



Release Notes for the Solaris 2.5(1) and 2.6 Packages

June 26, 2007

Contents

- [Introduction, page 2](#)
- [Determining Which Solaris Release Version is Loaded on Your System, page 2](#)
- [Solaris Packages, page 3](#)
- [Volume Manager, page 3](#)
- [Log and Spool File Systems, page 4](#)
- [Solaris 2.x Patch Cluster, page 4](#)
- [System Security Patch, page 6](#)
- [Installation, page 7](#)
- [Patch Installation and Upgrade, page 7](#)
- [Solaris Patch CSCOh007 Modification History, page 9](#)
- [Solaris Patch CSCOh008 Modification History, page 10](#)
- [Solaris Patch CSCOh013 Modification History, page 10](#)
- [New Features and Featurettes, page 10](#)
- [Known Issues and Operational Recommendations, page 11](#)
- [World Wide Web, page 11](#)
- [Documentation CD-ROM, page 11](#)
- [Ordering Documentation, page 12](#)
- [Documentation Feedback, page 12](#)
- [Cisco.com, page 12](#)



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

Copyright © 2003. Cisco Systems, Inc. All rights reserved.

- [Technical Assistance Center, page 13](#)

Introduction

This document describes the Solaris patches for the Cisco Media Gateway Controller (MGC) software. These packages might be required as a part of the installation procedures for the following products running on the Solaris 2.6 platform:

- SC2200—all systems running Solaris 2.6 through release 7.4(12).
- PGW 2200—all systems running Solaris 2.6 through release 9.1(5).



Note

For information on application and installation of the Sun Solaris patches, refer to the *Cisco Media Gateway Controller Software Release (7 or 9) Installation and Configuration Guide*.

The currently deployed Solaris patch set is release 1.0(9).



Caution

To maintain tested configurations, do not download packages directly from the Sun website. Although Sun's website may contain later patch versions, you should only apply patches that are provided by Cisco via CD or CCO.

Determining Which Solaris Release Version is Loaded on Your System

To determine the Solaris release version of a patch that is installed on your system, use the following command:

pkginfo -l <package instance>

The following shows an example of the **pkginfo** command.

```
hostname% pkginfo -l CSCOh007
  PKGINST: CSCOh007
    NAME: Media Gateway Controller Solaris 2.6 patch cluster
  CATEGORY: utilities
    ARCH: sparc
  VERSION: 1.0(7)
  BASEDIR: /opt/sun_install
  VENDOR: Cisco System, Inc.
  PSTAMP: 2002/01/07 22:10 GMT (embassy)
  INSTDATE: Jan 07 2002 17:12
    EMAIL: sctac@cisco.com
  STATUS: completely installed
  FILES: 154 installed pathnames
         2 shared pathnames
         2 directories
         4 executables
        561747 blocks used (approx)
```

To determine the Solaris release version of a patch that is not installed on your system, use the following command:

pkginfo -l -d <package instance>.pkg

The following shows an example using the **-d** option with the **pkginfo** command.

```
hostname% pkginfo -l -d CSCOh013.pkg
```

```

PKGINST: CSCOh013
NAME: Media Gateway Controller Security 2.6 package installation and patches
CATEGORY: utilities
ARCH: sparc
VERSION: 1.0(5)
BASEDIR: /opt/sun_install
VENDOR: Cisco System, Inc.
PSTAMP: 2001/07/20 17:48 GMT (embassy)
EMAIL: sctac@cisco.com
STATUS: spooled
FILES:      8 spooled pathnames
           2 directories
           1 executables
           5 package information files
           4 blocks used (approx)

```

**Note**

You should always check to ensure that you have the latest required patch version released by Cisco on your system, CD, or file system (if downloaded previously from CCO).

Solaris Packages

The following packages are available:

**Note**

The latest version of a package is always required. Refer to CCO to determine the latest package version available.

