
cisco Live!
ALL IN

The bridge to possible

Troubleshooting the Video Mesh Solution

Unraveling the mystery

Paul Stojanovski – Technical Leader
@CiscoCloudPaul

BRKCOL-3005

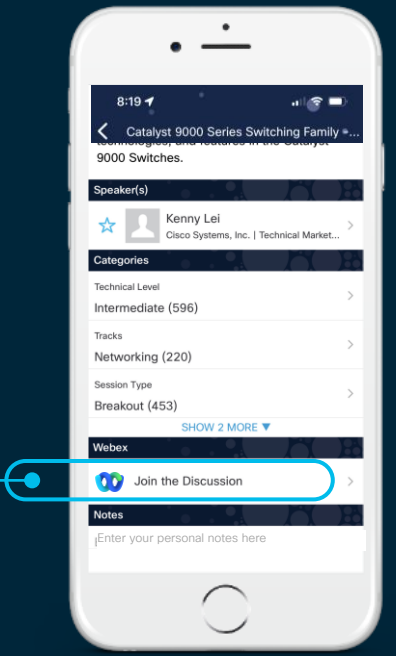
Cisco Webex App

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-3005

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

BRKCOL-2750 | Richard Murphy

Understanding the new call flows and meeting type for the Video Mesh Solution

Agenda

- Introduction
- Tools Breakdown
- Troubleshooting
  - Developing a baseline
  - Deployments
  - Meetings
- Conclusion

Introduction

Troubleshooting Video Mesh

Unraveling the mystery in 45 minutes

Tools Breakdown

“If the only tool you have is a hammer, you tend to see every problem as a nail.”

Abraham Maslow

Video Mesh Toolbox

Understand the the tool for the job

Video Mesh

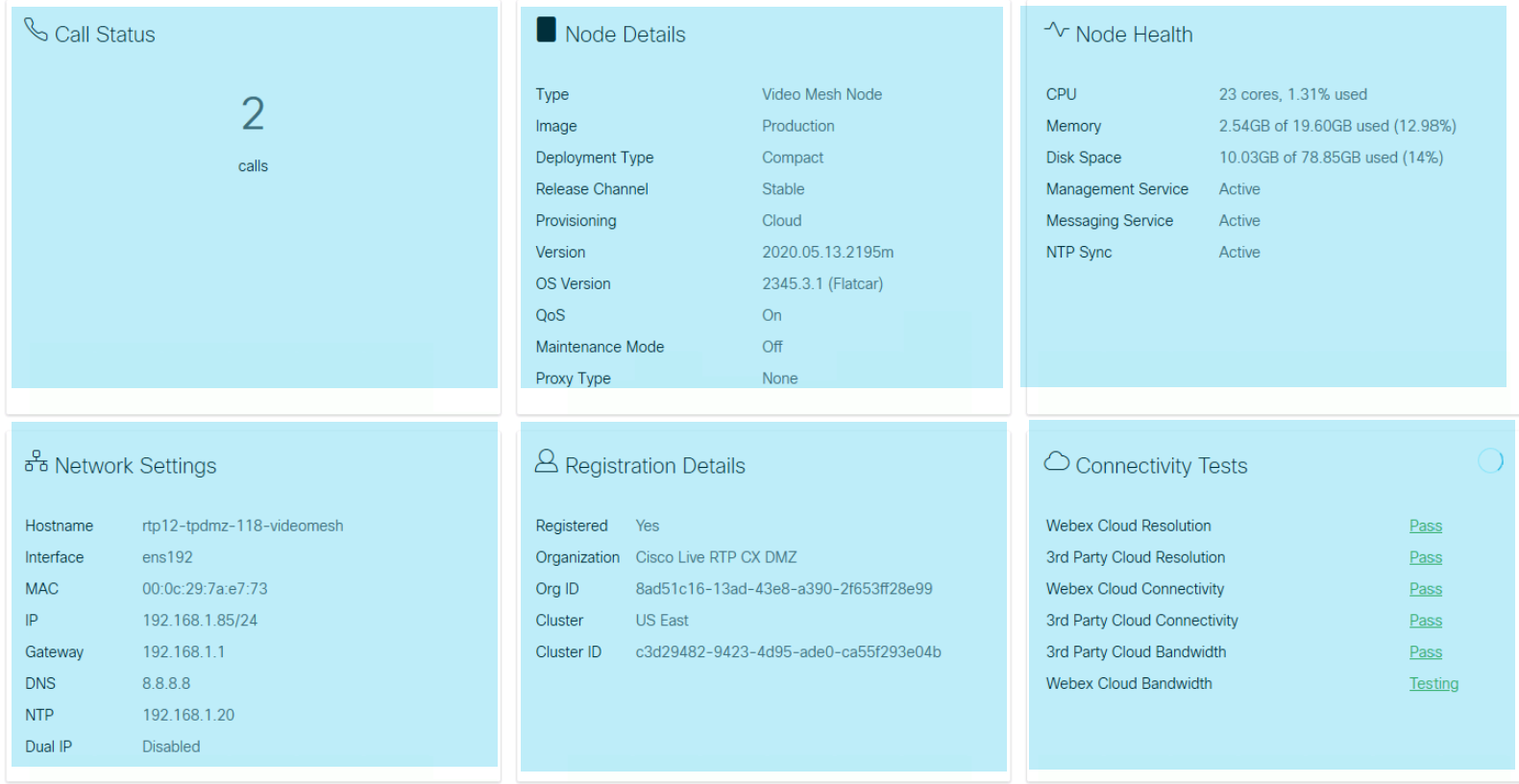
- Overview Page
- Log Capture
- Packet Capture
- Traceroute
- Ping
- NTP Connectivity Check
- Cloud Connectivity Check
- Port Reflector

