



IP Communications Systems Test Release 1.2

IPCC Release Notes

Corporate Headquarters

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

<http://www.cisco.com>

Tel: 408 526-4000
800 553-NETS (64387)
Fax: 408 526-4100

Customer Order Number:

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the *Cisco Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R)

IP Communications Systems Test Release 1.2: IPCC Release Notes
Copyright © 2003, Cisco Systems, Inc.
All rights reserved.

Table of Contents

1	Overview	2
2	System Requirements	3
2.1	Cisco CallManager	3
2.2	Cisco Intelligent Contact Management Software (ICM).....	3
2.3	Cisco Unity	3
2.4	Cisco IP IVR.....	4
2.5	CTI OS Server	4
2.6	Cisco Security Agent (CSA).....	4
2.7	Cisco IOS Router and Voice Gateways.....	4
2.8	Cisco Catalyst Switches and Voice Gateways	5
3	Install and Upgrade Documentation and Links.....	5
4	Software Version Matrix.....	5
5	Limitations	6
5.1	Open Caveats for IP Communications Systems Release 1.2 - IPCC	6
5.2	Important Notes	8
5.2.1	JTAPI Client Parameter Tuning.....	9
5.2.2	Configure /LOAD 0 parameter for PG	10
5.2.3	Implement Agent Busy and Ring No Answer (RNA/RONA) call logic for agent ACD lines.....	12
5.2.4	Avoid Conference and Consultative Transfers Involving IP IVR ports.....	13
5.2.5	Implement Call Recovery Logic for IP IVR Route Points and CTI Ports.....	13
5.2.6	Implement Call Recovery Logic for ICM Route Points	14
5.2.7	Disable Call Waiting.....	14
5.2.8	Disk Drive Recommendations for High Traffic Systems	15

1 Overview

This document comprises the IP Communications (IPC) Systems Test release notes for voice systems built upon CallManager 3.3(3) and ICM 4.6.2. It is standard methodology for Cisco to perform systems wide testing of IP Communications, supplementing the systems test performed on each IPC product.

A major deliverable of the IPC Systems test is a recommendation of compatible software releases, verified through the test. Customers that have deployed or are planning to deploy multiple voice application and voice infrastructure products in their network can adopt these recommendations. These recommendations are not exclusive, and are in addition to interoperability recommendations for each of the individual voice application or voice infrastructure products.

The primary focus in this document is on the IP Contact Center (IPCC) component of these IP Communication systems. IP Telephony (IPT) components have also been tested. For the release notes for IPT, please refer to *IP Communications Systems Test Release 1.2: IPT Release Notes*.

The tested systems comprise a suite of IPC solutions containing a validated software set of the following components: Cisco CallManager, Intelligent Contact Manager, Cisco IP IVR, Cisco Voice Gateways, Cisco Catalyst Voice Gateways, Cisco routers, and Cisco Catalyst switches.

Access the documentation suite for voice products at:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/>

Access the documentation suite for customer contact products at:

<http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm>

Access the latest software upgrades and release notes for Cisco CallManager 3.3(3) and Cisco IP IVR 3.1(1) at:

<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

Access the latest software upgrades and release notes for Cisco Intelligent Contact Manager 4.6.2 at:

<http://www.cisco.com/kobayashi/sw-center/telephony/icm/icm46-planner.shtml>

Access the latest software upgrades and release notes for IOS Routers and Gateways on Cisco Connection Online (CCO) at:

<http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml>

Access the latest software upgrades and release notes for Catalyst Switches on Cisco Connection Online (CCO) at:

<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

2 System Requirements

The components of this solution are discussed below.

This section contains information on the platforms tested as part of this program. For additional information on specific hardware recommendations or bills of material for each product, refer to the links to product documentation in each subsection.

2.1 Cisco CallManager

Make sure that you install and configure Cisco CallManager Release 3.3(3) SR1 on a Cisco Media Convergence Server (MCS).

