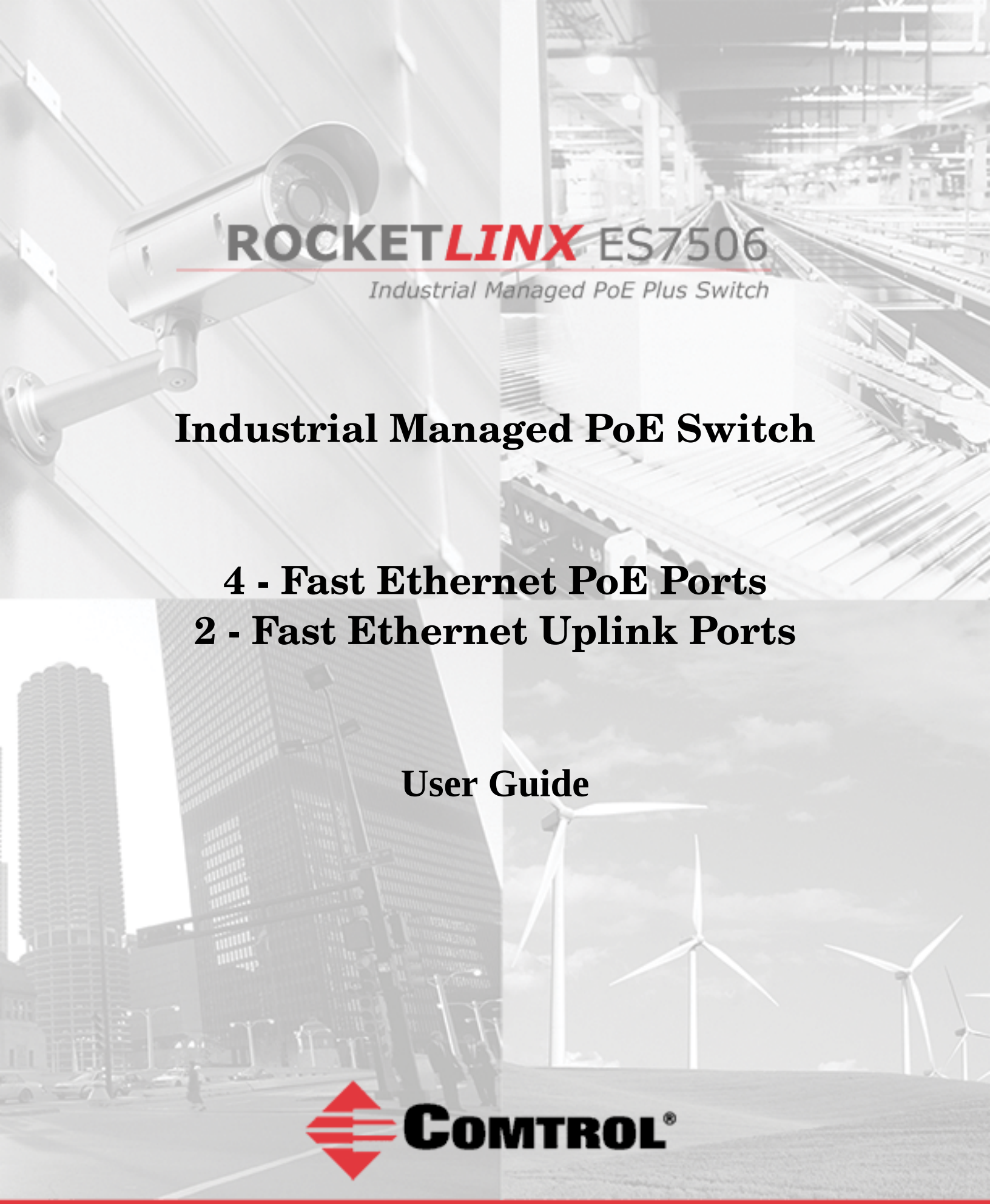


Industrial Managed PoE Switch

4 - Fast Ethernet PoE Ports
2 - Fast Ethernet Uplink Ports

User Guide

COMTROL®

Copyright Notice

Sixth Edition, January 31, 2014

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: 2000529 Rev. F

Table of Contents

Introduction

Overview

The RocketLinx ES7506 is designed for industrial PoE applications such as IP surveillance or wireless access points, where the power source is not conveniently located. The ES7506 provides:

- Four 10/100BASE-TX Power over Ethernet Plus ports
- Two redundant 10/100BASE-TX uplink ports

The ES7506 supports intelligent PoE control and schedule management. Each of the four PoE ports can be configured in a weekly schedule by hourly basis and PoE on/off can be remotely controlled via SNMP and web user interface.

It is compliant to both IEEE 802.3af PoE as well as the pioneer standard of IEEE 802.3at PoE Plus designed for boosting PoE delivery up to 30W in each of the four PoE ports. The ES7506 can auto-detect 24V and 48V power input and can deliver 24V and 48V PoE outputs which allow more applications where 48VDC is not an option.

The two uplink ports can be configured as Redundant Ring ports recovering network failure in less than 5ms, or RSTP ports integrating with other standard switches. Full network management features such as SNMP v3, QoS, IGMP v3 are all supported. If the powered device fails to respond after a pre-configured time interval, the ES7506 will reboot the powered device and continue to monitor the powered device in every pre-configured time interval. Also, unmanageable powered devices can be managed through the ES7506.

The IP31 rigid aluminum flat casing and wide operation temperature range ensure reliable operation in places such as mass transit vehicles or outdoor usage.

Detailed specifications are available for the ES7506.

Hardware Installation

You can use the following subsections to install the RocketLinx ES7506:

Connect the Power and Ground

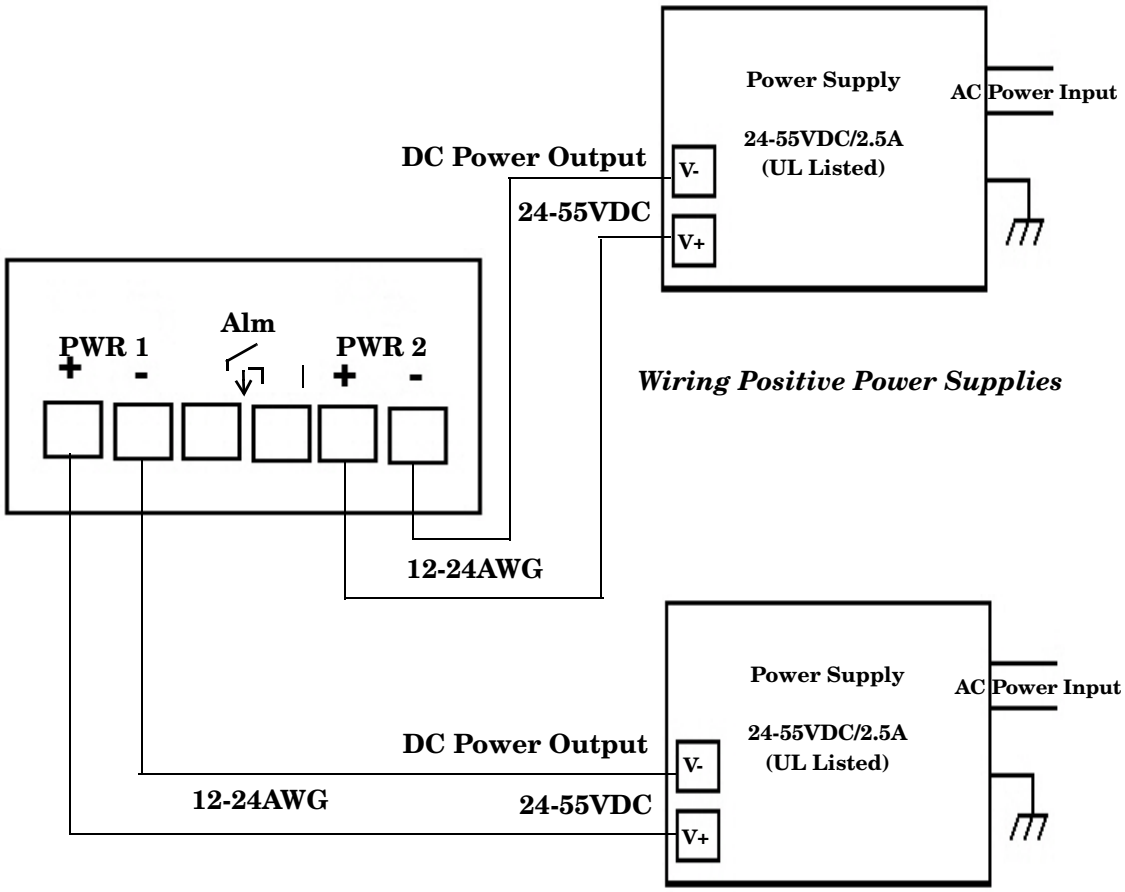
You can use the following procedure to connect power and the ground to the ES7506.

Electrical Specifications		Values
Power Input Voltage PWR1/PWR2	IEEE 802.3af Standard, Manual	48 (48-57VDC)
	IEEE 802.3af Ultra	55 (55-57VDC)
	Forced 15.4W	48 (48-57VDC)
	Forced 30W	55 (55-57VDC)
PoE Output Voltage	IEEE 802.3af Standard, Manual	44-57V
	IEEE 802.3af Ultra	50-57V
	Forced	44-57V
Maximum PoE Power/Port	IEEE 802.3af Standard, Manual	15.4W
	IEEE 802.3af Ultra, Forced	30W
Total Power Budget	Maximum	Up to 100 W
Power Consumption	Maximum	8W without PD load

1. Connect the DC power inputs.
   a. Insert positive and negative wires (12-24AWG) into the PWR+ and PWR- 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.*

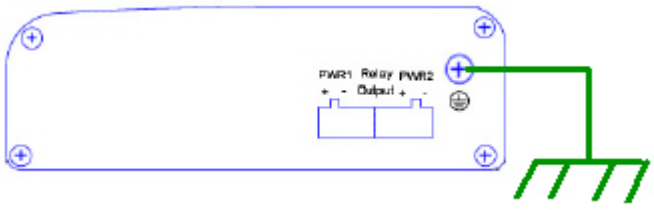
b. Tighten the wire-clamp screws to prevent the wires from coming loose.



Wiring Positive Power Supplies

- PWR1 and PWR2 support power redundancy and reverse polarity protection.
- Accepts a positive or negative power source but PWR1 and PWR2 must apply to the same mode.
- If both power inputs are connected, the ES7506 is powered from the highest connected voltage.
- The ES7506 can emit an alarm if PWR1 or PWR2 are no longer receiving power. See*Warning* discussion on Page 81 to configure an alarm.

2. Connect a ground wire between the chassis and earth ground using 12-24AWG wire to ensure that the ES7506 is not damaged by noise or electrical shock.

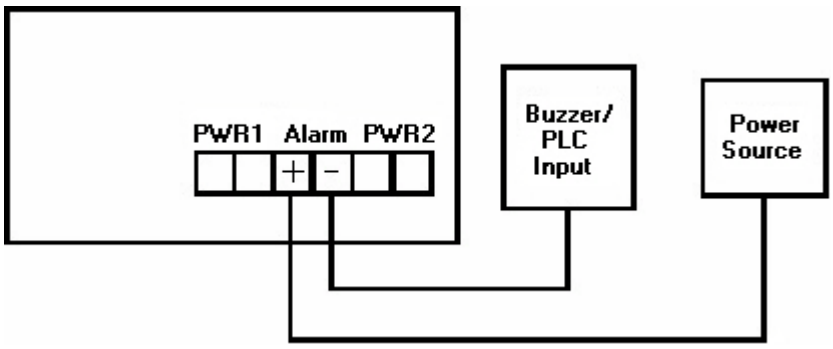


   a. Loosen the earth ground screw on the right side of the ES7506.
   b. Insert the ground wire.
   c. Tighten the ground screw after the earth ground wire is connected.

Connect the Alarm Relay Output

The ES7506 provides one alarm relay output. The relay contacts are energized (open) for normal operation and close under error conditions that include:

- Dry output
- Power failure
- Link failure
- Ping failure
- Super Ring failure



The alarm relay can be configured in one of the ES7506 user interfaces (*Warning* on Page 81) or through the Command Line Interface (*Global Configuration Mode* on Page 103).

Wiring the alarm relay output is the same as wiring power inputs in *Connect the Power and Ground* on Page 9.

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 ES7506

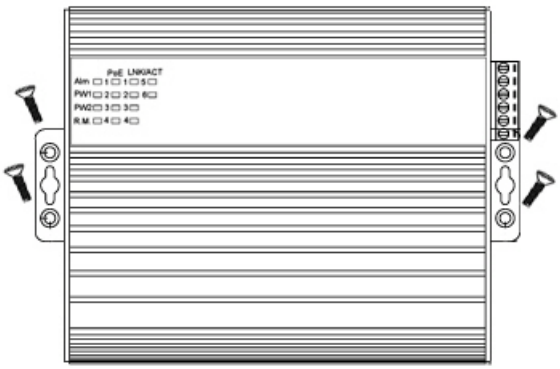
You can use the following procedure to mount the ES7506 on a DIN rail or on the wall.

Note: *The ES7506 will disperse heat through the metal case during PoE port operation. The ES7506 should be installed and mounted onto a panel which provides good heat dispersion.*

DIN Rail Mounting

Two DIN rail clips and four screws are shipped with theES7506. Use the screws to attach the DIN rail clip to the wall-mount plate.

Attaching the ES7506 On a Wall



Use the hook holes located at the corners of the wall-mount plate to mount the ES706.

Connect the Ethernet Ports

You can use the following information to connect standard Ethernet cables between the ES7506 Ethernet ports and the network nodes.

- Ports 1-4 are Fast Ethernet (10/100BASE-TX) PoE ports that are IEEE 802.3af (PoE) compliant with Standard, Manual, and Ultra mode support and also provides forced power.
- Ports 5-6 are Fast Ethernet Uplink ports.

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

10/100BASE-TX PoE Pin-Out (Alternative B)	
1	RX +
2	RX -
3	TX +
4, 5	Vport+
6	TX -
7, 8	Vport-

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**: Category 3, 4, or 5 cable
- **100BASE-TX**: Category 5 or 5e cable
- **PoE Ports:** Category 5e / 6 cable

LED Descriptions

This subsection provides information about the ES7506 LEDs. You can also refer to *Device Front Panel* on Page 92 for information about using the web user interface to remotely view LED information.

LEDs	LED On	LED Blinking	LED Off
Alm (Alarm)	Alarm activated or port link down	Not applicable	Alarm not activated
PW1 PW2	Green: Power	Not applicable	No Power
R.M. (Ring Master)	Green: Working as a Ring Master	Amber: Ring failed	Ring function disabled
PoE 1-4	Amber: PoE powering	Blinking: PoE Detect Blinking fast: PoE power failure	PoE disabled: power output over current, a cable short, or PoE is disabled for that port
LNK/ACT 1-6	Port link up	Active connection	Port link down or port not connected

Using PortVision DX

There are several ways to configure network information. Comtrol Technical Support recommends connecting the ES7506 to a PC or laptop running *Windows* and installing *PortVision DX* for initial configuration.

This section shows how to use PortVision DX for initial network configuration and discusses how to:

- Install PortVision DX (Page 15)
- Configure the network address (Page 17)
- Check the firmware and bootloader version on the ES7506 to verify that the latest versions are loaded (Page 20) before configuration
- Download the latest version firmware and bootloader and upload it to the ES7506 (Page 21)
- Perform other PortVision DX tasks, such as:
  - Configuring multiple ES7506 switches (Page 22)
  - Uploading firmware to multiple ES7506 switches (Page 23)
  - Adding a new RocketLinx (managed or unmanaged) or a third party device to PortVision DX to maintain device information on your network (Page 24)
  - Using configuration files for use in configuring multiple installations with the same features (Page 25)
  - Using the LED Tracker (Page 26)
- Organize how PortVision DX displays your Comtrol Ethernet attached products (Page 25)
- Access the latest documentation for your Comtrol Ethernet attached product

Optionally, you can use the web user interface or the CLI to perform these tasks on the ES7506 using these subsections:

- *IP Configuration* on Page 45
- *Firmware Upgrade* on Page 55
- *Basic Settings (CLI)* on Page 108

NetVision

NetVision, the configuration utility that only supported RocketLinx has been replaced by PortVision DX, which supports all Comtrol Ethernet attached products.

If you are familiar with NetVision and wish to use it, NetVision is still available but has been moved to *Legacy status*, meaning that it is no longer being maintained. If any bugs or issues exist, Technical Support will have you load and use PortVision DX.

PortVision DX Overview

PortVision DX automatically detects Comtrol Ethernet attached products physically attached to the local network segment so that you can configure the network address, upload firmware, and manage the following products:

- RocketLinx switches
- DeviceMaster family
  - DeviceMaster PRO
  - DeviceMaster RTS
  - DeviceMaster Serial Hub
  - DeviceMaster UP
  - DeviceMaster 500
- DeviceMaster LT
- IO-Link Master

In addition to identifying Comtrol Ethernet attached products, you can use PortVision DX to display any third-party switch and hardware that may be connected directly to those devices. All non-Comtrol products and unmanaged RocketLinx switches are treated as non-intelligent devices and have limited feature support. For example, you cannot configure or update firmware on a third-party switch.

PortVision DX Requirements

Use PortVision DX to identify, configure, update, and manage the ES7506 on the following Windows operating systems:

- Windows 8.1
- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Windows XP

PortVision DX requires that you connect the Comtrol Ethernet attached product to the same network segment as the Windows host system if you want to be able to scan and locate it automatically during the configuration process.

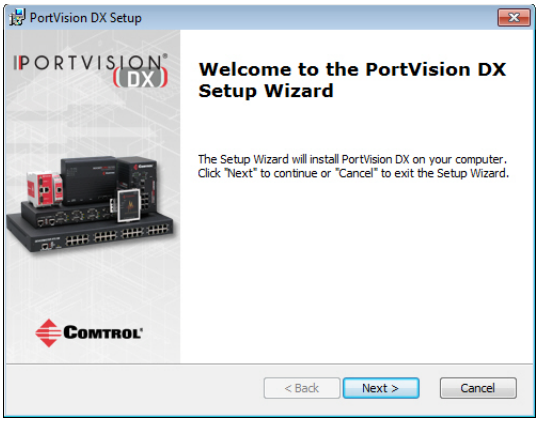
Installing PortVision DX

During initial configuration, PortVision DX automatically detects and identifies ES7506 switches, if they are in the same network segment.

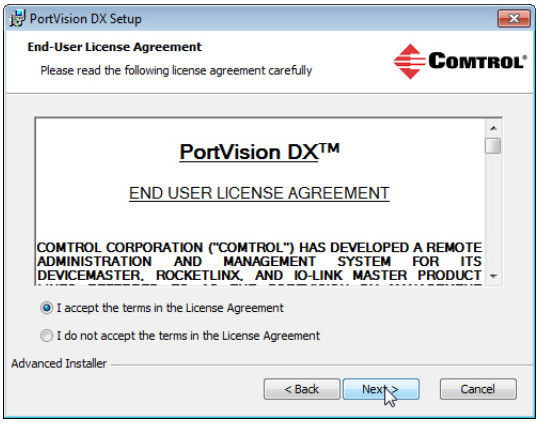
Use the *Software and Documentation* CD that came with the ES7506 to check for the latest version of PortVision DX or use the link below to download the latest version.

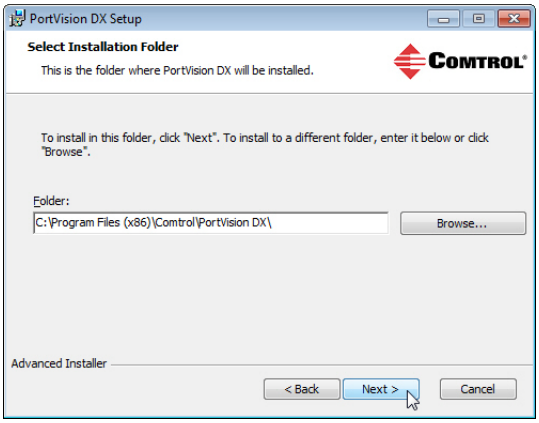
1. Locate PortVision DX using one of the following methods to download the latest version:
   - ***Software and Documentation CD***: You can use the CD menu system to check the version on the CD against the latest released version.
   - ***FTP site subdirectory***: ftp://ftp.comtrol.com/rocketlinx/portvision_dx.

   Note: *Depending on your operating system, you may need to respond to a Security Warning to permit access.*
2. Execute the **PortVision_DX[*version*].msi** file.
3. Click **Next** on the *Welcome* screen.

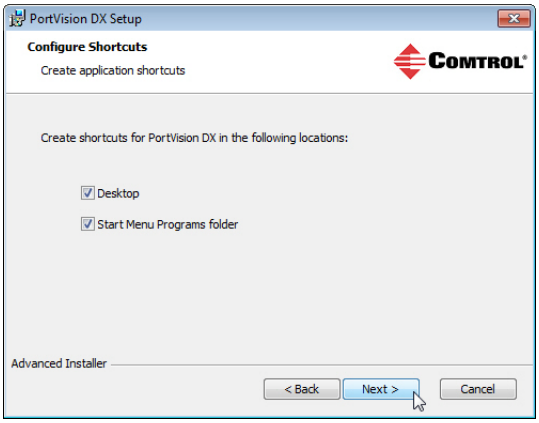


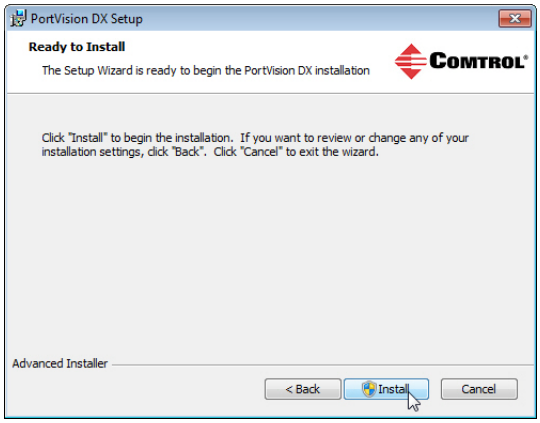
4. Click **I accept the terms in the License Agreement** and **Next**.
5. Click **Next** or optionally, browse to a different location and then click **Next**.



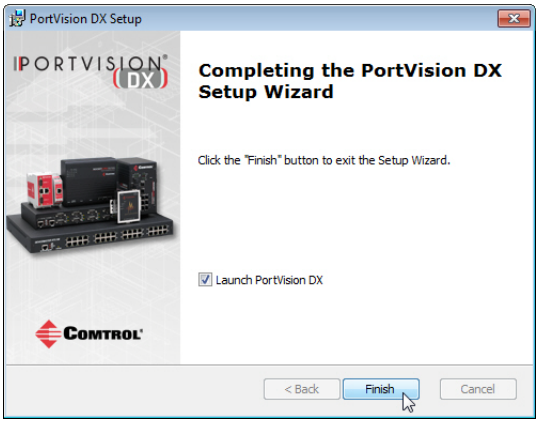


6. Click **Next** to configure the shortcuts.
7. Click **Install**.





8. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer?* query.
9. Click **Launch PortVision DX** and **Finish** in the last installation screen.
10. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.
11. Go the next subsection to use PortVision DX to program the network information.



Configuring the Network Settings

The ES7506 has the following default values when shipped from the factory:

- IP address: 192.168.250.250
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.250.1

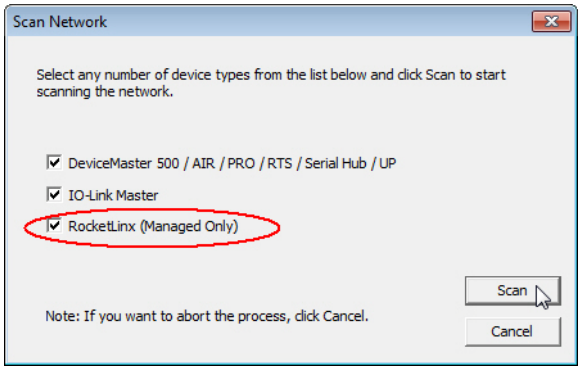
Use the following procedure to change the default network settings on the ES7506 for your network.

1. If necessary, start PortVision DX using the **PortVision DX** desktop shortcut or from the **Start** button, click **All Programs > Comtrol > PortVision DX > PortVision DX**.

