rogram

s	Téma	Přednášející
30 – 10:30	Novinky v Cisco Collaboration	Jaroslav Martan
:45 – 11:45	Nástroje pro management multimediální sítě (Medianet)	Jiří Rott
	oběd	
:45 – 13:45	Architektura collaboration řešení - Jabber Design - Integrace Cisco UC a MS OCS/Lync	 Jaroslav Martan Ivan Sýkora
:00 - ???	Architektura – whiteboard (jam) session - Edge design - SIP trunk - Video – jednotný call control - Trusted Relay Point (TRP) a L3 VPN	 Jaroslav Martan Jiří Rott Jaroslav Martan Jaroslav Martan

Cisco Connect

Praha, hotel Clarion
10. – 11. dubna 2013

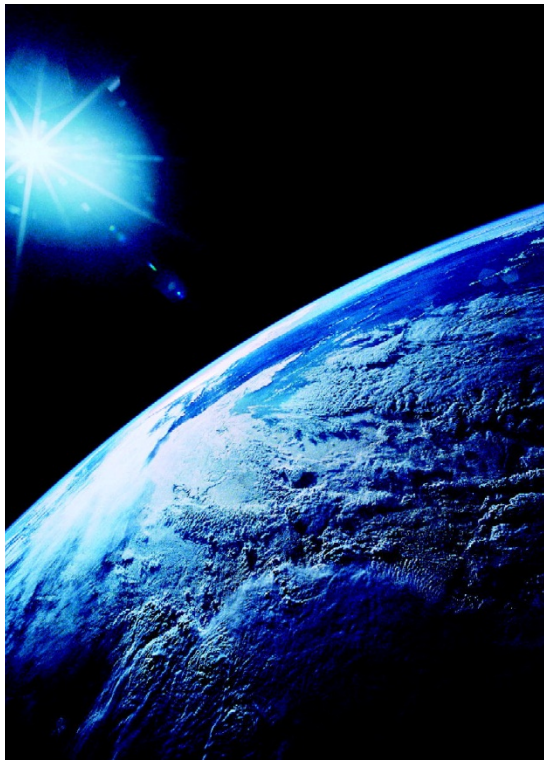
Architektura Collaboration řešení

COL3 / 2

roslav Martan, CCIE #5871, jmartan@cisco.com

n Sýkora, CCIE #7398, ivsykora@cisco.com

Rott, jirott@cisco.com



bsah

Jabber Design

ntegrace Cisco UC s MS OCS/Lync

<přestávka>

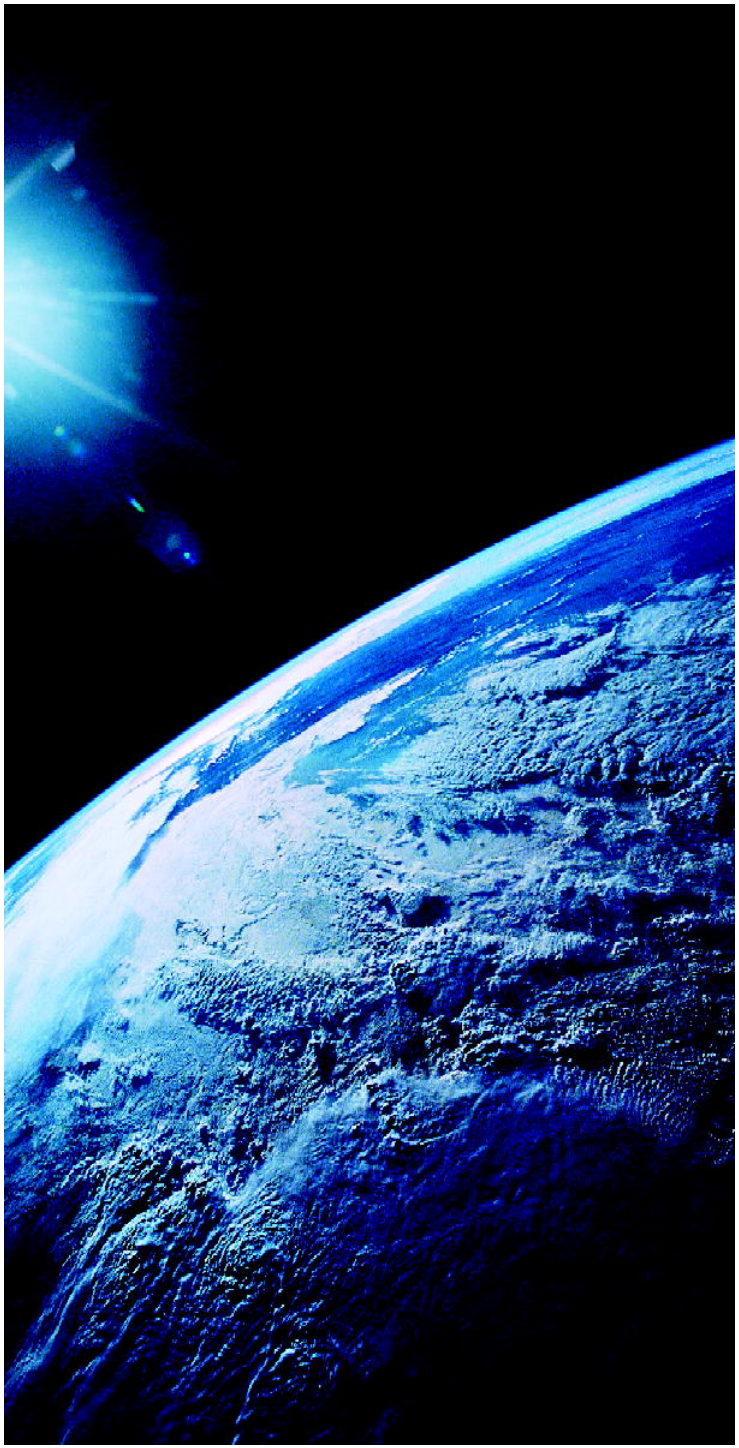
Edge Design

SIP trunk

Video Design

Trusted Relay Point (TRP) & L3 VPN

abber Design



abber je univerzální klient.

Tato přednáška není o „jediném
správném řešení“, ale
o možnostech přizpůsobit
abber klienta aplikačnímu
rostředí zákazníka.

Jabber Design

Session Agenda

Integration Points:

- Office Tools (MS Office, IBM Domino)
- Directory Services
  (network-based, local in a computer)
- Calendar
- Voice & Video Services (CUCM)
- Collaboration Tools
  (Webex Cloud, Webex Meetings Server, MeetingPlace)
- Web applications

Configuration Tools:

- Client profile on CUCM
- jabber-config.xml file

Cisco Jabber

Deploying Cisco Jabber Desktop Clients

Cisco Jabber Product Portfolio

All-in-one UC Application

Presence & IM

Voice, Video, voice messaging

Desktop sharing, conferencing

Collaborate from Any Workspace

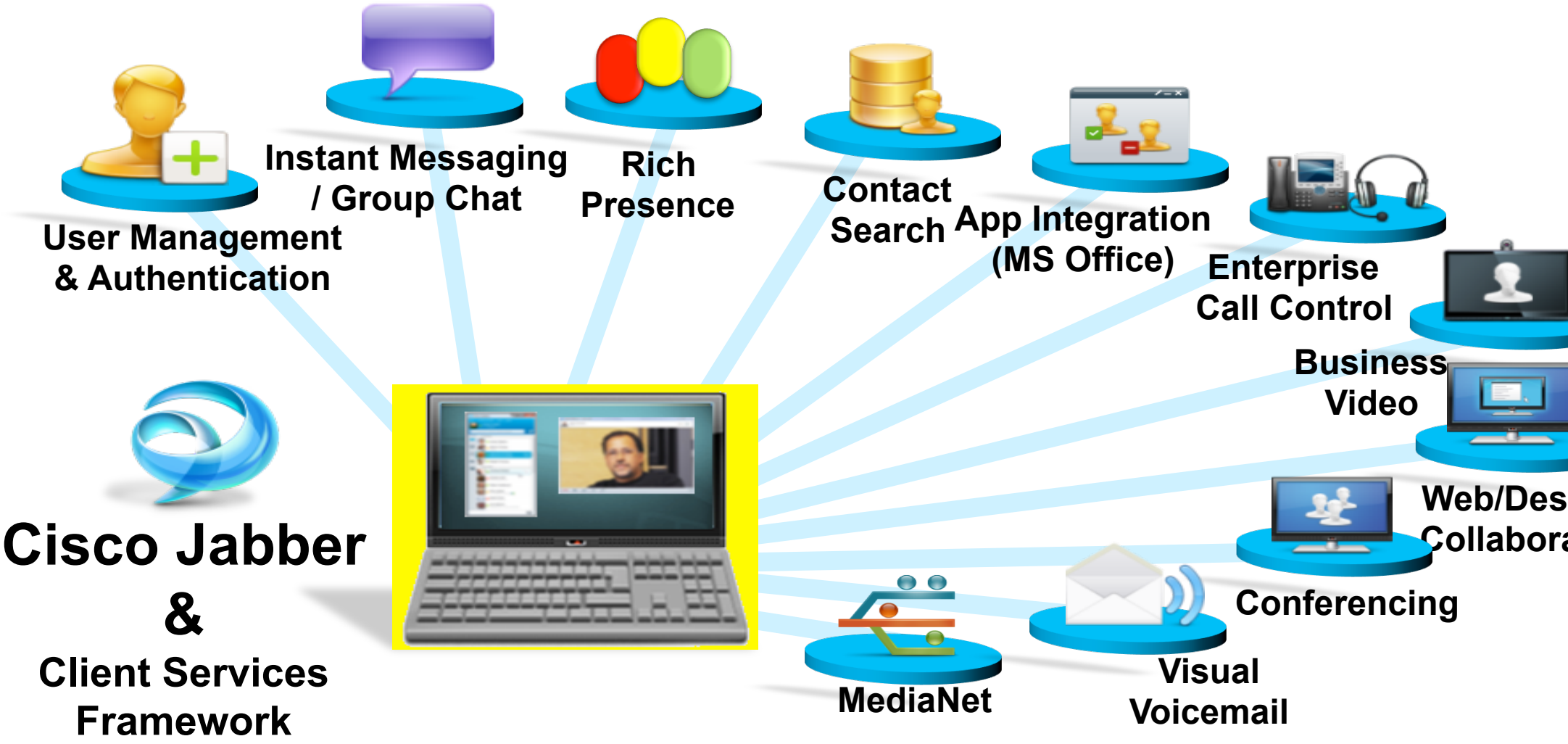
PC, Mac, tablet, smart phone

On-premises and Cloud

Integration with Microsoft Office

Cisco Jabber

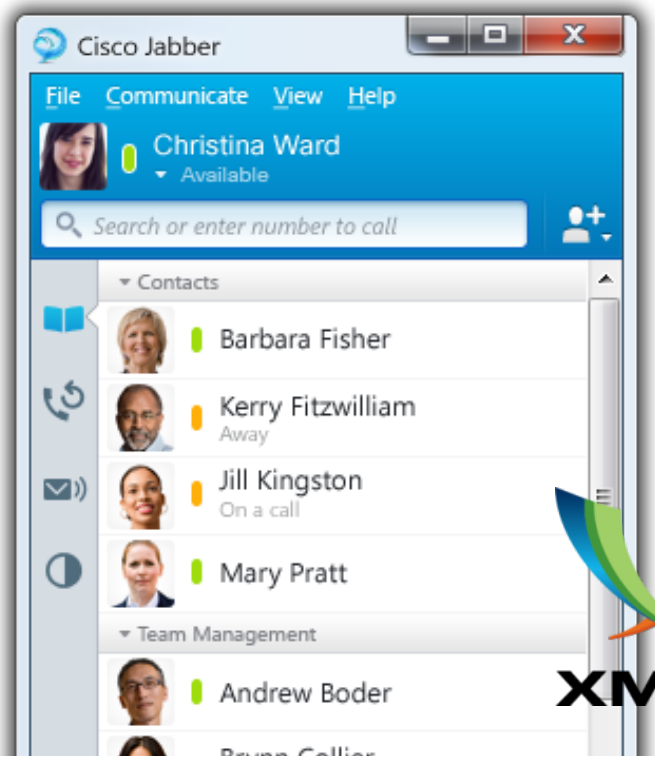
Workflows available in Cisco Jabber



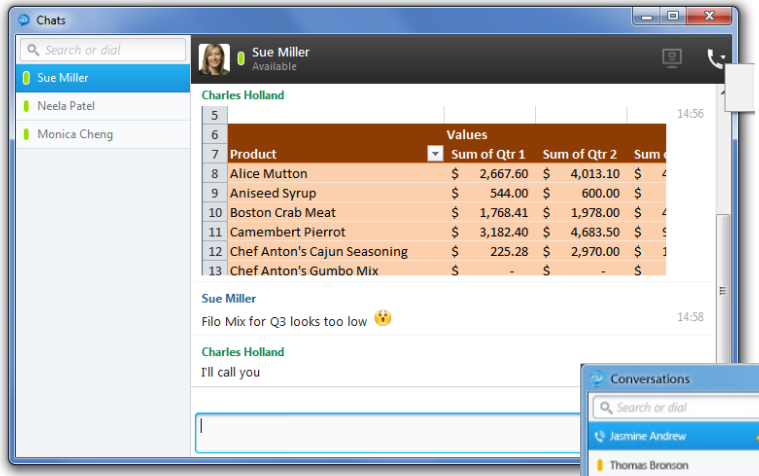
A Brief tour of Jabber

Jabber for Windows

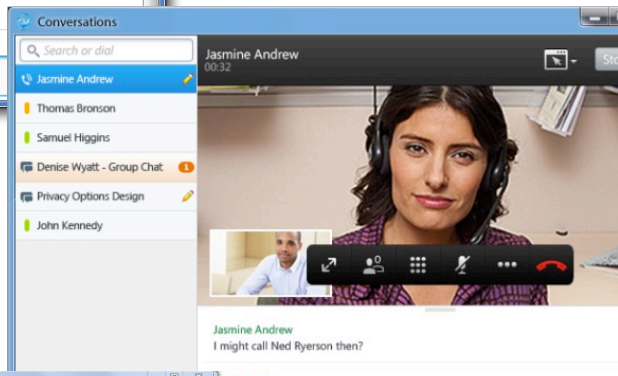
Cisco Jabber provides you a hub view. The hub view displays **contacts** with **presence** and provides **search** capabilities



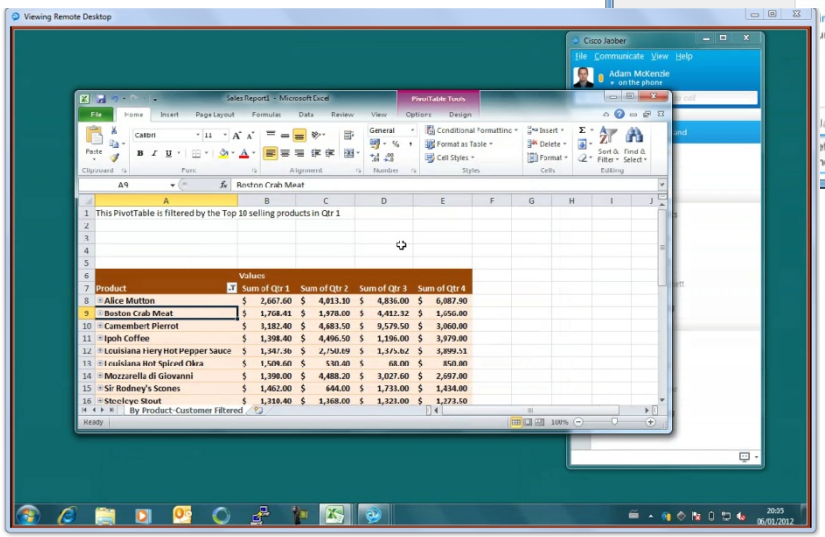
XMPP



Chat, Group Chat, Federated Chat, Ch history, File Transfe Screen Capture and Emoticons



Standards based **Voice** and high definition **video** calling



Collaboration usin **Desktop sharing** Web Conferencing

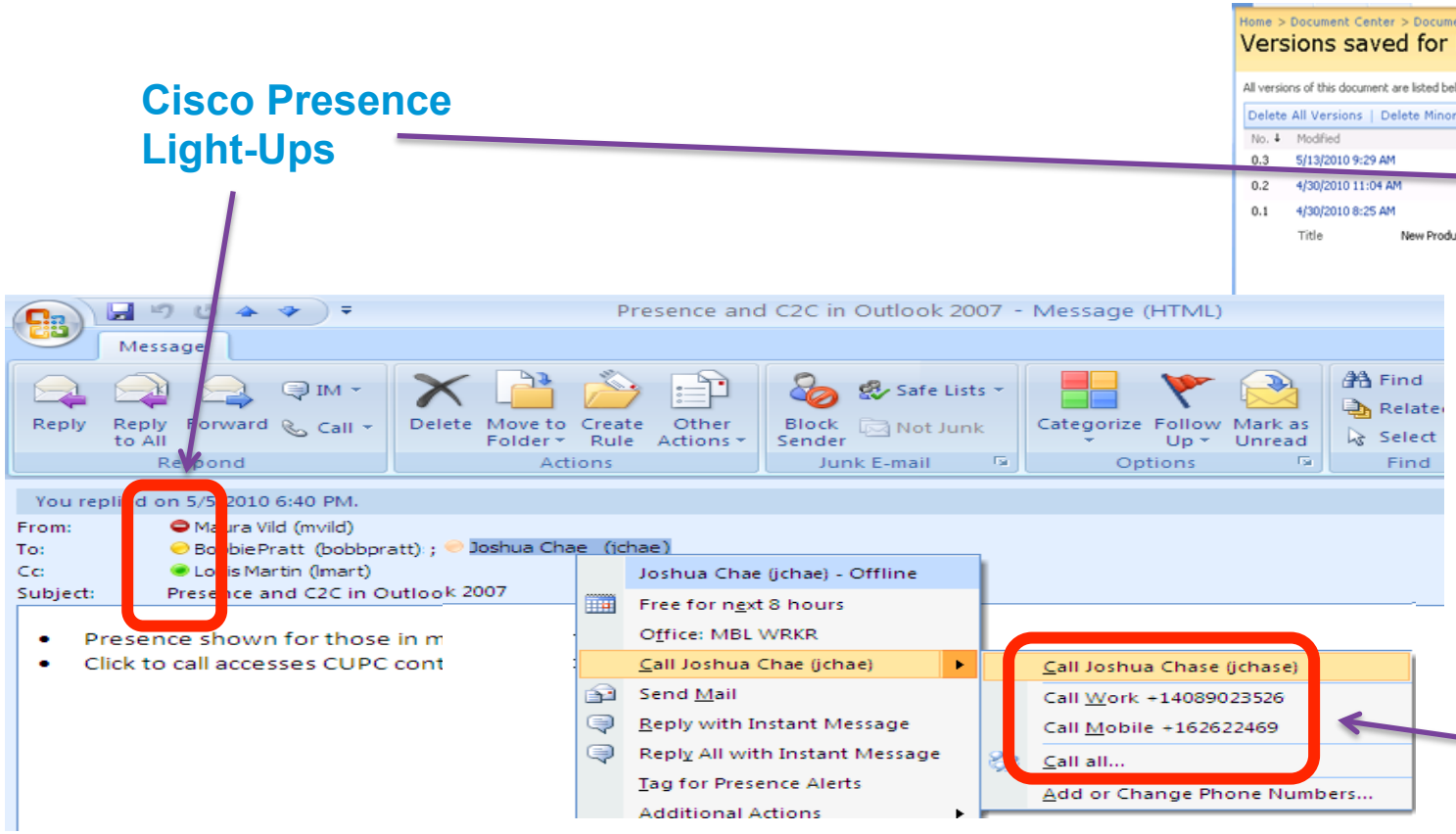
Microsoft Office Integration

Microsoft Office 2007 Integration

Office 2007 integration allows conversations to be initiated directly inside Office and SharePoint applications

Microsoft SharePoint 2007

Cisco Presence Light-Ups



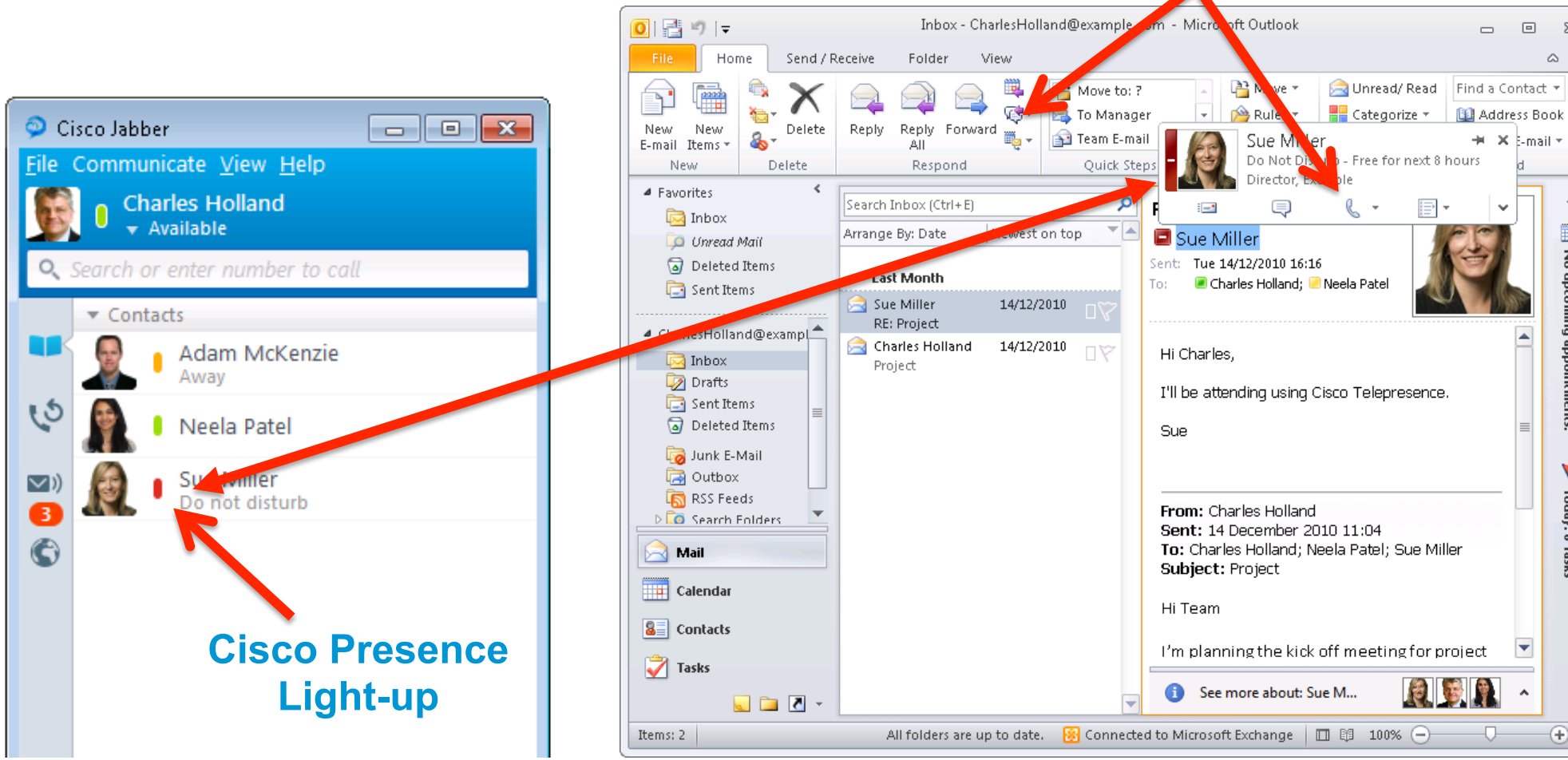
Cisco Click to IM/Call

Microsoft Outlook 2007

Microsoft Office Integration

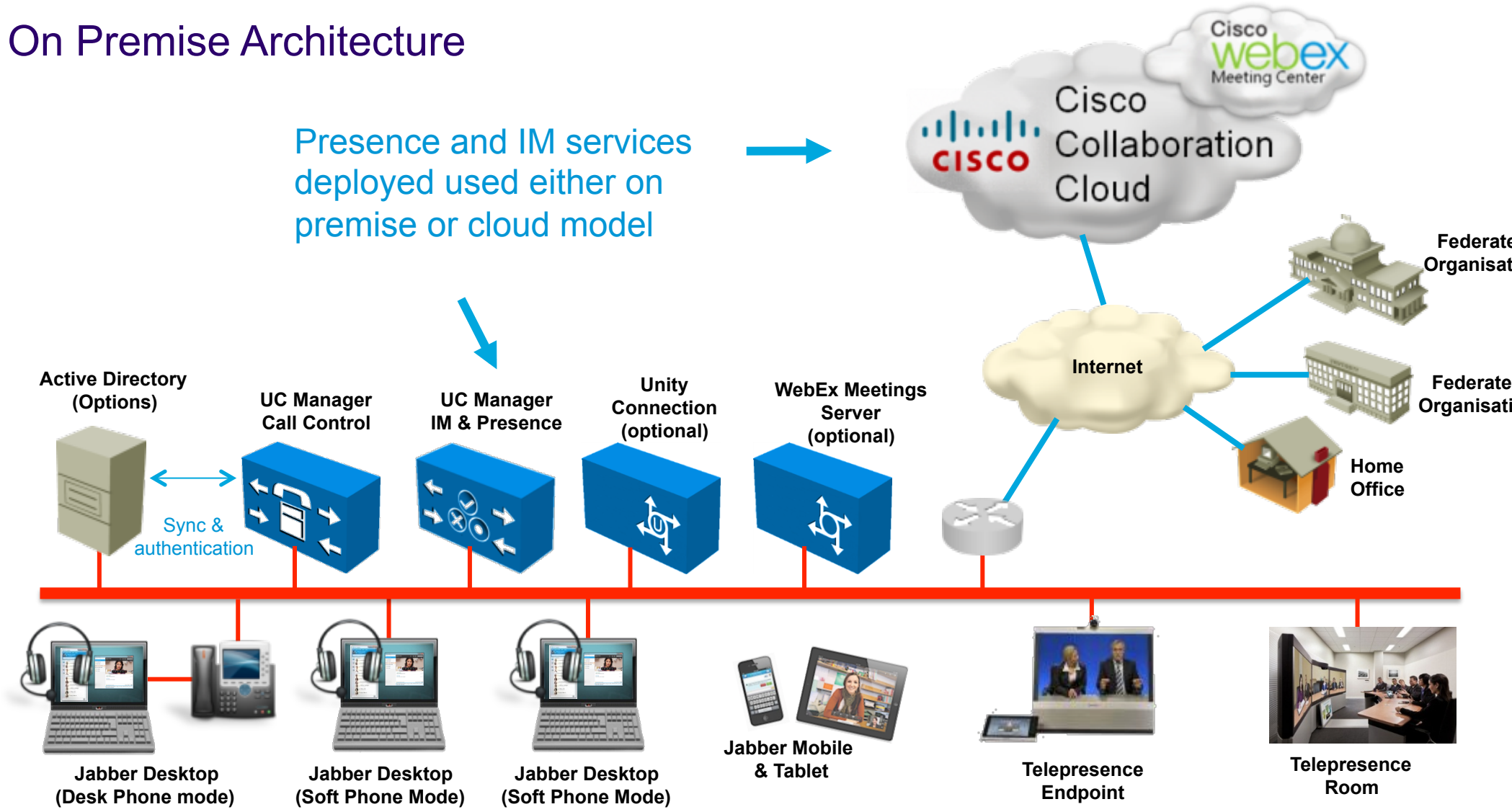
Microsoft Office 2010 Integration

Office 2010 integration allows conversations to be initiated directly inside Office and SharePoint applications



Jabber On Premise Solution Architecture

On Premise Architecture

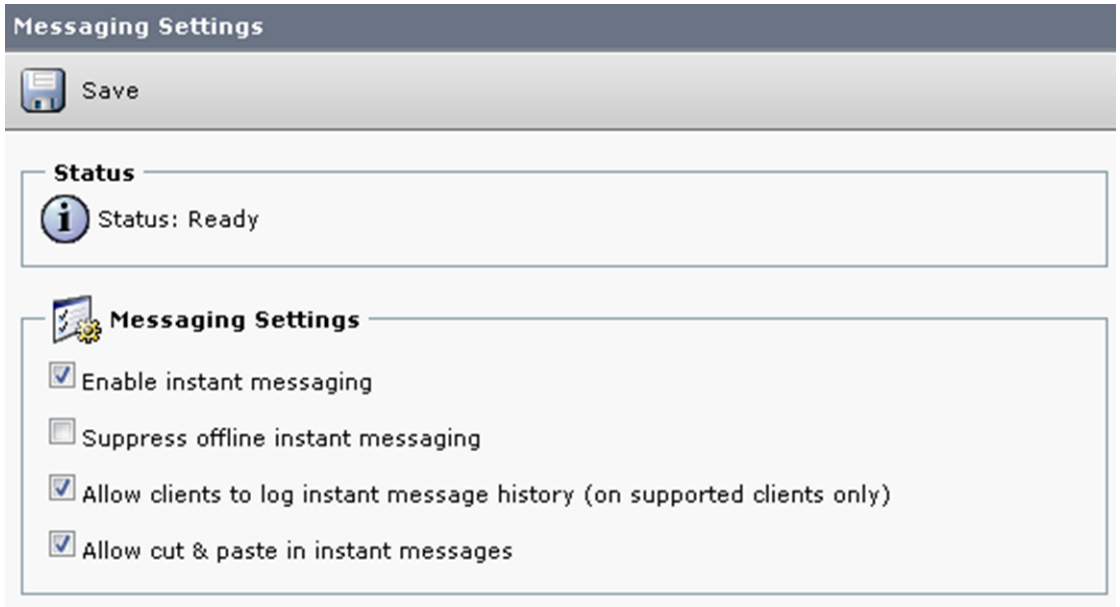


Jabber On Premise Solution Architecture

Instant Message Policy

IM Policy can be managed by the admin

IM Policy can be set to disable IM or features



Policy for File Transfer and Screen Capture are controlled via jabber-config.xml file on windows

Users enabled for IM will be able to:

Start Point to Point IM
Start group chat session
Use Rich Text IM

Screen Capture (Windows only)
File Transfer (Jabber Clients o

IM logging can be configured on Cisco presence server

- Server logging
- Actiance application

Jabber On Premise Solution Architecture

IM Federation

Industry standard based federation for presence and IM services

Multi-protocol federation

- XMPP
- SIP/SIMPLE

Inter-domain federation

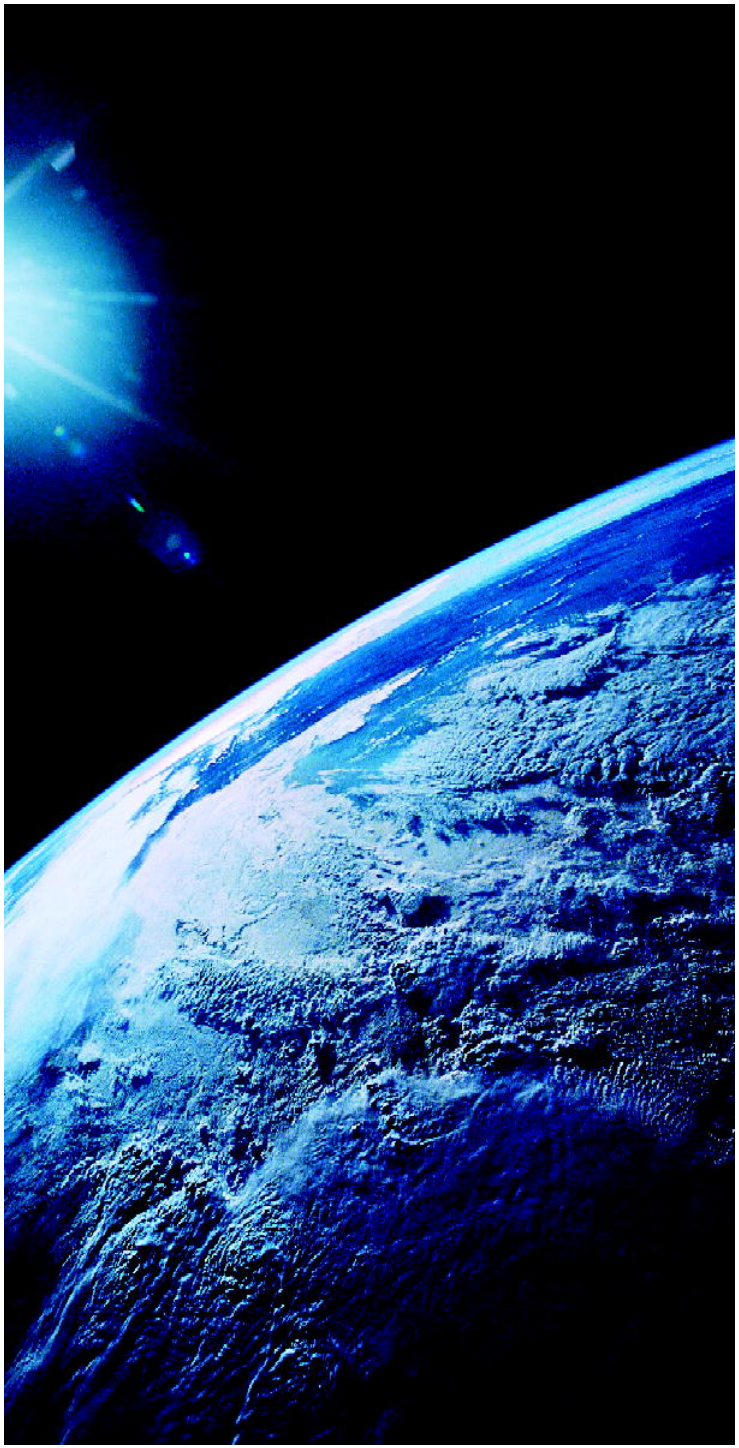
- Inter-organisation

Intra-domain federation (Microsoft OCS / LYNC)

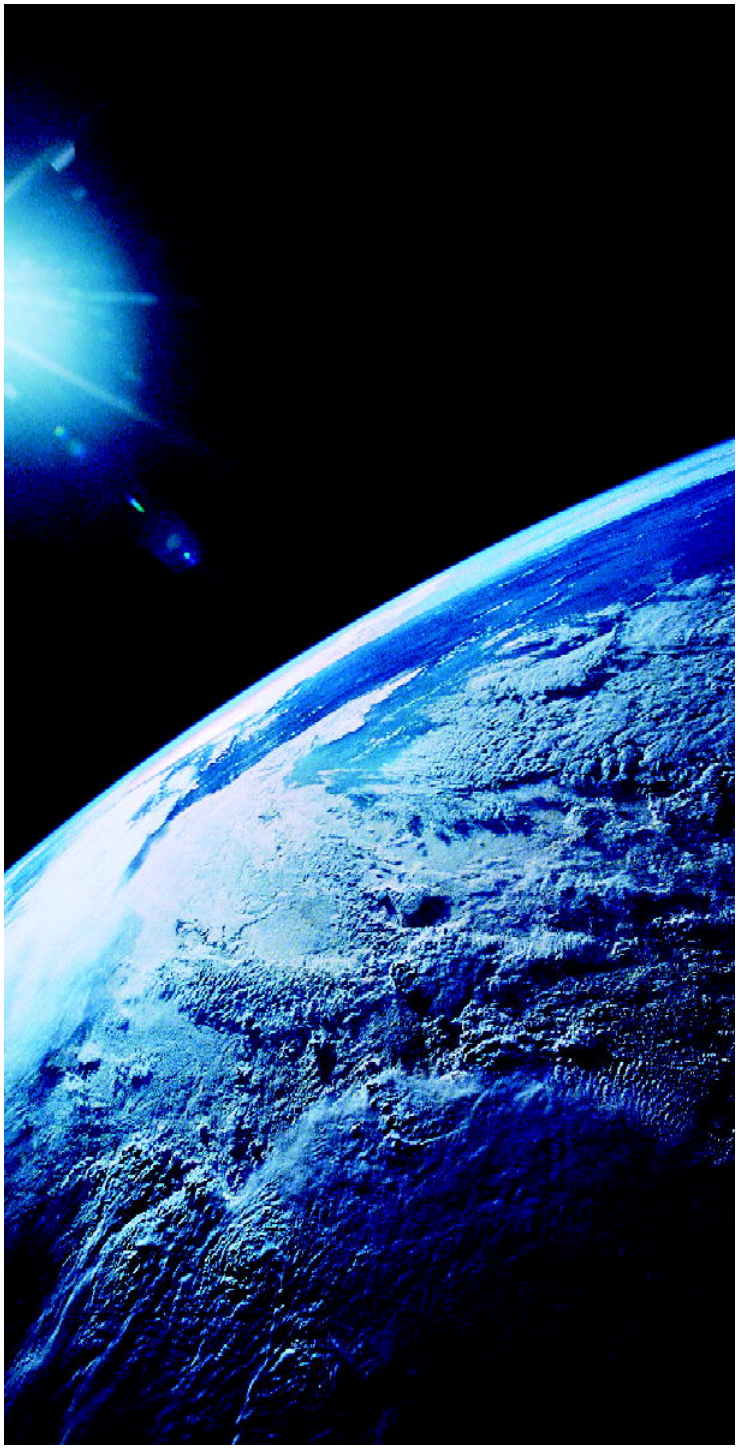
Public Service Federation

- Google / AOL

Demo



Now into the Detail...



