Cisco Expressway at the Collaboration Edge

Tobias Neumann
Technical Solutions Architect
Cisco Collaboration Central EMEAR
tneumann@cisco.com
Agenda

- Terminology Introduction
- Expressway Mobile & Remote Access Solution Overview
- Product Line Options, Licensing, Scalability
- Design and Deployment Considerations
- Expressway Configuration
- UCM Requirements
- Security
- Expressway Server Certificates
- Closing Remarks
- Q & A
Terminology Introduction
Introducing Cisco Collaboration Edge Architecture
Industry’s Most Comprehensive Any-to-Any Collaboration Solution

All the capabilities of Cisco Any-to-Any collaboration to-date
- TDM & analog gateways
- ISDN Video gateways
- Session border control
- Firewall traversal
- Standards-based & secure

- Mobile Workers
- Teleworkers
- B2B
- 3rd Parties
- Consumers
- Branch Office
- PSTN or IP PSTN
- TDM or IP PBX
- Cloud Services
- Analog Devices
Cisco Expressway
A new gateway solving & simplifying business relevant use cases.

- For Unified CM & Business Edition environments
- Based on Cisco VCS Technology
- Standards-based interoperability
X8.1 Product Line Options

VCS
- "VCS Control" No Change
- "VCS Expressway" No Change
- Specialized video applications for video-only customer base and advanced video requirements
- Superset of X8.1 features
- No changes to existing licensing model

Expressway
- New Offering
- "Expressway C" Or Core
- "Expressway E" Or Edge
- Solution designed for and sold exclusively with UCM 9.1 and above
- Subset of X8.1 features
- No additional cost for server software licenses for UCM 9.1+ customers
Collaboration Edge
umbrella term describing Cisco’s entire collaboration architecture for edge
... features and services that help bridge islands to enable any to any collaboration...
...collaborate with anyone anywhere, on any device....

Cisco VCS
Existing product line option providing advanced video and TelePresence applications
Includes VCS Control and VCS Expressway

Cisco Expressway
New product line option for UCM customers, providing firewall traversal & video interworking
Includes Expressway Core and Expressway Edge

Mobile and Remote Access
Feature available on both VCS and Expressway product lines with X8.1 s/w
Delivers VPN-less access to Jabber and Fixed Endpoints
Expressway Mobile & Remote Access Solution Overview
Mobile and Remote Collaboration with Expressway

- **Inside firewall (Intranet)**
- **DMZ**
- **Outside firewall**
- **Internet**
- **Fixed Remote Endpoints (TC Series)**

- **Collaboration Services**
- **UCM**
- **Expressway**
- **Expressway C**
- **Expressway E**

**Jabber @**
- **work**
- **SFO, LHR**
- **Home**
- **the café**
- **SFO, LHR or PVG**

**Simple, Secure Collaboration:**
It just works...inside and outside the network, no compromises.

**Easy to use, easy to deploy:**
Works with most firewall policies.

**True Hybrid:**
Supports on-premise and cloud offerings simultaneously.

**Standards-based Interoperability, Widely Adopted Protocols**

**Application Driven Security:**
Allow the application to establish security associations it needs.

**Expressway**

**Mobile and Remote Collaboration with Expressway**
Cisco Jabber Remote Access Options

- Layer 3 VPN Solution
- Secures the entire device and its contents
- AnyConnect allows users access to any permitted applications & data

- New Complementary Offering
- Session-based firewall traversal
- Allows access to collaboration applications ONLY
- Personal data not routed through enterprise network
What can a Jabber client do with Expressway?
A fully featured client outside the network

- Make voice and video calls
- Instant Message and Presence
- Access visual voicemail
- Search corporate directory
- Launch a web conference
- Share content
- Inside firewall (Intranet)
- DMZ
- Outside firewall (Public Internet)
- Collaboration Services
- Unified CM
- Expressway C
- Expressway E
- Internet
- Make voice and video calls
- Search corporate directory
Expressway Firewall Traversal Basics

1. **Expressway E** is the traversal server installed in DMZ. **Expressway C** is the traversal client installed inside the enterprise network.

2. **Expressway C** initiates traversal connections outbound through the firewall to specific ports on **Expressway E** with secure login credentials.

3. Once the connection has been established, **Expressway C** sends keep-alive packets to **Expressway E** to maintain the connection.

4. When **Expressway E** receives an incoming call, it issues an incoming call request to **Expressway C**.

5. **Expressway C** then routes the call to **UCM** to reach the called user or endpoint.

