Release Notes for Catalyst 6500 Series and Cisco 7600 Series Communication Media Module Software Release 12.2(13)ZP3

Current Release: 12.2(13)ZP3—February 12, 2004

This publication describes the features, modifications, and caveats for the Catalyst 6500 series and Cisco 7600 Series Router Communication Media Module (CMM) software release 12.2(13)ZP3.

Note For detailed installation and configuration procedures for the CMM, refer to the *Catalyst 6500 Series and Cisco 7600 Series Router CMM Installation and Configuration Note* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_14107.htm

Note Except where specifically differentiated, the term "Catalyst 6500 series switches" includes both Catalyst 6500 series and Catalyst 6000 series switches.

Note Throughout this publication, except where specifically differentiated, the term *supervisor engine* refers to Supervisor Engine 1, Supervisor Engine 2, and Supervisor Engine 720. Additionally, the term *Multilayer Switch Feature Card (MSFC)* refers to MSFC, MSFC2, and MSFC3.

CISCO SYSTEMS

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

Contents

System Requirements

This section describes the system requirements for the CMM software release.

Hardware Supported

The CMM requires either a Supervisor Engine 1, Supervisor Engine 2, or Supervisor Engine 720. The supervisor engine can have an MSFC, MSFC2, or MSFC3, but the CMM does not require one for configuration or operation.

Product Number	Product Description	Minimum Software Version	Recommended Software Version	IOS Release[1]	Catalyst Release[1]
WS-SVC-CMM	Communication Media Module	12.2(13)ZP	12.2(13)ZP3		

1. See the "Software Compatibility" section on page 3 for detailed information on which software releases support the various supervisor engines.

Software Compatibility

Note The CMM has its own software image; the image is not bundled with the supervisor engine or MSFC images. See the "Software Upgrade Procedure" section of the *Catalyst 6500 Series and Cisco 7600 Series Router CMM Installation and Configuration Note* for instructions on downloading the image to the CMM Flash memory.

Note Supervisor Engine 720 requires CMM software release 12.2(13)ZP1 or later.

The software requirements for the CMM are as follows:

- Catalyst software release:
  - Supervisor Engine 1 and Supervisor Engine 2—Minimum and recommended software release is 8.1(1) or later
  - Supervisor Engine 720—Minimum and recommended software release is 8.2(1) or later

  Note Online diagnostic features require software release 8.2(1) or later.

- Cisco IOS Release
  - Supervisor Engine 1 and Supervisor Engine 2— Minimum Cisco IOS Release is 12.1(13)E and the recommended Cisco IOS Release is 12.1(20)E
  - Supervisor Engine 720—Minimum Cisco IOS Release is 12.2(14)SX and the recommended Cisco IOS Release is 12.2(17)SX

  Note If your system is running Cisco IOS software on both the supervisor engine and the MSFC, the following images are available: sup11, sup12, sup22, and s720.

Cisco CallManager Support

Software release 12.2(13)ZP3 supports Cisco CallManager release 3.2(2) and later releases.

Orderable Software Images

Table 1 lists the software versions and applicable ordering information for the CMM software.

Table 1 Orderable Software Images

Software Version	Filename	Orderable Product Number[1]
12.2(13)ZP3 image	wscmm-i6s-mz.122-13.zp	S6CMVG3-12213ZP

1. Installed on system; append with "=" for spare on floppy media.

Feature Sets

Table 2 lists the supported features for the CMM T1 and E1 port adapters.

Table 3 lists the supported features for the CMM ad-hoc conferencing and transcoding port adapter.

Table 4 lists the supported features for the CMM FXS module.

Table 5 lists the fax and modem transport parameters for the CMM FXS module.

Table 2 T1 and E1 Port Adapters Supported Features

WS-SVC-CMM-6T1 Port Adapter	WS-SVC-CMM-6E1 Port Adapter
Line code—B8ZS[1], AMI[2]	Line code—HDB3[3], AMI
Frame format—SF[4], ESF[5]	Frame format—with CRC4/no CRC4[6]
SRST[7, 8]	SRST[8]
MGCP gateway fallback[8]	MGCP gateway fallback[8]
FDL[8, 9] with T1 CAS/PRI for extended super frame (only) signaling.	
MGCP and H.323[8]: T1-PRI—Supports up to 18 ports[10] T1-CAS—Supports up to 18 ports[10] T1-CAS E&M[11] Wink Start T1-CAS E&M Delay Dial T1-CAS E&M Immediate Start[12] T1-CAS FXS Loop Start[12] T1-CAS FXO Loop Start[12] T1-CAS FXS Ground Start[12] T1-CAS FXO Ground Start[12] Fax Pass-through Cisco Fax Relay Modem Pass-through Music on Hold (unicast, multicast) DTMF Relay[13, 14] G711 codec (sampling size: 10, 20, and 30 ms) G729 codec (sampling size: 10, 20, 30, 40, 50, 60 ms) QSIG backhaul[15] NSF[8, 15, 16]	MGCP and H.323[8]: E1-PRI—Supports up to 18 ports[10] Fax Pass-through Cisco Fax Relay DTMF Relay[13] Modem Pass-through Music on Hold (unicast, multicast) G711 codec (sampling size: 10, 20, and 30 ms) G729 codec (sampling size: 10, 20, 30, 40, 50, 60 ms) QSIG backhaul[15] E1 R2 CAS signaling[8, 12]

