TDM – TC6.2

CTG TME Endpoint Team

Information in this slide deck is subject to change until FCS

June, 2013

Agenda

- What is new in TC6.2
- Known issues
- Troubleshooting
- Q & A

TC software evolution

EX
MX
SX
Profile
C-Series

TC 6.0

CUCM encryption
AS-SIP Phase 1
Medianet
Support for ISDN Link
Improved video layout control
CTMS encryption

TC 6.1

TC6 Features
TE6 Features
G.729 Audio Codec
Release key removal

Released

TC 6.2

Summer 2013

TC 6.3

EX Series
(CUCM only)

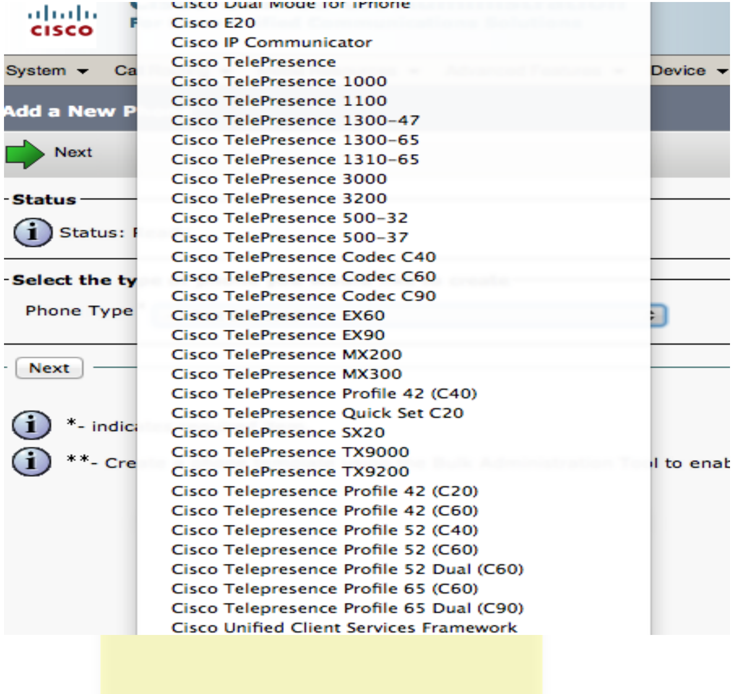
TE 6.0

Voicemail indicator
Call forward all
Consultative transfer
Shared Lines
Ad-hoc conferencing
Remote Expert support

TC6.2 Vision:
To complete the remaining integration of CUCM feature functionality, take the first step towards Lync 2013 interoperability, improve the integration between Cisco Telepresence endpoints and Cisco conferencing platforms, and continue to improve the serviceability of TC SW based endpoints

What is new in TC6.2

TC6.2 Endpoints supported in Cisco CUCM 9.0



- EX Series
- MX Series
- C Series
- SX 20
- Profile Series

- No changes from TC6.0/TC6.1

TC 6.2 Overview

Active Control

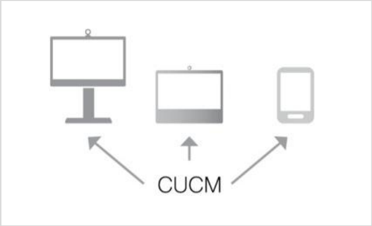
Control the TelePresence Server experience intuitively from the Touch interface: see participant list, change video layout, disconnect participants, etc.

CUCM Redundancy

High reliability, always connected.
Failover / fallback: If CUCM registration is lost, endpoints will automatically register to another CUCM.
Call preservation: If an endpoint loses CUCM registration during call, the call will be preserved

CUCM Provisioning

Allows endpoints to be fully and securely provisioned from CUCM and simplifies deployment.



Products Supported:

- C Series Codecs
- SX20 Quick Set
- Profile Series
- MX Series
- EX Series

H264 SVC

Supports scalable conferencing
Improves MSFT Lync 2013 P2P interop

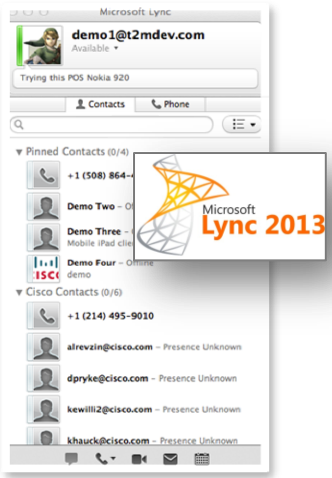
SIP ICE

Optimizes media path by always securing shortest media route between locations, thus avoiding bottlenecks especially for unknown network topology.

Extending Reach with H.264 SVC

Continued commitment to standards

B2B and
Intra-Enterprise

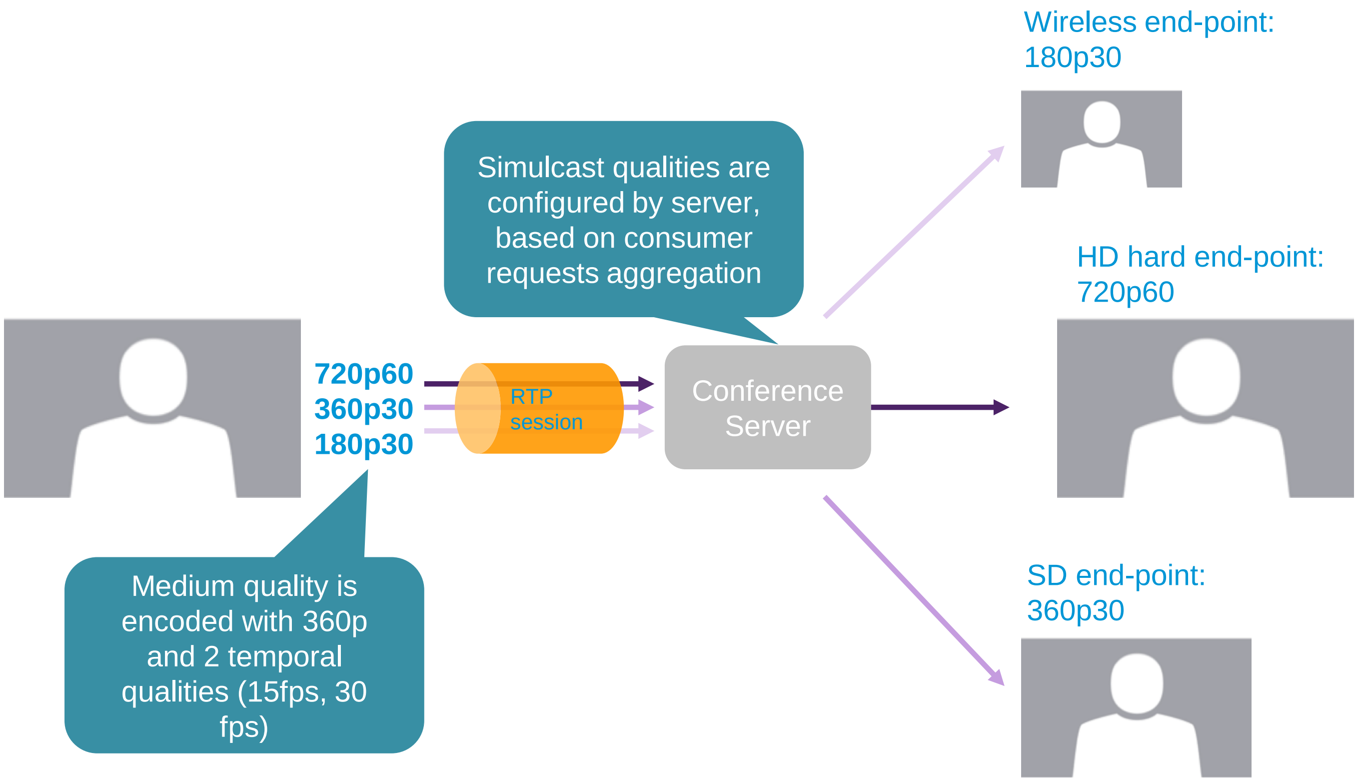


Cisco Collaboration interoperability with Microsoft Lync 2013

- Business-to-Business and Intra-Enterprise 720p HD video
- Enabled by VCS Expressway and Endpoint SVC support
- SIP trunking interop without transcoding (no AMG*)

