



New Features of Unified Communications System 8.0

Agenda

- Extension Mobility Cross Cluster (EMCC)
- Service Advertisement Framework (SAF) – Call Control Discovery (CCD)
- SAF-CCD Demo
- New Phones Experience
- New Phones Demo
- Q&A

Agenda

EMCC Overview

EMCC Registration

EMCC Call Processing

EMCC Call Admission Control

EMCC Security

EMCC Design Considerations



EMCC Overview



Overview – Extension Mobility

- Extension Mobility was first offered in CallManager 3.1 release
- EM has been limited to intra-cluster users/devices
- Customers want a seamless experience, no matter where they log in:

User wants the same set of features and services - all lines, speed dials, message button, MWI and features.

Administrator wants security, CAC, local gateway access, local media resources and serviceability.

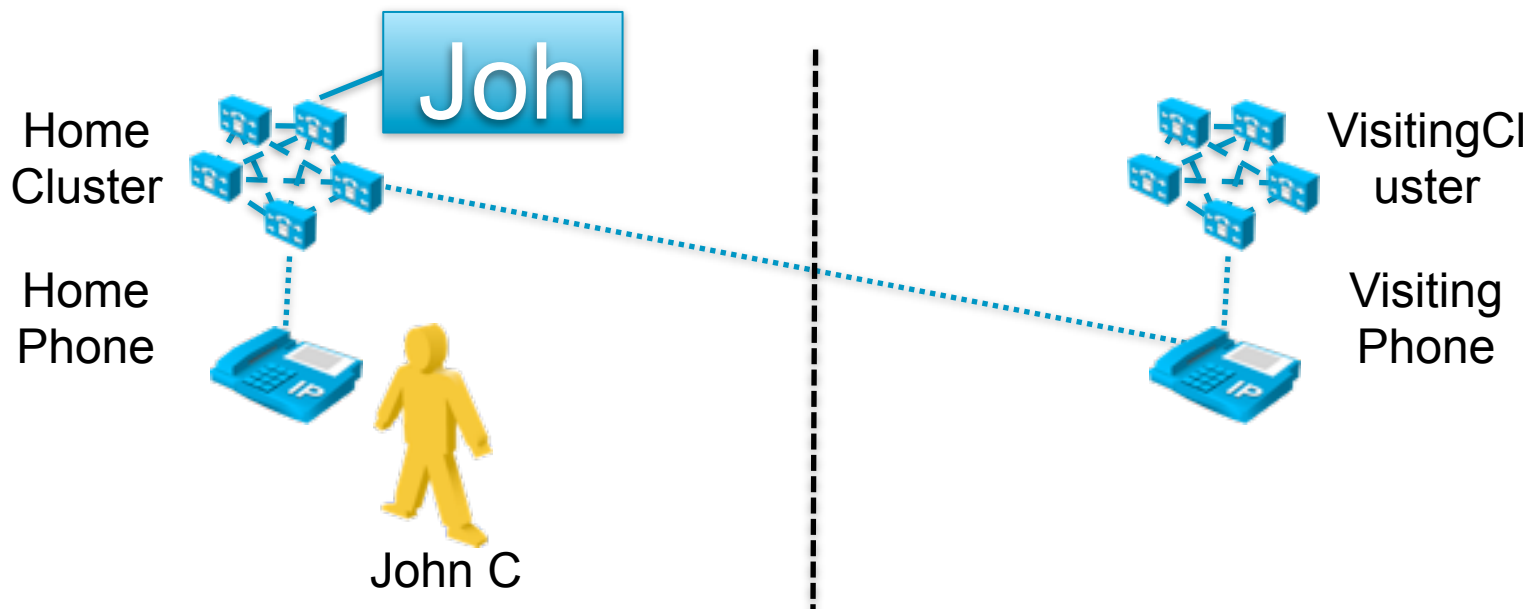
Overview – Extension Mobility Cross Cluster Challenges

Extension Mobility Cross Cluster must support ...

- EM Login/Logout across clusters
- Cross-cluster Security By Default (more later)
- IP phones with non-secure security profiles
- PSTN access suitable for the visiting phone (Local calls must route to local gateways in visiting cluster)
- RSVP agent-based CAC using RSVP agents in the visiting cluster
- Dynamic CTI control of a visiting phone

Overview – Extension Mobility Cross Cluster Concepts

 New Terminology: “Visiting” & “Home” Clusters
(from USER’s perspective!)



 Visiting Phone registers with Home Cluster

Home Cluster dialing habits are maintained!

EMCC Overview



Good News - Features Work!

- Shared line, hunt lists, transfer/conference/hold/call forward, cellular mobility, barge/cBarge, iDivert, applications, speed dials, services, address book, device labels, line appearance management, MWI, voice mail, do-not-disturb, monitoring, recording, callback busy/NR, MLPP...

Note: Functionality works ... but keep in mind these features may now be occurring across a WAN – not all will be tested with added delay.

- Features supported in future releases
 - Media resources local to the visiting phone (Other than RSVP Agents)
 - Secure phones, sRTP support

EMCC Registration

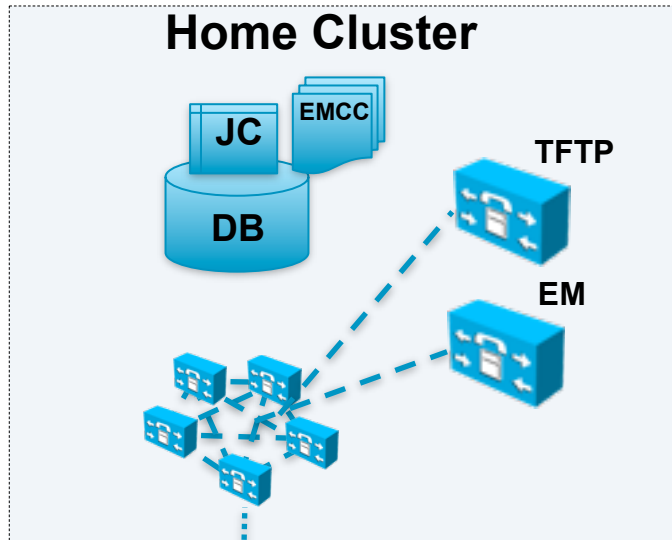


EMCC Login Process Summary

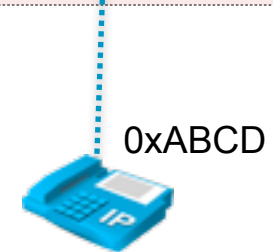
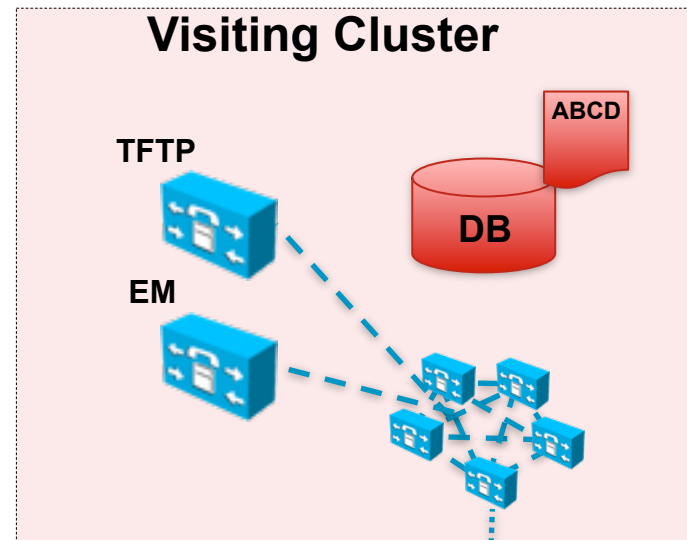
- Users from a “Home” Cluster (HC) login to a phone at a “Visiting” Cluster (VC)
- Login procedure brings the device information into the HC database
- HC database builds a temporary phone device with user’s device profile
- HC TFTP server builds the phone configuration file
- After login, VC directs the phone to HC TFTP server
- Phone downloads its TFTP configuration from HC TFTP server and then cross-registers with HC CUCM

EMCC Login (1 of 4)

The “Before” picture ...



John C



0xABCD



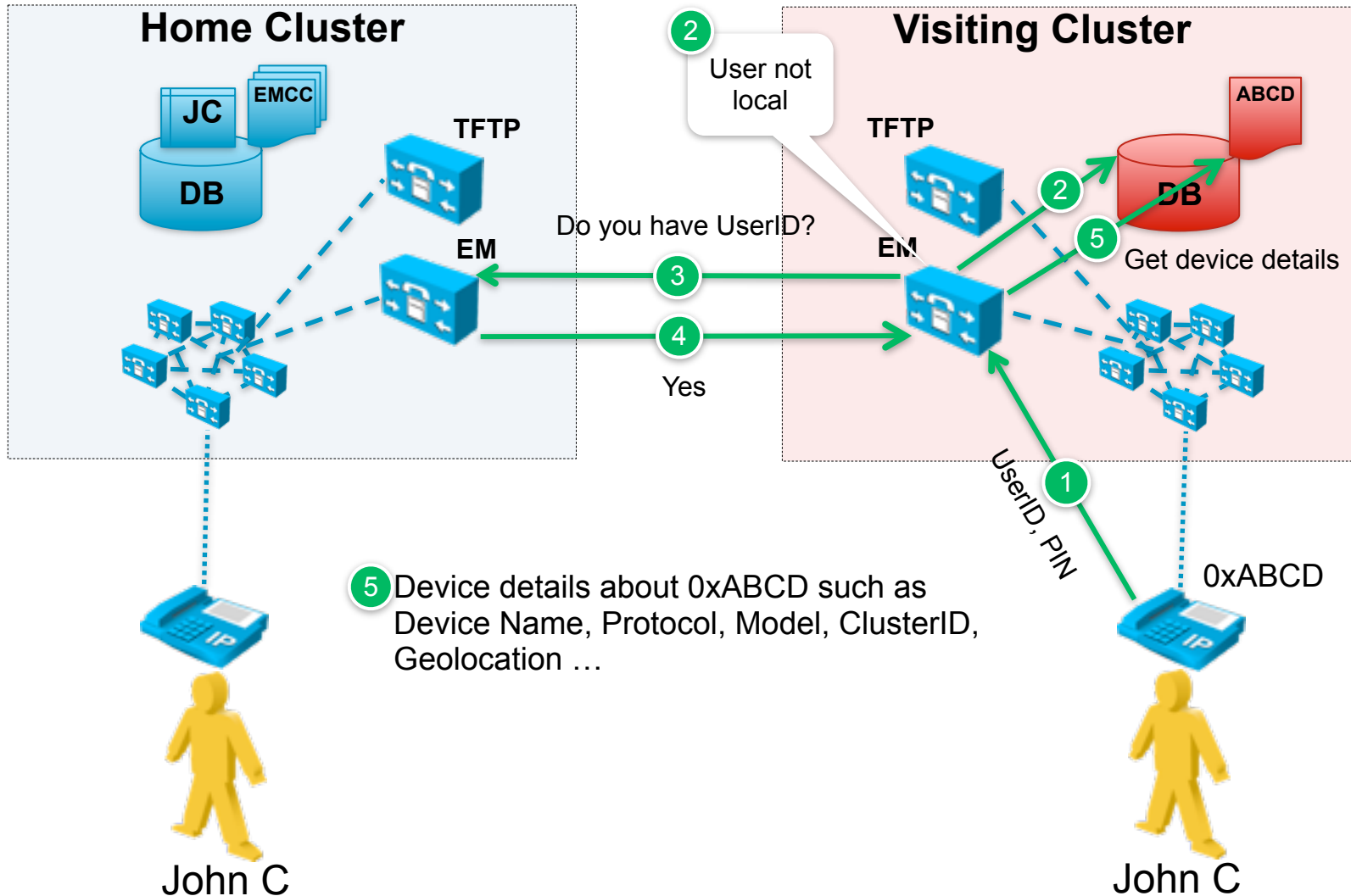
= Device Profile



= Phone Config

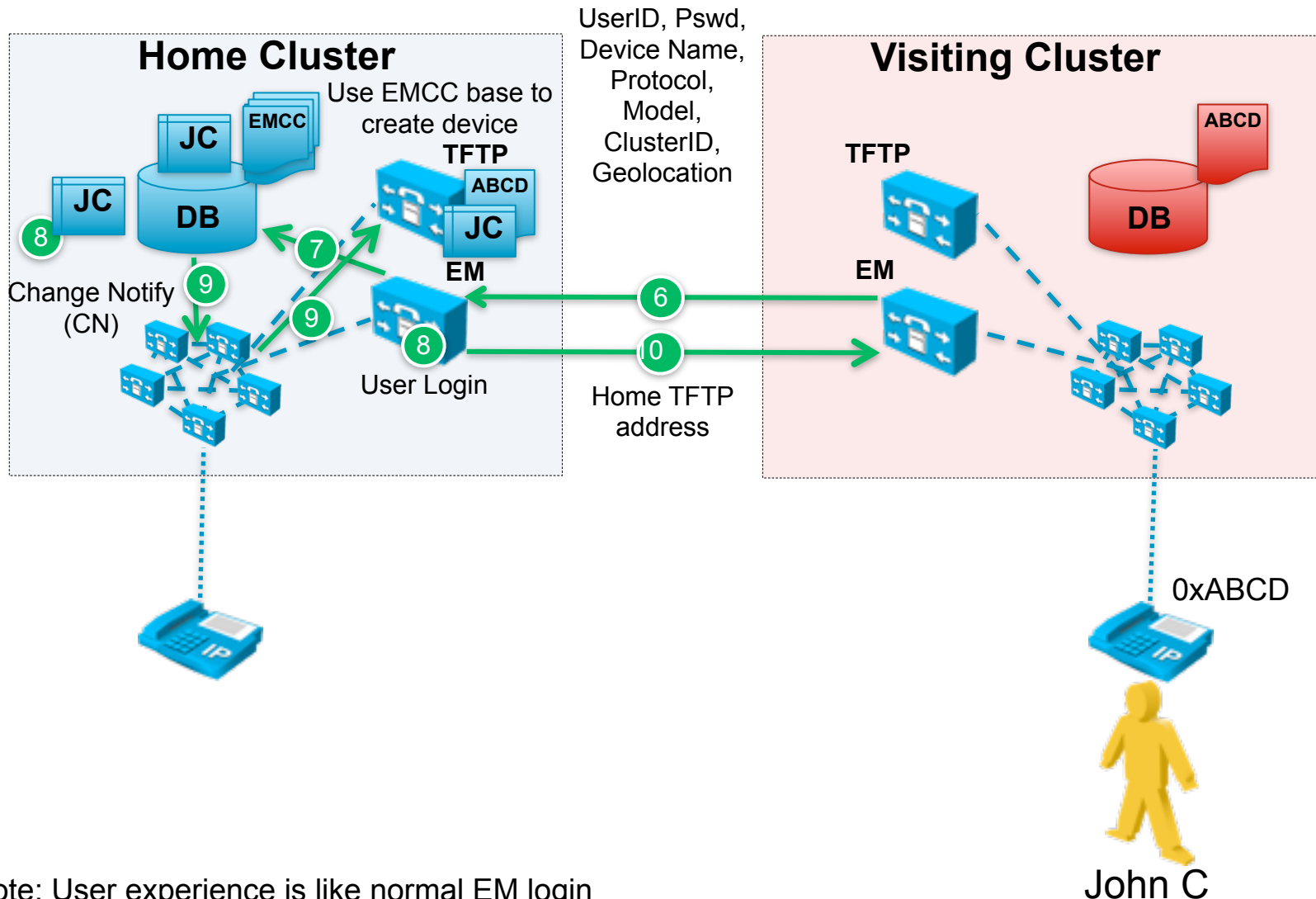
EMCC Login (2 of 4)

Find User's Home Cluster ...



EMCC Login (3 of 4)

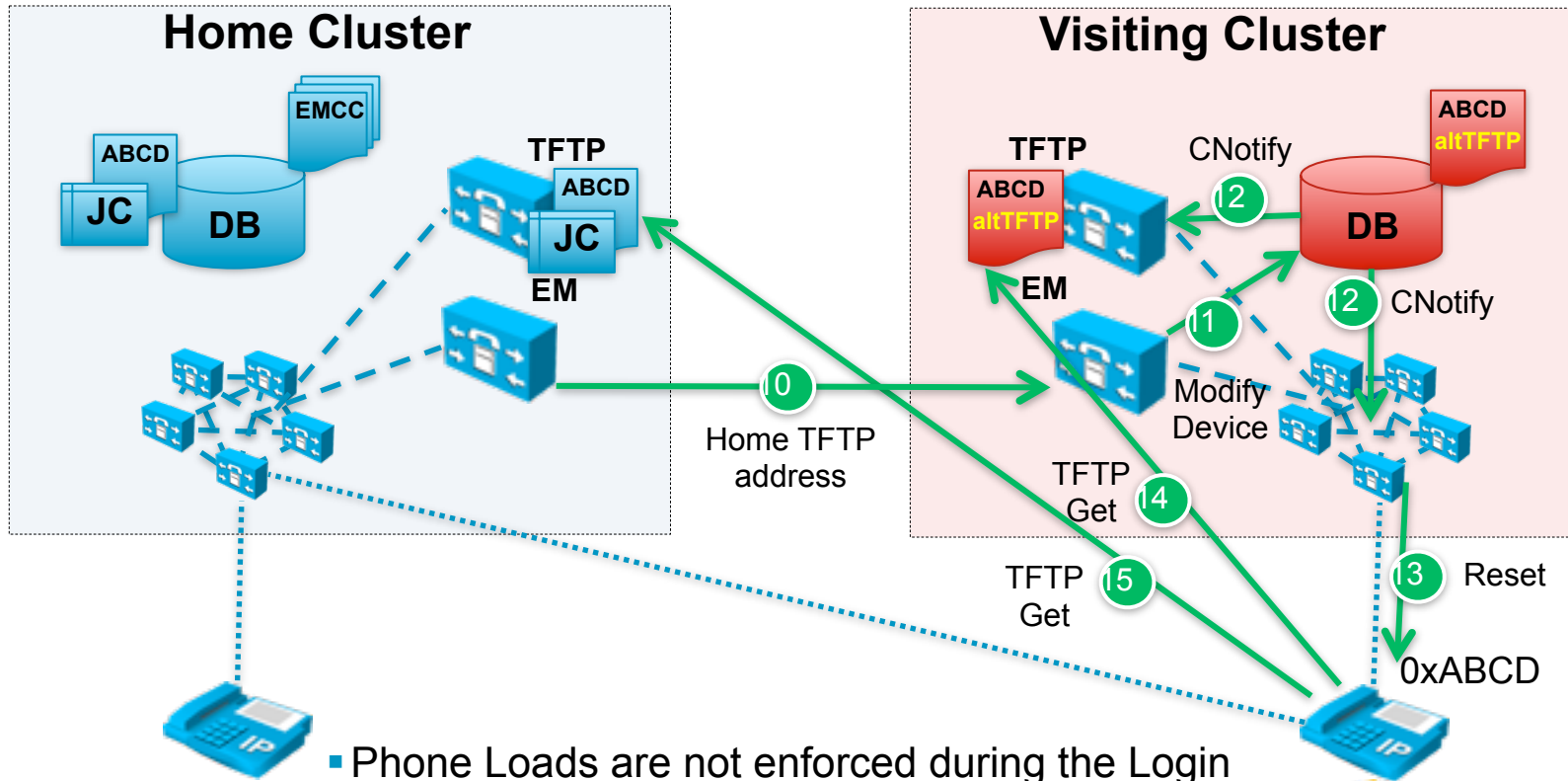
Home Cluster Preparation ...



Note: User experience is like normal EM login during this process.

EMCC Login (4 of 4)

Visiting Cluster Preparation



- Phone Loads are not enforced during the Login process. Removed from Home Cluster config.
- Step 16: If HC locale is different, phone will download new locale from Visiting TFTP server. If not available, maintains VC locale.
- DLUs are NOT consumed in the Home Cluster for John C the visiting phone.

EMCC Registration

Where Do Device Attributes Come From?

