Cisco Expressway with Jabber Guest

Deployment Guide

First Published: December 2016

Last Updated: July 2017

Cisco Expressway X8.10

Cisco Jabber Guest Server 10.6.9 (or later)

Contents

Preface

Change History

Table 1 Deployment Guide Change History

Date	Change	Reason
July 2017	Clarified firewall configuration, and other minor updates. Removed VCS variant of this document.	Information improved during X8.10 development.
December 2016	First published with X8.9 release.	

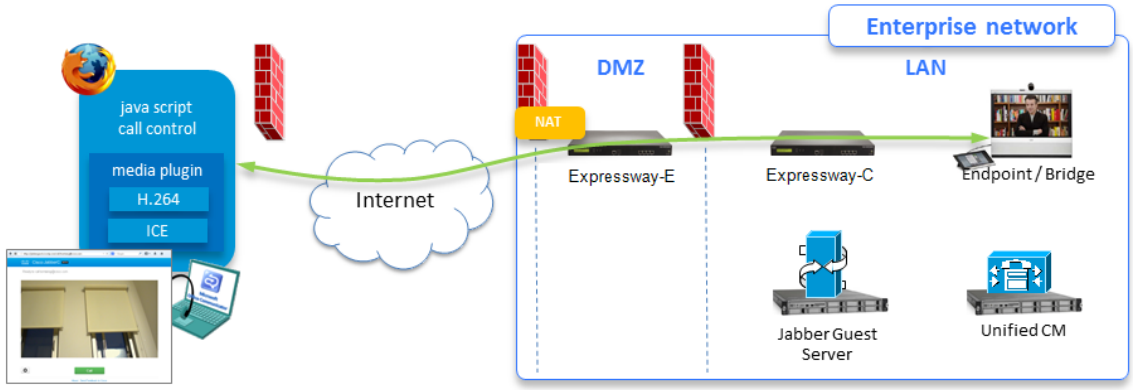
Jabber Guest Services Overview

Cisco Jabber Guest is a consumer to business (C2B) solution that extends the reach of Cisco's enterprise telephony to people outside of a corporate firewall who do not have phones registered with Cisco Unified Communications Manager.

It allows an external user to click on a hyperlink (in an email or a web page) that will download and install (on first use) an H.264 plugin into the user's browser. It then uses http-based call control to "dial" a URL to place a call to a predefined destination inside the enterprise. The user is not required to open an account, create a password, or otherwise authenticate.

To enable the call to be placed, it uses the Expressway solution (a secure traversal zone between the Expressway-C and Expressway-E) as a Unified Communications gateway to traverse the firewall between the Jabber Guest client in the internet and the Jabber Guest servers inside the enterprise to reach the destination user agent (endpoint).

Figure 1 Jabber Guest Components



Information Scope

This Expressway guide also now applies to VCS. Any VCS-specific information is noted where necessary in the guide. (Older VCS guides on Cisco.com are still valid for the VCS versions they apply to—as specified on the title page of each guide.)

The topics here focus on the Expressway configuration required to deploy the Jabber Guest solution. You can read more detailed information about Jabber Guest in the following documents:

- *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the Jabber Guest Installation and Upgrade Guides page.
- *Cisco Jabber Guest Administration Guide*, for your version, at the Jabber Guest Maintain and Operate Guides page.
- *Cisco Jabber Guest Release Notes*, for your version, at the Jabber Guest Release Notes page.

Deployment Options

You can deploy the Expressway-E using either one network interface or two, which affects the call signaling and media paths of the Jabber Guest calls. This document covers both the "single NIC" and "dual NIC" deployment options.

Expressway-E and Expressway-C provide the following functionality:

- Both provides reverse proxy for HTTPS traffic.
- Expressway-E provides TURN relays.

- Expressway-C routes calls to Cisco Unified Communications Manager through a SIP trunk.

Note: Configure a dual NIC deployment if you require static NAT on the Expressway-E.

Jabber Guest Licensing and Call Capacity

The Expressway licensing requirements for Jabber Guest sessions are as follows:

- Each session typically uses four TURN server relays on the Expressway-E.
- **Expressway only**: One rich media session (RMS) license is required per Cisco Jabber Guest session on the Expressway-E.
- **VCS only**: One traversal call license is required per Cisco Jabber Guest session on the Cisco VCS Expressway.

Note:

- Prior to X8.8, one RMS (or traversal) license was required on the Expressway-C for each Jabber Guest session.
- Changes to the licensing model in X8.8 release have revealed an issue with licensing of the Jabber Guest service on the Expressway-E server. When the Expressway pair is part of a "single NIC" deployment, the Expressway-E should count one RMS (or traversal) license for each Jabber Guest call, but it does not. This issue could cause confusion about the server's load because the usage appears low, even when the server is processing multiple calls. We recommend the dual NIC Jabber Guest deployment. If you are using the single NIC deployment, make sure your Expressway-E is correctly licensed to ensure continuity of service when upgrading in future.
- An Advanced Networking license (required for the dual NIC deployment) is included when you order Expressway.

The maximum number of Jabber Guest sessions supported depends on the Expressway platform size, and whether the systems are deployed as a single Expressway-C and Expressway-E pair, or as a pair of clusters.

Table 2 Jabber Guest Session Limits

	Small / Medium systems	Large systems
One Expressway-C and one Expressway-E	100	500
A cluster of Expressway-Cs and a cluster of Expressway-Es (4 or more peers per cluster for maximum capacity)	400	2000

Configure Jabber Guest Services on Expressway

Important Notes:

- You cannot use Jabber Guest services in conjunction with Mobile and Remote Access.
- The domain part of the Expressway-E's FQDN must be the same as the domain you create for Jabber Guest services.
- Your external firewall must allow media coming out from the DMZ that is destined for the public-facing IP address of the Expressway-E:
  - In the single NIC deployment, media is sent from the Expressway-C to the public-facing (static NAT) address of the Expressway-E. See Configure your Firewall for Jabber Guest Traffic, page 25.
  - In the dual NIC deployment, media is sent from the inward-facing NIC of the Expressway-E to the public-facing (static NAT) address of the Expressway-E. See Configure your Firewall for Jabber Guest Traffic, page 25.

Where examples are required, we're using the example of a Jabber Guest client calling the URL `https://expressway.example.com/call/8111@example.com`.

