

Release Notes Cajun™ P550™ Switch - Version 4.3.7

Overview

This set of release notes supports the Cajun P550 switch for software release v4.3.7. Release notes are periodically updated with pertinent information. For detailed information about your product, refer to the basic set of user documentation. You can access the latest release notes and other documentation at:

<http://support.avaya.com>

These release notes cover the following topics:

- Important Information
- Downloading Version 4.3.7 onto the Active CPU
- Product Binaries
- Corrected Problems
- Known Problems and Workarounds
- Functional Restrictions
- New and Changed CLI Commands
- Technical Support

*** Note:** If you plan on running an ATM Uplink module with v4.3.7 on your Cajun switch, Avaya recommends that the ATM Uplink module is running a minimum version of v1.0.3 up to version v1.2.7.

Important Information

This section contains information that is crucial to know before proceeding to install or use the Cajun switches. Please review the following Cautions before continuing.



If you have a redundant supervisor configured on your switch, both supervisors must have the same software release installed on the same APP (app1 or app2).



When making configuration changes to the switch, explicitly save changes by copying the running configuration to the startup configuration to ensure that the changes persist after the switch is restarted. When running a redundant supervisor configuration, you must also synchronize the CPUs in order for both CPUs to have the same configuration.



When running a redundant supervisor configuration, if you remove a CPU and are planning to use it elsewhere in your network, then reset your MAC prefix on the old switches, copy the running config to the startup config to save changes, and reboot the switch. Repeat this procedure on the new switch, as well. This ensures no duplicate MAC addresses on the network.

*** Note:** If you are using Netscape® to view the online help, it is recommended that you use a direct connection to the Internet. To set up a Direct Connection to the Internet:

- Select **Edit > Preferences** from the Netscape menu bar.
- In the Category panel, expand **Advanced**.
- Select **Proxies**.
- Select **Direct connection to the Internet**.
- Click virtual ports.

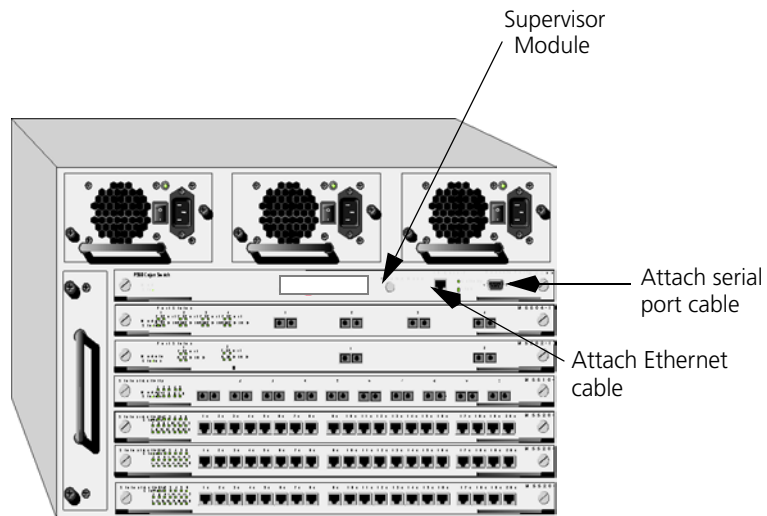
Downloading Version 4.3.7 onto the Active CPU

To download the new software onto the Active CPU:

1. **Connect** the **Ethernet console** supervisor module in **slot 1** to the network.

*** Note:** Use an Ethernet cable in the 10/100Base-T port on the supervisor module front panel (Figure 1).

Figure 1. P550 Switch Front View



2. **Login** to the switch using the CLI. Refer to the *Cajun P550/P220 Switch Operation Guide Version 4.0* for more information on logging into the switch.
3. **Configure** the Ethernet serial port by running **setup** from the CLI. Refer to the *Cajun P550 Switch Command Line Interface Reference Guide* for more information on running setup in the CLI.
4. Download Version 4.3.7 software into both APP1 and APP2 of the CPU module in slot 1.

