

Release Notes for Cisco Media Gateway Controller Node Manager, Version 2.6.1

Cisco Media Gateway Controller Node Manager (Cisco MGC Node Manager) is an element management system (EMS) for Cisco Media Gateway Controller Node, a call control node based on the Cisco PGW 2200 Softswitch. Cisco MGC Node Manager provides basic management of the Cisco Media Gateway Controller Node devices including fault, configuration, performance, and security.

These release notes provide:

- [New Features, page 2](#)
- [System Requirements, page 4](#)
- [Supported Configurations, page 5](#)
- [Product Documentation, page 5](#)
- [Software Requirements, page 6](#)
- [Supported Network Elements, page 7](#)
- [Installation Procedure Checklist, page 7](#)
- [Upgrade Procedure Checklist, page 8](#)



REVIEW DRAFT—CISCO CONFIDENTIAL

- [Patch Procedure Checklist, page 9](#)
- [Deinstallation Procedure, page 9](#)
- [Known Issues and Operational Recommendations, page 10](#)
- [Resolved Problems, page 11](#)
- [Hints and Tips, page 11](#)
- [Troubleshooting, page 14](#)
- [Obtaining Documentation, page 19](#)
- [Documentation Feedback, page 20](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 22](#)

New Features

This release of Cisco Media Gateway Controller Node Manager (CMNM) contains the following new features:

- Support for receiving, processing, displaying, and forwarding the following traps:
 - LCM: Invalid destination for RO/PR routing number
 - LCM: No response from Call Instance
 - CTI connection failure
 - CTI version mismatch
- Support for discovering and displaying call limiting related configuration data in PGW 9.6(1)
- Support for new external node CCM Cluster, CTI trunk group, and CTI route trunk group
- Support for the new component types: CTI sigpath, CTI manager, and AXL server
- Support for CALL and LABEL performance measurement

REVIEW DRAFT—CISCO CONFIDENTIAL

This package also includes the existing features of the previous release, that is CMNM2.5.2 .

Features in the Previous Versions

Version CMNM2.5.2 Package

Following are the features for the CMNM 2.5.2 package

- Support for receiving, processing, displaying, and forwarding the traps.
- Support for SIP Service Fail Over, Tariff Table Access Failures, Charge Rate Table Access Failure
- Support for receiving traps regardless of whether they come from primary or back-up interface.
- Support for user query for ANNOUNCEMENT, trunkgroup, sigpath properties the new Trunkgroup, DPNSS, sigpath properties as required in the design specification.
- Support for result type BNBRMODMWI
- Implementation of Virtual IP feature.
- Support for new MML component, Basic Rate Interface signalling services.
- Support for new parameters subunit, tcplnk in D Channel provisioning
- Provision of Donzi, in discovery and GUI display.
- Provision of H323AdjunctLink as a sigpath property.
- Support for CALL, SIPSP, ISUP and sigpath performance measurement.

Version CMNM2.4.1 Package

Following are the features for the CMNM 2.4.1 package

- Support for ssh/sftp usages on PGW/BAMS/HSI
- Support for new and modified MML components for 2.4(1)
- Support for SGP and Association performance measurement
- Support for Farm deployment, seedfile and related functions
- Support for Switch deployment changes as required in design specification.

REVIEW DRAFT—CISCO CONFIDENTIAL

- Support for ssh/sftp usages on PGW boxes
- Inclusion of existing features from the earlier release CMNM2.3(2).

**Note**

Stand-alone SLT does not support ssh as its deployment template does not have security policy option.

System Requirements

The following is the minimum hardware and software you need to install and run Cisco MNM:

- Sun Fire 280R (UltraSPARC III) supporting two hard drives in a single rack-mount package; other Sun platforms in the UltraSPARC II and III families are also supported (two CPUs at 440 MHz or faster)
- Sun Solaris 8 operating system
 - April 2001 release recommended
 - Open Windows with the Common Desktop Environment (CDE)
- 2.0 GB of RAM (or greater)
- Properly configured 9 GB SCSI drives. The database drives should be configured as raw devices and connected to a separate SCSI controller for maximum performance.
- The tmpfs file system must be mounted to /tmp for maximum performance.

