Cisco TelePresence Firewall and Access List Considerations

Revised: November 2014, OL-18391-01

Contents

This appendix contains the following sections:

Overview

Cisco TelePresence is a component of the Cisco Unified Communications suite and is designed to be deployed on a converged IP network. Many enterprise customers rely on firewalls and/or Access Control Lists (ACLs) to protect their Unified Communications network from various sorts of malicious threats. ACLs are also frequently used to enforce Quality of Service (QoS) settings, including marking, shaping and policing traffic at various places in the network, such as at the access edge of a local area network (LAN), or at the intersection of a LAN and wide area network (WAN).

The Cisco Unified Communications suite already fully supports a proven security framework, which in turn is one component of the Security Architecture for Enterprises (SAFE) Blueprint for Unified Communications. As a SIP-based end user device of Cisco Unified Communications Manager, Cisco TelePresence fits into this framework and the existing concepts, methodologies and best practices for deploying firewalls and ACLs with Cisco Unified Communications. For more details on these and related security concepts, please refer to the following link:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/security.html

There are three key considerations for using Firewalls and/or Access Control Lists with Cisco TelePresence:

1. The specific TCP and UDP ports that need to be permitted between each component of the solution.
2. The bandwidth required for the audio and video media streams of a Cisco TelePresence meeting is significantly higher and far less tolerant to latency, jitter and loss than a typical voice call and should be taken into consideration when considering specific router, firewall and intrusion prevention (IPS) platforms and their performance characteristics.

3. Firewalls that rely on Application Layer Inspection in order to dynamically open/close certain UDP ports may not support the specific SIP protocol implementation of Cisco TelePresence, or may not be able to inspect the contents of the application layer protocol because it is encrypted.

This document only addresses the first of the above three considerations. It provides the list of TCP and UDP ports used by Cisco TelePresence. It does not provide guidance on which router, firewall or IPS platforms or configurations customers should use. General firewall design guidance for Cisco TelePresence can be found in Chapter 13 of the Cisco TelePresence Network Systems Design Guide at the following path:

http://www.cisco.com/go/cvd > **Design Zone for Video** > **Cisco TelePresence**

This document should be used in conjunction with the above chapter.

Note Customers are advised to thoroughly test Cisco TelePresence against their specific firewall, ACL, or IPS configurations prior to deploying them in production.

Table A-1 contains document terminology definitions.

Table A-1 Terminology Used in This Document

Term	Definition
CTS Primary Codec	Cisco TelePresence System Primary Codec.
Phone	Cisco Unified 797X Series IP Phone which is attached to the Cisco TelePresence System.
CTS-Manager	Cisco TelePresence Manager.
CTMS	Cisco TelePresence Multipoint Switch.
CUCM (Cisco Unified CM)	Cisco Unified Communications Manager.
ephemeral	A random range of TCP or UDP ports which are dynamically assigned. Many protocols use ephemeral source ports with well-known destination ports. However, TFTP is an exception, as noted in the tables below, which uses ephemeral ports in both directions.

TCP and UDP Ports for Cisco TelePresence

This appendix contains information about ports used by Cisco TelePresence that are relevant to a firewall or ACL administrator. Ports used for internal communications, such as between the Cisco TelePresence Primary and Secondary Codecs, and between the Cisco TelePresence Primary Codec and the Cisco Unified IP Phone 797X are not included in this appendix. For a comprehensive list of all ports used by Cisco Unified CM release 7.0, please refer to the following information:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/7_0/CCM_7.0PortList.pdf

The following tables provide lists of TCP and UDP ports that are used by the Cisco TelePresence solution.

- Cisco TelePresence System (CTS) Codec, page A-3
- Cisco Unified IP Phone 797X, page A-5
- Cisco TelePresence Manager (CTS-Manager), page A-7
- Cisco TelePresence Multipoint Switch (CTMS), page A-11

- Cisco TelePresence Recording Server (CTRS), page A-13
- Cisco IOS IP Service Level Agreements (IPSLA), page A-14
- Cisco Media Experience Engine (MXE) 5600, page A-15

Cisco TelePresence System (CTS) Codec

Table A-2 contains information about the CTS codec.

