SuperStack® 3 Switch 3870 Family Software Version 2.5 Release Notes

Related Documentation

Please use these notes in conjunction with the following documents:

- "*SuperStack 3 Switch 3870 Family Getting Started Guide*"
  Part number: DUA1745-0AAA03
  (supplied with your Switch and in PDF format on the 3Com Web site)
- "*SuperStack 3 Switch 3870 Family Implementation Guide*"
  Part number: DUA1745-0BAA02
  (supplied in PDF format 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: DQA1745-0AAA02
  (supplied with your Switch and in PDF format on the 3Com Web site)
- "*SuperStack 3 Switch 3870 Family Management Interface Reference Guide*"
  Part number: DHA1745-0AAA02
  (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 s3h2_50s56.bin and s3h2_50s168.bin software provides support for the following products:

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

Part No. DNA1745-0AAA04
Published June 2005

Fixes for Known Faults

The following issues with previous software versions have been fixed in this release.

Security Features

- The Radius Setup Wizard now contains a prompt to configure the Shared Secret. You will no longer need to configure the Shared Secret separately.
- The Switch now can authenticate SSH client connections using a public key as well as using passwords.

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.

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 1 minute.
- A stack with approximately 150 MAC address entries is likely to encounter TFTP upgrade failures, if the software version on the stack is either version 1.0 or version 2.01. To ensure a successful upgrade, 3Com recommends splitting the stack before upgrading the software.

  If the upgrade fails, please contact 3Com Support.

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.

Multicast Filtering

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

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.

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.

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.
- To create a user with administrator privileges when using RADIUS device authentication you must ensure that user has the "Service-Type" attribute set to 15.
- Some RADIUS servers will not authenticate users with a blank password, all user accounts should have a valid password configured.

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 attempt to enable LACP on a port which is currently a manual member of a link aggregation then the following error will be displayed:

  ```
  Failed to set port 1:48 lacp status
  ```

If you wish 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

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.

  Please use the console to configure the unit with an IP address or connect the unit to a network with a DHCP server. If using DHCP you will need to use a console connection or log information from your DHCP server to discover the address which has been assigned to the unit.

- If the number of multicast traffic groups on your network exceeds the maximum supported by the Switch (64) then you may see occasional bursts of multicast traffic as the Switch updates its internal configuration.

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 ACL to a port you may see the following error generated:

```
Fail 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 number rules available depends on the port type:
  - 10/100/1000 Ports - Maximum of 2 rules per port.
- You try to bind an ACL to a port which forms part of an aggregated link, or a port that has LACP enabled.

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. The unit will respond with the following error if you attempt to remove the untagged membership of VLAN1:

  ```
  Failed to delete untagged port 1:2 from VLAN
  1
  ```

- 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 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.
- 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

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.

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.

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.

Spanning Tree

- When connecting switches together, 3Com recommends that spanning tree fast start should be disabled on the interconnecting ports (it is enabled by default on 10/100/1000 and SFP 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.
- When connecting switches together, if spanning tree fast start is not disabled on the interconnecting ports, any previously learned addresses on links that become blocked will not correctly age out until the aging time has passed. If the switch is power cycled then the device will learn the addresses correctly.
- 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, all spanning tree settings are reset to their default values. 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 *STP State* to *Enable* and configure STP version to *MSTP* in order to configure the Multiple Spanning Tree Protocol (MSTP) successfully.
- If you change the *STP Version* to a value other than *MSTP*, some MSTP parameters will be reset to their default values.
- If you reboot the Switch while the *STP Version* is set to a value other than *MSTP*, all MSTP configuration will be lost.
- Multiple Spanning Tree instance 0 (the Common and Internal Spanning Tree) cannot be configured using the **`bridge port mstCost`** or **`bridge port mstPriority`** commands. The Common and Internal Spanning Tree (CIST) should be configured using the **`bridge port stpCost`** and **`bridge spanningTree stpPriority`** commands.
- The summary information for MST instance 0 (CIST) cannot be viewed using the **`bridge port mstSummary`** command. Instead, use the **`bridge port summary`** command.

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 mirror port. The Switch does not currently 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 or protocol control packets such as RIP which are being sent out of the 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.

- Control packets such as BPDU cannot be monitored through a Roving Analysis port. When using Roving Analysis you must set the port security mode to *No Security*.
- 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

Auto-negotiation of Port Speed and Duplex

- All ports on the unit default to using auto-negotiation to determine the correct speed and duplex setting. If the link partner also supports auto-negotiation 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 auto-negotiation and select a fixed speed and duplex.

- When connected to a device that will not auto-negotiate, the device follows the algorithm required by the auto-negotiation 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.

LACP Protocol

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).

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.

MAC Address Forwarding

The 3870 will flood packets that have a destination MAC address of 00-00-00-00-00.

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.

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.

Known Problems

- Spanning Tree stpCost does not return to default value of 2000 when end station is disconnected from the a port. The stpCost will be recalculated when an endstation is plugged back into the port.
- The per port *mstCost* and *mstPriority* are not saved when the Switch is rebooted. Any values you have entered will be lost and must be re-entered.
- Each port is allowed be members of multiple VLAN as tagged member, but can only be in one VLAN as an untagged member. Using SNMP to edit dot1qPvid and dot1qVlanStaticUntaggedPorts will allow the port to belong to both the original VLAN and the new VLAN as untagged member.
- When listing VLAN members of an MST instance using the Command Line Interface, long lines may not wrap correctly and the VLAN members may be incorrectly displayed in the Instance ID column.
- If a MAC address is manually added to a secure port, the Web interface incorrectly displays its status as *Secured*. The Command Line Interface displays the port's status correctly as `Permanent`.
- 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.
- When modifying a VLAN name that wraps on two lines characters may not appear to be deleted when pressing backspace. The characters may be deleted when though they do not disappear from the display.
- 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. 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.
- If a large number of addresses have been learned on an aggregated link (for example, 1000 or more), it could take 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 a 3870 stack is power cycled while configuration information is being saved, the following error message could appear:

  ```
  FS_ReadFileContent::ERROR!! Check sum failed,
  Please contact technical support or try
  again.
  ```

If this occurs, the stack should be power cycled again to clear this condition.

- 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

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.

Documentation Errors and Omissions

In the following documents:

- *SuperStack 3 Switch 3870 Family Management Quick Reference Guide* (DQA1745-0AAA02)
- *SuperStack 3 Switch 3870 Family Management Interface Reference Guide* (DHA1745-0AAA02)

the following commands have been omitted:

- *Bridge* > *Jumbo Frames* (Web interface) and **`bridge jumboFrames`** (CLI)

  Standard Ethernet packets have a maximum frame-size of 1500 bytes. Your Switch supports jumbo frames which have a maximum frame-size of 9000 bytes (jumbo frames). You can enable or disable jumbo frames by using the *Jumbo Frames* window or **`jumboFrames`** command.

- **`security device ssh userAuth userkey delete`** (CLI)

  You can delete a user public key using the **`userkey delete`** command on the **`userAuth`** menu.

  From the menu, select username and key type of the public key to be deleted.

- **`security device ssh userAuth userkey detail`** (CLI)

  You can display a user public key using the **`userkey detail`** command on the **`userAuth`** menu.

  From the menu, enter the username of the public key you want to display.

- **`security device ssh userAuth userkey download`** (CLI)

  You can download a user public key to the Switch using the **`userkey download`** command on the **`userAuth`** menu.

  From the menu, enter TFTP server IP address and file name of the file to be downloaded. Enter a username.

  The file will begin to download and the message `Key File Download in progress` will be displayed.

- **`security device ssh userAuth userkey summary`** (CLI)

  You can display a summary of users using the `summary` command on the `userAuth` menu.

- **`security network access systemMode`** (CLI)

  You can enable and disable network security on the Switch using the systemMode command on the access menu.

3Com Network Supervisor

The CD-ROM contains 3Com Network Supervisor.

3Com Network Supervisor provides powerful yet easy-to-use network management. Focused on the needs of small to medium enterprises, it enables you to manage your network more efficiently. For larger networks (up to 2,500 nodes) and extra functionality you can purchase the 3Com Network Director Package.

To download the latest 3Com Network Supervisor and Service Pack please visit:

http://www.3com.com/3ns/

To download the latest 3Com Network Director please visit:

http://www.3com.com/3nd/

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

For HP OpenView users the Switch 3870 (and all other 3Com managed products) are fully supported by the 3Com Integration Kit for HP OpenView (3C15300).