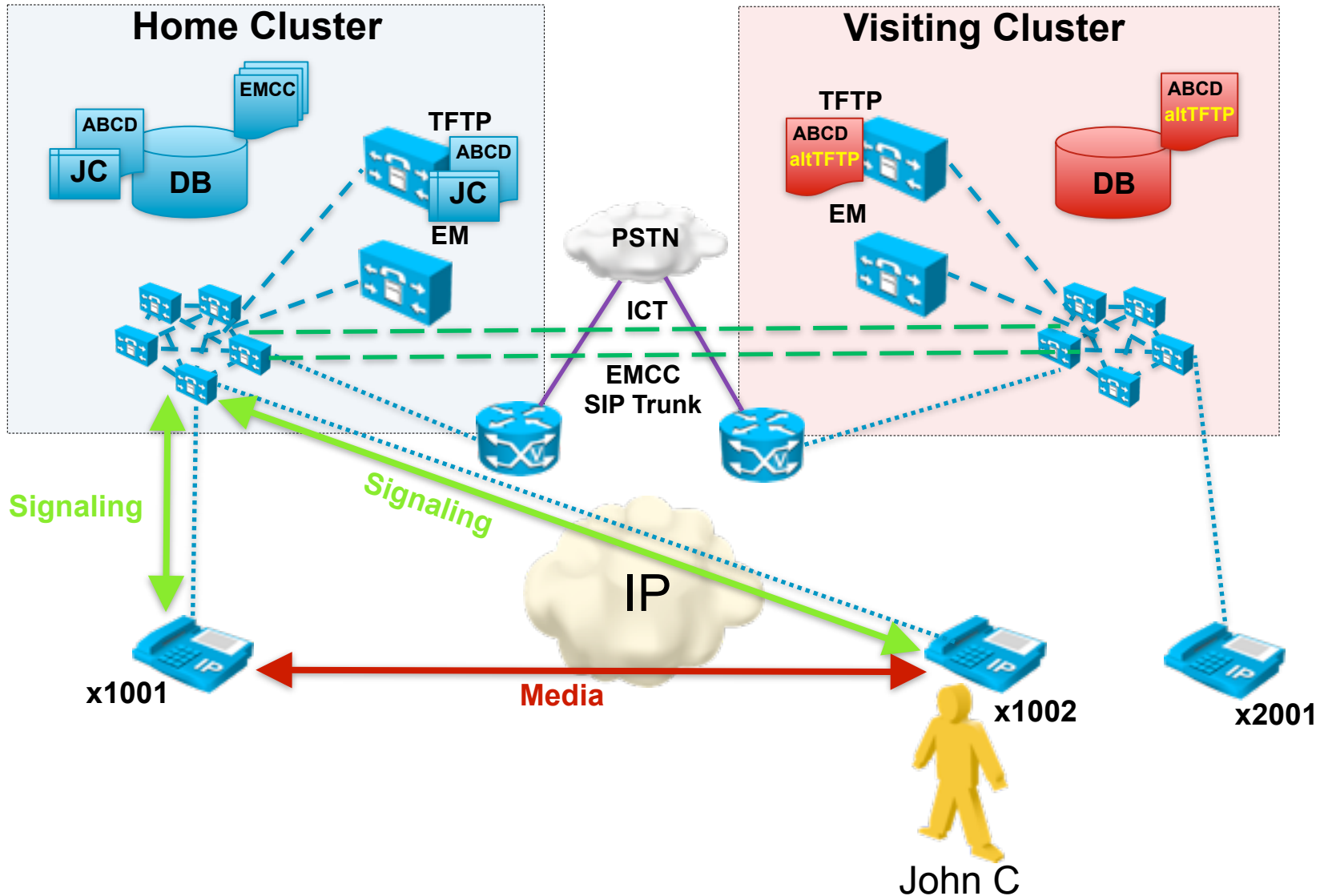
- Bulk Administration => EMCC => EMCC Template
 - Common Device Configuration
 - Common Phone Profile

EMCC Call Processing



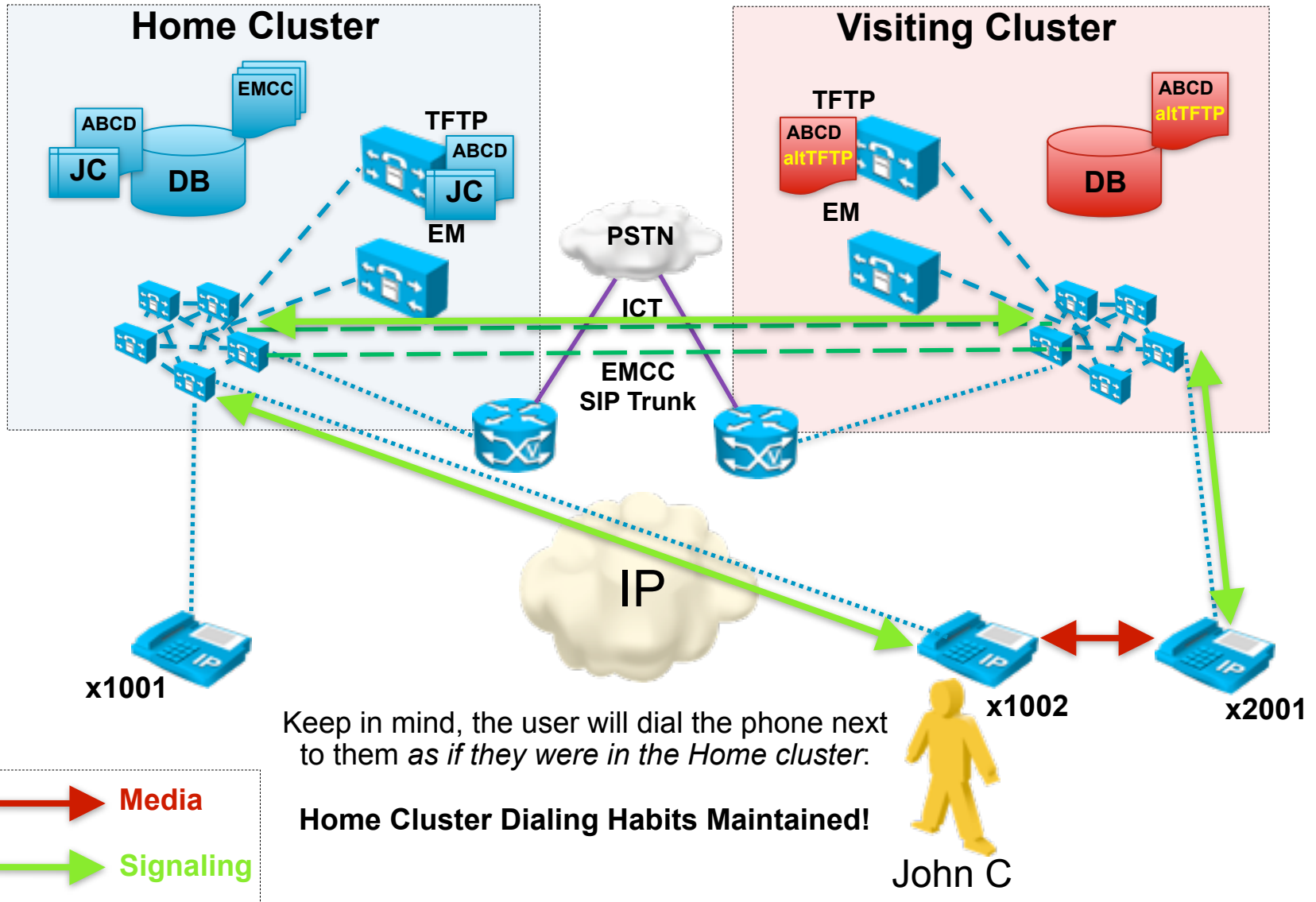
EMCC Call Flows

Phone to HC Phone



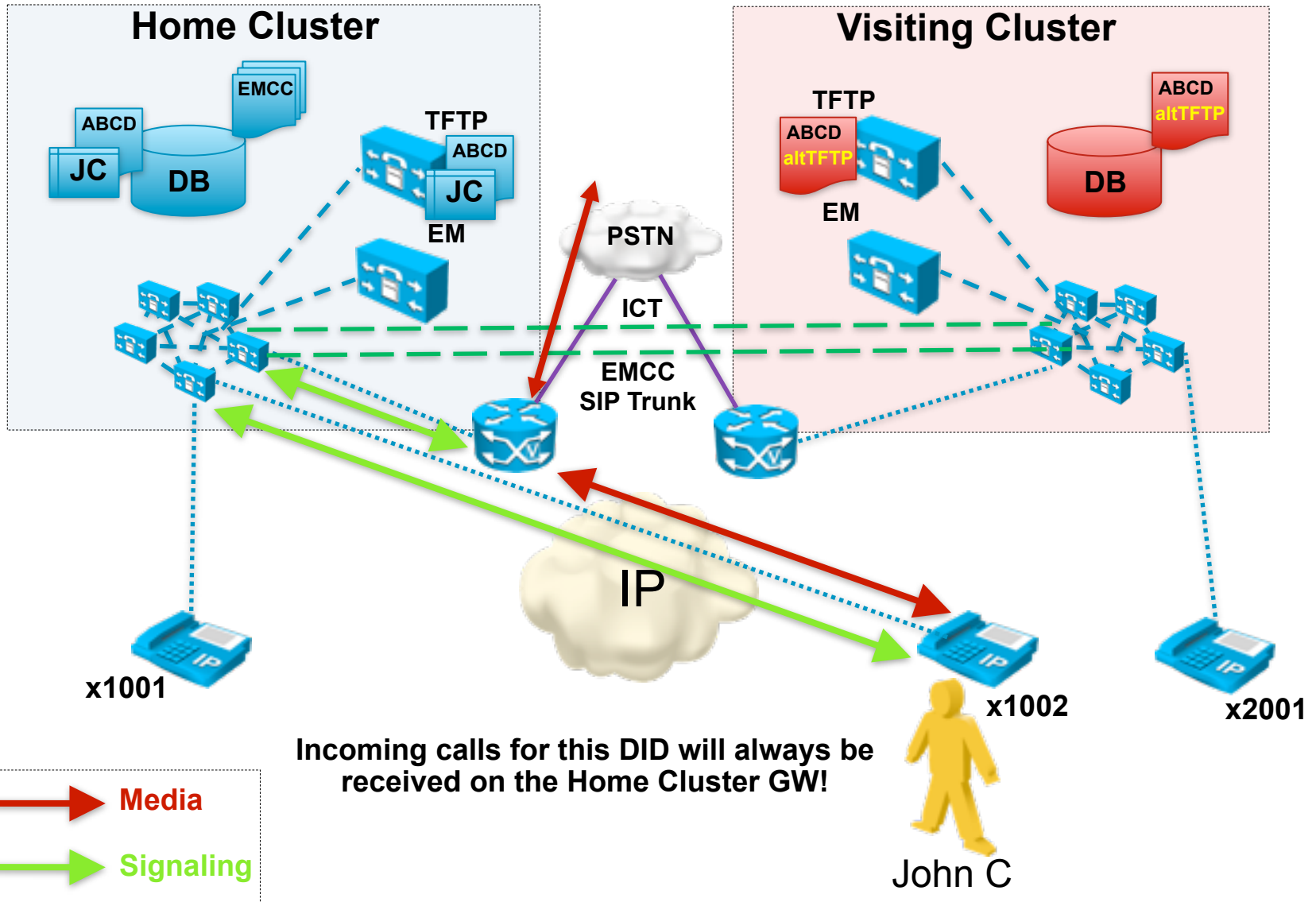
EMCC Call Flows

Phone to VC Phone



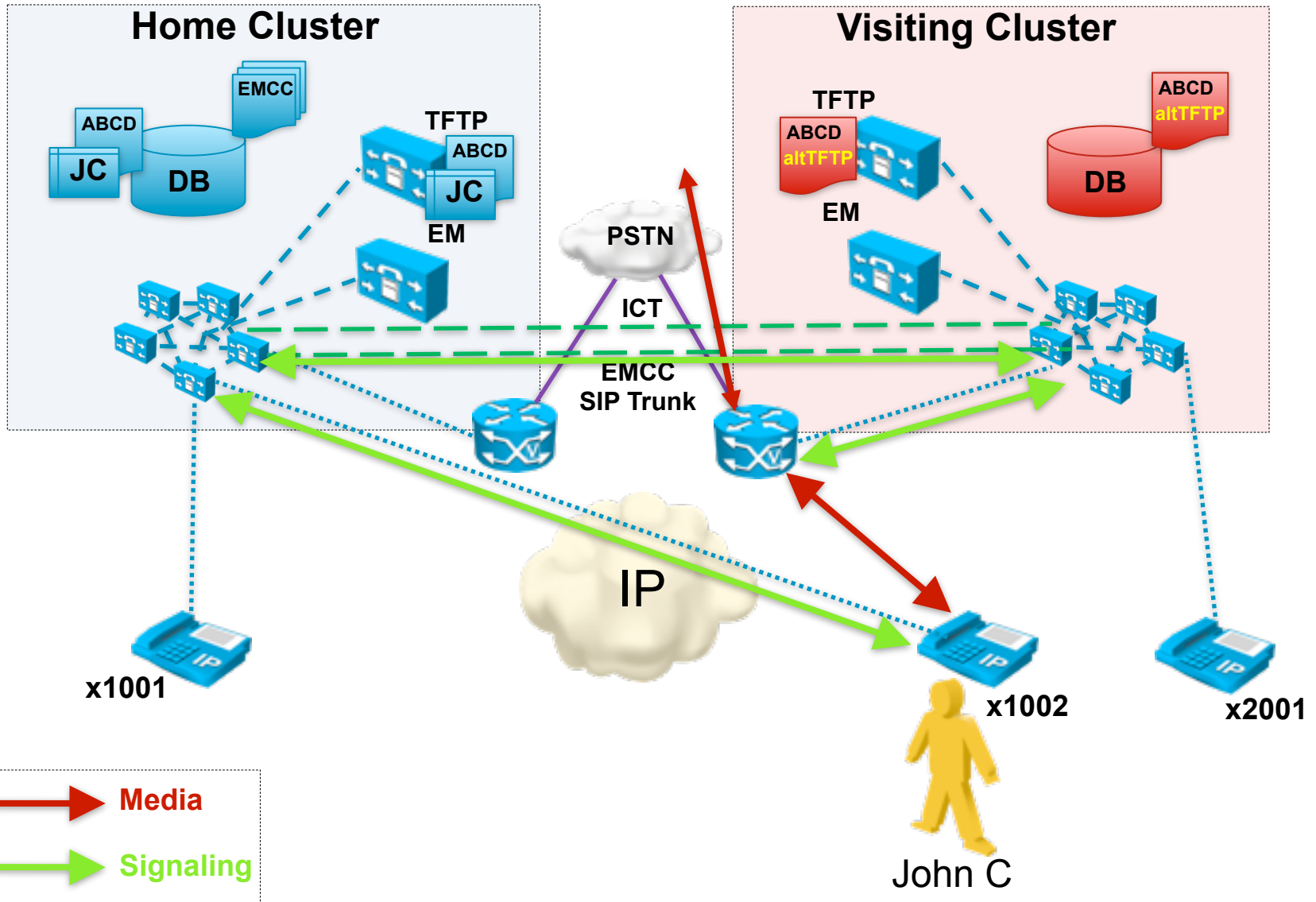
EMCC Call Flows

Phone to PSTN – NO Local Route Group



EMCC Call Flows

Phone to PSTN – WITH Local Route Group



EMCC Call Flows

EMCC SIP Trunk for PSTN Access

Other Considerations:

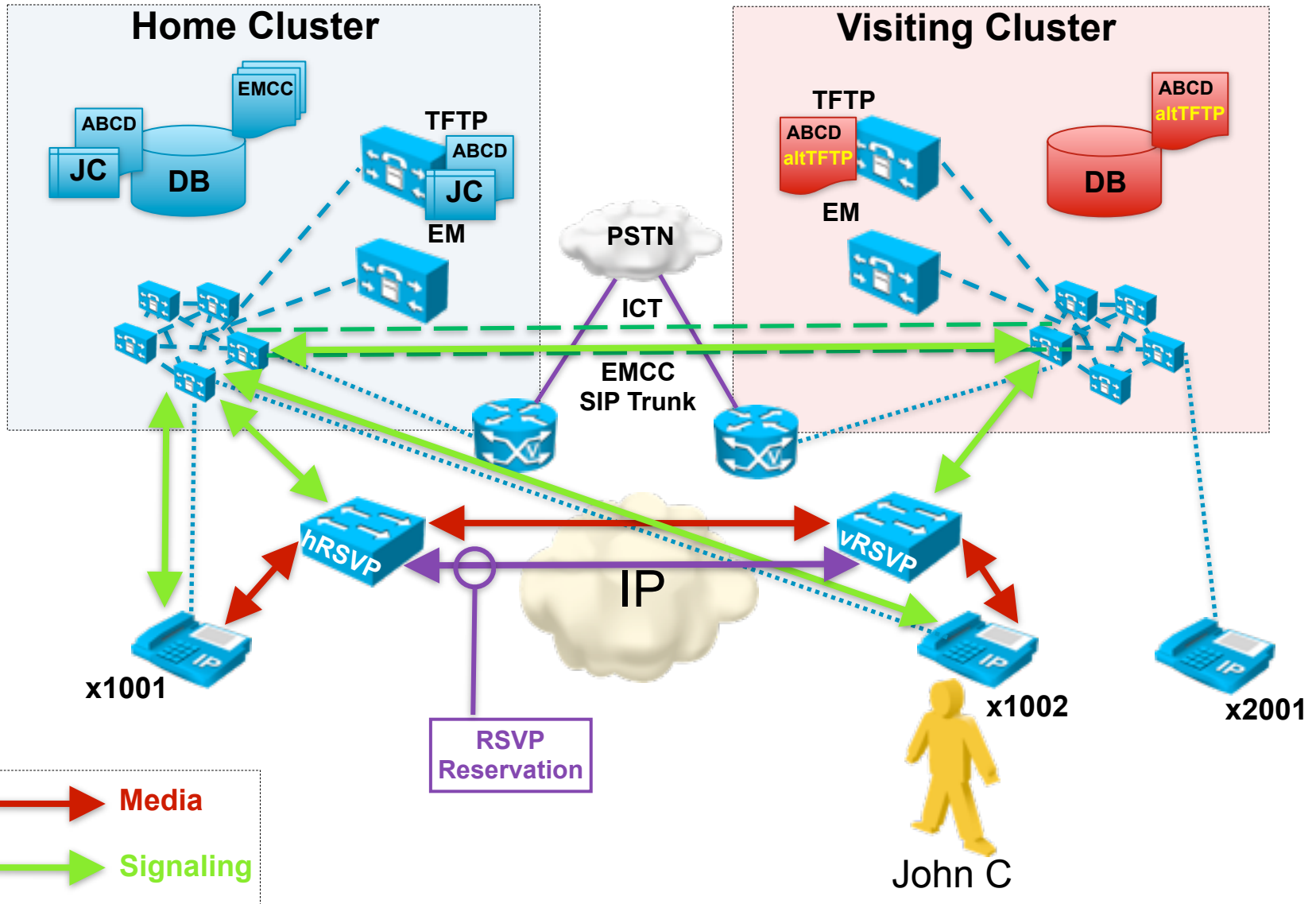
- Home cluster may or may not use LRG. If no LRG, then call follows the configured Route List => Route Group => Gateway path.
- If Yes LRG, Visiting cluster receives call and looks up the *original Visiting phone configuration* in the database to determine its LRG setting (via its Device Pool) to find the appropriate gateway for the call.

EMCC Call Admission Control



EMCC Call Flows

Phone to HC Phone with RSVP



Configure RSVP for EMCC phones

- Configure a Location in the HC, and assign to the EMCC roaming device pool.
- Set RSVP policy for Location pairs in the HC that include this Location associated with the EMCC roaming device pool.
- HC and VC, must have RSVP Agent media resources configured. Visiting phone must have them in its MRGL.
- When allocating RSVP agent, HC CUCM will recognize the RSVP agent is for EMCC phone and redirect the request to VC over RSVP SIP Trunk
- *Note: When allocating all other media resources, HC Unified CM will allocate them based on the MRGL configured in HC EMCC roaming device pool.*
- *Note: Remember, Region settings (Audio/Video bandwidth) come from EMCC Feature Configuration:*

EMCC Region Max Audio Bit Rate *	8 kbps (G.729)	8 kbps (G.729)
EMCC Region Max Video Call Bit Rate (Includes Audio) *	384	384
EMCC Region Link Loss Type *	Low Loss	Low Loss

EMCC Security





HTTPS: Phone Services and Phones

- Phone Services that support HTTPS
 1. **Extension Mobility (EM)**
 2. **Extension Mobility Cross Cluster (EMCC)**
 3. Manager Assistant (IPMA)
 4. IP Phone Services (CCMCIP)
 5. Personal Directory (CCMPD)
 6. **Change Credentials**
- Supported phones: 7906, 7911, 7931, 7941, 7961, 7970, 7942, 7945, 7962, 7965, 7975
- If the device does not support HTTPS, non-secure version of URL used

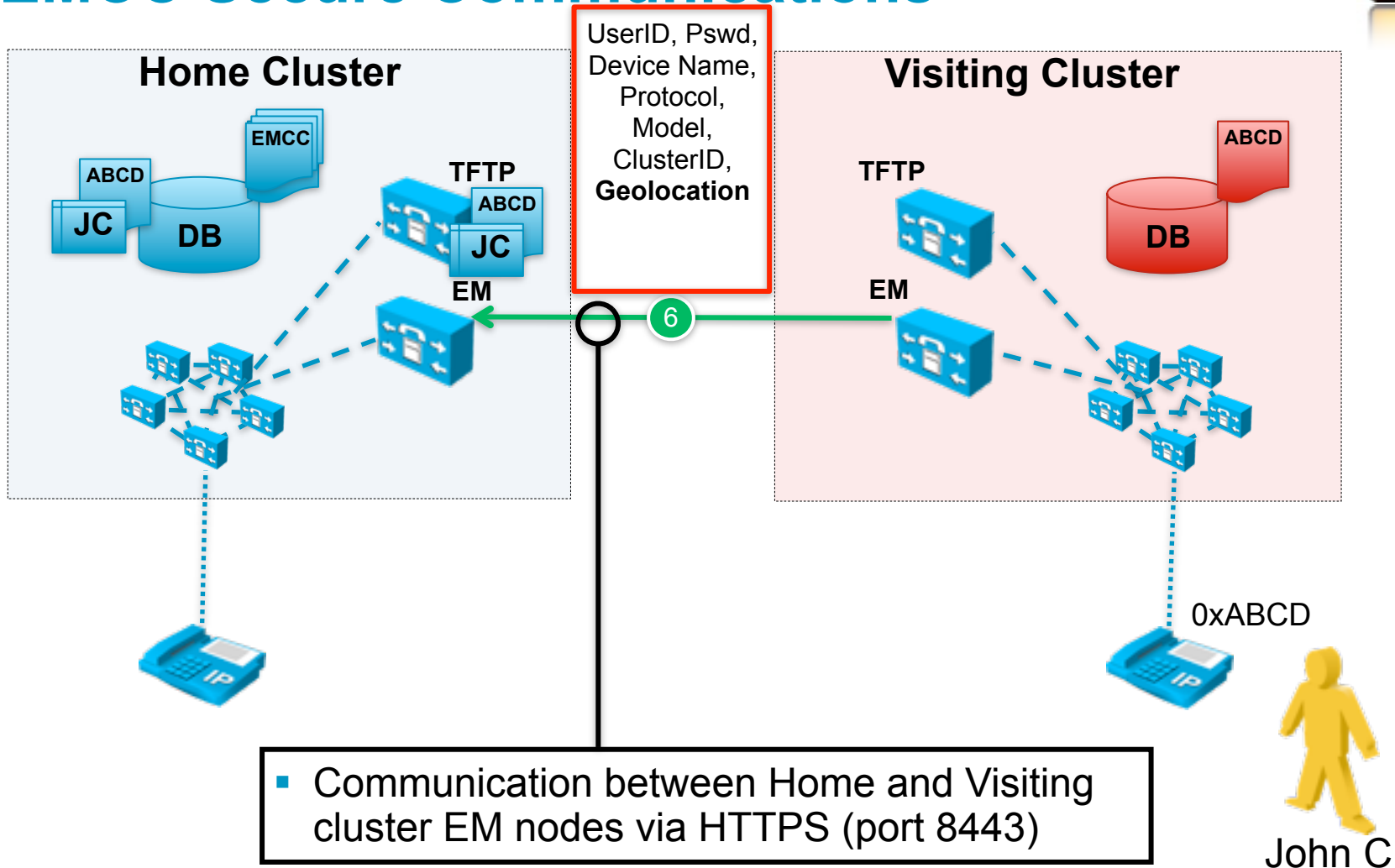
Security By Default (SBD) & Trust Verification Service (TVS)



- Automatic phone security features
 - Signing of phone configuration files
 - Phone configuration file encryption
 - HTTPS with Tomcat and other Web services (Midlets)
- Trust Verification Service (TVS) runs on each CUCM server and authenticates certificates on behalf of the phone (ITL File)
- Instead of downloading all the trusted certificates, phones need only to trust TVS (TVS will validate HC certs for Visiting phone)
- *For more details, UC 8.0 System Security Feature Update (Monday) or see Brad Ramsley's CUCM 8.0 Security Update, 2009-11-02:*
<http://vsearch.cisco.com/?auid=17161>



EMCC Secure Communications



EMCC Security

Change Credential phone service



- Allow user to change PIN from the phone
- Invoked via 2 methods:
 - 1) “User must change at next login” setting
 - 2) Configure as a separate service
Set Secure-Service URL – <https://server:8443/changecredential/ChangeCredentialServlet?device=#DEVICENAME#>
- No additional configuration needed to use for EM
 - If EM service configured for HTTP, uses HTTP (yes, PIN change can be seen)
 - If EM service configured for HTTPS, uses HTTPS

EMCC Security

Change Credential At EM Login



EMCC



EMCC Design Considerations

- Control total number of EMCC logins via BAT – number of devices inserted.
- Users must be unique across all clusters. If DirSync pulling in common users for multiple clusters, must apply some type of filtering .
- If H323/SIP gateways are only setup for G711, but EMCC phones coming across now as G729 – must add multiple codec capability to dial-peers (or use transcoders).
- *Calling* number for Emergency Calls leaving Visiting gateways may potentially have a Home cluster DID.
- Calls sent across the EMCC SIP Trunk will have gone through digit manipulation. Called number may require manipulation to match Visiting cluster route patterns.
- EMCC Performance testing is underway ...