Jabber Guest Configuration Summary

Table 3 Taskflow for Configuring Expressway for Jabber Guest

Command or Action	Purpose
Configuring a Secure Traversal Zone Connection for Unified Communications, page 10	Unified Communications features such as Mobile and Remote Access or Jabber Guest, require a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E. This involves: ■ Installing suitable security certificates on the Expressway-C and the Expressway-E. ■ Configuring a Unified Communications traversal zone between the Expressway-C and the Expressway-E. See Configuring a Secure Traversal Zone Connection for Unified Communications, page 10 for instructions about how to do this if your system does not already have a secure traversal zone in place.
Configure the Expressway-E for Jabber Guest, page 14	To turn on Jabber Guest services and enable media routing between Jabber Guest client and Expressway-C. For the dual NIC deployment only, you also enable Jabber Guest on the appropriate domain, create Jabber Guest servers to link to that domain, and create neighbor zones to route calls from those servers.
Configure the Expressway-C for Jabber Guest, page 16	To turn on Jabber Guest services. For the single NIC deployment only, you also enable Jabber Guest on the appropriate domain, create Jabber Guest servers to link to that domain, and create neighbor zones to route calls from those servers.
Configure Call Routing for Jabber Guest, page 19	To route the SIP calls coming from Jabber Guest toward the on-premises endpoints or bridges, create search rules that target the appropriate neighbor zones.

Table 3 Taskflow for Configuring Expressway for Jabber Guest (continued)

Command or Action	Purpose
Configure your Firewall for Jabber Guest Traffic, page 25	To translate destination addresses and ports for inbound calls, and to enable the various call legs to traverse the external and internal firewalls as necessary. Much of the firewall configuration for the single NIC and dual NIC options is the same, but there are some differences.

Configuring a Secure Traversal Zone Connection for Unified Communications

Unified Communications features such as Mobile and Remote Access or Jabber Guest, require a Unified Communications traversal zone connection between the Expressway-C and the Expressway-E. This involves:

- Installing suitable security certificates on the Expressway-C and the Expressway-E.
- Configuring a Unified Communications traversal zone between the Expressway-C and the Expressway-E.

Note: Configure only one *Unified Communications traversal* zone per Expressway traversal pair. That is, one *Unified Communications traversal* zone on the Expressway-C cluster, and one corresponding *Unified Communications traversal* zone on the Expressway-E cluster.

Installing Expressway Security Certificates

You must set up trust between the Expressway-C and the Expressway-E:

1. Install a suitable server certificate on both the Expressway-C and the Expressway-E.
   - The certificate must include the **Client Authentication** extension. The system will not let you upload a server certificate without this extension when Unified Communications features are enabled.
   - The Expressway includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:
     - Ensure that the CA that signs the request does not strip out the client authentication extension.
     - The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled.
   - To generate a CSR and /or to upload a server certificate to the Expressway, go to **Maintenance > Security > Server certificate**. You must restart the Expressway for the new server certificate to take effect.
2. Install on both Expressways the trusted Certificate Authority (CA) certificates of the authority that signed the Expressway's server certificates.

   There are additional trust requirements, depending on the Unified Communications features being deployed.

   For Mobile and Remote Access deployments:

   - The Expressway-C must trust the Unified CM and IM&P tomcat certificate.
   - If appropriate, both the Expressway-C and the Expressway-E must trust the authority that signed the endpoints' certificates.

   For Jabber Guest deployments:

   - When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the Expressway-C either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate.

   To upload trusted Certificate Authority (CA) certificates to the Expressway, go to **Maintenance > Security > Trusted CA certificate**. You must restart the Expressway for the new trusted CA certificate to take effect.

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

Configuring Encrypted Expressway Traversal Zones

To support Unified Communications features via a secure traversal zone connection between the Expressway-C and the Expressway-E:

- The Expressway-C and Expressway-E must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on Expressway-C or a traversal server zone when selected on Expressway-E) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.
- Both Expressways must trust each other's server certificate. As each Expressway acts both as a client and as a server you must ensure that each Expressway's certificate is valid both as a client and as a server.
- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

To set up a secure traversal zone, configure your Expressway-C and Expressway-E as follows:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.

3. Configure the fields as follows (leave all other fields with default values):

	Expressway-C	Expressway-E
Name	"Traversal zone" for example	"Traversal zone" for example
Type	*Unified Communications traversal*	*Unified Communications traversal*
Connection credentials section		
Username	"exampleauth" for example	"exampleauth" for example
Password	"ex4mpl3.c0m" for example	Click **Add/Edit local authentication database**, then in the popup dialog click **New** and enter the **Name** ("exampleauth") and **Password** ("ex4mpl3.c0m") and click **Create credential**.
SIP section		
Port	7001	7001
TLS verify subject name	Not applicable	Enter the name to look for in the traversal client's certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.
Authentication section		
Authentication policy	*Do not check credentials*	*Do not check credentials*
Location section		
Peer 1 address	Enter the FQDN of the Expressway-E. Note that if you use an IP address (not recommended), that address must be present in the Expressway-E server certificate.	Not applicable
Peer 2...6 address	Enter the FQDNs of additional peers if it is a cluster of Expressway-Es.	Not applicable

4. Click **Create zone**.

Overview of Expressway-E Deployment

Single NIC Deployment Summary

- The Expressway-E is in the DMZ with a single NIC enabled.
- Expressway-E in static NAT mode is optional and requires extra configuration on the Jabber Guest server.
- The Expressway-E is used for TURN services and reverse proxy, not call control.
- SIP traffic goes from the Jabber Guest server to the Expressway-C.
- Media flows between the Expressway-E and Expressway-C using TURN relay and not a traversal zone.

Note: You can optionally configure the Expressway-E LAN interface to use static NAT mode. If you do, you must configure the Jabber Guest server with the public IP address (static NAT address), and the private IP address of the Expressway-E. These details are on **System > Network interfaces > IP**.

Dual NIC Deployment Summary

- The Expressway-E is in the DMZ with both NICs enabled.
- Expressway-E in static NAT mode is optional and requires extra configuration on the Cisco Jabber Guest server.
- The Expressway-E is used for TURN services, reverse proxy, and call control.
- SIP traffic goes from the Jabber Guest server to the Expressway-E.
- Media flows between the Expressway-E and Expressway-C using a traversal zone.

Note:

- If the outward-facing LAN interface of the Expressway-E has static NAT mode on, you need to configure the Jabber Guest server with the Expressway-E's public IP address, and both of its private IP addresses. These details are on **System > Network interfaces > IP**.
- If Expressway-E is used for reverse proxy functionality, the Cisco Jabber Guest URL looks like *http://expressway-e.example.com/call* where *expressway-e.example.com* is the FQDN of the Expressway-E.

