



Troubleshooting

This chapter provides these topics about avoiding and resolving problems related to the switch software:

- [Statistics](#), page 9-2
- [Avoiding Configuration Conflicts](#), page 9-7
- [Avoiding Autonegotiation Mismatches](#), page 9-8
- [GBIC Security and Identification](#), page 9-8
- [Troubleshooting LRE Port Configuration](#), page 9-9
- [Troubleshooting CMS Sessions](#), page 9-11
- [Determining Why a Switch Is Not Added to a Cluster](#), page 9-14
- [Copying Configuration Files to Troubleshoot Configuration Problems](#), page 9-15
- [Troubleshooting Switch Software Upgrades](#), page 9-16
- [Recovery Procedures](#), page 9-18

For additional troubleshooting information:

- See [Appendix A, “System Messages,”](#) for information about the system messages sent by the switch software.
- Refer to the switch hardware installation guide.

Statistics

This section describes the statistics you can retrieve from the switch and from connected LRE CPEs. Use the **show controllers ethernet-controller** and **show controllers lre status** privileged EXEC command to display these statistics:

- [Table 9-1](#) for switch statistics
- [Table 9-2](#) for Ethernet port statistics
- [Table 9-3](#) for LRE link statistics
- [Table 9-4](#) for CPE Ethernet link statistics

Table 9-1 Switch Statistics

Statistic Type	Explanation
Transmit Rate	The transmit rate in Mbps. It includes the transmission of bad packets and retransmission because of collisions in half-duplex operations.
Receive Rate	The receive rate in Mbps. It includes the data bytes of bad packets, discarded packets, and no-destination packets.
Transmit Bandwidth Usage	The percentage of the bandwidth usage for transmission, based on the transmit rate and actual speed.
Receive Bandwidth Usage	The percentage of the bandwidth usage for reception, based on the receive rate and actual speed.
Transmit Packet Rate	The transmit rate of well-formed packets. It includes unicast, multicast, and broadcast packets.
Receive Packet Rate	The receive rate of well-formed packets. It includes unicast, multicast, and broadcast packets.
Transmit Multicast/Broadcast Packet Rate	The transmit rate of well-formed multicast and broadcast packets. It excludes unicast packets.
Receive Multicast/Broadcast Packet Rate	The receive rate of well-formed multicast and broadcast packets. It excludes unicast packets.
Total Discarded Packets	The total number of packets discarded from both transmission and reception.
Total Packets with Errors	The total number of packets with errors from both transmission and reception.

Table 9-2 Ethernet Port Statistics

Statistic Type	Explanation
Transmit	
Unicast Packets	The total number of well-formed unicast packets sent by a port. It excludes packets sent with errors or with multicast or broadcast destination addresses.
Multicast Packets	The total number of well-formed multicast packets sent by a port. It excludes packets sent with errors or with unicast or broadcast destination addresses.
Broadcast Packets	The total number of well-formed broadcast packets sent by a port. It excludes packets sent with errors or with unicast or multicast destination addresses.
Discarded	The total number of transmit frames discarded.
Too old	The total number of transmit frames discarded because they have exceeded their age limit.
Deferred	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
Total Collision Packets	The total number of packets sent without error after having 1 to 15 collisions. It includes packets of all destination address types and excludes packets discarded because of insufficient resources or late collisions.
Excessive Collision Packets	The total number of packets that failed to be sent after 16 collisions. It includes packets of all destination address types.
Late Collision Packets	The total number of packets discarded because of late collisions detected during transmission. It includes all transmit packets that had a collision after the transmission of the packet's 64th byte. The preamble and SFD are not included in the frame's byte count.
Receive	
Unicast Packets	The total number of well-formed unicast packets received by a port. It excludes packets received with errors, with multicast or broadcast destination addresses, or with oversized or undersized packets. Also excluded are packets discarded or without a destination.
Multicast Packets	The total number of well-formed multicast packets received by a port. It excludes packets received with errors, with unicast or broadcast destination addresses, or with oversized or undersize packets. Also excluded are packets discarded or without a destination.
Broadcast Packets	The total number of well-formed broadcast packets received by a port. It excludes packets received with errors, with unicast or multicast destination addresses, or with oversized or undersize packets. Also excluded are packets discarded or without a destination.
Discarded Packets	The total number of packets discarded because of insufficient receive bandwidth or receive buffer space or because the forwarding rules stipulate that they not be forwarded.
No bandwidth	A count of frames received on this port that were discarded due to a lack of bandwidth resources in the switch forwarding engine.
No buffers	A count of frames received that were discarded due to a lack of frame buffer resources in the switch forwarding engine.

Table 9-2 Ethernet Port Statistics (continued)

Statistic Type	Explanation
No destination unicast packets	The total number of well-formed unicast frames that are discarded because the forwarding rules stipulate that they not be forwarded. This total excludes frames with errors and frames with multicast or broadcast destination address types or oversize frames and undersize frames.
No destination multicast packets	The total number of well-formed multicast frames that are discarded because the forwarding rules stipulate that they not be forwarded. This total excludes frames with errors and frames with unicast or broadcast destination address types or oversize frames and undersize frames.
No destination broadcast packets	The total number of well-formed broadcast frames that are discarded because the forwarding rules stipulate that they not be forwarded. This total excludes frames with errors and frames with unicast or broadcast destination address types or oversize frames and undersize frames.
Alignment Errors	The total number of packets received with alignment errors. It includes all the packets received with both an FCS error and a nonintegral number of bytes.
FCS Errors	The total number of packets received with FCS errors. It excludes undersized packets with FCS errors.
Collision Fragments	The total number of frames of less than 64 bytes that have an integral number of bytes and bad FCS values.
Undersize Packets	The total number of packets received of less than 64 bytes that have good FCS values.
Undersize frames	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Minimum size frames	The total number of packets received that were 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of packets received of more than 1518 bytes that have good FCS values.

