Release Notes for Cisco ONS 15530 4-Port 1-Gbps/2-Gbps FC Aggregation Card Functional Image Release 1.23

This document describes the features and caveats for the functional image, release 1.23, for the 4-Port 1-Gbps/2-Gbps FC aggregation card used with the Cisco ONS 15530 DWDM multiservice aggregation platform.

February 23, 2006

Text Part Number: OL-9735-01

Contents

This release note includes the following sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The 4-port 1-Gbps/2-Gbps FC aggregation card uses up to four small form-factor pluggable (SFP) optical transceivers to support client traffic. Each client interface can be configured using the command-line interface (CLI) for FC, fibre connection (FICON), or InterSystem Channel (ISC) links traffic at a 1-Gbps or 2-Gbps rate.

The 4-port 1-Gbps/2-Gbps FC aggregation card connects through four 2.5-Gbps electrical signals, or portgroup interfaces, to the switch module. The client port data streams must be mapped to one of these portgroup interfaces using the CLI.

The signal on the portgroup interfaces connects through the backplane and the CPU switch module to a 2.5-Gbps ITU trunk card, a 10-Gbps ITU trunk card, a 10-Gbps ITU tunable trunk card, or a 10-Gbps uplink card, where the signal is converted to/from an ITU channel. The cross-connections are configured using the CLI.

The 1-Gbps client traffic from a 4-port 1-Gbps/2-Gbps FC aggregation card is interoperable with the 8-port FC/GE aggregation card at the other end of the network. Any 1-Gbps FC, FICON, or ISC client signal can be transmitted between a 4-port 1-Gbps/2-Gbps FC aggregation card and an 8-port FC/GE aggregation card.

Note Open Fibre Control is supported only with FC and FICON encapsulation. Forward Laser Control is implicitly enabled with ISC.

For FC and FICON traffic, the node monitors the following conditions on the 4-port 1-Gbps/2-Gbps FC aggregation card:

- 8b10b Code Violation and Running Disparity (CVRD) error counts
- Invalid transmission words
- Tx frame counts
- Rx frame counts
- Tx byte counts
- Rx byte counts
- Tx CRC errors
- Rx CRC errors
- Link failures
- Sequence protocol errors
- 5 minute input/output rates
- Loss of Sync
- Loss of Light

For ISC traffic, the node monitors the following conditions on the 4-port 1-Gbps/2-Gbps FC aggregation card:

- CVRD error counts
- Loss of Light
- Tx frame counts
- Rx frame counts

- Byte counts
- Bit rates
- Frame rates (5 minute)
- Loss of Sync

Determining the Release of Your 4-port 1-Gbps/2-Gbps FC Aggregation Card Functional Image

This section describes the process you use to determine the existing functional image version installed on your 4-port 1-Gbps/2-Gbps FC aggregation card.

To display the functional image version in a 4-port 1-Gbps/2-Gbps FC aggregation card, use the following command in privileged EXEC mode:

Command	Purpose
show hardware linecard *slot*	Displays the functional image information.

Example

The following example shows the hardware version and the functional image information for the 4-port 1-Gbps/2-Gbps FC aggregation card in slot 4:

```
Switch# show hardware linecard 4
--------------------------------------------------------------------------------
Slot Number             : 4/*
Controller Type         : 0x1111
On-Board Description    : ONS 15530 1G/2G Fibre Channel Aggregation Module
Orderable Product Number: 15530-FC-4P=
Board Part Number       : 68-2014-02
Board Revision          : A0
Serial Number           : CNH08350243
Manufacturing Date      : 09/09/2004
Hardware Version        : 2.6
RMA Number              : 0x00
RMA Failure Code        : 0x00
Functional Image Version: 1.23
Function-ID             : 0
Version-ID (VID)        : V01
```

Updating to a New Release

For detailed functional image upgrade instructions, refer to the *Cisco ONS 15530 Software Upgrade Guide*. To download the 4-port 1-Gbps/2-Gbps FC aggregation card functional image, go to the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/ons15530-fpga.

Note After copying the `fi-ons15530-2xfc.A.1-23.exo` image to the Flash disk of the Cisco ONS 15530, download the image to the 4-port 1-Gbps/2-Gbps FC aggregation card (15530-FC-4P) using the reprogram CLI.

Caution A functional image reprogram cannot revert once the reprogram is started. Do not interrupt the reprogram procedure. Wait until it has finished before attempting any commands on the switch. Confirm that the image file download is done in binary mode and check file sizes before and after the download. A failure during reprogramming can result in the card being unusable.

New Features in Functional Image 1.23

The following new features are available for functional image 1.23, when combined with Cisco IOS software Release 12.2(29)SV or later:

- End-to-end speed negotiation
- Oversubscription
- Superportgroup

Note The end-to-end speed negotiation, oversubscription, and superportgroup features are supported only with FC and FICON encapsulations.

Caveats

This section lists the caveats for the 4-port 1-Gbps/2-Gbps FC aggregation card functional image.

