CMUG
Cisco Collaboration Edge Architecture

William Bell
Hao Tran
February 18, 2015
Agenda

Introductions

Collaboration Edge Architecture Overview

Mobile and Remote Access (MRA) Overview

MRA Implementation

Q&A
Introductions

• William Bell, CCIE #38914
  William’s background spans an array of technical disciplines including application
development, network infrastructure, protocol analysis, virtualization, and UC. He leads
the UC&C practice and works with customers on architecting solutions that align with
core business drivers. Bill is a regular contributor on the Cisco Support Community, a 3-
time Cisco Designated VIP, and blogs on the NetCraftsmen and UC Guerrilla sites.

• Hao Tran, CCNP/CCNP-V
  A senior unified communications engineer with over 14 years of experience, with a
deep focus in both VoIP and networking technologies. Hao is a CCNP in both network
and voice and is currently pursuing the CCIE in collaboration. He is part of the
NetCraftsmen senior engineering team and supports customers in deployment,
troubleshooting, and operational readiness.

• Jeff Chun (Cisco), CCNP/CCNP-V
  With 10+ years of experience in Consulting and Sales, Jeff’s drive is to create solutions
that solve business challenges. His focus is on deploying Cisco Collaboration solutions
throughout the Enterprise, Commercial, and Federal space. Currently at Cisco, I work
with partners and customers to provide best in class solutions in our Borderless
Networks, Collaboration and Data Center spaces.
Agenda

Introductions

Collaboration Edge Architecture Overview

Mobile and Remote Access (MRA) Overview

MRA Implementation

Q&A
Collaboration Edge – Solution Overview

**Business to Business (B2B)**
Secure communications with partners, customers & suppliers over the internet
- Video, URI Dialing, Federation

**Business to Consumer (B2C)**
Browser based communications with consumers, interview candidates, potential customers
- Jabber Guest

**Cloud Services**
Flexible and scalable, “pay as you go” shared resources
- WebEx, WebEx Enabled Telepresence

**Mobile and Remote Access**
Ubiquitous user experience – Any Device, Anywhere
- Jabber Mobile & Desktop / TelePresence

**Interoperability**
Investment protection with existing 3rd party and legacy communication solutions
- IPv4-v6, H323-SIP, Standards Based video

NetCraftsmen
Collaboration Edge
Architecture Components

Enterprise
UC Infrastructure

Communications Manager
Expressway-C
Expressway-E
Voice Gateway
CUBE
IM & Presence
Unity Connection
UC Apps
MCU
Conductor

Public Internet
PSTN

Supplementary Services
Call Park
Call Forward
Email
UC Communications Infrastructure

Endpoints

Jabber Clients (Windows, OS X, iOS, Droid)
TelePresence Clients (MRA-Capable)
IP Phones (MRA-Capable)

NetCraftsmen

Copyright 2015
Customer Confidential
Collaboration Edge
Architecture Components

Enterprise
UC Infrastructure

Collab Edge

PSTN
✓ TDM Voice
✓ ISDN Video

CUBE/SBC
✓ SIP PSTN
✓ Phone Proxy

Cisco Expressway
✓ Mobile and Remote Access
✓ B2B Video
✓ XMPP Federation
✓ Jabber Guest

Copyright 2015
Customer Confidential
Agenda

- Introductions
- Collaboration Edge Architecture Overview
- Mobile and Remote Access (MRA) Overview
- MRA Implementation
- Q&A
Mobile and Remote Access (MRA)
Solution Overview

Allows the UC infrastructure to provide client registration, call control, provisioning, messaging, and IM/P services to endpoints and software clients that are not connected to the enterprise network.