Detailed system requirements are documented in Chapter 1 of the Cisco MGC Node Manager Installation Guide at http://www.cisco.com/en/US/products/sw/netmgtsw/ps1912/products_user_guide_list.html.

Review this chapter prior to installing or configuring the software.

REVIEW DRAFT—CISCO CONFIDENTIAL

**Note**

Installing drives greater than 9 GB does not result in performance gains. The main bottleneck of the CEMF application is hard disk input/output (i/o) speed, not capacity. Maximum performance is achieved using many drives of lower capacity instead of a few, larger capacity drives.

Supported Configurations

These configurations are supported:

- Cisco MGC Node Manager and Cisco VSPT installed together on a network management server. (Recommended)
- Cisco MGC Node Manager installed on a network management server and Cisco VSPT installed on a Cisco PGW host machine.
- Cisco MGC Node Manager installed on a network management server and Cisco VSPT installed on a separate server.

**Note**

Other element managers may be installed on the network management server.

**Caution**

Cisco MGC Node Manager should not be installed on a Cisco PGW 2200 host machine.

Product Documentation

[Table 1](#) describes the product documentation that is available.

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 Product Documentation

Document Title	Available Formats
<i>Release Notes for Cisco Media Gateway Controller Node Manager Version 2.6.1.</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/
<i>Installation [and Configuration Guide] for Cisco Media Gateway Controller Node Manager Version 2.6.1.</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/
<i>User Guide for Cisco Media Gateway Controller Node Manager Version 2.6.1.</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/
Online help	<ul style="list-style-type: none"> Online help in HTML format is packed along with the product CD-ROM.

Software Requirements

Following are the requirements for installing the CMNM

- Server/Client: Solaris 2.6 or 2.8
- cemf 3.2 build 136
- cemf patch
/auto/nonvobs/packages/AccessVision/CEMF-3.2-P-07-RELEASE
- cemf patch
/auto/nonvobs/packages/AccessVision/CEMF-3.2-P-07.1-RELEASE
- perl ssh pkg: /users/scotttere/CEMF-SSH-ADDON-0.1.tar.Z

REVIEW DRAFT—CISCO CONFIDENTIAL

Supported Network Elements

This release provides support for the following network elements. These network elements have been tested and verified to work with this release of the Cisco CMNM.

- PGW2200: 7.4(11), 7.4(12), 9.1.4(T), 9.1.5, 9.2.2, 9.3.1, 9.3.2, 9.4.1, 9.5(2), 9.6(1)
- Billing and Measurement Server (BAMS): 2.63, 2.64, 2.65, 2.67i, 2.68, 3.10, 3.11, 3.20
- Catalyst 5500 (5.x)
- Catalyst 2900XL (12.x)
- Catalyst 2600 (12.1(x), 12.2(x))
- Catalyst 6509
- HSI adjunct (2.20, 2.21, 4.1)
- Eldora (5400 & 5350) 12.2(10.6)T

Installation Procedure Checklist

Before installing the software, make sure you read the section, "Installing CMNM (Chapter 2) in the Cisco MGC Node Manager User's Guide. If you are setting up a Client/Server architecture, then the CEMF and CMNM software must be installed on both the Client and Server workstations. The CMNM installation software will determine whether the Client or Manager software should be installed.

Verify the Minimum hardware requirements pertaining to your site have been met.

Check to see if the computer is in DNS. If it is using DNS, the computer must have a valid entry in DNS and if it is NOT using DNS, then you must disable Name Resolution completely (that is, no /etc/resolv.conf file).

Verify the Cisco Element Management Framework (CEMF) software has been installed and is running (the CEMF software *must* be running for the Cisco MGCM software to be installed).