Table A-2 Cisco TelePresence System Primary Codec

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	CTS Primary Codec: N/A	Switch: N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached and learn what Virtual LAN (VLAN) it should tag its packets with. **Note** CDP is a layer-2 protocol and hence does not use TCP or UDP for transport.
DHCP	UDP	0.0.0.0: 68 CTS Primary Codec: 68	Broadcast: 67	Requests an IP address from the DHCP server. **Note** It is recommended to use static IP addressing instead of DHCP on every CTS endpoint.
	UDP	0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTS Primary Codec: 123	NTP: 123	Synchronizes the hardware clock on the CTS with an NTP server.
DNS	UDP	CTS Primary Codec: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
HTTP	TCP	ANY: Ephemeral	CTS Primary Codec: 80, 443	Accesses the administrative web interface of the CTS Codec. Port 80 is automatically redirected to port 443.

Table A-2 Cisco TelePresence System Primary Codec

		CTS Primary Codec: Ephemeral	CUCM: 6970	Downloads configuration and firmware files from the Cisco Unified CM TFTP service. **Note** The CTS Primary Codec uses HTTP instead of TFTP for accessing these files.
		CTS Primary Codec: Ephemeral	CUCM: 8080	Used by the Directories feature on the CTS Cisco Unified IP Phone user interface to search the Cisco Unified CM LDAP directory.
		• CTS Primary Codec: Ephemeral • CTS-Manager: Ephemeral	• CTS-Manager: 8080, 8444 • CTS Primary Codec: 8081, 9501	Uses XML/SOAP to coordinate meeting schedule and system operational status with CTS-Manager: • When security is enabled, the CTS uses port 8444 and CTS-Manager uses port 9501 on the CTS (recommended). • When security is not enabled, CTS uses port 8080 on CTS-Manager and CTS-Manager uses port 8081 on the CTS.
		CTS Primary Codec: Ephemeral	CTS Administrative GUI: 8082	Sends an HTML request to the GUI to check the status of a software upgrade.
		CTS Primary Codec: Ephemeral	CTMS: 9501	Uses XML between each CTS and the CTMS for in-meeting controls such as Site/Segment Switching and Meeting Lock/Unlock.
SSH	TCP	ANY: Ephemeral	CTS Primary Codec: 22	Accesses the CTS codec administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTS Primary Codec: 161	Receives SNMP queries from a management station.
		CTS Primary Codec: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
CAPF	TCP	CTS Primary Codec: Ephemeral	CUCM: 3804	Registers its Manufacturing Installed Certificate (MIC), or obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	CTS Primary Codec: Ephemeral	CUCM: 6970 and 2444 (see notes)	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List (CTL) Provider service. When downloading the CTL, port 2444 is used.
SIP	UDP	CTS Primary Codec: Ephemeral	CUCM: 5060	Used for registration and call signaling between the CTS and Cisco Unified CM. Can be one of the following: • UDP port 5060 • TCP port 5060 • TCP port 5061 if SIP over TLS is enabled (recommended).
	TCP		CUCM: 5060, 5061	
RTP	UDP	CTS Primary Codec: 16384 – 32768	ANY: ANY	Sends and receives audio and video media.

Table A-2 Cisco TelePresence System Primary Codec

XML-R PC	TCP	CTS Primary Codec: Ephemeral	Phone: 61456	Autostarts the MIDlet phone user interface (UI).
		Phone: Ephemeral	CTS Primary Codec: 61457	Sends notifications to the MIDlet phone UI.
		Phone: Ephemeral	CTS Primary Codec: 61458	Receives notifications from the MIDlet phone UI.

Cisco Unified IP Phone 797X

Table A-3 contains information about the Cisco Unified IP Phone 797x for Cisco Unified CM Release 8.5(3).

Note This section only applies to systems that use the Cisco Unified IP Phone for call control. Systems that use the Cisco Touch device for call control do not require additional access to external ports.

Table A-3 Cisco Unified IP Phone 797x - Release 8.5(3)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	Phone: N/A	Switch: N/A	Advertises its existence to the CTS Primary Codec and to the upstream Cisco Catalyst Ethernet Switch to which it is attached to learn what Virtual LAN (VLAN) it should tag its packets with and to negotiate Power over Ethernet. **Note** CDP is a layer-2 protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 Phone: 68	Broadcast: 67	Requests an IP address from the DHCP server.
	UDP	0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	Phone: 123	NTP: 123	Synchronizes the hardware clock on the phone with an NTP server.
DNS	UDP	Phone: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-3 Cisco Unified IP Phone 797x - Release 8.5(3) (continued)