Configure the Expressway-E for Jabber Guest

Note: Before you begin ensure that you have set up Expressway security certificates and a Unified CM traversal zone. See Configuring a Secure Traversal Zone Connection for Unified Communications, page 10

Task 1: Enable Jabber Guest Services

1. On the Expressway-E, go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Jabber Guest services*.
3. Click **Save**.

   Jabber Guest services are enabled. You need to enable Jabber Guest on a domain, then you can configure Jabber Guest servers. You do this on the Expressway-E for the dual NIC deployment, or on the Expressway-C for the single NIC deployment.

Task 2: Enable TURN Services

You must enable the Expressway-E's TURN server to allow media routing from the Jabber Guest clients to the Expressway-C to be established through ICE:

1. Go to **Configuration > Traversal > TURN**.
2. Set **TURN services** to *On*.
3. Set the **Authentication realm** to its default of TANDBERG.
4. Click **Save**.

You do not have to set up any TURN client credentials in the local authentication database.

Note: To configure TURN credential provisioning and set up TURN server information on Jabber Guest, see the *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the Jabber Guest Installation and Upgrade Guides page.

Task 3: Reduce the Default MTU to 1400 Bytes

In some call scenarios, such as when using VPN / SSL tunnels, the available Maximum Transmission Unit (MTU) can be reduced. The default MTU on Expressway-E of 1500 bytes can be too high and can cause packet loss. We recommended that you lower the MTU size on the relevant network interfaces to 1400 bytes.

1. Go to **System > Network interfaces > IP**.
2. In the **Maximum transmission unit (MTU)** field, enter 1400.

   If you have multiple interfaces, you will typically want to do this on the externally facing interface.
3. Click **Save**.

Task 4: [Dual NIC Deployment Only] Create Corresponding Neighbor Zones for Each of the Jabber Guest Servers

Note: These neighbor zones are used to receive traffic **from** the Jabber Guest servers. Do not configure any search rules to route traffic **to** these zones.

1. On the Expressway-E, go to **Configuration > Zones > Zones**.
2. Click **New**.

3. Configure the fields as follows (leave all other fields with default values):

Name	Enter the name you want to give this zone, for example “Jabber Guest server [name]”.
Type	*Neighbor*
H.323 mode	*Off*
SIP mode	*On*
Transport	*TLS*
TLS verify mode	*On* As these zones use a TLS verified connection you must ensure certificate trust between the Expressway and the Jabber Guest servers. – When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the Expressway-C either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate.To upload trusted Certificate Authority (CA) certificates to the Expressway, go to **Maintenance > Security > Trusted CA certificate**. You must restart the Expressway for the new trusted CA certificate to take effect. – You must install on the Jabber Guest server the trusted CA certificates of the authority that signed the Expressway-C's server certificate. To manage certificates on the Jabber Guest server, go to **Settings > Local SSL Certificate**.
Media encryption mode	*Force encrypted*
Location	Enter the same FQDN of the Jabber Guest server as configured on the **Jabber Guest servers** page.
Zone profile	Default

4. Click **Create zone**.
5. Repeat this process for every Jabber Guest server.

Task 5: [Dual NIC Deployment Only] Create a Search Rule for the Traversal Zone Between the Expressway-E and Expressway-C Servers

For proper call routing, the SIP domain that you specify on the Jabber Guest server (click **Settings**, click **Call Control and Media**) and the domain that you optionally specify for **Destination** when you create a link (click **Links**, click **New**) must be configured on the Expressway-E search rule to point to the traversal zone. See Configure Call Routing for Jabber Guest, page 19 for more information.

Configure the Expressway-C for Jabber Guest

Task 1: Enable Jabber Guest Services

1. On the Expressway-C, go to **Configuration > Unified Communications > Configuration**.
2. Set **Unified Communications mode** to *Jabber Guest services*.
3. Click **Save**.

   Jabber Guest services are enabled. You need to enable Jabber Guest on a domain, then you can configure Jabber Guest servers.

Task 2: Enable Jabber Guest on the Required Domain

Important! The domain that you create on the Expressway-C, for associating Jabber Guest servers, is not related to any SIP domain(s) or internal DNS domains. The only requirement is that the domain must match the domain of the Expressway-E's public-facing FQDN.

1. Go to **Configuration > Domains**.
2. Select the domain that supports Jabber Guest services.

   (If the domain does not yet exist, click **New** and enter the **Domain name**, in this case, `example.com`).
3. Set **Jabber Guest** to *On*.
4. Click **Save**.

   (The button reads **Create domain** if you are setting up the domain for the first time).

Note:

- Only one Jabber Guest domain is supported per Expressway (cluster) deployment.
- Make sure that the domain has an associated DNS record that resolves to the Expressway-E. The domain information is propagated from the Expressway-C to the Expressway-E through the SSH tunnel (port 2222). The information is used by the Expressway-E to validate incoming HTTP requests for the Jabber Guest service.

Task 3: Configure Jabber Guest Servers and Associate Their Addresses with the Jabber Guest Domain

1. Go to **Configuration > Unified Communications > Jabber Guest servers**.

   This takes you to the **Jabber Guest servers** page.
2. Click **New**.
3. Enter the details of the Jabber Guest server:
   a. **Domain**: select the Jabber Guest domain that is to be mapped to a server hostname.
   b. **Server hostname**: enter the FQDN of a Jabber Guest server to use for the selected domain.

      This must be an FQDN, not an unqualified hostname or an IP address. The domain part of the FQDN does not need to match what you enter in **Domain** field.
   c. **Priority**: this controls the order in which connections to this hostname are attempted for this domain.

      All priority 1 hostnames are attempted first, followed by priority 2 hostnames, and so on.

      Give each Jabber Guest server a different priority so that calls are only sent to one Cisco Jabber Guest server in the deployment at a time.
4. Click **Create entry**.

5. If necessary, add further Jabber Guest server addresses for the domain. You can give each server the same priority for even load balancing.

Task 4: Verify that the SSH Tunnel is Active

1. On either the Expressway-C or the Expressway-E, go to **Status > Unified Communications**.
2. Click **View ssh tunnel status**.
3. Make sure that the Cisco Jabber Guest domain is listed and that the SSH tunnel is active.

Task 5: [Single NIC Deployment Only] Create Corresponding Neighbor Zones for Each of the Jabber Guest Servers

Note: These neighbor zones are used to receive traffic **from** the Jabber Guest servers. Do not configure any search rules to route traffic **to** these zones.

