Configuration and Troubleshooting Guide for Cisco IPCC Remote Agent Option

IPCC Enterprise and Hosted Editions Release 7.0(0), IPCC Express Edition Release 4.0(0)

October 12, 2005

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 (6387)
Fax: 408 526-1400

Table of Contents

List of Figures

Preface

Purpose

This manual provides the system configuration guidelines and checklists that remote agents need to follow in order to successfully set up Cisco IPCC Remote Agent Option. The troubleshooting entries documented in this manual will help eliminate setup problems.

Note: Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)* and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web site** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm)) for details about operating system and software requirements.

Audience

There are two major audiences for IPCC Remote Agent Option:

- System Administrators/Installers – These users will use the existing design guides to design their system, and use existing Cisco IPCC/CallManager documentation.
- Remote Agents – These users set up the system at their remote location and use the system on a regular basis for customer interaction.

Organization

The following table describes the information contained in each section of this guide:

Section	Description
Introduction to IPCC Remote Agent Option (page 9)	Describes the IPCC Remote Agent Option application.
System Configuration for Remote Agent with IP Phone (page 15)	Describes how to configure IPCC Remote Agent Option when using an IP Phone.

Section	Description
System Configuration for Remote Agent with Analog Phone (page 17)	Describes how to configure IPCC Remote Agent Option when using an analog phone.
Remote Agent User Information (page 19)	Provides information about the desktops and installation and configuration validation checklists.
Troubleshooting Cisco IPCC Remote Agent Option (page 27)	Describes caveats and limitations, along with troubleshooting tips.
Sample Cisco IOS Configuration for Analog FXO to PRI Gateway (page 31)	Provides sample Cisco IOS configuration for an analog FXO to PRI gateway.

Related Documentation

For additional information about Cisco IP Contact Center (IPCC) software, see **the Cisco web page** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm) listing IPCC documentation.

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/techsupport

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD from the Ordering tool or Cisco Marketplace.

Cisco Ordering Tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL::

http://www.cisco.com/go/marketplace/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- 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 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL: **http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html**

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL: **http://www.cisco.com/go/psirt**

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL: **http://www.cisco.com/en/US/products/products_psirt_rss_feed.html**

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies - security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies - psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Note: We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list: **http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on**

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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

Note: Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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 provides recommended solutions. If your issue is not resolved using the recommended

resources, your service request is 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/

- 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

Chapter 1

Introduction to IPCC Remote Agent Option

IPCC Remote Agent Option provides the capability to use remote agents when staffing contact centers.

Note: A *remote agent* is classified as limited to a single agent working at a remote site, such as the agent's home or in an office outside the contact center's headquarters. They are not classified as agents working at one of the contact center's sites. Multiple agents sitting in remote sites are considered *branch agents*.

Support is provided for remote agents using one of the following options:

- Remote Agent with IP Phone (over a Cisco Business Ready Teleworker setup)

  Note: Refer to the Teleworker documentation set at the following web sites: **http://www.cisco.com/go/teleworker**, **http://www.cisco.com/go/v3pn**, and **http://www.cisco.com/go/srnd**.

- Remote Agent with analog phone

By means of this support, Cisco IPCC remote agents *with IP Phone* can benefit from standard Cisco 8xx series Router support, persistent VPN, Cisco IOS based security, and QoS for voice.

Agents are connected to the corporate network using a residential broadband (cable or DSL) network connection that can support voice, data, and video traffic. The connection is secure, and provides "always-on" access to call-center applications using a VPN. Built-in, end-to-end security helps ensure that confidential customer information, such as medical records and financial information, is protected, and the corporate network is secure from "back door" attacks.

This section contains the following topics:

About IPCC Remote Agent Option Primary Components

The primary components of the IPCC Remote Agent Option are:

- **Cisco IP Contact Center solution**: Cisco IP Contact Center combines Cisco IP telephony and ready-to-use computer telephony integration (CTI) capabilities in a call-center product suite. The software includes intelligent call routing, multichannel automatic call distribution (ACD) capability, IVR, call queuing, and consolidated reporting features.

  Cisco IP Contact Center components include the following:

  – Cisco CallManager: Provides traditional private branch exchange (PBX) telephony features and functions to packet-telephony devices. Installed on a server-class PC, Cisco CallManager software provides basic call processing, signaling, and connection services to Cisco IP Phones, VoIP gateways, and software applications.

  – Cisco Computer Telephony Integration Object Server (CTI OS) Desktop and Cisco Agent Desktop (CAD): Allow an agent to control the remote agent state (for example, Login, Available/Unavailable, and Work or Wrap Up) and perform call control (answer, release, hold, and transfer).

  – Cisco Customer Voice Portal (formerly Internet Service Node) or Cisco IP IVR: Provides announcements, prompting, gathering of caller-entered digits, and a queue point to park calls when all remote agents are busy.

  – VoIP gateways.

  – Centralized monitoring and recording: Provides call-center managers with real-time and historic data for all remote agents.

