CISCO SYSTEMS

Port Utilization Guide
Cisco CRS (IP IVR and IPCC Express)
Release 4.01

August 12, 2005

Table of Contents

Preface

Purpose

This document provides a list of the TCP and UDP ports used by Cisco CRS 4.0(1), including IP IVR and IPCC Express.

Audience

This document is intended primarily for network administrators.

Organization

Port listing are presented in a table format.

Related Documentation

For port utilization of ICM/IPCC 7.0(0), see the **7.0(0) Port Utilization Guide for Cisco ICM/IPCC** (http://www.cisco.com/univercd/cc/td/doc/product/icm/port_uti/).

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

Cisco CRS (IP IVR and IPCC 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 exchanging 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.

- 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 Cisco IP Telephony 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 IP IVR Port Utilization

Cisco IP IVR Port Utilization For Product Revisions: IP IVR 4.x

Table 1: Cisco 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
HTTP		TCP 6294		IP IVR Server	Cluster View Daemon (CVD)
		TCP 994		IP IVR Server	Cluster View Daemon (CVD)
		TCP 996		IP IVR Server	Cluster View Daemon (CVD)
		UDP 996		IP IVR Server	Cluster View Daemon (CVD) Heartbeats
LDAP			TCP 8404	DCD Directory on CallManager	
LDAP			TCP 389	Microsoft Active Directory	
LDAP			TCP 390	Netscape Directory	
SVCHOST		TCP 135	TCP 135		Windows Service Loader

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
		TCP 789	TCP 789	IP IVR Main Server	WFEngineService Process (Debug Port)
		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	IP IVR DB Subsystem
CTI/QBE			TCP 2748	CallManager	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		IPCC Enterprise VRU PG	Port number is configurable.
			TCP 1444	CiscoWorks	Alarm Service
		TCP 3927		BARS Server	BARS/Upgrade
		TCP 4027		BARS Server	BARS/Upgrade
		TCP 4127		BARS Server	BARS/Upgrade
Nuance					
RTSP			TCP 554	Nuance MRCP Speech Server	
RTP/RTCP	UDP 16384 -32767		UDP 16384 -32767	Nuance MRCP Speech Server	

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

Cisco IPCC Express Port Utilization

Cisco IPCC Express Port Utilization For Product Revisions: IPCC Express 4.x

Table 2: Cisco IPCC Express 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
HTTP		TCP 6294		IPCC Express Server	Cluster View Daemon (CVD)
		TCP 994		IPCC Express Server	Cluster View Daemon (CVD)
		TCP 996		IPCC Express Server	Cluster View Daemon (CVD)
		UDP 996		IPCC Express Server	Cluster View Daemon (CVD) Heartbeats

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
LDAP			TCP 8404	DCD Directory on CallManager	
LDAP			TCP 389	Microsoft Active Directory	
LDAP			TCP 390	Netscape Directory	
SVCHOST		TCP 135	TCP 135		Windows Service Loader
		TCP 789	TCP 789	IPCC Express Main Server	WFEngineService Process (Debug Port)
		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	IPCC Express DB Subsystem
CTI/QBE			TCP 2748	CallManager	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 IPCC Express.
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), IPCC Gateway PG	Port number is configurable.
SCCP			TCP 2000	CallManager	Used by the phones (media termination and hard phones) to communicate with the CallManager.

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
			TCP 1444	CiscoWorks	Alarm Service
		TCP 3927		BARS Server	BARS/Upgrade
		TCP 4027		BARS Server	BARS/Upgrade
		TCP 4127		BARS Server	BARS/Upgrade
Nuance					
RTSP			TCP 554	Nuance MRCP Speech Server	
RTP/RTCP	UDP 16384 -32767		UDP 16384 -32767	Nuance MRCP Speech Server	
Scansoft					
RTSP			TCP 4900	Scansoft MRCP Speech Server	
RTP/RTCP	UDP 16384 -32767		UDP 16384 -32767	Scansoft MRCP Speech Server	
Cisco Agent Desktop					
		TCP 59020		Cisco Desktop Chat Service	The Chat service sends messages to the CAD desktop via this port
CORBA		TCP 59028		Cisco Supervisor Desktop, Cisco Recording and Playback Service	Desktop Monitor service CORBA port. CSD sends monitoring requests to this port. The Recording and Playback service sends recording reqests to this port.
Cisco Supervisor Desktop					

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
		TCP 59021		Cisco Desktop Chat Service	The Chat service sends messages to the CSD desktop via this port.
RTP		UDP 59010 and 59012		Cisco Desktop VoIP Monitor Service, Cisco Agent Desktop	The configured VoIP Monitor service or 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 will send requests to this port to obtain their VPN IP address.
Cisco Desktop Chat Service					

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
CORBA		TCP 59000		Cisco Agent Desktop,Cisco Supervisor Desktop,Cisco Desktop IP Phone Service.	Chat service CORBA port
		TCP 37350		Cisco Agent Desktop,Cisco Supervisor Desktop, IP Phone Agent service	VPN IP address discovery port. Clients behind a VPN will 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		UDP 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.
		TCP 59027		Cisco Supervisor Desktop	VPN IP address discovery port. Clients behind a VPN will 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 IP Phone Agent					
CORBA		TCP 59010		Cisco Desktop Administrator, IPPA JSP client	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					
CORBA		TCP 59030		Cisco Desktop Administrator	LDAP Monitor service CORBA port
Cisco License and Resource					

Protocol	Remote Source Port	Destination Port	Remote Device Destination Port	Remote Device	Notes
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

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 the IPCC Express Server(s) 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	IPCC Express CTI Server
TCP 59000	LDAP Server port
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

Destination Port	Description
TCP 59016	Recording server's from-client port
TCP 59018	Recording server's null client port
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.