

CISCO *Live!*



#CiscoLive



The bridge to possible

Enabling Collaboration for Your Remote Workforce with Cisco Expressway

Part II

Luis Garcia
BRKCOL-2060b



#CiscoLive

Cisco Webex App

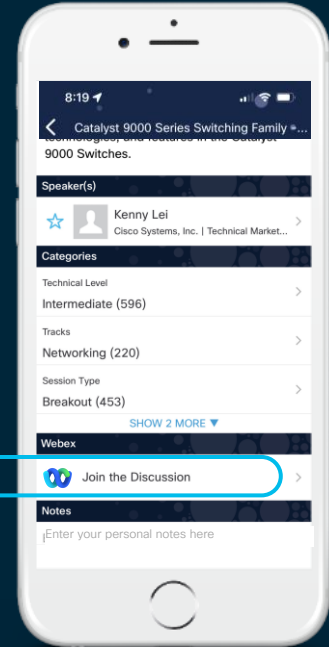
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2060b>



Agenda

- Introduction
- SIP-Base DoS Attack Protection
- SIP Registration Failover for Soft Clients
- Webex UCM Calling Enhancement
- IPv6 Support
- Serviceability Enhancements
- Conclusion

Introduction

Introduction

Watch My Session

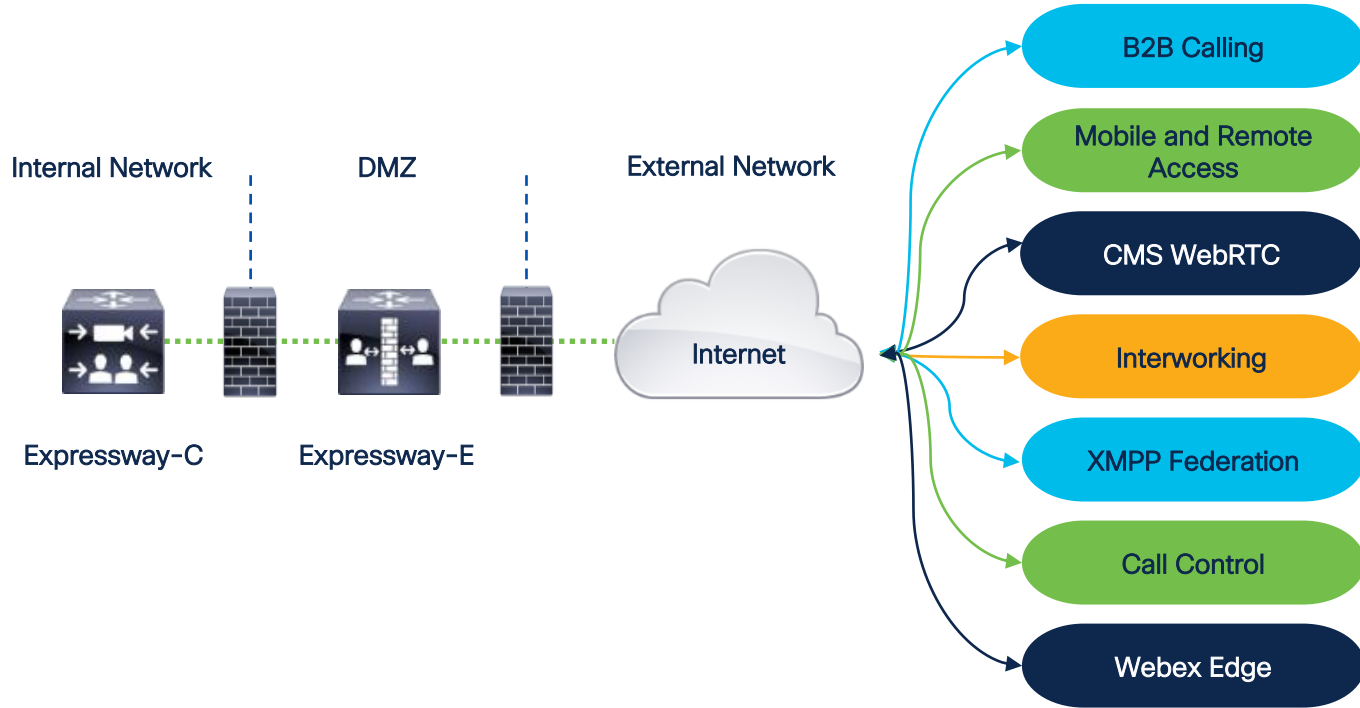
Enabling Collaboration
for your Remote
Workforce with Cisco
Expressway - Part 1

