GIGABIT MULTILAYER SWITCHING SOFTWARE VERSION 4.21 RELEASE NOTES

Related Documentation

Please use these notes in conjunction with the following documents:

- "*SuperStack 3 Switch 4900 Family Getting Started Guide*"
  Part number: DUA1770-0AAA05
  (supplied with your Switch and in PDF format on the 3Com Web site)
- "*3Com Switch 40x0 Family Getting Started Guide*"
  Part number: DUA1770-0AAA05
  (supplied with your Switch and in PDF format on the 3Com Web site)
- *"Gigabit Multilayer Switching Software V4.0 Implementation Guide*"
  Part number: DUA1770-0BAA06
  (supplied in PDF format on the CD-ROM that accompanies your Switch and on the 3Com Web site)
- "*Gigabit Multilayer Switching Software V4.0 Management Quick Reference Guide*"
  Part number: DQA1770-0AAA06
  (supplied with your Switch and in PDF format on the 3Com Web site)
- "*Gigabit Multilayer Switching Software V4.0 Management Interface Reference Guide*"
  Part number: DHA1770-0AAA06
  (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 Gigabit Multilayer Switching 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 website.

If you intend to use a Switch 4900 Family unit or Switch 40x0 Family unit with version 4.21 software in a Distributed Fabric, ensure that all other units in the Distributed Fabric are upgraded to version 4.21 as well. 3Com cannot guarantee correct operation if different software versions are used within a Distributed Fabric. Please

Part No. DNA1770-0AAA15v420
Published June 2005

note that under the terms and conditions of the 3Com End User Software License Agreement, you will need to purchase a service contract for each existing Switch before upgrading to version 4.21 software.

About this Software Version

The version 4.21 software feature set is a compatible superset of that provided by all previous versions of this software.

The s3g4_21.bin software provides support for the following:

- SuperStack 3 Switch 4900 (3C17700)
- SuperStack 3 Switch 4900 SX (3C17702)
- SuperStack 3 Switch 4924 (3C17701)
- SuperStack 3 Switch 4950 (3C17706)



The SuperStack 3 Switch 4900 Family Gigabit Multilayer Switching Software Version 4.21 (s3g4_20.bin) does not operate on any other 3Com Switch.

This gmi4_21.bin software provides support for the following:

- 3Com Switch 4050 (3C17708)
- 3Com Switch 4060 (3C17709)
- 3Com Switch 4070 (3C17707)



The 3Com Switch 40x0 Family Gigabit Multilayer Switching Software Version 4.21 (gmi4_20.bin) does not operate on any other 3Com Switch.

Upgrading to Software Version 4.21

3Com strongly recommends that you upgrade all Switch 4900 Family units and Switch 40x0 Family units that are running a previous version of software to version 4.21.

Fixes for Known Problems

The following known faults have been fixed in version 4.21:

- Synchronizing the Mac Address database on systems with multi-homed hosts connected to separate units in the stack could result in system resets with system errors 0x00e07421 or 0x00e07437.

.

Points to Note when using the Switch 4900 Family and Switch 40x0 Family

Supported Expansion Modules

- 3C17710 – 4 port 1000BASE-SX module
- 3C17711 – 4 port 1000BASE-T module
- 3C17712 – 4 port 1000BASE-LX module
- 3C17714 – 4 port GBIC module
- 3C17716 – XRN Interconnect module

Inserting and Replacing Expansion Modules



CAUTION: *The Modules are not hot-insertable or hot-swappable. You must always power down the Switch and disconnect it from the mains before installing or removing a Module.*

- When you insert a Module into the Switch, push the Module in until the Module's back plate is in full contact with the Switch's chassis.
- When you have inserted the Module, secure the Module to the Switch by tightening the three captive screws fully with a screwdriver.
- If an error is indicated during the Power On Self Test, check that the module has been correctly inserted.



Ensure that the blanking plate and its fastenings are stored in a suitable place. If the module is removed, the blanking plate must be replaced.

