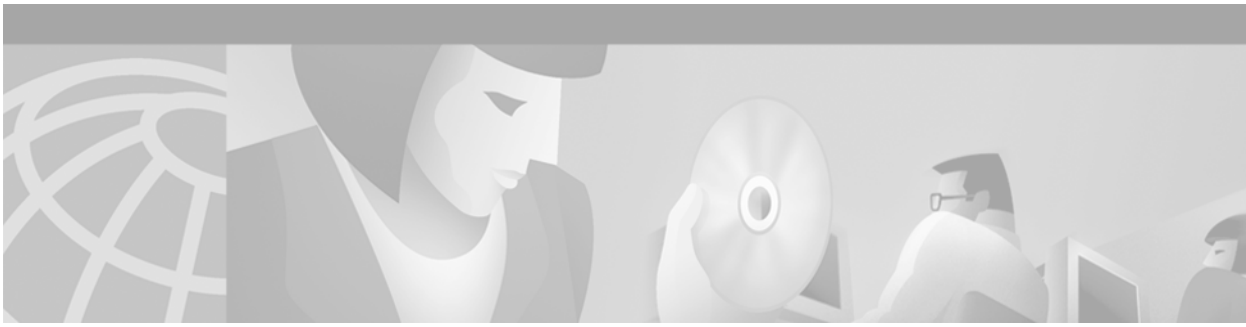

Release Notes for Cisco Telephony Controller Software Release 4.2(19)

February 5, 2007

These release notes describe the features and caveats in the software for the Cisco Telephony Controller software release 4.2(19).

This introductory section lists the contents of this document and describes the system and software.

Document Contents

- Product Description, page 2
- Related Documentation, page 2
- Platform Support, page 3
- Important Notes, page 5
- Upgrade Procedures, page 5
- Required Patches, page 6
- General Issues, page 23
- Release 4.2(19) Caveats, page 29
- Terms and Abbreviations, page 30
- Service and Support, page 32
- Cisco Connection Online, page 32
- Documentation CD-ROM, page 33

CISCO SYSTEMS

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

78-7191-02 Rev BO

Product Description

The Cisco Telephony Controller software is part of several solutions designed to perform call processing, protocol conversion, and call switching and routing functions.

The Telephony Controller software runs on a Sun Microsystems host server and is used in a variety of solutions. Currently, the software is available as part of a Cisco Virtual Switch Controller (VSC) or Cisco Dial Access Solution (DAS). See also the "Platform Support" section on page 3.

Note This software is also used with the TransPath 2000 (also referred to as TransPath Classic) configuration tool. This tool is no longer being marketed; however, existing installations are supported.

See the "Terms and Abbreviations" section on page 30 for definitions of terms and abbreviations used in these release notes.

Related Documentation

In addition to these release notes, this software release is supported by the following documents:

- Telephony controller documentation:

  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/index.htm
- *Cisco Dial Solutions Quick Configuration Guide*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/dsqcg3/index.htm
- *Cisco Dial Solutions Configuration Guide*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/dial_c/index.htm
- *Cisco Dial Solutions Command Reference*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/dial_r/index.htm
- Cisco Access Server documentation:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/index.htm
- Cisco Network Access Server configuration:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/cfios/
- Cisco IOS and Catalyst Software Release Notes: See the "Access Devices and Trunking Gateways" section on page 3.
- SS7 tutorial:

  http://www.iec.org/

  Click on **Web ProForum Tutorials (Online Tutorials, Communications Networks)**, then scroll down the list and click **Signaling System #7 (SS7)**.
- Release Notes for the Solaris 2.5(1) and 2.6 Packages:

  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/relnote/sol26rn.htm

Platform Support

The Cisco SC22XX is available in high-availability (redundant) or simplex configurations. Supported platforms include the following:

- Cisco SC2201: Simplex configuration of Sun Netra t1100 or Netra t1120 (NEBS, DC)
- Cisco SC2202: High-availability configuration of two Sun Netra t1100s or Netra t1120s (NEBS, DC)
- Cisco SC2211: Simplex configuration of Sun Enterprise 450 (AC)
- Cisco SC2212: High-availability configuration of two Sun Enterprise 450s (AC)

The Cisco VSC27XX is available in high-availability or simplex configurations. Supported platforms include the following:

- Cisco VSC2701: Simplex configuration of Sun Netra t1120 (NEBS, DC)
- Cisco VSC2702: High-availability configuration of two Sun Netra t1120s (NEBS, DC)

The telephony controller software runs on these platforms. The Configuration Tool (CT) and Dial Plan Provisioning (DPP) run on a separate server; see the “Related Hardware Components” section on page 3.

Related Hardware Components

The Cisco SC22XX requires the hardware components listed in the following sections:

Note The Cisco TransPath Classic does not use an access device.

Access Devices and Trunking Gateways

Access Devices[1]	• Cisco AS5200 • Cisco AS5300 • Cisco AS5800
Trunking Gateways	• Catalyst 5500 • Catalyst 8510 MSR • Catalyst 8540 MSR • Cisco LS1010

1. Contain MICA modems running Portware 2.6.1.0 and Cisco IOS 11.3(7)AA or later, or 12.03(T) or later

Note The Cisco LS1010 can be used as a multiplexing device if your system requires one.

CT and DPP Windows NT Server

The CT and DPP require a standalone Windows NT server with the following requirements:

- 200 MHz Pentium CPU
- 128 MHz RAM
- 2 GB hard drive
- Additional 4-GB hard drive
- Keyboard, mouse, floppy drive, internal 8X CD ROM drive
- 3COM Etherlink III network interface card
- Internal HP SureStore 6000 4 mm DAT
- SVGA video adapter (4 MB VRAM)
- Motorola 56 KB internal modem

Telephony Controller Ancillary Equipment

- E1/T1 cards manufactured by ITK or PTI
- V.35 cards manufactured by PTI
- Sun FastEthernet PCI card
- Sun asynchronous interface card
- Alarm Relay Unit (ARU)
- Switchover controller (or A/B switch)—for high-availability configurations only
- Patch panel
- Serial port expander
- Ethernet hub

Software Required

The Cisco VSC3000 requires the following software:

Sun host server	Sun Solaris 2.5.1
MGW and trunking gateways	• Cisco IOS Release 11.2(7)AA or later, or 12.0(3)T or later • Catalyst software Release 12.0(3x)W5(9)
CT and DPP	• Netscape Navigator, Versions 4.03 to 4.51 • Windows NT server running WWW services and Option Pack 3 • Microsoft Access 97

Memory Requirements

Access Devices

For Cisco IOS memory requirements, see the following Cisco IOS release notes:

Cisco AS5200	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5200/ios52/index.htm
Cisco AS5300	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/iosrn/index.htm
Cisco AS5800	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/58_iosrn/index.htm

Trunking Gateways

For trunking gateway software memory requirements, see the following release notes:

Catalyst 8510 MSR	http://www.cisco.com/univercd/cc/td/doc/product/atm/c8510/wa5/12_0/12_9/rn641202.htm
Catalyst 8540 MSR	http://www.cisco.com/univercd/cc/td/doc/product/atm/c8540/wa5/12_0/12_3/rn619005.htm
Catalyst 5500 and Cisco LS1010	http://www.cisco.com/univercd/cc/td/doc/product/atm/ls1010s/wa5/12/12_0_9/rel_nts/rn619104.htm

CT and DPP

The CT and DPP require a standalone Windows NT server with 128 MHz RAM, a 2-GB hard drive, and an additional 4-GB hard drive.

Important Notes

Upgrade Procedures

To upgrade from an earlier version of the Telephony Controller software to release 4.2(19), you must remove the existing telephony controller software first (including the configuration tool software, telephony controller software, and dial plan provisioning software), then reinstall. You can find procedures for software removal and installation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/r2/sc22tct.htm

Note These instructions apply to the removal and installation of any telephony controller software version.

Required Patches

Release 4.2(19) requires you to install the following patches after you install release 4.2(19):

PF9900073.pkg
PF9900074.pkg
PF0000090.pkg
PF0000094.pkg
PF0000095.pkg
PF0000098.pkg
PF0000100.pkg
PF0000104.pkg
PF0000109.pkg
PF0000110.pkg
PF0000111.pkg
PF0000112.pkg
PF0000114.pkg
PF0000115.pkg

In addition, Release 4.2(19) contains the following nonrequired patches:

PF9900062.pkg
PF9900063.pkg
PF9900064.pkg
PF9900065.pkg
PF9900066.pkg
PF9900067.pkg
PF9900068.pkg
PF9900069.pkg
PF9900070.pkg
PF9900071.pkg
PF9900072.pkg
PF9900075.pkg
PF9900076.pkg
PF9900077.pkg
PF9900078.pkg
PF0000080.pkg
PF0000081.pkg
PF0000082.pkg
PF0000083.pkg
PF0000084.pkg
PF0000085.pkg
PF0000086.pkg
PF0000087.pkg
PF0000088.pkg
PF9900089.pkg
PF0000091.pkg
PF0000092.pkg
PF0000093.pkg
PF0000096.pkg
PF0000097.pkg
PF0000099.pkg
PF0000101.pkg
PF0000102.pkg
PF0000105.pkg
PF0000106.pkg
PF0000107.pkg
PF0000108.pkg

A brief summary of each patch is provided below.

Before installing a patch, the user must shut down the Cisco MGC application, as the affected programs are part of the running system. In order to ensure that the MGC application has been shut down, execute the following command:

```
sudo /etc/init.d/transpath stop
```

Now that the MGC application has been shut down, installation can begin.

Note Many patches contain additional information that is required before installing that particular patch. This information can be found in the summary information on each patch, below.

The general patch installation procedure is as follows:

Step 1 Install version 4.2(19) of the Telephony Controller software according to the instructions referenced above. Remain logged in as the root user.

Step 2 At the UNIX prompt, enter:

```
cd cdrom/cdrom0
cd PATCHES
pkgadd -d PF#######.pkg
```

where ####### is the patch number.

Step 3 Follow the on-screen prompts. Answer **Y** to each prompt that requires a response.

To remove a patch, log in as the root user and then type the following

```
pkgrmPF#######
```

where ####### is the patch number.

Patch removal will restore the data to its state prior to the upgrade.

PF0200117.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCdw75318

Additional Information:

- This patch provides updates to the SNMP component.
- SNMP Packaging Modifications Introduced With Patch PF0200117

  Patch PF0200117 has been created as a result of the PSIRT SNMP security advisory posted at the following url:

  http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

Caution Because of differences between the snmp daemons that were originally packaged with 4.2(19) and the modifications delivered in patch PF0200117, the snmpd.cnf file will not function properly with the newer version of the snnp daemon. When PF0200117 is installed on your system, the current snmpd.cnf file is backed up as snmpd.cnf.custorig and a default version of this file is installed on your system to run with the new snmp daemon. The snmpd.cnf.custorig file is for reference only; it is not compatible with the new snmp daemon delivered in patch PF0200117. After installing patch PF0200117, you must reload the SC2200 configuration using config-lib tool. This tool automatically creates the snmpd.cnf file with the appropriate configuration.

- Installing Patch PF0200117

Step 1 Install patch PF0200117.

Step 2 Using option 3 (Copy Library Version to Production) of the config-lib tool, reload your SC2200 configuration.

The config-lib tool merges files /opt/TransPath/etc/snmpmgr.dat and /opt/TransPath/snmp/snmp.gen to create snmpd.cnf. This tool also restarts snmp daemon.

Step 3 Start your SC2200 software and verify that traps are generated.

- Uninstalling Patch PF0200117

  Beginning with PF0200117 and continuing forward, SNMP related data files and executables will not be removed from the system platform when a patch is removed. When uninstalling the patch, a copy of the snmpd.cnf, snmpinfo.dat, and snmpd.gen files are stored with an .backup extension in the /optTransPath/snmp directory. These backup files are for reference only. After uninstalling the patch, start your SC2200 software and verify traps are generated.

