SuperStack® 3 Switch 3870 Family
Software Version 3.00 Release Notes

Related Documentation

Please use these notes in conjunction with the following documents:

- "*SuperStack 3 Switch 3870 Family Getting Started Guide*"
  Part number: DUA174509-1AAA01
  (supplied with your Switch and in PDF on the 3Com Web site)
- "*SuperStack 3 Switch 3870 Family Implementation Guide*"
  Part number: DUA174509-1BAA01
  (supplied in PDF on the CD-ROM that accompanies your Switch and on the 3Com Web site)
- "*SuperStack 3 Switch 3870 Family Management Quick Reference Guide*"
  Part number: DQA174509-1AAA01
  (supplied with your Switch and in PDF on the 3Com Web site)
- "*SuperStack 3 Switch 3870 Family Management Interface Reference Guide*"
  Part number: DHA174509-1AAA01
  (supplied in HTML format on the CD-ROM that accompanies your Switch and on the 3Com Web site)

You can obtain the latest technical information for your Switch, including a list of known problems and solutions, from the 3Com Knowledgebase:

`http://knowledgebase.3com.com`

Software License Agreement

Before you use the Switch software, please ensure that you read the license agreement text. You can find the license.txt file on the CD-ROM that accompanies your product, or in the self-extracting exe that you have downloaded from the 3Com Web site.

About this Software Version

The software supports the following products:

- Switch 3870-24 (3CR17450-91)
- Switch 3870-48 (3CR17451-91)

The software does not operate on any other 3Com Switch.

The software is available in two versions:

- s3h3_00s56 — Provides normal levels of encryption with keys of up to 56 bits in length.
- s3h3_00s168 — Provides higher levels of encryption including 168-bit 3DES and 256-bit AES.

The Switch ships with software providing normal levels of encryption.

Documentation Errors and Omissions

The following errors and omissions have been identified in the *SuperStack 3 Switch 3870 Family Getting Started Guide*, part number DUA174509-1AAA01.

- 3Com Network Supervisor is not included on the CD-ROM that accompanies your Switch. You can download an evaluation copy of 3Com Network Supervisor from www.3com.com/3ns.
- The Switch currently provides only two user access levels – monitor and admin. The second user access level (manager) that is documented in the *SuperStack 3 Switch Family Getting Started Guide* (part number DUA174509-1AAA01) and *Implementation Guide* (part number DUA174509-1BAA01) is not provided in this release.

Fixes for Known Faults

The following fixes apply to version 3.00.

- In RADA, permanent MAC addresses were displayed in the Web interface as "secure." This has been solved by not allowing permanent MAC addresses to be set with port security mode.
- When using the bridge/spanningTree/mstConfiguration/summary command, and there are a lot of VLANs in an instance, the text is no longer misaligned.
- When using MSTP, port cost and port priority are no longer lost after rebooting or using TFTP backup and restore.
- Port security and the mirror destination for roving analysis can no longer be configured on the same port.
- If you disable Spanning Tree and have loops in a stack or a network, the device will no longer spontaneously re-topologize or reboot.
- If a large number of addresses have been learned on an aggregated link (for example, 1000 or more), it no longer takes over a minute for the addresses to appear when the **`bridge address summary ALx`** command is issued on the CLI or the Web interface.
- If the Switch is configured with a large number of VLAN members, the system will no longer crash, and the VLANs are now restored after rebooting.

Updating the Switch Software

Software Updates are the bug fix and maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com Web site at:

`http://eSupport.3com.com/`

First time users will need to apply for a user name and password. A link to software downloads can be found from this **`http://eSupport.3com.com/`** page, or located from the **`www.3Com.com`** home page.