REVIEW DRAFT—CISCO CONFIDENTIAL



Note See the "Installing CMNM" section in the "Cisco Media Gateway Controller Node Manager Users's Guide" for detailed instruction on how to mount the CD-ROM.

-
- Step 1** Become the "root" user
 - Step 2** Place CMNM installation media in the CD-ROM drive
 - Step 3** Change to the `"/cdrom/cdrom0"` directory
 - Step 4** Execute the command `./cmmninstall`
 - Step 5** Follow the on-screen prompts
 - Step 6** Eject the CD-ROM when the installation is complete.
-

Upgrade Procedure Checklist

The Cisco MGC Node Manager upgrade process enables you to easily upgrade from earlier releases.

-
- Step 1** Become the "root" user
 - Step 2** Place Cisco MGC Node Manager CD in the CD-ROM drive.
 - Step 3** Change to the `"/cdrom/cdrom0"` directory.
 - Step 4** Execute the command `./installcmmn -upgrade`.
 - Step 5** Follow the on-screen prompts.
 - Step 6** Eject the CD-ROM when the installation is complete.
-

REVIEW DRAFT—CISCO CONFIDENTIAL

Patch Procedure Checklist

The Cisco MGC Node Manager patch process is cumulative. Downloading and installing the latest patch installs all previous patches. The patch process automatically determines which portions of the Cisco MGC Node Manager need to be patched. In order for you to install a patch, the base Cisco MGC Node Manager software must be installed. Use the following steps to install the desired patch.

-
- Step 1** Verify that the base Cisco MGC Node Manager software is installed.
 - Step 2** Become the root user.
 - Step 3** Create a temporary installation directory `"/opt/cmmn_tmp_install"`.
 - Step 4** Download the patched software:
 - a. Go to www.cisco.com.
 - b. Log in.
 - c. Navigate to Technical Support > Software Center > Products and Downloads > Voice Software. On this page find and click on Cisco Media Gateway Controller Node Manager. You go to the patch download page.
 - d. Download the desired patch to the temporary installation directory.
 - Step 5** Extract the patched software. For example, you can use:

```
zcat CSC0cmmnPatch_0x.tar.Z | tar xvf -
```
 - Step 6** Execute the command: `./cmmninstall`
 - Step 7** Follow the on-screen prompts.
-

Deinstallation Procedure

Following is the procedure for deinstallation.

-
- Step 1** Login as root.
 - Step 2** Become the "root" user

REVIEW DRAFT—CISCO CONFIDENTIAL

- Step 3 Place CMNM installation media in the CD-ROM drive
 - Step 4 Change to the `"/cdrom/cdrom0"` directory
 - Step 5 Execute the command `./cmnminstall -r`
 - Step 6 Follow the on-screen prompts
 - Step 7 Eject the CD-ROM when the uninstallation is complete.
-

Known Issues and Operational Recommendations

This section contains information about known issues and the corresponding workarounds.



Note

For more information about Cisco IOS issues and workarounds, see the Cisco IOS release notes for your platform.

Cisco MGC Node Manager Checks for Available Disk Space For Installation

During installation, Cisco MGC Node Manager detects how much disk space is available for installation. If the system does not have enough available disk space, you are prompted whether you want to continue the installation routine. If you enter 'N' to stop the Cisco MGC Node Manager installation, the installation continues.

The workaround is to ensure that enough free disk space is available before Cisco MGC Node Manager is installed. The amount of disk space required is detailed in the Cisco MGC Node Manager installation guide.

REVIEW DRAFT—CISCO CONFIDENTIAL

Cisco MGC Node Manager Cannot Discover an Interface or IP Address for BAMS

Sometimes Cisco MGC Node Manager reports that it cannot discover an interface or IP address for BAMS. This might be caused by the mib2agt getting into a strange state. You can restart the mib2agt by stopping the current process. The new process mib2agt is restarted automatically.

```
ps -ef | grep mib2agt
kill -9 <PID>
```

Resolved Problems

The following table describes problems resolved since the last release of Cisco Media Gateway Controller Node Manager.