Creating Jabber Users

TASK LIST (on premise / pre 9)

Create/Sync Users in CUCM

Enable Users for Presence/Client Access

Configure Contact Source Access

Configure LDAP/EDI access

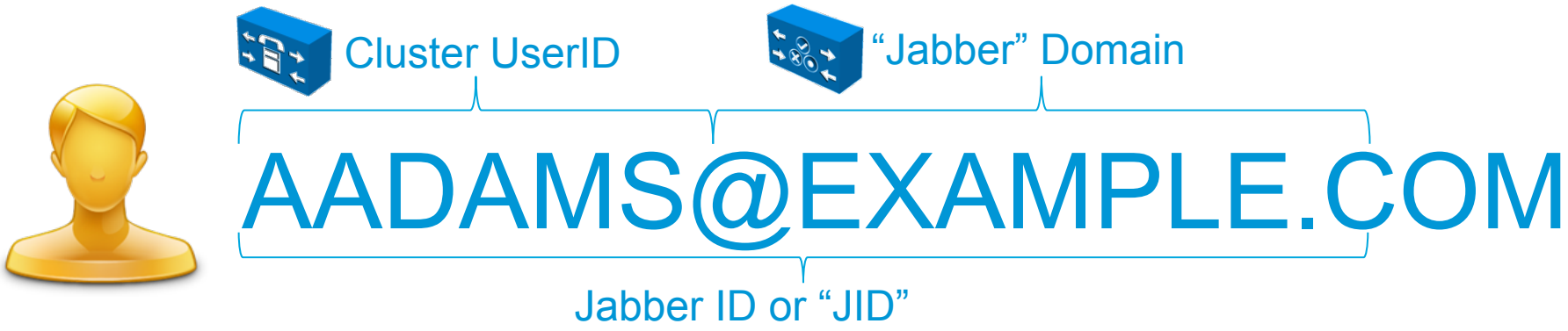
- or -

Configure UDS Contact Service

Deploy Client Installer

Creating Jabber Users

What's your JID? (Jabber ID)



- Consider your Jabber domain carefully, you'll live with it for a while!
- Multi-modal communications address (Email, IM, Voice, Video & Federation)

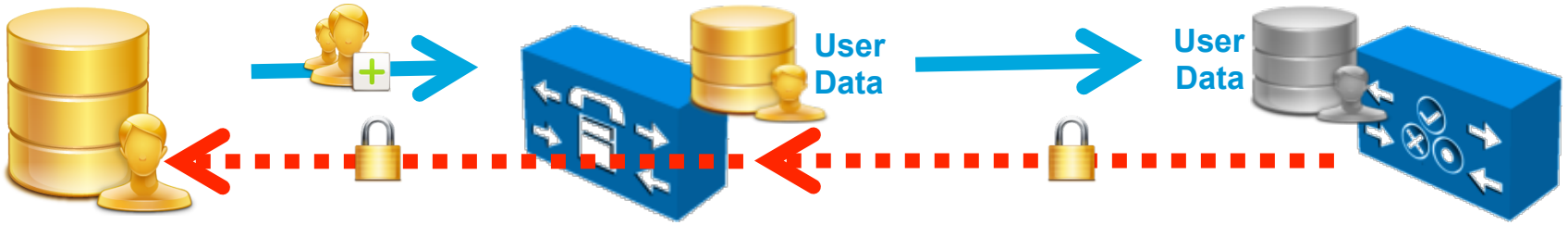
- User created on UC Manager (can be synced from LDAP, AD Server)
- User is authenticated (can be authenticated from LDAP/AD or *SSO) (H1 CY13)
- Presence domain is configured on Presence server

Creating Jabber Users

Adding Users as UC Manager Users

Unified Communication Manager

Option 1 (recommended)



Recommended Configuration is to synchronise Corporate directory with UC Manager.
Key **sAMAccountName**, mail, employeeID, Telephone, UserPrinciplename

Option 2

UC manager User Administration

Users created via Web admin or via Bulk Administration Tool (BAT)

Jabber Client

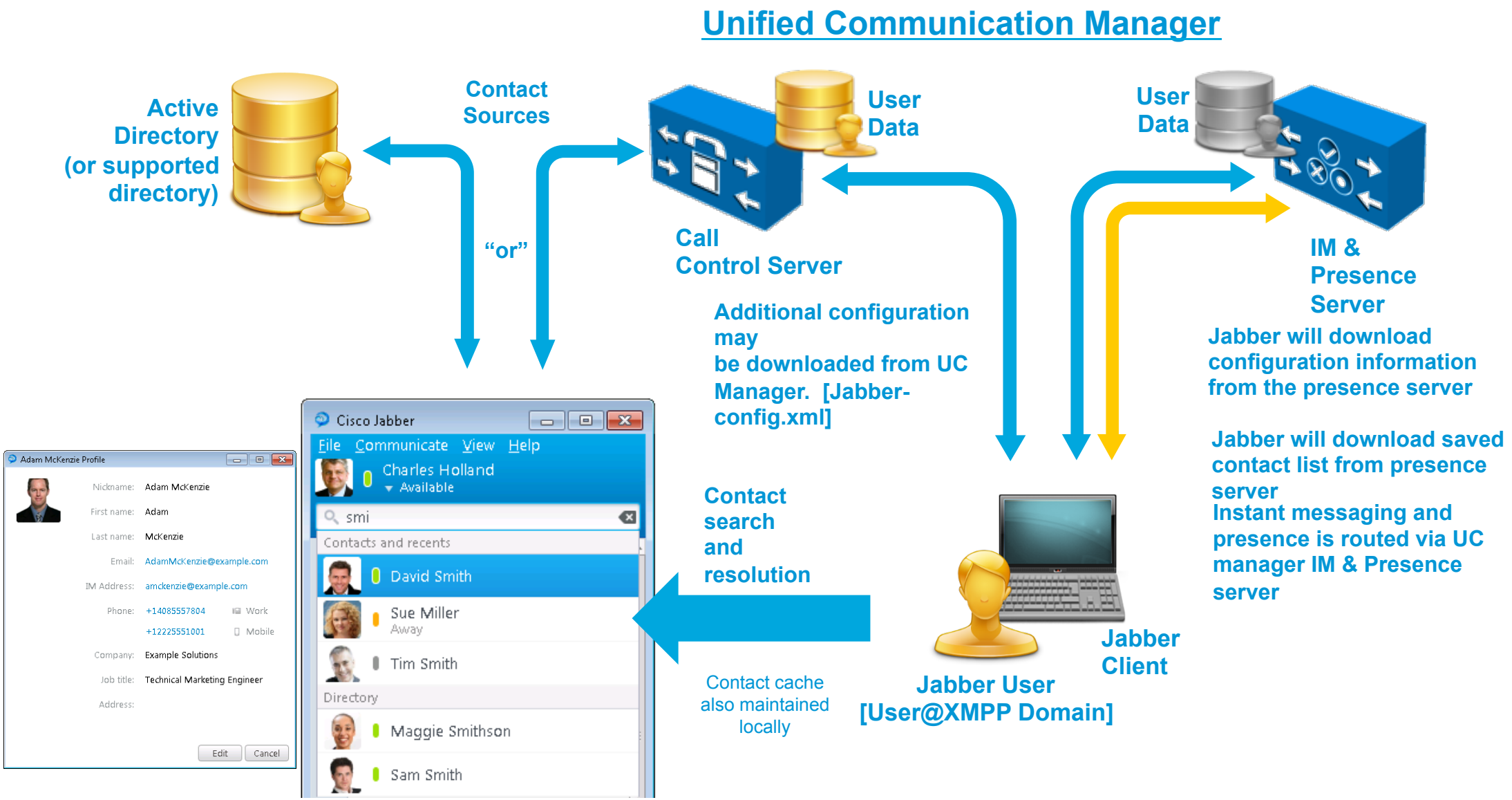
Jabber User [User@XMPP Domain]

Jabber will authenticat services on UC manag and Presence server Services can authentic user locally or back to directory service

Jabber on premise deployment will introdu single sign on (SSO) ir CY13

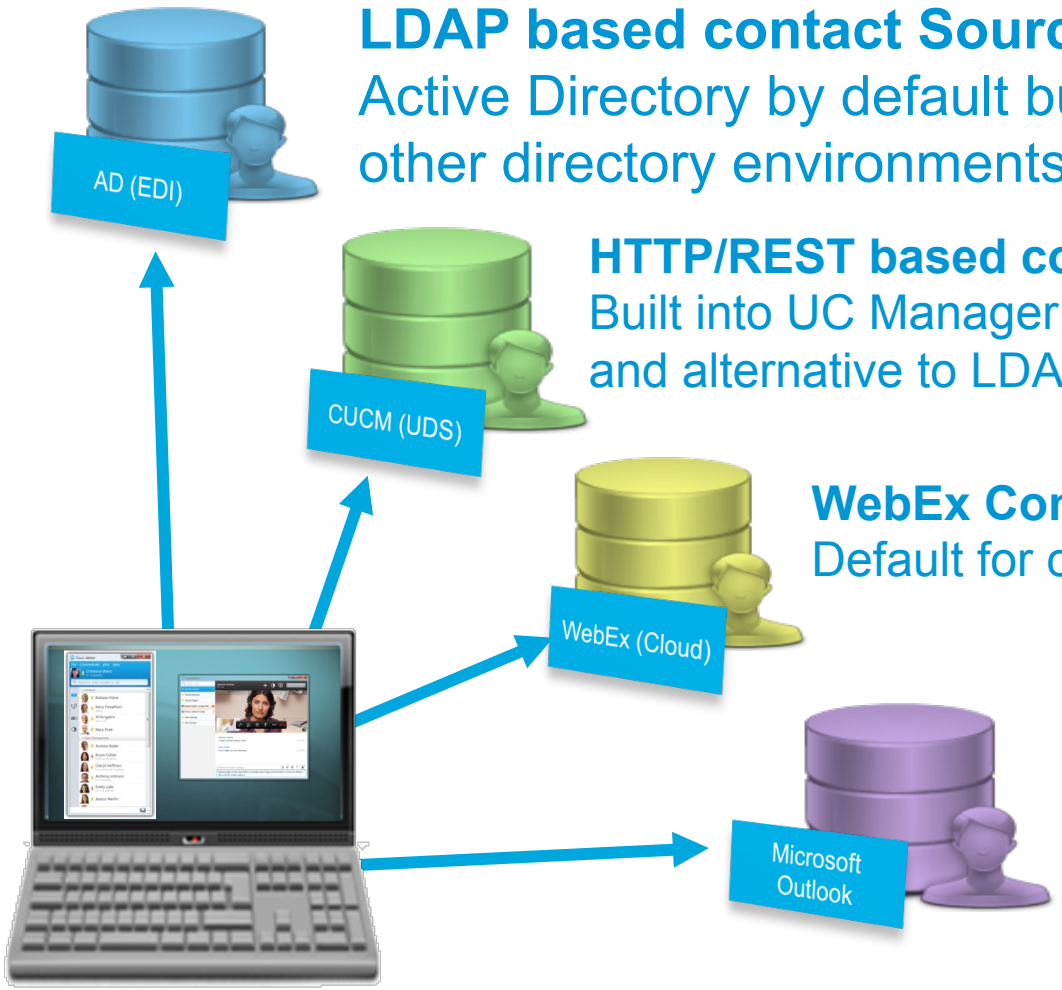
Creating Jabber Users

IM and Presence Architecture



Jabber Contact Sources

Selecting a Contact Source



LDAP based contact Source (On Prem Default)
Active Directory by default but can be customized for other directory environments

HTTP/REST based contact Source (On Prem)
Built into UC Manager 8.6(2)+ and provides and alternative to LDAP integration

WebEx Contact Source (cloud)
Default for cloud based deployments

MS Outlook Contacts
Search local contacts from Jabber (requires 9.1 for Windows)

Jabber Contact Sources

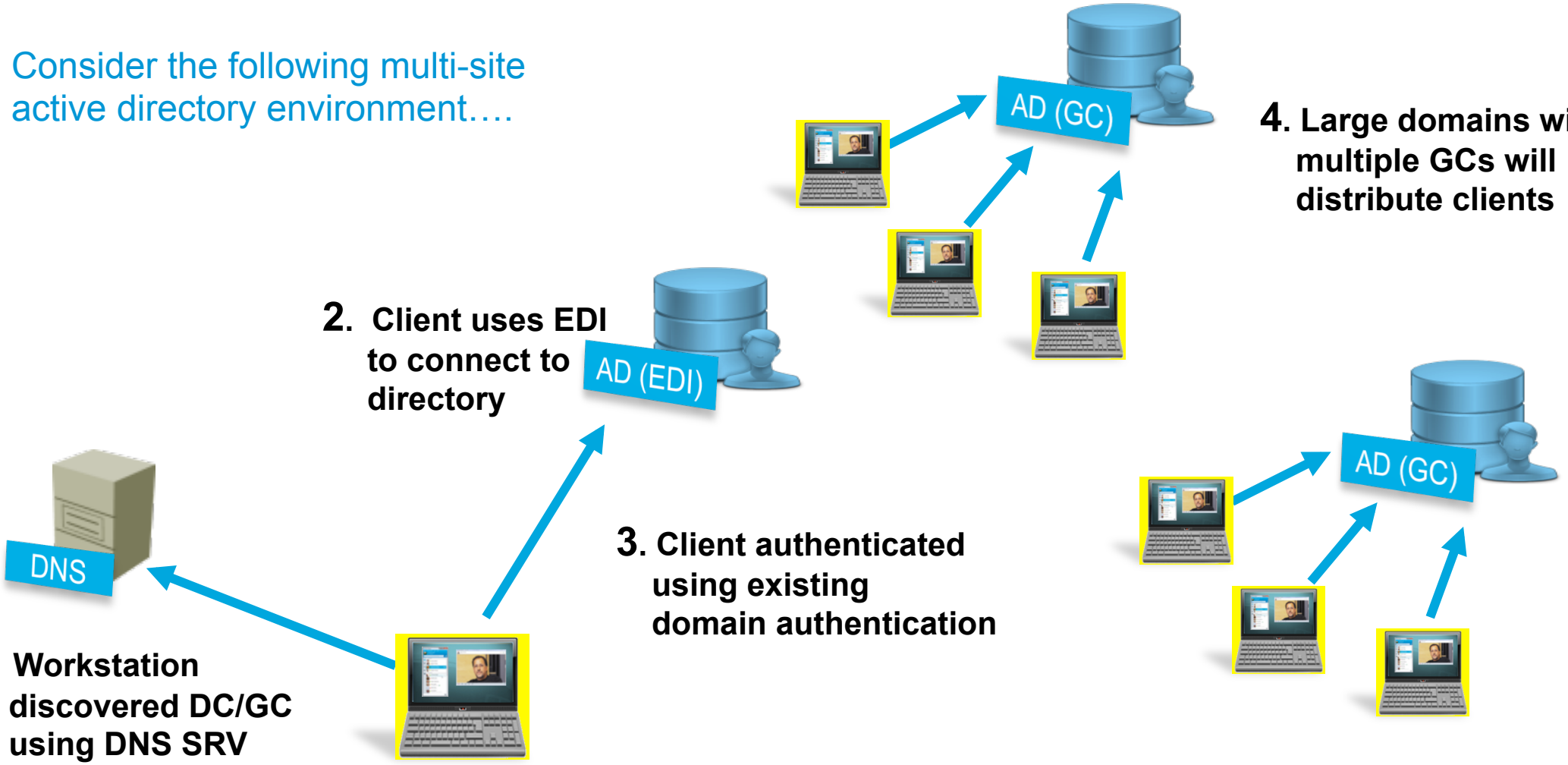
EDI : Enhanced Directory Integration (LDAP)

- **On Premise Jabber for Windows by default uses auto-discovery for LDAP directory access (EDI Mode)**
- **Workstation MUST be a member of a domain for auto discovery to work**
- Clients connect to a Global Catalog server in the current domain (windows selects exact GC, so distributes load)
- Client uses encrypted authentication to directory based on current logged on user (workstation)
- Ambiguous name resolution (ANR) is used for search, ANR is more efficient and uses less server resources than other search methods.

Jabber Contact Sources

EDI : Enhanced Directory Integration (LDAP)

Consider the following multi-site active directory environment….



2. **Client uses EDI to connect to directory**

3. **Client authenticated using existing domain authentication**

4. **Large domains wi multiple GCs will distribute clients**

1. **Workstation discovered DC/GC using DNS SRV**

Jabber Contact Sources

EDI : Customization - One Model doesn't fit all….

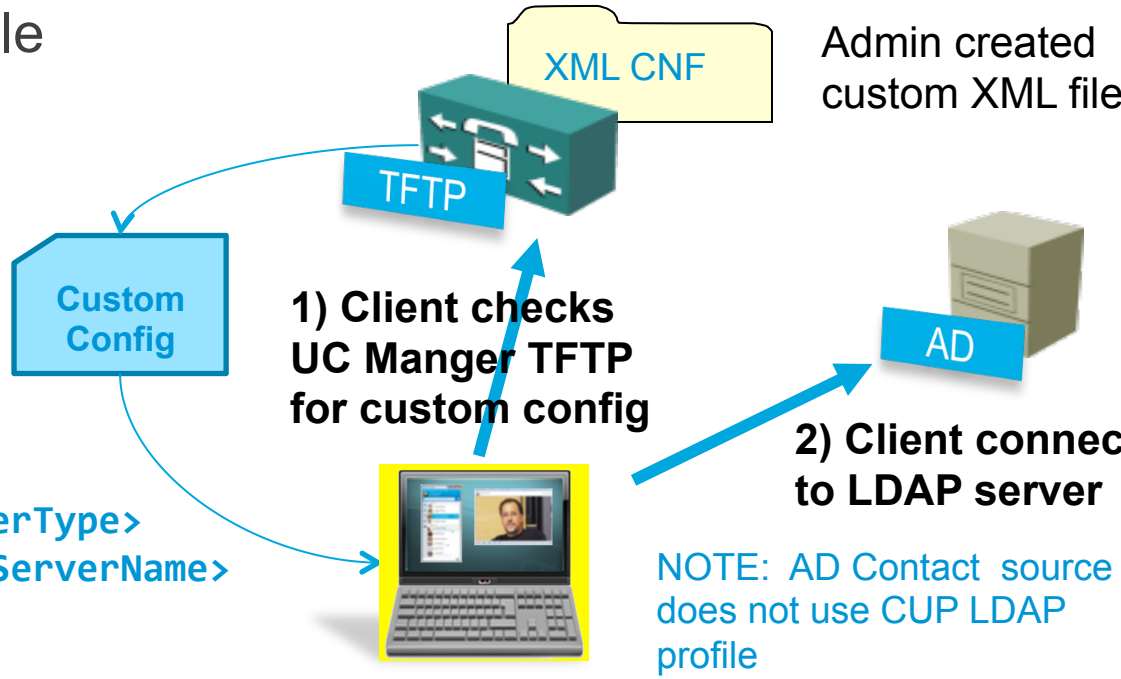
Administrator can customize many elements of EDI operation for different deployment environments.

The Administrator creates a custom XML configuration file for directory access.

TFTP or HTTP is used to download file

Filename: Jabber-config.xml

Only define non default items.




```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Directory>
    <DirectoryServerType>EDI</DirectoryServerType>
    <PrimaryServerName>D1.test.lab</PrimaryServerName>
    <ServerPort1>1234</ServerPort1>
  </Directory>
</config>
```

(example only)

http://www.cisco.com/en/US/docs/voice_ip_comm/jabber/Windows/9_1/JABW_BK_CA48EE46_00_cisco-jabber-for-windows-administration_chapter_0101.htm

Jabber Contact Sources

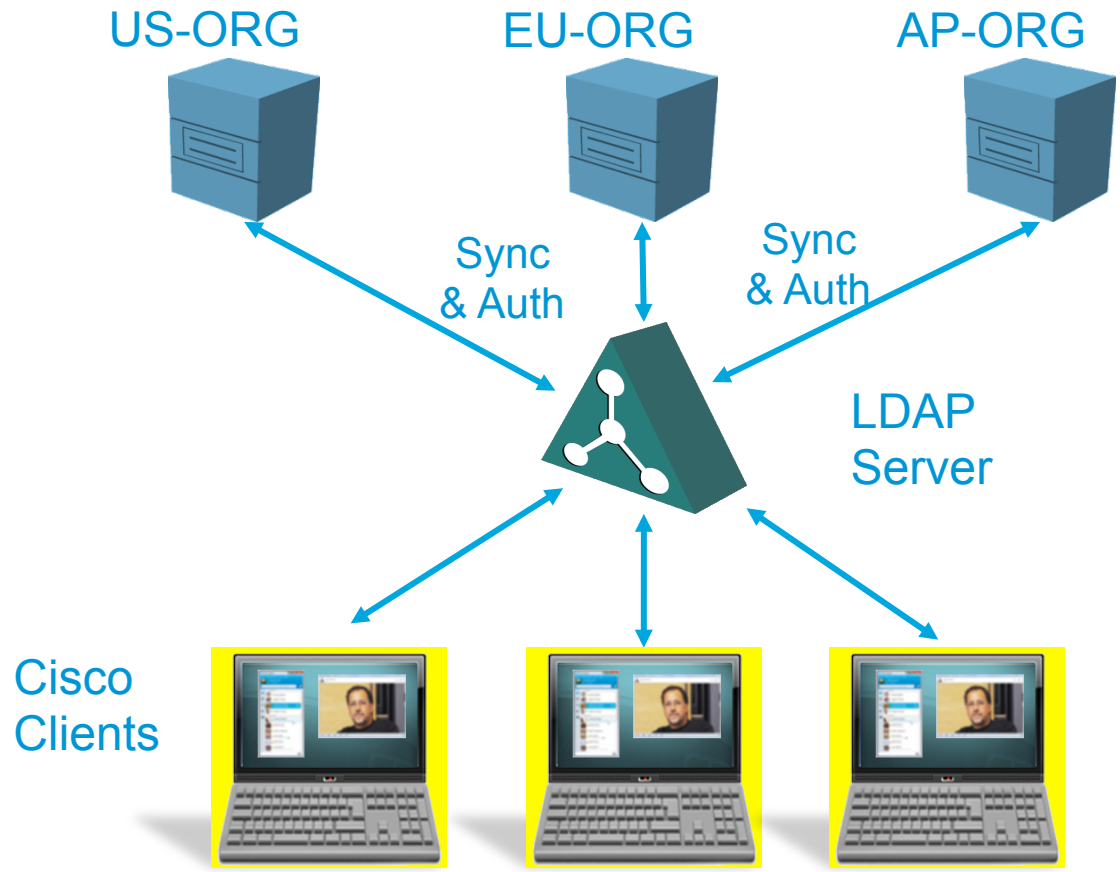
EDI : Alternative Directory Access

EDI can connect to a single AD forest. If you need to connect to multiple forests you c
use Microsoft AD Application mode / lightweight directory services.

ADAM/LDS is commonly used to build to an aggregated directory from multiple AD forests

EDI also supports ADAM/LDS using proxy authentication.

Connection to other LDAP application servers (i.e. non Microsoft)



Jabber Contact Sources

EDI : Custom Directory Access Parameters

Connection Settings
Connection Type
UseSecureConnection
UseSSL
PrimayServerName
Port1
SecondaryServerName
Port2

Search
SearchBase1
SearchBase2
SearchBase3
BaseFilter

Attribute Map	
CommonName	Nickname
FirstName	PostalCode
LastName	State
EmailAddress	StreetAddress
SipUri	PhotoURI
BusinessPhone	CompanyName
HomePhone	UserAccount
OtherPhone	Domain
PreferredNumber	Location
Title	

Authentication
UseWindowsCredentials
ConnectionUsername
ConnectionPassword

Jabber Contact Sources

EDI: Example Configurations

Connect to DC not GC

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0“>
<Directory>
     <DirectoryServerType>EDI</DirectoryServerType>
     <ConnectionType>1</ConnectionType>
</Directory>
</config>
```

Manual Server selection

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0“>
<Directory>
     <DirectoryServerType>EDI</DirectoryServerType>
     <PrimaryServerName>primary_server_name.domain.com</PrimaryServerName>
     <ServerPort1>1234</ServerPort1>
     <SecondaryServerName>secondary_server_name.domain.com</SecondaryServerName>
     <ServerPort2>5678</ServerPort2>
</Directory>
</config>
```

Jabber Contact Sources

EDI : Example Configurations

Common access account

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<ConnectionUsername>ldap_user</ConnectionUsername>
<ConnectionPassword>ldap_password</ConnectionPassword>
```

Search specified OU

```
<SearchBase1>ou=employee,dc=example,dc=com</SearchBase1>
```

Exclude defined entry based on attribute

```
<BaseFilter>(&amp;(objectCategory=person)(UserAccountControl:1.2.840.113556.1.4.803:=2)
</BaseFilter>
```

- Use alternative attribute for phone

```
<BusinessPhone>aNonDefaultTelephoneNumberAttribute</BusinessPhone>
 <MobilePhone>aNonDefaultMobileAttribute</MobilePhone>
 <HomePhone>aNonDefaultHomePhoneAttribute</HomePhone>
 <OtherPhone>aNonDefaultOtherTelephoneAttribute</OtherPhone>
```

Note: Jabber-config.xml file also holds a number of other configuration parameters, alternative files can also be defined by administrator.

Jabber Contact Sources

Retrieving Photos for Contacts

- Jabber provides a number of methods to retrieve contact photos to support many different customer environments

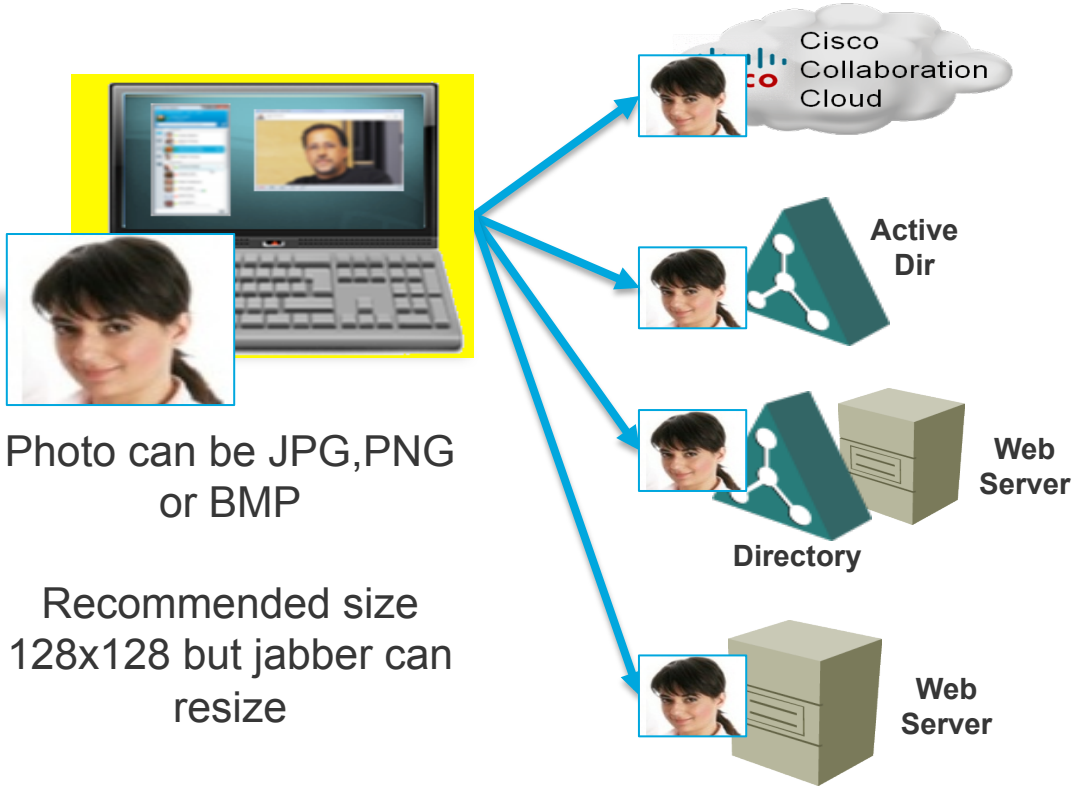


Photo can be JPG,PNG or BMP

Recommended size 128x128 but jabber can resize

Note: Option 2 & 3 phase object to detect binary object or URL

Option 1: Cloud Default (no config)
WebEx Contact Photos

Option 2: On Prem Default (no config)
Active Directory Binary Objects
Retrieve binary photo from thumbnailPhoto attr
load with Powershell

Option 3: On Prem
PhotoURL Attribute/ Retrieve URL
http://photo.example.com/staff/msmith.jpg

Option 4: On Prem (XML config)
URL Substitution/Macro style
http://photo.example.com/staff/%uid%.jpg

Jabber will also retrieve thumbnail photos from MS Outlook for personal contacts if photo avail

Jabber Contact Sources

Retrieving Photos for Contacts

EDI Photo Service Configuration – XML file settings

- Number / Name resolution should be configured/operational
- Use custom configuration settings to configure photos
- Directory method

Photo Parameters	Example Value
PhotoSource	Client will parse attribute to binary object or URI

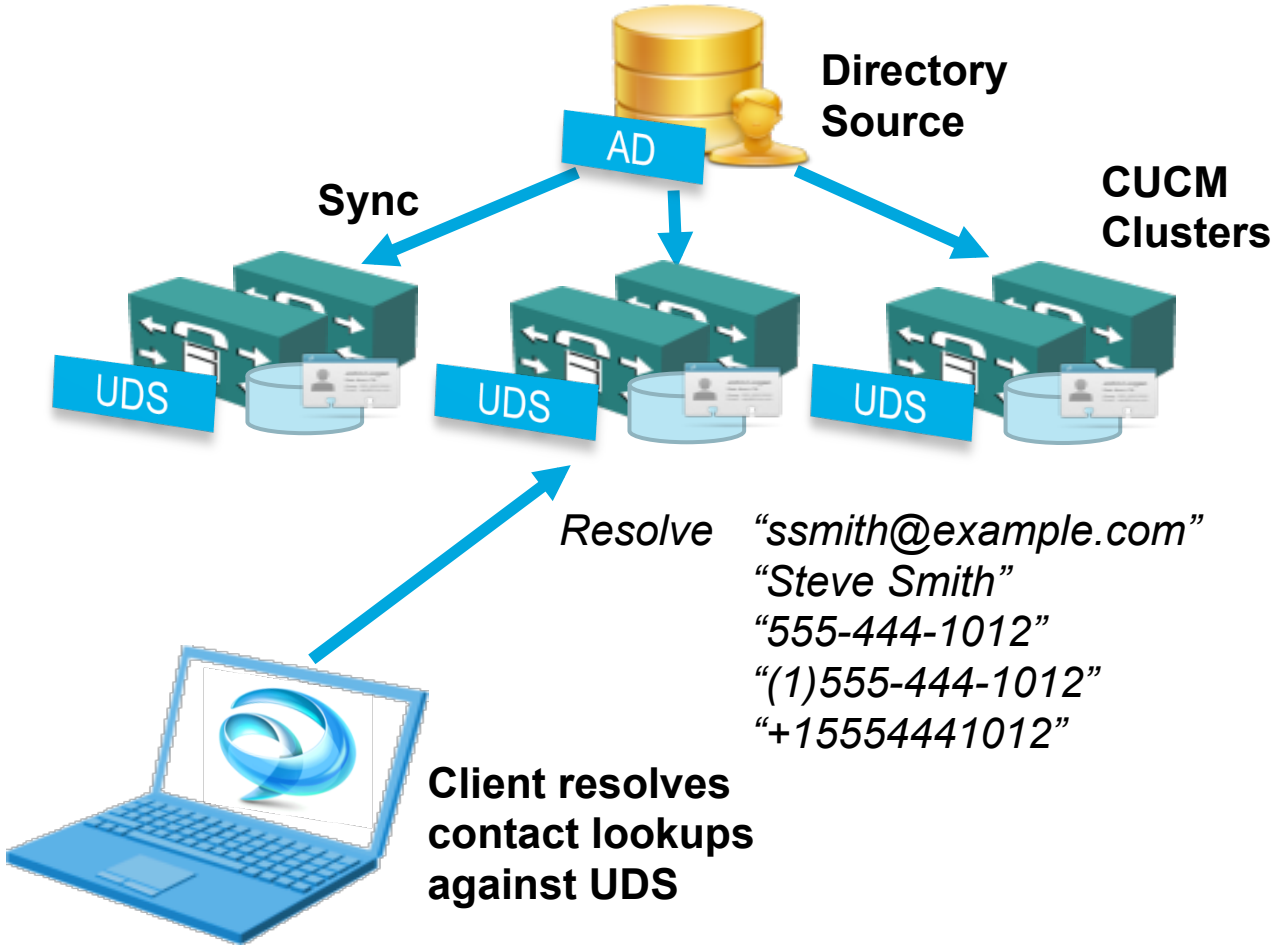
- Substitution method

Photo Parameters	Example Value
PhotoUriSubstitutionEnabled	True
PhotoUriWithToken	http://photosvr/dir/**sAMAccountName**.jpg
PhotoUriSubstitutionToken	**sAMAccountName**

Define in XML Config File

Jabber Contact Sources

UDS – User Data Services (Contact Service)



When using the UDS Contact Record Source the client performs contact resolution against communication manager.

The communications manager Universal Data Service provides an optimized contact lookup service from CUCM 8.6(2)

UDS provides a cross cluster contact service supporting up to 160,000 contacts.

UDS support being added to all Jabber clients.

Jabber Contact Sources

UDS – Configuration

UDS Record source is configured in UC manager 8.x via jabber-config.xml file

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Directory>
    <DirectoryServerType>UDS</DirectoryServerType>
    <PhotoURISubstitutionEnabled>True</PhotoURISubstitutionEnabled>
    <PhotoURISubstitutionToken>uid</PhotoURISubstitutionToken>
    <PhotoURIWithToken>http://10.53.54.240/staff/%%uid%%.jpg</PhotoURIWithTo
  </Directory>
</config>
```

Software Deployment

Client Deployment

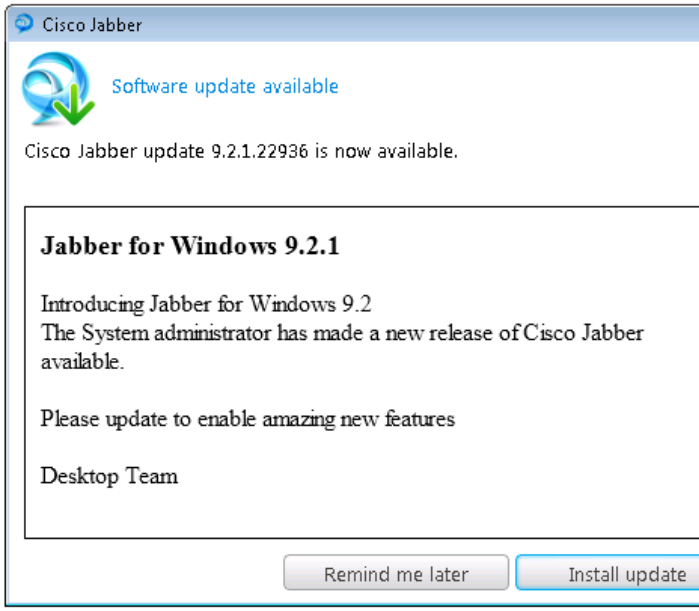
Jabber for Windows is shipped as an MSI Installer

- Windows XP 32bit, Vista 32/64 bit, Windows 7 32/64 bit and Apple OS X

Jabber doesn't need to prompt users for server addresses.

