



Release Notes for Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution, Release 1.0

December 1, 2005

These release notes include the following topics:

- [Solution Description, page 2](#)
- [Solution Components, page 3](#)
- [Important Notes, page 6](#)
- [Limitations and Restrictions, page 7](#)
- [Caveats, page 8](#)
- [Related Documentation, page 9](#)
- [Obtaining Documentation, page 10](#)
- [Documentation Feedback, page 11](#)
- [Cisco Product Security Overview, page 11](#)
- [Obtaining Technical Assistance, page 12](#)
- [Obtaining Additional Publications and Information, page 14](#)



Tip

Use this document online. This document provides hyperlinks to related documents and websites, including release notes for solution components and Cisco IOS images.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Document History

Document Version	Date	Notes
1	08/25/2005	This document was first published.
2	12/01/2005	DDTS CSCsc16554 is documented. See Open Caveats—Release 1.0, page 9 .

Solution Description

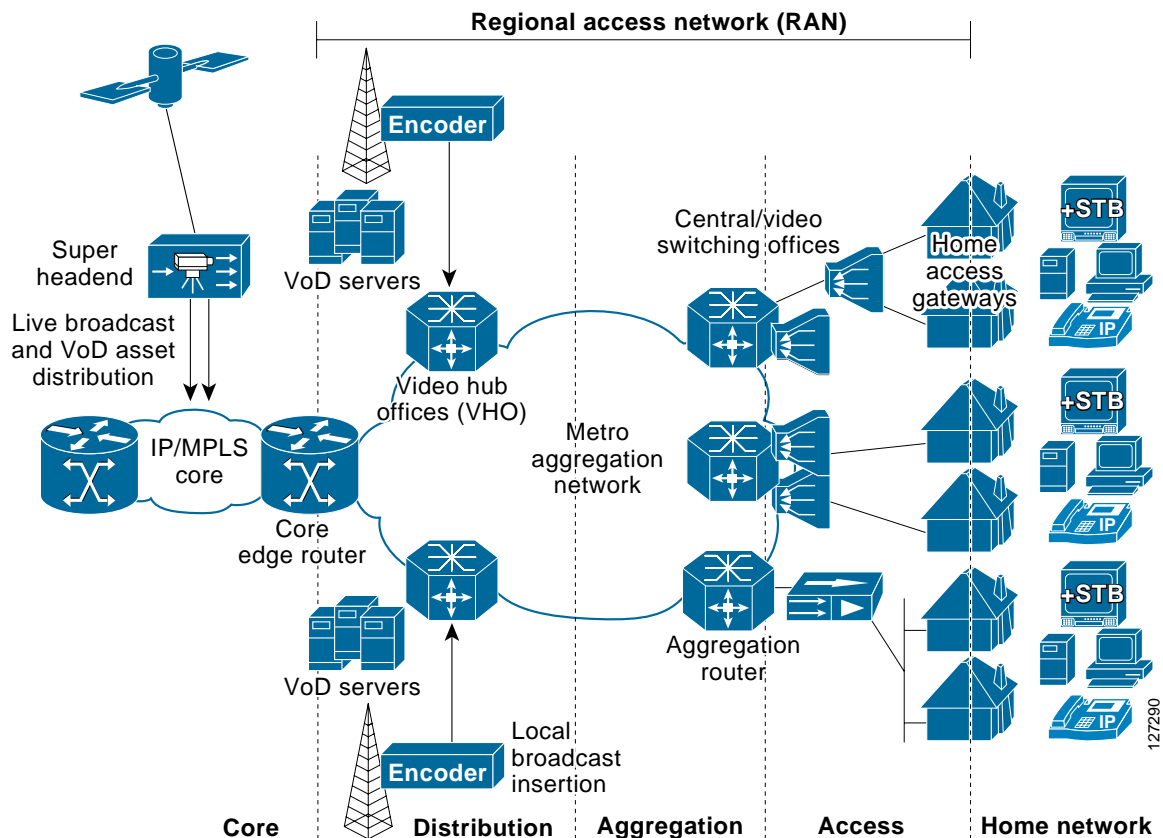
The Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband (GOVoBB) Solution, Release 1.0, supports IPTV, broadcast video, and video on demand (VoD) for the video over broadband/telco market, enabling operators that use digital subscriber lines (DSL) and fiber (FTTx) to offer not only video but also voice over IP (VoIP) and data (Internet access)—collectively referred to as “triple play”—over their existing infrastructure, now intelligently optimized for video service. (The solution assumes that Internet access is already available.)