Table 2 *Resolved Problems in Cisco Media Gateway Controller Node Manager Version 2.6.1*

Bug ID	Summary
CSCeg57477	mgcController restarts after getting SLT MTP2 channel properties
CSCeg32709	CMNM cannot log in to router when login local and ip domain-look up (not clear, check with Selin))

Hints and Tips

Initial Cisco MGC Node Manager Configuration

Cisco MGC Node Manager is initially configured with one user:

```
id: admin
password: admin
```

Installing CEMF/Cisco MGC Node Manager on a Server

If you have installed CEMF/Cisco MGC Node Manager on a server and need to change the IP address/hostname, you must make the changes shown in the following procedure:



Note The following example uses the hostname CMNM and the IP address 10.1.1.1.

Step 1 `#cd <CEMF Directory>/bin`

Step 2 `#./cemf stop`

Step 3 Edit `"/var/adm/Atlantech/system/info"` to reflect the following hostname and ip address:

```
MGRHOSTNAME=rambler
MGRIPADDRESS=10.1.1.1
COREHOSTNAME=rambler
```

Step 4 Edit `"<CEMF Directory>/config/env/avCore.sh"` to reflect the hostname in the lines below, and save the file.

```
MgrSystemManager=rambler1270; export MgrSystemManager
PortAllocator=rambler1270; export PortAllocator
transRouter=rambler1271; export transRouter;
```

Step 5 Edit `"/var/sadm/pkg/CSCOcemfm/pkginfo"` to reflect the following values:

```
MGRIPADDRESS=10.1.1.1
MGRHOSTNAME=10.1.1.1
COREHOSTNAME=10.1.1.1
LOCALHOSTNAME=10.1.1.1
```

Step 6 You will also need to make these same changes for each Element Manager. To do so, edit the following files:

```
/var/sadm/pkg/hostEM/pkginfo
/var/sadm/pkg/mgcEM/pkginfo
```

REVIEW DRAFT—CISCO CONFIDENTIAL

Step 7 Rename "<CEMF Directory>/ODI/OS5.1/ostore/<hostname>_server_parameter" to reflect the new hostname.



Note You must obtain a new CEMF license. For information on obtaining a new CEMF license, refer to "CEMF Licensing" in the "Troubleshooting" section.

Step 8 Type `<CEMF Directory>/bin/cemf start`

Configuring the CEMF Software for Maximum Performance

The following are guidelines for installing CEMF:

- Use the primary drive for the Solaris operating system and the ObjectStore transaction log.
- The second drive should contain the CEMF software (that is, /opt/cemf).
- Configure the ObjectStore database for Raw File Systems. The remaining hard drives should contain the RAW File System partitions for the CEMF database (preferably on a separate SCSI controller).

Mount the tmpfs file system to /tmp so the ObjectStore cache files can be kept in memory. ObjectStore is the database program included with CEMF. Keeping the cache files in memory provides for an enormous performance boost for CEMF. Here is how the tmpfs line should read in the /etc/vfstab file (the blank areas between the keywords are spaces):

```
swap - /tmp tmpfs - yes -
```

Troubleshooting

Viewing Core Files Generated by CEMF and Cisco MGC Node Manager

Use the `"/opt/cemf/bin/listCores"` command to view all core files generated by CEMF and Cisco MGC Node Manager.

CEMF Licensing

If you are having problems with CEMF licensing, you might need to stop and restart the license manager daemon. To do so, execute the following commands:

```
#> /etc/rc2.d/S98alvm stop
#> /etc/rc2.d/S98alvm start
```

**Note**

The CEMF licenses are fixed for a particular machine. You cannot copy the license file from one machine to another. If you want to install the CEMF software on another machine, you must contact Cisco TAC and ask for a new license. You will need the hostname and hostid of the new machine.

Viewing the Most Recently Changed Log Files

Cisco MGC Node Manager log files are stored in `<CEMF Directory>/logs`. You can view the most recently changed log file with `ls -lt` command.