When an expansion module is replaced by another module of a different type, the configuration will not be completely reset to factory defaults. Specifically, the following module parameters will not be reset:

- Static addresses
- Resilient links
- IGMP router ports
- RMON alarm variables
- Spanning Tree port data

It is recommended that all module configuration should be reviewed after the expansion module has been replaced.

Subnet Broadcasts

From version 4.11, subnet broadcasts will be blocked by default. Earlier versions of the software always forwarded subnet broadcasts. From version 4.11, subnet broadcast forwarding can be enabled using the CLI or Web management. See the section "Documentation Errors and Omissions" for further details.

Apple networks and Rapid Spanning Tree

With default settings there is a 30 second delay between a front panel port activating its link status and passing network traffic. Users of Apple networks, which may transmit initialization packets during this time, may not have been able to see some network devices. The delay between a port activating its link status and passing network can be reduced for edge devices by setting the stpFastStart value for a port to "Enable". See the section "Documentation Errors and Omissions" for further details.

Auto-MDIX

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

Serial Cable

When using a serial cable you must ensure that it is wired correctly as described in Appendix B of the Getting Started Guide.

TFTP Upgrades

Note that 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 5 minutes.

You can avoid the 5 minute time out period by aborting the upgrade, either using the *Abort* button in the Web interface or the *Esc* character in the Command Line Interface.

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.

LACP Protocol



CAUTION: *The LACP protocol is disabled by default in the version 3.00 or later agent. 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).*

Software Update Utility

The Software Update Utility (SUU) is a Windows application used to serially update the software to the Switch via the console port. The preferred method for updating the software on the Switch is via a TFTP upgrade. The SUU should only be used if a TFTP upgrade has failed. This utility is available on the CD-ROM that accompanies your Switch.

SLIP

Although it is possible to set up a SLIP connection through the console port on unit 1, the resulting connection may only work intermittently. The console port on unit 2 does not support SLIP.

Traceroute

Traceroute implementation is using UDP probe packets to perform the traceroute operation. MS-DOS or PC-DOS systems have a Non-Standard implementation of TCP/IP, which may cause them to not respond to the Traceroute UDP probe packets.

QoS

If you have configured QoS on a single unit (such as the SuperStack 3 Switch 4924, 4950, or the 3Com Switch 40x0) and it merges with a unit having fewer QoS capabilities (Switch 4900 and 4900 SX) to create a mixed Distributed Fabric, some of the user config- ured settings may be lost. 3Com recommends config- uring QoS after the Distributed Fabric has been created.

Software Upgrade

If you start a software upgrade using the CLI or a web browser, the Switch will report the status of each unit as it finishes its upgrade. If you are upgrading a Distributed Fabric and use the web, or connect to the CLI using telnet, and your computer is directly connected to a port on the Distributed Fabric, the connection will break when the unit with that port completes its upgrade and restarts. If there are other units still to upgrade at this point, you will not get status reports about them, but the upgrade should continue normally. You can check this by using the **`system summary`** command on each unit and verifying that the Operational Version shows the correct version of software. Note that this problem will not occur if your computer is connected indirectly via a hub, a router, or another Switch that is not part of the Fabric.

IGMP

- IGMP querying is disabled by default due to potential interoperability issues with core products that do not follow the lowest IP address election method. Refer to Chapter 3 “Using Multicast Filtering” of the Implementation Guide for more information about this method.
- If you wish to run multicast sessions in a network that does not contain any IGMP routers (or queriers), you can configure the Switch to automatically negotiate with compatible devices on a VLAN to become the querier. Use the **`bridge multicastFilter igmp queryMode`** CLI command. The Switch 4900 Family and Switch 40x0 Family

are compatible with any device that conforms to the IGMP v2 protocol.

- If IGMP snooping is enabled then IP multicasts will only be forwarded within a VLAN if an IGMP querier is present in that VLAN.