Speaker: Luis Garcia

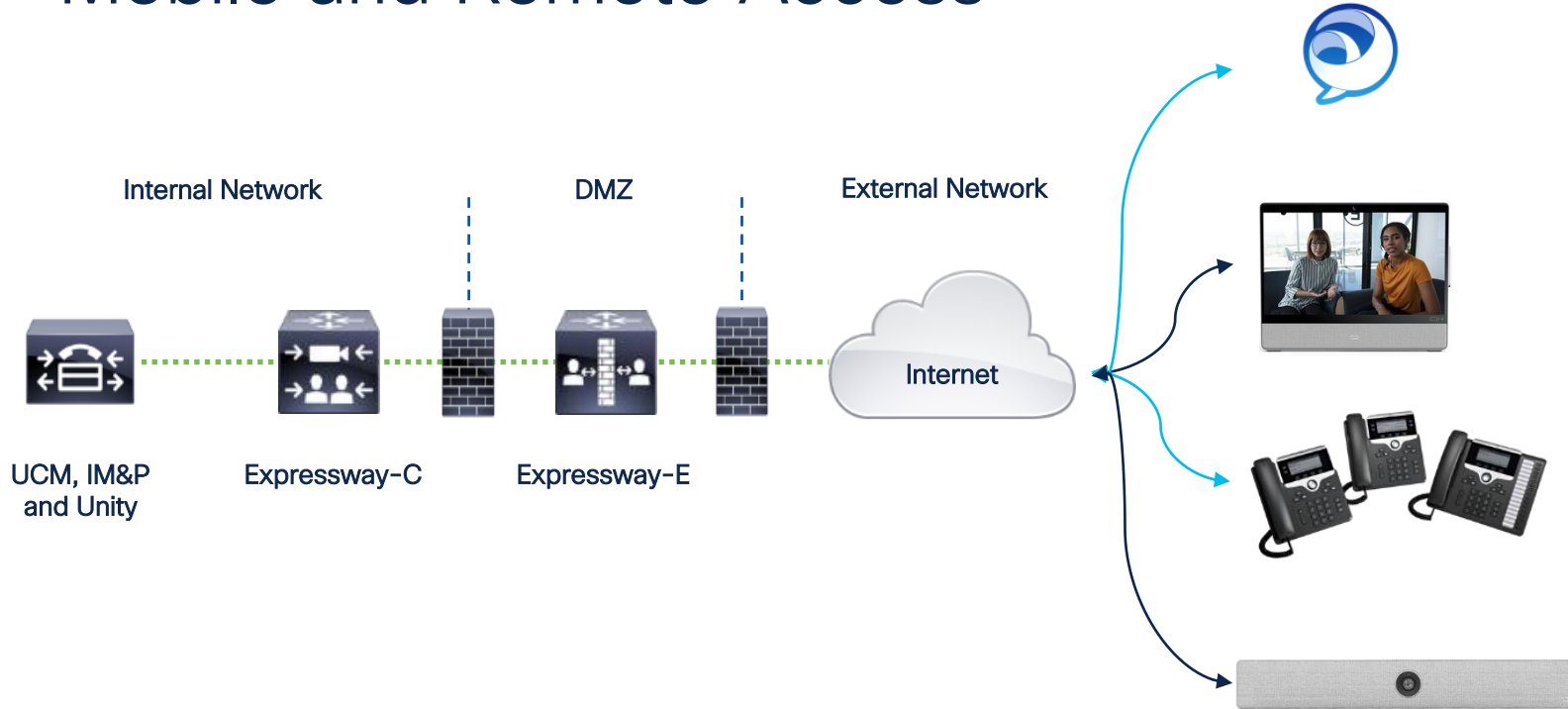
BRKCOL-2060a



Expressway Deployments



Mobile and Remote Access



X14 Upgrade Benefits



Security

The #1 priority for each release



Resilience

Registration failover



User Experience

Webex App Enhancements



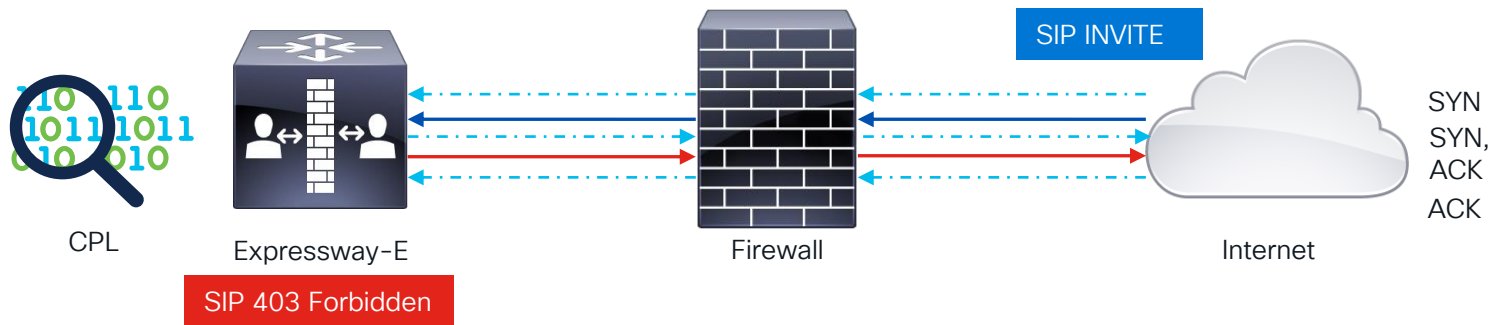
Serviceability

Improved operational efficiencies

SIP-Base DoS Attack Protection



SIP-Base DoS Attack Protection - Pre-X14



Spam Calls - Toll Fraud attempt

Applications > Users > Maintenance >

Search type	Source	Destination	SIP variant	Status
SIP (INVITE)	22229@vcse1.ucdemolab.com	sip:9000046812400810@vcse1.ucdemolab.com	Standards-based	Forbidden
SIP (INVITE)	22229@guest.ucdemolab.com	sip:9000046812400810@guest.ucdemolab.com	Standards-based	Forbidden
SIP (INVITE)	22229@jabber.guest.ucdemolab.com	sip:9000046812400810@jabber.guest.ucdemolab.com	Standards-based	Forbidden
SIP (INVITE)	22229@exp-e04.ucdemolab.com	sip:9000046812400810@exp-e04.ucdemolab.com	Standards-based	Forbidden
SIP (INVITE)	22229@vcse1.ucdemolab.com	sip:946812400810@vcse1.ucdemolab.com	Standards-based	Forbidden

SIP-Base DoS Attack Protection - X14

- The “SIP Authentication Failure” category under System > Protection > Automated Detection, will now match against 403 Forbidden reason codes.

Status >	System >	Configuration >	Applications >	Users >	Maintenance >	? Help Logout
Automated detection overview			You are here: System > Protection > Automated detection > Configuration			
Category	Status	Currently blocked	Total failures	Total blocks	Exemptions	Action
<input type="checkbox"/> External API authorization failure	✔ On - Active	0	0	0	0	View/Edit View exemptions
<input type="checkbox"/> HTTP proxy authorization failure	✔ On - Active	0	0	0	0	View/Edit View exemptions
<input type="checkbox"/> HTTP proxy protocol violation	✔ On - Active	0	0	0	0	View/Edit View exemptions
<input type="checkbox"/> HTTP proxy resource access failure	Off	-	-	-	0	View/Edit View exemptions
<input type="checkbox"/> SIP authentication failure	✔ On - Active	0	0	0	0	View/Edit View exemptions

Category settings

→ Detection window (seconds)	★ 600	i
→ Trigger level	★ 5	i
→ Block duration (seconds)	★ 600	i

SIP-Base DoS Attack Protection - X14

- Web GUI shows an example of the log message that will trigger the protection.

Example log messages that trigger blocks in this category

```
tvcs: Event="Authentication Failed" Service="SIP" Src-ip="101.110.101.101" Src-port="5060" Detail="User not found" Protocol="TCP" Method="REGISTER" Level="1" UTCTime="2004-04-28 17:07:02,887"
tvcs: Event="Search Completed" Reason="Forbidden" Service="SIP" Src-ip="101.110.101.101" Src-port="5060" Src-alias-type="SIP" Src-alias="1000@cisco.com" Dst-alias-type="SIP" Detail="found:false, searchtype:OPTIONS, Info:Policy Response" Protocol="TCP" Level="1" UTCTime="2004-04-28 17:07:02,887"
```

Status (last updated: 00:48:42 EDT)

Service state	On - Active
Total blocks	2
Total failures	18



Address ▼

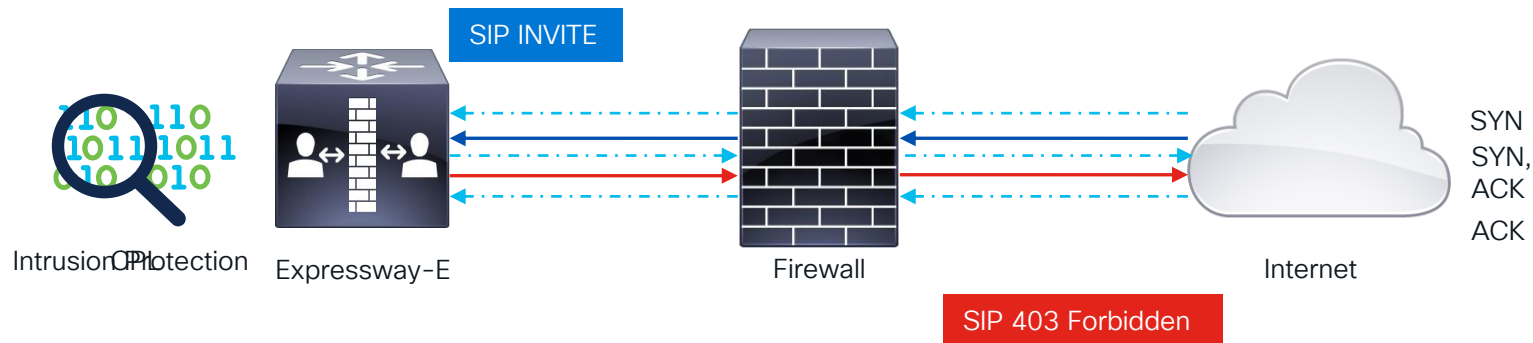
Time left until address is unblocked (last updated: 00:44:28 EDT)



128.107.83.84

9 minutes 59 seconds

SIP-Base DoS Attack Protection - X14



Exp-E will stop replying to any messages coming from an IP that is blocked.