Table 9-3 LRE Link Statistics

Statistic Type	Explanation
Upstream Bandwidth Usage	The percentage of the bandwidth used for upstream traffic, based on the current upstream rate and actual upstream speed of LRE link.
Downstream Bandwidth Usage	The percentage of the bandwidth used for downstream traffic, based on the current downstream rate and actual downstream speed of the LRE link.
Signal to Noise Ratio	The amount of increased received signal noise (in decibels) relative to the ambient, environment, and electromagnetic noise power level that the switch is designed to tolerate without disconnecting from the remote LRE CPE. The higher the ratio, the more resilient the link.
Upstream Reed-Solomon Errors	<p>The number of detected and corrected data errors being received on the switch LRE port. Reed-Solomon errors result from noise exceeding the noise margin. For short bursts of noise (such as motor startup or power surges), the Reed-Solomon error correction prevents the loss of Ethernet data packets.</p> <p>The LRE interface corrects the data bytes that are incorrectly received on the switch LRE port (up to a designed 8-byte limit). The residual error rate is better than the detection capability of the Ethernet cyclic redundancy check (CRC). If the error burst is larger than the correction capability of the LRE interface, the Ethernet CRC is used to determine the corrupted packets and to discard them.</p>
Downstream Reed-Solomon Errors	The number of detected and corrected data errors being received on the CPE RJ-11 wall port.

Table 9-4 CPE Ethernet Link Statistics

Counter	Description
Tx Octets	The count of octets sent from an LRE CPE Ethernet port.
Tx Drop Pkts	The count of packets dropped during transmission out an LRE CPE Ethernet port.
Tx Broadcast Pkts	The count of packets with a broadcast destination sent from LRE CPE Ethernet port.
Tx Multicast Pkts	The count of packets with a multicast destination sent from an LRE CPE Ethernet port.
Tx Unicast Pkts	The count of packets with a unicast destination sent from an LRE CPE Ethernet port.
Tx Collisions	The count of packets that could not be sent due to a single collision on the medium.
Tx Multiple Collisions	The count of packets that could not be sent due to multiple collisions on the medium.
Deferred transmits	The count of packets that could not be sent because the medium was busy
Late collisions	The count of packets that were not sent because a collision happened after 512 bit times into the transmission of the packet.
Excessive collisions	The count of packets that could not be sent due to excessive collisions.
In frame discards	The number of valid packets received that were discarded due to lack of space on an output queue.
Tx Pause Pkts	The count of 802.3X pause frames sent out by the LRE CPE Ethernet port.
Carrier sense errors	The number of times that the carrier sense condition was lost or never asserted when attempting to send a frame on the Ethernet interface of a CPE.
Rx Octets	The count of octets received by the LRE CPE Ethernet port.
Rx Undersize Pkts	The count of packets received by the LRE CPE Ethernet port, with size lesser than 64 bytes.

Table 9-4 CPE Ethernet Link Statistics (continued)

Counter	Description
Rx Pause Pkts	The count of 802.3X pause packets received by the LRE CPE Ethernet port.
Rx FCS Errors	The count of packets received with FCS errors.
Rx Alignment Errors	The count of packets received with alignment errors.
Rx Oversize Pkts	The count of packets received with size greater than 1518 bytes.
Rx Jabbers	The number of packets received by a port that are longer than 1522 bytes and have either an FCS error or an alignment error.
Rx Drop Pkts	The count of received packets that were dropped.
Rx Unicast Pkts	The count of received packets that had a unicast destination.
Rx Broadcast Pkts	The count of received packets that had a broadcast destination.
Rx Multicast Pkts	The count of received packets that had a multicast destination
Rx Good Octets	The count of received octets that had no errors.
Rx Fragments	The count of received fragments. Fragments are pieces of a packet.
Rx Excess Size Discards	The count of packets that were dropped because their size exceeded the maximum size.
Rx SA changes	The number of times the source address of good received packets has changed from the previous value.
Rx Symbol Errors	The total number of times a valid length packet was received at a port and had at least one invalid data symbol.
Rx Collisions and Runts	The total number of packets received whose size is less than 64 bytes.

Avoiding Configuration Conflicts

Certain combinations of port features conflict with one another. For example, if you define a port as the network port for a VLAN, all unknown unicast and multicast traffic is flooded to the port. You could not enable port security on the network port because a secure port limits the traffic allowed on it.

In [Table 9-5](#), *no* means that the two features are incompatible and that both should not be enabled; *yes* means that both can be enabled at the same time and will not cause an incompatibility conflict.

If you try to enable incompatible features by using CMS, CMS issues a warning message that you are configuring a setting that is incompatible with another setting, and the switch does not save the change.