Control Hub

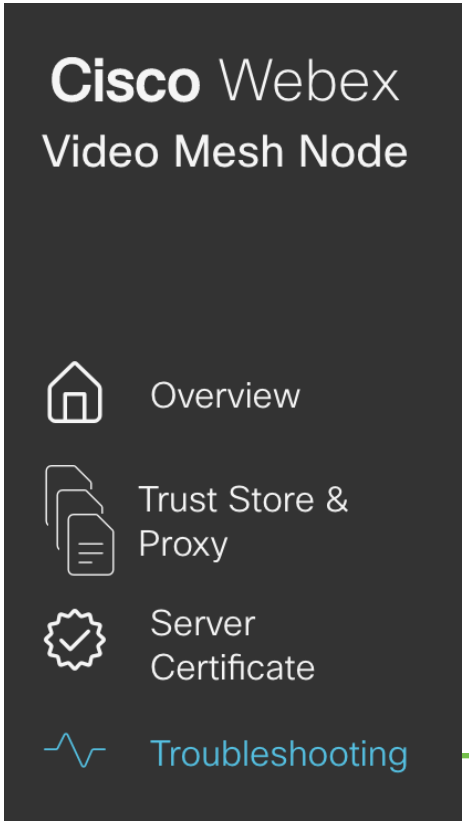
- Alarms
- Events
- Notifications
- Meeting Health Monitor
- Video Mesh Analytics
- Troubleshooting
  - Meetings & Calls