SIP Registration Failure Detection

- The regular expression for “SIP registration failure” was updated to match more registration failures.
- All reasons for the event “Registration Rejected” will be matched.

Example log messages that trigger blocks in this category

tvcs: Event="Registration Rejected" Reason="Unknown domain" Service="SIP" Src-ip="101.110.101.101" Src-port="5060" Protocol="TCP" AOR="sip:bad_domain_xxxxx.int"

Status (last updated: 09:17:29 EDT)

Service state	On - Active
Total blocks	0
Total failures	0

Pre-X14

Example log messages that trigger blocks in this category

tvcs: Event="Registration Rejected" Reason=. * Service="SIP" Src-ip="101.110.101.101" Src-port="5060" Protocol="TCP" AOR="sip:bad_domain_xxxxx.int" C

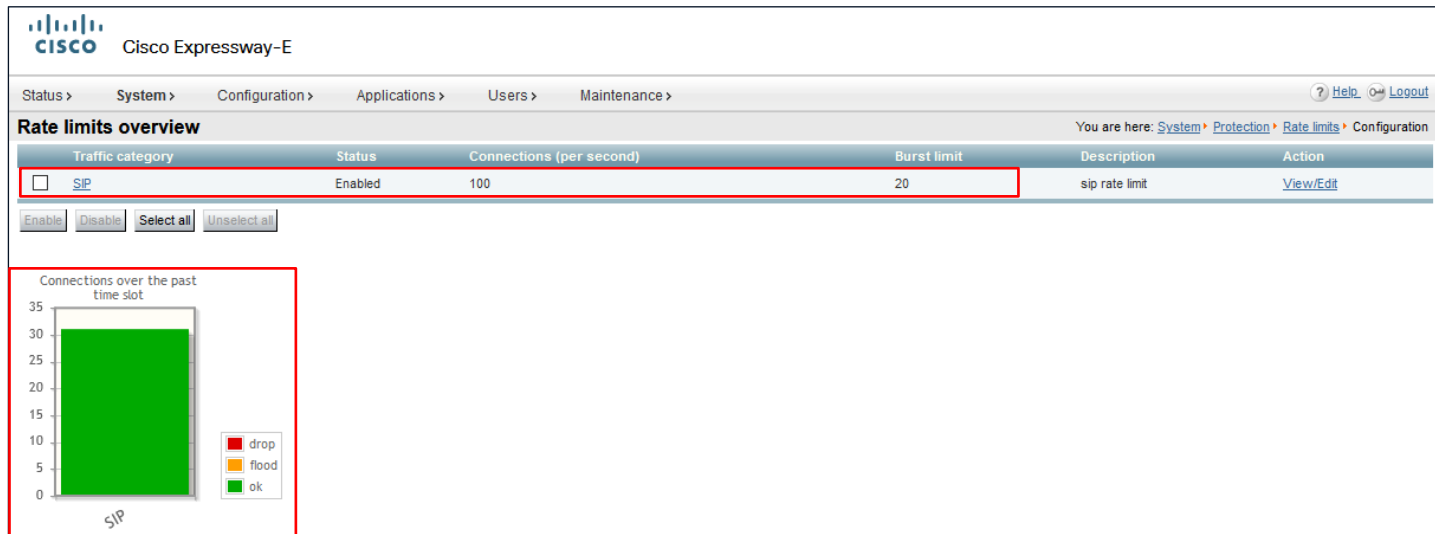
Status (last updated: 09:04:28 EDT)

Service state	On - Active
Total blocks	X14 0
Total failures	0

X14

Rate Limits for SIP

- SIP over TCP, only state NEW is considered as new connection.
- SIP over UDP, consider all the related and established connections as new connections.



Rate Limits for SIP

- Connections per second range value is from 1 to 150 and default value is 100.
- Burst limit range value is from 15 to 30 and default value is 20

Rate limits configuration

You are here: [System](#) > [Protection](#) > [Rate limits](#) > Rate limits configuration

Configure rate limits

Traffic category: SIP

Status: Enabled

Connections (per second): 100

Burst limit: 20

Description: sip rate limit

SIP Registration Failover



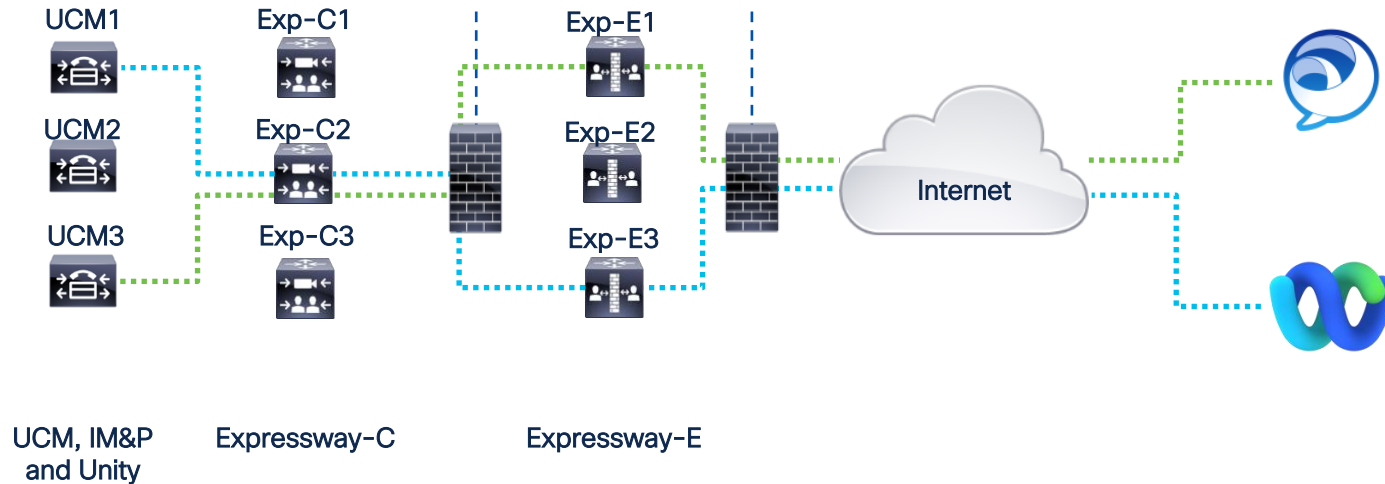
MRA SIP Registration Failover

Routing Feature	Minimum Release required
Adaptive Routing	<ol style="list-style-type: none">1. Expressway X12.7 (Feature Preview)2. Cisco Jabber 12.9 MR3. Cisco Webex App
STUN Keepalives	<ol style="list-style-type: none">1. Expressway X12.7 (Feature Preview)2. CUCM 143. Cisco Jabber 12.9 MR4. Cisco Webex App

These features are not supported for IP Phones or Webex devices using MRA.