[Figure 1 on page 3](#) presents a generic view of the Cisco GOVoBB Solution transport architecture. The solution uses a Gigabit-Ethernet (GE) transport network consisting of the following:

- A super headend (SHE), where live feeds for the broadcast video service are located
- A video headend office (VHO), where the video server complex resides
- A video switching office (VSO), where aggregation routers (ARs) that aggregate local or remotely attached GE DSLAMs are located

The regional access network, or RAN, consists of distribution, aggregation, and access layers. There is one SHE per region or network, and one VHE per metropolitan area. A distribution edge router (DER) provides transport for video traffic between the IP/MPLS core network and the VHO. The real-time encoder encodes and compresses analog signals. The VHO, in turn, is connected to the VSOs through one or more ARs. The customer premises equipment (CPE) consists of residential gateways, most commonly referred to as home access gateways, or HAGs.

Figure 1 Cisco GOVoBB Solution Transport Architecture: Generic View



Solution Components

Release 1.0 of the Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution features both Cisco and third-party components. Cisco components are listed in the following sections:

- [Cisco Hardware Components](#)
- [Cisco Software Matrix](#)

Third-party components are listed in [Important Notes, page 6](#).



Note

This solution is primarily for Cisco products. To establish and maintain the third-party products and applications that may be a part of the Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution, refer to the documentation provided by the vendors of those products.

Cisco Hardware Components

[Table 1](#) describes the Cisco hardware components tested for Release 1.0 of the Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution. Software releases that were tested for the solution are listed in [Table 2 on page 5](#).

**Tip**

When viewing this document online, the components in the Hardware columns of [Table 1](#) serve as links to the platform-specific user documentation. Refer to the release notes for each platform and software image that you use in this solution.

**Note**

Different applications of this solution may use different subsets of the following components.

Table 1 *Cisco Hardware Components*

Network Role	System	Product Number	Removable Optics
DER, AR	Catalyst switch	7609, 6509	
	Supervisor	WS-SUP720-3BXL	N/A
	10 GE x 4 optic	WS-X6704-10GE	XENPAK-10GE-LR
	1 GE x 24 optic	WS-X6724-SFP	1GE-SR/LR/DWDM
	1 GE x 16 DWDM optic	WS-X6816-GBIC	1GE-GBIC-DWDM-xxxx
	48-port copper Ethernet	WS-X6748-SFP	1GE-COPP-SR or -LR
	Switch	4948-10GE WS-4516-SupV	N/A X2-10GE-LR

See also [Related Documentation](#), page 9.

Cisco Software Matrix

[Table 2](#) is a matrix that describes the tested Cisco IOS and other software releases for Release 1.0 of the Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution. If you are implementing this solution for the first time, we recommend that you use the most recent software releases in [Table 2](#). If you have already implemented the solution in your network, use the entries in [Table 2](#) as options for upgrading your solution components.

[Table 2](#) also provides hyperlinks to release notes and the Cisco IOS Upgrade Planner from which you can download Cisco IOS images for Cisco components of the solution. See [How to Use the Cisco Upgrade Planner](#), page 5.

Before you select a Cisco IOS image, do the following:

- Select a feature set. Consult with your Cisco account representative to determine the Cisco IOS features that are required for your installation.
- Check the release notes for the platform and software release for flash and DRAM memory requirements.

**Tip**

If you view this document online, some of the components in the first column of [Table 2](#) serve as links to the platform-specific release notes. The software release names in the rest of the table serve as links to the Cisco IOS Upgrade Planner from which you can download the Cisco IOS images.

Table 2 *Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution, Release 1.0, Software Matrix*

Component	Cisco Release Tested for This Solution
Cisco Catalyst 6500 series switches	Cisco IOS Release 12.2(18)SXE
Cisco 7609 router	
Cisco Catalyst 4500 series switches, including Cisco Catalyst 4948-10GE	Cisco IOS Release 12.1(25)EWA

How to Use the Cisco Upgrade Planner



Note You need a Cisco.com password and user ID to access the Cisco IOS Upgrade Planner.