6. The call is established and media traverses the firewall securely over an existing traversal connection.
X8.1 Firewall Traversal Capabilities Expanded

The X8.1 release delivers 3 key capabilities enabling the Expressway Mobile and Remote Access feature

- XCP Router for XMPP traffic
- HTTPS Reverse proxy
- Proxy SIP registrations to UCM

(details on new firewall port requirements covered later)
# Solution Components Software Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Min Software Version</th>
<th>Projected Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Expressway or Cisco VCS</td>
<td>X8.1</td>
<td>Available</td>
</tr>
<tr>
<td>Cisco Expressway or Cisco VCS</td>
<td>X8.1.1 (MR)</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>UCM</td>
<td>9.1(2) SU1</td>
<td>Available</td>
</tr>
<tr>
<td>UCM IM&amp;P</td>
<td>9.1</td>
<td>Available</td>
</tr>
<tr>
<td>Unity Connection</td>
<td>8.6(1)</td>
<td>Available</td>
</tr>
<tr>
<td>Jabber for Windows</td>
<td>9.7</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>Jabber for iOS</td>
<td>9.6.1</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>Jabber for MAC</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>Jabber for Android</td>
<td>9.6</td>
<td>Q1CY14</td>
</tr>
<tr>
<td>EX/MX/SX/C Series TelePresence Endpoints</td>
<td>TC7.0.1</td>
<td>Available</td>
</tr>
</tbody>
</table>
Product Line Options, Licensing, Scalability
X8.1 Product Line Options

VCS

- “VCS Control” No Change
- “VCS Expressway” No Change

• Specialized video applications for video-only customer base and advanced video requirements
• Superset of X8.1 features
• No changes to existing licensing model

Expressway

- New Offering
- “Expressway C” Or Core
- “Expressway E” Or Edge

• Solution designed for and sold exclusively with UCM 9.1 and above
• Subset of X8.1 features
• No additional cost for server software licenses for UCM 9.1+ customers
# VCS and Cisco Expressway Feature Comparison

<table>
<thead>
<tr>
<th>Feature Comparison</th>
<th>Cisco Expressway Series</th>
<th>Cisco VCS Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and Remote Access</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business to Business Video</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business to Consumer / Public to Enterprise Access with Jabber Guest</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video Interworking (IPv4 to IPv6, H.323-SIP, MS H.264 SVC-AVC, Standards-based 3rd Party Video endpoints)</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video / TelePresence Device Registration &amp; Provisioning</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Video Session Management &amp; Call Control</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>WebEx Enabled TelePresence</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Enhanced Security (e.g. JITC)</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
Cisco Expressway Licensing

Fixed and Mobile Users at no additional cost

- Mobile and Fixed Endpoint registration
- IM & Presence
- Video and Audio Media Sessions
- Includes Virtual Edition Expressway Server Software
- No Cost with UCM 9.1.2 or later

Business to Business, Jabber Guest, 3rd party interworking – Concurrent Sessions

- Business to Business Video and Audio Media Sessions
- Includes Virtual Edition Expressway Server Software
- Expressway Rich Media Session licenses available à la carte
Calls from endpoints using the Mobile and Remote Access feature are classified as **Unified CM calls**.

Unified CM calls do not consume Rich Media Sessions (Expressway) or Traversal Licenses (VCS).

But Unified CM Calls do count against the overall system capacity.
Flexible Call Licensing

- X8.1 introduces audio-only classification for SIP traversal or Unified CM calls
- Calls with only one m= line in the SDP will be classified as Audio calls
- 1 Expressway Rich Media Session license allows either 1 video call or 2 audio-only SIP calls
- 1 VCS Traversal license allows either 1 video call or 2 audio-only SIP calls
- Example: 100 VCS Traversal licenses allows for 90 video and 20 audio-only simultaneous calls
New Compute Platforms for X8

Specs Based
Virtual Machine Support

<table>
<thead>
<tr>
<th>OVA Size</th>
<th>vCPU</th>
<th>Reserved RAM</th>
<th>Disk Space</th>
<th>vNIC(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>2 x 1.8 GHz</td>
<td>4GB</td>
<td>132GB</td>
<td>1Gb</td>
</tr>
<tr>
<td>Medium</td>
<td>2 x 2.4 GHz</td>
<td>6GB</td>
<td>132GB</td>
<td>1Gb</td>
</tr>
<tr>
<td>Large</td>
<td>8 x 3.3 GHz</td>
<td>8GB</td>
<td>132GB</td>
<td>10Gb</td>
</tr>
</tbody>
</table>

Appliance Support

Existing VCS Appliance

- New appliances based on UCS C220 M3
- Bare metal – no hypervisor
- Fixed configurations for high and low end deployment
- Solution for customers with security policies that do not allow VMware in the DMZ
- CE500 Single components, 1Gbps interfaces
- CE1000 Redundant components, 1 or 10Gbps
- Target FCS Q1 CY2014
## Expressway X8.1 Scalability