Video Mesh Overview Page

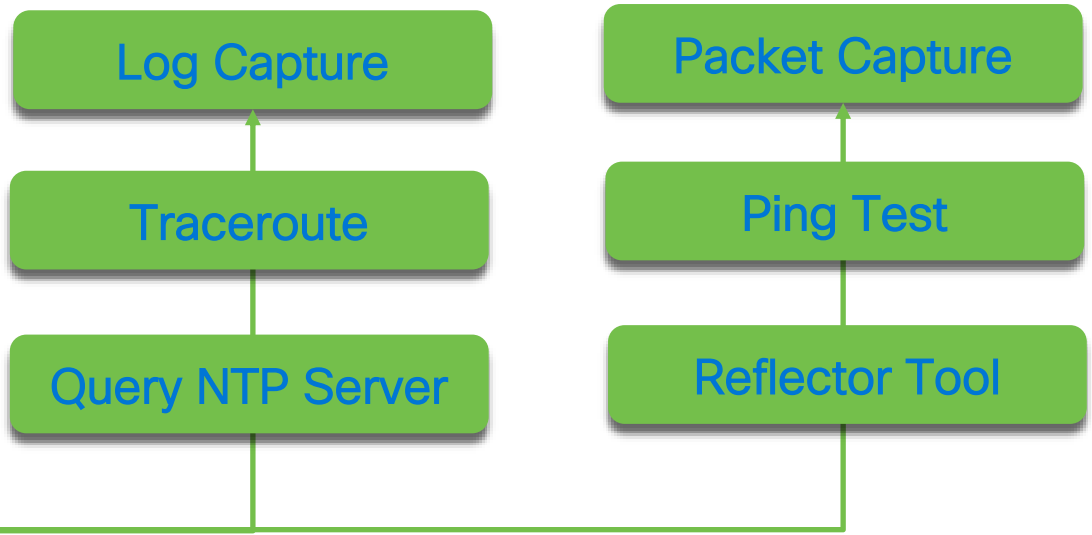
https://<VMN_IP>/setup



Video Mesh Troubleshooting Features

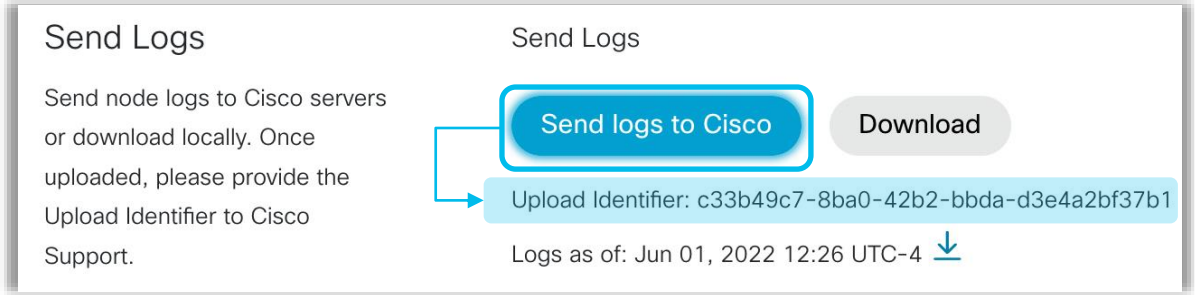


- Video Mesh **serviceability tools** can be found in the **Troubleshooting** menu of the local node



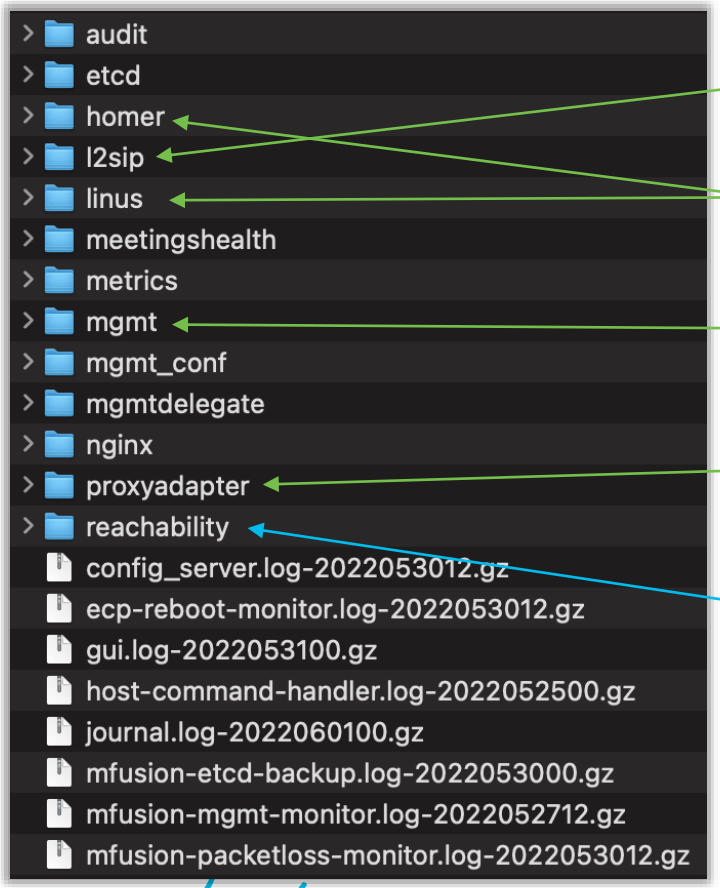
Note: External Logging (syslog) capability NOW available

