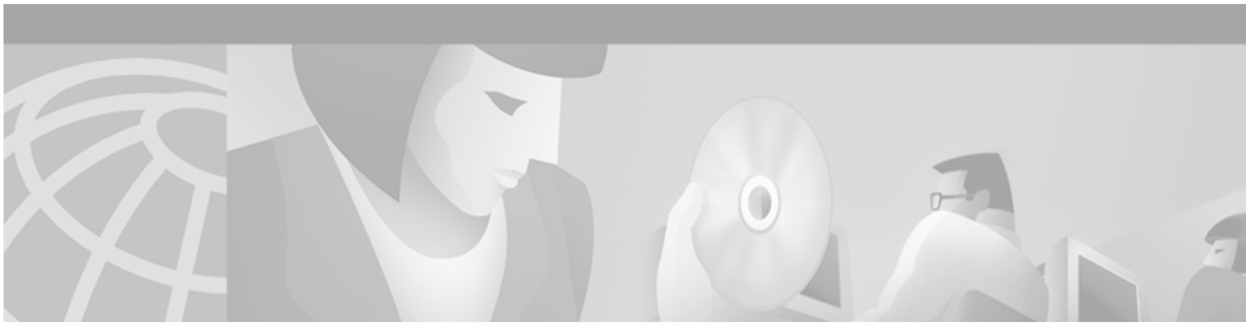

Release Notes for Cisco ASAP Solution Releases 1.0 and 2.0

These release notes describe the following topics:

- Introduction
- Solution Components
- Supported Features
- Caveats
- Important Notes
- Limitations and Restrictions
- Upgrading to the Cisco ASAP Solution
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance

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

Document History

Document Version	Date	Notes
1	12/12/01	This document was first published as *Cisco ASAP Solution 1.0 Release Notes*.
2	03/04/02	Updated the recommended IOS software images that contain fixes for the security issues related to SNMP message handling.
3	06/11/02	This document was renamed *Release Notes for Cisco ASAP Solution Releases 1.0 and 2.0*, and includes Release 2.0 information.

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

Introduction

The Cisco Any Service, Any Port (ASAP) Solution architecture allows service providers to deliver integrated data, voice, fax, and wireless data (V.110) services on a single platform. For an overview of the Cisco ASAP Solution architecture, components, and services, see the "Solution-Specific Documents" section on page 20.

The Cisco ASAP Solution provides the following benefits and features:

- Universal ports provide *any service on any port* of a single universal gateway *at any time*. Call types that are supported are modem, asynchronous data, voice, fax, and wireless data (V.110).
- As all the above call types are implemented on a single universal gateway, capital costs are minimized and the complexity of preprovisioning gateways for different services is eliminated.
- *Dynamic call-by-call handling*—Offering any call type on any port—is the key software function that makes it possible for you to use the universal port DSP functionality by mapping incoming calls to different service-implementation software running on the gateway.
- *Enhanced call admission control*—Ensures that a gateway never accepts a call that it cannot complete; this feature proactively informs network elements, such as H.323 gatekeepers, when the gateway is reaching capacity to aid in intelligent voice/fax call-routing decisions.

Note For more features supported by the Cisco ASAP Solution, see the "Supported Features" section on page 9.

What Changed Between Releases 1.0 and 2.0?

Cisco IOS Software

Cisco ASAP Solution Release 2.0 introduces Cisco IOS Release 12.2(2)XB5 on the gateway components. See Table 3 on page 6.

Caveats

See the "Caveats" section on page 10 for resolved and open caveats for Cisco ASAP Solution Release 2.0.

Note There are no new features in Cisco ASAP Solution 2.0.

Solution Components

The Cisco ASAP Solution may feature both Cisco and third-party components, as listed in the following sections:

- Cisco Core Components
- Cisco Network Management Components and Other Tools
- Cisco ASAP Solution Software Matrix
- Third-Party Components

Cisco Core Components

Table 1 describes the core components tested in Cisco ASAP Solution Releases 1.0 and 2.0. The software releases that were tested for the Cisco ASAP Solution are listed in Table 3 on page 6.

Note Different customers use different subsets of the following components.

Tip When you view this document online, the components in the Hardware column of Table 1 serve as links to the platform-specific release notes. Refer to the release notes for each platform and software image that you use in the Cisco ASAP Solution.

Table 1 Cisco Core Components for the Cisco ASAP Solution

Hardware	Purpose
Cisco AS5350	Universal gateways
Cisco AS5400	
Cisco AS5850	
Cisco AS5300	Dial-only gateways
Cisco AS5800	
Cisco 3660	H.323 gatekeepers and directory gatekeepers
Cisco 7200	
Cisco SC2200 (Sun Netra t 100/105, t 1400/1405, t 1100/1105, t 1120/1125)	Signaling controller (required for SS7)
Cisco SLT 2611	SS7 signaling link termination system

Cisco Network Management Components and Other Tools

Table 2 describes the optional Cisco network management components and additional tools that you can use with the Cisco ASAP Solution. For a list of the software releases that were tested for the Cisco ASAP Solution, see Table 3 on page 6.

Tip When you view this document online, the components in the first column of Table 2 serve as links to release notes and platform-specific documentation. Refer to the release notes for each platform and software release that you use in the Cisco ASAP Solution.

