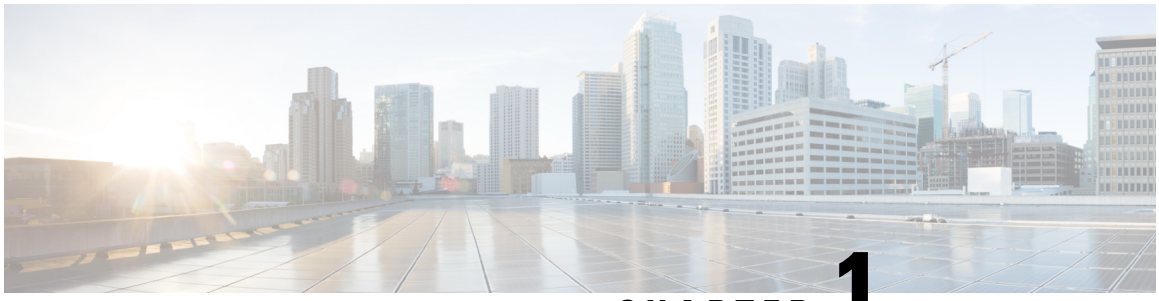
Cisco Expressway IP Port Usage Configuration Guide (X14.0)

First Published: 2021-04-14

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: 408 527-0883



CHAPTER 1

Preface

Change History

Table 1: Cisco Expressway IP Port Usage Configuration Guide Change History

Date	Change	Reason
May 2020	Updated for X12.6	X12.6 Release
April 2020	Correction	Fix entry for Tunneled media in Web Proxy for Meeting Server Port Reference table from port 443 to 3478. Also clarify TLS as transport is the same thing as TCP in context of this guide.
March 2020	Correction	Add missing Webbridge signaling entries to Web Proxy for Meeting Server Port Reference table.
February 2020	Correction	MRA connection for Headset Configuration file fixed to HTTPS/TLS.
December 2019	Update	In the Point to Point Microsoft Interoperability Using Meeting Server diagram, show media paths both with and without Meeting Server load balancing.
July 2019	Update	Updated the MRA Connections for Headset Management.
May 2019	Update	NAT reflection is not needed for Web Proxy for CMS connection (only for standalone Expressways).
February 2019	Update	Added details on how to configure NAT reflection on firewall for Web Proxy for Meeting Server.
January 2019	Updated for X12.5	X12.5 release. ACME certificates, SIP OAuth, and ICE passthrough for MRA.
September 2018	Update	Updated software version from X8.11 to X8.11.1 (version X8.11 withdrawn).

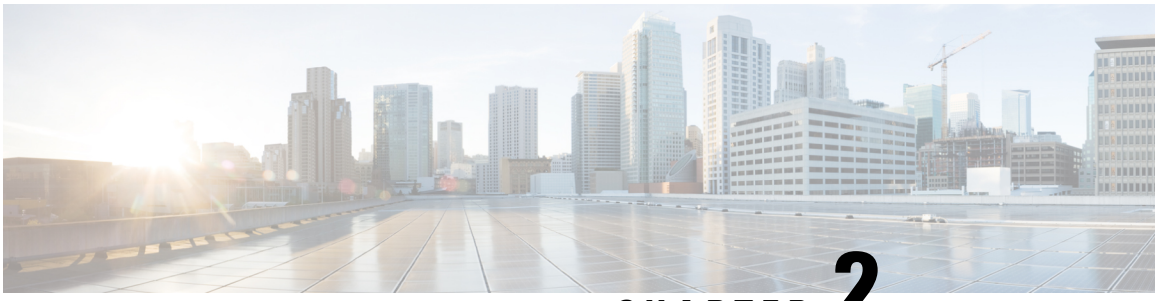
Date	Change	Reason
August 2018	Corrections	Errors in IM&P Federation with Microsoft Clients and Web Proxy for Cisco Meeting Server connections.
July 2018	Updated for X8.11	X8.11 release
April 2018	Corrections	Errors in SIP Edge for CMS media connections.
December 2017	Corrections	For SIP traversal calls, B2BUA on Expressway-C may need to make TURN requests to Expressway-E.
November 2017	Corrections	Errors in Web Proxy media connections.
July 2017	Update	X8.10 release. TURN listening port configurable to 443.
April 2017	New document	New format for information previously held in *Expressway IP Port Usage for Firewall Traversal*.

Related Documentation

Table 2: Links to Related Documents and Videos

Support Videos	Videos provided by Cisco TAC engineers about certain common Expressway configuration procedures are available on the Expressway/VCS Screencast Video List page.
Installation - Virtual Machines	*Cisco Expressway on Virtual Machine Installation Guide* on the Expressway install and upgrade guides page
Installation - Physical Appliances	*Cisco Expressway CE1200 Appliance Installation Guide* on the Expressway install and upgrade guides page
Basic configuration for registrar / single systems	*Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page
Basic configuration for firewall traversal / paired systems	*Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway configuration guides page
Administration and maintenance	*Cisco Expressway Administrator Guide* on the Expressway maintain and operate guides page *Cisco Expressway Serviceability Guide* on the Expressway maintain and operate guides page

Clusters	*Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Expressway configuration guides page
Certificates	*Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page
MRA	*Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page
Cisco Meeting Server	*Cisco Meeting Server with Cisco Expressway Deployment Guide* on the Expressway configuration guides page *Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server programming guides page Other Cisco Meeting Server guides are available on the Cisco Meeting Server configuration guides page
Cisco Webex Hybrid Services	Hybrid services knowledge base
Cisco Hosted Collaboration Solution (HCS)	HCS customer documentation
Microsoft infrastructure	*Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the Expressway configuration guides page *Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on the Expressway configuration guides page
Rest API	*Cisco Expressway REST API Summary Guide* on the Expressway configuration guides page (high-level information only as the API is self-documented)
Multiway Conferencing	*Cisco TelePresence Multiway Deployment Guide* on the Expressway configuration guides page



CHAPTER 2

How To Use This Guide

How To Use This Guide

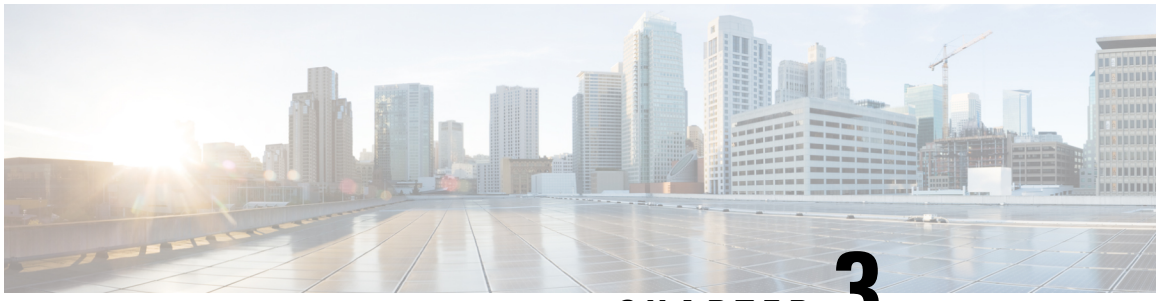
The purpose of this guide is to help you configure and troubleshoot connections between infrastructure components related to Expressway deployments.

There is a section for each of the popular Expressway deployments. Each has a diagram showing the major infrastructure components and the connections between them, and also lists the connections in a table format.

The deployments build on each other where necessary. For example, if you want to implement Mobile and Remote Access (MRA), you first configure a traversal pair. These relationships are described in the relevant deployment guides.

References in the guide to TLS (transport layer security protocol) as transport, in the context of Expressway effectively mean the same thing as the underlying TCP transport protocol on which TLS is built.

How To Use This Guide



CHAPTER 3

Firewall Configuration

Firewall Configuration

Here are some points to keep in mind when you are configuring your firewalls to permit the connections described in this document:

- If you have a cluster of Expressways, ensure that the destination ports to the public IP address of each Expressway peer are open on the external firewall.
- Sometimes there are different connection types that could be used to achieve the same task. You do not need to always open every port shown in the diagrams and tables. We recommend that you close any that you are not using.

  For example, if your web administration port is TCP 7443 but you only ever use SSH to configure the Expressway, you can close 7443 and leave TCP 22 open. Management ports should only be open to connections originating from inside the network.
- Some firewalls actively close connections that appear inactive, which could interfere with the operation of your video infrastructure.

  For example, TCP port 1720 is used for H.323 call signaling but may be inactive during the call. If this is prematurely closed by the firewall, the H.323 endpoint could interpret that as a dropped call and respond by tearing down the call.

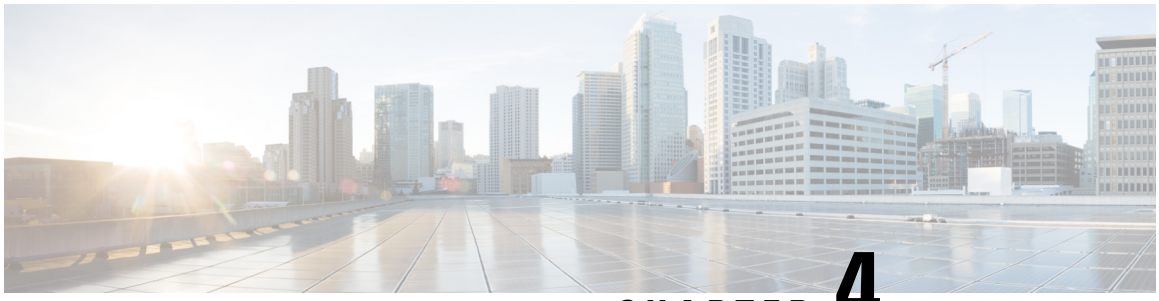
  We recommend extending inactivity timeouts on the known ports to at least two hours, particularly if you are seeing calls fail after a specific duration.
- Firewalls that contain ALG (Application Layer Gateway) for SIP / H.323 protocols may not work as expected with Expressway-E.

  We strongly recommend that you disable SIP or H.323 ALG inspection / awareness on the NAT firewall. We may not be able to support your configuration if you cannot make this change.

  We recommend that you disable UDP inspection on the NAT firewall to avoild media issues.
- In some deployments, media packets can hairpin on the Expressway-E external NIC. Some firewalls cannot allow for hairpinning, and mistrust packets that are destined to their own source.

  We recommend configuring an exception to allow hairpinning on the Expressway-E public interface, if your deployment requires it.

- If you want to use the static NAT feature of Expressway-E, we strongly recommend using two NICs. Dedicating one NIC to the external interface and the other to the internal interface is much better for your network than using one NIC with the static NAT enabled.



CHAPTER 4

Default Port Ranges

Default Port Changes

The following defaults are used throughout this document. Default port ranges may occasionally change (if unavoidable) as new features are developed. Our documents list the current default ports for the given version number.

Note In some cases throughout this document we list port ranges used by third party infrastructure. These are default values and we cannot guarantee that these are correct for your environment. We recommend you follow the supplier's documentation to configure those connections.

Table 3: Default Port Ranges on Expressway

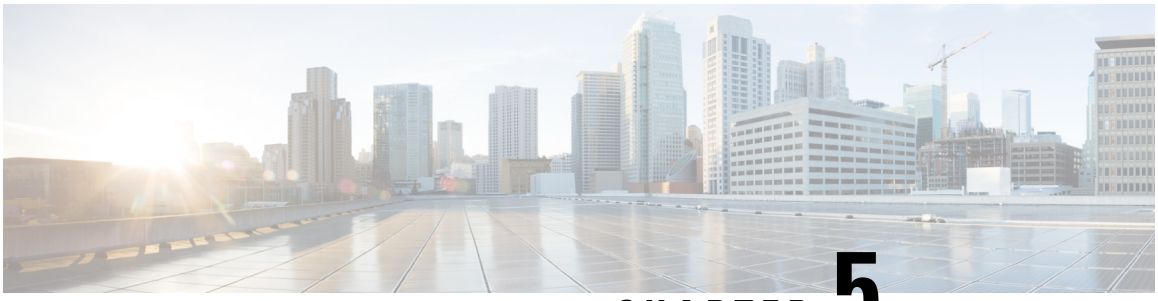
Protocol	Purpose	Current Range	Details
TCP	Ephemeral ports	1024-65535	Outbound HTTP/S, LDAP
UDP	Ephemeral ports	1024-65535	DNS, outbound TURN requests
TCP	Ephemeral ports	30000-35999	
UDP	Ephemeral ports	30000-35999	
TCP	Outbound SIP	25000-29999	
UDP&TCP	Inbound TURN requests on Small/Medium Expressway-E	3478	On Expressway-E only. Configurable to 443 or any port >= 1024

Protocol	Purpose	Current Range	Details
UDP&TCP	Inbound TURN requests on Large Expressway-E	3478-3483	On Large Expressway-E only. Configurable to a six port range with first port >=1024. Configurable to a single port, if port multiplexing is enabled. For more information on TURN port multiplexing, see the Expressway Administrator Guide
TCP	Inbound TCP TURN request on Cisco Expressway-E	443	On Expressway-E only if TCP 443 TURN service is enabled.
UDP	TURN relays	24000-29999	On Expressway-E only.
UDP	RTP/RTCP media	36000-59999	The range is configurable within the default bounds. E.g., 37000-38200, but not 35000-36200. On S/M Expressway, the first two ports can be used for multiplexed media if you do not use default/custom ports. On L Expressway, the first twelve ports of the range are used for multiplexed media. You cannot customize that subrange.

Protocol	Purpose	Current Range	Details
UDP	Multiplexed media on Small/Medium Expressway-E systems	2776/2777 OR 36000/36001	2776/2777 is older pair but kept as default by the ability to customize when the new default range was introduced with S/M system options. Custom pair is defined on **Configuration** > **Traversal** > **Ports**. On Expressway-E only. **Note** In the connection maps and port references we do not show all the port options for the sake of clarity. For example, if the diagram shows 2776/2777, but you have chosen to use 36000/36001 instead, then you don't need to also open 2776/2777.

Protocol	Purpose	Current Range	Details
UDP	Multiplexed media on Large Expressway-E systems	36000-36011	New range introduced with Large system option. This range is always the first twelve ports of the RTP/RTCP media range, so it will be different if you configure a different media range. On Expressway-E Large OVAs or large scale appliances only. **Note** In the connection maps and port references we do not show all the port options for the sake of clarity. For example, if the diagram shows 2776/2777, but you have a large Expressway, then you should open the first twelve ports of the media range instead of 2776/2777.
TCP	SIP traversal	7001	Configurable. SIP listening port on the first Expressway-E traversal server zone. Subsequent traversal server zones will use incremental port numbers, eg. 7002, by default.

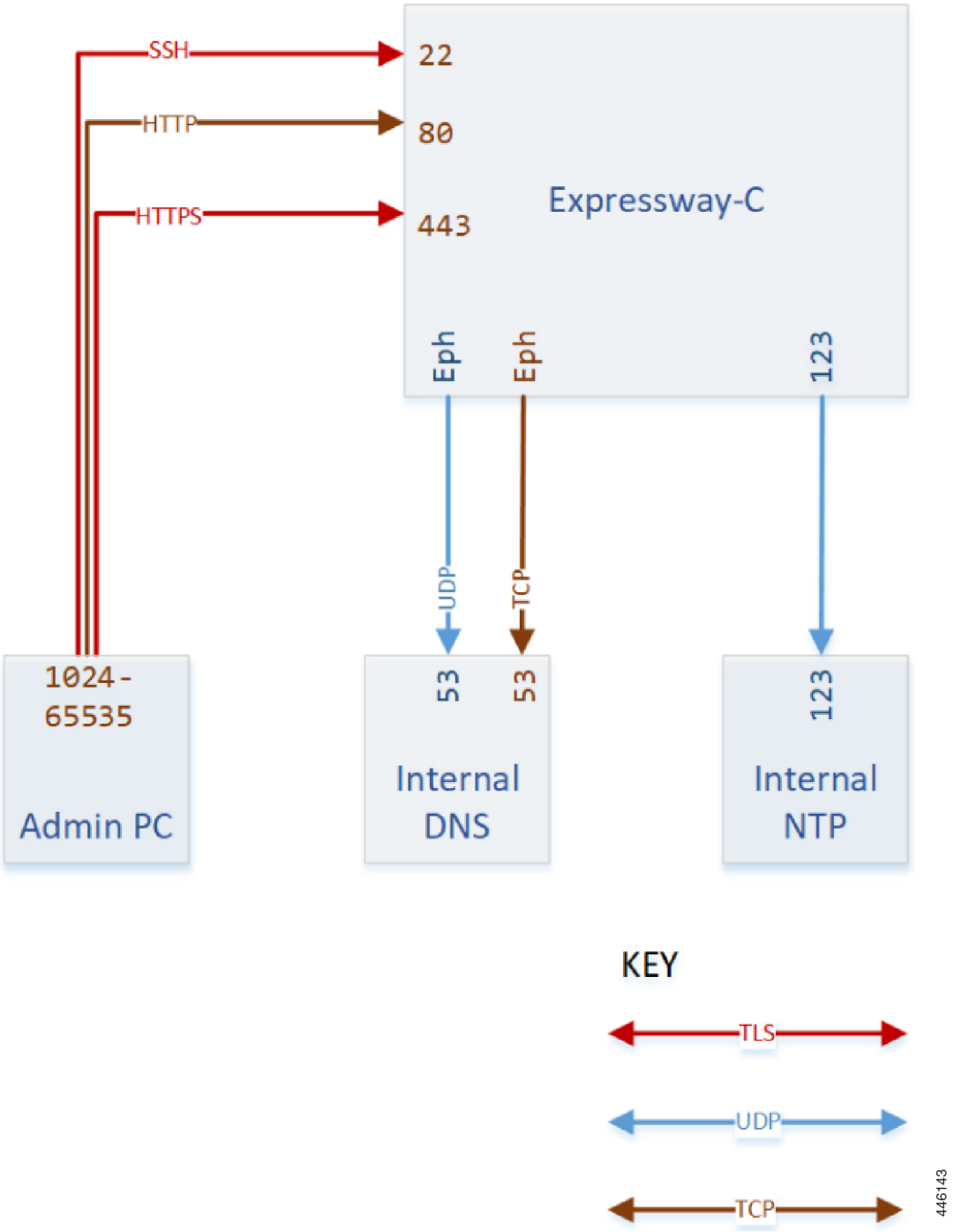
Protocol	Purpose	Current Range	Details
UDP	H.323 traversal	6001	Configurable. H.323 listening port on the first Expressway-E traversal server zone. Subsequent traversal server zones will use incremental port numbers, eg. 6002, by default.