XRN Distributed Fabric

- If the XRN Interconnect breaks or is disconnected, all router interfaces in one of the units (including the management interface if it was set manually) will go to the DOWN state. The interfaces will stay down as long as the unit detects another unit with the same interfaces. Even if the management inter- face is modified it will stay in the DOWN state. If the management interface was set by AutoIP, then one unit will shut down all interfaces, but the management interface will acquire a new IP address via the AutoIP process.
- To ensure maximum security after connecting units in a Distributed Fabric, and the units have reconfigured themselves, 3Com recommends that you reconfigure the user names and passwords defined in the local database using the *Security* > *User* web operation or the **`system management password`** CLI command. This recommendation is not necessary if you are using a RADIUS authentication server on your network to validate management access to the units.
- To provide support for XRN's Distributed Resilient Routing, XRN-enabled Switches send periodic (once a second) ARP based broadcasts on the VLAN associated with the first non-default IP inter- face defined on the Fabric. This is typically, but not always, interface 3. This protocol will also occur on a single Switch Fabric as long as it has at least one non-default interface. These broadcasts will not impact network performance.
- When the Switch units are in an XRN Distributed Fabric created using the GBIC Module, they assume their unit IDs from the MAC address of the Switch unit within which the GBIC Module is installed. So the unit with the lowest MAC address will assume Unit 1 ID and the unit with the highest MAC address will assume Unit 2 ID.

WinSock 2 Libraries for Windows 95

Microsoft WinSock 2 is an application that helps other applications talk to other computers and devices on networks and the Internet.

Microsoft Windows 98, Microsoft Windows NT 4 and Microsoft Windows 2000 already have this application installed, so if you use these operating systems, you will not need to install WinSock 2 on your machine.

If you use Windows 95, you may need to install this. Early versions of Windows 95 did not include this, while later versions did. If your system requires WinSock 2 you can locate this application in the "Software and Utilities section" of the CD-ROM that accompanies your Switch.

Spanning Tree Protocol

Switch 40x0 Family only: In the v2.52 release and later, Spanning Tree is enabled by default.

Known Problems

- In previous releases, Static and Static Default routes were incorrectly advertised out the same subnet the route was defined on. Since v4.0 soft- ware, Static Routes are no longer advertised out the same subnet, Static Default routes are still advertised incorrectly. If Static and Static Default routes are being used in a subnet with more than one RIP router, then all of the RIP routers within the subnet must have the Static and Static Default routes manually configured to the same gateway.
- From v4.0 software release, the precedence of RIP learned routes was changed to be higher than Static Default Routes. RIP learned routes will over- write Static Default Routes in the routing table. A summary of the routing table will reflect this change to the Static Default Route. If the dynami- cally learned route is flushed or aged from the routing table, the software will immediately restore the Static Default Route until the RIP route is dynamically learned again.
- When modifying the area ID of an active OSPF interface on an XRN Fabric, it is possible that OSPF adjacency and neighbor information may not be properly synchronized between the units. To avoid this, set the OSPF interface mode to "dis- abled" using the protocol `ip ospf interface` mode command prior to modifying the area ID. After modifying the area ID, issue another protocol ip ospf interface mode command to set the OSPF interface mode back to "enabled".
- If a GBIC module is used to form a distributed Fabric, both units must be configured so that the GBIC modules operate in Interconnect mode. Unexpected behavior including, corrupted packets or leaked intra-fabric management traffic will occur if cables are connected and the mode is not set accordingly.
- 3Com recommends that you do not perform software upgrades during heavy traffic periods. Upgrades should occur while there is under 90% utilization.
- To avoid possible misrepresentation of information when using the web interface in a Windows NT environment, it is necessary to select small fonts for display purposes.
- To avoid a failure during Configuration and Restore mode, 3Com recommends that you do not remove or insert cables during save or restore operation.
- To avoid a failure during an expansion module swap, 3Com recommends that you initialize the unit afterwards. This is especially true if you replace a new version of a module and then revert to the older model, in which case the old configuration settings would apply and could possibly be wrong.
- IF the XRN Fabric has been disabled as a result of conflicting software versions, every unit in the Fabric must upgraded to the same software version and the unit must be rebooted.
- 3Com recommends that link aggregations should not be configured with a mixture of automatic and manual member ports. In addition, 3Com recommends that LACP is disabled on ports that are added manually to aggregations. Otherwise:

- If the port is initially unconnected when it is manually added to an aggregation: LACP may unexpectedly move the port to another aggregation when the port is subsequently connected to a partner device.
- If the port is initially connected to another LACP enabled partner device: The LACP partnerId of the device may conflict with that of the manual aggregation and cause a CLI error message to be generated.



If an automatic aggregated link (created by LACP) contains ports with different VLAN membership, the aggregated link will inherit the VLAN membership of the first port that comes up in the aggregated link. It will override any pre-defined VLAN membership for the aggregated link.

- 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.
- If in the Distributed Fabric you define the management interface only (i.e. the unit is used as a Layer 2 Switch), when the Distributed Fabric is split both units will continue to use the same IP address for management. This can make the units management interface unreachable until the IP address is changed on one of the units. 3Com recommends that in this case the management interface be set to auto configure.
- **Switch 4900 Family only**: On downgrade to an agent earlier than version 4.00 (e.g. 2.00) any QoS configuration created before the downgrade will be lost. However, if a QoS configuration was created originally on 2.00, and no additional QoS configuration have been made with a v4.xx agent, then on downgrade the original QoS configuration will still exist on 2.00.
- In a Layer 2-only network (i.e. with no Multicast Routers) multicast traffic destinations may not be learnt for up to 5 minutes after a Switch is powered on, or is reset.
- The Switch does not display an error message if inappropriate, but otherwise legal, IP addresses are used for certain configurations. For example, the IP address of the Switch can be supplied as the TFTP server address for software upgrade. No error is displayed to warn of the mistake. The solution is to supply a more appropriate IP address.
- The **`system management password`** CLI command should not be used when logged in as a user authenticated via RADIUS. To change a password in the local (non-RADIUS) database, use the **`security device user modify`** CLI command.
- The spanning tree mode is not synchronized between units following a Distributed Fabric merge. This should not cause any problems for the network since rapid spanning tree is fully backward compatible with legacy spanning tree. Where units within the Distributed Fabric are operating in different spanning tree modes, the user interfaces are not capable of reflecting this – they will choose one setting or the other when asked to show the current spanning tree mode. When a new spanning tree mode is written to the Distributed Fabric (via any of the user interfaces), this will be set on

all units within the Distributed Fabric regardless of whether the spanning tree mode previously differed from unit to unit.

- Half-duplex flow control (backjamming) cannot be enabled or disabled on a per port basis. If any port on a specific unit is reconfigured, all half-duplex ports on that unit will be changed to the new configuration.
- When setting up a SLIP IP address and an IP address for the unit you must ensure that the assigned IP addresses are different.
- The default set-up for Netscape 4.76 on Solaris 2.6 may cause problems when using *System->Telnet->Connect*. By changing the application that Netscape launches from '`xterm`' to '`dtterm`' the problem is overcome. This is accomplished as follows:

1 From the *Edit* menu in Communicator, select *Preferences*.

2 Click the arrow next to Navigator to expand its sub-menu and select *Applications*.

3 In the *Applications* list in the right-hand pane, click on the row that has telnet in the *Description* column and click the *Edit* button.

4 In the *Edit* window, the text in the *Application*: box should be changed from:

```
xterm -e telnet %h %p
```

to:

```
dtterm -e telnet %h %p
```

5 Click *OK* to close the *Edit* window and click *OK* to close the *Preferences* window. *System->Telnet->Connect* should now connect correctly with the device.