Use Table 1 to determine the status of a particular caveat and its relevancy to your functional image release. In the table, “C” indicates a fixed caveat, “O” indicates an open caveat, and “NA” indicates the caveat is not applicable to the release.

\

Table 1 4-port 1-Gbps/2-Gbps Aggregation Card Functional Image Release Caveat Reference

DDTS Number	Release 1.0	Release 1.23
CSCsd66381	O	C
CSCee84190	O	C
CSCin80542	O	C
CSCin87284	O	C
CSCsc14597	NA	O
CSCsb85494	O	O

Caveat Symptoms and Workarounds

This section describes the open and resolved caveats for this release of the 4-port 1-Gbps/2-Gbps FC aggregation card functional image.

- CSCsd66381

  Symptom: Flow control does not become active when the 4-port 1-Gbps/2-Gbps FC aggregation card is interoperating between FC switches whose World Wide Switch Names are in a certain relative range. The link initializes normally and traffic passes without any errors, but flow-control remains inactive. Therefore, throughput compensation over distance is not realized.

  The output of the **show interface** command for the affected twogigabitphy interface shows flow control as enabled but inactive.

  Conditions: This symptom is seen when flow control is enabled in the 4-port 1-Gbps/2-Gbps FC aggregation card with Functional version 1.0.

  Resolution: Upgrade to Functional version 1.23 or later.

- CSCee84190

  Symptom: CRC-errored or Dropped/Out-of-Order/Duplicated frames may be transmitted by the 4-port 1-Gbps/2-Gbps FC aggregation card ports (with symmetric flow control configured and active) if the client device connected to remote port is operating in asymmetric credit mode.

  `EXCESS_FRAME_ALM` alarm message may be logged by the (peer) Cisco ONS 15530 when the errors are being generated, or prior to the occurrence of the errors if conditions with potential to cause the error are detected on the link.

  Conditions: This symptom is seen only if all the following conditions are true:

  – The link has at least one 4-port 1-Gbps/2-Gbps FC aggregation card that has a Functional version lower than 1.23.

  – If buffer credit sizes are configurable/readable on the end clients, the credit numbers at both ends are not the same.

  – When flow control is disabled or inactive, the link runs without any errors.

  – When the link is run with flow control enabled and active, the client device sees errors transmitted from the 4-port 1-Gbps/2-Gbps FC aggregation card port.

  – Symmetric flow control is active on the 4-port 1-Gbps/2-Gbps FC aggregation card ports, and is indicated by `flow-control (symmetric)` in the **show interface** output.

  – If the peer card is a 4-port 1-Gbps/2-Gbps FC aggregation card, `EXCESS_FRAME_ALM` alarm is detected on the peer Cisco ONS 15530.

  – If the peer card is a Cisco ONS 15530 8-port FC/GE aggregation card (15530-GEFC-8P), `EXCESS_FRAME_ALM` alarm is detected on the peer Cisco ONS 15530 (if supported).

  Note If the remote card is a 8-port FC/GE aggregation card, `EXCESS_FRAME_ALM` alarm message will be logged at the remote node only if the Functional version on that card is 2.30 or later, and Cisco IOS version on the remote Cisco ONS 15530 is 12.2(24)SV or later.

  – The transmitted errors are not traceable to TX CRC errors on the interface.

  – The transmitted errors are not traceable to hardware data parity errors (`QDR PARITY error count` in the **show controller** output).

Workaround/Resolution: Perform any one of the following actions in decreasing order of preference:

- Upgrade the 4-port 1-Gbps/2-Gbps FC aggregation cards to Functional version 1.23 or later, and remove any symmetric configuration from the ports.
- Configure asymmetric mode on all the 4-port 1-Gbps/2-Gbps FC aggregation card ports in the affected link. (Symmetric mode is the default in Functional versions prior to 1.23).
- If feasible, configure equal buffer credits on the client devices at both ends of the FC/FICON link. Symmetric/asymmetric mode configuration on the 4-port 1-Gbps/2-Gbps FC aggregation card is then ignored, and both modes work equally well.

- CSCin80542

  Symptom: Interoperation of the 4-port 1-Gbps/2-Gbps FC aggregation card with the 8-port FC/GE aggregation card is possible only in the symmetric mode flow control.

  Conditions: This occurs when all the following conditions are satisfied:

  - The 4-port 1-Gbps/2-Gbps FC aggregation card has a Functional version lower than 1.23.
  - The 4-port 1-Gbps/2-Gbps FC aggregation card is configured to operate in asymmetric mode flow control by CLI.
  - The 8-port FC/GE aggregation card has Functional version 2.30 or later.
  - Client credit behavior is asymmetric.

  Workaround: None.

  Resolution: Upgrade the 4-port 1-Gbps/2-Gbps FC aggregation card to Functional version 1.23 or later. In addition, it is recommended to remove any symmetric or asymmetric configuration from the flow control CLI.

