Doc. No. 78-1367-08

Catalyst Series Workgroup Switch Release Note

Supplement to DOC-CATALYSTUG4 (Document Number 78-1264-04)
Boot Firmware Version 1.1
Data Movement Processor (DMP) Flashcode Version 3.27
Network Management Processor (NMP) Flashcode Version 3.27

Introduction

This release note describes the features and modifications of the Catalyst Series Workgroup Switch and also contains applicable caveats and workarounds. Refer to the *Catalyst Series Workgroup Switch User Guide* for detailed information about the Catalyst Series Workgroup Switch.

Product Overview

The Catalyst Series Workgroup Switch is an Ethernet-to-CDDI/FDDI switch that provides high-speed transparent bridging between Ethernets, and high-speed translational bridging between Ethernet and CDDI/FDDI (Copper Distributed Data Interface/Fiber Distributed Data Interface). The switch has eight 10-megabit-per-second (Mbps) Ethernet ports and two 100-Mbps CDDI or FDDI ports. Refer to the "Product Overview" chapter in the *Catalyst Series Workgroup Switch User Guide* for details of product features and functions.

DMP Version 3.27 is an upgrade to the previously released DMP Version 3.2.

NMP Version 3.27 is an upgrade to the previously released NMP Version 3.2.

Version 3.27 Fixed Caveats

The following is a list of the modifications to earlier versions of the DMP and NMP software to fix previous caveats:

1. When a giant Ethernet packet was present, an Ethernet port was locked on the receive side of the port. This was due to a race condition between the normal-flow code and the error-recovery code. With this release, these conditions no longer affect the port.
2. The Catalyst console screen was locking whenever it received a duplicate IP address of one of the Catalyst's IP addresses, or when it received prefragmented frames sent to Catalyst's IP address from the network. With this release the console does not lock when these things occur.

3 The Catalyst did not report all IP interface addresses in response to a simple network management protocol (SNMP) request for IP address table. When using HP Openview for Unix or any conventional SNMP Manager, if you polled the Catalyst switch for .iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry, the Catalyst only responded with the lo0 interface. The Catalyst did not respond with the 1,3-10 or the sc0 intrerfaces.With this release, the Catalyst now returns all of the IP addresses in the routegroup configuration.

4 Under certain conditions, because of an RMON buffer spill-over situation, an NMP exception occurred when RMON (default_groups) was enabled. This version of the NMP software corrects this problem.

5 Network management traffic was affecting the precision of Spanning-Tree timers, as well as the generation of bridge protocol data units (BPDUs). This caused instability in the network topology. With this release, the Spanning-Tree process is assigned the highest priority.

6 The DMP software sent a copy of every multicast frame to NMP causing extra processing on the NMP. With this release, DMP delivers only Internet Group Management Protocol (IGMP) multicast frames and Spanning-Tree multicast frames.

7 All of the IP routing information protocol (RIP) frames were delivered to NMP even though RIP was disabled. With this release, DMP does not deliver the IP RIP frames to NMP when RIP is disabled.

8 The Catalyst was originating IP broadcast frames on a blocked Spanning-Tree port, under certain conditions. Other than Cisco discovery protocol (CDP) frames and IP packets to be routed to specific host or gateways, no other packets will be transmitted on blocked Spanning-Tree ports.

9 When multiple IP routegroups were configured on the Catalyst with Spanning-Tree enabled, the ports sometimes toggled between blocking and listening states. This caused Spanning-Tree instability. With this release, the problem no longer occurs.

10 When a Catalyst was routing IP and it receives an IP frame to be routed to a non-existent host, some of the receive buffers were being permanently locked. This was due to the lack of an address resolution protocol (ARP) response from the non-existent host. With this release, the receive buffers will not be permanently locked if an IP host does not respond.

11 The Catalyst was not accepting RIP packets that were truncated. With this release, the NMP software accepts all RIP packets.

12 When the Catalyst was configured as a non-root bridge it was not accurately handling such Spanning-Tree parameters, as forward delay, and maxage. This release corrects all Spanning Tree issues.

13 With default_groups enabled, the Catalyst was reporting non-zero RMON statistics for unconnected ports. With this release, the Catalyst always reports zero statistics for unconnected ports.

14 The message_age timer in the Spanning-Tree BPDU was overestimated under certain conditions. With this release, the message_age timer has been modified.

15 FDDI Banyan Vines frames with protocol ID 80C4 were not being translated properly. With this release the translation is correct.

16 When the Catalyst received a large (greater than 1500 bytes) IP FDDI frame with the don’t fragment (DF) bit set, it was sending an Internet Control Message Protocol (ICMP) unreachable message to the source without resetting the flags field. With this release, the DF will be set correctly.

Version 3.27 Enhancements

The following is a list of enhancements to earlier versions of the DMP and NMP software:

1. The Catalyst could not learn default route through RIP. This release enables the Catalyst to learn default route when RIP is enabled.
2. With Spanning Tree enabled, the default state of an unconnected bridge port was in “forwarding” mode, which would cause a temporary broadcast storm on all the connected ports. With this release, any unconnected port is in “not-connected” state, preventing the broadcast storm when the port is dynamically connected.
3. The CDP default state has been changed to enabled.
4. CPD packets were being forwarded even when CPD was disabled. With this release, the Catalyst only forwards CDP packets if CDP is enabled.
5. Significant performance enhancements have been made to the IP-routing capabilities of the Catalyst through gateways.

Version 3.27 Caveats

The following caveats have been identified and workarounds provided:

1. RMON with default_groups enabled affects the Spanning-Tree process under extended SNMP traffic conditions.

   Description:

   With RMON default_groups enabled, under *extended* SNMP conditions the console screen may freeze, but the Catalyst will still switch packets as long as there are no loops in the topology.

   This problem will be fixed in the next release of the Catalyst software.

2. Catalyst switch RIP limitations.

   Description:

   The Catalyst switch can learn and advertise up to 1400 IP routes without a loss of resources. If the switch is learning more than 500 routes via RIP, and if Spanning-Tree is enabled and the hello timer is set to 1 second, the Catalyst switch may temporarily run out of input resources. This may temporarily affect the stability of the Spanning-Tree configuration.

   This may also cause the non-root bridge to send duplicate ping responses on a blocked Spanning-Tree port. The Catalyst cannot respond to pings on a blocked Spanning-Tree port.

   Users should not set up redundant routing paths between two Catalyst switches when multiple IP routegroups is enabled.

   Workaround:

   Use the **set filter broadcast** command throttling mechanism to setup default routes in the Catalyst switch’s routing table and limit the number of broadcast frames that the Catalyst switch receives.

   These problems will be fixed in the next release of the Catalyst software.

3 Slow response from the console may occur with RMON default_routegroup enabled and multiple SNMPWALK sessions running on the Catalyst.

Note This condition does not affect the switching capabilities of the Catalyst.

Description:

Stability of Spanning-Tree may be affected when the Catalyst is learning a large number of new MAC addresses, as well as learning new IP routes via RIP.

Workaround:

For IP connectivity, configure a default route on the Catalyst instead of allowing it to learn RIPs.

This problem will be resolved in the next release of the Catalyst software.

4 After a Spanning-Tree topology change, end stations may not be able to reach the Catalyst on a port that was previously blocked.

Workaround:

Clear the ARP entry for the Catalyst's IP address from the originating IP station's ARP table, or clear the ARP table on the Catalyst you are trying to reach.

5 The console becomes locked if the Catalyst's SUM port is connected to an active Ethernet segment and if the user sets either a duplicate IP address or a zero address (0.0.0.0).

Workaround:

Ensure that you have not set a duplicate or a zero address to sc0.

6 Aborting a serial download will cause an NMP exception error when you enter the **show interface** command at the admin port.

Workaround

Do not abort a serial download. Let the serial download complete. If you do abort a serial download, reset the switch and reinitiate the serial download.

7 The Catalyst switch may continue to learn routes using the routing information protocol (RIP) but cannot route packets on interfaces that are administratively set to down using the **set interface** <*port#*> **down** command.

Note The switch can still bridge data on interfaces that are administratively configured as down.

Workaround

To have the Catalyst stop learning RIP updates on an interface, disable the port using the **set port** <*port#*> **disable** command.

8 Use the **connect fddi** and **disconnect fddi** commands carefully while the switch is bridging and routing traffic. If you use the **connect fddi** command, the connect state LED may change to ORANGE, indicating a minor alarm.

Workaround

Reissue the **disconnect fddi** command and then reconnect the port using the **connect fddi** command until the connect state LED changes to GREEN, indicating no alarms.

9 Adding route groups through the Workgroup Director requires the correct entry of all IP information, otherwise an error message will be displayed.

Description:

When you use Workgroup Director Version 4.1 to add new route groups, you must correctly enter all IP information. Otherwise Workgroup Director may display error messages about bad values

Workaround:

Using the Brouter Table menu form in Workgroup Director, while entering new route groups, correctly enter all the IP information. This must include the IP address, subnet mask, and broadcast address. Click the **SET** button to add the new route group configuration.

Version 3.2 Modifications

The following modifications have been made since the previous release:

1 When user datagram protocols (UDP) based BOOTP REQUEST frames were sent they were flooded on all the ports within the route group. With this release the BOOTP REQUEST frame flooding is extended to the nine ports of the Catalyst switch regardless of the bridge group and route group configuration.

2 The **set ipx** command has been modified to allow compatibility with DEC FDDI bridges. A new **FDDIRAW** variable has been added to the s**et ipx 8023rawtofddi** command. An FDDIRAW frame will have the IPX header checksum FFFF immediately following the source address field.

To use FDDI RAW translation enter the following command at the command prompt:

```
Console> (enable) set ipx
Usage: set ipx snaptoether <8023|SNAP|EII|8023RAW>
set ipx 8022toether <8023|SNAP|EII|8023RAW>
set ipx 8023rawtofddi <8022|SNAP|FDDIRAW>

Console> (enable) set ipx 8023rawtofddi FDDIRAW
```

3 To allow the Catalyst switch to begin packet gathering for RMON immediately when the switch restarts, the optional **default_groups** variable has been added to the **set rmon** command. To enable the default_groups option at system restart enter, the **set rmon** command with the **default_groups** option and **enable** as in the following example:

```
Console> (enable) set rmon
Usage: set rmon [default_groups] <enable|disable>
Console> (enable)
Console> (enable) set rmon default_groups enable
```

Then the Catalyst switch responds with a message:

```
This command will restart the system for RMON Default Groups re-configuration. Do you
want to continue (y/n) [n]? y
```

Enter **y** to restart the system and the default groups option for RMON will be enabled.

Note To disable the default groups for RMON enter the command **set rmon default_groups disable**.

4 To eliminate an obscure FDDI-to-Ethernet CAM table entry problem the **set fddicheck** command has been added. The **set fddicheck** command, if on, checks if a newly learned station MAC address on the FDDI port already appears as a CAM entry on an Ethernet port. If the MAC entry already appears in the CAM table on Ethernet port the entry will not be overwritten. Following are two scenarios: the typical scenario, where you do not need to use the command; and the rare scenario, where you may need to use the command:

Typical scenario:

A station is attached to a Catalyst switch at an Ethernet port, and the MAC address appears in the CAM table for that port. The station is then physically moved and is attached to a different Catalyst switch. Both Catalyst switches are attached via FDDI connections at port number 1. In this scenario, you do not need to use the **set fddicheck** command.

Rare scenario:

A station is attached to a Catalyst switch at an Ethernet port, and the MAC address appears in the CAM table for that port. The station transmits a frame out to the FDDI ring where erroneous void-frames transmitted on to the FDDI ring by a router force the Catalyst switch to incorrectly interpret that the station now appears on the FDDI port; the Catalyst switch overwrites the original CAM table entry. To eliminate this problem use the **set fddicheck** command.

Following is an example of the **set fddicheck** command:

```
Console> (enable) set fddicheck
Usage: set fddicheck <on|off>
Console> (enable)
Console> (enable) set fddicheck on
```

Note The **set fddicheck** command default is off, which allows the CAM entry to be overwritten even if its MAC address previously appears on the Ethernet port after appearing on an FDDI port.

Version 3.2 Caveats

The following caveats have been identified and workarounds provided:

1 The SUM port (sc0) IP address scheme has changed with Catalyst Switch Software Release 3.1. The switch IP address previously assigned to the SUM port will now, by default, be assigned to route group 1. Route group 1 will include all ports of the switch including the FDDI port. The SUM port (sc0) will be set to IP address 0.0.0.0. The SUM port will not be part of the default route group 1 and will not be able to communicate with the switch.

Workaround

The SUM port must be assigned a unique IP address to allow communication with the switch.

2 Aborting serial download will cause an NMP exception error when the you enter the **show interface** command at the admin port.

Workaround

Do not abort a serial download. Let the serial download complete. If you do abort a serial download, reset the switch and reinitiate the serial download.

3 The Catalyst switch may continue to learn routes using the router interface protocol (RIP) but cannot route packets on interfaces that are administratively set to down using the **set interface** *<port#>* **down** command.

Note The switch can still bridge data on interfaces administratively configured as down.

Workaround

To stop learning RIP updates on an interface, disable the port using the **set port** *<port#>* **disable** command.

4 The **show bridge** command displays an FDDI port to be forwarding although it is disconnected physically or disconnected using the **disconnect fddi** command. The erroneous status is displayed because the bridge still considers the FDDI port to be in the forwarding state. This is because the **disconnect fddi** command only *temporarily* disconnects the switch from the FDDI ring.

Workaround

The Spanning Tree will be informed that the FDDI port is disabled only when using the **disable port 1** command.

5 Use the **connect fddi** and **disconnect fddi** commands carefully while the switch is bridging and routing traffic. If you use the **connect fddi** command, the connect state LED may change to ORANGE, indicating a minor alarm.

Workaround

Reissue the **disconnect fddi** command and then reconnect the port using the **connect fddi** command until the connect state LED changes to GREEN, indicating no alarms.

6 Terminal sessions may freeze if the switch receives fragmented internet control message protocol (ICMP) packets destined to itself on the FDDI ring. The switch will still respond to any ping and telnet requests destined to it and bridge or route any packets.

Workaround

Reset the switch to eliminate the frozen terminal session.

7 Catalyst switch RIP limitations.

Description:

The Catalyst switch with RIP enabled can learn up to 1400 IP routes (approximately) without any loss of resources. Because of the resource limitation if the Catalyst switch is installed in an IP network where more than 1400 routes are being advertized the Catalyst switch might run out of input resources temporarily, which can temporarily impact the overall bridging and routing of traffic.

Workaround:

Setup default routes in the Catalyst switch's routing table and limit the number of broadcast frames that the Catalyst switch receives by using **set filter broadcast** command throttling mechanism.

8 Adding route groups through the Workgroup Director must include all IP information entered correctly, otherwise an error message will be displayed.

Description:

When using Workgroup Director Version 4.1, while adding new route groups, the Workgroup Director may display error messages about bad values if the complete IP information is not entered.

Workaround:

Using the Brouter Table menu form in Workgroup Director, while entering new route groups, enter all the IP information including, IP address, subnet mask and broadcast address, correctly and click the **SET** button to add the new route group configuration.

Version 3.2 Fixed Caveats

Following are the problems that were found in Version 3.1 of the Catalyst switch and resolved in Version 3.2:

1 The Catalyst switch with routing interface protocol (RIP) enabled would have periodic NMP exceptions or watchdog resets when it was learning thousand(s) of IP routes using RIP.

2 The Catalyst switch with internet group membership protocol (IGMP) disabled was not forwarding any IP multicast frames.

3 The Catalyst switch with RMON enabled was displaying blank IP host lists when the Domain View was used by the NetScout RMON software.

4 The Catalyst switch with RMON enabled was displaying incorrect time stamp for packets viewed through RMON.

5 The Catalyst switch was not handling Ethernet frames with zero length properly.

6 The Catalyst switch's broadcast threshold was not functioning to the finest granularity.

7 The Catalyst switch could incorrectly learn an Ethernet MAC address on a FDDI interface in the presence of erroneous VOID frames on the FDDI ring.

8 The Catalyst switch was incorrectly handling giant Ethernet frames on the SUM port.

9 IP connectivity between end stations was being disrupted because of a problem with IP route caching.

Version 3.1 Modifications

The following modifications have been made since the previous release:

1 When the **set optimization** command variable **encheck** was set to **on**, false giant packets were being reported causing poor switch performance. With this version of Flashcode, if giant packets are received, the encheck parameter is automatically set to on, eliminating the problem.

2 The **set tlmin** command has been added to set the time required for PHY hardware to transmit a given line state before advancing to the next physical connection management (PCM) state at the station management (SMT) level. The <port_num> should be 1 or 2, and the <hexvalue> should

be between 0 and 0xffff. The tl_min setting is stored in the TL_MIN register (also known as the LS_MAX register) as part of the SMT management information base (MIB) structure in nonvolatile memory, and is used for initializing the PHY hardware setting each time the switch is rebooted.

```
Console> (enable) set tlmin ?
Usage: set tlmin <port_num> <hexvalue>
       (hexvalue is in 2's complement)
Console> (enable) set tlmin 1 fdfd
Port 1 tlmin set to 0xfdfd.
Console> (enable)
```

3. Some FDDI SNAP frames with the proprietary organizationally unique identifier (OUI) field were not being translated correctly. This version of Flashcode corrects this problem.
4. Performance enhancements have been made to boost the Catalyst switch performance significantly while handling broadcast frames at wire speed.
5. All non-ODI (open data-link interface) IPX (internetworking packet exchange) drivers and some other LAN drivers that were sensitive to 802.3 frame length were experiencing connectivity problems with the Catalyst switch. This version of Flashcode corrects this problem.
6. Static CAM entries were not allowed with the last byte set to 00. This version of Flashcode corrects this problem.
7. Static CAM entries were not being handled correctly. This version of Flashcode corrects this problem.

Version 3.1 Caveats

The following caveats have been identified and workarounds provided:

1. The SUM port (sc0) IP address scheme has changed with Catalyst Switch Software Release 3.1. The switch IP address previously assigned to the SUM port will now, by default, be assigned to route group 1. Route group 1 will include all ports of the switch including the FDDI port. The SUM port (sc0) will be set to IP address 0.0.0.0. The SUM port will not be part of the default route group 1 and will not be able to communicate with the switch.

   Workaround

   The SUM port must be assigned a unique IP address to allow communication with the switch.

2. Aborting serial download will cause an NMP exception error when the you enter the **show interface** command at the admin port.

   Workaround

   Do not abort a serial download. Let the serial download complete. If you do abort a serial download, reset the switch and reinitiate the serial download.

3 The Catalyst switch may continue to learn routes using the router interface protocol (RIP) but cannot route packets on interfaces that are administratively set to down using the **set interface** <*port#*> **down** command.

Note The switch can still bridge data on interfaces administratively configured as down.

Workaround

To stop learning RIP updates on an interface, disable the port using the **set port** <*port#*> **disable** command.

4 The **show bridge** command displays an FDDI port to be forwarding although it is disconnected physically or disconnected using the **disconnect fddi** command. The erroneous status is displayed because the bridge still considers the FDDI port to be in the forwarding state. This is because the **disconnect fddi** command only *temporarily* disconnects the switch from the FDDI ring.

Workaround

The Spanning Tree will be informed that the FDDI port is disabled only when using the **disable port 1** command.

5 Use the **connect fddi** and **disconnect fddi** commands carefully while the switch is bridging and routing traffic. If you use the **connect fddi** command, the connect state LED may change to ORANGE, indicating a minor alarm.

Workaround

Reissue the **disconnect fddi** command and then reconnect the port using the **connect fddi** command until the connect state LED changes to GREEN, indicating no alarms.

6 Terminal sessions may freeze if the switch receives fragmented internet control message protocol (ICMP) packets destined to itself on the FDDI ring. The switch will still respond to any ping and telnet requests destined to it and bridge or route any packets.

Workaround

Reset the switch to eliminate the frozen terminal session.

7 The switch does not automatically delete the default route if the routing group configuration is changed using the **set routegroup** command. For example:

- A switch has a default route set to 199.133.219.42, which is part of a route group 199.133.219.161
- The user deletes or reconfigures the route group 199.133.219.161 to be part of 194.133.216.219
- The default route is still set as 199.133.219.42 and *not* deleted.
- The switch will not allow a new default route to be configured until the user manually deletes the default route group 199.133.219.42.

Workaround

If you remove an IP network from your routing group, delete the corresponding default route using the **clear route default** command.

Version 3.1 NetScout RMON Caveats

The following caveats to the NetScout RMON have been identified and workarounds provided:

1. The Resource Manager, Remote Login, and Token Ring Main screen icons are not supported by the NetScout Manager software and should not be used.
2. If the screen appears frozen or unresponsive this may be caused by a series of unintended actions by the user. For example, if the Main screen is opened, and at the same time the Add Agent submenu screen is opened, if the user clicks on an inappropriate button, for example, cancel, the Main screen will move to the front obscuring the Add Agent submenu. However, the Add Agent submenu screen will remain active in the background, making the Main screen unaccessible.

   All submenu actions items must be completed before other Main menu items may be activated.

   Workaround

   Reduce the frozen screen(s) to icons to find the active submenu screen hidden behind. The active submenu screen must be closed to allow another Main menu selection.
3. From the Main screen menu, all other submenus require only one click of the mouse to activate. If the user clicks two times on a selection, two instances of the same selection will be activated, causing multiple instances of the same function with overlapping screens. Multiple instances of the same submenu are a drain on the Client and Agent resources, and should be closed when not in use.

Note The submenus of the Main Screen are independent and can be activated from the Main menu screen with a single click of their button.

4. The Client may run out of resources because the user has too many processes opened at the same time for the amount of RAM and swap space configured in the Client workstation. The agent may also run out of resources due to limited memory availability.

   The Catalyst Switch will attempt to install all possible resources using the available memory. If the switch is not successful installing all of the enabled groups for the chosen domain, it will install as many as possible and display the following error messages:

   ```
   no resources...
   could not install
   ```
5. If the system appears slow to respond to a command, the possible causes for delayed responses are:

- The network may be very busy, causing the Client to retransmit the messages to the agent for proper responses.
- The screens that generate graphic displays, pie charts and bar graphs, for example, may be compiling data needed to generate the graphic display. Initial screen updates may take up to a minute or longer while the system command is sent to the probe, and an initial period of 15 seconds is required for the agent to wait for updated information before returning a screen update.

6 If you use the **Config** option from the Main screen to configure RMON, the system does not respond back to you when the configuration has been completed.

Note RMON configuration may take up to two minutes to complete.

Workaround

Use the Domain Management menu to confirm completion of the RMON configuration or use the Domain Manager submenu from the Main menu screen to install logical agents.

7 While communicating with an agent, an error message similar to the following may appear:

```
-- Error accessing agent < agent name >
   While retrieving Domains
   Error: cannot communicate with agent
```

This error message does not indicate the Catalyst switch is down. This error message may be caused by one or more of the following conditions:

- Busy network
- Two clients are accessing the same agent at the same time
- Not enough socket resources in the TCP/IP stack

Workaround

To verify the Catalyst state, ping the switch or refer to the console window to determine the exact nature of the problem.

8 The sample configuration files, with the file extension .cfg, stored in the usr/nohome/samples directory, should not be modified. These files should be copied to the user’s working directory and modified to create “user specific” configuration files.

Caution If the sample configuration files become corrupted the RMON must be completely reinstalled to create new sample configuration files.

9 The two terms *segment* and *domain* have different meanings in the context of NetScout Manager:

- Domain means an aggregate of protocol filters supported by the NetScout Manager.
- Segment means the network itself or the subnet which is fully connected.

Note For a subnet of nodes to form a segment, the nodes do not have to be separated by bridges, routers, or gateways.

To specify segments, a drawing of all nodes including bridges, routers, and gateways should be made. This would facilitate interpretation of the data collected and comparison of the various segments in terms of various data collection activities and remote monitoring of the MIBs.

10 When creating logical agents using the Edit Window, any of the following entries will generate an SNMP error code 3:

- Incorrect interface number
- Incorrect Read community name
- Incorrect Write community name

Workaround

Correct the mistakes by editing the configuration file associated with that agent and then reinstalling the file.

The correct interface number range is 3 through 10

Cisco Information Online

Cisco Information Online (CIO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CIO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CIO provides a wealth of standard and value-added services to Cisco's customers and business partners. CIO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CIO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CIO (called "CIO Classic") supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CIO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CIO in the following ways:

- WWW: `http://www.cisco.com.`
- Telnet: `cio.cisco.com.`
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CIO's Frequently Asked Questions (FAQ), contact `cio-help@cisco.com.` For additional information, contact `cio-team@cisco.com.`

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or `tac@cisco.com.` To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or `cs-rep@cisco.com.`

This document is to be used in conjunction with the *Doc Name Here* publication.