- Package the client for your organisation
- Use SRV service discovery
- Use Installer command line options
- Use Installer properties file

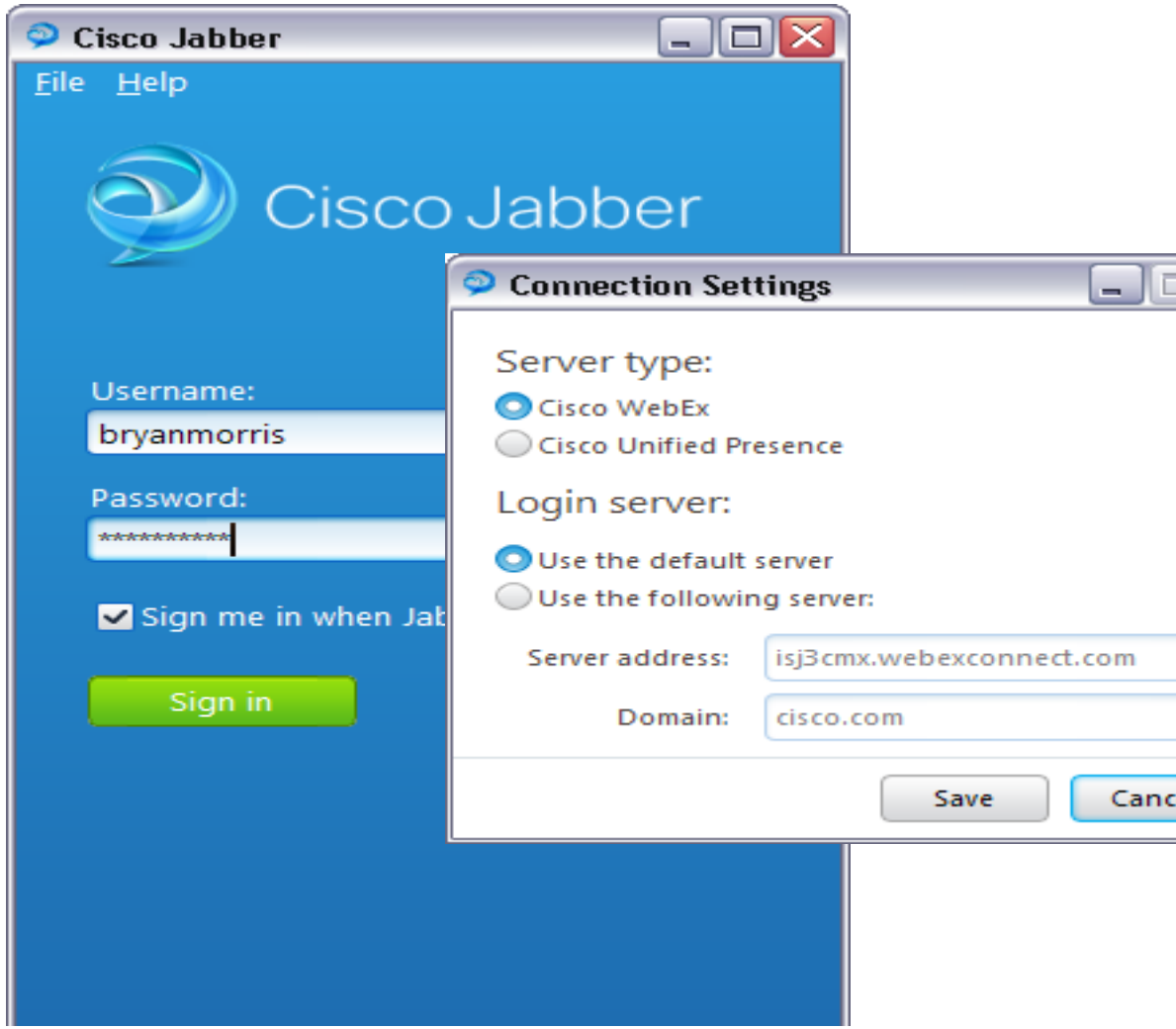
Client can check for updates on start-up



Software Deployment

Manual Service Configuration

- Server and server type can also be manually configured in Jabber client.
- Settings can also be configured during installer
- Admin can specify installer parameters to select presence server



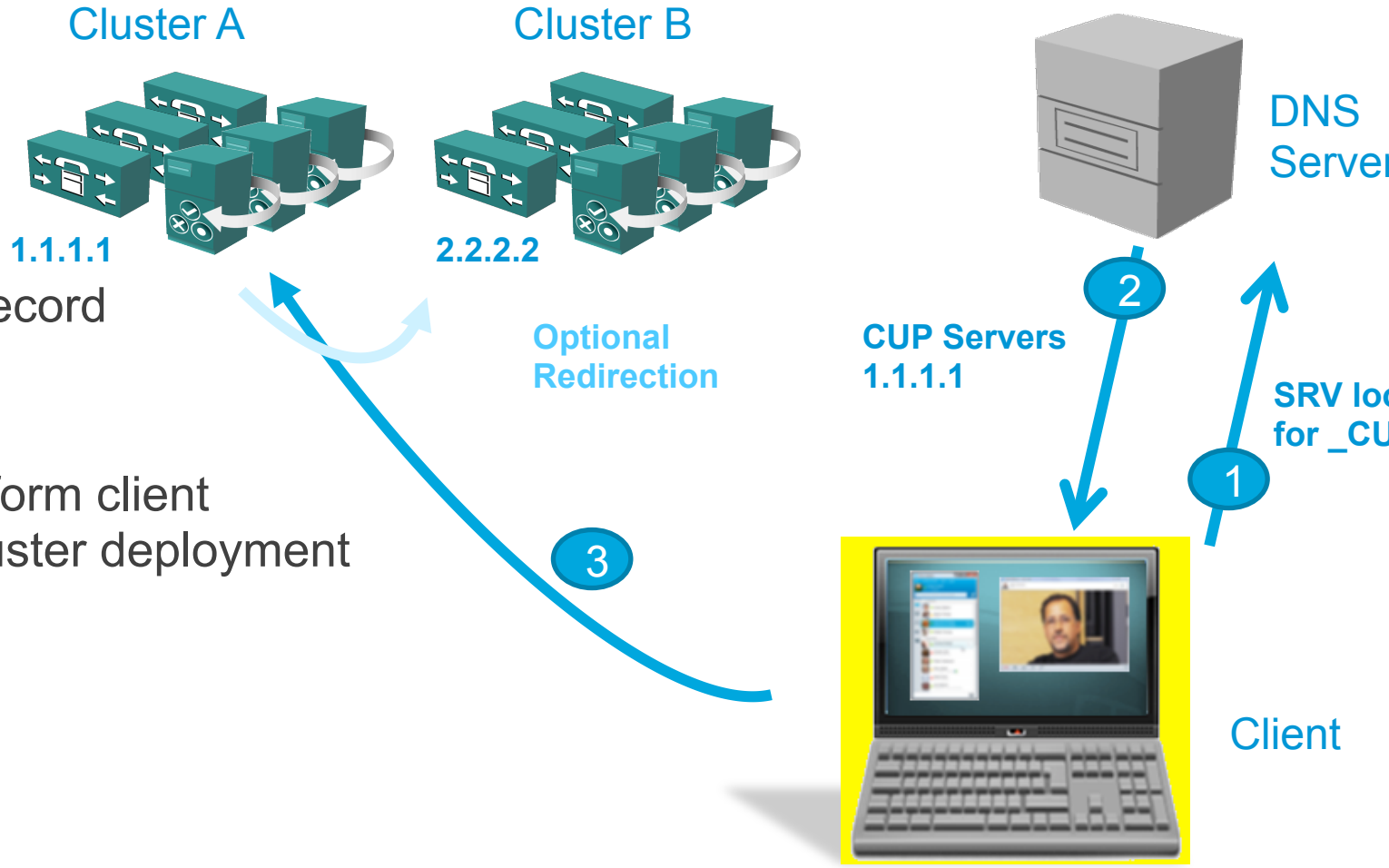
Software Deployment

DNS SRV Service Discovery

Jabber windows can use DNS SRV records for IM & P service discovery

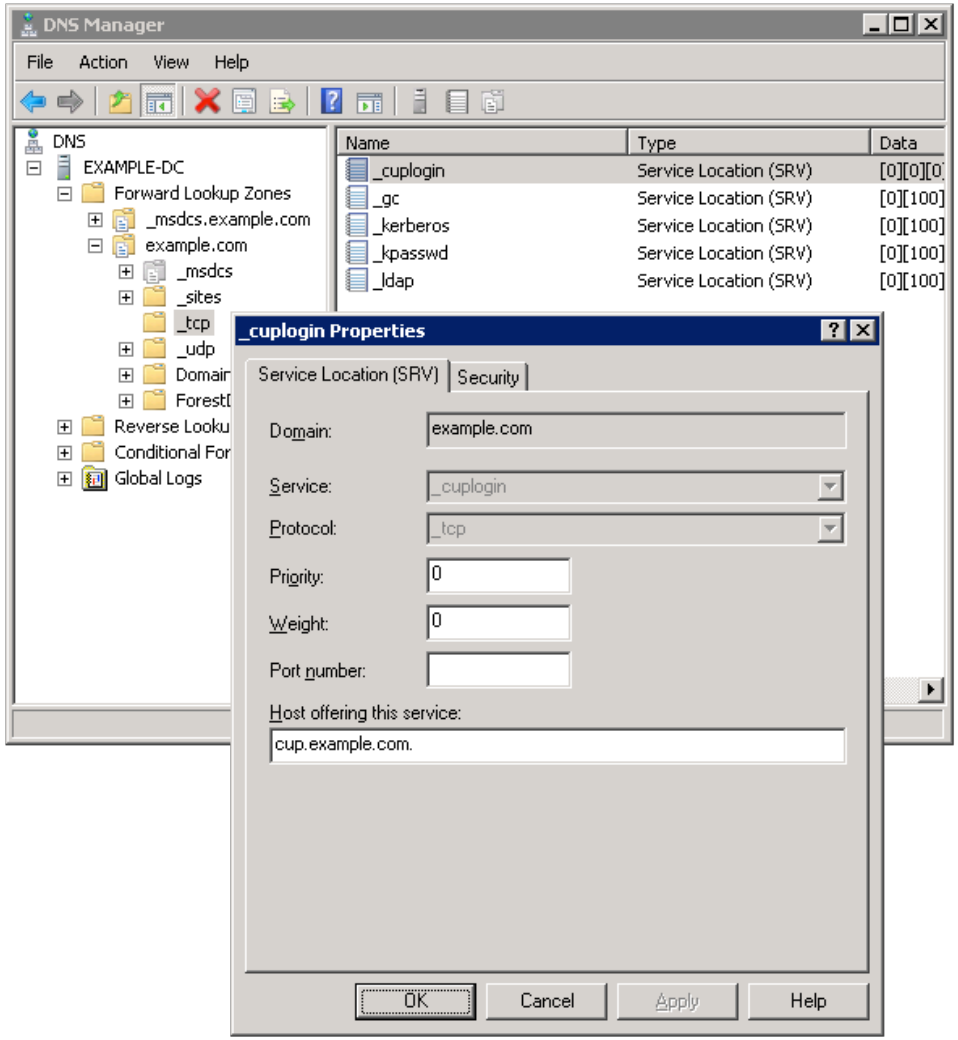
Admin defines SRV record in DNS server

IM&P cluster can perform client redirection in multi cluster deployment



Software Deployment

Creating DNS SRV Record



SRV record is created in DNS server

In DNS Manager create SRV record with:

Server:_cuplogin

Protocol:_tcp

Unified Communications

Modes of Operation

Desk Phone Mode

Jabber client controls Cisco Phone to make and receive calls.
Includes Video for Cisco Voice handsets

Soft Phone Mode

Audio uses sound devices on workstation. Video is displayed on workstation, audio is via headset (recommended) or PC Speakers.

Extend & Connect Mod

Control PBX/PSTN Phone from Jabber (Requires UC Manger 9.1 which must be connected to PBX via SIP/Telco trunk)

Clients can be configured for all modes of operation

Voice/Video only available now in Jabber 9.2

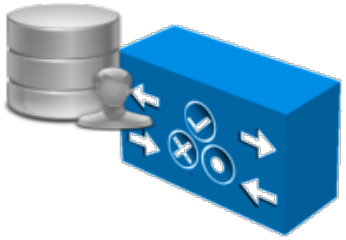
Unified Communications

Voice and Video

Unified Communication Manager

User Data

Call Control Server



User Data

IM & Presence Server

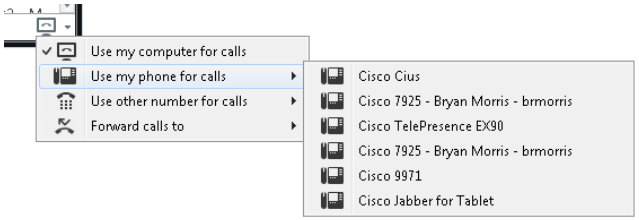
Jabber Client

Jabber User [User@XMPP Domain]

Jabber connect to UC Manager using CCMCIP(UDS) to Populate device list

If connecting in Soft phone mode Jabber connects as a SIP / CSF endpoint

If connecting in Desk phone mode Jabber connects to manager with CTI



Unified Communications

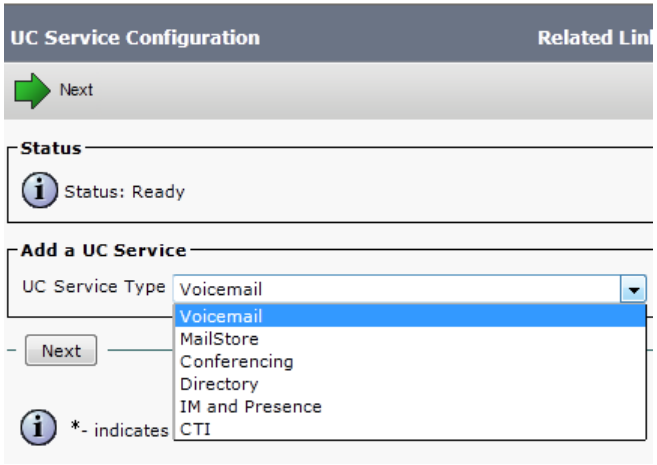
Client Configuration

Jabber / UC Manager User

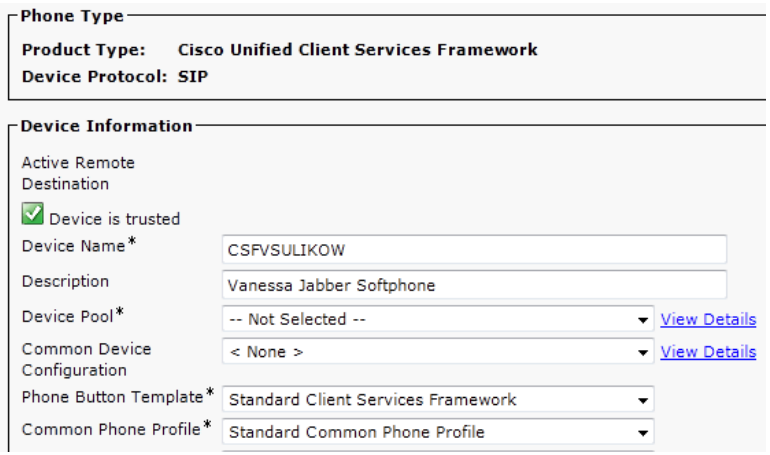
Profile for UC Services

Device Types – eg CSF, TAB, BOT, TCT

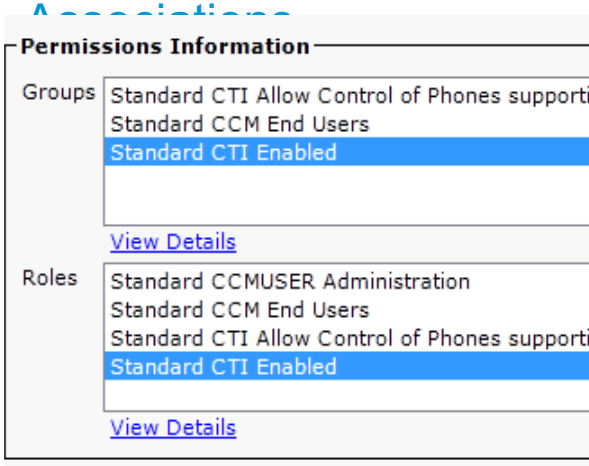
User Roles, Rights and Associations



Configure Profiles



Add Devices



Assign Rights

Unified Communications

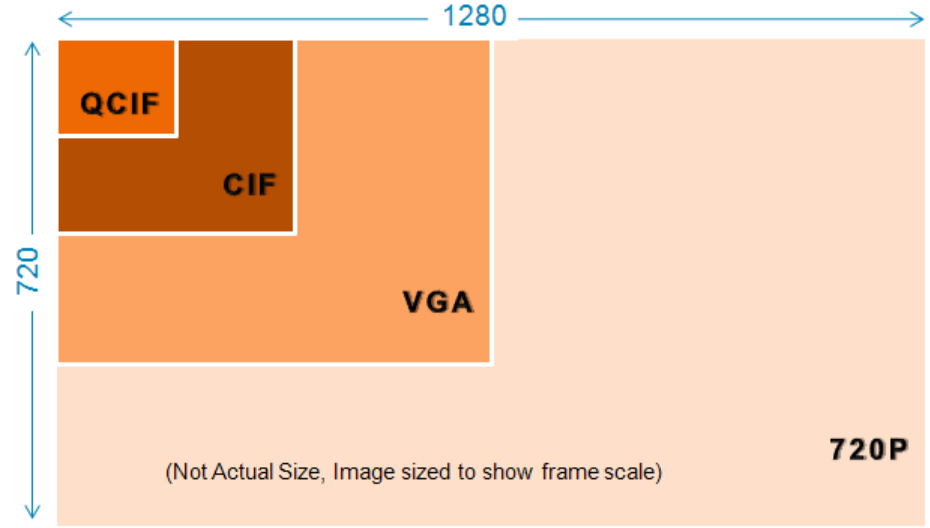
Cisco Jabber Video Engine

- Cisco Jabber Video Engine is a **H.264 AVC standard based media engine** using in Cisco Jabber clients.
- The Engine provides **full HD interoperability** between Jabber desktop clients and telepresence solutions.
- Provides **standard based audio** (G.711a/u, G.722.1, G.729a)
- Provides **Video rate adaption** and support for **Cisco ClearPath** Media Resilience Mechanisms. (Rate adaption required RTCP)
- Supports frame sizes from **QCIF to 720p HD** at up to **30 frames per second.**

Unified Communications

Cisco Jabber Video Engine

Supported Encoding for transmit



QCIF (176 x 144) @30fps
CIF (352 x 288) @30fps
w288p(512 x 288) @30fps
q720p (640 x 360) @30fps
VGA (640 x 480) @30fps
w448p(768 x 448) @30fps
w576p(1024 x 576) @30fps
w720p (1280 x 720) @30fps

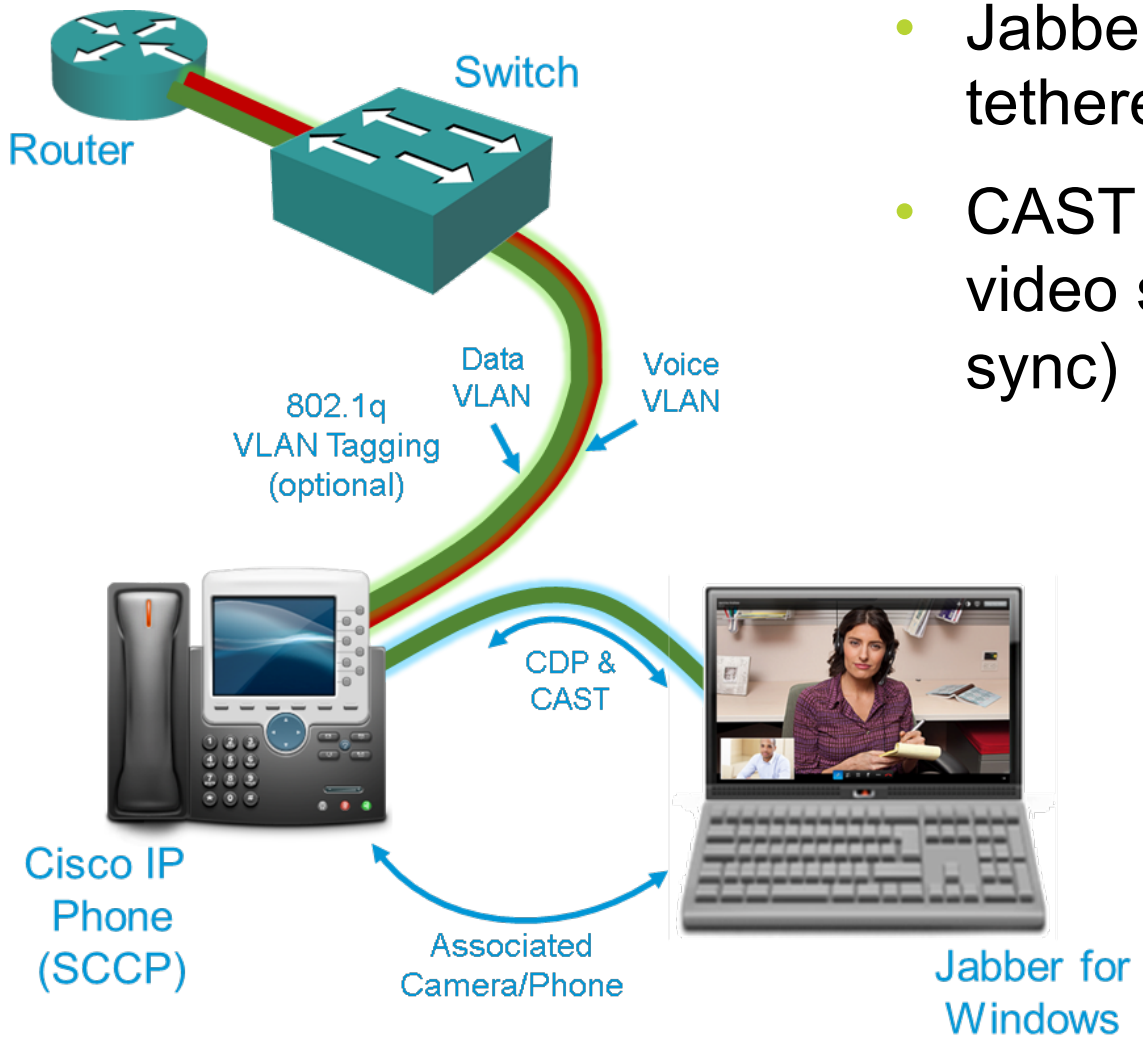
Client will decode any resolution within negotiated H.264 level

Factors which influence video frame rates

- Camera / Light Conditions
- Network conditions
- CPU and load on receiver
- Rate encoded by sender
- UC Manager configuration
- Rate Adaption (RTCP)

Unified Communications

Desk Phone Video



- Jabber uses CDP protocol to discover tethered Cisco Phone.
- CAST protocol is used to negotiate video sessions based on call setup (lip sync)

- Jabber controls the phone using CTI protocol in desk phone mode
- CDP/CAST support is provided by Cisco Mediane MSI installer.
  (must be present)

Unified Communications

Multi-Party Voice & Video Calling

- Jabber clients support multi-party conferences
- Ad-hoc conference uses Media groups in UC Manager
- Conference capability will depend on DSP architecture available in media resource group
  - Audio only
  - Audio and video
- DSP provided by
  - Software bridge only
  - Router DSP Farm
  - Multi-point conference unit
- Scheduled video conferences call also supported

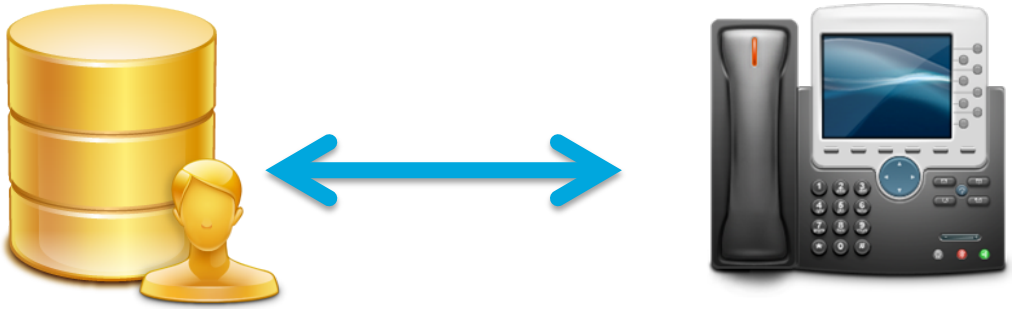
Video Multipoint Conferencing Units

Cisco TelePresence MCU 4500 Series
Cisco TelePresence Server 7010
Cisco TelePresence Server 8000
Cisco Integrated Services Router (with PVDM3)

Unified Communications

Dial Plan Considerations

Directory Number
+14085253777



Destination Numbe
883777

If UC Manager dial plan does not match the LDAP dial plan you may need to use rules or translation patterns.

When initiating calls we need convert E.164 numbers to the UC manager dial plan → Application Dial Rules, Translation Patterns

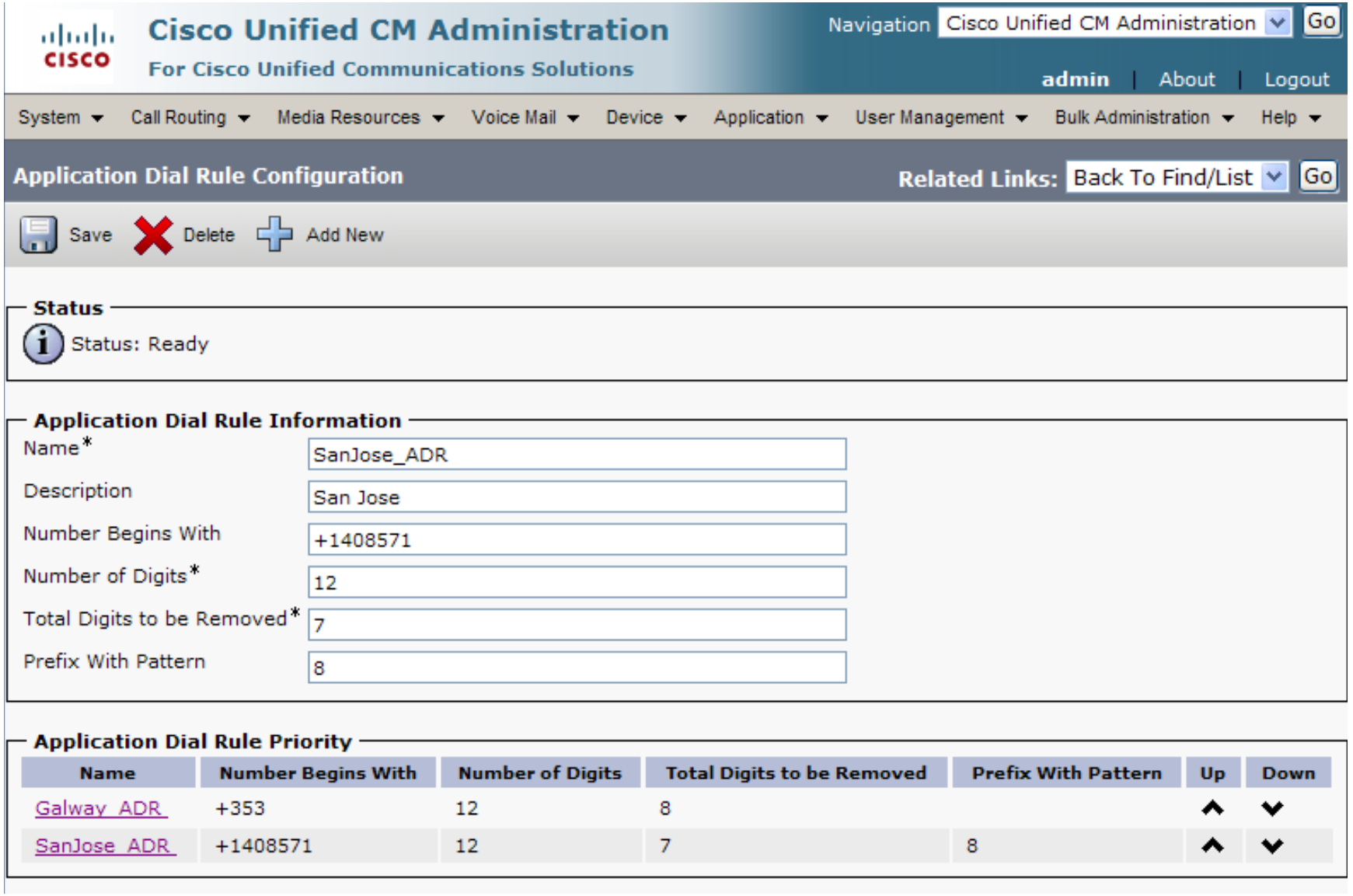
When receiving calls we need to extend internal numbers to E.164 → Directory Lookup Rules, PhoneLookupMasks

Rules are created on CUCM and downloaded using TFTP

A COP file must be applied to update dial rules

Unified Communications

Dial Plan Mapping



Unified Communications

Using Phone Masks for Formatted Strings

A phone mask can be used if your directory has formatted number strings in phone attributes

A phone mask can be used to add brackets, spaces, dashes and other character to a number string before a search

+(1) 408 555 0100

+1-510-5550101

A phone mask is a client configuration parameter and is part of the EDI custom director configuration

Phone mask	
PhoneNumberMasks	+1408|+(#) ### ### ####|+1510|+#-###-########

Single parameters supports multiple masks, format is area code (pipe) mask. Use pipe for additional masks.

Unified Communications

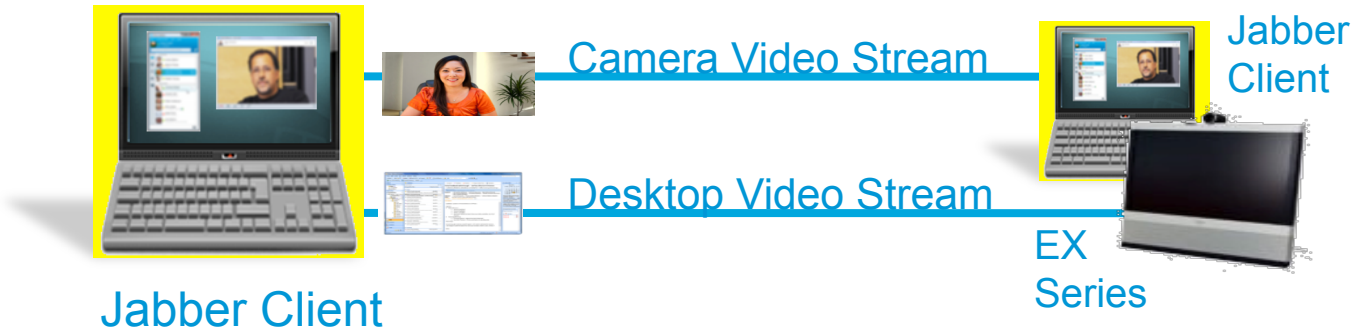
Configuring Video Desktop Share

Jabber for Windows supports Binary Floor Control Protocol (BFCP) for desktop sharing (RFC 4582).

BFCP will encode a video stream of the senders desktop, this can be in addition to a camera video stream.

Video desktop sharing can be between Jabber client and Cisco Video endpoints

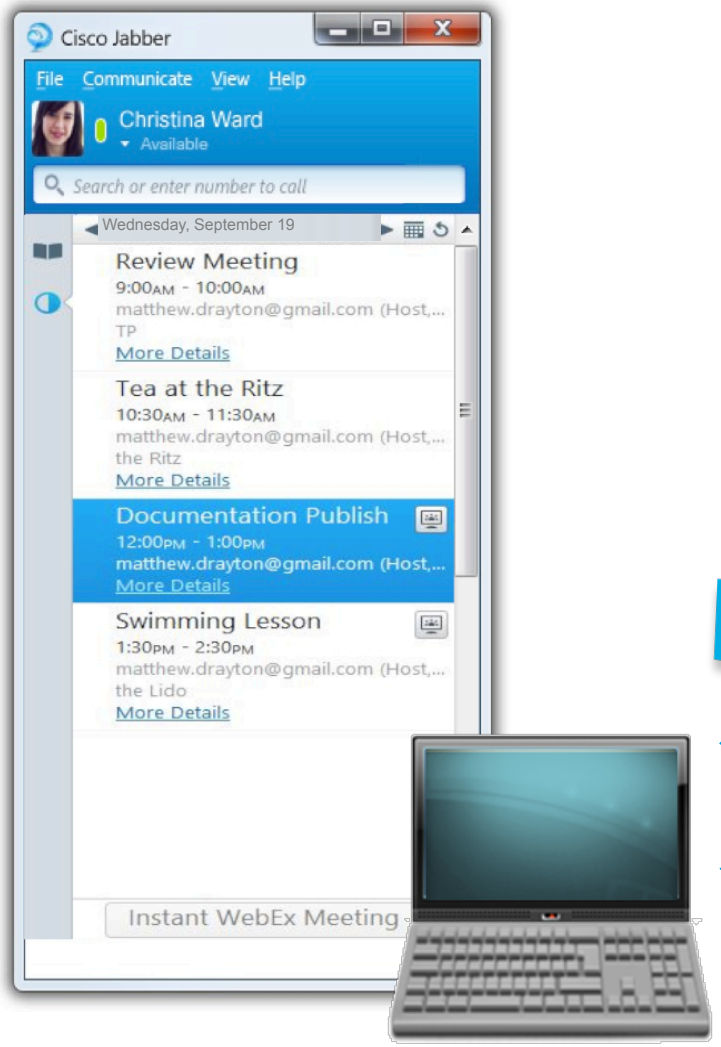
Requires UC Manager 8.6 and based on version may require COP file



Device Configuration or SIP profile

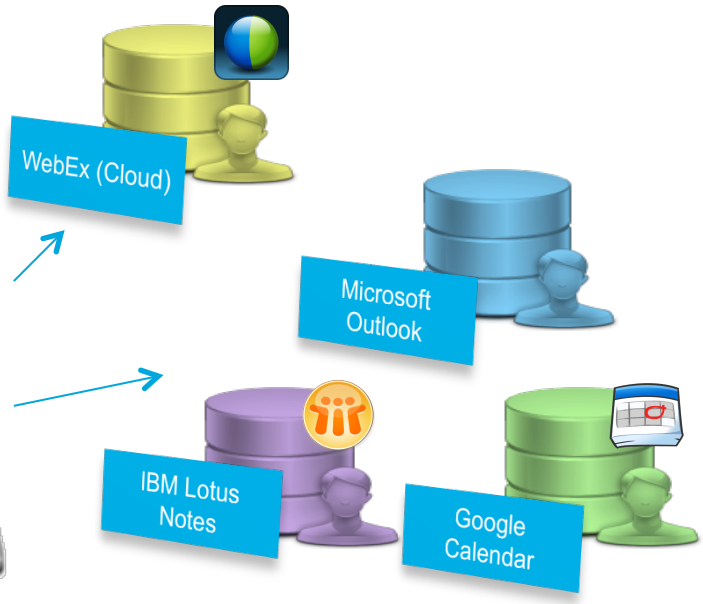
Cisco WebEx Meetings

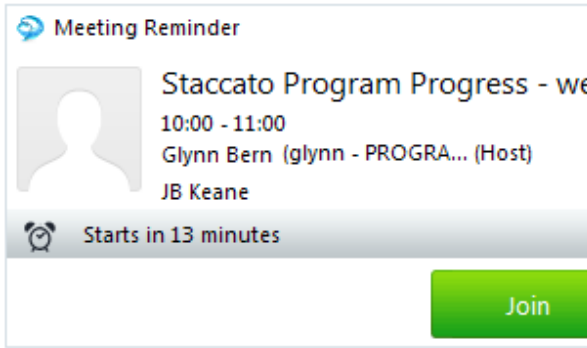
Calendar Integration



Jabber will show a schedule of WebEx meetings and other appointments in a Jabber Tab.