To update the software on the Switch, do the following:

1. Locate the software update for the Switch and run the (`filename.exe`) executable file.
2. If necessary, download the TFTP server applications into the management station.
3. Install the TFTP server (file name `3ts01_04.exe`) on a Microsoft Windows 95, 98, NT, 2000 or XP machine.
4. Launch the TFTP server application.
5. Point the Upload/Download default directory on the TFTP server to the directory where the upgrade file is located.
6. Make sure the Switch being upgraded has an IP address assigned to it.
7. Telnet to the Switch.
   a. To Telnet to the Switch, click *Start* in Microsoft Windows 95, 98, NT, 2000, or XP machine.
   b. Click *Run*.
   c. In the text area, type **`telnet IP address`**
   d. Click *OK*.
8. Press *Enter* to receive a login prompt.
9. Log into the Switch management.
   a. The default user login is **`admin`**.
   b. There is no default password for admin (press *Enter*).
10. From the main menu, select *System*, then select *Control*.
11. Select *SoftwareUpgrade*.
12. Enter the IP address of the TFTP server connected to the Switch.
13. Enter the upgrade file name.
    a. The message will appear, '`Software Upgrade in progress.....`'.
    b. The entire time the upgrade is in process, the Power/Self test LED will flash ON/OFF Green, and a series of dots will indicate that the upgrade is progressing successfully.
    c. When the software upgrade is complete, the Switch will reboot itself.

TFTP Upgrades

If you start a TFTP upgrade using the CLI or a Web browser, the Switch will report the status of any unit or module it has failed to upgrade to the console interface. If you upgrade a stack using the Web, or connect to the CLI using Telnet, and your computer is directly connected to a port on the stack, the connection will break when the stack completes its upgrade and restarts. If the system detects that the code version on any unit or expansion module is not consistent when you log into the Web or CLI, it will display a message indicating that the code versions are inconsistent and should be upgraded.

The Software Upgrade feature will not automatically re-establish connection to the 3Com TFTP server if the connection is lost temporarily for more than 15 seconds. In these circumstances the TFTP connection will timeout approximately 30 seconds before the upgrade can be restarted manually.

Points to Note When Upgrading Software

- When initiating a TFTP upgrade using the Web interface or CLI, if an incorrect TFTP server IP address or software upgrade filename is entered you will not be able to correct the IP address or filename until the TFTP upgrade operation has timed out. The default time out period is 30 seconds.
- When attempting to upgrade the software on the unit it may occasionally report the following error:

  ```
  Warning: Please wait for Configuration
  Synchronization to complete, and then
  re-enter the command.
  ```

  If you encounter this error, please wait a minute and try the command again.

Points to Note When Using the Switch 3870

Link Aggregation

The Switch only supports link aggregation for ports with the same speed. Since there can only be one aggregated link between two devices, aggregated links with higher port capability will replace the position of aggregated link with lower port capability.

Configuring Link Aggregations

When creating a manual aggregation between two systems the ports in the aggregation must not be physically connected together until the aggregation has been correctly configured at both ends of the link. Failure to configure the aggregation at both ends before physically connecting the ports can result in a number of serious network issues such as lost packets and network loops.

3Com recommends that you set individual ports that are to be members of an aggregated link to the same VLAN membership. This ensures communication between all VLANs at all times.

Link Aggregation and Gigabit Ports

- When manually configuring an aggregated link, the Switch may report the following error message:

  ```
  No more ports may be added to aggregated link.
  ```

  You should check the configuration of the following items on the physical port:

  - Port security is disabled on the port.
  - The VLAN membership of the port matches that of the aggregated link
  - LACP is disabled.
  - No ACL is bound to the port.

- If you want the ports to automatically form a trunk using LACP, then the ports must first be removed from the manual aggregation.
- If a trunk is disabled by using the **`bridge linkAggregation modify linkState`** CLI command then the physical trunk member ports for the aggregation will be disabled. A side effect of the ports being disabled is that they will no longer negotiate to become LACP-trunk members. If the trunk was formed by LACP, then the trunk will disappear because it no longer has any member ports.

  If the LACP trunk is disabled as above, then attempting to enable the trunk with the **`linkState`** command will respond with an error that the trunk can not be configured. In order to form the LACP trunk you must manually re-enable the individual trunk member ports using the **`physicalInterface ethernet portState`** CLI command.