Platforms tested in this recommendation are :

[MCS-7835-1266](#)

For MCS platform information, see:

<http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html>

For system hardware component information and system requirements, refer to Installing Cisco CallManager Release 3.3:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/install/index.htm

2.2 Cisco Intelligent Contact Management Software (ICM)

Make sure that you install and configure Cisco ICM software, version 4.6.2 SR1 with ES1, on the platforms listed below.

Platforms tested in this recommendation are:

ICM Rogger – 2 x [MCS-7835-1266](#) (with dual processor)

ICM Hybrid PG – 2 x [MCS-7835-1266](#) (with dual processor)

ICM AW/HDS – 1 x [MCS7825-1133](#)

2.3 Cisco Unity

Cisco Unity integration with IPCC was not tested as part of IP Communications Systems Test Release 1.2. However, Unity integration **was** tested as part of the IP Telephony components testing—see *IP Communications Systems Test Release 1.2: IPT Release Notes*.

2.4 Cisco IP IVR

Make sure that you install and configure Cisco IP IVR 3.1(1) SR2 on a Cisco Media Convergence Server (MCS).

Platforms tested in this recommendation are:

[MCS-7835-1266](#)

For IP IVR 3.1(1) system requirements and supported hardware and software, see the following:
http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_1/index.htm

Release Notes for IP IVR 3.1(1) are accessible from:
http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_1/english/admn_app/elnote/index.htm

2.5 CTI OS Server

Make sure that you install and configure CTI OS Server on a Cisco Media Convergence Server (MCS).

Platforms tested in this recommendation are:

[MCS7825-1133](#)

2.6 Cisco Security Agent (CSA)

CSA 4.0.1.539-1.1(3) was tested with all applicable platforms and had no effect on system performance.

2.7 Cisco IOS Router and Voice Gateways

Platforms tested in this recommendation are:

Cisco IOS Gateways – 12.2(15)T8

Cisco 6608 Gateway – CatOS 6.3(10)

Cisco 2691 (MGCP and H323 Gateways)

Cisco 3660 (MGCP and H323 Gateways)

For Cisco 3660 System Requirements, see:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tfeat.htm - 1003904>

For Cisco 2691 System Requirements, see:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tfeat.htm - 54895>

2.8 Cisco Catalyst Switches and Voice Gateways

Platforms tested in this recommendation are:

Catalyst 3524XL

For Catalyst 3524XL System Requirements, see:

http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35wc5/index.htm

3 Install and Upgrade Documentation and Links

For Cisco CallManager, see

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/install/index.htm

For Cisco Intelligent Contact Management, see

<http://www.cisco.com/univercd/cc/td/doc/product/icm/icm46/core/index.htm>

For Cisco IP IVR, see

http://www.cisco.com/univercd/cc/td/doc/product/voice/sw_ap_to/apps_3_0/english/admn_app/g_etst303/index.htm

4 Software Version Matrix

Table 4.1 lists the recommended software releases of the system components.

Table 4.1: Software recommendations for the IP Communications Systems Release 1.2 - IPCC

Component	Release Version
CallManager	3.3(3)SR1
7960 (Phone Sets)	P00305000101
Intelligent Contact Manager (ICM)	4.6(2) SR1 with ES1 ¹
CTI OS	4.7 SR1 ²
IP IVR	3.1(1)SR2
CS3660 (Gateway)	12.2(15)T8
CS2691 (Gateway)	12.2(15)T8
CAT6506 (Core Switch)	6.3(10)
CAT6509 (Access Switch)	6.3 (10)
CAT4006 (Access Switch)	7.5.1
CAT3524 (Access Switch)	12.0(5)WC5
JTAPI	1.4(3.12)
CAT6608 Gateway	CatOS 6.3(10)
Cisco Security Agent (CSA)	4.0.1.539-1.1(3)

¹ To download ES1 (Engineering Special 1), go to Bug Toolkit via http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl ; once you have launched Bug Toolkit, type **CSCec14316** into the **Enter known bug ID** field, and click the **Search** button. (Or simply use the following URL <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec14316>) When the Bug Details page appears, go to the bottom of the page and click on the link **ICM4.6(2) SR1 ES1**, then download the ES1 Release Notes and Installer.