Meetings information is retrieved from WebEx Meetings services as well as a choice between Microsoft Outlook, Lotus Notes or Google calenda





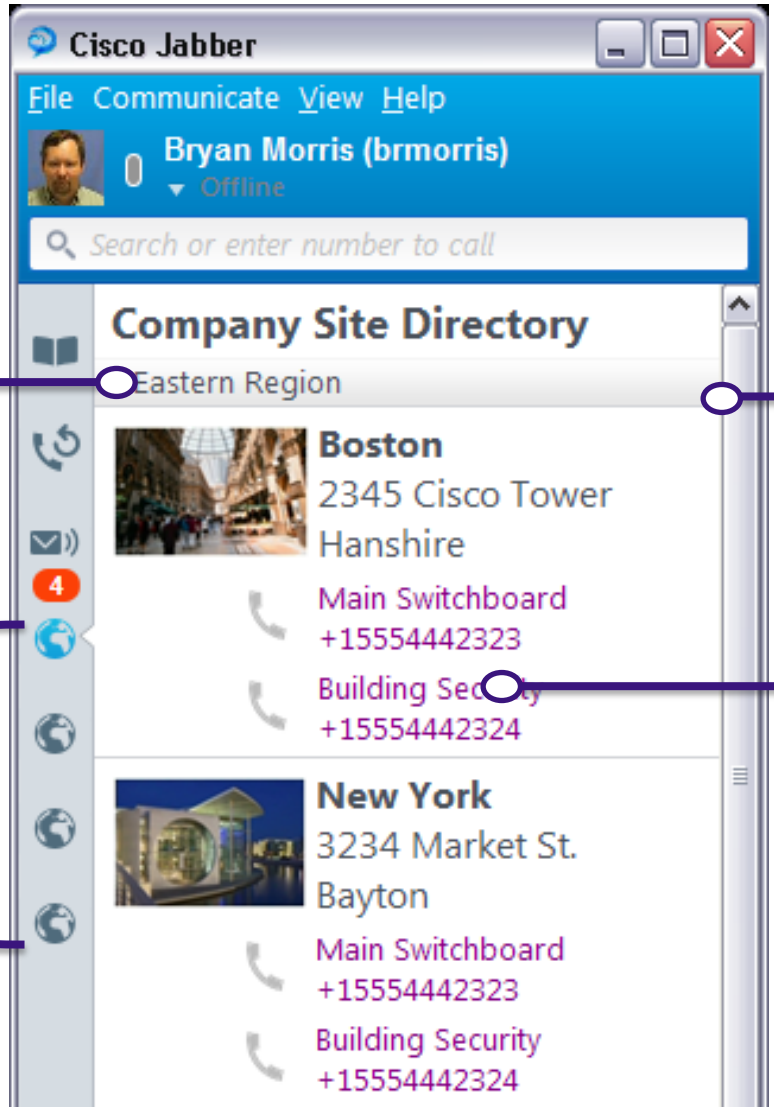
Extending Cisco Jabber

Extensible Tab / HTML Apps

Jabber uses the Segoe UI font which can be applied using CSS for common UE styling

Up to 4 user defined tabs can be created

If no Icon is created default globe icon is displayed



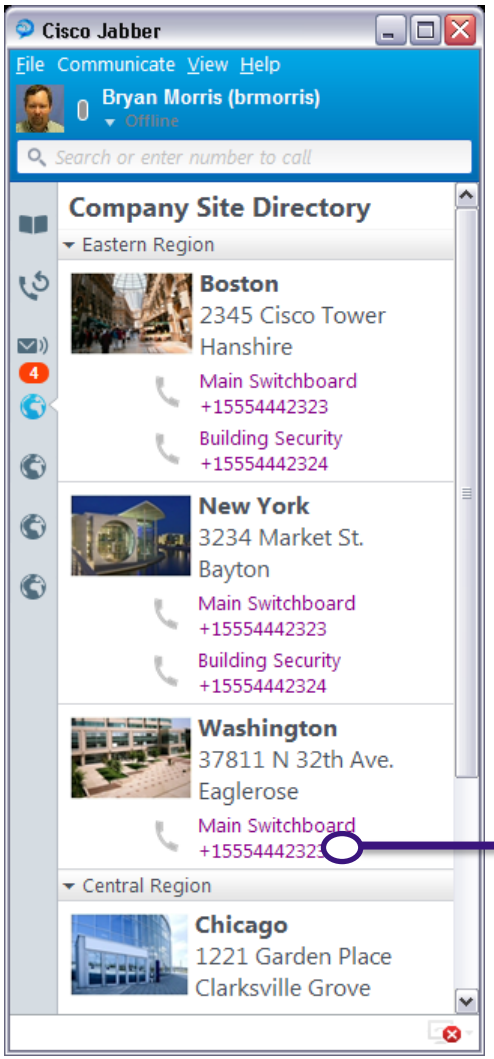
HTML window instance running in c

HTML apps can leverage IM and Call URI for click to X

Jabber SDK could used to provide fu functions.

Extending Cisco Jabber

Creating dynamic tabs with URI's



TEL: URI

Administrators can include URL's in the HTML to provide cl
X functions:

This include

XMPP:
Start an IM conversation with a contact

TEL:
Make a call to a number (with confirmation, RFC base

Clicktocall:
make a call to a number without confirmation

Extending Cisco Jabber

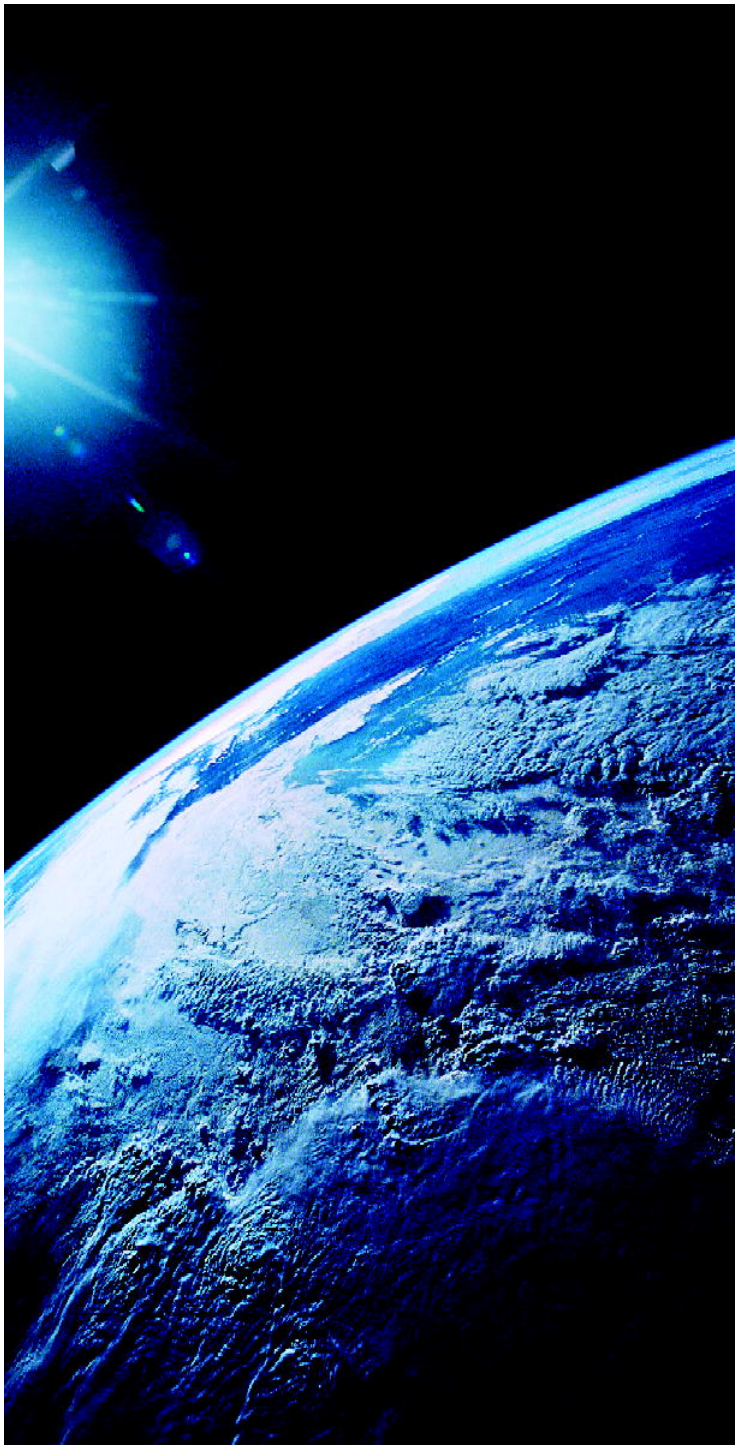
Custom Tab – Configuration File

- All tabs are held in the custom configuration file

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
<jabber-plugin-config>
            <browser-plugin>
          <page refresh="false" preload="true">
                  <tooltip>Sample App</tooltip>
                  <icon>http://server_name.example.com/icon.png</icon>
                  <url>http://example.com/app</url>
          </page>
          <page refresh="true" preload="true">
                  <tooltip>Cisco</tooltip>
                  <icon>http://server_name.cisco.com/logo.gif</icon>
                  <url>http://www.cisco.com</url>
          </page>
            </browser-plugin>
        </jabber-plugin-config>
  </Client>
</config>
```

Registry Settings are no longer used for Tab configuration

ntegrace Cisco UC MS OCS/Lync



Cisco and Microsoft Advanced Call Control Design

General Thoughts on Split Brain

all Routing

Explicit vs. implicit reachability

- Explicit: each call control has explicit routes to any destination
  - Possibly based on prefix based routing (e.g. with +E.164)
  - Static or Dynamic?
- Implicit: the call controls use some form of hunting
  - Route list in Unified CM used with “Stop Routing On…” service parameters
  - Search rules in VCS

mplicit reachability (hunting) requires loop detection/prevention

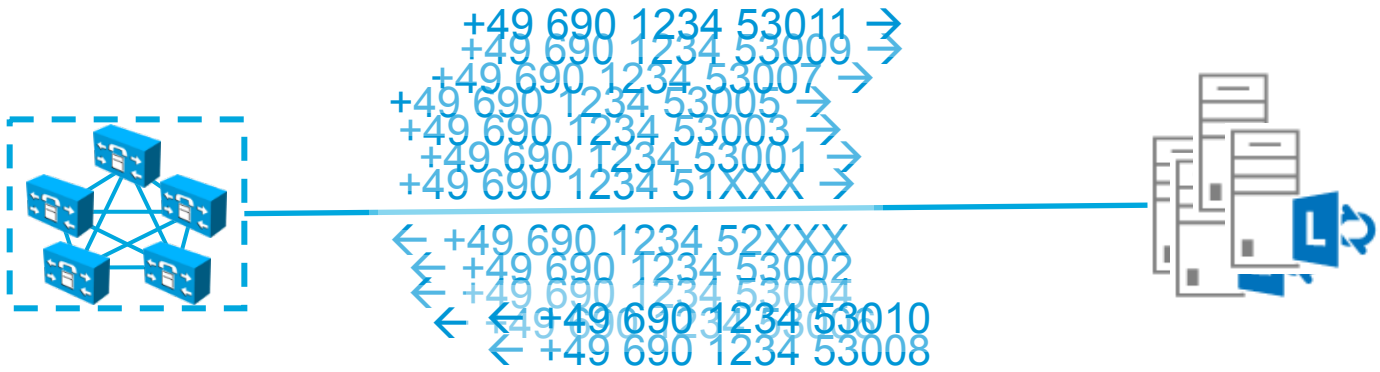
- VCS not routing back to source zone
- Prefix based routing avoiding loops (trunk specific CSS in Unified CM)
- SIP hop count: decremented with each routing step

xplicit Routing (Deterministic)

Each call control has explicit routes to all destinatons remote from the local call control

Only scales with prefix-based summarized address separation

With arbitrary distributed destinations too many route entries have to be maintained



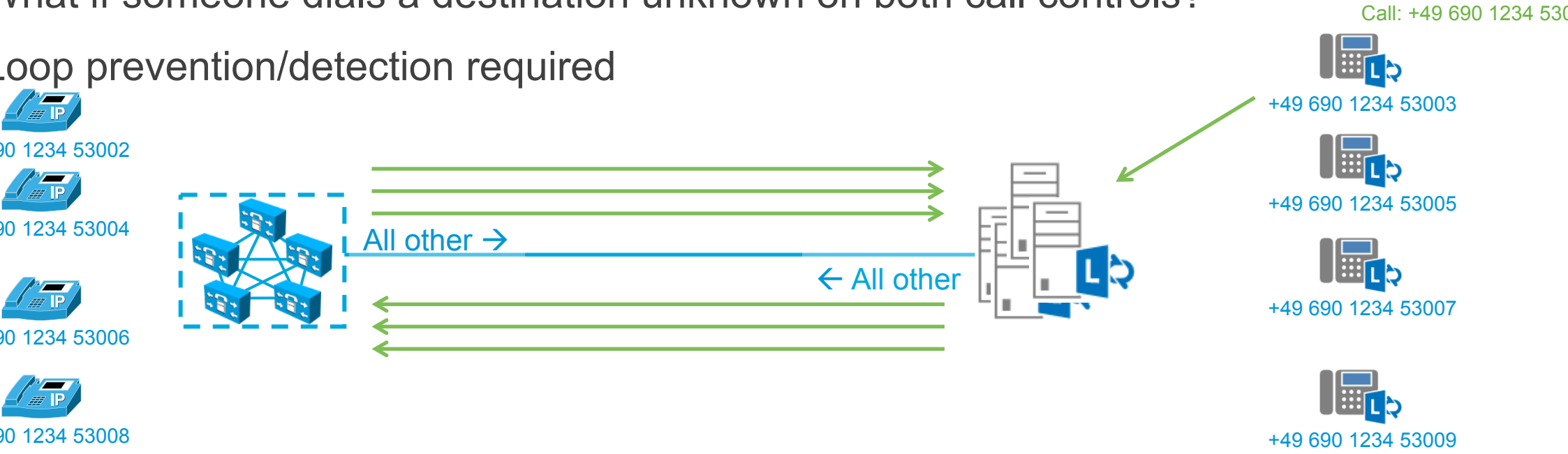
nplicit Routing (Hunting)

Each call control simply routes all non-local traffic to remote call control

non-local”: based on provisioned local addresses

What if someone dials a destination unknown on both call controls?

Loop prevention/detection required

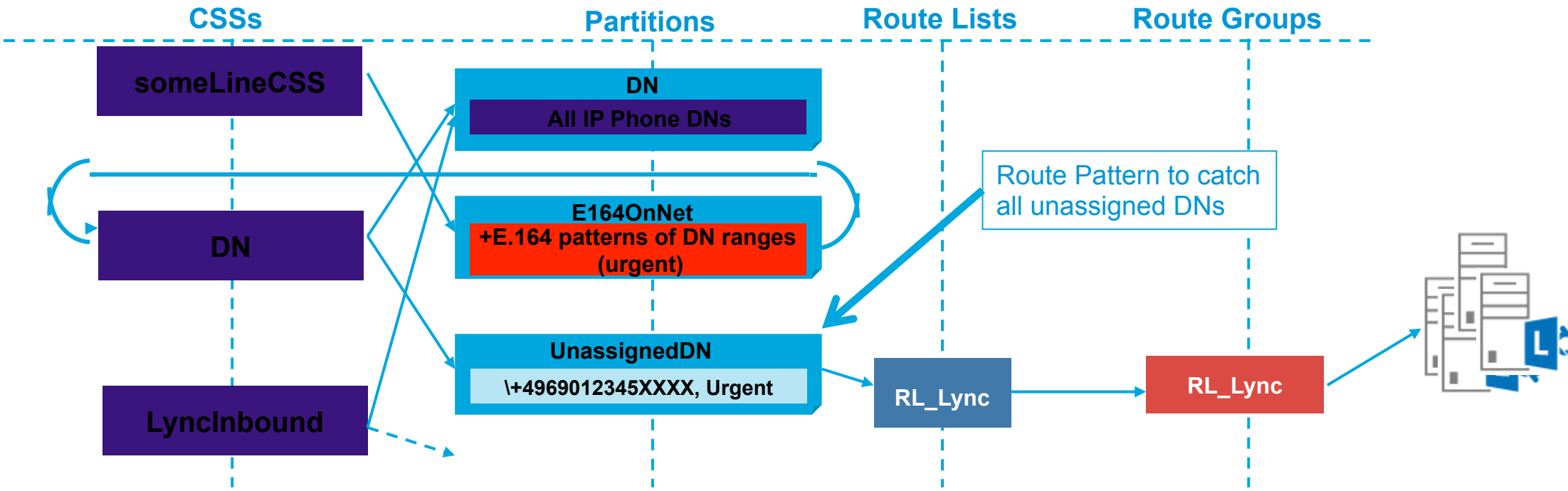


oop prevention

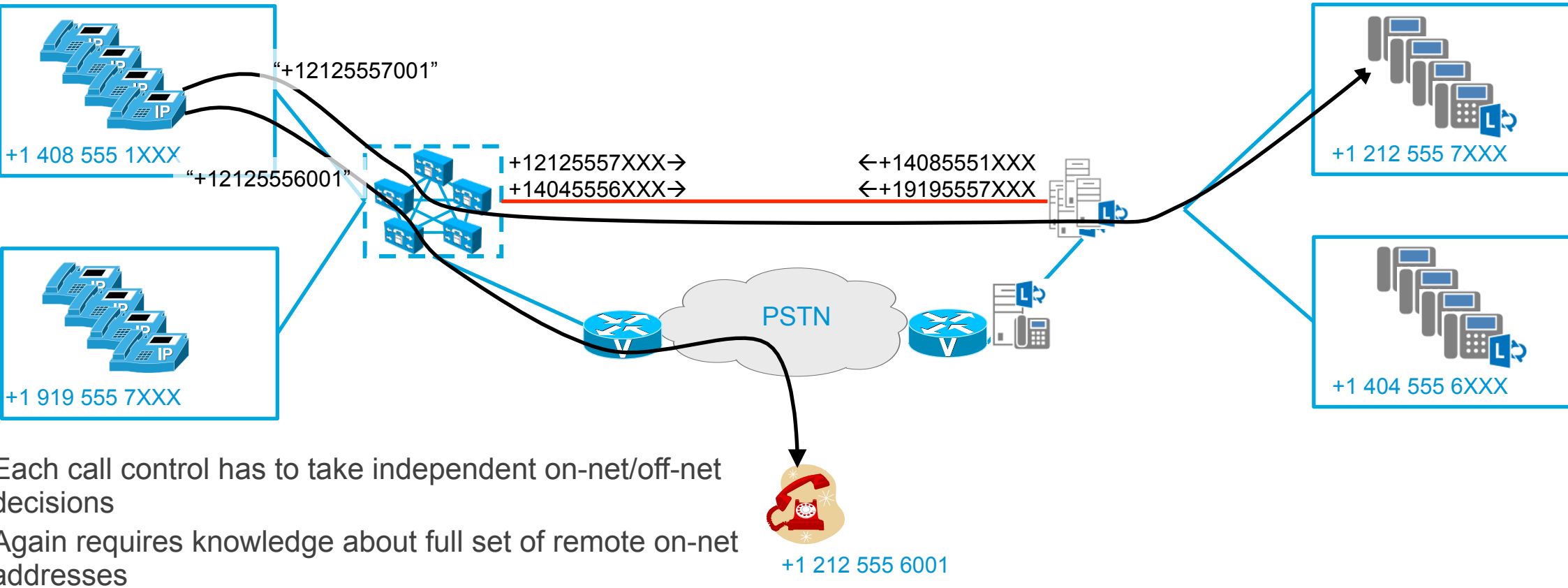
On UCM simply make sure that an inbound call from a trunk can not be routed back to he trunk

- "Default" route pattern not accessible by trunks inbound CSS

Note: VCS will by default not route a call back to the zone it came from

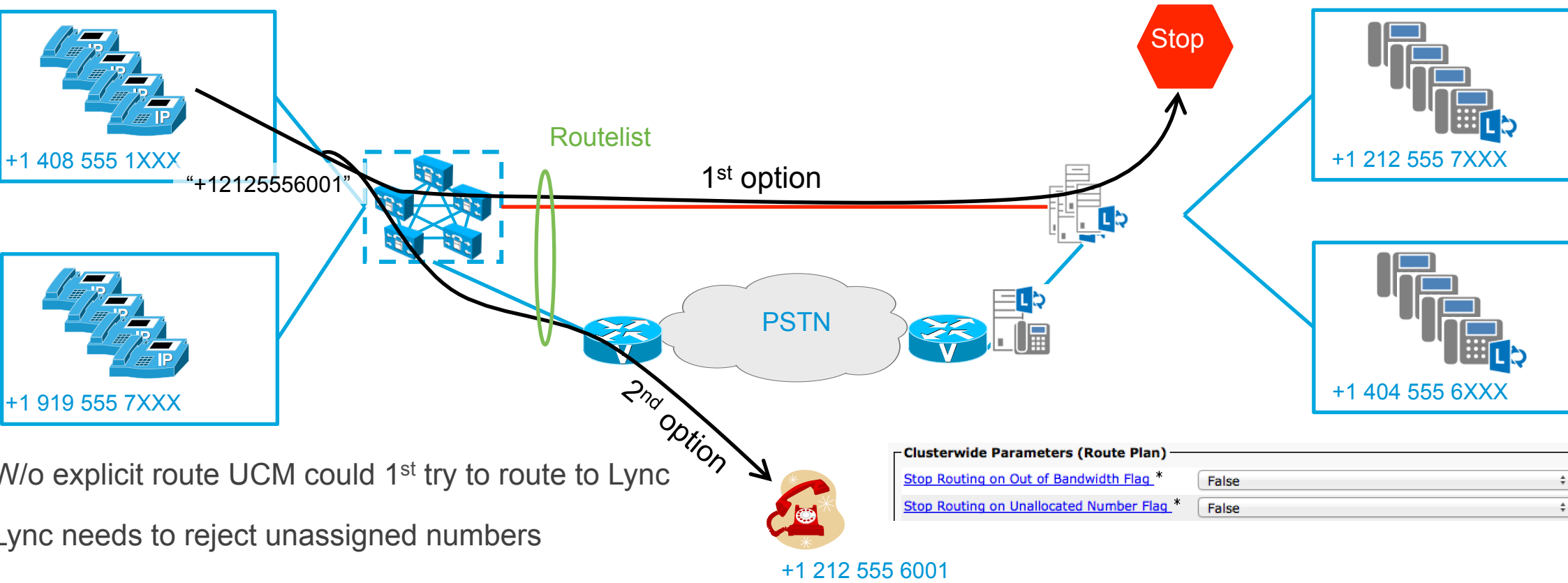


istributed On-Net/Off-Net decision w/ multiple call ontrols and independent PSTN access



- Each call control has to take independent on-net/off-net decisions
- Again requires knowledge about full set of remote on-net addresses
- W/o deterministic routing this gets more complex

istributed On-Net/Off-Net decision w/ multiple call ontrols and independent PSTN access (hunting)



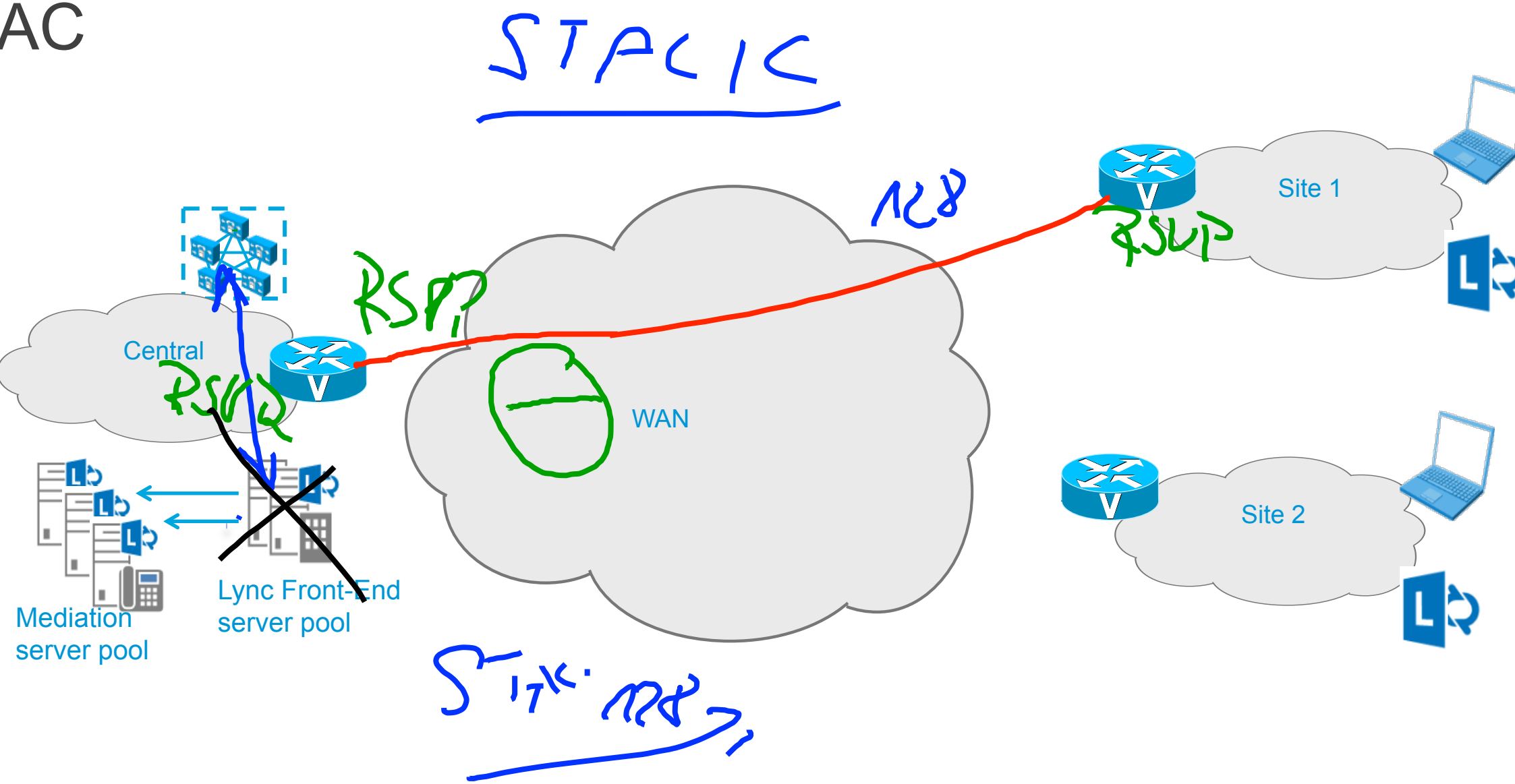
W/o explicit route UCM could 1st try to route to Lync

Lync needs to reject unassigned numbers

UCM can continue to route on unassigned number

Global service parameter setting

AC

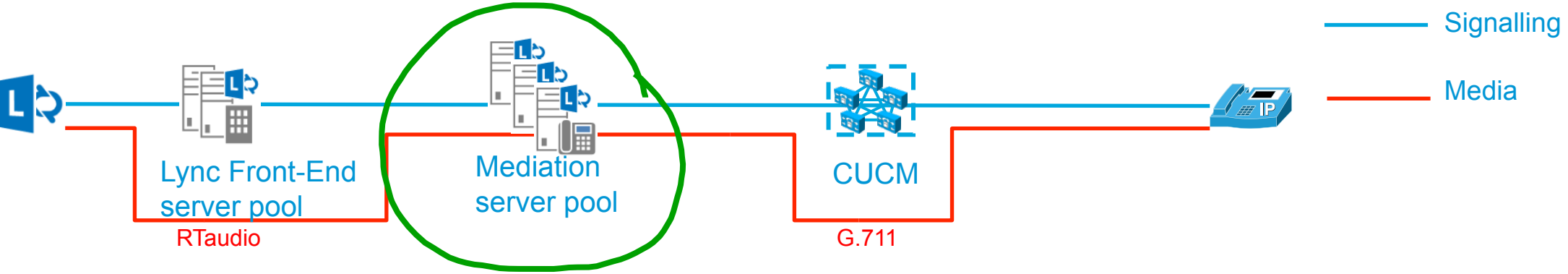

Central
WAN
Site 1
Site 2
Lync Front-End
server pool
Mediation
server pool

Call Routing

tandard Topology for Lync Integration

- Direct SIP trunk integration requires Mediation Server
- Mediation server starting with Lync 2010 supports media bypass
  - Always or based on site and region information
  - Media Bypass and MSFT CAC are mutually exclusive: bypassed calls are not subject to MSFT CAC
- Media bypass requirements
  - Mediation server must support multiple forked responses (early dialogs)
  - Mediation server must accept media directly from Lync endpoints
  - Lync clients and mediation server peer need to be “well connected” ☺ (no CAC → no BW constraints)

ync w/o media bypass



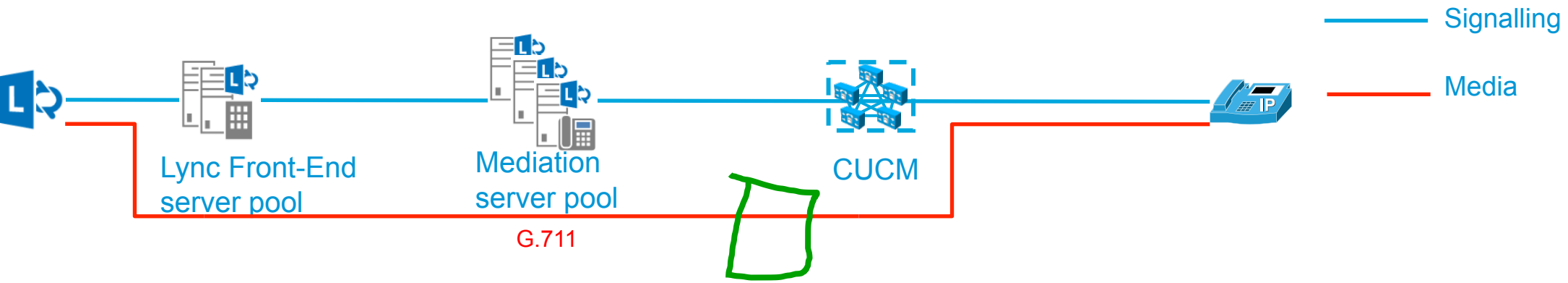
Without media bypass direct SIP trunk requires media to pass through mediation server

roblems:

- Mediation server scalability (transcoding)
- Mediation server selection for inter-system intra-site calls requires complex mediation server and trunking system to avoid media hairpinning

ync 2010 introduced “media bypass” which promised to solve these problems

ync with media bypass



With media bypass media does not have to traverse through a mediation server any more

Direct media (no RTaudio) between Lync client and Unified CM endpoint

Really?

edia Bypass Requirements

ttp://technet.microsoft.com/en-us/library/gg398238.aspx

"Media bypass can be enabled only under the following circumstances:

- The ConcentratedTopology parameter is set to True
- ..."

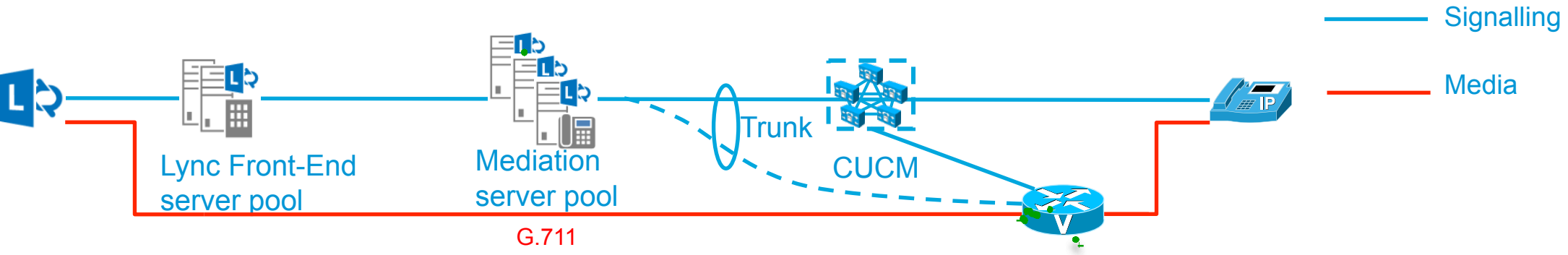
→ well-known media processor IP (MTP) required

Media Processor IP by default is the same as the signaling address

f MTP and signaling entity are different different Media Processor IP needs to be onfigured explicitly:

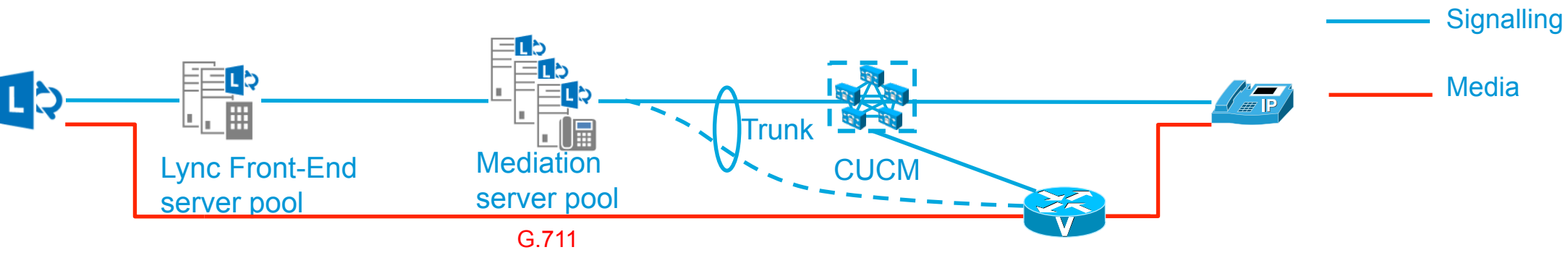
```
Set-CsPstnGateway … -RepresentativeMediaIP <IP address>
```

ync with media bypass; the truth (1)



- Media bypass requires a predefined next hop media IP address (MTP)
- GW definition has signaling and media next hop defined independently
  - MSFT always assumes that SIP trunks are terminated on ITSP GWs, GWs or IP PBXes
  - Completely ignore the reality that the whole idea of IP is to not tie media streams to central switches!
- Assumes “LAN like” conditions; Lync client “colocated” with next hop
  - No BW restrictions between Lync client and media processor
  - No requirement to CAC
- MTP selection controlled by Unified CM

ync with media bypass; the truth (2)



Media stream has to be bound to single IP address*

Single MTP per trunk → MRGL of inbound trunk on Unified CM only can have a single MTP

OS SW based MTP can be used for this role (no transcoding, pass-through)

*Needs to be verified w/ Lync 2013.

ync Media Bypass Design Considerations

Dynamic decision to bypass mediation server based on comparing “bypass ID”s of Lync client and gateway’s media processor IP

Media Bypass can be activated globally in two ways:

- Always Bypass:
  - all subnets mapped to one and only one bypass ID
  - Not compatible with MSFT CAC
- Use Site and region information:
  - Supports interaction with CAC
  - Single unique bypass ID per region
  - WAN connected site w/o BW constraint inherits region’s bypass ID
  - WAN connected site w/ BW constraint gets unique bypass ID
  - Subnets associated w/ site inherit site’s bypass ID

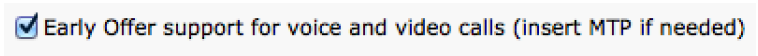
edia bypass and CAC

Media bypass and CAC both based on same site and region information

For media bypass and CAC to work media bypass has to be set to “Use Site and Regio
nformation”

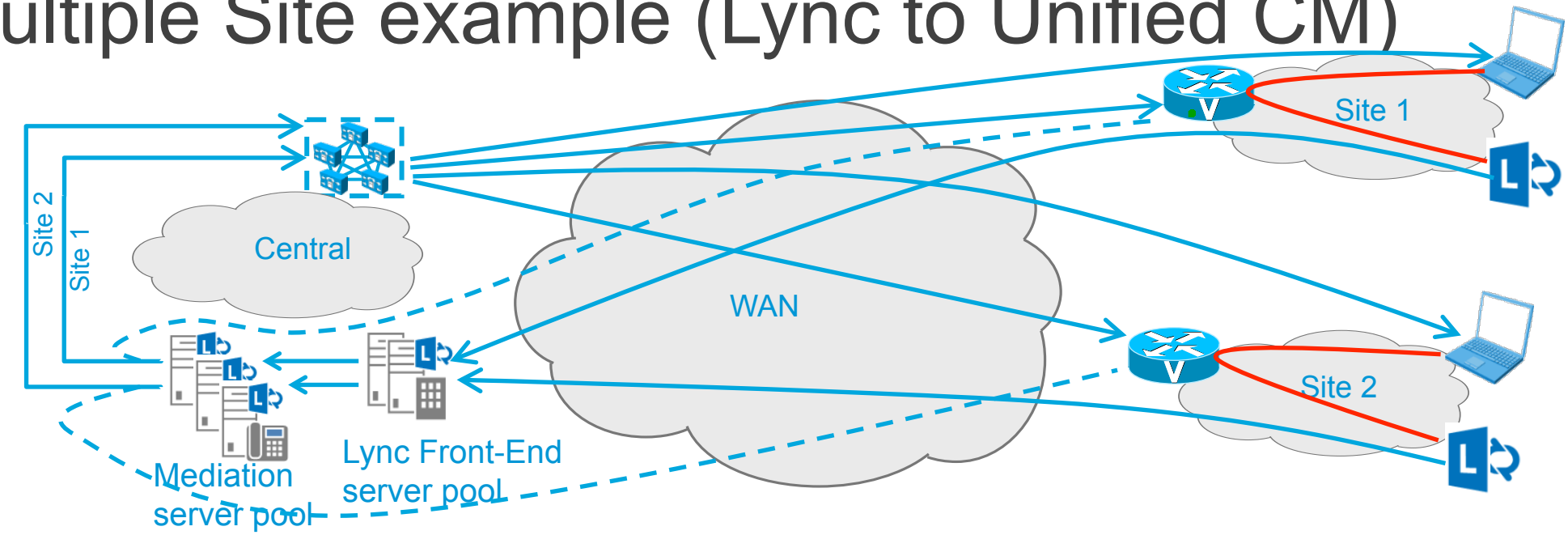
Media Bypass	CAC	Result
Use Site and Region nformation	On/Off	Bypass decision based on bypass ID. CAC only for calls that are not bypassed b/c media bypass assumes “LAN like” connection to peer. CAC only applied if CAC is enabled AND bypass IDs do not match
Always Bypass	On	Invalid
Always Bypass	Off	All calls bypass (single bypass ID), no CAC applied
Off	On	Mediation server always employed; CAC applied

CM SIP trunk characteristics

- Lync requires Early Offer inbound/outbound
- Although UCM now can do early offer w/o relying on an MTP
  - SIP profile setting: 

- … we still have to allocate a media resource (single media IP address in Lync GW definition)
  - Trunk setting: “MTP required”
- For every trunk we need a dedicated MRGL/MRG and a single media resource
- On UCM SIP trunk configure IP addresses of possible mediation servers as peers
- Multiple inbound SIP trunks with the same peer IP require different local signaling ports
  - Inbound trunk selection on UCM based on remote peer and local signaling port
  - Local signaling port defined in SIP trunk security profile

ultiple Site example (Lync to Unified CM)



- To keep media local to a site we need site local media resources
  - Alternate media IP definition in Lync trunk configuration matches
  - … IP address of single media resource in MRGL/MRG of the trunk on Unified CM side
- Multiple sites require multiple trunks
  - … and multiple MRGs, MRGLs and media resources
  - … and multiple SIP security profiles, because we need to be able to uniquely identify the trunk on UCM based on the signaling port (UCM side trunk identification based on peer IP address and local signaling port)