  Note: IPCC Remote Agent Option is supported on the Cisco IPCC Enterprise Edition, the Cisco IPCC Hosted Edition, and the Cisco IPCC Express Edition solutions.

- **Cisco Business Ready Teleworker architecture** (for IP Phone only): The Cisco Business Ready Teleworker architecture, combined with Cisco IP Contact Center, gives remote agents the same accessibility to call-center applications as staff based at central sites. Cisco Business Ready Teleworker provides the most comprehensive security and network management available in a teleworking environment over a standard cable or broadband connection. This includes QoS to help ensure prioritization of mission-critical or delay-sensitive traffic. Cisco Business Ready Teleworker can be quickly and cost-effectively deployed to deliver high-quality, consistent application access for remote agents through an always-on, secure, and centrally managed connection to the enterprise network.

  Note: A remote agent using an analog phone does not require a Cisco 8xx Series Router and does not use the Cisco Business Ready Teleworker setup.

  Cisco Business Ready Teleworker components include the following:

– VPN: Provides secure, consistent access to information, call-center applications, and customer data. The VPN tunnel is transparent to applications and the end user, and promotes stable and consistent application behavior over the WAN, protecting and extending existing infrastructure investments.

  Note: Agents will receive persistent VPN communication from the Cisco 800 Series Router.

– Advanced application access: With IP telephony a separate PBX, voice switch, or ACD call-control platform at the remote-agent location is not needed. Network-based ACD extends call-center services to thousands of remote-agent locations simultaneously.

– QoS: Helps ensure high-quality voice communication between the caller and remote agent. Voice, data, and video can be delivered over the same line by prioritizing applications based on bandwidth requirements or business priorities.

  Note: QoS delivers marked tagged packets, but the service is not guaranteed since it is over a service provider network.

– Network security and authentication: Security is integrated completely with all other functions. End-to-end security options for remote agents include trust and identity options (802.1x authentication), integrated firewall, intrusion detection system (IDS), and host-based intrusion detection with Cisco Security Agent.

– Centralized management and support: Helps ensure control over the performance of remote agents as though they were based on the main call center. Administrators can push policies and configurations transparently to remote-agent locations, perform quality surveys, and do real-time remote monitoring.

See Also

Refer to the Cisco IPCC, CTI OS, and CAD documentation set at **the Cisco web page** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm) for detailed information about these applications.

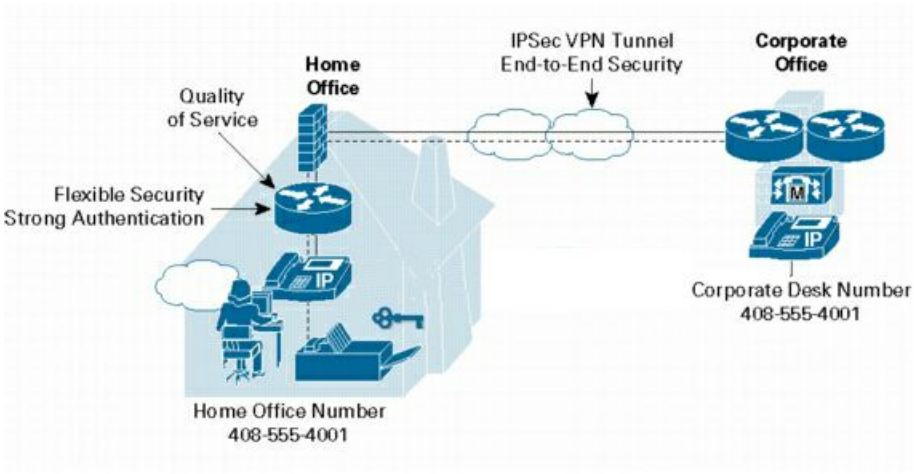
Refer to the Teleworker documentation set at the following web sites: **http://www.cisco.com/go/teleworker**, **http://www.cisco.com/go/v3pn**, and **http://www.cisco.com/go/srnd**.

How Cisco IPCC Remote Agent Option Works with an IP Phone

At the remote agent site, a Cisco IP Phone, with an ACD extension number, connects to a Cisco 8xx Series secure, persistent Broadband Router that provides a secure VPN connection back to the call center over a broadband facility. The router, based on Cisco IOS Software, provides all the features necessary for an always-on, business-ready connection in a single cost-effective platform. A Cisco CallManager on the corporate network provides the call management on the IP Phone.

Note: This is one option available when using IPCC Remote Agent Option. This product is also available using the Remote Agent with analog phone.