*AMG: Cisco Advanced Media Gateway not required

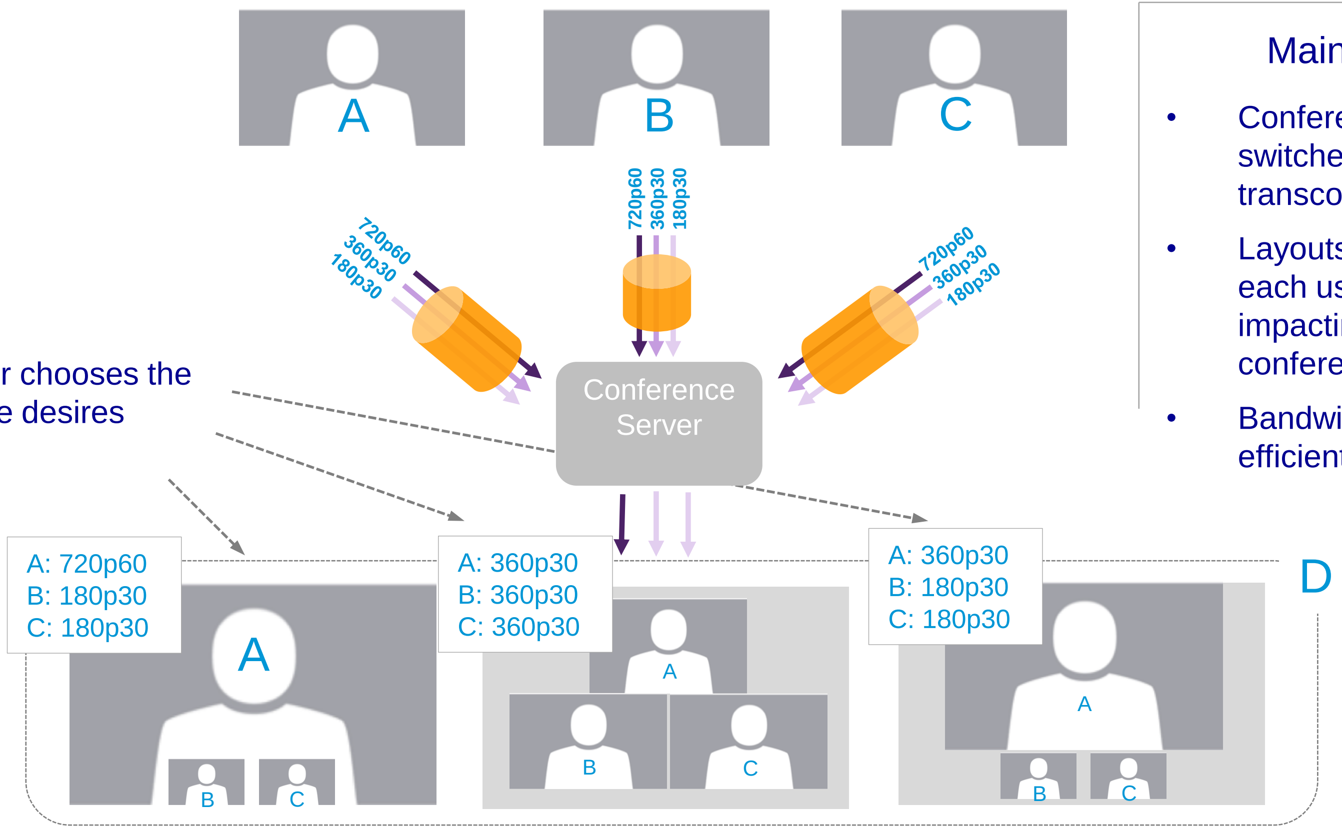
Multistream: How does it work?



1. Transmitting end-point generates different resolutions and FR of the same stream
2. TS listens to other end-points requests
3. TS switches received images, and sends the appropriated stream
4. Receiving end-points decodes stream

Local Composited Layout

The end user chooses the layout he/she desires

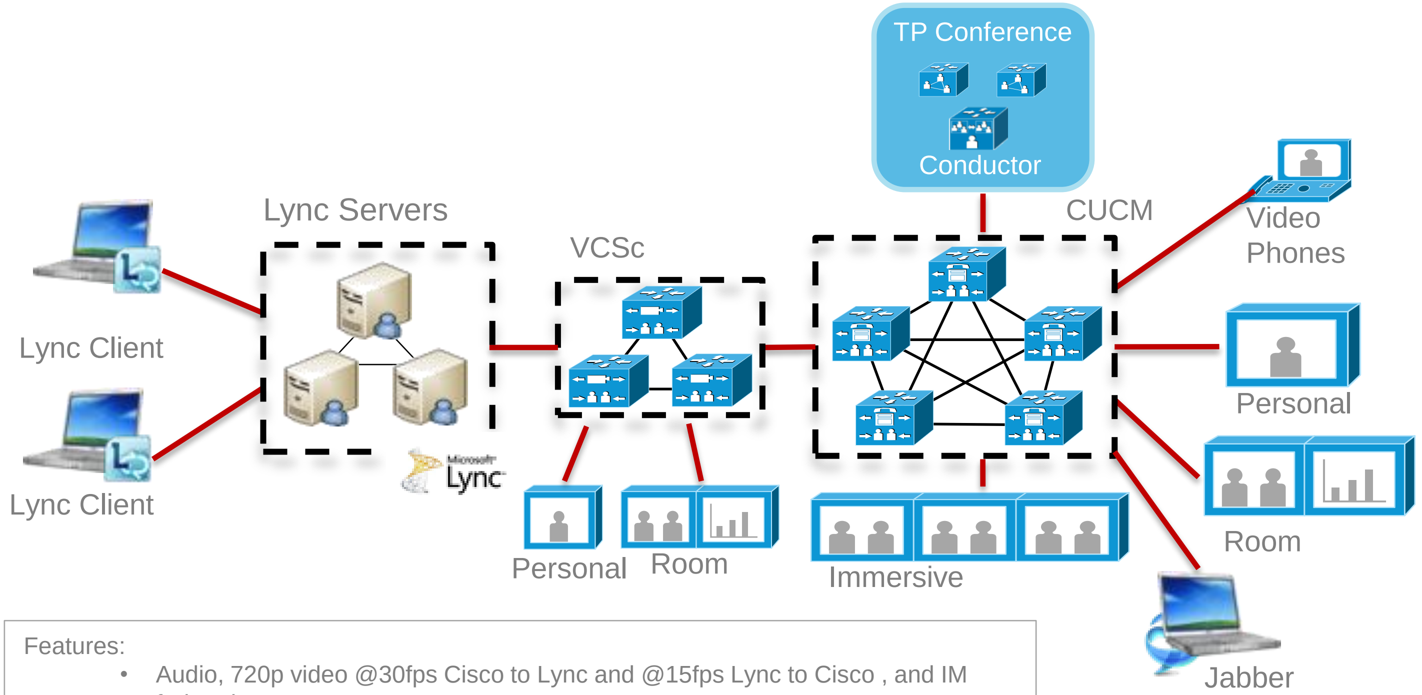


Main Benefits

- Conference server switches, it does not transcode
- Layouts are independent to each user without impacting load on the conference server
- Bandwidth is used efficiently

Cisco & Lync 2013 Interop – Phase 1

Device	Min. Version
CUCM	9.0
VCSc	8.0
MX, SX, C-series, Profile and EX series	TC6.0
Lync Server	2013
Immersive	CTS1.9/TX6



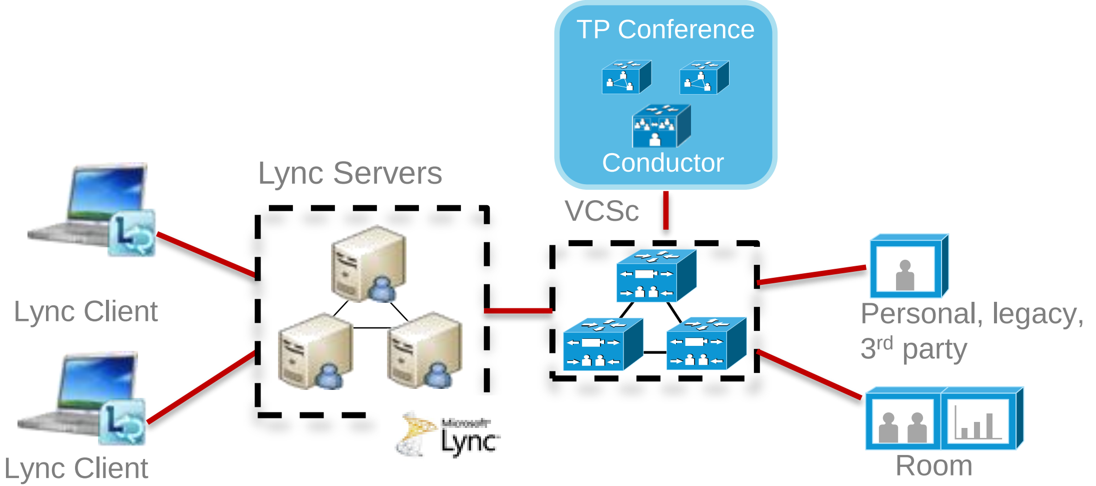
Features:

- Audio, 720p video @30fps Cisco to Lync and @15fps Lync to Cisco , and IM federation
- Conferences using Cisco conferencing resources only (TPS can host Lync @15fps)
- Encryption
- Presentation support from Cisco to Lync only

Cisco & Lync 2013 Interop – Phase 1

VCS Only option

Device	Min. Version
VCSc	8.0
MX, SX, C-series, Profile and EX series	TC6.0
Lync Server	2013

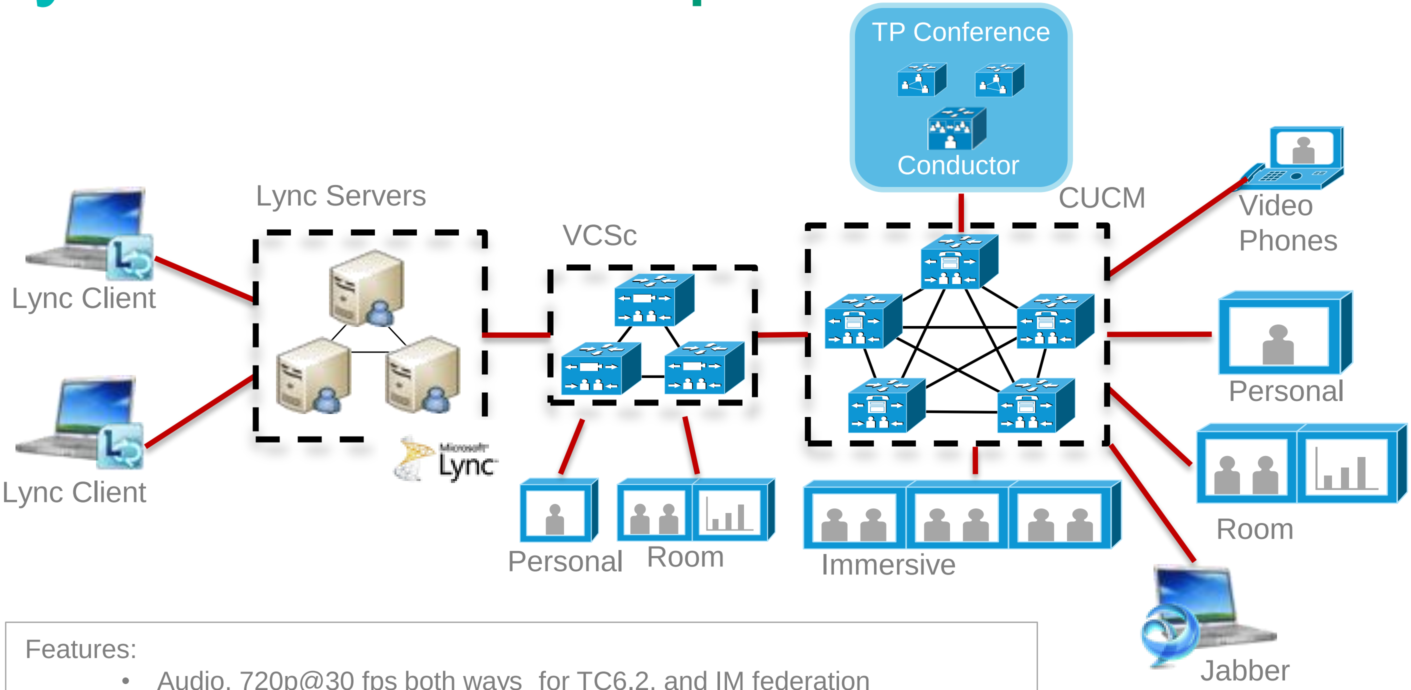


Features:

- Audio, 720p video @30fps Cisco to Lync and @15fps Lync to Cisco , and IM federation
- Conferences using Cisco conferencing resources only (TPS can host Lync @15fps)
- Encryption
- Presentation support from Cisco to Lync only

Cisco & Lync 2013 Interop – Phase 2
(CUCM 10.1)

Device	Min. Version
CUCM	10.1
VCSc	8.0
MX, SX, C-series, Profile and EX series	TC6.2
Lync Server	2013
Immersive	CTS1.9/TX6



Features:

- Audio, 720p@30 fps both ways for TC6.2, and IM federation
- Conferences possible with Cisco's conference resources
- Encryption
- Telepresence Server can host Lync clients
- Presentation support from Cisco to Lync only

TC SVC Configuration

- xConfiguration Conference [1..1] LyncCompatibility Mode: <Off/On>
- TC endpoints must have Lync Compatability mode turned on for Lync 2013 native interop to work.

Lync 2013 Integration For Point-To-Point Calls

- See Lync 2013 users in TC endpoints phonebook (TMS)
- The ability to dial between TC-endpoint and a Lync user to receive high quality audio and video
- HD quality at full frame rate – 720p30 (bi-directional)
- Native media interop using H264 SVC (UC Config Mode 1)
- Able to answer calls on either TC-endpoints or Lync 2013-clients when receiving an incoming call (VCS version X8)

New CUCM features: Encrypted Configuration

- Encrypted configuration: CUCM provisioning data is now sent encrypted to the endpoint if it has a secure connection with CUCM. The configuration will be transmitted over HTTPS (encrypted with AES).
- TC endpoints will only read the admin password if the endpoint has been set up with an encrypted security profile.
- The password can not be empty.
- The user name must be admin.

New CUCM features: CUCM Redundancy/Failover

- Failover: CUCM redundancy is now possible. An Endpoint will automatically failover to the next CUCM in the cluster if the connection to the active CUCM is lost. Supported in CUCM´s with at least 8.6 or higher.
- The re-registration with a new CUCM will occur in the background during the call unlike the IP phones which will wait until the call is completed.
- Since the new CUCM is unaware of the active SIP dialog, active calls can only hang up.

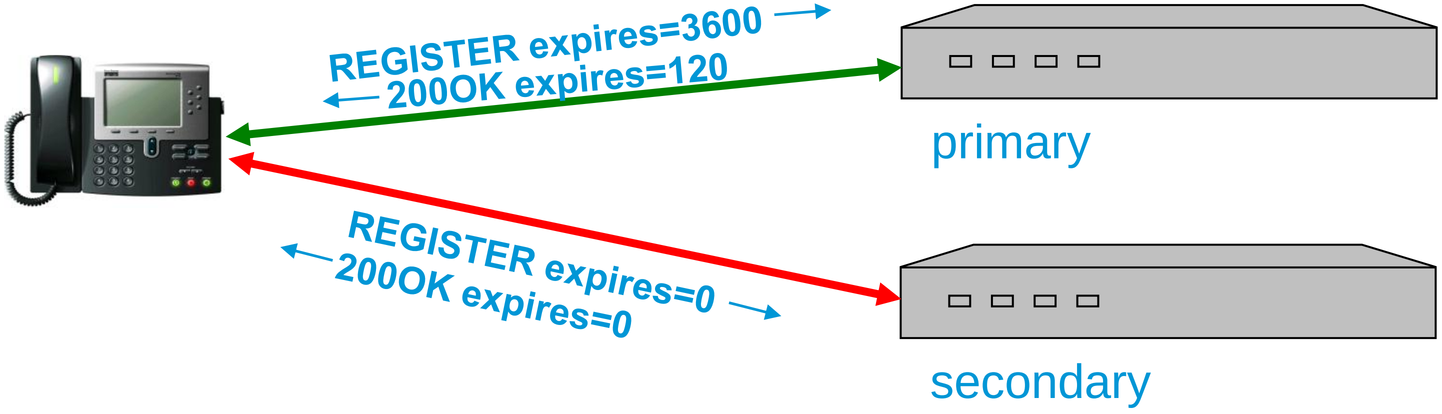
New CUCM features: CUCM Redundancy/Failover

- SIP does not have a well defined message sequence for “hot standby” operations.
- SIP endpoints use a REGISTER message with an expire value = 0 as a keep alive message to their backup Call Manager.
- SIP endpoints use a REFER message with a special tag “*X-cisco-remotecc:token-registration*” to check on whether their primary Call Manager is available again.

Registered with Primary CUCM

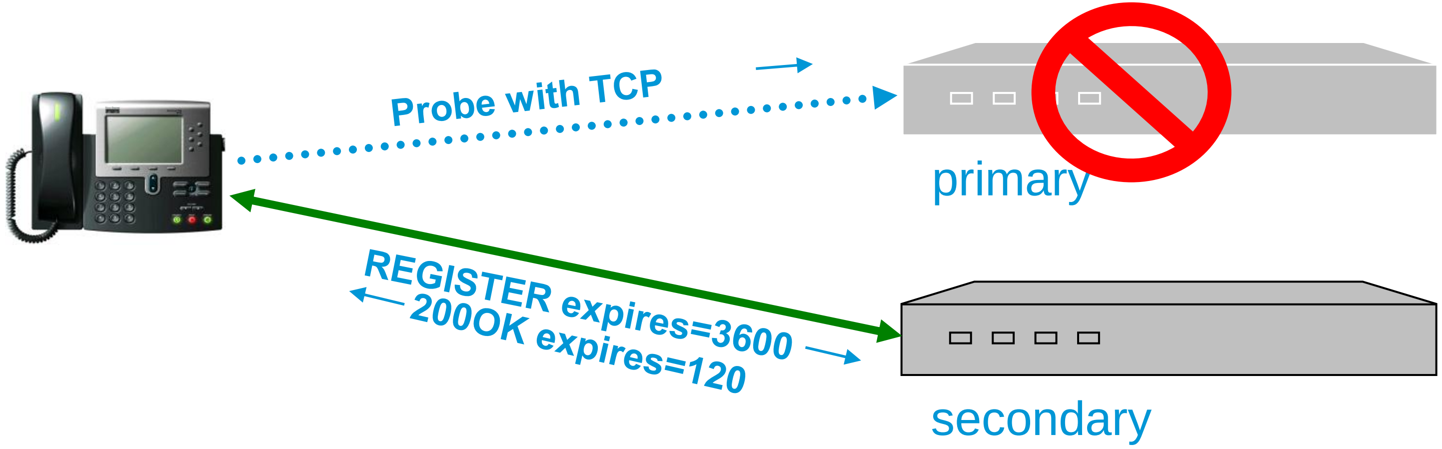
Active — Active REGISTER messages contain an Expires header > 0

Keep alive — Keep alive REGISTER messages contain an Expires header = 0 and a Cisco-keep-alive tag in the Contact header.



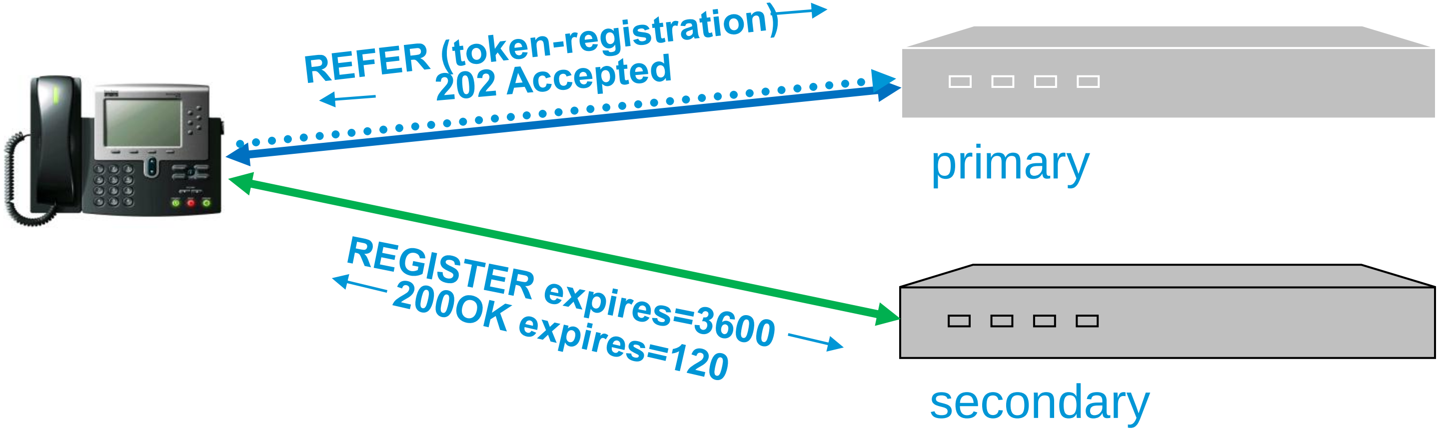
Failover to Standby CUCM

The phone detects the primary is down (e.g. TCP link down) and immediately registers with secondary. Then the phone begins to probe the primary with TCP SYN and, once the TCP connection is up, REGISTER w/ Expires=0 and cisco-keep-alive in the Contact header.