Table 2 Cisco Network Management Components for the Cisco ASAP Solution

Component	Minimum Software Release Required	Platform Hardware	Platform Software
Cisco Info Center	CIC Release 3.0		Solaris 2.6 or 2.7 with latest patches
Cisco Resource Pool Management Server (Cisco RPMS)	RPMS Release 1.1	Sun Ultra 60 or higher	Solaris 2.6, 2.7, or 2.8 with latest patches Oracle 8.*x* and later releases
			Netscape 4.04 or later releases Microsoft Internet Explorer 4.*x* and later releases
Cisco L2TP Network Server (Cisco 7200)	Release 12.1(5)T9		
CiscoWorks2000 Voice Manager	CiscoWorks2000 VM Release 2.0.2	Windows server with 450 MHz CPU	Windows NT 4.0 with Service Pack 5, Cisco Works2000 CD One
		Sun server (SPARC/ UltraSPARC) with 333 MHz CPU	Solaris 2.6 with the latest kernel, Cisco Works2000 CD One for Solaris
		Any client	Windows 95 running Netscape 4.04 or Internet Explorer 4.01 and 64 MB of virtual memory; or Windows NT running Netscape 4.04 or Internet Explorer 4.01 and 64 MB of virtual memory; or Solaris running Netscape 4.04 with Telnet and Java enabled and 64 MB of virtual memory
Cisco Universal Gateway Manager (Cisco UGM)	Cisco UGM Release 1.0	Sun Ultra 60 or later versions	Solaris 2.6; Cisco EMF 3.0.4, Patch 12.
Cisco MGC Node Manager (CMNM)	CMNM Release 1.5	Sun Ultra 60 or later versions	Sun Solaris 2.6
Cisco Billing and Measurements Server (Cisco BAMS)	Cisco BAMS Release 3.08	Sun Netra series	

Table 2 Cisco Network Management Components for the Cisco ASAP Solution (continued)

Component	Minimum Software Release Required	Platform Hardware	Platform Software
Cisco Voice Services Provisioning Tool (Cisco VSPT)	Cisco VSPT Release 1.6	Sun Ultra-5 Workstation	Sun Solaris 2.6
Cisco Access Registrar (Cisco AR)	Cisco AR Release 1.7 R1		Sun Solaris 2.6
Cisco Internet Performance Manager (Cisco IPM)[1]	Cisco IPM Release 2.3, Cisco IOS 12.1(3) or later	Windows server and client	Windows NT 4.0 with Service Pack 6a; Windows 2000 Professional with Service Pack 1; Windows 2000 Server with Service Pack 1; Windows 98 (client only
		Sun server and client	Solaris 2.6 or 2.7 with latest patches

[1] Requirements depend upon client-server architecture. See documentation for Internetwork Performance Monitor, Release 2.3, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ipmcw2k/cipm23/index.htm

Note Consult with your Cisco account representative regarding the suitability of the above components for your needs.

Cisco ASAP Solution Software Matrix

Table 3 on page 6 is a matrix that describes the tested Cisco IOS and other software releases for a given release of the Cisco ASAP Solution. If you are implementing the Cisco ASAP Solution for the first time, Cisco recommends that you use the most recent software releases in Table 3. If you have already implemented the Cisco ASAP Solution in your network, use the entries in Table 3 as options for upgrading your solution components.

Table 3 also provides hyperlinks to release notes and the Cisco IOS Upgrade Planner where you can download Cisco IOS images for components of the Cisco ASAP Solution. See the "How to Use the Cisco IOS Upgrade Planner" section on page 7.

Tip To determine the release currently running on a platform, see the "Determining Software Release Versions" section on page 8.

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

- Select a feature set. Consult with your Cisco account representative to determine the Cisco IOS features that are required for your installation.
- Check the release notes for the platform and software release for Flash and DRAM memory requirements which vary, depending on whether IP Plus or Enterprise Plus Cisco IOS software images are used, and whether the images support Open Settlement Protocol (OSP).

Note OSP enables service providers who use Cisco Open Packet Telephony to communicate directly with a clearinghouse service provider. OSP may also be required in certain billing environments. Contact your Cisco account representative for further information.

OSP and clearinghouses are described as part of the Cisco Wholesale Voice Solution at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/index.htm

The binary images of the following feature sets are different, although their functionality is the same:

Identifier	Feature Set (Image Variant)
-is-	IP Plus
-js-	Enterprise Plus
-ik8s-	IP Plus with OSP
-jk8s-	Enterprise Plus with OSP
-ix-	IP with H.323

Tip When you view this document online, some of the components in the first column of Table 3 serve as links to the IOS Upgrade Planner where you can download the Cisco IOS images. The software release names in the rest of the table serve as links to the platform-specific release notes.