PF0000116.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCdv44184

This patch provides updates to:

- ISDNIP
- ISDNPRI
- IOCCIP

PF0000115.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCdt83578

This patch provides updates to:

- engine

PF0000114.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCds68645
- CSCdt17397
- CSCdt18341

This patch provides the following updates to:

- engine
- protocols
- ASP
- DPNSS
- ISDNPRI
- ISDNIP

PF0000112.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCds70464

This patch provides the following updates to:

- ioChanMgr

PF0000111.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCds33066

This patch provides the following updates to:

- SAGT

Additional information:

- The problem that is fixed in this patch occurred as follows:

  The 4.2(19) release SNMP trap agent registers the system MIB table, but does not respond to the query. Therefore, NMS resends the query once it times out. The NMS is tuned to send query every second to SNMPDM. This can cause the SNMPDM to use all of the threads, so it can not respond.

  This patch prevents this from happening because it causes a response to be returned to the NMS query.

PF0000110.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCds08534

PF0000109.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS tickets:

- CSCds03123
- CSCds16286

This patch also resolves the following DDTS tickets previously delivered in earlier patches:

DDTS Ticket # Resolved in Patch 109	Previously Delivered in Patch
CSCds13626	108
CSCdr85817	105
CSCdr45476 CSCdr45496	102
CSCdr45476 CSCdr45496	101
CSCdr38290	97
CSCdr29974	96
CSCdr20146	91
CSCdp98451 CSCdr00259 CSCdr03213	88
CSCdp67913 CSCdp97095	86
CSCdp94528	85
CSCdp45696	75
CSCdp35071	70
CSCdp12148	68
CSCdm64616 CSCdm83283	66

This patch provides the following updates to:

ANSISS7.mdo
ASP_NotRealProtocol.mdo
ATT_41459.mdo
ATT_41459_C2.mdo
BELL_1268.mdo
BELL_1268_C3.mdo
BTNUP.mdo
BTNUP_INTEROUTE.mdo
BTNUP_IUP.mdo
BTNUP_MOBEX.mdo
BTNUP_NRC.mdo
DPNSS.mdo
DPNSS_MOBEX.mdo
EISUP.mdo
ETSI_102.mdo
ETSI_102_C1.mdo
ETSI_172.mdo
HKTA_2202.mdo
INS_1500.mdo
ISUPV1.mdo
ISUPV1_POLI.mdo
ISUPV2.mdo
ISUPV2_FRENCH.mdo
ISUPV2_GERMAN.mdo
ISUPV2_KPNPB.mdo
ISUPV2_NTT.mdo
ISUPV2_SPANISH.mdo
ISUPV2_SWISS.mdo
ISUPV3.mdo
ISUPV3_UK.mdo
Q721.mdo
Q721_CHINA.mdo
Q761.mdo
Q761_AUSTRL.mdo
Q761_BELG_MOBI.mdo
Q761_JAP.mdo
Q761_KOREAN.mdo
Q767.mdo
Q767_ITAL.mdo
Q767_ITAL_INTERCONNECT.mdo
Q767_RUSS.mdo
Q767_SPAN.mdo
Q767_SWED.mdo
SFS_5779.mdo
SGCPdummy.mdo
T113_BELL.mdo
cc.mdo
lcm.mdo

PF0000108.pkg

This patch is superseded by patch PF9900109.

PF0000107.pkg

Caution Do not install this patch. It is superseded by patch PF9900110.

PF0000106.pkg

This patch is superseded by patch PF9900108.

PF0000105.pkg

This patch is superseded by patch PF9900108.

PF0000104.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS tickets:

- CSCdr38973
- CSCdr53856

PF0000103.pkg

The purpose of this patch package is to provide showstopper and/or test-stopper bug fixes to NSSU customers, be they devtest, solution test, customers, etc., for the 4.2(19) software release. Specifically, this patch resolves the following new DDTS ticket:

- CSCdr90481

This patch also resolves the following DDTS tickets previously delivered in earlier patches:

DDTS Ticket # Resolved in Patch 103	Previously Delivered in Patch
CSCdp45499 (engine, ISDNPRI)	100
CSCdp81697 CSCdp87703	85
CSCdp72636	84
CSCdp58516 CSCdp66427	81
CSCdp50186	77
CSCdp34109 (ISDNPRI)	69

This patch also resolves the following DDTS tickets previously delivered in earlier patches:

DDTS Ticket # Resolved in Patch 104	Previously Delivered in Patch
CSCdp45499 (IOCM)	100
CSCdp63674	99
CSCdp80270	83
CSCdp70673	81

DDTS Ticket # Resolved in Patch 104	Previously Delivered in Patch
CSCdp41316 (IOCM) CSCdp46124 (IOCM)	74
CSCdp41316	72
CSCdp37929	71

Additional information:

- Patch 104 is being delivered to address ITK problems where the workaround is to perform a manual ixload on the ITK card.

  The resolution for CSCdr38973, ITK card freeze, is to automatically perform a software-initiated ixload when the ITK card freezes or crashes. The ITK card can freeze when traffic surges above the supported capacity for prolonged periods.

  CSCdr53856, SS7 links go OOS, SUPPENT on failover (ITKs with orange link lights), is a rarely seen problem where the ITK cards do not initialize properly during failover or system startup. When this condition occurs, the ITK card link light turns orange and the SS7 links are in the OOS, SUPPENT state. If this condition is noticed on your system, please update the XECfgParm.dat file to initiate the recovery script. This script will reload all ITK cards on startup.

  In XECfgParm.dat, update the following line:

  ```
  Foverd.procMCmdLine = /opt/TransPath/bin/procM
  ```

  to

  ```
  Foverd.procMCmdLine = /opt/TransPath/local/recovery
  ```

  If your system does not display the above behavior as described for CSCdr53856, these modifications are not necessary.

PF0000102.pkg

This patch is superseded by patch PF9900105.

PF0000101.pkg

This patch is superseded by patch PF9900102.

PF0000100.pkg

In order to provide a timely fix for caveat CSCdr45499, it has becomes necessary to build and deliver patch PF0000100, which updates the all the processes in the /opt/TransPath/bin directory. This patch also resolves the following DDTS tickets previously delivered in earlier patches:

DDTS Ticket # Resolved in Patch 100	Previously Delivered in Patch
CSCdr21155 (sagt)	95
CSCdr22780 (foverd)	94
CSCdr21155 (sagt)	93
CSCdp77065	89

DDTS Ticket # Resolved in Patch 100	Previously Delivered in Patch
CSCdr03308	87
CSCdp32322 CSCdp48333	84
CSCdp77058	82
CSCdp70673	81
CSCdp48333	80
CSCdp12160 (foverd)	79
CSCdp57306	78
CSCdp34109 (ISDNIP)	69
CSCdp07629	63

This patch is superseded in part by patches PF9900103 and PF9900104.