Downloading Version 4.3.7 onto the Redundant CPU

*** Note:** You must download the v4.3.7 software code onto both CPUs. Load the software onto the Active CPU first, then repeat this procedure for the Standby CPU after you have installed it into the chassis.

1. **Connect** the **Ethernet console** supervisor module in **slot 2** to the network (Figure 1).
2. Repeat steps 2 - 4 in the "Downloading Version 4.3.7 onto the Active CPU" section to upgrade the software on the Redundant Supervisor module.

Verifying the Operation of the Redundant CPU

To verify that the Redundant CPU is operational:

1. Install both supervisor modules into their respective slots (slot 1 and slot 2), if not already installed.
2. **Ping** the internal IP network address of the standby CPU in slot 2.

```
Cajun> ping 10.2.2.2
```

*** Note:** The P550 use the 10.2.2.0 subnet as the internal network for CPU redundancy. If you are using this subnet in your operational network, use the P550 Web Agent or CLI to change the internal address to another address that is not being used.

3. Use the following command to check the status of the standby CPU and to verify that the active CPU in slot 1 is sending and receiving CPU Redundancy Health messages:

```
Cajun>show cpu_redundancy status
```

Configuring a Redundant Supervisor Using the Web Agent

The supervisor module manages the resources of the switch, provides access to these resources and supports numerous network protocols, such as Spanning Tree Protocol (STP). Access is provided to these resources via the Command Line Interface (CLI), HTTP (Web Agent), Simple Network Management Protocol (SNMP), and TELNET. These resources include:

- Configuration information
- Spanning tree topology
- Address forwarding tables
- Network statistics

* **Note:** To configure the redundant CPU using the CLI, refer to “CPU Redundancy Commands”, later in these release notes, for more information.


Complete the following steps if you want to always have access to the supervisor module in both slots 1 and 2 via their Ethernet consoles:

* **Note:** The Ethernet Console on the active supervisor is still accessible.

1. Start your browser and log on to your switch. The Web agent window appears.
2. Click **Redundancy Config** in the **System Information** section of the Web Agent window. The CPU Redundancy Configuration dialog box appears (Figure 2).

Figure 2. CPU Redundancy Configuration Dialog Box

CPU Redundancy Configuration



	Slot1 CPU	Slot2 CPU
Redundant CPU Console IP Address	<input type="text" value="192.168.33.10"/>	<input type="text" value="192.168.33.11"/>
Redundant CPU Default Gateway	<input type="text" value="192.168.33.240"/>	
Switch MAC Prefix	<input type="text" value="02:e0:3b:dd:67:ff"/>	

3. Enter the **IP addresses** for the supervisor modules in slots 1 and 2 in the **Redundant CPU Console IP Address** field. This sets the Ethernet Console IP address for both CPUs. The default IP address for both modules is **0.0.0.0**.
4. Enter the **default gateway IP address** for the standby supervisor in the **Redundant CPU Default Gateway** field. The standby supervisor's Ethernet console's IP address default gateway must be on the same subnet as the Standby Ethernet Console IP interface. It does not have to match the default gateway for the Active supervisor. By default this does not exist. The default value is **0.0.0.0**.
5. Click **APPLY** to save your changes.
6. Click **RESET SWITCH MAC PREFIX** to reset your MAC prefix setting, if needed. This resets the switch MAC prefix to the MAC address that is assigned to the active supervisor by the manufacturer. Do this when you insert or remove a supervisor module from a chassis.

*** Note:** Changing this setting could affect the operation of your system.

Product Binaries

Table 1 shows the binary files that contain embedded software release v4.3.7 for the switch.

Table 1. Product Binary Files

Type of Switch	Binary File	Boot Code
P550	m5500_v4.03.07.bin	m55boot_v302.bin

Corrected Problems

The section describes the Corrected Problems for Version 4.3.7.

- Cisco Discovery Protocol (CDP) now interoperates correctly on the Cajun switch.
- Prior to this release, if an active supervisor module that is running v4.3.6 failed over to the redundant supervisor module, the configuration of the ATM Uplink module was lost.