   Note: *Depending on your operating system, you may need to click* **Yes** *to the Do you want to allow the following program to make changes to this computer? query.*

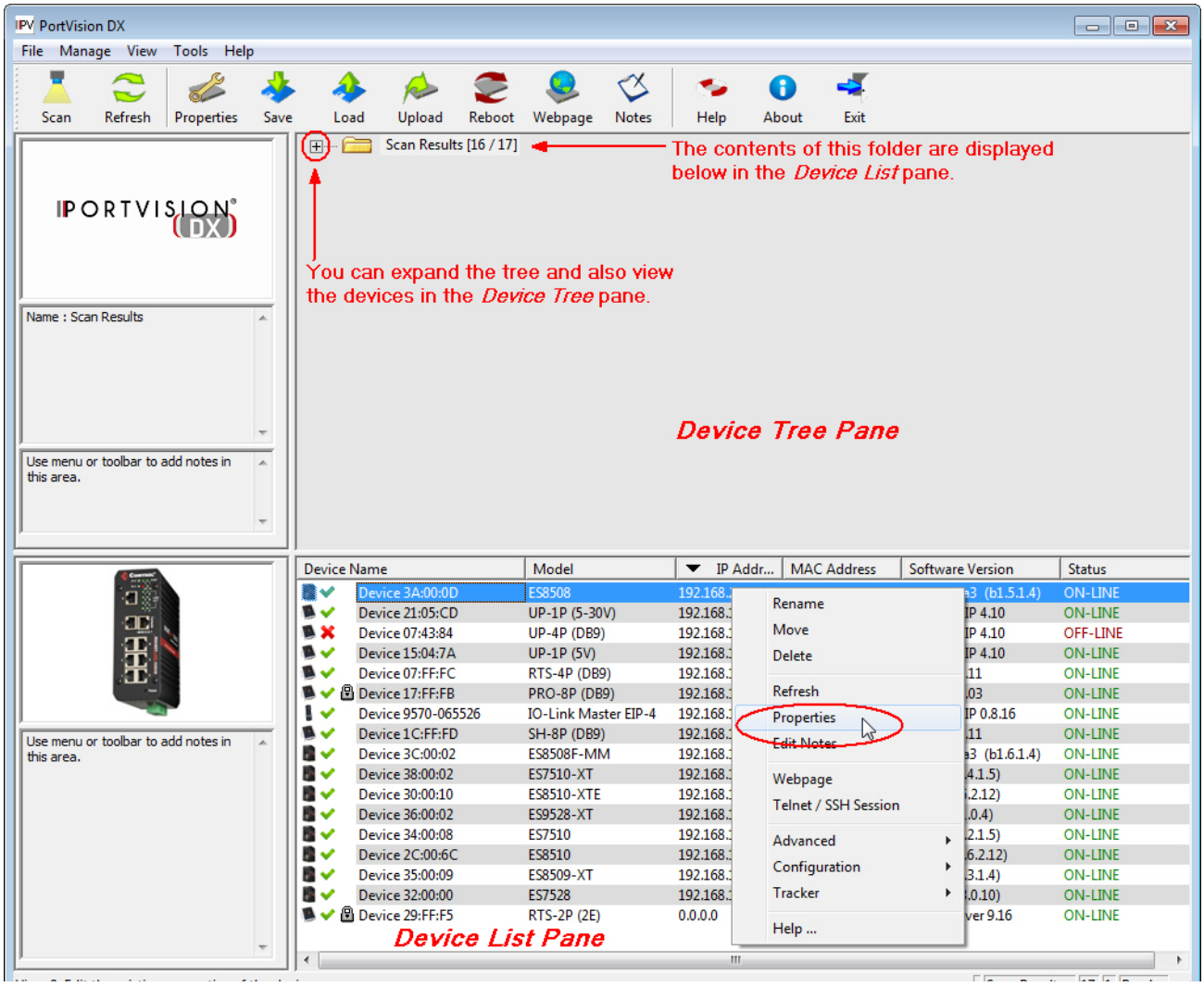
2. Click the **Scan** button in the *Toolbar*.
3. Select the Comtrol Ethernet attached products that you want to locate and then click **Scan**.

   You can save time if you only scan for RocketLinx switches.

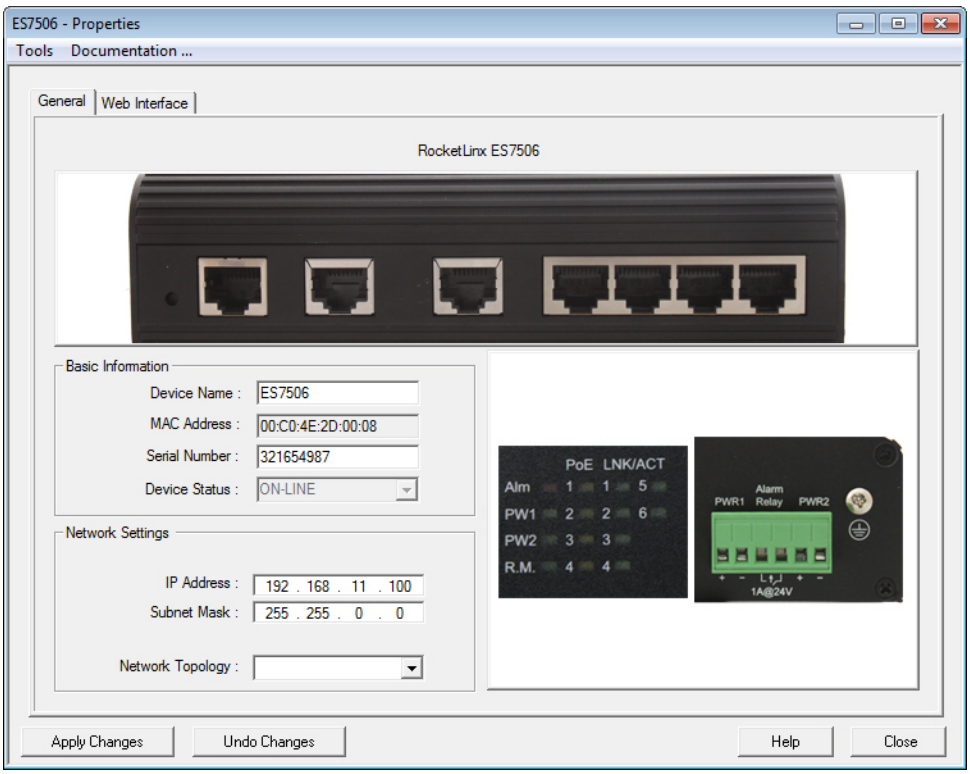


Note: *If the Comtrol Ethernet attached product is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the Comtrol Ethernet attached product to PortVision DX.*

4. Highlight the ES7506 for which you want to program network information and open the **Properties** screen using one of these methods.
   - Double-click the ES7506 in the *Device Tree* or *Device List* pane.
   - Highlight the ES7506 in the *Device Tree* or *Device List* pane and click the **Properties** button.
   - Right-click the ES7506 in the *Device Tree* or *Device List* pane and click **Properties** in the popup menu
   - Highlight the ES7506, click the **Manage** menu and then **Properties**.



5. *Optionally*, rename the ES7506 in the **Device Name** field for a PortVision DX friendly name. The default name displays as *Device* and the last three sets of hex numbers from the MAC address.



Note: *The MAC address and Device Status fields are automatically populated and you cannot change these values.*

6. Optionally, enter the serial number, which is on a label on the ES7506.
7. Enter a unique **IP address** as required for your site.
8. Enter a valid **Subnet Mask** value for your network.

   Note: *If you want to DHCP addressing, you can use the CLI or the IP Configuration page under Basic Settings.*

9. Optionally, select the **Network Topology** type, which is an informational field.
10. Click **Apply Changes** to update the network information on the ES7506.

    Note: *If you are deploying multiple ES7506 switches that share common values, you can save the configuration file and load that configuration onto other ES7506 switches. See* *Using Configuration Files on Page 25* *for more information.*

11. Click **Close** to exit the *Properties* window.
12. You should verify that you have the latest firmware loaded on the ES7506 because a newer version typically includes feature enhancements and bug fixes. Refer to *Checking the Firmware Version* on Page 20 and if necessary, *Uploading the Latest Firmware or Bootloader* on Page 21.
13. If you have the latest firmware, you can begin feature configuration, see one of these sections:
    - *Configuration Using the Web User Interface* on Page 31
    - *Configuration Using the Command Line Interface (CLI)* on Page 95
    - Right-click the ES7506 in the *Device List* pane and click **Webpage** in the popup menu.

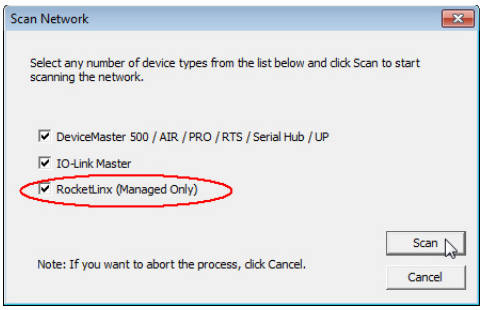
    Note: *The default User Name and Password are both* **admin**.

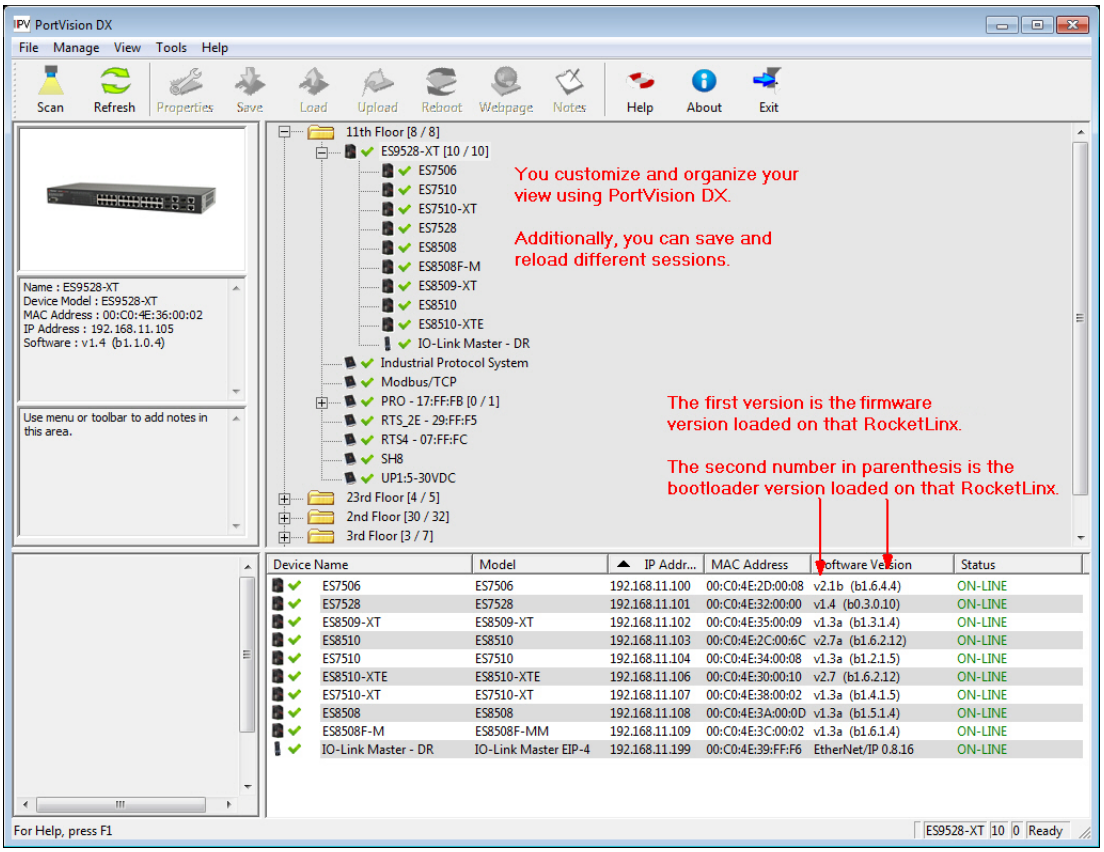
Checking the Firmware Version

Checking your web interface and bootloader versions is easy in PortVision DX.

Comtrol recommends loading the latest firmware and bootloader so that you have all of the latest feature enhancements and bug fixes.

1. If the ES7506 is not displayed in PortVision DX, click the **Scan** button.
2. Select the Comtrol Ethernet attached product type and click the **Scan** button.
3. Locate the ES7506 in the *Device List* pane. Under *Software Version*:
   - The first number reflects the firmware version.
   - The second number displays the bootloader version.





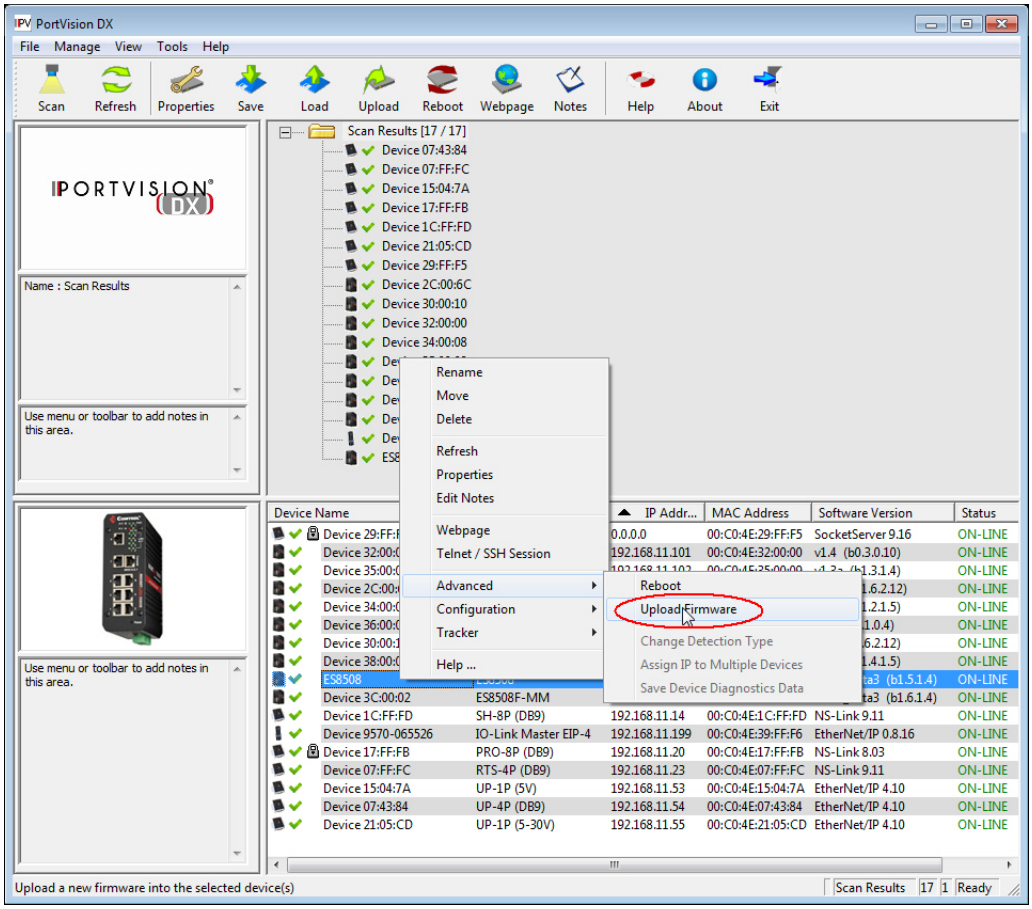
4. Check the Comtrol ftp site for the latest firmware and bootloader. Simply, click your product type and click the **Software** link and check the latest version against the version on the ES7506.

Use the next subsection for procedures to upload the firmware (web interface) and bootloader.

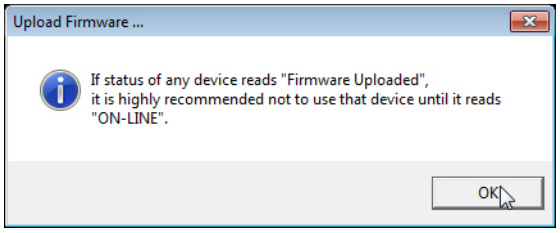
Uploading the Latest Firmware or Bootloader

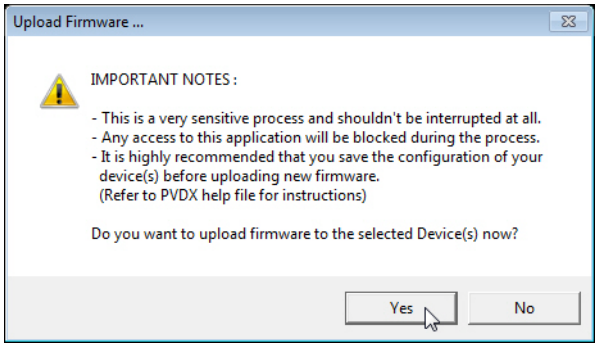
You can use the following procedure to upload the latest firmware or bootloader.

1. If you have not done so, download the latest firmware and bootloader using the previous subsection.
2. Right-click the ES7506 in the *Device List* pane that you want to update, click **Advanced --> Upload firmware**.



3. Click **Yes** to the *Upload Firmware* message.
4. Click **Ok** to the message notifying you that you should wait to use the ES7506 when the status returns to ON-LINE.





5. Right-click ES7506 in the *Device List* pane and click **Refresh**. Optionally, you can click the **Refresh** button in the *Toolbar* and that refreshes all devices in PortVision DX.
6. Verify that the version change is reflected in under the *Software Version*.

Configuring Multiple RocketLinx Switches Network Addresses

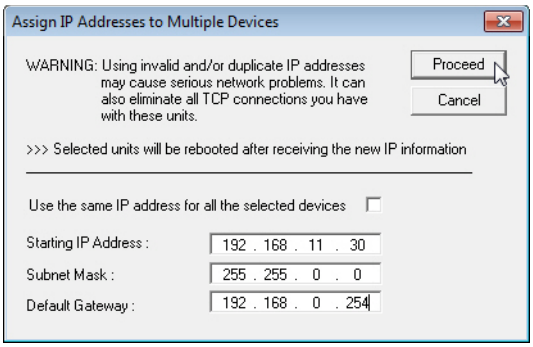
You can configure the network addresses for multiple ES7506 switches using the **Assign IP to Multiple Devices** option.

In addition, you can also configure common settings for the ES7506 web page and save the settings to a configuration file that you can load to all or selected ES7506 switches. See *Using Configuration Files* on Page 25 for more information.

You can use this procedure if your ES7506 is connected to the host PC, laptop, or if the ES7506 resides on the local network segment. Use the following steps to configure multiple ES7506 switches.

1. Shift-click the ES7506 switches for which you want to program network information, right-click, and click **Advanced > Assign IP to Multiple Devices**.
2. Enter the starting IP address, subnet mask, IP Gateway and click **Proceed**.

   PortVision DX displays the programmed IP addresses in the *Device List* pane after the next refresh cycle.

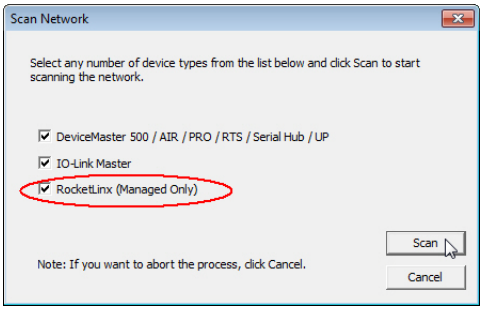


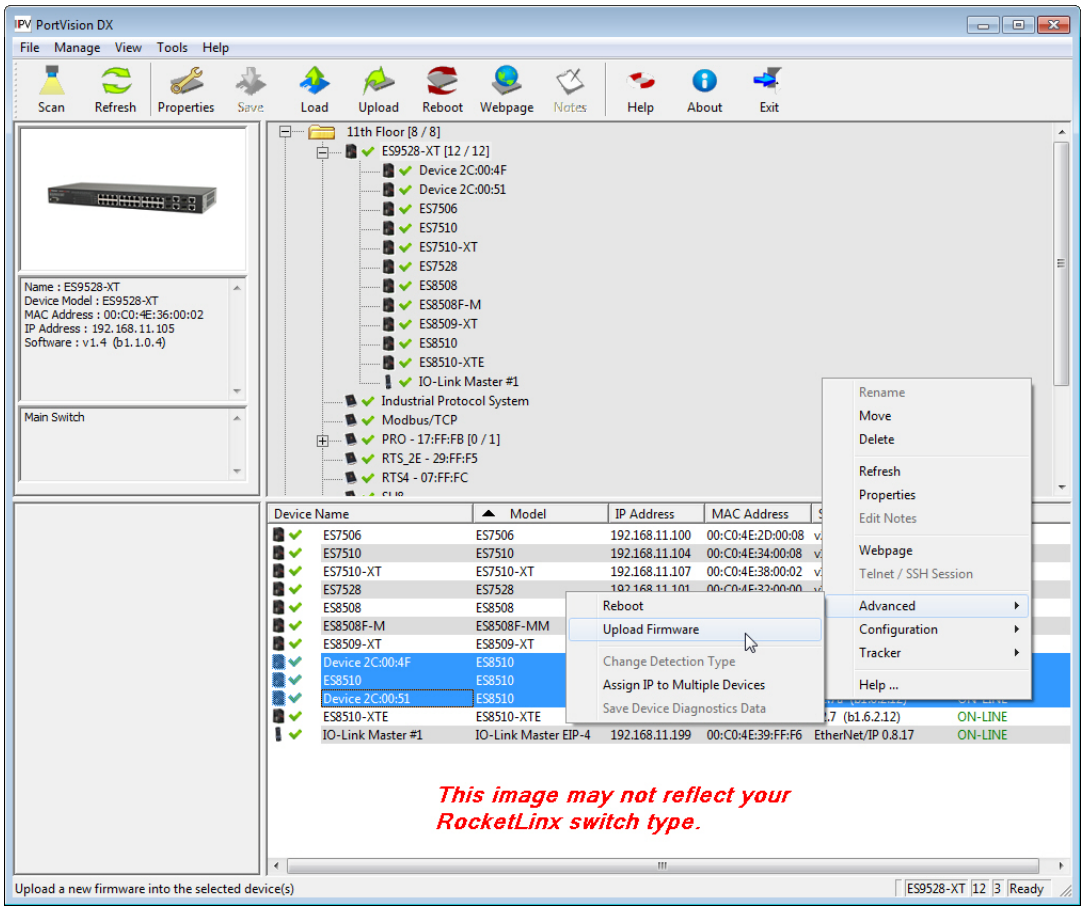
Uploading Firmware to Multiple ES7506 Switches

You can use this procedure if your ES7506 is connected to the host PC, laptop, or if the ES7506 resides on the local network segment.

Note: *Technical support does not advise uploading bootloader to multiple ES7506 switches. Remember that uploading firmware reboots the ES7506, which depending on your network connections may cause firmware uploading to fail on another ES7506.*

1. If the ES7506 is not displayed in PortVision DX, click the **Scan** button.
2. Select the Comtrol Ethernet attached product type and click the **Scan** button.
3. Shift-click the multiple ES7506 switches on the **Main** screen that you want to update and use one of the following methods:
   - Click the **Upload** button.
   - Right-click and then click **Advanced > Upload Firmware**.
   - Click **Advanced >Upload Firmware** in the **Manage** menu.





4. Browse, click the firmware (**.bin**) file, **Open** (*Please locate the new firmware*), and then click **Yes** (*Upload Firmware*).

   It may take a few minutes for the firmware to upload onto all of the ES7506 switches. The ES7506 reboots itself during the upload process.
5. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**.

In the next polling cycle, PortVision DX updates the *Device List* pane and displays the new firmware version.

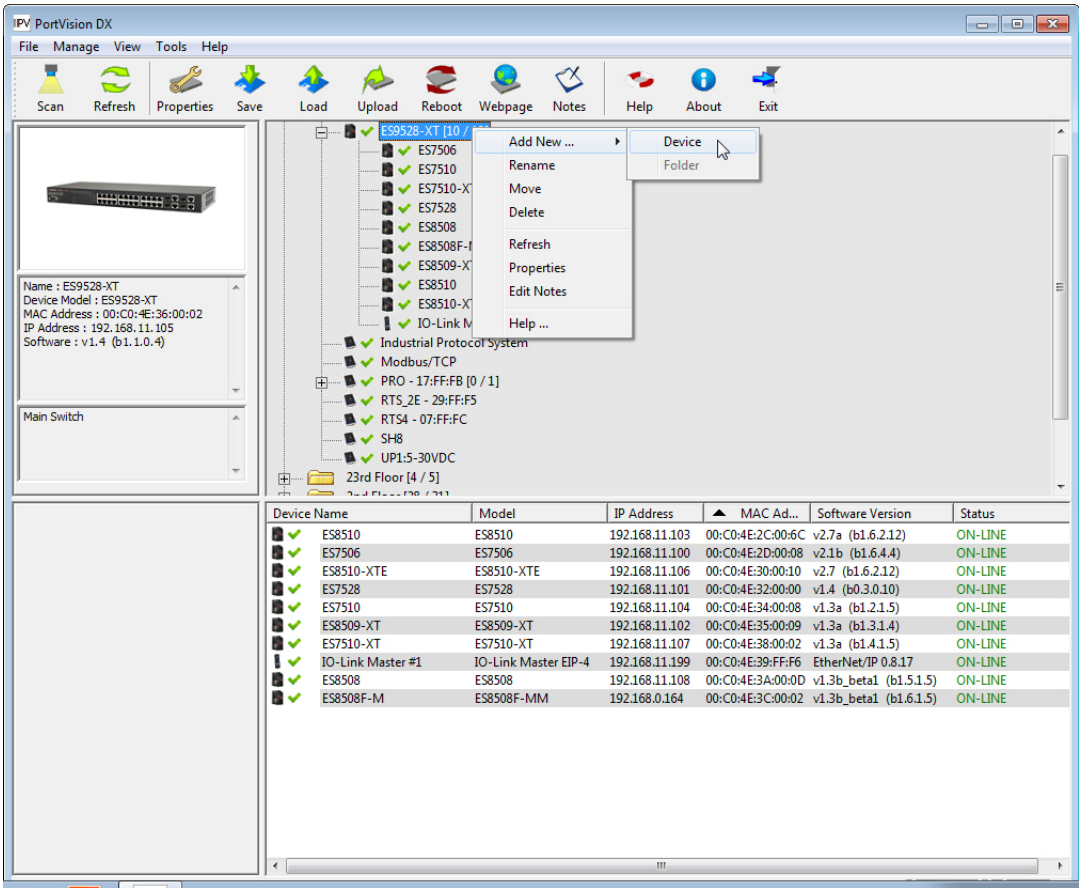
Adding a New Device in PortVision DX

You can add a new ES7506 manually, if you do not want to scan the network to locate it or you want to pre-configure an ES7506 before connecting it to the network. Optionally, you can also add unmanaged devices or RocketLinx switches to maintain information about devices on the network.

See the PortVision DX help system for additional information about adding unmanaged RocketLinx switches or third party devices or switches.

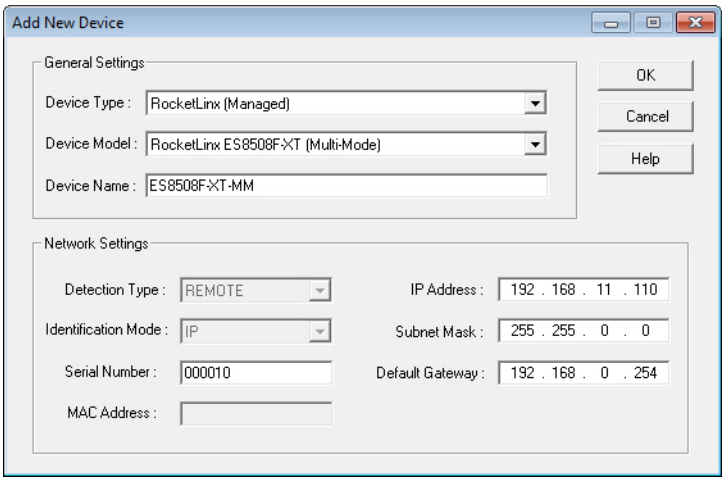
Use the following procedure to add a remote ES7506 to PortVision DX.