Other Supported Features in EMCC

- Consider the delays between the clusters in combination with the features you plan to use. Not all applications/features have been tested with delays – User Experience may vary.
- CTI control of vPhone
 - In CUCM 7.x and earlier, CTI control is based on static assignment of devices to a user
 - In CUCM 8.x and later, CTI device assignment can be dynamic. Device Profile login triggers CTI to control device
- EMCC Supports Non-Secure clusters and Mixed Mode clusters.
 - *Note: All participating EMCC clusters must be of the same mode.*
 - Only NON-SECURE phones supported in this release.
- Firmware version is not sent in xml config from home cluster
 - Prevents phones from having to download new firmware images
- HC Locales supported if VC has locale files in TFTP server.

Key Takeaways

The Key Takeaways of this presentation are:

- Understand the basic operation of EMCC
- Understand EMCC-related configuration
- Know limitations and supported features
- Able to describe EMCC call flows
- Understand EMCC Emergency calling

Additional Resources

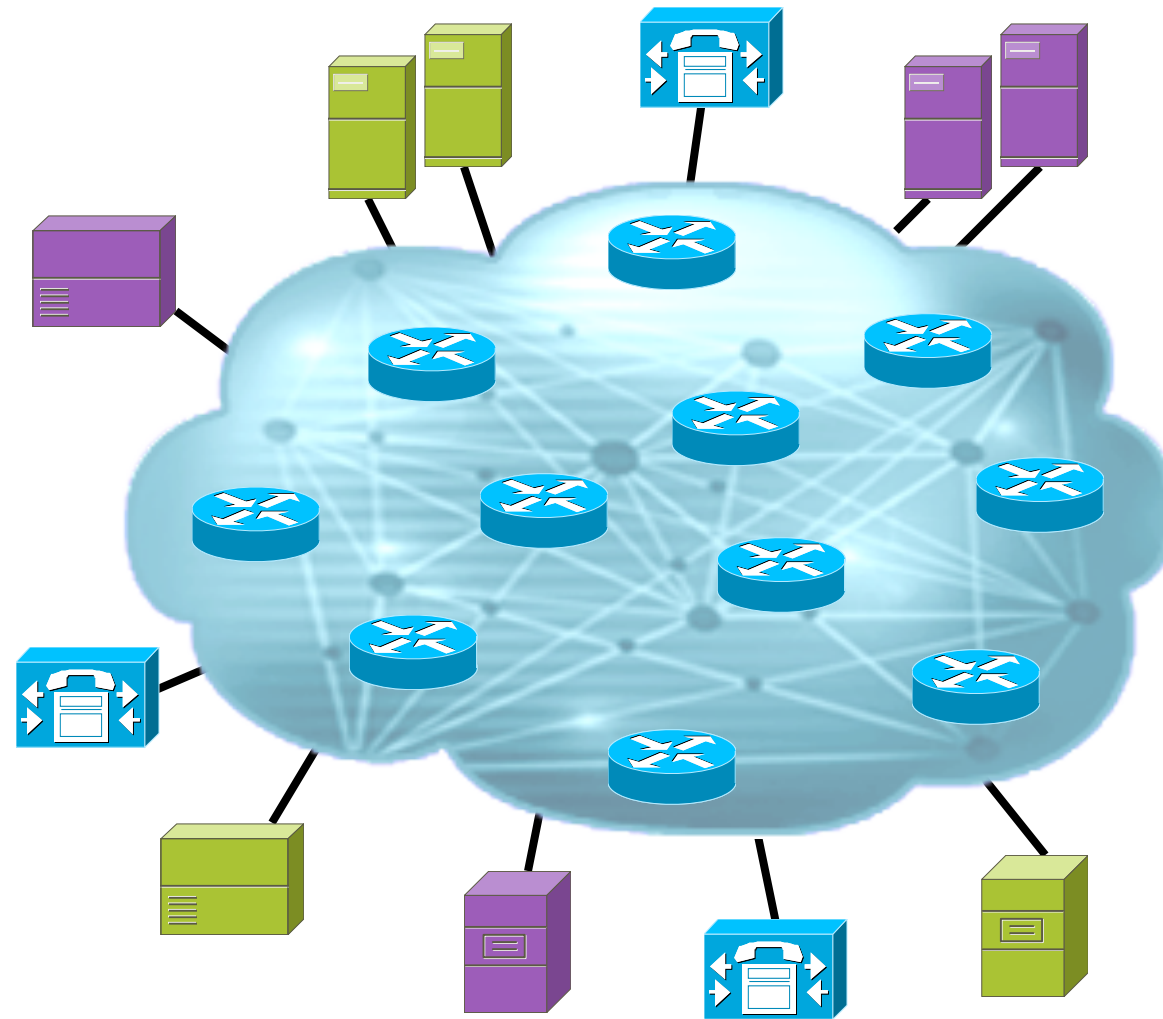
- You can find additional information about the topics and products covered in this session at the following links:
 - [CUCM Features and Services Guide for Release 8.0\(1\)](#)
 - [CUCM 8.0\(1\) Release Notes](#)
 - [8.x UC SRND – CM Applications chapter \(released April 2010\)](#)

SAF - CCD

- Introduction
- Call Control Discovery (CCD)
 - Scope and Objectives
 - Features and Functionality
 - Configuration Examples
- Service Advertisement Framework (SAF)
 - The SAF Network
 - The SAF Client-Network Interface
- Conclusions

Introduction

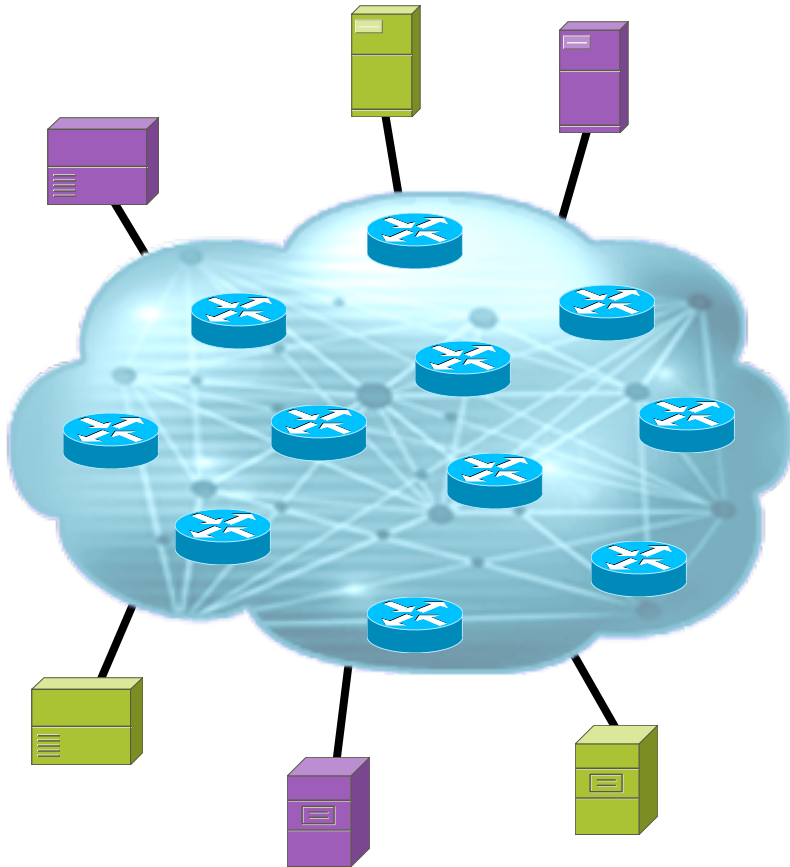
Problem Statement and Goals



- Advanced network services and applications are often deployed as **overlays**
- Can the network leverage **dynamic** properties of routing to help these services communicate?
- Goals:
 - Provide a **network foundation** for service awareness
 - Enable **applications**

Introduction

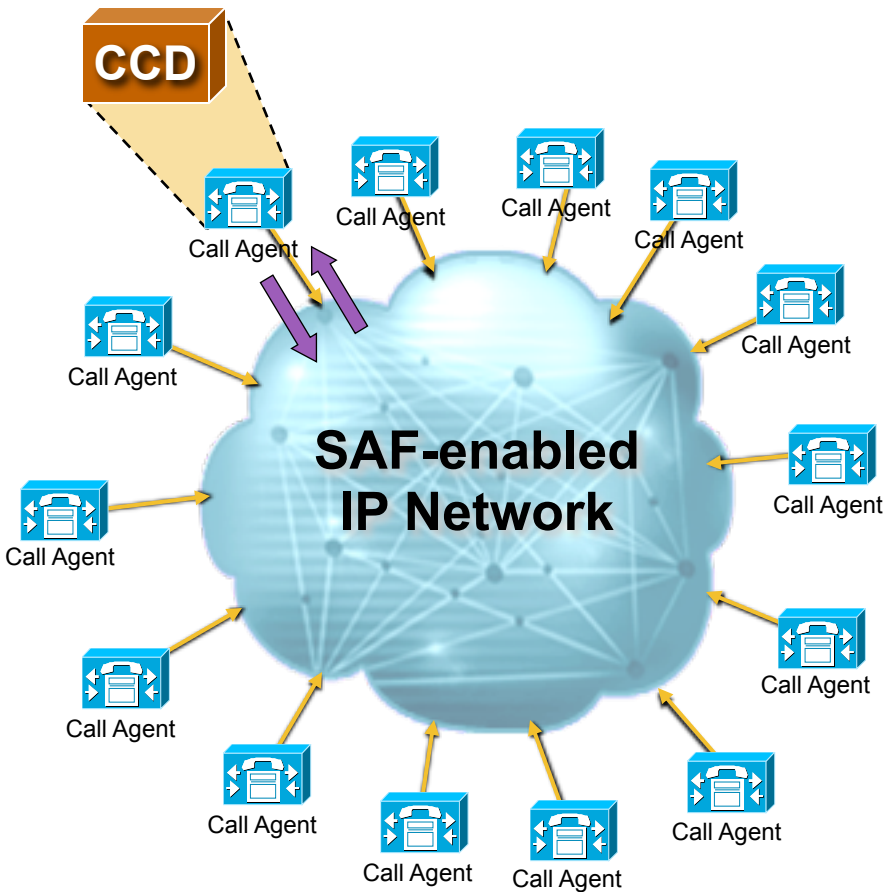
The Service Advertisement Framework (SAF) Vision



- A network-based, scalable, bandwidth-efficient, real-time approach to **service advertisement and discovery**
- Is based on EIGRP technology, but is **independent** of IP routing protocol (*works with OSPF, BGP,...*)
- Supports “**dark nets**” (non-SAF nodes) for phased roll-outs and heterogeneous deployments
- Will allow administrators to control **scope** of each service through domains, filtering, VRF's, ...

Introduction

Call Control Discovery (CCD): a SAF Service



- Call agents 'discover' each other through the SAF network by:
 - Advertising their reachability information along with the DN ranges they own
 - Requesting to learn about other call agents in the network
- Call agents **dynamically** route calls to remote destinations based on received advertisements

Introduction

SAF Terms and Definitions



SAF Client: any application wishing to advertise a service to the network or request a service from the network or both



SAF Forwarder: router feature – provides relationship between client and framework, stores service information and propagates it to other forwarders



Service: any information that a SAF client wishes to advertise and “consume” (e.g., dial plans for CCD)



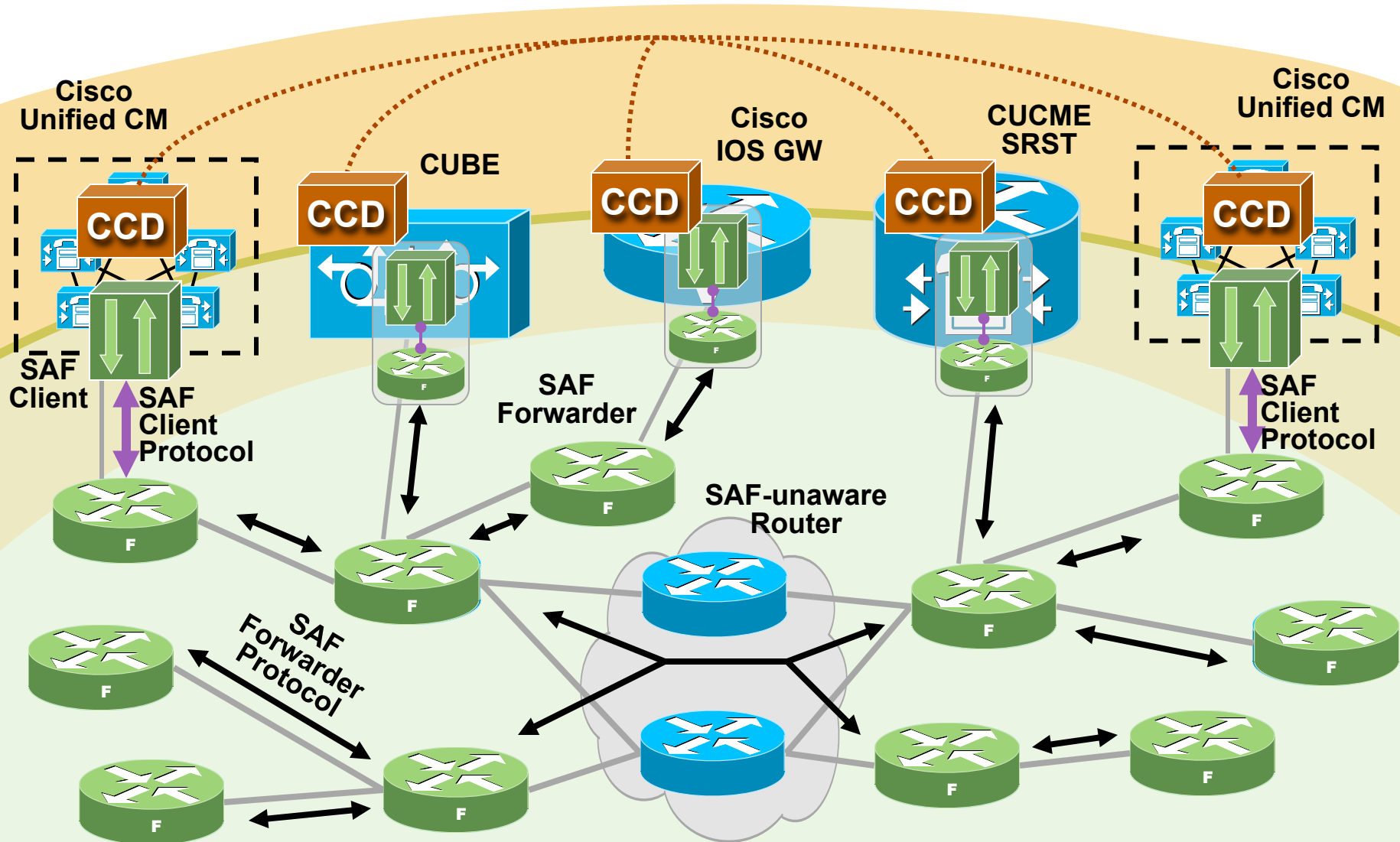
SAF Advertisement: carries service information, consists of SAF Header and Service Data



Non-SAF Node: any router that does not run the SAF protocols

Introduction

SAF Architecture



Call Control Discovery (CCD)

Scope and Objectives

Features and Functionality

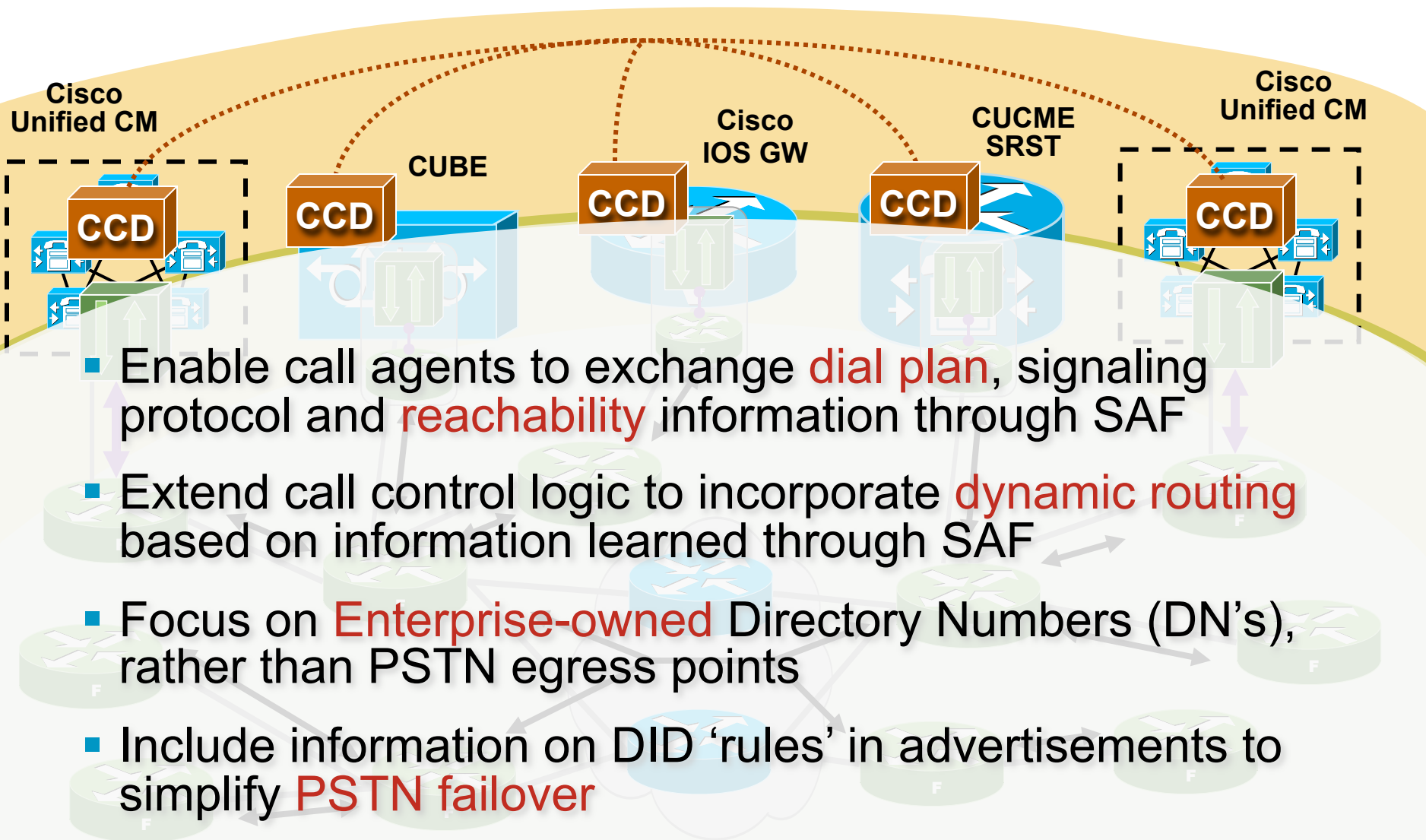
Configuration Examples (Unified CM and IOS)

Integration with “Static Routing”



Call Control Discovery (CCD)

Scope and Objectives



Call Control Discovery (CCD)

Advertising DN Ranges

Service Advertisement

IP address: 10.1.1.1

Protocol: SIP

DN Patterns:

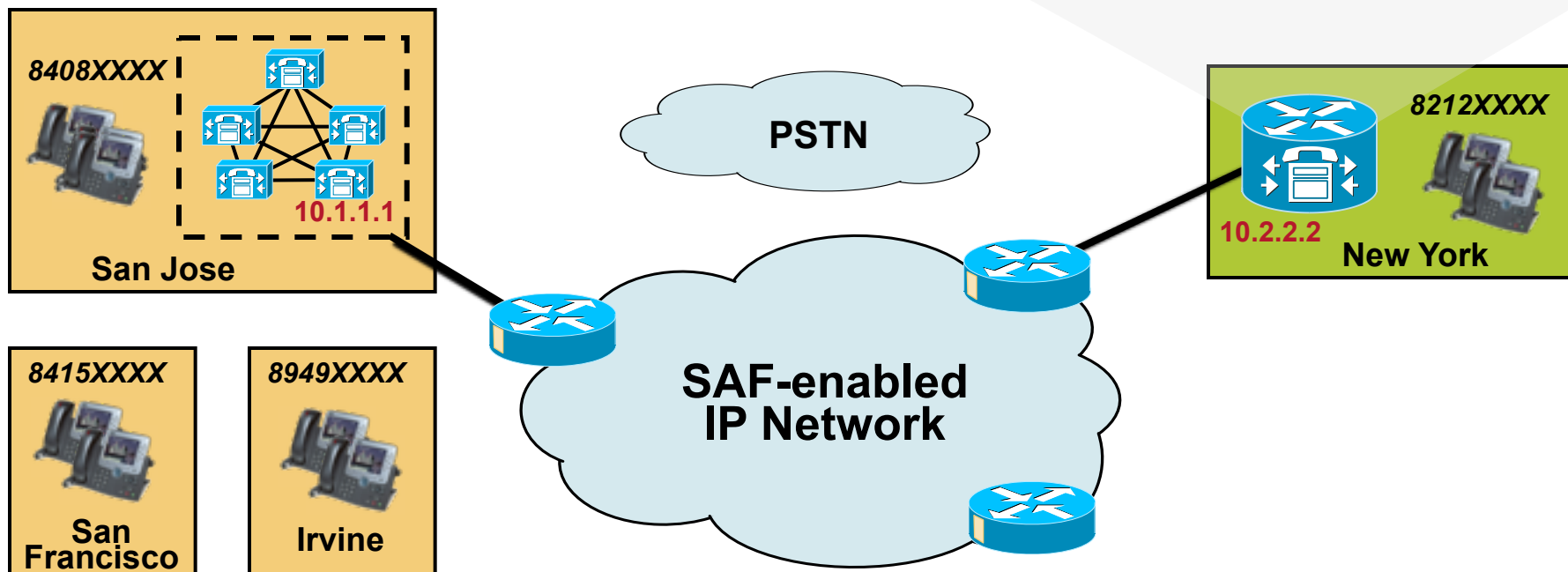
8408XXXX [4:+1408555],

8415XXXX [4:+1415777],

8949XXXX [4:+1949222]