This no longer happens in v4.3.7.

- Prior to this release, if you changed the internal network IP address to something other than 10.2.2.1/255.255.255.224, then used this same address to create a new IP interface, the new IP address would function correctly until you rebooted the switch. After reboot, the new IP interface would come up as INVALID.

This has been fixed in this release. The new IP address is now preserved on reboot, providing you copied the running-config file to the startup-config file.

-
- Prior to this release, if the AFT was full, or close to full, you could not create a VLAN. If you attempted to create a VLAN, you would get a “PLE memory exhausted error” message.

This message has been enhanced in this release to read:

“PLE memory full. Try reducing the Hash Table size of the VLAN.”

- Prior to this release, some settings that were saved to the startup-config did not make it into the running-config after a reboot.

They are:

- Set max Event log size to 1024.
- Set max shutdown event log size to 64.

As of this release, these settings are now present in the running-config after re-boot as of this release.

- Prior to this release, the P550 switch could not save Known-mode to disable on 1/1. It allowed you to enter the Disable command but on reboot the line, “set port known-mode enable 1/1” returned.

This setting now persists after a reboot. Now the way it works is that the default case for the CPU port is Enabled but Disabled on any other port. When you boot the switch, you will not see the setting but it will be enabled on the CPU port. When you disable Known-mode on the CPU port it will show up in the running config.

- Prior to this release, the following error message sometimes displayed:

“FILE: alarm.cpp LINE: 104 Value 0x10 : Failed to register alarm resource”

The problem that caused this message to display has been corrected in this release and the message will no longer display.

-
- Prior to this release, the CERT Advisory, CA-2002-03, exposed a number of SNMP vulnerabilities that might have prevented the switch from responding. Avaya has addressed these vulnerabilities to be PDU drops by the switch that contain invalid:

- Object identifiers
- Integers
- Counters, gauges, and time ticks
- IP addresses
- Counter64
- Community strings (longer than 255 characters. This is a restriction of the switch, not SNMP).

Each time the switch drops a PDU for one of these protocol violations, the MIB-II SNMP statistic object, **snmpInAsnParseErrs**, is increased by an increment of one.

- The P550 switch web agent and CLI now allows you to enter community strings of 32 characters.



Avaya highly recommends that you set community strings to at least six (6) characters and change all community strings to something other than public (default setting). For more information on SNMP security, and preventive actions that you can take, go to:

<http://support.avaya.com/security/2002-1/index.html>

- Prior to this release, Intrusion Security Scan (ISS) software run against the P550 switch crashes within six (6) seconds and displays the following error message:

Description: Undefined Error -- FILE: malloc.c LINE: 526
Value 0x3eeb3e8 : free() - corrupted buffer

This has been fixed in this release.

-
- Prior to this release, half of the 20-port L2 10/100 cards would occasionally stop forwarding. Only half of the card is affected when this happens. The ports fail when they are in this state, however the link lights still indicate that they are linked.

When this occurs with the v4.3.7 code release, an error is logged and the module is reset so they will return to an operational state. This error message provides debug information that should be reported to Technical Support.

Known Problems and Workarounds

The following known problems and workarounds apply to the P550 switch. In some cases, the known problems are listed as statements. In others, the Known Problem is immediately followed by a viable Workaround.

CLI Configuration:

Problem	If you use the "set vlan" command with multiple ports may cause the switch to reboot.
Workaround	When using the "set vlan" command, do not commit multiple ports with a single command.

Command Line Interface (CLI)

- The "!" character is considered a comment by the Cajun P550 switch software when used as part of a CLI command.
 - If you type this character BEFORE a CLI command, the command is ignored and you are returned to the CLI prompt
 - If you type this character after a CLI command, an "Invalid Command" or "Syntax Error " error message displays.

CPU

- The Layer 2 CPU erroneously displays settings for LDAP, AppleTalk, OSPF, and RIP in the Event Configure group.