CHAPTER 5

Basic Networking Connections

Basic Networking - Expressway



Networking Port Reference - Expressway

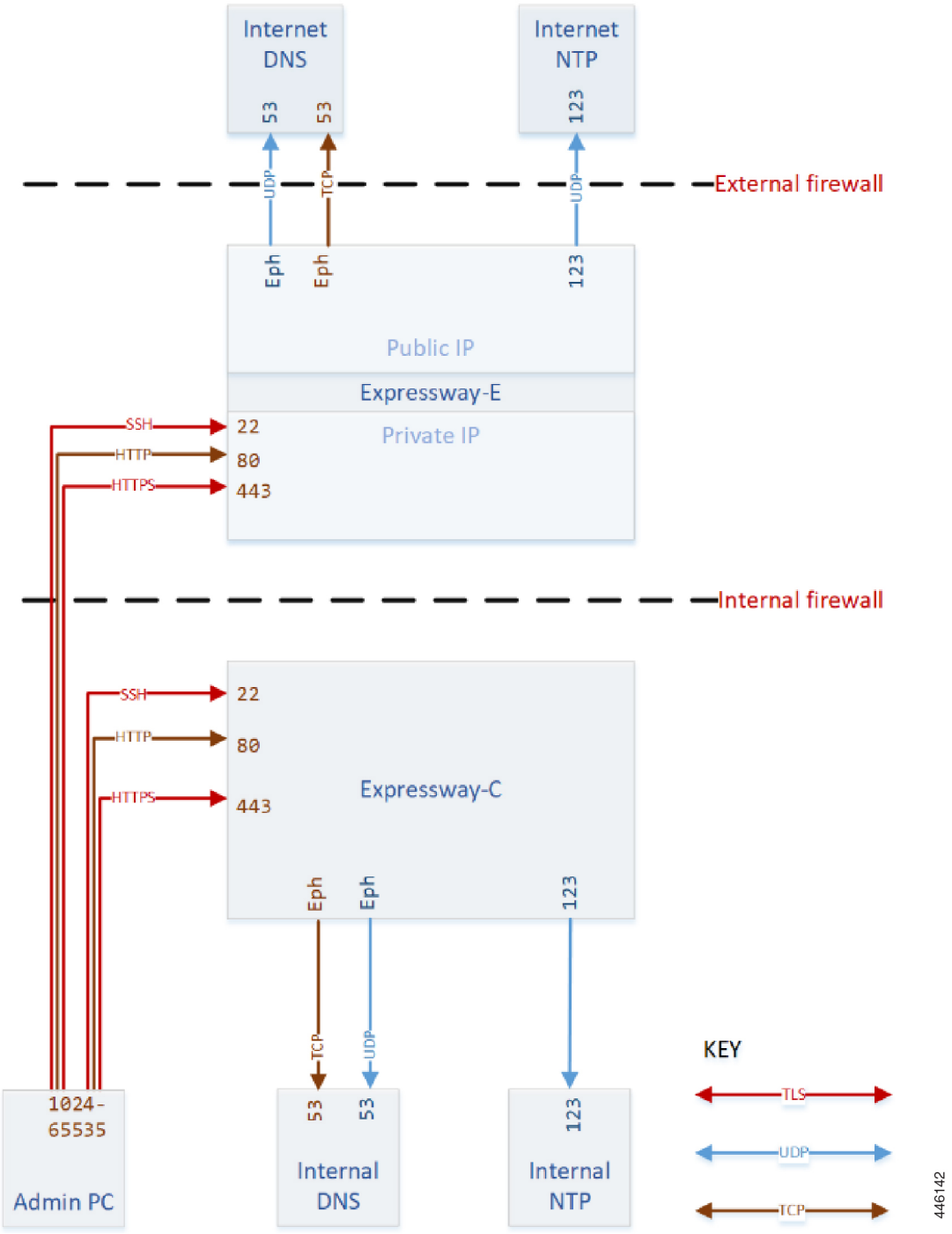
Table 4: Basic Networking Ports for Expressway-C

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Administrator SSH	Admin PCs	1024-65535	TCP	Expressway-C	22
Administrator HTTP*	Admin PCs	1024-65535	TCP	Expressway-C	80
Administrator HTTPS	Admin PCs	1024-65535	TCP	Expressway-C	443
Name resolution (DNS)	Expressway-C	30000-35999	UDP & TCP†	Internal name server	53
Time synchronization (NTP)	Expressway-C	123	UDP	Internal time server	123

* Expressway redirects HTTP to HTTPS by default. You don't need to open the HTTP port, but you can allow HTTP for convenience and redirect to HTTPS.

† Expressway will attempt DNS resolution over TCP if the response is too large.

Basic Networking - Traversal Pair



Networking Port Reference - Expressway Traversal Pair

Table 5: Basic Networking Ports for Expressway-C

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Administrator SSH	Admin PCs	1024-65535	TCP	Expressway-C	22
Administrator HTTP*	Admin PCs	1024-65535	TCP	Expressway-C	80
Administrator HTTPS	Admin PCs	1024-65535	TCP	Expressway-C	443
Name resolution (DNS)	Expressway-C	30000-35999	UDP & TCP †	Internal name server	53
Time synchronization (NTP)	Expressway-C	123	UDP	Internal time server	123

* Expressway redirects HTTP to HTTPS by default. You don't need to open the HTTP port, but you can allow HTTP for convenience and redirect to HTTPS.

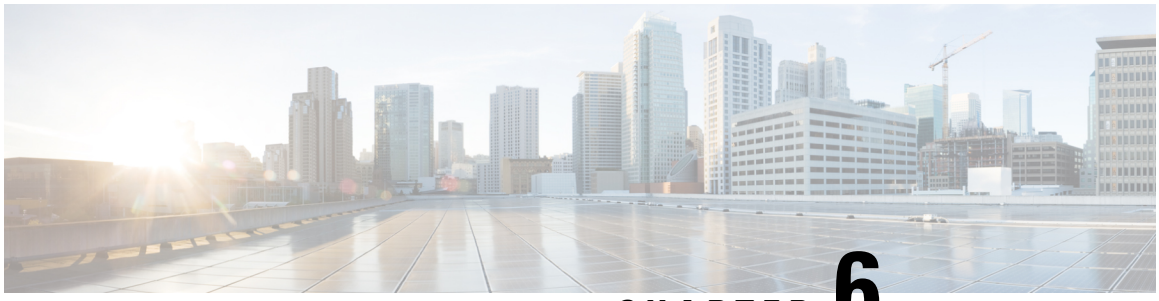
† Expressway will attempt DNS resolution over TCP if the response is too large.

Table 6: Basic Networking Ports for Expressway-E

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Administrator SSH	Admin PCs	1024-65535	TCP	Expressway-E private IP	22
Administrator HTTP	Admin PCs	1024-65535	TCP	Expressway-E private IP	80
Administrator HTTPS	Admin PCs	1024-65535	TLS	Expressway-E private IP	443
Internal name resolution (DNS)*	Expressway-E private IP	30000-35999	UDP & TCP	Internal name server	53
External name resolution (DNS)	Expressway-E public IP	30000-35999	UDP & TCP	External name server	53
Internal time synchronization (NTP)*	Expressway-E private IP	123	UDP	Internal time server	123

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
External time synchronization (NTP)	Expressway-E public IP	123	UDP	External time server	123

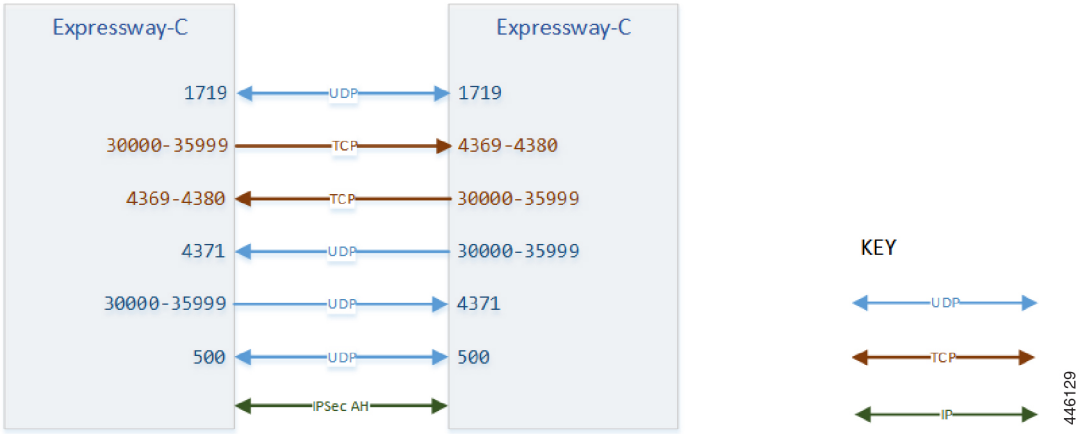
* You may prefer to connect Expressway-E to external DNS and NTP. You do not need both.



CHAPTER 6

Clustering Connections

Cluster Connections Before X8.8



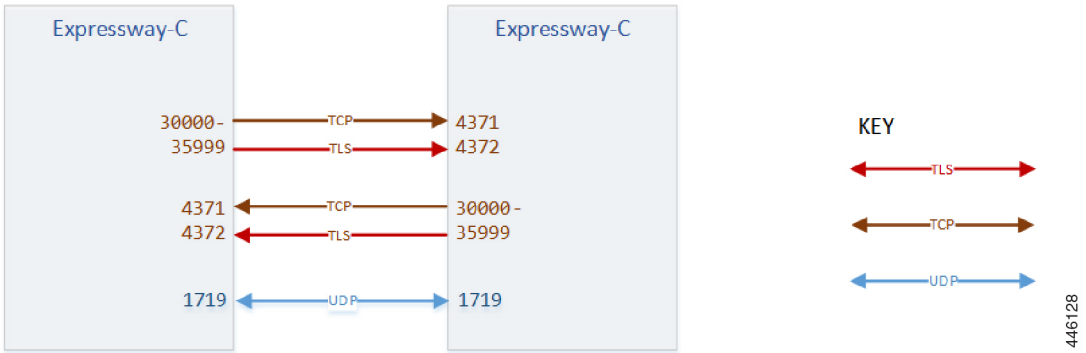
Cluster Port Reference Before X8.8

Table 7: Cluster Synchronization and Communications

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Cluster database synchronization (IPSec AH)	This peer	N/A	51	Other peers	N/A

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Key exchange between peers (ISAKMP)	This peer	500	UDP	Other peers	500
Cluster recovery	This peer	30000-35999	UDP	Other peers	4371
Cluster communication	This peer	30000-35999	TCP	Other peers	4369-4380
Bandwidth management (Expressway-C cluster only)	This peer	1719	UDP	Other peers	1719

Cluster Connections X8.8 Onwards



Cluster Port Reference X8.8 Onwards

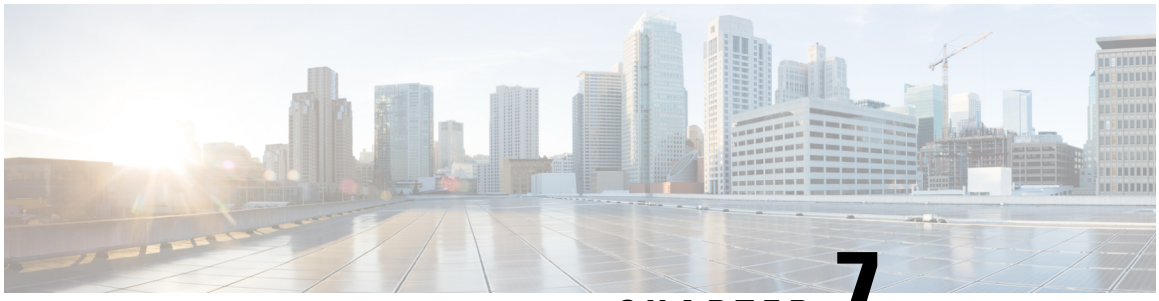
Table 8: Expressway-C Cluster Database Synchronization and Communications

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Cluster recovery	This peer	30000-35999	TCP	Other peers	4371
Cluster communication	This peer	30000-35999	TLS	Other peers	4372
Bandwidth management	This peer	1719	UDP	Other peers	1719

Table 9: SIP Calls Routed Between Peers (not shown on diagram)

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
SIP TCP Signaling	This peer	25000-29999	TCP	Other peers	5061
SIP TLS Signaling	This peer	25000-29999	TLS	Other peers	5061
RTP/RTCP	This peer	36000-59999	UDP	Other peers	36000-59999
Bandwidth management	This peer	1719	UDP	Other peers	1719

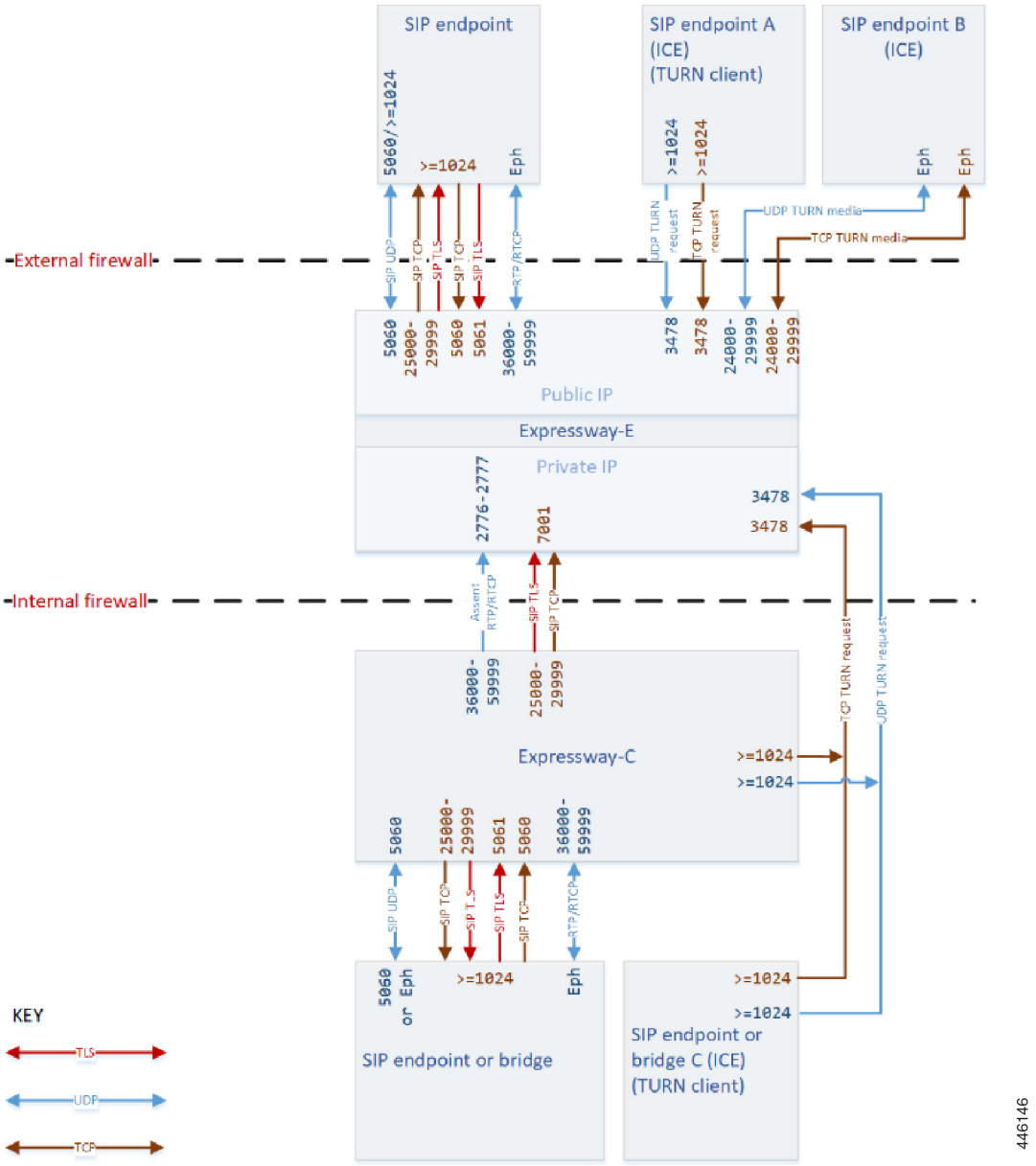
Note Dbxsh is a python script that connects to a cluster database on the local loopback address over port 4370. The Dbxsh does not need to authenticate the database before executing the commands. The port is open for connection and is strictly for internal use only. This is accessible from root only.