1. Access the *New Device* window using one of these methods:
   - Click **Add New > Device** in the *Manage* menu.
   - Right-click a folder or a RocketLinx switch in the *Device Tree* pane and click **Add New > Device**.



2. Select the appropriate RocketLinx in the **Device Type** drop list.
3. Select the appropriate model in the **Device Model** drop list.
4. Enter a friendly device name in the **Device Name** list box.
5. Optionally, enter the serial number in the **Serial Number** list box.

6. Enter the IP Address for the ES7506. It is not necessary to enter the Subnet Mask and Default Gateway
7. Click **Ok** to close the *Add New Device* window. It may take a few moments to save the ES7506.
8. If necessary, click **Refresh** for the new RocketLinx to display in the *Device Tree* or *Device List* panes. The RocketLinx shows OFF-LINE if it is not connected to the local network or if an incorrect IP address was entered.



Using Configuration Files

If you are deploying multiple ES7506 switches that share common firmware values, you can save the configuration file (**.dc**) from the *Main* screen in PortVision DX and load that configuration onto other ES7506 switches.

You may want to program the network settings in multiple ES7506 switches using *Configuring Multiple RocketLinx Switches Network Addresses* on Page 22.

Saving a Configuration File

Use this procedure to save a configuration file.

1. Highlight the ES7506 in the *Device List* pane and use one of the following methods:
   - Click the **Save** button.
   - Right-click and then click **Configuration > Save**.
2. Browse to the location you want to save the file, enter a file name, and click **Save**.
3. Click **Ok** to close the *Save Configuration Completed* message.

Loading a Configuration File

Use the following procedure to load a previously saved a ES7506 configuration file. Load a configuration file and apply it to a selected ES7506 switch or switches from the *Device List* pane.

Use this procedure to load a configuration file using the *Device List* pane to one or more ES7506 switches.

1. Highlight the device or devices in the *Device List* pane and use one of the following methods:
   - Click the **Load** button
   - Right-click and then click **Configuration > Load**
2. Click **Yes** to the warning that it will take 25 seconds per device and it may also reboot the devices.
3. Browse to the location of the configuration file, click the file name (**.dc**) and then **Open**.
4. Close the *Load Configuration* popup message.

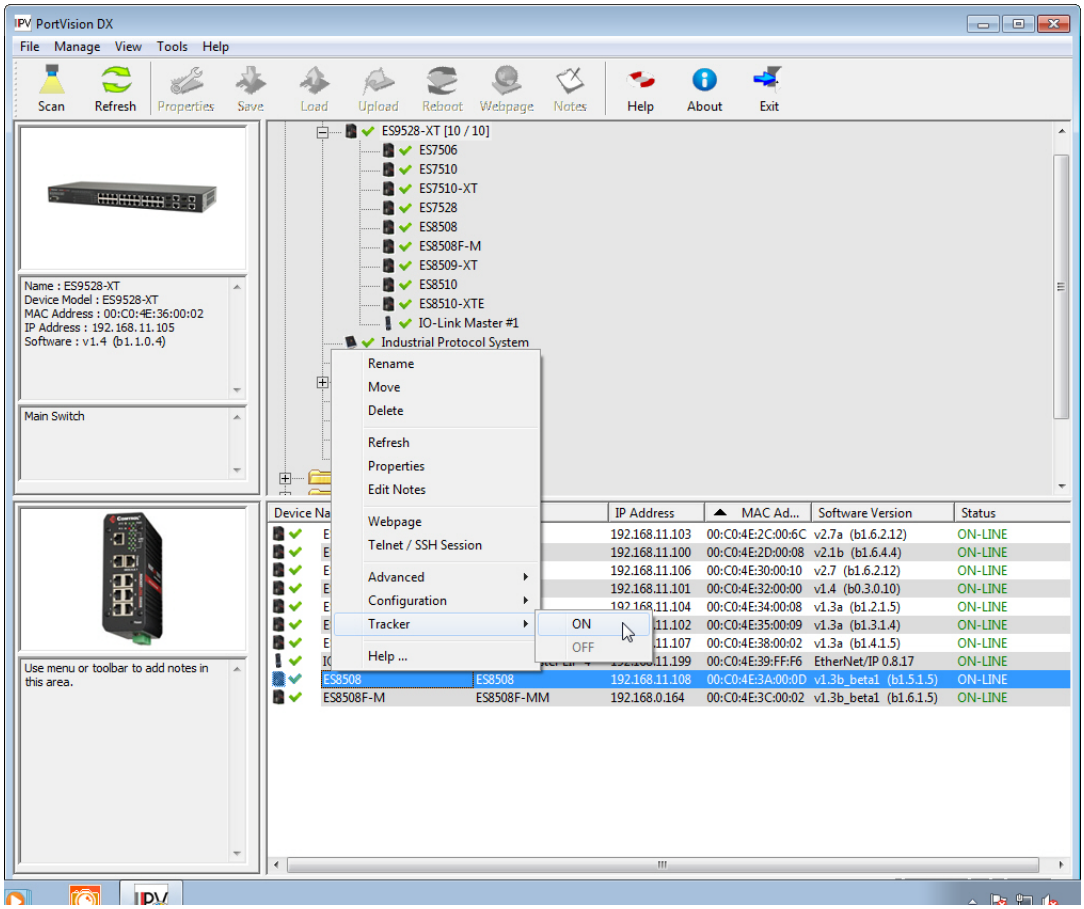
Using the LED Tracker

RocketLinx managed switches support the LED Tracker feature, which allows you to toggle on/off the LEDs on a specific device so that you can locate the physical unit.

Use this procedure to toggle the **LED Tracker** feature on RocketLinx switches.

1. Right-click the ES7506 in the *Device List* pane, click **Tracker**, and then click **ON**.

   The ES7506 **SYS** LED will flash for five seconds.

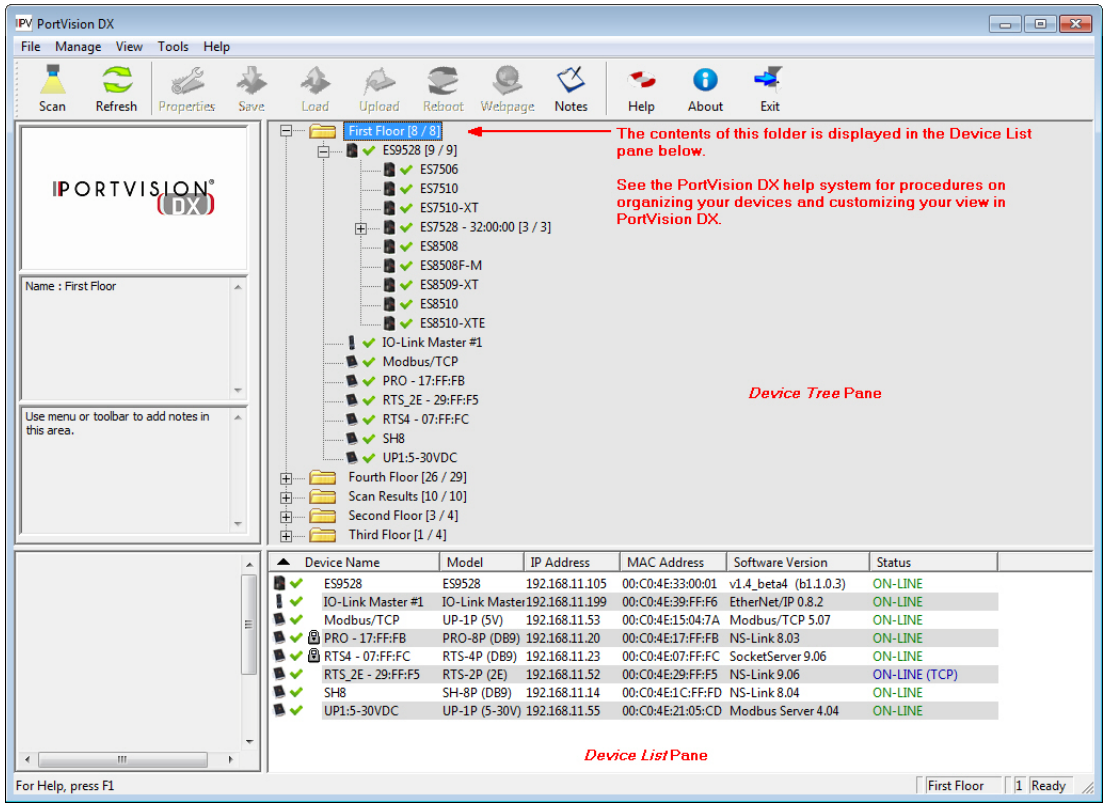


2. If necessary, you may need to click **Tracker** and **ON** several times to catch the flashing **SYS LED**.

Customizing PortVision DX

You can customize how PortVision DX displays the devices. You can even create sessions tailored for specific audiences. You can also add shortcuts to other applications using **Tools > Applications > Customize** feature.

The following illustrates how you can customize your view.



See the PortVision DX Help system for detailed information about modifying the view. For example, the above screen shot illustrates devices layered in folders.

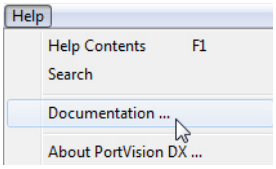
Accessing RocketLinx Documentation from PortVision DX

You can use this procedure in PortVision DX to download and open the previously downloaded documents for the RocketLinx.

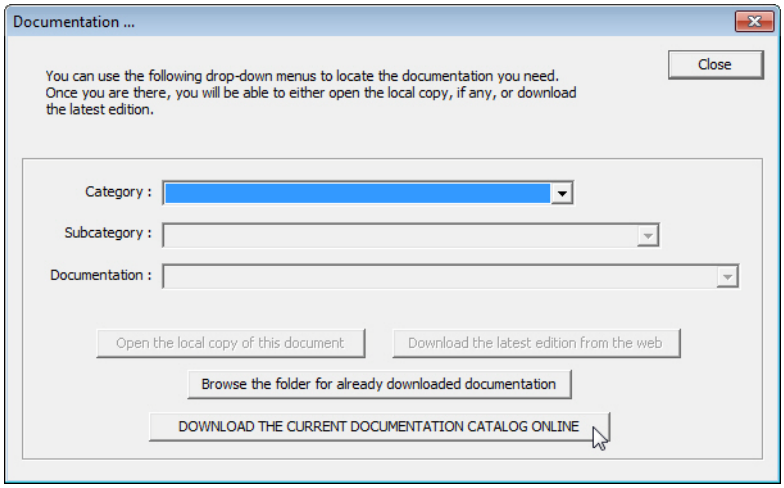
How to Download Documentation

Use this procedure to initially download a document or documents.

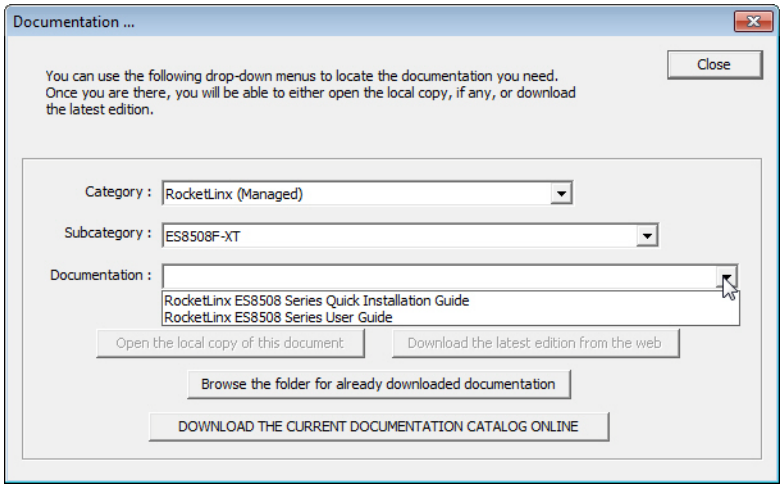
1. If necessary, open PortVision DX.
2. Click **Help > Documentation**.



3. Optionally, click the **DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE** button to make sure that the latest documentation is available to PortVision DX.



4. Select the product **Category** from the drop list.
5. Select the document you want to download from the **Documentation** drop list.



Note: *This image may not reflect your RocketLinx.*

6. Click the **Download the latest edition from the web** button.

   Note: *It may take a few minutes to download, depending on your connection speed. The document opens automatically after it has downloaded.*

7. Click **Close** if you have downloaded all of the documents that you wanted.

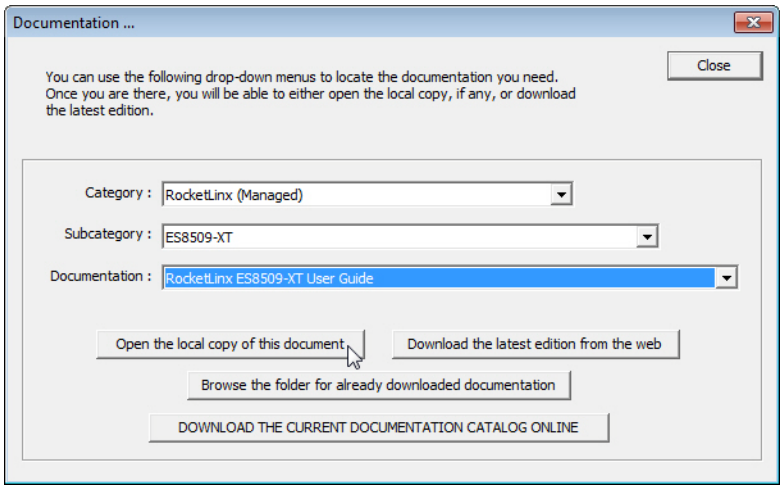
How to Open Previously Downloaded Documents

Use the following procedure to access previously downloaded documents in PortVision DX.

Note: *Optionally, you can browse to the* **Program Files (x86) > Comtrol > PortVision DX > Docs** *subdirectory and open the document.*

1. If necessary, open **PortVision DX > Start/Programs > Comtrol > PortVision DX > PortVision DX** or use the desktop shortcut.
2. Click **Help > Documentation**.
3. Click the **Open the local copy of the document** button to view the document.

   Note: *This image may not reflect your RocketLinx.*



   Note: *If the document fails to open, it may be that your browser has been disabled. You can still access the document by clicking the* **Browse the folder for already downloaded documentation** *button and opening the document with your custom browser.*

4. Click **Close** in the *Documentation...* popup, unless you want to open or download other documents.

Configuration Using the Web User Interface

The ES7506 provides in-band and out-band configuration methods:

- Out-band management means that you configure the ES7506 using the RS-232 console cable and the Command Line Interface (CLI) to access the ES7506 without attaching an admin PC to the network. You can use out-band management if you lose the network connection to the ES7506. The CLI and Telnet are discussed in *Configuration Using the Command Line Interface (CLI)* on Page 95.
- In-band management means that you connect remotely using the ES7506 IP address through the network. You can remotely connect with the ES7506 embedded Java applet web user interface or a Telnet console and the CLI. The ES7506 provides HTTP web user interface (Page 32) and secure HTTPS web user interface (Page 34) for web management.

Configuration Overview

This subsection discusses a minimum level of configuration required to operate the ES7506.

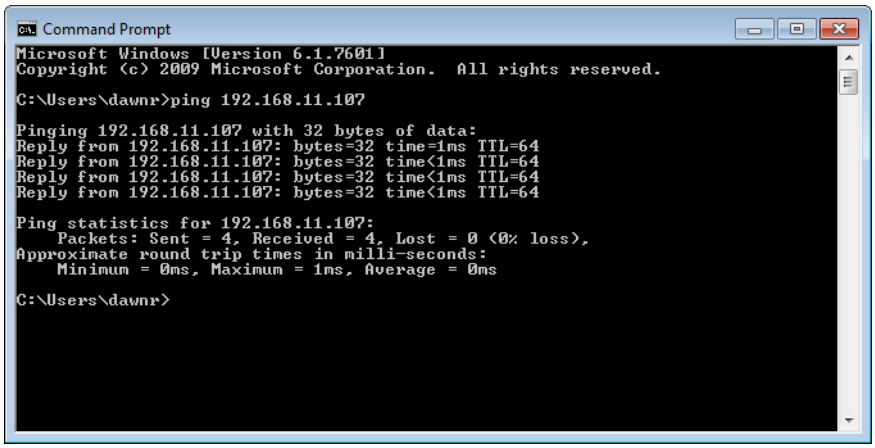
1. If you have not done so, install the hardware, see *Hardware Installation* on Page 9.
2. If you are planning on using in-band management, you need to program the ES7506 IP address to meet your network requirements. The easiest way to configure the IP address is using a Windows system and PortVision DX, see *Configuring the Network Settings* on Page 17.
3. Configure other features as desired. You can refer to the *Feature Overview* on Page 37 to locate configuration information or use these links:
   - *Basic Settings* on Page 43
   - *Port Configuration* on Page 58
   - *Power over Ethernet* on Page 62
   - *Network Redundancy* on Page 65
   - *VLAN* on Page 87
   - *Traffic Prioritization* on Page 71
   - *Multicast Filtering* on Page 74
   - *SNMP* on Page 77
   - *Security* on Page 80
   - *Warning* on Page 81
   - *Monitor and Diag* on Page 86
   - *Device Front Panel* on Page 92
   - *Save to Flash* on Page 93
   - *Logout* on Page 93

Web User Interface

The ES7506 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 ES7506 from anywhere on the network.

If you did not program the IP address for your network using PortVision DX (*Programming Network Information* on Page 20), 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 ES7506 is *192.168.250.250*.

1. If necessary, install the latest version of the Java Runtime Environment.
2. Open a command prompt window and ping the IP address for the ES7506 to verify a normal response time.



3. Launch the web browser on the PC using one of these methods:
   - Right-click the ES7506 in PortVision DX and click **Webpage**.
   - Type **http://192.168.250.250** (or the IP address of the switch), and then press **Enter**.

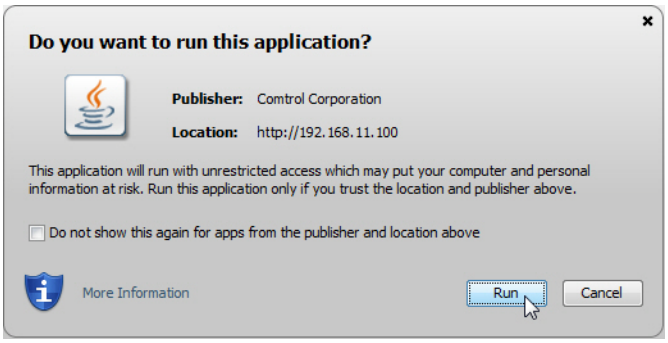
   Note: *Since Java is constantly updated, the prompts may be different from what the following subsections display.*

   Windows XP - Windows Server 2003

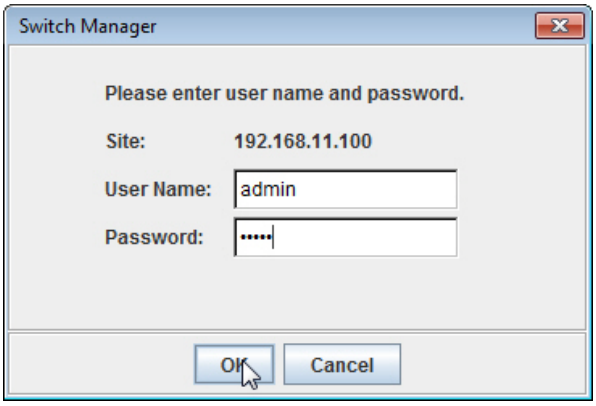
   If a *Warning - Security* message appears, click **Always trust content from this publisher** and then **Run** when requested to run the application (IP address).

   Windows Vista - Windows 8.1

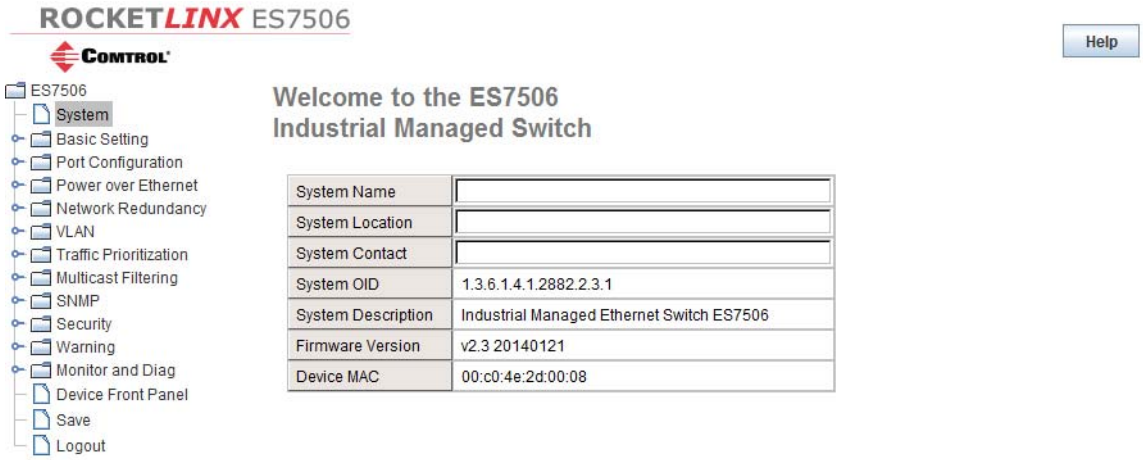
   If necessary, click **I accept the risk and want to run this application**, and then **Run** if a security warning popup message appears.



4. Enter the user name, 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 ES7506 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**.
6. If you are planning on connecting PDs, configure the PoE port characteristics, see *PoE Control* on Page 62.

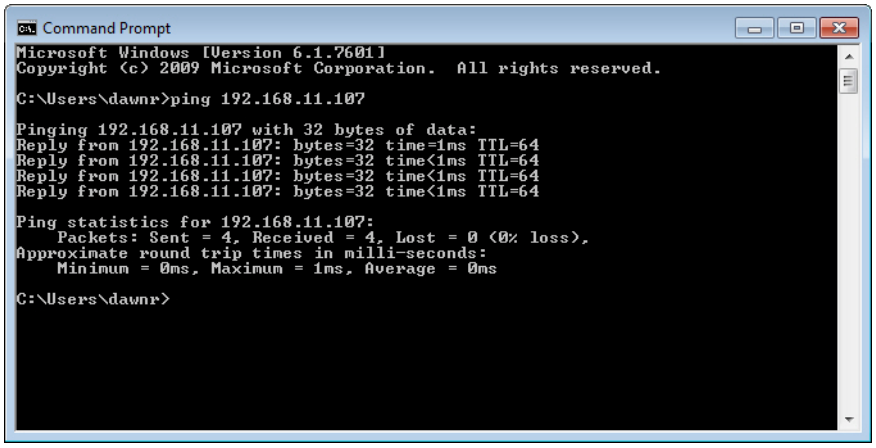
You can use the *Feature Overview* on Page 37 to locate other features that you may want to configure.

Secure Web User Interface

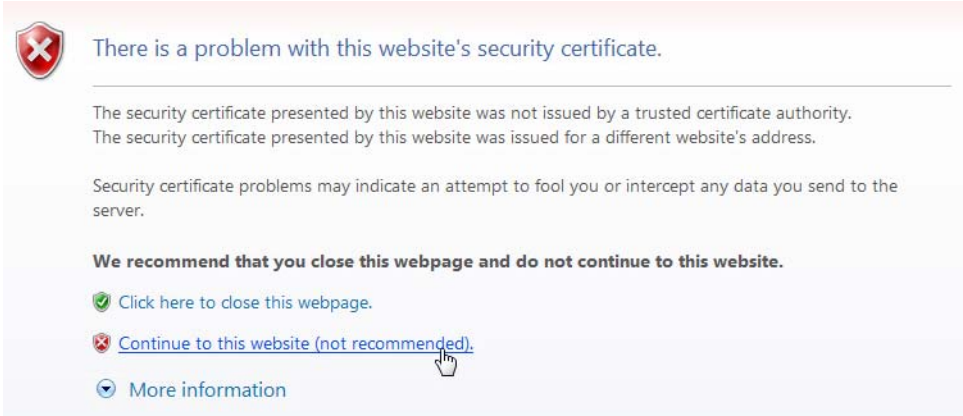
The ES7506 web user interface also provides secured management through an HTTPS login so that all of the configuration commands are secure.

If you did not program the IP address for your network using PortVision DX (*Configuring the Network Settings* on Page 17), 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 ES7506 is *192.168.250.250*.

1. Open a command prompt window and ping the IP address for the ES7506 to verify a normal response time.

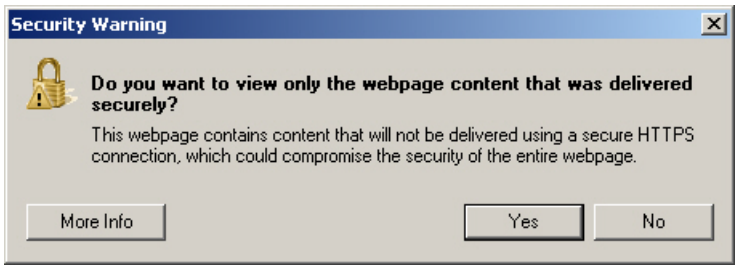


2. Launch the web browser and type **https://192.168.250.250** (or the IP address of the ES7506).and then press **Enter**.
3. Click **Continue to the web site (not recommended)**.