Frames Transmitted with Cyclic Redundancy Check (CRC) Errors

Problem

For certain revisions of the P550 switch 20-port module (Model M5520-100TX, module Type 9, revision level A or B) and MM5512-100TX, Revision A, a temperature sensitivity problem has been found when operating at 10 Mbps. This sensitivity results in the port transmitting frames with CRC errors. These frames, since they have CRC errors, are then dropped by the receiving station.

Workaround

The following **legacy-cli** mode command that allows you to implement a new configuration to disable the power saving mode of the Phy chip. This has the same effect as moving the port's operational temperature past the problem range. The new configuration is saved only in NVRAM:

```
Cajun> port set DisablePowerSave  
<slot>.<port> on
```

*** Note:** To enter legacy-cli mode, type `legacy-cli` at the command prompt. To return to the Enhanced CLI from legacy mode, type `exit` at the command prompt.

Hot Swap Modules

The following problems exist with no workaround:

- Hot swapping modules may cause SEEPROM and SMAC panic messages to appear in the event log. These messages are for informational purposes only and should be ignored.

When a module is inserted into the switch, traffic may be affected for up to seven seconds while the module performs its hardware diagnostics.

Intelligent Multicasting

Problem If you add a static port through a static session, then delete that port, it is still listed if you do a static session on the Web Agent. Also, you cannot re-add that same static port in the same static session in either the Web Agent or the CLI.

Workaround Delete the static session and create a new one.

Problem Intelligent Multicasting can block protocols to non-multicast routers. If you have enabled Intelligent Multicasting and configured a VLAN to one or more non-multicast routers or multicast-capable endstations, Intelligent Multicasting configures router ports where multicast-enabled routers reside. These multicast router ports are necessary to allow all multicast packets to the adjacent multicast routers. Non-multicast enabled routers are not considered router ports, and do not receive multicast traffic for which an Intelligent Multicast session was created. The problem can arise when multiple IP multicast addresses map to the same multicast MAC address, resulting in protocol packets not being sent to the adjacent non-multicast enabled routers.

Example:

The unicast routing protocol in use on all connected routers is OSPF, and all ports are on the same VLAN. An endstation joins the IP multicast group 226.128.0.5 on port 1. The MAC address for the group is 01:00:5E:00:00:05. IGMP snooping creates a session for this MAC address, with port 1 as the client port. There is a non-multicast OSPF router attached to port 2. OSPF uses the IP multicast link scoped group 224.0.0.5, which also maps to a MAC address of 01:00:5E:00:00:05. Because port 2 is not a router port, and it is not part of the 01:00:5E:00:00:05 session, the switch only passes OSPF messages out port 1. Other protocols, such as the Service Location Protocol (RFC 2608), use 224.0.1.22 and 224.0.1.35, which can be blocked by endstations joining sessions that map to the same MAC address.

Workaround Make certain that all ports connected to a router are configured as router ports to ensure that all router-to-router messages are not blocked. If other non-router protocols, such as the Server Location service, are in use, create static sessions as needed. Do not create static sessions that conflict with the protocols in use on your network. For a complete list of internet multicast addresses recognized by the IANA, refer to:

`http://www.isi.edu/in-notes/iana/assignments/multicast-addresses`

*** Note:** The default state for “Rate Limiting” on 10/100 Mbps ports is **Enable**, and multicast traffic is rate-limited (to 20%) on 10/100 Mbps ports. Multicast traffic is rate-limited unless Intelligent Multicasting is enabled. If you enable Intelligent Multicasting, the multicast traffic for which the Intelligent Multicast session was created is not subject to rate limiting unless the rate limiting state is set to **Enable (all multicast included)**. If you do not want to enable rate limiting of multicast traffic on a port, either:

- Enable Intelligent Multicasting
- Disable Rate-limiting on the port.

IP

The following Known Problem has no workaround:

- If you enter a non-numeric value for Network Address or Mask on the IP Static Route page, all of the numbers are rejected and the field converts back to 0.

