Dynamic  1  fa4`
	`00c0.4e32.0386  Dynamic  1  fa6`

Show MAC Address Table – Multicast MAC addresses	`Switch# show mac-address-table multicast`
	`Vlan  Mac Address  COS  Status  Ports`
	`1  00c0.4e32.0800  0  fa5-6`
	`1  00c0.4e32.fffa  0  fa3,fa5-6`

MAC Address Table (continued)	
Show MAC Address Table – Static MAC addresses	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ---------- ---------- ---- ---------- 00c0.4e32.0101 Static 1 fa4 00c0.4e32.0102 Static 1 fa5
Show Aging timeout time	Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec.
Port Statistics	
Port Statistics	Switch# show rmon statistics fa4 (select interface) Interface fastethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 598, Broadcast: 1764, Multicast: 160 Pause: 0, Undersize: 0, Fragments: 0 Oversize: 0, Jabbers: 0, Discards: 0 Filtered: 0, RxError: 0, FCSError: 0 Outbound: Good Octets: 330500 Unicast: 602, Broadcast: 1, Multicast: 2261 Pause: 0, Deferred: 0, Collisions: 0 SingleCollision: 0, MultipleCollision: 0 ExcessiveCollision: 0, LateCollision: 0 Filtered: 0, FCSError: 0 Number of frames received and transmitted with a length of: 64: 2388, 65to127: 142, 128to255: 11 256to511: 64, 512to1023: 10, 1024toMaxSize: 42
Port Mirroring	
Enable Port Mirror	Switch(config)# mirror en Mirror set enable ok.
Disable Port Mirror	Switch(config)# mirror disable Mirror set disable ok.
Select Source Port	Switch(config)# mirror source fa1-2 both Received and transmitted traffic rx Received traffic tx Transmitted traffic Switch(config)# mirror source fa1-2 both Mirror source fa1-2 both set ok. ***Note:*** *Select source port list and TX/RX/Both mode.*
Select Destination Port	Switch(config)# mirror destination fa6 Mirror destination fa6 set ok

Port Mirroring (continued)	
Display	Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination Port : fa6 Egress Monitor Destination Port : fa6 Ingress Source Ports :fa1,fa2, Egress Source Ports :fa1,fa2,
Event Log	
Display	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Topology Discovery (LLDP)	

Enable LLDP	Switch(config)# lldp
	  holdtime Specify the holdtime of LLDP in seconds
	  run Enable LLDP
	  timer Set the transmission frequency of LLDP in seconds
	Switch(config)# lldp run
	LLDP is enabled!

Change LLDP timer	Switch(config)# lldp holdtime <10-255> Valid range is 10~255 Switch(config)# lldp timer <5-254> Valid range is 5~254
Ping	
Ping IP	Switch# ping 192.168.11.14 PING 192.168.11.14 (192.168.11.14): 56 data bytes 64 bytes from 192.168.11.14: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.11.14: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.11.14 ping statistics --- packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 1.3/1.3/1.4 ms

Saving to Flash (CLI)

Save Configuration allows you to save any configuration you just made to the flash. Powering off the switch without saving the configuration causes loss of the new settings.

Saving to Flash	

Save to Flash	`SWITCH# write`
	`Building Configuration…`
	`[OK]`
	
	`Switch# copy running-config startup-config`
	`Building Configuration...`
	`[OK]`

Logging Out (CLI)

The CLI connection logs out of configure terminal mode, if you do not input any command after 30 seconds.

Logging Out	

Logout	`SWITCH> exit`
	
	`SWITCH# exit`

Service (CLI)

The service command provides the ability to disable HTTP and Telnet.

Note: *There is not a web user interface page for the service command.*

Service	
Disable HTTP	`Switch(config)# service http disable` `Switch(config)#`
Enable HTTP	`Switch(config)# service http enable` `Switch(config)#`
Disable telnet	`Switch(config)# service telnet disable` `Switch(config)#`
Enable telnet	`Switch(config)# service telnet enable` `Switch(config)#`

Complete CLI List

This section provides the complete listing of RocketLinx ES7528 commands with the supporting options:

User EXEC Mode

For information about accessing *User EXEC* mode, see *User EXEC Mode* on Page 201.

```
Switch> list
  enable
  exit
  list
  ping A.B.C.D
  ping WORD
  ping X:X::X:X
  quit
  show gvrp statistics [IFNAME]
  show ip forwarding
  show ip route
  show ip route A.B.C.D
  show ip route A.B.C.D/M
  show ip route supernets-only
  show version
  telnet WORD
  telnet WORD PORT
  traceroute WORD
```