TFTP	UDP	Phone: Ephemeral	TFTP: 69	Downloads configuration and firmware files from the Cisco Unified CM TFTP service.
		TFTP: Ephemeral	Phone: Ephemeral	The initial TFTP request to port 69 spawns unique sessions for each configuration and firmware file downloaded. These sessions are established using ephemeral source and destination ports.
HTTP	TCP	ANY: Ephemeral	Phone: 80	Accesses the administrative web interface for the CTS Cisco Unified IP phone (for troubleshooting purposes only).
SSH	TCP	ANY: Ephemeral	Phone: 22	Accesses the administrative command-line interface (CLI) of the CTS Cisco Unified IP Phone (for troubleshooting purposes only).
CAPF	TCP	Phone: Ephemeral	CUCM: 3804	Registers its Manufacturing Installed Certificate (MIC), or obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	Phone: Ephemeral	CUCM: 2444	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List (CTL) Provider service.
SIP	UDP	Phone: Ephemeral	CUCM: 5060	Used for registration and call signaling between the phone and Cisco Unified CM. Can be UDP port 5060, TCP port 5060, or TCP port 5061 if SIP over TLS is enabled. SIP over TLS is recommended.
	TCP	—	CUCM: 5060, 5061	
RTP	UDP	Phone: 16384 – 32768	ANY: ANY	Sends and receives audio media.
XML-RPC	TCP	CTS Primary Codec: Ephemeral	Phone: 61456	Autostarts the MIDlet phone UI.
		Phone: Ephemeral	CTS Primary Codec: 61457	Sends notifications to the MIDlet phone UI.
		Phone: Ephemeral	CTS Primary Codec: 61458	Receives notifications from the MIDlet phone UI.

Cisco TelePresence Manager (CTS-Manager)

See the following tables for CTS-Manager support:

- Cisco TelePresence Manager (CTS Manager) for Microsoft Exchange, page A-7
- Cisco TelePresence Manager for IBM Domino, page A-9

Cisco TelePresence Manager (CTS Manager) for Microsoft Exchange

Table A-4 contains information about CTS Manager Release 1.7(x) and later with Microsoft Exchange 2003 WebDAV and 2010 EWS.

Table A-4 Microsoft Exchange 2003 WebDAV and 2010 EWS For Cisco TelePresence Manager 1.7(x) and Later

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. **Note** CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTS-Manager: 68	Broadcast: 67	Requests an IP address from the DHCP server. **Note** It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTS-Manager: 123	NTP: 123	Synchronizes the hardware clock on the CTS-Manager with an NTP server.
DNS	UDP	CTS-Manager: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-4 Microsoft Exchange 2003 WebDAV and 2010 EWS For Cisco TelePresence Manager 1.7(x) and Later

HTTP	TCP	CTS Primary Codec: Ephemeral CTS-Manager: Ephemeral	CTS-Manager: 8080, 8444 CTS Primary Codec: 8081, 9501	Uses XML/SOAP to coordinate meeting schedule and system operational status with CTS-Manager. • When security is enabled, the CTS uses port 8444 on CTS-Manager and CTS-Manager uses port 9501 on the CTS (recommended). • When security is not enabled, CTS uses port 8080 on CTS-Manager and CTS-Manager uses port 8081 on the CTS.
		CTMS: Ephemeral CTS-Manager: Ephemeral	CTS-Manager: 8080, 8444 CTMS: 8080, 8444	Uses XML/SOAP over HTTP or HTTPs to coordinate meeting schedule and system operational status between CTS-Manager and the CTMS.
		CTS-Manager: Ephemeral	CUCM: 8444	Uses XML/SOAP over HTTPs to the AXL Web Services on Cisco Unified CM to interrogate the Cisco Unified CM database to discover the existence of CTS endpoints.
		ANY: Ephemeral	CTS-Manager: 80,443	Accesses the administrative web interface of CTS-Manager. Port 80 is automatically redirected to port 443.
SSH	TCP	ANY: Ephemeral	CTS-Manager: 22	Accesses the CTS-Manager administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTS-Manager: 161	Receives SNMP queries from a management station.
		CTS-Manager: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
CAPF	TCP	CTS-Manager: Ephemeral	CUCM: 3804	Obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	CTS-Manager: Ephemeral	CUCM: 2444	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List (CTL) Provider service.
JTAPI	TCP	CTS-Manager: Ephemeral	CUCM: 2748, 2749	Uses JTAPI to register with Cisco Unified CM CTI Manager service to receive device event status of CTS endpoints. • When security is enabled, CTS-Manager uses port 2749 on Cisco Unified CM (recommended). • Otherwise, port 2748 is used.
LDAP	TCP	CTS-Manager: Ephemeral	AD: 389,3268,636	Discovers the Microsoft Exchange mailbox name of each CTS endpoint and authenticates users logging into CTS-Manager. • Port 389 is used for single AD server deployments. • If AD deployment uses a Global Catalogue Server, then port 3268 is used. • If AD uses LDAP over Secure Sockets Layer (LDAP/SSL), then port 636 is used (recommended).