CHAPTER 7

Provisioning Registrations Authentication and Calls

SIP Calls


SIP endpoint
SIP endpoint A (ICE) (TURN client)
SIP endpoint B (ICE)
5060/>=1024
>=1024
Eph
>=1024
>=1024
Eph
Eph
UDP TURN media
TCP TURN media
External firewall
SIP UDP
SIP TCP
SIP TLS
SIP TCP
SIP TLS
RTP/RTCP
UDP TURN request
TCP TURN request
5060
25000-29999
5060
5061
36000-59999
3478
3478
24000-29999
24000-29999
Public IP
Expressway-E
Private IP
2776-2777
7001
3478
3478
Internal firewall
Assent
RTP/RTCP
SIP TLS
SIP TCP
36000-59999
25000-29999
Expressway-C
>=1024
>=1024
TCP TURN request
UDP TURN request
5060
25000-29999
5061
5060
36000-59999
SIP UDP
SIP TCP
SIP TLS
SIP TCP
RTP/RTCP
5060 or Eph
>=1024
Eph
>=1024
>=1024
SIP endpoint or bridge
SIP endpoint or bridge C (ICE) (TURN client)
KEY
TLS
UDP
TCP
446146

SIP Calls Port Reference

Table 10: SIP Calls Port Reference

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
SIP signaling	Expressway-C	25000-29999	TCP or TLS	Expressway-E	7001 (for first traversal zone; 7002 for second etc.)
SIP signaling	Expressway-C	5060	UDP	SIP endpoint	5060 (often, but could be different, >=1024) Port number defined by registration (if registered) or by DNS lookup
SIP signaling	Expressway-C	25000-29999	TCP or TLS	SIP endpoint	>=1024 Port number defined by registration (if registered) or by DNS lookup
SIP signaling	Expressway-E	25000-29999	TCP or TLS	SIP endpoint (or its firewall)	>=1024 Port number defined by registration (if registered) or by DNS lookup
SIP signaling	SIP endpoint (or its firewall)	>=1024	UDP	Expressway-E	5060 SIP UDP disabled by default. Not recommended for internet facing connections.

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
SIP signaling	SIP endpoint (or its firewall)	>=1024	TCP	Expressway-E	5060 SIP TCP disabled by default (X8.9.2 and later).
SIP signaling	SIP endpoint (or its firewall)	>=1024	TLS	Expressway-E	5061
SIP signaling	SIP endpoint (or its firewall)	>=1024	MTLS	Expressway-E	5062
Assent RTP (traversed media)	Expressway-C	36000-59999	UDP	Expressway-E	2776 or 36000 (Small/Medium) 36000 - 36010 (even ports) (Large)
Assent RTCP (traversed media)	Expressway-C	36000-59999	UDP	Expressway-E	2777 or 36001 (Small/Medium) 36001 - 36011 (odd ports) (Large)
Assent RTP (traversed media)	SIP endpoint (or its firewall)	>=1024 Could be the firewall port where the media egressed, rather than an endpoint port	UDP	Expressway-E	36000-59999
Assent RTCP (traversed media)	SIP endpoint (or its firewall)	>=1024 Could be translated by the firewall to port where the media egressed, rather than an endpoint port	UDP	Expressway-E	36000-59999

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Assent RTP (traversed media)	Expressway-E	36000-59999	UDP	SIP endpoint (or its firewall)	>=1024 Expressway waits until it receives media, then sends media to that source port (which could be the port where the media egressed the firewall, not an endpoint port)
TURN control	Any IP address†	>=1024 (signaling port from endpoint or the firewall)	UDP & TCP	Expressway-E	3478 (Small/Medium) 3478-3483 (Large)
TURN control	Expressway-C	>=1024	UDP & TCP	Expressway-E	3478 (Small/Medium) 3478-3483 (Large)
TURN media	Expressway-E	24000-29999	UDP & TCP	Any IP address	>=1024
TURN media	Any IP address‡	>=1024 Port of relevant ICE candidate: host IP port, server reflexive port (outside firewall port), or TURN server port	UDP & TCP	Expressway-E	24000-29999

† The request could be from any IP address, unknown to the TURN server. Assume for example, that endpoint A and endpoint C (TURN clients) can use the Expressway-E TURN server. The actual IP address from which the TURN server receives the request could be the endpoint's firewall egress address (NATed).

‡ The media could go to any of the candidate addresses. For example, before ICE negotiation the TURN server does not know which of endpoint B's candidate addresses will be the highest priority.

H.323 Calls

H.323 Calls Port Reference

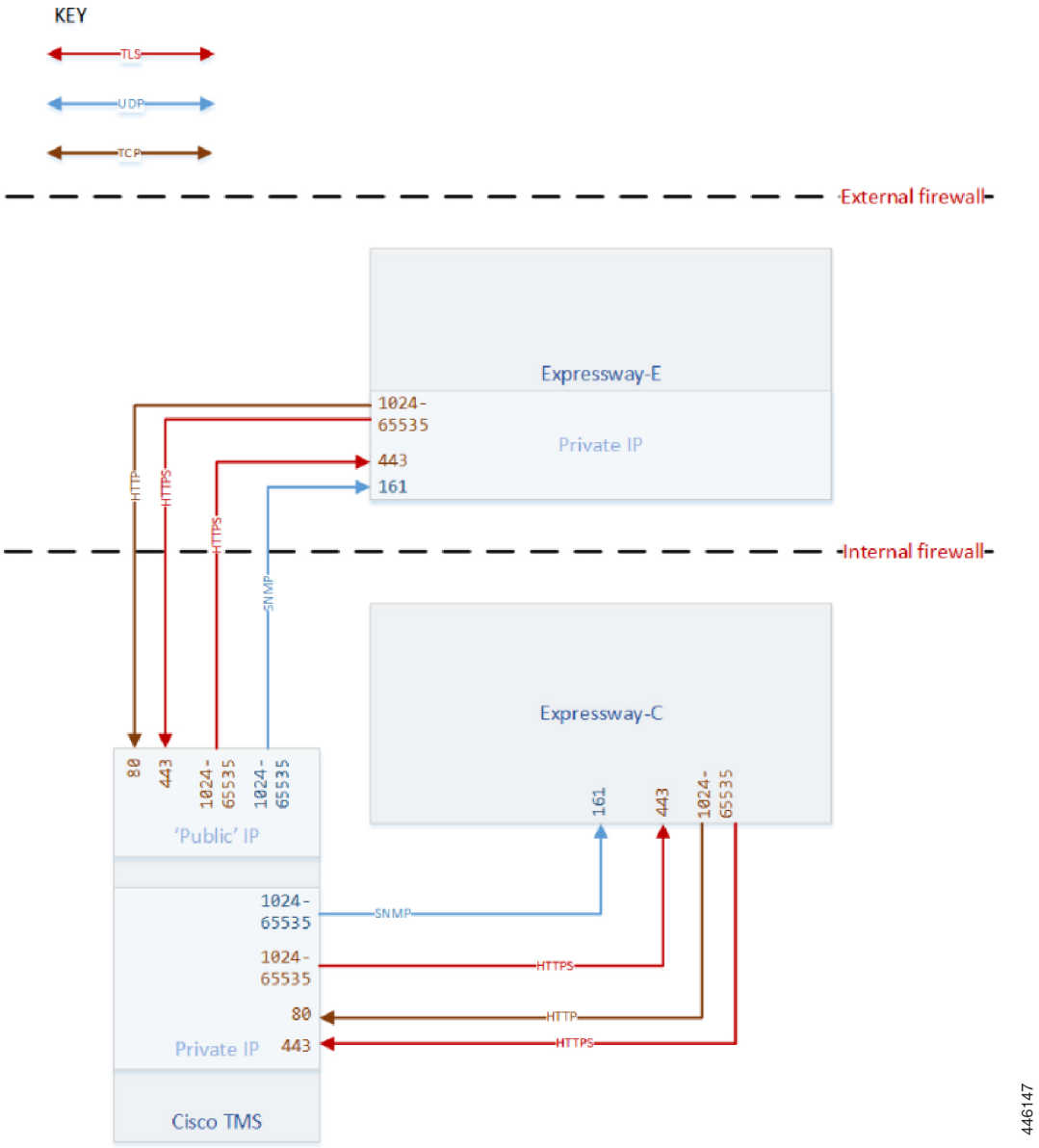
Table 11: H.323 Ports Reference

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Initial RAS connection	Registered endpoint in the Internet	1719	UDP	Expressway-E (public)	1719
Initial RAS connection	Expressway-E (public)	1719	UDP	Registered endpoint in the Internet	1719
Initial RAS connection	External address of firewall protecting off-premises endpoint	>=1024	UDP	Expressway-E (public)	1719
Initial RAS connection	Expressway-C	1719	UDP	Expressway-E (private)	6001 (for first traversal zone, 6002 for second etc.)
Q.931 / H.225 signaling	Any (endpoint in the Internet)	1720	TCP	Expressway-E (public)	1720
Q.931 / H.225 signaling	External address of firewall protecting off-premises Assent endpoint	>=1024	TCP	Expressway-E (public)	2776
Q.931 / H.225 signaling	External address of firewall protecting off-premises H.460.18/19 endpoint	>=1024	TCP	Expressway-E (public)	1720
Q.931 / H.225 signaling	Expressway-E (public)	15000-19999	TCP	Any (endpoint in the Internet)	1720 (endpoint signaling port, specified during registration. Could be another port >=1024)
Q.931 / H.225 signaling	Expressway-C	15000-19999	TCP	Expressway-E (private)	2776 (Assent calls)

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Q.931 / H.225 signaling	Expressway-C	15000-19999	TCP	Expressway-E (private)	1720 (H.460.18 calls)
H.245	Expressway-C	15000-19999	TCP	Expressway-E (private)	2776 (Assent calls)
H.245	Expressway-C	15000-19999	TCP	Expressway-E (private)	2777 (H.460.18 calls)
H.245	Any (endpoint in the Internet)	>=1024	TCP	Expressway-E (public)	15000-19999
H.245	Expressway-E (public)	15000-19999	TCP	Any (endpoint in the Internet)	>=1024 (endpoint H.245 signaling port)
H.245	External address of firewall protecting off-premises Assent endpoint	>=1024	TCP	Expressway-E (public)	2776
H.245	External address of firewall protecting off-premises H.460.18/19 endpoint	>=1024	TCP	Expressway-E (public)	2777
RTP (multiplexed traversal media)	Expressway-C	36000-59998 (even ports)	UDP	Expressway-E (private)	2776 (Small/Medium) or 36000-36010 (even ports) (Large)
RTCP (multiplexed traversal media)	Expressway-C	36001-59999 (odd ports)	UDP	Expressway-E (private)	2777 (Small/Medium) or 36001-36011 (odd ports) (Large)
RTP (non-multiplexed traversal media)	Expressway-C	36000-59998 (even ports)	UDP	Expressway-E (private)	36000-59998 (even ports)
RTCP (non-multiplexed traversal media)	Expressway-C	36001-59999 (odd ports)	UDP	Expressway-E (private)	36001-59999 (odd ports)

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
RTP (non-multiplexed)	Expressway-E (public)	36000-59998 (even ports)	UDP	Any (endpoint in the Internet)	>=1024 (endpoint media range)
RTCP (non-multiplexed)	Expressway-E (public)	36001-59999 (odd ports)	UDP	Any (endpoint in the Internet)	>=1024 (endpoint media range)
RTP (non-multiplexed)	Any (endpoint in the Internet)	>=1024 (endpoint media range)	UDP	Expressway-E (public)	36000-59998 (even ports)
RTCP (non-multiplexed)	Any (endpoint in the Internet)	>=1024 (endpoint media range)	UDP	Expressway-E (public)	36001-59999 (odd ports)
RTP (multiplexed traversal media)	External address of firewall protecting off-premises H.460 endpoint (multiplexed media)	>=1024	UDP	Expressway-E (public)	2776 (Small/Medium) or 36000-36010 (even ports) (Large)
RTCP (multiplexed traversal media)	External address of firewall protecting off-premises H.460 endpoint (multiplexed media)	>=1024	UDP	Expressway-E (public)	2777 (Small/Medium) or 36001-36011 (odd ports) (Large)
RTP (multiplexed traversal media)	External address of firewall protecting off-premises H.460 endpoint (non-multiplexed media)	>=1024	UDP	Expressway-E (public)	36000-59998 (even ports)
RTCP (multiplexed traversal media)	External address of firewall protecting off-premises H.460 endpoint (non-multiplexed media)	>=1024	UDP	Expressway-E (public)	36001-59999 (odd ports)

TMS Connections



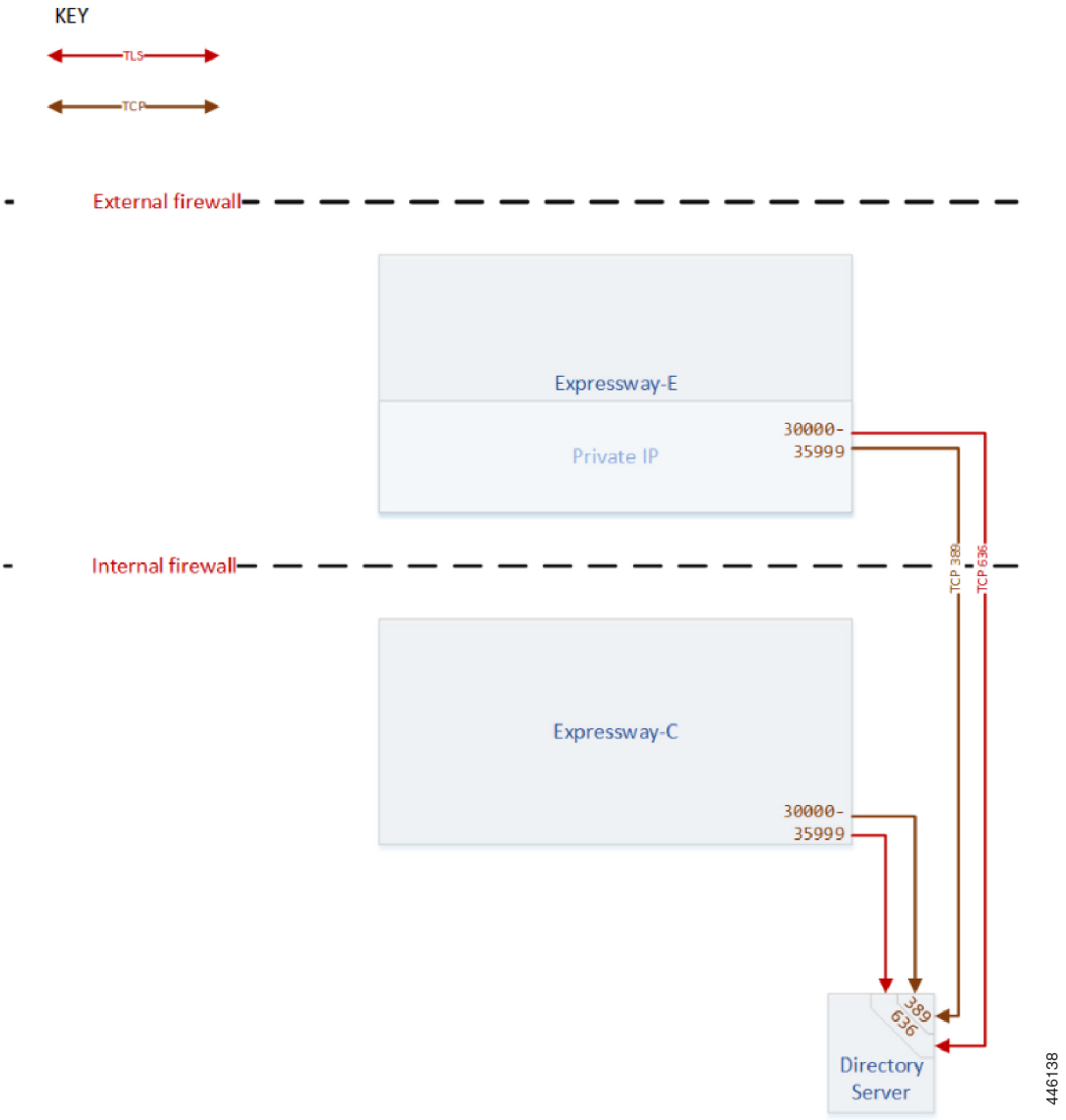
TMS Port Reference

Cisco TMS can have two IP addresses; for managing public systems, or managing systems on the LAN. On Cisco TMS, go to **Administrative Tools** > **Configuration** > **Network Settings** > **Advanced Network Settings**. You should use the TMS public address with the Expressway-E, and the default LAN address with the Expressway-C.