Privileged EXEC Mode

For information about accessing *Privileged EXEC* mode, see *Privileged EXEC Mode* on Page 202.

```
Switch# list
  archive download-boot /overwrite tftp IPADDRESS IMAGE
  archive download-sw /overwrite tftp IPADDRESS IMAGE
  clear event-log
  clear gvrp statistics [IFNAME]
  clear lacp counters
  clear mac-address-table dynamic
  clear mac-address-table dynamic address MACADDR
  clear mac-address-table dynamic interface IFNAME
  clear mac-address-table dynamic vlan VLANID
  clear redundant-ring statistics [0-31]
  clear rmon statistics [IFNAME]
  clear spanning-tree counters
  clear spanning-tree counters interafce IFNAME
  clear spanning-tree detected-protocols
  clear spanning-tree detected-protocols interface IFNAME
  clock set TIME MONTH DAY YEAR
  configure terminal
  copy running-config startup-config
  copy startup-config tftp: URL
  copy tftp: URL (ssh-dss|ssh-rsa)
  copy tftp: URL ssl-cert
  copy tftp: URL startup-config
  debug dot1x all
  debug dot1x errors
  debug dot1x events
  debug dot1x packets
  debug dot1x registry
  debug dot1x state-machine
  debug gmrp
  debug gvrp (all|rcv|tx|gvrp_event|vlan_event)
  debug ip dhcp (all|event)
  debug ip dhcp snooping
  debug ip igmp
  debug ip igmp snooping (all|group|management|router|timer)
  debug l2 mac (all|trace|debug)
  debug lacp (all|event|fsm|misc|packet)
  debug lldp
  debug meminfo
  debug mirror (enable|disable)
  debug poe (all|trace|debug)
  debug proto pdu
  debug ptpd all
  debug qos
  debug rate-limit
  debug redundant-ring (pdu|trace|debug|rapid-dual-homing|rstp|multi-ring|all) <0-
   31>
  debug snmp
  debug spanning-tree (all|bpdu|config|events|general|root|sync|tc)
  debug sw-rate-limit get <0-64>
```

Privileged EXEC Mode (continued)

```
debug sw-rate-limit ioctl_dump
debug sw-rate-limit pkt_dump
debug sw-rate-limit set <0-64> <0-1000>
debug sw-rate-limit set <0-64> off
debug trunk
debug vlan (all|trace|debug)
disable
dot1x initialize interface IFNAME
dot1x reauthenticate interface IFNAME
end
exit
list
mac access-group dump <1-1536>
mac access-group show
no debug dot1x all
no debug dot1x errors
no debug dot1x events
no debug dot1x packets
no debug dot1x registry
no debug dot1x state-machine
no debug gmrp
no debug gvrp (all|rcv|tx|gvrp_event|vlan_event)
no debug ip dhcp (all|event)
no debug ip dhcp snooping
no debug ip igmp
no debug ip igmp snooping (all|group|management|router|timer)
no debug l2 mac (all|trace|debug)
no debug lacp (all|event|fsm|misc|packet)
no debug lldp
no debug mirror
no debug poe (all|trace|debug)
no debug proto
no debug ptpd
no debug qos
no debug rate-limit
no debug redundant-ring <0-31>
no debug snmp
no debug spanning-tree (all|bpdu|config|events|general|root|sync|tc)
no debug sw-rate-limit ioctl_dump
no debug sw-rate-limit pkt_dump
no debug trunk
no debug vlan (all|trace|debug)
no pager
pager
ping A.B.C.D
ping WORD
ping X:X::X:X
quit
reboot
reload default-config file
reload default-ssh file
reload default-ssl file
```

Privileged EXEC Mode (continued)

```
show acceptable frame type [IFNAME]
show administrator
show clock
show clock summer-time
show clock timezone
show debugging dot1x
show debugging gvrp
show debugging ip dhcp
show debugging ip igmp
show debugging ip igmp snooping
show debugging lacp
show debugging snmp
show debugging spanning-tree
show deny host mac-address
show dot1q-tunnel
show dot1x
show dot1x all
show dot1x authentic-method
show dot1x interface IFNAME
show dot1x radius
show dot1x statistics interface IFNAME
show dot1x username
show event-log
show garp timer [IFNAME]
show gmrp
show gvrp configuration [IFNAME]
show gvrp portstate IFNAME VID
show hardware led
show hardware mac
show ingress filtering [IFNAME]
show interface [IFNAME]
show interface vlan [VLANID]
show ip access-group [INTERFACE]
show ip access-list
show ip access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)
show ip dhcp relay
show ip dhcp server statistics
show ip forwarding
show ip igmp
show ip igmp group
show ip igmp interface IFNAME
show ip igmp query-interval
show ip igmp query-max-response-time
show ip igmp snooping
show ip igmp snooping multicast (dynamic|user|all) [VLANLIST]
show ip igmp snooping multicast count
show ip igmp snooping vlan (VLANLIST|all)
show ip igmp timers
show ip igmp version
show ip route
show ip route A.B.C.D
show ip route A.B.C.D/M
```

Privileged EXEC Mode (continued)

```
show ip route supernets-only
show ipv6 neighbour
show ipv6 route
show l2_interface [IFNAME]
show lacp counters [GROUPID]
show lacp group [1-8]
show lacp internal [1-8]
show lacp neighbor [1-8]
show lacp port-setting [IFNAME]
show lacp system-id
show lacp system-priority
show lldp
show lldp neighbors
show lldp power remote IFNAME
show lldp statistics
show mac access-group [INTERFACE]
show mac access-list [WORD]
show mac-address-table
show mac-address-table aging-time
show mac-address-table dynamic
show mac-address-table dynamic address MACADDR
show mac-address-table dynamic interface IFNAME
show mac-address-table dynamic vlan VLANID
show mac-address-table multicast
show mac-address-table multicast MACADDR vlan VLANID
show mac-address-table multicast filtering
show mac-address-table static
show mac-address-table static address MACADDR
show mac-address-table static interface IFNAME
show mac-address-table static vlan VLANID
show mirror
show modbus
show module
show module <1-3>
show nameserver
show netvision password
show ntp associations
show poe interface [IFNAME]
show poe pd-detect
show poe schedule [IFNAME]
show poe system
show ptpd
show qos cos-map
show qos dscp-map
show qos port-priority
show qos queue-sched
show rate-limit egress [IFNAME]
show rate-limit ingress [IFNAME]
show redundant-ring [0-31]
show relay 1
show rmon statistics [IFNAME]
show running-config
```