LACP Protocol

CAUTION: *The LACP protocol is disabled by default. Some legacy devices do not support LACP and 3Com strongly recommends LACP remains disabled on ports connected to these devices (in rare cases, if LACP is enabled on ports connected to these devices, it can result in incorrect network configurations).*

Multicast Filtering

Unknown Multicast data packet will be flooded during the initial learning stage as the Switch processes these packets. Flooding duration is approximately 1 second for 100 Multicast groups. Flooding will stop once learning is completed.

IGMP

Disabling IGMP when there are hosts subscribing to multicast IP streams may prevent clients from subscribing to multicast IP groups. Hosts may be unable to re-subscribe to the same multicast IP group for more than 5 minutes, or until the unit is re-booted.

Password Recovery

The password recovery feature allows you to reset the admin user password by logging into the unit via the console port using the username **`recover`** and password **`recover`**. If you power cycle the unit

within 30 seconds then the password will be reset and you will be prompted to enter a new password on restart. There is no command to disable the password recovery feature.

Telnet and HyperTerminal

Accessing the Command Line Interface via Telnet or Windows HyperTerminal using TCP/IP may not work correctly on some platforms unless it has been configured to send line feeds with carriage returns. To set this for Telnet enter **`set crlf`** when in command mode. To set this for HyperTerminal click on the *Settings* tab in the *Properties* screen, click *ASCII Setup* and ensure that *Send line ends with line feeds* is checked within the *ASCII Sending* section.

You should not configure HyperTerminal in the above way if you are using a console cable to make a direct connection to the Switch.

Accessing the Command Line Interface is not possible using the default Telnet program supplied with Windows XP. Use another Telnet program, such as Hyperterminal. See the 3Com Knowledgebase for updates and a solution, when available:

`http://knowledgebase.3com.com`

Port Security and Authentication

- If the address of a device is added as a static secure address on one port and then it is subsequently moved to a different port with security disabled then the device may get intermittent network connectivity. To fix this problem you should remove the address from the original port and consider enabling security on the new port.
- The Switch does not log authentication requests or support logging to a RADIUS accounting server. Please use the logs generated on your RADIUS authentication server instead.
- To create a user with administrator privileges when using RADIUS device authentication you must ensure that user has the "Service-Type" attribute set to "Administrative" as specified in RFC 2865.
- Some RADIUS servers will not authenticate users with a blank password, all user accounts should have a valid password configured.

IP Configuration and Routing

- When the unit is in the default IP mode of *auto* it will attempt to contact a DHCP server on the network to obtain an IP address. If there is no DHCP server available on the network then the unit will not be accessible using TCP/IP.
- Reconfiguring an IP interface may cause the RIP configuration and static routes settings for that interface to be lost.
- If the number of multicast traffic groups on your network exceeds the maximum supported by the Switch (255), then you may see occasional bursts of multicast traffic as the Switch updates its internal configuration.
- Some combinations of IP commands in a multinetted environment may cause the IP address of interface 1 to become a secondary address. Rebooting the unit will reset this interface as the

primary address. There is no other means of clearing this condition.

Access Control Lists

Although multiple rules can be added to an Access Control List (ACL), only a single ACL can be assigned to an individual port.

When trying to bind an Access Control List (ACL) to a port you may see the following error generated:

```
Failed to bind port 26 ACL
```

This error will appear if:

- The ACL which is being bound has more rules than can be accommodated by the hardware.

The Switch supports ACLs based on IP addresses and port ranges rather than VLAN IDs. To set up ACLs to restrict routing between VLANs, each VLAN should comprise a clearly defined subnet.

ACLs should not be used on inter-switch links as they may interfere with routing messages required for normal network operation.

Traffic Prioritization

- The IP Port traffic prioritization only examines the destination port number field of TCP and UDP frames when determining the priority of the packet. This may result in the request and response frames being prioritized differently as they traverse the network.
- The Switch prioritizes traffic internally but does not mark or remark packets other than NBX packets. NBX traffic is remarked to DSCP 46 and 802.1d priority 6.