IPX

Problem

802.3 IPX routed frames are sometimes padded such that they are incompatible and discarded by older IPX clients/drivers.

Workaround

Use newer client software (v2.5 or later) or use a frame format other than 802.3. Format 802.2 is recommended.

Port Mirroring

Problem

If you use port mirroring, and the piggy-back port **Frame Tag** field on the **Switch Port Configuration** dialog box is set to **Ignore** frames, traffic cannot pass through the port that you are trying to mirror.

Workaround

Verify that the port **Frame Tag** field on the **Switch Port Configuration** dialog box is set to **Use** frames.

- When you try to mirror a blocked port, the Web Agent displays the port as forwarding, but it is indeed blocked. When you remove the blocked port from being mirrored, you receive panic messages on the console. The problem does not interrupt traffic or cause any other problems in the network.
- If a standby supervisor module installed in slot 2 has become the Active supervisor (CPU) due to a failover, the web agent shows the supervisor module in slot 1 as available for mirroring during a port mirroring operation. This is incorrect. This problem does not affect traffic running in the network.
 - * **Note:** The Supervisor module should not be configured for port mirroring even if it displays as available for port mirroring.
- If a router port for intelligent multicasting is mirrored with a piggyback port, the piggyback port is listed instead of the router port.

Point-to-Point Protocol (PPP) and Telnet

- A Telnet session to the serial port via PPP may time out during attempts to transfer large files, such as executable images, to a Trivial File Transfer Protocol (TFTP) server. This does not terminate the file transfer. An in-progress TFTP file transfer ends only after the file transfer is completed.
- File transfer via TFTP over PPP links may terminate before completion, if the dial-in PC is using a TFTP server.
- A new baud rate may take effect before the current PPP connection is terminated if the **baud rate change** command is entered more than once. This results in the termination of the PPP connection. This requires re-establishment of a PPP connection.

Remote Monitoring (RMON)

- 30 minute RMON statistics always show utilization as 0 on an heavily used Gigabit Ethernet port.
- Statistics for unicast frames do not work when using multilayer (ISL) tagging.

Simple Network-Management Protocol (SNMP)

The following problems do not have workarounds:

- Cold start traps cannot be transmitted out of inband interfaces after you enable Spanning Tree.
- ipAddrTable does not display inactive interfaces (VLANs). An inactive interface occurs when there are no active ports on a VLAN.

Problem

If you remove the Public community string from the SNMP Community Management, save the running config to the startup config and then reset the switch, the Public community string is not deleted.

Workaround

Do not reset the switch after you delete any community strings.

Supervisor Module

- The display on the P550 switch stand-by supervisor module may not initialize properly. However, if it becomes the active supervisor module, the displays becomes functional and displays the proper information.
- The following error message displays in the P550 Standby Supervisor console:

```
Log entry 4 by event 2 at [date:time]: normal(0)
Description: Undefined Error -- FILE: 12ipmgr.cp
LINE: 351 Value 0[no description available]
```

Ignore this message.

Switch Ports

The following problem has no workaround:

- While switch port parameters are reflected across all ports of a hunt group, spanning tree parameters are not. If you change the spanning tree priority of the flood port of a hunt group, but that port does not come up first when bringing up the hunt group, the spanning tree priority for the groups reverts to the default.

Problem

If a switch port is moved from **Bind to Receive** to **Static**, all previously bound VLANs are not removed.

*** Note:** This is NOT a problem with the **Bind to All** setting.

Workaround

Remove VLANs manually from a port when changing a switch port connection from **Bind to Receive** to **Static**.

VLAN Issues

The following problem has no workaround:

- If the Switch Port attribute Automatic VLAN Creation is set to Enable, do not set the port VLAN attribute to Discard.

Configuring VLANs

The following problem have no workarounds:

- If you set a port's VLAN trunking mode to **Clear**, keep the VLAN Binding Type to the default value: **Static**.
- If you are using both the VLAN auto-learning feature and the Binding Type **Bind to Received** or **Bind to All**, make sure that you set the binding type before you set Auto-learn to **Enable** or else the port may not be automatically added to the VLAN.

