SuperStack® 3 Switch 3226 and Switch 3250 Software Version 1.02 Release Notes

Related Documentation

Please use these notes in conjunction with the following documents:

- "*SuperStack 3 Switch 3226 and Switch 3250 Getting Started Guide*"
  Part number: DUA1750-0AAA01
  (supplied with your Switch and in PDF format on the 3Com Web site)
- "*SuperStack 3 Switch 3226 and Switch 3250 Implementation Guide*"
  Part number: DUA1750-0BAA01
  (supplied in PDF format on the CD-ROM that accompanies your Switch and on the 3Com Web site)
- "*SuperStack 3 Switch 3226 and Switch 3250 Management Quick Reference Guide*"
  Part number: DQA1750-0AAA01
  (supplied with your Switch and in PDF format on the 3Com Web site)
- "*SuperStack 3 Switch 3226 and Switch 3250 Management Interface Reference Guide*"
  Part number: DHA1750-0AAA01
  (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

This software provides support for the following:

- Switch 3226 (3CR17500-91)
- Switch 3250 (3CR17501-91)

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

Part No. DNA1750-0AAA02
Published April 2004

The software is available in two versions:

- s3201_02.bin — Provides normal levels of encryption with keys of up to 56 bits in length.
- s3201_02s.bin — Provides higher levels of encryption including 168-bit 3DES and 256-bit AES.

The Switch ships with software providing normal levels of encryption.

Errors and Omissions

The **`system console speed`** command is available on the unit but has been omitted from the "*SuperStack 3 Switch 3226 and Switch 3250 Management Quick Reference Guide*" and the "*SuperStack 3 Switch 3226 and Switch 3250 Management Interface Reference Guide*".

To change the speed of the console port:

1. Enter **`system console speed`** from the top-level menu of the Command Line Interface.
2. Enter the speed at which you want to set the console port or **?** to see a list of available speeds.

SuperStack 3 Switch 3226 and Switch 3250 Getting Started Guide

Pages 15 and 16 contain the following statement:

"The console port uses a standard null modem cable and is set to auto-baud, 8 data bits, no parity and 1 stop bit."

This is incorrect. It should read:

"The console port uses a standard null modem cable and is set to 19200 baud, 8 data bits, no parity and 1 stop bit."

If you change the speed, make a note of the new setting. If you cannot connect using the console port and do not know the speed at which it is set, connect using a network port and enter the **`system console speed`** command to check the speed of the console port.

Enhancements and Fixes for Known Faults

The following features and enhancements are supported in version 1.02.

Web Interface

The unit only allows printable ASCII characters, with character codes between 32 and 127, to be used for strings such as the unit location or VLAN name. Characters such as those used for accented letters in non-English languages are rejected. In previous firmware these characters where rejected with a

`Data is invalid` error with no explanation. The new firmware returns an error describing the field containing the error and then returns to the page allowing the error to be corrected.

Command Line Interface

The output of the **`bridge port summary`** CLI command has been improved:

- The `stpState` field has been replaced by `Link` and `Spanning Tree` columns to more accurately report the active port status.
- The `fwdTransitions` field has been renamed `Forward Trans`.
- The `LACP PartnerID` field now reports `LACP disabled` if the protocol is disabled or not supported on the port.

The output of the **`bridge port detail`** CLI command has been improved:

- The `stpState` field has been added. This shows if the Spanning Tree Protocol (STP) has been enabled on the port. The field will read `Enabled` if STP is enabled on the port, even if STP is disabled globally on the unit.
- The currently active spanning tree state for the port is reported in the `Spanning Tree` column of the VLAN table. Please note that the product supports a single spanning tree state for all VLANs as per the *802.1d Spanning Tree* specification. It does not support *802.1s Spanning Tree per VLAN*.
- The `LACP PartnerID` field now reports `LACP disabled` if the protocol is disabled or not supported on the port.

Traffic Prioritization

In previous versions of the software, the DSCP prioritization of the *CS6* code point defaulted to 802.1d priority 7. This has been corrected. The *CS6* code point now defaults to 802.1d priority 6.

VLANs

In previous versions of the software, removing a port from a VLAN left static entries bound to the port-VLAN. This has been fixed. When you remove a port from a VLAN all static entries for that port-VLAN will be deleted.

802.1x Network login authentication:

- In previous versions of the software, authentication attempts for valid users would occasionally fail. The bug causing this has been fixed.
- The user name reported in the CLI command **`security network access detail`** was occasionally displayed with incorrect trailing characters. This has been fixed. The user names are now displayed correctly.

RMON history statistics and Web port history statistics

A bug in previous software versions prevented statistics being generated for the first timing interval. This has now been fixed.

In previous software versions the 1 hour statistics did not appear until the unit had been running for 2 hours. The statistics would then be correctly generated on an hourly interval. This has now been fixed. 1 hour statistics are available after 1 hour.

Similarly the 6 hour statistics would not appear until the unit had been running for 12 hours and then update every 6 hours. This has now been fixed. 6 hour statistics are available after 6 hours.

Software Version Number

The software version number reported by the **`system control swapSoftware`** CLI command is displayed incorrectly in previous versions of the software. For example, software version 1.01 displays the version as `1.1`.

When running the 1.02 or later software, it displays all software versions correctly, including 1.00 and 1.01.