Figure 1: IPCC Remote Agent Option with IP Phone

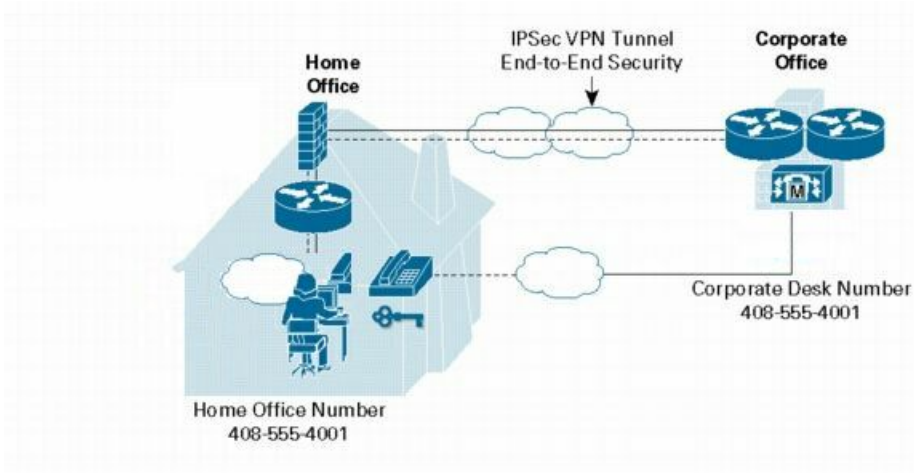


When a call comes in to the call center, the Cisco CallManager alerts the Cisco IP Contact Center, which then finds the best available remote agent based on customer-defined business rules. If no remote agents are available, the call is held in an IVR queue (so customers can listen to a recorded message or music) until an agent becomes available.

How Cisco IPCC Remote Agent Option Works with an Analog Phone

At the remote agent site, an analog phone connects to the PSTN and using an active broadband connection, the agent uses VPN to access the corporate site (using SoftVPN client) from his/her PC.

Figure 2: IPCC Remote Agent Option with Analog Phone

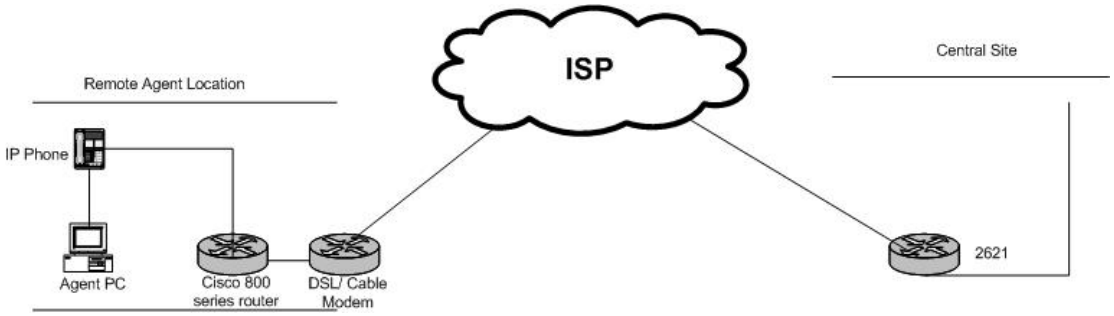


When a call comes in to the contact center, the Cisco CallManager alerts the Cisco IP Contact Center, which then finds the best available remote agent based on customer-defined business rules. If the remote agent is on an analog phone, CallManager sends the call to the Voice Gateway (VG248) which in turn sends it to the PSTN through the VoIP gateway's PRI lines. If no remote agents are available, the call is held in an IVR queue (so customers can listen to a recorded message or music) until an agent becomes available.

Remote Agent with IP Phone Call Flow

The following figure displays a typical call flow.