Table 12: TMS Port Reference

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
SNMP for discovery of Expressway-E	Cisco TMS External IP	1024-65535	UDP	Expressway-E private	161
SNMP for discovery of Expressway-C	Cisco TMS	1024-65535	UDP	Expressway-C	161
HTTP Management of Expressway-E	Cisco TMS External IP	1024-65535	TCP	Expressway-E private IP	80
HTTP Management of Expressway-C	Cisco TMS	1024-65535	TCP	Expressway-E private IP	80
HTTPS Management of Expressway-E	Cisco TMS External IP	1024-65535	TCP	Expressway-E private	443
HTTPS Management of Expressway-C	Cisco TMS	1024-65535	TCP	Expressway-C	443
Feedback events (HTTP)	Expressway-E private	1024-65535	TCP	Cisco TMS External IP	80
Feedback events (HTTP)	Expressway-C	1024-65535	TCP	Cisco TMS	80
Feedback events (HTTPS)	Expressway-E private	1024-65535	TCP	Cisco TMS External IP	443
Feedback events (HTTPS)	Expressway-C	1024-65535	TCP	Cisco TMS	443

LDAP Connections

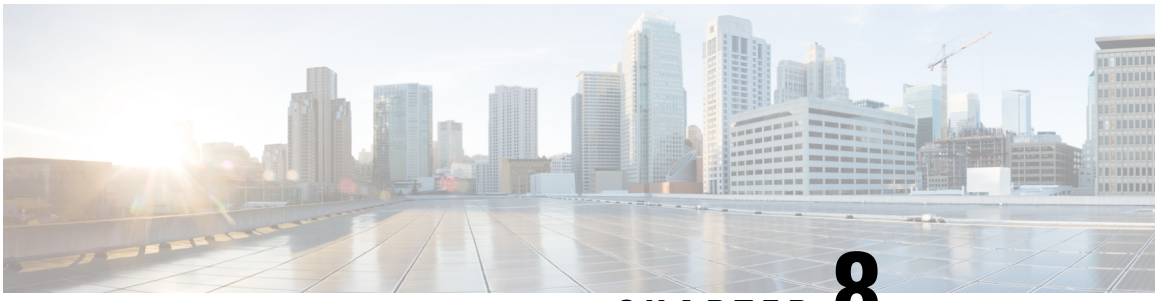


LDAP Port Reference

You can choose to use an LDAP server to authenticate and authorize administrator or user logins. You would only need to allow the LDAP ports inbound from the Expressway-E in the rare case where you want a user to log in from outside the network and you also do not allow credentials to be stored on the Expressway.

Table 13: LDAP Port Reference

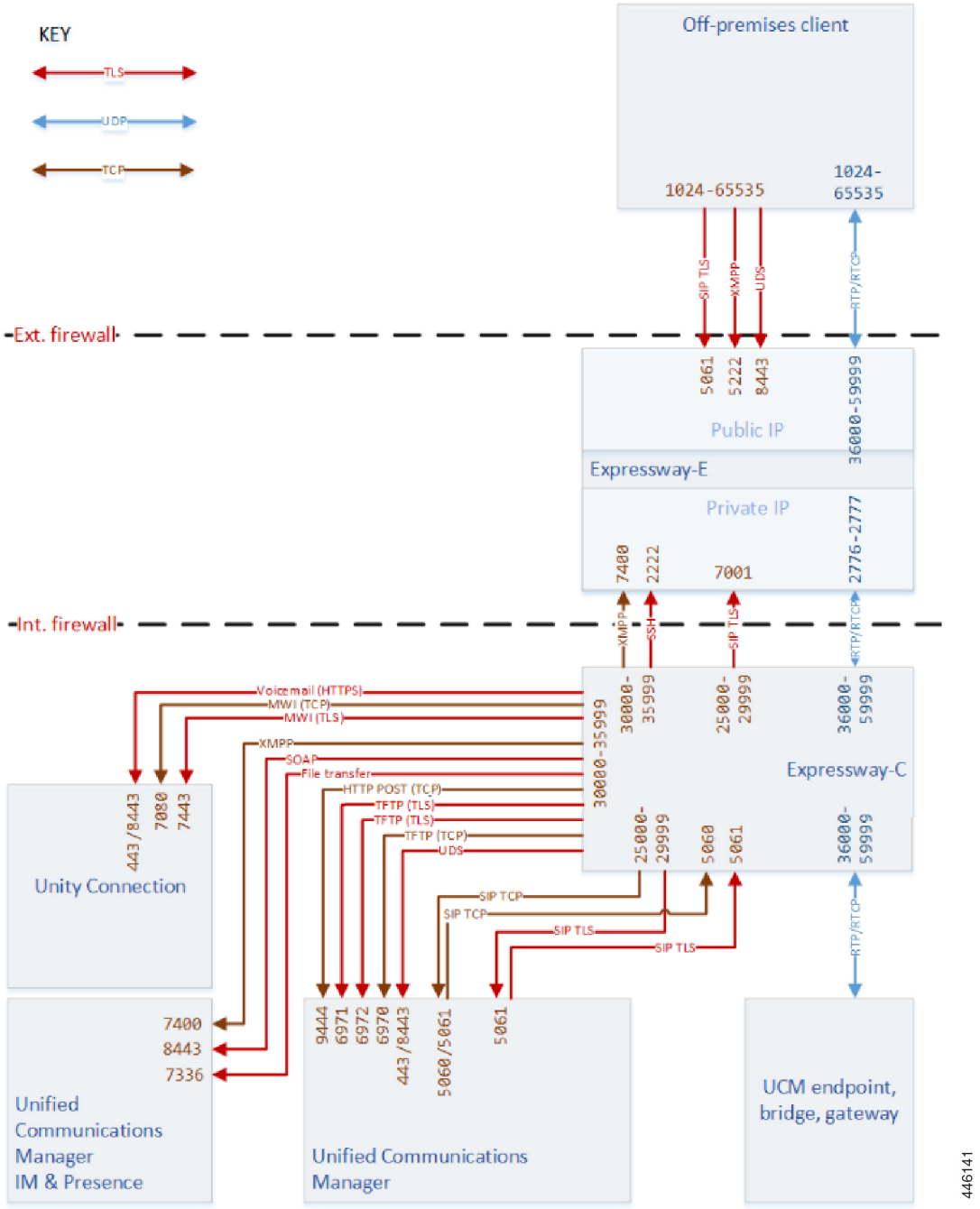
Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Authentication requests from the Expressway-C	Expressway-C	1024-65535	TCP	Directory Server	389
Authentication requests from the Expressway-E	Expressway-E private	1024-65535	TCP	Directory Server	389
Encrypted authentication requests from the Expressway-C	Expressway-C	1024-65535	TLS	Directory Server	636
Encrypted authentication requests from the Expressway-E	Expressway-E private	1024-65535	TLS	Directory Server	636



CHAPTER 8

Mobile and Remote Access

MRA Connections



MRA Port Reference

Table 14: ICE Passthrough Connections Between Off-premises Endpoints

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
RTP/RTCP (ICE passthrough media)†	Off-premises endpoint	Eph	UDP	Off-premises endpoint	Eph

† ICE passthrough calls are supported only between off-premises endpoints. Not supported between off-premises and on-premises endpoints.

Table 15: Connections Between Off-premises Endpoints and the Expressway-E

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
UDS (phonebook and provisioning)	Off-premises endpoint	1024-65535	TLS	Expressway-E Public IP	8443
SIP signaling	Off-premises endpoint	1024-65535	TLS	Expressway-E Public IP	5061
RTP/RTCP media	Off-premises endpoint	1024-65535	UDP	Expressway-E Public IP	36000-59999
RTP/RTCP media	Expressway-E Public IP	36000-59999	UDP	Off-premises endpoint	1024-65535
XMPP (IM and Presence)	Off-premises endpoint	1024-65535	TCP	Expressway-E Public IP	5222
TURN control (ICE passthrough)	Any IP address†	>=1024 (signaling port from endpoint or the firewall)	UDP	Expressway-E	3478 (Small/Medium) 3478-3483 (Large)
TURN media (ICE passthrough)	Any IP address‡	>=1024 Port of relevant ICE candidate: host IP port, server reflexive port (outside firewall port), or TURN server port	UDP	Expressway-E	24000-29999

† The request could be from any IP address, unknown to the TURN server. For example, assume that endpoint A and endpoint B (TURN clients) can use the Expressway-E TURN server. The actual IP address from which the TURN server receives the request could be the endpoint's firewall egress address (NATed).

‡ The media could go to any of the candidate addresses. For example, before ICE passthrough negotiation the TURN server does not know which of endpoint B's candidate addresses will be the highest priority.

Table 16: Connections Between Expressway-C and Expressway-E

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
SSH tunnels	Expressway-C	30000-35999	TLS	Expressway-E Private IP	2222
SIP signaling	Expressway-C	25000-29999	TLS	Expressway-E Private IP	7001
SIP media	Expressway-C	36000-59999	UDP	Expressway-E Private IP	2776/7 or 36000-11
XMPP (IM and Presence)	Expressway-C	30000-35999	TCP	Expressway-E Private IP	7400
TURN control	Expressway-C	>=1024	UDP & TCP	Expressway-E	3478 (Small/Medium) 3478-3483 (Large)

Table 17: Connections Between Expressway-C and On-premises Infrastructure

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
SIP signaling (TCP)	Expressway-C	25000-29999	TCP	Unified CM	5060†
SIP signaling (TCP)	Unified CM	Ephemeral	TCP	Expressway-C	5060
SIP signaling (TLS)	Expressway-C	25000-29999	TLS	Unified CM	5061*
SIP signaling (TLS)	Unified CM	Ephemeral	TLS	Expressway-C	5061
SIP signaling (OAuth)	Expressway-C	25000-29999	TLS	Unified CM	5091
SIP signaling (OAuth)	Unified CM	5091	TLS	Expressway-C	5061

Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
HTTP Configuration file download (TFTP) (Pre 11.x Jabber and pre 11.x Unified CM)	Expressway-C	30000-35999	TCP	Unified CM Node	6970
HTTPS Headset Configuration file download (TFTP)	Expressway-C	30000-35999	TLS	Unified CM	6971
HTTPS Configuration file download (TFTP) (11.x or later Jabber and 11.x or later Unified CM)	Expressway-C	30000-35999	TLS	Unified CM Node	6972
HTTP for UDS (User Data Services) and AXL (Administrative XML Layer)	Expressway-C	30000-35999	TLS	Unified CM Node	443 or 8443
XMPP (IM and Presence)	Expressway-C	30000-35999	TLS	IM and Presence Service Node	7400
HTTPS SOAP (IM and Presence)	Expressway-C	30000-35999	TLS	IM and Presence Service Node	8443
File transfer (IM and Presence)	Expressway-C	30000-35999	TLS	IM and Presence Service Node	7336
HTTPS to visual voicemail	Expressway-C	30000-35999	TLS	Cisco Unity Connection	443 or 8443
MWI (Message Waiting Indicator)	Expressway-C	30000-35999	TCP	Cisco Unity Connection	7080
MWI (Message Waiting Indicator)	Expressway-C	30000-35999	TLS	Cisco Unity Connection	7443

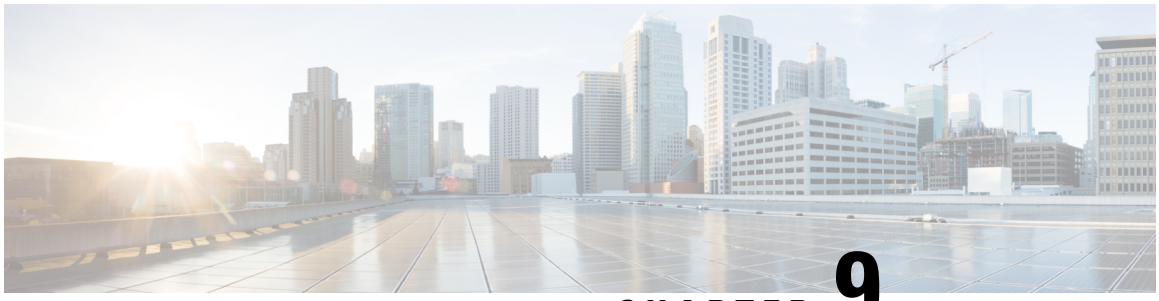
Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
HTTP for metrics POST (Headset Management)	Expressway-C	30000-35999	TCP	Unified CM	9444
Audio Video Media (RTP/RTCP)	Expressway-C	36000-59999	UDP	On-prem media destination	Destination media's range eg, 16384-32767 (DX Series)

† Unified CM can listen on 5061 for TCP SIP but we discourage it.

* If you have MRA connections to the Unified CM which are line-side connections to 5060/5061, avoid using 5060/5061 as the listening port for any SIP trunks you create on that Unified CM.