1. On the Expressway-C, go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

Name	Enter the name you want to give this zone, for example "Jabber Guest server [name]."
Type	*Neighbor*
H.323 mode	*Off*
SIP mode	*On*
Transport	*TLS*
TLS verify mode	*On* As these zones use a TLS verified connection you must ensure certificate trust between the Expressway and the Jabber Guest servers. – When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the Expressway-C either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server's certificate. To upload trusted Certificate Authority (CA) certificates to the Expressway, go to **Maintenance > Security > Trusted CA certificate**. You must restart the Expressway for the new trusted CA certificate to take effect. – You must install on the Jabber Guest server the trusted CA certificates of the authority that signed the Expressway-C's server certificate. To manage certificates on the Jabber Guest server, go to **Settings > Local SSL Certificate**.
Media encryption mode	*Force encrypted*
Location	Enter the same FQDN of the Jabber Guest server as configured on the **Jabber Guest servers** page.
Zone profile	Default

4. Click **Create zone**.

5. Repeat this process for every Jabber Guest server.
   Do not configure any search rules for these neighbor zones. These zones are used to receive traffic only.

Task 6: Set up a Connection Between Expressway-C and Cisco Unified Communications Manager

1. On Cisco Unified Communications Manager, set up a nonsecure or secure SIP trunk to the Expressway-C.
2. On Expressway-C, set up a neighbor zone to Cisco Unified Communications Manager.

See *Cisco Unified Communications Manager with Expressway (SIP Trunk) Deployment Guide* on the Expressway configuration guides page.

Task 7: [Single NIC Deployment Only] Create a Search Rule on Expressway-C to Route Calls to Cisco Unified Communications Manager

You must create a search rule on Expressway-C to route calls to Cisco Unified Communications Manager. See Configure Call Routing for Jabber Guest, page 19 for more information.

Task 8: Force the Protocol Between the Cisco Jabber Guest Server and the Expressway-C to be HTTP:

1. Sign in to the Expressway-C command line interface as an administrator. In a clustered Expressway-C deployment, sign in to the primary peer Expressway-C.
2. Enter the following command: `xconf CollaborationEdge JabbercProxyProtocol: http`

Note: HTTP requests go from the Expressway-E to the Expressway-C to the Jabber Guest server.

Configure Call Routing for Jabber Guest

You configure call routing on the Expressway-C or on the Expressway-E, depending on whether you're deploying the Expressway-E with a single NIC or with both NICs. In each case, the objective is to listen for SIP calls from Jabber Guest servers and route them toward the on-premises destinations.

You already created neighbor zones to the Jabber Guest servers. Now you need to create search rules for calls originating from these zones.

Single NIC Deployment

For each Jabber Guest server neighbor zone on the Expressway-C, create a search rule that:

- Matches the pattern of the destinations set by Jabber Guest on calls to that zone.

  The destinations are either DN numbers or SIP URIs in the Jabber Guest database, where they are associated with call URIs. Jabber Guest server forms them as SIP URIs by appending the domain as required. Hopefully the incoming SIP URIs match endpoints or bridges that are routable by call control agents neighbored to this Expressway-C.
- Targets the neighbor zone of the call control agent that knows how to route to the matched destination (see Onward Routing Options (Both Deployment Types), page 19).

Dual NIC Deployment

For each Jabber Guest server neighbor zone on the Expressway-E, create a search rule that:

- Matches the pattern of the destinations set by Jabber Guest on calls to that zone.

  The destinations are either DN numbers or SIP URIs in the Jabber Guest database, where they are associated with call URIs. Jabber Guest server forms them as SIP URIs by appending the domain as required.
- Targets the secure traversal zone to the Expressway-C.

Onward Routing Options (Both Deployment Types)

When the Jabber Guest SIP call arrives at the Expressway-C, either in the Expressway-E traversal client zone (dual NIC), or the Jabber Guest neighbor zone (single NIC), the search rule must target the neighbor zone that can route to the supplied destination.

For example, if the destination address is `8111@example.com`, the alias pattern would be something like `(8(\d{3})@example\.com`, and the target zone options could include:

- **Endpoints / bridges registered to Unified CM**: the search rule targets the SIP trunk / neighbor zone between Unified CM and Expressway-C. See *Cisco Unified Communications Manager with Expressway (SIP Trunk) Deployment Guide* on the Expressway configuration guides page.
- **Endpoints registered to a neighbor system (such as a Cisco VCS)**: the search rule targets the neighbor zone that you created when neighboring to that system.
- **Endpoints registered to the local Expressway-C**: in this case you need suitable search rules to route calls for the Jabber Guest domain to the relevant endpoints.

Note: For endpoints that are registered with Expressway, the call path must include Cisco Unified Communications Manager.

Single NIC Deployment Signaling and Media Paths

This topic summarizes the Jabber Guest traffic flow through the Expressway-E and Expressway-C deployment when the Expressway-E has one network interface card (NIC) active.

For more information on configuring signaling and media, see the *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the Jabber Guest Installation and Upgrade Guides page.

Call Flow Summary in Single NIC Deployment

1. The Jabber Guest client sends an HTTP(S) request which is routed using HTTPS tunnels through the Expressway solution and on to the Jabber Guest server inside the enterprise.
2. The Jabber Guest server converts the HTTP(S) request into SIP and sends it to the Expressway-C.
3. The Expressway-C routes the call to the appropriate destination endpoint or bridge, typically through a SIP trunk to Unified CM.
4. Expressway-C back-to-back user agent (B2BUA) connects the call (media) to the originating Jabber Guest client through the Expressway-E's TURN server.

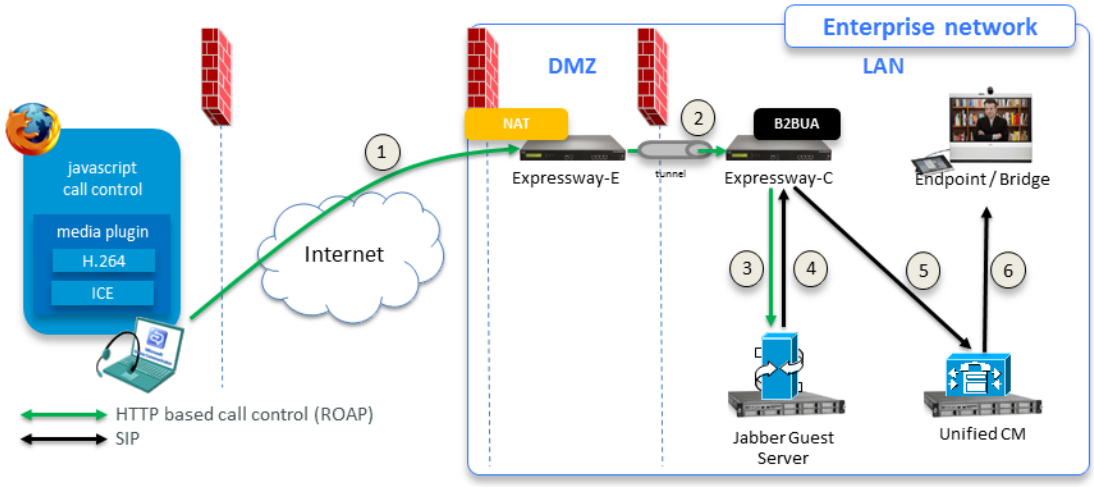
   Media path: Collaboration endpoint or bridge <--> Expressway-C (B2BUA) <--> Expressway-E (TURN server) <--> Jabber Guest client