² SR1 location: <http://www.cisco.com/cgi-bin/special.cgi> ; Special Access Code: ICM123658918

5 Limitations

5.1 Open Caveats for IP Communications Systems Release 1.2 - IPCC

Table 5.1 lists and describes open caveats related to the testing of the IP Communications Systems Release 1.2 – IPCC that were not resolved at the time of this recommendation.

For additional caveats and fixes, go to www.cisco.com and view the product Maintenance Releases and Service Releases that have been released since the versions tested and listed in Table 4.1.

Tip: If you have an account with Cisco.com (Cisco Connection Online), you can use the Bug Toolkit to find caveats of any severity for any release.

To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Table 5.1: Open Caveats for IP Communications Systems Release 1.2 - IPCC

Identifier	Headline	Summary
CSCec11441	NPE-G1 reports rx_overrun rx_int_drop unexpected_sop with low %CPU	Symptom: A Cisco router may experience low NDR performance with very low %CPU utilization (ca 30-40%). Condition: When MLPoA LFI are configured. Workaround: None at this time.
CSCec42602	Calls fail in SRST mode - mgcp app cpu at 99%	Problem: When MGCP/CallManager and SRST are configured in the same gateway and the gateway communicates with the Cisco CallManager over a slow WAN link, the gateway can reach 100% CPU utilization if a large value is configured for "max-dn" (SRST phones). The WAN link is too slow to get all the MGCP signaling responses back to the CallManager before a timeout occurs. The MGCP timeout parameter on CallManager must be tuned accordingly. Workaround: Increase the MGCP timer on the CallManager service panel from 3 seconds to 6 seconds. This will not affect performance, but will insure that the GW will be able to respond before a timeout occurs.
CSCec48931	Dependency Records for Route List Takes 5 Minutes To Display	Symptom: Selecting the "Dependency Records" option takes at least 5 minutes to display. Publisher CPU spikes to 100% and all other database administration is extremely slow. Condition: Normal operations. Workaround: None.
CSCec12689	CCM MGCP PRI does not re-establish layer 2 when router reload	Symptom: ISDN PRI doesn't re-establish layer 2 state to MULTIPLE_FRAME_ESTABLISH when router is reloaded. Condition: Router communicating with CCM (Cisco