Figure 3: Remote Agent with IP Phone Call Flow

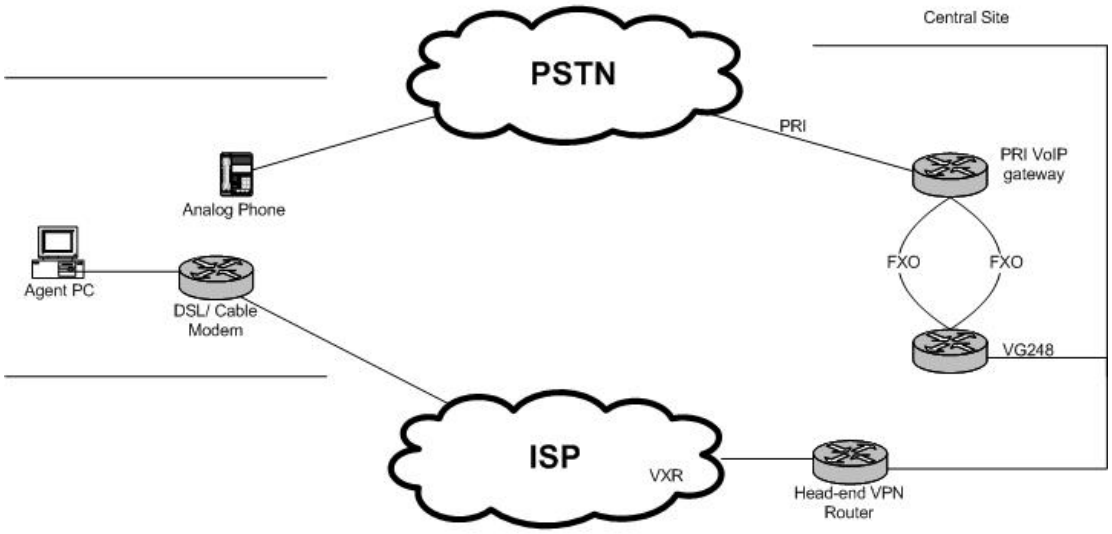


1. The remote agent becomes available by logging on to the corporate domain via VPN over the ADSL/Cable connection, and by launching the agent desktop interface to log on the CTI server. The remote agent then goes into a ready mode.
2. Customer calls in from PSTN.
3. Call flows in on PRI VoIP gateway.
4. Call is processed by CallManager and routed to Cisco IP IVR.
5. Call is sent to the remote agent.
6. The remote agent's IP Phone rings and the agent desktop receives a screen pop with the incoming call.
7. The supervisor, whether remote or in contact center, can fully control an agent, including barge, intercept, chat, and state controls.

Remote Agent with Analog Phone Call Flow

The following figure displays a typical call flow.

Figure 4: Remote Agent with Analog Phone Call Flow



1. The remote agent becomes available by logging on to the corporate domain via soft VPN over the ADSL/Cable connection, and by launching the agent desktop interface to log on the CTI server. The remote agent then goes into a ready mode.
2. Customer calls in from PSTN.
3. Call flows in on PRI VoIP gateway.
4. Call is processed by CallManager and routed to Cisco IP IVR.
5. A VG248 port is designated as the remote agent phone. An incoming call to IPCC sends a ring command to the VG248 port.
6. The VG248 FXS port is connected to the FXO port on the voice gateway.
7. The voice gateway using Private line automatic ring down (PLAR) forwards the ring command via the PSTN to the remote agent's analog phone.
8. The analog phone receives the ring command via its local PSTN provider. (This happens because the PLAR was sent from the IPCC voice gateway.)
9. The remote agent’s analog phone rings and the agent desktop receives a screen pop with the incoming call.

Chapter 2

System Configuration for Remote Agent with IP Phone

Configuration Guidelines

The following tables provide configuration checklists and guidelines users should follow when using the Remote Agent with IP Phone.

Note: Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)* and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web site** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm)) for details about operating system and software requirements.

Configuring Remote Agent with IP Phone

Step	Description
1.	Provision the remote agent PC and IP Phone on the IPCC central site to ensure operability *before* distributing it to a remote agent site.
2.	At a remote agent site, connect the agent desktop to the RJ45 port on the back of the IP Phone. **Note:** The IP Phone and agent desktop PC get their network settings from DHCP.
3.	Create a DNS entry for the remote agent desktop; otherwise, an agent will not be able to connect to a CTI server. DNS entries can be dynamically updated or entered as static updates.
4.	Configure the agent desktop PC at the remote site with an IP address, network mask, DNS, and default gateway configured for DHCP.
5.	Make sure the 7960 IP Phone has a power supply. (The Cisco 8xx Series Router will not supply power to the IP Phone.)
6.	Critical remote agents must have a backup power supply. The backup power supply must be able to power a PC, an 831 Router, a broadband modem, and an IP Phone.

Step	Description

Remote Agent with IP Phone Network Requirements Checklist

Complete	Network Requirements
[ ]	Ensure the ADSL and Cable bandwidth values are set to at least 256kb uplink and 1 Mbps downlink.
[ ]	Do not exceed 60ms to 90ms of jitter delay each way on the maximum ADSL network delay. If the ADSL delay is greater than the maximum, the IPCC application will encounter longer response times.
[ ]	Make sure the IPCC bandwidth value does not exceed 128k uplink; otherwise, the remote agent solution might not work properly.
[ ]	The default codec for 256kb uplink is the G.729. To achieve higher voice quality, use the G.711.
[ ]	Only unicast Music on Hold (MOH) streams are supported.
[ ]	Set up a transcoder to enable outside callers to receive MOH, if the MOH server is not set up to stream G.729 codec.
[ ]	As a backup to the remote agent desktop, you can configure the remote agent to use the IP Phone as a login device when possible.

IP Phone Considerations

IP Phones supported with IPCC Remote Agent Option are those currently compatible with IPCC as listed in the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)*.

Chapter 3

System Configuration for Remote Agent with Analog Phone

Configuration Guidelines

The following tables provide configuration checklists and guidelines users should follow when using the Remote Agent with analog phone.

Note: Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)* and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web site** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm)) for details about operating system and software requirements.

Configuring Remote Agent with Analog Phone

Step	Description
1.	Provision the remote agent PC and IP Phone on the IPCC central site to ensure operability *before* distributing it to a remote agent site.
2.	At a remote agent site, connect the agent desktop to the RJ45 port on the back of the IP Phone. **Note:** The IP Phone and agent desktop PC get their network settings from DHCP.
3.	Create a DNS entry for the remote agent desktop; otherwise, an agent will not be able to connect to a CTI server. DNS entries can be dynamically updated or entered as static updates.
4.	Configure the agent desktop PC at the remote site with an IP address, network mask, DNS, and default gateway configured for DHCP.
5.	Make sure you set up the soft VPN client to connect to the contact center's headquarters.