PF0000099.pkg

This patch is superseded by patch PF9900100.

Additional information:

- The default value for the timer parameter "*.delayTimer" specified in properties.dat is now changed to 3 seconds, for example:

```
*.delayTimer = 30
```

PF0000098.pkg

In order to provide a timely fix for caveat CSCdr42570, it has becomes necessary to build and deliver patch PF0000098, which updates the CCGen executable. This patch also resolves the following Distributed Defect Tracking System (DDTS) tickets previously delivered in patch 92:

- CSCdr20158
- CSCdp74657

PF0000097.pkg

This patch is superseded by patch PF9900101.

Note IOS implementations in the 5200 and 5300 differ, as v110 calls have been successfully set up on the 5200 in the past.

PF0000096.pkg

This patch is superseded by patch PF9900097.

Additional information:

- T309 timers already configurable due to changes made in earlier releases, as follows:

```
*.T309Time   =   50000
```

PF0000095.pkg

In order to provide a timely fix for caveat CSCdr21155, it has becomes necessary to build and deliver patch PF0000095, which fixed the snmp OID. This patch also temporarily addresses the problem with the snmpv1 trap that was indicated in caveat CSCdr26639. This patch is superseded in part by patch PF9900100.

You must stop the SNMP daemon before installing this patch. Log in as the root user and enter the following:

```
/etc/init. d/snmpd stop
```

After installing the patch, start the SNMP daemon by logging in as the root user and entering the following:

```
/etc/init. d/snmpd start
```

Additional information:

- This installed PF0000095.pkg patch is based on the assumption that:
  - user should have already configured the IP address of the snmp manager from TCT. The IP address shall show in the /opt/TransPath/etc/snmpmgr.dat file.
  - snmp configured file /opt/TransPath/snmp/snmpd.cnf is not manually edited.
  - This patch will back up snmpd.cnf to becomes snmpd.cnf.org file, and concatenate /opt/TransPath/snmp/snmpd.gen with /opt/TransPath/etc/snmpmgr.dat into snmpd.cnf file that will correct the snmp OID.
- This patch temporarily makes the snmp send v1 type trap behave correctly with the current configured snmpmgr.dat on the user 's TransPath box. However, it will not fix the snmpmgr.dat in other previous configurations. For future configuration files, user shall use the next TCT release to generate the snmpmgr.dat.

PF0000094.pkg

In order to provide a timely fix for caveat CSCdr22780, it has becomes necessary to build and deliver patch PF0000094, which updated the foverd process and frepld.cfg file. This patch is superseded in part by patch PF9900100.

PF0000093.pkg

This patch is superseded by patches PF9900095 and PF0000100.

Caution Do not install this patch—it does not completely fix the problem.

PF0000092.pkg

This patch is superseded by patch PF9900098.

PF0000091.pkg

This patch is superseded by patch PF9900096.

PF0000090.pkg

Under special circumstances, it has becomes necessary to deliver patch PF0000090 regarding caveat CSCdr12582.

PF9900089.pkg

This patch is superseded by patch PF9900100.

PF0000088.pkg

This patch is superseded by patch PF9900091.

PF0000087.pkg

This patch is superseded by patch PF9900100.

PF0000086.pkg

This patch is superseded by patch PF9900088.

PF0000085.pkg

This patch is superseded by patches PF9900086, PF9900088, and PF0000100.

PF0000084.pkg

This patch is superseded by patches PF9900085, PF9900087, and PF0000100.

PF0000083.pkg

This patch is superseded by patch PF9900099.

PF0000082.pkg

This patch is superseded by patch PF9900100.

PF0000081.pkg

This patch is superseded by patches PF9900083, PF9900084, PF9900085, and PF0000100.

Additional information:

- SERVICE message discard (CSCdp70673)

Handshaking between the SC2200 and the NAS on channel In Service/Out of Service state change messages breaks down when the SC2200 goes into congestion. The result is that the NAS can mark channels remotely out of service due to mis-sequenced SERVICE_ACK messages when they should be available for new calls.

With this patch, the channel controller used by the NAS interface will discard all incoming bearer SERVICE messages and not therefore generate corresponding SERVICE_ACK messages; thus, the SC2200 will not go into congestion and the NAS channel state will not be marked remotely out of service.

Assumptions:

- NAS does not care if SC acknowledges service messages or not
- Remote switch knows when physical transmission link goes down and will not originate calls on those affected circuits

Provisioning:

- When enabled, this fix blocks incoming Service Message inside the ISDNIP channel controller. A parameter can be added in properties.dat to turn this action on/off, as follows:

  properties.dat

```
*.notBlockEngServ = false# discard SERVICE messages : default
*.notBlockEngServ = true# pass SERVICE messages through to engine
```

- PropagateSvcMsgBlock Propagation (CSCdp58516)

  Propagation of individual SS7 blocking/unblocking messages on systems with large numbers of SS7 bearer channels mated to few NAS signal paths has been noted to cause engine, IO card and switch overload. The changes implemented in this patch control the rate at which BLO/UBL messages may be transmitted so as to avoid overloading any specific part of the system or network.

  Specifically, when blocking propagation is turned on in an SS7 Interconnect for Access Servers 2.0 environment (*.PropagateSvcMsgBlock = true), the engine will queue outgoing messages and start sending individual block/unblock messages for all circuits associated with a single span per time interval.

  Assumptions:

  - Blocking propagation (PropagateSvcMsgBlock) is only enabled for SS7 Interconnect for Access Servers 2.0 configurations
  - Blocking/unblocking messages are always sent for all bearers in a span at the same time
  - If LOCMAN blocking exists prior to propagation on loss of NAS link, this will be REMOVED when the NAS link is restored. (that is, all channels will be locally unblocked due to propagation of In Service condition)
  - Queuing of messages is only done for NAS link state change. No attempt will be made to queue individual bearer state changes brought about by reception of SERVICE messages. (See fix for CSCdp70673).