Cisco MGC Node Manager Log Files

Some Cisco MGC Node Manager log files are:

- `hostController.log` [MGC Host]
- `mgcController.log` [MGC Node]
- `trapLog.log` Incoming traps are logged here, to separate them from CEMF log messages collected in `mgcTrapProcessor.log`.

REVIEW DRAFT—CISCO CONFIDENTIAL

Error Messages That Are Safe to Ignore

Most of the entries in the Cisco MGC Node Manager log files are created by the CEMF platform and are of limited value. The following error messages are safe to ignore:

- SNMP and MIB parsing errors (which display when an EM controller starts):
 - SNMP : ERROR mib.cc:1283 Mib Object is already on the tree for
 - SNMP : ERROR mibDependencyMgr.cc:191 mibDependencyMgr.cc:196 Mib . not defined
 - SNMP : ERROR mibParser.y:359 EXPORTS are currently ignored (, line 8)
 - SNMP : WARN mibParser.y:1154 Name and number form OIDs are not properly implemented ().
- Database warning (which display when an EM controller is first installed):
 - general : WARN Creating Database /opt/AV3/db/mgcController.db
- General errors (which display when the EM controller starts up):
 - general : ERROR Unable to get event channel ID for channel ' '
 - general : ERROR EventChannelManager : Failed to find location for event channel
 - general : WARN OGManager::OGManager - Unable to get deleteEventChannel from .ini file
 - general : ERROR OGManager::processGroupClass - invalid class id
 - general : ERROR EventChannelManager : Failed to find location for event channel ERROR OGManager::processGroupClass - invalid class id
 - general : ERROR OGChangeEventHandler::process - could not find drep!
 - general : ERROR IdAllocatorOS : Deprecated constructor called
 - Task : WARN PerfPollTask::createGroupsResult : group . already exists.
 - mgcController : WARN Controller::initialiseController Controller is configured NOT to auto populate tech tree on autodiscover
- Other miscellaneous errors:
 - general : WARN CommsBuffer::serialize - resizing buffer size

REVIEW DRAFT—CISCO CONFIDENTIAL

- general : ERROR PersistentAttributeStore::PersistentAttributeStore() nameInit = 'xxx. is longer than 16 characters. All Objectstore segment comments will be truncated to use the first 16 characters.

Resetting the User Password

If you forget your password, you can reset the CEMF user IDs and passwords. The following command removes all passwords, and resets the admin user ID's password to administrator.

```
<CEMF Directory>/bin/cemf shell
<CEMF Directory>/bin/partitioningTool -r
```

Backing Up and Restoring the CEMF/Cisco MGC Node Manager Databases

The following command backs-up the CEMF/Cisco MGC Node Manager databases. By default the backup files are placed in /opt/AVBackup.

```
/opt/CSC0cemf/bin/cemf stop
/opt/CSC0cemf/bin/cemf backup
/opt/CSC0cemf/bin/cemf start
```

The following command will restore a CEMF/Cisco MGC Node Manager database.

```
/opt/CSC0cemf/bin/cemf stop
/opt/CSC0cemf/bin/cemf restore -t mm-dd-yyyy
/opt/CSC0cemf/bin/cemf start
```

For more information on backing up and restoring CEMF/Cisco MGC Node Manager Databases refer to the "Cisco EMF Database Backup and Restore Procedures" section of the Installing, Licensing, and Configuring Cisco EMF Manual.

REVIEW DRAFT—CISCO CONFIDENTIAL

Forcing an Uninstall of an Element Manager

The CEMF daemons must be running for the Element Managers (EMs) to uninstall. There are two ways to force an uninstall of an EM; both cause loss of all CEMF/Cisco MGC Node Manager data. Before running these commands, it is recommended that you back up your databases.