Privileged EXEC Mode (continued)

```
show service
show sfp
show sfp ddm
show smtp-server
show smtp-server authentication
show smtp-server email-alert
show smtp-server receipt
show smtp-server server
show snmp-server community
show snmp-server contact
show snmp-server host
show snmp-server location
show snmp-server name
show snmp-server trap
show snmp-server user
show spanning-tree active
show spanning-tree interface IFNAME
show spanning-tree mst
show spanning-tree mst <0-15>
show spanning-tree mst <0-15> interface IFNAME
show spanning-tree mst configuration
show spanning-tree mst interface IFNAME
show spanning-tree mst root
show spanning-tree summary
show startup-config
show storm-control [IFNAME]
show system mtu
show system status
show trunk group [1-8]
show trunk load-balance group [1-8]
show version
show vlan
show vlan (static|dynamic) [VLANID]
show vlan VLANID
show vlan management
show vlan name VLANAME
show vlan private-vlan
show vlan private-vlan port-list
show vlan private-vlan type
show warning-event
telnet WORD
telnet WORD PORT
terminal length <0-512>
terminal no length
traceroute WORD
write
write file
write memory
write terminal
```

Global Configuration Mode

For information about accessing *Global Configuration* mode, see *Global Configuration Mode* on Page 207.

```
Switch(config)# list
  access-list test
  administrator NAME PASSWORD
  clock set TIME MONTH DAY YEAR
  clock summer-time (enable|disable)
  clock summer-time <1-5> <0-6> <1-12> START_TIME <1-5> <0-6> <1-12> END_TIME
  clock timezone
   (01|02|03|04|05|06|07|08|09|10|11|12|13|14|15|16|17|18|19|20|21|22|23|24|25|26|27
   |28|29|30|31|32|33|34|35|36|37|38|39|40|41|42|43|44|45|46|47|48|49|50|51|52|53|54
   |55|56|57|58|59|60|61|62|63|64|65|66|67|68|69|70|71|72|73|74)
  default dot1x system-auth-control
  default gvrp configuration
  default ip igmp snooping
  dot1x authentic-method (radius|local)
  dot1x radius secondary-server-ip A.B.C.D key RADIUS_KEY [PORT] [PORT]
  dot1x radius server-ip A.B.C.D key RADIUS_KEY [PORT] [PORT]
  dot1x system-auth-control
  dot1x username WORD passwd WORD vlan <1-4094>
  end
  exit
  gmrp mode (enable|disable)
  gmrp mode (enable|disable) IFNAME
  gvrp mode (enable|disable)
  gvrp mode (enable|disable) IFNAME
  gvrp registration (normal|fixed|forbidden) IFNAME
  hostname .DWORD
  interface IFNAME
  interface vlan VLAN-ID
  ip access-list extended (<100-199>|<2000-2699>)
  ip access-list extended WORD
  ip access-list standard (<1-99>|<1300-1999>)
  ip access-list standard WORD
  ip forwarding
  ip igmp snooping
  ip igmp snooping immediate-leave
  ip igmp snooping immediate-leave vlan (VLANLIST|all)
  ip igmp snooping last-member-query-interval TIMEVALUE
  ip igmp snooping last-member-query-interval TIMEVALUE vlan (VLANLIST|all)
  ip igmp snooping source-only-learning
  ip igmp snooping vlan (VLANLIST|all)
  ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)
  ip route A.B.C.D/M (A.B.C.D|INTERFACE)
  ipv6 route X:X::X:X/M (X:X::X:X|INTERFACE)
  lacp group <1-8> IFLIST
  lacp system-priority <1-65535>
  list
  lldp holdtime <10-255>
  lldp run
  lldp timer <5-254>
  log file FILENAME
```

Global Configuration Mode (continued)

```
log stdout
log syslog local
log syslog remote A.B.C.D
mac access-list extended NAME
mac-address-table aging-time TIMEVALUE
mac-address-table multicast MACADDR vlan VLANID interface IFLIST
mac-address-table multicast filtering
mac-address-table static MACADDR vlan VLANID interface IFNAME
mirror (enable|disable)
mirror destination IFNAME
mirror source IFLIST (rx|tx|both)
modbus (enable|disable)
modbus idle-timeout <200-10000>
modbus master <1-20>
modbus port <1-65535>
nameserver A.B.C.D
netvision password PASS
no administrator
no clock set
no clock summer-time
no clock timezone
no dot1x authentic-method
no dot1x radius secondary-server-ip
no dot1x system-auth-control
no dot1x username WORD
no hostname [HOSTNAME]
no interface IFNAME
no interface vlan VLAN-ID
no ip access-list extended (<100-199>|<2000-2699>|WORD)
no ip access-list standard (<1-99>|<1300-1999>|WORD)
no ip forwarding
no ip igmp snooping
no ip igmp snooping immediate-leave
no ip igmp snooping immediate-leave vlan (VLANLIST|all)
no ip igmp snooping last-member-query-interval
no ip igmp snooping last-member-query-interval vlan (VLANLIST|all)
no ip igmp snooping source-only-learning
no ip igmp snooping vlan (VLANLIST|all)
no ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)
no ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE) <1-255>
no ip route A.B.C.D/M (A.B.C.D|INTERFACE)
no ipv6 route X:X::X:X/M (X:X::X:X|INTERFACE)
no lacp group <1-8>
no lacp system-priority
no lldp run
no log file
no log stdout
no log syslog local
no log syslog remote
no mac access-list extended NAME
no mac-address-table aging-time
no mac-address-table multicast MACADDR vlan VLANID
```