New York CME Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8408XXXX	4:+1408555	10.1.1.1	SIP
8415XXXX	4:+1415777	10.1.1.1	SIP
8949XXXX	4:+1949222	10.1.1.1	SIP



Call Control Discovery (CCD)

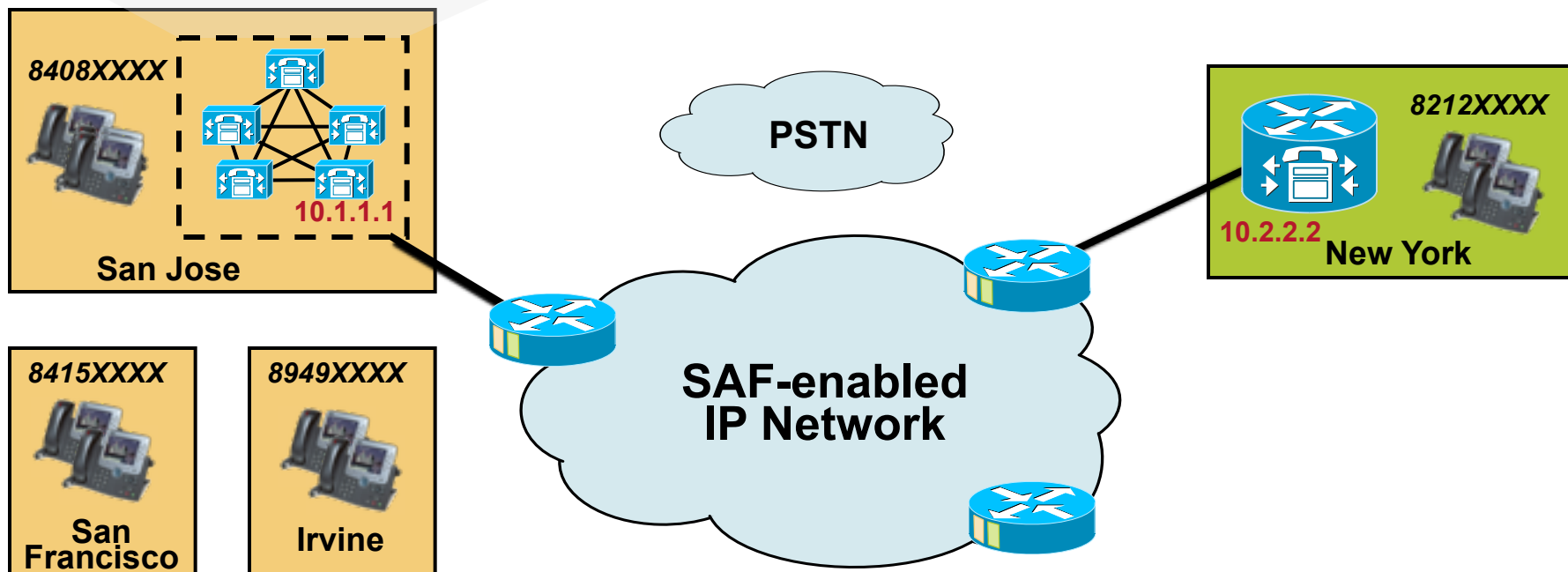
Learning DN Ranges

San Jose CUCM Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8212XXXX	4:+1212444	10.2.2.2	SIP

Service Advertisement

IP address: 10.2.2.2
Protocol: SIP
DN Patterns:
8212XXXX [4:+1212444]



Call Control Discovery (CCD)

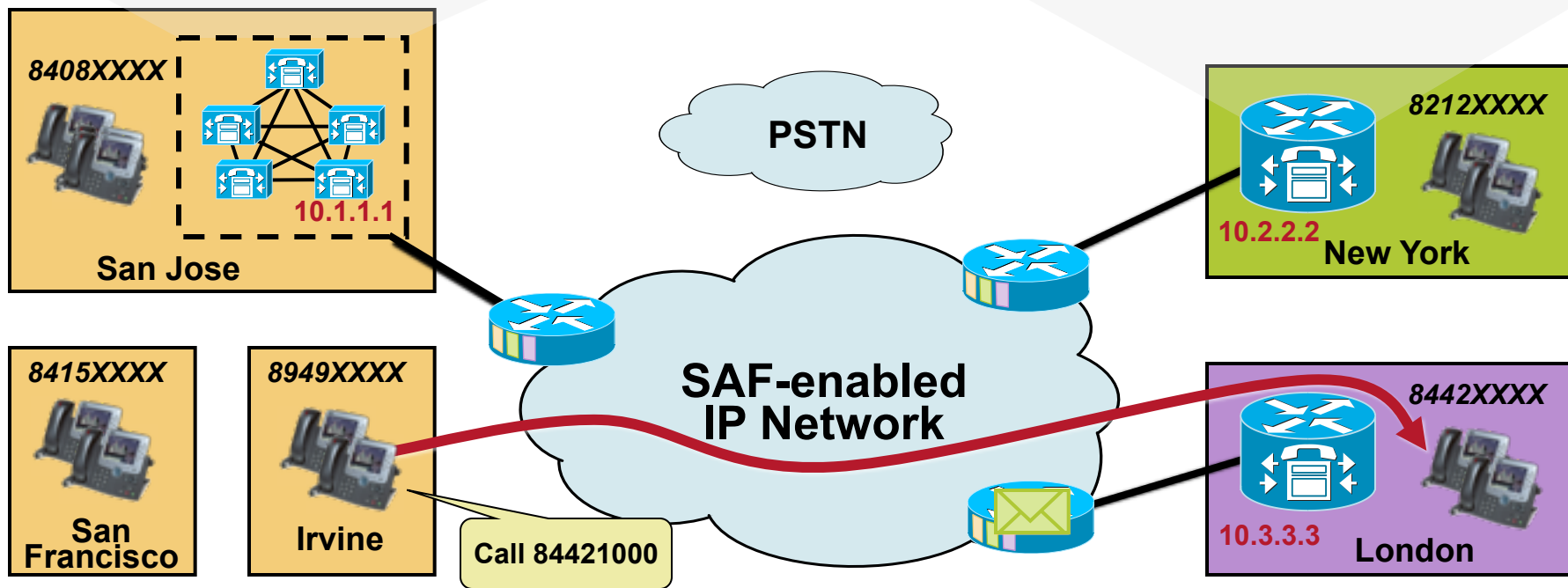
Dynamic Routing

San Jose CUCM Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8212XXXX	4:+1212444	10.2.2.2	SIP
8442XXXX	4:+442077111	10.3.3.3	H.323

New York CME Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8408XXXX	4:+1408555	10.1.1.1	SIP
8415XXXX	4:+1415777	10.1.1.1	SIP
8949XXXX	4:+1949222	10.1.1.1	SIP
8442XXXX	4:+442077111	10.3.3.3	H.323



Call Control Discovery (CCD)

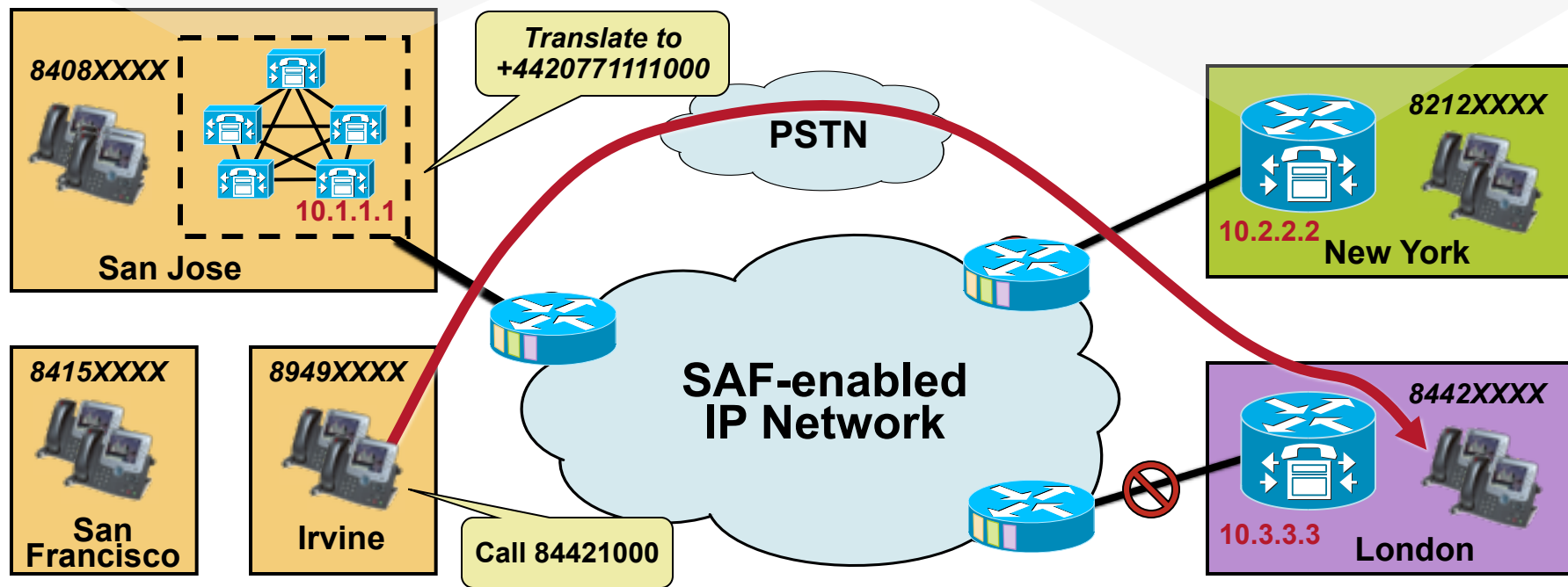
Automatic PSTN Failover

San Jose CUCM Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8212XXXX	4:+1212444	10.2.2.2	SIP
8442XXXX	4:+442077111	10.3.3.3	H.323

New York CME Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8408XXXX	4:+1408555	10.1.1.1	SIP
8415XXXX	4:+1415777	10.1.1.1	SIP
8949XXXX	4:+1949222	10.1.1.1	SIP
8442XXXX	4:+442077111	10.3.3.3	H.323



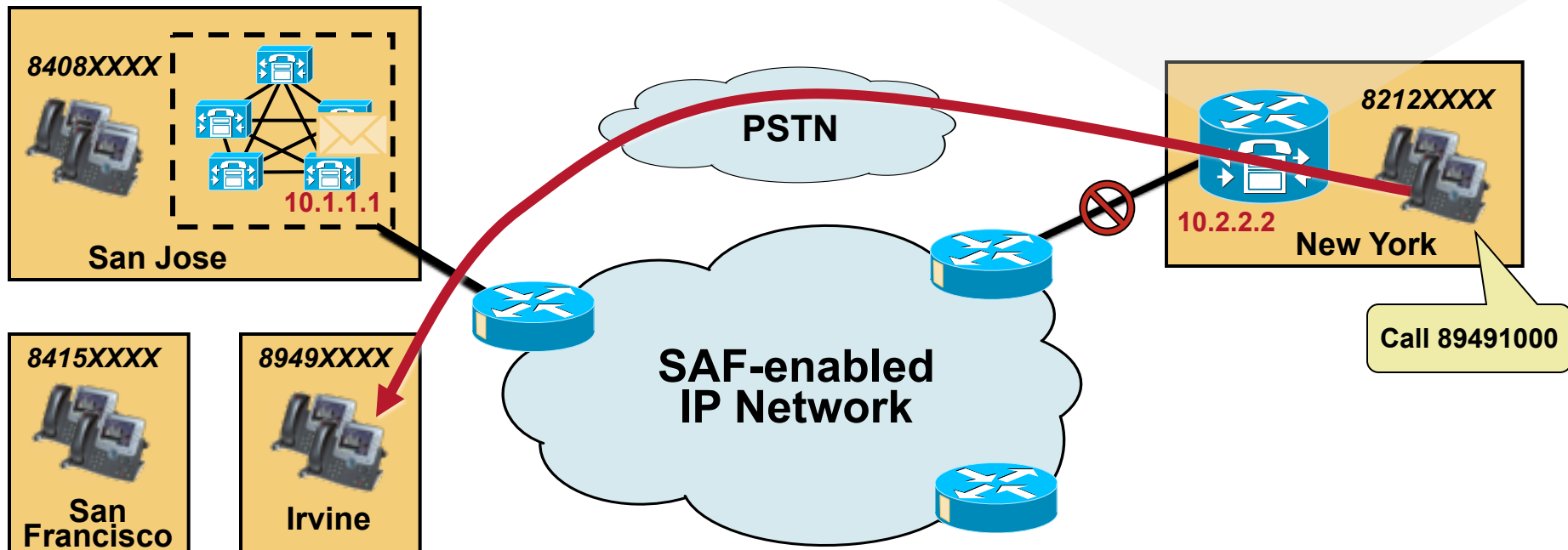
Call Control Discovery (CCD)

Automatic Rerouting for SRST

- SRST subscribes to CCD service but does not publish any patterns
- During WAN failures, SRST uses learned patterns to transparently re-route calls over the PSTN

New York SRST Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8408XXXX	4:+1408555	10.1.1.1	SIP
8415XXXX	4:+1415777	10.1.1.1	SIP
8949XXXX	4:+1949222	10.1.1.1	SIP



Call Control Discovery (CCD)

3rd Party IP PBX Integration

San Jose CUCM Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8442XXXX	4:+442077111	10.3.3.3	H.323
8312XXXX	4:+1312888	10.4.4.4	SIP

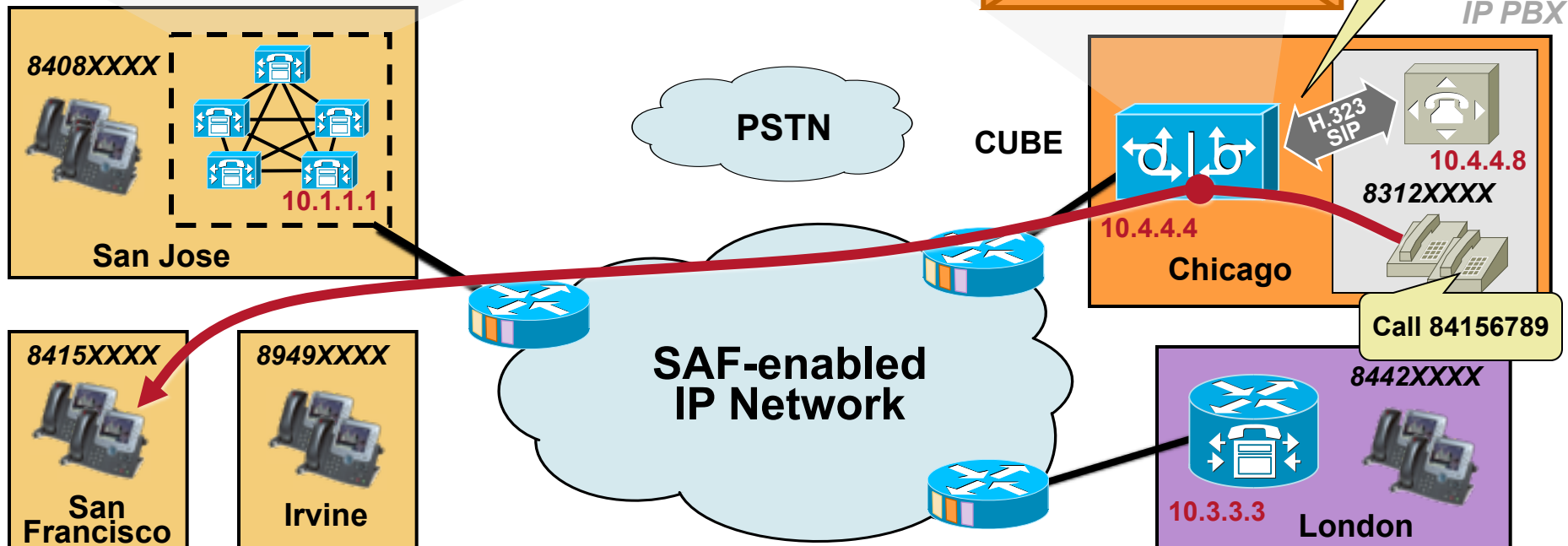
Chicago CUBE Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8408XXXX	4:+1408555	10.1.1.1	SIP
8415XXXX	4:+1415777	10.1.1.1	SIP
8949XXXX	4:+1949222	10.1.1.1	SIP
8442XXXX	4:+442077111	10.3.3.3	H.323

IP address: 10.4.4.4
Protocol: SIP
DN Patterns:
8312XXXX [4:+1312888]

Static dial peer for destination 8312XXXX

3rd Party IP PBX



Call Control Discovery (CCD)

3rd Party TDM PBX Integration

San Jose CUCM Routing Table

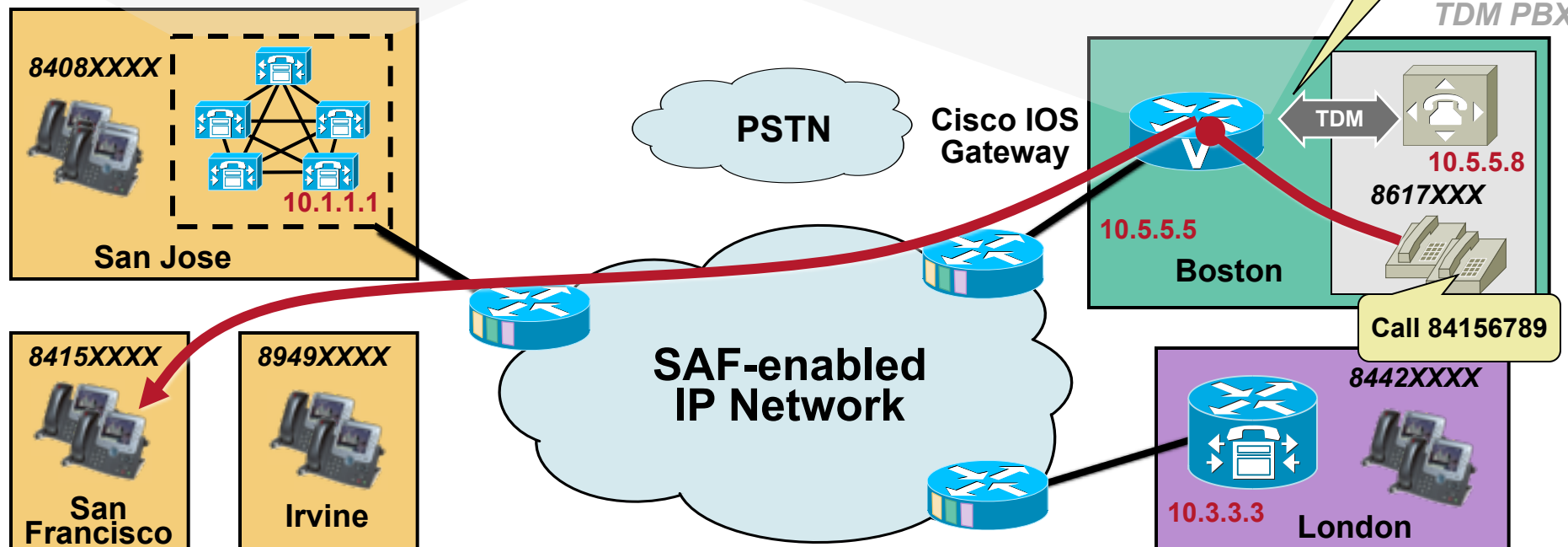
DN Pattern	"to DID" rule	IP address	Protocol
8442XXXX	4:+442077111	10.3.3.3	H.323
8617XXXX	4:+1617999	10.5.5.5	SIP

Boston Gateway Routing Table

DN Pattern	"to DID" rule	IP address	Protocol
8408XXXX	4:+1408555	10.1.1.1	SIP
8415XXXX	4:+1415777	10.1.1.1	SIP
8949XXXX	4:+1949222	10.1.1.1	SIP
8442XXXX	4:+442077111	10.3.3.3	H.323

Static dial peer
for destination
8617XXXX

3rd Party
TDM PBX



Call Control Discovery (CCD)






Cisco Unified CM Support Details


- Starting with release 8.0(1), ability to advertise and/or subscribe to the CCD service
- Learned DN patterns dynamically inserted in a specified partition
- Transparent PSTN failover when destination is unreachable
- Scalability:
 - Up to **2,000** advertised DN patterns per cluster
 - Up to **20,000** learned DN patterns per cluster
- DN patterns must be unique (*if duplicates, warning can be issued*)
- Ability to purge and block unwanted patterns (*e.g., from rogue or mis-configured call agents*)
- Extensive troubleshooting support through RTMT and traces

Call Control Discovery (CCD)

Unified CM Configuration – SIP Trunk

Trunk Configuration Related Links: [B](#)

 Save  Delete  Reset  Apply Config  Add New

Status
 Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	Call Control Discovery
Device Name*	SAFSIPCT
Description	

SIP Information

MTP Preferred Originating Codec*	711ulaw
Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	test1
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

Call Control Discovery (CCD)

Unified CM Configuration – Hosted DN's

Hosted DN Group Configuration

Save Delete Copy Add New

Status
Update successful

Hosted DN Group Info

Name* HDNgrp1

Description

PSTN Failover Strip Digits 4

PSTN Failover Prepend Digits +1972555

☐ Use HostedDN as PSTN Failover

Save Delete Copy Add New

Applies the same "toDID" rules to all DN Patterns in this group

Used to advertise full E.164 ranges instead of internal numbers + "toDID" rules

Hosted DN Pattern Configuration

Save Delete Copy Add New

Status
Update successful

Hosted DN Patterns Info

Hosted Pattern* +1408555XXXX

Description

Hosted DN Group* HDNgrp1

PSTN Failover Strip Digits 0

PSTN Failover Prepend Digits 888





☒ Use HostedDN as PSTN Failover


Save Delete Copy Add New

Call Control Discovery (CCD)



Unified CM Configuration – Hosted DN's (2)

Find and List Hosted DN Patterns

 Add New  Select All  Clear All  Delete Selected

Status
 3 records found

Hosted DN Pattern (1 - 3 of 3) Rows

Find Hosted DN Pattern where begins with  

<input type="checkbox"/>	Hosted Pattern ^	Description	Hosted DN Group
<input type="checkbox"/>	+9997XXX		HDNGrp2
<input type="checkbox"/>	7XXX		HDNgrp1
<input type="checkbox"/>	9727XXX		HDNgrp1

- Hosted DN patterns to be advertised are configured by the administrator
- Allows flexibility in designing on-net dial plan and choosing which DN ranges to advertise to other call agents

Call Control Discovery (CCD)

Unified CM Configuration – Advertising Service

The screenshot shows the 'CCD Advertising Service Configuration' page. At the top is a navigation bar with menus: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below this is a header bar with the title 'CCD Advertising Service Configuration' and a 'Related Links: Find and List C' button. A toolbar contains icons for Save, Delete, Copy, Reset, and Add New. The 'Status' section shows an information icon and the text 'Add successful'. The 'CCD Advertising Service Info' section contains the following fields: 'Name*' with the value 'CCD Advertising Service 2', 'Description' (empty), 'SAF SIP Trunk' with a dropdown menu showing 'SAFSIPICT', 'SAF H323 Trunk' with a dropdown menu showing '< None >', and 'HostedDN Group*' with a dropdown menu showing 'HDNGrp2'. At the bottom, there is a checkbox labeled 'Activated Feature' which is checked.