Table 18: Connections from Expressway-E to the Cloud

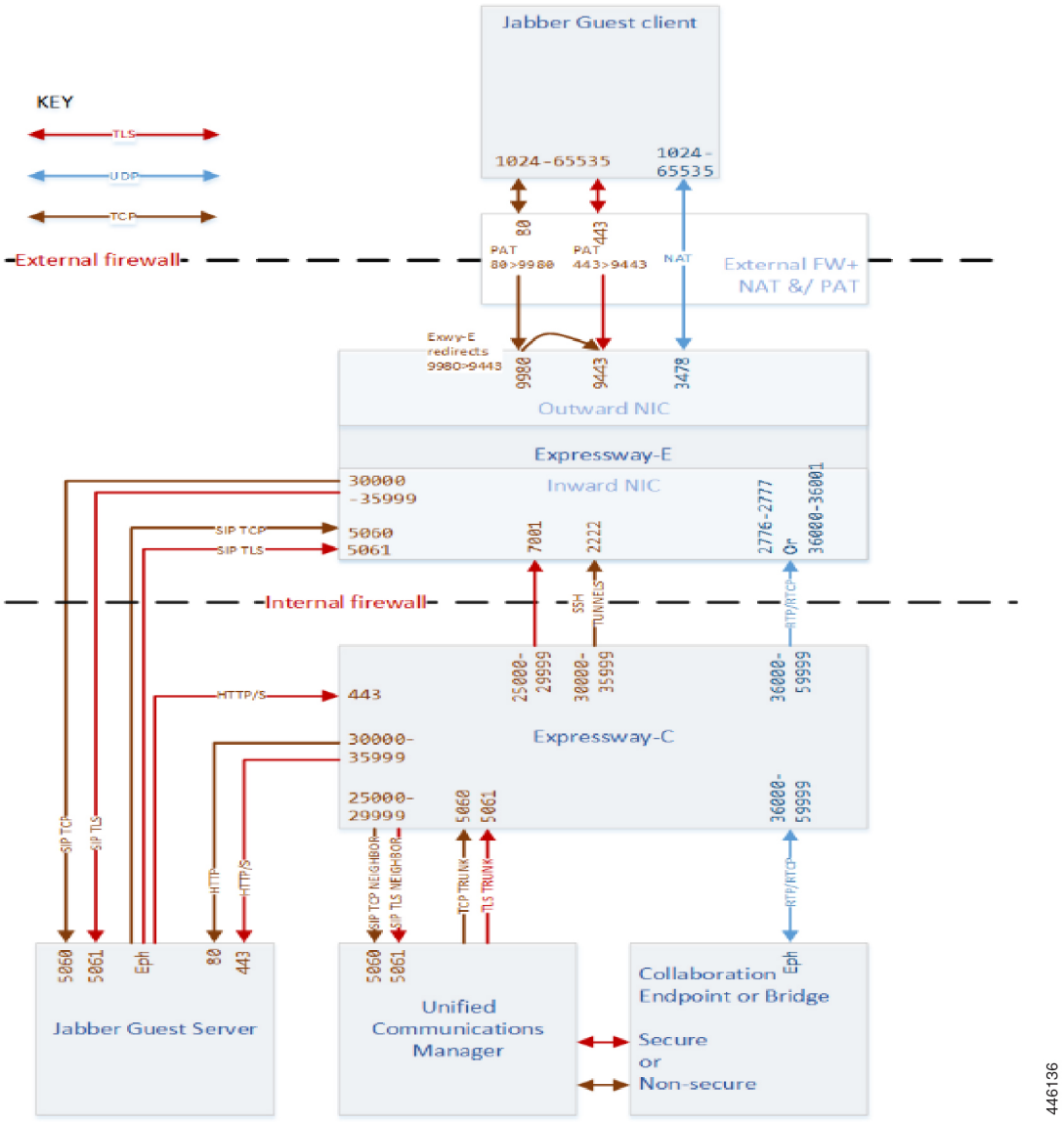
Purpose	Src. IP	Src. Ports	Protocol	Dest. IP	Dest. Ports
Subscription requests originating from Unified CM	Expressway-E	Ephemeral (30000- 35999)	TLS	fos-a.wbx2.com (onboarding service)	443
Authentication requests originating from Unified CM or IM and Presence Service	Expressway-E	Ephemeral (30000- 35999)	TLS	idbroker.webex.com (Common Identity Service)	443
Smart Licensing requests originating from Expressway-E	Expressway-E	Ephemeral (30000- 35999)	TLS	https://smartreceiver.cisco.com/licservice/license	443



CHAPTER 9

Jabber Guest Services

Jabber Guest - Dual NIC Deployment



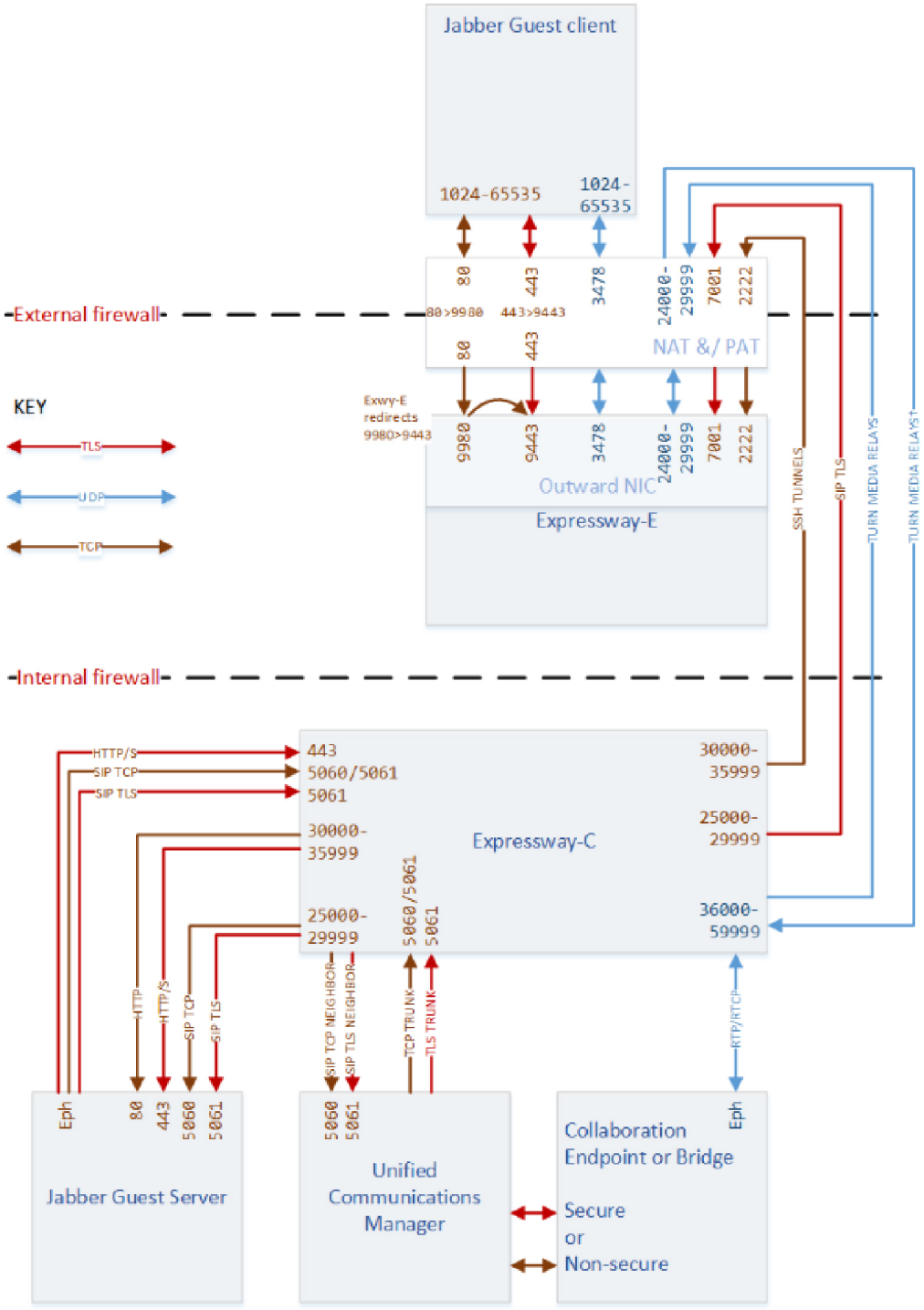
Jabber Guest - Dual NIC Deployment Ports

Table 19: Port Reference for Jabber Guest Dual NIC Deployment

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Jabber Guest Client Signaling (HTTP always redirected to HTTPS)	Any (web browser)	1024-65535	TCP	Expressway-E Public IP	80
Jabber Guest Client Secure Signaling (HTTPS)	Any (web browser)	1024-65535	TLS	Expressway-E Public IP	443
To avoid port conflicts, traffic to Expressway-E public:80 must NAT&PAT to private:9980. HTTP is always redirected to HTTPS.			TLS	Expressway-E Private IP (Outward NIC)	9980 #1
To avoid port conflicts, traffic to Expressway-E public:443 must NAT&PAT to private:9443			TLS	Expressway-E Private IP (Outward NIC)	9443 #2
Jabber Guest Client Media (TURN)	Any (web browser	1024-65535	UDP	Expressway-E Public IP	3478 (S/M systems) 3478-3483 (L systems)*3
SIP TCP signaling	Expressway-E private IP	30000-35999	TCP	Jabber Guest Server	5060
SIP TLS signaling	Expressway-E private IP	30000-35999	TLS	Jabber Guest Server	5061
SIP TCP signaling	Jabber Guest Server	Eph	TCP	Expressway-E private IP	5060
SIP TLS signaling	Jabber Guest Server	Eph	TLS	Expressway-E private IP	5061
Multiplexed media traversal	Expressway-C	36000-59999	UDP	Expressway-E Inward NIC	2776-2777 or 36000-36001

1 Port translation required
2 Port translation required
3 On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483. On Large systems, you can configure a single port for TURN requests, if port multiplexing is enabled. For more information on TURN port muliplexing, see the (missing or bad snippet)

Jabber Guest - Single NIC Deployment



Jabber Guest - Single NIC Deployment Ports

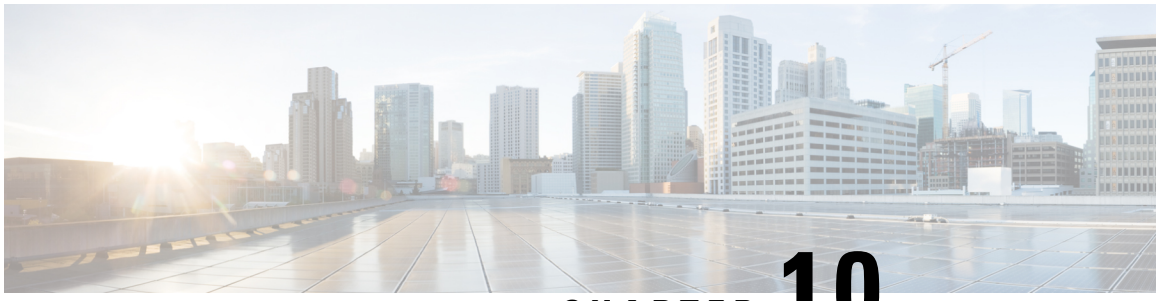
Table 20: Port Reference for Jabber Guest Single NIC Deployment

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Jabber Guest Client Media (TURN)	Any	1024-65535	UDP	Expressway-E Public IP	3478 (S/M systems) 3478-3483 (L systems)*4
Jabber Guest Client Signaling (HTTP always redirected to HTTPS)	Any	1024-65535	TCP	Expressway-E Public IP	80
Jabber Guest Client Secure Signaling (HTTPS)	Any	1024-65535	TLS	Expressway-E Public IP	443
To avoid port conflicts, traffic to Expressway-E public:80 must NAT&PAT to private:9980. HTTP is always redirected to HTTPS.			TLS	Expressway-E Private IP	9980 #5
To avoid port conflicts, traffic to Expressway-Epublic:443 must NAT&PAT to private:9443			TLS	Expressway-E Private IP	9443 #6
SSH Tunnels from Expressway-C to Expressway-E	Expressway-C	35000-35999	TCP	Expressway-E Public IP	2222
SIP Signaling	Expressway-C	25000-25999	TLS	Expressway-E Public IP	7001
TURN media relays	Expressway-C	36000-59999	UDP	Expressway-E Public IP	24000-29999
TURN media relays**7	Expressway-E Public IP	24000-29999	UDP	Expressway-C	36000-59999
SIP TCP signaling	Expressway-C	30000-35999	TCP	Jabber Guest Server	5060
SIP TLS signaling	Expressway-C	30000-35999	TLS	Jabber Guest Server	5061
SIP TCP signaling	Jabber Guest Server	Eph	TCP	Expressway-C	5060

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
SIP TLS signaling	Jabber Guest Server	Eph	TLS	Expressway-C	5061

[4] On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.
[5] Port translation in external firewall
[6] Port translation in external firewall
[7] Inbound media ports only required for unidirectional media initiated from Jabber Guest client, eg. BFCP. Otherwise it is enough to allow the outbound media range from Expressway-C to Expressway-E (previous row).

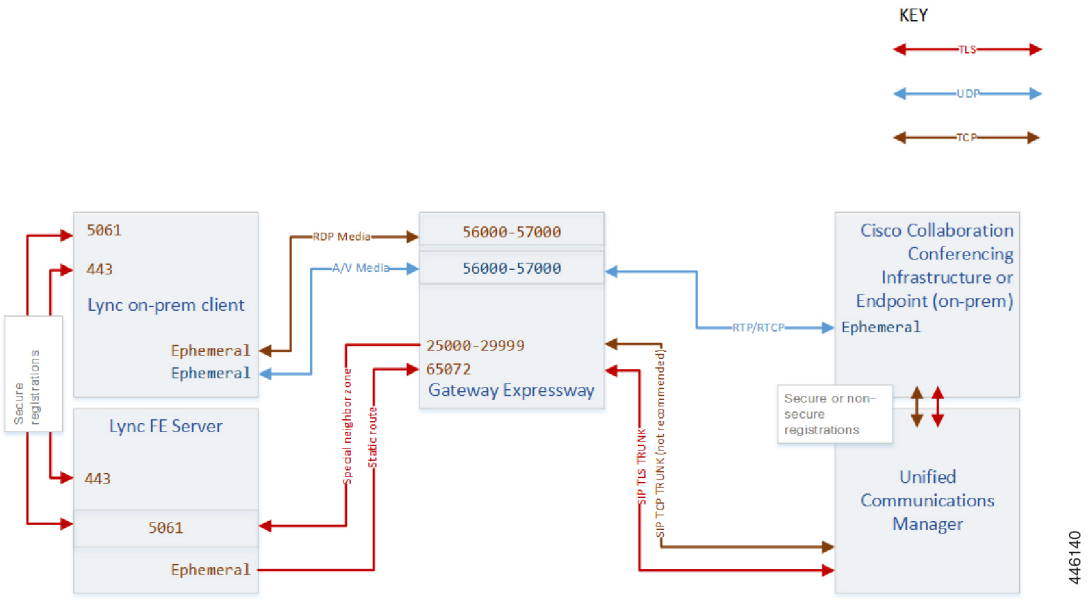
Note If you are using single NIC deployments, the communication between core and edge must use NAT reflection, while the destination IP from core to edge would be the Public.



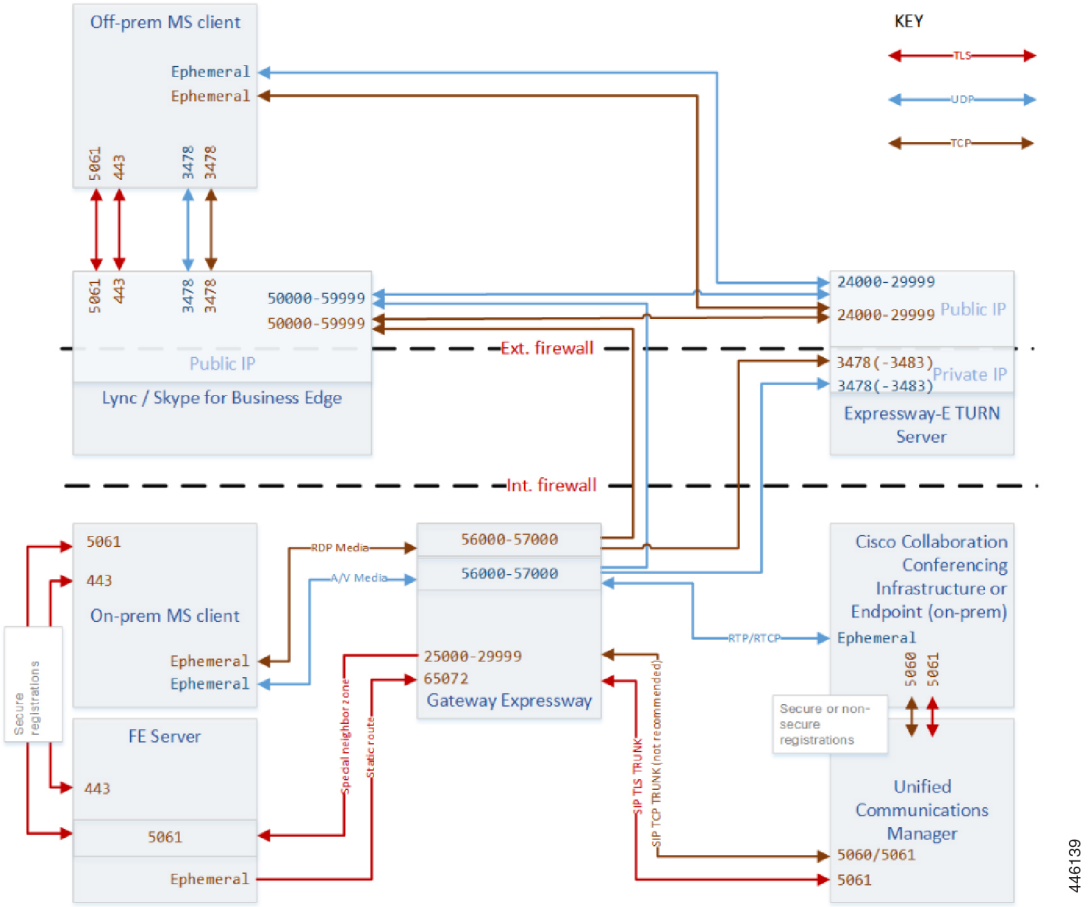
CHAPTER 10

Microsoft Interoperability Using Gateway Expressway

On-Premises Microsoft Clients



Off-Premises Microsoft Clients



Expressway with Microsoft Infrastructure Port Reference

About the deployment connections and ports

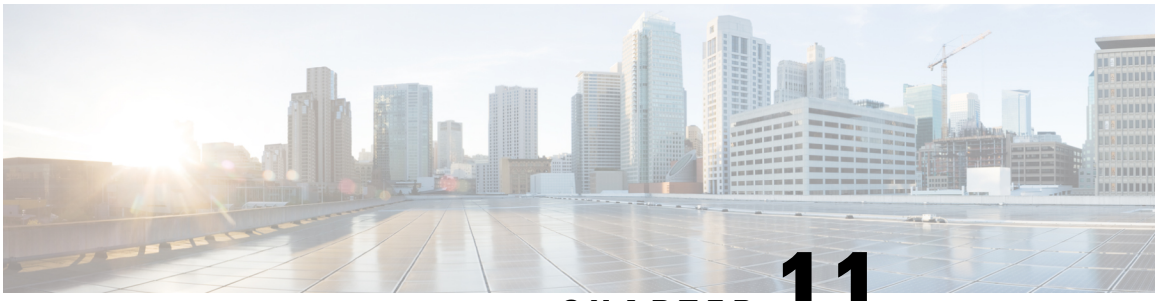
- Trunk connections between Microsoft infrastructure elements not shown.
- Media/signaling connections required for Microsoft client to client calls not shown.
- Microsoft port ranges may vary from those shown here; check the Microsoft documentation to determine the port ranges defined for your infrastructure.
- Cisco Unified Communications Manager and collaboration endpoint connections not shown (for clarity). You can see an example of those on MRA Connections, on page 40.