Global Configuration Mode (continued)

```
no mac-address-table multicast MACADDR vlan VLANID interface IFLIST
no mac-address-table multicast filtering
no mac-address-table static MACADDR vlan VLANID interface IFNAME
no mirror destination
no mirror source IFLIST (rx|tx|both)
no nameserver A.B.C.D
no netvision password
no ntp peer (primary|secondary)
no poe pd-detect A.B.C.D
no ptpd run
no qos cos-map
no qos dscp-map
no qos queue-sched
no relay 1
no smtp-server authentication
no smtp-server authentication username password
no smtp-server enable email-alert
no smtp-server receipt <1-4>
no smtp-server server
no snmp-server community WORD (ro|rw)
no snmp-server community trap
no snmp-server contact
no snmp-server enable trap
no snmp-server host A.B.C.D [VERSION]
no snmp-server location
no snmp-server name
no snmp-server user WORD v3
no spanning-tree bridge-times
no spanning-tree forward-time
no spanning-tree hello-time
no spanning-tree max-age
no spanning-tree mst MSTMAP priority
no spanning-tree mst configuration
no spanning-tree mst forward-time
no spanning-tree mst hello-time
no spanning-tree mst max-age
no spanning-tree mst max-hops
no spanning-tree priority
no spanning-tree transmission-limit
no system mtu
no trunk group <1-8>
no trunk load-balance group <1-8>
no vlan [VLANID]
no warning-event (coldstart|warmstart)
no warning-event (linkdown|linkup) [IFLIST]
no warning-event authentication
no warning-event fault-relay
no warning-event poe-powering [IFLIST]
no warning-event power <1-3>
no warning-event sfp-ddm
no warning-event super-ring
no warning-event time-sync
```

Global Configuration Mode (continued)

```
no write-config (daemon|integrated)
ntp peer (enable|disable)
ntp peer (primary|secondary) IPADDRESS
poe (enable|disable)
poe budget (DC1|DC2) <0-400>
poe budget vin (DC1|DC2) <46-57>
poe budget warning <0-100>
poe pd-detect (enable|disable)
poe pd-detect A.B.C.D <10-3600>
ptpd run
ptpd run preferred-clock
ptpd run slave
qos cos-map PRIORITY QUEUE
qos dscp-map PRIORITY QUEUE
qos queue-sched rr
qos queue-sched sp
qos queue-sched wrr <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10>
redundant-ring <0-31>
relay 1 dry <0-4294967295> <0-4294967295>
relay 1 ping WORD
relay 1 ping WORD reset <1-65535> <0-65535>
relay 1 port PORTLIST
relay 1 power <1-3>
relay 1 power any
relay 1 ring
router dhcp
service http (enable|disable)
service telnet (enable|disable)
sfp ddm eject all
smtp-server authentication
smtp-server authentication username WORD password WORD
smtp-server enable email-alert
smtp-server receipt <1-4> EMAIL
smtp-server server A.B.C.D ACCOUNT
snmp-server community WORD (ro|rw)
snmp-server community trap WORD
snmp-server contact .DWORD
snmp-server enable trap
snmp-server host A.B.C.D
snmp-server host A.B.C.D version (1|2) [COMMUNITY]
snmp-server location .DWORD
snmp-server name .DWORD
snmp-server user WORD v3 auth (md5|sha) WORD
snmp-server user WORD v3 noauth
snmp-server user WORD v3 priv (md5|sha) WORD des WORD
spanning-tree (enable|disable)
spanning-tree bridge-times <4-30> <6-40> <1-10>
spanning-tree forward-time <4-30>
spanning-tree hello-time <1-10>
spanning-tree max-age <6-40>
spanning-tree mode (stp|rst)
spanning-tree mode mst
```

Global Configuration Mode (continued)

```
spanning-tree mst MSTMAP priority <0-61440>
spanning-tree mst configuration
spanning-tree mst configuration
spanning-tree mst hello-time <1-10>
spanning-tree mst max-age <6-40>
spanning-tree mst max-hops <1-40>
spanning-tree mst sync vlan <1-4094>
spanning-tree pathcost method (long|short)
spanning-tree priority <0-61440>
spanning-tree transmission-limit <1-10>
system mtu <1500-1546>
system mtu jumbo <1500-9216>
trunk group <1-8> IFLIST
trunk load-balance group <1-8> (src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-
 ip)
vlan <1-4094>
warning-event (coldstart|warmstart)
warning-event (linkdown|linkup) [IFLIST]
warning-event authentication
warning-event fault-relay
warning-event poe-powering [IFLIST]
warning-event power <1-3>
warning-event sfp-ddm
warning-event super-ring
warning-event time-sync
write-config (daemon|integrated)
```