Remote Agent with Analog Phone Network Requirements Checklist

Complete	Network Requirements
[ ]	Do not exceed 150ms Round Trip Time (RTT) of ADSL/Cable network delay.
[ ]	Do not exceed not exceed 60ms of jitter delay.
[ ]	The minimum broadband bandwidth for the agent desktop is 256kb uplink and 1 Mbps downlink.
[ ]	Configure the voice gateway/access server with at least one active PRI, T1, E1, or DS3 connection to the PSTN.
[ ]	The remote agent's phone number is the number assigned via PLAR routing in the VoIP gateway. **Note:** The remote agent PSTN phone number might vary in an actual deployment.
[ ]	The phones at the remote sites will be analog phones only connected to the PSTN.
[ ]	The current configuration only supports unicast Music on Hold (MoH) streams. A Cisco CallManager is the MoH server.
[ ]	The maximum PSTN delay supported is 250ms.
[ ]	Configure the VG248 to use G.711.

Remote Agent with Analog Phone Considerations

An analog phone is classified as any PSTN phone; for example, a regular touchtone phone or a mobile/cell phone both qualify as analog phones.

Chapter 4

Remote Agent User Information

IPCC Remote Agent Option is available on the following Cisco desktops:

- **Cisco CTI Toolkit Agent Desktop**: Provides an interface that enables agents to perform telephony call control and agent state control. The CTI Toolkit Agent Desktop provides an interface to allow call data to be presented to an agent in the form of a screen pop. The CTI Toolkit Agent Desktop also provides agents with statistics and chat capability.

  Note: CTI OS only supports chat between agents on the same peripheral.

- **Cisco CTI Toolkit IPCC Supervisor Desktop**: The Supervisor Desktop has all of the functionality of the Agent Desktop, with additional functions for monitoring and managing Agent Team members.

  Note: The CTI Toolkit IPCC Supervisor Desktop is supported for use on Cisco IPCC Enterprise only. It is not supported for use on TDM peripherals.

- **Cisco Agent Desktop**: Provides call control capabilities—such as call answer, hold, conference, and transfer, and ACD state control—ready/not ready, wrap up, etc. Customer information is presented to an agent through an enterprise data window and an optional screen pop. Cisco Agent Desktop requires minimum screen real estate and enables agents to customize its functionality to meet their individual needs.

  Note: CAD is *not* available with IP Phone Agent using an analog phone.

Note:

- Refer to the Cisco CTI OS and CAD documentation at **the Cisco web page** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm) for detailed information about the desktops.

- Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)* and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web site** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm)) for details about desktop operating system and software requirements.

This section contains the following topics:

Using CTI Toolkit and CAD Desktops

Using the CTI Toolkit Agent Desktop

Action	Resolution
How does an agent log in to the desktop?	To log into CTI Toolkit Agent Desktop, click the **Login** button. The **Login** button connects agents to the CTI Server and logs agents into a selected ACD switch. When an agent clicks the **Login** button, the CTI Login dialog box appears. Enter the following information in the dialog box: • **Connect to**. Use the drop-down menu to select the connection profile that you want to use. • **Agent ID**. The agent ID as assigned by the agent's manager. **Note:** Depending on the option chosen for logging in during the installation of the CTI OS Server, the Login dialog on the Agent desktop will prompt for either the Agent ID or the Login Name. • **Password**. The password as assigned by the agent's manager. • **Instrument**. The device ID assigned to the teleset where the agent will receive calls. After entering this information, click the **OK** button. On a successful login, the following occurs: • The agent automatically enters the state configured on the switch, either Ready or Not Ready state. • The status bar on the bottom of the CTI Toolkit Agent Desktop Screen displays the following information – Agent ID for the logged in agent – Agent Extension – Agent Instrument – Current Agent Status – The server that the agent is connected to • Buttons for actions that are allowed from your current agent state are enabled.

Action	Resolution
	Note: If the **Login** button is not enabled when the CTI Toolkit Agent Desktop displays, the remote agent did not successfully log in.
How can an agent verify a successful login?	On a successful login, the following occurs: • The remote agent automatically enters the state configured on the switch, either Ready or Not Ready state. • The status bar on the bottom of the CTI Toolkit Agent Desktop window displays the following information: – Agent ID for the logged in agent – Agent Extension – Agent Instrument – Current Agent Status – The server that the agent is connected to • Buttons for actions that are allowed from your current agent state are enabled.
How does an agent enter the Ready state to start accepting calls?	An agent enters either Ready or Not Ready state on comletion of a successful login, depending on the configuration of the agent's switch. If the agent is in the Not Ready state and the **Ready** button is enabled, enter the Ready state by clicking the **Ready** button.
How does an agent perform a conference transfer?	To transfer a call, perform the following steps: 1. Click the **Transfer** button. The CTI Dialing Pad dialog box appears. 2. Enter the phone number to be dialed in the Dialed Number field or select a destination from the pull-down menu. The pull-down menu contains the last six numbers dialed from this desktop. 3. Optionally, click the **More** button to display the Call Data tab, where you can optionally enter data associated with the call. The remaining steps depend on whether or not the agent wants to speak with the consulted agent upon call transfer. • If the agent does not want to speak with the consulted agent, click the **Single Step** button. The call is transferred automatically. • If the agent wants to speak with the consulted agent, click the **Transfer Init** button. Once the **Transfer Init** button is pressed, the call will be put on hold. The agent has an opportunity to speak to the consulted agent before completing the transfer. When the consult call is answered, the button changes to **Transfer Complete**. To complete the transfer, click the **Transfer Complete** button.