Windows XP and Windows Server 2003

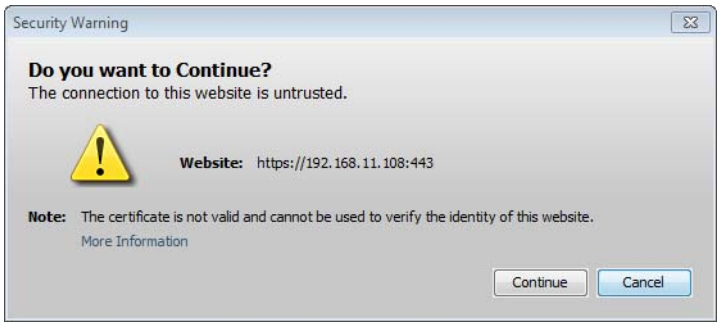
a. Click **No** when the popup screen appears and requests you to trust the secured HTTPS connection distributed by the ES7506.



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

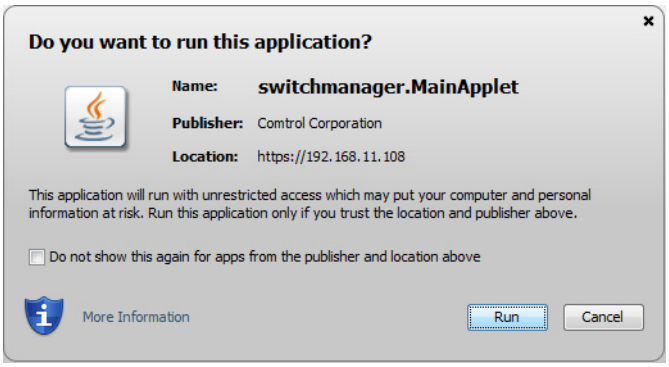
Windows Vista - Windows 7

a. Click the **Continue** button.

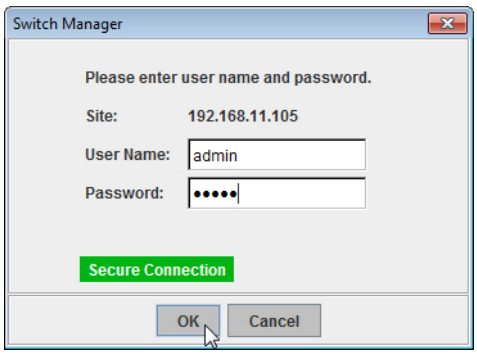


b. If necessary, click **Show all content**.

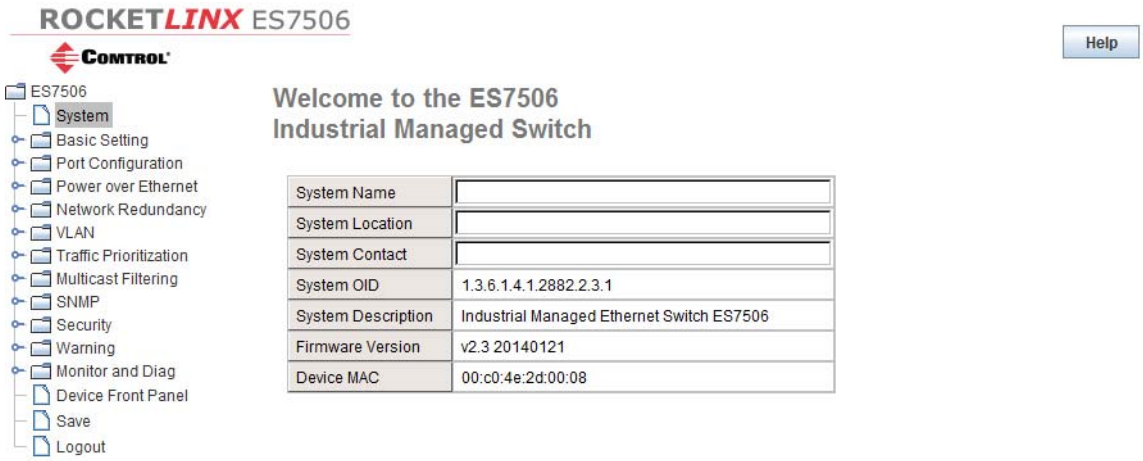
c. If desired, click **Do not show this again for apps from the publisher and location above** and then click **Run** if a security warning popup message appears.



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 ES7506 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 62.

Feature Overview

The following table provides detailed information about ES7506 features and provides the location of the configuration information in the web user interface.

Type	Category	Details
Admin Password	*Admin Password* on Page 44	• Admin
Backup and Restore	*Backup and Restore* on Page 52	Local or TFTP
CoS-Queuing Mapping	*CoS-Queue Mapping* on Page 72	• CoS 0 through 7 • Queue 0 through 3 • Queue 3 highest priority
DHCP Server Configuration	*DHCP Server Configuration* on Page 49 *DHCP Leased Entries* on Page 50 *DHCP Relay Agent* on Page 51	• Excluded Addresses and Manual Binding • DHCP Leased Entries • DHCP Relay Agent (Helper Address 1-4)
DSCP-Queuing Mapping	*DSCP-Queue Mapping* on Page 73	• DSCP 0 through 7 • Queue 0 through 3 • Queue 3 highest priority
Event Selection	*Event Selection* on Page 83	• Device Cold Start • Device Warm Start • Authentication Failure • Time Synchronization Failure • Power 1 Failure • Power 2 Failure • Fault Relay • Super Ring Topology Change • Port by Port Event SelectionPort by Port PoE Event Selection
Fault Relay	*Fault Relay* on Page 81	Relay 1 • Dry Output - On Period (Sec) and Off Period (Sec) • Power Failure - Power 1 or Power 2 • Link Failure (Port or Ports) • Ping Failure, IP Address, Reset Time (Sec), and Hold Time (Sec) • Super Ring Failure
IGMP Query	*IGMP Query* on Page 76	• Version - Version 1, Version 2, or Disable • Query Intervals • Query Maximum Response Time

Type	Category	Details
IGMP Snooping	*IGMP Snooping* on Page 75	• Enable/Disable • VID • Port by Port IGMP Snooping Table - IP Address - VID
IP Configuration	*IP Configuration* on Page 45	• IPv4 • DHCP • DNS1 and DNS2
IP Security	*IP Security* on Page 80	• Enable/Disable • Security IP • Security IP List - Index and Security IP
MAC Address Table (8K)	*MAC Address Table* on Page 86	• 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
Ping Utility	*Ping Utility* on Page 91	Target IP Address
PoE Control	*PoE Control* on Page 62	• Powering Mode - 802.3af or Force • Port by Port - PoE - Enable/Disable/Schedule - Power Mode - 802.3af or Force • PD Status Detection - Enable/Disable - PD IP Address - Cycle Time
PoE Scheduling	*PoE Scheduling* on Page 64	PoE Ports On/Off on an hourly/daily basis.
PoE Status	*PoE Status* on Page 64	Port by Port: • PoE Mode • Operation Status • PD Class • Consumption(W) • Voltage(V) • Current(mA)

Type	Category	Details
Port Control	*Port Control* on Page 58	• Enable/Disable Port State • • Flow control - Disable/Symmetric • User-Defined Description
Port Statistics	*Port Statistics* on Page 88	Port by Port • Type • Link • State • Rx and Tx Good • Rx and Tx Bad • Rx Abort • Collision
Port Status	*Port Status* on Page 60	• Port Type • Link - Up/Down • State - Enable/Disable • Speed/Duplex • Flow Control
Port-Based VLAN	*Port Based VLAN* on Page 70	• Management VLAN ID (1-4094) • PVID • Allow to send to • Egress Tagged/Untagged
QoS Setting	*QoS Setting* on Page 71	Queue scheduling • Use 8.4.2.1 Weighted Fair Queuing Scheme • Use A Strict Priority Scheme Port Setting • CoS - 0 through 3 • Trust Mode - COS Only, DSCP Only, COS First, DSCP First, or Port Based
Rate Control	*Rate Control* on Page 61	• Ingress Packet Types - Broadcast Only, Broadcast/Multicast, Broadcast/Multicast/Unknown Unicast, and All • Ingress Rate/Egress Rate (No-limit, 128Kbps, 256Kbps, 512Kbps, 1024Kbps, 2048Kbps, 4096Kbps, and 8192Kbps) •

Type	Category	Details
Redundant Ring	*Redundant Ring* on Page 68	• 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 69	• 32 Ring ID Maximum (0-31) • Supports up to three 100M rings in one switch • Version • Role • Status • RM MAC • Blocking Port • Role Transition Count • Ring State Transition Count
Reset/Reboot	*Load Default* on Page 57 *System Reboot* on Page 57	• System Reset Button • Reset to Factory Default Values • Reboot from Interface
RSTP	*RSTP* on Page 65	Bridge Configuration: • Priority • Max Age (6-40 seconds) • Hello Time (1-10 seconds) • Forward Delay (4-30 seconds) Port Configuration: • Admin Path Cost • Priority • Admin P2P (Auto, P2P, or Shared) • Admin Edge (Enable/Disable)

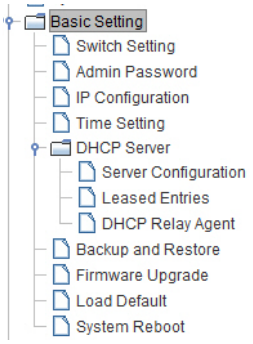
Type	Category	Details
RSTP Information	*RSTP Information* on Page 67	Root Information: • Bridge ID • Root Priority • Root Port • Root Path Cost • Max Age • Hello Time • Forward Delay Port Information (Port by Port): • Role • Port State • Oper Path Cost • Port Priority • Oper P2P • Oper Edge
SNMP Configuration	*SNMP Configuration* on Page 77	• V1/V2c Community • Public - Read Only or Read and Write • Private - Read Only or Read and Write
SNMP Traps	*SNMP Traps* on Page 79	• Enable/Disable • Trap Server - Server IP Address, Community, and Version (V1 or V2c) • Trap Server Profile - Displays Server IP, Community, and Version
SNMP V3 Profile	*SNMP V3 Profile* on Page 78	SNMP V3 • User Name • Security Level • Authentication Level • Authentication Password • DES Password SNMP V3 Users - Displays Profile Information
SYSLOG Mode	*SysLog Configuration* on Page 84	• Disable, Local, Remote, or Both • Remote IP Address
System Event Logs	*Event Log* on Page 89	• Index • Date • Time • Event Log
Time Setting	*Time Setting* on Page 46	• Manual or NTP Client • Time Zone Setting • Daylight Savings Time

Type	Category	Details
Topology Discovery	*Topology Discovery (LLDP)* on Page 90	• LLDP - Enable/Disable • LLDP Configuration - Timer and Hold Time • LLDP Port State - Local Port, Neighbor ID, Neighbor IP, and Neighbor VID
Upgrade Firmware	*Firmware Upgrade* on Page 55	Local or TFTP
Warning - SMTP Configuration	*SMTP Configuration* on Page 85	• 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:

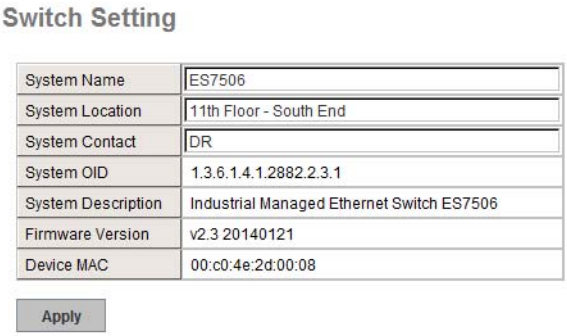


- *Switch Setting* on Page 43
- *Admin Password* on Page 44
- *IP Configuration* on Page 45
- *Time Setting* on Page 46
- *DHCP Server Configuration* on Page 49
- *DHCP Leased Entries* on Page 50
- *DHCP Relay Agent* on Page 51
- *Backup and Restore* on Page 52
- *Firmware Upgrade* on Page 55
- *Load Default* on Page 57
- *System Reboot* on Page 57

Optionally, you can use the CLI for configuration, see *Basic Settings (CLI)* on Page 108.

Switch Setting

You can assign the **System Name**, **Location**, **Contact** and view ES7506 information.

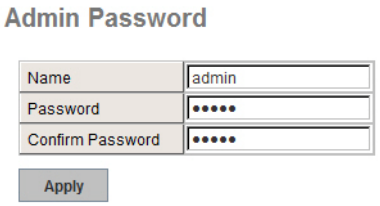


Switch Setting Page	
System Name	You can assign a name to the ES7506. You can input up to 64 characters. After you configure the name, The CLI system selects the first 12 characters as the name in CLI system.
System Location	You can specify the ES7506 physical location with up to 64 characters.
System 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 ES7506. 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	Industrial Managed Switch ES7506.
Firmware Version	Displays the firmware version installed in this ES7506.

Switch Setting Page (Continued)	
Device MAC	Displays a unique hardware address (MAC address) assigned at the factory.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

Admin Password

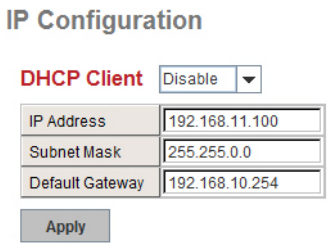
You can change the user name and the password here to enhance security.



Admin Password Page	
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 93), if you want to maintain these settings if the ES7506 is powered off.*

IP Configuration

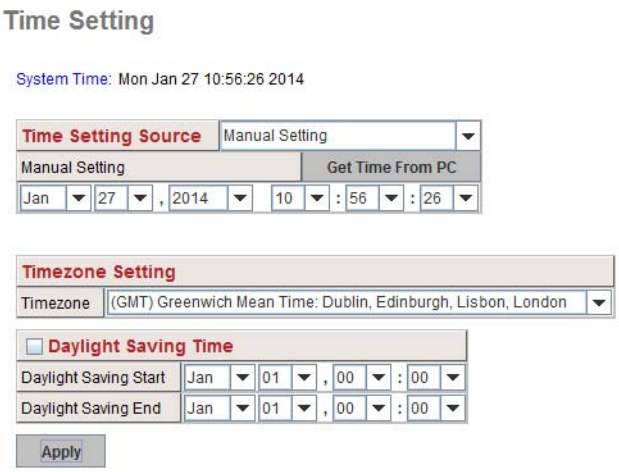
This function allows you to configure the ES7506's IP address settings.



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 ES7506. If the DHCP Client function is enabled, you do not need to assign an IP address to the ES7506, because it is overwritten by the DHCP server and displays here. The default IP Address is 192.168.250.250.
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.*
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 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 ES7506 also provides Daylight Saving functionality.