  Provisioning:

  - The time interval and number of spans to send per interval are configurable as follows:

    XECfgParm.dat

```
engine.SysPropagateSpansPerTimer = 1# number of spans to send per interval
engine.SysPropagateSpansDelay = 500# milliseconds pause between sending
engine.SysInitialManBlk = true# default CIC state (true = blocked)
```

properties.dat

```
*.PropagateSvcMsgBlock = true# perform blocking propagation for TD2.0
*.GRSEnabled = true# send GRS immediately after engine startup
```

Note Reducing the default interval time interval or increasing the spans/interval count may lead to message loss and engine overload.

- Recommended Settings

  The following settings were derived during Solution Testing:

  Low call volume system (10 cps or less)

  – Info level: debugging or less

  – properties.dat:

  ```
  *.PropagateSvcMsgBlock=true
  ```

  – XECfgParm.dat

  ```
  engine.SysPropagateSpansPerTimer=1
  engine.SysPropagateSpansDelay=500
  engine.SysInitialManBlk=true
  ```

  With these settings, a Netra 1120 should be able to process 10 cps while blocking 15000 circuits over 6:20 minutes with minimal interruption in call processing due to processing of the BLOs from a failure.

  High call volume system (<20 cps)

  – Info level: debugging or less

  – properties.dat

  ```
  *.PropagateSvcMsgBlock=true
  ```

  – XECfgParm.dat

  ```
  engine.SysPropagateSpansPerTimer=1
  engine.SysPropagateSpansDelay=800
  engine.SysInitialManBlk=true
  ```

  With these settings, a Netra 1120 should be able to process 20 cps while blocking 15000 circuits over 8:32 minutes with minimal interruption in call processing due to processing of the BLOs from a failure.

PF0000080.pkg

This patch is superseded by patch PF9900084.

PF9900079.pkg

Under special circumstances, it has becomes necessary to deliver patch PF9900079 regarding caveat CSCdp12160, which will update the foverd. This patch is superseded in part by patch PF9900094.

PF9900078.pkg

This patch is superseded by patch PF9900082.

PF9900077.pkg

This patch is superseded by patches PF9900081 and PF0000085.

Additional information:

- The new thresholds value for parameters listed below represent the percentage of engine queue size:

```
*.Ovl1OnsetThresh = 40          # ovlxOnsetThresh = a percentage of total queue capacity
                                at which
*.Ovl2OnsetThresh = 50          #the overload level will be in effect
*.Ovl3OnsetThresh = 60
*.Ovl1AbateThresh = 30           #ovlxAbateThresh = a percentage of total queue capacity
                                at which
*.Ovl2AbateThresh = 35          #the overload level will no longer be in effect
*.Ovl3AbateThresh = 45          #abatement must be less than onset
*.Ovl1RejectPercent = 25        #ovlxRejectPercent = a percentage of new calls that will be
                                rejected
*.Ovl2RejectPercent = 50        #at this overload level. EX: 20% means 1 out of every
*.Ovl3RejectPercent = 100       #five new calls will be rejected at this level
```

These new sets of overload values need to be implemented to the engine section in the XECfgParm.dat file.

PF9900076.pkg

This patch is superseded by patch PF9900085.

PF9900075.pkg

This patch is superseded by patch PF9900076.

PF9900074.pkg

In order to provide a timely fix for caveats CSCdp41316 and CSCdp46124, it has becomes necessary to build and redeliver patch PF9900074, which updates the protocols. This patch is superseded in part by patch PF9900100.

PF9900073.pkg

In order to provide a timely fix for caveat CSCdp38893, it has becomes necessary to build and deliver patch PF9900073, which updates the BCGen process.

PF9900072.pkg

This patch is superseded by patch PF9900074.

PF9900071.pkg

This patch is superseded by patch PF9900072.

Additional information:

Currently, the ioChanMgr reads the RLM.port property to configure the ISDNIP IOCC. Only one IOCC can bind to the local IP address using the RLM.port. Multiple IOCCs are needed to support the number of d-channels required by customers. If multiple IOCCs are used, the RLM port number must be configurable on a per-IOCC basis. The ioChanMgr changed to read the RLM properties using the IOCC label. If no properties are found prefaced by the IOCC label, ioChanMgr uses RLM as a default. The VSC changes are in properties.dat and sigChanDevIp.dat: (using the IOCC labels from components.dat:; this uses IOCC-PRIIP1, IOCC-PRIIP2, the customer's names and compIds will differ). The configuration must be changed on any NAS that is not configured with 3001 in sigChanDevIp.dat. If you configure the NAS rlm port, it will automatically configure the ISDN port as RLM port + 1. (You can also reconfigure the ISDN port if you want.) Following is an example:

properties.dat:

```
RLM.port = 3000
IOCC-PRIIP1.port = 3000  (w/compId 30010 )
IOCC-PRIIP2.port = 3002  (w/compId 30011)
IOCC-PRIIP3.port = 3004  (w/compId 30012)
IOCC-PRIIP3.port = 3006  (w/compId 30013)
```

in sigChanDevIp.dat, change both local and remote ports for 30010 to:

```
001000xx   IP_Addr1  3001  <nas1 ip1>  3001
001000xx   IP_Addr2  3001  <nas1 ip2>  3001
```

for 30011 to:

```
001000xx  IP_Addr1   3003  <nas33 ip1> 3003
001000xx  IP_Addr2   3003  <nas33 ip2> 3003
```

for 30012 to:

```
001000xx  IP_ Addr1   3005  <nas65 ip1> 3005
001000xx  IP_Addr2   3005  <nas65 ip2> 3005
```

for 30013 to:

```
001000xx  IP_ Addr1   3007  <nas65 ip1> 3007
001000xx  IP_Addr2   3007  <nas65 ip2> 3007
```

in NAS config file

```
rlm group 0
timer keepalive 10
server va-dorset
link hostname va-dorset source Ethernet0 weight 1
!
rlm group 1
protocol rlm port 3002
timer keepalive 10
server va-dorset
link hostname va-dorset source Ethernet0 weight 1
!
rlm group 2
protocol rlm port 3004
timer keepalive 10
server va-dorset
link hostname va-dorset source Ethernet0 weight 1
!
rlm group 3
protocol rlm port 3006
timer keepalive 10
server va-dorset
link hostname va-dorset source Ethernet0 weight 1
```

PF9900070.pkg

This patch is superseded by patch PF9900075.