VLAN Configuration

- Every port on the unit must be an untagged member of a single VLAN. Every port defaults to being an untagged member of VLAN1. If you add the port as an untagged member of another VLAN then this will replace the VLAN1 membership. If the port is an untagged member of a VLAN other than 1, then removing membership of this VLAN will cause the port to return to being an untagged member of VLAN1.
- A port may be removed from VLAN 1 as an untagged member using the CLI. To avoid disrupting network traffic, the VLAN should be re-assigned to another VLAN as an untagged member.
- VLAN IDs from 4090 to 4094 inclusive are reserved for internal usage. Therefore, when creating VLANs, you will be limited to VLAN IDs in the range 2 to 4089.

Management via SNMP/MIBs

- Items configured using SNMP/MIB that do not have corresponding CLI commands will be lost when the unit is power cycled. 3Com recommends that the CLI and Web interfaces are used to configure the unit instead.

- The counters for the *etherStatsPkts(64~1518)* MIB item count traffic which is sent and received by the unit. This does not conform to the MIB which states that it should count only received packets. This occurs because an RMON probe is a passive device which monitors all traffic passing through the Switch, port-by-port, and does not distinguish between packets that are "received" and "sent".
- Small variations in the sampling of traffic statistics may cause the unit to incorrectly measure the traffic rates used for RMON alarms. To minimize the generation of incorrect alarms 3Com recommends that they are configured with a minimum sampling period of 10 seconds and a minimum hysteresis of 20%.

SSH Management

- The SSH server in the unit will reject all connection requests unless the unit has a SSH host key. This host key may be generated using the *Security* > *Device* > *SSH* > *Server Auth* > *Key Gen* command on the Web interface. You may wish to keep a record of the host key to allow you to confirm the identity of the Switch when connecting remotely using SSH.
- If the unit reboots while using SSH, you may have to manually restart your SSH client to reconnect once the unit has restarted.
- The Switch does not support SSHv2 RSA public keys. If you try to download a SSHv2 RSA public key to the Switch the error message `Key File Download failed` will be displayed.
- The default authentication method is to authenticate first using the public key and then to prompt for a password if the public key fails. There is no command to select either public key nor password authentication by itself.
- The prompt to download a public key displays the users "admin,monitor,…". Press "?" to display all the users who can download a key.

HTTPS Management

- The secure Web server on the unit is supplied with a default certificate which will fail the browsers security checks and an error message like the following will be generated:

  ```
  The name on the security certificate is
  invalid or does not match the name of the
  site.
  ```

  It is not possible for 3Com to ship a certificate with the unit that will satisfy these security checks. The browser will normally allow you to accept the connection regardless. All of the data which is sent between the browser and the unit will be securely encrypted. You may upload your own valid certificate to the Switch if you want to avoid these warnings. The software to generate these certificates is beyond the scope of this document.
- The presence of both a secure (HTTPS) and insecure (HTTP) Web interface on a single unit causes some browsers to incorrectly report the following warning message:

  ```
  This page contains both secure and insecure
  items. Do you wish to proceed?
  ```

This warning message may be safely ignored. All traffic to and from the unit using the HTTPS interface is encrypted. Alternatively you may try clearing the Web cache or upgrading your browser to the latest version.

SNMP Management

- Only one notification per target destination IP address can be created by either SNMPv1 trap or SNMPv3 trap / notification.
- SNMPv1/v2 traps and v3 traps and informs are counted together, for a maximum of 5.
- You cannot use the SNMPv3 MIB to clone users or change their properties, or change the properties of a notification. This prevents SNMP from setting the device into a state which is not recognized by the CLI and Web.
- The Switch does not provide a command to disable SNMPv1 and SNMPv2. In order to operate under a secured SNMPv3 environment, the default SNMPv1 and SNMPv2 community string should be changed to something random and complex to avoid intrusion.
- In order to gain access to the MIB at the user access level of "security", the user must be an authenticated security user. Note that SNMP users with an access level set to "noAuthNoPriv" will have no access to the Switch.
- The Switch currently works with version 7 of MG-Soft Application for SNMPv3. Versions other than 7 are not supported.

Saving Configuration

When making configuration changes to the Switch, do not reboot or turn off the unit for at least 10 seconds after the last configuration change. If the unit is rebooted or switched off before the 10 seconds is complete, the configuration changes may be lost.