ultiple Trunks between Lync and Unified CM

At least single trunk per site so that we have at least one MTP “local” to each site

Trunk selection based on site of calling Lync client, to make sure that MTP is “local” to Lync client so that media bypass can be activated

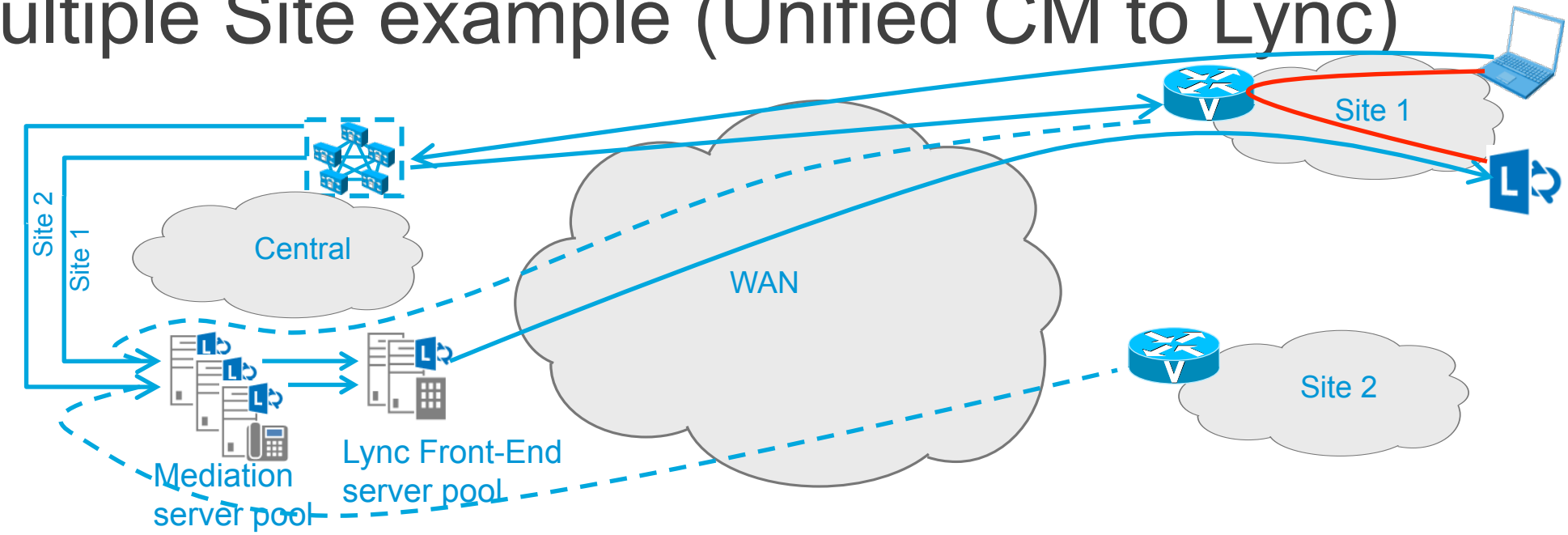
How do we select the correct trunk for calls from Unified CM to Lync?

Need to select a trunk with an MTP “local” to the called Lync client

Only “location” attribute we could use is the called number

… but is this sufficient?

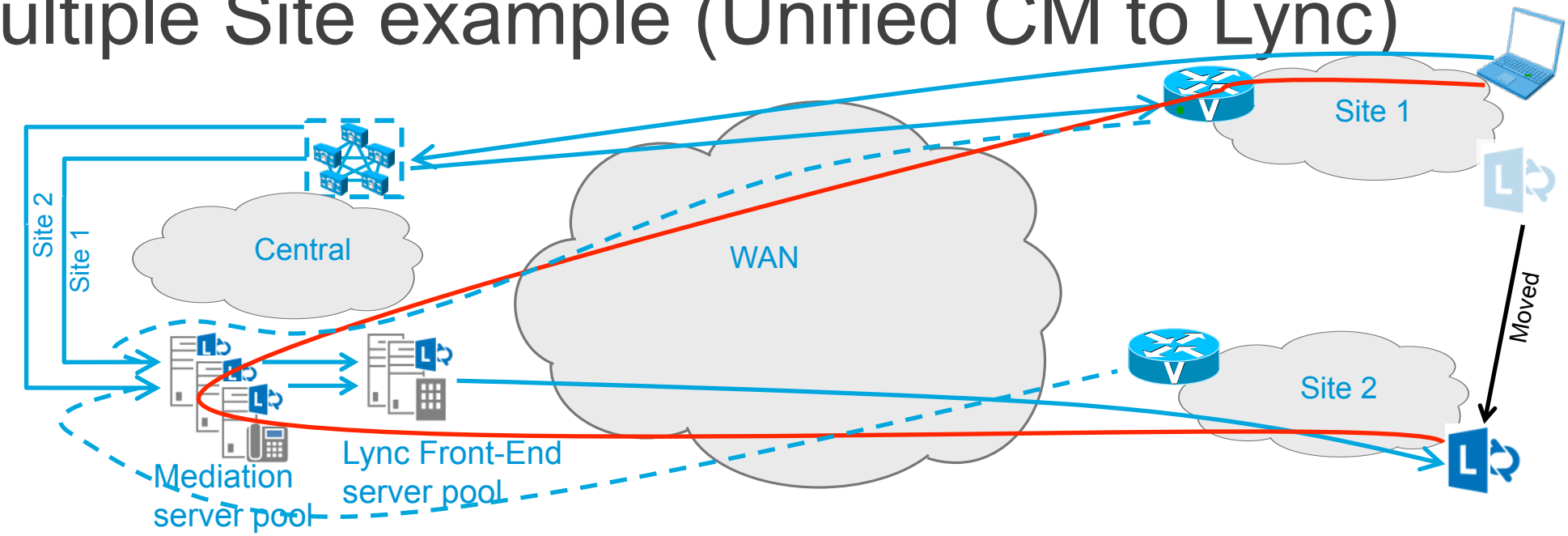
ultiple Site example (Unified CM to Lync)



Unified selects trunk to Lync based on called destination (+E.164 prefix)

- MTP (assumed) local to Lync client selected
- Alternate media IP definition in Lync trunk configuration in same site as Lync client
- →bypass activated,
- local media

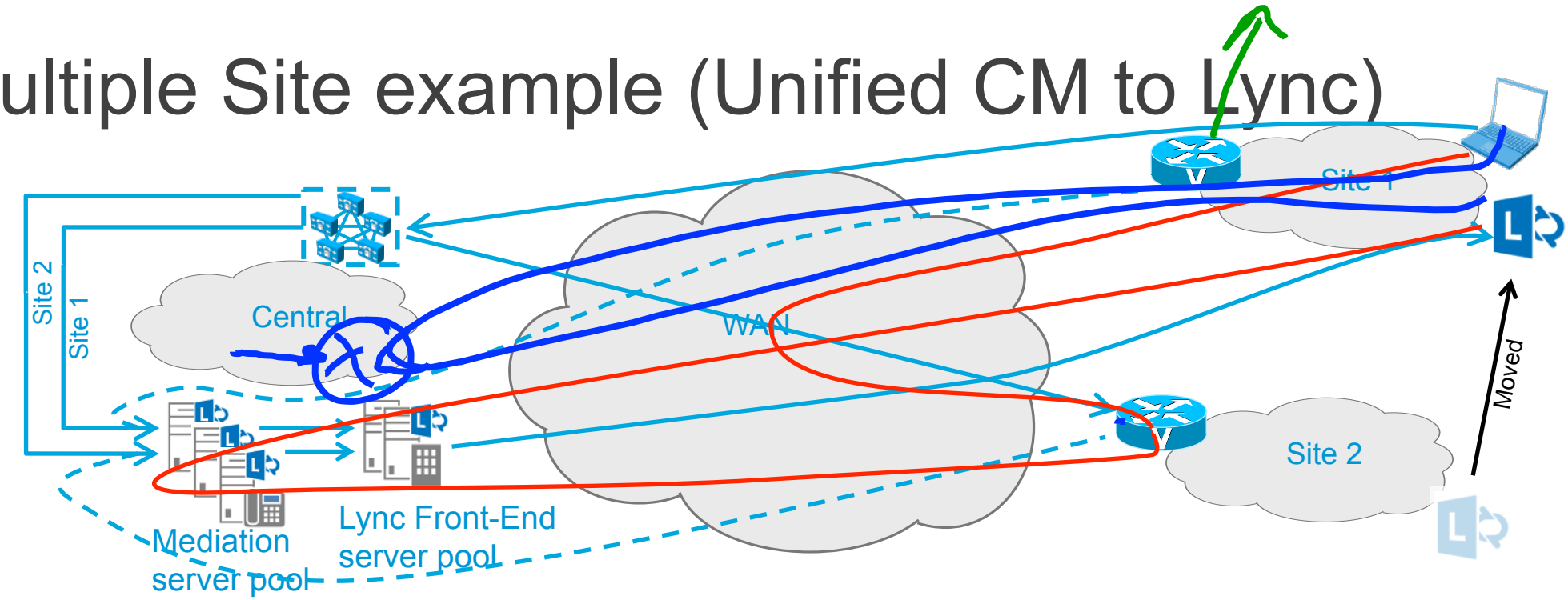
ultiple Site example (Unified CM to Lync)



Unified CM selects trunk to Lync based on called destination (+E.164 prefix), but Lync client moved to other site

- MTP (assumed) local to Lync client selected
- Alternate media IP definition in Lync trunk configuration no in same site as Lync client → no media bypass
- Mediation server in media path
- Media hairpins through central site

ultiple Site example (Unified CM to Lync)



False assumption about Lync client location could lead to even worse media path:

- Unified CM selects trunk with MTP local to (assumed) location of Lync client: Site 2
- Lync rejects media bypass, because MTP not local to IP address of Lync client
- Mediation server in media path
- Media hairpinned through remote site AND central site

edia hairpinning: Root Cause Analysis

MSFT trunk architectural limitations

- MTP required to enable media bypass
- MTP needs to be “local” to Lync client

Only call control authoritative for endpoint is aware of client location

- Source call control aware of source client location
- Destination call control aware of destination client location

Problem: what if destination client (Lync) locations determines required MTP location, but source call control (Unified CM) is not aware of the location?

Fundamental limitation of Lync that can not be solved by Unified CM

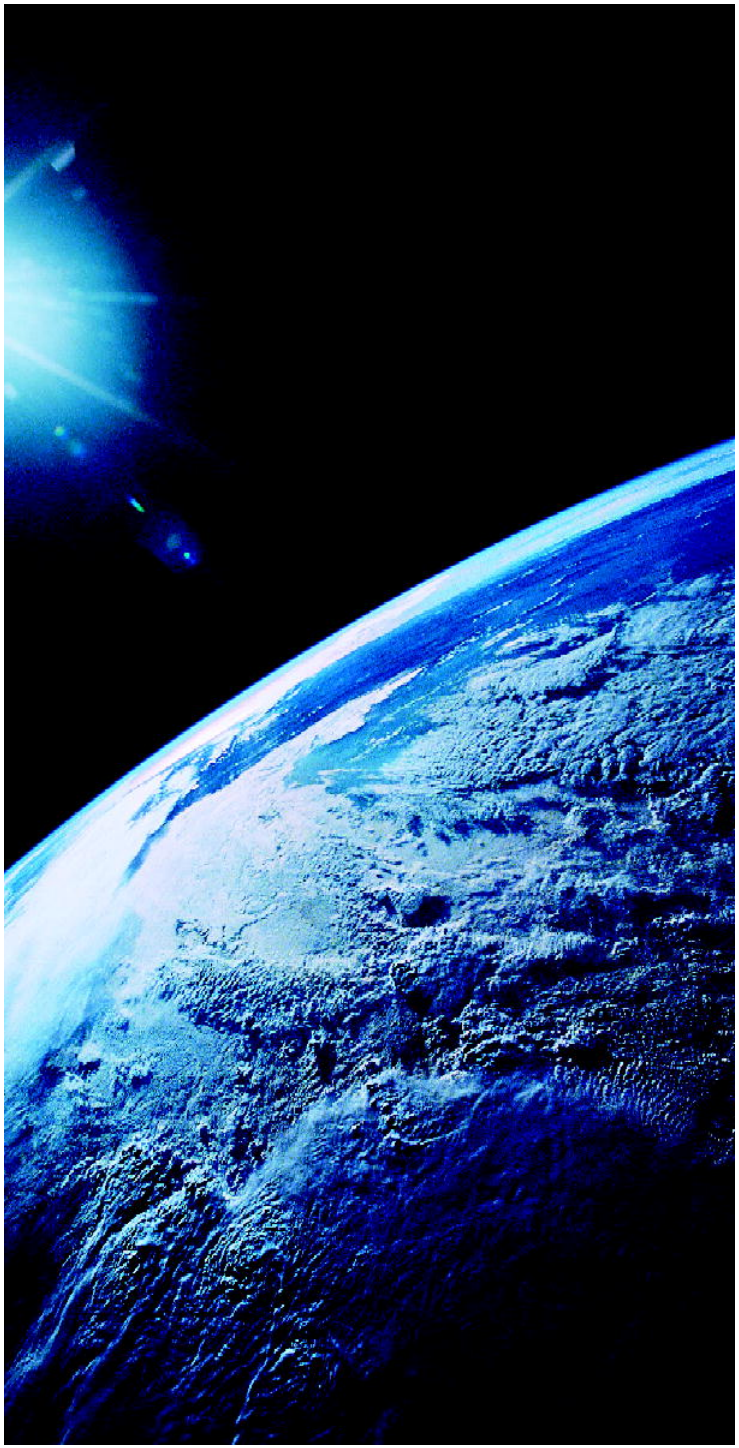
… or any other call control

… unless “Always bypass” is configured which prohibits MSFT CAC (and still requires MTPs)

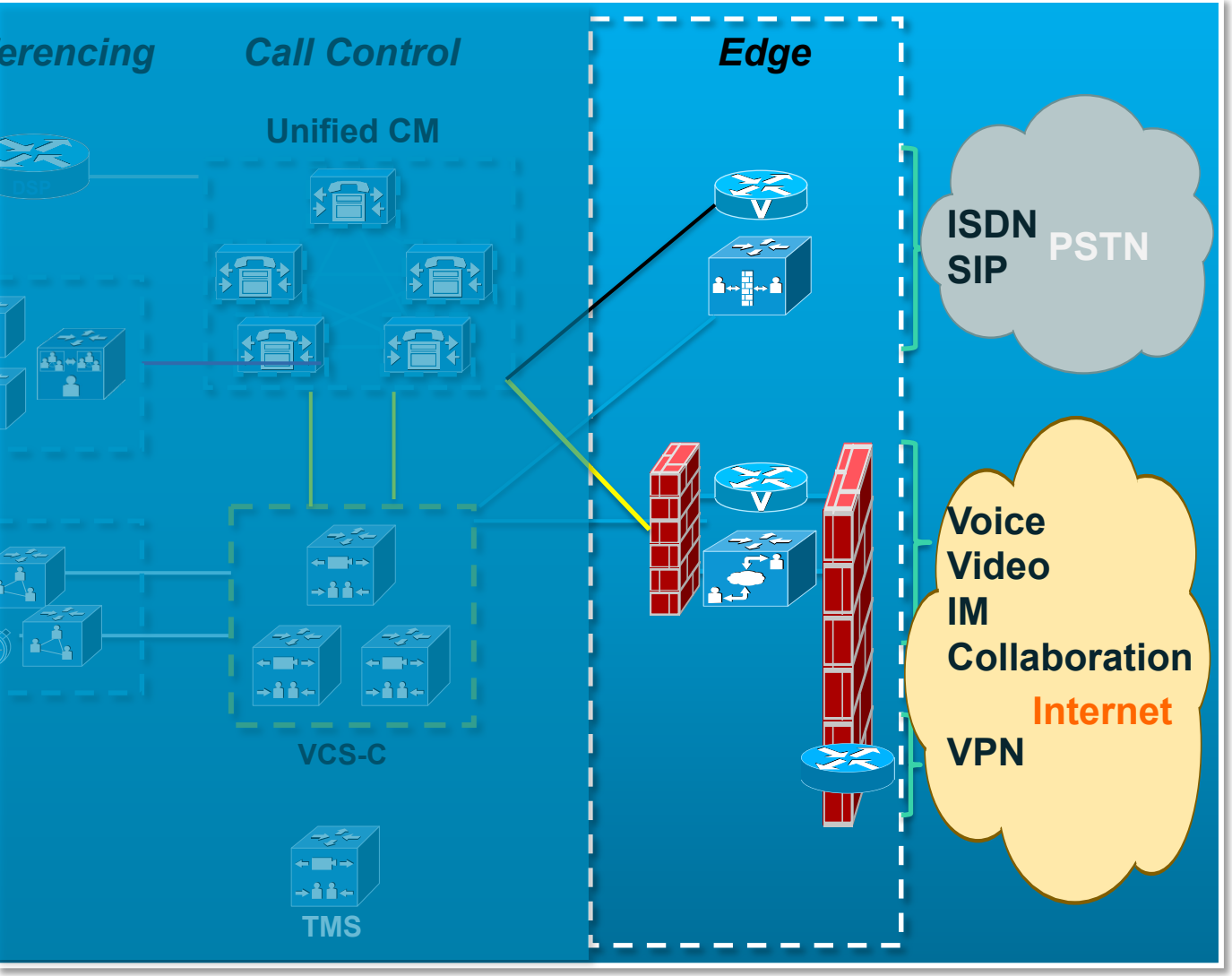
rogram

s	Téma	Přednášející
30 – 10:30	Novinky v Cisco Collaboration	Jaroslav Martan
:45 – 11:45	Nástroje pro management multimediální sítě (Medianet)	Jiří Rott
	oběd	
:45 – 13:45	Architektura collaboration řešení - Jabber Design - Integrace Cisco UC a MS OCS/Lync	 Jaroslav Martan Ivan Sýkora
:00 - ???	Architektura – whiteboard (jam) session - Edge design - SIP trunk - Video – jednotný call control - Trusted Relay Point (TRP) a L3 VPN	 Jaroslav Martan Jiří Rott Jaroslav Martan Jaroslav Martan

Edge Design



Services at Network Edge
Overview

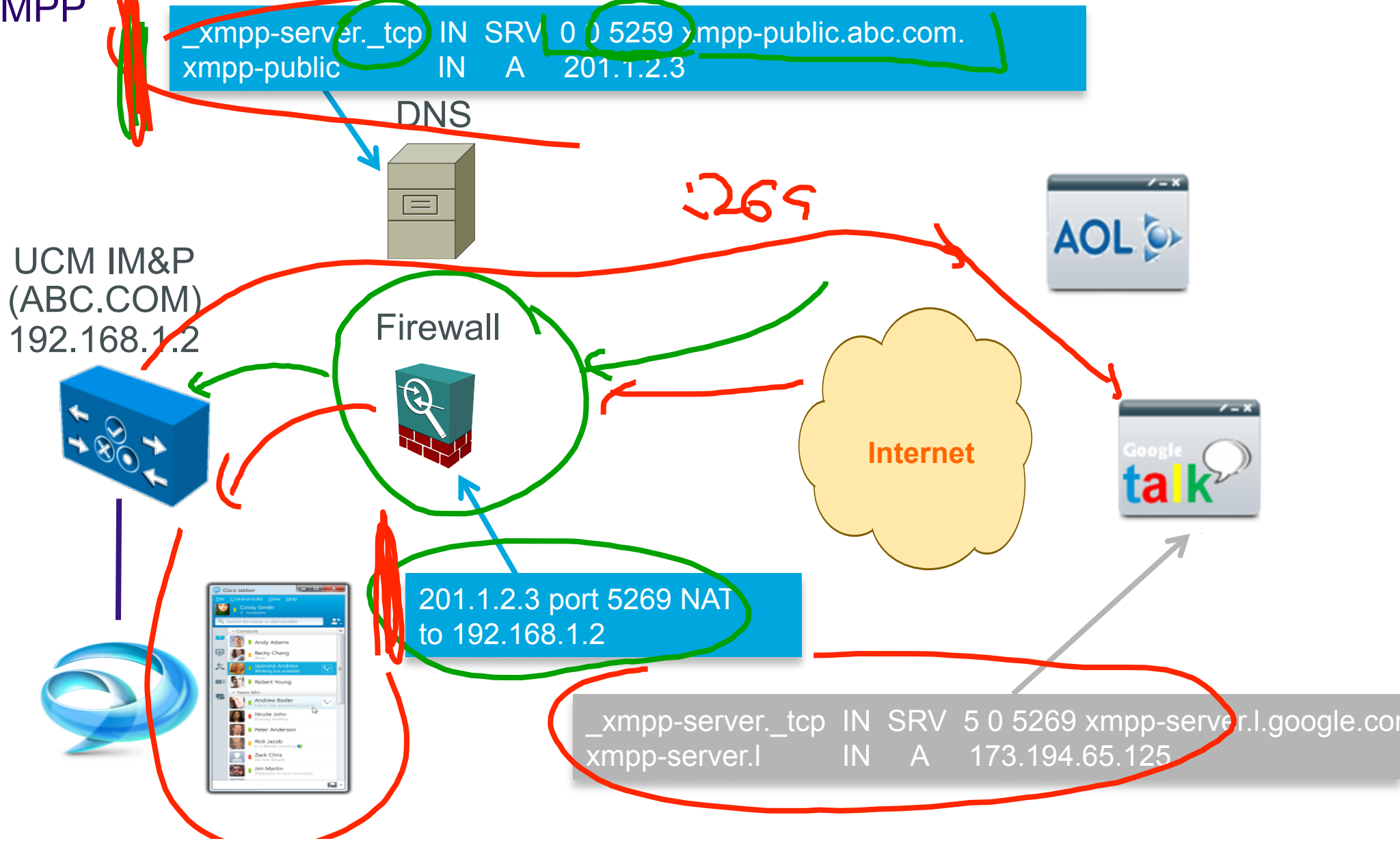


External Communications:

- PSTN
  - ISDN or SIP trunk – voic only
- Internet
  - URI dialing – voice+vide
  - Instant Messaging – XM SIP
  - Collaboration – Webex
  - Remote Access – VPN, Edge gateway

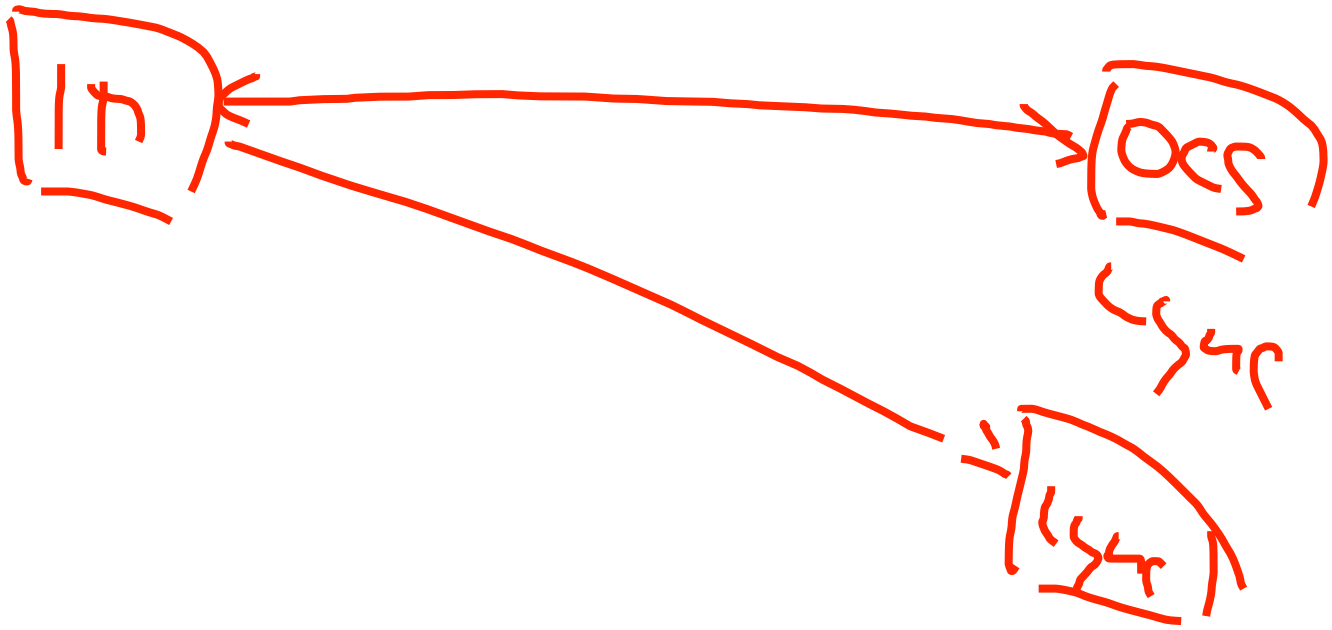
Instant Messaging & Presence

XMPP



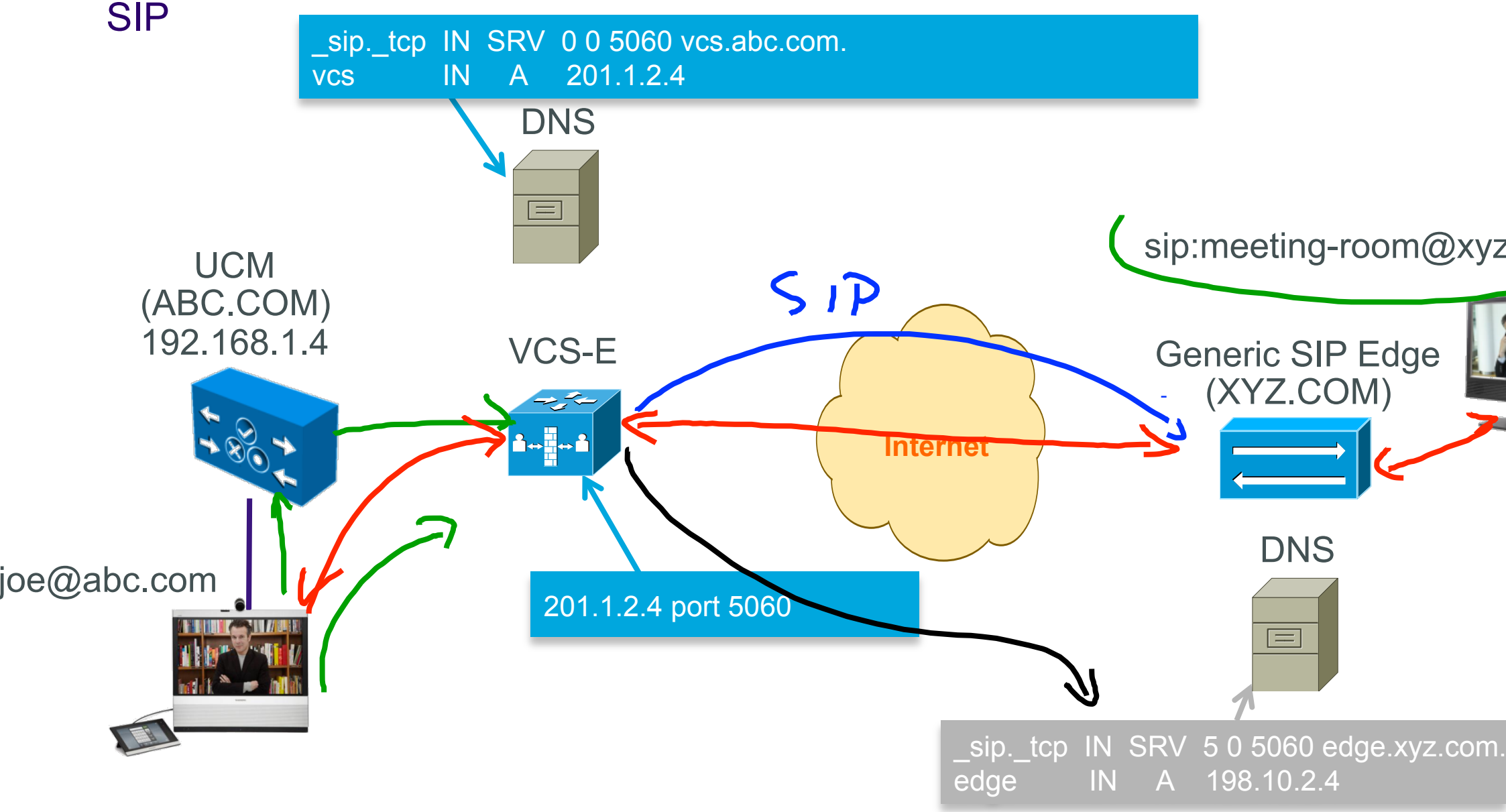
Instant Messaging & Presence

SIP IM (SIMPLE)



B2B Voice+Video over Internet

SIP



Remote Access

AnyConnect

Remote Access

Phone VPN

VPN Gateway Information

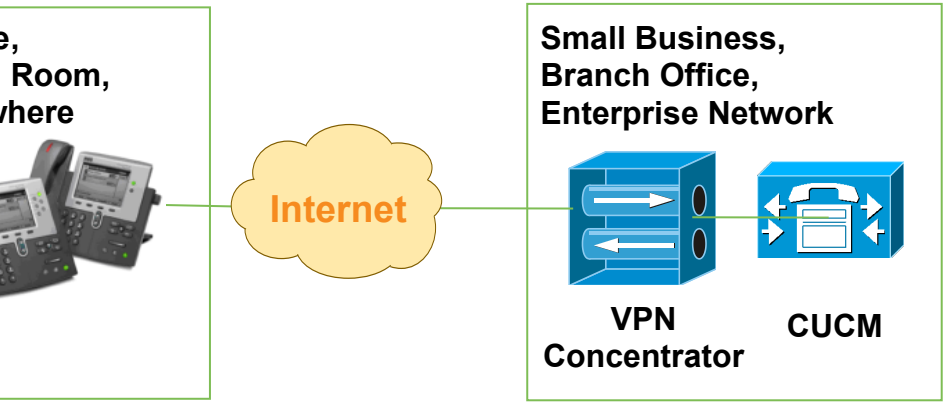
VPN Gateway Name*	San Jose VPN Gateway
VPN Gateway Description	
VPN Gateway URL*	https://sjcvpn.cisco.com

VPN Gateway Certificates

VPN Certificates in your Trustsore

Subject: O=Cisco Systems, CN=CAP-RTP-001, Issuer: O=Cisco Systems, CN=CAP-RTP-001, Serial Number: 76:12:f9:60:15:3d:6f:9f:4e:42:20:20:32:b7:23:56
Subject: O=Cisco Systems, CN=Cisco Root CA 2048, Issuer: O=Cisco Systems, CN=Cisco Root CA 2048, Serial Number: 5f:f8:7b:28:2b:54:dc:8d:42:a3
Subject: O=Cisco Systems, CN=CAP-RTP-002, Issuer: O=Cisco Systems, CN=CAP-RTP-002, Serial Number: 35:3f:b2:4b:d7:0f:14:a3

VPN Certificates for this Gateway



VPN Group	San_Jose_VPN_Group
VPN Profile	ExecutiveProfile

Collaboration Edge

Unified Voice, Video, Messaging, & Conferencing

Remote and Mobile Access

Consistent experience outside the network

Jabber and EX/MX Series

Business to Business

Secure communications with anyone

Enterprise Border, Internal Border

Cloud Services

Enterprise grade flexibility and scale

Rich WebEx Integration , Service Provider Offerings

Consumer Services

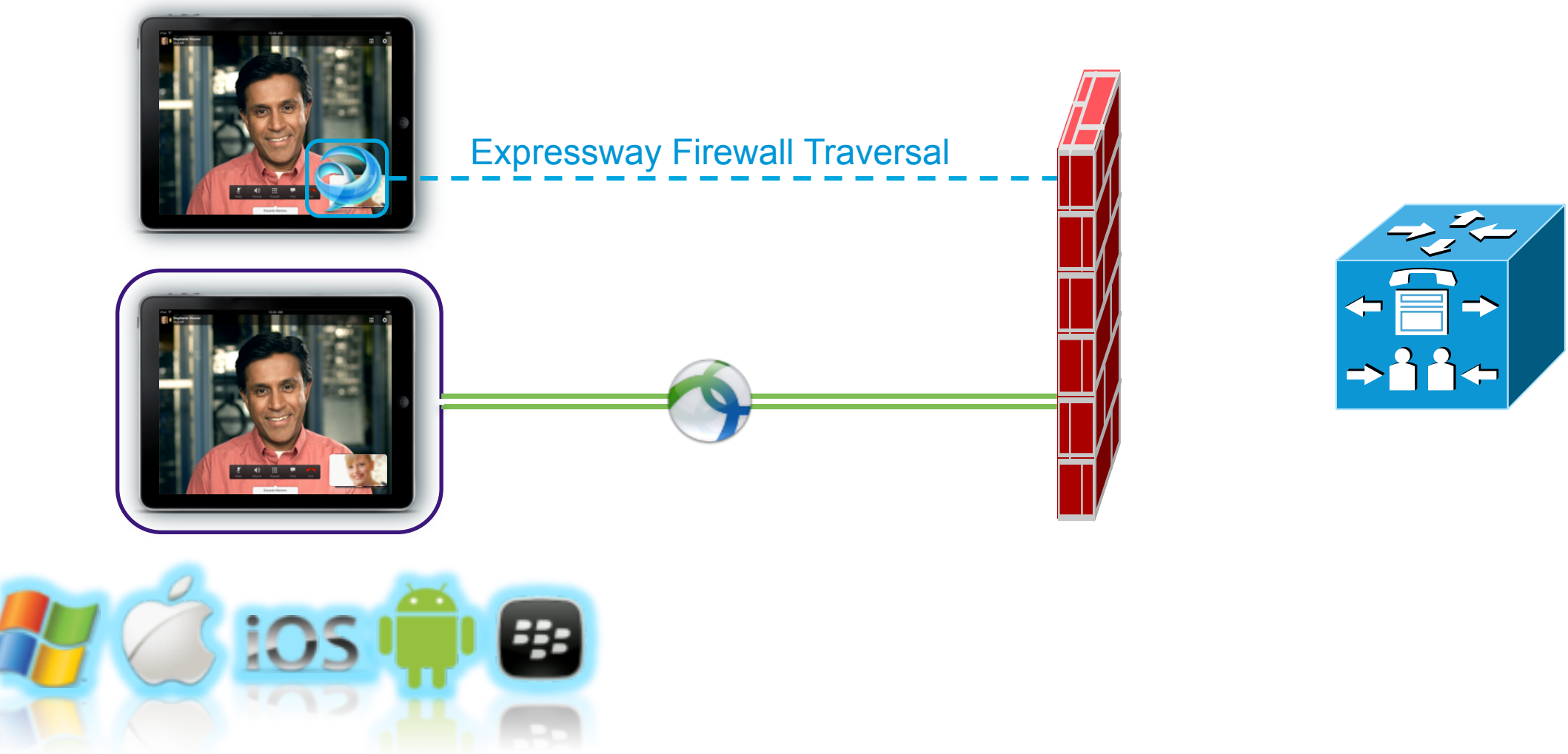
Media and Signaling Normalization

Non-standard EP termination, Consumer to Business

- **Proven Technology**
- **Consistent Experience**
- **Easy to Deploy**
- **Optimized Media**

Remote Access

Collaboration Edge or AnyConnect



Remote Access

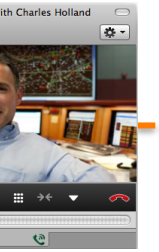
Collaboration Edge

Outside corporate firewall (Public Internet)

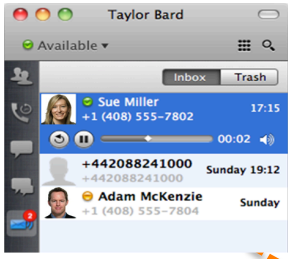
Inside corporate firewall (Intranet)

based
ts: Win,
iOS,
oid, SDK

voice and
calls



Access visual voicemail



Instant Message and Presence

Outside Firewall

VCS Expressway

Inside Firewall

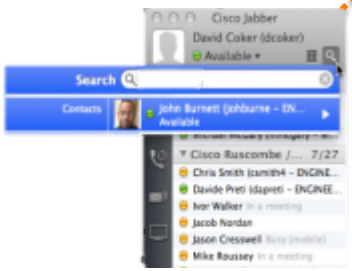
VCS Control

UCM

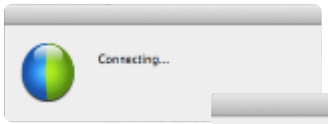
Jabber Clients

IP Communications

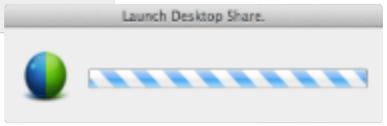
Search corporate directory



Launch a web conference



Share content



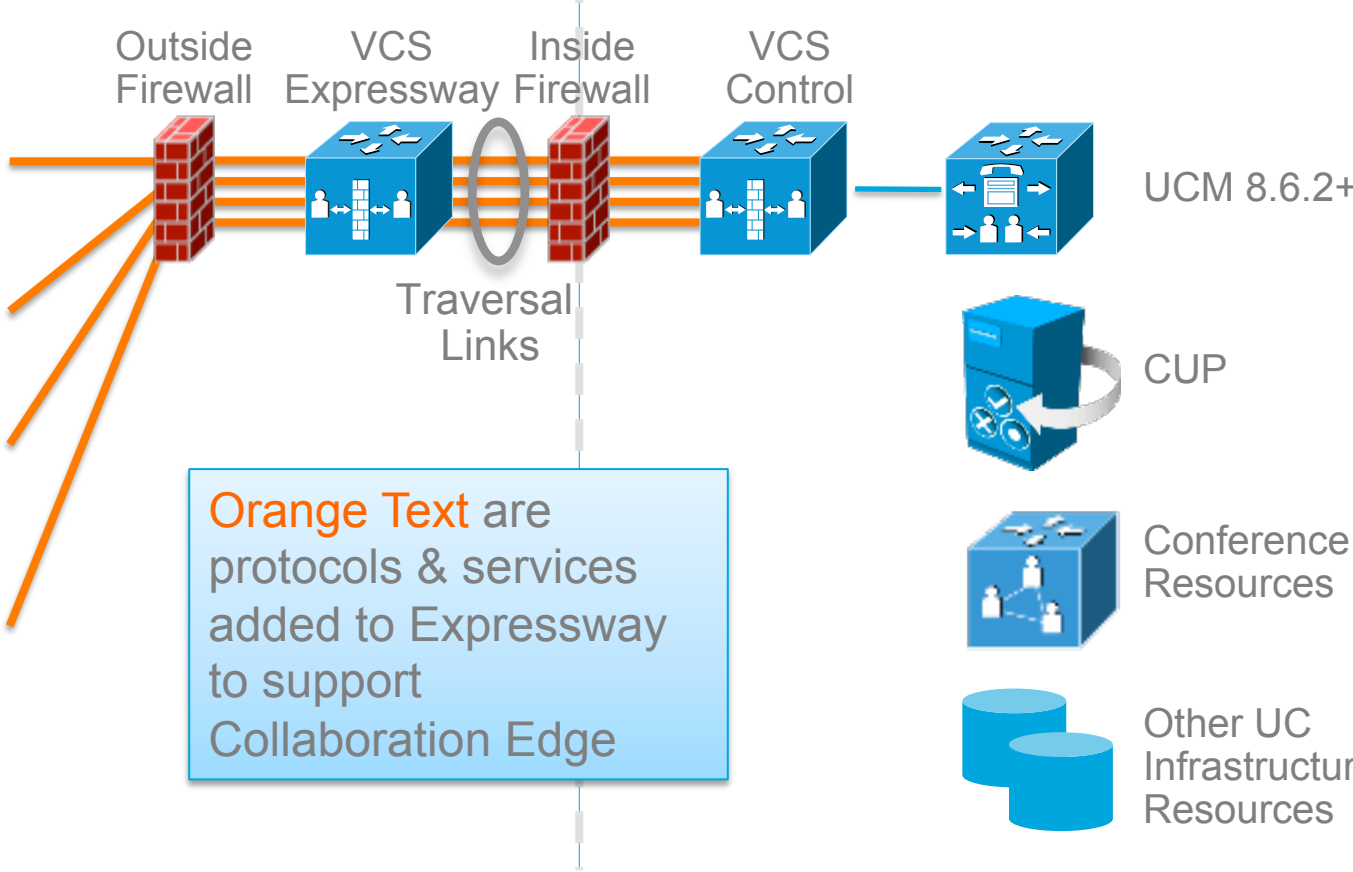
Personal TelePresence

Immersive TelePre

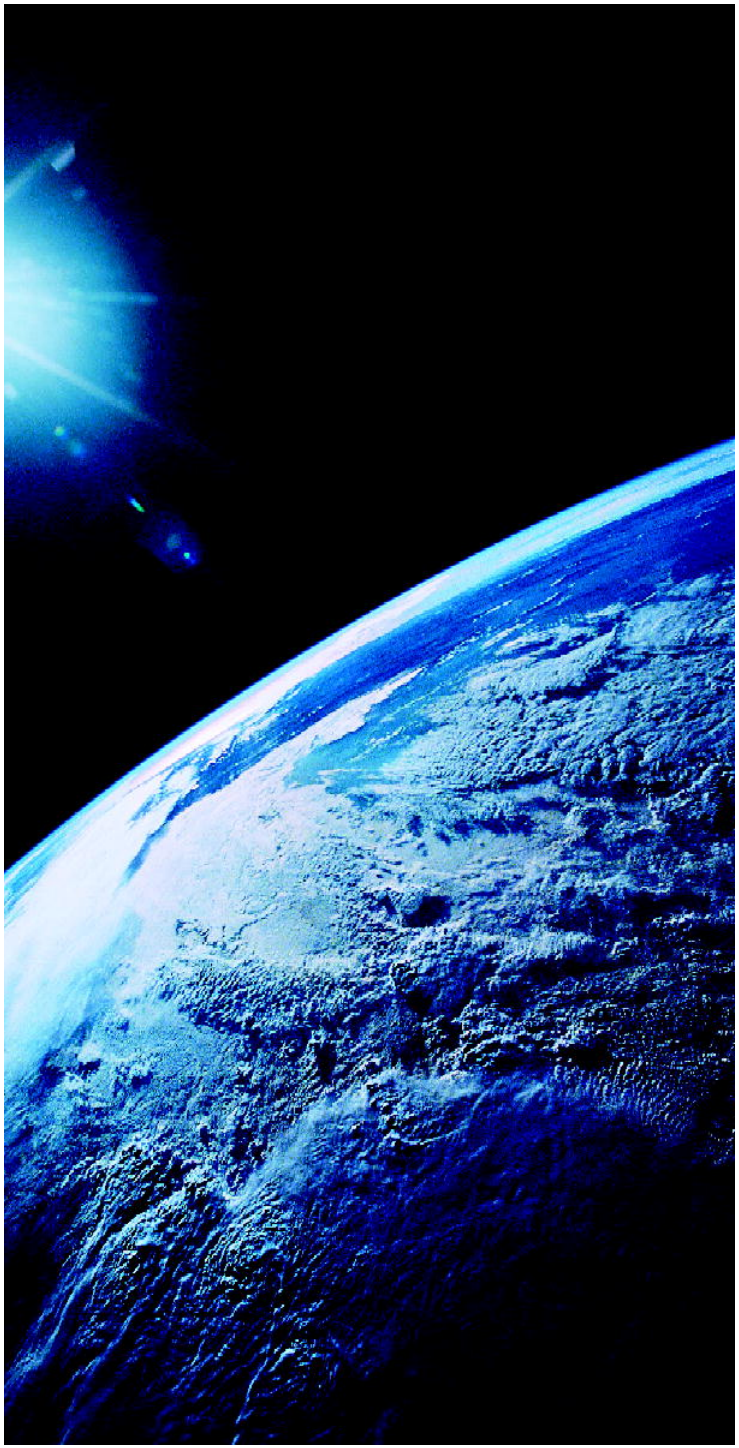
Remote Access
Protocol Summary

Outside corporate firewall (Public Internet) | **Inside corporate firewall (Intran**

ocol	Security	Service
	TLS	Session Establishment – Register, Invite, etc. via UCM
PS	TLS	Logon, Provisioning/ Configuration, Directory, Visual Voicemail
P	TLS	Instant Messaging, Presence, Federation
ia	RFC 3711	Audio, Video, Content Share, Advanced Control (RTP/SRTP, BFCP, iX/ XCCP)

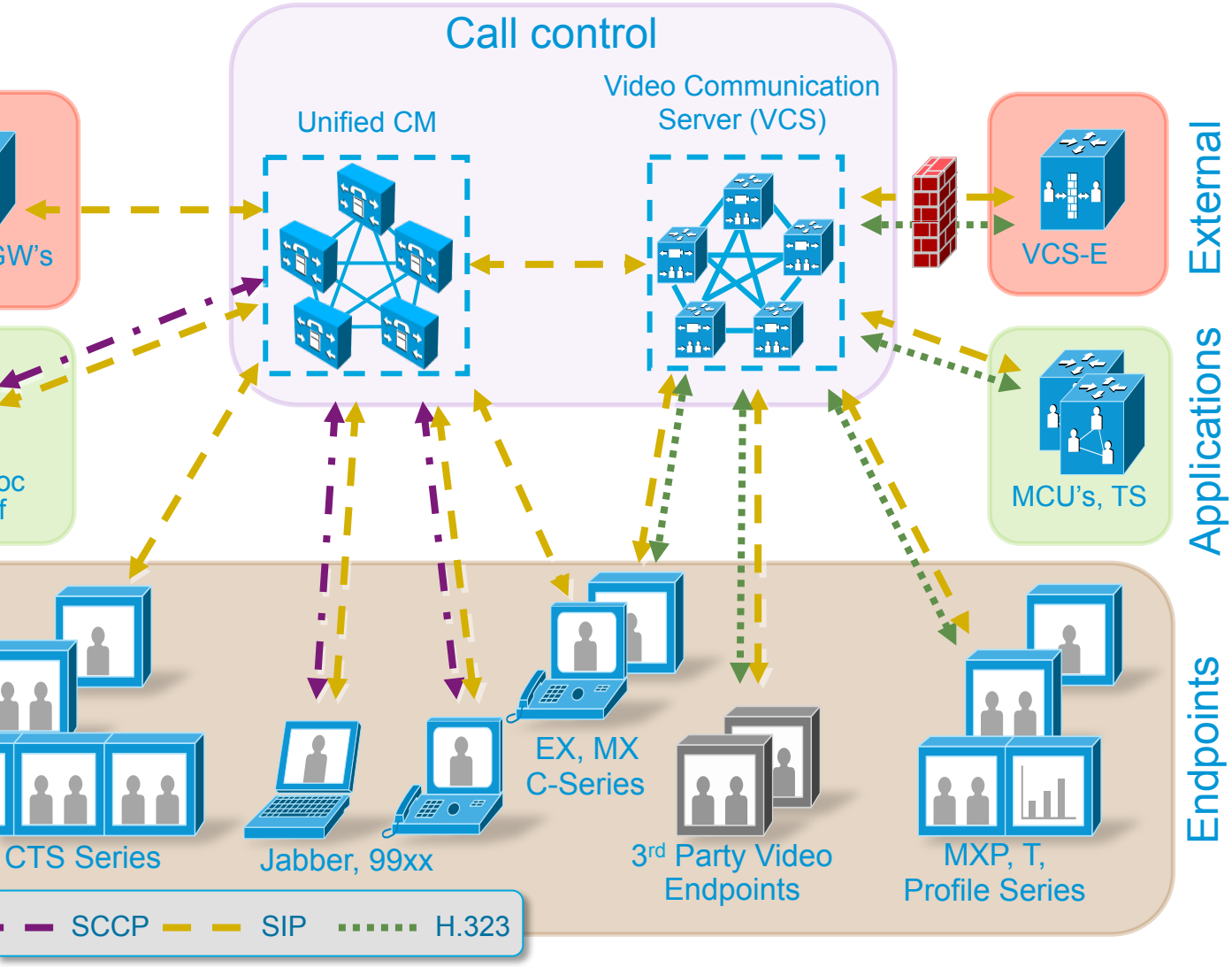


Video Design



Video Design

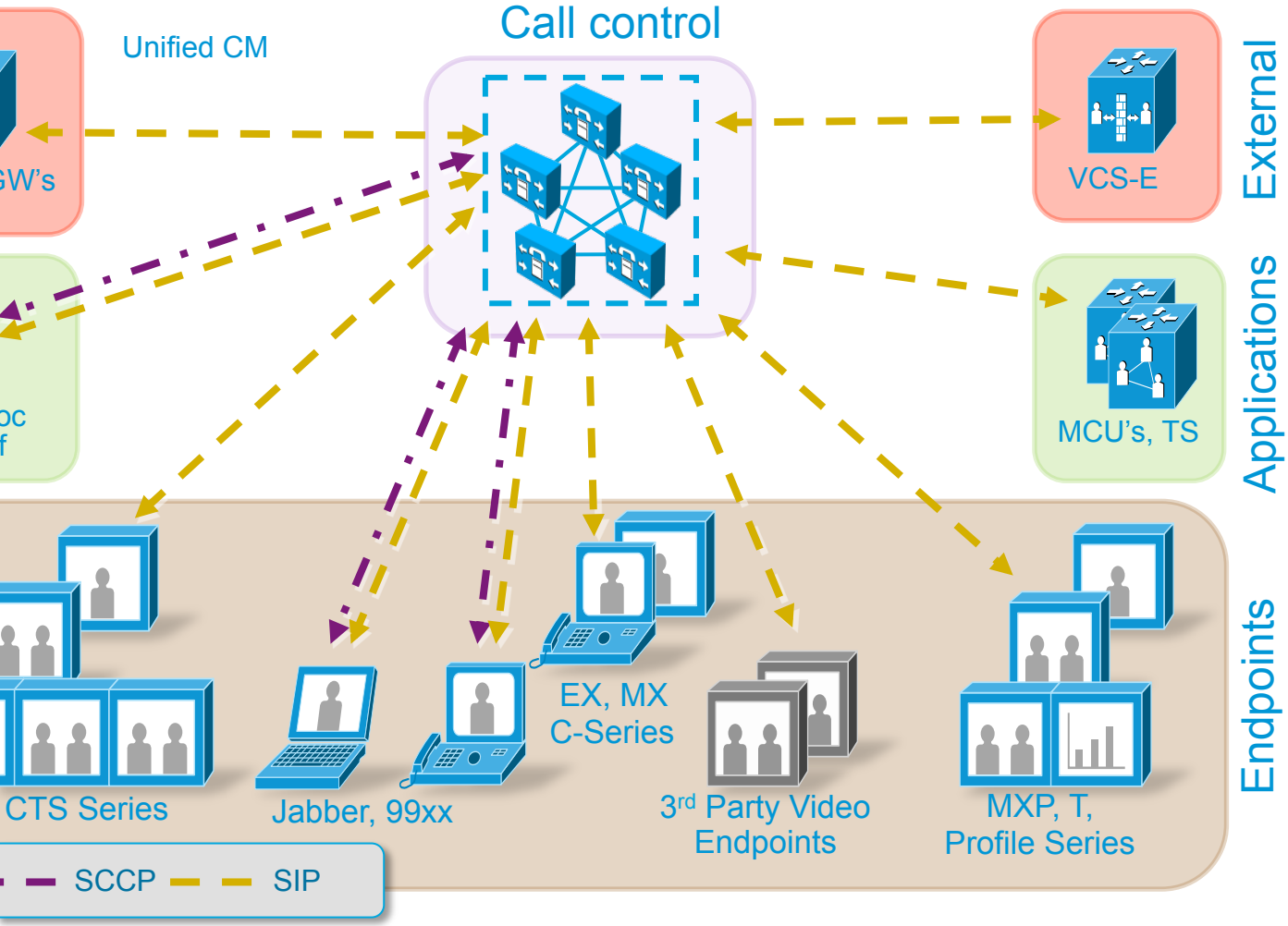
CUCM + VCS-C + VCS-E



Reasons to deploy VCS-C:

- H.323 video clients
- No SIP inspection on firew
  between intranet and DMZ

Video Design
CUCM + VCS-E

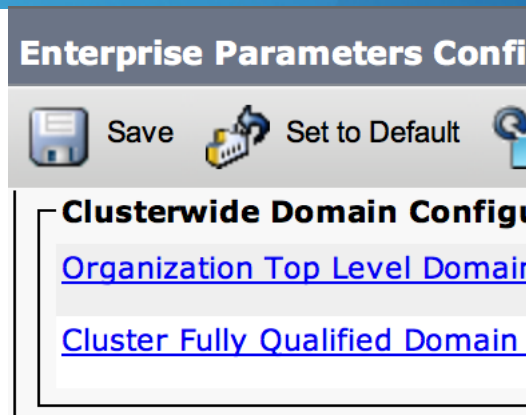


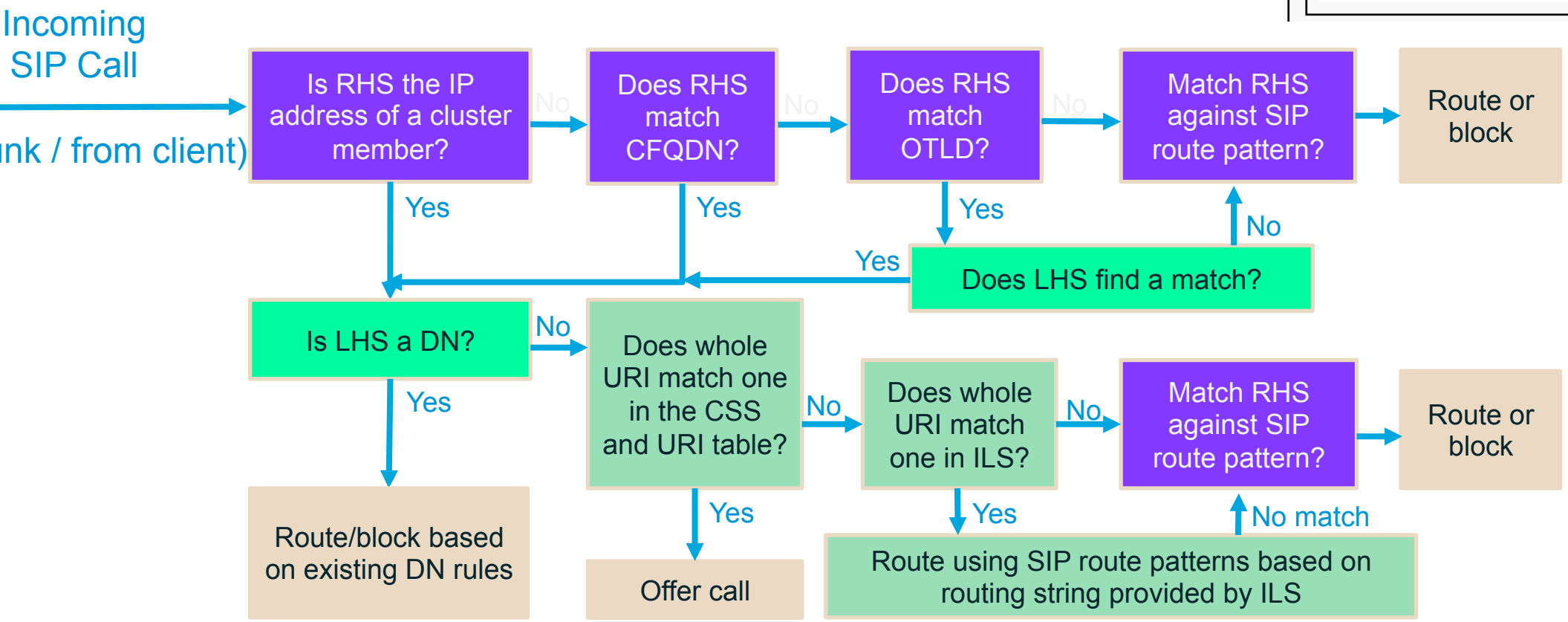
Single Call Control (from 9

- Number and URI dialing
- Native TelePresence endpoint registration
- MCU interoperability – scheduled & ad-hoc
- For external connectivity VCS-E can act both as traversal client & server

Video Design
CUCM Call Routing

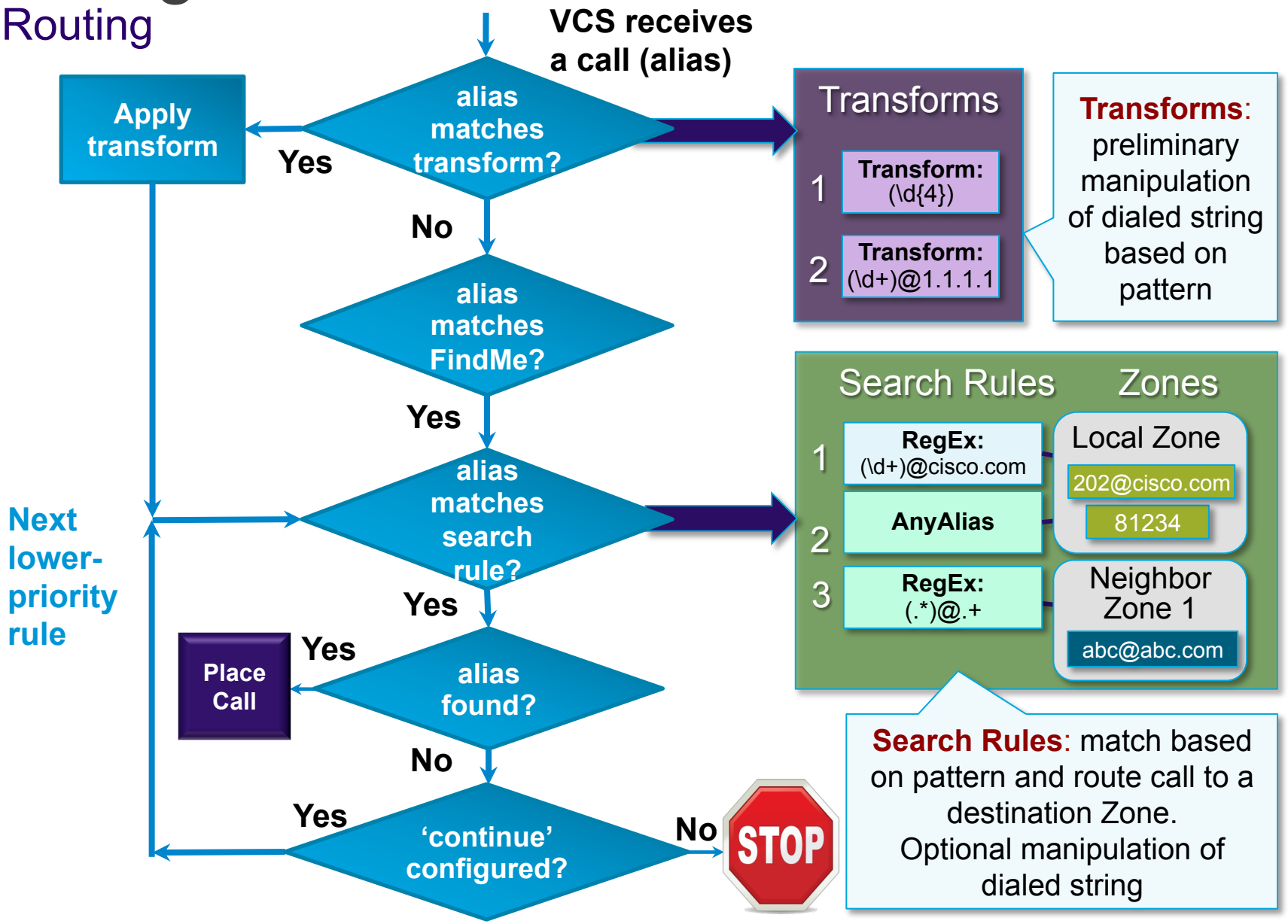
LHS = Left Hand Side (of URI)
RHS = Right Hand Side
OTLD = Organization Top-Level Domain
CFQDN = Cluster Fully Qualified Domain Name
ILS = Inter-Cluster Lookup Service



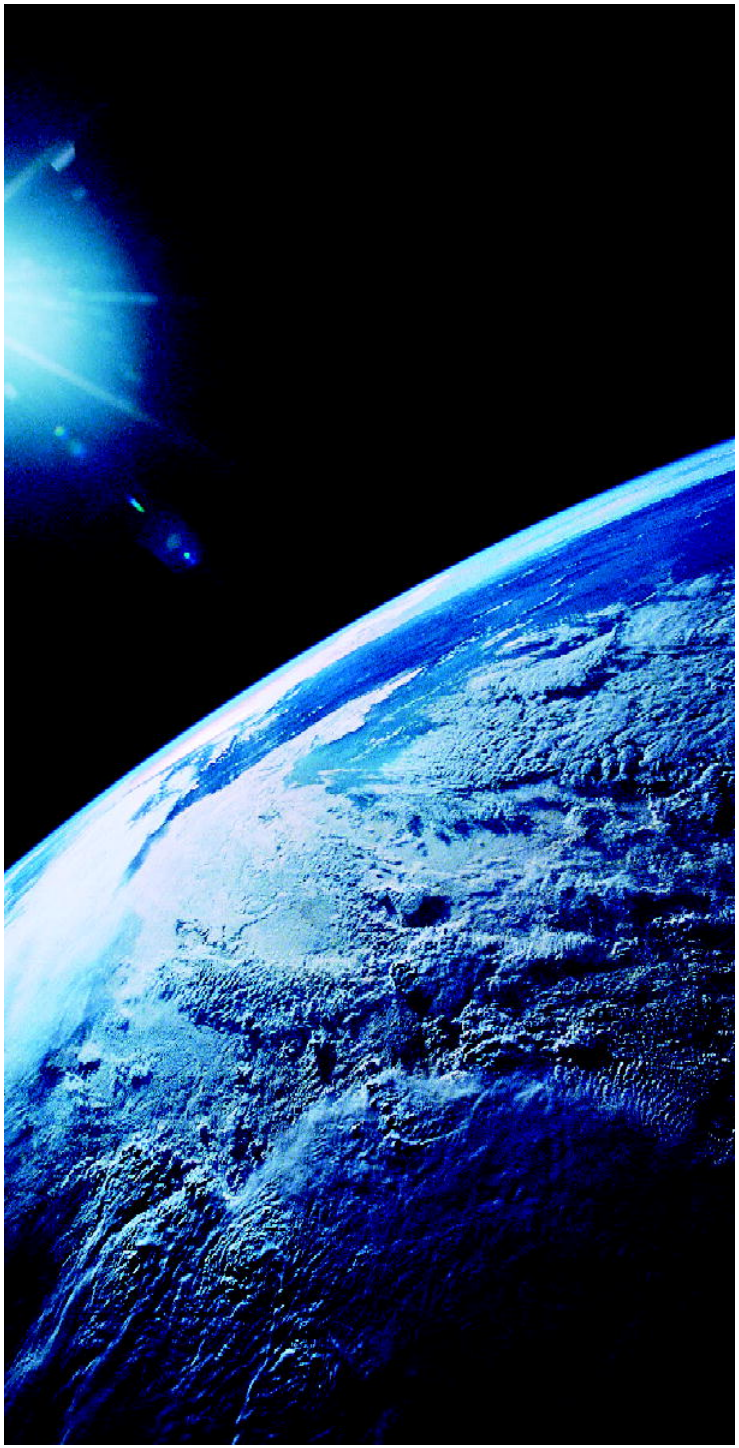


Video Design

VCS Call Routing



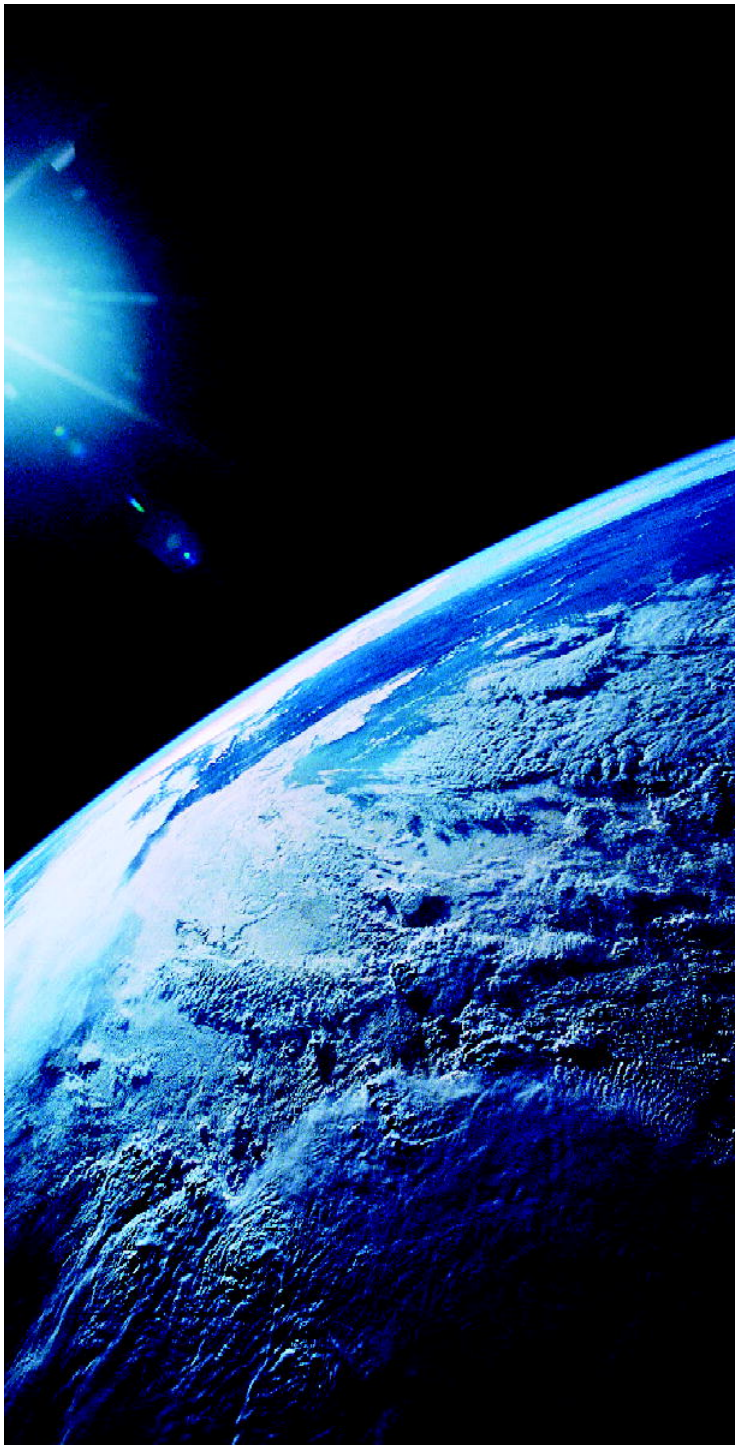
SIP Trunk



What this Session is About

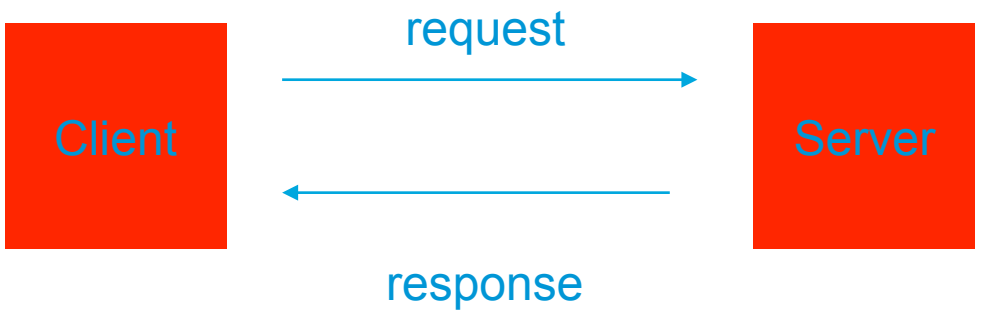
- Fact 1: SIP is a “Standard”
- Fact 2: SIP Configurations are not standardized
  - Which headers are included…
  - Format of data in headers (URIs, etc.)…
  - Ordering of header fields…
  - Content of SIP Message Body…
- What do we do when Fact #1 and Fact #2 are at odds in our deployment?

Brief Review of SIP (for Reference)



Basic Design

- SIP is a Client-Server Protocol
  - Clients send requests, receive responses
  - Servers receive requests, send responses
- Modeled after HTTP
  - Text Encoded Protocol
- Each request invokes *method* on server
  - Main purpose of request
- Messages contain bodies



SIP Methods and Messages

- Call signaling performed by SIP Methods
- Six ‘Standard’ SIP Methods:
  - INVITE
  - ACK
  - OPTIONS
  - BYE
  - CANCEL
  - REGISTER
- SIP Messages have distinct parts:
  - IP/TCP/UDP Envelope
  - SIP Header
  - SIP Message Body
    - MIME-Encoded
    - Session Description Protocol (SDP)
    - May contain other data

For Your Reference

SIP Methods

INVITE

- Invites a participant to a session
- idempotent - reINVITEs for session modification

BYE

- Ends a client's participation in a session

CANCEL

- Terminates a search

OPTIONS

- Queries a participant about their media capabilities, and finds them, but doesn't invite
- PING identifies reachability

ACK

- For reliability and call acceptance

REGISTER

- Informs a SIP server about the location of a use

SIP Message Syntax

- Many header fields from http
- Payload contains a media description
  - SDP – Session Description Protocol