PF9900069.pkg

This patch is superseded by patches PF9900081 and PF0000100.

PF9900068.pkg

This patch is superseded by patch PF9900075.

PF9900067.pkg

This patch is superseded by patch PF9900093.

PF9900066.pkg

This patch is superseded by patch PF9900068.

PF9900065.pkg

This patch is superseded by patch PF9900066.

PF9900064.pkg

This patch is superseded by patch PF9900065.

PF9900063.pkg

This patch is superseded by patches PF9900078 and PF0000100.

PF9900062.pkg

This patch is superseded by patch PF9900064.

Installing the ITK Driver

In order to provide enhancements that may impact the resolution of CSCdr48971 bug, it has becomes necessary to build and deliver the ITK Driver package. To install this package, follow these steps:

Step 1 Type the command **su**

Step 2 Remove the existing ITK driver by typing **pkgrm -d ITKP40AA**

Step 3 Type **Y** when prompted

Step 4 Type **pkgadd -d ITK-HDLCP40AA.pkg**

Step 5 Press Return to accept the default prompt

Step 6 Type **Y** to install the new patch

The system will reboot automatically after installing the new ITK Driver.

The LED indications on the ITK Card provide comprehensive visual indication of the ITK Card status.

LED	Status	Indication
top	solid green	Layer 1 of the ISDNPRI or SS7 Link terminating into ITK Card is OK
top	solid red	Layer 1 of the ISDNPRI or SS7 Link terminating into ITK Card is broken
bottom	blinking green	Communication Link Between ITK Card and SC2200 software is OK
bottom	blinking red/solid green/solid red	Communication Link Between ITK Card and SC2200 is broken

The blinking rate of the bottom LED is directly proportional to the rate at which the ITK Card processes data. The fix also puts a timestamp on the date the ITK Driver was created. This helps track the version of the ITK software. Use the following command at the UNIX prompt to find out the date:

```
>modinfo | grep itk
```

Year 2000 Compliance

Information about Y2K compliance and Cisco products is available at the following URL:

http://www.cisco.com/warp/public/752/2000/

Limitations and Restrictions

The signaling software does not currently support 7-digit dialing in the United States.

General Issues

Addition of Services During System Operation

Release 4.2(19) does not support dynamic reconfiguration during operation (for example, adding new components or making other configuration changes). The application must be shut down to add needed services during routine maintenance.

For instructions on shutting down the telephony controller, see Chapter 3, "Operating Your Telephony Controller," in the *Telephony Controller Release 4 Software Operations and Maintenance Guide*.

Configuration Tool Client/Browser Session Problems

In release 4.2(19), a configuration tool session that has been inactive for 2 minutes may time out or have other difficulties such as an inability to view existing data. You may also experience problems when resizing your browser window or if the Netscape client hard disk cache is less than 8 MB.

If you experience problems, exit the affected configuration tool session and initiate a new configuration tool session.

The Orbix Web server may experience confusion resulting in a **10191 Orbix not running** error message. If this occurs, or if the Orbix daemon fails, stop and restart the system.

Configuration Tool Scroll Bar

The line scroll bar in the configuration tool may lose its position on a list box refresh due to an unresolved situation with the underlying third-party technology.

Configuration Tool Requires Full Host Table Entries When Not Using DNS

On systems that are not using DNS entries or networks where DHCP is being used without DNS entries, you must fully qualify complete host table entries in the **C:\winnt\system32\drivers\etc\hosts** file as follows:

```
171.17.193.101 hostname hostname.domain.com
```

Workaround: Your hosts file on the server must contain the IP address, computer name, and network address of each computer you want to access. For example:

```
172.29.12.113          your-pc           your-pc.company.com

172.17.192.101         ms-tel1           ms-tel1.company.com

172.17.192.102         ms-tel2           ms-tel2.company.com
```

Ensure that DNS is enabled on the server (even if you do not have any DNS server entries). Also be sure you give it a host name and domain on the DNS screen. You must have a **c:\windows\hosts** on your client because you cannot use the IP address as the URL. Then close down the **server.bat** windows and delete the two files in **c:\lightspeed\orbixweb\config\NamingRepository** (**root** and **No_0**).

Internal Release Code Causes

This section provides information for the various values displayed within CDRs.

Table 1 Internal LCM Causes for ETSI

Internal Release Cause Name	Decimal Value	Hex Value
ACCESS_INFO_DISCARDED	1	1
BEARCAP_NOT_AUTHORIZED	2	2
BEARCAP_NOT_AVAIL	3	3
BEARCAP_NOT_IMP	4	4
CALL_AWARDED_DELIVERED_EST_CH	5	5
CALL_ID_HAS_BEEN_CLEARED	6	6
CALL_ID_IN_USE	7	7
CALL_REJECTED	8	8
CH_ID_NOT_EXIST	9	9
CH_TYPE_NOT_IMP	10	a
CH_UNACCEPTABLE	11	b
DEST_OUT_OF_ORDER	12	c
ELEM_TYPE_NOT_IMP	13	d
FACILITY_REJECTED	14	e
INCOMPATIBLE_DEST	15	f
INTERWORK_UNSPEC	16	10
INVALID_CALL_REFERENCE_VALUE	17	11
INVALID_ELEM_CONTENTS	18	12
INVALID_MSG_UNSPEC	19	13
INVALID_NUMBER_FORMAT	20	14
INVALID_TNS	21	15
MANDATORY_ELEMENT_MISSING	22	16
MSG_IN_WRONG_STATE	23	17
MSG_TYPE_NOT_IMP	24	18
MSG_TYPE_NOT_IMP_OR_WRONG_STATE	25	19
NETWORK_OUT_OF_ORDER	26	1a
NO_CALL_SUSPENDED	27	1b
NO_ANSWER_ALERTED_USER	28	1c
NO_CIRCUIT_AVAILABLE	29	1d

Table 1 Internal LCM Causes for ETSI (continued)