Table 9-5 Conflicting Features

	ATM Port ¹	Port Group	Port Security	SPAN Port	Multi-VLAN Port	Network Port	Connect to Cluster?	Protected Port
ATM Port	N/A	No	No	No	No	No	Yes	No
Port Group	No	–	No	No	Yes	Yes ²	Yes	Yes
Port Security	No	No	–	No	No	No	Yes	Yes
SPAN Port	No ³	No	No	–	No	No	Yes	Yes
Multi-VLAN Port	No	Yes	No	No	–	Yes	Yes	Yes
Network Port	No	Yes (source-based only)	No	No	Yes	–	No ⁴	Yes
Connect to Cluster	Yes	Yes	Yes	Yes	Yes	No	–	Yes
Protected Port	No	Yes	Yes	Yes ⁵	Yes	No	Yes	–

1. Catalyst 2900 XL switches only.
2. Cannot be in a destination-based port group.
3. An Asynchronous Transfer Mode (ATM) port cannot be a monitor port but can be monitored.
4. Cannot connect cluster members to the command switch.
5. Switch Port Analyzer (SPAN) can operate only if the monitor port or the port being monitored is not a protected port.

Avoiding Autonegotiation Mismatches

The IEEE 802.3u autonegotiation protocol manages the switch settings for speed (10 Mbps or 100 Mbps) and duplex (half or full). Sometimes this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

**Note**

If a remote Fast Ethernet device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate. To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the remote device.

GBIC Security and Identification

Cisco-approved Gigabit Interface Converter (GBIC) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When a GBIC module is inserted in the switch, the switch software reads the EEPROM to check the serial number and the vendor name and ID, and to recompute the security code and CRC. The switch shuts down the interface and displays a GBIC_SECURITY error message if the GBIC serial number, the vendor name or ID, the security code, or CRC is invalid.

**Note**

If you are using a non-Cisco approved GBIC module, remove the GBIC module from the switch, and replace it with a Cisco-approved module. For the GBIC modules supported on the switch, refer to the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

After inserting a Cisco-approved GBIC module, use the **show interface** user EXEC command or the **show tech-support** privileged EXEC command to verify the port status.

Troubleshooting LRE Port Configuration

Table 9-6 lists problems you might encounter when configuring and monitoring the Long-Reach Ethernet (LRE) ports on the Catalyst 2900 LRE XL switches. For additional information about what can affect LRE connections, see the “[Environmental Considerations for LRE Links](#)” section on page 7-18.

LRE command descriptions provide additional troubleshooting information. Refer to the switch command reference.

Table 9-6 LRE Port Problems

Problem	Suspected Cause and Suggested Solution
Amber LRE port LED	<p>The switch and CPE are unable to establish an LRE link using the selected profile.</p> <ul style="list-style-type: none"> • Change to a profile with a lower data rate (for example, use LRE-5 instead of LRE-15). • Reduce the effect of stubs or bridge taps by terminating them with 300-ohm microfilters.
Excessive CRC errors on an LRE link	<ul style="list-style-type: none"> • A noisy environment (such as motors and power surges) is causing interference with the LRE link. <ul style="list-style-type: none"> – Change to a profile that has the interleaver feature enabled, such as the LRE-5, LRE-10, LRE-15, LRE-10-1, LRE-10-3, or LRE-10-5 profile. – Change to a profile with a lower data rate (for example, use LRE-5 instead of LRE-15) to increase the noise margin. • The LRE link length and quality are close to the limit of operation. <ul style="list-style-type: none"> – Change to a lower profile (for example, LRE-5 instead of LRE-15). – Reduce the effect of stubs or bridge taps by terminating them with 300-ohm microfilters.
High Reed-Solomon error count without CRC errors	<ul style="list-style-type: none"> • Interleaver is helping Reed-Solomon error correction to function correctly in a noisy environment. This situation means that the system is on the verge of generating CRC errors. <ul style="list-style-type: none"> – Change to a profile that has the interleaver feature enabled, such as the LRE-5, LRE-10, LRE-15, LRE-10-1, LRE-10-3, or LRE-10-5 profile. – Change to a profile with a lower data rate (for example, use LRE-5 instead of LRE-15) to increase the noise margin. • The LRE link length and quality are close to the limit of operation. <ul style="list-style-type: none"> – Change to a profile with a lower data rate (for example, use LRE-5 instead of LRE-15). – Reduce the effect of stubs or bridge taps by terminating them with 300-ohm microfilters.

Table 9-6 LRE Port Problems (continued)

Problem	Suspected Cause and Suggested Solution
Ethernet performance degradation due to excessive network latency	<p>Interleaver introduces extra latency to increase noise margin.</p> <ul style="list-style-type: none"> • Adjust upper-layer network protocols to allow for high latency. • Change to a profile with a higher data rate to increase link bandwidth. This decreases the noise margin. • Select a low-latency (LL) LRE profile, such as LRE-5LL, LRE-10LL, or LRE-15LL. <p>Note Use the low-latency (LL) private profiles with care. The LL profiles have the LL feature enabled and the interleaver feature turned off. The LL feature does not delay data transmission, but it makes data more susceptible to interruptions on the LRE link.</p> <p>All other profiles, public and private, have the interleaver feature enabled and the LL feature disabled. The interleaver feature provides maximum protection against small interruptions on the LRE link but delays data transmission. For more information about the LRE profiles, see the “Types of LRE Profiles” section on page 7-17.</p>
LRE link quality reduced in installations with bundled cables	<p>Cross-talk between the LRE links is causing all links to degrade. Disable unused LRE ports by using the lre shutdown interface configuration command.</p>

Troubleshooting CMS Sessions

Table 9-7 lists problems commonly encountered when using CMS.