The **`system control swapSoftware`** *command does not include an indication of the encryption level supported by the firmware; the firmware supporting the normal encryption level* 1.02*, and the strong encryption firmware* 1.02s *both appear as* `1.02` *when using this command. The encryption level of the current firmware can be verified by running the* **`system summary`** *command:*

Static port security and the bridge MAC address table

If static port security is enabled on a port with more than 200 addresses the previous software versions would report that the command had failed, but would add the first 200 addresses to the bridge address table and move the port into the secure state.

In addition, disabling port security would occasionally fail to flush the secure addresses from the bridge address table.

The current software correctly rejects the attempt to move the port into secure mode if there are more than 200 addresses. When this condition occurs it does not change the port security mode or make any of the addresses secure. In addition, disabling port security always removes all static bridge address entries from the port.

Binding an ACL to a port fails occasionally

In previous versions of the software, the unit would incorrectly count the number of ACL rules when trying to determine whether the ACL could be bound to the port.

This has been fixed. In the current software version the software correctly allows for an ACL to be bound if it is within the limits of the particular port.

See "Access Control Lists" in the "Points to Note when using the Switch 3226 and Switch 3250" section of this document for further details.

3Com Network Supervisor Discovery

When using 3Com Network Supervisor with previous versions of the software, 3Com Network Supervisor was unable to display the unit on the network topology. This will prevent you from using 3Com Network Supervisor to update the software from 1.00 or 1.01.

This has been fixed. The Switch running software version 1.02 and above can be discovered successfully using 3Com Network Supervisor and the correct network topology generated.

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

- The Switch ships with a version of software that supports up to 56-bit encryption for SSH and SSL (HTTPS). For higher levels of encryption including 168-bit 3DES and 256-bit AES, download the strong encryption version of the Switch software from the 3Com Web site and install as detailed in "Updating the Switch Software" above.

  When you have a strong encryption version of the Switch software loaded, the Software Version field on the Web interface will show the version number of the software followed by the words `(Strong encryption)`.

- 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.

- When attempting to upgrade the software on the unit it may occasionally report the following error:

  `Error: File service in progress.`

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

Points to Note when using the Switch 3226 and Switch 3250

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

- When enabling the static port security feature on a port the Switch will report *static fail* if you exceed the maximum number of secure addresses (200). The unit will not move the port into secure mode. 3Com recommends that port security be enabled on only edge ports which will typically have only a few addresses.
- 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.
- When configuring RADIUS using the CLI command **`security radius setup`** you should note that the wizard does not include a step to configure the RADIUS shared secret. You will need to configure the shared secret using the **`security radius sharedSecret`** command before RADIUS will operate.
- 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 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 1:50 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

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.

IP Configuration and Routing

- The Switch is optimized to operate as an edge router with a single default gateway acting as the next hop route to all other subnets.
- In larger networks it may take several minutes for the unit to learn the correct routing information. The unit may have to flush and relearn the routing information if there is a topology change in the network. During this time the network connectivity may be intermittent.
- In certain situations, the Switch will be unable to used hardware routing display the following error message in the system summary and route table:

```
Current network configuration requires use of
software routing, resulting in degraded
performance.
```

This message can be caused by one of the following situations:

- if there are more than14 routes whose next hop is not the default gateway. 3Com recommends reconfiguring the network so that the uplink from the Switch goes directly to another layer 3 router which is configured as the default gateway.
- if the unit is unable to contact one or more of its next-hop routers then software routing will be used. Find the reason why the router cannot be contacted and correct the problem.
- if there is no default gateway configured. Configure a default gateway and check to see if the problem is solved.
- when the Switch is learning new routes. The Switch may take up to a minute to learn new routes. The above message may be displayed for a short time while a route is learned. This is normal behavior.

- 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.

- Reconfiguring an IP interface may cause the RIP configuration and static routes settings for that interface to be lost.
- When adding or modifying an IP interface the CLI and Web interface may appear to hang for up to 30 seconds while the operation takes place.
- When forwarding DHCP and BOOTP requests in a multinetted environment, the UDP helper will only use the primary IP interface in the forwarded requests. This will cause the BOOTP/DHCP server to allocate all dynamic addresses from the primary subnet of a multinetted VLAN.
- 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.
- 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

When trying to bind an Access Control List (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 Ports - At least 15 rules per port
  - 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

- There is no CLI command available to remove IP port based traffic prioritizations. If you wish to remove these entries you must either use the Web interface or initialize the unit.
- 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
```

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.

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 all 10/100 ports and disabled by default on 10/100/1000 and SFP ports). This can be done using the *Physical Interface* > *Ethernet* > *Setup* command on the Web interface.
- 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.

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.
- 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.

Combination Ports

- The two 10/100/1000 ports are combination ports. When an SFP module is inserted it has priority over the 10/100/1000 port of the same number. The corresponding 10/100/1000 port is disabled. The combination ports are numbered 25-26 on the Switch 3226 and 49-50 on the Switch 3250.

Supported SFP Modules

- 3CSFP91 — SFP 1000BASE–SX
- 3CSFP92 — SFP 1000BASE–LX
- 3CSFP97 — SFP 1000BASE–LH70

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 autonegotiation is enabled, the unit asks for a *fallback mode* to be entered for use when the port connects to a non-autonegotiation device. This fallback mode parameter has been left in the CLI for compatibility with other 3Com devices but is ignored by this device.

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.

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.

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 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 Supervisor Advanced Package.

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

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

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

For HP OpenView users the Switch 3226 and Switch 3250 (and all other 3Com managed products) are fully supported by the 3Com Integration Kit for HP OpenView (3C15300).