Duplicate VLAN Error Message

The following problem has no workaround:

- You may receive an error message after you add a VLAN and refresh your browser stating that the VLAN name is already in use.

Functional Restrictions

This section provides the functional restrictions for Release 4.3.4 switch software.

Auto-Negotiation

- M5520-TX (P/N M5520-100TX) boards manufactured with a Quality Phy do not auto-negotiate with Xircom brand adapter cards. If you are having this problem, disable auto-negotiation on the affected ports, and set the port speed and duplex state manually.

Problem

You may experience difficulties with auto-negotiation between some releases of the 10/100Base-TX Module (M5510-100FX, M5520-100TX, M5510R-100FX, M5512R-100TX) and adapter cards using physical interfaces manufactured by National Semiconductor. The symptom is loss of connectivity.

Workaround

Either:

- Disable auto-negotiation
- Use a patch cable that is longer than 5 meters
- Enter the following Enhanced CLI command in **legacy mode**:

```
> port set NationalPhyMode <slot>.<port>
enable
```

The factory default for the National Phy Mode is **Enable**.

Command Line Interface (CLI)

The following CLI command is used to bind additional ports to a VLAN if trunking is enabled on that port:

*** Note:** This command is only available in the CLI and not in the Web Agent.

```
> set vlan <vlan-id> <port>
```

To set the port default VLAN for a port, use the following CLI command:

```
> set port vlan {<mod-num>|<mod-port  
range>}[...[,]{<mod-num>|<mod-port-  
range>}]<vlan-id>
```

Distance Vector Multicast Routing Protocol (DVMRP)

- The switch may lose a small number of DVMRP neighbor-to-neighbor probe messages which may cause multicast routing instability under heavy loads.

Gigabit Ports that Do Not Perform Auto-Negotiation

The 50-Series Gigabit Ethernet ports operate at 1 Gbps, full-duplex and have been widely tested for interoperability with other devices. Certain gigabit modules do not support auto-negotiation. To determine if a gigabit module supports the auto-negotiation feature, you can check the hardware revision of your gigabit module by viewing the **Name** field in the **Modules and Ports** dialog box on the **Web Agent**.

Table 2 lists the 50-Series Gigabit modules that do not support the auto-negotiation feature:

Table 2. 50-Series Gigabit Modules that do not Support Auto-Negotiation

Model Number	Hardware Revision
M5502-1000SX-F	M or earlier
M5502-1000LX-F	M or earlier
M5502-1000SLX-F	F or earlier
M5504-1000SX-F	H or earlier
M5504-1000LX-F	H or earlier
M5504-1000SLX-F	H or earlier
M5502R-1000SX-F	J or earlier
M5502R-1000LX-F	J or earlier
M5502R-1000SLX-F	H or earlier

*** Note:** If a 50-Series Gigabit module does not support the auto-negotiation feature and a device that supports auto-negotiation is connected to it, you must disable auto-negotiation to ensure proper operation.

IEEE 802.1Q Packets

Problem

When a tagged IEEE 802.1Q packet arrives on a port that is set to “bind-to-all” and the VLAN does not exist on the switch, the packet is forwarded to that ports default VLAN.

Workaround

To prevent unintended forwarding of unknown VLAN traffic to the port default VLAN, configure the port default VLAN to “discard”. However, please note that automatic VLAN creation does not work if the port default VLAN is “discard”, because the switch does not learn this VLAN.

IGMP Issues with L2 Supervisor Modules

The following IGMP issues are functional restrictions in the P550 switch code when the switch is configured with an L2 Supervisor module that is running v4.3.5 switch code and v1.0.4 ATM Uplink module code:

- One multicast group which is connected across a VLAN/ELAN to another switch when the multicast server is transmitting all traffic, is flooded to all ports within that VLAN
- When configuring a static multicast network and adding port, the ATM Uplink module cannot be added as a static port.