- CSCin87284

  Symptom: Errored data may temporarily be transmitted from the 4-port 1-Gbps/2-Gbps FC aggregation card when the card transitions from the flow control active state to inactive state (due to link events such as Link Reset by the FC client). This causes the client FC device to record Transmission Word Errors. The burst of errors are temporary and settles to a clean state after re-login of the link. This symptom occurs rarely.

  Conditions: This symptom is observed only when flow control is enabled on the Cisco ONS 15530 4-port 1-Gbps/2-Gbps FC aggregation card.

  Workaround: None.

  Resolution: Upgrade the functional image to version 1.23 or later.

- CSCsc14597

  Symptom: When end-to-end speed negotiation is enabled on the twogigabitphy interfaces of the 4-port 1-Gbps/2-Gbps FC aggregation cards and the FC client devices, the twogigabitphy interfaces may lock to 1 Gbps even though the maximum negotiable speed is 2 Gbps. Error-free link connectivity and operation are maintained and the only impact observed is the reduced throughput. This problem occurs rarely.

  Workaround: Perform any of the following operations:

  - Perform **shut**/**no shut** on both the twogigabitphy interfaces in the affected link.
  - Perform **shut**/**no shut** on the affected interfaces of the client devices that are connected to the 4-port 1-Gbps/2-Gbps FC aggregation card.

  - Perform **encapsulation**/**no encapsulation** on both the twogigabitphy interfaces in the affected link.

  Resolution: None.

- CSCsb85494

  Symptom: CRC errors are observed on the FC client devices that are connected to the 4-port 1-Gbps/2-Gbps FC aggregation card when jumbo GE traffic is mixed on the same 10-Gbps trunk.

  Conditions: This symptom is seen when the GE traffic (with frame size greater than 1500 bytes) and the FC traffic from the 4-port 1-Gbps/2-Gbps FC aggregation card pass through the same 10-Gbps trunk card, and any one of the following conditions is satisfied:

  - Flow control is enabled on the 4-port 1-Gbps/2-Gbps FC aggregation card.
  - The affected FC link passes through a superportgroup on the 4-port 1-Gbps/2-Gbps FC aggregation card.

  Resolution: None.

Limitations and Restrictions

This section provides limitations and restrictions for Cisco ONS 15530 hardware and software.

4-port 1-Gbps/2-Gbps FC aggregation card

The following are the limitations of the 4-port 1-Gbps/2-Gbps FC aggregation card:

- Errors are transmitted by the 4-port 1-Gbps/2-Gbps FC aggregation card to the clients in some transitional events such as configuration changes on the card.

  Rarely, client FC device port may get into the error disabled state under such conditions.

Note The above mentioned limitation can be worked around by following the procedures documented in the *Cisco ONS 15530 Configuration Guide*.

- The reported byte count and bit rate values for the ISC service are higher than the actual values. They are inclusive of all data in the ISC frame such as frame headers, trailers, or checksums. The actual payload byte count and bit rate will therefore be lower than the displayed value.

Related Documentation

Use this release notes in conjunction with the following referenced publications:

- *Cisco ONS 15530 Configuration Guide*

  Provides procedures to configure and manage the Cisco ONS 15530.

- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series*

  Provides the regulatory compliance and safety information for the Cisco ONS 15500 Series.

- *Cisco ONS 15530 Planning Guide*

  Provides detailed information on the Cisco ONS 15530 architecture and functionality.

- *Cisco ONS 15530 Hardware Installation Guide*

  Provides detailed information about installing the Cisco ONS 15530.
- *Cisco ONS 15530 Optical Transport Turn-Up and Test Guide*

  Provides acceptance testing procedures for Cisco ONS 15530 nodes and networks.
- *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections*

  Provides processes and procedures for cleaning the fiber optic connectors and component interfaces of the Cisco ONS 15530.
- *Cisco ONS 15530 Command Reference*

  Provides commands to configure and manage the Cisco ONS 15530.
- *Cisco ONS 15530 System Alarms and Error Messages*

  Describes the system alarms and error messages for the Cisco ONS 15530.
- *Cisco ONS 15530 Troubleshooting Guide*

  Describes how to identify and resolve problems with the Cisco ONS 15530.
- *Network Management for the Cisco ONS 15530*

  Provides information on the network management systems that support the Cisco ONS 15530.
- *Cisco ONS 15530 TL1 Commands*

  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15530.
- *MIB Quick Reference for the Cisco ONS 15500 Series*

  Describes the Management Information Base (MIB) objects and explains how to access Cisco public MIBs for the Cisco ONS 15500 Series.
- *Cisco ONS 15530 Software Upgrade Guide*

  Describes how to upgrade system images and functional images on the Cisco ONS 15530.
- *Introduction to DWDM Technology*

  Provides background information on the dense wavelength division multiplexing (DWDM) technology.
- *Cisco IOS Configuration Fundamentals Configuration Guide*

  Provides useful information on the CLI (command-line interface) and basic shelf management.

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.

Convention	Application
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, the user might do something that could result in equipment damage or loss of data.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15xxx systems. It also includes translations of the safety warnings that appear in the ONS 15xxx system documentation.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.