Port Interface Configuration Mode

For information about accessing *Port Interface Configuration* mode, see *Port Interface Configuration Mode* on Page 212.

```
Switch(config)# interface fa1
Switch(config-if)# list
  acceptable frame type (all|vlantaggedonly)
  auto-negotiation
  description .LINE
  dot1x admin-control-direction (both|in)
  dot1x default
  dot1x guest-vlan <1-4094>
  dot1x host-mode (single-host|multi-host)
  dot1x max-req <1-10>
  dot1x port-control (auto|force-authorized|force-unauthorized)
  dot1x reauthentication
  dot1x timeout (reauth-period|quiet-period|tx-period|supp-timeout|server-timeout)
   TIMEVALUE
  duplex (half|full)
  end
  ethertype [0x0800-0xFFFF]
  exit
  flowcontrol (off|on)
  garp join-timer <10-10000>
  garp leave-timer <30-30000>
  garp leaveall-timer <150-150000>
  ingress filtering (enable|disable)
  ip access-group (<1-199> |<1300-2699>|WORD) in
  lacp port-priority <1-65535>
  lacp timeout (long|short)
  list
  loopback
  mac access-group NAME in
  mdix auto
  no description
  no dot1x admin-control-direction
  no dot1x guest-vlan
  no dot1x host-mode
  no dot1x max-req
  no dot1x port-control
  no dot1x reauthentication
  no dot1x timeout (reauth-period|quiet-period|tx-period|supp-timeout|server-
   timeout)
  no duplex
  no garp join-timer
  no garp leave-timer
  no garp leaveall-timer
  no ip access-group
  no lacp port-priority
  no lacp timeout
  no loopback
  no mac access-group
  no mdix auto
  no poe schedule <0-6>
```

Port Interface Configuration Mode (continued)

```
no qos priority
no rate-limit egress bandwidth
no rate-limit ingress bandwidth
no shutdown
no spanning-tree bpdufilter
no spanning-tree bpduguard
no spanning-tree cost
no spanning-tree edge-port
no spanning-tree link-type
no spanning-tree mst MSTMAP cost
no spanning-tree mst MSTMAP port-priority
no spanning-tree port-priority
no spanning-tree stp-state
no speed
no storm-control (broadcast|dlf|multicast)
no switchport access vlan VLANID
no switchport block
no switchport dot1q-tunnel mode access
no switchport dot1q-tunnel mode uplink
no switchport mode private-vlan host
no switchport mode private-vlan promiscuous
no switchport port-security
no switchport private-vlan host-association
no switchport trunk native vlan
poe budget [POWER]
poe budget warning <0-100>
poe control-mode (user|schedule)
poe powering-mode (802.3af|forced)
poe powering-mode 802.3at (lldp|2-event)
poe priority (critical|high|low)
poe schedule <0-6> HOUR
poe type TYPE
poe user (enable|disable)
qos priority DEFAULT-PRIORITY
quit
rate-limit egress bandwidth <0-1000000>
rate-limit ingress bandwidth <0-1000000>
sfp ddm eject
shutdown
spanning-tree bpdufilter
spanning-tree bpduguard
spanning-tree cost <1-200000000>
spanning-tree edge-port
spanning-tree link-type (auto|point-to-point|shared)
spanning-tree mst MSTMAP cost <1-200000000>
spanning-tree mst MSTMAP port-priority <0-240>
spanning-tree port-priority <0-240>
spanning-tree stp-state (enable|disable)
speed (10|100|1000)
storm-control (broadcast|dlf|multicast) <0-262143>
switchport access vlan VLANID
switchport access vlan add VLANLIST
```

Port Interface Configuration Mode (continued)

```
  switchport access vlan remove VLANLIST
  switchport block (multicast|unicast|both)
  switchport dot1q-tunnel mode access
  switchport dot1q-tunnel mode uplink
  switchport mode private-vlan host
  switchport mode private-vlan promiscuous
  switchport port-security
  switchport private-vlan host-association <2-4094> <2-4094>
  switchport private-vlan mapping <2-4094> add VLANLIST
  switchport private-vlan mapping <2-4094> remove VLANLIST
  switchport trunk allowed vlan add VLANLIST
  switchport trunk allowed vlan remove VLANLIST
  switchport trunk native vlan VLANID
```

VLAN Interface Configuration Mode

For information about accessing VLAN Interface Configuration mode, see *VLAN Interface Configuration Mode* on Page 214.

```
Switch(config-if)# interface vlan1
Switch(config-if)# list
  description .LINE
  end
  exit
  ip address A.B.C.D/M
  ip dhcp client
  ip dhcp client renew
  ip igmp
  ip igmp last-member-query-count CNT
  ip igmp last-member-query-interval SECONDS
  ip igmp query-interval SECONDS
  ip igmp query-max-response-time SECONDS
  ip igmp robustness-variable CNT
  ip igmp version (1|2)
  ipv6 address X:X::X:X/M
  list
  no description
  no ip address A.B.C.D/M
  no ip dhcp client
  no ip igmp
  no ipv6 address X:X::X:X/M
  no shutdown
  quit
  shutdown
```