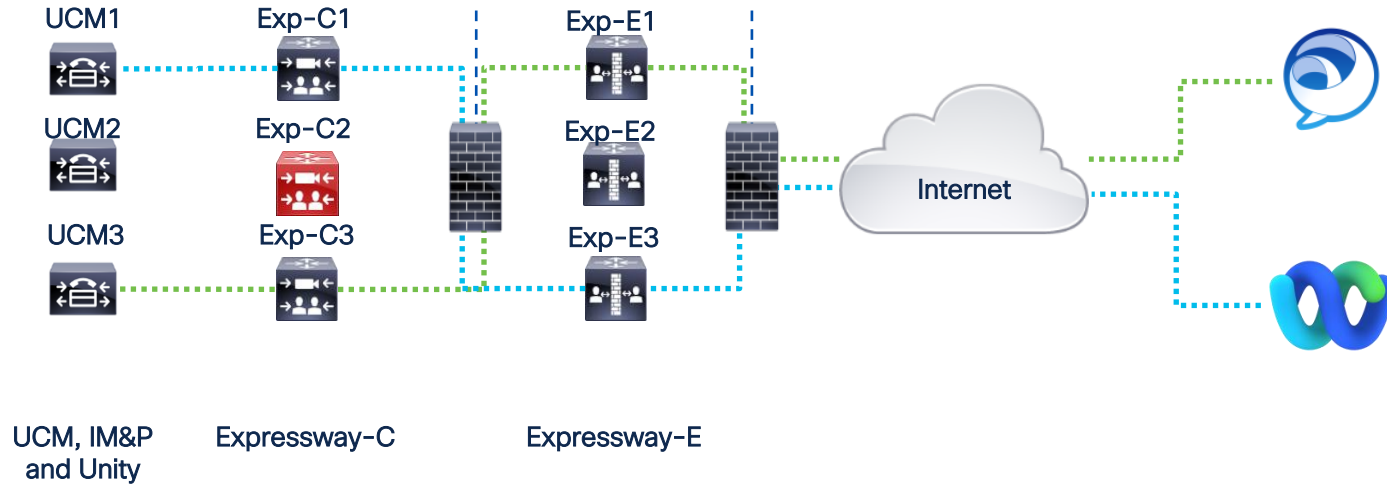
Adaptive Routing

Expressways can dynamically alter the routing path for SIP Registers when an Exp-C node is detected to be down.