Provides a secure, VPN-less communication solution for mobile devices and teleworkers.
MRA
Business Drivers

BYOD
✓ Borderless workforce
  Contractors, teleworkers
✓ Significant cost savings
  CapEx-Yes, OpEx-Maybe
✓ Employee productivity
  24x7x365 – Anytime, Anywhere

Teleworking
✓ Cost savings
  OpEx – Infrastructure cost reduction
✓ Employee satisfaction and retention
  - 2012 – 40% of US working pop telecommutes at least part time
  - Work-Life Integration
✓ Employee productivity

Solution Benefits
✓ MRA is an “enabler”
✓ Feature continuity and transparency
✓ Borderless communications
✓ Secure communications
✓ Cloud services support
MRA Solution Components
Cisco UCM

Cisco UCM

- UDS Provisioning
- End user authentication
- Client registration
- Voice/Video Call Control
MRA Solution Components
Cisco IM&P

Cisco IM & Presence

- XMPP Client connection
- Messaging service
- Presence / Contact Management
Cisco Unity Connection

- Visual Voice Messaging
MRA Solution Components

Cisco Expressway

- Introduced mid-2014
- Initial VCS/Expressway version X8.1
- Based on the Cisco Video Communications Server (VCS)

**Cisco VCS**

- Specialized video applications
- Used for video only customer base
- Virtual Machine or HW appliance
- **Superset** of platform feature set
- Two versions:
  - VCS Control (VCS-C)
  - VCS Expressway (VCS-E)

**Expressway**

- Designed for UCM 9.1+
- Virtual Machine only
- No cost licensing for MRA functionality
- **Subset** of platform feature set
- Two versions:
  - “Core” (Expressway-C)
  - “Edge” (Expressway-E)
### MRA Solution Components

**Cisco Expressway**

#### Expressway-C (Core)
- Traversal client
- Proxy endpoint registration
  - SIP to UCM
  - XMPP to IM/P
  - HTTP to VM and directory

#### Expressway-E (Edge)
- Traversal server
- Hosts external client connections

### Traversal Basics

1. **Core** initiates client connection to **Edge**
2. Once connected, **Core** sends keep-alive packets to **Edge**
3. **Edge** receives incoming requests from clients
4. The traversal connection is used to signal client request to **Core**
Supplementary Services

- Domain Name Services (DNS)
- Perimeter Firewall(s)
- Certificate Services
  - Internal Enterprise Hosts
  - Externally Accessible Hosts
- Intranet Web Server
Agenda

- Introductions
- Collaboration Edge Architecture Overview
- Mobile and Remote Access (MRA) Overview
- MRA Implementation
- Q&A
MRA Implementation

• UC Infrastructure Provisioning
  ✓ Expressway and the DMZ
  ✓ Certificate Provisioning

• Service Discovery and Client Registration
  ✓ DNS Provisioning
  ✓ Edge Discovery
  ✓ Service Discovery
  ✓ DNS Considerations
  ✓ Client Registration

• Deployment Considerations (*Time Permitting*)
MRA Implementation
Infrastructure Provisioning
Infrastructure Provisioning
Expressway and the DMZ

• **Expressway-C**
  - Always deployed on the internal LAN
  - Uses a Firewall Traversal mechanism to communicate with Expressway-E

• **Expressway-E**
  - Typically deployed in the DMZ
  - Can adapt to a variety of DMZ environments
  - Supports Static NAT (SNAT) using Advanced Networking Option
  - Supports dual network connections using DUAL NIC feature (part of Advanced Networking Option)

• **Firewall**
  - Various deployment options are supported
  - ALG is not a viable option w/ MRA solution
Infrastructure Provisioning
Expressway and the DMZ – DUAL + SNAT

Deployment Scenario
- Two separate DMZ subnets
- No routing between DMZ subnets
- Expressway-C on internal LAN
- Two physical firewalls

Expressway-E Config
- Dual NIC enabled
- LAN1 is bridged to LAN2
- Static routes to internal subnets manually added on Edge

Traversal Zone
- Edge-LAN1 is **not** NATted
- Core establishes connection to Edge-LAN1 IP address
- FQDN and Cert CN considerations

Internet “Zone”
- Edge-LAN2 uses Static NAT (SNAT)
- FW responsible for Layer 3 SNAT
- External DNS resolves to public IP
- FQDN and Cert CN considerations
• **Deployment Scenario**
  - Two separate DMZ subnets
  - No routing between DMZ subnets
  - Expressway-C on internal LAN
  - Two physical firewalls

• **Expressway-E Config**
  - Dual NIC enabled
  - LAN1 is bridged to LAN2
  - Static routes to internal subnets manually added on Edge

• **Traversal Zone**
  - Edge-LAN1 is not NATted
  - Core establishes connection to Edge-LAN1 IP address
  - FQDN and Cert CN considerations