Internal Release Cause Name	Decimal Value	Hex Value
NON_SELECTED_USER_CLEARING	30	1e
NORMAL_CLEARING	31	1f
NORMAL_UNSPECIFIED	32	20
NO_ROUTE_TO_DEST	33	21
NO_ROUTE_TO_TNS	34	22
NO_USER_RESPONDING	35	23
NUMBER_CHANGED	36	24
ONLY_RESTRICT_DIG_INFO_BEARER	37	25
PROTOCOL_ERROR_UNSPEC	38	26
QUALITY_UNAVAIL	39	27
RECOVERY_ON_TIMER_EXPIRY	40	28
REQ_CIRCUIT_UNAVAIL	41	29
REQ_FACILITY_NOT_IMP	42	2a
REQ_FACILITY_NOT_SUBSCR	43	2b
RESOURCES_UNAVAIL_UNSPEC	44	2c
RESPONSE_TO_STATUS_ENQUIRY	45	2d
SERVICE_OR_OPTION_NOT_IMP_UNSPEC	46	2e
SERVICE_OR_OPTION_NOT_AVAIL	47	2f
SUSPEND_EXIST_BUT_NOT_THIS_ID	48	30
SWITCHING_EQUIP_CONGESTION	49	31
TEMPORARY_FAILURE	50	32
UNALLOCATED_NUMBER	51	33
USER_BUSY	52	34

Table 2 Internal LCM Causes for DPNSS

Internal Release Cause Name	Decimal Value	Hex Value
ACCESS_BARRED	53	35
ACKNOWLEDGEMENT	54	36
ADDRESS_INCOMPLETE	55	37
BUSY	56	38
CHANNEL_OUT_OF_SERVICE	57	39
DTE_CONTROLLED_NOT_READY	58	3a
CONGESTION	59	3b
CALL_TERMINATION	60	3c
FACILITY_NOT_REGISTERED	61	3d

Table 2 Internal LCM Causes for DPNSS (continued)

Internal Release Cause Name	Decimal Value	Hex Value
INCOMING_CALLS_BARRED	62	3e
SERVICE_INCOMPATIBLE	63	3f
MESSAGE_NOT_UNDERSTOOD	64	40
NETWORK_ADDRESS_EXTENSION_ERROR	65	41
NETWORK_TERMINATION	66	42
NUMBER_UNOBTAINABLE	67	43
PRIORITY_FORCED_RELEASE	68	44
REJECT	69	45
ROUTE_OUT_OF_SERVICE	70	46
SUBSCRIBER_INCOMPATIBLE	71	47
SIGNAL_NOT_UNDERSTOOD	72	48
SIGNAL_NOT_VALID	73	49
SUBSCRIBER_OUT_OF_SERVICE	74	4a
SIGNALLING_SYSTEM_INCOMPATIBLE	75	4b
SERVICE_TEMPORARILY_UNAVAILABLE	76	4c
SERVICE_UNAVAILABLE	77	4d
DTE_UNCONTROLLED_NOT_READY	78	4e
TRANSFERRED	79	4f

Table 3 Internal LCM Causes for Extra Q767 Causes

Internal Release Cause Name	Decimal Value	Hex Value
INCOMING_CALLS_BARRED_IN_CUG	80	50
SPECIAL_INFORMATION_TONE	81	51
USER_NOT_MEMBER_OF_CUG	82	52

Table 4 Internal LCM Causes for Extra Q761_4 Causes

Internal Release Cause Name	Decimal Value	Hex Value
MISDIALLED_TK_PREFIX	83	53
PARAM_UNREC_PASSED	84	54

Table 5 Internal LCM Causes for ANSI Ibn7

Internal Release Cause Name	Decimal Value	Hex Value
PROPRIETARY	85	55
PREEMPTION	86	56
PREEMPTION_CCT_UNAVAILABLE	87	57

Table 6 Internal LCM Causes for ANSI SS7

Internal Release Cause Name	Decimal Value	Hex Value
UNREC_ELEM_PASSED_ON	88	58
SUB_ABSCENT	89	59
UNDEFINED_BG	90	5a
ROUTING_ERROR	91	5b
PRECEDENCE_BLOCKED	92	5c
CALL_TYPE_INCOMPATIBLE	93	5d
GROUP_RESTRICIONS	94	5e

Table 7 Internal LCM Causes for ATT PRI

Internal Release Cause Name	Decimal Value	Hex Value
CALLING_PARTY_OFF_HOLD	95	5f
CALLING_DROPPED_WHILE_ON_HOLD	96	60
NEW_DESTINATION	97	61
OUTGOING_CALLS_BARRED	98	62

Table 8 Internal LCM Causes for BTNUP

Internal Release Cause Name	Decimal Value	Hex Value
SUB_CONTROLLED_ICB	99	63
CALL_REJECT_CALL_GAPPING	100	64
REJECTED_DIVERTED_CALL	101	65
SELECTIVE_CALL_BARRING	102	66
REMOTE_PROC_ERROR	103	67
TEMPORARY_OOS	104	68
OPERATOR_PRIORITY_ACCESS	105	69
CUG_ACCESS_BARRED	106	6a

Table 8 Internal LCM Causes for BTNUP (continued)

Internal Release Cause Name	Decimal Value	Hex Value
SUBSCRIBER_CALL_TERMINATE	107	6b
FLOW_CONTROLLED_CONGESTION	108	6c
OUT_OF_CATCHMENT_AREA	109	6d
TRANSLATION_OOS	110	6e
PERMANENT_ICB	111	6f
SUBSCRIBER_MOVED	112	70
SUB_NOT_FOUND_DLE	113	71
ANONYMOUS_CALL_REJECTION	114	72
TERMINAL_CONGESTION	115	73
REPEAT_ATTEMPT	116	74

Table 9 Internal LCM Causes for Bell 1268

Internal Release Cause Name	Decimal Value	Hex Value
VACENT_CODE	117	75
PREFIX_0_DIALLED_IN_ERROR	118	76
PREFIX_1_DIALLED_IN_ERROR	119	77
PREFIX_1_NOT_DIALLED	120	78
EXCESSIVE_DIG_CALL_PROCEEDING	121	79
PROT_ERR_THRESHOLD_EXCEEDED	122	7a

Table 10 Internal LCM Causes for ETSI ISUP Version 2

Internal Release Cause Name	Decimal Value	Hex Value
OUTGOING_CALLS_BARRED_IN_CUG	123	7b
INCON_OUTGOING_ACC_AND_SUB_CLASS	124	7c
NON_EXISTENT_CUG	125	7d
MESG_WITH_UNREC_ELEM_DISCARDED	126	7e