ModBus TCP /IP Support

This section provides the following information:

Overview

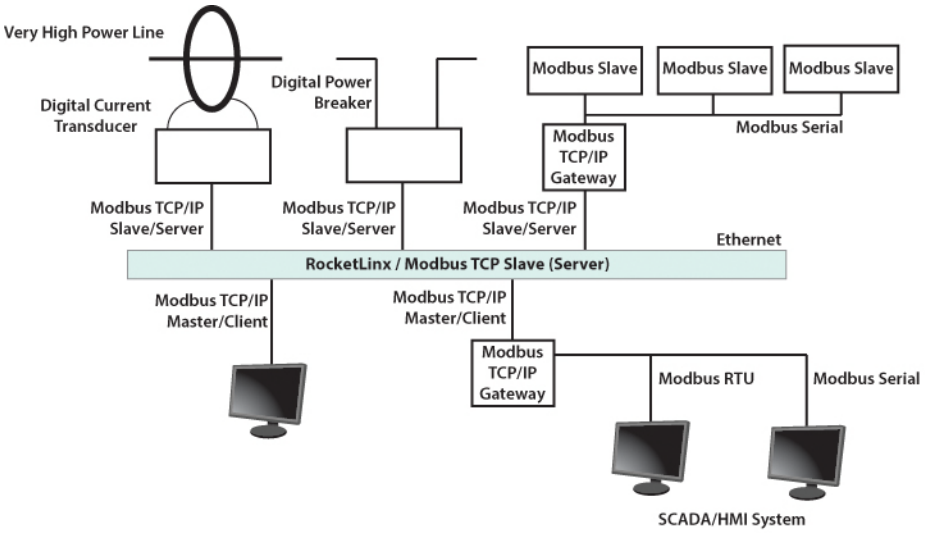
The ES7528 supports Modbus TCP/IP communications through the CLI, which does not support Modbus ASCII or Modbus RTU. This functionality is not available on a web user interface page.

Modbus TCP/IP is commonly used to communicate over TCP/IP networks, connecting over Port 502. Modbus TCP/IP is used in industrial automatic communications systems and has become a standard protocol for industrial communications to transfer data to analog I/O devices or PLC systems.

Modbus TCP/IP defines a simple protocol data unit independent of the underlying data link layer. The Modbus TCP/IP packet includes three parts:

- MBAP header is used in the TCP/IP header to identify the Modbus application data unit. The MBAP header also includes a unit identifier to recognize and communicate between multiple independent Modbus end units.
- Function code
- Data payload

Modbus devices communicate using a master (client) /slave (server) architecture, only one device can initiate a transaction and the others respond to the master/client. The other devices (slave/server) respond by supplying the requested data to the master/client, or by taking the action requested in the query. The slave/server can be any peripheral device that processes information and sends the output data to the master using Modbus TCP/IP protocol.



The ES7528 operates as slave/server device, while a typical master/client device is a host computer running appropriate application software, for example, a SCADA / HMI system. The ES7528 can be polled through

Ethernet, thus the Modbus TCP/IP master can read or write to the Modbus registers provided by the Modbus TCP/IP.

The ES7528 firmware provides Modbus TCP/IP registers that map to the ES7528 operating system information which, includes the description, IP address, power status, interface status, interface information and inbound/outbound packet statistics. With the register support, you can read the information through the Modbus TCP/IP based progress/ display/ monitor applications and monitor the status of the switch easily.

Modbus TCP/IP Function Codes

Modbus TCP/IP devices use a subset of the standard Modbus TCP/IP function codes to access device-dependent information. Modbus TCP/IP function codes are defined in the following table.

Function Code	Name	Usage
01	Read Coils	Reads the state of a digital output.
02	Read Input Status	Reads the state of a digital input.
03	Read Holding Register	Reads the holding register in 16-bit register format.
04 (see note)	Read Input Registers	Reads data in 16-bit register format.
05	Write Coil	Writes data to force a digital output ON/OFF.
06	Write Single Register	Writes data in 16-bit register format.
15	Force Multiple Coils	Writes data to force multiple consecutive coils.
Note: *The ES7528 supports Function Code 04, the Read Input Registers. With this support, the remote SCADA or other Modbus TCP/IP applications can poll the information of the device and monitor the major status of the ES7528.*		

Error Checking

The utilization of the error checking helps eliminate errors caused by noise in the communications link. In Modbus TCP/IP mode, messages include an error-checking field that is based on a Cyclical Redundancy Check (CRC) method. The CRC field checks the contents of the entire message. It is applied regardless of any parity check method used for the individual BYTE characters of the message. The CRC value is calculated by the transmitting device, which appends the CRC to the message. The receiving device recalculates a CRC during receipt of the message, and compares the calculated value to the actual value it received in the CRC filed.

Exception Response

If an error occurs, the slave sends an exception response message to master consisting of the slave address, function code, exception response code and error check field. In an exception response, the slave sets the high-order bit (MSB) of the response function code to one.

Code	Name	Descriptions
01	Illegal Function	The message function received is not an allowable action.
02	Illegal Data Address	The address referenced in the data field is not valid.
03	Illegal Data Value	The value referenced at the addressed device location is not within range.
04	Slave Device Failure	An unrecoverable error occurred while the slave was attempting to perform the requested action.