<table>
<thead>
<tr>
<th>Platform</th>
<th>Server</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proxied Registrations</td>
<td>Video Calls</td>
</tr>
<tr>
<td>Large OVA</td>
<td>5,000</td>
<td>500</td>
</tr>
<tr>
<td>Medium OVA</td>
<td>2,500</td>
<td>100</td>
</tr>
<tr>
<td>Small OVA (BE6K)</td>
<td>2,500</td>
<td>100</td>
</tr>
<tr>
<td>VCS Appliance</td>
<td>2,500</td>
<td>100</td>
</tr>
</tbody>
</table>

Note: Expressway C&E or VCS-C can be clustered across multiple BE6000s for redundancy purposes, but with no additional scale benefit.
Expressway Rich Media Session Licenses

- Rich Media Session is the only session license type sold with Expressway (simple!)
- Rich Media Session licenses are consumed for either traversal or non-traversal call types
- A traversal call will require a Rich Media Sessions license on both the Expressway E and Expressway C
- Mobile and Remote Access Feature has no requirements for Rich Media Sessions licenses
- Rich Media Sessions should be purchased for Expressways deployed for
  - B2B Video
  - Jabber Guest
  - 3rd party video interworking
## Expressway License Keys

<table>
<thead>
<tr>
<th>License Description</th>
<th>PID</th>
<th>Expressway C (EXPWY-VE-C-K9)</th>
<th>Expressway E (EXPWY-VE-E-K9)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X8 Release Key</td>
<td>LIC-SW-EXP-K9</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Expressway Series</td>
<td>LIC-EXP-SERIES</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>H323-SIP interworking Gateway</td>
<td>LIC-EXP-GW</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Traversal Server Feature Set</td>
<td>LIC-EXP-E</td>
<td>N/A</td>
<td>Included</td>
</tr>
<tr>
<td>Advanced Networking Option</td>
<td>LIC-EXP-AN</td>
<td>N/A</td>
<td>Included</td>
</tr>
<tr>
<td>TURN Relay Option</td>
<td>LIC-EXP-TURN</td>
<td>N/A</td>
<td>Included</td>
</tr>
</tbody>
</table>
Design and Deployment Considerations
Expressway & Jabber Service Discovery

Inside firewall (Intranet)  DMZ  Outside firewall (Public Internet)

Collaboration Services  UCM  Expressway C  Expressway E  Public DNS

Jabber Service Discovery Response Priority
1. _xmpp_client SRV response
2. Result of http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
3. _cisco-uds SRV response
4. _collab-edge SRV response

Cisco Jabber Client

DNS SRV lookup _cisco-uds._tcp.example.com
  Not Found

expwyNYC.example.com

DNS SRV lookup _collab-edge._tls.example.com

HTTPS: get_edge_config?
  service_name=_cisco-uds&service_name=_cuplogin
Split DNS SRV Record Requirements

- `_collab-edge` record needs to be available in **Public** DNS
- Multiple SRV records (and Expressway E hosts) can be deployed for HA
- A GEO DNS service can be used to provide unique DNS responses by geographic region

```plaintext
_collab-edge._tls.example.com. SRV 10 10 8443 expwy1.example.com.
_collab-edge._tls.example.com. SRV 10 10 8443 expwy2.example.com.
```

- `_cisco-uds` record needs to be available only on **internal** DNS (available to Expressway C at a minimum)

```plaintext
_cisco-uds._tcp.example.com. SRV 10 10 8443 ucm1.example.com.
_cisco-uds._tcp.example.com. SRV 10 10 8443 ucm2.example.com.
```
Reverse proxy usage

Initial get_edge_config and internal SRV record request (decrypted)
GET /dWNkZW1vbGFiLmNvbQ/get_edge_config?service_name=cisco-uds&service_name=cuplogin HTTP/1.1
Authorization: Basic bWR1ZGU6dGhpc3Bhc3N3ZHdpbGxiZXJlc2V0
Host: collabedge1e.ucdemolab.com:8443
Accept: */*
User-Agent: Jabber-Win-472

Base64 encoded credentials
Base64 decode = ucdemolab.com

Subsequent home cluster discovery request (decrypted)
GET /dWNkZW1vbGFiLmNvbS9odHRwcy9jdWNtLXB1Yi51Y2RlbW9sYWIuY29tLzg0NDM/cucm-uds/clusterUser?
username=mdude HTTP/1.1
Host: collabedge1e.ucdemolab.com:8443
Accept: */*
Cookie: X-Auth=7f501814-e61f-483a-8620-ed0b5d3792db
User-Agent: Jabber-Win-472