1. B8ZS = binary 8-zero substitution.
2. AMI = alternate mark inversion.
3. HDB3 = high-density bipolar with three zeros.
4. SF = super framing.
5. ESF = extended super framing.
6. CRC = cyclic redundancy check.
7. SRST = Survival Remote Site Telephony.
8. Requires software release 12.2(13)ZC.
9. FDL = Facility Data Link.
10. Number of ports is based on running 12.2(11)ZC software, 20-ms packetization with VAD ON or 30-ms packetization with VAD OFF. With 20-ms packetization and VAD OFF, you are limited to 18 T1-PRI ports, 14 E1-PRI ports, and 16 T1-CAS ports.

11. E&M = ear and mouth.
12. Supported only with H.323.
13. DTMF = Dual Tone Multi-Frequency.
14. DTMF is supported; DTMF/MF is not supported.
15. QSIG backhaul and QSIG supported with H.323 in software release 12.2(13)ZP.
16. NSF = Network-Specific Facilities.

Table 3 Ad-Hoc Conferencing and Transcoding Port Adapter Supported Features

WS-SVC-CMM-ACT Port Adapter
Media support for transcoding and conferencing: • Codec support for G.711 MuLaw, G.711 Alaw, G.729 annex A and annex B, and G.723.1 • Packetization support: – 10 ms to 60 ms for G.711 MuLaw and G.711 Alaw – 10 ms to 60 ms for G.729AB – 30 ms and 60 ms for G.723
Speaker selection (three loudest speakers)
Performance: Up to 8 parties per conference and up to 64 conferences per port adapter
IP precedence bits, DSCP[1], and 802.1Q marking.
One registration entity per port adapter.
Standalone transcoding without associated conference. Codecs and packetization intervals supported are the same as for conferencing.
MTP [2] support.
Modem and fax support through MTP.
Fallback support for transcoding and ad-hoc conferences.
Support for spanning conferences between DSPs on the same port adapter.

1. DSCP = differentiated services code point.
2. MTP = media termination point.

Table 4 FXS Analog Interface Module Features

Digital Signal Processing per Port
G.711, G.729, G.729A voice encoding
Silence suppression
Comfort noise generation
Ring cadence is selectable in 12 different patterns and is programmable in a user-defined cadence
Dual tone multifrequency (DTMF) detection
Signaling, loop start
Modem Pass-through
Line echo cancellation
Impedance (600 ohms), complex 1
Programmable analog gain, signaling timers
FXS Interface Features
Address signaling formats: In-band DTMF
MGCP and H.323 support
Fax Pass-through
Cisco Fax Relay
Signaling formats: Loop start and ground start
Ringing tone: Programmable
Ringing frequency: 25 Hz and 50 Hz
Distance: 300-ohms maximum loop

Table 5 FXS Analog Interface Module Fax and Modem Transport Parameters

Parameter Name	Description	Default
Fax relay enable	Enables/disables fax relay support in the gateway. Enabling this parameter will result in the gateway attempting fax relay negotiation as part of the call setup. If it is enabled but the far end does not support fax relay, the fax call will switch to pass-through mode.	Checkbox checked
Fax error correction mode (ECM) override	ECM occurs in some higher-end fax models that enable fax pages to be transmitted error free. If ECM is enabled, the transmission has a low tolerance to jitter and packet loss. This results in a higher number of failed fax calls. For better reliability (even with higher packet loss), ECM needs to be disabled. ECM is disabled by enabling the checkbox.	Checkbox checked
Maximum fax rate	Defines the maximum fax transmission rate to be used during the fax call. This can be used to restrict the bandwidth utilized for fax transmission.	14400

Table 5 FXS Analog Interface Module Fax and Modem Transport Parameters (continued)

Fax payload size	Configures the size of the fax payload (fax data) carried over the real-time transport protocol (RTP). The value can range between 20 and 48.	20
Non standard facilities country code	Overrides the country code passed by the fax machine with the value defined. Setting the value to default (65535) results in the gateway passing the country code values received from the fax machine to the far end. If the value is not the default, then the gateway will pass the configured value as the country code to the far end. It will suppress the actual country code passed by the fax machine. The country code can be received by the gateway from the far end through ISDN. For details about the nonstandard facilities country code, refer to the T.35 specification.	65535
Non standard facilities vendor code	Overrides the vendor/provider code passed by the fax machine with the value defined. Setting the value to default (65535) results in the gateway passing the vendor code values received from the fax machine to the far end. If the value is not the default, the gateway passes the configured value as the vendor code to the far end. It will suppress the actual vendor code passed by the fax machine. The vendor code can be received by the gateway from the far end through ISDN. For details about the nonstandard facilities vendor code, refer to the T.35 specification.	65535
Fax/Modem Packet Redundancy	Enables packet redundancy support for fax and modem calls. Packet redundancy support results in retransmission of packets in case of problems. Enabling redundancy can have a negative impact on performance.	Checkbox unchecked
Named service event (NSE) type	NSE type attempts to standardize the transfer of tones over the real-time transport protocol (RTP). Two NSE standards exist in Cisco products: one for Cisco IOS gateways and one for non-Cisco IOS gateways. The Catalyst 6500 series switch 8-port T1/E1 PSTN interface module supports both standards. You need to configure the right NSE type based on the network setup. If the module needs to talk to a Cisco IOS gateway (a VG200 or AS5300 for example), set this option to IOS Gateway. If the gateways need to talk to other non-Cisco IOS gateways (such as a WS-X6608-E1/T1, VG248, WS-X6624-FXS, or another WS-SVC-CMM-24FXS), set this option to non-IOS Gateway.	Non-IOS Gateway