Action	Resolution
How does an agent initiate a conference call?	To initiate a conference call, perform the following steps 1. Click the **Conference** button. The CTI Dialing Pad dialog box appears. 2. Enter the phone number to be dialed in the Dialed Number field or select a destination from the pull-down menu. The pull-down menu contains the last six numbers dialed from this desktop. 3. Optionally, click the **More** button to display the CTI Dialing Pad. 4. Click the **Conference Init** button. The call is now put on hold. The agent will have an opportunity to speak to the consulted agent before completing the conference. When the consult call is answered, the button changes to **Conference Complete**. To complete the conference, click the **Conference Complete** button. When the conference operation completes, the two calls then appear on the Call Information Grid as one call.
When is an agent available to make calls?	An agent is able to make calls if the **Dial** button is enabled. Depending on the agent's switch, the agent might also be able to make calls if the **Ready** or **Not Ready** buttons are enabled.

Using the CAD Desktop

Action	Resolution
How does an agent log in to the desktop?	To start Agent Desktop: 1. Choose **Start** > **Programs** > **Cisco** > **Desktop** > **Agent**. The Agent Login dialog box appears. **Note:** • For IPCC Enterprise only, Agent Desktop prompts for either the remote agent's Login ID or the Login Name in the Login dialog box. Which prompt appears depends on how the administrator has configured the system. • If the login method (Login Name or Login ID) is changed while the remote agent is in the process of logging in, an error message appears stating that the login method has changed. The remote agent must restart Agent Desktop in order to log in using the new method. (The information in this note is not applicable to IPCC Express.) 2. Enter the remote agent login ID or login name, password, and extension in the appropriate fields, and then click OK or press Enter. – If the remote agent attempts to log in and the login ID/login name (with or without the same extension used in association with it) is already in use by another agent, the remote agent will be asked to forcibly log in. If the remote agent opts to do so, that agent is logged in and the other agent using that ID will be logged out.

Action	Resolution
	– If the remote agent attempts to log in and the extension is already in use by another agent, that agent will not be able to log in unless a different extension is entered. Agent Desktop starts and is immediately minimized on the taskbar at the bottom of the remote agent's Windows desktop. Login notes: • The Login Name field can be a maximum of 32 characters. The Login ID, Extension, and Password fields can be a maximum of 12 characters. • Agent Desktop can control only those calls on the extension entered in the Login dialog box, even if the remote agent is configured with multiple extensions. • When logging in, the remote agent might see the error message, "A licensing error has occurred. Please see your administrator." This generally appears when all Agent Desktop software licenses are in use. For this reason, it is important that the remote agent close Agent Desktop completely when finished using it, rather than simply logging off. As long as Agent Desktop is running, one license is being used.
How does an agent get into the Ready state to start accepting calls?	Clicking the **Ready** button changes the state to Ready, indicating that the remote agent is available to receive ACD calls.
How does an agent transfer a call?	There are two types of transfer calls: • **Supervised transfers**. In a supervised transfer, the remote agent speaks to the third party to whom the call is being transferred before connecting the active call, in order to confirm that the third party is ready to accept the call. • **Blind transfers**. In a blind transfer, the remote agent transfers the active call to the third party without speaking. The remote agent hangs up before the third party answers the phone and therefore, can't confirm if the third party is ready to accept the call. To transfer a call: 1. With a call active, click **Transfer**. The Transferring Call window appears. 2. Enter the phone number to which the remote agent is transferring the call in the Name: Number field. 3. Click **Dial**. When the phone rings, the **Dial** button changes to the Transfer button. 4. Take one of the following actions:

Action	Resolution
	– For a supervised transfer, wait for the third person to answer the phone, announce the transfer, then click **Transfer**. – For a blind transfer, click **Transfer** without waiting for the third person to pick up the phone.
How does an agent initiate a conference call?	There are two types of conference calls: • **Supervised conference**. In a supervised conference, the remote agent speaks to the third party he or she wants to add to the call before completing the conference, in order to confirm that the third party is ready to accept the call. • **Blind conference**. In a blind conference, the remote agent adds the third party to the conference without speaking to him or her. **Note:** When using a blind conference to add someone to the call, the remote agent might or might not see the call tagged as a conference call in the dashboard pane. To make a conference call: 1. With a call active, click **Conference**. The Conferencing window appears. 2. Enter the phone number of the person the remote agent wants to add to the call in the Name: Number field. 3. Click **Dial**. When the phone rings, the **Dial** button changes to the **Add to Conf.** button. 4. Take one of the following actions: – For a supervised conference, wait for the third person to answer the phone, announce the conference, then click **Add to Conf**. – For a blind conference, click Add to Conf. without waiting for the third person to pick up the phone. The Conferencing window closes. 5. To add one or more people to the conference call, repeat Steps 1 to 4 for each person. **Note:** The total number of conference call participants on a call is determined by settings on the Cisco CallManager. Ask you supervisor for the total number configured for your contact center.