```
INVITE sip:alice@company.com SIP/2.0
From: Bob <sip:bob@university.edu>
To: Alice <sip:alice@company.com>
Via: SIP/2.0/UDP pc.university.edu
Call-ID: 199723450578@192.169.100.100
Content-type: application/sdp
CSeq: 4711 INVITE
Content-Length: 187

v=0
o=CCM-SIP 2000 1 IN IP4 192.168.100.100
s=SIP Call
c=IN IP4 192.168.200.200
m=audio 26542 RTP/AVP 0 8 18 101
a=rtpmap:0 PCMU/8000
a=ptime:20
a=mid:1
c=IN IP6 2001:0db8:aaaa::
0987:65ff:fe01:234b
m=audio 26662 RTP/AVP 0
a=mid:2
```

For Your Reference

Negotiating the Session

- Called party receives SDP offered by caller
- Each stream can be
  - accepted
  - rejected
- Accepting involves generating an SDP listing same stream
  - port number and address of called party
  - subset of codecs from SDP in request
- Rejecting indicated by setting port to zero
- Resulting SDP returned in 200 OK
- Media can now be exchanged

Audio stream accepted, PCMU only

Video stream rejected, Port 0

```
v=0
o=user2 16255765 8267374637 IN IP4 4.3.2
t=0 0
m=audio 3456 RTP/AVP 0
c=IN IP4 4.3.2.1
m=video 0 RTP/AVP 86
c=IN IP4 4.3.2.1
```

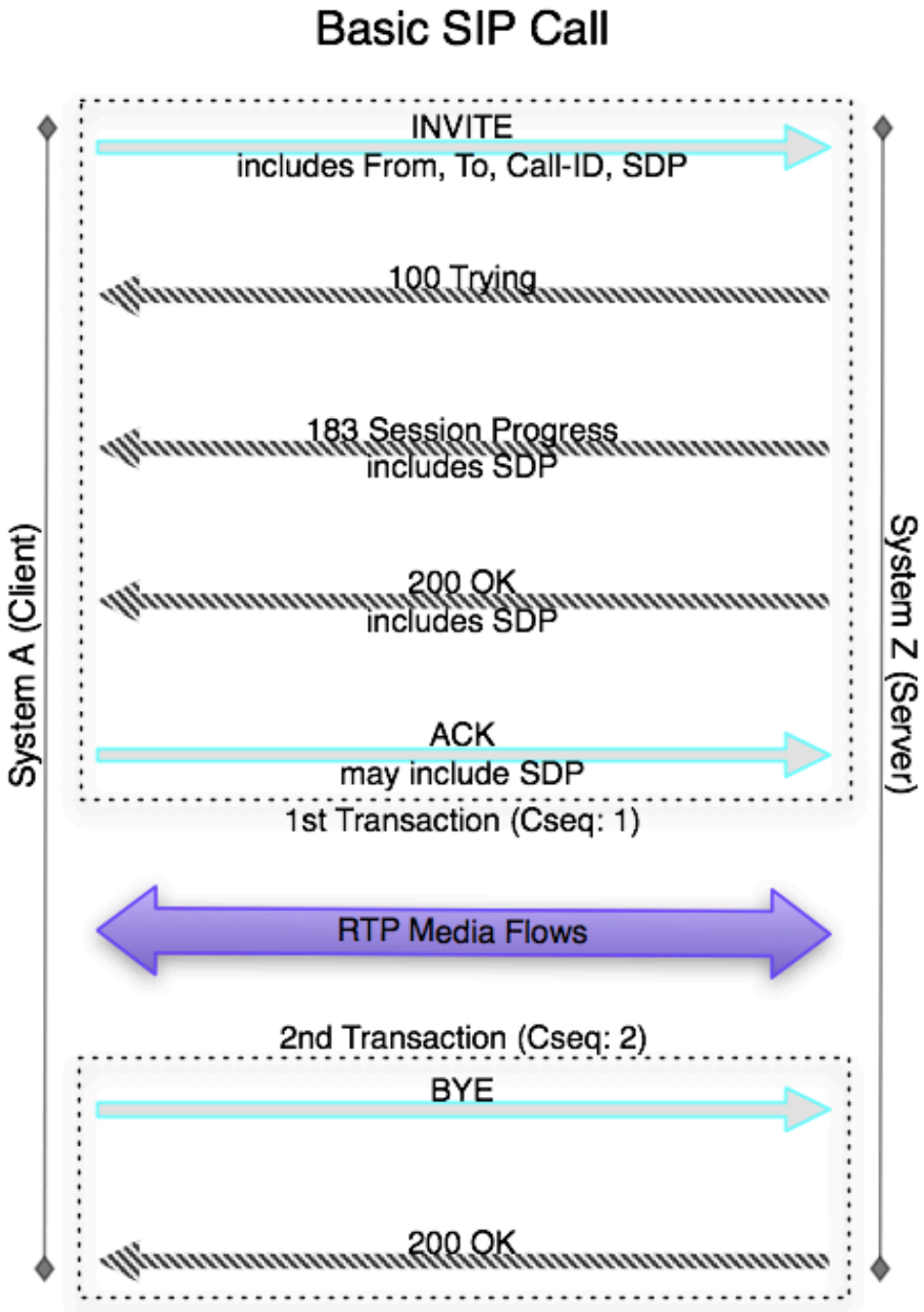
SIP Responses

- Look much like requests
  - Headers, bodies
- Differ in top line
  - Status Code
    - Numeric, 100 - 699
    - Meant for computer processing
    - Protocol behavior based on 100s digit
    - Other digits give extra info
  - Reason Phrase
    - Text phrase for humans
      - Can be anything

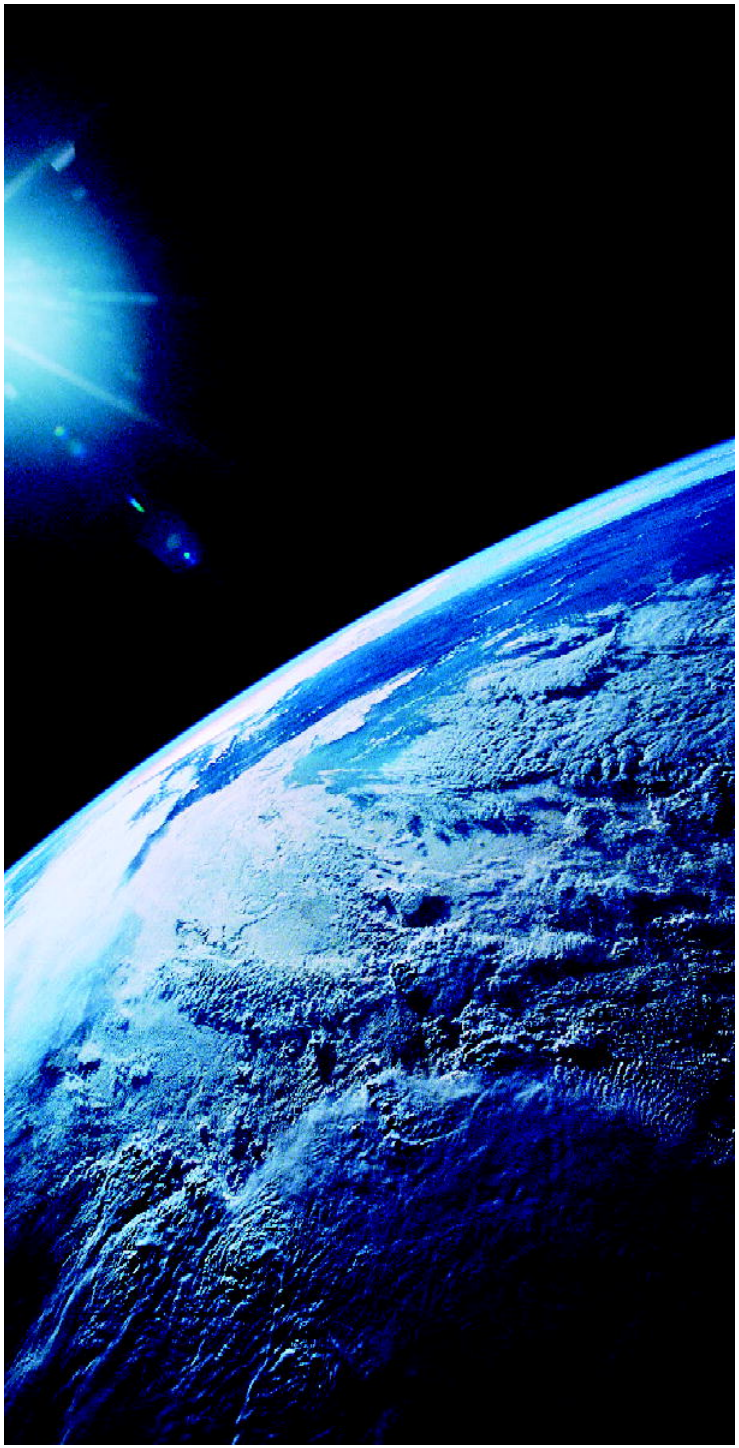
- Status Code Classes
  - 100 - 199 (1XX): Informational
  - 200 - 299 (2XX): Success
  - 300 - 399 (3XX): Redirection
  - 400 - 499 (4XX): Client Error
  - 500 - 599 (5XX): Server Error
  - 600 - 699 (6XX): Global Failure
- Two groups
  - 100 - 199: Provisional (Not reliable)
  - 200 - 699: Final, Definitive
- Example
  - 200 OK
  - 180 Ringing

SIP Transactions

- Fundamental unit of messaging exchange
  - Request
  - Zero or more provisional responses
  - Usually one final response
  - Maybe ACK
- All signaling composed of independent transactions
- Transactions identified by Cseq
  - Sequence number
  - Method tag

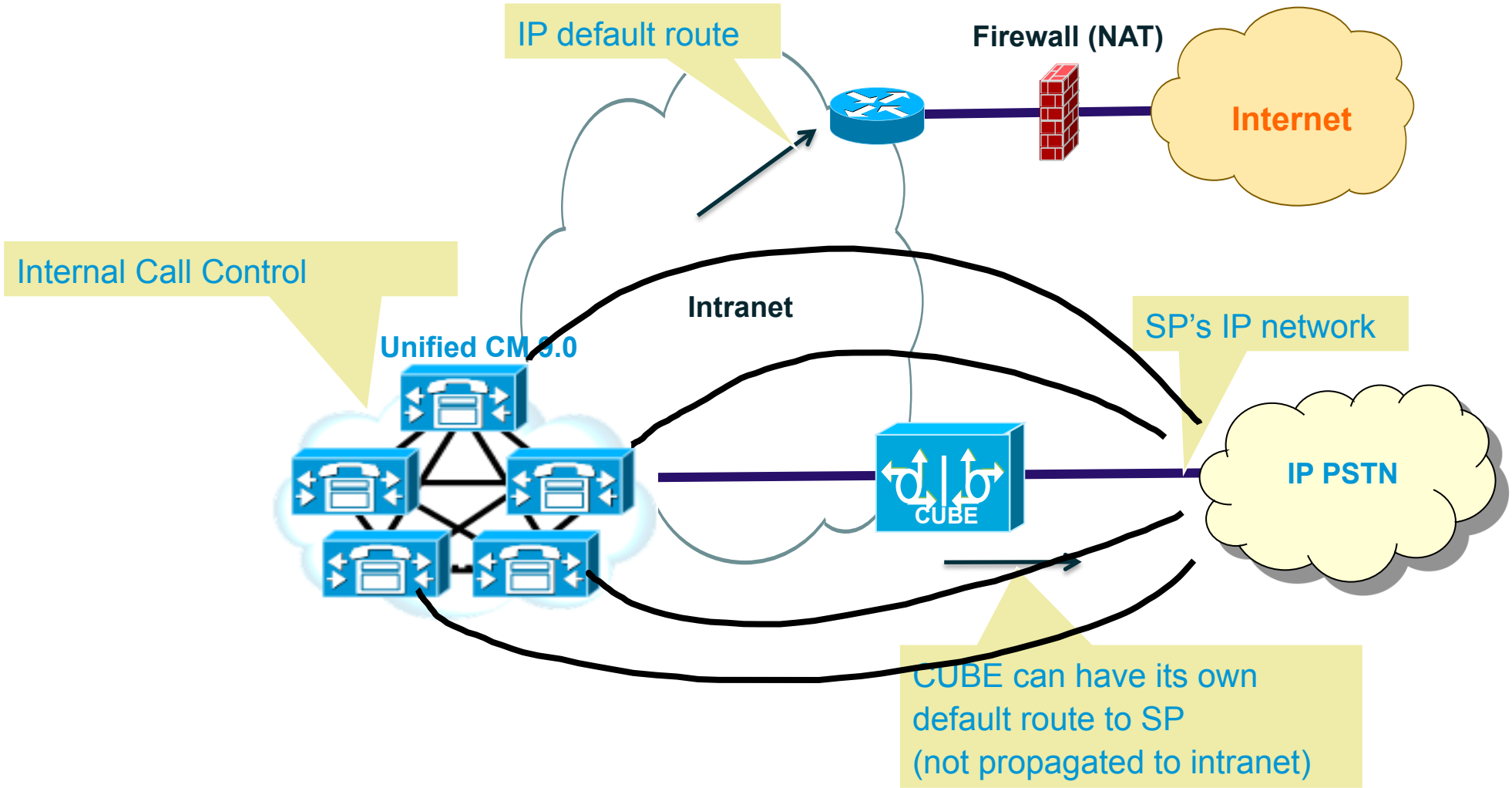


SIP Trunk Topology & Tools



SIP Trunk Topology

Overview



Cisco Unified Border Element
Feature Summary

SESSION CONTROL

Call Admissions Control
Ensuring QoS
Statistics and Billing
Redundancy/
Scalability

SECURITY

Encryption
Authentication
Registration
SIP Protection
Firewall Placement
Toll Fraud

INTERWORKING

SIP - SIP
H.323 - SIP
SIP Normalization
DTMF Interworking
Transcoding
Codec Filtering

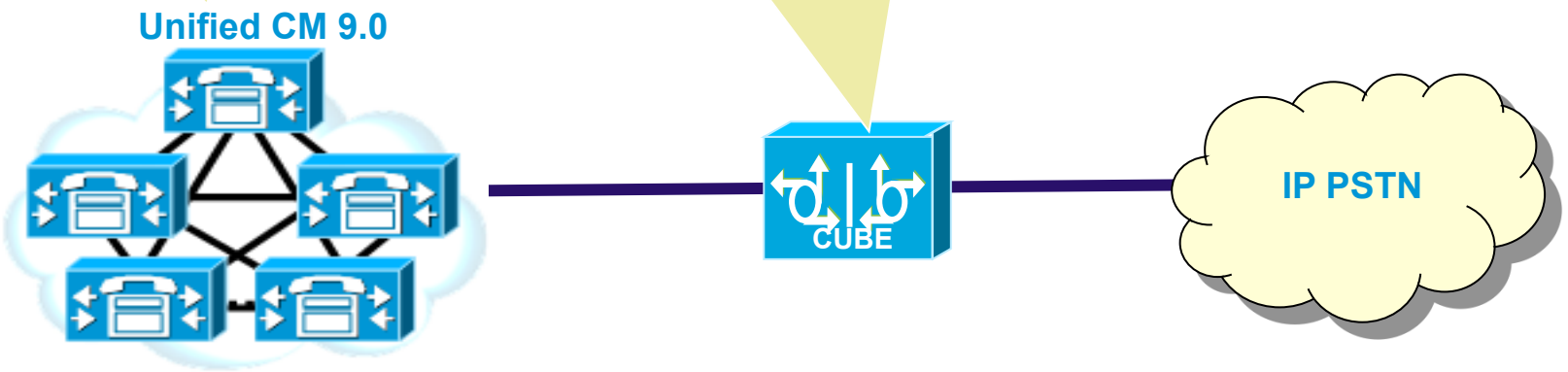
DEMARCATION

Fault Isolation
Topology Hiding
Network Borders
L5/L7 Protocol
Demarcation

SIP Trunk Topology

Normalization Tools

- **Lua scripts**



CUBE normalization

sip-profiles

l, Remote, Modify:

P headers

DP

//www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-mt/voi-condl-header.html

//www.cisco.com/en/US/products/sw/voicesw/ps5640/products_configuration_example09186a0080982499

```
voice service voip
 allow-connections sip to sip
 sip
  sip-profiles 100
!
voice class sip-profiles 100
 request INVITE sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone SIP/2.0"
 request REINVITE sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone SIP/2.0"
```

CUBE normalization

TCL script

odify call handling finite state achine (FSM)

odify SIP headers

p://developer.cisco.com/web/vgapi/home

```
service voip
-connections sip to sip

er-passing

ation
e test tftp://192.168.21.63/caller-name.tcl
m localhost 192.168.24.8

eer voice 992 voip
ce test
ing called-number 3100
 g711ulaw
d
```

optional

```
proc act_Setup { } {
 .......
    set localhost [param read localhost]
    set callInfo(displayInfo) $mytext
    set idInfo "\"$mytext\" <sip:$ani@$localhost>"
    set sipHeaders(Remote-Party-ID) $idInfo
    set sipHeaders(P-Preferred-Identity) $idInfo
    set sipHeaders(P-Asserted-Identity) $idInfo
    set callInfo(protoHeaders) sipHeaders
    leg setup $dnis callInfo leg_incoming
}
........
param register localhost "hostname or IP address of

#---------------------------------
#   State Machine
#---------------------------------
set fsm(any_state,ev_disconnected)  "act_Cleanup,sa

set fsm(CALL_INIT,ev_setup_indication) "act_Setup,C
set fsm(CALL_PROCEEDING,ev_setup_done) "act_SetupDo

fsm define fsm CALL_INIT
```

CUCM normalization

Lua script

dd, Remote, Modify:

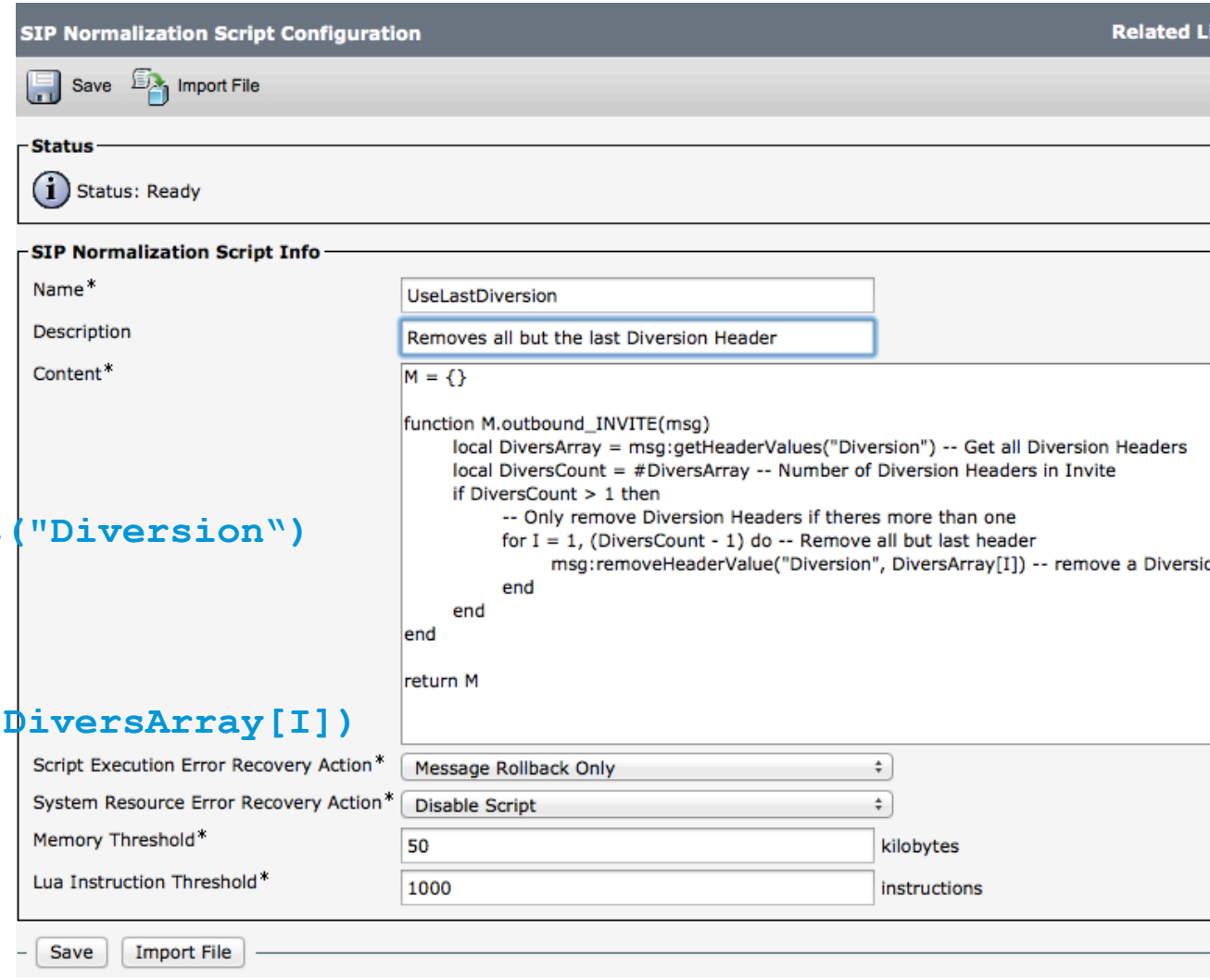
SIP headers

SDP

p://developer.cisco.com/web/sip/home

```
{}
tion M.outbound_INVITE(msg)
cal DiversArray = msg:getHeaderValues("Diversion")
cal DiversCount = #DiversArray
 DiversCount > 1 then
for I = 1, (DiversCount - 1) do
  msg:removeHeaderValue("Diversion", DiversArray[I])
end
d

rn M
```



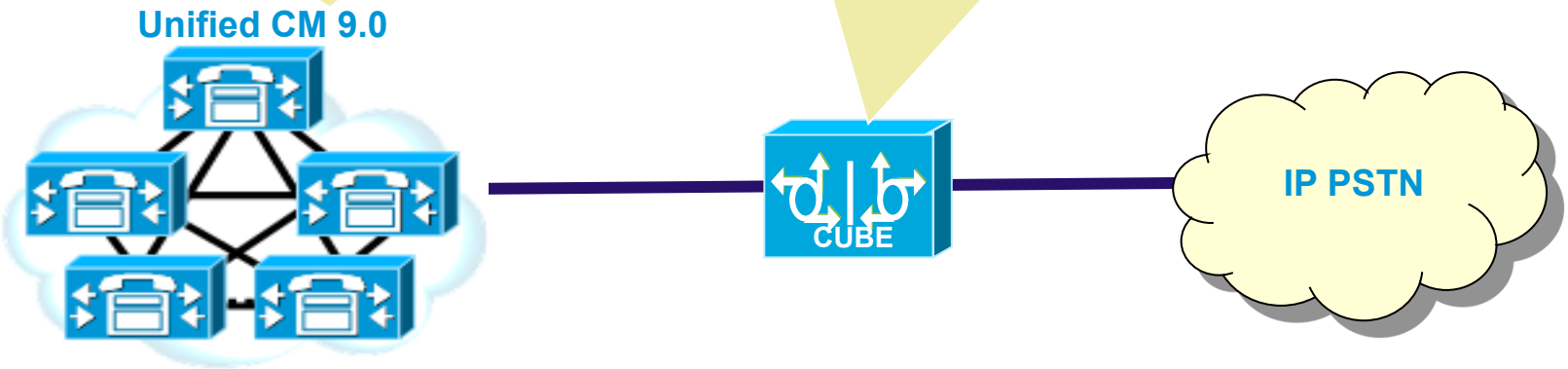
SIP Trunk Topology

Troubleshooting Tools

http://www.employees.org/~tiryaki/tc/

Trace (only with Triple Combo Tool)
CLI:utils network capture

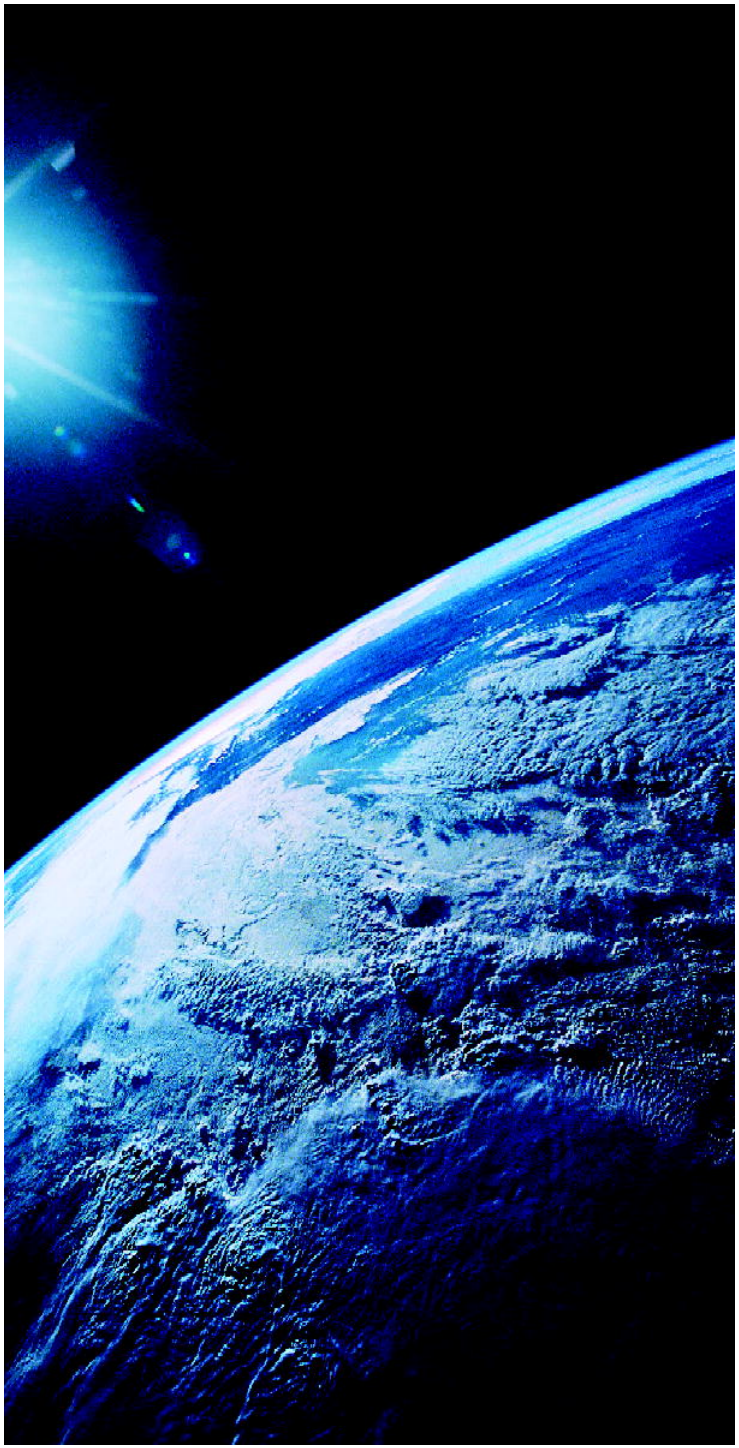
debug ccsip messages



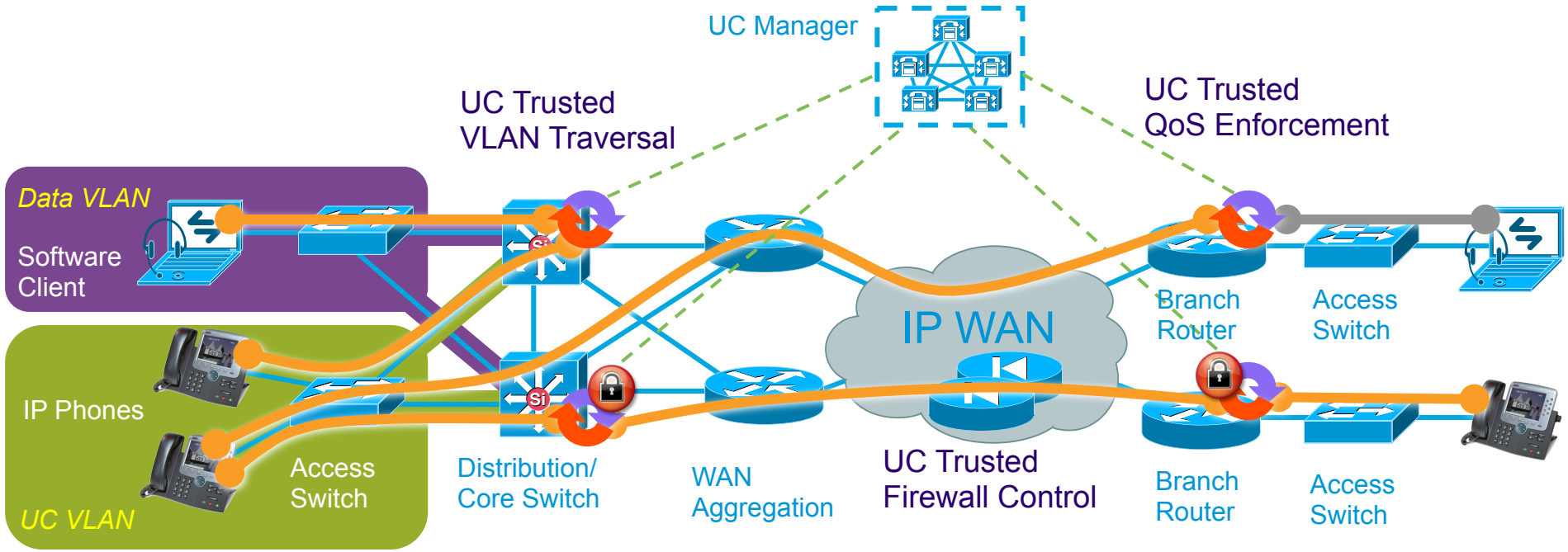
Using Unified CM Network Capture

```
admin:utils network capture size 1500 port 5060 file testsipcap verbose
Executing command with options:
 size=1500              count=1000             interface=eth0
 src=                   dest=                  port=5060
 ip=
admin:file list activelog platform/cli/
testsipcap.cap
dir count = 0, file count = 1
admin:file get activelog platform/cli/testsipcap.cap
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 6040
Total size in Kbytes: 5.8984375
Would you like to proceed [y/n]? y
SFTP server IP: 192.168.101.101
SFTP server port [22]:
User ID: admin
Password: ********
Download directory: Downloads
.
Transfer completed.
```

rusted Relay
oint (TRP)
& L3 VPN



rusted Relay Point (TRP) Overview

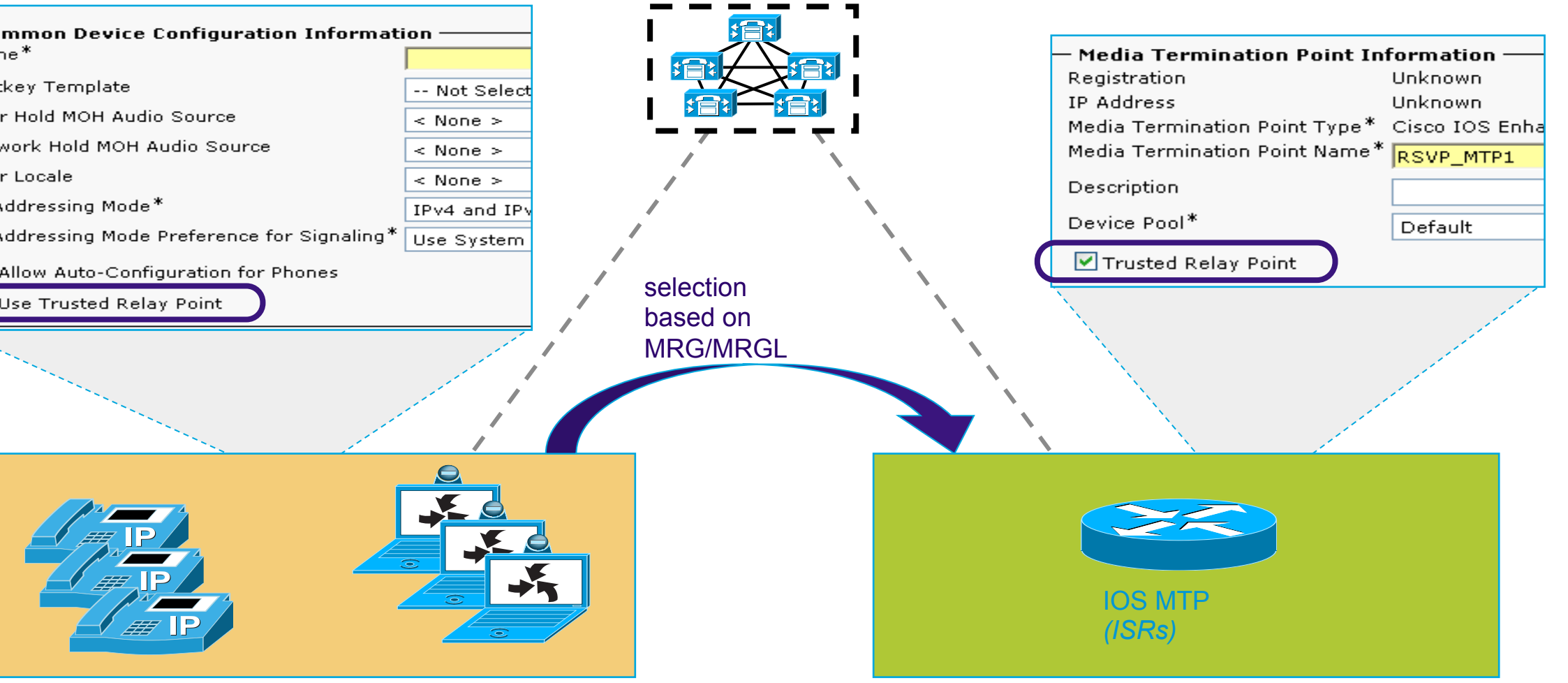


Software function that runs on Cisco network devices such as campus switches and routers *(similar to an MTP)*

Inserted in the call flow by CUCM 7.0 (or CUCME 4.0) based on config

Provides **trusted** anchoring point for media to enable several functionalities (QoS enforcement, Trusted VLAN traversal, ...)

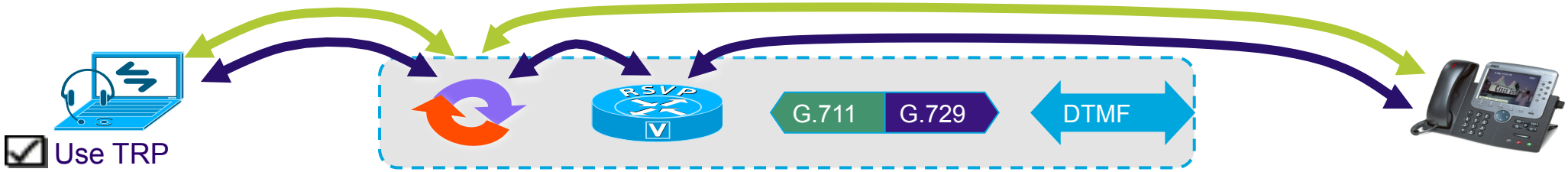
onfigurating TRP Features in CUCM 7.0



dpoints *(anything that terminates media)*

Media Termination Points (MTPs)

UCM TRP Insertion “Rules”



If multiple functions are required for a given call (Xcoder, TRP, RSVP Agent, DTMF relay...), CUCM will first attempt to select an MTP that can fulfill them all

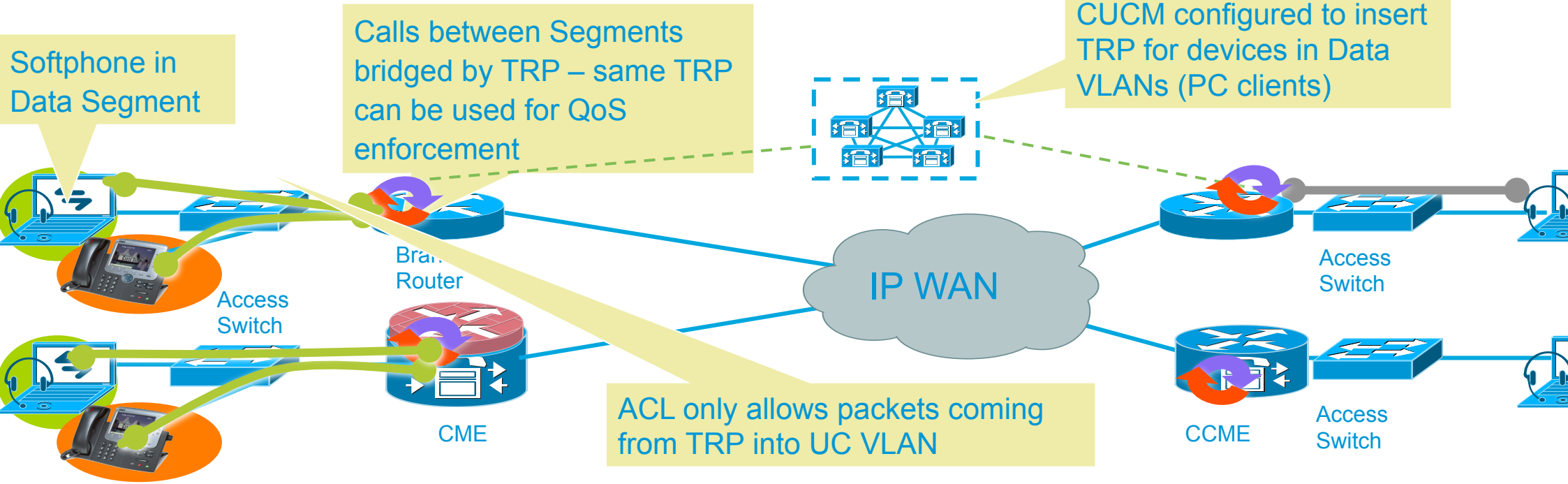
If that is not possible, the TRP will be placed ‘closest’ to the endpoint

TRP supports SRTP and video (“pass-through” codec)

If a call is placed on hold, TRP stops streaming media, but resource is kept

If CUCM is unable to allocate a TRP for a call, the call will fail or not depending on the service parameter “Fail Call if Trusted Relay Point allocation fails” (default is true)

C-Trusted VLAN Traversal



TRP enables Secure IP Phone Connectivity by securely bridging only “authorized” (CUCM or CME) media from Data to UC VLAN

TRP can also remark the QoS for “authorized traffic” from the Softphone

CUCM 7.0 and CME 4.0 (12.4.9T)

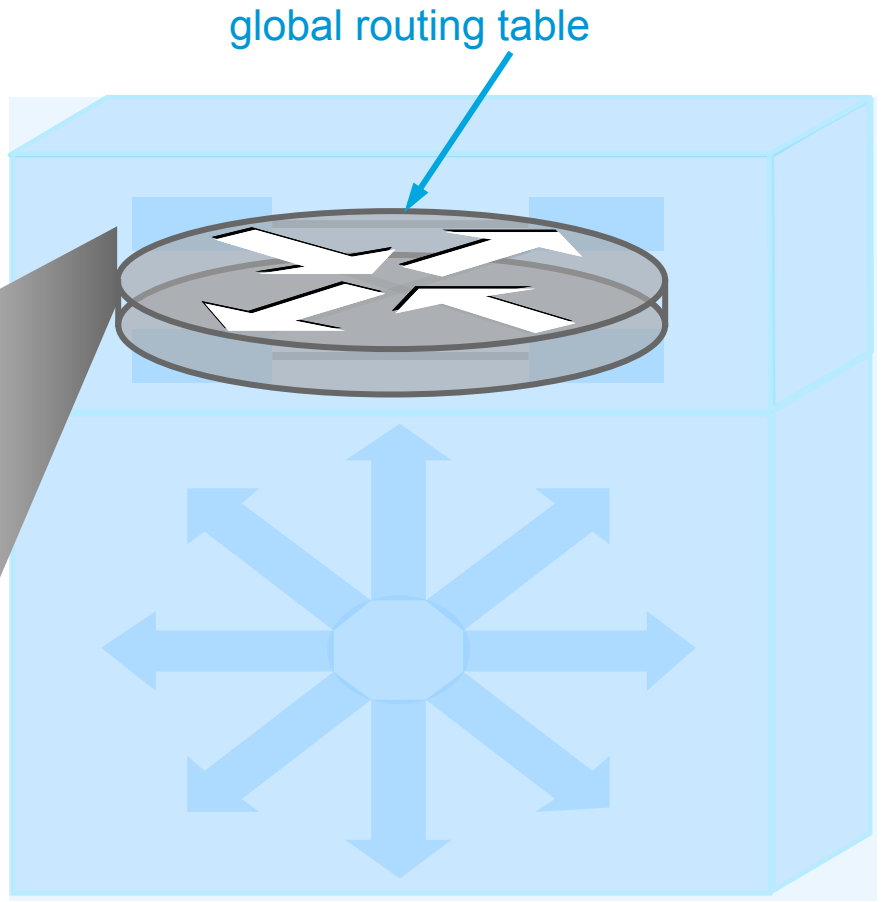
Reference

RF Overview

hat is a VRF (Virtual Routing and Forwarding)?

Typically all route processes and static routes are populating one routing table

All interfaces are part of the global routing table