- Netscape 4.7x browsers may crash if the browser window is maximized or re-sized whilst loading Switch management screens.
- If while using Netscape with the Web management interface, you attempt to access an area which is restricted due to your current access level, you may be prompted repeatedly for a username and password. To get out of this situation, click *OK* when you are asked if you want to reauthenticate, then click *Cancel* on the username and password entry box. A message stating *401 Unauthorized* will be displayed. You may now log in to the Web management interface again. To avoid this, log in using a higher access level, or do not attempt to access areas of the Web interface which are restricted for your access level.
- When using Netscape 4.7 it is recommended not to open multiple browsers and then visit other Web sites before returning to the 3Com web management page. Scripts loaded by other web sites can overwrite the settings required by the 3Com web management.
- If Netscape is being used to log into the device via the Web interface, and all attempts to the RADIUS server time out, the next authentication attempt may fail immediately. To avoid this, wait several seconds before retrying the authentication attempt.
- If you use Netscape to manage your Switch you may experience problems when trying to change

the user password. 3Com recommends that if you use Netscape and you need to change the password you do so via the CLI command. To do this from the Web interface Device View, use the *System > Telnet > Connect* operation to start a Telnet connection and then use the **`security device user modify`** CLI command.

- If the error, *The previous command window is still active* is displayed when using the Web interface, you must close that window before you can select another operation. You should then press *Reload* (Netscape) or *Refresh* (Internet Explorer) in your Web browser.
- When performing a software upgrade via the *System->Control->Software Upgrade* Web interface, the *OK* and *Cancel* buttons may be partially obscured by the edge of the window. This issue only occurs when all of the following conditions exist:
  - Windows 95
  - IE5.0 or IE5.5
  - Screen resolution set to 800x600.
  - Java plugin version earlier than 1.3.1

  This problem can be fixed by upgrading to Java plugin version 1.3.1 or later via the following link. `http://java.sun.com/getjava/download.html`
- The Switch Web interface can only be accessed by any of the following Web browsers:
  - Microsoft Internet Explorer v5.0
  - Microsoft Internet Explorer v5.5
  - Microsoft Internet Explorer v6.0
  - Netscape Communicator v4.76
  - Netscape Communicator v6.2
- The Switch Web interface can be accessed on any of the following PC operating systems:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT v4.0
  - Microsoft Windows 2000
  - Microsoft Windows XP
  - Solaris 2.6
- **Switch 4900 Family only**: If a Switch is running v2.50 software and Smart AutoSensing is enabled (the default state), the RMON Alarm table will be corrupted the next time that the Switch is rebooted or power cycled. The effect of this is that Broadcast Storm Control will be disabled and the customer will have limited or no protection against broadcast storms.

  If you are upgrading a Switch that is running software prior to v2.50, or you are running v2.50 software but Smart AutoSensing is disabled, you can upgrade directly to v4.21 software and skip the details which follow.

  If, however, you are upgrading a Switch that is running v2.50 software and Smart AutoSensing is enabled you must perform the following steps to

ensure that Broadcast Storm Control functions properly:

1 Reinitialize the Switch to factory defaults using the **system control initialize** command. The Switch will have to be reconfigured to your site specific information, this includes VLANS, IP interfaces, static routes.

2 Immediately after reinitializing to factory defaults and before power cycling or rebooting the Switch, Smart AutoSensing must be disabled using the **physicalInterface ethernet smartAutoSense disable** command. The Switch can then be reconfigured.

3 Download the v4.21 software to the Switch.

4 Once the v4.21 software has been downloaded and the Switch has rebooted, you can re-enable smart AutoSensing using the **physicalInterface ethernet smartAutoSense enable** command.

Broadcast Storm Control will now behave correctly even if the Switch is rebooted or power cycled.

- If an IP interface goes down, any static routes that were defined for that interface will continue to appear as up in the routing table. This happens despite the fact that they are unreachable. If a new route is learned that has the same IP address as the one that is down then this route will appear in the routing table twice; once as static and once as RIP. When this occurs, the learned route is the valid route.