Volume Manager

These packages provide the install/uninstall scripts needed to support volume manager on Solaris 2.6. Volume manager allows disk mirroring in systems that have two or more disks. Disk mirroring enables file system backup and recovery on a secondary disk if the primary disk fails or needs to be replaced.

Table 1 *Solaris Volume Manager Packages*

Package	Description
CSCOh000	Volume manager 3.1 installation
CSCOh001	Volume manager 2.5 installation
CSCOh002	Obsolete.
CSCOh003	Obsolete.
CSCOh004	Obsolete.
CSCOh006	Volume manager installation scripts and patches (T112x)

**Note**

To enable the Veritas volume manager you must purchase the required software key.

Log and Spool File Systems

The log and spool file system package for the Netra T1/T112x/T140x and E450 provides the scripts needed to configure the /opt/CiscoMGC/var/log and /opt/CiscoMGC/var/spool directories on a secondary disk. It allows a MGC to use the primary disk for the MGC application while allowing billing, alarms, and measurement information to be stored on a secondary disk. This configuration is appropriate for MGC systems with small (4M) disk drives; this configuration cannot be used if you use Volume Manager for disk mirroring.



Note

CSCOh005 should not be installed if packages CSCOh000, CSCOh001, or CSCOh006 are installed.

Table 2 Solaris Log and Spool File System Package

Package	Description
CSCOh005	Log and spool file system configuration scripts (T112x)



Note

The E450 is an end-of-life product. Customers should upgrade from all E450s on their network.

Solaris 2.x Patch Cluster

The Solaris 2.x patch cluster package provides the required security patches provided by Sun. These patches have been regression tested with the product and are supported by Cisco. Patches downloaded from Sun are not supported until they are officially tested and released by Cisco. These patches are updated quarterly to ensure that they are synchronized with Sun's latest recommended and security patch cluster.

Table 3 Solaris 2.5.1 Patch Cluster Packages

Package	Description
CSCOh008	Cisco Solaris 2.5.1 patch cluster (Solaris 2.5.1) (Required)

Table 4 Solaris 2.6 Patch Cluster Packages

Package	Description
CSCOh007	Cisco Solaris 2.6 patch cluster (Solaris 2.6) (Required)

Solaris 2.6 Return Codes

When a patch cluster is installed, some individual patches might fail to install because they are already installed on the machine (as part of the Solaris 6 installation or as part of an earlier application of the patch cluster) or because the individual patch applies to an application which we do not install. For example, there are security patches for UUCP, but since we do not install UUCP on the machine, these patches fail to install. This is not considered an error as far as the installation process is concerned.

When an individual patch fails to install, a return code displays to indicate the reason the patch did not install. [Table 5](#) lists the return codes for Solaris 2.6:

Table 5 *Solaris 2.6 Return Codes*

Return Code	Description
0	No error.
1	Usage error.
2	Attempt to apply a patch that's already been applied.
3	Effective UID is not root.
4	Attempt to save original files failed
5	Pkgadd failed.
6	Patch is obsoleted.
7	Invalid package directory.
8	Attempting to patch a package that is not installed.
9	Cannot access /usr/sbin/pkgadd (client problem).
10	Package validation errors
11	Error adding patch to root template.
12	Patch script terminated due to signal.
13	Symbolic link included in patch.
14	Not used.
15	The prepatch script had a return code other than 0.
16	The postpatch script had a return code other than 0.
17	Mismatch of the -d option between a previous patch install and the current one.
18	Not enough space in the file systems that are targets of the patch.
19	\$\$SOFTINFO/INST_RELEASE file not found.
20	A direct instance patch was required but not found.
21	The required patches have not been installed on the manager.
22	A progressive instance patch was required but not found.
23	A restricted patch is already applied to the package.
24	An incompatible patch is applied.
25	A required patch is not applied.
26	The user specified backout data can't be found.
27	The relative directory supplied can't be found
28	A pkginfo file is corrupt or missing.
29	Bad patch ID format.
30	Dry run failure(s).
31	Path given for -C option is invalid.
32	Must be running Solaris 2.6 or greater.