- Each HostedDN Group can be associated with only one CCD Advertising Service
- SAF Trunks can be re-used by different CCD Advertising Services and CCD Requesting Services
- The SAF trunks' Unified CM groups determine on which nodes this service runs and which IP addresses are advertised through SAF

Call Control Discovery (CCD)

Unified CM Configuration – Requesting Service

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

CCD Requesting Service Configuration

 Save  Delete  Reset

CCD Requesting Service Info

Name*

Description

Route Partition

Learned Pattern Prefix

PSTN Prefix

Available SAF Trunks

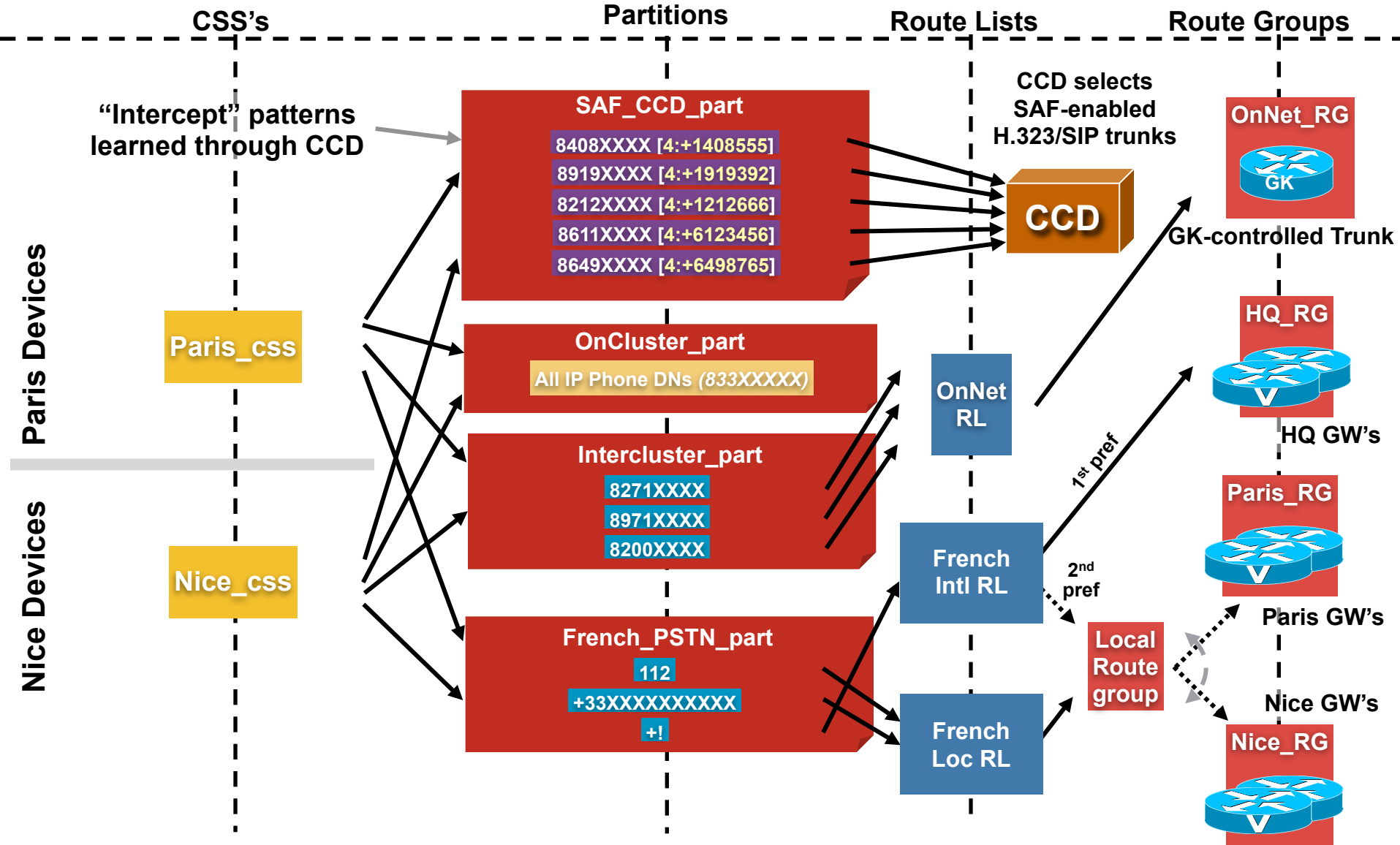
Selected SAF Trunks

☒ Activated Feature

Selected SAF trunks are used to originate outbound calls towards learned destinations

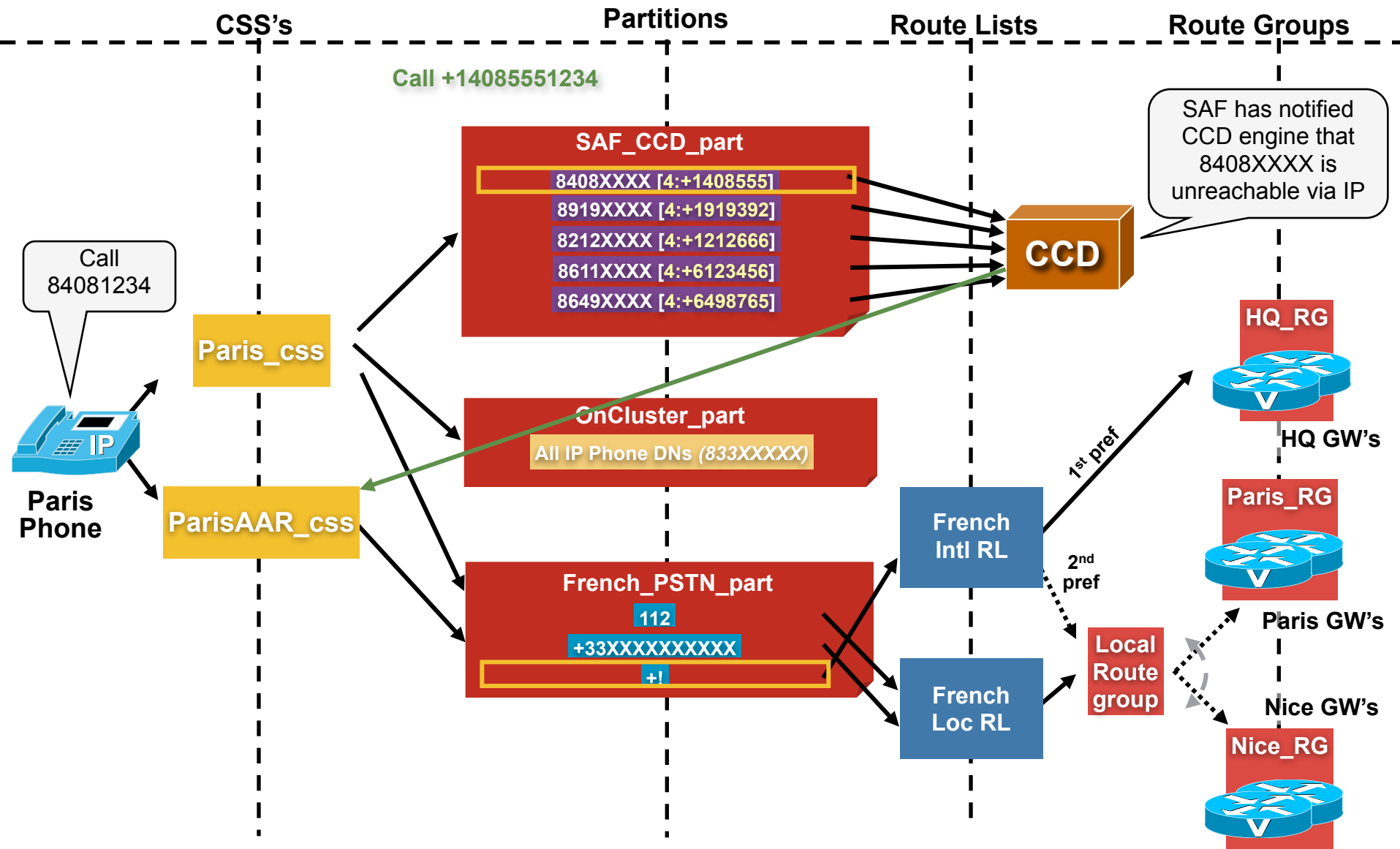
Call Control Discovery (CCD)

Integration with "Static Routing"



Call Control Discovery (CCD)

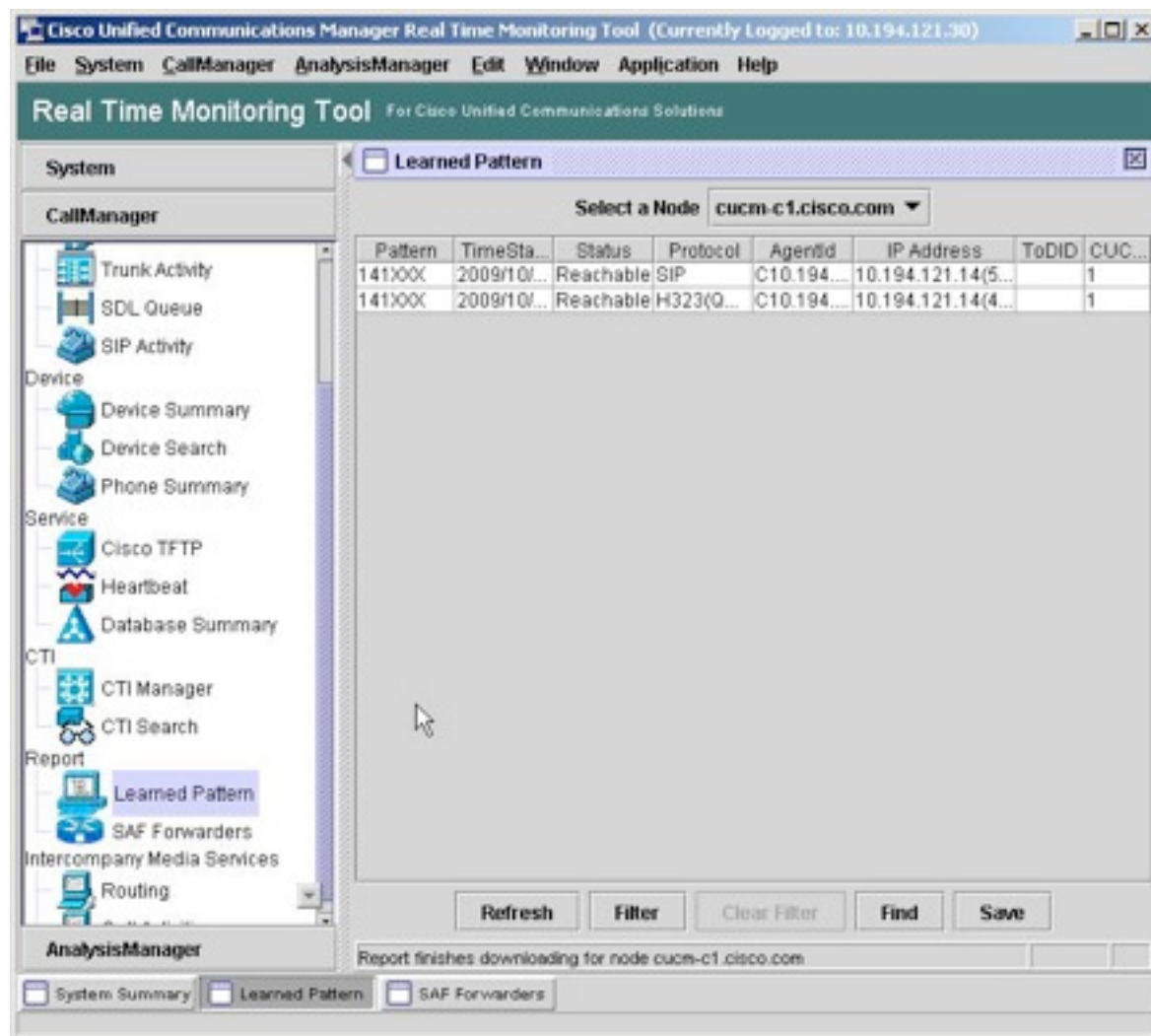
Integration with “Static Routing” – PSTN Failover



Call Control Discovery (CCD)

Monitoring and Troubleshooting for Unified CM

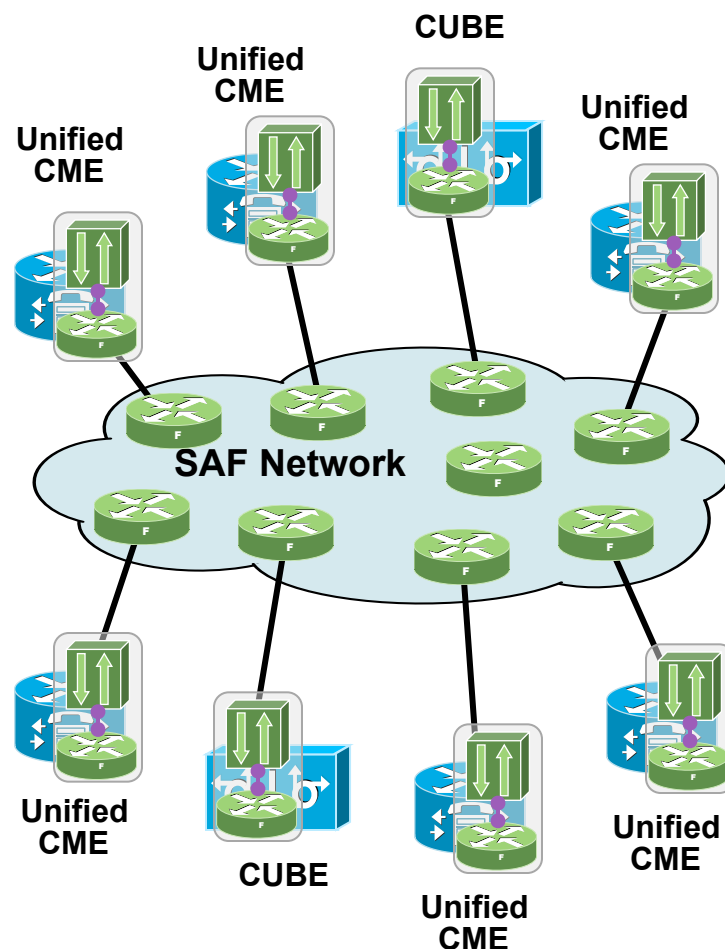
- RTMT is used to monitor learned routes and configured SAF Forwarders
- SAF/CCD tracing is included as part of the Unified CM SDI and SDL traces



Call Control Discovery (CCD)

Unified CME, SRST, CUBE, Gateway Support Details

- Starting with Cisco IOS 15.0(1)M, Unified CME, CUBE and IOS Gateways can advertise and/or subscribe to the CCD service
- Listen-only mode for SRST
- Transparent PSTN failover when destination is unreachable
- Scalability:
 - Up to **125** advertised DN patterns per CME/CUBE
 - Up to **6,000** learned DN patterns per CME/CUBE/SRST (*platform-dependant*)



Call Control Discovery (CCD)

Unified CME or CUBE Configuration Example

```
router eigrp SAF-fwdr
 service-family ipv4 autonomous-system 1
 sf-interface Ethernet0/0
 topology base
```

Co-resident SAF Forwarder

```
voice service saf
```

```
 profile trunk-route 1
   session protocol int Eth0/0 sip transport tcp port 5060
```

Trunk route: signaling IP address, port, protocol

```
 profile dn-block 1
   pattern 1 extension 5xxx
   pattern 2 global 1408555xxx
```

DN blocks: patterns to be advertised and “to DID” transformation rules

```
 profile dn-block 2 alias 14085258 strip 4
   pattern 3 extension 8123xxx
```

```
 profile callcontrol 2
   dn-service
     dn-block 1
     dn-block 2
     trunk-route 1
     site-code 8333
   exit dn-service
 exit-profile
```

CCD instance: integrates DN blocks and trunk route

```
 channel 1 vrouter SAF-fwdr asystem 1
   publish callcontrol 2
   subscribe callcontrol wilddcarded
```

SAF client: publish and/or subscribe to services

```
 dial-peer voice 100 voip
   destination-pattern .T
   session target saf
```

Enable call agent to look up routes learned through SAF

Case Study

Service Advertisement Framework (SAF)