• **Internet “Zone”**
  - Edge-LAN2 uses public IP
  - External DNS resolves to public IP
  - FQDN and Cert CN considerations
**Infrastructure Provisioning**

**Expressway and the DMZ – Single FW w/SNAT**

- **Deployment Scenario**
  - Single DMZ subnet
  - Expressway-C on internal LAN
  - One firewall (or HA Pair)
  - A static 1:1 NAT configured on FW

- **Expressway-E Config**
  - Advanced Networking enabled
  - LAN1 configured with SNAT

*NOTE: This works w/o SNAT as well
If not using SNAT, Advanced Networking not required

- **Traversal Zone**
  - Core establishes connection to LAN1 NATted IP address
  - Requires that FW support NAT Reflection

- **Internet “Zone”**
  - External DNS resolves to public IP
  - Jabber connects to NATted IP address

---
Infrastructure Provisioning
Expressway and the DMZ – Two Firewalls, SNAT

• **Deployment Scenario**
  ✓ Single DMZ subnet
  ✓ Expressway-C on internal LAN
  ✓ Internal and External firewalls
  ✓ Static 1:1 NAT configured on FW2

• **Expressway-E Config**
  ✓ Advanced Networking enabled
  ✓ LAN1 configured with SNAT
  ✓ (optional) Static routes to internal subnets manually added on Edge

• **Traversal Zone**
  ✓ Core establishes connection to LAN1 NATted IP address
  ✓ Requires that FW support NAT Reflection
  ✓ Design Consideration: Asymmetric routing

• **Internet “Zone”**
  ✓ External DNS resolves to public IP
  ✓ Jabber connects to NATted IP address
  
  *NOTE: This works w/o SNAT as well
  If not using SNAT, Advanced Networking not required
• **Deployment Scenario**
  - One DMZ subnet
  - Edge LAN1 on internal LAN
  - Core on internal LAN
  - No routing between DMZ and internal LAN
  - One firewall (or HA pair)

**Considerations**
- From the Expressway-E perspective, this is identical to the previous scenario
- Same considerations for certs and DNS resolution
- This is *not* one of Cisco’s reference configurations
- But, it works...
Infrastructure Provisioning
Certificate Provisioning - Overview
Infrastructure Provisioning
Certificate Provisioning – Jabber Considerations

• **Jabber clients enforce certificate validation**

  **Certificates Affected**

<table>
<thead>
<tr>
<th>Application</th>
<th>Certificate</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCM</td>
<td>Tomcat (HTTP)</td>
<td>Secure Phone Profiles for Mixed mode</td>
</tr>
<tr>
<td>Cisco IM&amp;P</td>
<td>Tomcat (HTTP) XCP Router (XMPP)</td>
<td>XMPP domain added as SAN</td>
</tr>
<tr>
<td>Unity Connection</td>
<td>Tomcat (HTTP)</td>
<td></td>
</tr>
<tr>
<td>Expressway-E</td>
<td>Server Cert</td>
<td>UCM Mixed Mode: no impact SAN: service discovery domains</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*When using OCSP or CRL: Required RTT &lt;= 5s</td>
</tr>
<tr>
<td>WebEx Services</td>
<td>CAS, WAPI</td>
<td>Meeting Center, WebEx Messenger</td>
</tr>
</tbody>
</table>

• **General Considerations**

  ✓ Client will prompt user when cert is not trusted
  ✓ To avoid identity mismatch, configure UC applications to use FQDN
    - Cisco UCM: System servers and UC service profiles
    - Cisco IM/P: Cluster topology, TFTP servers, CCMCIP profiles
  ✓ Public CAs do not support IP address, non-FQDN, or bogus FQDN in CSR
Infrastructure Provisioning
Certificate Provisioning - Expressway

• Server Certificates
  ✓ X.509 Extended Key usage: TLS Web Client Auth + TLS Web Server Auth
  ✓ No support for wildcard certificates
  ✓ No requirement to add Expressway certs to CTL (for UCM Mixed Mode)

• Expressway-E Certificates
  ✓ Server Certificate should be signed by Public CA
  ✓ All service discovery domains need to added as SANs in the CSR