- Multiple media paths are possible because there are two TURN servers in the DMZ. "Any" source IP address is listed because ICE negotiation could mean the media path uses a relay address provided by one of the TURN servers, or a reflexive address from the egress side of a firewall/NAT.
- The Microsoft Interoperability service on the gateway Expressway has a shared pool of media ports (default 56000-57000). The service can use any port in the range for media connection on either TCP or UDP transport.
- The drawing shows two IP addresses on the Expressway-E because you may have one or two NICs enabled on the Expressway-E. The address you enter for the TURN server (on the Microsoft interoperability configuration of the gateway Expressway) is the one that should listen on 3478 (TCP and UDP).

Table 21: SIP Signaling Port Reference

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
SIP signaling to Lync environment	Gateway Expressway	25000-29999	TLS	Lync FE Server	5061
SIP signaling from Lync environment	Lync FE Server	Ephemeral ports (1024-65535)	TLS	Gateway Expressway: MS interop B2BUA	65072
SIP signaling	Microsoft client	5061	MTLS	Microsoft Edge	5061
SIP signaling	Microsoft Edge	5061	MTLS	Microsoft client	5061
SIP/TLS & TCP TURN	Microsoft client	443	TLS	Microsoft Edge	443
SIP/TLS & TCP TURN	Microsoft Edge	443	TLS	Microsoft client	443
STUN	Microsoft client	3478	UDP	Microsoft Edge	3478
STUN	Microsoft Edge	3478	UDP	Microsoft client	3478
AV media to on-prem Lync clients	Gateway Expressway	56000-57000	UDP	Lync clients	Lync client media ports
Screen sharing from on-prem Lync clients	Lync client	443	TCP	Gateway Expressway	56000-57000

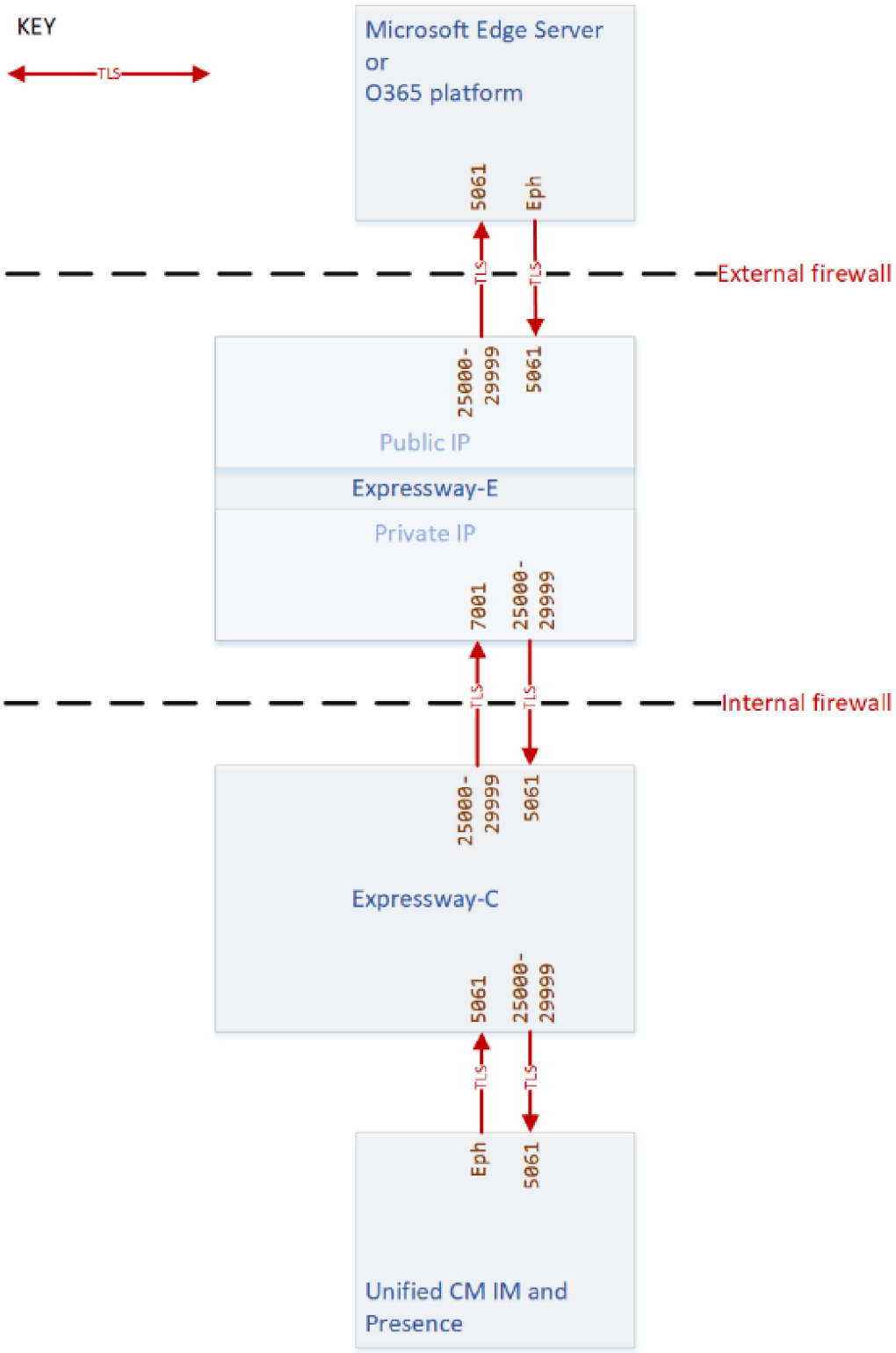
Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Media from Microsoft interoperability B2BUA towards on-premises Cisco collaboration recipients	Gateway Expressway	56000-57000	UDP	Deployment dependent; bridge, endpoint, or a SIP proxy	Endpoint media ports
ICE negotiation and TURN requests from Gateway Expressway to Expressway-E TURN server	Gateway Expressway	56000-57000	UDP or TCP	Expressway-E TURN server	UDP 3478 TCP 3478 (3478-3483 on large systems)
UDP TURN media relays	Expressway-E TURN server	24000-29999	UDP	Any (reflexive or relay) from MS client or Edge	50000-59999 (Edge range) or client media ports
TCP TURN media relays	Expressway-E TURN server	24000-29999	TCP	Any (reflexive or relay) from MS client or Edge	50000-59999 (Edge range) or client media ports



CHAPTER 11

IMP Federation with Microsoft Clients

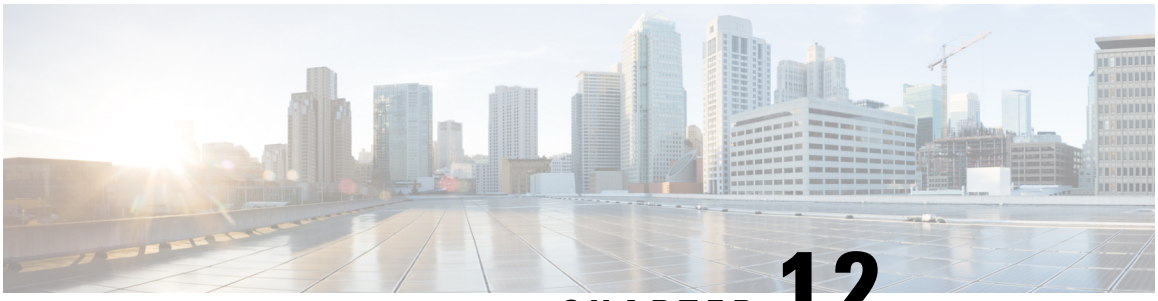
IM and Presence Service Federation with Microsoft Connections


KEY
TLS
Microsoft Edge Server
or
O365 platform
5061
Eph
TLS
TLS
External firewall
25000-
29999
5061
Public IP
Expressway-E
Private IP
7001
25000-
29999
TLS
TLS
Internal firewall
25000-
29999
5061
Expressway-C
5061
25000-
29999
TLS
TLS
Eph
5061
Unified CM IM and
Presence
446135

IM and Presence Federation with Microsoft Clients Port Reference

Table 22: IM and Presence Service Federation with Microsoft Infrastructure

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Expressway-E listens for inbound Microsoft SIP IM&P	Any (Microsoft infrastructure for federated domain)	1024-65535	TLS	Expressway-E public	5061
Expressway-C listens for inbound Microsoft SIP IM&P	Expressway-E private	25000-29999	TLS	Expressway-C	5061
IM and Presence Service listens for inbound Microsoft SIP IM&P	Expressway-C	25000-29999	TLS	IM and Presence Service publisher	5061
Expressway-C listens for outbound Microsoft SIP IM&P	IM and Presence Service publisher	1024-65535	TLS	Expressway-C	5061
Expressway-E listens for outbound Microsoft SIP IM&P	Expressway-C	25000-29999	TLS	Expressway-E private	7001 (for first traversal zone; 7002 for second etc.)
Microsoft infrastructure listens for inbound Microsoft SIP IM&P	Expressway-E	25000-29999	TLS	Any (Microsoft infrastructure for federated domain)	5061



CHAPTER 12

Cisco Meeting Server

Web Proxy for Cisco Meeting Server Connections

Web Proxy for Cisco Meeting Server Port Reference

Table 23: Web Proxy for Meeting Server

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
CMA Web client signaling	Guest PCs	1024-65535	TLS	Expressway-E public IP	443 [18]
Tunneled media	CMA Cisco Meeting WebRTC App	1024-65535	UDP	Expressway-E public IP	3478 (and TCP override port if configured)
Web interface access	Administrator PCs	1024-65535	TLS	Expressway-E IP	NOT 443 [29] 8443 [310]
SSH tunnels for firewall traversal	Expressway-C	30000-35999	TCP	Expressway-E private IP	2222
SIP signaling	Expressway-C	25000-29999	TCP or TLS	Expressway-E	7001 (for first traversal zone; 7002 for second etc.)
CMA Cisco Meeting WebRTC App TURN requests	Any IP	1024-65535	UDP	Expressway-E TURN server public IP	3478
CMA Cisco Meeting WebRTC App TURN requests (TCP fallback)	Any IP	1024-65535	TCP	Expressway-E TURN server public IP	3478 [411]
Webbridge signaling (HTTPS)	Expressway-C	30000-35999	HTTPS	Meeting Server	443
Webbridge signaling (HTTPS)	Meeting Server	>=1024	HTTPS	Expressway-C	30000-35999
TURN client requests	Meeting Server	1024-65535	UDP	Expressway-E TURN server private IP	3478

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
TURN relays [5][12]	Original Source: Expressway-E Private IP Translated Source: Expressway-E Public IP	24000- 29999	UDP and TCP	Original Destination: Expressway-E Public IP Translated Destination: Expressway-E Private IP	24000-29999
TURN relay (On premises)	Expressway-E Private IP	24000- 29999	UDP and TCP	Expressway-E Private IP	24000-29999
TURN relays [6][13]	Meeting Server	Ephemeral	UDP	Expressway-E public IP	24000-29999

8 You must change the administration port because WebRTC clients use 443. If the WebRTC browser tries to access port 80, the Expressway-E redirects the connection to 443.

9 Options for alternative management ports are shown on the web interface. You can use the CLI to change it to a different port, eg. 7443, so that you can lock it down. We strongly advise against opening an external management port on the public IP address. If the browser tries to access port 80, the Expressway-E redirects the connection to your chosen port

10 If your Meeting Server and Expressway deployment is coexisting with MRA, you must not use port 8443 for web administration.

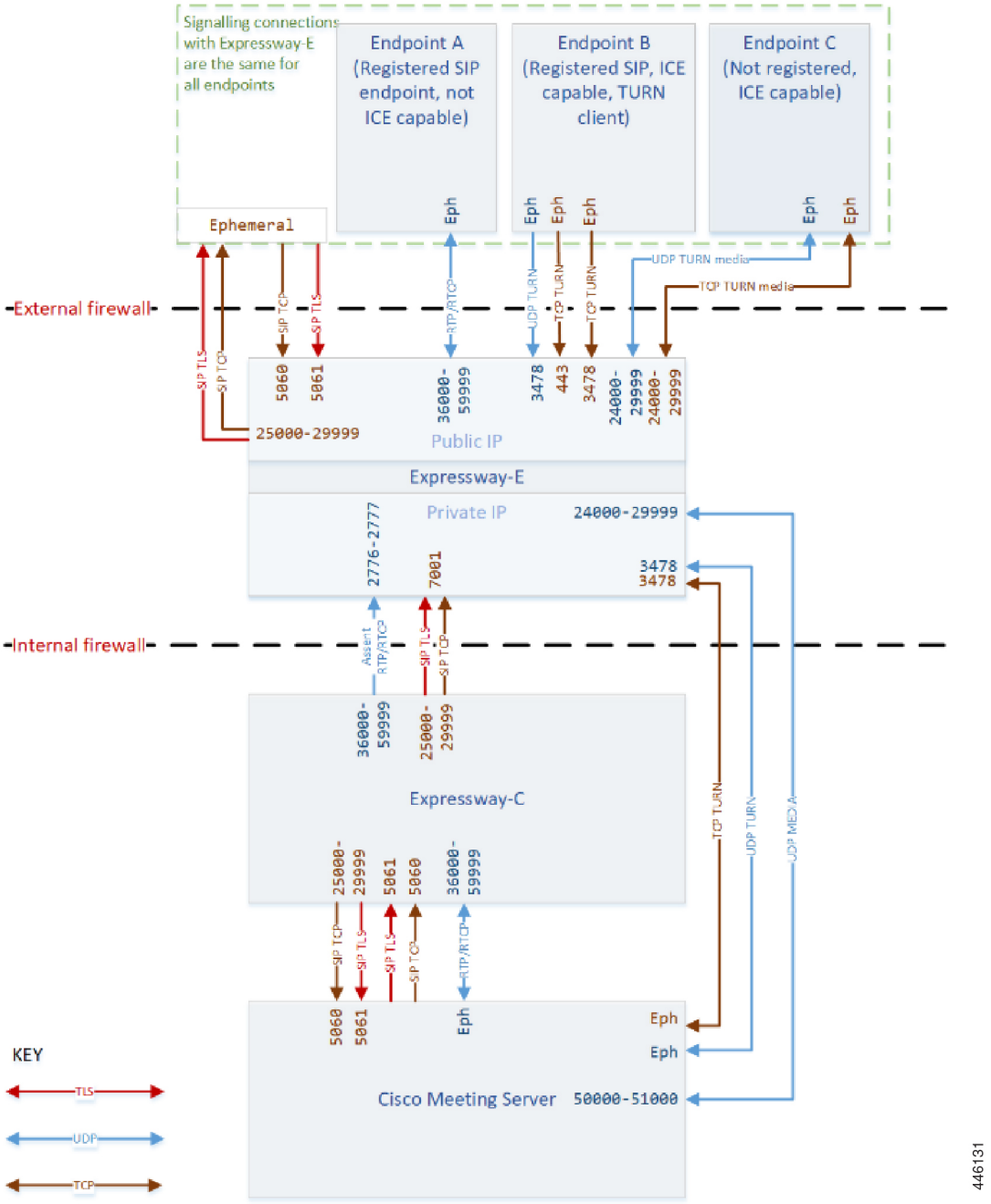
11 In version X8.10, the Expressway cannot listen on TCP 443 for TURN at the same time as it is listening on TCP 443 for signaling from the Cisco Meeting WebRTC App. TCP 3478 is shown, because the Expressway listens on the configured TURN port for both transport protocols. From X8.11, Expressway-E can listen to both TURN and Cisco Meeting Server requests on the TCP port 443.