Code	Name	Descriptions
05	Acknowledge	The slave has accepted the request and processing it, but a long duration of time is required to do so.
06	Slave Device Busy	The slave is engaged in processing a long-duration program command.
07	Negative Acknowledge	The slave cannot perform the program function received in the query.
08	Memory Parity Error	The slave attempted to read extended memory, but detected a parity error in the memory.

Modbus TCP Register Table

The latest firmware provides the initial release of the Modbus TCP/IP client service support for factory automation applications. You can implement the modbus command using the command line interface in console and Telnet modes, which allows you to modify some parameters such as, idle time, number of Modbus masters, and the Modbus service port.

Note: *The Modbus TCP client returns 0xFFFF to a Modbus master when pulling a reserved address.*

Word Address	Data Type	Description
System Information		
0x0000	16 words	Vender Name = “Comtrol” Word 0 Hi byte = ‘C’ Word 0 Lo byte = ‘o’ Word 1 Hi byte = ‘m’ Word 1 Lo byte = ‘t’ Word 2 Hi byte = ‘r’ Word 2 Lo byte = ‘o’ Word 3 Hi byte = ‘l’ Word 3 Lo byte = ‘\0’ (other words = 0)
0x0010	16 words	Product Name = "ES7528" Word 0 Hi byte = ‘E’ Word 0 Lo byte = ‘S’ Word 1 Hi byte = ‘7’ Word 1 Lo byte = ‘5’ Word 2 Hi byte = ‘2’ Word 2 Lo byte = ‘8’ Word 3 Hi byte = ‘\0’ (other words = 0)
0x0020	128 words	SNMP system name (string)
0x00A0	128 words	SNMP system location (string)

Word Address	Data Type	Description
0x0120	128 words	SNMP system contact (string)
0x01A0	32 words	SNMP system OID (string)
0x01C0	2 words	System uptime (unsigned long)
0x01C2 to 0x01FF	60 words	Reserved address space
0x0200	2 words	Hardware version
0x0202	2 words	S/N information
0x0204	2 words	CPLD version
0x0206	2 words	Bootloader version
0x0208	2 words	Firmware Version Word 0 Hi byte = major Word 0 Lo byte = minor Word 1 Hi byte = reserved Word 1 Lo byte = reserved
0x020A	2 words	Firmware Release Date Firmware was released on 2010-08-11 at 09 o'clock Word 0 = 0x0B09 Word 1 = 0x0A08
0x020C	3 words	Ethernet MAC Address For example: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x0300	2 words	IP address For example: IP = 192.168.250.250 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x020F to 0x2FF	241 words	Reserved address space
0x0302	2 words	Subnet Mask
0x0304	2 words	Default Gateway
0x0306	2 words	DNS Server
0x0308 to 0x3FF	248 words	Reserved address space (IPv6 or others)
0x0400	1 word	AC1 0x0000:Off 0x0001:On 0xFFFF: unavailable

Word Address	Data Type	Description
0x0401	1 word	AC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0402	1 word	DC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0403	1 word	DC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0404 to 0x040F	12 words	Reserved address space
0x0410	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0411	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0412	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0413	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0414 to 0x041F	12 words	Reserved address space
0x0420	1 word	RDY 0x0000:Off 0x0001:On
0x0421	1 word	RM 0x0000:Off 0x0001:On
0x0422	1 word	RF 0x0000:Off 0x0001:On
0x0423	1 word	RS
Port Information (32 Ports)		
0x1000 to 0x11FF	16 words	Port Description

Word Address	Data Type	Description
0x1200 to 0x121F	1 word	Administrative Status 0x0000: disable 0x0001: enable
0x1220 to 0x123F	1 word	Operating Status 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1240 to 0x125F	1 word	Duplex 0x0000: half 0x0001: full 0x0003: auto (half) 0x0004: auto (full) 0x0005: auto 0xFFFF: unavailable
0x1260 to 0x127F	1 word	Speed 0x0001: 10 0x0002: 100 0x0003: 1000 0x0004: 2500 0x0005: 10000 0x0101: auto 10 0x0102: auto 100 0x0103: auto 1000 0x0104: auto 2500 0x0105: auto 10000 0x0100: auto 0xFFFF: unavailable
0x1280 to 0x129F	1 word	Flow Control 0x0000: off 0x0001: on 0xFFFF: unavailable
0x12A0 to 0x12BF	1 word	Default Port VLAN ID 0x0001-0xFFFF
0x12C0 to 0x12DF	1 word	Ingress Filtering 0x0000: disable 0x0001: enable
0x12E0 to 0x12FF	1 word	Acceptable Frame Type 0x0000: all 0x0001: tagged frame only