Table 3 Cisco ASAP Solution Software Matrix

	Cisco Software Releases That Were Tested for Cisco ASAP Solution Release —		
Component	2.0 06/11/02	1.0 03/04/02	(Before Cisco IOS Security Update)[1] 1.0 12/12/01
Cisco AS5350 (Universal Port)	12.2(2)XB5	12.2(2)XA5	12.2(2)XA4
Cisco AS5400 (Universal Port)	12.2(2)XB5	12.2(2)XA5	12.2(2)XA4
Cisco AS5300 (Dial Only)	12.2(2)XB5	12.2(2)XA5	12.2(2)XA4
Cisco AS5850 (Dial Only)	12.2(2)XB5	12.1(5)XV4	12.1(5)XV3

Table 3 Cisco ASAP Solution Software Matrix (continued)

	Cisco Software Releases That Were Tested for Cisco ASAP Solution Release —		
Component	2.0 06/11/02	1.0 03/04/02	(Before Cisco IOS Security Update)[1] 1.0 12/12/01
Cisco AS5800 (Dial Only)	12.2(2)XB5	12.1(5)XM7	12.1(5)XM5
Cisco 3660 (Gatekeeper)	12.2(2)XA5	12.2(2)XA5	12.2(2)XA1
Cisco 7200 (Gatekeeper)	12.2(2)XA5	12.2(2)XA5	12.2(2)XA1
Cisco SC2200 (Signaling Controller)	7.4(12) Patches[2] CSCOgp016, CSCOgs016	7.4(12) Patch[2] CSCOgs012	7.4(12) Patches[2] CSCOgp008, CSCOgs009
Cisco 2611 SLT (Signaling Link Terminal)	12.2(8)T	12.2(2)XA5	12.2(2)XA4
Cisco RPMS	1.1	1.1	1.1
Cisco CMNM	1.5 P 2	1.5	1.5
Cisco UGM	2.0 with Cisco EMF 3.2 patch 1.4	2.0	1.0
Cisco VSPT	1.6(4)	1.6	1.6
Cisco AR	1.7R3	1.7R1	1.7R1
CIC	3.0.1	3.0.1	3.0.1

[1] Because of security concerns, Cisco recommends that you do not use the Cisco IOS releases in this column. For details see Cisco Security Advisory: Malformed SNMP Message-Handling Vulnerabilities at the following URL: http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

[2] For the current list of patches, refer to the Release Notes for the Cisco Media Gateway Controller (MGC) software Release 7.4(12) at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/relnote/7412tv12.htm

How to Use the Cisco IOS Upgrade Planner

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

Step 1 To access the Cisco IOS Upgrade Planner, complete one of the following steps:

a. Within the online version of these release notes, click the platform name in Table 3.

b. Go to http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?, and select the platform name from the first column.

Step 2 Go to the Select Release column and find the heading Early Deployment Updates.

Step 3 Search for the release name that corresponds with the name in the Solution Release column in Table 3 (under "Cisco Software Releases That Were Tested for Cisco ASAP Solution Release —").

Step 4 Click the link for that release.

The IOS Upgrade Planner is refreshed.

Step 5 Read all instructions on that page. Then, click the appropriate software feature in the column Select Software Feature.

The IOS Upgrade Planner is refreshed.

Step 6 Read all instructions and the agreement on that page. If you agree with the conditions, click **I read above requirements and agree with them**.

The IOS Upgrade Planner is refreshed.

Step 7 Read all instructions on that page. You can select from a variety of download options. Cisco recommends that you click the file name of the binary image under File name in the Software Download table.

⚠ **Caution** Make sure that you have enough memory on your system for the file. Note the Size 'Bytes' column in the Cisco IOS Upgrade Planner.

Step 8 Continue as prompted.

Third-Party Components

Table 4 lists optional third-party components for the Cisco ASAP Solution. The Trinagy product is used for managing network performance, and MIND-iPhonEX is used for billing.

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

Table 4 Third-Party Components

Component	Manufacturer	Product and Version	Website
Trinagy network performance management	Trinagy	TREND 3.6.1 or later versions; TRENDweb 3.2	http://www.trinagy.com
MIND-iPhonEX	MIND CTI	MIND-iPhonEX 4.2 (w/ Oracle 8.06)	http://www.mindcti.com

Determining Software Release Versions

The following will assist you in determining the software versions currently running on the following platforms. For other platforms, refer to their respective documentation.

Cisco IOS Software

To determine the release of Cisco IOS software that is currently running, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 Software c5350-i-mz, Version 12.2(2), RELEASE SOFTWARE
```

Cisco SC2200

Enter the following MML command on the Cisco SC2200:

```
va-perch mml> rtrv-ne
   MGC-01 - Media Gateway Controller 2001-11-16 14:13:44 M  RTRV
   "Type:MGC"
   "Hardware platform:sun4u sparc SUNW,Ultra-80"
   "Vendor:"Cisco Systems, Inc.""
   "Location:MGC-01 - Media Gateway Controller"
   "Version:"7.4(12)""
   "Platform State:ACTIVE"
```

To determine the patch level, enter the following command on the Cisco SC2200:

```
hostname# pkginfo | grep CSCO
```

Cisco RPMS Host

Enter the following command from within the RPMS home directory of the RPMS host:

```
<RPMS_home_dir> /sbin/crpms-info
```

Supported Features

The following features are enabled by the Cisco ASAP Solution, Release 1.0, and are supported by Release 2.0:

- Call-by-call voice, dial, and fax services on a single platform (Cisco AS5350 and AS5400 universal gateways) using a universal port DSP
- Dial support through the Cisco AS5400, Cisco AS5350, Cisco AS5300, Cisco AS5800, and the Cisco AS5850
- SS7 interconnect
- ISUP-to-ISUP TDM switching (without ISUP transparency)
- ISUP-to-PRI TDM switching
- ISUP-to-ISUP VoIP calls (without ISUP transparency)
- ISUP-to-CAS VoIP calls
- ISUP-to-PRI VoIP Calls

The following features are supported by the Cisco ASAP Solution, Releases 1.0 and 2.0:

- Cisco RPMS for port policy management (for dial calls only)
- VoIP services: phone to phone, PC to phone, prepaid and postpaid calling, and long-distance toll bypass
- Remote SLTs and gateways
- Network management using Cisco UGM, CMNM, Cisco RPMS, Cisco VSPT, and Cisco AR (for RADIUS-compliant proxy and local AAA services)

For a list of other features that are applicable to components that support the Cisco ASAP Solution, refer to the Cisco IOS Release 12.2(2)XA at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/index.htm

Note For available features, always refer to the most recent Cisco documentation, including release notes, for the Cisco operating system that a particular platform is running. Refer also to Cisco IOS Software Configuration at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm

Caveats

The following are the severity 1, severity 2, and some key severity 3 caveats for the components in the Cisco ASAP Solution. Workarounds are provided where applicable.

Note For additional caveats that may affect your Cisco ASAP Solution network, refer to the release notes for each platform and software release that you use as a solution component. If you view this document online, the software release numbers in Table 3 serve as links to the platform-specific release notes.

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To find the open caveats for all components used in a specific implementation of the Cisco ASAP Solution, you must query the system for each of the component and software releases used or being planned for your Cisco ASAP Solution network. To reach Bug Navigator II, go to http://www.cisco.com and press Login. Then choose Software Center > Cisco IOS Software > Cisco Bugtool Navigator II. You can also go directly to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats—Cisco ASAP Solution Release 2.0

- The Cisco AS5400 or AS5350 echo cancelers are not disabled. (**CSCdv53170**)

  The echo cancelers for the Cisco AS5350 and AS5400 are not disabled when a 2100-Hz disabler tone with periodic phase-reversals is sent.

  There is no workaround.

- Cisco AS5800 displays `XCSP:Slot 0 not initialized` messages on the console. (**CSCdw70558**)

  While calls are being cleared, `XCSP:Slot 0 not initialized` messages are sometimes displayed on the console of the Cisco AS5800.

  There is no workaround.

- Cisco AS5850 does not answer more than 256 ISDN calls. (**CSCdw81168**)

  When SS7 is used, the Cisco RPMS server creates a resource group with the name "rg_ss7_rpms_digital" for digital calls. The number of resources under the rg_ss7_rpms_digital resource group is greater than the number of available HDLC resources for the trunk card, which can handle up to 256 digital calls. Because the Nextport resources are not used when the trunk card resources are depleted, the Cisco AS5850 fails to terminate calls after the 256th digital call.

  There is no workaround.

- Tracebacks and `%CSM-1-NO_CSM_CALL_INFO` messages appear during call teardown. (**CSCdx05186**)

  Symptom: After about 30 hours of stress testing, the Cisco AS5800 and Cisco AS5850 start to reject calls, and the `%CSM-1-NO_CSM_CALL_INFO: NO call control block` syslog message is seen.

  Conditions: This behavior was seen on the Cisco AS5850 and Cisco AS5800 after about 30 hours of stress testing, during which the Cisco AS5850 handles about 500 sustained calls and places calls at about 5 calls per second (cps). The tracebacks and syslog messages are seen as the calls are being rejected. At this stage, the system was unable to sustain more than approximately 50 calls. The unexpected behavior is seen on systems that handle SS7 calls and that are configured to get VPDN tunnel information from Cisco RPMS Releases 1.0 or 1.1.

  Workaround options:

  – Reload the box. It was observed that the box starts functioning at full capacity after a reload.

  – Use a RADIUS AAA server to provide VPDN tunnel information.

  – Use Cisco RPMS Release 2.0 to provide VPDN tunnel information.

- Traceback is seen at rm_author_local_vpdn_session_request. (**CSCdx07948**)

  During call setup, tracebacks and the following message are seen on the console:

  ```
  %RM-3-NORESP: No response-code from local RM
  ```

  This behavior occurred when 400 digital and modem calls were brought up and a script was used to tear down and set up calls at 2 cps. See also CSCdx46416 for similar traceback behavior.

  There is no workaround.

- Reloading brings up a previously shut ISDN D channel serial interface. (**CSCdx41056**)

  If you manually shut down the ISDN D channel serial interface and then reload the Cisco AS5400, the interface may become active.

  There is no workaround.

- The **no shut** command does not bring up the ISDN D channel serial interface. (**CSCdx41187**)

  In an ISDN PRI back-to-back configuration, entering the **no shut** command on the ISDN D channel serial interface may not bring up the interface.

  Workaround: Enter the **no shut** command on the interface and reload the router.

- Local RPM CLI commands for VPDN profiles are lost during reload. (**CSCdx41626**, **CSCdx50498**)

  Symptoms: Upon reload or bootup, the resource pooling VPDN CLI commands in the startup configuration are not recognized by the universal access server.

  Conditions: This behavior is observed on the Cisco AS5400 and Cisco AS5850 running Cisco IOS Release 12.2(2)XB5.

  Workaround: Manually enter the CLI commands that are used to configure local RPM profiles for VPDN. The commands can be recovered from the startup configuration.

- The **show isdn active** command may display some disconnected calls as active and increment their Seconds Used counter. (**CSCdx44718**)

  There is no workaround.

- RADIUS access-requests fail; tracebacks are generated. (**CSCdx46416**)

  In a mixed call environment, RADIUS access-requests may start to fail for no apparent reason. The access-requests are continually retried in a loop until the dialer idle time-out expires or the call is manually cleared. Tracebacks at rm_author_local_vpdn_session_request are continuously generated and CPU process usage increases. See also CSCdx07948 for similar traceback behavior.

  This behavior was only seen:

  – On ISDN non-VPDN calls on the Cisco AS5800 and Cisco AS5400 platforms.

  – When RPM is configured on the NAS.

  This behavior was not seen with modem calls. There is no workaround.

- Cisco AS5400 stops dialing after 256 calls; **debug dialer** command displays `No bundle in dialer_fsm_up` messages. (**CSCdx60991**)

  The Cisco AS5400 running Cisco IOS Release 12.2(2)XB5 stops dialing after 256 calls when tested in a 100% ISDN environment.

  There is no workaround.

- Spurious memory access at ds_set_digital_call_ctx. (**CSCdx64379**)

  Symptom: On the Cisco AS5850 access server, spurious memory accesses can occur and some traffic gets forwarded by CEF instead of DCEF when making digital calls.

  Conditions: This unexpected behavior occurs when digital calls are terminated by a DSP that is not on the same feature board as the serial interface. This problem exists in Cisco IOS Release 12.2(2)XB5.

  There is no workaround.

- Calls are not marked as terminated by Cisco RPMS during a NAS failover. (**CSCdx64599**)

  Cisco RPMS 1.1 may not correctly clear calls for a particular NAS from its active call counters after it has lost communication with that NAS for the amount of time specified in its NAS synchronization settings.

  Workaround: Enter NAS hostnames as well as NAS IP addresses for each NAS in the Cisco RPMS Administration:NAS list.

- Traceback occurs at mfcl_modify_ip_entry. (**CSCdx68017**)

  The following traceback might be seen on the Cisco AS5850 running Cisco IOS Release 12.2(2)XB5 when handling about 5 cps for more than 30 hours:

  ```
  1d18h: %FCL-3-INSERT_FAIL: FCL unable to insert entry through FDM, error code = 6
  -Process= "PPP IP Route", ipl= 0, pid= 88
  -Traceback= 6085916C 60859520 6008C0D0 603CD65C 6039B904 603A0080 603A51E8 60397F90
  603A692C 6048B264 6048B304 60485C74 60485DC0 6048D330 601C1384 601C1370
  ```

  The error message does not seem to affect CPU utilization or call processing. There is no workaround.

- Cisco AS5300 generates `Unavailable B-Channel` messages (**CSCdx69420**)

  The Cisco AS5300 may not dial out and may generate `Unavailable B-Channel` messages even if B channels are available.

  There is no workaround.

Resolved Caveats—Cisco ASAP Solution Release 2.0

- CSCdv01493—The Cisco AS5800 and AS5850 send an MLP bundle ID for a non-MLP VPDN call.
- CSCdv05516—Cisco AS5850 calls are not disconnected following a T309 timeout.
- CSCdv11344—The call threshold does not account for modem or digital calls.
- CSCdv15041—An MML session reports ACE_SV_Semaphore_Complex.
- CSCdv29892—Spurious memory access occurs on the Cisco AS5850 running Cisco IOS Release 12.1(5)XV3 while dial traffic is being processed.
- CSCdw01688—The Cisco SC2200 does a core dump following a **prov-copy** for a large configuration.
- CSCdw16716**—**The Cisco Voice Services Provisioning Tool (VSPT) generates commands in the wrong order.
- CSCdw17056—When both regular PRI and NFAS PRI are configured on a Cisco AS5800 and a **shut**/**no shut** is performed on a T1 controller, the GSM (group service message) may exchange the incorrect NFAS span's channel state between the Cisco AS5800 and a Cisco SC2200 signaling controller.
- CSCdw49546—The install/uninstall order of Solaris security patch CSCOh013 causes the Cisco SC2200 to fail.

Open Caveats—Cisco ASAP Solution Release 1.0

1. The call threshold does not account for modem or digital calls. (CSCdv11344)

   The **call threshold** global configuration command provides the option to select either treatment or busyout when throttling calls using one of these six methods: cpu-5sec, cpu-avg, io-mem, proc-mem, total calls, or total-mem. The call treatment option works for voice only calls, but not for analog dial-up or ISDN switched digital data calls.

   Workaround: Configure call threshold for the *expected* number of voice calls only, not for the total number of calls that the Cisco gateway can support.

2. The group service is indicated as being out of service after the Redundant Link Manager (RLM) D-channel is restored. (CSCdv24310)

   If an RLM Non-Facility Associated Signaling (NFAS) D-channel serial interface has been **shut** followed by a **no shut** before the ISDN layer 2 is declared to be down, the Cisco AS5400 sends a group service message (GSM) indicating that the first span of bearer channels is out of service. However, the ISDN group service message indicates that the channels are still in service.

   Workaround: After issuing the **shut** command, wait approximately 25 seconds before issuing the **no shut** command, or wait until a “layer 2 down” log message appears on the console.

3. The Cisco AS5400 or AS5350 echo cancelers are not disabled. (CSCdv53170)

   The echo cancelers for the Cisco AS5350 and AS5400 are not disabled when a 2100-Hz disabler tone, with periodic phase-reversals, is sent.

   Workaround: None.

4. The Cisco AS5400 or AS5350 inserts 6 dB of loss during double-talk. (CSCdv52639)

   The Cisco AS5400 and AS5350 echo canceler inserts 6 dB of loss in the transmit path during periods of double-talk (voice plus echo). This may affect adherence to a loss plan and some voice tests, such as the 105 responder test.

   Workaround: None.

5. The **isdn bchan-number-order ascending** command does not work correctly on the Cisco AS5400 or AS5350. (CSCdv78580)

   If the RLM ISDN D-channel is not configured on the lowest controller, the **isdn bchan-number-order ascending** command does not work correctly when specified on a Cisco AS5400 or AS5350 equipped with T1s.

   Workaround. When configuring the ISDN RLM D-channel, configure the lowest-numbered controller to be the primary NFAS group's primary D-channel. For example, if the unit is equipped with controllers 2/0 through 2/7 and 3/0 through 3/7, configure 2/0 as the primary NFAS group's primary D-channel (**pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 0**). This bug applies to SS7 RLM ISDN on a Cisco AS5400 or AS5350 T1 unit.

6. If all SS7 c7iplinks fail in a Cisco SC2200 protocol family, the Cisco SC2200 will failover. (CSCdw09838)

   This may cause a complete outage on other links in other protocol families.

   Workaround: There is no workaround that prevents this problem completely, but it can be minimized by ensuring diversity (redundancy) in IP and SS7 resources. This includes redundant SLTs and switches. The Cisco SLTs should also be powered from a power system protected by UPS or battery backup.

7. When configuring SS7-to-SS7 TDM switching, the user must carefully consider using the **isdn bchan number order hunt** command versus assigning the outbound T1 controllers manually in ascending or descending order. (CSCdv78580)

   Because this release of the Cisco ASAP Solution supports either trunk groups or T1 controller port selection, the outbound controllers to the far-end DPC must be physically allocated to start (a) at the lowest numbered controller and progress upwards (ascending) or (b) at the highest numbered controller and then descend. Similarly, the user must provision **bchannel number order hunt** in either ascending or descending order. See also CSCdv78580.

Note For the details of a practical solution, refer to the section Configuring TDM Switching Services in Chapter 2, "Voice and Dial Networks: Design Fundamentals," of the *Cisco ASAP Solution Implementation Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

8. The Cisco ASAP Solution supports only the 105 responder test using the G711ulaw codec. (CSCdv52639)

   Workaround: None.

9. Dtmf-relay using h245-alphanumeric or h245-signal mode adds an 8 dB loss to digits outpulsed at the terminal end. (CSCdw00026)

   Workaround: None.

10. A transponder (2-wire) COT (continuity test) fails when initiated from the Nortel DMS-100. (CSCdv26918)

    Workaround: Request that the far end be set to loop method (4-wire COT). If the switch is not a DMS-100 and the loop method is not an option, have the far end initiate several manual continuity tests and test calls, then verify their success or failure. If a transponder is failing and it is proven that this is a result of this bug, then the only workaround is to request that the far end SP be set to zero percent.