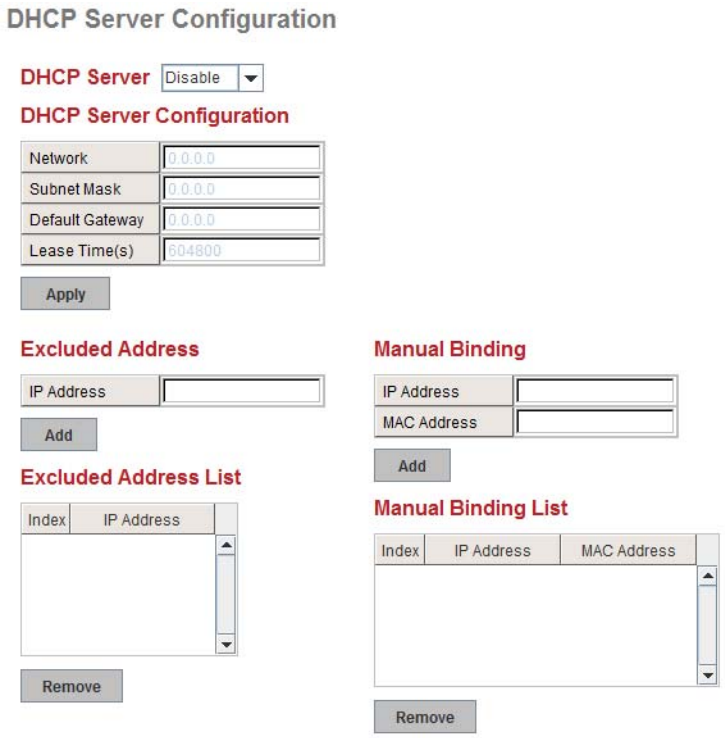
Time Setting Page	
Time Setting Source	**Manual Setting**: Click **Manual Setting** to change time as needed. You can also click the **Get Time from PC** button to get PC's time setting for the ES7506. **NTP client**: Click **Time Setting Source** if you want the NTP client to permit the ES7506 to enable 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.
Timezone Setting	Select the time zone where the ES7506 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 ES7506 time is one hour earlier than the actual time.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 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
```

DHCP Server Configuration

Use this page to configure DHCP server services.

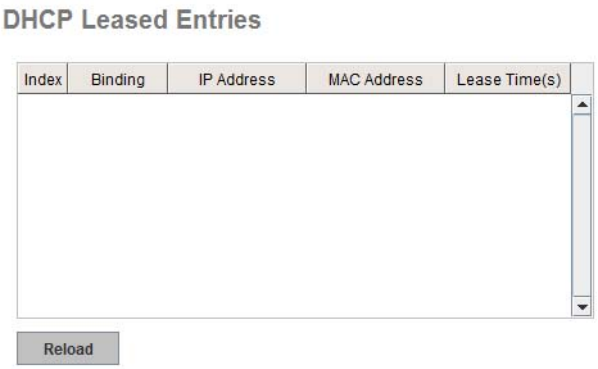


DHCP Server Configuration Page	
DHCP Server	You can select to **Enable** or **Disable** the DHCP Server function. The ES7506 assigns a new IP address to link partners.
DHCP Server Configuration	
Network	Enter the IPv4 address for the DHCP server.
Subnet Mask	Enter the subnet mask for the DHCP server.
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 93), if you want to maintain these settings if the ES7506 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**.

DHCP Server Configuration Page (Continued)	
Manual Binding	
IP Address	The ES7506 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 ES7506 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, 00C0.4E2D.0001. To remove a MAC address from the Manual Binding List, highlight the rule and click **Remove**.

DHCP Leased Entries

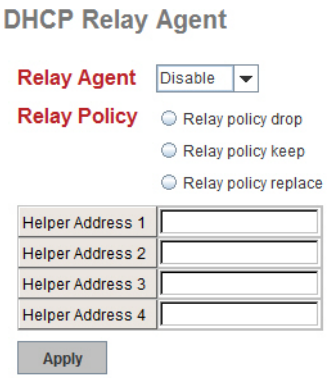
The ES7506 provides an assigned IP address.



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* page.



DHCP Relay Agent Page	
Relay Agent	You can select to **Enable** or **Disable** the DHCP Relay Agent function. The ES7506 assigns a new IP address to link partners.
Relay Policy	
Relay policy drop	Drops the option 82 field and do not add any option 82 field.
Relay policy keep	Keeps the original option 82 field and forwards to server.
Relay policy replace	Replaces the existing option 82 field and adds new option 82 field. (This is the default setting).
Helper Address 1-4	DHCP Server addresses for the Relay Agent.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

Backup and Restore

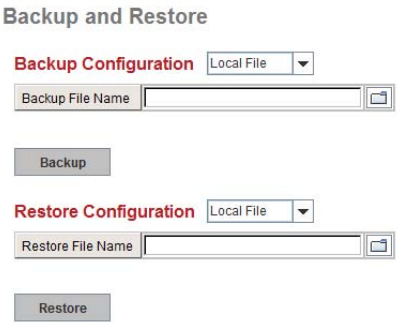
You can use the **Backup** option to save the current configuration saved in the ES7506 flash to a PC/laptop or a TFTP server.

This allows you to use the **Restore** option to restore a configuration file back to the ES7506 or load the same settings to another ES7506. Before you can restore a configuration file, you must save the backup configuration file in the PC or TFTP server. The ES7506 then downloads this file back into the flash.

The ES7506 configuration file is a standard text file. You can open the file with WordPad or Notepad. You can also modify the file, add/remove the configuration settings, and then restore the file back to the ES7506.

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

- Local File (Windows XP, only).
- TFTP Server



Note: *If you have Windows Server 2003 through Windows 8, you must use the TFTP Server method, the CLI, or PortVision DX to backup or restore configuration files.*

PortVision DX supports saving and loading configuration files, without any Windows operating system restrictions.

Backup & Restore Page	
Backup Configuration	• **Local File**: The ES7506 acts as the file server in Windows XP. Other Windows operating systems must use the TFTP method or PortVision DX. For procedures, see *Backup the Configuration - Local File Method* on Page 53. • **TFTP Server**: The ES7506 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 for 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 55.
Restore	Click to restore ES7506 startup configurations to the ES7506.
Backup Configuration	• **Local File**: The ES9528 acts as the file server in Windows XP. Other Windows operating systems must use the TFTP method or PortVision DX. For procedures, see *Backup the Configuration - Local File Method*. • **TFTP Server**: The ES9528 acts as a TFTP client. For procedures, see *Backup the Configuration - TFTP Server Method*. ***Note:*** *Pointing to the wrong file causes the entire configuration to be skipped.*
• The ES7506 provides a default configuration file in the ES7506. To load the default configuration file, you can use the **Reset** on the *Load Default* page on Page 57 or the **Reload** command in the CLI (Page 112). • You can use the CLI to view the latest settings running in the ES7506. 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 112. • 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.	

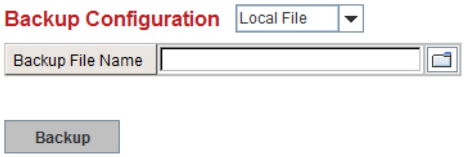
Backup the Configuration - Local File Method

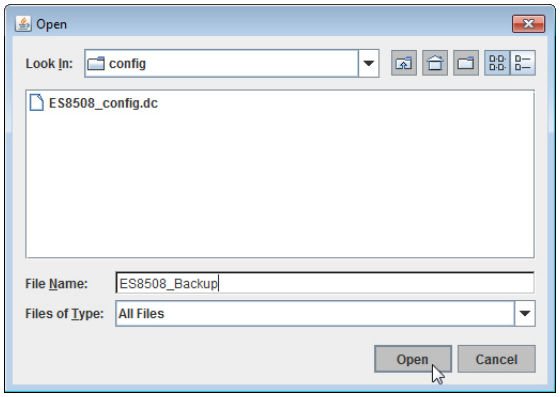
You can use **Local File** method to backup (or restore) with a Windows XP system.

Note: *If you have a Windows Server 2003 through Windows 7operating system, you must use the TFTP server method (Page 54). You can use PortVision DX which does not have any operating system restrictions.*

1. Open the web user interface for the ES7506 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.



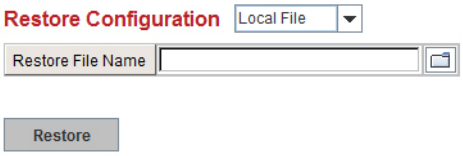


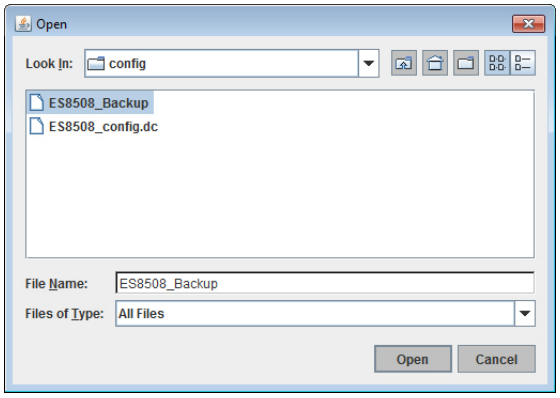
Restore the Configuration - Local Method

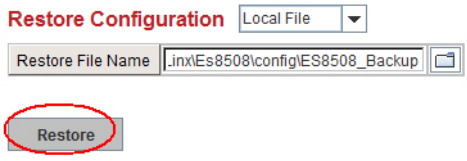
You can use **Local File** method to restore with a Windows XP system.

Note: *If you have a Windows Server 2003 through Windows 8 operating system, you must use the TFTP server method (Page 55) or use PortVision DX, which has no Windows operating system restrictions.*

1. Open the web user interface for the ES7506 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*.

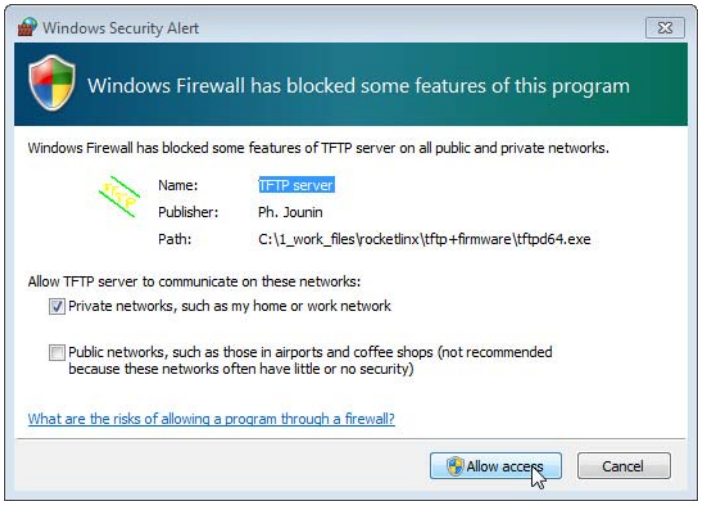
Backup the Configuration - TFTP Server Method

You must use a TFTP server to create or load backup files if you are using Windows Server 2003 through Windows 8.1 or PortVision DX. If you do not have a TFTP server, you can download one from Comtrol using the *Start the TFTP Server* subsection.

Start the TFTP Server

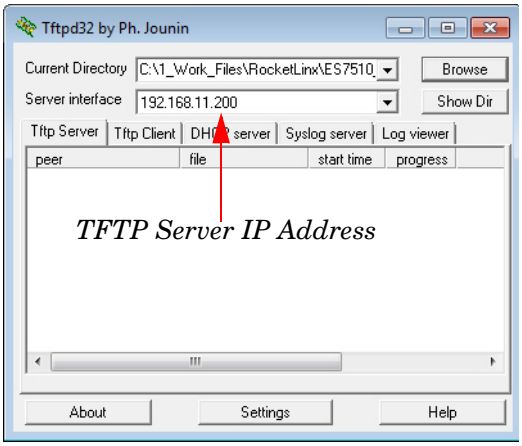
Use this procedure to download either the 32-bit or the 64-bit version from Comtrol.

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 *Create a Backup File* on Page 54..

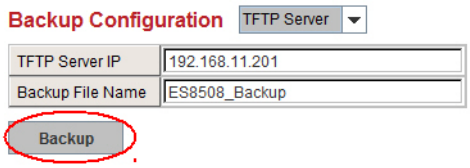
Note: *You will need the TFTP Server IP address in the next procedure.*



Create a Backup File

You must have a TFTP server open.

1. Open the web user interface for the ES7506 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.

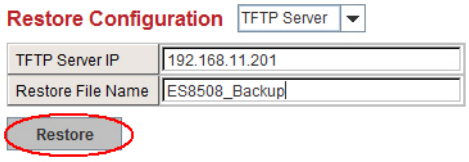
The backup file is located in the same directory that the TFTP server resides.

Restore the Configuration - TFTP Server Method

To restore a configuration file, you must open a TFTP server. If necessary, use *Start the TFTP Server* on Page 54.

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 ES7506, 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*.



Firmware Upgrade

Note: Use this section to update the ES7506 with the latest firmware. Comtrol provides the latest firmware on the Comtrol FTP site. Updated firmware may include new features, bug fixes, or other software changes. Comtrol Technical Support suggests you use the latest firmware before installing the ES7506 at a customer site.*Optionally, you can use PortVision DX to upload the latest firmware. If you need to upload a new version of the Bootloader, you must use PortVision DX. You cannot use the web user interface to upload the Bootloader.*

Firmware Upgrade Page	
System Firmware Version	The firmware version on the ES7506. You should check the version number after the switch reboots.
System Firmware Date	The build date of the firmware on the ES7506.
Firmware Upgrade	• **Local File (Windows XP) - see** *Upgrading Firmware (Local File)* on Page 56 • **TFTP Server** (Window Server 2003 - Windows 8.1) - see *Upgrading Firmware (TFTP Server)* on Page 57

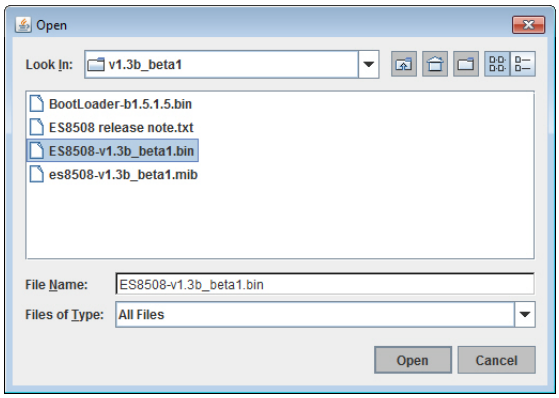
Note: *The system is automatically rebooted after you finish upgrading firmware. You should alert the attached users before updating the firmware that network interruption may occur.*

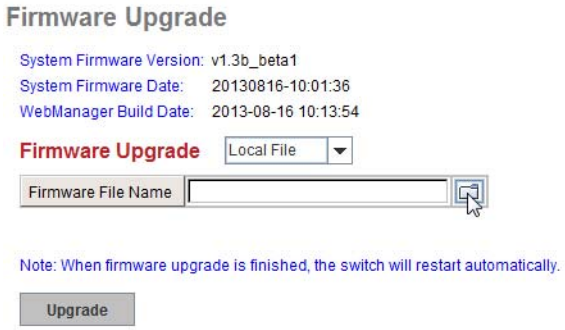
Upgrading Firmware (Local File)

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

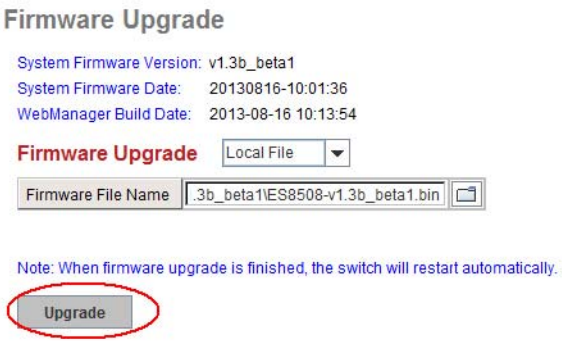
Note: *You can use PortVision DX to upload firmware. You must use PortVision DX or the CLI to upload Bootloader.*

1. Open the web user interface for the ES7506, 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.*

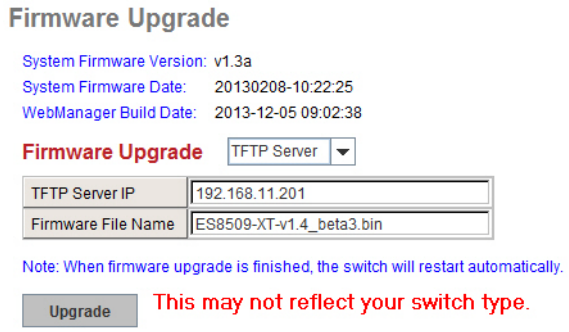
Upgrading Firmware (TFTP Server)

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

Note: *You can use PortVision DX to upload firmware. You must use PortVision DX or the CLI to upload Bootloader.*

1. Open a TFTP server, if necessary, see *Start the TFTP Server* on Page 54.
2. Place the ES7506 **.bin** file in the same directory where the TFTP server resides.
3. If necessary, open the web user interface, open the **Firmware Upgrade** page in the *Basic Settings* group.
4. Select **TFTP Server** in the **Firmware Upgrade** drop list.
5. Enter the IP address of the TFTP server, enter the firmware file name, and click the **Upgrade** button.
6. Click **Yes** to the *Confirm Dialog* message.
7. Click **Ok** to the *Warning Message*.
8. 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.*



Load Default

You can reset the ES7506 configuration values to default settings, excluding the network information.

Note: *You can also use PortVision DX to reset the switch to the default configuration values (excluding the network settings.).*

1. Click **Reset**, if you want the ES7506 to reset all configurations to factory default settings.

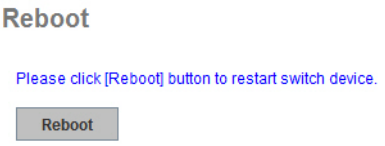
   The system displays a popup message window after finishing. The default settings work after rebooting the ES7506.
2. Click **Yes** in the popup message to reset the configuration to the factory defaults.
3. Click **OK** to the *Success Message*.
4. Go to the **Reboot** page, click the **Reboot** button.
5. Click **Yes** to reboot the ES7506.
6. Click **OK** to the *Success Message*.

System Reboot

System Reboot allows you to reboot the device. Most feature changes require a switch reboot to take affect.

Note: *Before rebooting, remember to click **Save** to save your settings. Otherwise, the settings you are lost when the ES7506 is powered off.*

1. Click the **Reboot** button to reboot your ES7506.
2. Click **Yes**. The switch reboots immediately.
3. Click **Ok**.



Port Configuration

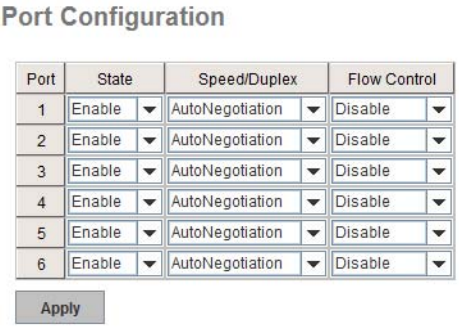
The *Port Configuration* group allows you to enable/disable port state, or configure port auto-negotiation, speed, duplex, flow control, rate limit control. It also allows you to view port status. The following pages are included in this group:

- *Port Control*
- *Port Status* on Page 60
- *Rate Control* on Page 61

Optionally, you can use the CLI for configuration, see *Port Configuration (CLI)* on Page 114.

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.

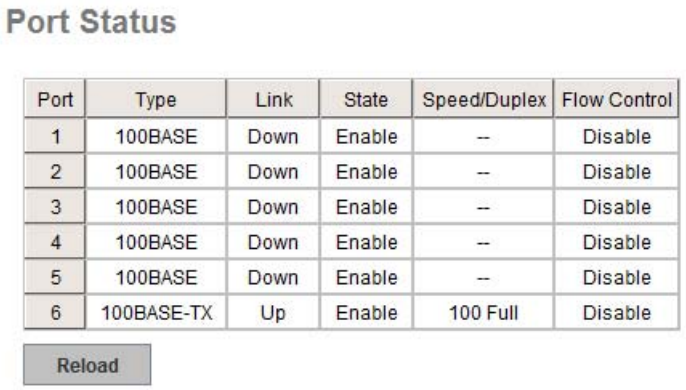
Port Configuration Page	
State	You can enable or disable the state of this port. Once you click **Disable**, the port stops to link to the other end and stops to forward any traffic. The default setting is **Enable** which means all the ports are workable when you receive the ES7506.
Speed/Duplex	You can configure port speed and duplex mode of each port. Below are the selections you can choose: • Fast Ethernet Ports 1~ 6 (fa1~fa6) - Auto Negotiation (default) - 10M full-duplex (10 Full) - 10M half-duplex (10 Half) - 100M full-duplex (100 Full) - 100M half-duplex (100 Half)
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.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 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

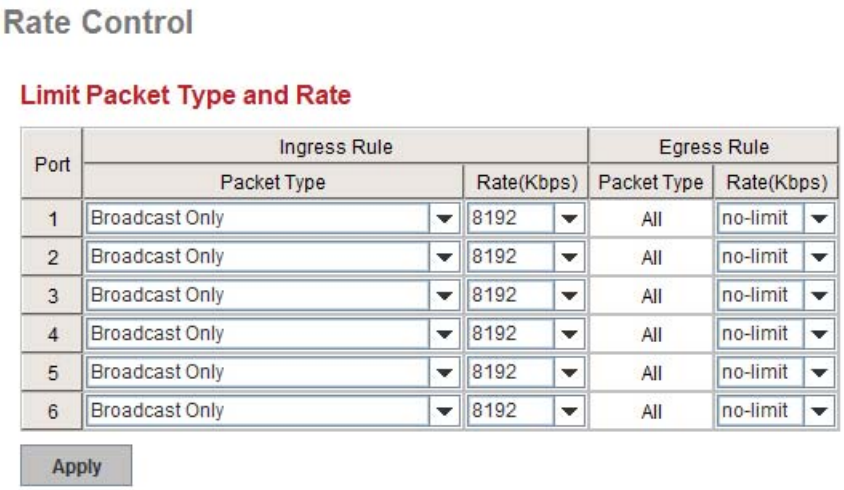
The *Port Status* page displays the current port status.



Port Status Page	
Type	100BASE-TX displays for Fast Ethernet 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.

Rate Control

Rate control is a form of flow control used to enforce a strict bandwidth limit of a port. You can program separate transmitting (Egress Rule) and receiving (Ingress Rule) rate limits for each port, and even apply the limit to certain packet types as described below.



Rate Control Page	
Ingress Packet Type	You can select the packet type that you want to filter. The Ingress packet types supported are: • Broadcast/Multicast/Unknown Unicast • Broadcast/Multicast • Broadcast • All The Egress rate supports all types of packets.
Ingress/ Egress Rate	These columns allow you to manually assign the limit rate of the port. Valid values support 128Kbps, 256Kbps, 512Kbps, 1024Kbps, 2048Kbps, 4096Kbps, and 8192Kbps.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

Power over Ethernet

Power over Ethernet is one of the key features of the ES7506.It supports IEEE 802.3at higher power capabilities and is in compliance with IEEE 802.3af standards. The ES7506 is equipped with power injectors on ports one through four. Each port is capable of delivering 0.651mA of current.

The following pages are included in this section:

PoE Control

The ES7506 also provides PD Status Detection. This provides automatic detection of a remote device powered by the ES7506. If the remote system crashes or is unstable, the ES7506 performs a system reboot by turning off and on again to trigger the remote device.

The power mode can be changed between IEEE 802.3af and forced via the combo box on the PoE configuration page. When using IEEE 802.3af the ES7506 provides power to any device that complies with the IEEE 802.3af specification.

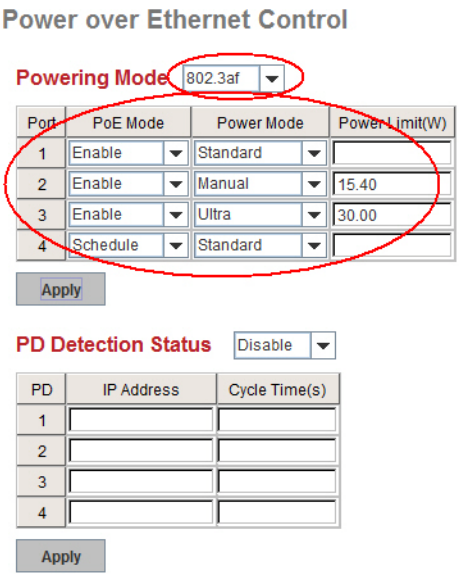
Note: *If **Forced** mode is selected, power is provided even if no Ethernet cable is plugged in. Only use **Forced** mode if you are attaching a device that is capable of receiving power through its Ethernet connection.*

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 the appropriate **Powering Mode** (**802.3af** or **Force**) for the ES7506 from the drop list.
2. Select the appropriate **PoE mode** (**Enable**, **Disable**, or **Schedule**) for the ES7506.

   Note: *If you select **Schedule**, you must configure the port or ports using PoE Scheduling on Page 64.*
3. Select the appropriate **Power Mode** (**Standard**, **Manual**, or **Ultra**) for each port that you enable or schedule.
4. Enter a valid **Power Limit** based on the attached power supply.
5. Click **Apply**.
6. If desired, set up **PD Status Detection**.
7. You must **Save** the settings (Page 93), if you want maintain these settings if the ES7506 is powered off.



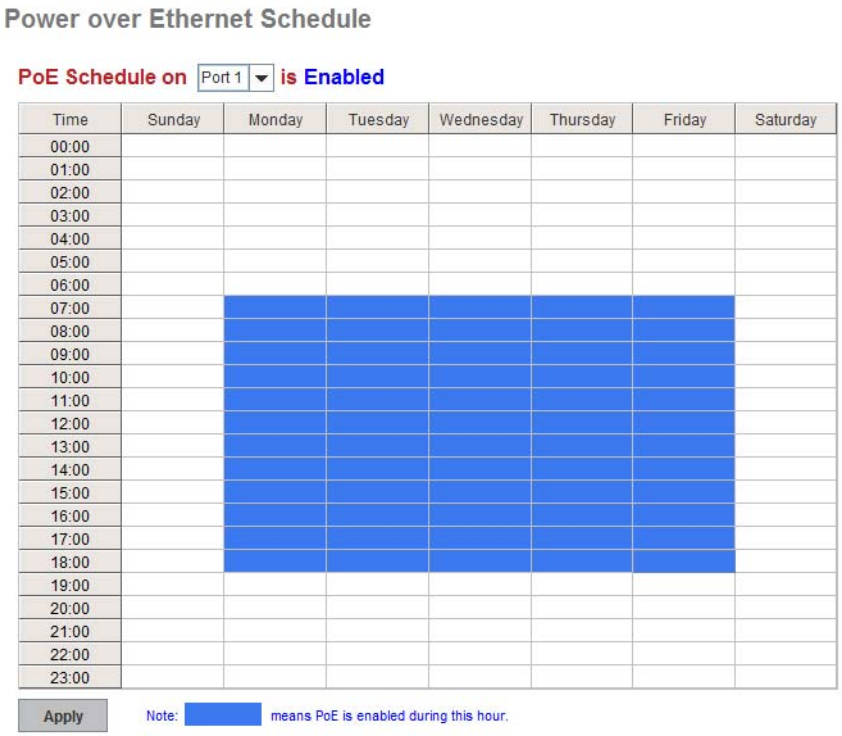
Power Over Ethernet Control Page	
Powering Mode	
PoE Mode	Each port's ability to deliver power can be individually enabled or disabled using the **PoE Mode** combo box. You can select **802.3af** or **forced**.
Power Mode	There are three power modes available for each port. • **Standard** mode delivers power following the IEEE 802.3af specification. • **Manual** mode allows the user to specify the wattage limit delivered to an IEEE 802.3af device. • **Ultra** mode should be used for IEEE802.3at power requirements and allows the user to configure the wattage limit above 15.4 watts. ***Note:*** *To deliver higher amounts of power the ES7506 must be powered with a 55VDC power supply.* *When delivering more than 15.4W of power, ensure the ES7506 is mounted on panel capable of dissipating heat. Also ensure the temperature where the ES7506 is located is kept under 60°C. Delivering power above 15.4W causes the ES7506 to generate more heat.*
Power Limit	The limitation of the output power (watts) range is standard mode: N/A, Manual mode: 0.44 - 15.4W, and Ultra mode: 0.44 - 30W.
PD Status Detection	
PD Status Detection	**Enable/Disable** 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 93), if you want maintain these settings if the ES7506 is powered off.*

PoE Scheduling

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

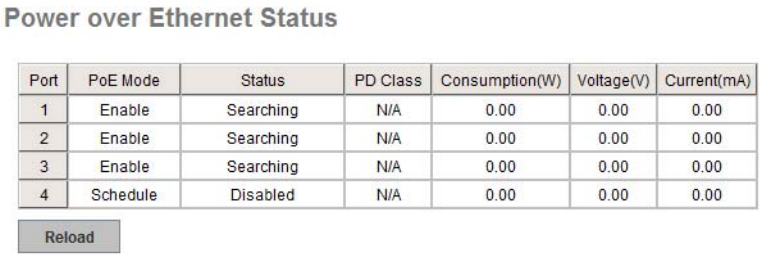
You can schedule a PoE port after the **PoE Mode** has been set to **Schedule** in the *PoE Control* page.

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 62) if you need to make any changes.



Network Redundancy

It is critical for industrial applications that the network remains running at all times. The ES7506 supports:

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

  The ES7506 supports RSTP versions IEEE 802.1D-2004, IEEE 802.1D-1998 STP, and IEEE 802.1w RSTP.
- 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 ES7506 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:

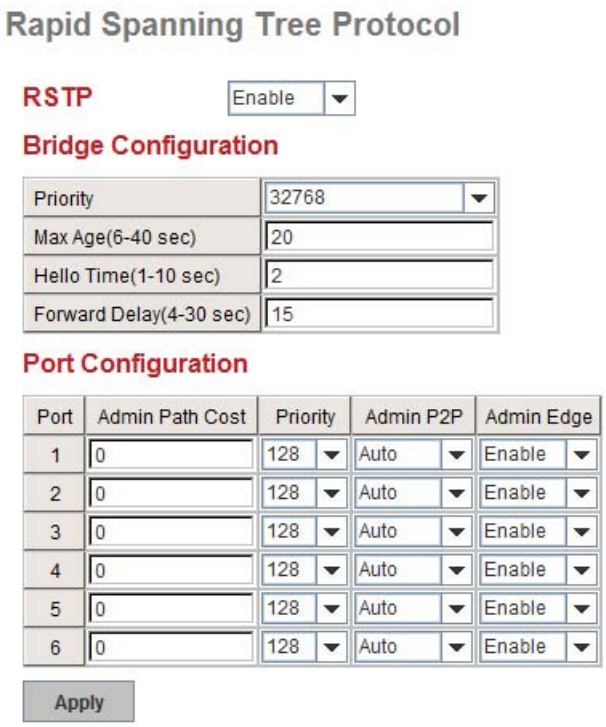
- *RSTP* on Page 65
- *RSTP Information* on Page 67
- *Redundant Ring* on Page 68
- *Redundant Ring Information* on Page 69

Optionally, you can use the CLI to configure these features, see *Network Redundancy (CLI)* on Page 121.

RSTP

If a switch has more than one path to a destination, it leads to message loops that can generate broadcast storms and quickly bog down a network.

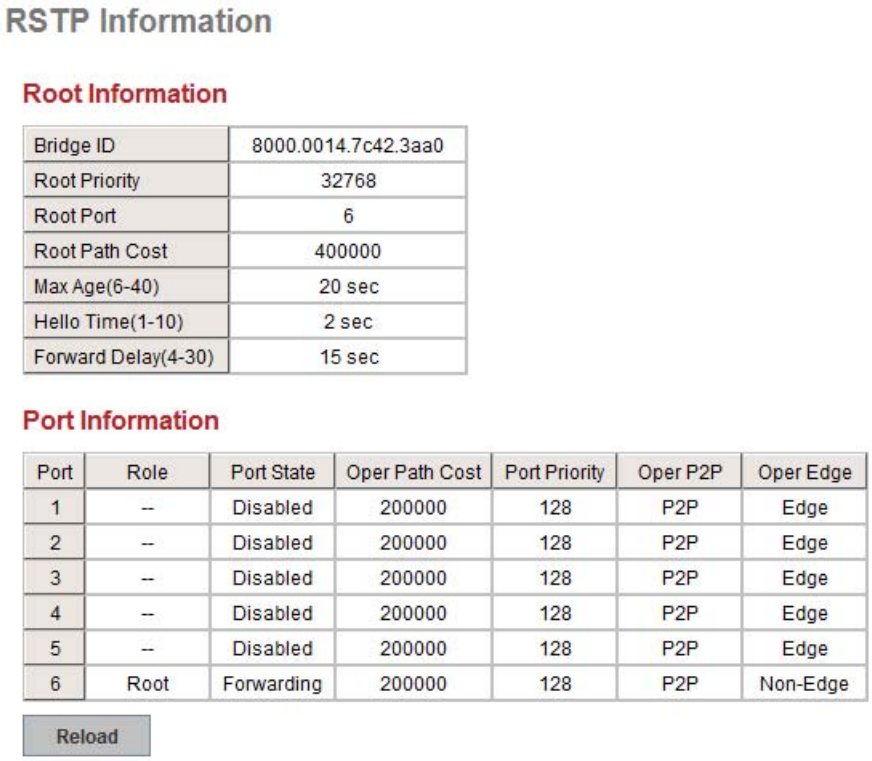
The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree uses a spanning tree algorithm (STA) to automatically sense whether a switch has more than one way to communicate with a node. It then selects the best path (primary), and blocks the other paths. It also keeps track of the blocked paths in case the primary path fails. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. It is specified in IEEE 802.1D-1998. Later, Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, IEEE 802.1w is included into the IEEE 802.1D-2004 version. This switch supports both RSTP and STP (all switches that support RSTP are also backward compatible with switches that support only STP).This page allows you to enable/disable RSTP, configure the global setting and port settings.



Rapid Spanning Tree Protocol Page	
RSTP	You must first **Enable** STP/RSTP mode, before configuring any related parameters. Parameter settings required for both STP and RSTP are the same. 802.1d refers to STP mode, while 802.1w refers to faster RSTP mode.
Bridge Configuration	
Priority (0-61440)	RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. The bridge with the highest priority becomes the highest bridge ID. If all the bridge IDs have the same priority, the bridge with the lowest MAC address then becomes the root bridge. ***Note:*** *The bridge priority value must be in multiples of 4,096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32,768.*
Max Age (6-40)	Enter a value from 6 to 40 seconds here. This value represents the time that a bridge waits without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure. If the ES7506 is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then the ES7506 reconfigures itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices renegotiate to set up a new spanning tree topology.
Hello Time (1-10)	Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out bridge protocol data unit (BPDU) packet to check current STP status. The root bridge of the spanning tree topology periodically sends out a *hello* message to other devices on the network to check if the topology is *healthy*. The *hello time* is the amount of time the root has waited during sending *hello* messages.
Forward Delay Time (4-30)	Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state. This is the amount of time the ES7506 waits before checking to see if it should be changed to a different state.
Note: *You must observe the following rule to configure Hello Time, Forwarding Delay, and Max Age parameters.* `2 × (Forward Delay Time – 1 sec) ≥ Max Age Time ≥ 2 × (Hello Time value + 1 sec)`	
Port Configuration	
Admin Path Cost	Enter a number between 1 and 200,000,000. This value represents the *cost* of the path to the other bridge from the transmitting bridge at the specified port.
Priority	Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.
Admin P2P	Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (that is, it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e, it is served by a shared-medium LAN segment). This function allows P2P status of the link to be manipulated administratively. **Auto** means to auto select P2P or Share mode. **P2P** means P2P is enabled, while **Share** means P2P is disabled.
Admin Edge	A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the **Enable** state. When the non-bridge device connects an admin edge port, this port is in a blocking state and turns to a forwarding state in 4 seconds.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

RSTP Information

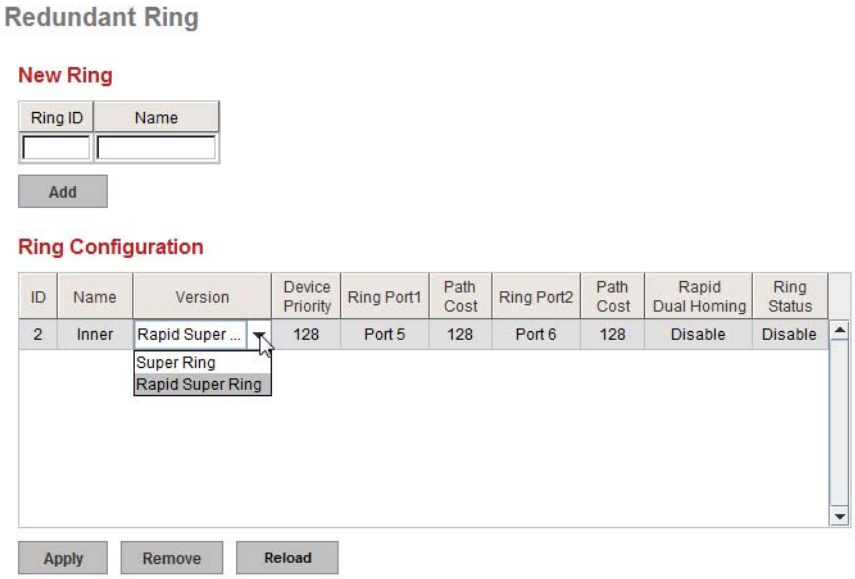
This page allows you to see the information of the root switch and port status.



RSTP Information Page	
Root Information	You can see root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.
Port Information	
Port Role	Descriptive information about the RSTP switch port role. Role Root, Designated, Alternate, Backup, Disabled, Unknown.
Port State	Descriptive information about the 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.
Oper P2P	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).
Oper Edge	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 admin edge port, this port is in blocking state and turn to forwarding state in 4 seconds.
Reload	Click to reload.

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. The ES7506 can only create a single ring.

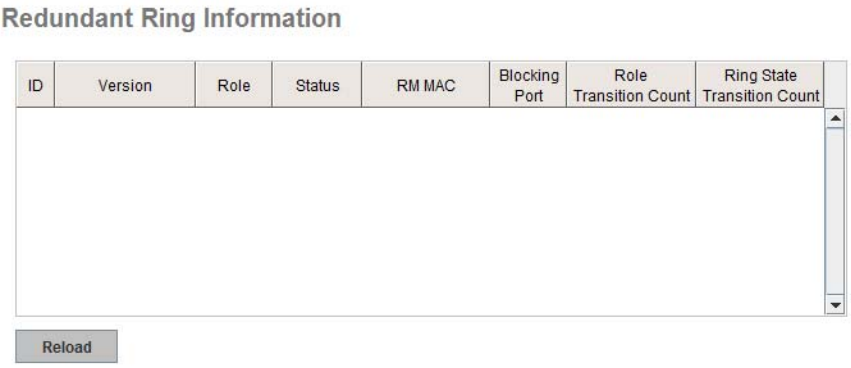


Redundant Ring Page	
