Cisco Customer Response Solutions (CRS) Port Utilization Guide

5.0(1)

May 2007

Americas 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: 408 527-0833

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 UCBs 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.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0704R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

Table of Contents

Preface 1
- Purpose 1
- Audience 1
- Organization 1
- Related Documentation 1
- Conventions....1
- Obtaining Documentation....2
  - Cisco.com....3
  - Product Documentation DVD....3
  - Ordering Documentation....3
- Documentation Feedback....3
- Product Alerts and Field Notices 4
- Cisco Product Security Overview....4
  - Reporting Security Problems in Cisco Products 5
- Obtaining Technical Assistance....5
  - Cisco Technical Support & Documentation Website....6
  - Submitting a Service Request....6
  - Definitions of Service Request Severity....7
- Obtaining Additional Publications and Information....7

1. Cisco Unified IP IVR and Cisco Unified Contact Center Express Port Utilization....9
- Port Utilization Table Column Definitions....9
- Cisco Unified IP IVR Port Utilization 10
- Cisco Unified Contact Center Express Port Utilization 12

Preface

Purpose

This document provides a list of the TCP and UDP ports used by Cisco CRS 5.0(1), including Cisco Unified IP IVR (Unified IP IVR) and Cisco Unified Contact Center Express (Unified CCX).

Audience

This document is intended primarily for network administrators.

Organization

Port listings are presented in a table format.

Related Documentation

For port utilization of Unified ICM/IPCC 7.x, see the *7.2 Port Utilization Guide for Cisco Unified ICM/IPCC.*

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: **`<html><title>Cisco Systems,Inc. </title></html>`**
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

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

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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 (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at **tech-doc-store-mkpl@external.cisco.com** or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

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 submit comments about Cisco documentation 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.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can register to receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information. Access the tool at this URL: **http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en**.

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 will find information about how to:

- 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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at 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:

- For Emergencies only: 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.

- For 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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

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

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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 & Documentation 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 Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- 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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- 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

Cisco Unified IP IVR and Cisco Unified Contact Center Express Port Utilization

Port Utilization Table Column Definitions

The columns in the Port Utilization tables in this document describe the following:

- **Protocol**. A value representing a formal description of rules to follow and messages to be used by two or more systems to exchange information. The protocol is also used to communicate with an application or service listening to or connecting to a remote device.
- **Remote Source Port**. An identifier—usually dynamic—for the port the remote application or service uses to connect to the local destination port.
- **Destination Port**. An identifier for the TCP or UDP port that the local service or application is listening on, along with the IP address for incoming connection requests when acting as a server.
- **Source Port**. An identifier—usually dynamic—for the port the local application or service uses to connect to the remote device's destination port.
- **Remote Device Destination Port**. The identifier for the TCP or UDP port that the remote device's service or application is listening on, along with the IP address for incoming connection requests when acting as the server.
- **Remote Device**. The remote application or device making a connection to the server or service specified by the protocol.

NOTE: When accessing the Real Time Reporting (RTR) Client on CRS using a browser, the following occurs: The client will initially communicate to CRS via the pre-configured RMI Port (1099). The CRS server side OS will then determine what port out of the Ephemeral port

range will be used. These have traditionally been between 1024 and 4999 for the Windows OS. Ephemeral (Dynamic) port range for OS 2000.2.7 and beyond has been changed to 49152 – 65534. This change was implemented to prevent ports used by Cisco IP Telephony applications from being dynamically assigned and to bring the OS in alignment with the IANA recommendations. These additional ports have been reserved for compatibility with some Cisco IP Telephony applications: 57606, 59000-59100, 63432. Previous OS versions used the Windows 2000 default of 1024 – 4999.

Cisco Unified IP IVR Port Utilization

Cisco Unified IP IVR Port Utilization For Product Revisions: Unified IP IVR 5.0.

Table 1: Unified IP IVR Port Utilization

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
MS Terminal Services		TCP 3389		Windows Terminal Services	
VNC HTTP Helper		TCP 580x			Remote Control
VNC Display		TCP 690x		Virtual Network Computer Display	Remote Control
SMTP			TCP 25	Email POP server	Email notification
HTTP		TCP 6293		Administrator Web browsers	Required for system maintenance
		TCP 6294		Unified IP IVR server	Cluster View Daemon (CVD)
		TCP 994		Unified IP IVR server	CVD
		UDP 996		Unified IP IVR server	CVD
SVCHOST		TCP 135	TCP 135		Windows Service Loader