  If you issue the **protocol ip route remove** command for the route which appears twice, the static route will be removed. The learned route will continue to appear in the routing table until it ages out or another **protocol ip route remove** command is issued again.

- Do not disable IGMP snooping on the unit when there are hosts in the segments 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.

- Pause packets are counted incorrectly. Received pause packets are included in the transmit packet counters. Transmitted pause packets are included in the receive packet and octet counters.

- If a port is being blocked by Spanning Tree Protocol (STP), and STP is disabled, then the port remains blocked until the Switch is reset.

- Internet Explorer 5. If *Ignore font styles specified on Web Pages* or *Ignore font sizes specified on Web Pages* are selected, then the appearance of the web interface will be unpredictable. 3Com recommends that neither of these tools are selected (options are found under Internet Explorer 5 menu *Tools* > *Internet Options* > *Accessibility* > *Formatting*).

- If you should decide to downgrade to an older version of the agent software, you may notice inaccurate information displayed within the web browser interface. This is typically seen as inactive hotspots in the interface. If this should occur, we recommend that you exit the browser, clear the browser cache, and begin another session.

- BOOTP address does not renew after 1 hour. The IP address is dropped and replaced with 0.0.0.0. The IP address is lost for only a few minutes every hour but is re-established.
- If routing is configured on the management interface (interface 1) - the routing configuration will be lost if the user switches the manual IP configuration for the interface to automatic configuration.
- **Switch 4900 Family only**: Beginning with the v2.50 release, Spanning Tree is enabled by default. If Spanning Tree is currently disabled on your Switch 4900 Series unit, and you are running an image prior to v2.02, upgrading to v2.50 or later software may change the Spanning Tree state to the enabled state unexpectedly. This will only occur if you have never modified the Spanning Tree state on your unit or if you have reinitialized your unit.

  If your unit is running software prior to v2.02 and you wish your Spanning Tree state to remain disabled, there are two ways to prevent the state from being automatically enabled. Either modify the Spanning Tree state on your unit (disabled to enabled back to disabled) before upgrading to v2.50 software or later, or upgrade to v2.04 soft- ware and then upgrade to the newer software. Please note that if you reinstalled your unit running v2.50 or later software using the **`system con- trol initialize`** command that Spanning Tree will be enabled when the unit boots up.
- If you have a QoS profile applied to a port with a service level that remarks the DSCP field, then all the incoming traffic will be remarked. Traffic which is identified by the service level profile will be marked accordingly. Traffic that does not match the service level profile will be remarked with a DSCP value of 0 (best effort). The effect of this is that traffic which identified as "no mark" will be remarked. To avoid this, 3Com recommends that you do not mix "DSCP marking" and "DSCP No-change" service levels.
- **Switch 4924, 4950 and 40x0 Family only**: 802.1p (packet prioritization) overwriting. If the ingress port is untagged and the egress port is tagged, the packet's 802.1p priority will be marked appropriately. However, if the ingress port is tagged and the egress port is tagged, the packet's 802.1p priority will not be remarked.
- **Switch 4924, 4950 and 40x0 Family only**: DSCP value of 0 cannot be used as a QoS classifier.
- **Switch 4924, 4950 and 40x0 Family only**: Ether-type IP (0x800) and ARP (0x806) cannot be used as QoS classifiers.
- **Switch 4900 Family only**: If you upgrade from software version 2.02/2.04 to version 2.50 or later, you must reassign the desired QoS profile to all ports.
- The *OK* button in the *System ->Cache Config ->Summary* of the web browser interface does not function properly if you have Windows 95 loaded and are using Internet Explorer version 5.5. The status may change while the summary screen is open and therefore reflect an inaccurate reading.
- **Switch 4900 Family only**: When upgrading to version 2.50 or later software, the default setting for Spanning Tree will be Rapid Spanning Tree ON.