Usage Guidelines and Restrictions

This section provides usage guidelines and restrictions for the CMM:

- The recommended VAD setting for the CMM is off.
- SNMP is currently not supported on the CMM.

Caveats

These sections describe the following caveats:

Open Caveats in Release 12.2(13)ZP3

This section describes the known limitations that exist in CMM software release 12.2(13)ZP3.

General Caveats

- For Supervisor Engine 1 and Supervisor Engine 2 in Cisco IOS Release 12.1(19)E, ping does not work between the supervisor engine and the CMM. The functionality of the CMM is not affected. In Cisco IOS Release 12.1(20)E or later releases, ping works between the Supervisor Engine 1 or Supervisor Engine 2 and the CMM. For Supervisor Engine 720, the ping problem was resolved in Cisco IOS Release 12.2(17)SX or later releases. (CSCea27431, CSCed38552)
- Fax relay and pass-through mixed environments result in a fax call failure and VTSP-TIMEOUT messages on the gateway that is configured for fax pass-through.

  Workaround: Configure the same fax mode on both the originating and the terminating gateways. (CSCea38859)
- MGB errors 3, 4, 5, 12, and 30 are seen during stress tests (high number of calls). Some MGB errors appear on both the originating CMM and the terminating CMM during stress tests. The errors are as follows:
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:3
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:4
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:5
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:12
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:30

Note that there is no impact on functionality with these errors. (CSCec13112)

T1/E1 Port Adapter-Related Caveats

- Reconfiguring either T1 or E1 PRI ports using the automatic XML download feature causes all the controllers to shut down. An example of this problem is as follows:
  - 1. Delete a few ports from the XML GUI.
  - 2. Click **Update**.
  - 3. Click **Reset Gateway**.
  - 4. The XML download feature starts downloading the XML file; it takes more than 15 minutes to finish.
  - 5. All 18 controllers are shut down after the configuration has downloaded (including those controllers that were removed from the GUI).

  Workaround: Do a manual reconfiguration. (CSCec26796)
- A few faulty DSPs are displayed in the **show voice dsp** command field, and some DSP errors can occur during stress tests (high number of calls) with 360 E1/PRI calls (four calls per second). Error-related displays are as follows:

```
1. CMM_dsp_open_channel, Err ! Dim FAILED
2. %VTSP-3-DSP_TIMEOUT:DSP timeout on channel 1/1:15 (443175
      event 0x0:DSP ID=0x28101:DSP Disc
3. #show voice dsp
         03     none           BAD           0  0           00     0         0/0
         00     none     1.0   BAD   READY   0  0           00     0         0/0
         01     none           BAD           0  0           00     0         0/0
         02     none           BAD           0  0           00     0         0/0
         03     none           BAD           0  0           00     0         0/0
         04     none           BAD           0  0           00
```

  These conditions apply to this caveat:
  - CCM version: 3.3(3)
  - CMM version: wscmm-i6s-mz.zp1Oct9

  (CSCec66741)
- Sack processing errors are followed by DSP failure and traceback errors with 144 fax relay calls and one CPS. These problems are only seen with T1 CAS. Error-related displays are as follows:

```
*Mar  2 03:25:23.129:jagger_dspmgr_sack_processing:Invalid port 2 0 0
*Mar  2 03:25:23.129:State ack for 1, tcid = 511
*Mar  2 03:25:23.905:jagger_dsp_open_channel, Err ! Dim FAILED TO RESPOND to open
channel. tcid 511 2/2/8

*Mar  2 03:25:27.937:%VTSP-3-DSP_TIMEOUT:DSP timeout on channel 2/2:1:498489,
event 0x0:DSP ID=0x33101:DSP Disc (call mode=0)
*Mar  2 03:25:31.937:%VTSP-3-DSP_TIMEOUT:DSP timeout on channel 2/2:1:498489,
event 0x0:DSP ID=0x33101:DSP error stats (call mode=0)
*Mar  2 03:25:31.937:jagger_dspmgr_tx_flow_disable, Dim chan Err -1 ! reject protocol
modify. tcid 511. 0/0/0

*Mar  2 03:25:32.773:%SYS-3-MGDTIMER:Uninitialized timer, timer stop, timer = 240.
-Process= "VTSP", ipl= 0, pid= 74
-Traceback= 6010F648 60110768 6099D350 609A07F4 60965B20 60571560 605B3988 6060D230
6060DC80 605F1AC0 605F2280
*Mar  2 03:25:58.289:%ALIGN-3-SPURIOUS:Spurious memory access made at 0x6099D3
04 reading 0x12
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D304 609A07F4 60965B20 605
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D34C 609A07F4 60965B20 605
```

```
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 60110750 6099D350 609A07F4 609
65B20 60571560 605B3988 6060D230 6060DC80
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D350 609A07F4 60965B20 605
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:38:23.973:DIM:51:1 - MGB_DM_ERROR_INDICATION (Channel-Dependent):
           Error Code:3 Msg Id:13 TCID 511
*Mar  2 03:38:24.773:jagger_dsp_open_channel, Err ! Dim FAILED TO RESPOND to open
channel. tcid 511 2/2/2

 show voice dsp | include BAD
 5441 16a 00     none     1.0   BAD   READY   0  0           00     0         0/0
```