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
HTTPS			TCP 8443	AXL on Unified CM	
		TCP 1039	TCP 1039		Windows Task Scheduler
		TCP 1042	TCP 1042	SQL Server Process	
		TCP 4433		HR Reporting Client	
RMI		TCP 1099	TCP 1099	RMI Service	
JDBC/SQL		TCP 1433	TCP 1433	Enterprise Database Server	Unified IP IVR DB Subsystem
CTI/QBE			TCP 2748	Unified CM Cisco Unified E-main Integration Manager (Unified EIM) Cisco Unified Web Integration manager (Unified WIM)	JTAPI
HTTP		TCP 8080	TCP 8080	User Web Browser/Web Server	HTTP Trigger/HTTP Steps
RTP	UDP 16384 -32767		UDP 16384 -32767	IP Phones, IP Communicator, Voice Gateways	Voice Media
VRU message interface GED-125		TCP 5000		Unified CCE VRU PG	Port number is configurable.
			TCP 1444	CiscoWorks	Alarm Service
MRCP					

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
RTP/RTCP	UDP 16384 -32767		UDP 16384 -32767	MRCP Speech Server	
RTSP			TCP 554 or TCP 4900	MRCP Speech Server	

Cisco Unified Contact Center Express Port Utilization

Cisco Unified Contact Center Express Port Utilization For Product Revisions: Unified CCX 5.0.

Table 2: Unified CCX Port Utilization

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
MS Terminal Services		TCP 3389		Windows Terminal Services	
VNC HTTP Helper		TCP 580x			Remote Control
VNC Display		TCP 690x		Virtual Network Computer Display	Remote Control
SMTP			TCP 25	Email POP server	Email notification
HTTP		TCP 990			Bootstrap service request listening port
		TCP 6295			Server port used by Bootstrap Service
		TCP 6293		Administrator Web Browsers	Required for System Maintenance
		TCP 6294		Unified IP IVR server	Cluster View Daemon (CVD)
		TCP 994		Unified IP IVR server	CVD
		UDP 996		Unified IP IVR server	CVD
SVCHOST		TCP 135	TCP 135		Windows Service Loader

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
HTTPS		TCP 8443	AXL on CallManager		
		TCP 1039	TCP 1039		Windows Task Scheduler
		TCP 1042	TCP 1042	SQL Server Process	
		TCP 4433		HR Report Client	
RMI		TCP 1099	TCP 1099	RMI Server	
JDBC / SQL		TCP 1433	TCP 1433	Enterprise Database Server	Unified CCX DB Subsystem
CTI/QBE			TCP 2748	Unified CM Unified EIM Unified WIM	JTAPI
HTTP		TCP 59010		Phone Agent, User Web Browser	The Cisco Agent Desktop agent login through the phone display is an IP phone service linked to an HTTP trigger on Unified CCX.
RTP	UDP 16384 –32767		UDP 16384–32767	IP Phones, IP Communicator, Voice Gateways	Voice Media
ACMI message interface; GED-188		TCP 42027		Cisco Agent Desktop (CAD), Unified CCX Gateway PG	Port number is configurable.
SCCP			TCP 2000	Cisco Unified CM	Used by the phones (media termination and hard phones) to communicate with Unified CM.
			TCP 1444	CiscoWorks	Alarm Service
MRCP					

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
RTSP			TCP 554 or TCP 4900	MRCP Speech Server	
RTP/RTCP	UDP 16384-32767		UDP 16384-32767	MRCP Speech Server	
Cisco Agent Desktop					
		TCP 59020		Cisco Desktop Chat Service	The Chat service sends messages to the CAD desktop via this port.
		TCP 38983		LDAP Service	CAD and CSD
		TCP 63432		LRM Service	CAD and CSD
CORBA		TCP 59028		Cisco Supervisor Desktop, Cisco Recording and Playback Service	Desktop Monitoring service CORBA port. CSD sends monitoring requests to this port. The Recording and Playback service sends recording requests to this port.
ICMP				Unified CCX Server	CAD uses ICMP to constantly check its communication path with the Unified CCX Server. **Note:** A customer deploying a firewall between CAD and the Unified CCX server should **not** disable ICMP in the firewall.
Cisco Supervisor Desktop					
		TCP 59021		Cisco Desktop Chat Service	The Chat service sends messages to the CAD desktop via this port.
RTP		UDP 59010–59012		Cisco Desktop VoIP Monitor	The configured VoIP Monitor service or

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
				Service, Cisco Agent Desktop	agent desktop sends the RTP streams for monitoring requests to the supervisor to these ports. The To-Agent RTP stream is sent to port 59010 and the From-Agent stream is sent to port 59012.
RTP		UDP 59014, 59016 and 59018		Cisco Recording and Playback Service	When a supervisor is listening to a recorded call (playback), the To-Agent RTP stream is sent to port 59014. The From-Agent stream is sent to port 59016. Port 59018 is used to test the connection to the Recording and Playback service before accepting the RTP streams.
Cisco Desktop VoIP Monitor Service					
CORBA		TCP 59002		Cisco Supervisor Desktop, Cisco Recording and Playback Service	VoIP Monitor service CORBA port. CSD sends monitoring requests to this port. The Recording and Playback service sends recording requests to this port.
		TCP 37606		Cisco Desktop Recording and Statistics Service, Cisco Supervisor Desktop, Cisco Agent Desktop	VPN IP address discovery port. Clients behind a VPN send requests to this port to obtain their VPN IP address.