Base64 decode = ucdemolab.com/https/cucm-pub.ucdemolab.com/8443

X-Auth token

Not a general purpose reverse proxy, intended for Cisco clients only!
Expressway C will use the following UDS API to determine a user’s home cluster:
https://<UCM>/cucm-uds/clusterUser?username=<USERNAME>

  <result version="10.0.1" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/user/mjackson" found="true"/>
  <homeCluster>cucm2-1.eft.cisco.com</homeCluster>
</clusterUser>

- <clusterUser version="10.0.1" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/clusterUser?username=mjackson">
  <result found="true" uri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/user/mjackson" version="10.0.1"/>
  <homeCluster serversUri="https://cucm2-1.eft.cisco.com:8443/cucm-uds/servers">cucm2-1.eft.cisco.com</homeCluster>
  <homeClusterDetails>
    <selfProvisioningSecureMode>true</selfProvisioningSecureMode>
    <adminProvisionMode>false</adminProvisionMode>
  </homeClusterDetails>
</clusterUser>
Protocol Workload Summary

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Security</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP</td>
<td>TLS</td>
<td>Session Establishment – Register, Invite, etc. via UCM</td>
</tr>
<tr>
<td>Media</td>
<td>SRTP</td>
<td>Audio, Video, Content Share, Advanced Control</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TLS</td>
<td>Logon, Provisioning/Configuration, Contact Search, Visual Voicemail</td>
</tr>
<tr>
<td>XMPP</td>
<td>TLS</td>
<td>Instant Messaging, Presence</td>
</tr>
</tbody>
</table>

Inside firewall (Intranet) | DMZ | Outside firewall (Public Internet)
Hybrid Deployment - Cloud based IM&P

Inside firewall (Intranet) | DMZ | Outside firewall (Public Internet)

Unified CM | Expressway C | Expressway E

Internet

Protocol
- SIP
- Media
- HTTPS
- XMPP

Security
- TLS

Service
- Session Establishment – Register, Invite, etc. via UCM
- Audio, Video, Content Share, Advanced Control
- Logon, Provisioning/Configuration, Contact Search, Visual Voicemail
- Instant Messaging, Presence
Contact Search Considerations (Cloud based IM&P)

- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to UCM
- Corporate directory is also exported to WebEx Messenger cloud
- All Jabber clients will use WebEx Messenger cloud as a contact source for contact search
Contact Search Considerations (on-premise IM&P)

- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to UCM
- User Data Services (UDS) is a UCM RESTful API allowing for contact search, among other things
- All Jabber clients connecting via Expressway will use UDS for contact search
- Jabber clients deployed on-premise will use LDAP for directory search
- Jabber clients will automatically use UDS for directory search when connecting via Expressway
- The entire corporate directory needs to be sync’d on every UCM cluster for best contact search experience
Media Path Summary

UCM provides call control for both mobile and on-premise endpoints

Media Traversal
- “C” calls “A” on-premise
- Expressway solution provides firewall traversal for media
- Expressway C de-multiplexes media and forwards toward “A”

Media Relay
- “C” calls “B” off-premise
- Media is relayed via Expressway C

Optimized Media (roadmap ICE support)
- “B” calls “D” off-premise
- Both “B” and “D” are ICE-enabled
- STUN binding success
- Media flows are optimized between endpoints
Expressway Clustering, 4+2

- Cluster Expressways for scale and redundancy
- Expressway Clusters support up to 6 peers
- Expressway E and C node types cannot be mixed in the same cluster
- Deploy equal number of peers in Expressway C and E clusters
- Deploy same OVA sizes throughout cluster
- Expressway remote access is limited to one customer domain per cluster
- However customers can deploy multiple clusters for the same customer domain
### Mobile & Remote Access Deployment Options

Customer domain shared across all UCM & IM&P clusters

<table>
<thead>
<tr>
<th>UCM Clusters</th>
<th>Expressway C Clusters</th>
<th>Expressway E Clusters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Single Expressway deployment providing remote access to a central UCM cluster</td>
</tr>
<tr>
<td>1</td>
<td>2+</td>
<td>2+</td>
<td>Regional Expressway deployments providing remote access to a central UCM cluster</td>
</tr>
<tr>
<td>2+</td>
<td>1</td>
<td>1</td>
<td>Single Expressway deployment providing remote access to a multiple UCM clusters</td>
</tr>
</tbody>
</table>
Global Deployment Topology & Geo DNS