11. The Cisco AS5800 and AS5850 send an MLP bundle ID for a non-MLP VPDN call. (CSCdv01493)

    This problem occurs in Cisco IOS Releases 12.1(5)XV3 and 12.1(5) XM5 of the Cisco AS5800 and AS5850, respectively. The Cisco AS5800 or AS5850 sends a Multilink Point-to-Point Protocol (MLP) bundle ID to the Cisco RPMS in a TACACS+ VPDN session request, without MLP being configured. Thus, the Cisco RPMS identifies the incoming call as an MLP call. From the Cisco RPMS's viewpoint, such calls are translated as MLP calls and thus get rejected even if the session count limit is not reached for that particular VPDN group.

    Workaround: Increase the MLP bundle count to equal the session count.

12. Cisco AS5850 calls are not disconnected following a T309 timeout. (CSCdv05516)

    The Cisco AS5850 running Cisco IOS Release 12.1(5)XV3 might not disconnect active calls following a T309 timeout. This problem is *rare* because both Ethernet connections have to be lost in order to trigger a T309 timeout.

    Workaround: None.

13. Spurious memory access occurs on the Cisco AS5850 running Cisco IOS Release 12.1(5)XV3 while dial traffic is being processed. (CSCdv29892)

    On a Cisco AS5850 running Cisco IOS Release 12.1(5)XV3, spurious memory access messages followed by traceback messages may be encountered. This problem would indicate a spurious memory access made at 0x6091A5EC reading 0x6C4.

    Workaround: None.

14. An MML session reports `ACE_SV_Semaphore_Complex`. (CSCdv15041)

    Starting an MML session may generate the following errors:

    ```
    ACE_SV_Semaphore_Complex: No space left on device
    ACE_SV_Semaphore_Complex: No space left on device
    ```

    Workaround: None. There is no impact on call processing or on running MML.

15. The Cisco Voice Services Provisioning Tool (VSPT) generates commands in the wrong order. (CSCdw16716)

    The signaling controller requires the commands to be specified in the following order: **external node**, **sessionset**, **c7lnk**.

    Workaround: You must edit the order of the commands in Cisco VSPT prior to deployment.

16. The Cisco SC2200 does a core dump following a **prov-copy** for a large configuration. (CSCdw01688)

    The Cisco SC2200 might do a core dump when a large configuration is activated (6-opc, 200-dpc, 256-NAS, or 12-linkset). This causes a failover to the standby, but calls are not lost in an active/standby configuration.

    Workaround: Stop and start the Cisco SC2200 on which a core dump occurs, to put this Cisco SC2200 in standby mode.

17. The MML session hangs up. (CSCdv78016)

    The MML session may hang up under normal operation.This has no effect on the Cisco SC2200 operation or other MML sessions. However, the MML session that hangs is lost.

    Workaround: On the Cisco SC2200, kill the MML session process that is identified as being “hanged” and start another MML session.

18. The *components.dat* file gets corrupted when configurations are large. (CSCdv52794)

    When attempting to do dynamic provisioning of the Cisco SC2200, the *components.dat* file might get corrupted.

    Workaround: None.

19. When both regular PRI and NFAS PRI are configured on a Cisco AS5800 and a **shut**/**no shut** is performed on a T1 controller, the GSM (group service message) may exchange the incorrect NFAS span's channel state between the Cisco AS5800 and a Cisco SC2200 signaling controller. (CSCdw17056)

    When the NFAS configuration is not started from the first T1 controller or is not continuous, the physical controller ID will not match with the NFAS ID. A **shut**/**no shut** on an individual controller causes the physical controller ID, rather than the NFAS ID, to be used in the GSM, reflecting the channel state of the incorrect NFAS span. For example, if the first two controllers are regular PRI and the remaining controllers are NFAS (through RLM), a shut/no shut on the first NFAS controller causes the physical controller ID (02 instead of 00) to be used in the GSM.

    Workaround: To ensure that the NFAS ID maintains its correspondence with the physical controller ID, configure the NFAS group beginning with the very first controller, and configure regular PRI toward the end of the remaining available controllers. If this workaround is not applied and the NFAS IDs and physical controller IDs do lose their correspondence, you can clear the problem by performing a **shut/no shut** on the entire RLM group. However, this will drop all active calls for the entire RLM group.

20. The install/uninstall order of Solaris security patch CSCOh013 causes the Cisco SC2200 to fail. (CSCdw49546)

    When installing or uninstalling the security patch CSCOh013 in the following order, the Cisco SC2200 fails:

    a. Install the Solaris OS.
    b. Install the security patch CSCOh013.
    c. Install the MGC software (at this point, the system runs fine).
    a. Remove the security patch (at this point the system does not work).

    Workaround: Follow this order when installing the security patch CSCOh013:

    a. Install the Solaris OS.
    b. Install the Solaris OS patch CSCOh007 for Solaris 2.6.
    c. Install the MGC software (or MGC Adjunct).
    d. Install the Solaris system security patch CSCOh013.

    To uninstall, patch CSCOh013 must be uninstalled *before* the MGC software is uninstalled.

Important Notes

Updates to Release Notes

Check these release notes periodically for new tested configurations of the solution. Cisco is working to resolve the Caveats.

TAC

If you call TAC for assistance, specify that you are working with an SS7 Cisco ASAP Solution configuration. TAC may recommend software releases that are not listed in these release notes. Follow the TAC recommendations.

Cisco IOS Release Rebuilds

The Cisco software releases are undergoing improvements to resolve the Caveats. If a release rebuild becomes available, Cisco recommends that you upgrade to the latest software images. An example of a release rebuild: from 12.2(2)XA4 to 12.2(2)XA5.

Limitations and Restrictions

Cisco Access Registrar

The Cisco Access Registrar (AR) might respond with attributes that are not supported by the universal gateway (UG) when the UG requests VPDN profile information for a user. For the call to work, those attributes must be filtered by Cisco AR or on the NAS. The solution is to write a Tcl script similar to that illustrated in the following steps:

Step 1 Create a script and place it in *$ARHOME/scripts/radius/tcl*. The following example shows how the *removeBadAttribute* script is created. In the example, the script removes the RADIUS attributes “State” and “Termination-Action” before sending the RADIUS response back to the network access server.