Logging Capability



- Logs written to */home/mfusion/logs/*
- Logs are non-adjustable, historical, and persist reboots
- When sent to Cisco "Upload Identifier" should be provided to CX support engineer (TAC)
  - Logs retrieved from internal tooling
- Does not include Personally Identifiable Information (PII)
- Provides useful information for:
  - Connectivity to Webex
  - Platform Issues
  - Call Setup / Media

Logging Construct



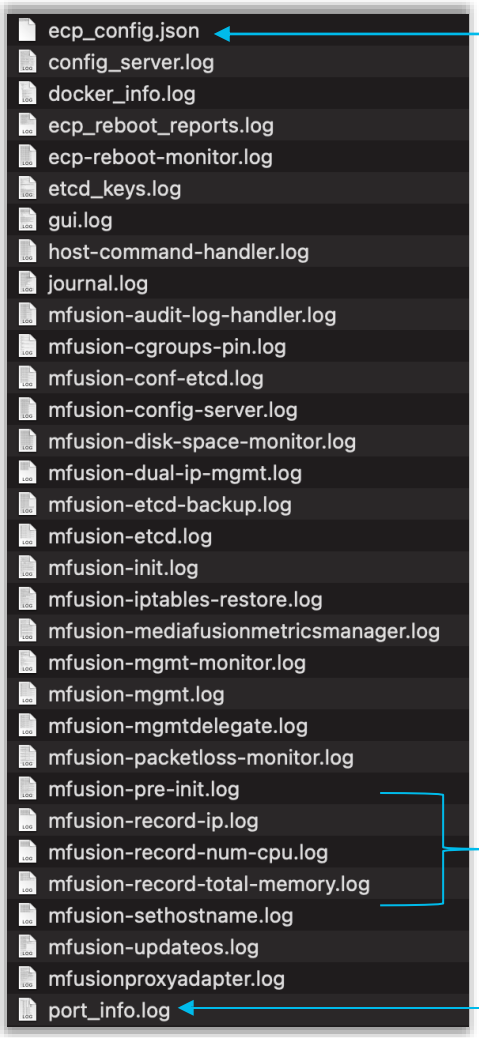
SIP Device Signaling

Media & Cascade

Alarms sent to Control Hub

Communication through Proxy

Cloud Reachability Checks



VMN Configuration json

Records VM Config Changes

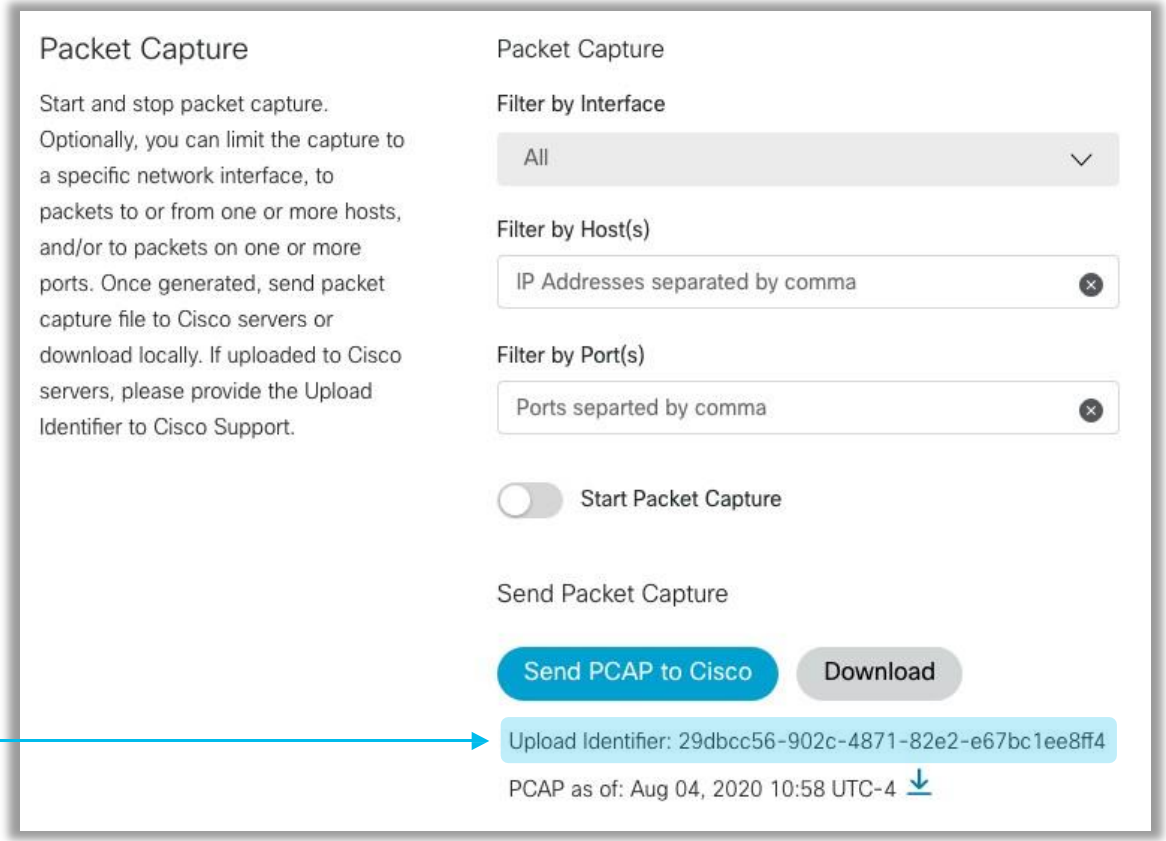
Displays active IP/port information

VMN Logging Anatomy – ecp_config.json


```
{ "disk_space_info"
      "totalMB": "80746",
       "percentUsed": "14%"     },

    "ecp_info": {
     os_name": "flatcar",
    "ova_build_type": "FIELD",
     version": "2020.07.15.2245m

 "ova_deployment_info": {
        "ovaDeploymentType": "compact",
        "memorySizeInBytes": "20550860",
        "hardDiskSizeInGigaBytes": "80",
        "cpuCount": "23",
        "cpuModelName": "Intel(R) Xeon(R) CPU E5-2695 v4 @