- Step 1** To access the Cisco IOS Upgrade Planner, complete one of the following steps:
- Within the online version of these release notes, click the release version in [Table 2](#), and launch the Cisco IOS Upgrade Planner.
 - Go to <http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?>, and launch the Cisco IOS Upgrade Planner.
- Step 2** Select the platform name from the Select Platform column in the Choose Options window.
- Step 3** Go to the Select Release column and find the heading Early Development Updates.
- Step 4** Search for the release name that corresponds with the name in the Cisco Releases Tested for This Solution column in [Table 2](#).
- Step 5** Click the link for that release. The Cisco IOS Upgrade Planner is refreshed.
- Step 6** Read all instructions on the page, then click the appropriate software feature in the Select Software Feature column. The Cisco IOS Upgrade Planner is refreshed.
- Step 7** Read the information on that page. If you agree with the requirements, click **I Agree**. The Cisco IOS Upgrade Planner is refreshed.



Caution Make sure that you have enough memory on your system for the file. Note the values in the Minimum Memory and Minimum Flash columns in the File Download Information table.

- Step 8** Read all instructions on that page, then click the filename of the binary image in the Download: line.
- Step 9** Continue as prompted.

Important Notes

Third-Party Components



Note

While third-party components are tested for interoperability in this solution, they are not supported as part of this solution. Configurations relevant to the transport network are documented in the *Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution Design and Implementation Guide*. Refer to third-party documentation for configuration of third-party equipment.

Table 3 lists third-party components of the solution.



Note

For the most current information, contact your Cisco account representative, visit the manufacturer’s website, or contact the manufacturer’s representative.

Table 3 *Third-Party Components*

Network Role	Vendor	System	Product Number
DSL switch	Ericsson	Ethernet DSL Access ECN320	FAB 801 3908
DSLAM		EDN312xp, version R3, revision R1A, ADSL2, ADSL2+	FAB 801 4246
Home access gateway (HAG)		HM340d, version 2, ADSL2 CPE modem	ZAT 759 94/A101
VoD server	Kasenna	GB Media Server	GB-MS-BASEA-LB GB-MS-GIGE-COP
Application server		Living Room Application Server	LR-VSIF-HWSW
IP STB	Amino	STB	110

Third-Party Hardware and Software Requirements

Special Issues in Using DSL Equipment

If you are using Ericsson DSL equipment, see Appendix D, “Using Ericsson Equipment,” in the *Cisco Gigabit Ethernet-Optimized IPTV/Video over Broadband Design and Implementation Guide*.

Limitations and Restrictions

IGMP Versions

According to RFC 3376, Internet Group Management Protocol (IGMP) version 3 is backwards compatible with IGMP versions 1 and 2. The Cisco switches in the solution were verified to support IGMP clients of IGMP versions 2 and 3 on the same aggregation VLAN. At the time of this writing, Ericsson DSL equipment does not support IGMP version 3, and so does not respond to IGMPv3 messages. Those messages are discarded, and the broadcast is therefore not played through the STB. Also, if the Cisco switch sends IGMPv3 queries to the DSLAM and they are discarded, a membership report is not sent to the Cisco switch. The switch, believing that there are no clients for the multicast group, stops forwarding the multicast group.

Consequently, Cisco switches connected to the Ericsson 320 switch must send IGMP version 2 commands to the Ericsson equipment. However, the solution requires IGMPv3 to be used on the switches.

The workaround is to ensure that the port that is connected to the Ericsson ECN 320 uses IGMPv2. (This is the default if no IGMP version is specified by means of a CLI command.) The Cisco switch then converts the IGMPv2 messages to version 3 when communicating with other Cisco switches in the network, while all messages sent to the Ericsson equipment use version 2.



Note

IGMP with SSM mapping on the Cisco switches provides a transitional step between IGMPv2 and IGMPv3. Although the current Ericsson gear does not allow both IGMPv2 and IGMPv3 clients to exist on the same network, the Cisco switches allow both to exist in the same aggregation VLAN. This supports a “cap and grow” scenario for deployments. Clients of both versions can coexist on the same VLAN and join different groups or the same multicast group.

SSM Mapping Configuration

The following Cisco implementation guide states that IGMP SSM must be configured on all edge switches that process IGMP messages:

- *Source Specific Multicast (SSM) Mapping*

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gtssmma.htm

SSM functions fine with this recommendation, but testing showed that enabling SSM on all switches in the network decreased the jitter in the reconvergence times. The minimum reconvergence times were a little larger with the latter configuration, but more predictable because there was less jitter.