Call Signaling Flow

When the Jabber Guest client initiates the call, the following diagram shows how the signaling is typically routed through the Expressway-C, Jabber Guest server, to Unified CM. Cisco Unified Communications Manager routes the call onward to the endpoint or bridge.

The return signaling, from the user agent to the Jabber Guest client, follows the same path in reverse.

Figure 2 Call Signaling Path



Media Flow

Media channels negotiation results in the allocation of TURN relays between the Jabber Guest client and the Expressway-E.

Note: Jabber Guest media does not go through the traversal link between Expressway-E and Expressway-C. Media is sent from the Expressway-C to the outward-facing/NAT interface of the Expressway-E. You may need to configure your external firewall to allow the media back in.

Figure 3 Media Path Negotiation

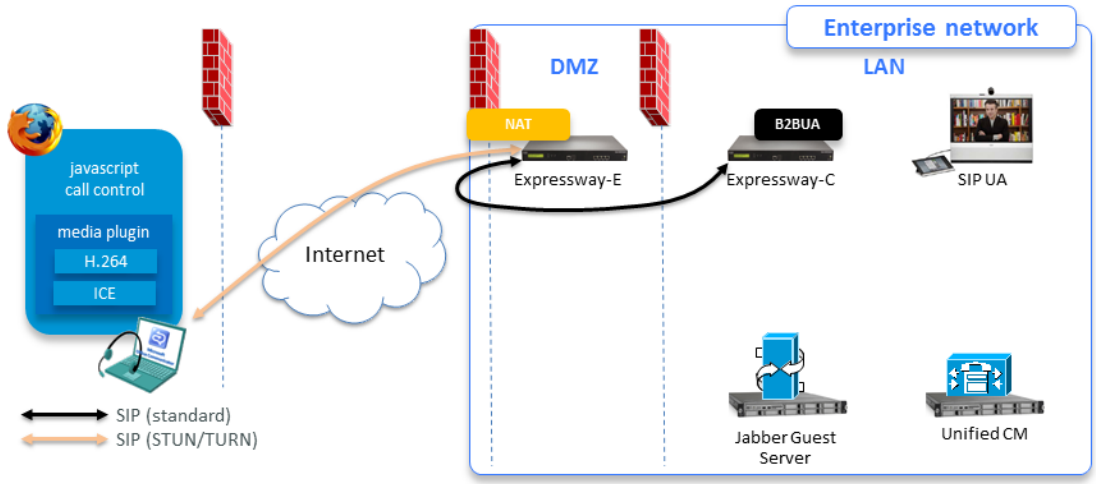
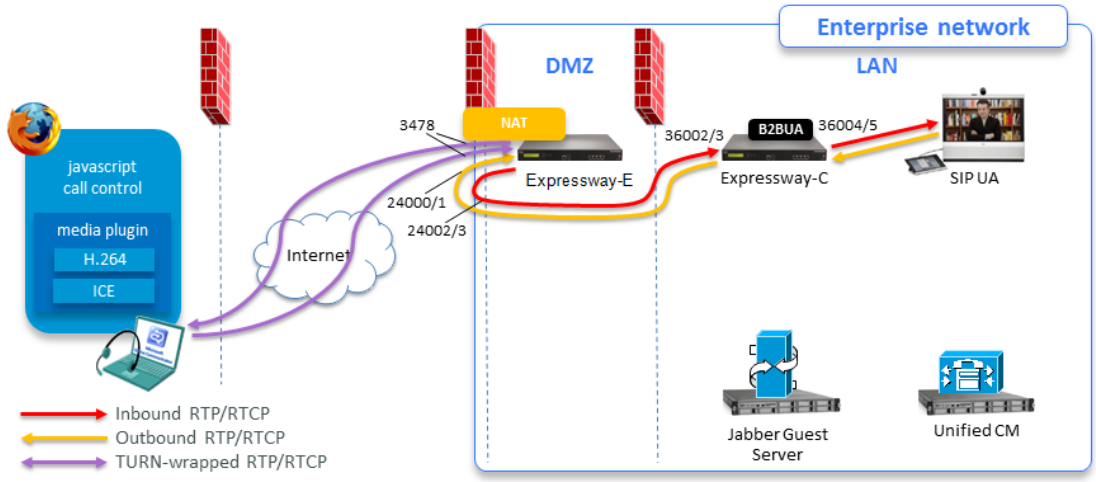


Figure 4 Media Path and Typical Ports

The following diagram shows the media flows and typical port usage on the Expressway-E and Expressway-C. The TURN server on the Expressway-E relays the media between the Jabber Guest client and the B2BUA on the Expressway-C, and the media also flows between the B2BUA and the internal endpoint.



See Configure your Firewall for Jabber Guest Traffic, page 25 for full information about port requirements.

Note: If the Expressway-E is behind a NAT, extra configuration is required on the Cisco Jabber Guest server to avoid the media flowing to the static NAT address. Turn on **Static NAT mode** and configure the static NAT address and DMZ external address of the Expressway-E on the Cisco Jabber Guest server. This allows media to be sent to the DMZ external address of the Expressway-E, avoiding NAT reflection on the outside firewall.

Jabber Guest Signaling and Media Flows in Dual NIC Deployment

This topic summarizes the Jabber Guest traffic flow through the Expressway-E and Expressway-C deployment when the Expressway-E has both NICs active.

For more information on configuring signaling and media, see the *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the Jabber Guest Installation and Upgrade Guides page.