2.10GHz"

    "ecp_config": {
          network_config": {
             "internal_nw_interface": "ens192",
              internal_ipaddress": "192.168.1.85
              DNS": "8.8.8.8 192.168.1.20
             "DHCP": "false",
             "internal_gateway": "192.168.1.1",
             "internalMtu": 1500,
             "docker_bip": "172.17.42.1/255.255.0.0"},
                                                    ,
    "hostname": "rtp12-tpdmz-118-videomesh
    "domain": "rtp.ciscotac.net",
    "ntp_servers": "192.168.1.20",
    "etcd_version": "3.1.8",
    "etcd_port": "2378","etcd_restore_events": "None",
    "coreos_version": "2345.3.1",
    "os_id": "flatcar",
    "mgmtdelegate_code_version": "2020.05.11.919m",
    "releaseChannel": "stable",
    "qosStatus": "on",
     local_provisioning": "false",
    "maintenanceMode": "off",
    "releaseTag": "2020.05.13.2195m",
    "pendingReleaseTag": "2020.05.13.2195m",
    "dual_ip_mode": "false",
    "proxy_info": {
        "proxy_status": "enabled",
        "proxy_type": "explicit"

"system_services": {
        "containerd_status": "active",
        "dockerd_status": "up",
        "etcd_status": "active",
        "ntp_synced": "yes"
```