Table 5 *Solaris 2.6 Return Codes (continued)*

Return Code	Description
33	Bad formatted patch file or patch file not found.
34	The appropriate kernel jumbo patch needs to be installed.

System Security Patch

The system security patch installs the Cisco security script. This script is used to reduce the number of known system security vulnerabilities.

Table 6 *Solaris Security Package*

Package	Description
CSCOh013	Solaris 2.6 system security package

The system security script disables the following:

- printer services
- standard UNIX mail
- NFS functionality
- the keyboard break key

**Note**

All failed login attempts are logged.

The following users do not have direct FTP access:

- root
- daemon
- bin
- sys
- adm
- nobody
- noaccess
- nobody4

**Note**

Only telnet, FTP, and ping network services are enabled.

**Note**

Not allowing root direct FTP access prevents a root user from overwriting system files. To use the root account, you must use the su command from a nonprivileged account.

**Caution**

CSCOh013 v1.0(7) must not be installed on adjunct systems such as BAMS. This restriction has been removed in v1.0(8).

**Note**

After installation of CSCOh013 FTP access should be restricted to the mgcusr login ID as part of the mgcgrp.

**Note**

To minimize MGC access issues after installation of CSCOh013, adjunct systems such as BAMS, VSPT, and CMNM should use the mgcusr login ID to access the MGC for information.

Installation

For new installations please refer to the installation procedures provided in the *Cisco Media Gateway Controller Software Release (7 or 9) Installation and Configuration Guide* at the following url:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/swinstl/index.htm>.

Patch Installation and Upgrade

This section provides information to use when installing Solaris packages when the MGC software has already been installed.

**Caution**

Packages CSCOh000, CSCOh001, CSCOh005, and CSCOh006 should not be uninstalled after their initial installation. These packages contain your system configuration and removing them might render your server unusable.

**Note**

If you are installing multiple packages, you can wait until installation of your final package before rebooting.

CSCOh007 Install and Update

The following procedure should be used to install package CSCOh007:

-
- Step 1 `pkgadd -d <package directory>/CSCOh007.pkg`
 - Step 2 `run /opt/sun_install/installPatches2.6`
 - Step 3 Reboot
-

The following procedure should be used to upgrade package CSCOh007:

-
- Step 1 `pkgrm CSCOh007`
 - Step 2 `pkgadd -d <package directory>/CSCOh007.pkg`
 - Step 3 `run /opt/sun_install/installPatches2.6`
 - Step 4 Reboot
-

**Note**

The installation and uninstallation of CSCOh007 has no effect on existing software. This package can be installed or updated at any time.

CSCOh008 Install and Update

The following procedure should be used to install package CSCOh008:

-
- Step 1 `pkgadd -d <package directory>/CSCOh008.pkg`
 - Step 2 `run /opt/sun_install/installPatches2.5.1`
 - Step 3 Reboot
-

The following procedure should be used to upgrade package CSCOh008:

-
- Step 1 `pkgrm CSCOh008`
 - Step 2 `pkgadd -d <package directory>/CSCOh008.pkg`
 - Step 3 `run /opt/sun_install/installPatches2.5.1`
 - Step 4 Reboot
-

CSCOh013 Install and Update

**Caution**

If the MGC software needs to be updated, package CSCOh013 must be uninstalled before the MGC software is updated, and reinstalled after reinstallation of the MGC software.

The following procedure should be used to install package CSCOh013:

-
- Step 1 `pkgadd -d <package directory>/CSCOh013.pkg`
 - Step 2 Reboot
-

The following procedure should be used to upgrade package CSCOh013:

-
- Step 1 pkgrm CSCOh013
- Step 2 pkgadd -d <package directory>/CSCOh013.pkg
- Step 3 Reboot
-

Solaris Patch CSCOh005 Modification History

Table 7 Modifications for Solaris Patch CSCOh005

Date	Solaris Release	Solaris Version	Modification
06/20/03	1.0(13)	2.6	Repackaged to incorporate changes for CSCea49014.
06/06/02	1.0(10)	2.6	Repackaged to incorporate changes for CSCdx39654.

Solaris Patch CSCOh006 Modification History

Table 8 Modifications for Solaris Patch CSCOh006

Date	Solaris Release	Solaris Version	Modification
06/06/02	1.0(10)	2.6	Repackaged to incorporate changes for CSCdx39654.

Solaris Patch CSCOh007 Modification History

Table 9 Modifications for Solaris Patch CSCOh007

Date	Solaris Release	Solaris Version	Modification
09/16/03	1.0(14)	2.6	Repackaged to incorporate changes for CSCec29299.
05/22/03	1.0(13)	2.6	Repackaged to incorporate changes for CSCeb13929.
02/03/03	1.0(12)	2.6	Repackaged to incorporate changes for CSCea06358.
09/23/02	1.0(11)	2.6	Repackaged to incorporate changes for CSCdv91223. Note This patch is required for proper operation of the Software Inventory Control feature delivered in Release 7.4(12) patch CSCogs024.
04/02/02	1.0(9)	2.6	Repackaged to incorporate the quarterly update of the latest 2.6 Solaris security-related patch updates.
02/14/02	1.0(8)	2.6	Repackaged to incorporate changes for CSCdw50335.

Table 9 *Modifications for Solaris Patch CSCOh007 (continued)*

Date	Solaris Release	Solaris Version	Modification
01/14/02	1.0(7)	2.6	Repackaged to incorporate changes for CSCuk30410 and latest recommended and security patches from Sun.
12/14/01	1.0(6)	2.6	Repackaged to incorporate changes for CSCdw12804.
11/30/01	1.0(5)	2.6	Repackaged to incorporate changes for CSCdu60188.

Solaris Patch CSCOh008 Modification History

Table 10 *Modifications for Solaris Patch CSCOh008*

Date	Solaris Release	Solaris Version	Modification
02/14/02	1.0(8)	2.5(1)	Repackaged to incorporate changes for Sun Solaris patch-id# 106160-02.

Solaris Patch CSCOh013 Modification History

Table 11 *Modifications for Solaris Patch CSCOh013*

Date	Solaris Release	Solaris Version	Modification
04/02/02	1.0(9)	2.6	Repackaged to incorporate changes for CSCdx06201, CSCdx11926, CSCdx20010, CSCdx20028, and CSCdx20098.
02/20/02	1.0(8)	2.6	Repackaged to incorporate changes for CSCdw77188.
02/14/02	1.0(8)	2.6	Repackaged to incorporate changes for CSCdw53443, CSCdw53428, CSCdw59900, and CSCdw53451.
01/14/02	1.0(7)	2.6	Repackaged to incorporate changes for CSCuk30410.
12/14/01	1.0(6)	2.6	Repackaged to incorporate changes for CSCdw12804.
11/30/01	1.0(5)	2.6	Repackaged to incorporate changes for CSCdu60188.

New Features and Featurettes

36 GB Disk Drive Upgrade

**Note**

This patch should only be installed if you want to use a 36 GB disk drive.

This featurette (CSCdx39654) enables you to upgrade your system from a 18 GB to a 36 GB disk drive. The CSCOh005 and CSCOh006 packages have been modified to support this featurette.



Note

This featurette can be used for existing and new system installations.

For more information on this featurette, refer to the *Cisco Media Gateway Controller Software Release 9 Installation and Configuration Guide* at the following url:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/swinstl/index.htm>

Known Issues and Operational Recommendations

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

Errors That May Display During Installation of CSCOh007

The following errors may display during installation of CSCOh007:

```
Skipping patch 105357-04 is already installed
```

```
Installing 105458-21...
```

```
Application supported by 105357-04 is not installed. Return code 8.
```

The patch numbers shown in the error messages that display on your system may differ from the patch numbers displayed in the example (above).



Note

These errors are expected and do not affect the installation of patch CSCOh007.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

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

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, 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, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, 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, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0406R)