DNS SRV lookup
_collab-edge._tls.example.com

US

Europe

Asia

Expressway edge access

SME global aggregation

UCM regional clusters

US SME

EU SME

Asia SME

expwy.us.example.com

expwy.uk.example.com

expwy.jp.example.com

Geo DNS

SIP Trunk
SIP Line
Expressway Traversal
Unsupported Features
Mobile & Remote Access

- CTI phone control
- CAPF client certificate provisioning
- Jabber file transfer (supported only in hybrid IM&P deployment)
- Jabber Mobile features include DVO-R, GSM handoff, session persistency
- TC Endpoint OBTP
- TC Endpoint management (SNMP, SSH/HTTP access)
- Media Path Optimization (ICE)
Unsupported: Unbalanced Expressway Deployments

- This model is still supported for traditional VCS Expressway deployments
- But this is not supported for the new mobile and remote access functionality introduced in X8.1
- Expressway X8.1 remote access requires a Expressway C cluster for each Expressway E cluster
- Only one “Mobile & Remote Access” enabled Traversal zone per cluster
Chained traversal is often used in environments with heightened security policies.

This option is still supported for traditional VCS deployments, or Expressway deployments do not require the remote and mobile access feature.

Not supported for the new mobile and remote access functionality introduced in X8.1.

Only one “Mobile & Remote Access” enabled Traversal zone per cluster.
Existing VCS Customers

- Customers with VCS-C and VCS-E can add Mobile and Remote Access to an existing deployment
- Simply add a parallel traversal zone on existing VCSs to support mobile and remote access
- Ideal for mid-market customers, POCs, or pilot programs
- Concurrent session scale is the primary reason for adding Expressways dedicated to Mobile & Remote access
  Will the number of remote Jabber users making calls over Expressway crush my existing TelePresence deployment?
- The difference in security posture between B2B video and remote access solutions is another consideration
  Does it makes sense for the customer to combine these solutions on the same VMs?
Parallel Deployments of VCS & Expressway

_collab-edge SRV records don’t conflict with existing VCS SRV record usage

Add _collab-edge SRV to Public DNS

- B2B Video SIP & H.323 (inbound & outbound)
- Cisco Jabber Video for TelePresence Registration
- Cisco TelePresence Endpoints (TC) Registration to VCS
- WebEx Enabled TelePresence (outbound)
AnyConnect & Expressway Coexistence

- Customers that have deployed AnyConnect can also deploy Expressway Mobile & Remote Access feature
- For the best end user experience, prevent all Jabber traffic from using the AnyConnect tunnel
  - 😞 Active calls going through Expressway will be dropped if AnyConnect tunnel is established mid-call
- 😊 Expressway can provide Jabber client access to on-prem collaboration services even with an active AnyConnect tunnel established
- Requirements to keep Jabber traffic going through Expressway
  1. AnyConnect split tunnel providing connectivity to internal enterprise network **only** (not including Expressway E)
  2. Deny access (ASA DNS inspection) to the internal DNS SRV records (_cisco-uds & _cuplogin) to AnyConnect clients
Expressway Configuration
Expressway Configuration Summary

- Enable Mobile & Remote Access feature, Configuration > Unified Communications
- Provide IM&P Publisher address and supply admin credentials for each IM&P cluster (not required for hybrid deployments)
- Provide UCM Publisher address and supply admin credentials for each UCM cluster
  - Expressway C connects to each Publisher and discovers all cluster nodes
  - Neighbor Zone auto-generated for each UCM node
  - Search Rules auto-generated for each UCM node
- Add the customer domain and select services
- Generate certificate signing requests and procure CA signed certs
- Configure Traversal Zone with Mobile & Remote Access feature enabled
Expressway C Domain Configuration

- Note: no domains configuration required on Expressway E
## Expressway E Traversal Server Zone

**Edit zone**

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Hop count</td>
</tr>
</tbody>
</table>

**Connection credentials**

<table>
<thead>
<tr>
<th>Username</th>
<th>traversal</th>
</tr>
</thead>
</table>

**H.323**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Off</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Assert</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>H.460.19 demultiplexing mode</th>
<th>Off</th>
</tr>
</thead>
</table>

**SIP**

<table>
<thead>
<tr>
<th>Mode</th>
<th>On</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>7001</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Transport</th>
<th>TLS</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Mobile and remote access</th>
<th>Yes</th>
</tr>
</thead>
</table>

**Authentication**

<table>
<thead>
<tr>
<th>Authentication policy</th>
<th>Do not check credentials</th>
</tr>
</thead>
</table>

**UDP / TCP probes**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>

| UDP retry interval             | 2     |
| UDP retry count                | 5     |
| UDP keep alive interval        | 20    |
| TCP retry interval             | 2     |
| TCP retry count                | 5     |
| TCP keep alive interval        | 20    |