These conditions apply to this caveat:

- Seen only with fax relay stress test (high number of calls) on T1 CAS
- CCM version: 3.3(3)
- CMM version: wscmm-i6s-mz.zp1Oct9

(CSCec45238)

Ad-Hoc Conferencing and Transcoding Port Adapter-Related Caveats

- Disabling SCCP (using the **no sccp** command) during active transcoding calls may cause spurious memory errors and tracebacks.

  Workaround: Reset SCCP when there are no active calls. (CSCeb39862)

FXS Port Adapter-Related Caveats

- The FXS complex 2 impedance level fails New Zealand compliance testing and is currently not supported. (CSCec18055)
- When a NetMeeting H.323 client call is terminating on a CMM FXS port, the FXS port does not ring. This problem is seen only in H.323 mode; there is no problem with MGCP mode. Note that if you pick up the terminating FXS phone (even though it is not ringing), the call is established with NetMeeting. (CSCec25698)
- Caller ID is currently not supported on FXS ports. (CSCdz87961)

Resolved Caveats in Release 12.2(13)ZP3

This section describes the resolved caveats in CMM software release 12.2(13)ZP3.

- A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

This problem is resolved in Release 12.2(13)ZP3. (CSCed27956, CSCed38527)

- With a Supervisor Engine 720, the **session** command to the CMM does not work with the 12.2(13)ZP1 or 12.2(13)ZP2 images.

  Workaround: Use a direct console connection to the CMM. This problem is resolved in Release 12.2(13)ZP3. (CSCed48518)

- The first Catalyst 6500 series switch has a CMM T1-PRI (H.323) port originating in codec g729r8. A second Catalyst 6500 series switch has a CMM T1-PRI (MGCP) port across an 802.1Q trunk. The transcoding resource includes a WS-SVC-CMM-ACT port adapter on both CMMs (one CMM per switch). On the originating side (the first switch) there is a WS-X6608-T1/E1 module. While calls are running, if you physically remove and then reinsert the WS-X6608-T1/E1 module, the DSP on the CMM on the second switch crashes. This problem is resolved in Release 12.2(13)ZP3. (CSCed50018)

Open Caveats in Release 12.2(13)ZP2

This section describes the known limitations that exist in CMM software release 12.2(13)ZP2.

General Caveats

- For Supervisor Engine 1 and Supervisor Engine 2 in Cisco IOS Release 12.1(19)E, ping does not work between the supervisor engine and the CMM. The functionality of the CMM is not affected. In Cisco IOS Release 12.1(20)E or later releases, ping works between the Supervisor Engine 1 or Supervisor Engine 2 and the CMM. For Supervisor Engine 720, the ping problem was resolved in Cisco IOS Release 12.2(17)SX or later releases. (CSCea27431, CSCed38552)

- Fax relay and pass-through mixed environments result in a fax call failure and VTSP-TIMEOUT messages on the gateway that is configured for fax pass-through.

  Workaround: Configure the same fax mode on both the originating and the terminating gateways. (CSCea38859)

- MGB errors 3, 4, 5, 12, and 30 are seen during stress tests (high number of calls). Some MGB errors appear on both the originating CMM and the terminating CMM during stress tests. The errors are as follows:

  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:3
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:4
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:5
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:12
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:30

  Note that there is no impact on functionality with these errors. (CSCec13112)

T1/E1 Port Adapter-Related Caveats

- Reconfiguring either T1 or E1 PRI ports using the automatic XML download feature causes all the controllers to shut down. An example of this problem is as follows:
  - 1. Delete a few ports from the XML GUI.
  - 2. Click **Update**.
  - 3. Click **Reset Gateway**.
  - 4. The XML download feature starts downloading the XML file; it takes more than 15 minutes to finish.
  - 5. All 18 controllers are shut down after the configuration has downloaded (including those controllers that were removed from the GUI).