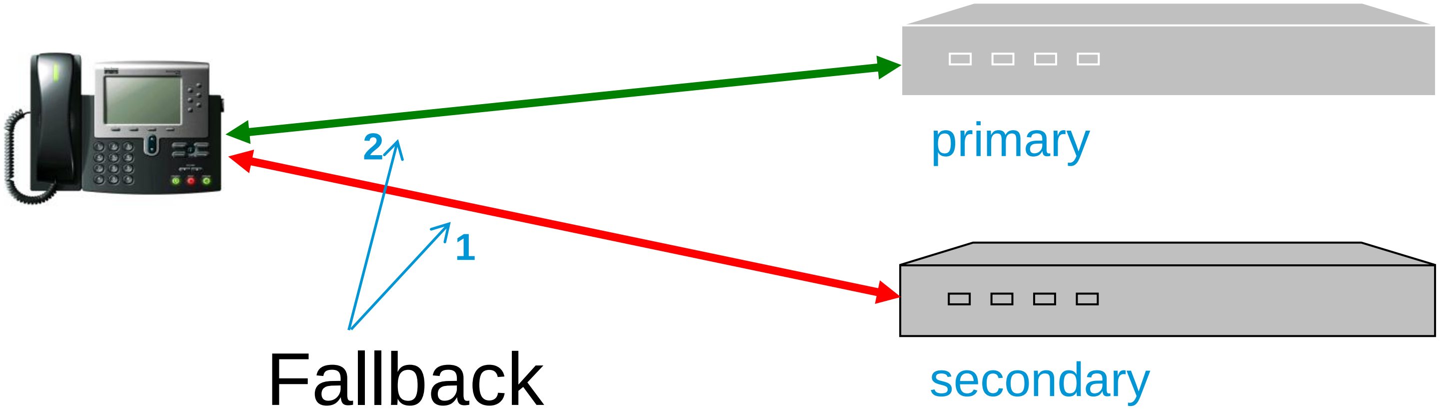


Fallback

Once the primary is up and responds to the keep-alive REGISTER with a 200OK, the phone sends a REFER with token-registration urn in the Refer-To header.



Fallback



[1]Register with expires=0 sent to the secondary to unregister.

[2]Then the phone will immediately register to the primary.

New CUCM Feature: Call Preservation

- If you lose connection to the CUCM, an active call will stay up. All actions will be greyed out except “Hang Up”.
- Next call will be handled by the secondary CUCM and all features are available again.
- When the primary CUCM is back online, the endpoint will change its registration back to the primary CUCM.

ICE Introduction

- What is ICE?

"Interactive Connectivity Establishment" as described in IETF draft

ICE provides a mechanism for SIP client NAT traversal

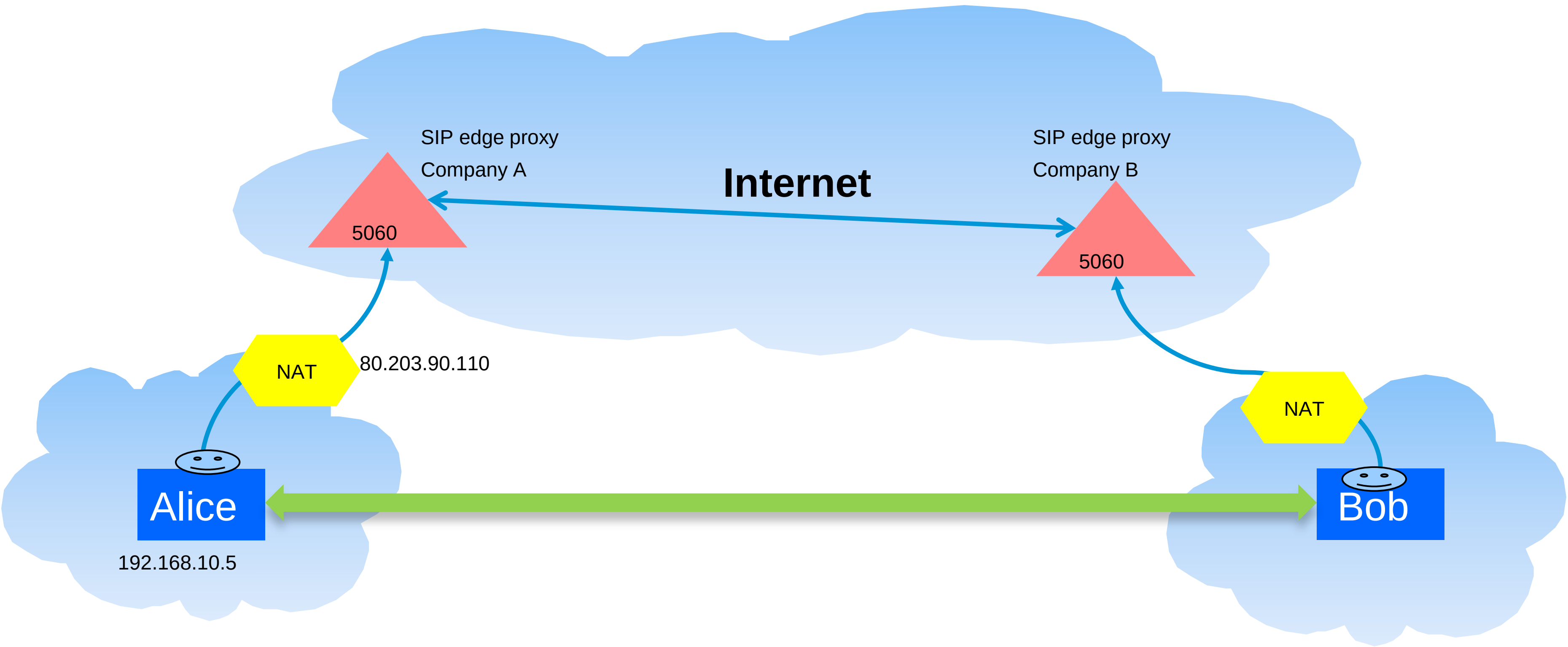
"Not a protocol – it is a 'framework'

"ICE allows the clients to discover enough information about their topologies to potentially find one or more paths by which they can communicate."

ICE Benefits

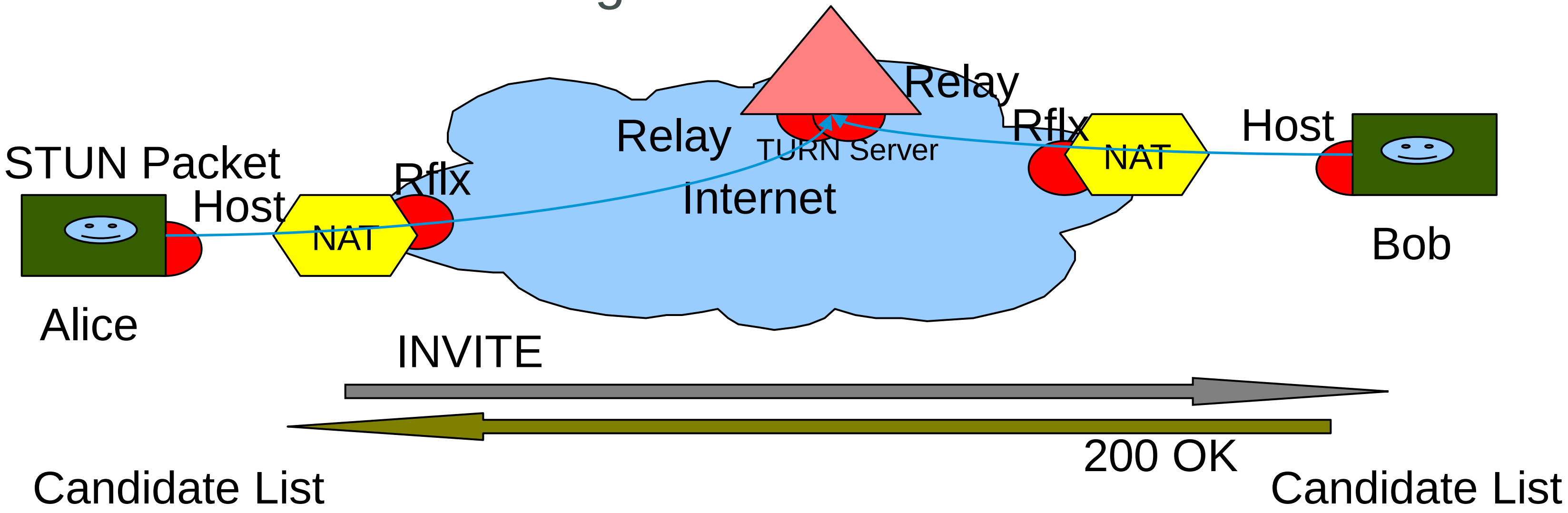
- Optimal media path by sending peer to peer when possible
  - Enables cloud scenarios
  - Reduces bandwidth cost. No need to traverse cloud or enterprise servers
  - Reduces traversal load of VCS
- Standardized IPv4/IPv6 dual stack solution
- Separates signalling and media
  - A signalling path must exist for ICE to work
- Industry proven
  - MSFT, Google, Apple ++ all uses flavours of ICE
- Building block for future extensions like:
  - Address mobility (MICE)
  - Resilience mechanisms
  - Cisco on Cisco smarter endpoint/network communication