*TLS verify mode* | On |

*TLS verify subject name* | cluster.collabsedge1c.ucdmerlab.com |

*Media encryption mode* | Force encrypted |

*ICE support* | On |

*Poison mode* | Off |

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public
Allowed Reverse Proxy Traffic

- Expressway E server will be listening on TCP 8443 for HTTPS traffic
- Basic mobile & remote access configuration allows inbound authenticated HTTPS requests to the following destinations on the enterprise network
  - All discovered UCM nodes TCP 6970 (TFTP file requests) & TCP 8443 (UDS API)
  - All discovered IM&P nodes TCP 7400 (XCP Router) & TCP 8443 (SOAP API)
- HTTPS traffic to any additional hosts need to be administratively added to the Expressway C allow list

<table>
<thead>
<tr>
<th>Server hostname</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuc2.ucdemolab.com</td>
<td>CUC2 FGDN</td>
<td>View/Edit</td>
</tr>
<tr>
<td>cuc1.ucdemolab.com</td>
<td>CUC1 FGDN</td>
<td>View/Edit</td>
</tr>
</tbody>
</table>

- Provides a mechanism to support Visual Voice Mail access, contact photo retrieval, Jabber custom tabs, etc.
# Expressway C Unified Communications Status

Status > Unified Communications

## Unified Communications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Jabber Guest support</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unified Communications services</td>
<td>Active</td>
</tr>
<tr>
<td>IM and Presence servers</td>
<td>2</td>
</tr>
<tr>
<td>Unified CM servers</td>
<td>3</td>
</tr>
<tr>
<td>Current provisioned sessions</td>
<td>0</td>
</tr>
<tr>
<td>Total provisioning requests since last restart</td>
<td>0</td>
</tr>
<tr>
<td>Total provisioned sessions since last restart</td>
<td>0</td>
</tr>
<tr>
<td>Unified CM calls</td>
<td>Current video: 0, Current audio (BIP): 0</td>
</tr>
</tbody>
</table>

## Domains

<table>
<thead>
<tr>
<th>Name</th>
<th>Services</th>
<th>Associated zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>cc.uctdmdlab.com</td>
<td>Unified CM registrations, IM and Presence</td>
<td>Traversal Client MRA</td>
</tr>
<tr>
<td>uctdmdlab.com</td>
<td>Unified CM registrations, IM and Presence, Jabber Guest</td>
<td>Traversal Client MRA</td>
</tr>
</tbody>
</table>

## Zones

<table>
<thead>
<tr>
<th>Name</th>
<th>SIP status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traversal Client MRA</td>
<td>Active</td>
</tr>
</tbody>
</table>

## Advanced status information

- View provisioning sessions
- View with tunnel status
UCM Requirements
Expressway Remote Access from UCM Perspective

- Remote access provided by Expressway is, for the most part, transparent to UCM
- Think SIP line integration, versus SIP trunk
- No requirement to build a SIP trunk on UCM to Expressway C or E
- No requirement to make dial plan changes
- No remote access policy mechanism to limit edge access to certain Jabber users or devices
- Remote Jabber clients or TelePresence Endpoints registering to UCM through Expressway will appear to UCM as Expressway-C IP address (opportunity for UCM Device Mobility feature usage)
Interaction with SIP trunk

- SIP trunk is **not required** between Expressway C (or VCS-C) and UCM for Mobile & Remote Access deployment.

- However, if UCM includes a SIP trunk for other integrations, **UCM will reject any SIP registration attempts from remote Jabber or TP endpoints**, as the register method is not accepted on UCM SIP trunk interface.

- Update UCM SIP trunk security profile to listen on ports other than TCP 5060 or 5061 (you could use 5560, 5561, etc.).

- Port change allows for SIP trunk integration + mobile & remote access.

SIP 405 will be returned to SIP Register request if there is SIP trunk port conflict.
UDS Directory Search

- All Jabber clients connecting via Expressway will use UDS for directory search (assuming UCM IM&P deployment)
- TelePresence endpoints always use UDS for directory search
- For the best contact search experience, all Enterprise Users should be imported into every UCM cluster’s end user table
- Home cluster check box needs to be selected on only one cluster for each user

- UCM clusters support 80K end users, and can scale as high as 160K with BU megacluster approval
Pre-requisites to supporting multiple UCM Clusters

- Cross cluster UDS API calls are used to find Jabber user’s home cluster
  https://<ucm>/cucm-uds/clusterUser?username=mdude
- Intercluster Lookup Service (ILS) networking needs to be established
  enterprise UCM clusters to allow for UCM cluster discovery
- SIP URI replication over ILS is optional, not a requirement
- UCM Tomcat certificates need to be exchanged between UCM clusters for
  UDS clusterUser API calls to work
UCM Bulk Certificate Management