Packet Capture Utility

- Capture is written to the following location:
  /home/mfusion/packet_capture
- Captures can be taken from **each interface** or **consolidated** into one file
  - **All** option contains internal docker address 172.17.42.0–172.17.42.63
- Captures can be filtered by **“Host(s)”** or **“Port(s)”**
- Captures capped at **2GB**
- When sent to Cisco “Upload Identifier” should be provided to TAC



Client Logging

Where are the logs located?

Webex Application

- \Users\UserName\AppData\Local**CiscoSpark**
  - current_log.txt

WME (Media Engine)

- \Users\UserName\AppData\Local\CiscoSpark**media**
  - current_log.txt

Webex Application

- /Users/UserName/Library/Logs/SparkMacDesktop/
  - current_log.txt

WME (Media Engine)

- /Users/UserName/Library/Logs/SparkMacDesktop/**media**
  - current_log.txt

```
C:\Users\Paul Stojanovski\AppData\Local\CiscoSpark>dir
 Volume in drive C has no label.
 Volume Serial Number is C6F1-B0A5

 Directory of C:\Users\Paul Stojanovski\AppData\Local\CiscoSpark

04/16/2019  02:12 PM    <DIR>          .
04/16/2019  02:12 PM    <DIR>          ..
04/16/2019  02:12 PM    <DIR>          17986407243965555266
12/21/2018  05:13 PM    <DIR>          8823894660671802294
04/05/2019  02:39 PM    <DIR>          callLogs
02/28/2019  04:52 PM                 0 crash_placeholder.dat
04/16/2019  02:12 PM             7,121 current_log.txt
04/09/2019  12:32 PM           203,080 last_run_current_log.txt
04/16/2019  02:12 PM                 9 lifecycle.dat
04/16/2019  02:12 PM    <DIR>          media
04/09/2019  11:17 AM    <DIR>          mercury
04/09/2019  12:32 PM    <DIR>          rendering
04/16/2019  02:12 PM            16,384 spark_shared_store.db
04/09/2019  12:32 PM               194 Webex Teams.ini
```

```
PSTOJANO-M-C58L:SparkMacDesktop paulstojanovski$ pwd
/Users/paulstojanovski/Library/Logs/SparkMacDesktop
PSTOJANO-M-C58L:SparkMacDesktop paulstojanovski$ ls -la
total 174296
drwxr-xr-x  27 paulstojanovski  staff       864 Apr 16 11:55 .
drwx------+ 30 paulstojanovski  staff       960 Mar 23 09:16 ..
-rw-r--r--@  1 paulstojanovski  staff      8196 Apr  9 12:50 .DS_Store
drwxr-xr-x   3 paulstojanovski  staff        96 Mar 21 18:47 0223f3b0-6500-4660-ba11-3e8c90babef5
drwxr-xr-x   3 paulstojanovski  staff        96 Feb 28 17:07 213b9135-5959-4df8-8a28-396b481c7787
drwxr-xr-x   3 paulstojanovski  staff        96 Mar  8 14:46 214799ee-0c9c-4d05-89cd-8db22291995e
drwxr-xr-x   3 paulstojanovski  staff        96 Mar 26 08:58 30e27cee-927b-499c-acbd-cfe5f8bfc030
drwxr-xr-x   4 paulstojanovski  staff       128 Jan 17 09:21 4ae73b29-6bd4-4f56-82b9-35fcbe2ed161
drwxr-xr-x   3 paulstojanovski  staff        96 Apr 11 21:08 5e67656b-fdb8-4a67-af74-cd82f3c5a40c
drwxr-xr-x   3 paulstojanovski  staff        96 Apr  9 12:47 7a1c8392-0b6a-4c10-bb9d-ad15d09a3b4e
drwxr-xr-x   4 paulstojanovski  staff       128 Jan 17 09:21 802333dd-c286-4263-9938-c3d3fbf2a712
drwxr-xr-x   4 paulstojanovski  staff       128 Jan 17 09:21 91cb7706-4497-453e-a6a9-b67a16968069
drwxr-xr-x  14 paulstojanovski  staff       448 Apr  9 12:49 LogsMisconfiguredSite
drwxr-xr-x   3 paulstojanovski  staff        96 Apr  9 12:40 a4afb3a9-0850-4aaa-9f77-0615fce5cb2d
drwxr-xr-x   2 paulstojanovski  staff        64 Apr 13 22:32 callLogs
-rw-r--r--   1 paulstojanovski  staff     10791 Apr 16 09:25 cout_current_log.txt
-rw-r--r--   1 paulstojanovski  staff      1753 Apr 15 10:26 cout_last_run_current_log.txt
-rw-r--r--   1 paulstojanovski  staff  24105265 Apr 16 13:30 current_log.txt
-rw-r--r--   1 paulstojanovski  staff  49999978 Apr 16 11:55 current_log1.txt
-rw-r--r--   1 paulstojanovski  staff     50044 Apr 16 08:05 current_log_header.txt
drwxr-xr-x   3 paulstojanovski  staff        96 Nov 29 16:38 f4e4b99b-0ed2-45b9-9dc8-19ace5de1453
-rw-r--r--   1 paulstojanovski  staff  13905887 Apr 15 10:51 last_run_current_log.txt
-rw-r--r--   1 paulstojanovski  staff     11186 Apr 15 10:51 launcher.log
drwxr-xr-x   6 paulstojanovski  staff       192 Apr 15 10:51 mainprocess
drwxr-xr-x   7 paulstojanovski  staff       224 Apr 16 08:47 media
drwxr-xr-x   5 paulstojanovski  staff       160 Mar 25 14:03 mercury
drwxr-xr-x   6 paulstojanovski  staff       192 Apr 15 10:25 restarter
```