ICE Example


SIP edge proxy
Company A
5060
Internet
SIP edge proxy
Company B
5060
NAT
80.203.90.110
NAT
Alice
Bob
192.168.10.5

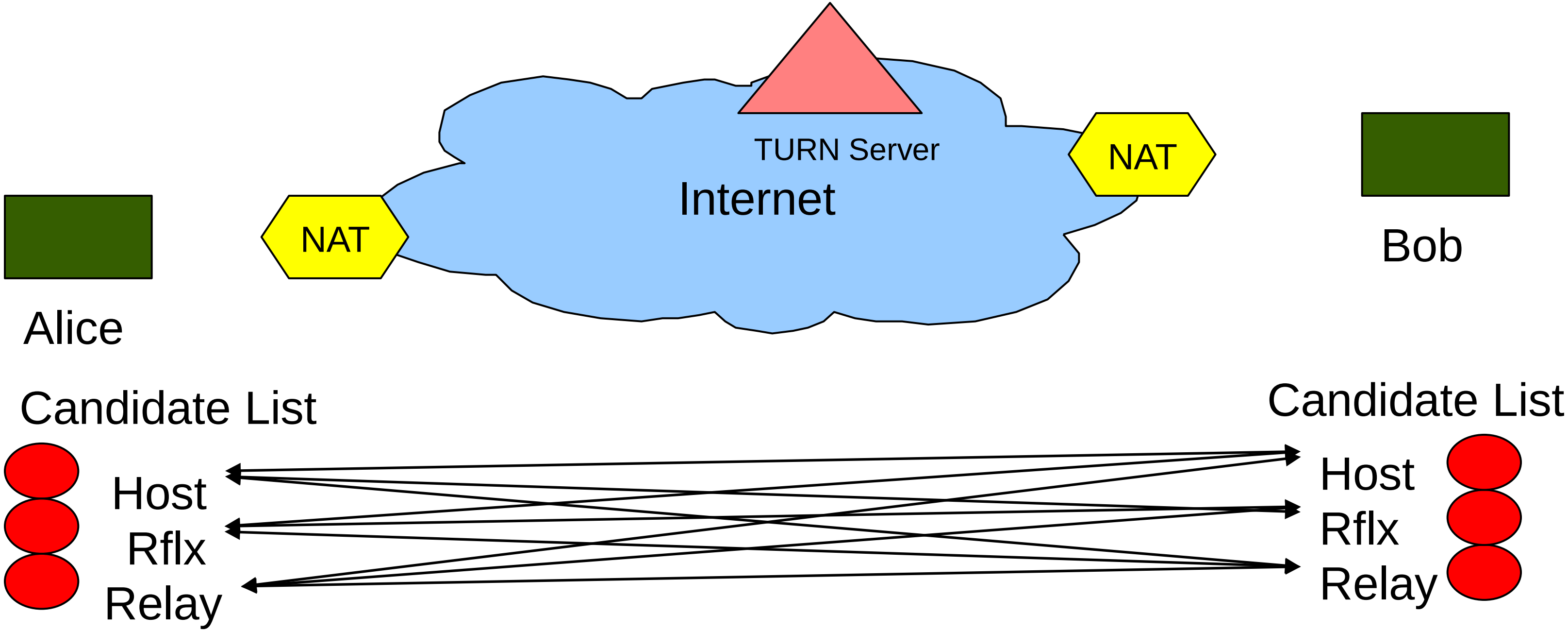
ICE Introduction

- ICE Candidate Gathering



ICE Introduction

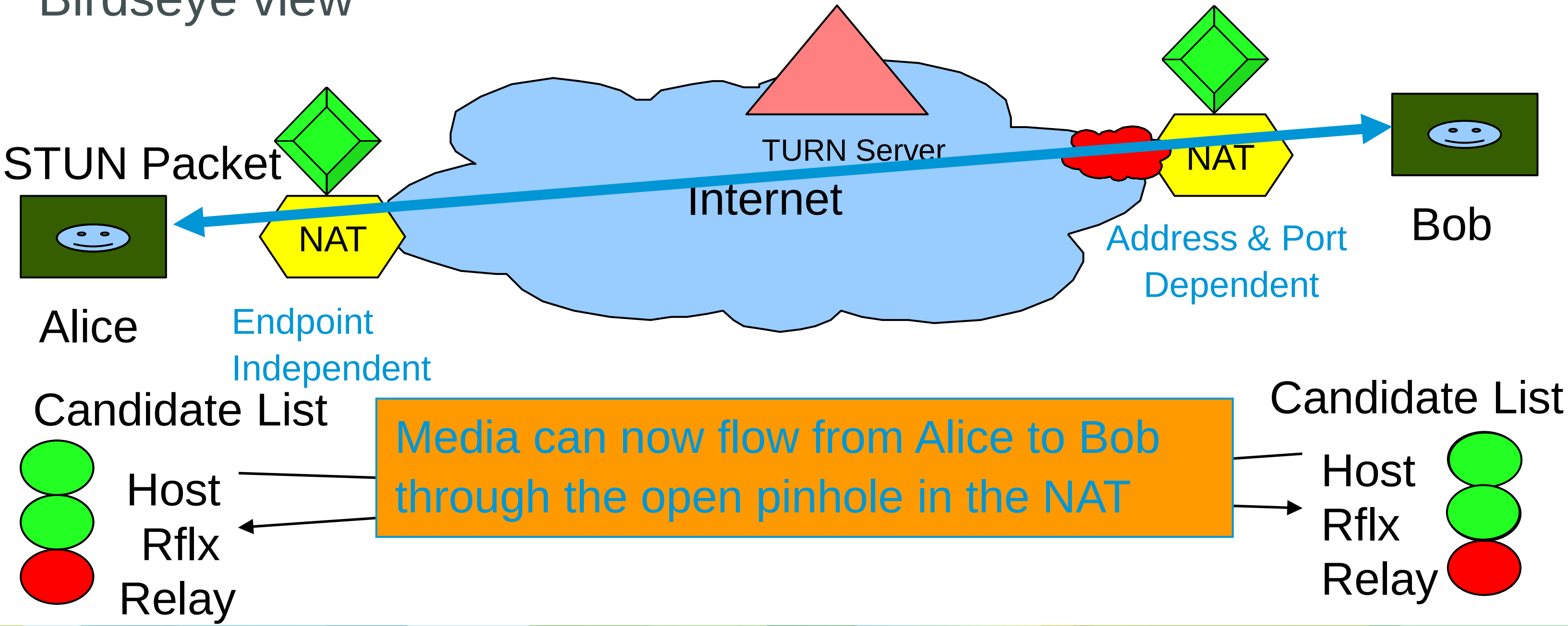
- ICE Connectivity Checks



ICE Introduction

- ICE Connectivity Checks
  - ✓ Birdseye view

If no NAT pinhole is possible, media will be sent through the TURN server.



Media can now flow from Alice to Bob through the open pinhole in the NAT

ICE Call Setup Sequence

To understand ICE better, below is a sequence of events in a ICE call:

1. Contact TURN server to allocate a TURN port and discover the reflexive address (outside global address)

2. Send INVITE with host, reflexive and relay candidate for each media line

3. Receive OK with host, reflexive and relay candidate for each media line from far end

4. Endpoints will now try establishing media on the default candidate (as the SDP will use that IP/Port in the offer)

5. ICE connection tests will start hammering through the (potential) firewall, and detect the best media path. This is done by sending STUN bind requests/responses between all the candidates (9 for each media line). As soon as we receive the bind response on a media line, we stop for this media line.

6. When ICE is done, we will send a re-INVITE with the RTP/RTCP ports from the best candidate pair, and also update the ICE media lines with the selected pair.

7. If only the relay address was reachable, we will send media through the TURN server

8. If relay was not necessary we will send an allocation request with time out=0 to release the TURN allocation

ICE Example: Configuration

- To use ICE, a TURN server needs to be available. VCS Expressway has a built-in TURN server. This server will be used to detect the ”public” IP address of the endpoint, and to allocate a TURN port if needed in the call. If a firewall is blocking communication directly between the two clients, the media will need to traverse the TURN server.

- For each call, the endpoint will contact the TURN server to allocate port and receive its reflexive IP address. If the endpoint gets no response from the TURN server, it will time out and place the call offering only the host address.

- To configure ICE:

- xConfiguration SIP Profile 1 Turn Server: ”IP_OF_TURN_SERVER”
  xConfiguration SIP Profile 1 Turn UserName: ”username”
  xConfiguration SIP Profile 1 Turn Password: ”password”
  xConfiguration SIP Profile 1 Ice: On

- Xstat: ICE will be useful at all times. If not in a call, it will provide the connection to the TURN server (if active). When in a call it will report the IP addresses in use (local and remote)

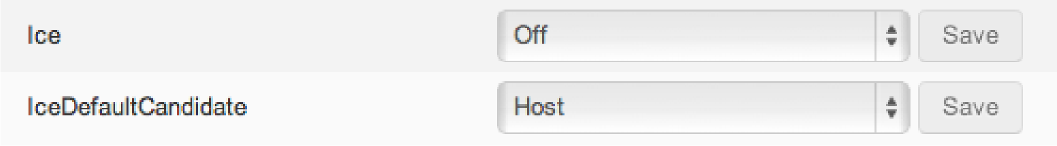
ICE Configuration

SIP ICE Paramters API:

xConfiguration SIP Profile [1..1] Ice: <Off/On>

xConfiguration SIP Profile [1..1] IceDefaultCandidate: <Host/Rflx/Relay>

SIP ICE Web:



SIP ICE TURN Server API:

xConfiguration SIP Profile [1..1] Turn Server: <S: 0, 255>

xConfiguration SIP Profile [1..1] Turn UserName: <S: 0, 128>

xConfiguration SIP Profile [1..1] Turn Password: <S: 0, 128>

SIP ICE TURN Server Web:

ICE – Nice To Know

- If ICE negotiation takes some time, the user may be left with no incoming media for a while in the beginning of the call. Negotiating the ports takes place as soon as the call is accepted (200 OK), and it may typically take 2-3 seconds to do all the connectivity checks, decide the connection tuples and re-INVITE with the decided ports.