```
router eigrp 1
 network 10.1.1.0 0.0.0.255
!
router ospf 1
 network 10.2.1.0 0.0.0.255 area 0
!
router bgp 65000
 neighbor 192.168.1.1 remote-as 65000
!
ip route 0.0.0.0 0.0.0.0 140.75.138.114
```

Reference

RF Overview

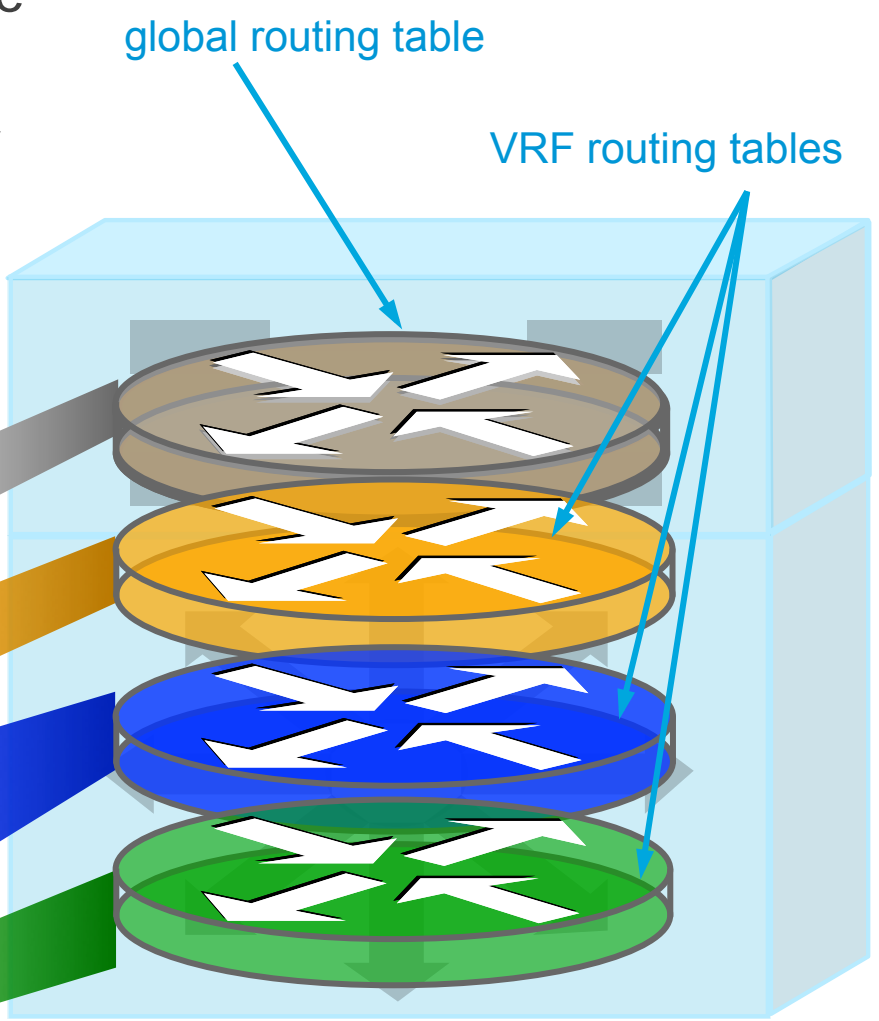
hat is a VRF (Virtual Routing and Forwarding)?

VRFs allow dividing up your routing table into multiple virtual tables

Routing protocol extensions allow binding a process/ address family to a VRF

Interfaces are bound to a VRF using ip vrf forwarding <vrf-name>

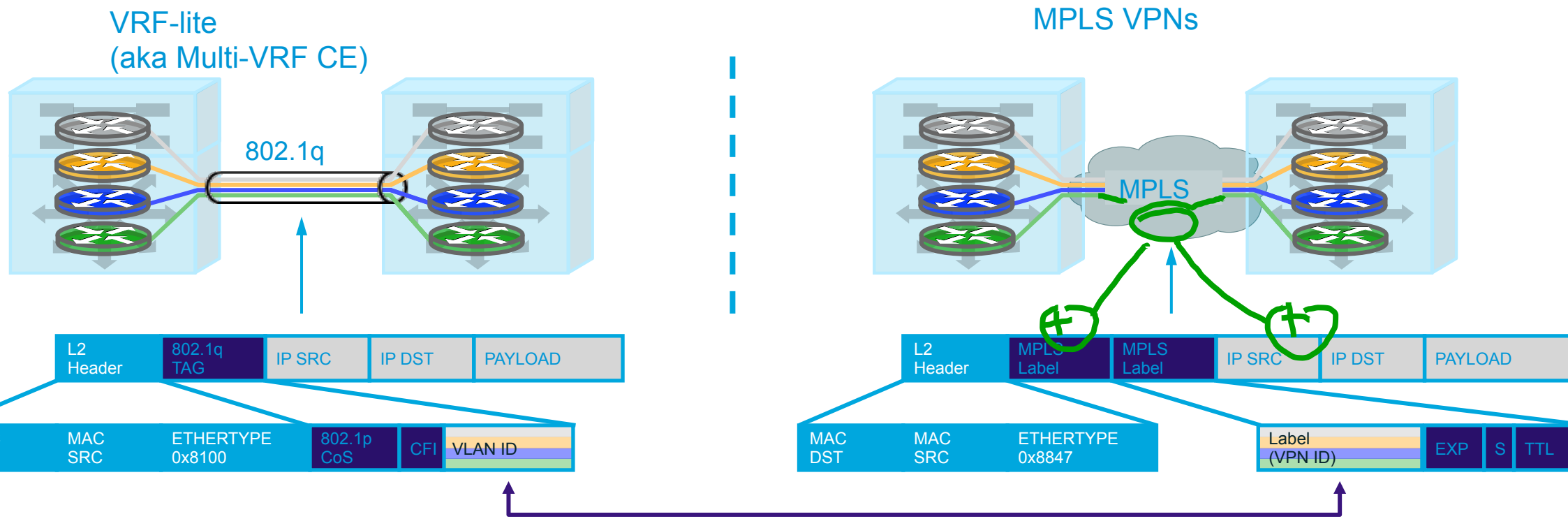
```
router eigrp 1
 network 10.1.1.0 0.0.0.255
!
router ospf 1 vrf orange
 network 10.2.1.0 0.0.0.255 area 0
!
router bgp 65000
 address-family ipv4 vrf blue
 …
!
ip route vrf green 0.0.0.0 0.0.0.0 …
```



RF Overview

ow are VRFs used?

VRFs can be used by themselves (multi-VRF or VRF-lite) or within an MPLS VPN

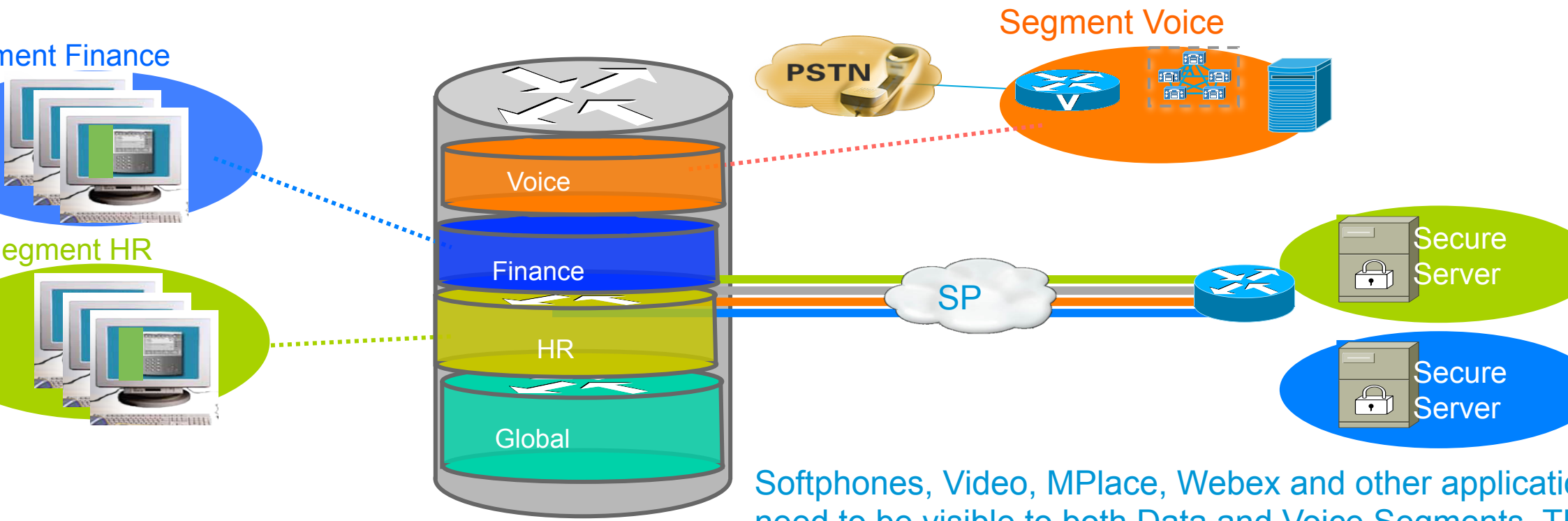


- Defines from which VRF traffic was sourced / for which VRF traffic is destined
- FIB table needs to have this information for each prefix

ecurity with Virtual Networks

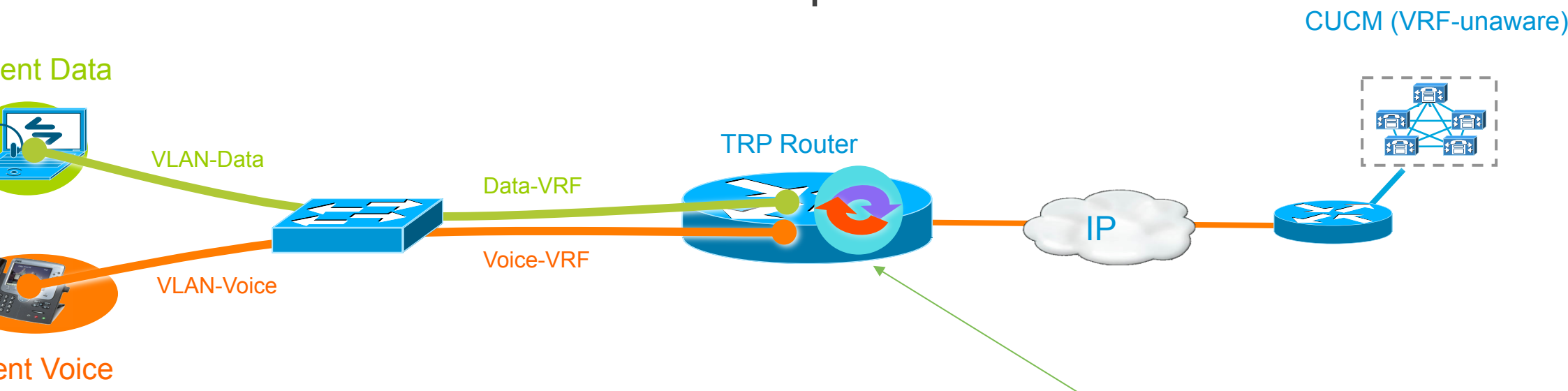
You cannot attack what you cannot reach

Virtualization allows multiple “networks” to share physical infrastructure without being visible to each other



Softphones, Video, MPlace, Webex and other applicati
need to be visible to both Data and Voice Segments. T
can bridge the gap with VRF traversal.

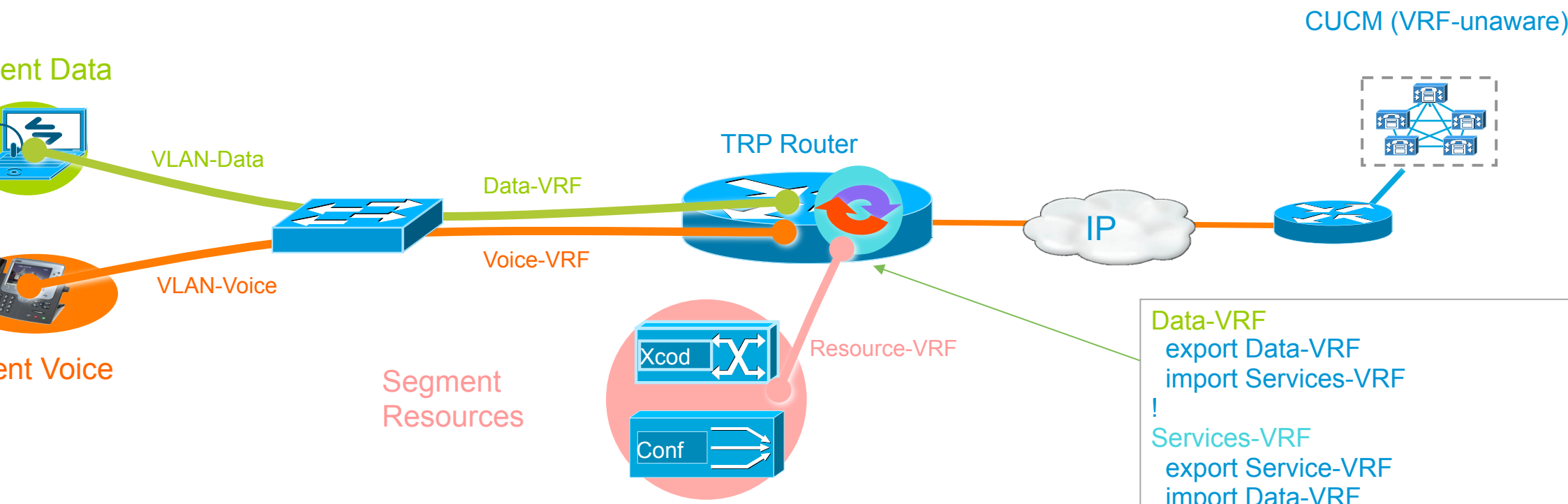
UCM Segmented Network
RP for VRF-Traversal between Endpoints



- Create a Services-VRF visible to all the VRFs to be bridged
- There is no direct path between the Data and Voice VRFs and endpoints on these VRFs can not ping each other
- CUCM connects a TRP to do VRF-traversal
  - TRP does this via the Services-VRF

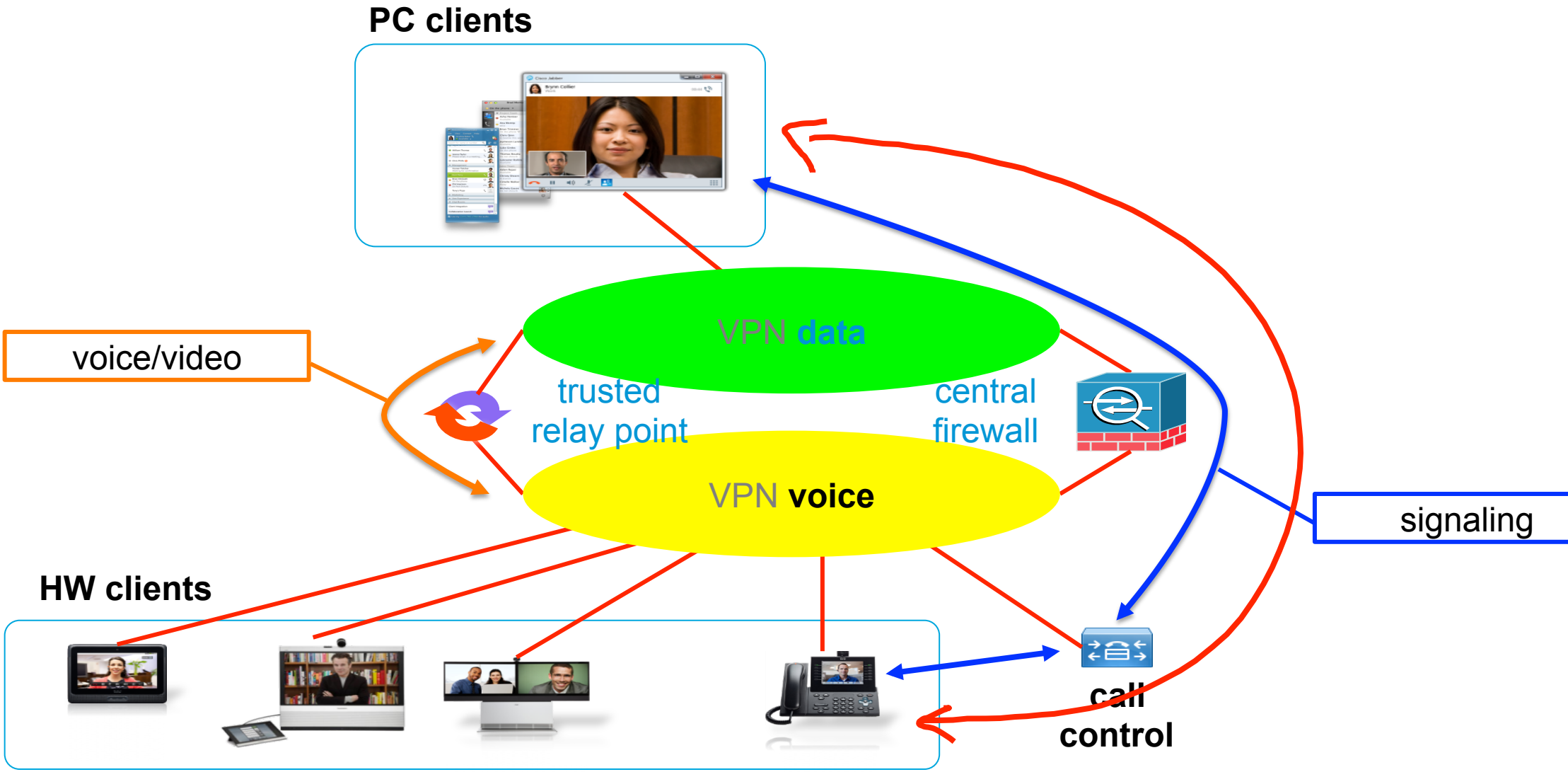
```
Data-VRF
  export Data-VRF
  import Services-VRF
!
Services-VRF
  export Service-VRF
  import Data-VRF
  import Voice-VRF
!
Voice-VRF
   export Voice-VRF
   import Services-VRF
```

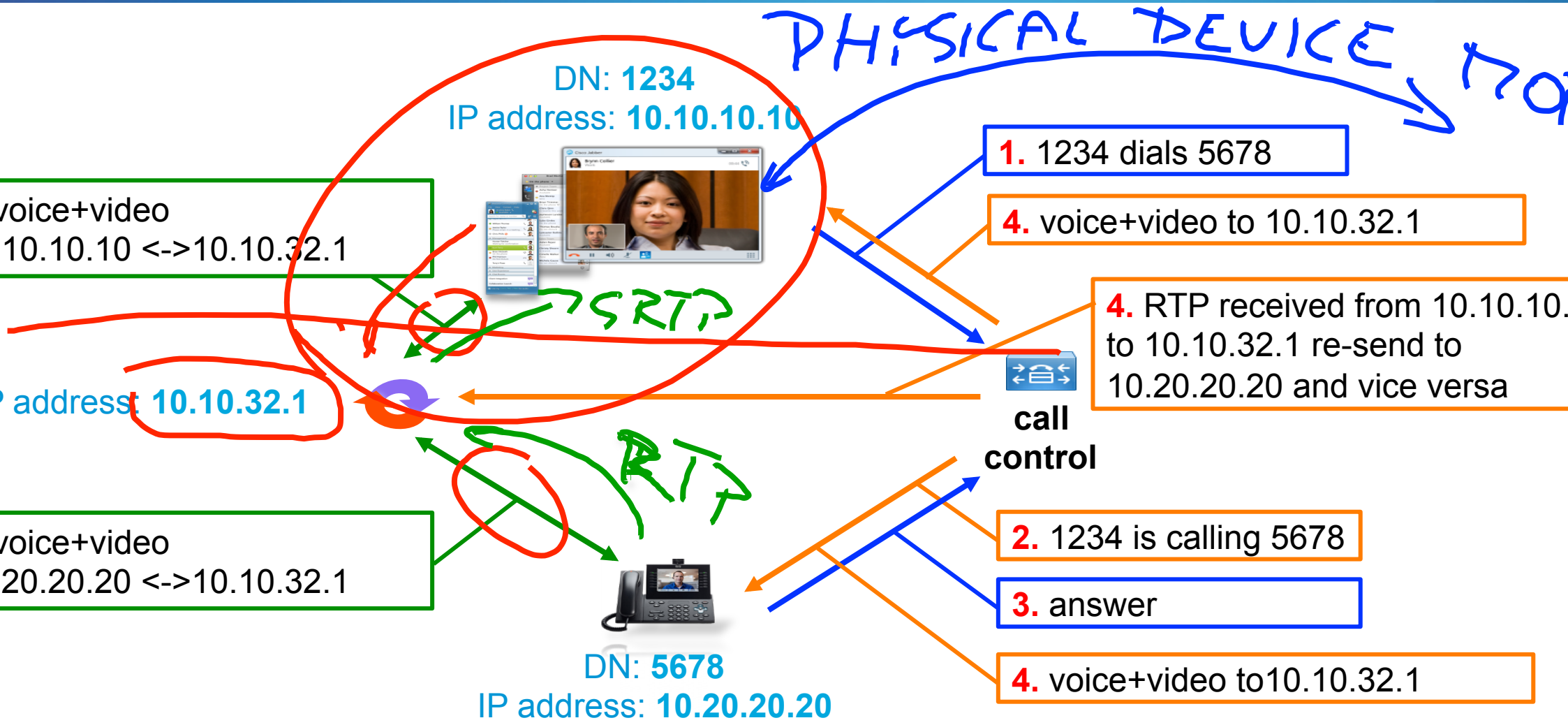
UCM Segmented Network
edia Resources in VRFs



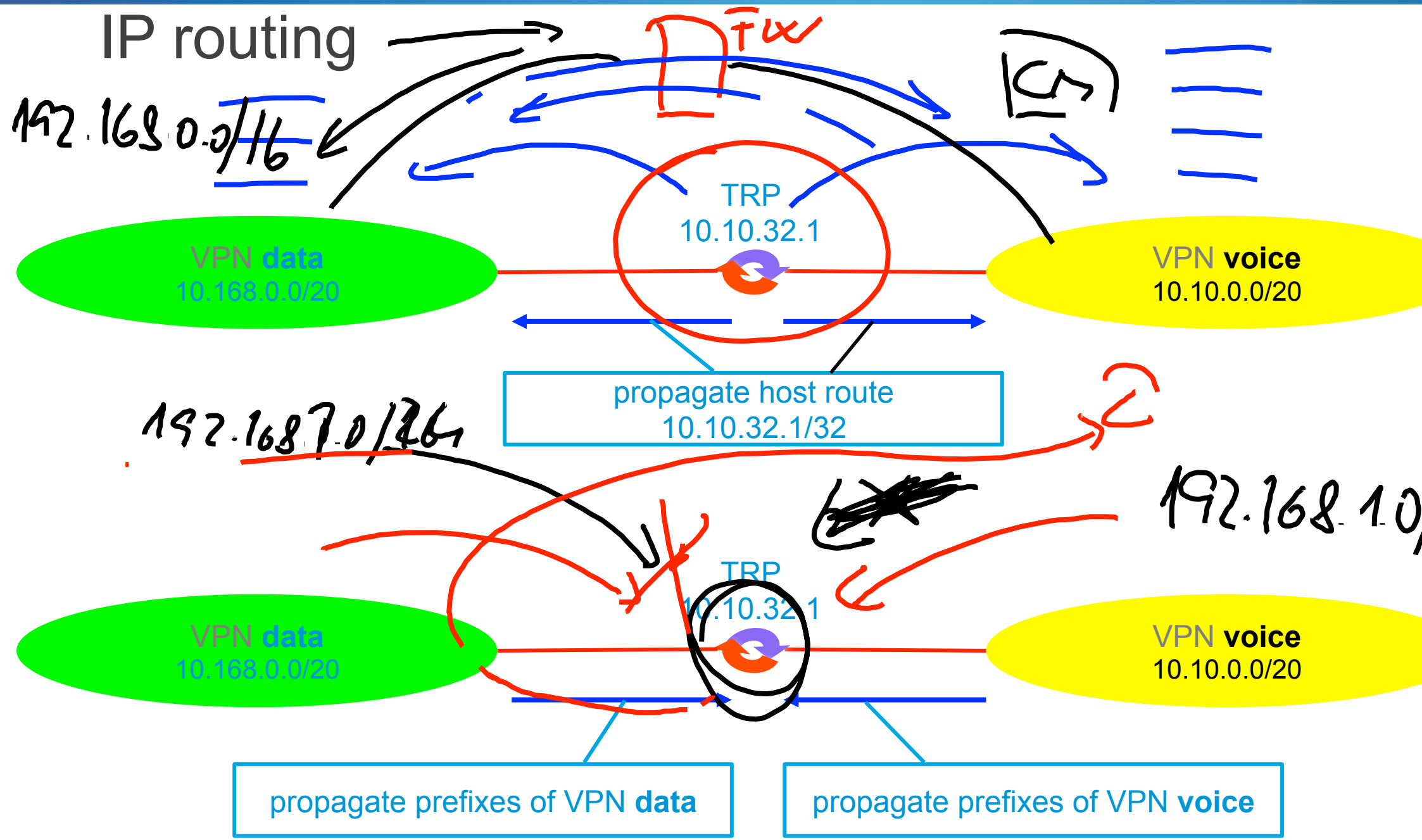
Put DSP resources for Conf/Xcod in a separate Resources-VRF so that the TRP (via a Services-VRF) can bridge any endpoint (from any VRF) to access the shared resources, w/o create a direct ping path between the endpoints

```
Data-VRF
  export Data-VRF
  import Services-VRF
!
Services-VRF
  export Service-VRF
  import Data-VRF
  import Voice-VRF
  import Resource-VRF
!
Voice-VRF
   export Voice-VRF
   import Services-VRF
!
Resource-VRF
  export resource-VRF
  import Services-VRF
```

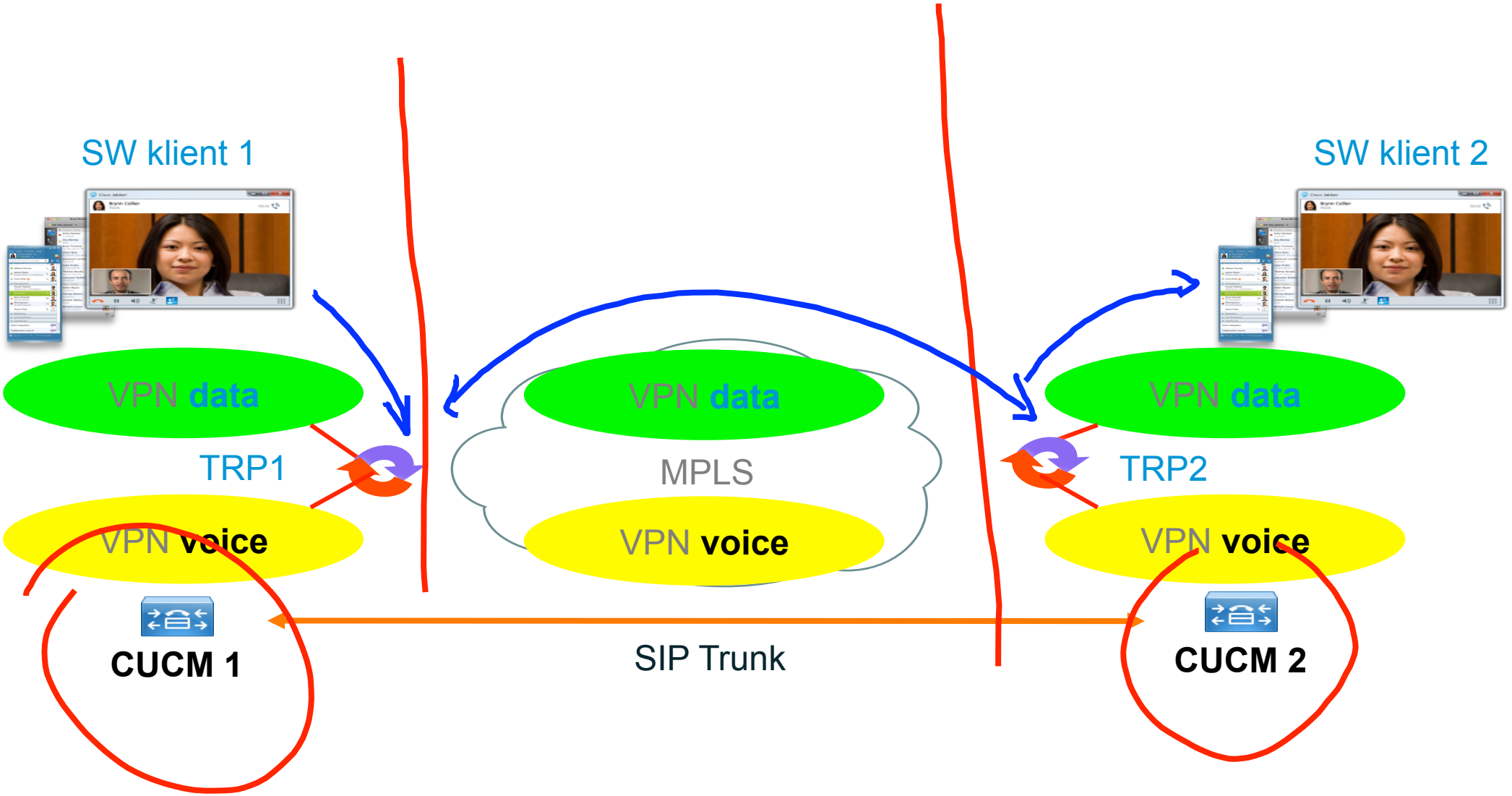

PC clients
voice/video
VPN data
trusted
relay point
central
firewall
VPN voice
signaling
HW clients
call
control


PHYSICAL DEVICE
DN: 1234
IP address: 10.10.10.10
voice+video
10.10.10 <->10.10.32.1
P address: 10.10.32.1
voice+video
20.20.20 <->10.10.32.1
SRTP
RTP
1. 1234 dials 5678
4. voice+video to 10.10.32.1
4. RTP received from 10.10.10.
to 10.10.32.1 re-send to
10.20.20.20 and vice versa
call
control
2. 1234 is calling 5678
3. answer
4. voice+video to10.10.32.1
DN: 5678
IP address: 10.20.20.20

IP routing


Fw
192.168.0.0/16
TRP
10.10.32.1
VPN data
10.168.0.0/20
VPN voice
10.10.0.0/20
propagate host route
10.10.32.1/32
192.168.1.0/24
192.168.1.0
TRP
10.10.32.1
VPN data
10.168.0.0/20
VPN voice
10.10.0.0/20
propagate prefixes of VPN data
propagate prefixes of VPN voice

Multiple CUCM Clusters



Sample Configuration

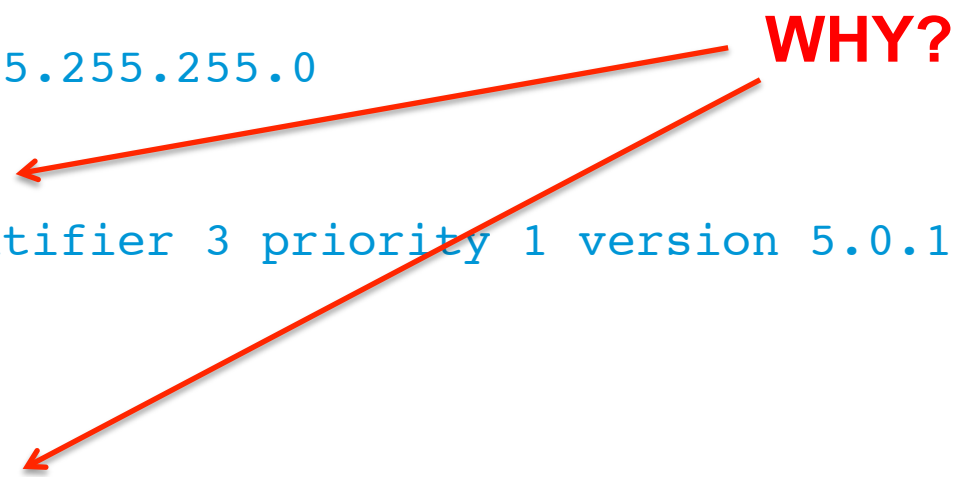
```
terface Loopback999
p vrf forwarding trp
p address 10.168.32.3 255.255.255.255

terface FastEthernet0/0
p address 192.168.24.8 255.255.255.0

cp local FastEthernet0/0
cp ccm 192.168.21.60 identifier 3 priority 1 version 5.0.1
cp

cp ccm group 3
ind interface Loopback999
ssociate ccm 3 priority 1
ssociate profile 30 register TRP-L-1

pfarm profile 30 mtp
odec g711ulaw
odec pass-through
aximum sessions software 20
ssociate application SCCP
```



Sample Configuration

```
al-peer voice 1 pots
estination-pattern 0T
irect-inward-dial
ort 2/0:15

al-peer voice 2 voip
estination-pattern 1...
ession protocol sipv2
ession target ipv4:192.168.21.60
tmf-relay sip-notify
odec g711ulaw
o vad
```

rogram

s	Téma	Přednášející
30 – 10:30	Novinky v Cisco Collaboration	Jaroslav Martan
:45 – 11:45	Nástroje pro management multimediální sítě (Medianet)	Jiří Rott
	oběd	
:45 – 13:45	Architektura collaboration řešení - Jabber Design - Integrace Cisco UC a MS OCS/Lync	 Jaroslav Martan Ivan Sýkora
:00 - ???	Architektura – whiteboard (jam) session - Edge design - SIP trunk - Video – jednotný call control - Trusted Relay Point (TRP) a L3 VPN	 Jaroslav Martan Jiří Rott Jaroslav Martan Jaroslav Martan

Prosíme, ohodnoťte tuto přednášku.

Děkujeme za pozornost.