When this happens the priority settings for Spanning Tree will be rounded down. Example: `Select menu option: br span stpp Select stp priority (0,4096,8192,12288,16384,20480,24576,28672,32768,36864,40960,45056,49152,53248,57344,61440)[32768]:`

- If Spanning Tree is disabled on your Switch, you must have each port assigned to an untagged VLAN. Ports can also be assigned to multiple tagged VLANs.
- Using the Web interface operation *Physical Interface > Ethernet > Setup*, it is not possible to dis- able a range of ports if the port types included in the range are different (for example, fiber and cop- per). The CLI command **`physicalInterface ethernet portstate`** must be used instead. The CLI also must be used to disable an empty GBIC port.
- You may see addresses in the RIP Neighbors table that do not belong to any of your locally configured subnets. This will not cause any negative effects to routing while using RIP.
- It is not possible to access the Device View in the Web interface if the Switches in your Distributed Fabric are running different versions of the Gigabit Multilayer Switching software.
- When upgrading the Gigabit Multilayer Switching software within a Distributed Fabric containing both SuperStack 3 Switch 4900 Family and 3Com Switch 40x0 Family units via the Web interface, it is necessary to enter both software file names on the same line in the Filename text box, separated by a space (e.g. gmi4_20.bin s3g4_20.bin). Failure to do so may result in a mixed software version Distributed Fabric and loss of connection to the Web interface.
- Configuration Save: Certain special character combinations in the User Notes can cause problems when executing a Configuration Save operation. The following are known to cause problems:
  - If a '<' character is not followed by '>' somewhere in the User Notes, none of the characters after the '<' character will be saved.
  - Typing two '\' characters in a row (e.g. "\\") will yield only a single '\' character in the User Notes.
  - The character combination ~! ('~' followed by '!') should not be used as this can cause the Save operation to hang.
- When using the Configuration Save and Restore feature, the restore operation will be unsuccessful if the physical configuration of the device or Distributed Fabric is different, and an error message will be displayed. The one exception to this is for units that have front panel GBIC slots. If a save operation is performed and then a GBIC is inserted into a previously empty slot, the restore operation will complete successfully with no error generated. You will then need to configure the newly inserted GBIC manually.

  If a GBIC is removed after a save operation, leaving an empty slot, the subsequent restore operation

will fail as expected and an appropriate error message will be generated.

Known Interoperability Issues

- An incompatibility exists in the default settings for Link Aggregation between the Switch and the following 3Com products:
  - 3Com Switch 4007
  - SuperStack II Switch 3900
  - SuperStack II Switch 9300
  - CoreBuilder 9000 family
  - CoreBuilder 9400
  - CoreBuilder 3500

  The products listed above disable auto-negotiation when a port is added to an aggregated link (trunk). In order for link aggregation (trunking) to work, ports at either end of an aggregated link (trunk) must be identically configured. To resolve the incompatibility, you must complete the following steps:

1. On any of the Switches listed, you must disable TCMP on a trunk (aggregated link) that connects to a Switch, as TCMP is not supported on the Switch.
2. You must disable auto-negotiation on all ports on the Switch that you want to place in an aggregated link *before* you place them in the aggregated link.



Refer to the *Management Interface Reference Guide on the CD-ROM or 3Com Web site for more information about configuring aggregated links.*

- 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.
- Although it is possible to set up a slip connection from a PC running Windows 2000 to the console port of the Switch using the "Communications Cable between 2 computers" modem type, the resulting setup only works intermittently.

Software Upgrades

To upgrade the software on the Switch do the following:

1. Locate the upgrade software 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 or 2000 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 or 2000 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.

3Com Network Management

3Com Network Supervisor (3C15100E)

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/`

However, for larger networks and access to more major features, 3Com recommends 3Com Network Director, described below.

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.