Table A-4 Microsoft Exchange 2003 WebDAV and 2010 EWS For Cisco TelePresence Manager 1.7(x) and Later

WebDAV	TCP	CTS-Manager: Ephemeral	Exchange: 80	Subscribes to the Microsoft Exchange mailbox of each Cisco TelePresence endpoint to process meeting requests.
	UDP	Exchange: Ephemeral	CTS-Manager: 3621	Notifies CTS-Manager of any events in the mailboxes to which it is subscribed.
EWS	TCP	CTS-Manager: Ephemeral	Exchange: 80,443	Subscribes to the Microsoft Exchange mailbox of each Cisco TelePresence endpoint to process meeting requests. • If Exchange is setup to support SSL, then port 80 and port 443 are used (recommended). • If Exchange is non-secure, port 80 is used.

Cisco TelePresence Manager for IBM Domino

Table A-5 contains information about Cisco TelePresence Manager 1.7(x) for IBM Domino.

Table A-5 IBM Domino for Cisco TelePresence Manager 1.7(x) and Later

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. **Note** CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTS-Manager: 68	Broadcast: 67	Requests an IP address from the DHCP server. **Note** It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTS-Manager: 123	NTP: 123	Synchronizes the hardware clock on the CTS-Manager with an NTP server.
DNS	UDP	CTS-Manager: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-5 IBM Domino for Cisco TelePresence Manager 1.7(x) and Later (continued)

HTTP	TCP	• CTS Primary Codec: Ephemeral • CTS-Manager: Ephemeral	• CTS-Manager: 8080, 8444 • CTS Primary Codec: 8081, 9501	Uses XML/SOAP to coordinate meeting schedule and system operational status with CTS-Manager. • When security is enabled, the CTS uses port 8444 on CTS-Manager and CTS-Manager uses port 9501 on the CTS (recommended). • When security is not enabled, CTS uses port 8080 on CTS-Manager and CTS-Manager uses port 8081 on the CTS.
		• CTMS: Ephemeral • CTS-Manager: Ephemeral	• CTS-Manager: 8080, 8444 • CTMS: 8080, 8444	
		CTS-Manager: Ephemeral	CUCM: 8444	Uses XML/SOAP to interrogate the Cisco Unified CM database to discover the existence of CTS endpoints.
		ANY: Ephemeral	CTS-Manager: 80,443	Accesses the administrative web interface of CTS-Manager. Port 80 is automatically redirected to port 443.
SSH	TCP	ANY: Ephemeral	CTS-Manager: 22	Accesses the CTS-Manager administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTS-Manager: 161	Receives SNMP queries from a management station.
		CTS-Manager: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
CAPF	TCP	CTS-Manager: Ephemeral	CUCM: 3804	Obtains a Locally Significant Certificate (LSC) from the Cisco Unified CM Certificate Authority Proxy Function (CAPF) service.
CTL	TCP	CTS-Manager: Ephemeral	CUCM: 2444	Downloads the Certificate Trust List (CTL) from the Cisco Unified CM Certificate Trust List Provider service.
JTAPI	TCP	CTS-Manager: Ephemeral	CUCM: 2748, 2749	Uses JTAPI to register with Cisco Unified CM CTI Manager service to receive device event status of CTS endpoints. • When security is enabled, CTS-Manager uses port 2749 on Cisco Unified CM (recommended). • Otherwise, port 2748 is used.
LDAP	TCP	CTS-Manager: Ephemeral	Domino: 389,636	Discovers the Domino mailbox name of each CTS endpoint, and authenticates users logging into CTS-Manager. • If Domino uses LDAP over Secure Sockets Layer (LDAP/SSL), then port 636 is used (recommended). • Otherwise, port 389 is used.