12 You must configure your external firewall to allow NAT reflection for the Expressway-E public IP address. (Firewalls typically mistrust packets that have the same source and destination IP address). From X12.5.3 release, there is no need to configure NAT reflection on external firewall. This is because Expressway has the ability to detect its own address without NAT reflection.

Important From X12.5.5, support for static NAT functionality on TURN is extended to clustered systems. However, peers which are configured as TURN servers must be reachable using the private addresses for their corresponding public interfaces.

13 If the relay ports are not open, then the Meeting Server will use UDP port 3478 to relay media in all cases. This adds load on the TURN server in cases where the CMA web client is also using a relay.

SIP Edge for Meeting Server Connections (Standards-based Endpoints)



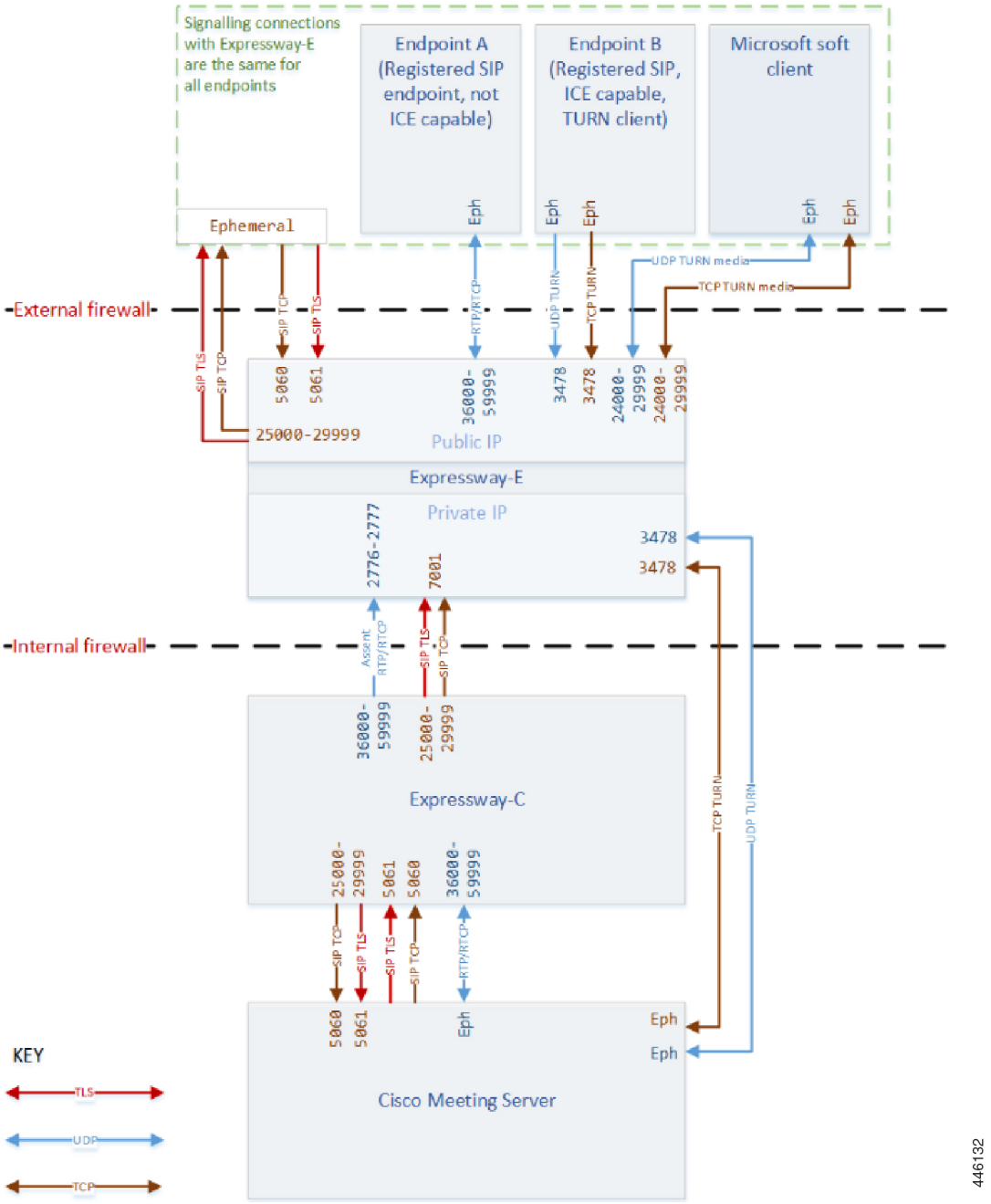
SIP Edge for Cisco Meeting Server Port Reference (Standards-based Endpoints)

Table 24: SIP Edge for Meeting Server Port Reference

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
SIP signaling	Expressway-C	25000-29999	TCP or TLS	Expressway-E	7001 (for first traversal zone; 7002 for second etc.)
SIP signaling	Expressway-C	5060	UDP	Meeting Server	5060
SIP signaling	Expressway-C	25000-29999	TLS	Meeting Server	5061
SIP signaling	SIP endpoint (or its firewall)	>=1024	TCP	Expressway-E	5060
SIP signaling	SIP endpoint (or its firewall)	>=1024	TLS	Expressway-E	5061
Assent RTP (traversed media)	Expressway-C	36000-59999	UDP	Expressway-E	2776 or 36000 (Small/Medium) 36000 - 36010 (even ports) (Large)
Assent RTCP (traversed media	Expressway-C	36000-59999	UDP	Expressway-E	2777 or 36001 (Small/Medium) 36001 - 36011 (odd ports) (Large)
Assent RTP (traversed media)	SIP endpoint (or its firewall)	>=1024 Could be the firewall port where the media egressed, rather than an endpoint port	UDP	Expressway-E	36000-59999

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Assent RTCP (traversed media)	SIP endpoint (or its firewall)	>=1024 Could be the firewall port where the media egressed, rather than an endpoint port	UDP	Expressway-E	36000-59999
Assent RTP (traversed media)	Expressway-E	36000-59999	UDP	SIP endpoint (or its firewall)	>=1024 Expressway waits until it receives media, then sends media to that source port (which could be the port where the media egressed the firewall, not an endpoint port)
TURN request	Any IP address	>=1024 (signaling port from endpoint or the firewall)	UDP & TCP	Expressway-E public IP	3478 (Small/Medium) 3478-3483 (Large)
TURN request	Meeting Server	>=1024	UDP	Expressway-E private IP	3478 (Small/Medium) 3478-3483 (Large)
TURN media	Expressway-E	24000-29999	UDP & TCP	Any IP address	>=1024
TURN media	Any	>=1024 Port of relevant ICE candidate: host IP port, server reflexive port (outside firewall port), or TURN server port	UDP & TCP	Expressway-E	24000-29999
TURN media	Meeting Server	50000-51000	UDP	Expressway-E private IP	24000-29999

SIP Edge for Meeting Server Connections (Microsoft Clients)



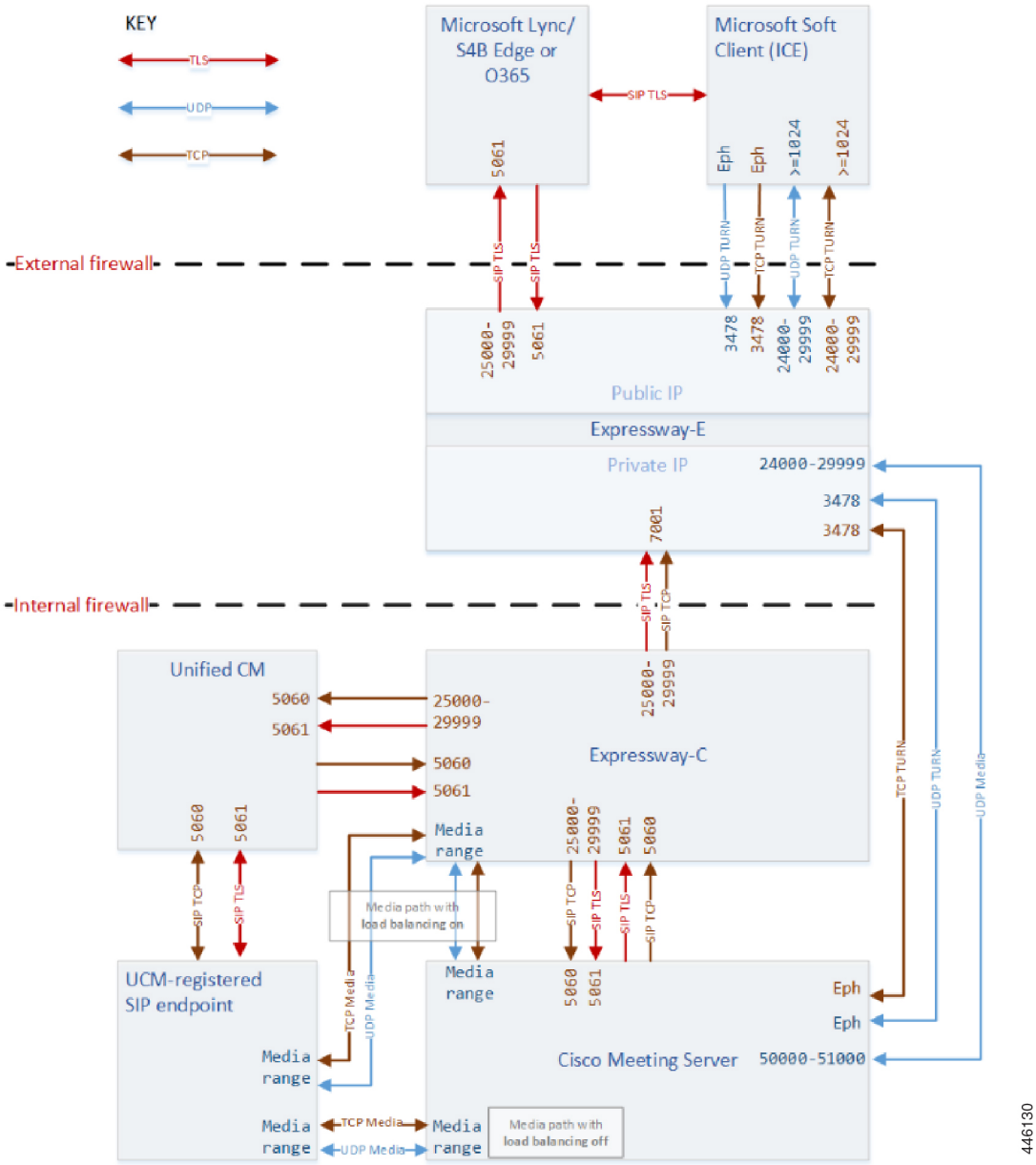
SIP Edge for Cisco Meeting Server Port Reference (Microsoft Clients)

Table 25: SIP Edge for Meeting Server Port Reference

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
SIP signaling	Expressway-C	25000-29999	TCP or TLS	Expressway-E	7001 (for first traversal zone; 7002 for second etc.)
SIP signaling	Expressway-C	25000-29999	TLS	Meeting Server	5061
SIP signaling	SIP endpoint (or its firewall)	>=1024	TCP	Expressway-E	5060
SIP signaling	SIP endpoint (or its firewall)	>=1024	TLS	Expressway-E	5061
Assent RTP (traversed media)	Expressway-C	36000-59999	UDP	Expressway-E	2776 or 36000 (Small/Medium) 36000 - 36010 (even ports) (Large)
Assent RTCP (traversed media)	Expressway-C	36000-59999	UDP	Expressway-E	2777 or 36001 (Small/Medium) 36001 - 36011 (odd ports) (Large)
Assent RTP (traversed media)	SIP endpoint (or its firewall)	>=1024 Could be the firewall port where the media egressed, rather than an endpoint port	UDP	Expressway-E	36000-59999
Assent RTCP (traversed media)	SIP endpoint (or its firewall)	>=1024 Could be the firewall port where the media egressed, rather than an endpoint port	UDP	Expressway-E	36000-59999

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Assent RTP (traversed media)	Expressway-E	36000-59999	UDP	SIP endpoint (or its firewall)	>=1024 Expressway waits until it receives media, then sends media to that source port (which could be the port where the media egressed the firewall, not an endpoint port)
TURN control	Any IP address	>=1024 (signaling port from endpoint or the firewall)	UDP & TCP	Expressway-E	3478 (Small/Medium) 3478-3483 (Large)
TURN media	Expressway-E	24000-29999	UDP & TCP	Any IP address	>=1024
TURN media	Any	>=1024 Port of relevant ICE candidate: host IP port, server reflexive port (outside firewall port), or TURN server port	UDP & TCP	Expressway-E	24000-29999

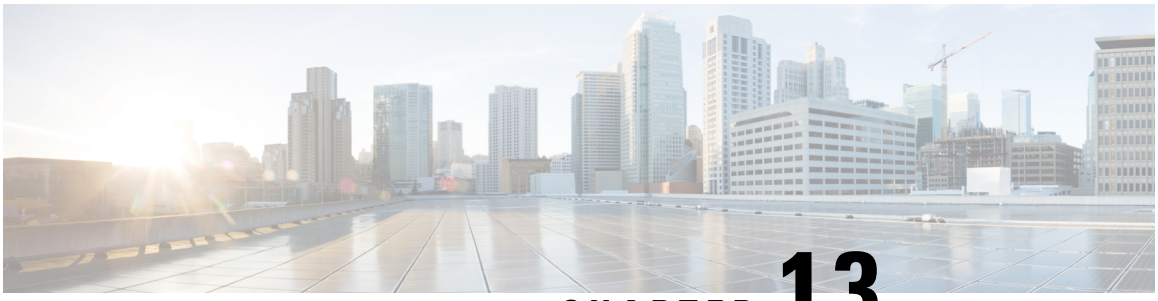
Connection Map-Point to Point Microsoft Interoperability Using Meeting Server



Port Reference-Point to Point Microsoft Interoperability Using Meeting Server

Table 26: Point to Point Microsoft Interoperability Using Meeting Server Port Reference