**Note**

- If your cluster has these member switches running earlier software releases and if you have read-only access to these member switches, some configuration windows for those switches display incomplete information:
 - Catalyst 2900 XL or Catalyst 3500 XL member switches running Release 12.0(5)WC2 or earlier
 - Catalyst 2950 member switches running Release 12.0(5)WC2 or earlier
 - Catalyst 3550 member switches running Release 12.1(6)EA1 or earlier

For more information about this limitation, refer to the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

- These switches do not support read-only mode on CMS:
 - Catalyst 1900 and Catalyst 2820
 - Catalyst 2900 XL switches with 4-MB CPU DRAM

In read-only mode, these switches appear as unavailable devices and cannot be configured from CMS.

For more information about CMS access modes, see the “[Access Modes in CMS](#)” section on [page 2-33](#).

**Note**

If you have configured the Terminal Access Controller Access Control System Plus (TACACS+) or feature on the switch, you can still access the switch through CMS. For information about how inconsistent authentication configurations in switch clusters can affect access through CMS, see the “[TACACS+ and RADIUS](#)” section on [page 5-17](#).

For more troubleshooting and debugging information while using CMS, you can:

- Use the Java plug-in console to display the status and actions of CMS. To display the console, select **Start > Programs > Java Plug-in Control Panel**, and select **Java Console**.
- From CMS (**Reports > System Messages**), you can display the system messages of the Catalyst 2900 XL and Catalyst 3500 XL switches when they are in a cluster where the command switch is a Catalyst 2950 switch running Release 12.1(6)EA2 or later or Catalyst 3550 switch running Release 12.1(8)EA1 or later. The System Messages option is not available from the Catalyst 2900 XL and Catalyst 3500 XL switches. For more information about system messages, see [Appendix A, “System Messages.”](#)

Table 9-7 Common CMS Session Problems

Problem	Suspected Cause and Suggested Solution
<p>A blank screen appears when you click Cluster Management Suite from the Cisco Systems Access page.</p>	<p>A missing browser Java plug-in or incorrect settings could cause this problem.</p> <ul style="list-style-type: none"> • CMS requires a Java plug-in to function correctly. For instructions on downloading and installing the plug-in, refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm). <p>Note If your PC is connected to the Internet when you attempt to access CMS, the browser notifies you that the Java plug-in is required if the plug-in is not installed. This notification does not occur if your PC is directly connected to the switch and has no internet connection.</p> <ul style="list-style-type: none"> • If the plug-in is installed but the Java applet does not initialize, do this: <ul style="list-style-type: none"> – Select Start > Programs > Java Plug-in Control Panel. In the Proxies tab, verify that Use browser settings is checked and that no proxies are enabled. – Make sure that the port that connects the PC to the switch belongs to the same VLAN as the management VLAN. For more information about management VLANs, see the “Management VLANs” section on page 8-3.
<p>The Applet notinited message appears at the bottom of the browser window.</p>	<p>You might not have enough disk space. Each time you start CMS, the Java plug-in saves a copy of all the jar files to the disk. Delete the jar files from the location where the browser keeps the temporary files on your computer.</p> <p>Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the required Java plug-ins.</p>
<p>In an Internet Explorer browser session, you receive a message stating that the CMS page might not display correctly because your security settings prohibit running ActiveX controls.</p>	<p>A high security level prohibits ActiveX controls, which Internet Explorer uses to launch the Java plug-in, from running.</p> <ol style="list-style-type: none"> 1. Start Internet Explorer. 2. From the menu bar, select Tools > Internet Options. 3. Click the Security tab. 4. Click the indicated Zone. 5. Move the Security Level for this Zone slider from High to Medium (the default). 6. Click Custom Level and verify that the four ActiveX settings are set to prompt or enabled.
<p>Configuration changes are not always reflected in an Internet Explorer 5.0 browser session.</p>	<p>Microsoft Internet Explorer 5.0 does not automatically reflect the latest configuration changes. Make sure you click the browser Refresh button for every configuration change.</p>

Table 9-7 Common CMS Session Problems (continued)