Anycast Functionality

Anycast provides multicast redundancy of multicast streams in the Cisco network. Two multicast sources are configured with identical source and destination IP addresses, but reside on different locations in the network. The edge router builds the reverse path tree to the closest source by means of the Interior Gateway Protocol (IGP) routing table. When the IGP detects a topology change, the edge router builds

a new tree to the next closest source. This functionality works well on the Cisco switches, but requires third-party features to provide full functionality. For example, the Cisco network is not able to recognize a loss of video baseband or asynchronous serial interface (ASI) input to the IP encapsulator.

Incremental OSPF

On the Cisco Catalyst 4000 series switches, commands are available to configure incremental Open Shortest Path First (OSPF) under the OSPF process configuration. However, this feature is not completely supported by the Cisco Catalyst 4000 series, and incorrect routing tables may be witnessed when the anycast feature is used. To avoid this problem, it is recommended that incremental OSPF not be configured in this solution.

Ericsson Version Recommendation

During solution testing the Ericsson EAN, detailed in Appendix D of the *Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution Design and Implementation Guide*, exhibited an unacceptable number of packet drops between the DSLAM and HAG. When the EAN was upgraded to the version listed in that appendix, the packets drops were no longer witnessed. Contact Ericsson to obtain the latest software releases for all of the Ericsson equipment.

Caveats

This section lists the key caveats for the components in this solution. Workarounds are provided where applicable.



Note

For additional caveats that may affect this solution, refer to the release notes for each platform and software release that you use as a solution component. If you view this document online, the software release numbers in [Table 2 on page 5](#) serve as links to the platform-specific release notes.

If you have an account with Cisco.com, you can use the Bug Toolkit to find to find caveats of any severity for any release. To find the open caveats for Cisco components used in this solution, you must query the system for each of the component and software releases used or being planned for your network. To reach the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats—Release 1.0

- CSCef28346—Long IGMP join latencies for multicast with the Cisco Catalyst 6000 series and Sup 720 have been seen with Cisco IOS Release 12.2(18)SXE.

Workaround—Use static joins, as described in “Effect of Multicast on Channel-Change Performance,” in Chapter 3, “Solution Transport Architecture,” of the *Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution Design and Implementation Guide*.

- CSCsa98252—UDLR is not functional after a reload.

In the 1-GE topology, UDLR may not be functional on the Cisco Catalyst 4000 series after a reload or power cycle. This is related to ARP requests and responses during bootup. The Cisco Catalyst 4000 series sometimes fail to respond successfully, and the upstream switch considers the unidirectional link to be down. The link can be activated by pinging across the unidirectional link.

Workaround—Configure the upstream switch with static ARPs for the endpoint of the unidirectional link on the downstream Cisco Catalyst 4000 series switch.

- CSCsc16554—When the IGMP limit (state limit) feature is used with Source Specific Multicast (SSM) and source mapping, the feature does not work under all conditions.

When SSM is used and the client supports only IGMP version 2, source mapping is required. IGMPv2 messages cause the active group counter to increment properly. However, when the receiver sends an IGMPv2 leave message to the router, the active group counter (set by the **ip igmp limit** command) does not decrement. Consequently, all subsequent IGMP joins are denied.

Workaround—There is no workaround.

Related Documentation

Solution Documentation

This document, and the *Cisco Gigabit-Ethernet Optimized IPTV/Video over Broadband Solution Design and Implementation Guide*, are available under the following URLs:

<http://www.cisco.com/univercd/cc/td/doc/solution/vobbsols>

http://www.cisco.com/en/US/netsol/ns524/networking_solutions_market_segment_solutions_home.html

Cisco Catalyst 6500 Series Switches

Documentation resources for the Cisco 6500 series switches are available at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>

Cisco Catalyst 4500 Series Switches

Documentation resources for the Cisco Catalyst 4500 series switches, including the Cisco Catalyst 4948-10GE, are available at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm>

Cisco 7609 Router

Documentation resources for the Cisco 7609 router are available at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/index.htm>

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

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

Beginning June 30, 2005, 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/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Instructions for ordering documentation using the Ordering tool are at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

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 send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—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.

- 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 to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.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.htm

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

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)—Your 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 operation 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 your network is impaired, but 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.

- 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 [Related Documentation, page 9](#).

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