New Ring (Ring ID/Name)	To create a Redundant Ring enter the Ring ID, which has range from 0 to 31. If the name field is left blank, the name of this ring is automatically named with the Ring ID. The maximum number of rings is 32. ***Note:*** *Once a ring is created, you cannot change 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 93), if you want to maintain these settings if the ES7506 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 ES7506 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, which helps to find the redundant path.
Blocking Port	Shows which is blocked port of RM.
Role Transition Count	Shows how many times this ES7506 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

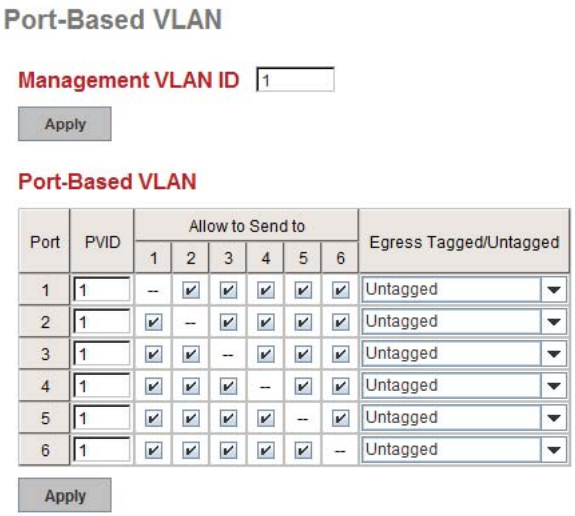
The RocketLinx ES7506 supports Port-Based VLAN functionality for the purpose of limiting a broadcast domain to specific members of a group by physically grouping the members together.

The RocketLinx ES7506 determines the membership of a data frame by examining the configuration of the port that received the transmission, or by reading a portion of the data frame's tag header. A four-byte field in the header is used to identify the VLAN. This VLAN identification indicates which VLAN the frame belongs to. If the frame has no tag header, the switch checks the VLAN setting of the port that received the frame. If the switch has been configured for port based VLAN support, it assigns the port's VLAN identification to the new frame.

The following commands are included in this section VLAN Port-Based (CLI) on Page 126.

Port Based VLAN

This subsection discusses port base VLAN.



Port-Based VLAN Page	
Management VLAN ID	This configuration is for the RocketLinx ES7506 management interface security. Only the management packet with the same VLAN ID will forward to a CPU interface. You can assign an ID number from 1 to 4094.
Port-Based VLAN	
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 1 to 4094 but, 0 and 4095 are reserved. You can not enter these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column.
Allow Send To	This column defines the to which port that traffic could be forwarded. You can click the icon to join the port as a Port Based VLAN group.
Egress Tagged/ Untagged	Each port of the RocketLinx ES7506 supports Tag modify function. It includes Untagged, Tagged or Un-modify modes. The packets egress from this port is modified according to the selected rule.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the RocketLinx ES7506 is powered off.*

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 ES7506 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.

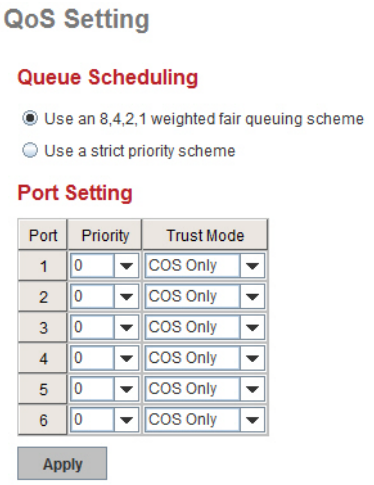
The following web pages are included in this group:

- *QoS Setting*
- *CoS-Queue Mapping* on Page 72
- *DSCP-Queue Mapping* on Page 73

Optionally, you can use the CLI for configuration, see *Traffic Prioritization (CLI)* on Page 127.

QoS Setting

Use this subsection to set up QoS settings for the ES7506.



QoS Setting Page	
Queue Scheduling	
Use an 8,4,2,1 weighted fair queuing scheme	This is also known as **WRR** (Weight Round Robin). The ES7506 follows the 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system processes 8 packets with the highest priority in the queue, 4 with middle priority, 2 with low priority, and 1 with the lowest priority at the same time.
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.

QoS Setting Page (Continued)	
Port Setting	
Trust Mode	**Trust Mode** indicates the Queue Mapping types that you can select. • **COS Only** (default): The port priority follows the CoS-Queue Mapping you have assigned. The ES7506 provides the default CoS-Queue table for which you can refer to for the next command. • **DSCP Only**: Port priority only follows the DSCP-Queue Mapping you have assigned. • **COS first**: Port priority follows the CoS-Queue Mapping first, and then the DSCP-Queue Mapping rule. • **DSCP first**: Port priority follows the DSCP-Queue Mapping first, and then the CoS-Queue Mapping rule. • **Port Based**: The port priority follows the queue priority that you have assigned.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

CoS-Queue Mapping

Use this page to change the CoS values into the Physical Queue mapping table. Since the switch fabric of ES7506 supports four queues, Lowest, Low, Middle, and High users should therefore assign how to map the CoS value to the level of the physical queue.

You can assign the mapping table or follow the suggestion of the IEEE 802.1p standard. The ES7506 uses IEEE 802.1p suggestion as default values. CoS Values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS Values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS Values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS Values 6 and 7 are mapped to physical Queue 3, the high 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.

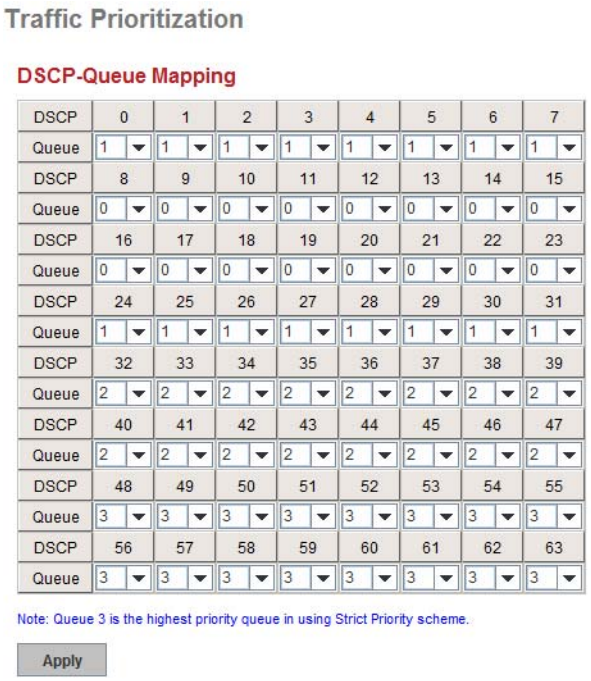
Differentiated Services (DiffServ) is a model where traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field. Defined in RFC2474 and RFC2475, the DiffServ standard supersedes the original specification for defining packet priority described in RFC791. 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 93), if you want to maintain these settings if the ES7506 is powered off.*

DSCP-Queue Mapping

Use this page to change DSCP values to Physical Queue mapping table. Since the switch fabric of the ES7506 only supports four queues. Lowest, Low, Middle and High users should therefore assign how to map DSCP values to the level of the physical queue. You should therefore assign how to map DSCP value to the level of the queue. 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 93), if you want to maintain these settings if the ES7506 is powered off.*

Multicast Filtering

For multicast filtering, the ES7506 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 75
- *IGMP Query* on Page 76

Optionally, you can use the CLI for configuration, see *Multicast Filtering (CLI)* on Page 130.

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.

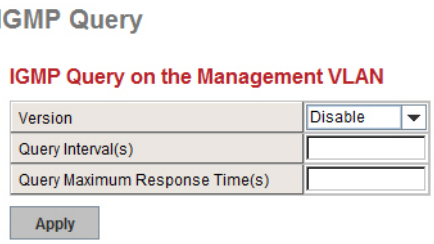
IGMP Snooping Page	
IGMP Snooping	You can select **Enable** or **Disable**. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN. You can **Enable** IGMP Snooping for some VLANs so that some of the VLANs support IGMP Snooping and others do not. To assign IGMP Snooping to 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 ES7506 supports 256 multicast groups. Click **Reload** to refresh the table.

Note: *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

IGMP Query

Use this page to configure the IGMP Query feature. Since the ES7506 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.

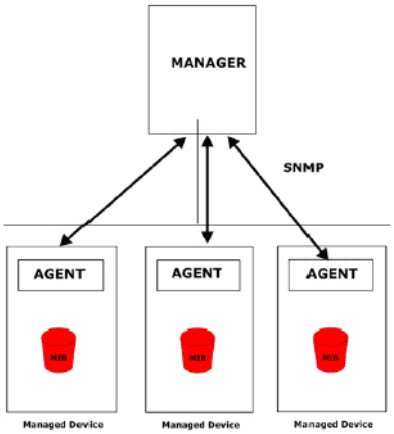
The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.



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 93), if you want to maintain these settings if the ES7506 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 ES7506 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.

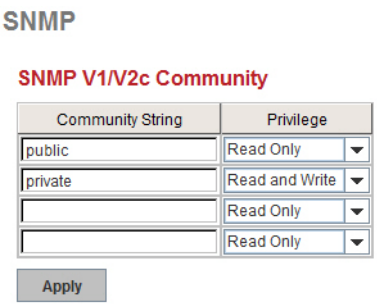
The following web pages are included in this group:

- *SNMP Configuration*
- *SNMP V3 Profile* on Page 78
- *SNMP Traps* on Page 79

Optionally, you can use the CLI for configuration, see *SNMP (CLI)* on Page 133.

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:

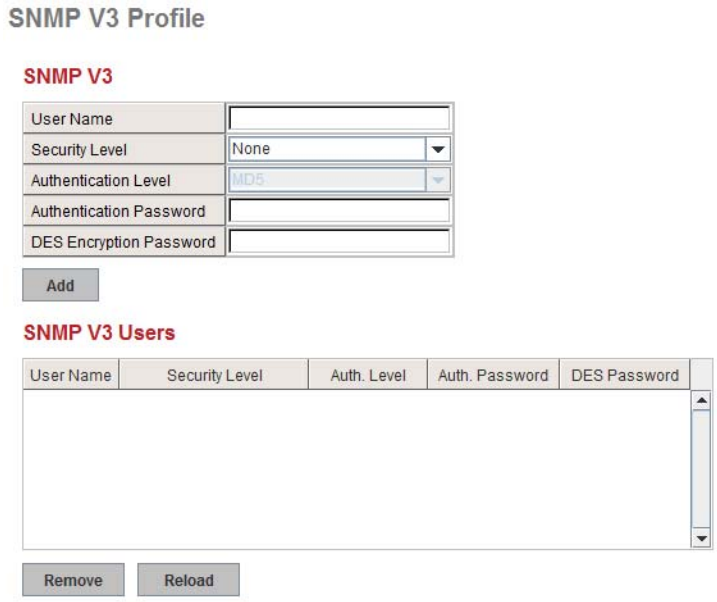
- **Read Only** privilege, you only have the ability to read the values of MIB tables. The default community string is **public**.
- **Read and Write** privilege, you have the ability to read and set the values of MIB tables. The default community string is **private**.

The ES7506 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 ES7506 and the administrator are encrypted to ensure secure communication.

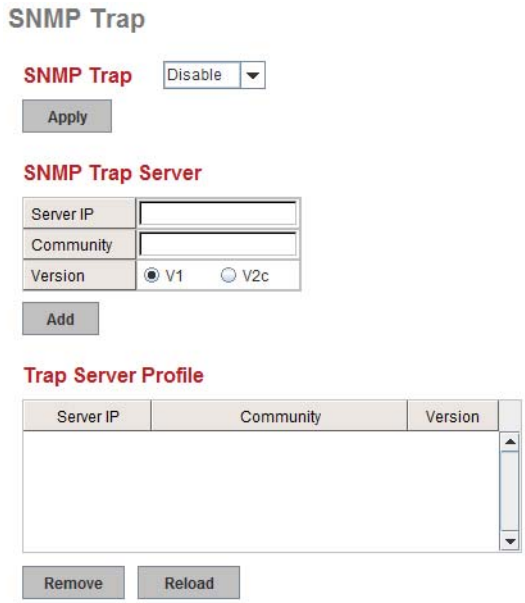


SNMP V3 Profile Page	
User Name	SNMP v3 user name.
Security Level	Select the following levels of security: **None**, **Authentication**, and **Authentication and Privacy**.
Authentication Level	Select either **MD5** (Message-Digest algorithm 5) or **SHA** (Secure Hash Algorithm). • **MD5** is a widely 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 ES7506 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.
Authentication 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 93), if you want to maintain these settings if the ES7506 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 93), if you want to maintain these settings if the ES7506 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 on the Comtrol ftp site.

Note: *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

Security

The ES7506 provides several security features for you to secure your connection. The following pages are included in this group:

- *IP Security* on Page 80

Optionally, you can use the CLI for configuration, see *Security (CLI)* on Page 134.

IP Security

Use the *Security IP* page to set up specific IP addresses to grant authorization for management access to this ES7506 through a web browser or Telnet.

IP Security Page	
IP Security	Select **Enable** and **Apply** to enable the IP security function.
Add Security IP	You can assign specific IP addresses and then click **Add**. Only these IP addresses can access and manage ES7506 through a web browser or Telnet. The maximum security IP is 10.
Security IP List	This table shows you added the security IP addresses.
Remove	Click **Remove** to delete a highlighted entry.
Reload	To reload the table.

Warning

The ES7506 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 83
- *SysLog Configuration* on Page 84
- *SMTP Configuration* on Page 85

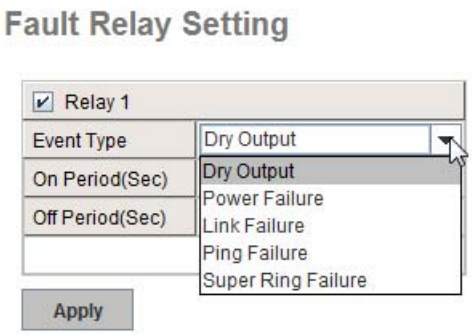
Optionally, you can use the CLI for configuration, see *Warnings (CLI)* on Page 136.

Fault Relay

The ES7506 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 Ring Topology Change. You can enable and select relay trigger by clicking the **Apply** button.

Relay 1: Enable the Relay 1 box, and then select the **Event Type** and its parameters.

Event Type: You are given the following options: Dry Output, Power Failure, Link Failure, Ping Failure, and Super Ring Failure. Each event type has its own parameters and is configurable. Each Relay can have one event type.

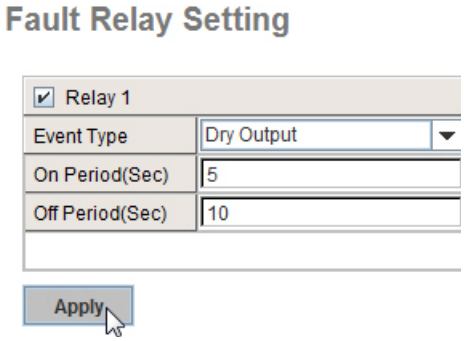


Event Type: Dry Output

On Period (Sec): Enter the amount of time you would like the Relay Output to be on. This can range from 0-4294967295 seconds.

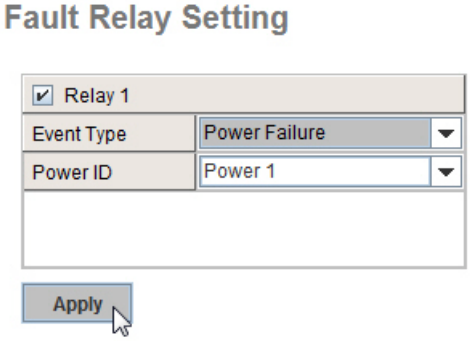
Off Period (Sec): Enter the amount of time you would like the Relay Output to be off. This can range from 0-4294967295 seconds.

When the amount of time is reached, the ES7506 turns the Relay Output on or off.



Event Type: Power Failure

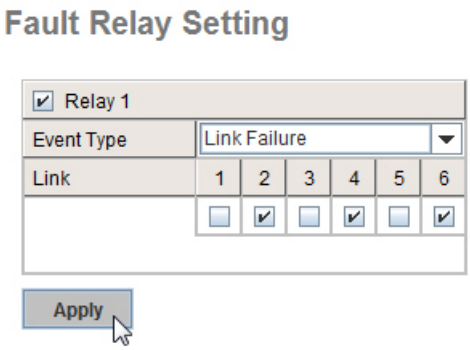
Power ID: Select either Power 1 or Power 2. When power is shut down, the ES7506 shorts the Relay Out and the DO LED lights.



Event Type: Link Failure

Link: Select the port ID you would like to monitor.

How to configure: Check the box of the Ethernet port or ports you want to monitor. When the selected ports are unlinked, the system shorts the Relay Output and light the DO LED.

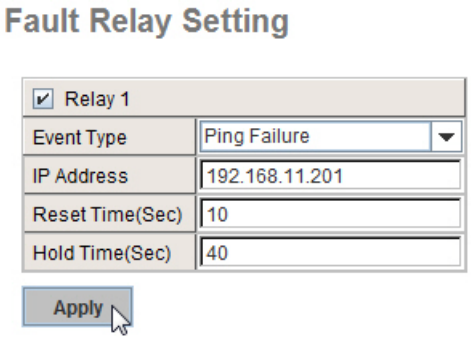


Event Type: Ping Failure

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

Reset Time (Sec): Enter the amount of time after a ping has failed that you would like the relay output to turn off.

Hold Time (Sec): Enter the amount of time after a ping has failed and relay output has been turned off, that you would like the relay output to be turned back on.



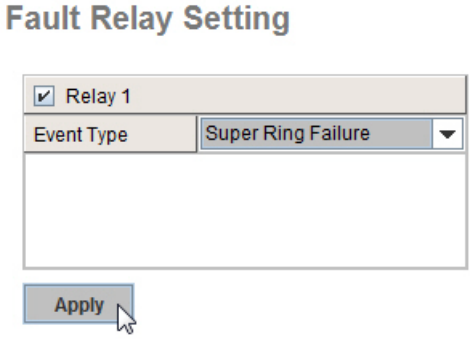
How to configure*:* After selecting the Ping Failure event type, the system changes the Relay Output to *short* state, lights the alarm LED, and continuously pings the target device. When the ping failure for the Reset Time times out, the system changes the Relay Output to *open* state and turns off the alarm LED for the amount of time entered in the Hold Time. After the Hold Time times out, the ES7506 starts sending ping commands to the remote device.

Example: When the Reset Time is set to 10 sec while the Hold Time is set to 40 sec the following occurs. After ping has failed after 10 seconds (Reset Time), the system turns the Relay Output and Alarm LED off. After 40 seconds (Hold Time), the system turns the Relay Output and the Alarm LED on again.

Event Type: Super Ring Failure

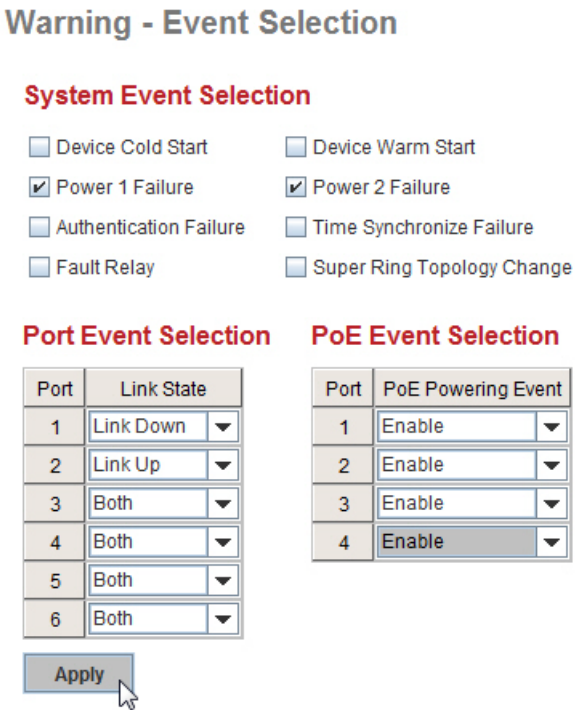
Select **Ring Failure** and when the Ring topology changes, the ES7506 shorts the Relay out and light the Alarm LED.

Once you have finished configuring the settings, click the **Apply** button 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.
Power 1 Failure	Select this if you want the ES7506 to send notification of a PW1 failure.
Power 2 Failure	Select this if you want the ES7506 to send notification of a PW2 failure.
Authentication failure	An incorrect password or SNMP Community String is entered.
Time Synchronize Failure	Accessing the NTP Server is failing.
Fault Relay	TheFault Relay is on.
Super Ring Topology Changes	Master of Super Ring has changed or backup path is activated.

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.
PoE Powering Event	**Warning Event is sent when…..**
Disable	The PoE port is not powering.
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

SysLog Configuration

The System Log provides the system administrator ES7506 events history. There are two System Log modes provided by the ES7506, **Local** mode and **Remote** mode.

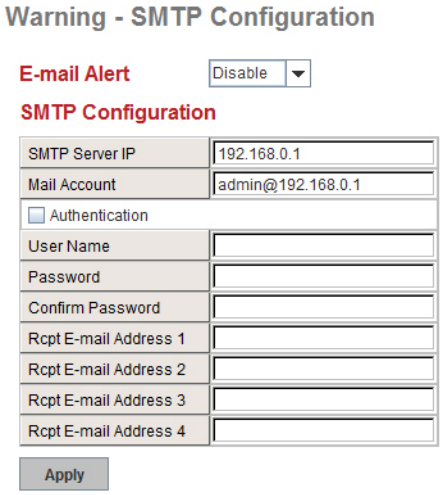
Warning - SysLog Configuration Page	
Syslog Mode	There are two system logs available: • **Local Mode**: The ES7506 prints the events that have been selected in the Event Selection page to the System Log table of the ES7506. You can monitor the system logs in the *Monitor and Diag /Event Log* page. • **Remote Mode**: Assign the IP address of the System Log server. The ES7506 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 93), if you want to maintain these settings if the ES7506 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 ES7506 supports an email alert feature. The ES7506 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 ES7506.	
Rcpt E-mail Address 1	The first email address to receive an email alert from the ES7506 (maximum 40 characters).
Rcpt E-mail Address 2	The second email address to receive an email alert from the ES7506 (maximum 40 characters).
Rcpt E-mail Address 3	The third email address to receive an email alert from the ES7506 (maximum 40 characters).
Rcpt E-mail Address 4	The fourth email address to receive an email alert from the ES7506 (maximum 40 characters)
Apply	Click **Apply** to apply the settings. ***Note:*** *You must **Save** the settings (Page 93), if you want to maintain these settings if the ES7506 is powered off.*

Monitor and Diag

The ES7506 provides several web user interface pages for you to monitor the status of the switch or diagnostics when encountering problems related to the ES7506. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log, and Ping.

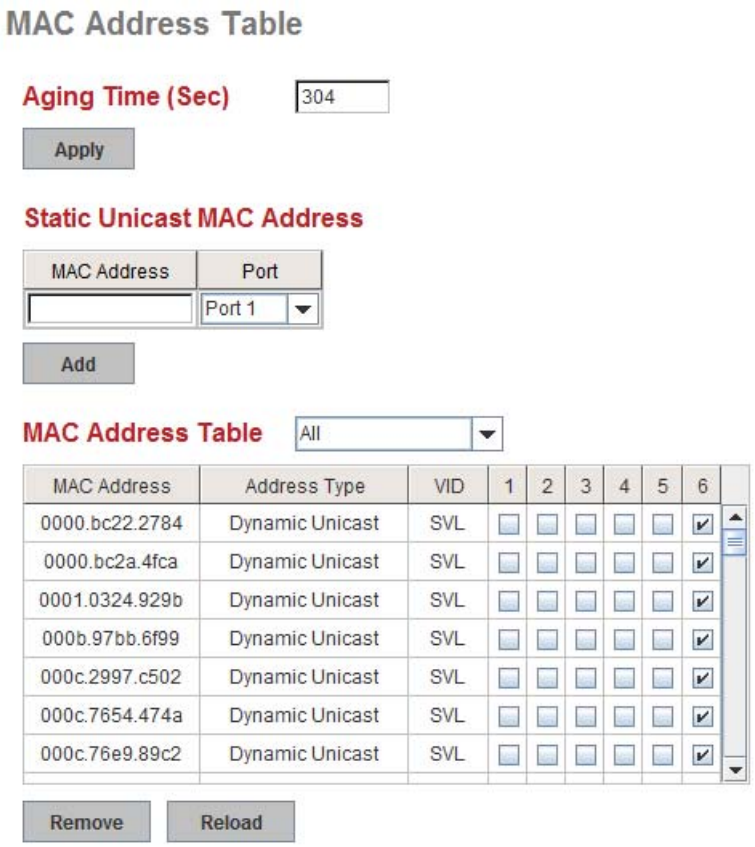
The following web pages are included in this group:

- *MAC Address Table*
- *Port Statistics* on Page 88
- *Event Log* on Page 89
- *Topology Discovery (LLDP)* on Page 90
- *Ping Utility* on Page 91

Optionally, you can use the CLI for configuration, see *Monitor and Diag (CLI)* on Page 139.

MAC Address Table

The ES7506 provides 2K 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 93), if you want to maintain these settings if the ES7506 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.*

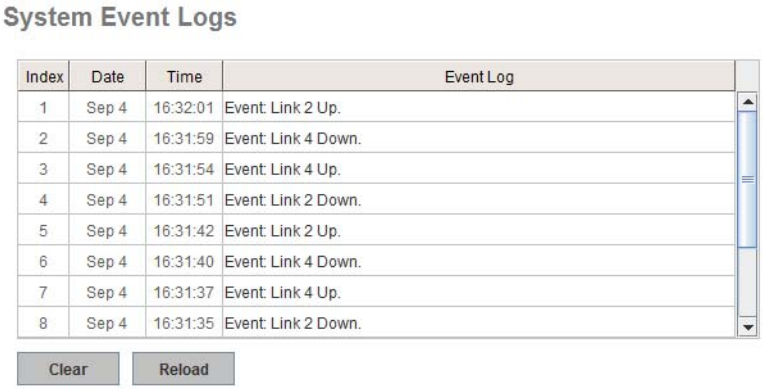
The following information provides a view of the current port statistic information.

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.
Bad-Collision Mode	Click to change the counter mode to RxBad and TxCollision mode.
Good Mode	Click to change the counter mode to RxGood and TxGood.

Event Log

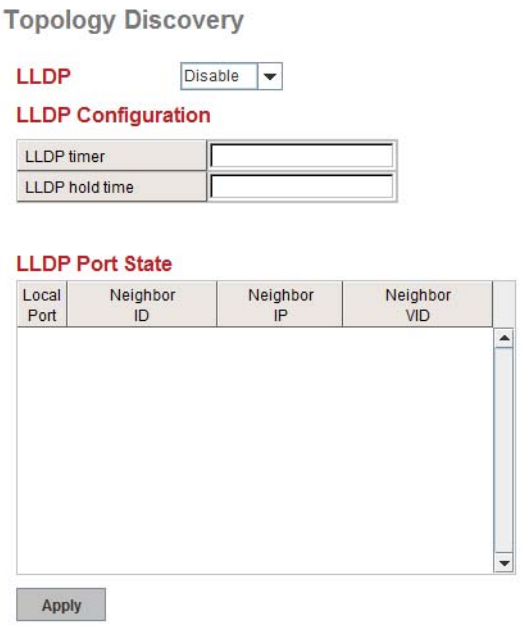
The System Log feature was introduced in *SysLog Configuration* on Page 84. When **System Log Local** mode is selected, the ES7506 records events that occurred in the local log table. This page shows the log table. The entry includes the index, occurred data and time, and content of the events.

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



Topology Discovery (LLDP)

The ES7506 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.

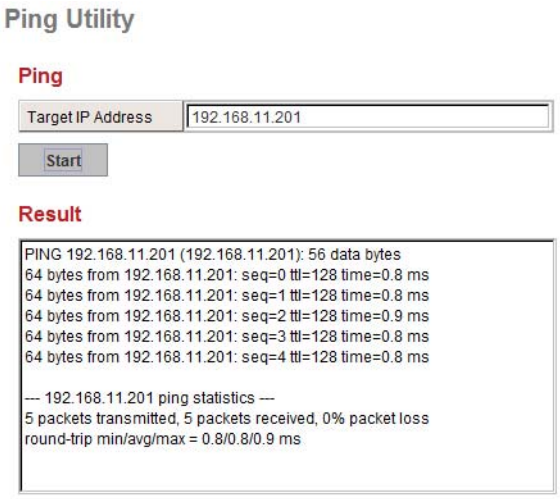


With LLDP functionality, NMS can easily maintain the topology map, display port ID, port description, system description, and VLAN ID. Once a link failure occurs, the topology changes the events that can be updated to the NMS as well. The **LLDP Port State** can display the neighbor ID and IP learnt 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 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 93), if you want to maintain these settings if the ES7506 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 ES7506.

Device Front Panel

LEDs	LED On/Link Up	LED Off/Link Down
Alm (Alarm)	Red	White
PW1	Green	White
PW2	Green	White
R.M. (Ring Master)	Green	White
PoE 1-4	Green	White
LNK/ACT 1-6	Green	White

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 12**, which provide detailed LED information.*

Save to Flash

The **Save Configuration** page saves any changes to the configuration to the flash.

If the switch loses power before clicking **Save Configuration** causes loss of the new settings. Applying changes on web user interface pages do not save the changes to the flash.

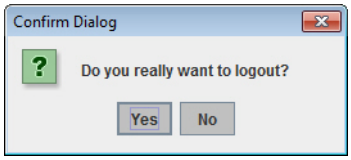
After selecting **Save Configuration**, click **Save to Flash** to save your new configuration.

Optionally, you can use the CLI, see *Saving to Flash (CLI)* on Page 141.

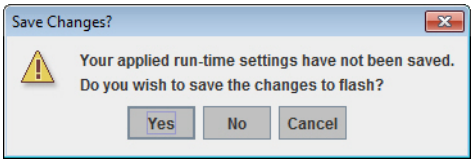
Logout

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 ES7506 provides in-band and out-band configuration methods:

- Out-band management means that you configure the ES7506 using the RS-232 console cable and the Command Line Interface (CLI) to access the ES7506 without attaching an admin PC to the network. You can use out-band management if you lose the network connection to the ES7506.
- In-band management means that you connect remotely using the ES7506 IP address through the network. You can remotely connect with the ES7506 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 ES7506 IP address to meet your network requirements. The easiest way to configure the IP address is using a Windows system and NetVisionPortVision DX, which is discussed in *Configuring the Network Settings* on Page 17.

If you want to use the web user interface for configuration, see *Configuration Using the Web User Interface* on Page 31.

Use the following procedures to access the ES7506 using the CLI:

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

This section contains information about the following groups of commands:

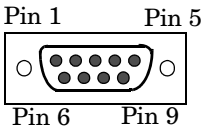
Using the Serial Console

Comtrol provides one RS-232 RJ45 console cable with the ES7506.

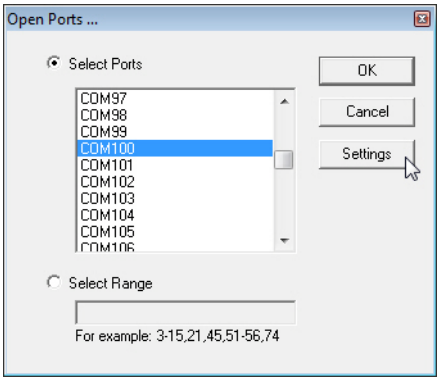
Note: *A system COM port is required to use a serial console connection. If you do not have an available COM port, use the Using a Telnet/SSH Console procedure on Page 98.*

1. Attach the RS-232 DB9 connector to your PC COM port and connect the other end to the **Console** port of the ES7506. If you misplace the cable, you can use this console cable pin assignment or purchase a null-modem cable.

RJ45 Pin	DB9F Pin
1	7
2	9
3	4
4	5
5	1
6	3
7	2
8	8

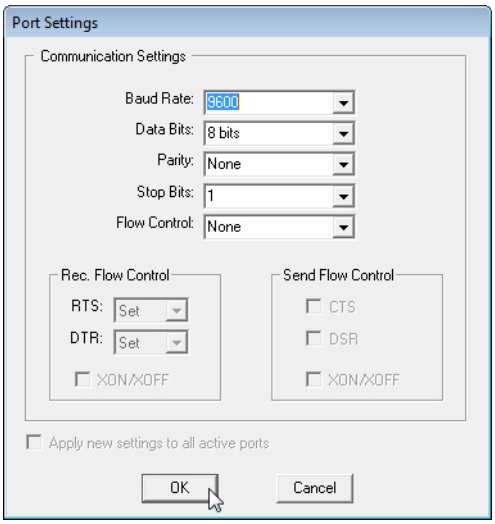


2. Start a terminal program such as HyperTerminal or the Comtrol Test Terminal program. You can download Test Terminal from the FTP site.
   - Test Terminal - WCom2 (Windows XP through Windows 8)
     - Unzip Test Terminal and place it in a location that you can execute an application.
     - Execute **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 2.3-20140127-18:03:09).


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/SSH Console

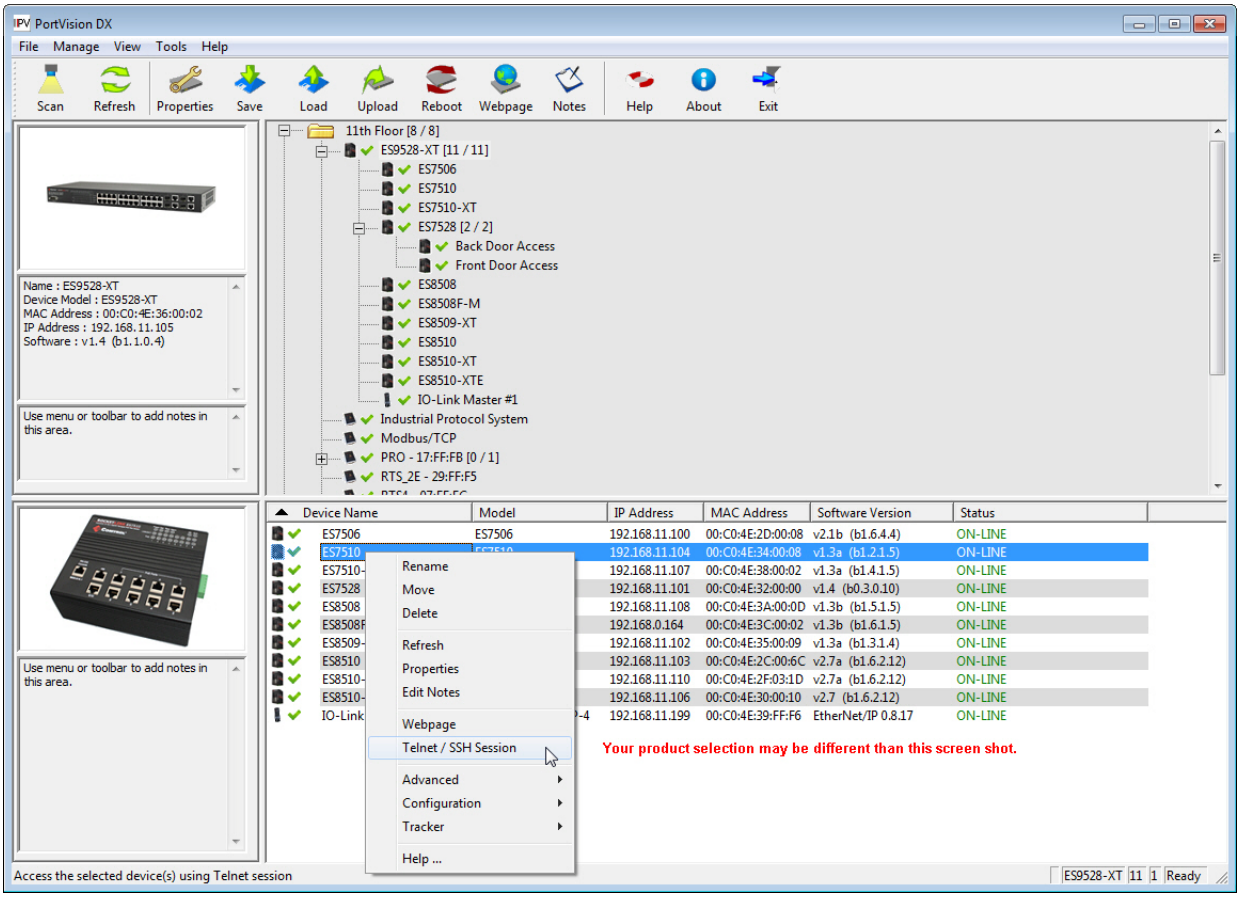
The ES7506 supports a Telnet console or SSH console with the Command Line Interface (CLI), which is the same as what you see using the RS-232 console port. The SSH connection can secure all the configuration commands you send to the ES7506.

SSH is a client/server architecture while the ES7506 is the SSH server. When you want to make SSH connection with the ES7506, you can use PortVision DX or download an SSH client tool.

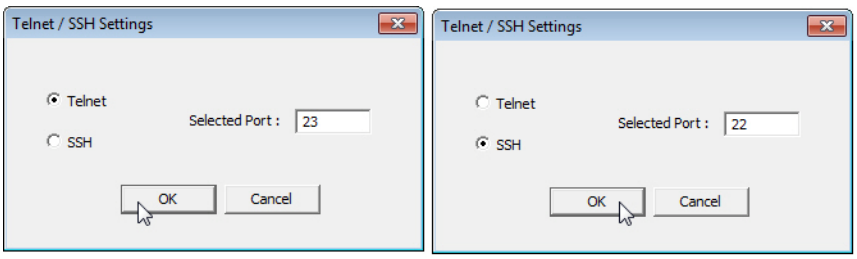
The next discussion provides procedures to use PortVision DX with a Telnet or SSH connection.

You can use PortVision DX to access the CLI using the following procedure.

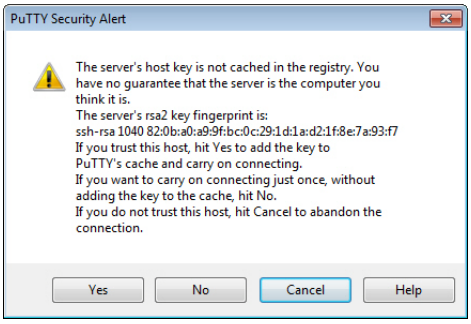
1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 15).
2. Start PortVision DX.
3. Right-click the ES7506 in the *Device List* pane (lower) and click **Telnet/SSH**.



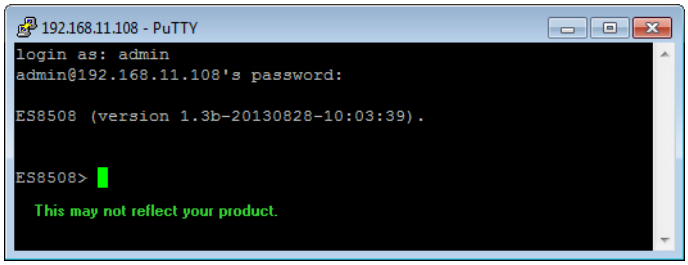
4. Select either Telnet or SSH and leave the default port number.



If you selected **SSH**, click **Yes**.

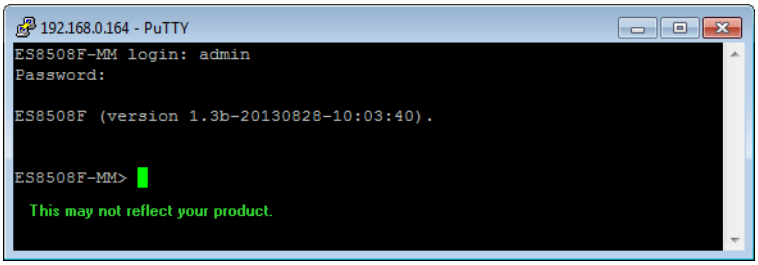


- Enter the user name (default = **admin**).
- Enter the password (default = **admin**).



If you selected **Telnet**:

- Enter the user name (default = **admin**).
- Enter the password (default = **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 ES7506 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 100, 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 102, 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 103, which you can use configure all ES7506 features and access to one of the *Interface Configuration* modes
- *(Port) Interface Configuration* on Page 104, which can be used to configure port settings
- *(VLAN) Interface Configuration* on Page 105, which can be used to configure the settings for a specific VLAN

Refer to *Configuration Using the Command Line Interface (CLI)* on Page 95 to access the CLI.

User EXEC Mode

When you login to the ES7506 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**:

```
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
```

- **enable** to access *Privileged EXEC* mode (*Privileged EXEC Mode* on Page 102).
- **exit** to logout.
- **?** to see the command list.
- **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 143.

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 ES7506 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 ES7506 provides information about the options for that command.

```
Switch> show
  arp             ARP table
  ip              IP information
  spanning-tree   Spanning-tree protocol
  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 ES7506.

```
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 192.168.0.254, sw0.1
C>* 127.0.0.0/8 is directly connected, lo
C>* 192.0.0.0/8 is directly connected, sw0.1
```

5. If you type **list** and press **Enter**, the ES7506 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.

```
ES7506> list
  enable
  exit
  list
  ping WORD
  ping ip WORD
  quit
  show arp
  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 spanning-tree statistics IFNAME
  show version
  telnet WORD
  telnet WORD PORT
  traceroute WORD
  traceroute ip WORD
```

Privileged EXEC Mode

If you type **enable** in *User EXEC* mode, you can access *Privileged EXEC* mode. In this mode, the ES7506 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 103).
- **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 144.

```
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
  end          End current mode and change to enable mode
  exit         Exit current mode and down to previous mode
  list         Print command list
  no           Negate a command or set its defaults
  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 ES7506 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 147..

```
Switch# configure terminal
Switch(config)#
  access-list         Add an access list entry
  administrator       Administrator account setting
  arp                 Set a static ARP entry
  clock               Configure time-of-day clock
  default             Set a command to its defaults
  end                 End current mode and change to enable mode
  exit                Exit current mode and down to previous mode
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  IP information
  list                Print command list
  log                 Logging control
  mac                 Global MAC configuration subcommands
  mac-address-table   Mac address table
  no                  Negate a command or set its defaults
  ntp                 Configure NTP
  password            Assign the terminal connection password
  poe                 Configure Power over Ethernet
  qos                 Quality of Service (QoS)
  redundant-ring      Configure redundant ring
  relay               relay output type information
  rmon                Remote monitoring
  router              Enable a routing process
  smtp-server         SMTP server configuration
  snmp-server         SNMP server
  spanning-tree       spanning tree algorithm
  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 fa6

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 155.

```
Switch(config)# interface fa1
Switch(config-if)#
  auto-negotiation  Enable auto-negotiation state of a given port
  description       Interface specific description
  duplex            Specify duplex mode of operation for a port
  end               End current mode and change to enable mode
  exit              Exit current mode and down to previous mode
  flowcontrol       Set flow-control value for an interface
  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
  shutdown          Shutdown the selected interface
  spanning-tree     spanning-tree protocol
  speed             Specify the speed of a Fast Ethernet port
  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, 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 156.

```
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
  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 ES7506 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
  arp             Set a static ARP entry
```

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.

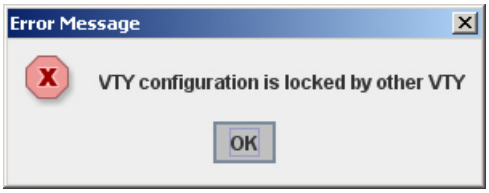
```
Switch# co (tab) (tab)
Switch# configure terminal

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 ES7506. If the administrator is in *Configuration* mode, then the web users cannot change settings. The ES7506 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 43.

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

Switch Setting	

System Name	`Switch(config)# hostname`
	`  WORD  Network name of this system`
	`Switch(config)# hostname ES7506`
	`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`
	`ES7506`
	`Switch# show snmp-server location`
	`Minnesota`
	`Switch# show snmp-server contact`
	`support@comtrol.com`
	`Switch> show version`
	`ES7506`
	`Loader Version : 1.6.4.4`
	`Firmware Version : 2.1b-20100224-22:06:36`
	`Hardware Version : 1.0`
	`CPLD Version : 1.0`
	`Switch# show hardware mac`
	`MAC Address: 00C04E2D0001`

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 192.168.250.100
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.*
Display	Switch# sh ntp associations 1 192.168.11.100 2 192.168.11.101 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

DHCP Server	
DHCP Server configuration	Enable DHCP Server on ES7506 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
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 (cont.)	
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 – Static IP and MAC binding	`Switch(config-dhcp)# ip dhcp static`
	`  MACADDR  MAC address`
	`Switch(config-dhcp)# ip dhcp static 00C0.4E2D.0001`
	`  A.B.C.D  leased IP address`
	`Switch(config-dhcp)# ip dhcp static 00C0.4E2D.0001`
	`192.168.10.99`

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 93 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 ES7506.bin Firmware upgrading, don't turn off the switch! Tftping file ES7506.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Load Default	
Load 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 58.

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`

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 – 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 fa1`
	`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.`
	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 0 is no limit
	  1024 1024 is 1024Kbps
	  128 128 is 128Kbps
	  2048 2048 is 2048Kbps
	  256 256 is 256Kbps
	  4096 4096 is 4096Kbps
	  512 512 is 512Kbps
	  8192 8192 is 8192Kbps
	Switch(config-if)# rate-limit ingress bandwidth 8192
	Set the ingress rate limit to 8192k for Port 1.

Power over Ethernet (CLI)

Power over Ethernet is one of the key features of ES7506.It supports IEEE 802.3at higher power capabilities and is in compliance with IEEE 802.3af standards. The ES7506 is equipped with power injectors on ports one through four. Each port is capable of delivering 0.651mA of current.

For more information or to use the web user interface, see *Power over Ethernet* on Page 62.

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

Syntax	**show poe status IFNAME**
Parameters	IFNAME : interface name
Command Mode	Enable mode
Description	Display the PoE status of interface.

Examples	Switch> enable
	Switch# show poe status fa1
	Interface fastethernet1
	  PoE Status
	  Powering mode : 802.3af
	  Control mode : User (Enable)
	  Status : Searching
	  Port Type : POE Port 1
	  Classification : N/A
	  PoE Usage
	  Power : 0.00 Watts, Voltage : 0.00 V, Current : 0.00 mA
	  PoE Limitation
	  Power Mode : Standard
	  Power Limit : Follow 802.3af
	  PoE Counter
	  MPS Absent Counter : 0
	  Invalid Signature Counter : 0
	  Denied Counter : 0
	  Overload Counter : 0
	  Short Counter : 0

Syntax	**show poe pd_detect**
Parameters	--
Command Mode	Enable mode
Description	Display the status of pd status detection.

Examples	Switch# show poe pd-detect
	PD Status Detection
	  Status : Enabled
	  Host 1 :
	  Target IP : 192.168.10.100
	  Cycle Time : 10
	  Host 2 :
	  Target IP : 192.168.10.200
	  Cycle Time : 20
	  Host 3 :
	  Target IP : 192.168.10.15
	  Cycle Time : 30
	  Host 4 :
	  Target IP : 192.168.10.20
	  Cycle Time : 40

Syntax	**show poe schedule IFNAME**
Parameters	IFNAME : interface name
Command Mode	Enable mode
Description	Display the status of schedule of interface.

Examples	Switch# show poe schedule fa1
	Interface fastethernet1
	  POE Schedule
	  Status : Disable
	  Weekly Schedule :
	  Sunday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23
	  Monday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23
	  Tuesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23
	  Wednesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23
	  Thursday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23
	  Friday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23
	  Saturday :
	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

Syntax	**poe powering-mode IEEE 802.3af/forced**
Parameters	802.3af: deliver power if and only if the attached PD comply with IEEE 802.3af forced: deliver power no maater what PD attached
Command Mode	Configuration mode
Description	Set the Powering mode of PoE
Examples	Set forced powering mode EX 1: Switch(config)# poe powering-mode forced Switch(config)# Set PoE port 2 to schedule mode. EX 2: Switch(config)# poe powering-mode 802.3af Switch(config)#
Syntax	**poe control-mode user/schedule**
Parameters	user: user mode schedule: schedule mode
Command Mode	Interface mode
Description	Set the control mode of port
Examples	Set PoE port 2 to user mode. EX 1: Switch(config)# interface fa2 Switch(config-if)# poe control-mode user Set PoE port 2 to schedule mode. EX 2: Switch(config-if)# poe control-mode schedule
Syntax	**poe user enable/disable**
Parameters	enable: enable port in user mode disable: disable port in user mode
Command Mode	Interface mode
Description	Enable/Disable the PoE of the port in user mode. If in schedule mode, it comes into affect when the control mode changes to user mode.
Examples	To enable the PoE function in user mode Switch(config-if)# poe user enable To disable the PoE function in user mode Switch(config-if)# poe user disable

Syntax	**poe limit power (standard|manual|ultra) [POWER]**
Parameters	Standard : Standard 802.3af mode Manual : Manual mode Ultra : Ultra mode POWER : 802.3af mode: N/A Manual mode: 0.44 - 15.4 Ultra mode: 0.44 - 30
Command Mode	Interface mode
Description	Set the mode and the max value of power consumption.
Examples	Set the mode to standard (802.3af). Ps. There is no POWER parameter in standard mode. Switch(config-if)# poe limit power standard Set the max value of power consumption to 12 W with manual mode. Switch(config-if)# poe limit power manual 12
Syntax	**poe schedule weekday hour**
Parameters	Weekday : Valid range 0-6 (0=Sunday, 1=Monday, …, 6=Saturday) Hour : Valid range 0-23, Valid format a,b,c-d
Command Mode	Interface mode
Description	Add a day schedule to an interface.
Examples	Add a schedule which enables PoE function at hour 1, 3, 5 and 10 to 23 on Sunday. Switch(config-if)# poe schedule 0 1,3,5,10-23

Network Redundancy (CLI)

It is critical for industrial applications that the network remains running at all times. The ES7506 supports:

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

  The ES7506 supports RSTP versions IEEE 802.1D-2004, IEEE 802.1D-1998 STP, and IEEE 802.1w RSTP.
- 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 ES7506 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 65.