Media Card Support

Older versions of certain media cards restrict the number of usable slots in the switch to 13. Table 3 lists specific media cards and the minimum revision required to allow you to use up to 16 slots. Media cards not listed in Table 3 do not have a minimum revision requirement.

Table 3. Media Card Revisions that Provide 16-Slot Support

Model Number	Description	Required Revision to Support 16 Slots in a P880 Switch
M5512R-100TX	L3 12 Port 10/100	Rev J
M5510R-100FX	L3 10 Port Fiber	Rev N
M5502R-1000SX-F	L3 2 Port Gigabit Short	Rev J
M5502R-1000LX-F	L3 2 Port Gigabit Long	Rev J
M5502R-1000SLX-F	L3 2 Port Gigabit Super Long	Rev H
M5504-1000SX-F	L2 4 Port Gigabit Short	Rev H
M5504-1000LX-F	L2 4 Port Gigabit Long	Rev H
M5504-1000SLX-F	L2 4 Port Gigabit Super Long	Rev H

Hunt Groups

- Layer 2 and layer 3 modules cannot share the same Hunt group.

Link Status

- When a large number of VLANs or endstations are on a hunt group, it may take several seconds for the link status LED to change upon failure.

Loopback Tests

- Loopback tests on ports may fail when there is traffic present on the link at start-up.

Oversized Packets

- Oversized packets are not counted in itemized statistics if the packet size is between 1519 and 1548 bytes.

Redundant Controller Support

- In the event that the redundant switch controller or element fails, the switch resets itself and records an entry of the event in the event log.

Spanning Tree Protocol (STP)

- In release 4.1 and later, the STP Port Priority range has been changed. The values are now 1 to 15. If you have changed the default range in a earlier release, you should verify that the priority is within the allowed range.

When the STP mode is set to IEEE 802.1D, Bridge Port Data Units (BPDUs) are sent out ports in Clear (non-trunked) format even if the port has a trunking format (3Com, IEEE 802.1Q, or Dual-Layer) defined. To alleviate this problem, disable STP for that port.

To disable STP mode for that port:

1. Select **Modules and Ports** from the **System Configuration** group. The **Module Information** dialog box opens.
2. Select **Switch Ports** from the **Module Information** dialog box for the module for which you want to disable Spanning Tree. The **Switch Ports** dialog box opens.
3. Select the port name for that port from the **Name** column. The **Switch Port Configuration** dialog box opens.

-
4. Select **Disable** from the **Spanning Tree Mode** field pull-down menu.

*** Note:** When disabling the STP for a port, BPDUs received on that port are ignored and are not generated. The port moves directly into the forwarding state from the disabled state and does not trigger a topology detection change.

For ports that have a 3Com® trunking format, the receiving end of the trunked port attempts to interpret the clear BPDUs as trunked packets. Consequently, these BPDUs are discarded at the receiving end. For Spanning Tree to function properly with 3Com trunked ports, the Spanning Tree mode should be set to per-VLAN. In per-VLAN Spanning Tree, there is one instance of Spanning Tree for each VLAN and the BPDUs are tagged with the VLAN ID, ensuring they are interpreted correctly on the receiving end.

Although this restriction does not apply to ports that use IEEE 802.1Q or Multi-Layer trunking modes, it is still recommended that you set Spanning Tree to per-VLAN when using trunked ports. This prevents an entire link from being blocked when there is a loop in one VLAN.

If you have an ATM Uplink module installed, and there is a loop through the uplink, the ATM Uplink module does not function properly if you use IEEE802.D.

TFTP File Naming Standard for Embedded NVRAM File System

*** Note:** All NVRAM files must use an 8.3 format for file names.

- When downloading code to the NVRAM file system, use standard 8.3 file naming conventions.

TFTP Download Status Delay

- It takes a few seconds before the **Status** button on the TFTP Download screen returns accurate information.

New and Changed CLI Commands

The following sections list and describe commands that are not included in the *Cajun P550/P220 Switch Command Line Reference Guide*, Release 4.0.