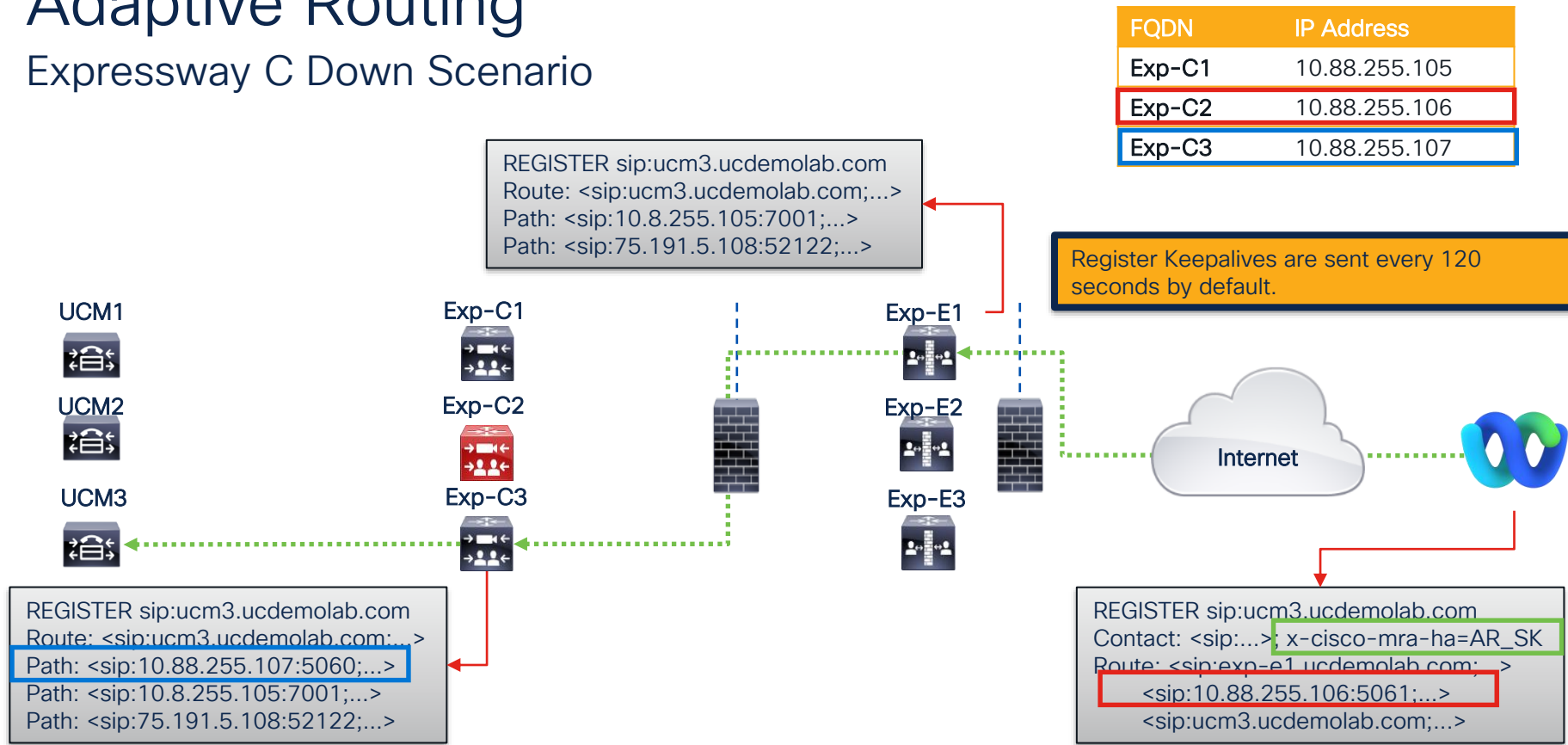
Adaptive Routing

Expressway C Down Scenario



Adaptive Routing

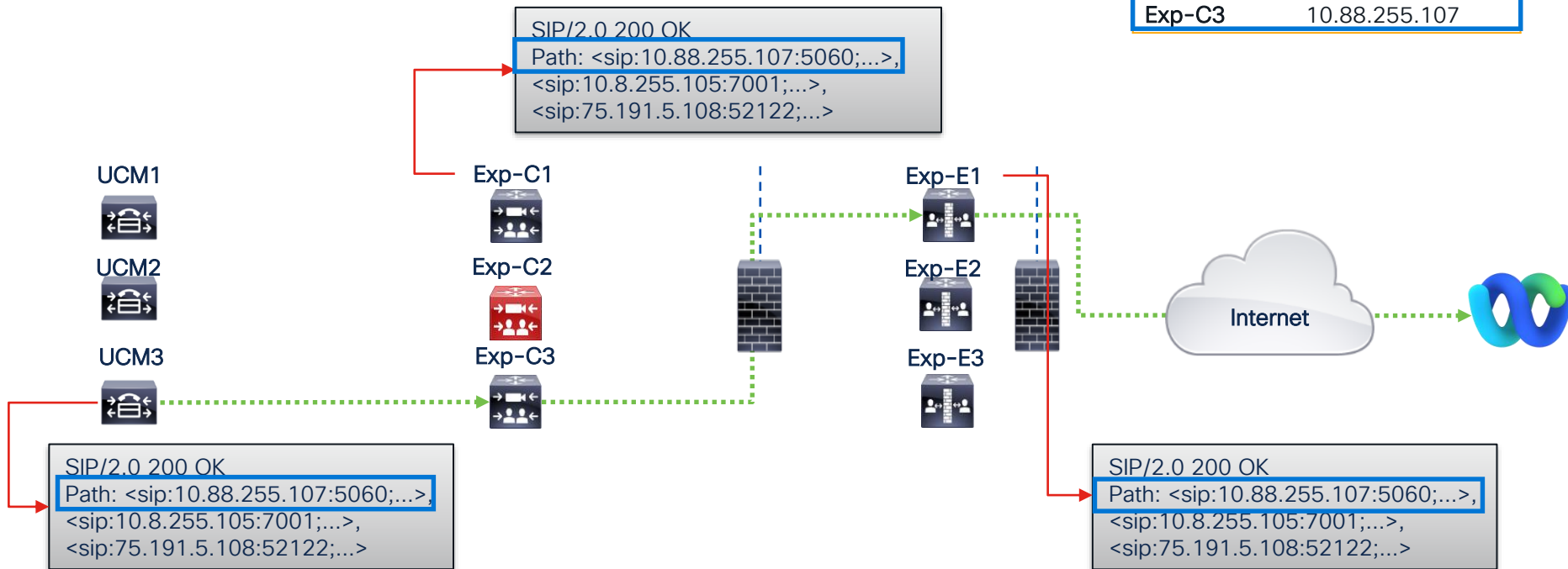
Expressway C Down Scenario



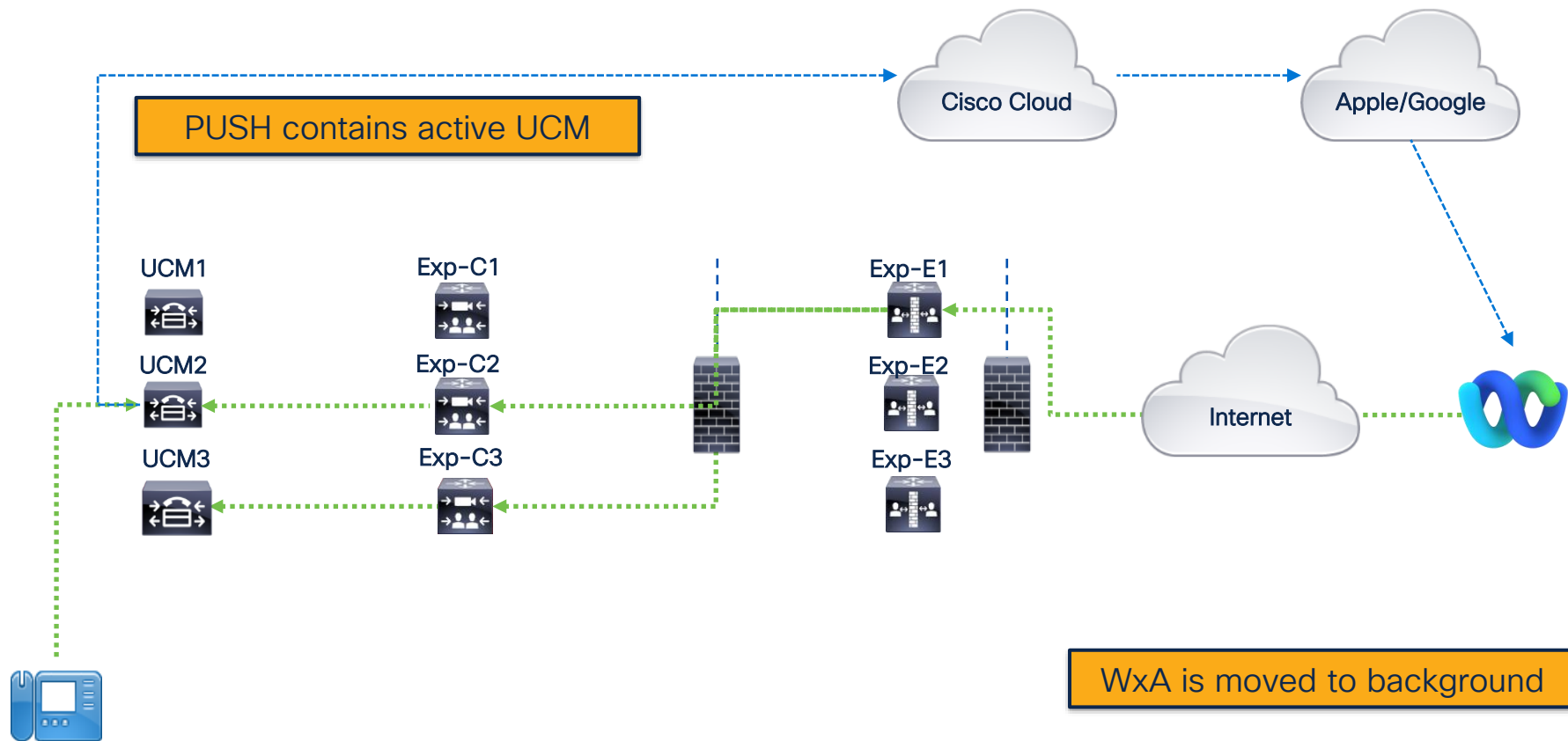
Adaptive Routing

Expressway C Down Scenario

FQDN	IP Address
Exp-C1	10.88.255.105
Exp-C2	10.88.255.106
Exp-C3	10.88.255.107



Adaptive Routing- APNS



STUN Keepalives

This is enabled from the Exp-C only, under Unified Communications > Configuration. Exp-E will automatically match the configuration of the Exp-C.

Exp-C

[See automatic inbound rules](#)

SIP Path headers	On ▾	
Credentials refresh interval (minutes)	 480	
Credentials cleanup interval (minutes)	 720	
Maximum authorizations per period	 0	
Rate control period (seconds)	 300	
STUN keepalive	On ▾	

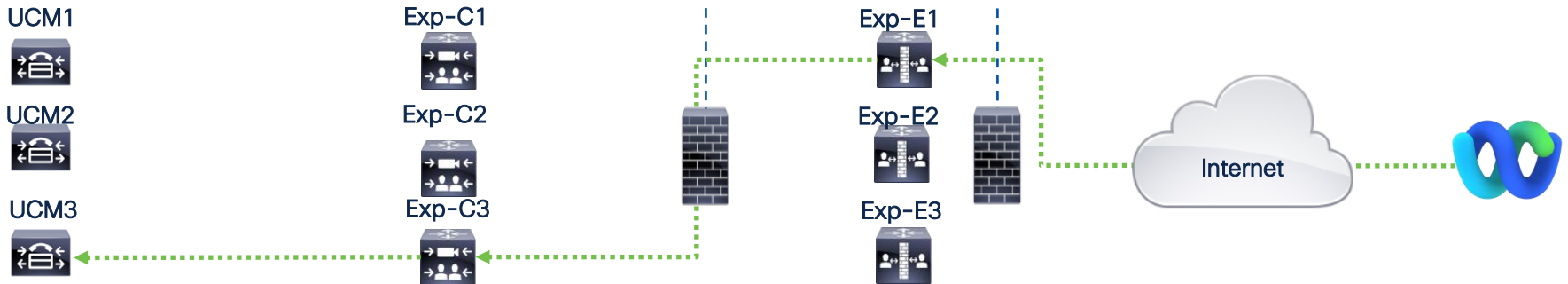
```
xconfig sip Advanced
*c xConfiguration SIP Advanced SipMaxSize: 32768
*c xConfiguration SIP Advanced SipTcpConnectTimeout: 1
*c xConfiguration SIP Advanced SipTlsDhKeySize: "1024"
*c xConfiguration SIP Advanced SipTlsVersions: "TLSv1.2"
*c xConfiguration SIP Advanced StunKeepAliveForRegisteredPathEnabled: On
```