• Expressway-C Certificates
  ✓ Recommend using Enterprise CA but can use Public CA
  ✓ For UCM Mixed Mode - add phone security profiles as SANs in CSR

• Other Considerations
  ✓ XMPP Federations and Federated Group chat SAN requirements
  ✓ Expressway Cluster considerations
## Infrastructure Provisioning

### Expressway Certificate Trust Store

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Core</th>
<th>Edge</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public CA chain used to sign Expressway-E (Edge) server certificate</td>
<td>Yes</td>
<td>Yes</td>
<td>Required to establish traversal zone</td>
</tr>
<tr>
<td>Public (or Enterprise) CA chain used to sign Expressway-C (Core) server certificate</td>
<td>Yes</td>
<td>Yes</td>
<td>Required to establish traversal zone</td>
</tr>
<tr>
<td>UCM Tomcat certificate or CA cert chain</td>
<td>Yes</td>
<td>No</td>
<td>For MRA only required when TLS verify mode is used</td>
</tr>
<tr>
<td>UCM CallManager service certificate or CA cert chain</td>
<td>Yes</td>
<td>No</td>
<td>Only required when UCM is provisioned for Mixed-Mode</td>
</tr>
<tr>
<td>IM/P Tomcat and XCP certificate or cert chain</td>
<td>Yes</td>
<td>No</td>
<td>For MRA only required when TLS verify mode is used</td>
</tr>
</tbody>
</table>
MRA Implementation

Service Discovery
Service Discovery
Process Overview

• **Determine Service Domain**
  - Leverage JID or read from configuration
  - Example: user@**company.com**

• **Edge Discovery**
  - Client queries DNS SRV records to determine service location
  - Attempt to discovery internal services then fallback to Edge Discovery

• **Determine if enterprise has a WebEx Cloud account**
  *We’ll come back to this later*

• **Get Edge Configuration**
  - Client establishes secure connection to Expressway-E ("Edge“)
  - Leverage UDS to determine user and device configuration

• **Client Registers to Cisco UCM, IM&P, and Voicemail**
Service Discovery

Edge Discovery

1. Jabber leverages DNS for discovery
2. Internal client DNS SRV query
3. If SRV query resolves then start TCP HS
4. If internal SRV queries fail then query for external SRV
5. If SRV query resolves then start TLS

Considerations

- Leverage “Split-Horizon” DNS
- Internal records:
  - _cisco-uds._tcp.<domain>
  - _cuplogin._tcp.<domain>
- External Record:
  - _collab-edge._tls.<domain>
Service Discovery
Get Edge Configuration

1. Jabber establishes TLS connection
   ✓ Client/Server Hello + cert exchange w/Edge

2. Jabber requests Edge configuration
   a) HTTPS request to Edge w/Authentication
   b) Edge proxies request to Core (over traversal)
   c) If not cached, Core sends DNS queries
   d) HTTPS/UDS request for user object to UCM
   e) UCM Authentiates User (TLS recommended)
   f) HTTPS/UDS request to Get Device configs

Process

SRV: _cisco-uds._tcp.<domain>
SRV: _cisco-phone-tftp._tcp.<domain>
SRV: _cuplogin._tcp.<domain>
A records (as needed)
Service Discovery
Get Edge Configuration

Process
1. Jabber establishes TLS connection
2. Jabber requests Edge configuration
3. UCM responds with 200 OK
   ✓ Response is relayed: Core->Edge->Client
   ✓ Response contains device and service config
4. Retrieve Configuration Files
   ✓ HTTPS: Get /jabber-config.xml, CTLSEP<csf>.tlv, SEP<csf>.cnf.xml
   ✓ Dial Rules, Directory Lookup Rules, etc.