Table 11 Internal LCM Causes for Italian ISUP

Internal Release Cause Name	Decimal Value	Hex Value
PREEMPTION_CCT_RES	127	7f

Table 12 Internal LCM Causes for Italian ISUP

Internal Release Cause Name	Decimal Value	Hex Value
PERMANENT_FRAME_MODE_OOS	128	80
PERMANENT_FRAME_MODE_OPERATIONAL	129	81

Table 13 Blacklist Cause Codes

Internal Release Cause Name	Decimal Value	Hex Value
BLACKLIST_NO_CLI	130	82
BLACKLIST_CLI_LENGTH_INVALID	131	83
BLACKLIST_CLI_MATCHED	132	84
BLACKLIST_CPC_RESTRICTED	133	85
BLACKLIST_NOA_RESTRICTED	134	86
BLACKLIST_SPARE_MATCHED	135	87

Table 14 Internal LCM Causes for ISUP V2

Internal Release Cause Name	Decimal Value	Hex Value
PORTED_NUMBER	136	88

Table 15 Internal LCM Causes for NTT ISUP

Internal Release Cause Name	Decimal Value	Hex Value
REDIRECTION_TO_NEW_DEST	137	89

Release 4.2(19) Caveats

This section describes issues and caveats (possibly unexpected behavior) of the Telephony Controller software release 4.2(19).

Open Caveats

There are no open caveats for release 4.2(19).

Resolved Caveats

Caveats listed in Table 16 are resolved.

Table 16 Resolved Caveats, Release 4.2(19)

Identifier	Severity	Component	Headline
CSCdt79938	3	doc	Cisco specific releasecodes.
CSCdt83578	3	ioccc7	GRS messages not answered after SS7 link problem.

Terms and Abbreviations

Term	Description
A/B switch	Switchover controller.
ANSI	American National Standards Institute.
ARU	Alarm Relay Unit.
ASN	Auxiliary Signaling Network.
BLO	Block.
BT	BT Cellnet (customer).
BTNR	British Telecommunications Network Requirement.
CCO	Cisco Connection Online.
CCR	Continuity Check Request.
CDR	Call Detail Record.
CGB	Circuit Group Blocking; message sent to block voice circuits from being used for voice calls.
CGBA	Circuit Group Block acknowledgment; message used to acknowledge receipt of a circuit group blocking message. Indicates that circuits have been blocked.
CGU	Circuit Group Unblocking; message sent to unblock voice circuits that were previously blocked.
CGUA	Circuit Group Unblocking Acknowledgment message.
CIC	Circuit Identification Code.
CNA	Channel Not Available
COOS	Commanded Out-of-service.
COT	Continuity Test.
CPC	Calling Party Category.
CQM	Circuit Group Query Message.
CT	Configuration tool.
DAS	Dial Access Solution. A distributed system used for interconnecting Cisco media gateways (MGWs) to a circuit-switched time-division multiplexing (TDM) network via Signaling System 7 (SS7) protocols for signaling.
DNS	Domain Naming System; mechanism that translates host computer names into Internet addresses.
DPP	Dial plan provisioning.

Term	Description
EISUP	Extended ISDN User Part.
FIFO	First in, first out. In telephony, the process of handling calls in a queue where the first call in is the first call to be handled.
FOOS	Forced Out-of-service.
Glare	When both ends of a line or trunk are seized at the same time but for different uses or users (system should prioritize and switch one to another line or trunk).
GRA	Group Reset Acknowledgment; message used to acknowledge receipt of a Group Reset message. Indicates that the reset has been performed.
GRS	Group Reset; message used to reset a group of voice circuits.
IAM	Initial Address Message; mandatory message; sends routing information.
I/O	Input-output.
IOCC	Input-output channel controller.
IS	In-Service.
ISDN	Integrated Services Digital Network.
ISUP	ISDN User Part; controls calls on SS7 network (setup, coordination, take down) and provides other information.
ITK	Digi International AG (formerly known as IT Telekommunikations AG
IUP	Interconnect User Part.
LCM	Lightspeed Call Model.
LIA	Link Inhibit Acknowledgement message.
LINH	Local Inhibit.
MCID	Malicious Caller ID.
MML	Man-machine language.
MTP	Message Transfer Part; in SS7 protocol it provides basic signaling routing; 3 levels (MTP1, MTP2, MTP3).
NAK	Negative acknowledgment.
NAS	Network access server.
NEBS	Network Equipment Building Standards developed by Bellcore (now Telcordia Technologies).
NEMS	Network element management system.
NOA	Nature of address.
OOS	Out-of-service.
PRI	Primary Rate Interface; fast ISDN designed for telephone switches, computer telephony, and voice processing systems; BRI is slower ISDN.
REL	Release message.
REMMAN	Remotely, manually blocked.
RSC	Reset Circuit.
SC	Service Controller.
SIB	Status Indication Busy.

Term	Description
SLS	Signaling Link Selection; used to distribute load among redundant routes.
SLTM	Signaling Link Test Message.
SNMP-AGT	Simple Network Management Protocol Agent.
SS7	Signaling System 7; a digital signaling system.
STP	Signal transfer point; the packet switch in a Common Channel Interoffice Signaling system.
TAC	Cisco Technical Assistance Center.
TFA	Transfer allowed. An MTP3 message sent to notify adjacent signaling points that it can receive messages.
TFR	Transfer restricted. An MTP3 message sent to notify adjacent signaling points to choose another route if possible.
TNT	Ascend TNT.
VoIP	Voice over IP.
VSC	Virtual Switch Controller. Provides the call control functions for a virtual switch.
Y2K	Year 2000.

Service and Support

You have 24-hour support via Cisco TAC. To initiate a case, contact the closest TAC and tell them your problem. You will be issued a case number that you can check via the phone or the Web. The telephone numbers for the TAC offices can be found at the following URL:

http://www.cisco.com/offices

Click Cisco Technical Assistance Center for business hours, languages available, and other information.

You can also initiate your case online via the Internet at www.cisco.com. Outside these locations, contact the Cisco regional sales office nearest you, or contact your local authorized Cisco distributor. See also the next section, “Cisco Connection Online.”

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems’ primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco’s customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, part of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate and value your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page -2.