Device Backup and Restore

- When the unit backs up the configuration file, a number of security sensitive settings such as the user accounts, RADIUS shared secret, and community strings are not backed up. The comments in the configuration file indicate that these commands may be manually appended to the end of the file. Contrary to these instructions, 3Com recommends that you restore the un-edited configuration file and manually reconfigure the security parameters using the CLI or Web interface.
- In some scenarios, backing up the configuration on one unit and restoring it on another will cause the default gateway setting to be lost. You should always check the IP address and route configuration when restoring the configuration on another unit.
- The Switch allows you to back up and restore configuration settings, even across different models. However, there are some limitations when backing up settings from one model and restoring them on another. For example, if you back up settings from a Switch 3870-48 and restore them to a Switch 3870-24, only system-wide settings (for example, system name) will be restored

successfully. Port-related settings (for example, port spanning tree settings) will not be restored and the system will not display a warning message.

Spanning Tree

- When connecting switches together, 3Com recommends that spanning tree fast start (also called admin edge port) should be disabled on the interconnecting ports (it is enabled by default on all ports). This can be done using the *Physical Interface* > *Ethernet* > *Setup* command on the Web interface or the **`bridge port stpFastStart`** command on the CLI.
- You must enable spanning tree before making changes to spanning tree settings. If you try to change spanning tree settings while the protocol is disabled the following error messages will be generated:

```
Failed to set forward-time
Failed to set hello-time
```

- When you enable spanning tree, not all previous settings are retained. If you want to use custom settings for spanning tree, you must configure spanning tree after enabling it.

Multiple Spanning Tree

- You must set the **`stpState`** to "enable" and configure **`stpVersion`** to *MSTP* in order to configure the Multiple Spanning Tree Protocol (MSTP) successfully.
- If you change the **`stpVersion`** to a value other than *MSTP*, some MSTP parameters will be reset to their default values.
- If you reboot the Switch while the **`stpVersion`** is set to a value other than *MSTP*, all MSTP configuration will be lost.

Roving Analysis Port

- When the roving analysis port feature is activated the analyzer should see a copy of all packets sent and received by the source mirror port. The Switch does not mirror frames sent by the management CPU of the Switch itself. The analyzer port will therefore be unable to show management traffic from the unit's CPU or protocol control packets such as RIP passing out the source mirror port.
- While the analyzer port is active, it still operates as a normal network port, allowing traffic to be switched to and from other network ports. You must be careful to differentiate traffic seen by the analyzer which is from the mirror port and other network traffic which may be being sent through the analyzer port.
- The traffic sent out of the analyzer port follows the VLAN membership setup for the analyzer port and not the mirror port. You must manually reconfigure the VLAN membership of the analyzer port to match the mirror port, or you will not see the correct tagged / untagged packets on the analyzer.

Start-up Time

The unit will take approximately 2 minutes to become fully operational. The unit is fully operational when the Self Test LED is lit solid green.

Autonegotiation of Port Speed and Duplex

- All ports on the unit default to using autonegotiation to determine the correct speed and duplex setting. If the link partner also supports autonegotiation then this will result in the optimum link speed and duplex.

  The speed and duplex of the port may be manually set by using the **`physicalInterface ethernet portMode`** command to disable autonegotiation and select a fixed speed and duplex.

- When connected to a device that will not autonegotiate, the device follows the algorithm required by the autonegotiation standard which states that ports must detect the link speed and then operate in half duplex mode.

Auto-MDIX is not available if auto-negotiation is disabled on a port. That port will only operate in MDIX mode.

MAC Address Forwarding

The Switch will flood packets that have a destination MAC address of 00-00-00-00-00-00.

Broadcast Storm Control

The threshold value set by the **`bridge broadcastStormControl`** command is applied to each port. It is not used as the sum of threshold values for all ports on the system.

Swapping Software Images

If you have a 10G expansion module on your Switch 3870 and you issue the **`system control swapSoftware`** command, only the software image on the Switch 3870 itself will be changed to the standby image. The software image on the expansion module will not be swapped. The only way to change the software image on the 10G expansion module is to use the **`system control softwareUpgrade`** command, which will change the Switch and the expansion module software at the same time.