- Tool used to simplify UCM Cluster certificate exchange
- All Clusters export TFTP (CallManager), Tomcat, and CAPF certificates to central SFTP server
- Certificates are consolidated into PKCS12 files
- Consolidated set of certificates are then imported to each publisher
- Cisco Certificate Change Notification Service replicates trusted certificates throughout the cluster
External NTP source for TC endpoints

- TC endpoints registered to UCM will try to use UCM as an NTP server
- NTP is not supported over Expressway Traversal, so use an external reference instead

1. Create a new Phone NTP Reference pointing to a public NTP server
2. Create a Date/Time Group using the public NTP reference
3. Apply to remote TC7 endpoints’ device pool
Firewall Port Details

- **No inbound ports required to be opened on the internal firewall**

- Internal firewall needs to allow the following outbound connections from Expressway C to Expressway E
  - SIP: TCP 7001
  - Traversal Media: UDP 36000 to 36011
  - XMPP: TCP 7400
  - HTTPS (tunneled over SSH between C and E): TCP 2222

- **External firewall needs to allow the following inbound connections to Expressway**
  - SIP: TCP 5061
  - HTTPS: TCP 8443
  - XMPP: TCP 5222
  - Media: UDP 36002 to 59999
  - TURN server control: UDP 3478 – 3483
  - TURN server media: UDP 24000 – 24999

  Jabber Guest, not required for Mobile & Remote Access
Media Port Range Expansion

- X8.1 scalability improvements require a media port range expansion
- X8.1 default media Port Range is now UDP 36000 – 59999
- VCS systems upgraded from X7 to X8.1 will need to manually update port range, Configuration > Local Zone > Traversal Subzone
Traversal Media Port Changes

Important change for existing VCS customers to understand

- X7 release included the ability to configure the Expressway Media demultiplexing RTP port and RTCP port
- Upon upgrading to X8.1 the traversal media ports are automatically migrated to the first 2 ports in the current media port range (details on previous slide)
- Customers will need to coordinate X8.1 upgrade with firewall port change
- New X8.1 installs on the Large OVA will use UDP 36000 – 36011, the expanded port range is required to support scalability improvements

Configuration Removed in X8.1
Client Authentication at the Edge

HTTPS
- Clients supply base64 encoded username and password to authenticate over HTTPS
  Authorization: Basic bWR1ZGU6dGhpc3Bhc3N3ZHdpbGxiZXJlc2V0
- Credentials are forwarded to Expressway C and then used to authenticate against UCM, upon determination of the user’s home cluster
- Upon successful authentication, X-Auth token provided for future HTTPS requests (8 hour lifetime)
  Cookie: X-Auth=7f501814-e61f-483a-8620-ed0b5d3792db

SIP
- SIP Digest authentication used to authenticate the users registering on tcp 5061
- Mutual TLS can be enforced on Expressway E by enabling default zone access rules
Edge Server Authentication

- No matter which client authentication model is deployed, server authentication is always performed by the remote device.
- i.e. remote Jabber clients and remote endpoints will always validate the Expressway E Server Certificate presented in the TLS handshake.
- Jabber Clients will rely on the underlying platform trusted CA list.
- TelePresence Endpoints will rely on a trusted CA list included in firmware.
- No CTL requirement for Edge Server authentication.
Expressway Server Certificates
Expressway Server Certificates

- Expressway E Server certificates should be signed by 3rd party Public CA
- Expressway C server certificates can be signed by 3rd party Public CA or Enterprise CA
- Expressway server certificates need to allow for both client & server authentication
  - Public CA signed certificates allow Jabber clients and endpoints to validate the server certificate without a CTL
  - Jabber clients with a CTL will not use the CTL to validate Expressway certificate - no requirement to include Expressway certs in CTL
- No support for wildcard certificates
- Don’t upload stacked certificates, separate signed server cert from CA chain
Expressway Certs and Clustering

- Set a cluster name (System > Clustering) even when starting with a single node
- Generate server certificate CSR with Common Name set to “FQDN of VCS Cluster”
- Build Expressway E Traversal Server zone with the “TLS verify subject name” set to “Cluster FQDN”
Expressway Certificate Signing Request (CSR)

Maintenance > Security Certificates > Server Certificate

Click **Generate CSR**

to load this page ----->
Cert Subject Alternative Name (SAN) requirements

- Customer’s primary domain required to be included as a DNS SAN in all Expressway E server certificates.
- Primary domain as in example.com or cisco.com or example.com or cisco.com or cisco.com.
- This domain is used for SRV lookups and extracted from here.
- This is a security measure that allows clients to verify connections to edge servers authoritative for their domain (RFC 6125).
- Similar usage exists with UCM IM&P XMPP certificates.
UCM Mixed Mode & Expressway SANs