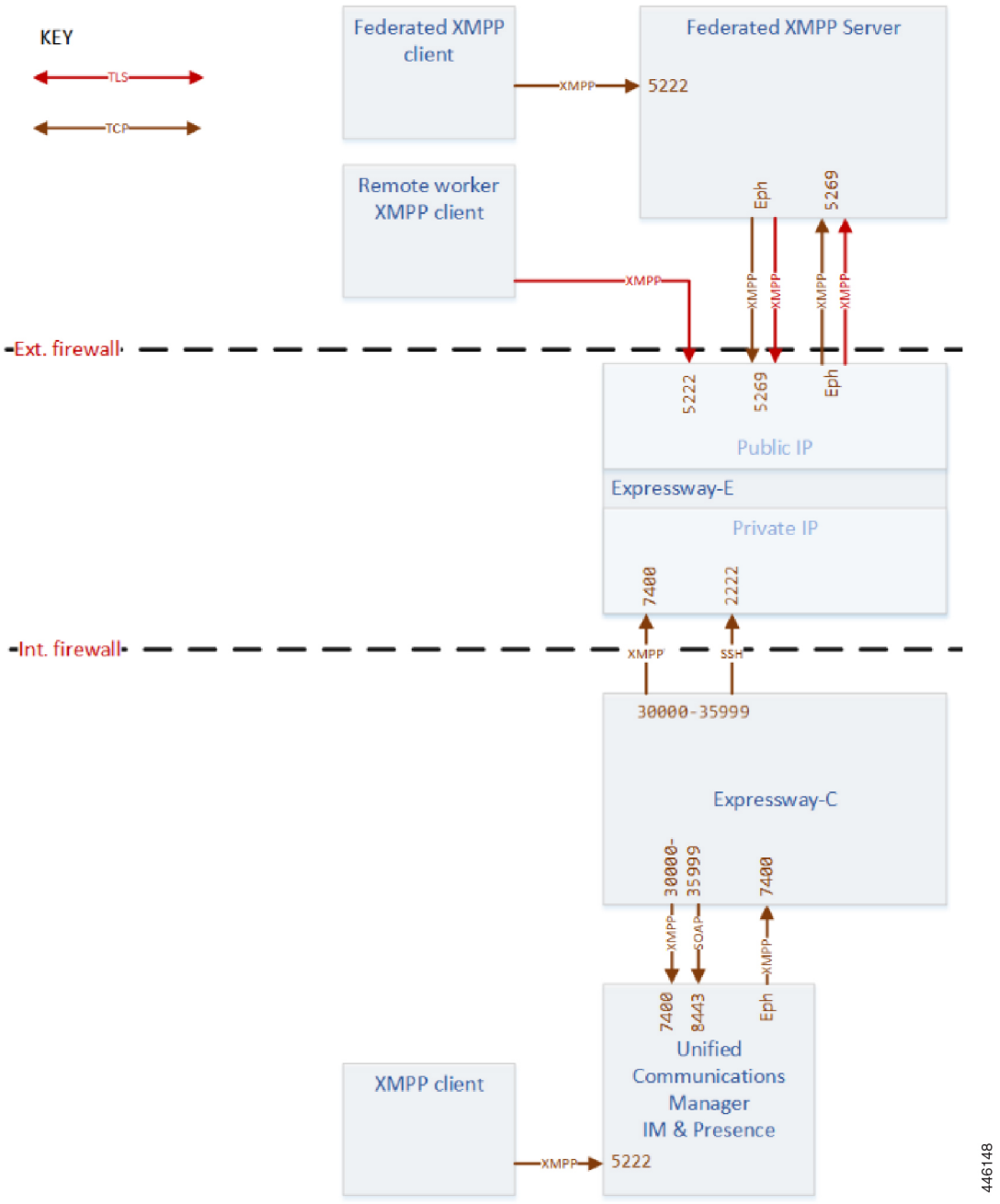
Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
SIP Signaling	Expressway-C	25000-29999	TCP or TLS	Expressway-E	7001 (for first traversal zone; 7002 for second etc.)
SIP Signaling	Expressway-C	25000-29999	TLS	Meeting Server	5061
SIP Signaling	Expressway-C	25000-29999	TCP	Meeting Server	5060
SIP Signaling	Microsoft client or its firewall	>=1024	TLS	Expressway-E	5061
SIP Signaling	Expressway-C	25000-29999	TLS	Unified CM	5061
SIP Signaling	Expressway-C	25000-29999	TCP	Unified CM	5060
SIP Signaling	Unified CM	Ephemeral	TLS	Expressway-C	5061
SIP Signaling	Unified CM	Ephemeral	TCP	Expressway-C	5060
TURN control	Any IP address	>=1024 (signaling port from endpoint or the firewall)	UDP & TCP	Expressway- E	3478 (Small/Medium)
TURN request	Meeting Server	>=1024	UDP/TCP	Expressway-E private IP	3478 (Small/Medium) 3478-3483 (Large)
TURN media	Expressway- E	24000-29999	UDP & TCP	Any IP address	>=1024
TURN media	Any	>=1024 Port of relevant ICE candidate: host IP port, server reflexive port (outside firewall port), or TURN server port	UDP & TCP	Expressway- E	24000-29999
TURN media	Meeting Server	50000-51000	UDP	Expressway-E private IP	24000-29999



CHAPTER 13

XMPP Federation

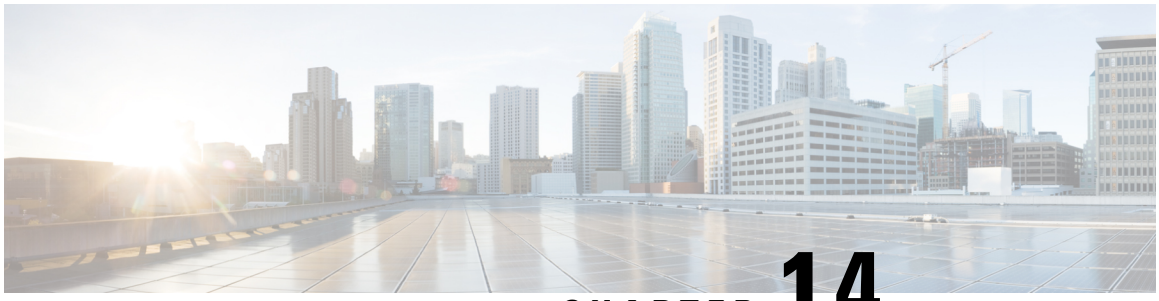
XMPP Federation Connections



XMPP Port Reference

Table 27: XMPP Federation Port Reference

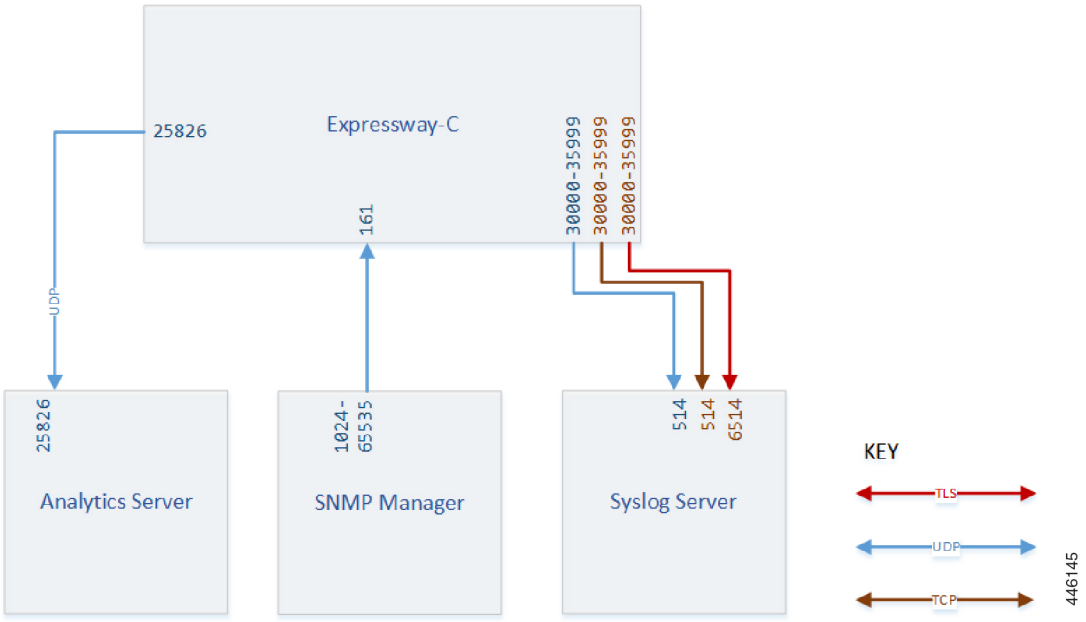
Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Internal XMPP connections	Expressway-C	Ephemeral (30000-35999)	TCP	IM and Presence Service	7400
Outbound XMPP traversal	Expressway-C	Ephemeral (30000-35999)	TCP	Expressway-E	7400
Inbound XMPP connections from federated domain	Any (An XMPP server)	Ephemeral	TCP or TLS	Expressway-E	5269
Outbound XMPP connections to federated domain	Expressway-E	Ephemeral (30000-35999)	TCP or TLS	Any (An XMPP server)	5269



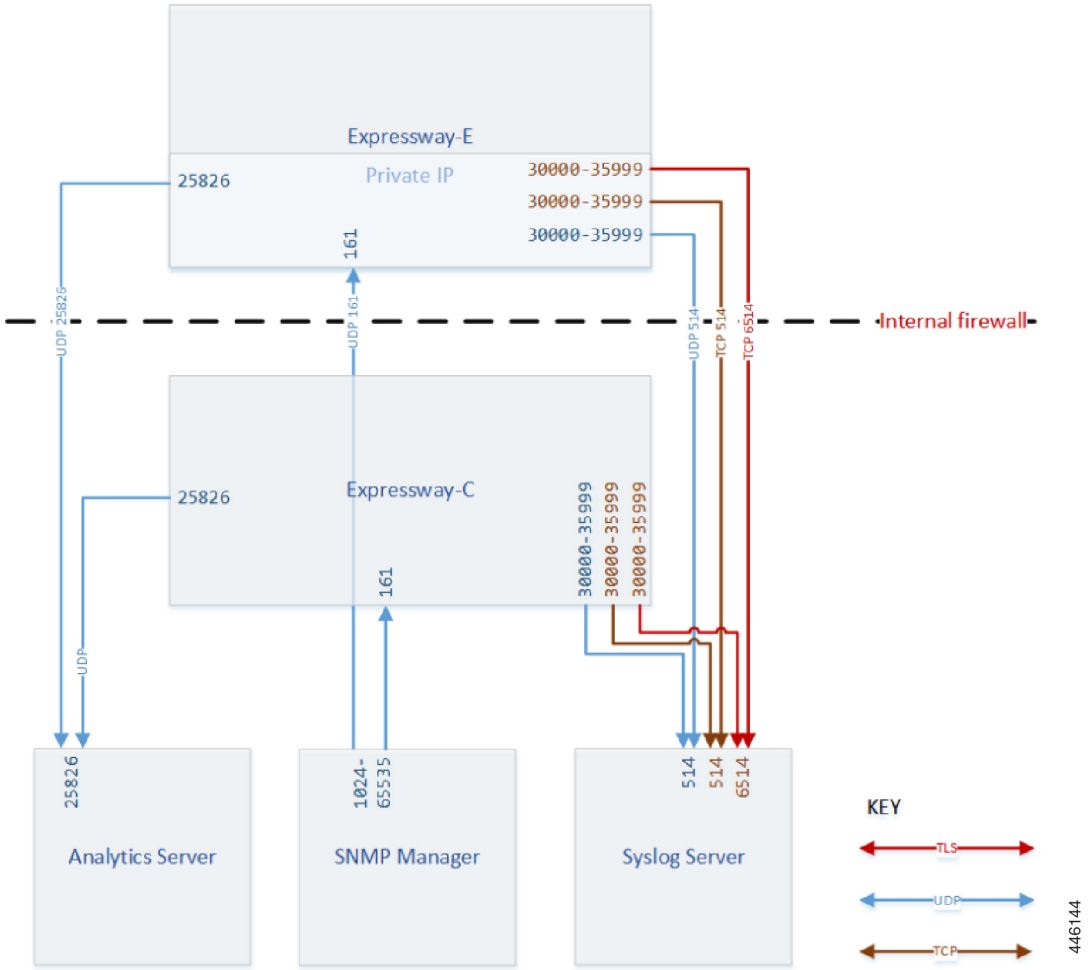
CHAPTER 14

Serviceability

Serviceability - Expressway-C



Serviceability - Traversal Pair

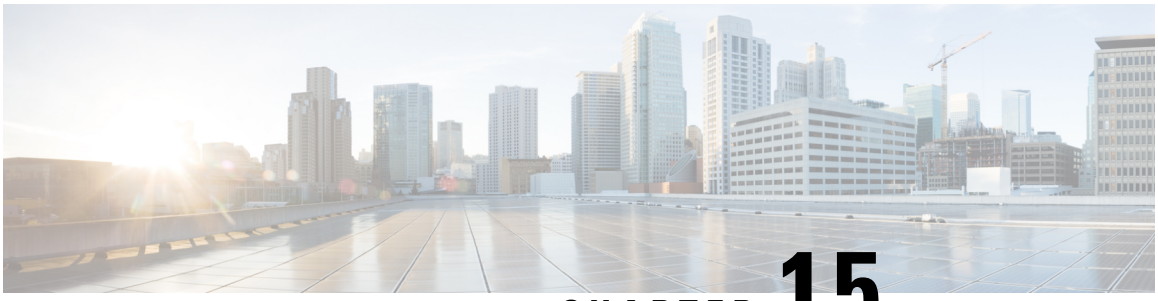


Serviceability Ports - Traversal Pair

Table 28: Serviceability Ports for Expressway-E and Expressway-C

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Network management (SNMP)	SNMP Manager	1024-65535	UDP	Expressway-C	161
System metrics	Expressway	25826	UDP	Analytics server(s)	25826

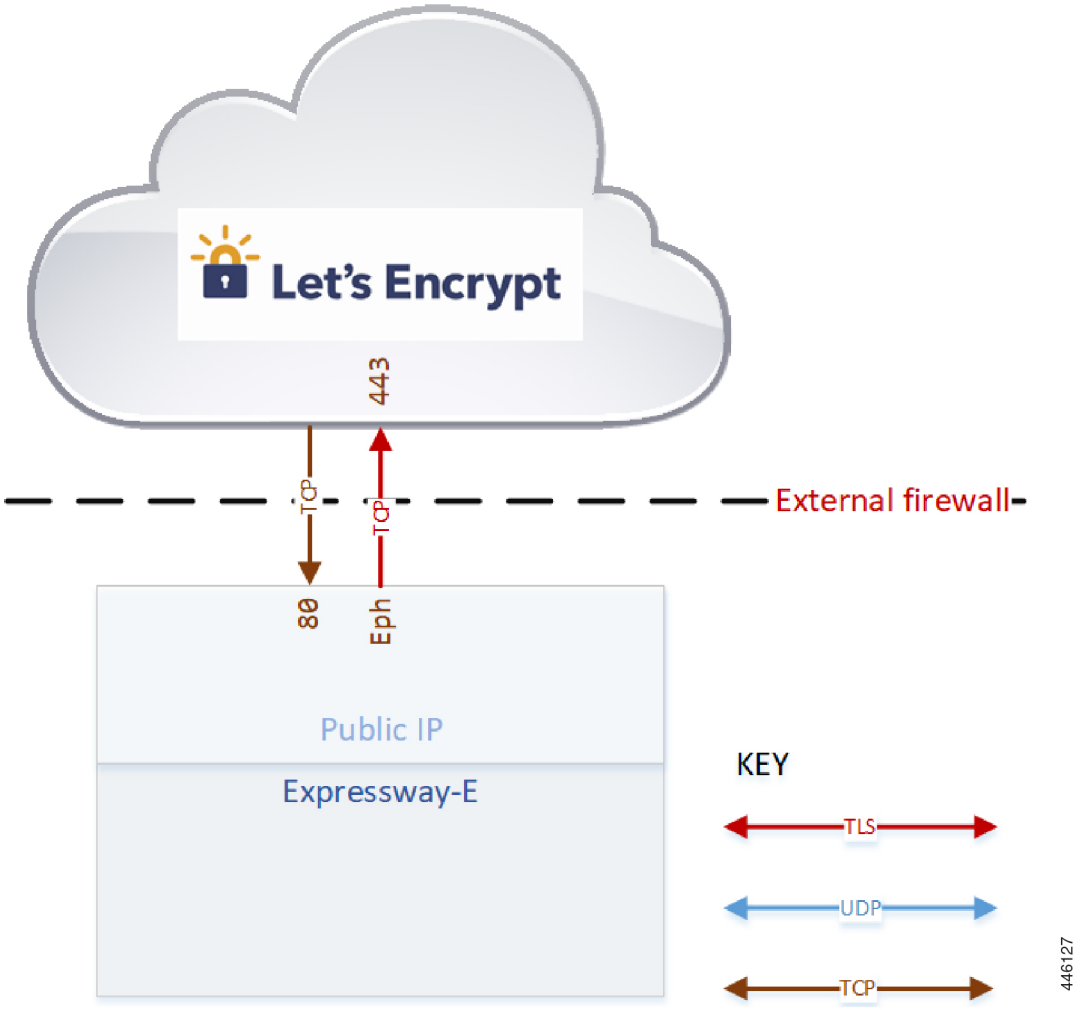
Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Remote logging (syslog)	Expressway	30000-35999	UDP	Syslog server(s)	514
Remote logging (syslog)	Expressway	30000-35999	TCP	Syslog server(s)	514
Remote logging (syslog)	Expressway	30000-35999	TLS	Syslog server(s)	6514



CHAPTER 15

ACME Certificate Management

ACME Certificate Management Connections



Expressway-E ACME Port Reference

Table 29: Ports required to implement ACME (Automated Certificate Management Environment) on Expressway-E

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Write challenge files	Any (ACME provider IP addresses not predictable)	1024-65535	TCP	Expressway-E public NIC	80

Purpose	Src. IP	Src. ports	Protocol	Dest. IP	Dst. Ports
Request certificate signing	Expressway-E public NIC	Ephemeral	TLS	Any (ACME provider domain)	443