- If ICE negotiation takes more than 5 seconds, the endpoint will default to Relay

- To force the media to go through the TURN server immediately it is possible to set the TURN relay as default media candidate: xConfiguration SIP Profile [1..1] IceDefaultCandidate: <Host/Rflx/Relay>

- This will put the Relay in the RTP address of the first INVITE, so the media should flow through immediately (unless there is a problem reaching the TURN server from either side). When the ICE decision is made, the media will be moved to the address/ports.

- When ICE is turned on the endpoint will show this explicitly in the Contact header:

    Contact: <sip:jrandby.c40@lys.cisco.com;gr=urn:uuid:ffed6f54-5611-5958-a951-5b51a5d5cf14>;**sip.ice=TRUE**

Example: xstatus ICE

- Xstat ICE in idle

  *s ICE Configured: "On”

  *s ICE Defaultcandidate: "Host"

  *s ICE Turn IP: "10.47.12.43:3478”

  *s ICE Turn Hostname: "lys-turn-stun.rd.cisco.com"

  *s ICE Turn Username: "turnuser”

- Xstat ICE. Call Successful

  *s ICE Configured: "On"

  *s ICE Defaultcandidate: "Relay"

  *s ICE Turn IP: "10.47.12.43:3478"

  *s ICE Turn Hostname: "lys-turn-stun.rd.cisco.com"

  *s ICE Turn Username: "turnuser"

  *s ICE Call 7 Result: **"Passed"**

  *s ICE Call 7 Local Candidate: "HOST"

  *s ICE Call 7 Local IP: "10.54.75.19"

  *s ICE Call 7 Remote Candidate: "HOST"

  *s ICE Call 7 Remote IP: "10.54.75.33”

- Xstat ICE. Call Failed

  *s ICE Configured: "On"

  *s ICE Defaultcandidate: "Host"

  *s ICE Turn IP: "10.47.12.43:3478"

  *s ICE Turn Hostname: "turn.qa.rd.cisco.com"

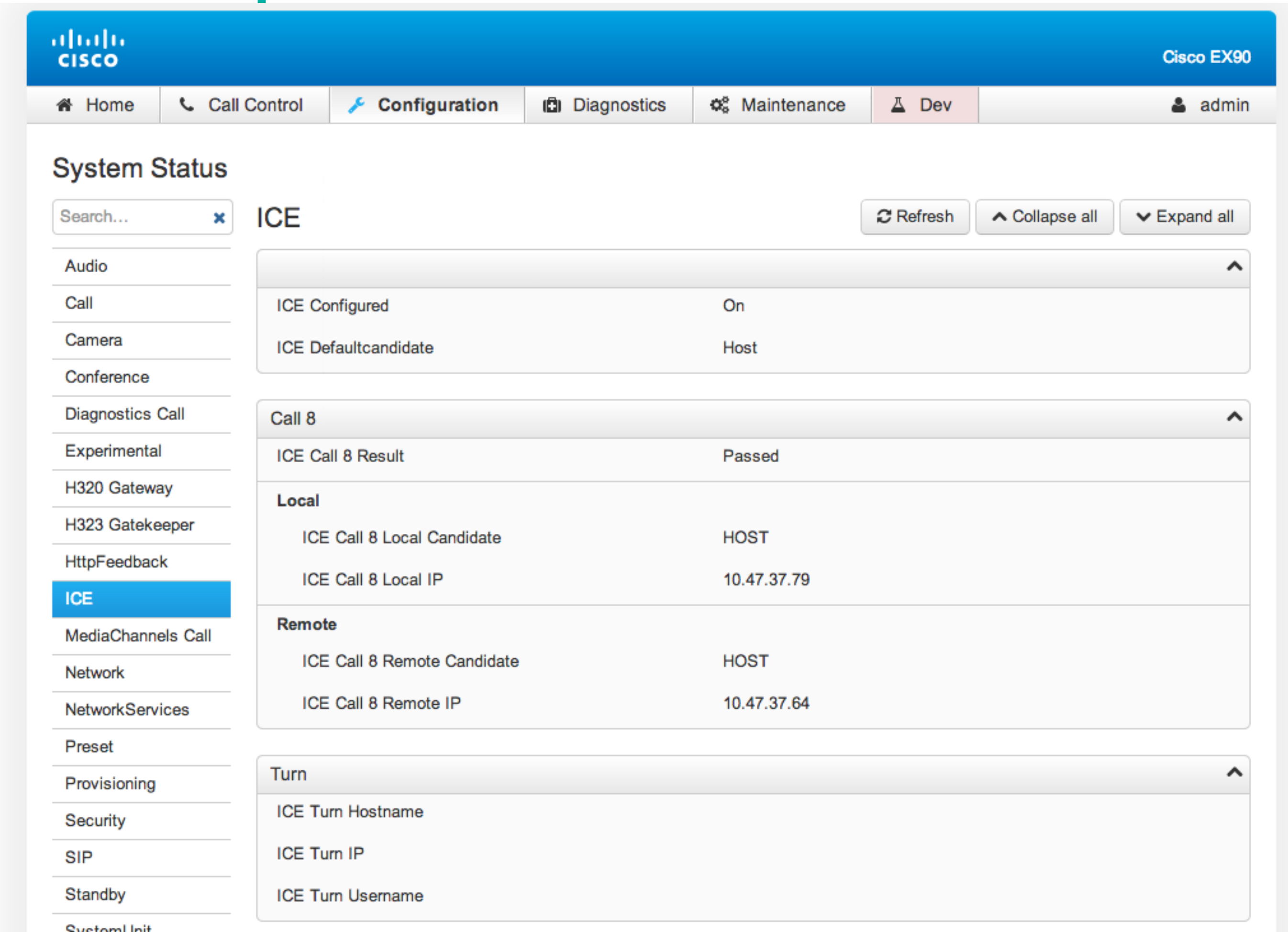
  *s ICE Turn Username: "turnuser"

  *s ICE Call 57 Result: **"Failed"**

  *s ICE Call 57 Local Candidate: "x"

  *s ICE Call 57 Local IP: "10.47.38.143"

Example: ICE Status



- ICE status on the web
- Same call on xstat ICE:
  - *s ICE Configured: "On"
  - *s ICE Defaultcandidate: ”Host"
  - *s ICE Turn IP: "10.47.12.43:3478"
  - *s ICE Turn Hostname: "lys-turn-stun.rd.cisco.com"
  - *s ICE Turn Username: "turnuser"
  - *s ICE Call 8 Result: "Passed"
  - *s ICE Call 8 Local Candidate: "HOST"
  - *s ICE Call 8 Local IP: "10.47.37.79"
  - *s ICE Call 8 Remote Candidate: "HOST"
  - *s ICE Call 8 Remote IP: "10.47.37.64”

ICE Pre-Requisites And Limitations

- Both endpoints in the call need to be ICE enabled and configured with a valid TURN server and credentials to allocate a relay port
    - Registration: Check TURN server connectivity (UDP, TLS, TCP)
    - Per call: Allocate relay port on TURN server (This will also discover Rflx address (Public side NAT IP address and port)
- Active Control (IX) is not supported with ICE:
    - xConfiguration Experimental Conference 1 ActiveControl Mode: Off
- ANAT (Applies Dual Stack Call protocol mode) SDP will have both an IPv4 and IPv6. (AS-SIP) must be turned Off (default Off)
- Not supported by CUCM until CUCM Release 10 (registration will work but calls will fail)
    - CUCM < 9 strips away all unkonwn elements from SIP Message