- Expressway C Server Certificate Generation CSR page will also include the option to include UCM security profile names as additional SANs

![DNS X509v3 Subject Alternative Name: DNS:secure.ex90.ucdemolab.com]

- This is **only required in deployments that include encrypted security profiles** (requires UCM to be in mixed mode with CTL deployed)

- The Expressway C server certificate will be presented to UCM during the TLS handshake on behalf of remote endpoints with encrypted security profiles

- UCM needs to find a match between the Expressway certificate’s CN or SAN and the phone security profile name to authorize the TLS registration on TCP 5061

- UCM phone security profile names cannot be shared across device types
Optional SANs for future usage

- The Expressway Server Certificate Generate CSR page will also insert “chat node aliases” as SANs
- These specific SANS will allow for TLS XMPP federation

There will be 1 chat node alias per deployed UCM IM&P server
Expressway XMPP federation is still a roadmap feature, but this inclusion will potentially save customers from having to get new certificates signed in the future when deploying XMPP federation
Expressway Trusted CA Certificates

- Trusted CA certificates can now be viewed in either a decoded human-readable format, or in base64 encoded PEM format.
- X8.1 release will **not** include the default trusted CA certificate list.
- VCS customers upgrading from X7 or prior should consider purging this list.

<table>
<thead>
<tr>
<th>Trusted CA certificate</th>
<th>You are here: Maintenance » Security certificates » Trusted CA certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Issuer</td>
</tr>
<tr>
<td>Certificate</td>
<td>O=Digital Signature Trust Co., CN=DST Root CA X3</td>
</tr>
<tr>
<td>Certificate</td>
<td>O=Cisco, OU=CTC-TME, CN=Kroarty-lab</td>
</tr>
<tr>
<td>Certificate</td>
<td>O=Digital Signature Trust Co., CN=DST Root CA X3</td>
</tr>
</tbody>
</table>

**Upload**

Select the file containing trusted CA certificates

[Browse] No file selected.

[Append CA certificate] [Reset to default CA certificate]
### Expressway Trusted CA Certificates

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Expressway C</th>
<th>Expressway E</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public CA cert chain used to sign Expressway E certificate</td>
<td>✔️</td>
<td>✔️</td>
<td>Required to establish Traversal Zone connections</td>
</tr>
<tr>
<td>Public or Enterprise CA cert chain used to sign Expressway C certificate</td>
<td>✔️</td>
<td>✔️</td>
<td>Required to establish Traversal Zone connections</td>
</tr>
<tr>
<td>UCM Tomcat certificates or CA chain</td>
<td>✔️</td>
<td>✗</td>
<td>Only required when Expressway C configured to use TLS Verify mode on Unified CM discovery</td>
</tr>
<tr>
<td>UCM CallManager certificates or CA chain</td>
<td>✔️</td>
<td>✗</td>
<td>Only required when UCM is in mixed mode for end to end TLS</td>
</tr>
<tr>
<td>UCM IM&amp;P Tomcat certificates or CA chain</td>
<td>✔️</td>
<td>✗</td>
<td>Only required when Expressway C configured to use TLS Verify mode on IM&amp;P discovery</td>
</tr>
<tr>
<td>UCM CAPF certificate(s)</td>
<td>✗</td>
<td>✔️</td>
<td>Only required when remote endpoints authenticate with LSC certificate</td>
</tr>
</tbody>
</table>
Closing Thoughts
High Level Deployment Guidance

- Start on solid ground
  - Jabber service discovery needs to work on-prem
  - Start on-prem and then add edge access
  - Verify end user home cluster discovery in multi UCM cluster deployments

- Don’t forget about DNS
  - Understand split DNS SRV requirements, get DNS change requests in the queue
  - A common DNS domain simplifies matters

- Review TCP and UDP port requirements with firewall team

- Verify Expressway CA signed certs
  - Confirm SANs returned in CA signed cert match what was requested in the CSR
  - Verify cert includes both TLS Web Server & Client Authentication Extended Key Usage
Key Takeaways

- Cisco Expressway: a new product offering specifically for UCM 9.1+ customers available today!
- Expressway is easy to deploy with no added costs for mobile & remote users
- Provide simple and secure Jabber VPN-less access with Expressway Mobile & Remote Access
- Cisco VCS includes the superset of X8 software features
- Cisco Expressway includes a subset of X8 software features
- AnyConnect and Expressway are complementary remote access solutions that can co-exist
Q&A