IP Communications Systems Test Release 1.2: IPCC Release Notes

		<p>CallManager) version 3.3(2) spC using MGCP protocol. When router is reloaded, the ISDN Layer 2 state is stuck in TEI_ASSIGNED state until user issues "no mgcp" / "mgcp" CLI in the global command line mode or issues a "shut" / "no shut" to the d-channel. Router registered to CCM just fine and the PRI backhaul tcp session is established and OPEN.</p> <p>Workaround: Issue "no mgcp" and "mgcp" CLI in the global configuration mode OR issue "shut" and "no shut" to the ISDN d-channel (interface Serial X/Y:23).</p>
CSCeb77852	SQL sp3.1.0.4 Update ReadMe File Needs additional Step	<p>Description: Executing the SQL update for CCM 3.3(3), using the document listed below and performing the verification steps in the section listed below, does not work.</p> <p>Document: SQL2K-ServicePack3.1-0-4Readme.htm http://ftp-sj.cisco.com/cisco/crypto/3DES/voice/cmva/SQL2K-ServicePack3.1-0-4Readme.htm</p> <p>Section: "Steps to manually confirm that the installation was successful"</p> <p>Symptom: Step #3 fails because the required information is not displaced. An error message is generated.</p> <p>Workaround: Add another step after #2. From the Main menu screen "Select the 'Start SQL Server if it Stopped' radio button".</p>
CSCeb85765	AIM VOICE PRI goes down if network-clock-participation is set last	<p>Symptom: A T1 or E1 PRI configured on a c3700 voice gateway with an AIM VOICE card will drop ISDN Layer 2 connectivity and refuse to re-establish itself. A <code>debug isdn q921</code> will show that the gateway continuously transmits SABMEPs to try to restart the ISDN connection but there are never any received UAfs.</p> <p>Condition: These symptoms are observed on a Cisco c3725 or c3745 voice gateway installed with an AIM-ATM-VOICE-30 or AIM-VOICE-30 AIM module and a T1 or E1 VWIC inserted into a chassis WIC slot. The T1 or E1 controller is configured for ISDN PRI and Layer 2 is verified via the <code>show isdn status</code> EXEC command to be up with MULTIPLE_FRAMES_ESTABLISHED. The ISDN connectivity will only go down if the AIM VOICE network clocking commands are configured AFTER the PRI connectivity has already been established: <code>network-clock-participate aim [0 1]</code> <code>network-clock-participate wic [0 1 2]</code> <code>network-clock-select 1 [T1 E1]</code> A <code>shutdown/no shutdown</code> of the PRI Serial interface or the T1/E1 controller will not be successful in re-establishing the PRI Layer 2 connectivity.</p> <p>Workaround: The basic problem is that the necessary network clocking commands must be configured on the c3700 before the PRI itself is configured. As such the following workarounds are available: 1. Configure all appropriate network-clock-participate and network-clock-select commands on the c3725 or c3745 router first, and then subsequently configure the pri-group under the T1 or E1 controller. 2. If the pri-group is already configured, the network clocking commands have also already been configured, and ISDN Layer 2 refuses to establish itself, unconfigure the pri-group and then re-configure it. 3. If all network clocking commands and the pri-group command have been configured as in (2) and it is not an issue to do so, just save the configuration to NVRAM and reload the router.</p>

IP Communications Systems Test Release 1.2: IPCC Release Notes

CSCma27281	CTI RP observed by both the IPCC PG Side A and B	Symptom: CTI Route Point is registered with both the IPCC PG Sides. Condition: CTI Manager loses connectivity with other CallManagers in the cluster. Workaround: None.
CSCma26358	AllAgents, AllCalls, Agent and Supervisor desktop leak memory	Symptom: AllCalls and AllAgents monitoring tools, Agent and IPCC Supervisor desktops, as well as any applications using the COM layer, have a client side memory leak. Condition: This problem exists in Cisco CTI OS Products 4.7 SR1, 4.7 SR2, 5.0, and 5.1. Workaround: Restart AllAgents and AllCalls monitoring tools, Agent and IPCC Supervisor desktops, and any applications using the COM layer. For more information on the resolution of this defect, use Bug Toolkit to access CSCma26358.

5.2 Important Notes

The following lists a number of design/configuration recommendations that should be considered for all IPCC implementations that require high availability and/or high call completion rates.

5.2.1 JTAPI Client Parameter Tuning

In order to speed up the detection of a CTI Manager failure on either the PG or the IP IVR, it is recommended that the JTAPI Server Heartbeat Interval be reduced from the default 30 seconds to 5 seconds.

Rationale:

Under normal operations, JTAPI client either waits for $2 * ServerHeartbeatInterval$ before closing the connection to the CTI Manager, or closes it when *socket closed* is detected. Therefore, for a 30sec Heartbeat value, JTAPI closes sockets either after $2 * 30 = 60$ sec or whenever socket closed is detected. For a 5sec Heartbeat value, JTAPI closes sockets either after $2 * 5 = 10$ sec or whenever socket closed is detected. (In testing it was determined that the change in time for detection of the failure condition improved 35-45 seconds).