The SAF Network

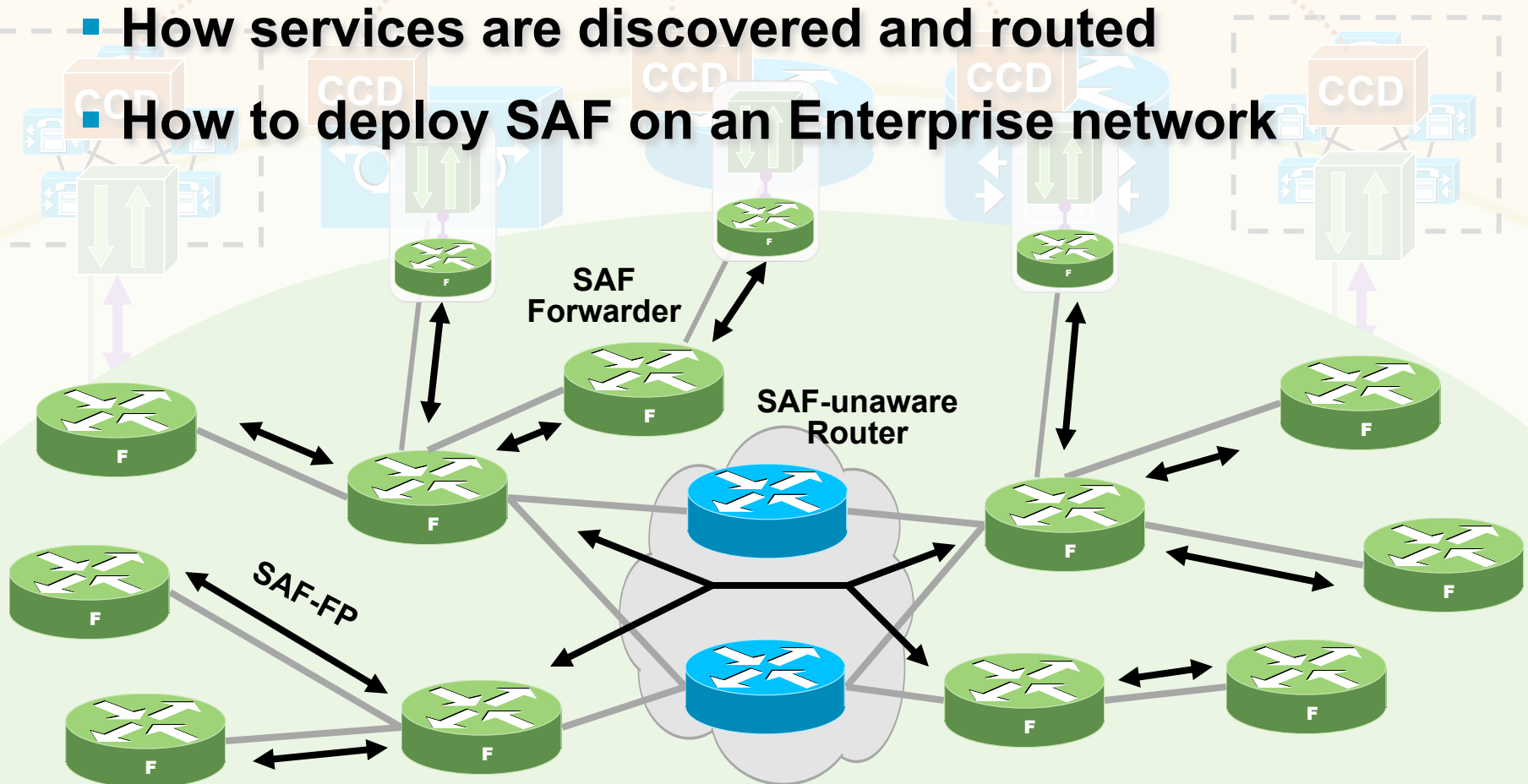
The SAF Client-Network Interface



The SAF Network

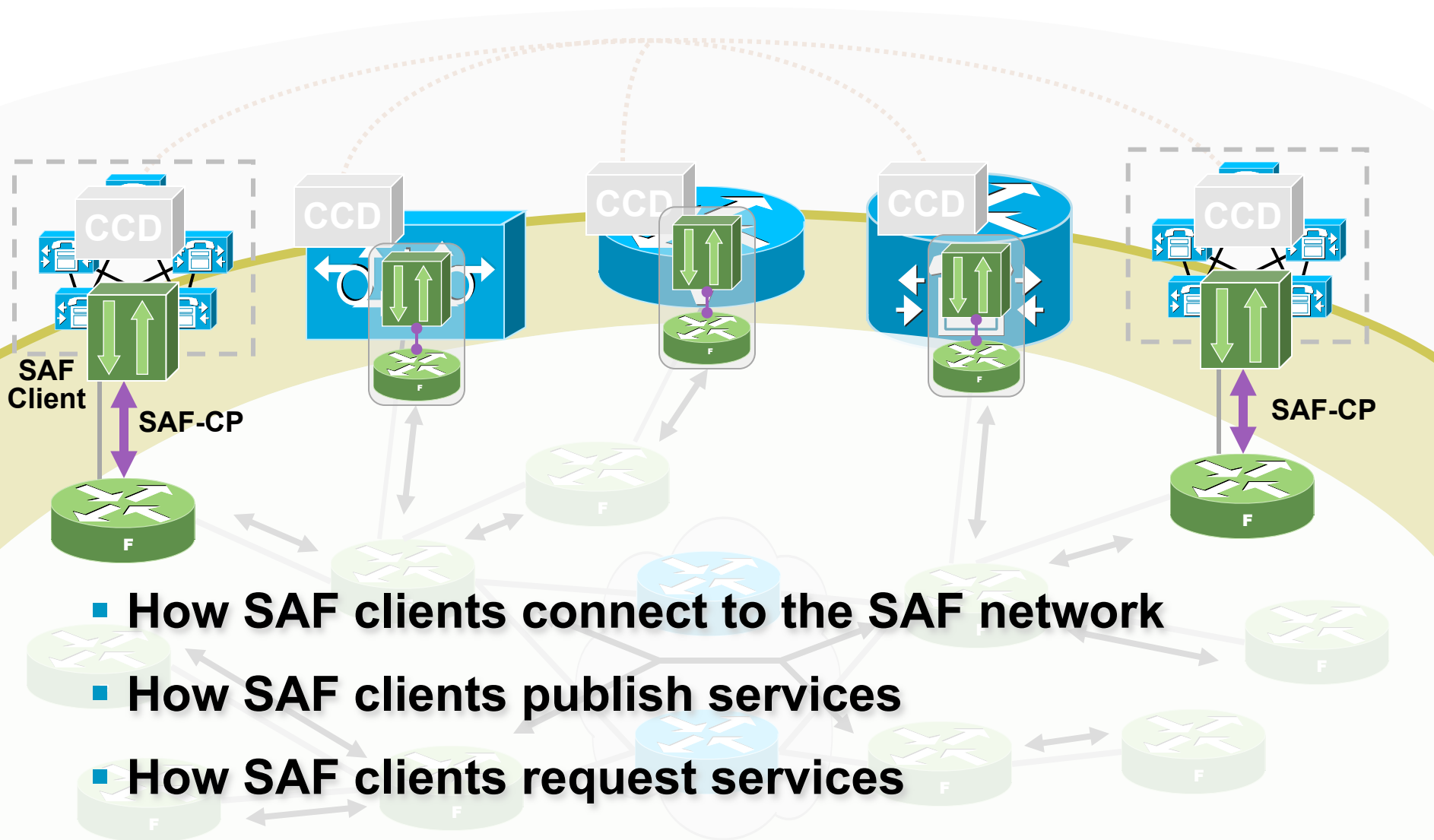
Agenda

- What is a SAF Advertisement
- How services are discovered and routed
- How to deploy SAF on an Enterprise network



The SAF Client-Network Interface

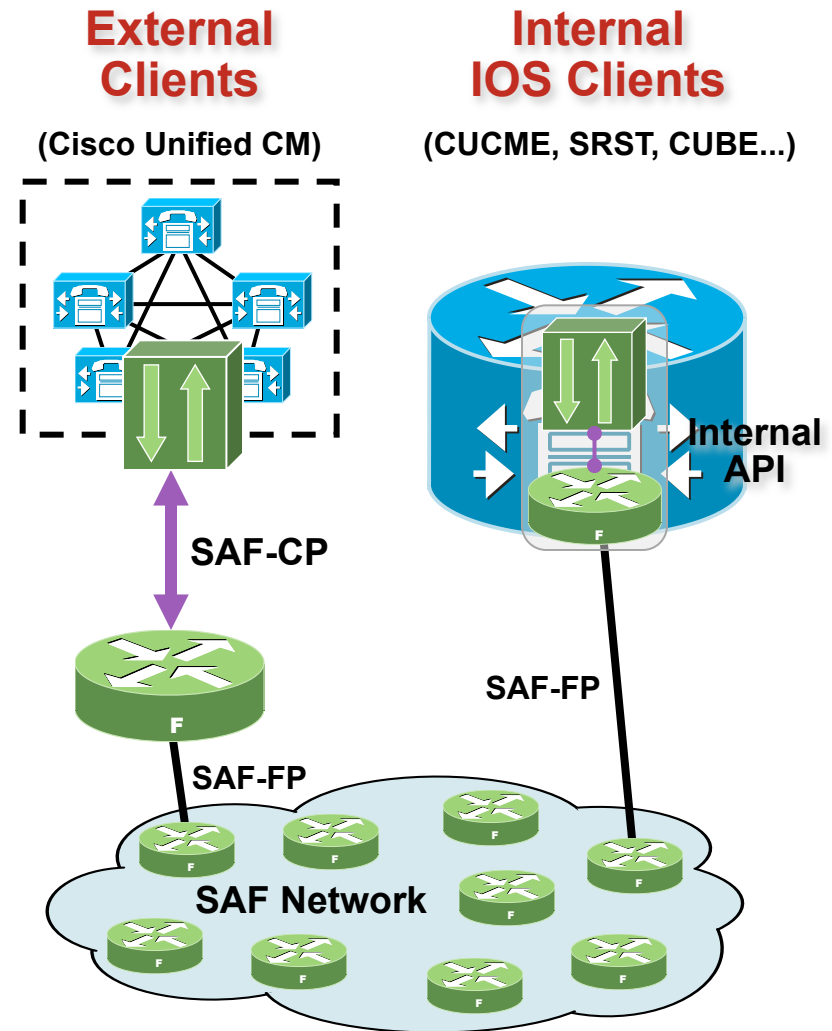
Agenda



The SAF Client-Network Interface

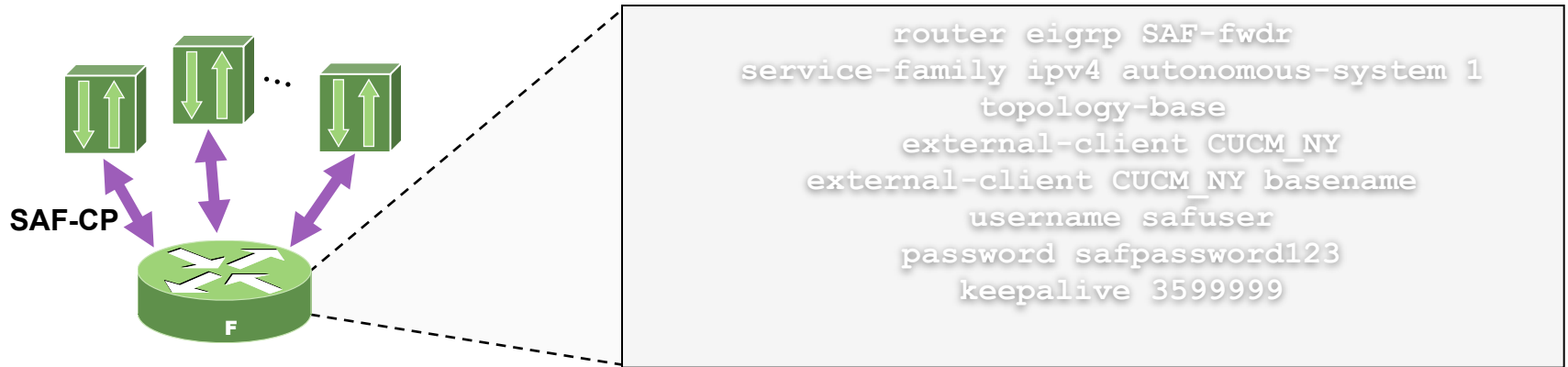
SAF Client Types

- SAF clients perform three functions:
 - Register** to the network
 - Publish** services
 - Subscribe** to services
- External clients communicate to a SAF forwarder via the SAF Client Protocol (SAF-CP)
- Internal Cisco IOS clients communicate to a co-located SAF forwarder via internal API



The SAF Client-Network Interface

Connecting External Clients to a Forwarder



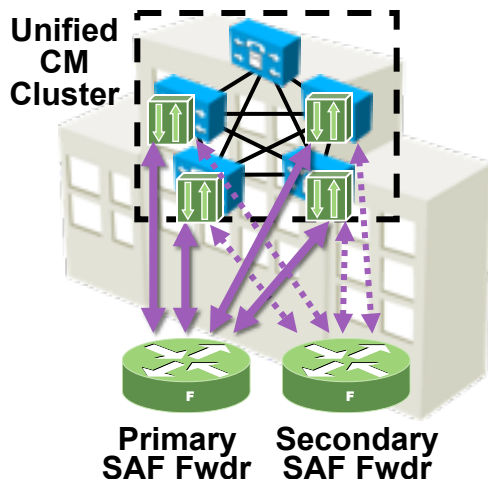
- Configure credentials for client authentication
- Multiple clients can share same credentials with 'basename' keyword (*e.g., nodes of the same Unified CM cluster*)
- Up to 50 clients can connect to the same forwarder in the current release

The SAF Client-Network Interface

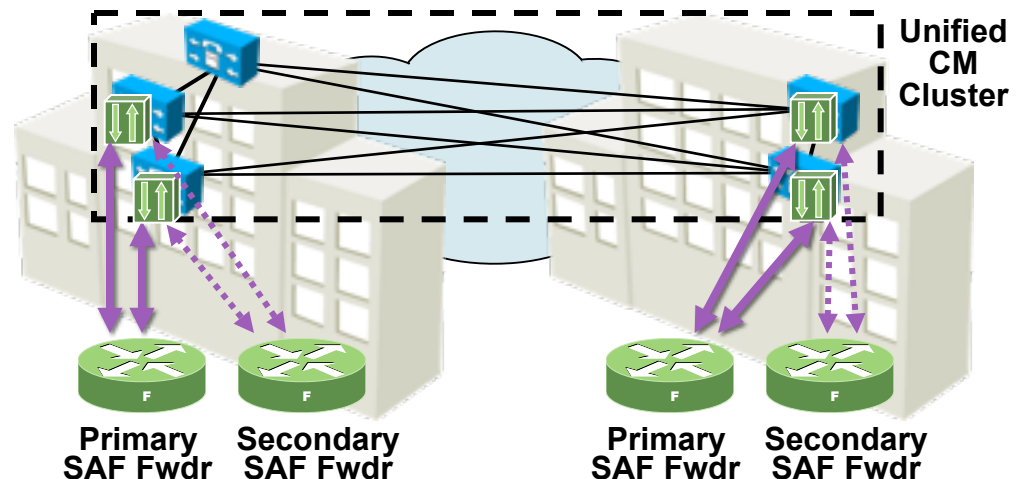
Cisco Unified CM as a SAF client

- Supports SAF client authentication
- Process runs on every subscriber node in the cluster
- Two configuration modes:
 - Basic** – all nodes use same primary/secondary SAF forwarders
 - Advanced** – multiple sets of forwarders (for CoW deployments)

Single-site Cluster



Clustering over the WAN



Case Study

Conclusions

Recap of Key Concepts

- SAF is a generic framework for service discovery
- Three main components:
 - The **network** – propagate service advertisements
 - The **client-network interface** – publish and subscribe to services
 - The **services** – e.g., Call Control Discovery
- Key differentiating aspects:
 - Scalability, bandwidth efficiency, fast convergence
 - “In the network” vs. overlay solution
 - “Service routing” independent of IP routing
 - Push-based model allows use for real-time applications
 - Modular approach to maximize re-use

Conclusions

Benefits of Call Control Discovery

- **Reduce deployment time, realize quicker ROI**

- Dial plan configuration complexity reduced from N^2 to N

- Allows optimal dial plan to be implemented quickly

- (i.e., on-net numbering plan with automatic PSTN failover)*

- **Reduce ongoing operational costs**

- Complexity of adding/removing/changing a site drastically reduced

- No need to purchase, maintain and configure dedicated gatekeepers

- Reduced reliance on static back-up configuration

- **Improve business continuity**

- Increased availability even during partial network failure thanks to dynamic awareness

- Implementable and maintainable mechanism for automatic PSTN rerouting

- Fast rerouting during failures

Cisco Unified IP Phone Portfolio At-A-Glance...

9900 Series



Advanced Collaborative Media Endpoints

- Interactive video, HD voice, large color displays
- Wide array of endpoint applications
- USB connectivity, Wi-Fi and Gigabit Ethernet
- Energy-friendly

8900 Series



Advanced Professional Media Endpoints

- HD voice, large color displays
- Wide array of endpoint applications
- USB connectivity
- Energy-friendly

7900 Series



Advanced Business Endpoints

- Desktop, Conference Room and Wireless endpoints
- HD voice, Gigabit Ethernet
- Wide array of endpoint applications
- Energy-friendly

6900 Series



Business Voice Endpoints

- Traditional telephony-like User Experience
- Flexible communications: Full-duplex speakerphone
- Selected basic endpoint applications (XML)
- Energy-friendly

6900 Phone Models



6921



6941



6961



- Supports SCCP. SIP Support in 2H CY2010
- SRST 8.0 with 15.0(1)XA. No SRST 7.1 support
- Targeted markets - SMB markets with low end PBX features

- Line keys are not labeled via LCD
- 7940G like features

- Line keys can be labeled via LCD
- 7960G like features

- Line keys are paper labeled
- Similar to 7931




Cisco Unified IP Phone 8900 & 9900 Series

Overview

8961

9951

9971

			
802.3at POE	Y	Y	Y
GigE Switchport	Y	Y	Y
USB	Y	Y	Y
Bluetooth		Y	Y
Wi-Fi			Y
SDIO			Y
Video Streaming	Y	Y	Y
2-way Video		Y	Y
Display Size	5" QVGA	5" VGA	5.6" VGA Touchscreen
Lines	Multi	Multi	Multi
Key Module	1 Color VGA	2 Color VGA	3 Color VGA



Standard
(6oz/170g)



Slimline
(5oz/140g)

Reference:
7975G Handset =
7.4oz/210g

- XML, Java Midlet, Browser (Future) app environments

- Requires CUCM 7.1 (3) or higher
- SRST 7.1 with 12.4 (24)T but as TNP SIP Phone
- SRST 8.1 has full support

Camera (Delivered with CUCM 8.0)

A “Hosted” USB Camera Module accessory that attaches to a Cisco Unified IP Phone 9971 or 9951. It provides support for encoding of video signals from camera and allows phones to communicate via two-way video conferencing.

- H.264 encode
- VGA video resolution @ 24fps encode; CIF/SIF @30fps encode
- 2 M-pixel auto-focus sensor SOC
- Not designed as PC Web Cam
- Orderable March 24, 2010



SDIO – 9971 Only

- Simulates running phone sessions, video and applications on the phone
- Useful for demos and customer briefings

SDIO Card
(actual card may look different)

SDIO Slot
Available on
9971 only



Key Expansion Model (KEM)

Intuitive UE on a Reduced Footprint

- 18 physical keys + “shift/page” keys = 36 key functions per KEM
- Built-in footstand and wall-mountable config

Two Configurations:

- Traditional - spine connection to base phone
- Tethered – cable connection to base phone



Phone Model	KEMs Supported
9971	3 KEMs with 108 lines
9951	2 KEMs with 72 lines
8961	1 KEM with 36 lines

**One KEM can
be powered up
if you use AT
PoE.**

**A KEM cannot
be powered up
if the Cisco**

Understanding the New User Experience



Buttons Ergonomically Arranged

Cisco Unified IP Phone 8900/9900 Button Differences



Applications button



Fixed Keys Added For Rich User Experience

Cisco Unified IP Phone 8900/9900 Button Differences



Most commonly used call features on fixed hard buttons (hold, transfer, and conference) for a rich user experience

Cisco Unified IP Phone New 8900/9900 Button Differences



- Programmable Feature Buttons
- Phone lines, speed dials, and calling features



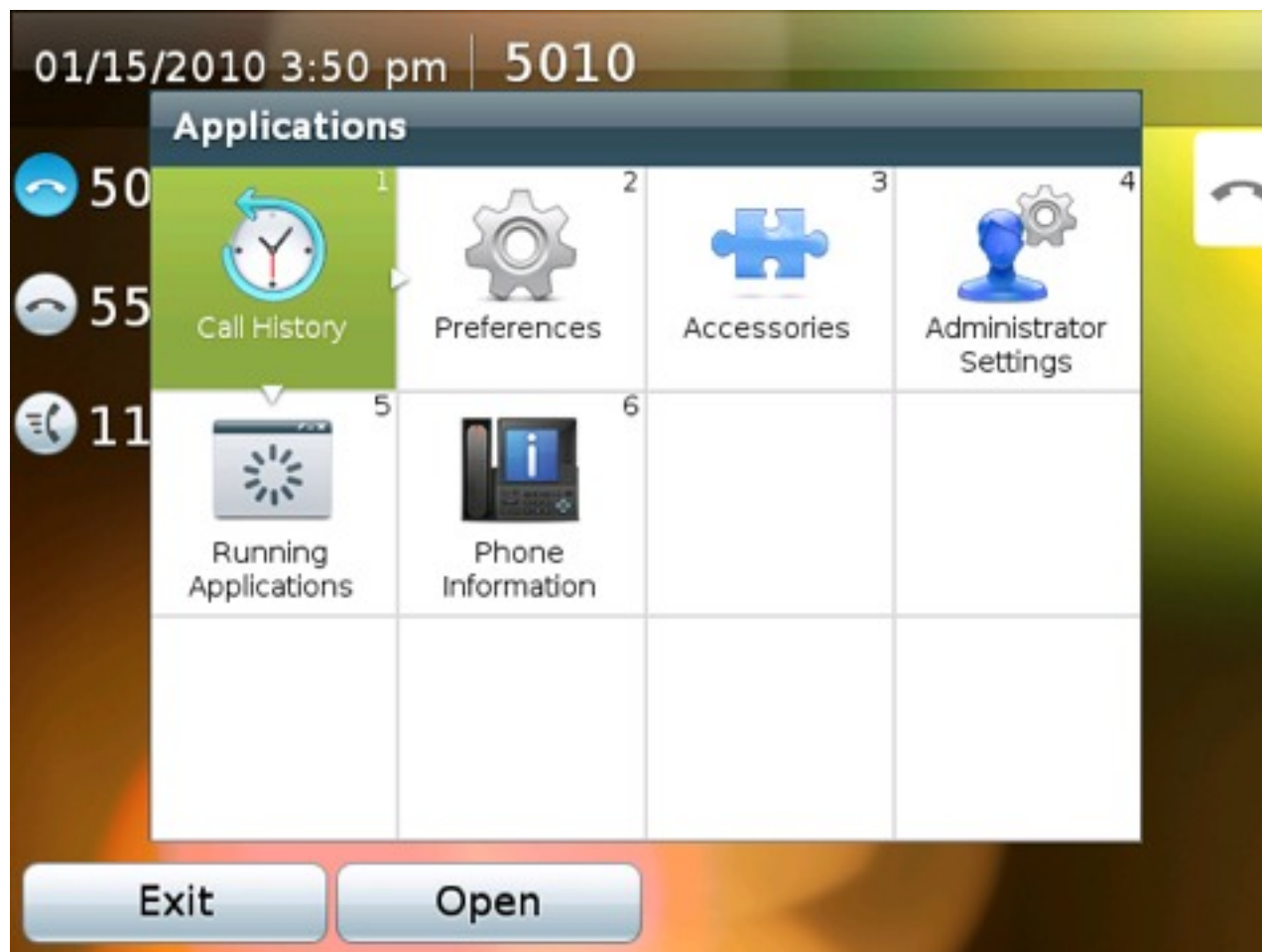
All Calls

Use for multiple lines



- Session Buttons
- Represents a call session
- Press button to answer ringing or held calls

Cisco Unified IP Phone 8900/9900



Simplified when Compared with the 7900 Experience



- Access this screen by pushing the Applications Button
- Access call history, preferences, accessories, and Administrator settings
- New future applications and services are accessible here



Cisco Unified IP Phone 8900/9900



- Toggle between missed calls and all calls
- This screen is invoked when missed calls are viewed
- This screen can also be invoked by pressing Application button