The `uninstallCSCOcmnm` script can be invoked with an undocumented option to force the removal of all or one EM. From a command line, as root, type the command:

```
/opt/CSCOcemf/uninstall/uninstallCSCOcmnm -force [-em <EM>]
```

You can specify only one EM to remove or all EMs by omitting that parameter. The list of EMs includes `hostEM`, `mgcEM`, and `mgxEM`.

Example:

```
/opt/CSCOcemf/uninstall/uninstallCSCOcmnm -force -em mgxEM -em mgcEM
```

After you run this command, the CEMF databases are corrupted. To correct this problem, reset the CEMF databases by running the following command. You must do this before using CEMF again, even using CEMF to reinstall Cisco MGC Node Manager.

```
/opt/CSCOcemf/bin/cemf stop  
/opt/CSCOcemf/bin/cemf reset  
/opt/CSCOcemf/bin/cemf start
```

After you have successfully reset the database and restarted CEMF, you must reinstall Cisco MGC Node Manager. If you want to restore a CEMF/Cisco MGC Node Manager database after you have reinstalled Cisco MGC Node Manager, refer to "Backing up and restoring the CEMF/CMNM Databases" in the preceding section.

If the above method does not remove the EMs, then you can try another method. When the EMs are installed, Solaris package information is placed in subdirectories of `/var/sadm/pkg`. The subdirectory is the name of the package, as specified above (that is, `hostEMm`, `mgcEMm`, and so on). As the root user, complete the following steps for each EM that you want to remove.

REVIEW DRAFT—CISCO CONFIDENTIAL

```

/opt/CSC0cemf/bin/cemf stop
touch /var/sadm/pkg/<EM>/install/.avload
pkgrm <EM>
/opt/CSC0cemf/bin/cemf reset
/opt/CSC0cemf/bin/cemf start

```

Example:

```

/opt/CSC0cemf/bin/cemf stop
touch /var/sadm/pkg/mgcEMm/install/.avload
pkgrm mgcEMm
/opt/CSC0cemf/bin/cemf reset
/opt/CSC0cemf/bin/cemf start

```

To restore a CEMF/Cisco MGC Node Manager database after you have reinstalled Cisco MGC Node Manager, refer to the preceding "Backing Up and Restoring the CEMF/CMNM Databases".

Managing Network Devices Over a Slow Link

If you are managing network devices over a slow link (T1 or slower), you might need to alter SNMP parameters used by Cisco MGC Node Manager for SNMP Get Requests. You can change these parameters for any existing objects by accessing the States dialog. You can also change these parameters in the Advanced tab of the Seed File Deployment dialog.

The default number of SNMP retries is 2. You might need to increase this value when the Cisco MGC Node Manager workstation is connected to network devices over a slow link.

The default SNMP timeout value is 5000 milliseconds (5 seconds). You may need to increase this value when the Cisco MGC Node Manager workstation is connected to network devices over a slow link.

REVIEW DRAFT—CISCO CONFIDENTIAL

Maximizing Logfile Output

By default Cisco MGC Node Manager logs only warning and error messages. If you want to turn on debug messages in all log files, complete the following steps, as the root user:

-
- Step 1 **cd <CEMF Directory>/bin**
 - Step 2 Type **./cemf stop**
 - Step 3 **cd <CEMF Directory>/config/init**
 - Step 4 Edit loggercommon.include and add or change the following line:
loggingLevelMask = 12
 - Step 5 **cd <CEMF Directory>/bin**
 - Step 6 Type **./cemf start**
 - Step 7 Add r change the following line to set the logging level back to warning,
loggingLevelMask = 10
-

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/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

REVIEW DRAFT—CISCO CONFIDENTIAL

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

- 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 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on

REVIEW DRAFT—CISCO CONFIDENTIAL

Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support 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>

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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

REVIEW DRAFT—CISCO CONFIDENTIAL

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, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>

REVIEW DRAFT—CISCO CONFIDENTIAL

- *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>

- *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>

- 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 “” section.

REVIEW DRAFT—CISCO CONFIDENTIAL

CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, Networking Academy, Network Registrar, *Packet*, 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. (0705R)

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