Action	Resolution
When is an agent available to make calls?	When the remote agent is in the Not Ready state and the system is functioning to enable call control, the agent is available to make and receive calls.

Installation and Configuration Checklists

Validating Installation and Configuration of Remote Agent with IP Phone Components Checklist

Complete	Issue	Resolution
[ ]	Does the IP Phone boot?	Make sure the separate power supply is used for the phone. The 831 router does not supply power to the IP Phone.
[ ]	Does the IP Phone register with CallManager?	The phone must be configured for DHCP; also, domain information must be entered in to the phone configuration.
[ ]	Is the IPsec tunnel running?	Reboot the 831.
[ ]	Do you have internet access?	Make sure you have network access to the internet.
[ ]	Can the agent desktop log in to CTI OS Server?	Make sure the PC is registered in DNS. Make sure the agent login ID/password is valid.
[ ]	When you pick up the IP Phone, does the desktop reflect that the line is off hook?	Cycle the PG for the remote agent.
[ ]	Are callers routed to the remote agent?	Make sure callers are routing to the remote agent and the PG is online.
[ ]	When the remote agent receives a call, does the desktop client's main window display the incoming call?	Check to see if the desktop client's main window displays the incoming call.
[ ]	Is the desktop window displaying the incoming call correctly?	Check to see if the desktop window displays the incoming call correctly.
[ ]	Does the MTP application log in?	If you are using the Platronics headset, make sure the USB connection is secure and that it is able to play sound from the desktop.
[ ]	What's the agent's readiness state when taking a call using an IP Phone?	Once the agent takes a call (either via the IP Phone or the agent desktop), the agent state changes to either the Talking state or the Not Ready state and the agent is unavailable for

Complete	Issue	Resolution
		calls. (The agent *will not* receive any calls while already on a call.)

Validating Installation and Configuration of Remote Agent with Analog Phone Components Checklist

Complete	Issue	Resolution
[ ]	Can the agent desktop log in to CTI OS Server?	Make sure the PC is registered in DNS. Make sure the agent login ID/password is valid.
[ ]	Is there a dial tone?	Pick up the analog phone and listen for a dial tone to ensure the phone is connected.
[ ]	Do you have internet access?	Make sure you have network access to the internet.
[ ]	Are callers routed to the remote agent?	Make sure callers are routing to the remote agent and the PG is online.
[ ]	What's the agent's readiness state when taking a call using an analog phone?	Remote agents using an analog phone must manually place themselves in the Not Ready state after taking a call.

Hardware Installation and Configuration

Refer to the *Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)* and the *Cisco Response Solutions (CRS) Software and Hardware Compatibility Guide* (located on the **Cisco web site** (http://www.cisco.com/univercd/cc/td/doc/product/icm/index.htm)) for details about desktop hardware requirements.

Chapter 5

Troubleshooting Cisco IPCC Remote Agent Option

Caveats and Limitations

Agent Limitations

- Only one IPCC Remote Agent Option per household is supported.
- IP Communicator for CTI OS or CAD Desktops is *not supported* for remote agents.
- Media Termination for CTI OS and CAD is *not* supported.
- CTI OS Agent Login might take up to 30 seconds. CAD Agent Login might take up to two minutes. Other operations such as Ready/Not ready are not impacted.
- There might be times when the ADSL/Cable link goes down. When the link is back up, the remote agent might have to reset their ADSL/Cable modem, 8xx Series Router, and IP Phone. The remote agent must become familiar with restarting the 8xx Series Router. Total time for the router to cycle is about two minutes. After which the remote agent will have to re-login again for CTI application.
- Cisco CAD-based IP Phone only agent and Cisco IP Phone control for CTI OS is *not* supported for remote agents.
- Remote agents might experience a delay in screen pop.
- The analog phone itself cannot initiate transfers, conferences, and holds. These functions can only be executed via the CTI OS/CAD desktop agent interface, and only to another agent.
- Remote agents can use the agent desktop interface to initiate calls, but only to other agents.

Supervisor Limitations

- Desktop-based Silent Monitoring/Recording will not work and is not supported. (Silent Monitor—for both CTI OS and CAD—is not supported with NAT.)
- Remote supervisors are *only* supported for the Remote Agent with IP Phone.