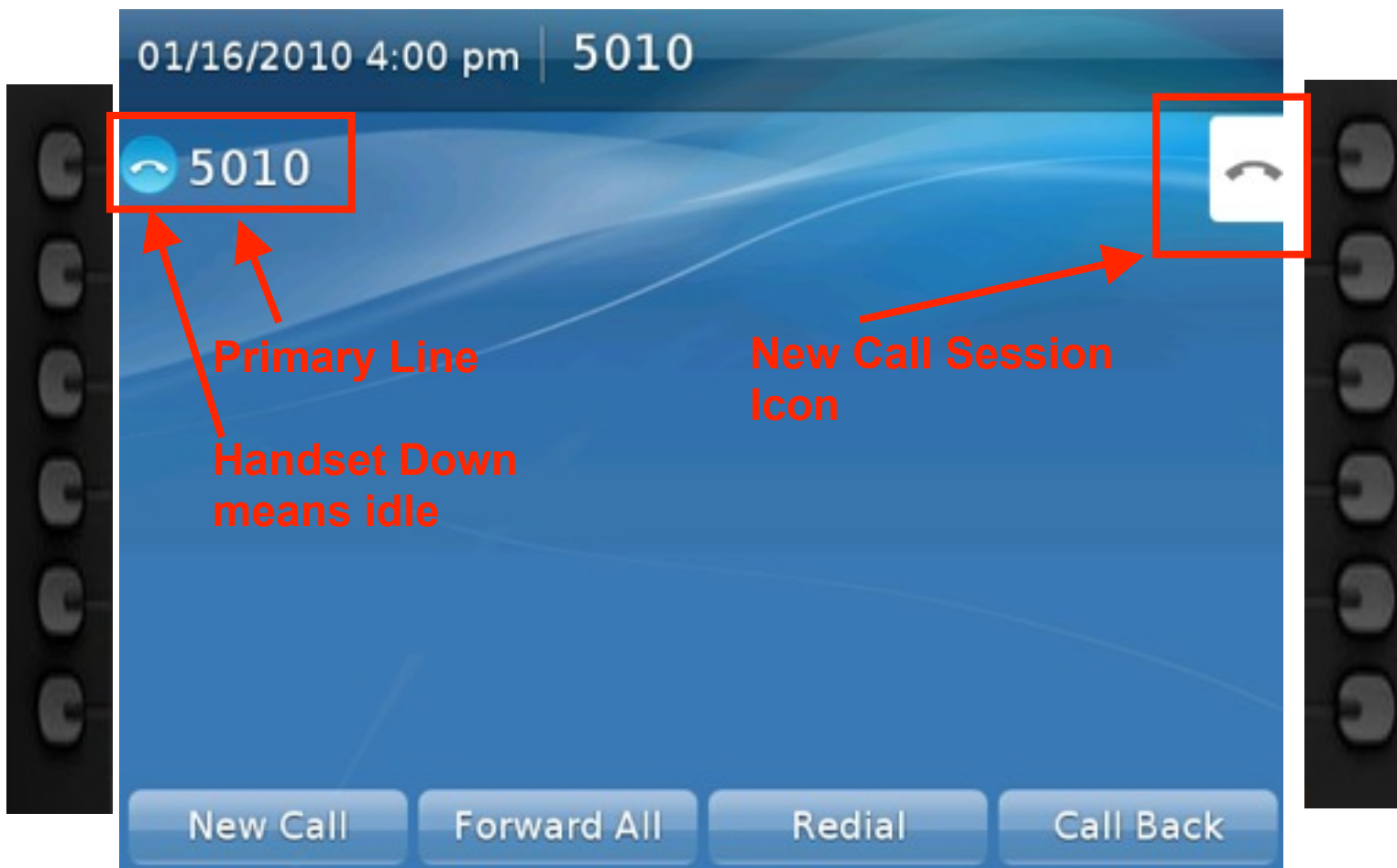
Cisco Unified IP Phone 8900/9900



- By default user can modify wallpaper, ringtone, and brightness
- End users see toast pop ups based upon various events

Basic Operations: IP Phone Completely Idle

Programmable Feature Buttons



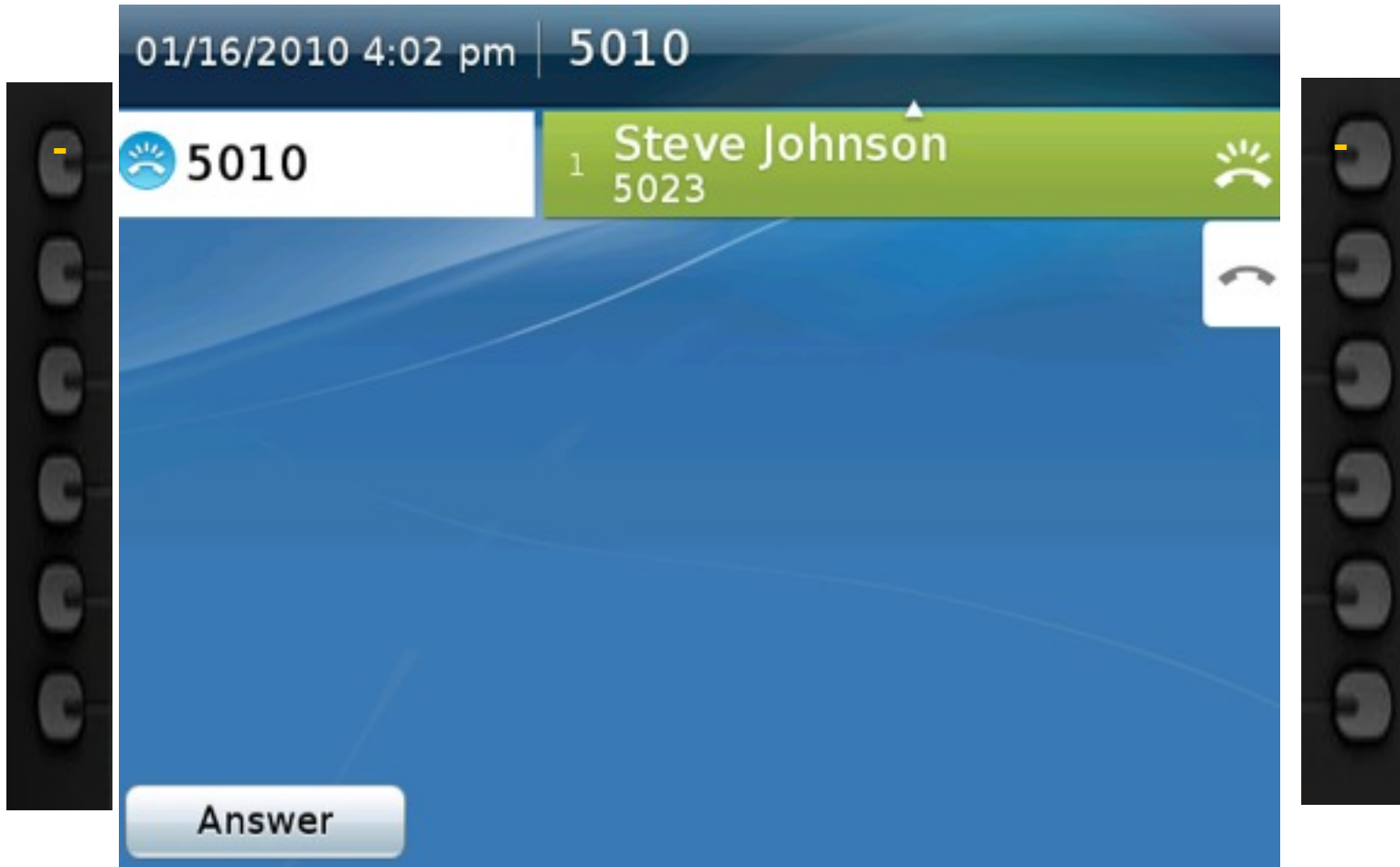
Session Buttons

- This is the “default” behavior if you do the bare minimum
- You can push top right session button to start call – NOT top left
- Of course, you can push speaker button or push “New Call” softkey

Basic Operations One Line One Incoming Call

Cisco Unified IP Phone 8900/9900

Programmable Feature Buttons



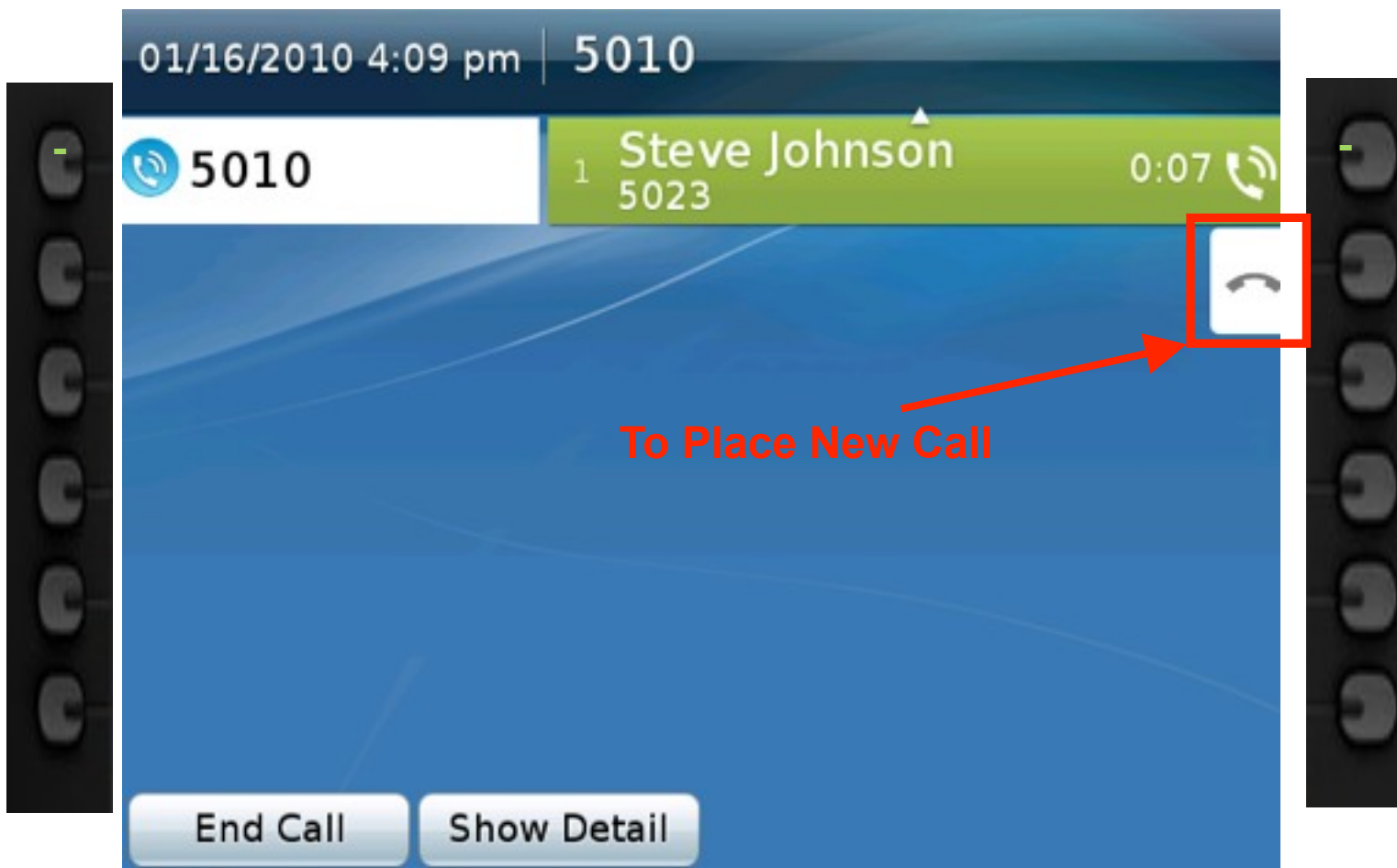
Session Buttons

- Phone icons change to alerting for incoming call
- Top left LED solid amber indicating call in coming in
- Top right flashing amber indicating you can push this button to answer

Basic Operations One Line One Answered Call

Cisco Unified IP Phone 8900/9900

Programmable Feature Buttons



Session Buttons

- Phone icons change to active when in a call
- Both LEDs solid green
- End call using “End Call” softkey, hang up handset, or push release



Cisco Unified IP Phone 8930/9930

Basic Operation: Multiple Calls on Hold

Programmable Feature Buttons



Session Buttons

- You can initiate new calls by pushing the new call session icon on right
- Calls go immediately on hold when you push the session key
- Calls stack based upon history and in descending order

Cisco Unified IP Phone 8800/9900

Programmable Feature Buttons



01/16/2010 4:14 pm | 5010

5010

1	Steve Johnson 5023	5:20	
2	Dan Jones 5030	1:40	
3	Tom Clark 5024	1:19	
4	Bob Lewis 5015	0:45	📞

Unable to create a call; the maximum number of calls for this line has been reached

End Call Show Video

Session Buttons



Multiple Call/Call Waiting Settings on Device SEP00254592E79F

Note: The range to select the Max Number of calls is: 1-200

Maximum Number of Calls*

Busy Trigger*

(Less than or equal to Max. Calls)

Cisco Unified IP Phone 8900/9900

Basic Operation: Navigate Multiple Stacked Calls

Programmable Feature Buttons



Session Buttons

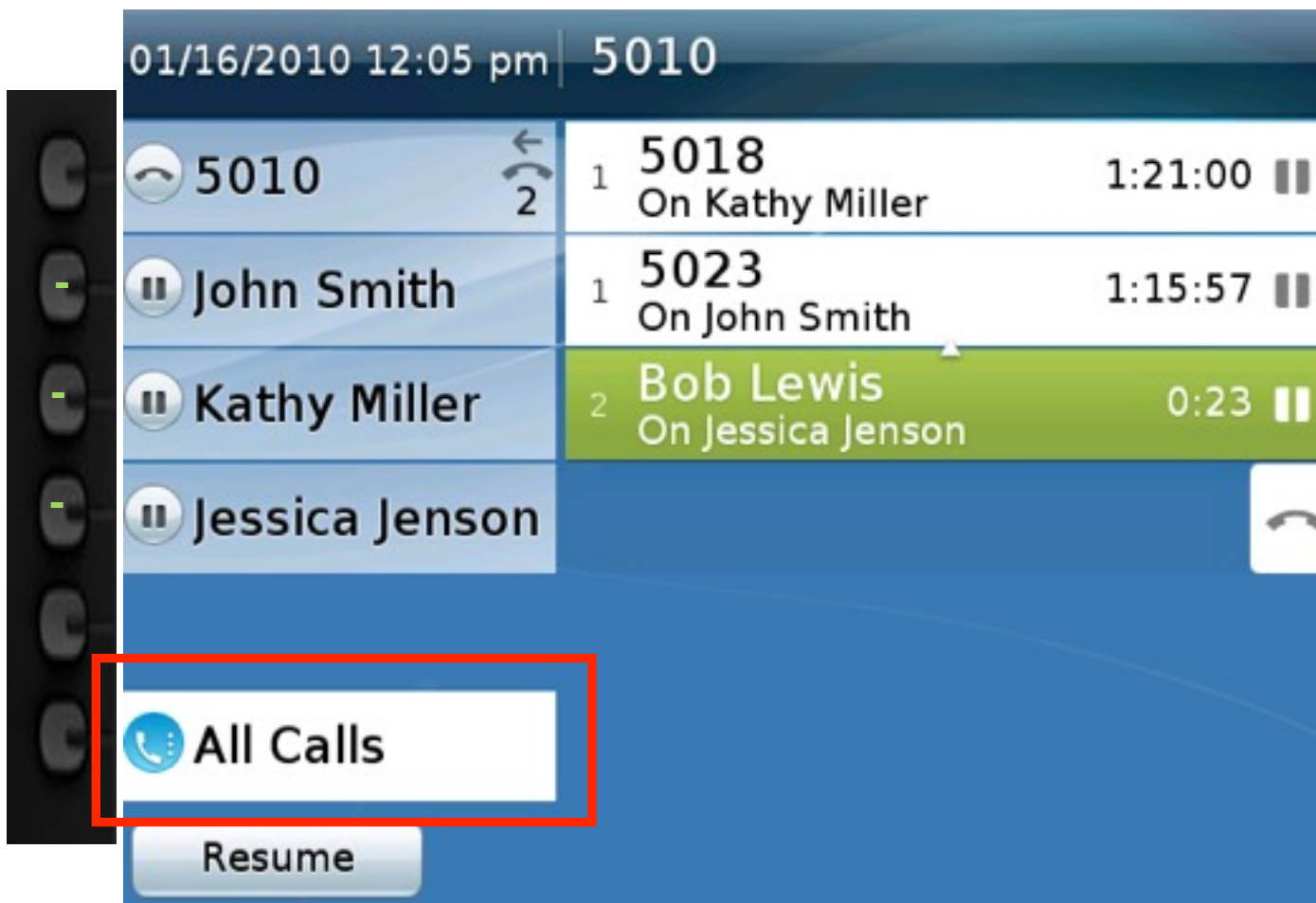


Simply select session button of caller to instantly move between calls and/or use navigation button to select

Best Practices for “All Calls” Multi-Party Calls

Cisco Unified IP Phone 8900/9900

Programmable Feature Buttons



Session Buttons

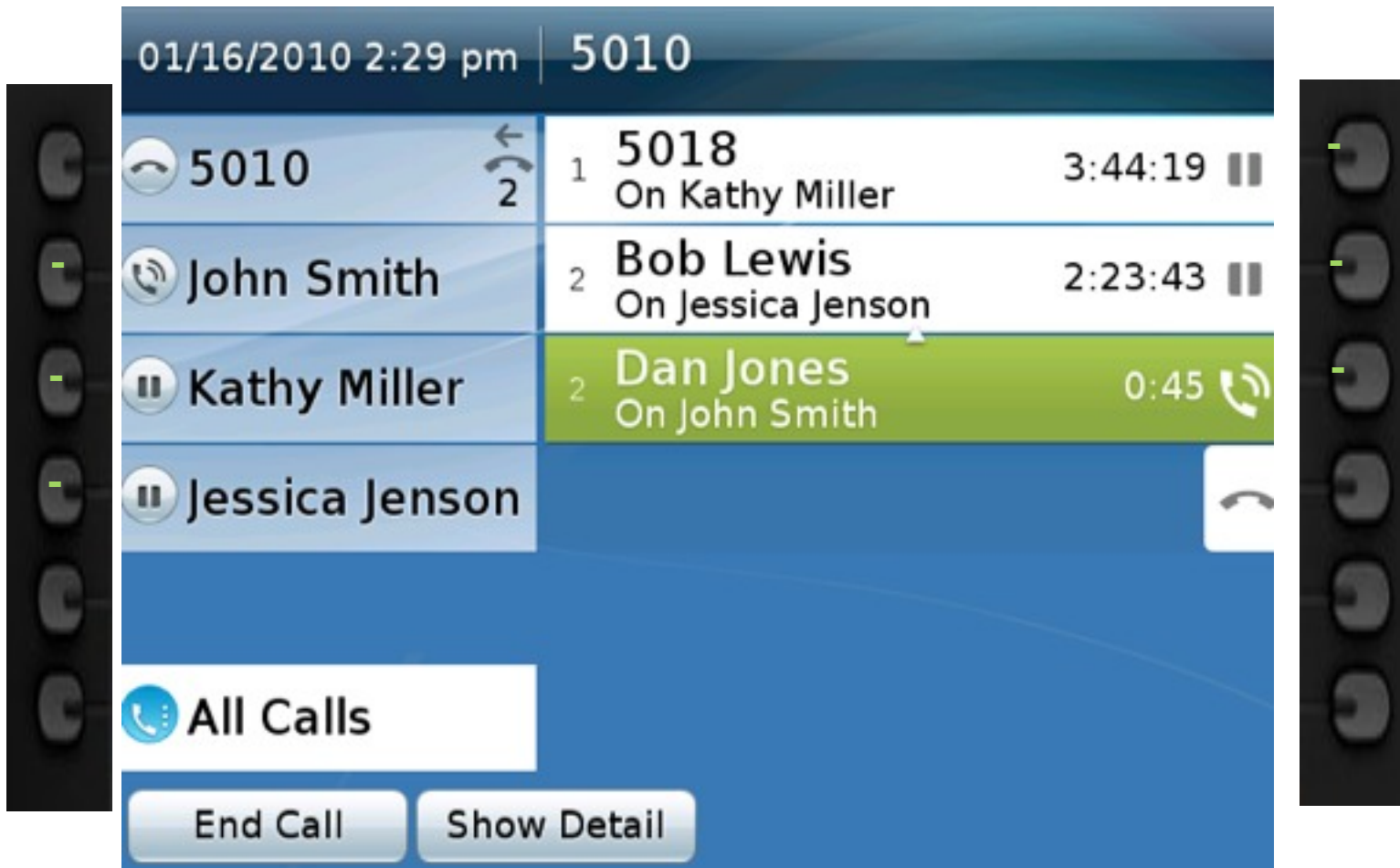
“All Calls” HIGHLY RECOMMENDED. Selecting “All Calls” provides full visibility and accessibility to all calls

Cisco Unified IP Phone 8900/9900



- John is on the phone as indicated by his phone icon
- We have calls on hold for Kathy and Jessica

Cisco Unified IP Phone 8900/9900



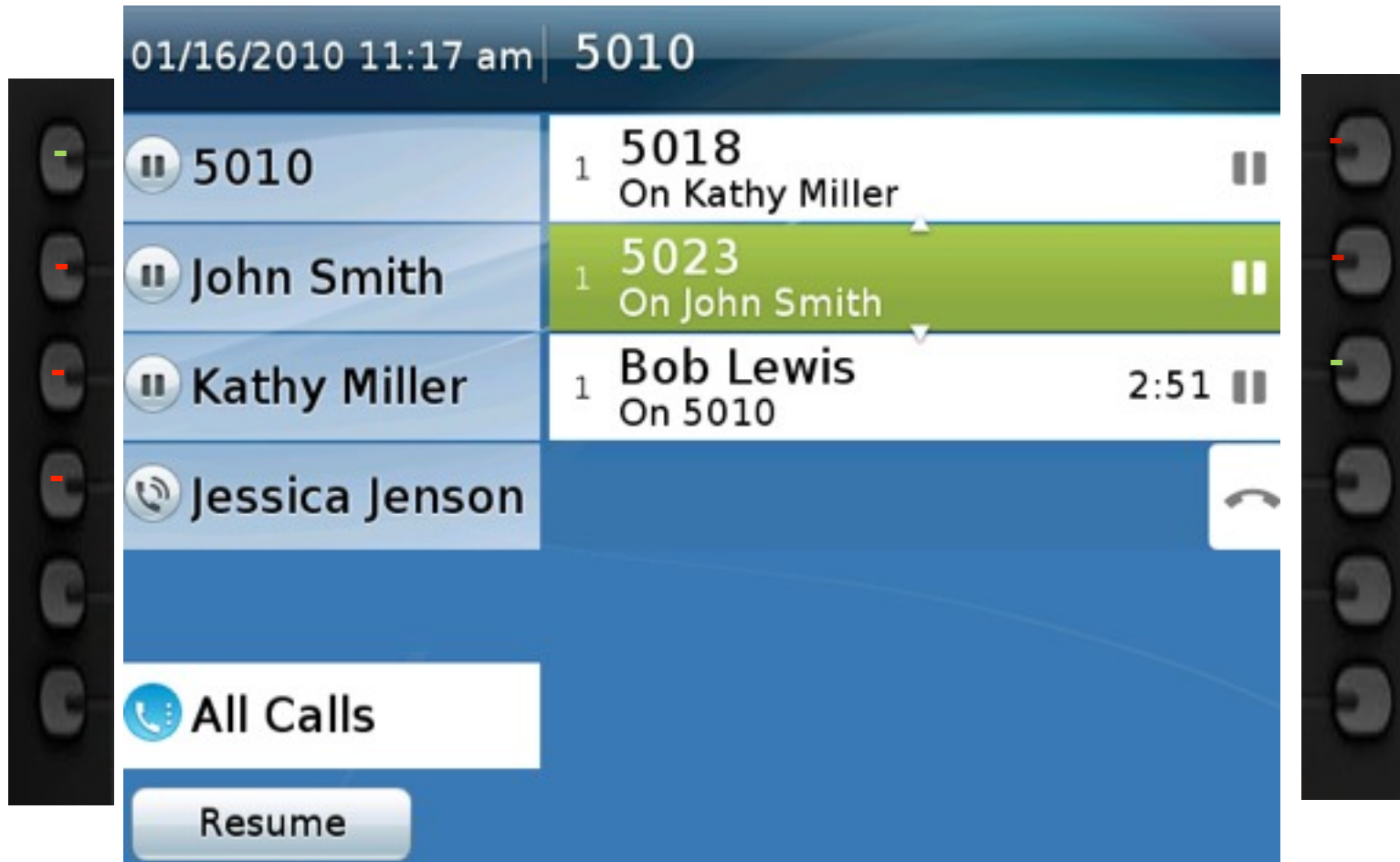
- Dan calls in on John's line but John is on the phone
- Dan's call is answered and asked if he wants to hold