Exp-E

STUN Keepalives

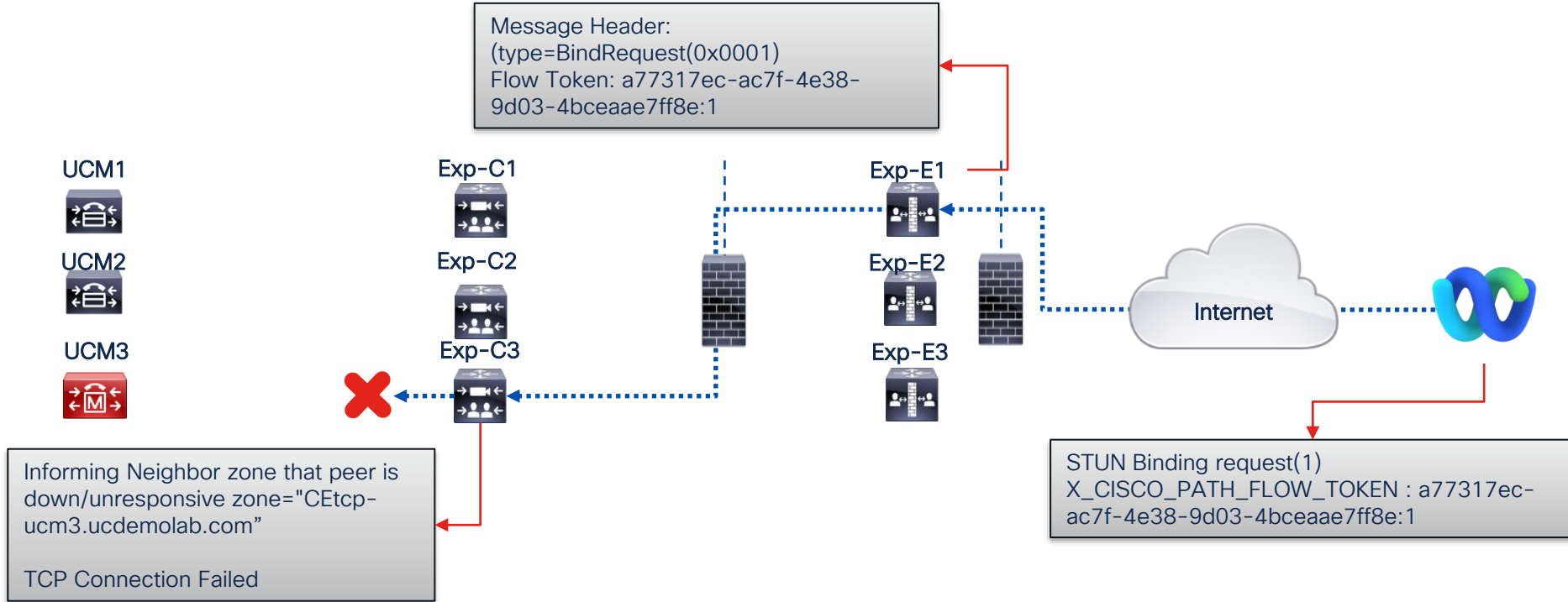
- Webex app and Jabber clients will send STUN Binding request messages to check the connection path.
- When running UCM 14 we can identify when a UCM node goes down.

STUN Keepalives are sent every 30 seconds.