Minimum safe heartbeat timer value is 5sec. If it is less than this, CTI will default to a 30sec value. Heartbeat values become important only when the system is idle. If call activity is present, CTI/JTAPI will not handshake using heartbeats, but will rely on each other's messages. When the system is idle, heartbeat handshaking goes into effect. So, in essence, a low timer value causes some traffic in the system during idle state, and high timer value causes less traffic during idle state. Since this occurs only when the system is idle, a low timer value is not problematic.

In order to speed up the fail-over of the IP IVR from primary CTI Manager to backup CTI Manager, it is recommended that the Provide Retry Interval be reduced from the default 30 seconds to 5 seconds. (This is in addition to the Server Heartbeat Interval setting).

Rationale:

Tuning both Server Heartbeat Interval and Provider Retry Interval parameters improves CTI Manager failure detection (Server Heartbeat Interval Parameter) and connecting to backup CTI Manager (Provider Retry Interval Parameter).

Considerations:

Decreasing the JTAPI client parameters is recommended for IPCC servers only and not regular JTAPI client applications.

1. Decreasing the timers exposes the application to the effect of network congestion.
2. For server applications, lowering these parameters is not problematic, but for client applications, like Softphone, decreasing retry interval means that all softphones will try to connect to CTI Manager around the same time.

It is assumed that an IPCC deployment will not suffer from either of these considerations in that all communication between PG or IP IVR and CTI Manager will be over a local high capacity network or protected via QoS over any WAN links. Additionally, the current recommendations

for a standalone CallManager cluster result in the total number of JTAPI connections to each CTI Manager being less than 5—thus avoiding the connection startup overload problem.

5.2.2 Configure /LOAD 0 parameter for PG

In deployments using ICM 4.6.2 and CTI OS, it is highly recommended that the "Configuration parameters" field on the "Peripheral" tab of the PG in the PG Explorer, left blank by default, be changed to /Load 0 to avoid extended failover downtime and state issues upon recovery—particularly for contact centers with more than 50 agents.

Rationale:

In the PG Explorer there is a field for “Configuration Parameters” for each peripheral. One parameter defines PIM behavior for failover whenever there is a CTI failure that could include closing the agent desktop without logging out, CTI OS failover, or CTI Server failure. This configuration parameter can be set to “/LOAD 0” or “/LOAD 1”. The PIM will default to using “/LOAD 1” behavior if no /LOAD parameter is configured.

/LOAD 1 will log out the agent on any CTI failure. /LOAD 0 will attempt to set the agent to “NotReady” on any CTI failure.

In essence, the PIM wants to prevent calls being routed to agents who were in the “Available” State before the client disconnected. The two approaches used are setting agents to either “NotReady” (/LOAD 0) or forcing agents to be logged out (/LOAD 1). In both cases a special reason code (50002) is passed as an Event Reason Code with the AgentState event and will be captured in the Agent_Logout table and reports.

In a CTI OS failover case, each CTI OS client attempts to restore state to its last known state after the agents have failed over to the alternate CTI OS server.

LOAD 0 Characterization:

Advantages

1. Faster failover time than /LOAD 1 because agents are not fully logged out after disconnect. Instead, they are forced to the NotReady state so calls will not be routed to them.
2. Generally a better state for the transition during failover for reporting purposes because agents are not reported as logged out during the outage period.
3. More call context is maintained (i.e., peripheral and ECC variables, PeripheralCallType indicating whether it is a conference call, transfer call, etc.).

Disadvantages

1. In some circumstances (rarely), when the CallManager provides an unexpected CTI event stream, the agent state can be out of step with the actual hard phone state. Normally the agent is left in a held or talking state but there is no call on the phone. The default method to recover the agent state used to be to close the agent desktop and log back in. This method of recovery does not work with the /LOAD 0 option. Other options include:
 - a. Press keys on the hard phone in the following five-character sequence: ****#****. This resets the phone.
 - b. An administrator can reset the phone from the CCMAAdmin web page.
2. In hot-seating scenarios, LOAD 0 may lead to a condition where agent login is rejected. This can happen because the previous agent who used a phone simply closed their desktop as a means to end their session. Possible remedies for this situation include:
 - a. Set inactivity timer in agent desk settings on the ICM configuration so agent is logged out after the defined inactivity time.
 - b. Use Supervisor phone to force agent to logout.
 - c. Use CTI OS AllAgents tool to force agent to logout.
 - d. Reset the instrument by pressing keys on the phone in the following five-character sequence: ****#****
 - e. Reset the instrument from the CallManager Administration program.