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

RSTP	
Enable	`Switch(config)# spanning-tree enable`
Disable	`Switch(config)# spanning-tree disable`
RSTP mode	`Switch(config)# spanning-tree mode rapid-stp` `SpanningTree Mode change to be RST(802.1w).`
STP mode	`Switch(config)# spanning-tree mode stp` `Spanning-Tree Mode change to be STP(802.1d).`

Priority	`Switch(config)# spanning-tree priority`
	`  <0-61440>  valid range is 0 to 61440 in multiple of 4096`
	`Switch(config)# spanning-tree priority 4096`

Max Age	`Switch(config)# spanning-tree max-age`
	`  <6-40>  Valid range is 6~40 seconds`
	`Switch(config)# spanning-tree max-age 10`

Hello Time	`Switch(config)# spanning-tree hello-time`
	`  <1-10>  Valid range is 1~10 seconds`
	`Switch(config)# spanning-tree hello-time 2`

Forward Delay	`Switch(config)# spanning-tree forward-time`
	`  <4-30>  Valid range is 4~30 seconds`
	`Switch(config)# spanning-tree forward-time 15`

algorithm-timer	`Switch(config)# spanning-tree algorithm-timer`
	`  <4-30>  value of forward-delay`
	`Switch(config)# spanning-tree algorithm-timer 15 20 2`

Port Path Cost	`Switch(config-if)# spanning-tree pathcost`
	`  method  the pathcost is used to determine the best path between devices`
	`Switch(config)# spanning-tree pathcost method`
	`  long  specifies 32-bit based values that range from 1-200,000,000`
	`  short  specifies 16-bit based values that range from 1-65535`
	`Switch(config-if)# spanning-tree pathcost 200000`

RSTP (cont.)	

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`

bpdufilter	`Switch (config-if)# spanning-tree dpdufilter enable`
bpduguard	`Switch (config-if)# spanning-tree dpduguard enable`
Link Type - Auto	`Switch(config-if)# spanning-tree link-type auto`
Link Type - P2P	`Switch(config-if)# spanning-tree link-type point-to-point`
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`
RSTP Info	

Active status	`Switch# show spanning-tree active`
	` Rapid Spanning-Tree feature  Enabled`
	` Spanning-Tree BPDU transmission-limit  3`
	` Root Address  00c0.4e2D.0386  Priority 4096`
	` Root Path Cost : 200000  Root Port : 7`
	` Root Times :  max-age 20 sec, hello-time  2 sec, forward-delay 15 sec`
	` Bridge Address  00c0.4e2D.0102  Priority 4096`
	` Bridge Times : max-age 10 sec, hello-time  2 sec, forward-delay 15 sec`
	` Aging time : 300`
	` Port  Role  Port-State  Cost  Prio.Nbr  Type`
	`-------  ----------  ------------  ---------  ----------  -----------`
	`  fa1  Root  Forwarding  200000  128.1  P2P(RST)  N/A`
	`  fa4  Designated  Forwarding  200000  128.4  P2P(RST)  N/A`

RSTP Info (cont)

RSTP Summary

```
Switch# show spanning-tree summary
 Rapid Spanning-Tree feature      Enabled
 Spanning-Tree BPDU transmission-limit     3
 Root Address     00c0.4e2D.004f   Priority 32768
 Root Path Cost : 400000           Root Port : 6
 Root Times :   max-age 20 sec, hello-time  2 sec, forward-delay 15 sec
 Bridge Address   00c0.4e2D.0008   Priority 32768
 Bridge Times : max-age 20 sec, hello-time  2 sec, forward-delay 15 sec
 BPDU skewing detection disabled for the bridge
 Backbonefast disabled for bridge
 Topology change flag not set, detected flag not set
 Number of topology changes 313, last change occurred 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         4
  Port Link-Type Summary
  AutoDetected   PointToPoint   SharedLink   EdgePort
  ------------   ------------   ----------   --------
             6              0            0          4
```

Port Info

```
Switch# show spanning-tree port detail fa7  (Interface_ID)
Rapid Spanning-Tree feature     Enabled
 Port 128.6 as Disabled Role is in Disabled State
 Port Path Cost 200000, Port Identifier 128.6
 RSTP Port Admin Link-Type is Auto, Oper Link-Type is Point-to-Point
 RSTP Port Admin Edge-Port is Enabled, Oper Edge-Port is Edge
 Designated root has priority 32768, address 00c0.4e2D.0112
 Designated bridge has priority 32768, address 00c0.4e2D.1aec
 Designated Port ID is 128.6, Root Path Cost is 600000
 Timers : message-age 0 sec, forward-delay 0 sec
 BPDU: sent 43759 , received 4854
 TCN : sent 0 , received 0
 Forwarding-State Transmit count   12
 Message-Age Expired count
```

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`
	`  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 Port-Based (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 ES7506 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 Port Based VLAN on Page 70.

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

VLAN Port Configuration	

Displays the current port based vlan configuration for each port, which include the default PVID, the ports for forwarding, and the egress mode of the port.	`show vlan`
	`ex:`
	`Switch# sh vlan`
	`Port-based vlan mode:`
	`Port PVID EgressMode Egress Ports`
	`---- ---- ---------- ----------`
	` fa1 1 Tagged fa2-3`
	` fa2 1 Untagged fa3-4`
	` fa3 1 Untagged fa1-2,fa4-6`
	` fa4 1 Untagged fa1-3,fa5-6`
	` fa5 3 Untagged fa1-4,fa6`
	` fa6 1 Untagged fa1-5`
	`Switch#`

The ports where the frame comes in to this port are allowed to forward to.	`switchport port-based-vlan egress-ports [IFLIST]`
	`ex: port 1 can forward packet to port 2,3`
	`Switch(config-if)# switchport port-based-vlan egress-ports fa2,fa3`
	`Set port-based vlan success`

Assign default PVID for this port	`switchport trunk native vlan VID`
	`ex: assign VID 1 to port 1`
	`Switch# configure terminal`
	`Switch(config)# interface fa1`
	`Switch(config-if)# switchport trunk native vlan 1`
	`Set port default vlan id to 1 success`
	`Switch(config-if)#`

Specify when a frame that is egressing from this port should be tagged, untagged or unmodified	`switchport port-based-vlan mode (untagged|tagged|unmodified)`
	`ex: Egress packet of port 1 with tagged.`
	`Switch(config-if)# switchport port-based-vlan mode tagged`
	`Set port-based vlan mode success`

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.

ES7506 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 71. This table provides detailed information about command lines for traffic prioritization configuration

QoS Setting	

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

Queue Scheduling - WRR	`Switch(config)# qos queue-sched wrr`

Port Setting – CoS (Default Port Priority)	`Switch(config)# interface fa1`
	`Switch(config-if)# qos priority`
	`  <0-3>  Assign a priority queue`
	`Switch(config-if)# qos priority 3`
	`The priority queue is set 3 ok.`
	Note: *When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.*

Port Setting – Trust Mode- CoS Only	`Switch(config)# interface fa1`
	`Switch(config-if)# qos trust cos`
	`The port trust is set CoS only ok.`

Port Setting – Trust Mode- CoS First	`Switch(config)# interface fa1`
	`Switch(config-if)# qos trust cos-first`
	`The port trust is set CoS first ok.`

Port Setting – Trust Mode- DSCP Only	`Switch(config)# interface fa1`
	`Switch(config-if)# qos trust dscp`
	`The port trust is set DSCP only ok.`

Port Setting – Trust Mode- DSCP First	`Switch(config)# interface fa1`
	`Switch(config-if)# qos trust dscp-first`
	`The port trust is set DSCP first ok.`

Port Setting - Trust Mode - Port Based	`Switch(config)# interface fa1`
	`Switch(config-if)# qos trust port-based`
	`The port trust is set port based ok.`

QoS Setting (Continued)	

QoS Priority Mode	`Switch(config)# qos priority`
	`  cos  CoS`
	`  dscp  DSCP/TOS`
	`  port-based  Port-based`
	`Switch(config)# qos priority dscp`
	
	`Switch# show qos priority`
	`QoS Priority Mode: DSCP`

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

Display - Port Setting - Trust mode	`Switch# show qos trust`
	`QoS Port Trust Mode :`
	`Port  Trust Mode`
	`-----+------------`
	`  1  COS first`
	`  2  COS only`
	`  3  COS only`
	`  4  COS only`
	`  5  COS only`
	`  6  COS only`

CoS-Queue Mapping	

Format	`Switch(config)# qos cos-map`
	`  PRIORITY  Assign an priority (3 highest)`
	`Switch(config)# qos cos-map 1`
	`  QUEUE  Assign an queue (0-3)`
	Note: *Format: qos cos-map priority_value queue_value.*

Map CoS 0 to Queue 1	`Switch(config)# qos cos-map 0 1` `The CoS to queue mapping is set ok.`
Map CoS 1 to Queue 0	`Switch(config)# qos cos-map 1 0` `The CoS to queue mapping is set ok.`
Map CoS 2 to Queue 0	`Switch(config)# qos cos-map 2 0` `The CoS to queue mapping is set ok.`
Map CoS 3 to Queue 1	`Switch(config)# qos cos-map 3 1` `The CoS to queue mapping is set ok.`
Map CoS 4 to Queue 2	`Switch(config)# qos cos-map 4 2` `The CoS to queue mapping is set ok.`
Map CoS 5 to Queue 2	`Switch(config)# qos cos-map 5 2` `The CoS to queue mapping is set ok.`
Map CoS 6 to Queue 3	`Switch(config)# qos cos-map 6 3` `The CoS to queue mapping is set ok.`
Map CoS 7 to Queue 3	`Switch(config)# qos cos-map 7 3` `The CoS to queue mapping is set ok.`

CoS-Queue Mapping	
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
DSCP-Queue Mapping	
Format	Switch(config)# qos dscp-map <0-63> Assign an priority (63 highest) Switch(config)# qos dscp-map 0 <0-3> Assign an queue (0-3) **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 | 1 1 1 1 1 1 1 0 0 1 | 0 0 0 0 0 0 0 0 0 0 2 | 0 0 0 0 1 1 1 1 1 1 3 | 1 1 2 2 2 2 2 2 2 2 4 | 2 2 2 2 2 2 2 2 3 3 5 | 3 3 3 3 3 3 3 3 3 3 6 | 3 3 3 3

Multicast Filtering (CLI)

For multicast filtering, the ES7506 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	
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 74.

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

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 6, 1 239.255.255.250 IGMP 6,
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
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 ES7506 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 77.

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 ES7506 provides several security features for you to secure your connection.
Optionally, you can use the web user interface for configuration, see *Security* on Page 80.
This table provides information about the command lines for security configuration.

Feature	Command Line
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`

Warnings (CLI)

The ES7506 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 81.

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

Fault Relay Output	

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`
	`<1-2> power id`
	`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`
	`<1-2> 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`
	`Switch# show relay 2`
	`Relay Output Type : Super Ring`

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
	  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: fastethernet1 or gi1 Switch(config)# warning-event linkup fastethernet1 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: fa1-4

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 ES7506 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 86.

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 00c0.4e2D.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 00c0.4e2D.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`
	`00c0.4e2D.ca3b  Dynamic  1  fa1`
	`00c0.4e2D.0386  Dynamic  1  fa2`
	`00c0.4e2D.0101  Static  1  fa3`
	`00c0.4e2D.0102  Static  1  fa3`
	`00c0.4e2D.0100  Management  1`
	`***** MULTICAST MAC ADDRESS *****`
	`Vlan  Mac Address  COS  Status  Ports`
	`1  00c0.4e2D.0800  0  fa6`
	`1  00c0.4e2D.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`
	`00c0.4e2D.ca3b  Dynamic  1  fa4`
	`00c0.4e2D.0386  Dynamic  1  fa6`

Show MAC Address Table – Multicast MAC addresses	`Switch# show mac-address-table multicast`
	`Vlan  Mac Address  COS  Status  Ports`
	`1  00c0.4e2D.0800  0  fa5-6`
	`1  00c0.4e2D.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 ------------------ -------------- ------- ------------------ 00c0.4e2D.0101 Static 1 fa4 00c0.4e2D.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)
	RMON statistics counter mode is RxGood and TxGood mode.
	Interface fastethernet1 is enable disconnected, which has
	  Inbound:
	  RxGood: 0
	  Outbound:
	  TxGood: 0
	fastethernet

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.
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 ES7506 commands with the supporting options:

User EXEC Mode

For information about accessing *User EXEC* mode, see *User EXEC Mode* on Page 143.

```
Switch> list
  enable
  exit
  list
  ping WORD
  ping ip WORD
  quit
  show arp
  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 spanning-tree statistics IFNAME
  show version
  telnet WORD
  telnet WORD PORT
  traceroute WORD
  traceroute ip WORD
```

Privileged EXEC Mode

For information about accessing *Privileged EXEC* mode, see *Privileged EXEC Mode* on Page 144.

```
Switch# list
  archive download-boot /overwrite tftp IPADDRESS IMAGE
  archive download-sw /overwrite tftp IPADDRESS IMAGE
  clear event-log
  clear mac-address-table address MACADDR
  clear mac-address-table dynamic
  clear mac-address-table dynamic address MACADDR
  clear mac-address-table multicast MACADDR vlan VLANID
  clear redundant-ring statistics [0-31]
  clear rmon statistics
  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 startup-config
  debug ip dhcp (all|event)
  debug ip igmp
  debug ip igmp snooping (all|group|management|router|timer)
  debug l2 mac (all|trace|debug)
  debug proto pdu
  debug qos
  debug rate-limit
  debug redundant-ring (pdu|trace|debug|rapid-dual-homing|rstp|multi-ring|all) ID
  debug snmp
  debug spanning-tree (all|bpdu|config|events|general|root|sync|tc)
  debug vlan (all|trace|debug)
  disable
  end
  exit
  list
  no debug ip dhcp (all|event)
  no debug ip igmp
  no debug ip igmp snooping (all|group|management|router|timer)
  no debug l2 mac (all|trace|debug)
  no debug proto
  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 vlan (all|trace|debug)
  no pager
  ping WORD
  ping ip WORD
  quit
  reboot
```

Privileged EXEC Mode (continued)

```
reload default-config file
show access-lists WORD
show administrator
show arp
show clock
show clock summer-time
show clock timezone
show debugging ip dhcp
show debugging ip igmp
show debugging ip igmp snooping
show debugging snmp
show debugging spanning-tree
show deny host mac-address
show event-log
show hardware led
show hardware mac
show interface [IFNAME]
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 timers
show ip igmp version
show ip route
show ip route A.B.C.D
show ip route A.B.C.D/M
show ip route supernets-only
show ip security
show l2_interface [IFNAME]
show lldp
show lldp neighbors
show lldp statistics
show mac access-group [INTERFACE]
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 multicast
show mac-address-table multicast MACADDR vlan VLANID
show mac-address-table static
show mac-address-table static address MACADDR
show mac-address-table static interface IFNAME
```

Privileged EXEC Mode (continued)

```
show ntp associations
show poe pd-detect
show poe schedule [IFNAME]
show poe status [IFNAME]
show qos cos-map
show qos dscp-map
show qos port-priority
show qos queue-sched
show qos trust
show rate-limit egress [IFNAME]
show rate-limit ingress [IFNAME]
show redundant-ring [0-31]
show relay 1
show rmon statistics [IFNAME]
show rmon statistics counter-mode
show running-config
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 blockedports
show spanning-tree port detail IFNAME
show spanning-tree summary
show startup-config
show version
show vlan
show vlan management
show warning-event
telnet WORD
telnet WORD PORT
terminal length <0-512>
terminal no length
traceroute WORD
traceroute ip WORD
write
write file
write memory
write terminal
```

Global Configuration Mode

For information about accessing *Global Configuration* mode, see *Global Configuration Mode* on Page 147.

```
Switch(config)# list
  access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>) remark .LINE
  access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D [IFNAME]
  access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D [IFNAME]
  access-list (<1-99>|<1300-1999>) (deny|permit) any [IFNAME]
  access-list (<1-99>|<1300-1999>) (deny|permit) host A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) A.B.C.D
   A.B.C.D A.B.C.D A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) A.B.C.D
   A.B.C.D any [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) A.B.C.D
   A.B.C.D host A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any A.B.C.D
   A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any any
    [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any host
   A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host A.B.C.D
   A.B.C.D A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host A.B.C.D
   any [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host A.B.C.D
   host A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.DA.B.C.D
   A.B.C.D eq <0-65535> [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.Deq <0-
   65535> A.B.C.D A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.Deq <0-
   65535> A.B.C.D A.B.C.D eq <0-65535> [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D any eq
   <0-65535> [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq <0-
   65535> any [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq <0-
   65535> any eq <0-65535> [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq <0-
   65535> host A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq <0-
   65535> host A.B.C.D eq <0-65535> [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D host
   A.B.C.D eq <0-65535> [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any A.B.C.D A.B.C.D eq
   <0-65535> [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any any eq <0-65535>
   [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535>
   A.B.C.D A.B.C.D [IFNAME]
  access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535>
   A.B.C.D A.B.C.D eq <0-65535> [IFNAME]
```

Global Configuration Mode (continued)

```
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535> any
 [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535> any eq
 <0-65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535> host
 A.B.C.D [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535> host
 A.B.C.D eq <0-65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any host A.B.C.D eq <0-
 65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D A.B.C.D
 A.B.C.D eq <0-65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D any eq <0-
 65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> A.B.C.D A.B.C.D [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> A.B.C.D A.B.C.D eq <0-65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> any [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> any eq <0-65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> host A.B.C.D [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> host A.B.C.D eq <0-65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D host
 A.B.C.D eq <0-65535> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D A.B.C.D
 A.B.C.D <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D any <1-255>
 [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D any <1-255>
 code <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D host
 A.B.C.D <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D host
 A.B.C.D <1-255> code <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp any A.B.C.D A.B.C.D <1-255>
 [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp any A.B.C.D A.B.C.D <1-255>
 code <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp any any <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp any any <1-255> code <1-255>
 [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host A.B.C.D <1-255>
 [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host A.B.C.D <1-255>
 code <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D A.B.C.D
 A.B.C.D <1-255> [IFNAME]
```

Global Configuration Mode (continued)

```
access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D A.B.C.D
 A.B.C.D <1-255> code <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D any <1-255>
 [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D any <1-255>
 code <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D host A.B.C.D
 <1-255> [IFNAME]
access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D host A.B.C.D
 <1-255> code <1-255> [IFNAME]
administrator NAME PASSWORD
arp A.B.C.D H.H.H
clock set TIME MONTH DAY YEAR
clock summer-time (enable|disable)
clock summer-time START_TIME START_DATE END_TIME END_DATE
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 ip igmp snooping
default spanning-tree algorithm-timer
default spanning-tree forward-time
default spanning-tree hello-time
default spanning-tree max-age
default spanning-tree priority
end
exit
hostname .DWORD
interface IFNAME
interface vlan VLAN-ID
ip forwarding
ip igmp snooping
ip igmp snooping immediate-leave
ip igmp snooping last-member-query-interval TIMEVALUE
ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)
ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE) <1-255>
ip route A.B.C.D/M (A.B.C.D|INTERFACE)
ip route A.B.C.D/M (A.B.C.D|INTERFACE) <1-255>
ip security
ip security host A.B.C.D
list
lldp holdtime <10-255>
lldp run
lldp timer <5-254>
log file FILENAME
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 interface IFLIST
mac-address-table static MACADDR interface IFNAME
```

Global Configuration Mode (continued)

```
no access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>) remark
no access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>) remark .LINE
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D [IFNAME]
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D [IFNAME]
no access-list (<1-99>|<1300-1999>) (deny|permit) any [IFNAME]
no access-list (<1-99>|<1300-1999>) (deny|permit) host A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) A.B.C.D
 A.B.C.D A.B.C.D A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) A.B.C.D
 A.B.C.D any [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) A.B.C.D
 A.B.C.D host A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any A.B.C.D
 A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any any
 [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) any host
 A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host
 A.B.C.D A.B.C.D A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host
 A.B.C.D any [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (ip|tcp|udp|icmp) host
 A.B.C.D host A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D
 A.B.C.D A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq
 <0-65535> A.B.C.D A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq
 <0-65535> A.B.C.D A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq
 <0-65535> host A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D eq
 <0-65535> host A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) A.B.C.D A.B.C.D
 host A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any A.B.C.D A.B.C.D
 eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any any eq <0-65535>
 [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535>
 A.B.C.D A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535>
 A.B.C.D A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535> any
 [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535> any
 eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535>
 host A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any eq <0-65535>
 host A.B.C.D eq <0-65535> [IFNAME]
```

Global Configuration Mode (continued)

```
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) any host A.B.C.D eq
 <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D
 A.B.C.D A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D
 A.B.C.D eq <0-65535> A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D
 A.B.C.D eq <0-65535> A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D any eq
 <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> any [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> any eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> host A.B.C.D [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D eq <0-
 65535> host A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp) host A.B.C.D host
 A.B.C.D eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp)) A.B.C.D A.B.C.D eq
 <0-65535> any [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp)) A.B.C.D A.B.C.D eq
 <0-65535> any [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp|udp)) A.B.C.D A.B.C.D eq
 <0-65535> any eq <0-65535> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D A.B.C.D
 A.B.C.D <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D A.B.C.D
 A.B.C.D <1-255> code <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D any<1-
 255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D any<1-
 255> code <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D host
 A.B.C.D <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp A.B.C.D A.B.C.D host
 A.B.C.D <1-255> code <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any A.B.C.D A.B.C.D<1-
 255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any A.B.C.D A.B.C.D<1-
 255> code <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any any <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any any <1-255> code <1-
 255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host A.B.C.D <1-255>
 [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp any host A.B.C.D <1-255>
 code <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D A.B.C.D
 A.B.C.D <1-255> [IFNAME]
```

Global Configuration Mode (continued)

```
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D A.B.C.D
 A.B.C.D <1-255> code <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D any <1-255>
 [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D any <1-255>
 code <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D host A.B.C.D
 <1-255> [IFNAME]
no access-list (<100-199>|<2000-2699>) (deny|permit) icmp host A.B.C.D host A.B.C.D
 <1-255> code <1-255> [IFNAME]
no administrator
no arp A.B.C.D
no clock set
no clock summer-time
no clock timezone
no hostname [HOSTNAME]
no interface IFNAME
no interface vlan VLAN-ID
no ip forwarding
no ip igmp snooping
no ip igmp snooping immediate-leave
no ip igmp snooping last-member-query-interval
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 ip route A.B.C.D/M (A.B.C.D|INTERFACE) <1-255>
no ip security
no ip security host A.B.C.D
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 interface IFLIST
no mac-address-table static MACADDR interface IFNAME
no ntp peer (primary|secondary)
no poe pd-detect A.B.C.D
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
```

Global Configuration Mode (continued)

```
no snmp-server host A.B.C.D [VERSION]
no snmp-server location
no snmp-server name
no snmp-server user WORD WORD v3
no spanning-tree transmission-limit
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 <1-2>
no warning-event super-ring
no warning-event time-sync
no write-config (daemon|integrated)
ntp peer (enable|disable)
ntp peer (primary|secondary) IPADDRESS
password (8|) WORD
password LINE
poe pd-detect (enable|disable)
poe pd-detect A.B.C.D <10-3600>
poe powering-mode (802.3af|forced)
qos cos-map PRIORITY QUEUE
qos dscp-map PRIORITY QUEUE
qos queue-sched (wrr|sp)
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 IFTLIST
relay 1 power <1-2>
relay 1 power any
relay 1 ring
rmon statistics counter-mode (good|error-collisions)
router dhcp
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 WORD v3 auth (md5|sha) WORD
snmp-server user WORD WORD v3 noauth
snmp-server user WORD WORD v3 priv (md5|sha) WORD des WORD
spanning-tree (enable|disable)
spanning-tree algorithm-timer <4-30> <6-40> <1-10>
```

Global Configuration Mode (continued)

```
spanning-tree forward-time <4-30>
spanning-tree hello-time <1-10>
spanning-tree max-age <6-40>
spanning-tree mode (stp|rapid-stp)
spanning-tree pathcost method (long|short)
spanning-tree priority <0-61440>
spanning-tree transmission-limit <1-10>
warning-event (coldstart|warmstart)
warning-event (linkdown|linkup) [IFLIST]
warning-event authentication
warning-event fault-relay
warning-event poe-powering [IFLIST]
warning-event power <1-2>
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 155.

```
Switch(config)# interface fa1
Switch(config-if)# list
  auto-negotiation
  description .LINE
  duplex (half|full)
  end
  exit
  flowcontrol (off|on)
  list
  loopback
  mac access-group NAME in
  mdix
  no description
  no duplex
  no loopback
  no mac access-group
  no mdix
  no poe schedule <0-6>
  no qos priority
  no qos trust
  no rate-limit egress bandwidth
  no rate-limit ingress bandwidth
  no rate-limit ingress mode
  no shutdown
  no spanning-tree cost
  no spanning-tree link-type
  no spanning-tree port-priority
  no speed
  no switchport block
  no switchport port-based-vlan egress-ports
  no switchport trunk native vlan
  poe control-mode (user|schedule)
  poe limit power (standard|manual|ultra) [POWER]
  poe schedule <0-6> HOUR
  poe user (enable|disable)
  qos priority DEFAULT-PRIORITY
  qos trust (cos|dscp|cos-first|dscp-first|port-based)
  quit
  rate-limit egress bandwidth (0|128|256|512|1024|2048|4096|8192)
  rate-limit ingress bandwidth (0|128|256|512|1024|2048|4096|8192)
  rate-limit ingress mode (all|flooded-unicast|multicast|broadcast)
  shutdown
  spanning-tree bpdufilter (enable|disable)
  spanning-tree bpduguard (enable|disable)
  spanning-tree cost <0-200000000>
  spanning-tree edge-port (enable|disable)
  spanning-tree link-type (auto|point-to-point|shared)
  spanning-tree port-priority <0-240>
  speed (10|100)
  switchport block (multicast|unicast|both)
```

Port Interface Configuration Mode (continued)

```
  switchport port-based-vlan egress-ports IFLIST
  switchport port-based-vlan mode (untagged|tagged|unmodified)
  switchport trunk native vlan VLANID
```

VLAN Interface Configuration Mode

For information about accessing VLAN Interface Configuration mode, see *VLAN Interface Configuration Mode* on Page 156.

```
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 v1
  ip igmp version (1|2)
  list
  no description
  no ip address A.B.C.D/M
  no ip dhcp client
  no ip igmp
  no shutdown
  quit
  shutdown
```

Technical Support

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 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/ES7506_main.htm
Downloads	ftp://ftp.comtrol.com/html/ES8508_main.htm
Web Site	http://www.comtrol.com
Phone	763.957.6000