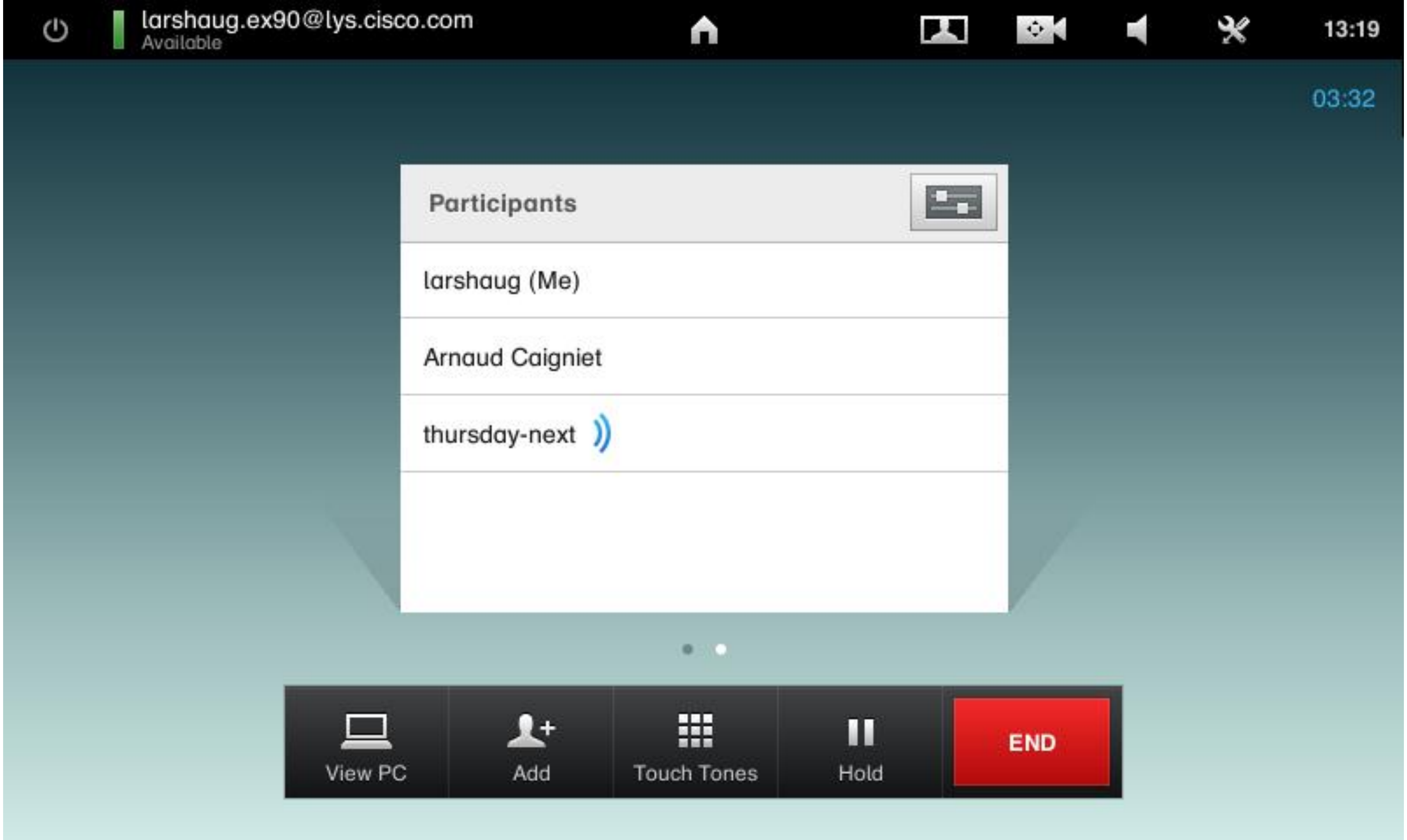
Conference Control

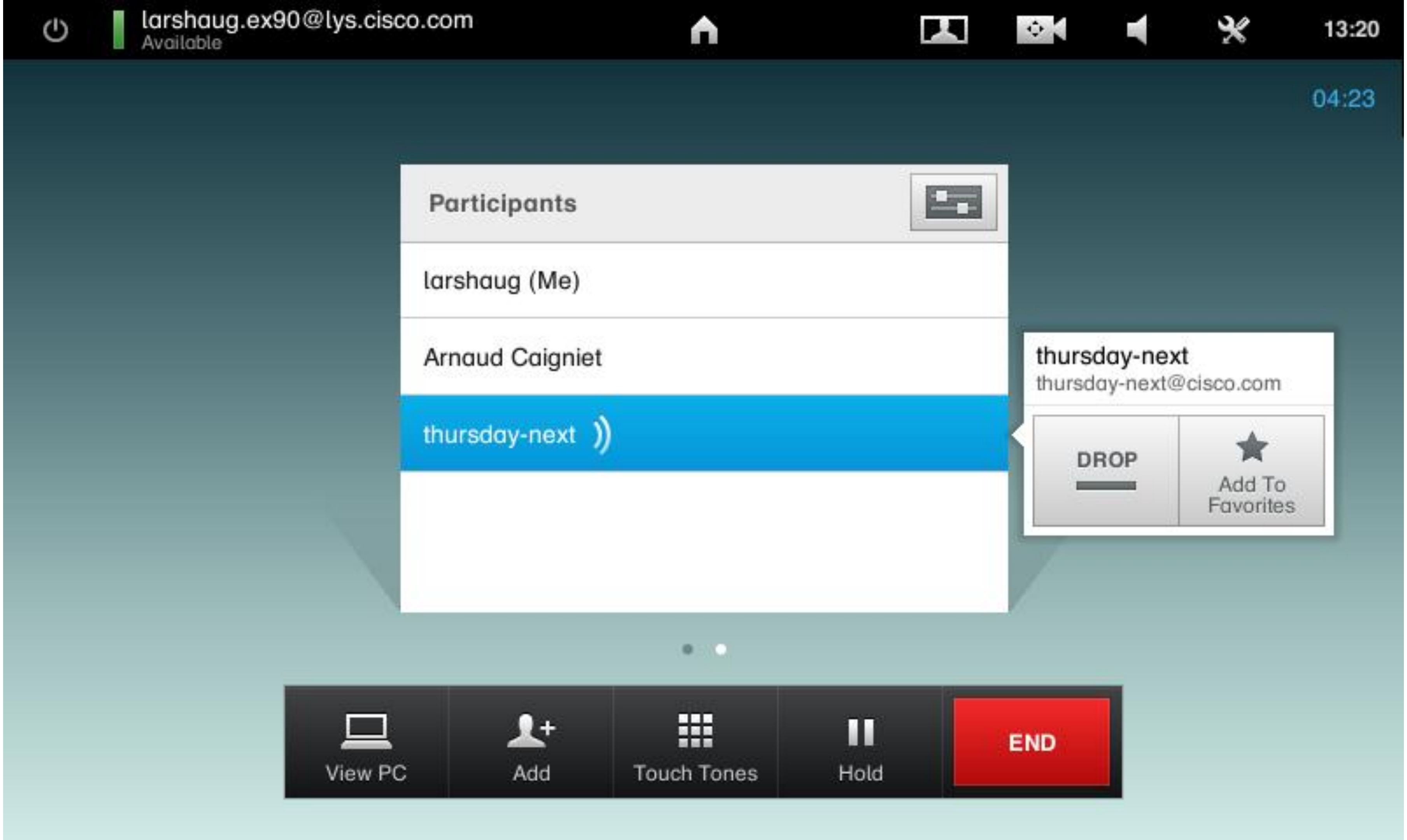
- Active control is a feature that will help conference participants administer a conference on TelePresence Server from the touch panel
- This is achieved with a new protocol: XCCP (eXtensive Conference Control Protocol) which is Cisco proprietary
- XCCP is signaled through “iX” which is a meta-protocol signaled in the SIP SDP. iX is designed to allow future extensions to use the same media line:
    - 88249.70 SipPacket m=application 5170 UDP/UDT/IX *
    - 88249.70 SipPacket a=ixmap:0 ping
    - 88249.70 SipPacket a=ixmap:2 xccp

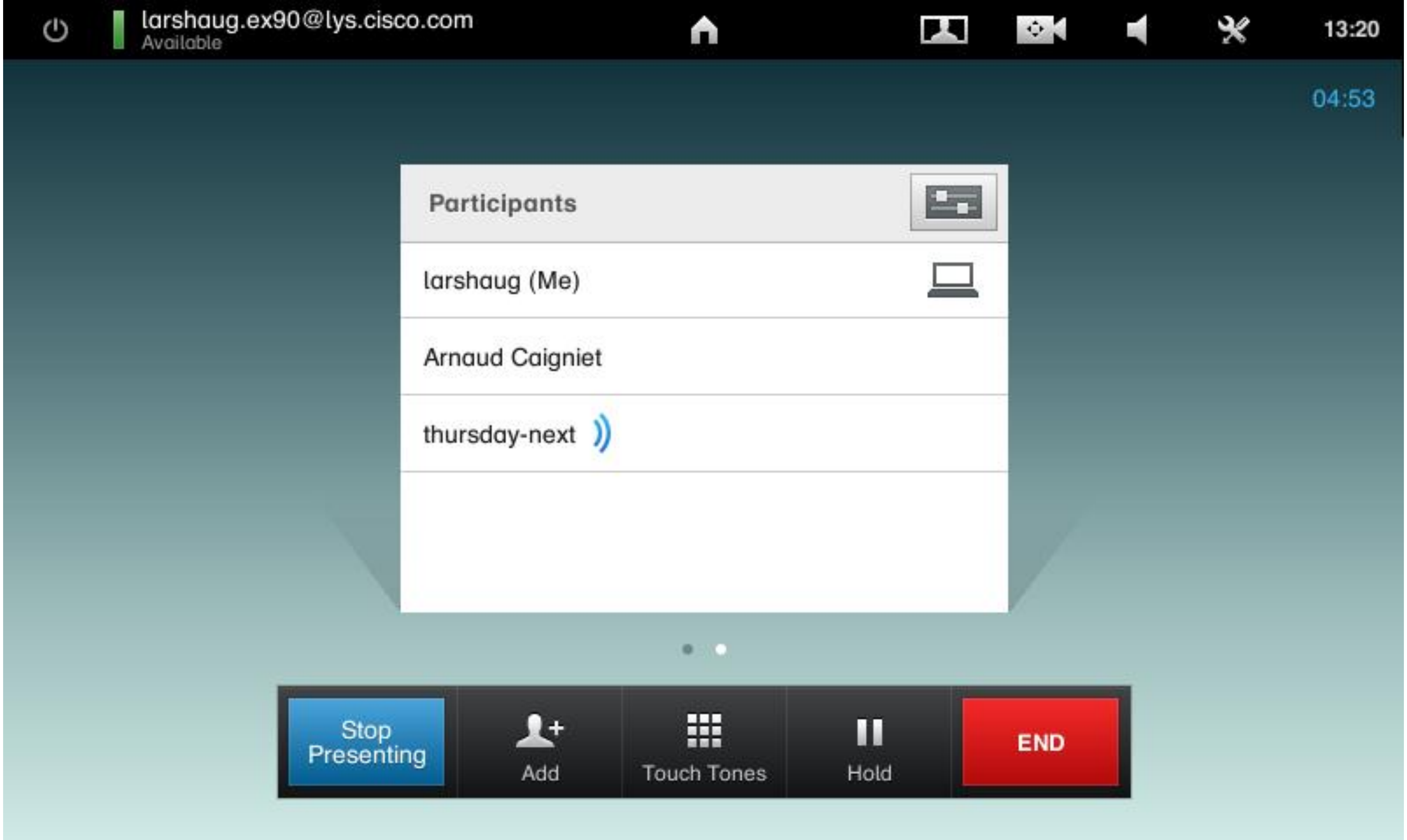
This shows that the data will be sent on UDP 5170 and it supports ix “Ping” and XCCP