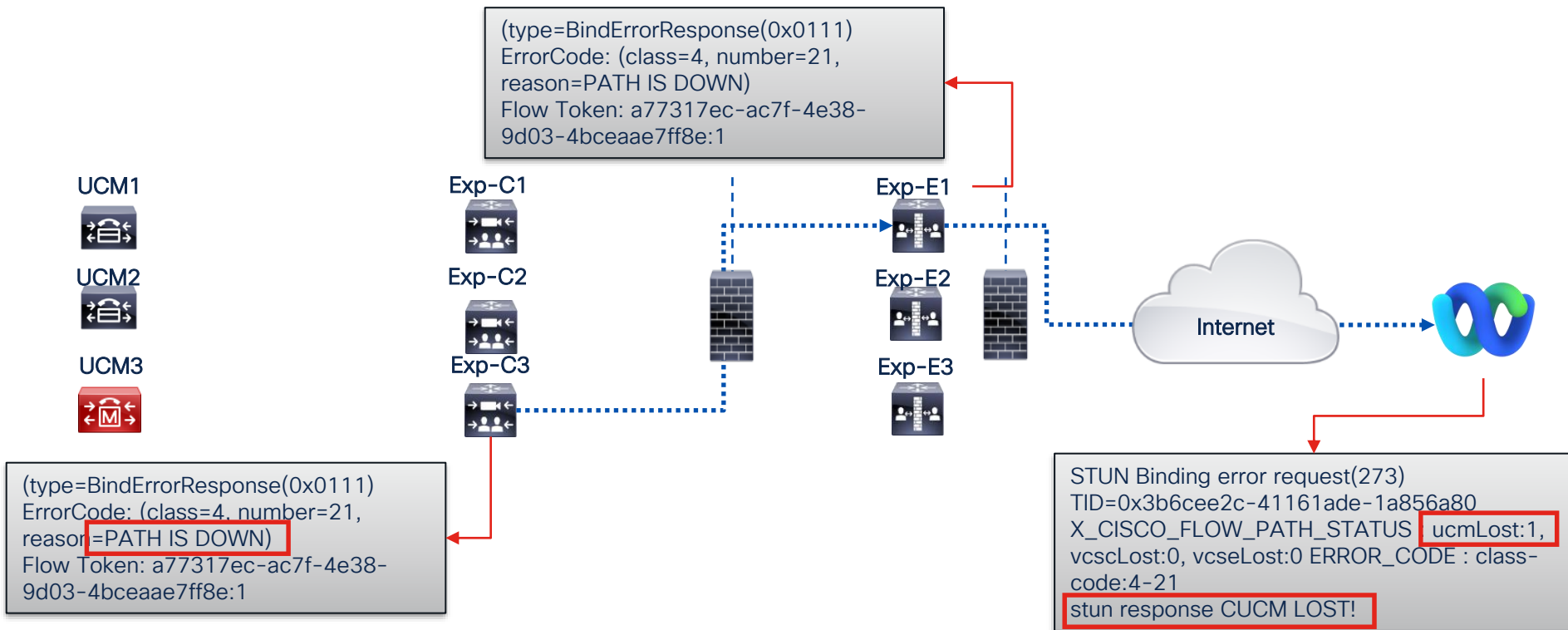
STUN Keepalives

UCM Down Scenario



STUN Keepalives

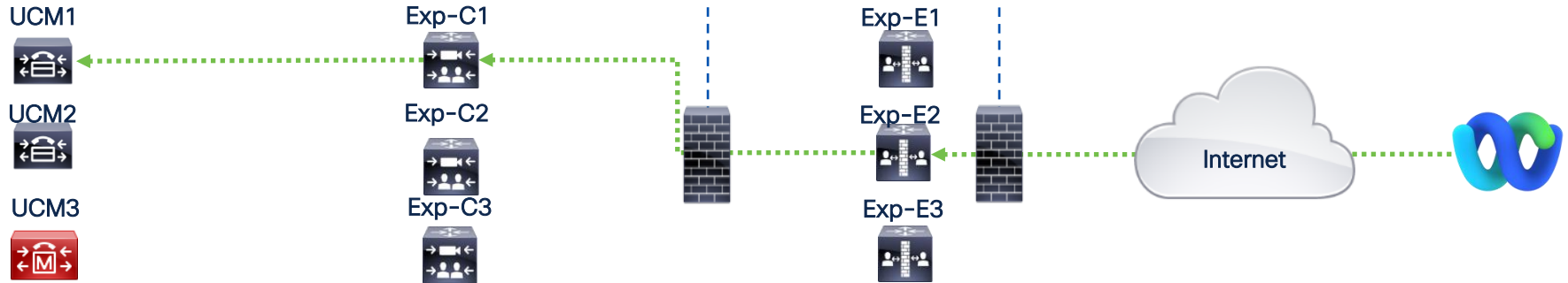
UCM Down Scenario



STUN Keepalives

UCM Down Scenario

- WxA or Jabber client will select a new SIP registration route and use it to failover to an active UCM server.



MRA SIP Registration Failover

✓ Benefits without UCM version 14:

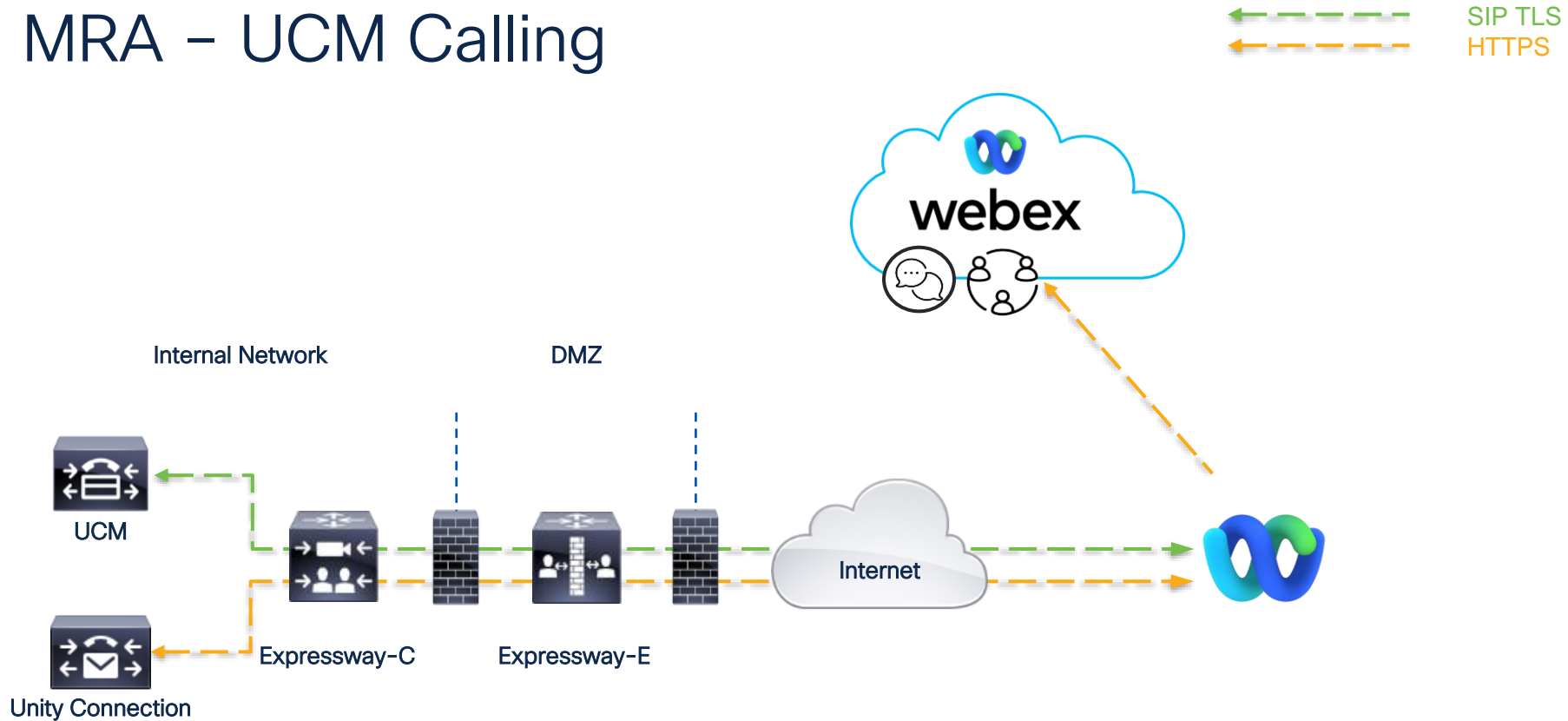
- Detection of UCM failure based on TCP timeout > 2 mins
- STUN Keepalives can detect Expressway failures
- Adaptive Routing selects an active Exp-C to prevent a Registration failure

✓ Benefits with UCM version 14:

- STUN KA allows a faster and more accurate detection of UCM failure (30 secs)

Webex App Enhancements

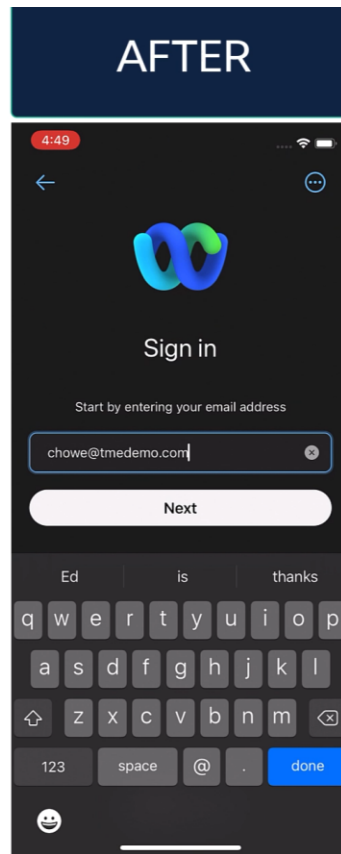
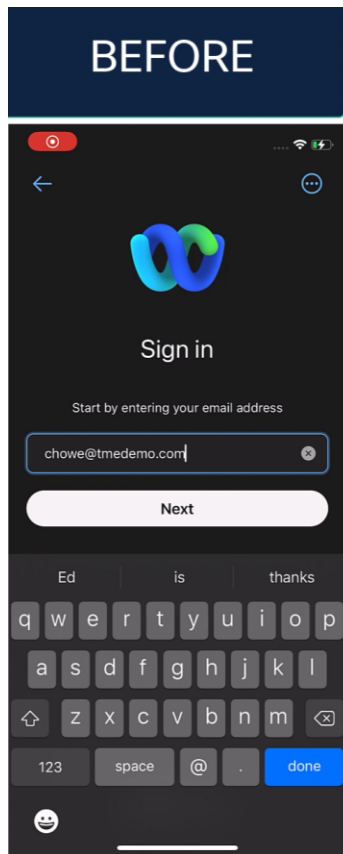
MRA - UCM Calling