Cisco Unified IP Phone 8900/9900



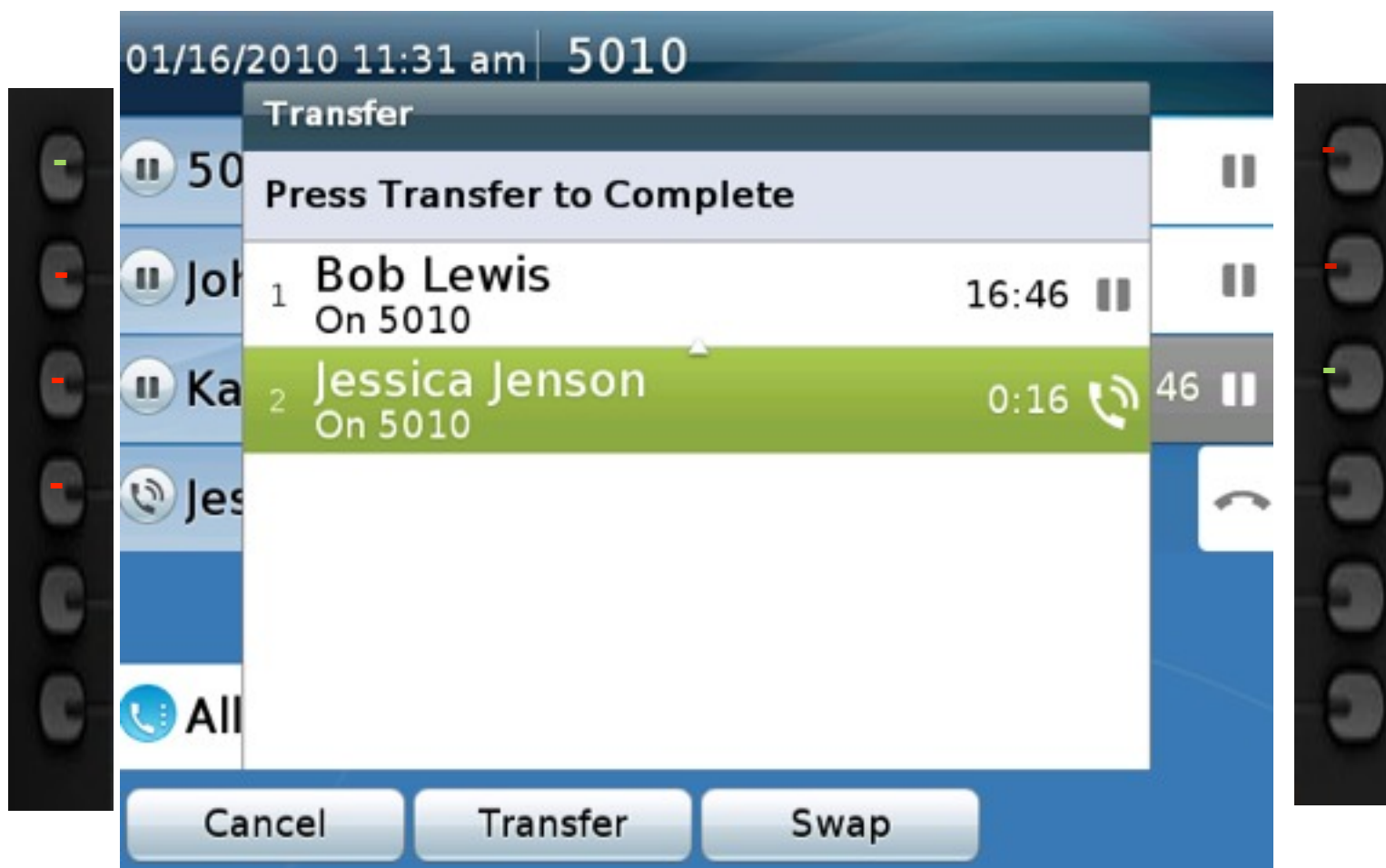
- Dan is now on hold
- Dan's call is stacked on John's 8900/9900 just like ours
- John will pick up Dan's call when ready

Scenario: Unified IP Phone 8000/9900



- Bob wants to speak with Jessica but Jessica is in a call
- Bob is on hold and Jessica asks for call to be transferred

Scenario: Cisco Unified IP Phone 8900/9900



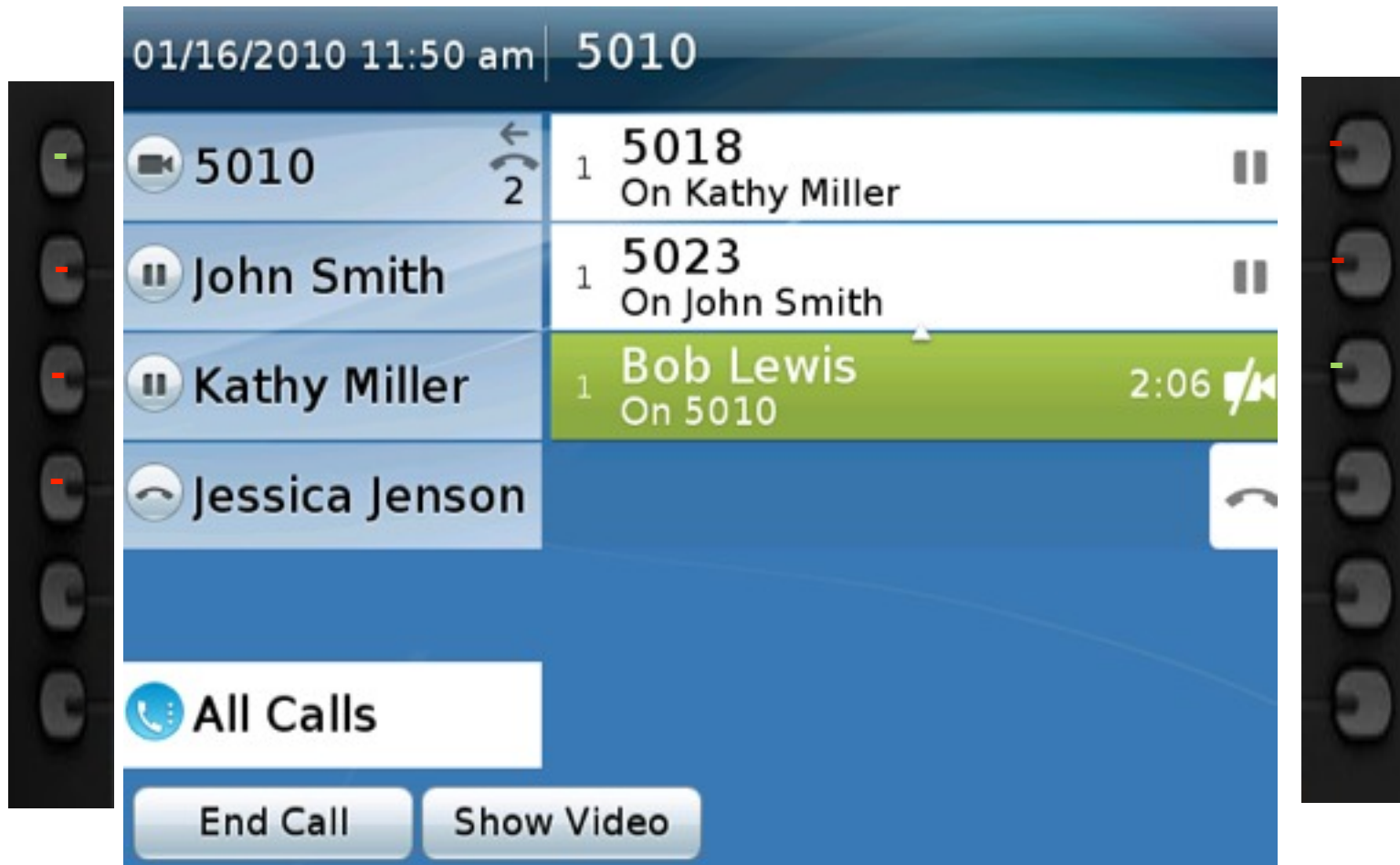
- Push session button for Bob, then push Transfer key
- You can push the Swap button to toggle back and forth

Transfer



Scenario: Bob Calls For Conference

Cisco Unified IP Phone 8900/9900



- A conference is needed with Bob and Jessica
- While on the line with Bob, press the Conference key

Conference



Scenario: Cisco Unified IP Phone 8900/9900



- Press conference button and dial Jessica
- Press conference button again just like with the 7900 series
- Use swap button to consult back and forth

Conference



Cisco Unified IP Phone 6900 Button Differences

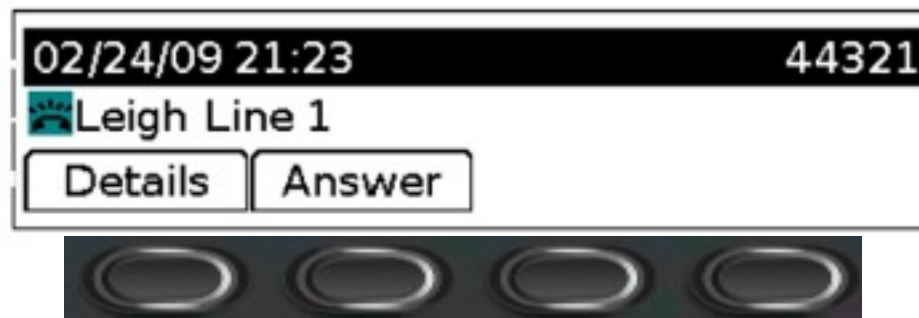


Maximum number of calls = 2, Busy trigger = 1.

Cisco Unified IP Phone 6900 Display

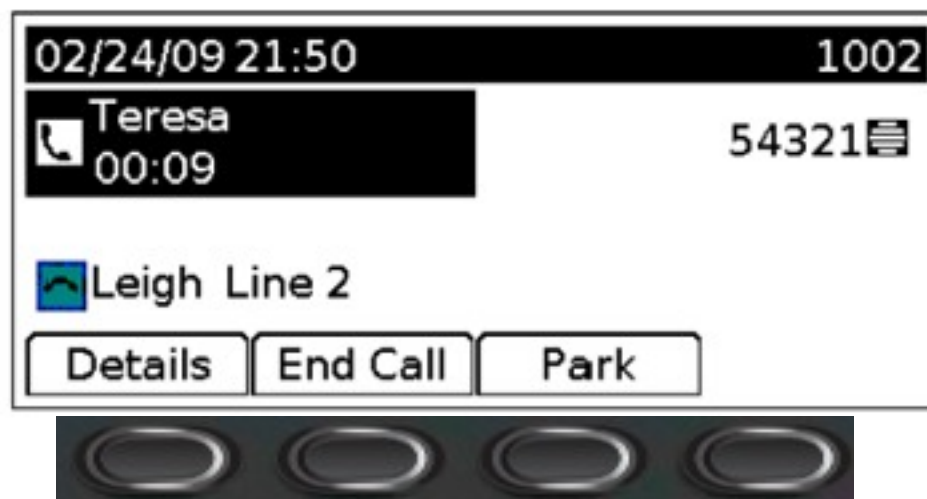
6921/6961 Display

6921 and 6961 has smaller display showing only one line or other status information



6941 Display

6941 has bigger display that can show multiple lines

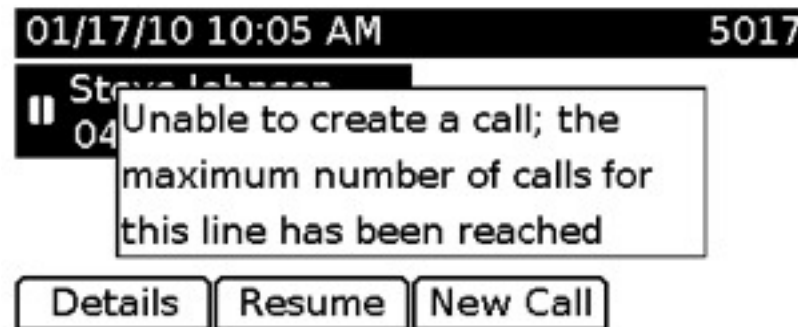


Configuration



■ Best Practice Configuration for 6900

- Scenario 1: Kathy received a 6921/41 to replace her 7960. The 6921/41 is configured with one line. She is on a speaker phone call with Steve. She puts Steve on hold and presses the speakerphone button again to initiate a new call. She gets error:



- Solution: The IT Administrator needs to configure an additional line on

Best Practice Configuration for 6900

Rollover Recommended

- Scenario 2: Kathy is on call with Steve. Kathy has only one line. Tom calls Kathy. Tom gets Busy or voicemail without Kathy being aware.

Multiple Call/Call Waiting Settings on Device SEP0026CBA7CFDD	
Maximum Number of Calls and Busy Triggers per Line are:	
Maximum Number of Calls	2
Busy Trigger	1

- Solution: IT Admin needs to have busy calls rollover to second line on Kathy's phone. Kathy's will hear call waiting beep and Tom's call will rollover to line 2.

Forward Busy Internal	<input type="checkbox"/> or
Forward Busy External	<input type="checkbox"/> or
Forward No Answer Internal	<input checked="" type="checkbox"/> or
Forward No Answer External	<input checked="" type="checkbox"/> or

5013
5013

Kathy's primary line 1 is 5017

Kathy's second line 2 is 5013 (or can be 5017 in a different partition)

Best Practice Configuration for 6900 Shared Lines Scenarios

- Scenario 3: Kathy is on call with Steve. Kathy has a shared line to 7900/8900/9900. Tom calls Kathy. Kathy does not see inbound call but 7900/8900/990 shared line rings.
- Rollover when busy on 2nd Ring will not work because 7900 rings
 - 1st Phone Call to Kathy – Both Phones Ring – Call is answered by Kathy
 - 2nd Phone Call to Kathy- Only 7900/8900/9900 Rings – Call is answered on shared line
 - 3rd Phone Call to Kathy – Neither Phone Rings - Call Forwards to VoiceMail or does rollover to Kathy's second line. Second line no answer forwards to VoiceMail.

Cisco Unified IP Phone 8900/9900

Sample configuration Model Differences

- No LCD Video Capabilities for 8900 (except future video streaming)
- CUVA for 8900 = Target 2HCY2010
- CUVA for 6900 = Target 2HCY2010

Back USB 9951/9971

Side USB
8961/9951/9971

Camera 9951/9971

LCD Video 9951/9971

USB Classes
8961/9951/9971

Bluetooth 9951/9971

The screenshot shows a configuration interface for a Cisco Unified IP Phone. Red arrows point from the text labels on the left to specific settings in the interface:

- Back USB 9951/9971** points to the **Back USB Port *** setting, which is set to **Disabled**.
- Side USB 8961/9951/9971** points to the **Side USB Port *** setting, which is set to **Disabled**.
- Camera 9951/9971** points to the **Cisco Camera *** setting, which is set to **Disabled**.
- LCD Video 9951/9971** points to the **Video Capabilities *** setting, which is set to **Enabled**.
- USB Classes 8961/9951/9971** points to the **Enable/Disable USB Classes** section, which is expanded to show **Mass Storage**, **Human Interface Device**, and **Audio Class**.
- Bluetooth 9951/9971** points to the **Bluetooth *** setting, which is set to **Disabled**.

Other visible settings include **Bluetooth Profiles *** (set to **Headset**), **Settings Access *** (set to **Enabled**), and a top **Enabled** dropdown.

Cisco Unified IP Phone 9951 & 9971

Configuring Video (Point-to-Point)

- Point-to-Point video supported on 9951/9971 LCDs – even one-way
- Same methods used today for 7985g, CIPC/CUVA, etc.
- Call Statistics are built into 9951/9971: we are sending 640x480 below
- Make sure “video capability” is enabled on CUCM for 9951/9971

Point-to-Point

Video Statistics Built into Phone



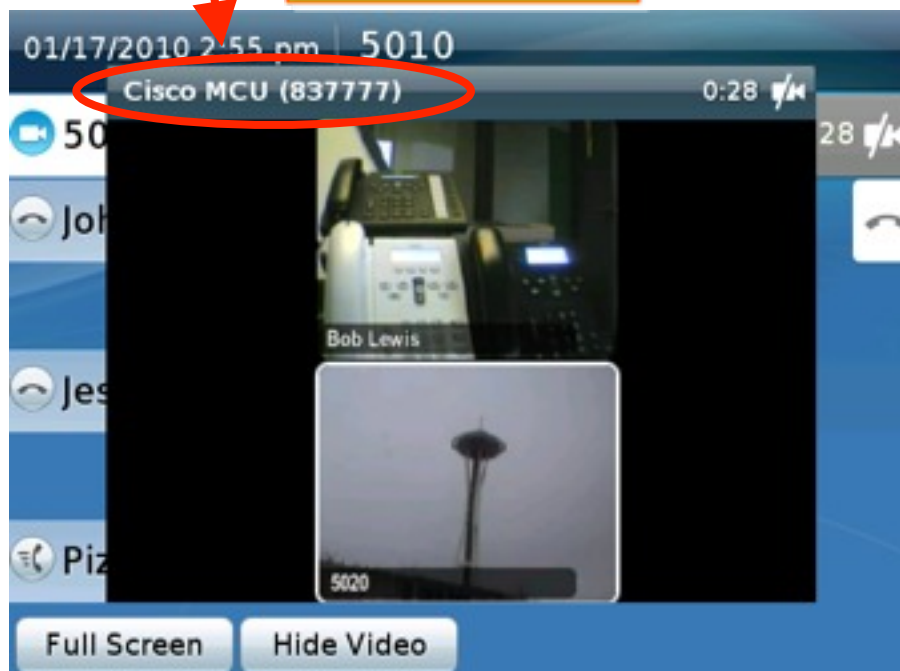
Cisco Unified IP Phone 9951 & 9971

Configuring Video Conferencing

- Using Conference Button is always preferred for CUCM directly attached endpoints. Must have CUVC MCU SCCP + Conf Bridge/MRG on CUCM.
- Use can run H.323 trunk from CUCM to Gatekeeper and dial digits. This is preferred for conferencing in 3rd party endpoints
- You can do both Conference & H.323 on the same CUVC at the same time

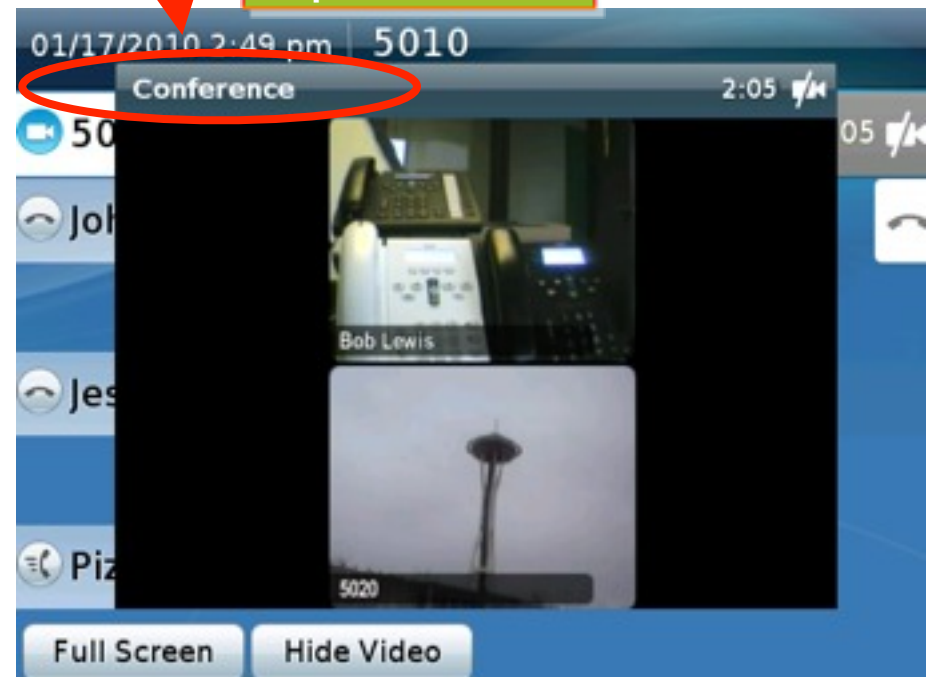
Dial Direct into MCU Bridge

Requires MCU



Use Conference Button on Phone

Requires CUVC



Cisco Unified IP Phone 9971

Configuring 9971 Wireless

- ❑ Users cannot connect a PC to the PC port of phone for network access
- ❑ Disconnect network port on the back of the phone for wireless to work
- ❑ Phone will switch to wired connection if network port is connected
- ❑ Phone must be powered by an external power source (No PoE). Given that, the WLAN could be a “backup” if the LAN fails – approximately 30 seconds to switch
- ❑ There are known issues of interference between 2.4 GHz wireless and Bluetooth Coexistence of Bluetooth and 802.11b/g is possible, but call capacity might be reduced. Multicast Music on hold in coexistence mode not supported
- ❑ Firmware downloads might be slower than expected
- ❑ Emergency Responder tracks Wireless Phones by IP address
- ❑ Wireless Access Density Needs to be Considered

Security Mode	
<input type="radio"/> Open with WEP	2
<input type="radio"/> Shared Key	3
<input type="radio"/> Leap	4
<input checked="" type="radio"/> EAP-FAST	5
<input type="radio"/> AKM	6

Administrator Settings	
802.11 Mode	
<input checked="" type="radio"/> 802.11b/g	1
<input type="radio"/> 802.11a	2
<input checked="" type="radio"/> Auto	3



CISCO