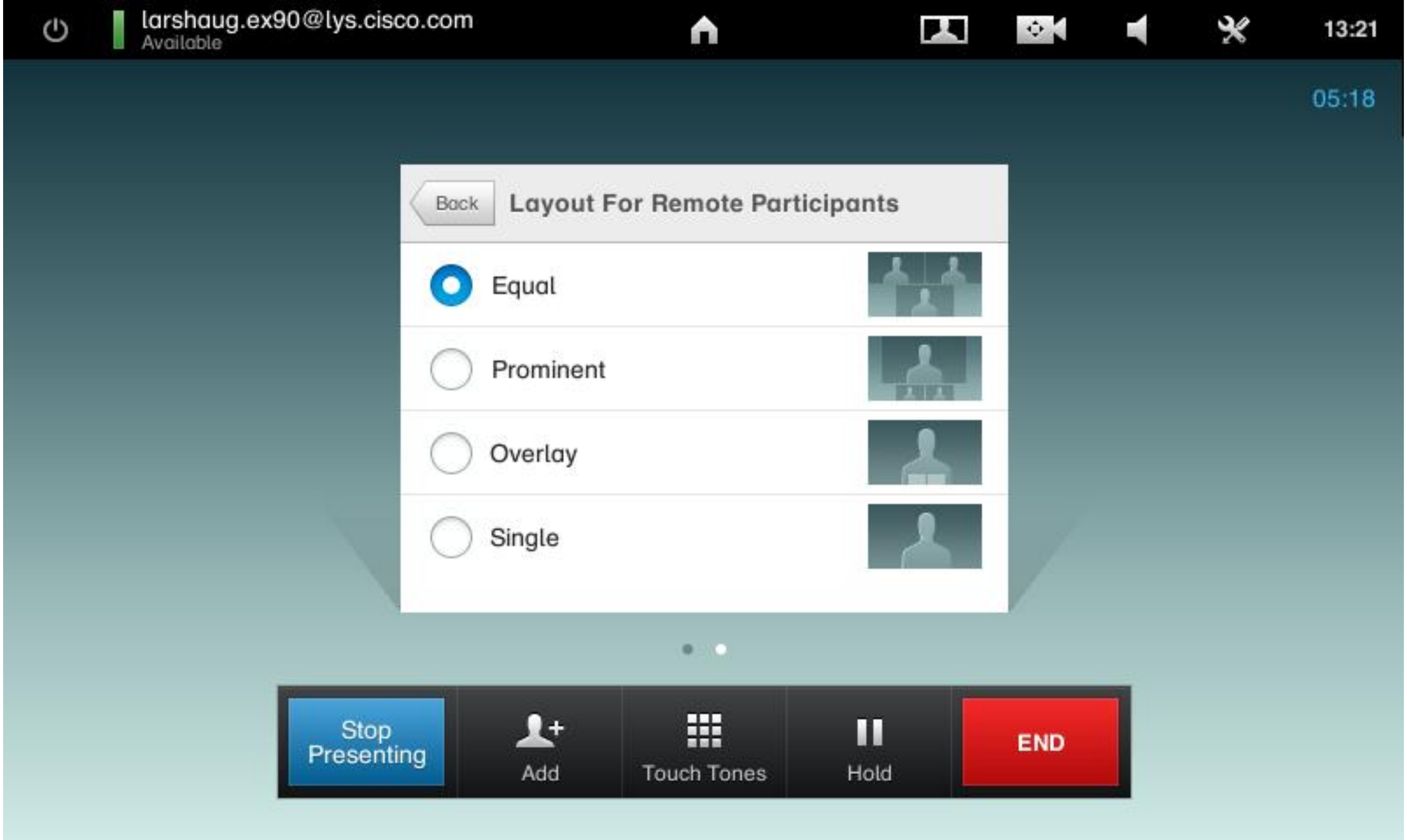
Conference Control

- Features in phase 1:
  - Participant lists → Friendly name and caller id)
  - Change layout locally → Applies to Main video channel only. When presentation is active, the layout will only select where to put main/presentation.
  - Conference information → Name of the conference
  - Mute remote participant → This feature will be added in TC6.3
  - Disconnect remote participant
  - See who is active speaker → An icon will appear next to the speaker in the participant list
  - See who is presenting → A PC icon will appear next to the speaker in the participant list


larshaug.ex90@lys.cisco.com
Available
13:19
03:32
Participants
larshaug (Me)
Arnaud Caigniet
thursday-next
View PC
Add
Touch Tones
Hold
END


larshaug.ex90@lys.cisco.com
Available
13:20
04:23
Participants
larshaug (Me)
Arnaud Caigniet
thursday-next
thursday-next
thursday-next@cisco.com
DROP
Add To Favorites
View PC
Add
Touch Tones
Hold
END


larshaug.ex90@lys.cisco.com
Available
13:20
04:53
Participants
larshaug (Me)
Arnaud Caigniet
thursday-next
Stop Presenting
Add
Touch Tones
Hold
END


larshaug.ex90@lys.cisco.com
Available
13:21
05:18
Back
Layout For Remote Participants
Equal
Prominent
Overlay
Single
Stop Presenting
Add
Touch Tones
Hold
END

Limitations And Requirements

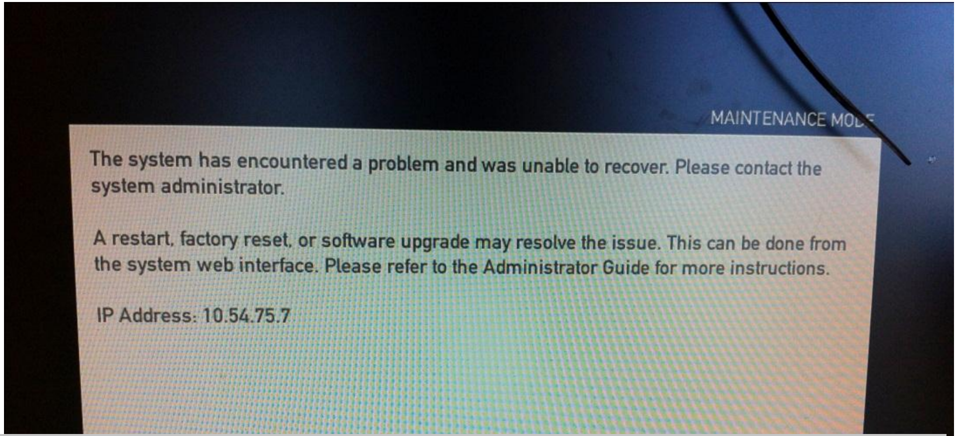
- Requires TC6.2 or later
- Requires TelePresence Server 3.1 or later
- Requires TelePresence Touch 8, no support for OSD
- No TelePresence MCU support
- SIP only feature. H323 interworking scenarios are not supported.

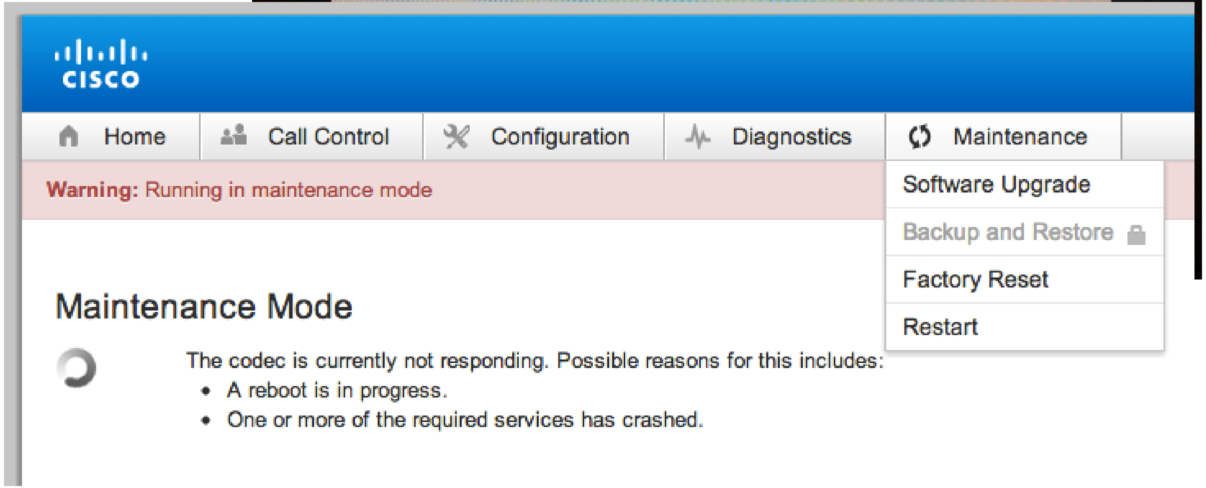
Configuring Conference Control

- In TC6.2, Conference Control is enabled by default so no configuration is necessary
- Conference Control support is signaled in the SDP as a media line

Maintenance mode

- New in TC6.2: OSD is showing IP address if on all systems when in Maintenance mode
- Factory reset should only be performed after collecting all information possible! (Logs)






```
Johans-MacBook-Pro:~ jrandby$ ssh admin@10.54.75.7
Password:
Welcome to the Cisco Telepresence maintenance shell.
Type 'help' or '?' for help.
?
          - User Commands -

help          factoryreset pkgverify    selectsw      reboot
rootsettings log
OK
version
TC6.1.0 Beta3 cc55cc4
Revision:tc-6.1.0-beta3-0-gcc55cc4
```

Known Limitations & Bug Fixes

Known Issues And Bugs

- When downgrading from TC6.2.0 to lower versions than 6.1.0 a network paired touch panel needs to be re-paired due to the encrypted file system on the touch panel
- No provisioning of endpoint SIP URI in CUCM 9.0
- A list of open and resolved bugs and known issues are always found in the release notes

Thank you.