Call Flow Summary in Dual NIC Deployment

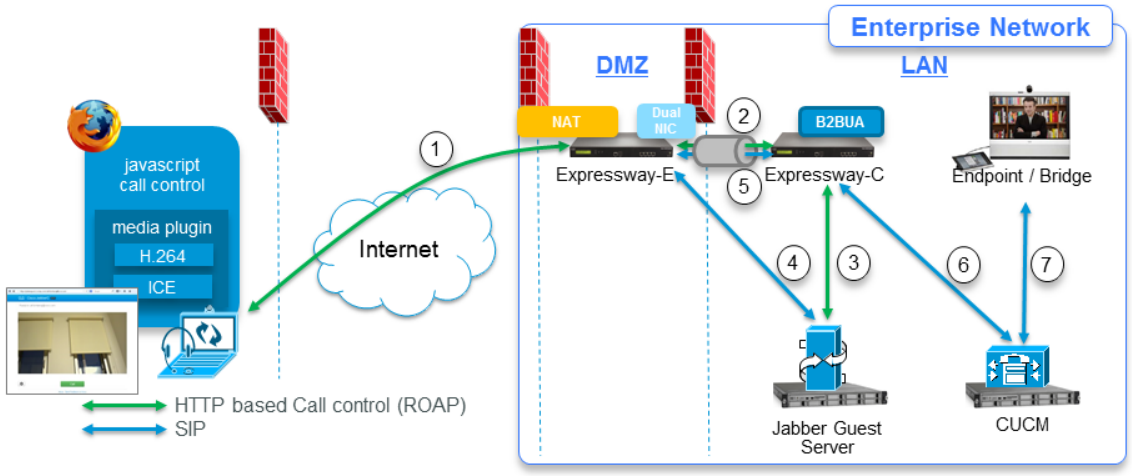
The typical call flow for Jabber Guest can be summarized as follows:

1. The Jabber Guest client sends an HTTP(S) request which is routed using HTTPS tunnels through the Expressway solution and on to the Jabber Guest server inside the enterprise.
2. The Jabber Guest server converts the HTTP(S) request into SIP and sends it to the inward-facing NIC of the Expressway-E.
3. The SIP traffic traverses the internal firewall from the Expressway-E to the Expressway-C.
4. The Expressway-C routes the call to the appropriate destination (typically to Unified CM which routes it on to an endpoint or conferencing bridge).
5. The media path is established from the bridge or endpoint as follows:

   Internal party <--> Expressway-C <--> Expressway-E (inward-facing NIC) <--> TURN server (Expressway-E outward-facing NIC) <--> Jabber Guest client.

Call Signaling Flow

Figure 5 Signaling Flow of Jabber Guest Call on Dual NIC Expressway-E Deployment



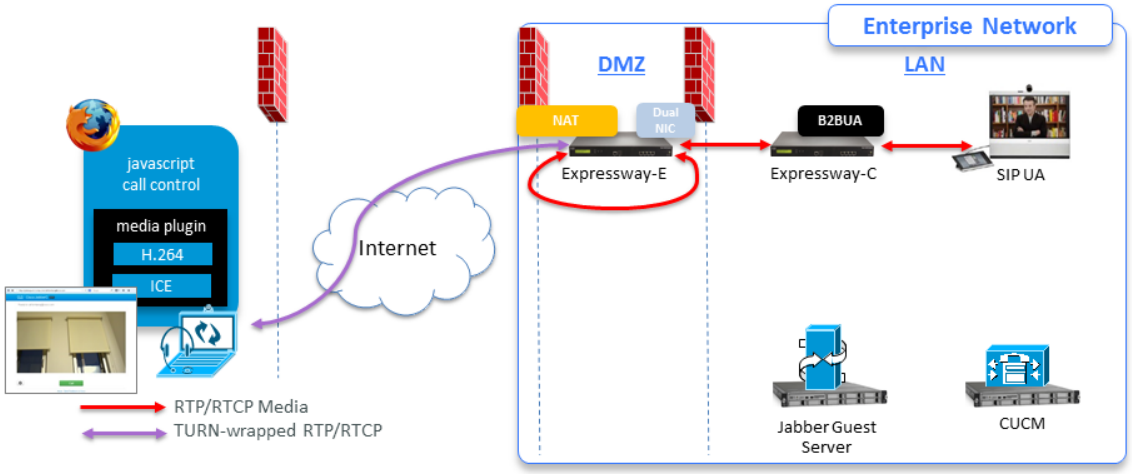
1. Jabber Guest client initiates call by HTTP(S) ROAP to external IP address of Expressway-E.

   The external firewall translates addresses and ports as necessary to reach correct listening socket on Expressway-E's outward-facing NIC.
2. Expressway-E tunnels HTTPS through internal firewall to Expressway-C.
3. Expressway-C routes HTTPS to Jabber Guest server through a neighbor zone.
4. Jabber Guest server wraps the HTTPS ROAP as SIP and connects out (through internal firewall) to the inward-facing NIC of Expressway-E.

5. SIP traverses the internal firewall through the Unified Communications traversal zone between Expressway-E and Expressway-C.
6. Expressway-C routes the call on the SIP trunk to Unified CM.
7. Unified CM routes the call to the destination endpoint or bridge.

RTP Media Flow

Figure 6 Media Path



1. The internal endpoint call connects to the Expressway-C.
2. The B2BUA sends media to the TURN server (on the public address of the outward-facing NIC of the Expressway-E).

   To get there, the media traffic goes through the Unified Communications traversal zone to the inward-facing NIC on Expressway-E, where it hairpins and goes out to the public IP address of the outward-facing NIC.
3. Expressway-E's TURN server negotiates TURN with the Jabber Guest client, and allocates TURN relays between the Jabber Guest client and the Expressway-C.

   The TURN server on the Expressway-E relays the media from the Jabber Guest client, across the traversal zone, to the B2BUA on the Expressway-C.
4. The media then flows between the B2BUA and the internal endpoint / bridge.

Note:

- Because the media hairpins between the two Expressway-E NICs, the TURN traffic and SIP traffic must reside on the same Expressway-E server. You must configure the static NAT address, DMZ external address, and DMZ internal address of the Expressway-E on the Cisco Jabber Guest server.
- If the Expressway-E is behind a NAT, extra configuration is required on the Cisco Jabber Guest server to avoid the media flowing to the static NAT address. Turn on **Static NAT mode** and configure the static NAT address and DMZ external address of the Expressway-E on the Jabber Guest server. This allows media to be sent to the DMZ external address of the Expressway-E, avoiding NAT reflection on the outside firewall.

See also:

- Jabber Guest Licensing and Call Capacity, page 7 for licensing requirements.
- Configure your Firewall for Jabber Guest Traffic, page 25 for full information about port requirements.