Adding Units to a Switch 3870 Stack

When a stack of Switch 3870 units is powered up, the unit with the lowest MAC address is elected stack master. After running for 20 seconds, the master unit enters master preemption mode, meaning that if a unit with a lower MAC address is added to the stack, this new unit will not take over as stack master.

If, however, a standalone unit has been allowed to run for 20 seconds, this unit will also enter master preemption mode. When this unit is added to the existing stack, the current stack master will determine that there are two units in master preemption mode and this will trigger a new master election process to determine the stack master.

If the new unit has a lower MAC address than the old stack master, and will overwrite the configuration of all units in the stack with its configuration during the stack synchronization process. This means that the existing stack could lose all of its configuration information (VLAN, Spanning Tree, Aggregated Link etc.).

To prevent this situation from occurring when adding units to a stack, you should power down the standalone, connect the stacking cables and then power up the unit. As the unit will not be in master preemption mode, a new stack master will not be elected and the current stack master will transfer its configuration to the new unit as part of the normal synchronization process.

If the stack is later rebooted, the new unit will be elected stack master, since it has the lowest MAC address. However, since all units in the stack have the same configuration information, nothing will be lost when the new stack master synchronizes all of the slave units in the stack.

SFP Modules

When adding or removing SFP modules, the Switch will reset a number of port parameters. 3Com recommends that you verify the following port parameters after adding or removing an SFP module:

- Media configuration (auto negotiation, speed and duplex)
- Link Aggregation membership.
- LACP state.
- Spanning tree port parameters.
- VLAN membership.

10 Gigabit Module

- If a packet is received on the 10G port with a valid source address, destination address and checksum yet the length field has a value of zero, the packet will be dropped and the CRC Error counter will be incremented.
- Oversize (or jumbo) packets received on the 10G port will be counted in the total packets counter. However, they will not be counted in the oversize packets counters.

Web Interface

- Many Web browsers can be configured to ignore stylesheets, substituting user configured fonts and font sizes. Ignoring stylesheets may cause unpredictable effects when accessing the Web interface. 3Com recommends that you enable stylesheets on browsers used to access the Web interface of the Switch.

Known Problems

- Spanning Tree *stpCost* does not return to the default value when the end station is disconnected from a port. The stpCost will be recalculated when an endstation is plugged back into the port.
- Each port is allowed to be members of multiple VLANs as a tagged member, but can only be in one VLAN as an untagged member. Using SNMP to edit

dot1qVlanStaticUntaggedPorts allows a port to be removed from all VLANs as an untagged member. To avoid disrupting network traffic, the VLAN should be re-assigned to another VLAN as an untagged member.

- Display speed of the address table is very slow during MAC address learning.
- Statistics for oversize and jabber packets of size 1600 octets from the 10G port are calculated as packets ranging from 1024 to 1518 Octets. Packet size of 1600 octets from other ports will be calculated correctly.
- If a manual aggregated link contains ports that are running at different speeds, all the ports will remain active. The Switch 3870 will not disable those ports running at lower speeds. Users should make sure that all ports (and partner devices connected to the ports), are all running at the same speed duplex mode. This can be done by using auto-negotiation based on the same supported capabilities, or manually configuring the ports to the same speed and duplex mode where required. If ports are not running at the same speed, network slowdowns could occur if traffic is directed across the slower links in the aggregation. This condition does not occur when using LACP.
- The Switch 3870 only supports the 56-bit DES cipher with SSH. By default, many SSH clients will not support the DES cipher with SSH and therefore fail to make a connection. For example, to make a successful SSH connection to the Switch 3870 with Putty (v0.55) you must check its `Enable legacy use of single-DES in SSH2` button.
- Due to the aging algorithm implemented in the Switch 3870, the MAC address may take longer than the specified aging time to age out.
- When configuration changes are made to a stack, they are initially made to the master and it is this configuration that is used to configure the stack on power up. A secondary background process synchronizes all of the slaves to the master to preserve the configuration, in the event that a slave has to be elected as a new master. This synchronization can take up to 15 minutes. De-powering the stack before this process has completed may prevent the configuration being saved to all of the slaves units. If the master then fails and the stack is re-booted, the configuration of the stack may be lost.
- If a stacking cable is defective (not completely broken, but still partially conducting), or a stack unit becomes defective (that is, still powered on, but not operating properly), the stack may not initialize properly. You will have to replace the defective item, and reboot the stack.
- The ARP entry timeout is one or two minutes longer than the nominal value.
- MSTP and Layer 3 functions cannot operate at the same time. If MSTP is enabled, Layer 3 functions are disabled. If you want to operate under Layer 3, you will need to set Spanning Tree to STP or RSTP.
- When jumbo frames are disabled, oversize packets are counted as jabbers on the Gigabit ports.
- When traffic is passing into a upstream port and out of downstream port, and the downstream port