Caveats

1. Customers must configure the Ring No Answer timeout and associated ring no answer dialed number in the ICM Agent Desk Settings. This is in the event that an agent is recovered to available after a failover, but that agent has stepped away—the call is then redirected to another available agent.
2. Customers must set the Agent No Activity timer in the ICM agent desk settings to log agents out after a period of inactivity while in the “NotReady” state. This reduces the occurrence of hot-seating agents not being logged into the same instrument at a later time.

LOAD 1 Characterization:

Advantages

1. If an agent disconnects without logging out, the next hot-seating agent will have no problem logging in with the same instrument because the previous agent was forcibly logged out.

Disadvantages

1. Can take a long time for failover (possibly several minutes) because it takes a while to log out and re-log in a lot of agents. The amount of time will vary with the number of agents and other factors such as heavy call load and number of skill groups per agent.
2. Softphone may appear to recover quickly but then logs out because it fails over to the alternate server before the PIM has forcibly logged out the agent. The automatic login that occurs after this may take a long time as described in the item above.
3. Has a negative impact on reporting because agents are reported as having logged out during the outage period.
4. Some call context may be lost when the call is recovered, e.g., peripheral call variables, ECC variables, and PeripheralCallType (particularly barge in, supervisor assist, and emergency assist PeripheralCallTypes).

Recommendations:

1. For CTI OS with more than 50 agents, and with the caveats above, /LOAD 0 is recommended.
2. For CTI OS with less than 50 agents, /LOAD 1 should be acceptable.

5.2.3 Implement Agent Busy and Ring No Answer (RNA/RONA) call logic for agent ACD lines

Implement a Route Point(s) and associated ICM routing scripts to recover calls normally lost due to line busy condition. Configure the Call Forward Busy (CFB) CallManager parameter on the agent ACD line pointing to this Route Point.

Rationale:

In traditional ICM ACD implementations, the RONA (Roll Over No Answer) logic implemented by the ICM CallRouter appears to be sufficient to handle call recovery in cases where call state failures occur (e.g., agent does not answer the ringing extension). In an IPCC environment this event corresponds to a Ring No Answer (RNA) event. In both of these cases the call is correctly routed to an on-hook extension and the error event is the failure to answer.

A new problem exists in the more distributed IPCC implementation that is similar to RNA but not identical. It is possible due to various race conditions in the end-to-end call signaling, to have inconsistent line state in the ICM CallRouter and the CallManager. While in most cases this is a transitory effect, it is possible to encounter scenarios where the ICM CallRouter will direct a call to a line that is currently busy. This is an uncommon problem in low call volume environments but is experienced in high volume scenarios and/or system error conditions. [Higher call volume scenarios currently may experience end-to-end call state signaling latencies in the 1-3 second range.]

In order to provide call recovery for this situation, it is highly recommended that another Route Point and associated ICM routing script be used that is distinct from, but implements similar logic to, the RNA call recovery logic. A distinct Route Point provides a mechanism to track the

occurrences of this specific error and allow for proactive actions to be taken if the event is seen occurring on a regular basis.

[Please note that it is highly recommended to implement RNA call recovery in addition to line busy recovery. System overload and error conditions may produce both failure events. RNA logic provides protection against system errors as well as failure of agents to answer.]

5.2.4 Avoid Conference and Consultative Transfers Involving IP IVR ports

Do not implement business logic that may invoke a consultative transfer or conference involving an IP IVR port.