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
Cisco Desktop Chat Service					
CORBA		TCP 59000		Cisco Agent Desktop, Cisco Supervisor Desktop, Cisco IP Desktop IP Phone Service	Chat service CORBA port
		TCP 37350		Cisco Agent Desktop, Cisco Supervisor Desktop, Cisco IP Desktop IP Phone Service	VPN IP address discovery port. Clients behind a VPN send requests to this port to obtain their VPN IP address.
Cisco Desktop Recording and Statistics Service					
CORBA		TCP 59003		Cisco Agent Desktop, Cisco Supervisor Desktop, IP Phone Agent service	Recording and Statistics service CORBA port. Recording requests, call status, and agent state change information are sent to this port.
Cisco Desktop Recording and Playback Service					
CORBA		TCP 59005		Cisco Desktop Recording and Statistics Service	Recording and Playback service CORBA port.
RTP		TCP 59500-59700		Cisco Desktop VoIP Monitor Service, Cisco Agent Desktop	The configured VoIP Monitor service or agent desktop sends the RTP streams for recording requests to these ports. Two unique ports are used for each concurrent recording session. This port range may be changed.

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
		TCP 59027		Cisco Supervisor Desktop	VPN IP address discovery port. Clients behind a VPN send requests to this port to obtain their VPN IP address.
Cisco IP Phone Agent					
		59022		Cisco Desktop Chat Service	
CORBA		TCP 59010		Cisco Desktop Administrator	IP Phone Agent CORBA port.
HTTP		TCP 8080		IPPA Servlet running under Tomcat web server.	
Cisco Desktop Directory Service					
LDAP		TCP 38983		Cisco Agent Desktop, Cisco Supervisor Desktop, Cisco Desktop Administrator, and all other Cisco Desktop Services	LDAP Directory services port. All Desktop applications and services use the LDAP client to access the information stored in LDAP.
Cisco Desktop Enterprise Service					
CORBA		TCP 59004		Cisco Desktop Administrator, Cisco Agent Desktop,, Cisco IP Phone Agent Service	Enterprise service CORBA port
Cisco Desktop Sync Service					
CORBA		TCP 59011		Cisco Desktop Administrator	Sync service CORBA port.
Cisco LDAP Monitor Service					

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
CORBA		TCP 59030		Cisco Desktop Administrator	LDAP Monitor service CORBA port
Cisco License and Resource Manager Service (LRM)					
CORBA		TCP 65432		Cisco Agent Desktop, Cisco Supervisor Desktop, Cisco Desktop Administrator, and all other Cisco Desktop Services	LRM service CORBA port.
Unified CME					
Cisco Unified Communications Manager Express (Unified CME) Deployment		5060			SIP communication with Unified CME

The entries for each component in the table above show the server connections for that component rather than all connections. In particular, the following table lists the ports from the machine running the Cisco Agent Desktop/Supervisor base services and from the IP Phone Agent. Cisco Agent Desktop/Supervisor applications and the IP Phone Agent must be able to communicate with the Unified CCX Server through these ports.

Destination Port	Description
Cisco Agent/Supervisor Desktop	
TCP 37350	Chat/LDAP server's VPN server port
TCP 37606	VoIP VPN Server
TCP 38983	LDAP Server
TCP 42027	Unified CCX CTI Server
TCP 59000	CORBA chat service
TCP 59002	VoIP Server
TCP 59003	Rascal Server
TCP 59004	Enterprise Server
TCP 59005	Recording Server
TCP 59011	Sync Server
TCP 59012	VoIP client's from-agent monitoring port
TCP 59014	Recording server's to-client port
TCP 59016	Recording server's from-client port
TCP 59018	Recording server's null client port

Destination Port	Description
TCP 59020	CAD Chat client's CORBA port
TCP 59021	CSD Chat client's CORBA port
TCP 59027	Recording server's VPN server port
TCP 59028	Desktop Monitor's CORBA port
TCP 59030	LDAP Monitor server port
UDP 59010 and 59012	VoIP client's recording port range
UDP 59014, 59016, and 59018	Recording client port range
TCP 65432	LRM Server
IP Phone Agent	
TCP 8080	IPPA Servlet running under Tomcat web server
UDP 59010	IPPA server CORBA port and VoIP client's to-agent monitoring port.