Configure your Firewall for Jabber Guest Traffic

This section summarizes the ports that need to be opened for Jabber Guest traffic on the firewalls between your internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located) and between the DMZ and the public internet.

Note:

- HTTP and HTTPS traffic from Jabber Guest clients in the internet is sent to ports 80 and 443 TCP respectively. Therefore the firewall between the Expressway-E and the public internet must translate destination port 80 to 9980 and destination port 443 to 9443 for all TCP traffic that targets the Expressway-E address.
- The Expressway-E redirects HTTP requests on port 9980 to HTTPS on 9443.
- 80/443 TCP are the standard HTTPS administration interfaces on the Expressway, so you need to change the HTTPS administration port if external systems are managing the Expressway-E (not recommended).
- You also need to ensure that appropriate DNS records exist so that the Jabber Guest client can reach the Expressway-E. The FQDN of the Expressway-E in DNS must include the Jabber Guest domain, so in this case it could be `expressway.example.com`. Use round-robin DNS if it is a cluster of Expressway-Es.

  Note that this is public DNS configuration and it does not impose any configuration requirements on the Expressway-E itself (host name / domain name on the DNS page, or the cluster name etc.)

Single NIC Deployment

Table 4 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)*
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-EPrivate IP	9980‡
To avoid port conflicts, traffic to Expressway-E public:443 must NAT&PAT to private:9443			TLS	Expressway-EPrivate IP	9443‡
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†	Expressway-E Public IP	24000-29999	UDP	Expressway-C	36000-59999

Table 4 Port Reference for Jabber Guest Single NIC Deployment (continued)

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

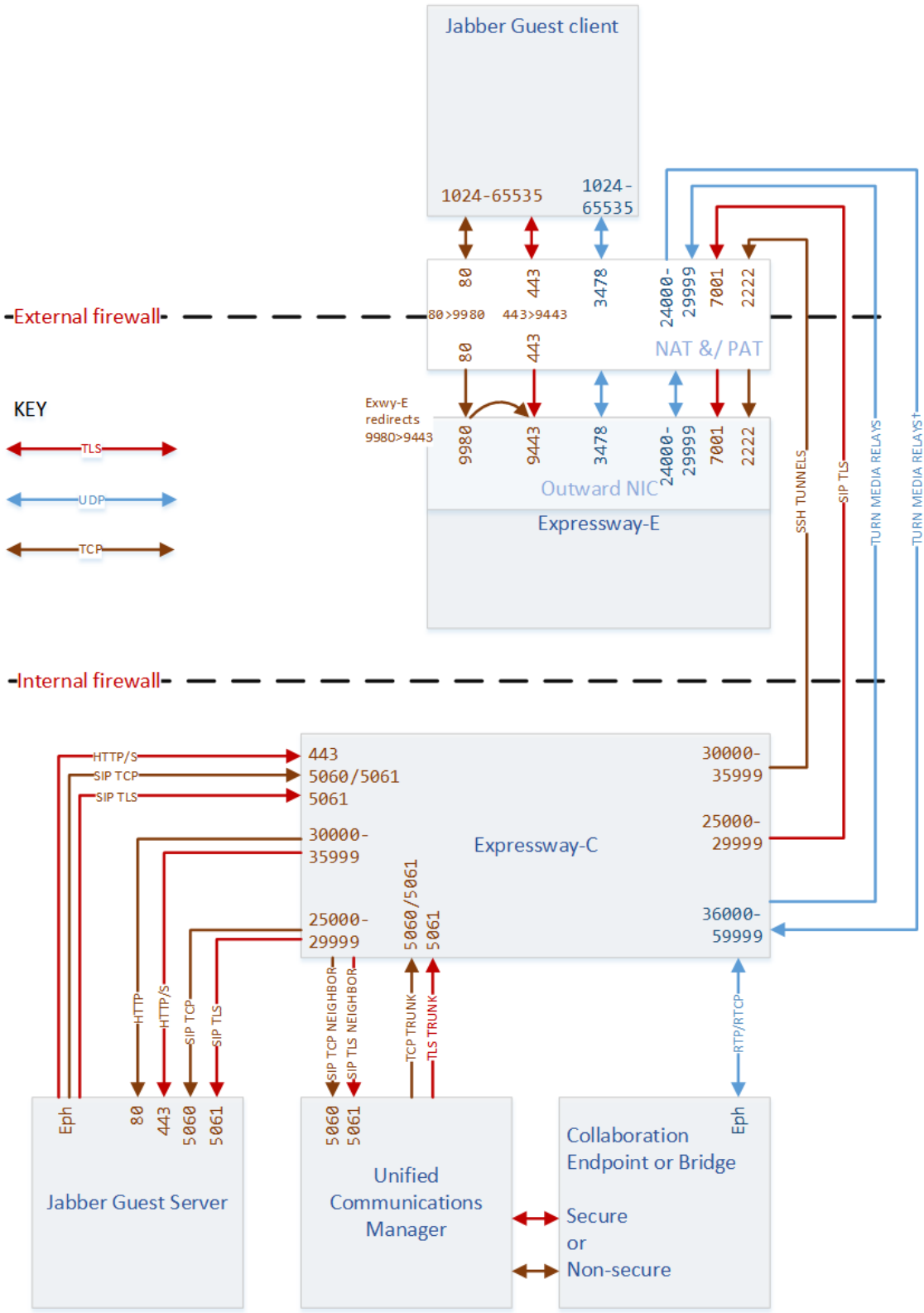
* On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

‡ Port translation in external firewall

† 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:

- Inbound firewall rules are required to allow media to flow from the Expressway-E to Expressway-C.
- You may find that two-way media can still be established even if the inbound from Expressway-E (DMZ) to Expressway-C (private) firewall rules are not applied. This is because the outbound media creates a pinhole in the firewall; however, these rules are required to support uni-directional media (that it, only from outside to inside).