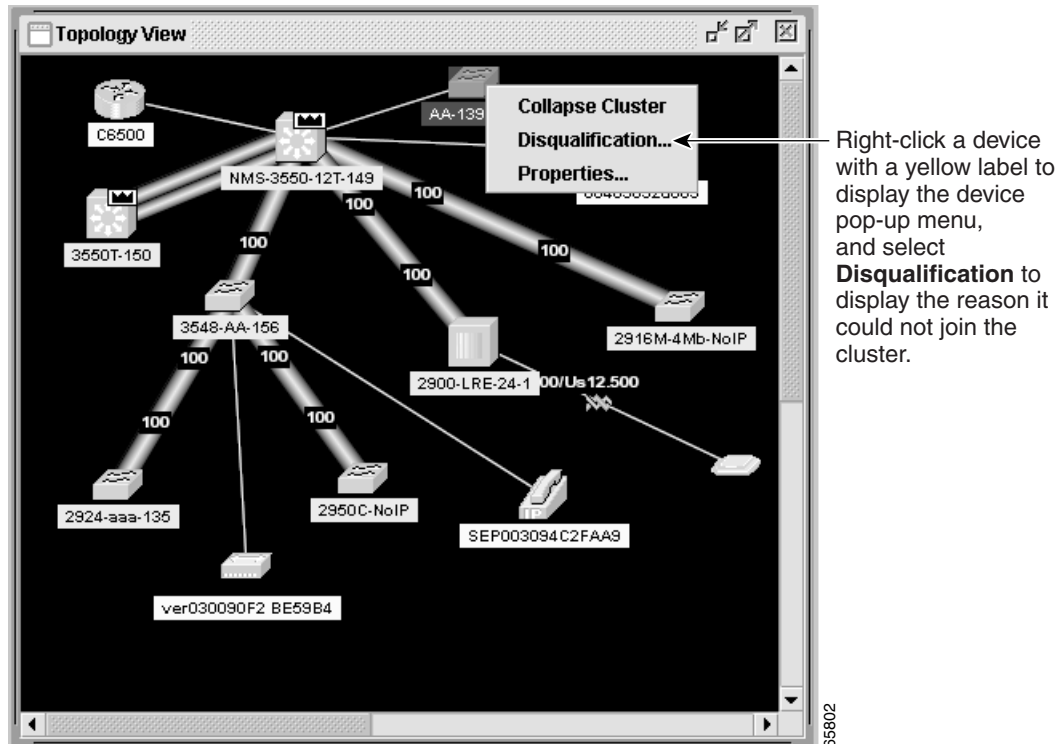
Problem	Suspected Cause and Suggested Solution
<p>Link graphs do not display information in an Internet Explorer 5.0 browser.</p> <p>(For switches running software earlier than Cisco IOS Release 12.0(5)WC1)</p>	<p>Your browser security settings could be incorrect. If your browser security settings are correct, the lower right corner of your browser screen should have a green circle with a checkmark. If it does not, follow these steps:</p> <ol style="list-style-type: none"> 1. Start Internet Explorer. 2. From the menu bar, select Tools > Internet Options. 3. From the Internet Options window, click Advanced. 4. Select the Java logging enabled and JIT compiler for virtual machine enabled check boxes, and click Apply. 5. In the Internet Options window, click General. 6. In the Temporary Internet Files section, click Settings, click Every visit to the page, and click OK. 7. In the Internet Options window, click Security, click Trusted Sites, and click Sites. 8. Deselect Require server verification. 9. Add the switches you want to manage by entering their URLs in the Add this web site to the zone field. Click Add to add each switch. A URL is the switch IP address preceded by <code>http://</code>. For example, you might enter: <code>http://172.20.153.36</code> 10. After you have finished entering the URLs for your switches, click OK. 11. While still in the Security tab of the Internet Options window, click Custom Level. 12. In the Security Settings window, select Java > Java permissions. If you do not see Java > Java permissions, you need to reinstall the browser. When you reinstall this browser, make sure to select the Install Minimal or Customize Your Browser check box. Then, from the Component Options window in the Internet Explorer 5 section, make sure to click the Microsoft Virtual Machine check box to display applets written in Java. 13. Click Custom, and click Java Custom Settings. 14. In the Trusted Sites window, click Edit Permissions. 15. Under Run Unsigned Content, click Enable, and click OK. 16. In the Security Settings window, click OK. 17. In the Internet Options window, click OK.

Determining Why a Switch Is Not Added to a Cluster

If a switch does not become part of the cluster, you can learn why by selecting **View > Topology**. Topology view displays the cluster as a double-switch icon and shows connections to devices outside the cluster (Figure 9-1). Right-click the device (yellow label), and select **Disqualification Code**.

For a list of devices that are cluster-enabled, refer to the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

Figure 9-1 Cluster View



Copying Configuration Files to Troubleshoot Configuration Problems

You can use the file system in Flash memory to copy files and to troubleshoot configuration problems. This could be useful if you wanted to save configuration files on an external server in case a switch fails. You can then copy the configuration file to a replacement switch and avoid having to reconfigure the switch.

Step 1 Enter the privileged EXEC **dir flash:** command to display the contents of Flash memory:

```
switch# dir flash:
Directory of flash:

 2  -rwx      843947   Mar 01 1993 00:02:18  C2900XL-h-mz-112.8-SA
 4  drwx       3776   Mar 01 1993 01:23:24  html
66  -rwx        130   Jan 01 1970 00:01:19  env_vars
68  -rwx       1296   Mar 01 1993 06:55:51  config.text

1728000 bytes total (456704 bytes free)
```

The file system uses a URL-based file specification. This example uses the TFTP protocol to copy the file `config.text` from the host `arno` to the switch Flash memory:

```
switch# copy tftp://arno//2900/config.text flash:config.text
```

You can enter these parameters as part of a filename:

- TFTP
- Flash
- RCP
- XMODEM

Step 2 Enter the **copy running-config startup-config** privileged EXEC command to save your configuration changes to Flash memory so that they are not lost if there is a system reload or power outage. This example shows how to use this command to save your changes:

```
switch# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration to Flash memory. After it has been saved, this message appears:

```
[OK]
switch#
```

Troubleshooting Switch Software Upgrades

Table 9-8 lists problems commonly encountered when upgrading the switch:

Table 9-8 Problems Encountered When Upgrading the Switch

Problem	Suspected Cause and Suggested Solution
Getting “Address Range” error message and boot up is failing.	<p>This error message appears when a 4-MB Catalyst 2900 XL switch is upgraded to an image that is not supported on this hardware. The switch in this case tries to load the image, but because this switch is not capable of loading this image, the bootup process fails. This also happens in cases when a 4-MB Catalyst 2900 XL switch is upgraded to an Cisco IOS 12.0 image.</p> <p>Download the IOS image file by using X-Modem.</p>
Getting “No Such File or Directory” error message during bootup.	<p>This error message appears when the names of the bootable file and the actual file in the Flash memory differ. This usually happens due to a mistyped filename when setting the boot parameters, during or after the upgrade.</p> <p>Go to Setting BOOT Parameters at ROMMON (Switch: Prompt) to verify and set the BOOT parameters correctly.</p> <p>If setting the BOOT parameters to the correct filename does not resolve the issue, perform an X-Modem upgrade, as the file in Flash memory could be corrupted or invalid.</p>
Getting “Permission Denied” error message during the bootup.	<p>This error message appears when the boot parameters are not set correctly. In most of the cases, when setting the boot parameters during or after the upgrade, the word flash: is mistyped or completely missed.</p> <p>Go to Setting BOOT Parameters at ROMMON (Switch: Prompt) to verify and set the BOOT parameters correctly.</p> <p>If setting the BOOT parameters to the correct filename does not resolve the issue, perform an X-Modem upgrade, as the file present on the Flash memory could be corrupted or invalid.</p>
Getting “Error Loading Flash” error messages.	<p>The error loading Flash message means that there is a problem loading the image in Flash memory. The image could be corrupt or incorrect, or the image in Flash memory could be missing. If the system is unable to load a software image in Flash memory, the system will load the boot helper and bring up a switch prompt.</p> <ol style="list-style-type: none"> 1. Enter the dir flash: command to verify if there is any bootable image on the Flash memory. The file with the .bin extension is the bootable image on the Flash memory. If you see a bootable image on the Flash memory, continue to Step 2. If you do not see any bootable image in the Flash memory, download the IOS image file by using X-Modem. 2. Enter the set BOOT flash: name of IOS file command to set the boot variable to the filename displayed in Step 1. <p>Note BOOT must be capitalized and make sure to include flash: before the filename.</p> <ol style="list-style-type: none"> 3. Enter the boot command. <p>Note If the switch boots properly, enter the setting boot parameters global configuration command to verify and set the BOOT parameters (if needed), and proceed to Step 4. If the switch fails to boot properly, download the IOS image file by using X-Modem. 4. After setting the BOOT parameters, reload the switch by entering the reload privileged EXEC command. The switch boots up automatically with the correct image. </p>

Table 9-8 Problems Encountered When Upgrading the Switch (continued)

Problem	Suspected Cause and Suggested Solution
Failed software upgrade; switch is resetting continuously.	<p>This might be due to a corrupt or incorrect image, or the image in Flash memory might be missing. Following these steps to recover if the switch is in a reset loop after or during the upgrade.</p> <ol style="list-style-type: none"> 1. Connect the PC to the switch console port. 2. Press the Enter key a few times. Are you seeing a <i>switch: prompt?</i> If not, go to Step 3. Otherwise, go to Step 4. 3. Disconnect the power cord. Hold down the mode button on the front of the switch, and plug the power cord back in. All LEDs above all ports are green. Continue to hold down the mode button until the light above port 1 goes out, and then release the mode button. The prompt should be <i>switch:</i>. 4. Download the IOS image file using X-Modem.
After the upgrade, the switch still boots up with the old image.	<p>This happens when either the BOOT parameters are not correct and the switch is still set to boot from the old image or the upgrade did not go through properly.</p> <p>Verify the BOOT parameters, and correct them if needed.</p> <ul style="list-style-type: none"> • If the BOOT parameters are correct, download the IOS image file using TFTP. • If the switch still boots with the old image, download the IOS image file using X-Modem.
Switch not booting automatically; needs a manual boot at the ROMMON (<i>switch: prompt</i>).	<p>The switch boot parameters might be set for manual boot. The switch can be set to boot automatically by following these steps:</p> <ol style="list-style-type: none"> 1. Use Telnet to access the switch, or connect the PC to the switch console port. 2. Enter the privileged EXEC mode by entering the enable command at the <i>switch> prompt</i>. 3. Enter the global configuration mode by entering configure terminal at the <i>Switch# prompt</i>. 4. Enter no boot manual to tell the switch to boot automatically. 5. Enter end to return to privileged EXEC mode, and save the configuration by entering the write memory command. 6. Verify the boot parameters by entering show boot. Verify that Manual Boot is set to <i>no</i>.

Recovery Procedures

The recovery procedures in this section require that you have physical access to the switch. Recovery procedures include these topics:

- [Recovering from Lost Member Connectivity, page 9-18](#)
- [Recovering from a Command Switch Failure, page 9-18](#)
- [Recovering from a Lost or Forgotten Password, page 9-24](#)
- [Recovering from Corrupted Software, page 9-26](#)

Recovering from Lost Member Connectivity

Some configurations can prevent the command switch from maintaining contact with member switches. If you are unable to maintain management contact with a member, and the member switch is forwarding packets normally, check for these port-configuration conflicts:

- Member switches cannot connect to the command switch through a port that is defined as a network port. For information on the network port feature, see the [“Enabling a Network Port” section on page 7-6](#).
- Member switches must connect to the command switch through a port that belongs to the same management VLAN. For more information, see the [“Management VLAN” section on page 5-18](#).
- Member switches connected to the command switch through a secured port can lose connectivity if the port is disabled due to a security violation. Secured ports are described in the [“Enabling Port Security” section on page 7-10](#).

Recovering from a Command Switch Failure

You can prepare for a command switch failure by assigning an IP address to a member switch that is command-capable, making a note of the command-switch password, and cabling your cluster to provide redundant connectivity between all member switches and the replacement command switch. Hot Standby Router Protocol (HSRP) is the preferred method for providing a redundant command switch to a cluster. For more information, see the [“HSRP and Standby Command Switches” section on page 5-12](#) and the [“Creating a Cluster Standby Group” section on page 5-23](#). For a list of command-capable Catalyst desktop switches, see the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

If you have not configured a standby command switch, and your command switch loses power or fails in some other way, management contact with the member switches is lost, and a new command switch must be installed. However, connectivity between switches that are still connected is not affected, and the member switches forward packets as usual. You can manage the members as standalone switches through the console port or, if they have IP addresses, through CMS Device Manager.

These sections describe how to recover if a standby command switch was not available when the command switch failed:

- [“Replacing a Failed Command Switch with a Cluster Member” section on page 9-19](#)
- [“Replacing a Failed Command Switch with Another Switch” section on page 9-21](#)
- [“Recovering from a Failed Command Switch Without Replacing the Command Switch” section on page 9-23](#)

Replacing a Failed Command Switch with a Cluster Member

Follow these steps to replace a failed command switch with a command-capable member of the same cluster:

- Step 1** Disconnect the command switch from the member switches, and physically remove it from the cluster.
- Step 2** Use a member switch in place of the failed command switch, and duplicate its connections to the cluster members.
- Step 3** Start a command-line interface (CLI) session on the new command switch.
- You can access the CLI by using the console port or, if an IP address has been assigned to the switch, by using Telnet. For details about using the console port, refer to the switch installation guide.
- Step 4** At the switch prompt, change to privileged EXEC mode:
- ```
Switch> enable
Switch#
```
- Step 5** Enter the password of the *failed command switch*.
- Step 6** From privileged EXEC mode, enter global configuration mode.
- ```
Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```
- Step 7** From global configuration mode, remove previous command-switch information from the switch.
- ```
Switch(config)# no cluster commander-address
```
- Step 8** Return to privileged EXEC mode.
- ```
Switch(config)# exit
Switch#
```
- Step 9** Use the setup program to configure the switch IP information.
- This program prompts you for an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.
- ```
Switch# setup
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use Ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:
```
- Step 10** Enter **Y** at the first prompt.
- ```
Continue with configuration dialog? [yes/no]: y
```
- Step 11** Enter the switch IP address, and press **Return**:
- ```
Enter IP address: ip_address
```
- Step 12** Enter the subnet mask, and press **Return**:
- ```
Enter IP netmask: ip_netmask
```
- Step 13** Enter **Y** at the next prompt to specify a default gateway (router):
- ```
Would you like to enter a default gateway address? [yes]: y
```