Table A-5 IBM Domino for Cisco TelePresence Manager 1.7(x) and Later (continued)

IIOP	TCP	CTS-Manager: Ephemeral	Domino: 80,443	Negotiates an Internet Inter-ORB Protocol (IIOP) session to the Domino mailbox of each CTS endpoint to process meeting requests. • If Domino is setup to support SSL, then port 443 is used (recommended). • Otherwise, port 80 is used.
	UDP	CTS-Manager: Ephemeral	Domino: 63148	Queries and synchronizes the Domino mailboxes it is subscribed to.

Cisco TelePresence Multipoint Switch (CTMS)

Table A-6 contains information about the Cisco TelePresence Multipoint Switch for Release 1.7(x).

Table A-6 Cisco TelePresence Multipoint Switch – Release 1.7(x)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. **Note** CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTMS: 68	Broadcast: 67	Requests an IP address from the DHCP server. **Note** It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTMS: 123	NTP: 123	Synchronizes the hardware clock on the CTMS with an NTP server.
DNS	UDP	CTMS: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.

Table A-6 Cisco TelePresence Multipoint Switch – Release 1.7(x) (continued)

HTTP	TCP	• CTMS: Ephemeral • CTS-Manager: Ephemeral	• CTS-Manager : 8080, 8444 • CTMS: 8080, 8444	Uses XML/SOAP over HTTP or HTTPs to coordinate meeting schedule and system operational status between CTS-Manager and the CTMS. • When security is enabled, the CTMS uses port 8444 on CTS-Manager and CTS-Manager uses port 8444 on the CTMS (recommended). • When security is not enabled, CTMS uses port 8080 on CTS-Manager, and CTS-Manager uses port 8080 on the CTMS.
		ANY: Ephemeral	CTMS: 80,443	Accessed the CTMS administrative web interface. Port 80 is automatically redirected to port 443.
		CTS Primary Codec: Ephemeral	CTMS: 9501	Uses XML between each CTS and the CTMS for in-meeting controls such as Site/Segment Switching and Meeting Lock/Unlock. This port is the same for both secure and non-secure modes.
SSH	TCP	ANY: Ephemeral	CTMS: 22	Accesses the CTMS administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTMS: 161	Receives SNMP queries from a management station.
		CTMS: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.
SIP	UDP	CTMS: Ephemeral	CUCM: 5060, 5061	Used for call signaling with Cisco Unified CM. • When security is not enabled, use UDP or TCP port 5060. • When security is enabled, use UDP or TCP. **Note** Unlike the CTS endpoints which always initiate the SIP TCP socket to Cisco Unified CM, in the case of CTMS either side can initiate the connection.
		CUCM: Ephemeral	CTMS: 5060, 5061	
	TCP	CTMS: Ephemeral	CUCM: 5060, 5061	
		CUCM: Ephemeral	CTMS: 5060, 5061	
RTP	UDP	CTMS: 16384 – 32768	ANY: ANY	Send and receives audio and video media.

Cisco TelePresence Recording Server (CTRS)

Table A-7 contains information about Cisco TelePresence Recording Server for Release 1.7(X).

Table A-7 Cisco TelePresence Recording Server – Release 1.7(X)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. **Note** CDP is a layer-2 management protocol and hence does not use TCP or UDP.
DHCP	UDP	0.0.0.0: 68 CTRS: 68	Broadcast: 67	Requests an IP address from the DHCP server. It is recommended to use static IP addressing instead of DHCP.
		0.0.0.0: 67 DHCP: 67	Broadcast: 68	Sent by the DHCP server in response to a request for an IP address.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	CTRS: 123	NTP: 123	Synchronizes the hardware clock on the CTRS with an NTP server.
DNS	UDP	CTRS: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
HTTP	TCP	ANY: Ephemeral	CTRS: 80,443	Accesses the CTRS administrative web interface. Port 80 is automatically redirected to port 443.
		• CTRS: Ephemeral • CTS-Manager; Ephemeral	• CTRS: 8080, 8444 • CTS-Manager : 8080, 8444	Uses XML/SOAP over HTTP or HTTPS to maintain a heartbeat with the CTS-Manager, if configured.
SSH	UDP	ANY: Ephemeral	CTRS: 22	Accesses the CTRS administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	CTRS: 161	Receives SNMP queries from a management station.
		CTRS: Ephemeral	SNMP: 162	Sends SNMP traps to a management station.