Redirect URI for SSO/OAuth

- This feature enhances the security of Cisco Jabber/Webex Client embedded browser support with following benefits:
- Provides protection against "Authorization Code Interception Attack" using RFC7636
- Allows clients running on an Operating Systems other than iOS, to use the Embedded Browser (For example: Android)
- Allows Jabber and Webex client to use the Embedded browser for Unified Communications Manager (and MRA) OAuth flow.
- Improves the user experience when using Webex client and Unified Communications Manager Calling.

Redirect URI for SSO/OAuth



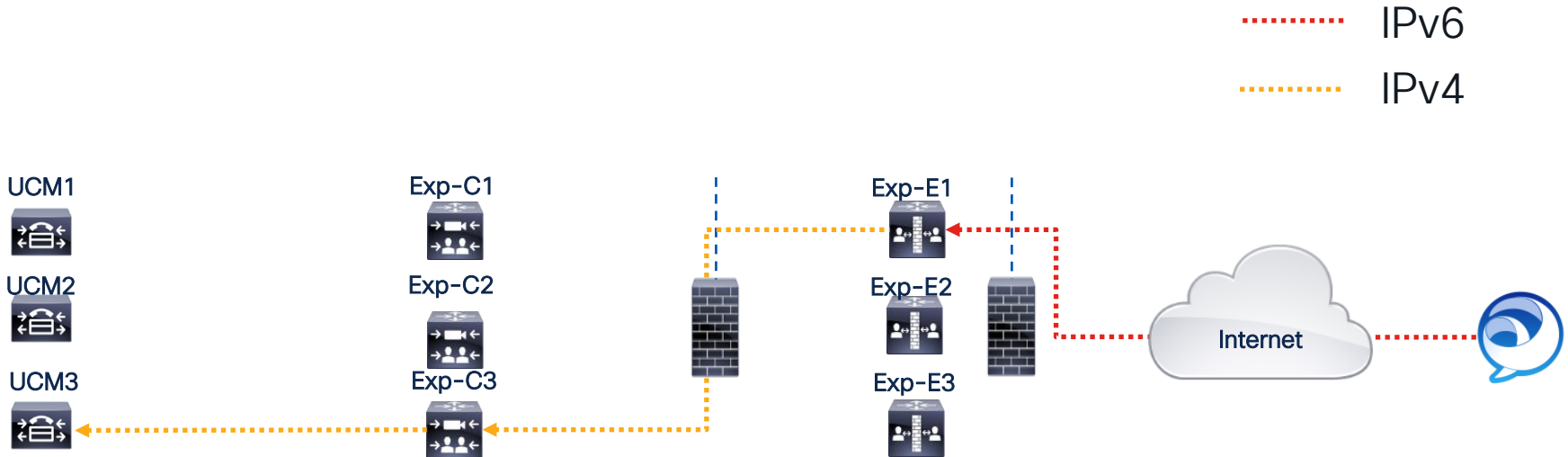
IPv6 Support



IPv6 Support – X14.2 Preview

X14.2 will support MRA Jabber clients using an IPv6 address. Exp-E is required to be setup in dual mode (IPv4/IPv6), Exp-C is setup as IPv4 only.

UCM servers need to be running in dual mode.



Serviceability Enhancements



System Key Recovery

- Clustering can fail and generate a “Failed to update system key” alert, to recover the system required a factory reset of the node showing the alert.
- New CLI command “`xcommand forcesystemkeyupdate`” allow us to recover from the error without a factory reset.

```
xstatus alarm
```

```
*s Alarm: /
```

```
1:      Description: "Failed to update system key file due to inconsistent state"  
      ID: "40055"
```

```
      Solution: "Restart the system. If that doesn't clear the problem, contact your Cisco  
representative"
```

```
      Title: "Failed to update key file"
```

```
xcommand forcesystemkeyupdate
```

```
OK
```

IP/Port Filter for tcpdump on Diagnostic Logging

- Filtering the packet capture will allow to prevent the pcaps from overwriting in a short period of time. We also increased the amount of data we collect from 40 MB per interface to 400 MB.

Diagnostic loggingYou are here: M

Logging status


Started logging at

Wednesday 17th of February 2021 05:35:08 PM (America/Los_Angeles) logging started by

Stopped logging at

Wednesday 17th of February 2021 05:36:24 PM (America/Los_Angeles)


Marker




Add marker

Take tcpdump while logging


☒



Filter tcpdump by address



Filter tcpdump by port



Start new log

Stop logging

Collect log

Analyze log

Conclusion



Highlights

- SIP DoS protections stops spam calls and toll fraud attempts.
- SIP Registration failover for Jabber and WxA takes only 30 seconds to discover failures in the SIP path when using UCM 14.
- WxA enhancements make it easier to use UCM Calling.
- Limited support for IPv6 when the infrastructure is IPv4.
- Serviceability enhancements help simplify the troubleshooting process.

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn



Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train



Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify



Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

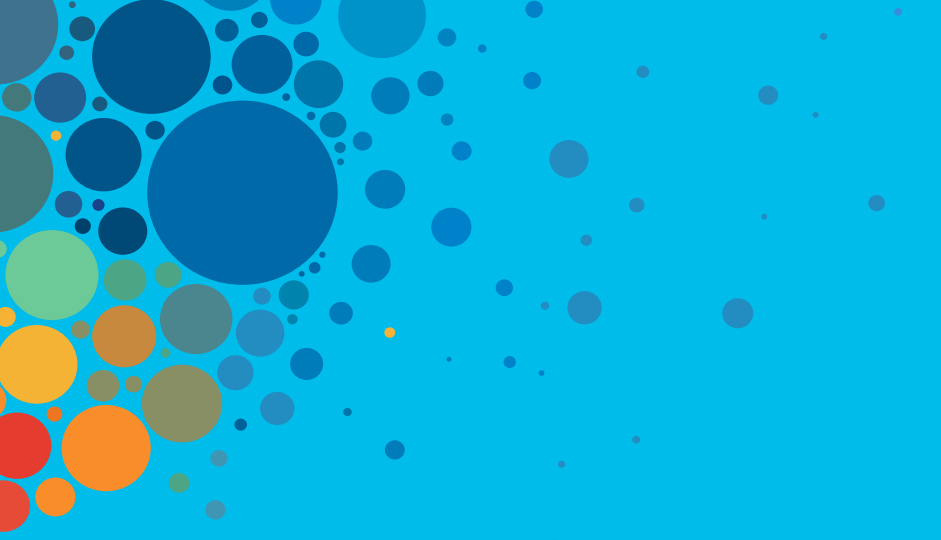
Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive