



Release Notes for Cisco ONS 15310-MA Release 7.0.5

June 2008



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

Release notes address closed (maintenance) issues, caveats, and new features for the Cisco ONS 15310-MA. For detailed information regarding features, capabilities, hardware, and software introduced with this release, refer to Release 7.0 of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*, *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*, *Cisco ONS SONET TLI Command Guide*, and the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*. For the most current version of the Release Notes for Cisco ONS 15310-MA Release 7.0.5, visit the following URL:

http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_release_notes_list.html

Cisco also provides Bug Toolkit, a web resource for tracking defects. To access Bug Toolkit, visit the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Contents

[Changes to the Release Notes, page 2](#)

[Caveats, page 2](#)

[Resolved Caveats for Release 7.0.x, page 5](#)

[New Features and Functionality, page 7](#)

[Related Documentation, page 8](#)



Corporate Headquarters:

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation, page 8](#)
- [Documentation Feedback, page 9](#)
- [Cisco Product Security Overview, page 10](#)
- [Obtaining Technical Assistance, page 11](#)
- [Obtaining Additional Publications and Information, page 12](#)

Changes to the Release Notes

This section documents supplemental changes that have been added to the *Release Notes for Cisco ONS 15310-MA Release 7.0.5* since the production of the Cisco ONS 15310-MA System Software CD for Release 7.0.5.

No changes have been added to the release notes for Release 7.0.5.

Caveats

Review the notes listed below before deploying the ONS 15310-MA. Caveats with tracking numbers are known system limitations that are scheduled to be addressed in a subsequent release. Caveats without tracking numbers are provided to point out procedural or situational considerations when deploying the product.

Maintenance and Administration



VxWorks is intended for qualified Cisco personnel only. Customer use of VxWorks is not recommended, nor is it supported by Cisco's Technical Assistance Center. Inappropriate use of VxWorks commands can have a negative and service affecting impact on your network. Please consult the troubleshooting guide for your release and platform for appropriate troubleshooting procedures. To exit without logging in, enter a Control-D (hold down the Control and D keys at the same time) at the Username prompt. To exit after logging in, type "logout" at the VxWorks shell prompt.

CSCsc56694

IPPM enabled by CTC for an OCn trunk card is disabled automatically after two hours. This issue will be resolved in Release 8.0.

Alarms

CSCse85355

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON

ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd52665

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

CSCsd56328

The NE should report alarms or conditions on ingress port not on any internal ports. Alarm detected at the internal ports (TERM) side will be ingress map to the MON side. So the NE raises the STS-MON/VT-MON and STS-TERM/VT-TERM alarms or conditions on the STS-MON/VT-MON ports, irrespective of the actual detection port (MON or TERM). If the user wants the customized severity to be reflected for a specific STS/VT alarms, the alarm profile entities of both STS-MON and STS-TERM, if available, should be changed to the same severity.

Electrical IO Card

CSCsh17691

The 3-DS3 / 84 DS1 pack does not output any DS3 rate signal, i.e. no pulses, while in the IS or IS, AINS states if a crossconnection to the port is not in effect. The pack should put out a DS3 AIS signal when not crossconnected, regardless of its state. This appears when the crossconnection to the port is not present. No workaround available. This issue will be resolved in Release 8.01.

Common Control Cards

CSCsc52028

The CTX 2500 card does not accept more than 52 ENE sessions. Figuring 16 ENE sessions per GNE session, the expected ENE logins for 7 GNE sessions is 112, whereas the CTX 2500 accepts only 52. This issue will be resolved in Release 8.0.

Alarms

CSCse85355

After setting the alarm profile to report UNEQ-V as CR, the alarm still reports as the default, MJ, in some instances. To see this, on a single ONS 15310-MA create a path protection VT circuit using a single source with a primary and secondary destination to create the path selector. Inject UNEQ-V into the

protect path (for example, CTX2). This declares a minor UNEQ-V. Now inject UNEQ-V into the working path (for example, CTX1). A major UNEQ-V will be declared, rather than the CR that the alarm profile is set to. If the UNEQ-V is injected into the working path first, then into the protect path, a CR UNEQ-V will be declared and is correct. The workaround is to apply profiles for UNEQ-V monitor and UNEQ-V term that both have the same severity desired. This issue will be resolved in a future release.

CSCsh20447

When you have two open slots and if you enable Alarms on open slots and do a retrieve all alarms from TL1 Session you can see only one alarm even though you have two open slots. In 7.04 load, in CTC Provisioning->defaults->node->general->RaiseAlarmOnOpenSlot set this flag to true. Open a TL1 session; give RETR-COND-ALL: C. This issue is expected to be fixed in a future release.

CSCsh22922

Create a path protection between 310ma and 454 nodes have a loopback for OC3 card in 454. Create a vt circuit from 310ma to OC3 in 454. Connect test set to ds1 and pump traffic on ds1 port. From the CTC do edit circuit option, in switch column give a Manual to Protection switch. MAN-REQ alarm rises with severity as MN/NA. Change the severity of this alarm from CTC and give APPLY. Do a SYNC option from CTC. Even though you changed the severity of the Alarm that wont reflect in Conditions Pane. If you do a switch from Manual to working this works fine. This issue will be resolved in Release 8.0.

CSCsh20419

When you have two OPEN SLOTS in 15310MA and if you enable alarms on Open slots you will see only one alarm getting raised in Condition Pane of CTC. In 7.04 load, in CTC Provisioning->defaults->node->general->RaiseAlarmOnOpenSlot, set this flag to true. Do retrieve in Conditions Pane. Only one alarm is raised, even though you have 2 open slots. This issue is expected to be fixed in a future release.

TL1



Note

To be compatible with TL1 and DNS, all nodes must have valid names. Node names should contain alphanumeric characters or hyphens, but no special characters or spaces.

CSCsc51017

When multiple TL1 GNE and ENE sessions are created on a 30+ node network, some of the TL1 sessions might continue to be displayed in the user login pane under the network view, even when the sessions have been closed. If this occurs, restart CTC. This issue will be resolved in a future release.

CSCsh24550

Issuing the RTRV-NE-IPMAP command with ALL aid from TL1 to a 15310MA node retrieves the IP of 454 on the other side of DCC more than once. Command that creates the problem: RTRV-NE-IPMAP:: ALL: A; This issue will be resolved in Release 8.0.

CSCsh21744

The performance Monitoring registers for the counts SASCPP, UASCPP, SESCPP, ESCP, and CVCPP are not initialized to zero. May lead to a Threshold Crossing Alert. 1. DS1-28-DS3-EC1-3 and DS1-84-DS3-EC1-3 cards on 15310MA. 2. The DS3 ports configured with C-BIT frame format. 3. Command which will create the problem INIT-REG-T3: T3-1-1:1:: CVCPP; or SASCPP or SESCPP or UASCP or ESCP.

Workaround: All the registers can be cleared at one go through the CTC or by the following TL1 command. INIT-REG-T3: T3-1-1:1: all. This issue is expected to be resolved in 8.01 release.

Resolved Caveats for Release 7.0.x

This section documents caveats resolved in Release 7.0.5.

Maintenance and Administration

CSCsg17018

The Inhibit FE loopback parameter for the mentioned cards should be set to true. (The check box should be checked.) Before you test this, a) Please delete the database. (FlmDeleteDb) b) And reboot the node. (Reboot)

You can check the parameter as mentioned below.

- Card View
- Maintenance Pane
- Loopback Pane
- Port pane on the card for which this is supported. (Mentioned in the bracket)

For 7.04 310MA

- DS1_28_DS3_EC1_3_LINE_CARD (DS3 Port)
- DS1_84_DS3_EC1_3_LINE_CARD (DS3 Port)

15454

- DS3XM_LINE_CARD (DS3)
- DS3XM12_LINE_CARD (DS3)
- DS3I_LINE_CARD (DS3I)
- DS3E_LINE_CARD (DS3)
- DS3_EC1_48_LINE_CARD (DS3 & EC1 Port)

DS1_E1_56_LINE_CARD (You can see these values on loopback pane itself)

CSCsi04127

When you upgrade nodes from R6.22 to R7.0.4, BITS-1 IN, BITS-2 IN, BITS-1 OUT, and BITS-2 OUT go into In-Service (IS), although the R6.2.2 line-timed nodes have all the BITS facilities set to Out-of-service (OOS), before the upgrade. This issue is resolved in Release 7.05 and 7.23.

CSCsi46648

The port labeling on the 15310 DS1 circuit is inconsistent with the DS1 labeling on the 15454 DS1 circuit.

In case of DS1 circuits created using DS1_84_DS3_EC1_3_LINE_CARD and DS1_28_DS3_EC1_3_LINE_CARD in 15310 MA the DS1 port information is displayed differently in the circuit table.

Workaround: The DS1 port information can be derived using the port and vt information displayed.

pDS1(1-28)/S1/V1-1 => port 1 (1-1 is the first port in the 1-28 range)

pDS1(1-28)/S1/V2-1 => port 2

pDS1(1-28)/S1/V7-4 => port 28 (last vt)

pDS1(29-56)/S1/V1-1 => port 29 (1-1 is first port in the 29-56 range)

The 28 VT 1.5s (DS1s) in each port range are in this order.

1-1, 2-1, ... 7-1, 1-2, 2-2, ... 7-2, 1-3, ... 7-4

<vt-group> - <vt-channel> where vt-group is 1-7 and vt-channel is 1-4

The formula is DS1 Port num = (X*28) + vt-group + ((vt-chan-1) * 7)

where X = 0 for 1-28 range, 1 for 29-56 range and 2 for 57-84 range

This issue is resolved in Release 7.05.

Electrical IO Cards

CSCsd59042

When upgrading the software from Release 6.x.x to Release 7.x.x, the DS3 and EC1-12 cards fail to load if the node name begins with the letters FL. Changing the node name resolves this issue.

TL1

CSCsg22884

This bug is about retrieval of Far end Performance Monitoring values through TL1 on the 15310MA on the cards DS1-28-DS3-EC1-3 and DS1-84-DS3-EC1-84. Now these are retrievable through TL1.

Path Protection

CSCsh77496

If path protection/SNCP circuits are created while path defects are present on path protection/SNCP trunks, then sometimes path protection/SNCP circuits may not switch and traffic outage is observed

Workaround: Avoid creating path protection circuits while faults are present on either of the path protection trunk ports. This issue is resolved in 6.03, 7.05 and 7.2.3

Electrical IO Cards

CSCsg23089

SF LED is ON even when all the DS3 or DS1 ports are in IS_AINS state. Expected behavior is, SF LED should be on only in IS state and if any of IS port has any alarms on it. In all other states it should be OFF. It is made consistent with expected behavior.

CSCsi56959

DS3 unidirectional traffic goes down when reverting from 8.x, 7.05 or higher versions.

The issue can be reproduced as follows :

-
- Step 1** A unidirectional STS circuit is connected between any two DS3 port in 15310MA with WBE cards running 7.04 version.
- Step 2** The traffic is up.
- Step 3** An upgrade is made to 7.05 or 8.x versions and then downgraded to 7.04 version.
- Workaround 1:
- Once the downgrade to 7.04 is done, hard reset the WBE card in 310MA that has the source port of the unidirectional circuit. This brings back the traffic.

Workaround 2:

1. Delete unidirectional circuit after the downgrade is done.
2. Create and delete a bidirectional circuit on the same source and destination, once.
3. Create the unidirectional circuit on the same port.

This brings back the traffic.



Note

This issue is valid only if we see the signal coming out of the destination port of the unidirectional circuit having DS3-AIS. For any other DS3 failures, this issue may not be the valid root cause.

New Features and Functionality

The following feature has been added to the ONS 15310-MA for Release 7.0.2.

Daylight Savings Time Support

With Release 7.0.2 CTC and TL1 display daylight savings time (DST) in keeping with the new DST rules applicable from 2007 forward. As described in the change in energy policy for the United States of America (USA), the DST start date will be the 2nd Sunday of March and the DST end date will be 1st Sunday of November.

Related Documentation

Release-Specific Documents

- *Release Notes for the Cisco ONS 15310-CL Release 7.0*
- *Release Notes for the Cisco ONS 15310-CL Release 7.0.x*
- *Release Notes for the Cisco ONS 15454 SDH Release 7.0.x*
- *Release Notes for the Cisco ONS 15327 Release 7.0.x*
- *Release Notes for the Cisco ONS 15600 Release 7.0.x*
- *Release Notes for the Cisco ONS 15454 Release 7.0.x*

Platform-Specific Documents

- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*
Provides installation, turn up, test, and maintenance procedures
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*
Provides technical reference information for cards, nodes, and networks
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*
Provides a list of SONET alarms and troubleshooting procedures, general troubleshooting information, transient conditions, and error messages
- *Cisco ONS SONET TLI Command Guide*
Provides a comprehensive list of TLI commands
- *Cisco ONS SONET TLI Reference Guide*
Provides general information, procedures, and errors for TLI
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*
Provides software feature and operation information for Ethernet cards

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>

Use this document in conjunction with the documents listed in the “Related Documentation” section on page 8.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Copyright© 2007 Cisco Systems, Inc. All rights reserved.