Considerations
- Firewall Rules
- Server Certificates
  - Expressway-E
  - Cisco UCM
  - LDAP (optional)
Service Discovery
MRA Jabber Client Registration

Process

1. Jabber initiates SIP registration process
   - SIP REFER/REGISTER/etc. sent to Edge
   - Edge challenges client for authentication
   - Edge proxies client request (PAI) to Core
   - Core proxies request to Cisco UCM

2. Jabber establishes XMPP connection
   - Client request proxied - similar to SIP
   - HTTPS used for provisioning

3. Jabber establishes HTTPS connection to Unity Connection
   - Visual voicemail
MRA Implementation

Deployment Considerations
Deployment Considerations
Multi-Domain Deployment

Considerations

- **Public domain:** public.com
  - Expressway-E
- **Internal domain:** internal.local
  - Cisco UCM, IM&P, and UC hosts
  - Expressway-C
  - User service domain

**Solution**

- Leverage Split-DNS
- Modify jabber-config.xml
  - VoiceServicesDomain = public.com
- Jabber must login locally first
Deployment Considerations
Cisco WebEx Cloud

- **IM&P Functionality Provided by WebEx Messenger**
  - CUCM IM/P Service not required

- **WebEx Cloud and Service Discovery**
  - Client queries for SRV records: _cisco-uds, _cuplogin, _collab-edge
  - Determine whether domain is registered to WebEx
    - [http://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>](http://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>)
  - If WebEx discovered:
    - Challenge user with WebEx credentials
    - Proceed with Enterprise sign-in on CUCM and Unity Connection
  - If no WebEx account then discovery proceeds as normal

- **What if you have a mixed environment?**
  - WebEx can be excluded from the Service Discovery process
Deployment Considerations
Customizing Service Discovery

• Methodology
  – J4W: Can push configuration parameters during MSI install
  – All Clients: Leverage “Configuration URL”

• Service Discovery Options
  – Exclude WebEx:
    – Client Does not check WebEx cloud
    – SRV queries: (a) _cisco-uds, (b) _cuplogin, (c) _collab-edge
  – Exclude CUCM:
    – Client does check WebEx but does not query for _cisco-uds
    – SRV queries: (a) _cuplogin and (b) _collab-edge
  – Exclude CUP:
    – I think you get the idea... [no _cuplogin, yes everything else]
# Deployment Considerations

Interoperability of Collaboration Edge Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Expressway</th>
<th>VCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile and Remote Access</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Business to Business Video</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Business to Consumer / Jabber Guest**</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Video Interworking (IPv4-IPv6, H323-SIP, MS H264 SVC-AVC, Standards based 3rd party)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Video / TelePresence Device Registration + Provisioning</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Video Session Management + Call Control</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WebEx Enabled TelePresence</td>
<td>Yes*</td>
<td>Yes</td>
</tr>
<tr>
<td>Enhanced Security (e.g. JITC)</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* TelePresence MCU must be trunked to the Cisco UCM

** Jabber Guest and MRA cannot run co-resident (due to TURN requirements)
### Deployment Considerations

#### Minimum Software Requirements

<table>
<thead>
<tr>
<th>Feature</th>
<th>UC Solution Component</th>
<th>Minimum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Processing</td>
<td>Cisco Unified CM</td>
<td>9.1(2)SU1</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified CM Business Edition</td>
<td></td>
</tr>
<tr>
<td>IM/Presence</td>
<td>Unified Presence</td>
<td>9.1.1</td>
</tr>
<tr>
<td></td>
<td>WebEx Connect service</td>
<td>Server 7.6 and later</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Cisco Unity Connection</td>
<td>8.6(1)</td>
</tr>
<tr>
<td>Collaboration Edge</td>
<td>Cisco Expressway or Cisco VCS</td>
<td>X8.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clients*</td>
<td>Jabber for Windows</td>
<td>9.7</td>
</tr>
<tr>
<td></td>
<td>Jabber for iPhone/iPad</td>
<td>9.6(1)</td>
</tr>
<tr>
<td></td>
<td>Jabber for Mac</td>
<td>9.6</td>
</tr>
<tr>
<td></td>
<td>Jabber for Android</td>
<td>9.6</td>
</tr>
<tr>
<td></td>
<td>EX/MX/SX/C Series Endpoints</td>
<td>TC 7.1</td>
</tr>
</tbody>
</table>

* Expressway X8.5 Preview Feature: Support for Cisco DX, 7800, and 8800 endpoints
Agenda

Introductions
Collaboration Edge Architecture Overview
Mobile and Remote Access (MRA) Overview
MRA Implementation
Q&A
Telephone: 888-804-1717
E-mail: info@netcraftsmen.com