Network Limitations

- Network Address Translation (NAT) is supported when IPCC Remote Agent Option is used with the Cisco Business Ready Teleworker Model. Design guides for Business Ready Teleworker can be found at:
  - **http://www.cisco.com/go/teleworker**
  - **http://www.cisco.com/go/v3pn**
  - **http://www.cisco.com/go/srnd**
- Routing through a Cisco 800 Series Router with Firewall enabled is supported.
- The G.729 codec is not supported for software conference bridges. Voice quality might degrade when the remote agent IP Phone is configured using a G.729 codec and an agent enters a call manager software conference bridge. The conference bridge must be configured on a DSP hardware device. There is no loss of conference voice quality using a DSP conference bridge.

  Note: Use this solution even for pure IP telephony deployments.
- The IPCC server recognizes failures when the remote agent desktop or connection breaks. It will stop routing calls to that agent until an agent logs back in and goes to a ready call state. Callers will be routed to other available agents.
- The only traffic that is marked for priority AF31 from the agent desktop is voice. CTI traffic and Desktop Application traffic is not marked. Voice gets the priority. CRM Desktops like Siebel and Oracle are supported; however, Silent Monitoring and Recording is not supported for CRM Desktops such as Siebel, Oracle, and so forth. Silent Monitoring, both Desktop based and SPAN Port based, is not supported with CRM Desktops and will not work.
- Do not use soft VPN clients to establish VPN connectivity for remote agents with IP Phones. VPN connection has to be set up using hardware-based VPN through a 8xx Series Router.
- If the remote agent PC modem is down or the connection goes down, ICM software via CTI/CAD/CTI OS server will recognize the failure and will stop routing calls to that agent, until an agent logs back in again, and goes to a ready call state.
- If the ADSL/Cable delay is greater than the maximum, the IPCC application encounters longer application response times.

Security Limitations

- Wireless access points are supported; however, determine their use by the enterprise security policies of the customer. Wireless use does not affect remote agent performance since the bandwidth that wireless supports is greater than the broadband link.

  Note: 7920 Wireless IP Phones are not supported.

- This solution has only been tested with centralized IPCC and CallManager Clusters. Testing was *not* performed with CTI OS using security and Cisco Support Tools.

Reporting Limitations

- No special reports exist for individual remote agents. IPCC Enterprise reports as they pertain to a Headquarter Contact Center are applicable.
- Real Time reporting, Historical reporting, and the monitoring of desktop queue statistics are not supported.

Troubleshooting Information

This section lists troubleshooting FAQs and recovery tips.

Problem	Resolution
How do I find out what Codec is being used?	On Cisco 7960 IP Phones, press the information button twice (this is the "?" or the "I" button, depending on the model you are using).

Table 11: IPCC Remote Agent Option Failure Recovery Tips

Recovery Issue	Resolution
Power failure	Once the power is back up, verify that the machine comes back up properly and that the network is available. For CTI OS, start the CTI desktop and login to the CTI OS server. For Remote Option with IP Phone configuration, the IP Phone needs to contact the tftp server and register with Cisco CallManager. **Note:** UPS can mitigate the risk of a power failure at home by keeping the cable modem and agent's PC powered up for a certain duration.
Internet failure	Once the internet goes down, the connection is lost and the agent goes offline.

Recovery Issue	Resolution
	For CTI OS, once the internet is back up, the agent must re-connect to the CTI OS server and log back in. For Remote Option with IP Phone configuration, the IP Phone will also be disconnected and needs to be reconnected with Cisco CallManager.
Reconnection of the phone to the desktop	Connect the desktop to the IP Phone's second switch port, then connect the IP Phone to the 800 Series Router.
Desktop reboot	See Power failure, above.
Application restart	Restart the application and log back into the server. If a call is still in progress, do not change the state to Ready.
IP Phone registration failure	Verify that the Internet is available, followed by the network. If yes, check if the tftp server and Cisco CallManager are online.
VPN tunnel failure	If Internet access is available, but the connection to the corporate site is not, verify that the VPN tunnel is not misconfigured / broken. If it is broken, it will have to be reconfigured by the System Administrator.

Chapter 6

Sample Cisco IOS Configuration for Analog FXO to PRI Gateway

The following section provides a sample Cisco IOS configuration for an analog FXO to PRI gateway.

Analog FXO to PRI Gateway

```
hostname pri-fxo-gateway
!
isdn switch-type primary-ni
!
controller T1 3/0
framing esf
linecode b8zs
cablelength short 133
pri-group timeslots 1-24
!
interface Serial3/0:23
bandwidth 230400
no ip address
encapsulation hdlc
no logging event link-status
isdn switch-type primary-ni
isdn incoming-voice voice
no cdp enable
!
voice-port 1/0/0
connection plar opx 4085551234
!
voice-port 1/0/1
connection plar opx 4085551235
!
dial-peer cor custom
!
dial-peer voice 1 pots
destination-pattern 4085551234
```

```
no digit-strip
port 3/0:23
!
dial-peer voice 100 pots
destination-pattern 4085551235
no digit-strip
port 3/0:23
!
end
```

Index