Rationale:

Currently the JTAPI messaging between CallManager and ICM does not provide a mechanism to handle all the potential call state events involved in this process and may fail under certain scenarios.

In high touch service scenarios it is often required that an agent attempt a warm transfer of a customer to a specialized agent group. If the environment requires that this customer be re-queued to an IVR if no agent is available, then this needs to be implemented as a manual two-step process.

1. Attempt a consultative transfer to specific skill group via Route Point.
2. If no agents are available (need to build logic into the first routing script to indicate this to agent) then the agent terminates the attempted conference/transfer event.
3. Agent then initiates a blind transfer of the customer call to a second queuing route point for the required skill group.

Currently this requires two route points and two routing scripts breaking up the business logic, but it is not possible to direct an attempted conference or consultative transfer to an IP IVR port and guarantee successful transfer.

5.2.5 Implement Call Recovery Logic for IP IVR Route Points and CTI Ports

Configure CFB, CFF, CFNA on all IP IVR Route Points and CTI Ports directing the call to an ICM call recovery Route Point(s) and associated routing script(s).

Rationale:

System/Server resource and call state information may be delayed between the various IPCC components resulting in call loss if error recovery mechanisms are not implemented. During various timing windows it is possible for ICM to direct CallManager to send a call to an IP IVR which is unable to process that call (e.g., IP IVR failover, IP IVR is out of service or is in partial service and only has one of 60 configured CTI ports operational). Implementing a mechanism that provides a way to recover from failure of the IP IVR to respond or process a call also allows

the entire solution to provide a level of redundancy and availability beyond that possible using only a standard configuration.

To maximize call processing success rates, it is recommended that you implement a layered call recovery design as described in these recommendations.

5.2.6 Implement Call Recovery Logic for ICM Route Points

Configure CFB, CFF, CFNA on all ICM Route Points (Post and Translation routes) directing the call to an independent call-processing component (e.g., Cisco Unity or standalone Cisco IP IVR).

Rationale:

The interface between CallManager and ICM is a single threaded JTAPI client connection. This connection has a redundant configuration but with the following limitations:

1. Failure of CTI Manager or PG results in 60 second Contact Center outage
2. JTAPI messaging congestion or failure results in lost calls

To minimize both of these limitations, it is recommended that CallManager be configured to forward calls to a third party application for processing. In failure tests it was possible to successfully answer > 95% of all calls arriving during the failure event window.

Note: These calls are not handled by ICM and thus do not appear in any ICM reports.

5.2.7 Disable Call Waiting

Set CallManager Cluster Call Waiting Flag to False

Rationale:

Inconsistency of device/line state between CallManager and ICM due to system error, race condition, or messaging latency can result in ICM directing calls to agent lines which are already off-hook. In order for the RNA/Agent Busy call recovery mechanisms to detect and recover this call, it is necessary to disable Call Waiting for the Contact Center agents. This enables CallManager to immediately detect failure of the agent to handle the call and invoke the ICM recovery scripts. [The assumption is made that these scripts have been implemented, see Section 4.2.3 above.]

<p>Call Waiting Enable Flag</p>	<p>This parameter enables or disables call waiting for the Cisco CallManager System. This is a required field. Default: true. <<< change to false</p>
---------------------------------	--

5.2.8 Disk Drive Recommendations for High Traffic Systems

Add additional disk drive for logfiles if sustained high traffic levels are anticipated

In cases where long periods of traffic at or above the system's engineered capacity are expected, directing logfiles to a disk drive that does not contain the OS or operating software is recommended.

Rationale:

During the course of system load and stress testing, it was observed that long periods of traffic at or above the system's engineered capacity ran with lower CallManager CPU rates if system logfiles were directed to a disk drive that did not contain the OS and operating software. This was especially true when log levels were set higher than normal (more data being logged simulating a troubleshooting activity). If the conditions described above are anticipated, it is highly recommended that a second disk drive be added to all nodes in a CallManager cluster, including any IP IVR servers.