*** Note:** Refer to the <http://support.avaya.com>, for the Version 4.0 release of the *Cajun P550/P220 Switch Command Line Reference Guide*.

CPU Redundancy Commands

Table 4 shows a new command set in Release 4.3.7:

Table 4. CPU Redundancy Commands

New Command	New Definition/Argument
To Enable: cpu_redundancy console slot1 <ip-addr> To Disable: no cpu_redundancy console slot1	Change the Slot 1 Ethernet console IP address. Use the no form of the command to clear the address of the Ethernet console IP address in slot 1, which returns it to its initial default value of 0.0.0.0. <ip-addr> - The IP address of the Ethernet console. Command Mode - Configuration
To Enable: cpu_redundancy internal slot1 <ip-addr> To Disable: no cpu_redundancy internal slot1	Change the internal IP address of slot 1. Use the no form of the command to reset the IP address of the slot 1 interface on the internal IP network back to its initial default value of 1.1.1.1. <ip-addr> - The internal IP address for slot 1. Command Mode - Configuration
To Enable: cpu_redundancy internal slot2 <ip-addr> To Disable: no cpu_redundancy internal slot2	Change the internal IP address of slot 2. Use the no form of the command resets the IP address of the slot 2 interface on the internal IP network back to its initial default value of 1.1.1.2. <ip-addr> - The internal IP address for slot 2. Command Mode - Configuration

Table 4. CPU Redundancy Commands *continued*

New Command	New Definition/Argument
To Enable: cpu_redundancy internal mask <mask> To Disable: no cpu_redundancy internal mask	Change the internal IP mask. Use the no form of the command to reset the IP mask of the internal IP network back to its initial default value of 255.255.255.252 . <mask> : The mask for the associated IP subnet. Command Mode: Configuration
To Enable: cpu_redundancy synchronize To Disable: N/A	Synchronize the standby supervisor with the active supervisor's operational images and configuration. Command Mode: Privileged
To Enable: cpu_redundancy mac prefix reset	Resets the MAC address of the switch to its manufacturer default MAC address value.
To View: show cpu_redundancy {config status}	Display the status of CPU redundancy. <ul style="list-style-type: none"> • config - Displays the CPU redundancy configuration information. • status - Displays the CPU redundancy status information. Command Mode: User

System Commands

Table 5 shows how previous system commands were updated:

Table 5. Updated System Commands

Old Command	New Command	New Definition/ Argument
copy tftp bootflash <image_opt_path> <ip-addr>	copy tftp bootflash <image_opt_path><tftp- server>	<tftp-server> The IP address of the TFTP server.
copy tftp flash {app1 app2} <image_opt_path> <ip-addr>	copy tftp flash {app1 app2} <image_opt_path> <tftp- server>	<tftp-server> The IP address of the TFTP server.
copy tftp running- config <filename_opt_path > <ip-addr>	copy tftp running-config <filename_opt_path> <tftp- server>	<tftp-server> The IP address of the TFTP server.
copy <filename_opt_path > tftp <ip-addr>	copy <filename_opt_path> tftp <tftp-server>	<tftp-server> The IP address of the TFTP server.
copy running-config tftp <filename_opt_path > <ip-addr>	copy running-config tftp <filename_opt_path> <tftp- server>	<tftp-server> The IP address of the TFTP server.
copy startup-config tftp <filename_opt_path > <ip-addr>	copy startup-config tftp <filename_opt_path> <tftp- server>	<tftp-server> The IP address of the TFTP server.
copy tftp <filename_opt_path > <ip-addr>	copy tftp <filename_opt_path> <tftp- server>	<tftp-server> The IP address of the TFTP server.
copy tftp startup- config <filename_opt_path > <ip-addr>	copy tftp startup-config <filename_opt_path> <tftp- server>	<tftp-server> The IP address of the TFTP server.

Technical Support

To contact Avaya's technical support:

*** Note:** These are new phone numbers as of October 1, 2000.

- From the United States:

1-800-237-0016

- From North America:

1-800-242-2121

- Outside North America:

Contact your distributor