  Workaround: Do a manual reconfiguration. (CSCec26796)
- A few faulty DSPs are displayed in the **show voice dsp** command field, and some DSP errors can occur during stress tests (high number of calls) with 360 E1/PRI calls (four calls per second). Error-related displays are as follows:

```
1. CMM_dsp_open_channel, Err ! Dim FAILED
2. %VTSP-3-DSP_TIMEOUT:DSP timeout on channel 1/1:15 (443175
      event 0x0:DSP ID=0x28101:DSP Disc
3. #show voice dsp
         03     none           BAD           0  0           00     0         0/0
         00     none     1.0   BAD   READY   0  0           00     0         0/0
         01     none           BAD           0  0           00     0         0/0
         02     none           BAD           0  0           00     0         0/0
         03     none           BAD           0  0           00     0         0/0
         04     none           BAD           0  0           00
```

  These conditions apply to this caveat:
  - CCM version: 3.3(3)
  - CMM version: wscmm-i6s-mz.zp1Oct9

  (CSCec66741)
- Sack processing errors are followed by DSP failure and traceback errors with 144 fax relay calls and one CPS. These problems are only seen with T1 CAS. Error-related displays are as follows:

```
*Mar  2 03:25:23.129:jagger_dspmgr_sack_processing:Invalid port 2 0 0
*Mar  2 03:25:23.129:State ack for 1, tcid = 511
*Mar  2 03:25:23.905:jagger_dsp_open_channel, Err ! Dim FAILED TO RESPOND to open
channel. tcid 511 2/2/8

*Mar  2 03:25:27.937:%VTSP-3-DSP_TIMEOUT:DSP timeout on channel 2/2:1:498489,
event 0x0:DSP ID=0x33101:DSP Disc (call mode=0)
*Mar  2 03:25:31.937:%VTSP-3-DSP_TIMEOUT:DSP timeout on channel 2/2:1:498489,
event 0x0:DSP ID=0x33101:DSP error stats (call mode=0)
*Mar  2 03:25:31.937:jagger_dspmgr_tx_flow_disable, Dim chan Err -1 ! reject protocol
modify. tcid 511. 0/0/0

*Mar  2 03:25:32.773:%SYS-3-MGDTIMER:Uninitialized timer, timer stop, timer = 240.
-Process= "VTSP", ipl= 0, pid= 74
-Traceback= 6010F648 60110768 6099D350 609A07F4 60965B20 60571560 605B3988 6060D230
6060DC80 605F1AC0 605F2280
*Mar  2 03:25:58.289:%ALIGN-3-SPURIOUS:Spurious memory access made at 0x6099D3
04 reading 0x12
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D304 609A07F4 60965B20 605
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D34C 609A07F4 60965B20 605
```

```
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 60110750 6099D350 609A07F4 609
65B20 60571560 605B3988 6060D230 6060DC80
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D350 609A07F4 60965B20 605
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:38:23.973:DIM:51:1 - MGB_DM_ERROR_INDICATION (Channel-Dependent):
           Error Code:3 Msg Id:13 TCID 511
*Mar  2 03:38:24.773:jagger_dsp_open_channel, Err ! Dim FAILED TO RESPOND to open
channel. tcid 511 2/2/2

 show voice dsp | include BAD
 5441 16a 00     none     1.0   BAD   READY   0  0           00     0         0/0
```

These conditions apply to this caveat:

- Seen only with fax relay stress test (high number of calls) on T1 CAS
- CCM version: 3.3(3)
- CMM version: wscmm-i6s-mz.zp1Oct9

(CSCec45238)

Ad-Hoc Conferencing and Transcoding Port Adapter-Related Caveats

- Disabling SCCP (using the **no sccp** command) during active transcoding calls may cause spurious memory errors and tracebacks.

  Workaround: Reset SCCP when there are no active calls. (CSCeb39862)

FXS Port Adapter-Related Caveats

- The FXS complex 2 impedance level fails New Zealand compliance testing and is currently not supported. (CSCec18055)
- When a NetMeeting H.323 client call is terminating on a CMM FXS port, the FXS port does not ring. This problem is seen only in H.323 mode; there is no problem with MGCP mode. Note that if you pick up the terminating FXS phone (even though it is not ringing), the call is established with NetMeeting. (CSCec25698)
- Caller ID is currently not supported on FXS ports. (CSCdz87961)

Resolved Caveats in Release 12.2(13)ZP2

This section describes the resolved caveats in CMM software release 12.2(13)ZP2.

- When setting FXS ports to ground start in H.323 mode, ringing does not stop for unpicked incoming calls. The port rings constantly even after the calling party goes onhook. This problem is resolved in Release 12.2(13)ZP2. (CSCeb80084)
- With Supervisor Engine 1, Supervisor Engine 2, and Supervisor Engine 720, the CMM fails the supervisor engine online diagnostic tests. This problem occurs when the diagnostics are set to minimal or complete. When the diagnostics fail, the following message is displayed:

  ```
  2003 Nov 25 18:59:02 PST -08:00 %SYS-4-NVLOG:SYNDIAGS:Syndiags failed on Module #2.
  Use 'show test 2' to see results of tests. 2003 Nov 25 18:59:02 PST -08:00
  %SYS-3-MOD_FAIL:Module 2 failed to come online
  ```

Workaround: Perform the following to bring the CMM online:

1) Use the **set test diaglevel** command to set the diagnostic level to **bypass**. With this setting, the CMM will come online.

2) After the CMM is online, session to the CMM and unshut the Gigabit interface and then write the configuration to memory.

3) From the supervisor engine CLI, turn the supervisor engine diagnostics back on using the **set test diaglevel complete** command.

4) Power cycle the CMM. The diagnostics will now run on the CMM. This problem is resolved in Release 12.2(13)ZP2. (CSCed12869)

- The CMM will fail the supervisor engine online diagnostics test. This will occur when the test is set to minimal or complete. The following message will display:

```
2003 Nov 25 18:59:02 PST -08:00 %SYS-4-NVLOG:SYNDIAGS:Syndiags failed on Module #2.
Use 'show test 2' to see results of tests. 2003 Nov 25 18:59:02 PST -08:00
%SYS-3-MOD_FAIL:Module 2 failed to come online
```

This failure occurs with any supervisor engine running Catalyst software release 8.2(1) when the online diagnostics are set to minimal or complete. All CMMs are affected and the problem occurs in any slot of a 6509 or 6513 switch. This problem occurs because the Gigabit interface on the CMM is shutdown at the factory.

Workaround: Set the supervisor engine diagnostics to bypass modules using the **set test diaglevel bypass** command. This allows the CMM to come online. After the CMM is online, session to the CMM and unshut the Gigabit interface and write to memory. Then from the supervisor engine CLI, set the diagnostics back on using the **set test diaglevel complete** command. Power cycle the CMM. Diagnostics will now run on the CMM. This problem is resolved in Release 12.2(13)ZP2. (CSCed12869)

Open Caveats in Release 12.2(13)ZP1

This section describes the known limitations that exist in CMM software release 12.2(13)ZP1.

General Caveats

- With Supervisor Engine 1, Supervisor Engine 2, and Supervisor Engine 720, the CMM fails the supervisor engine online diagnostic tests. This problem occurs when the diagnostics are set to minimal or complete. When the diagnostics fail, the following message is displayed:

```
2003 Nov 25 18:59:02 PST -08:00 %SYS-4-NVLOG:SYNDIAGS:Syndiags failed on Module #2.
Use 'show test 2' to see results of tests. 2003 Nov 25 18:59:02 PST -08:00
%SYS-3-MOD_FAIL:Module 2 failed to come online
```

Workaround: Perform the following to bring the CMM online:

1) Use the **set test diaglevel** command to set the diagnostic level to **bypass**. With this setting, the CMM will come online.

2) After the CMM is online, session to the CMM and unshut the Gigabit interface and then write the configuration to memory.

3) From the supervisor engine CLI, turn the supervisor engine diagnostics back on using the **set test diaglevel complete** command.

4) Power cycle the CMM. The diagnostics will now run on the CMM. (CSCed12869)

- Fax relay and pass-through mixed environments result in a fax call failure and VTSP-TIMEOUT messages on the gateway that is configured for fax pass-through.

  Workaround: Configure the same fax mode on both the originating and the terminating gateways. (CSCea38859)

- MGB errors 3, 4, 5, 12, and 30 are seen during stress tests (high number of calls). Some MGB errors appear on both the originating CMM and the terminating CMM during stress tests. The errors are as follows:
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:3
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:4
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:5
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:12
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:30

  Note that there is no impact on functionality with these errors. (CSCec13112)

T1/E1 Port Adapter-Related Caveats

- Reconfiguring either T1 or E1 PRI ports using the automatic XML download feature causes all the controllers to shut down. An example of this problem is as follows:
  - 1. Delete a few ports from the XML GUI.
  - 2. Click **Update**.
  - 3. Click **Reset Gateway**.
  - 4. The XML download feature starts downloading the XML file; it takes more than 15 minutes to finish.
  - 5. All 18 controllers are shut down after the configuration has downloaded (including those controllers that were removed from the GUI).

  Workaround: Do a manual reconfiguration. (CSCec26796)

- A few faulty DSPs are displayed in the **show voice dsp** command field, and some DSP errors can occur during stress tests (high number of calls) with 360 E1/PRI calls (four calls per second). Error-related displays are as follows:

```
1. CMM_dsp_open_channel, Err ! Dim FAILED
2. %VTSP-3-DSP_TIMEOUT:DSP timeout on channel 1/1:15 (443175
      event 0x0:DSP ID=0x28101:DSP Disc
3. #show voice dsp
         03     none           BAD           0  0           00     0          0/0
         00     none     1.0   BAD   READY   0  0           00     0          0/0
         01     none           BAD           0  0           00     0          0/0
         02     none           BAD           0  0           00     0          0/0
         03     none           BAD           0  0           00     0          0/0
         04     none           BAD           0  0           00
```

  These conditions apply to this caveat:
  - CCM version: 3.3(3)
  - CMM version: wscmm-i6s-mz.zp1Oct9

  (CSCec66741)

- Sack processing errors are followed by DSP failure and traceback errors with 144 fax relay calls and one CPS. These problems are only seen with T1 CAS. Error-related displays are as follows:

```
*Mar  2 03:25:23.129:jagger_dspmgr_sack_processing:Invalid port 2 0 0
*Mar  2 03:25:23.129:State ack for 1, tcid = 511
*Mar  2 03:25:23.905:jagger_dsp_open_channel, Err ! Dim FAILED TO RESPOND to open
channel. tcid 511 2/2/8

*Mar  2 03:25:27.937:%VTSP-3-DSP_TIMEOUT:DSP timeout on channel 2/2:1:498489,
event 0x0:DSP ID=0x33101:DSP Disc (call mode=0)
*Mar  2 03:25:31.937:%VTSP-3-DSP_TIMEOUT:DSP timeout on channel 2/2:1:498489,
event 0x0:DSP ID=0x33101:DSP error stats (call mode=0)
*Mar  2 03:25:31.937:jagger_dspmgr_tx_flow_disable, Dim chan Err -1 ! reject protocol
modify. tcid 511. 0/0/0

*Mar  2 03:25:32.773:%SYS-3-MGDTIMER:Uninitialized timer, timer stop, timer = 240.
-Process= "VTSP", ipl= 0, pid= 74
-Traceback= 6010F648 60110768 6099D350 609A07F4 60965B20 60571560 605B3988 6060D230
6060DC80 605F1AC0 605F2280
*Mar  2 03:25:58.289:%ALIGN-3-SPURIOUS:Spurious memory access made at 0x6099D3
04 reading 0x12
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D304 609A07F4 60965B20 605
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D34C 609A07F4 60965B20 605
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 60110750 6099D350 609A07F4 609
65B20 60571560 605B3988 6060D230 6060DC80
*Mar  2 03:25:58.293:%ALIGN-3-TRACE:-Traceback= 6099D350 609A07F4 60965B20 605
71560 605B3988 6060D230 6060DC80 605F1AC0
*Mar  2 03:38:23.973:DIM:51:1 - MGB_DM_ERROR_INDICATION (Channel-Dependent):
           Error Code:3 Msg Id:13 TCID 511
*Mar  2 03:38:24.773:jagger_dsp_open_channel, Err ! Dim FAILED TO RESPOND to open
channel. tcid 511 2/2/2

 show voice dsp | include BAD
 5441 16a 00     none     1.0   BAD   READY   0  0           00     0         0/0
```

  These conditions apply to this caveat:

  - Seen only with fax relay stress test (high number of calls) on T1 CAS
  - CCM version: 3.3(3)
  - CMM version: wscmm-i6s-mz.zp1Oct9

  (CSCec45238)

Ad-Hoc Conferencing and Transcoding Port Adapter-Related Caveats

- Disabling SCCP (using the **no sccp** command) during active transcoding calls may cause spurious memory errors and tracebacks.

  Workaround: Reset SCCP when there are no active calls. (CSCeb39862)

FXS Port Adapter-Related Caveats

- When setting FXS ports to ground start in H.323 mode, ringing does not stop for unpicked incoming calls. The port rings constantly even after the calling party goes onhook. (CSCeb80084)
- The FXS complex 2 impedance level fails New Zealand compliance testing and is currently not supported. (CSCec18055)

- When a NetMeeting H.323 client call is terminating on a CMM FXS port, the FXS port does not ring. This problem is seen only in H.323 mode; there is no problem with MGCP mode. Note that if you pick up the terminating FXS phone (even though it is not ringing), the call is established with NetMeeting. (CSCec25698)
- Caller ID is currently not supported on FXS ports. (CSCdz87961)

Resolved Caveats in Release 12.2(13)ZP1

This section describes the resolved caveats in CMM software release 12.2(13)ZP1.

- When the FXS port adapter is integrated to an Octel 250/350, a call may occasionally fail to reach the intended voice-mail box and instead go to an open tree.

  Workaround: When the call goes to an open tree, you can access the desired voice-mail box either to leave or retrieve messages. To leave a message, enter the voice-mail box number for the desired person when you hear the open-tree announcement and then leave a message as usual. To retrieve messages, press the # key when you hear the open-tree announcement and then enter the voice-mail box number and proceed as usual. This problem is resolved in Release 12.2(13)ZP1. (CSCec34206)
- When an E1 controller configured for no-CRC4 framing from the CMM is connected to another device, the CMM sends a continual remote alarm indication to the remote device without an alarm being detected. This problem does not happen when the default framing option CRC4 is used. This situation results in the remote end not bringing up the service and no data is passed on any circuit.

  Workaround: If you disconnect and reconnect the E1 very quickly, the alarm condition is not sent and the link comes up. Another workaround is to use CRC4 framing instead of no-CRC4 framing. This problem is resolved in Release 12.2(13)ZP1. (CSCuk46408)
- Some calls appear orphaned on the T1 and MTP/conferencing services. After a switchover or switchback occurs, some calls may not be cleaned up properly because the implementation for ICMP unreachable is missing.

  Workaround: Disable and reenable the profile or interface that is associated with the orphaned calls. This problem is resolved in Release 12.2(13)ZP1. (CSCec05656)

Open Caveats in Release 12.2(13)ZP

This section describes the known limitations that exist in CMM software release 12.2(13)ZP.

General Caveats

- Fax relay and pass-through mixed environments result in a fax call failure and VTSP-TIMEOUT messages on the gateway that is configured for fax pass-through.

  Workaround: Configure the same fax mode on both the originating and the terminating gateways. (CSCea38859)
- MGB errors 3, 4, 5, 12, and 30 are seen during stress tests (high number of calls). Some MGB errors appear on both the originating CMM and the terminating CMM during stress tests. The errors are as follows:
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:3
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:4
  - MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:5

- MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:12
- MGB_DM_ERROR_INDICATION (Channel-Dependent):Error Code:30

Note that there is no impact on functionality with these errors. (CSCec13112)

T1/E1 Port Adapter-Related Caveats

- Reconfiguring either T1 or E1 PRI ports using the automatic XML download feature causes all the controllers to shut down. An example of this problem is as follows:
  - 1. Delete a few ports from the XML GUI.
  - 2. Click **Update**.
  - 3. Click **Reset Gateway**.
  - 4. The XML download feature starts downloading the XML file; it takes more than 15 minutes to finish.
  - 5. All 18 controllers are shut down after the configuration has downloaded (including those controllers that were removed from the GUI).

  Workaround: Do a manual reconfiguration. (CSCec26796)
- When an E1 controller configured for no-CRC4 framing from the CMM is connected to another device, the CMM sends a continual remote alarm indication to the remote device without an alarm being detected. This does not happen when the default framing option CRC4 is used. This situation results in the remote end not bringing up the service and no data is passed on any circuit.

  Workaround: If you disconnect and reconnect the E1 very quickly, the alarm condition is not sent and the link comes up. Another workaround is to use CRC4 framing instead of no-CRC4. (CSCuk46408)

Ad-Hoc Conferencing and Transcoding Port Adapter-Related Caveats

- Some calls appear orphaned on the T1 and MTP/conferencing services. After a switchover or switchback occurs, some calls may not be cleaned up properly because the implementation for ICMP unreachable is missing.

  Workaround: Disable and reenable the profile or interface that is associated with the orphaned calls. (CSCec05656)
- Disabling SCCP (using the **no sccp** command) during active transcoding calls may cause spurious memory errors and tracebacks.

  Workaround: Reset SCCP when there are no active calls. (CSCeb39862)

FXS Port Adapter-Related Caveats

- When the FXS port adapter is integrated to an Octel 250/350, a call may occasionally fail to reach the intended voice-mail box and instead go to an open tree.

  Workaround: When the call goes to an open tree, you can access the desired voice-mail box either to leave or retrieve messages. To leave a message, enter the voice-mail box number for the desired person when you hear the open-tree announcement and then leave a message as usual. To retrieve messages, press the # key when you hear the open-tree announcement and then enter the voice-mail box number and proceed as usual. (CSCec34206)

- When setting FXS ports to ground start in H.323 mode, ringing does not stop for unpicked incoming calls. The port rings constantly even after the calling party goes onhook. (CSCeb80084)
- The FXS complex 2 impedance level fails New Zealand compliance testing and is currently not supported. (CSCec18055)
- When a NetMeeting H.323 client call is terminating on a CMM FXS port, the FXS port does not ring. This problem is seen only in H.323 mode; there is no problem with MGCP mode. Note that if you pick up the terminating FXS phone (even though it is not ringing), the call is established with NetMeeting. (CSCec25698)
- Caller ID is currently not supported on FXS ports. (CSCdz87961)

Resolved Caveats in Release 12.2(13)ZP

This section describes resolved caveats in CMM software release 12.2(13)ZP.

General Caveats

- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.2(13)ZP. (CSCdu53656)
- A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

  This problem is resolved in Release 12.2(13)ZP. (CSCea28131)

Manual Configuration in the Absence of CMM-Specific XML Files

If you do not have the CMM-specific XML files or do not want to install CMM-specific XML files, you need to perform the following:

Note The problem requiring manual configuration in the absence of CMM-specific XML files has been fixed in the Cisco CallManager 3.2(2c)spF-rc3 support patch. If you load that patch, you do not need to perform the following configuration commands.

- Configure the **clock source line primary** and **clock source line secondary** under T1/E1 controllers as per your requirements. The secondary clock source is a backup for the primary clock source and the CMM supports secondary clock sources from 1 to 17. The CMM must have **clock source line primary** and **clock source line secondary** configured to avoid any clock slips.
- The default configuration for the CMM is "Cisco Fax Relay." To run "Fax pass through calls," you need to supplement the default configuration with the following two commands:
  - **mgcp modem pass through voip mode cisco**
  - **no ccm fax protocol cisco**
- The default configuration for "echo cancel coverage" is set to 64 ms. This default can be changed as needed under **voice-port** configuration.
- The default configuration for "input gain" and "output attenuation" is set to 0 dB. This default can be changed as needed under **voice-port** configuration.

The manual configuration is lost on a reload if you set the CMM for configuration download from Cisco CallManager. If the configuration is lost, you must reconfigure it. To retain the manual configuration, disable the automatic configuration download from Cisco CallManager before doing a CMM reload.

Related Documentation

For more detailed installation and configuration information, refer to these publications:

- *Catalyst 6500 Series and Cisco 7600 Series Router CMM Installation and Configuration Note*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Regulatory Compliance and Safety Information for the Cisco 7600 Series Routers*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Cisco 7600 Series Router Module Installation Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Cisco 7600 Series Router Cisco IOS Command Reference*

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

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_inpck/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 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

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/

- *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 "Related Documentation" section on page 21.