then receives pause frames from the end station, the Switch cannot send pause frames out of the upstream port quickly enough, therefore causing some packet loss.

- If packets originally destined for the UDP Helper match an entry for "DSCP to CoS" or "IP Port to CoS" mapping, these packets will be mapped and forwarded according to the CoS setup, instead of relayed by the UDP Helper.
- If a trunk is configured using LACP, or if a trunk only has members on the optional media expansion modules, then after rebooting, the trunk's STP cost and MSTP cost will be lost.
- The **`system summary`** command displays the 10G-LR Xenpak (for 3Com 3CXENPAK92) as an "Unsupported Xenpak". In fact, this module is supported.
- In the Web page for *Security* > *Device* > *Trusted IP Host* > *Display/Edit*, you cannot change the trusted IP state to "Disabled" and select the last entry for removal at the same time. You must disable it first, and then delete the last entry.
- In the Web page for *Bridge* > *Broadcast Storm Control* > *Setup*, if you change the threshold value and disable broadcast storm control in one set operation, or the threshold value is changed while broadcast storm control is disabled, the new threshold value will be applied to the system even though broadcast storm control status is set to disabled. If you get into this situation, then take the following steps to correctly disable broadcast storm control. Change the state to "Enabled" first and then to "Disabled" again while keeping the threshold value unchanged throughout the operation.
- 3Com does not recommend power cycling the stack or exchanging units in the stack under heavy traffic. 3Com recommends that traffic be disabled when performing such actions to ensure that the system powers up correctly and that routes can be learned properly.
- 3Com does not recommend setting the IP address of interface 1 to 0.0.0.0 as it can result incorreect Layer 3 behavior on the management VLAN.

Known Interoperability Issues

- An incompatibility exists when changing link speed from 10 Mbps half duplex to 100 Mbps half duplex. If auto-negotiation on the Switch is disabled and the link speed on the Switch is changed from 10 Mbps half duplex to 100 Mbps half duplex, there is a possibility that the link partner will not detect the change. The link will have to be broken and reconnected before the link partner will detect the speed and change link speed to 100 Mbps half duplex.
- When using LACP to form a trunk with a SuperStack 3 Switch 4400, ensure that the Switch 4400 is running the latest software release. Older versions of software occasionally fail to correctly form the trunk resulting in a network loop. Alternatively you could consider configuring the trunk manually.

3Com Network Management

3Com Network Supervisor

3Com Network Supervisor is an easy-to-use application that discovers and manages up to 1,500 IP devices and 3Com NBX telephones.

For more information on how to obtain a copy of 3Com Network Supervisor, please visit:
http://www.3com.com/3ns/

3Com Network Director (3C15500)

3Com Network Director is a standalone application that allows you to carry out key management and administrative tasks on mid-sized enterprise networks. By using 3Com Network Director you can discover, map and monitor all the devices on the network, backup and restore 3Com device configurations, configure 3Com devices across the network in a single operation (including VLANs and Traffic Prioritization) and gather historical performance information for your network and generate flexible reports.

For more information on how to obtain a copy of 3Com Network Director, please visit:
http://www.3com.com/3nd/

After installation, click *LiveUpdate* to add support for the latest 3Com products.

Part No. DNA174509-1AAA01
Published November 2005