Jabber Guest client
1024-65535
1024-65535
80
443
3478
24000-29999
7001
2222
External firewall
80>9980
443>9443
NAT &/ PAT
80
443
KEY
TLS
UDP
TCP
Exwy-E redirects 9980>9443
9980
9443
3478
24000-29999
7001
2222
Outward NIC
Expressway-E
SSH TUNNELS
SIP TLS
TURN MEDIA RELAYS
TURN MEDIA RELAYS†
Internal firewall
HTTP/S
SIP TCP
SIP TLS
443
5060/5061
5061
30000-35999
25000-29999
Expressway-C
30000-35999
25000-29999
36000-59999
5060/5061
5061
HTTP
HTTP/S
SIP TCP
SIP TLS
SIP TCP NEIGHBOR
SIP TLS NEIGHBOR
TCP TRUNK
TLS TRUNK
RTP/RTCP
Eph
80
443
5060
5061
Jabber Guest Server
5060
5061
Unified Communications Manager
Collaboration Endpoint or Bridge
Eph
Secure
or
Non-secure

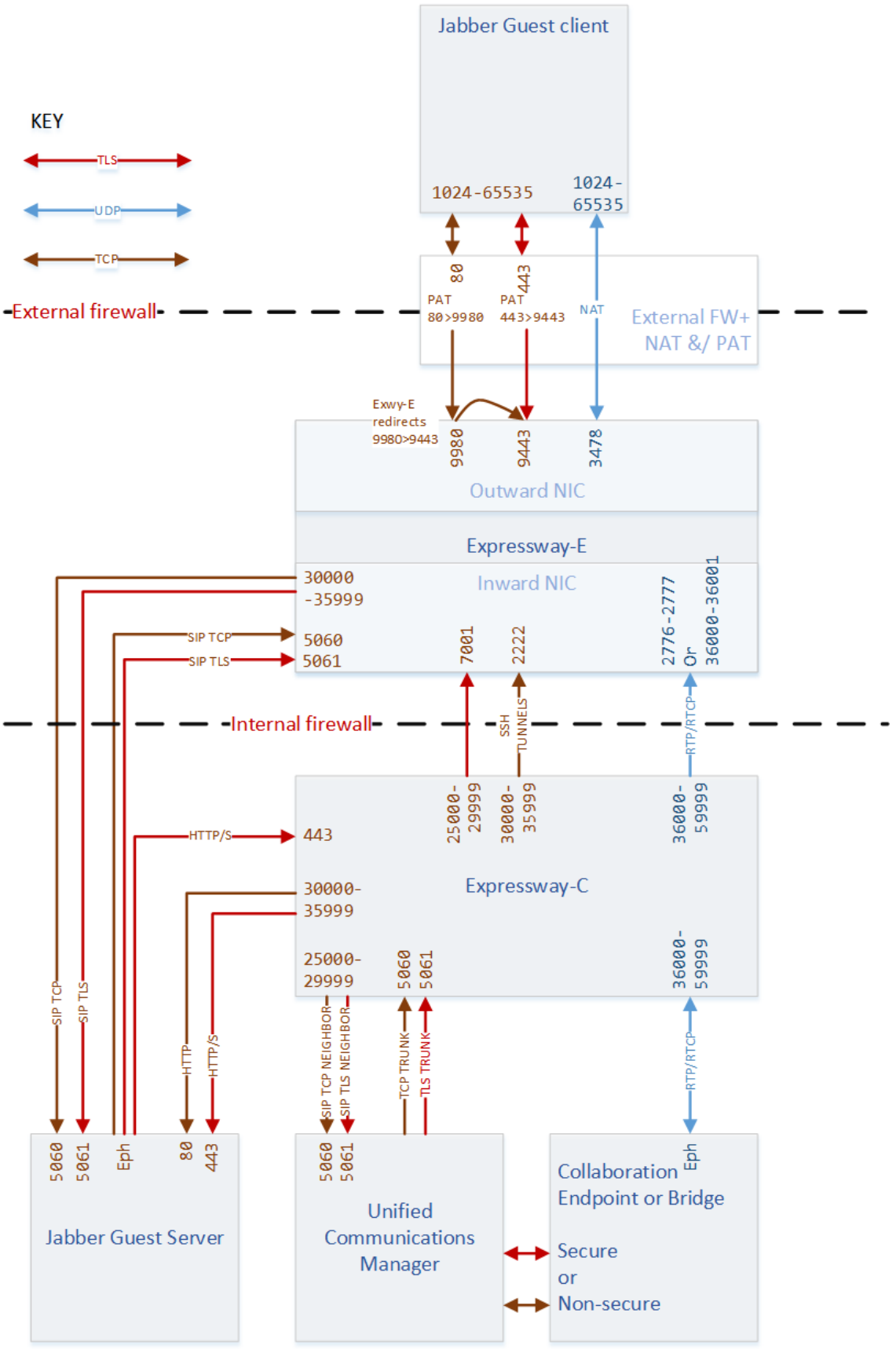
Dual NIC Deployment

Table 5 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-EPrivate IP (Outward NIC)	9980‡
To avoid port conflicts, traffic to Expressway-E public:443 must NAT&PAT to private:9443			TLS	Expressway-EPrivate IP (Outward NIC)	9443‡
Jabber Guest Client Media (TURN)	Any (web browser)	1024-65535	UDP	Expressway-E Public IP	3478 (S/M systems) 3478-3483 (L systems)*
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

* On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

‡ Port translation required


Jabber Guest client
KEY
TLS
UDP
TCP
1024-65535
1024-65535
80
443
PAT 80>9980
PAT 443>9443
NAT
External firewall
External FW+ NAT &/ PAT
Exwy-E redirects 9980>9443
9980
9443
3478
Outward NIC
Expressway-E
30000-35999
Inward NIC
2776-2777 Or 36000-36001
SIP TCP
SIP TLS
5060
5061
7001
2222
Internal firewall
SSH TUNNELS
RTP/RTCP
25000-29999
30000-35999
36000-59999
HTTP/S
443
Expressway-C
30000-35999
25000-29999
5060
5061
36000-59999
SIP TCP
SIP TLS
HTTP
HTTP/S
SIP TCP NEIGHBOR
SIP TLS NEIGHBOR
TCP TRUNK
TLS TRUNK
RTP/RTCP
5060
5061
Eph
80
443
Jabber Guest Server
5060
5061
Unified Communications Manager
Collaboration Endpoint or Bridge
Eph
Secure
or
Non-secure

Troubleshooting Jabber Guest Services on Expressway

Packet loss on calls

Check if the Maximum Transmission Unit (MTU) on Expressway-E is too high. We recommended that you lower the MTU size on the relevant network interfaces from 1500 to 1400 bytes.

Jabber Guest client fails to connect and gets "Not Found on Accelerator" message

This error can occur if:

- The Expressway-E domain is different from the Jabber Guest domain.
- The SIP trunk between the Jabber Guest server and the Expressway-C is not active.

Jabber Guest client fails to connect and gets "Link Not Found" message

This error can occur if:

- The URL being called is wrong.
- The correct URL is being called but it has not been enabled in the Jabber Guest server or it has expired.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)