**Step 14** Enter the IP address of the default gateway, and press **Return**.

IP address of the default gateway: *ip\_address*

**Step 15** Enter a host name for the switch, and press **Return**.



**Note** On a command switch, the host name is limited to 28 characters; on a member switch to 31 characters. Do not use *-n*, where n is a number, as the last character in a host name for any switch.

Enter a host name: *host\_name*

**Step 16** Enter the password of the *failed command switch*, and press **Return**.



**Note** The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces.

Enter enable secret: *secret\_password*

**Step 17** Enter **Y** to enter a Telnet password:

Would you like to configure a Telnet password? [yes] **y**



**Note** The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

**Step 18** Enter the Telnet password, and press **Return**:

Enter Telnet password: *telnet\_password*

**Step 19** Enter **Y** to configure the switch as the cluster command switch. Enter **N** to configure it as a member switch or as a standalone switch.



**Note** If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in [Step 20](#) does not appear.

Would you like to enable as a cluster command switch? **y**

**Step 20** Assign a name to the cluster, and press **Return**.

Enter cluster name: *cls\_name*



**Note** The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

**Step 21** The initial configuration is displayed:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 1M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
```

```
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

**Step 22** Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

```
Use this configuration? [yes/no]: y
```

**Step 23** Start your browser, and enter the switch IP address that you entered in Step 11.

**Step 24** Display the CMS Home page for the switch, and select **Enabled** from the Command Switch drop-down list.

**Step 25** Click **Cluster Management Suite** to display CMS.

CMS prompts you to add candidate switches. The password of the failed command switch is still valid for the cluster, and you should enter it when candidate switches are proposed for cluster membership.

## Replacing a Failed Command Switch with Another Switch

Follow these steps when you are replacing a failed command switch with a switch that is command-capable but not part of the cluster:

**Step 1** Insert the new switch in place of the failed command switch, and duplicate its connections to the cluster members.

**Step 2** Start a CLI session on the new command switch.

You can access the CLI by using the console port or, if an IP address has been assigned to the switch, by using Telnet. For details about using the console port, refer to the switch hardware installation guide.

**Step 3** At the switch prompt, change to privileged EXEC mode:

```
Switch> enable
Switch#
```

**Step 4** Enter the password of the *failed command switch*.

**Step 5** Use the setup program to configure the switch IP information.

This program prompts you for an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.

```
Switch# setup
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].
Continue with configuration dialog? [yes/no]:
```

**Step 6** Enter **Y** at the first prompt.

```
Continue with configuration dialog? [yes/no]: y
```

**Step 7** Enter the switch IP address, and press **Return**:

Enter IP address: *ip\_address*

**Step 8** Enter the subnet mask, and press **Return**:

Enter IP netmask: *ip\_netmask*

**Step 9** Enter **Y** at the next prompt to specify a default gateway (router):

Would you like to enter a default gateway address? [yes]: **y**

**Step 10** Enter the IP address of the default gateway, and press **Return**.

IP address of the default gateway: *ip\_address*

**Step 11** Enter a host name for the switch, and press **Return**.



**Note** On a command switch, the host name is limited to 28 characters; on a member switch to 31 characters. Do not use *-n*, where *n* is a number, as the last character in a host name for any switch.