Table A-7 Cisco TelePresence Recording Server – Release 1.7(X) (continued)

SIP	UDP	CTRS: Ephemeral	CUCM: 5060, 5061	Used for call signaling with Cisco Unified CM: • When security is not enabled, CTRS uses UDP or TCP port 5060. • When security is enabled, CTRS uses UDP or TCP port 5061.
	TCP	CTRS: Ephemeral	CUCM: 5060, 5061	
RTP	UDP	CTRS: 16384 – 32768	ANY: ANY	Sends and receives audio and video media.

Cisco IOS IP Service Level Agreements (IPSLA)

Cisco IOS IP Service Level Agreements (IPSLA) is commonly used prior to the installation of Cisco TelePresence to measure and assess the network path.

Table A-8 lists the specific ports relevant for the IPSLA UDP Jitter probe operation used to conduct Cisco TelePresence Network Path Assessment (NPA) testing. The term “Agent” refers to the router who generates the IPSLA test packets, and “Responder” refers to the router which replies to those requests. “Both” means that either the Agent or the Responder could generate such a packet.

Note Table A-8 provides the ports most commonly used by IPSLA Agent and IPSLA Responder routers. Because IPSLA runs on Cisco IOS, there may be other ports used for communications by those routers.

Table A-8 Cisco IOS IP Service IPSLA Support

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
CDP	N/A	N/A	N/A	Advertises its existence to the upstream Cisco Catalyst Ethernet Switch to which it is attached. **Note** CDP is a layer-2 management protocol and hence does not use TCP or UDP.
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
NTP	UDP	Both: 123	NTP: 123	Synchronizes the hardware clock on the Cisco IOS IPSLA router with an NTP server.
DNS	UDP	Both: Ephemeral	DNS: 53	Resolves hostnames to IP addresses.
SSH	TCP	ANY: Ephemeral	Both: 22	Accesses the Cisco IOS IPSLA router administrative command-line interface (CLI).
SNMP	UDP	ANY: Ephemeral	Both: 161	Receives SNMP queries from a management station.
		Both: Ephemeral	ANY: 162	Sends SNMP traps to a management station.

Table A-8 Cisco IOS IP Service IPSLA Support (continued)

IPSLA	UDP	Agent: Ephemeral	Responder: 1967	Signals a new IPSLA operation between the Agent and the Responder.
RTP	UDP	Agent: Ephemeral	Responder: 16384 – 32768 (configurable)	Sends and receives audio and video media from the Agent to the Responder. The Responder then returns these packets back to the Agent. The specific destination UDP ports can be defined in the IPSLA Agent configuration.

Cisco Media Experience Engine (MXE) 5600

The Cisco Media Experience Engine (MXE) 5600 provides interoperability between Cisco TelePresence and videoconferencing devices. The port assignments listed in Table A-9 are valid for Cisco Media Experience Engine Operating System (Cisco MXE-OS) Release 1.0.(x).

Table A-9 MXE Support for Release 1.0.(x)

Protocol	TCP or UDP	Source Device: Port	Destination Device: Port	Description and Use
ICMP	N/A	ANY: N/A	ANY: N/A	ICMP may sometimes to be used to determine whether a device is reachable (for example, ICMP echo request and response). ICMP unreachables may sometimes be sent by a device to indicate that a device or port is no longer reachable. ICMP time-exceeded may be sent by a device to indicate that the Time to Live (TTL) of a packet was exceeded.
DNS	UDP	MXE: Ephemeral	Server: 53	Used for name resolution.
NTP	UDP	MXE: 123	NTP: 123	Synchronizes the hardware clock on MXE with an NTP server.
SSH	TCP	ANY: Ephemeral	MXE: 22	Accesses MXE administrative command-line interface (CLI).
TELNET	TCP	ANY: Ephemeral	MXE: 23	
SNMP	UDP	ANY: Ephemeral	MXE: 161	Receives SNMP queries from a management station.
		MXE: Ephemeral	MXE: 162	Sends SNMP traps to a management station.
SIP	TCP	CUCM: 5060	MXE: Ephemeral	Used for call signaling with Cisco Unified CM (configurable).
		CUCM: Ephemeral	MXE: 5060	Used for call signaling with Cisco Unified CM (configurable).
RTP	UDP	CTMS: 16384 – 32768	ANY: ANY	Sends and receives audio and video media.