```
proc removeBadAttribute {request response environ} {
$response remove State
$response remove Termination-Action
}
```

Step 2 Create the script definition in */radius/scripts* using the **aregcmd** command as follows:

a. **aregcmd**

b. **cd /radius/scripts**

c. **add removeBadAttribute**

d. **cd removeBadAttribute**

e. **set language tcl**

f. **set filename $ROME/scripts/radius/removeBadAttribute.tcl**

Step 3 Set **/radius/OutgoingScript~** *scriptname* using the **aregcmd** command as follows:

a. **aregcmd**

b. **set /radius/OutgoingScript/removeBadAttribute**

Step 4 In the */Radius/Advanced* directory on the Cisco AR, set the object MaximumNumberOfRadiusPackets value to 8192. This enables the transfer of larger packets when the primary Cisco AR communicates with the backup Cisco AR. Core dumps occur on both master and backup Cisco ARs when this number is smaller than the largest packet used during replication.

Caution When the UG tries to get a VPDN profile from the RADIUS server, it uses a user ID in the form of *dnis:xxxxxxxxxx* for the username field. If this user does not exist in RADIUS database, the NAS (UG) fails to find a VPD N profile on the RADIUS.

Cisco RPMS

If Cisco RPMS is installed in the Cisco ASAP Solution and it has a VPDN profile that matches a call, the VPDN tunnel information must come from RPMS. If a customer wants VPDN information from elsewhere (like client or Wholesale AAA), the customer needs to ensure that RPMS does not have a matching VPDN profile.

MIND CTI Debit Card Payment

If using a MIND CTI server with multiple Ethernet interfaces, make sure to bind (in the Windows NT networking setup) the interface you want RADIUS traffic to go through first, before other interfaces are tried. The software looks for this interface first in the bind table and if it is not there, the process fails.

Cisco UGM

If the Cisco device running the Cisco UGM has more than one Ethernet interface, the user must configure the file so that the UNIX hostname command returns a name that is tied to the Ethernet interface that the Cisco UGM is to monitor.

VPDN

By not having direct access to the equipment, the retail service provider (virtual ISP) that terminates VPDN calls cannot control the call termination with idle-timeout values as can be done by the wholesale service provider, who has access to the serial interface configuration. A feature that allows this termination in the virtual-template on the LNS will be made available in later releases.

Cisco SC2200

The TLinkAlignTime-sigPath property (located in the *propSet.dat* file) removes the restriction of the TLinkAlignTime property, which is limited to only the ISUPV3_UK and UK_AXE10 protocols. The new property opens the code to all ITU protocols (Q.761, Q.767, and ANSI), plus ISUPV3_UK and UK_AXE10.

The value provisioned in the TLinkAlignTime property specifies the duration of the TLinkAlign timer. When the signaling links to a particular switch are lost as a result of excessive errors, the TLinkAlign timer is set against all call instances associated with that switch. Valid values are 0 to *n* (in milliseconds). The default is 0.

If the TLinkAlignTime value is set to any value other than 0, the affected calls wait for the specified amount of time. If the signaling link is restored before the TLinkAlign timer expires, the call continues and the TLinkAlign timer is reset. If the signaling link is not restored before the TLinkAlign timer expires, the call is dropped (released).

If the TLinkAlignTime value is set to 0, the TLinkAlign timer is disabled. In this case, the call instance either (1) waits for an infinite amount of time (until the signaling link is restored), or (2) the call is released by either the caller hanging up or some other call processing action.

Cisco BAMS

The Cisco Billing and Measurements Server (BAMS) software is still under test in the Cisco ASAP Solution. If you are using BAMS to provide billing data and are upgrading to the Cisco ASAP Solution, make sure to monitor your billing data for accuracy.

Cisco IPM

In order to support Cisco Internetwork Performance Monitor (IPM) for voice applications, Cisco Service Assurance Agent (SAA) must be enabled on those routers selected as the source and the target for probing and monitoring. That feature is available in the IP Plus and Enterprise Plus feature sets. See the feature sets table in the section Cisco ASAP Solution Software Matrix, page 5.

Note For more information about SAA and the commands and features it supports, refer to Network Monitoring Using Cisco Service Assurance Agent at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf017.htm

Upgrading to the Cisco ASAP Solution

The following solutions can be upgraded to the Cisco ASAP Solution:

- Cisco SS7 Interconnect for Access Servers Solution Release 2.1 or 2.2 to Cisco ASAP Solution Releases 1.0 or 2.0
- Cisco SS7 Interconnect for Voice Gateways Solution Release 1.0 or 1.1 to Cisco ASAP Solution Releases 1.0 or 2.0

Note For upgrade issues that are specific to your network, contact your Cisco account representative.

For step-by-step procedures for upgrading from any of these solutions to the Cisco ASAP Solution, refer to Chapter 1, “Solution-Level Upgrade Procedures” of the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Upgrade Guide,* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das/upgrade/index.htm

The document does not mention the Cisco ASAP Solution specifically, but the discussion in the "Upgrading within the Cisco SS7 Interconnect for Voice Gateways Solution, from Release 1.0 or 1.1 to Release 1.3" section applies to an upgrade to the Cisco ASAP Solution.

For the Cisco software images that you need for upgrading to the Cisco ASAP Solution, refer to Table 3 on page 6.

Related Documentation

Solution-Specific Documents

Documents supporting the Cisco ASAP Solution, including these release notes, are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

These include the following:

- *Cisco ASAP Solution Overview and Planning Guide*

  This document provides an overview of the solution architecture, components, and services for the Cisco ASAP Solution. It also introduces many factors that must be taken into account in designing a network that takes advantage of the capabilities of the Cisco AS5000 series universal gateways. The following major topic are covered:

  - Introduction to the solution
  - Solution architecture and services
  - Solution components
  - Designing a solution
  - Solution management

- *Cisco ASAP Solution Implementation Guide*

  This document will help you establish and manage the services introduced in the *Cisco ASAP Solution Overview and Planning Guide*. The following major topics are covered:

  - Voice and dial network: design fundamentals
  - Using management and shared support services
  - Establishing solution components

- *Cisco Integrated Network Solutions Operations, Maintenance, and Troubleshooting Guide*

  This document provides task-oriented procedures for operating, maintaining, and troubleshooting the end-to-end solution network. This document supports the Cisco ASAP Solution and the Cisco SS7 Interconnect for Voice Gateways Solution.

Documents for Related Solutions

Documents supporting the Cisco ASAP Solution, including these release notes, are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

These include the following:

- Cisco Wholesale Voice Solution

  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/index.htm
- Cisco SS7 Interconnect for Voice Gateways Solutions

  http://www.cisco.com/univercd/cc/td/doc/solution/dialvoic/tv/index.htm
- Cisco SS7 Interconnect for Access Servers Solutions

  http://www.cisco.com/univercd/cc/td/doc/solution/dialvoic/td/index.htm

Obtaining Documentation

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

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

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

http://www.cisco.com

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

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