Enter a host name: *host\_name*

**Step 12** Enter the password of the *failed command switch*, and press **Return**.



**Note** The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces.

Enter enable secret: *secret\_password*

**Step 13** Enter **Y** to enter a Telnet password:

Would you like to configure a Telnet password? [yes] **y**



**Note** The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

**Step 14** Enter the Telnet password, and press **Return**:

Enter Telnet password: *telnet\_password*

**Step 15** Enter **Y** to configure the switch as the cluster command switch. Enter **N** to configure it as a member switch or as a standalone switch.



**Note** If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in [Step 20](#) does not appear.

Would you like to enable as a cluster command switch? **y**

**Step 16** Assign a name to the cluster, and press **Return**.

Enter cluster name: *cls\_name*



**Note** The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

**Step 17** The initial configuration is displayed:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 1M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

**Step 18** Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

Use this configuration? [yes/no]: **y**

**Step 19** Start your browser, and enter the switch IP address that you entered in Step 7.**Step 20** Click **Cluster Management Suite** to display CMS.

It prompts you to add the candidate switches. The password of the failed command switch is still valid for the cluster. Enter it when candidate switches are proposed for cluster membership, and click **OK**.

---

## Recovering from a Failed Command Switch Without Replacing the Command Switch

If a command switch fails and there is no standby command switch configured, member switches continue forwarding among themselves, and they can still be managed through normal standalone means. You can configure member switches through the console-port CLI, and they can be managed through SNMP, HTML, and Telnet after you assign an IP address to them.

The password you enter when you log in to the command switch gives you access to member switches. If the command switch fails and there is no standby command switch, you can use the command-switch password to recover. For more information, see the [“Recovering from a Command Switch Failure” section on page 9-18](#).

## Recovering from a Lost or Forgotten Password

Follow the steps in this procedure if you have forgotten or lost the switch password.

- Step 1** Connect a terminal or PC with terminal emulation software to the console port. For more information, refer to the switch installation guide.



**Note** You can configure your switch for Telnet by following the procedure in the [“Accessing the CLI” section on page 3-7](#).

- Step 2** Set the line speed on the emulation software to 9600 baud.

- Step 3** Unplug the switch power cord.

- Step 4** Press the **Mode** button, and at the same time, reconnect the power cord to the switch.

You can release the **Mode** button a second or two after the LED above port 1X goes off. Several lines of information about the software appear, as do instructions:

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software:

```
flash_init
load_helper
boot
```

- Step 5** Initialize the Flash file system:

```
switch: flash_init
```

- Step 6** If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

- Step 7** Load any helper files:

```
switch: load_helper
```

- Step 8** Display the contents of Flash memory:

```
switch: dir flash:
```

The switch file system is displayed:

Directory of flash:

```
 2 -rwx 843947 Mar 01 1993 00:02:18 C2900XL-h-mz-112.8-SA
 4 drwx 3776 Mar 01 1993 01:23:24 html
66 -rwx 130 Jan 01 1970 00:01:19 env_vars
68 -rwx 1296 Mar 01 1993 06:55:51 config.text
```

1728000 bytes total (456704 bytes free)

- Step 9** Rename the configuration file to config.text.old.

This file contains the password definition.

```
switch: rename flash:config.text flash:config.text.old
```

**Step 10** Boot the system:

```
switch: boot
```

You are prompted to start the setup program. Enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

**Step 11** At the switch prompt, change to privileged EXEC mode:

```
switch> enable
```

**Step 12** Rename the configuration file to its original name:

```
switch# rename flash:config.text.old flash:config.text
```

**Step 13** Copy the configuration file into memory:

```
switch# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
```

Press **Return** in response to the confirmation prompts.

The configuration file is now reloaded. Follow the next steps to change the password.

**Step 14** Enter global configuration mode:

```
switch# config terminal
```

**Step 15** Change the password:

```
switch(config)# enable secret <password>
```

or

```
switch(config)# enable password <password>
```

**Step 16** Return to privileged EXEC mode:

```
switch(config)# exit
switch#
```

**Step 17** Write the running configuration to the startup configuration file:

```
switch# copy running-config startup-config
```

The new password is now included in the startup configuration.

---

## Recovering from Corrupted Software

Switch software can be corrupted during an upgrade, by downloading the wrong file to the switch, and by deleting the image file. In all these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

This procedure uses the XMODEM Protocol to recover from a corrupt or wrong image file. There are many software packages that support the XMODEM protocol, and this procedure is largely dependent on the emulation software you are using.

- 
- Step 1** Connect a PC with terminal-emulation software supporting the XMODEM Protocol to the switch console port.
- Step 2** Set the line speed on the emulation software to 9600 baud.
- Step 3** Unplug the switch power cord.
- Step 4** Reconnect the power cord to the switch.
- The software image does not load. The switch starts in boot loader mode, which is indicated by the `switch: prompt`.
- Step 5** Use the boot loader to enter commands, and start the transfer.
- ```
switch: copy xmodem: flash:image_filename.bin
```
- Step 6** When the XMODEM request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image to Flash memory.
-