Documentation Errors and Omissions

Initializing to factory defaults

Page 168 of the Gigabit Multilayer Switching Software (V4.0) Implementation Guide (DUA1770-0BAA06) should be corrected as follows:
The Switch unit must be reset to its factory default settings before you can restore a configuration onto it. You can reset the Switch using the **`system control initialize`** CLI command or the *System* > *Control* > *Initialize* Web interface operation.

not

The Switch unit must be reset to its factory default settings before you can restore a configuration onto it. You can reset the Switch using the **`protocol ip initializeConfig`** CLI command or the *System* >*Control* > *Initialize* Web interface operation.

Controlling subnet broadcasts

Note: From version 4.11, subnet broadcasts will be blocked by default.

There are CLI and WEB configuration options to enable and disable the forwarding of subnet broadcasts:
`protocol/ip/directedBroadcast`

The commands allows the reception and forwarding modes of network prefix directed broadcasts to be configured.

The first option presented is Receive directed broadcasts. The choices are:

- Disable — To drop network prefix directed broadcasts before they are processed.
- Enable — To allow reception and processing of network prefix directed broadcasts.

The second option presented is Forward directed broadcasts. The choices are:

- Disable — To prevent the forwarding of received and originated network prefix directed broadcasts.
- Enable — To allow forwarding of received and originated network prefix directed broadcasts.

The CLI commands are presented as follows and there is an equivalent Web management screen.

```
Select menu option: protocol ip
directedBroadcast
Receive directed broadcasts(enable,
disable)[disable]: enable
Forward directed broadcasts(enable,
disable)[disable]: enable
Select menu option:
```

CLI operation

The command line console supports cursor keys in VT100 compatible mode.

The delete, backspace and Cursor Left/Right keys modify the command line.

You can also use the Cursor Up/Down keys to recall a previous command.

In addition, the following keys can be used to edit the command line:

[Ctrl A] - moves the cursor to the start of the command line.

[Ctrl B] - moves the cursor back one character.

[Ctrl D] - deletes the character at the cursor.

[Ctrl E] - moves the cursor to the end of the command line.

[Ctrl F] - moves the cursor forward one character.

[Ctrl K] - delete all characters from cursor to the end of the line.

[Ctrl X] - delete all characters from cursor to the start of the line

Note that the Delete key now performs as a 'Delete' key, i.e. character to the right, rather than as Backspace.

Spanning Tree stpFastStart operation

In the following documents:

- *Gigabit Multilayer Switching Software V4.0 Implementation Guide*''
  Part number: DUA1770-0BAA06

- ''*Gigabit Multilayer Switching Software V4.0 Management Interface Reference Guide*''
  Part number: DHA1770-0AAA06

The description of the bridge port stpFastStart CLI command is incorrect for version 4.21 software. Please refer to the following for details.

Prior to the release of the v4.11 agent, in order to avoid the risk of temporary loops, ports set to stpFastStart enabled enforced a 4 second delay before entering forwarding mode. This delay is incompatible with AppleTalk networks. In version 4.11 and later software, RSTP can now operate ports in one of three different modes: ''Enable'', ''Auto'' or "Disable".

By default all ports are initialized to have stpFastStart disabled, which causes a maximum 30 second delay before a port becomes active. This would be the normal setting for ports connecting to other Switches. This mode is not compatible with AppleTalk networks.

''Enable'' mode now causes ports to enter forwarding mode immediately after becoming active. This mode should be used for ports connected to edge devices in an AppleTalk network. It can also be used on any net-

work when it is certain that the port will only ever be connected to an edge device.

"Auto" is a safe mode to use if it is not certain if an edge device, or another Switch, will be connected to the port. This mode enforces a 4 second delay before entering forwarding mode. This period is normally enough to detect another Switch and prevent the possibility of a temporary network loop. This mode is not compatible with AppleTalk networks.

Copyright © 2005, 3Com Corporation. All rights reserved.
Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, SuperStack, and the 3Com logo are registered trademarks of 3Com Corporation. XRN is a trademark of 3Com Corporation.

Windows is a registered trademark of Microsoft Corporation. Other brand and product names may be registered trademarks or trademarks of their respective holders.