Word Address	Data Type	Description
0x1300 to 0x131F	1 word	Port Security 0x0000: disable 0x0001: enable
0x1320 to 0x133F	1 word	Auto Negotiation 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1340 to 0x135F	1 word	Loopback Mode 0x0000: none 0x0001: MAC 0x0002: PHY 0xFFFF: unavailable
0x1360 to 0x137F	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x1380 to 0x139F	1 word	Default CoS Value for untagged packets
0x13A0 to 0x13BF	1 word	MDIX 0x0000: disable 0x0001: enable 0x0002: auto 0xFFFF: unavailable
0x13C0 to 0x13DF	1 word	Medium mode 0x0000: copper 0x0001: fiber 0x0002: none 0xFFFF: unavailable
0x13E0 to 0x14FF	288 words	Reserved address space
SFP Information (32 Ports)		
0x1500 to 0x151F	1 word	SFP Type
0x1520 to 0x153F	1 words	Wave length
0x1540 to 0x157F	2 words	Distance
0x1580 to 0x167F	8 words	Vender
SFP DDM Information (32 Ports)		
0x1800 to 0x181F	1 words	Temperature
0x1820 to 0x185F	2 words	Alarm Temperature
0x1860 to 0x187F	1 words	Tx power
0x1880 to 0x18BF	2 words	Warning Tx power

Word Address	Data Type	Description
0x18C0 to 0x18DF	1 words	Rx power
0x18E0 to 0x191F	2 words	Warning Rx power
0x1920 to 0x1FFF	1760 words	Reserved address space
Inbound Packet Information		
0x2000 to 0x203F	2 words	Good Octets
0x2040 to 0x207F	2 words	Bad Octets
0x2080 to 0x20BF	2 words	Unicast
0x20C0 to 0x20FF	2 words	Broadcast
0x2100 to 0x213F	2 words	Multicast
0x2140 to 0x217F	2 words	Pause
0x2180 to 0x21BF	2 words	Undersize
0x21C0 to 0x21FF	2 words	Fragments
0x2200 to 0x223F	2 words	Oversize
0x2240 to 0x227F	2 words	Jabbers
0x2280 to 0x22BF	2 words	Discards
0x22C0 to 0x22FF	2 words	Filtered frames
0x2300 to 0x233F	2 words	RxError
0x2340 to 0x237F	2 words	FCSError
0x2380 to 0x23BF	2 words	Collisions
0x23C0 to 0x23FF	2 words	Dropped Frames
0x2400 to 0x243F	2 words	Last Activated SysUpTime
0x2440 to 0x24FF	191 words	Reserved address space
Outbound Packet Information		
0x2500 to 0x253F	2 words	Good Octets
0x2540 to 0x257F	2 words	Unicast
0x2580 to 0x25BF	2 words	Broadcast
0x25C0 to 0x25FF	2 words	Multicast
0x2600 to 0x263F	2 words	Pause
0x2640 to 0x267F	2 words	Deferred
0x2680 to 0x26BF	2 words	Collisions
0x26C0 to 0x26FF	2 words	SingleCollision
0x2700 to 0x273F	2 words	MultipleCollision
0x2740 to 0x277F	2 words	ExcessiveCollision
0x2780 to 0x27BF	2 words	LateCollision
0x27C0 to 0x27FF	2 words	Filtered
0x2800 to 0x283F	2 words	FCSError
0x2840 to 0x29FF	447 words	Reserved address space
Number of Frames Received and Transmitted with a Length (Octets)		
0x2A00 to 0x2A3F	2 words	64
0x2A40 to 0x2A7F	2 words	65 to 127
0x2A80 to 0x2ABF	2 words	128 to 255
0x2AC0 to 0x2AFF	2 words	256 to 511
0x2B00 to 0x2B3F	2 words	512 to 1023

Word Address	Data Type	Description
0x2B40 to 0x2B7F	2 words	1024 to maximum size

CLI Commands for Modbus TCP/IP

The CLI commands for Modbus TCP/IP are listed in the following table.

Modbus TCP/IP Commands	
Enable	`Switch(config)# modbus enable`
Disable	`Switch(config)# modbus disable`

Set Modbus Interval Time between Request	`Switch(config)# modbus idle-timeout`
	`<200-10000>  Timeout value: 200-10000ms`
	`Switch(config)# modbus idle-timeout 200`

Set Modbus TCP Master Communicate Session	`Switch(config)# modbus master`
	`<1-20> Max Modbus TCP Master`
	`Switch(config)# modbus master 2`

Set Modbus TCP Listening Port	`Switch(config)# modbus port`
	`<1-65536>  Port Number`
	`Switch(config)# modbus port 502`

Technical Support

Comtrol SFP Modules

Comtrol provides a variety of SFP transceivers. These certified SFP transceivers can be identified by the RocketLinx ES7528 and displayed in the web user interface. We recommend using Comtrol SFP transceivers when configuring your RocketLinx ES7528.

Note: *Low quality SFP transceivers may result in poor network performance and may not meet claimed distance or temperature ratings.*

Comtrol Private MIB

Comtrol supports many standard MIBs for users to configure or monitor the switch configuration by SNMP. However, since some commands can't be found in standard MIBs, Comtrol provides a Private MIB file. Compile the private MIB file with your SNMP tool. The private MIB can be found on the *RocketLinx Software and Documentation* CD or downloaded it from the Comtrol FTP site.

The Private MIB tree is the same as the web tree. This is easier to understand and use. If you are not familiar with a standard MIB, you can directly use the private MIB to manage /monitor the switch, without the need to learn or find where the OIDs of the commands are.

Comtrol Support

You can use one of the following methods to contact Comtrol.

Contact Method	Web Address or Phone Number
Support	http://www.comtrol.com/pub/en/support
Downloads	ftp://ftp.comtrol.com/html/ES7528_main.htm
Web Site	http://www.comtrol.com
Phone	763.957.6000