Connectivity Checking: 2-3....7

2 Connectivity Checking "Checkpoints"

- Initial Deployment Wizard
- Video Mesh Overview page

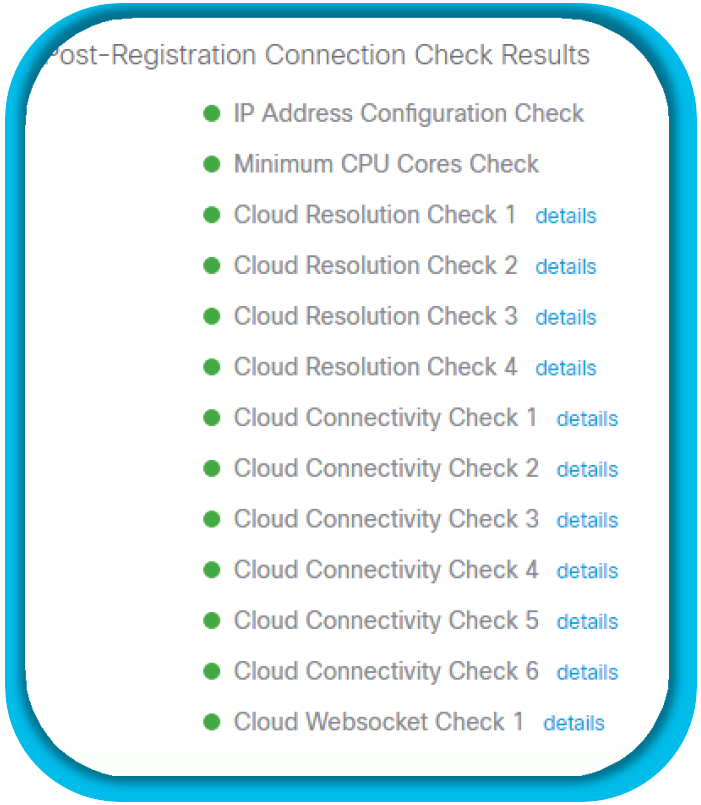
3 primary tests

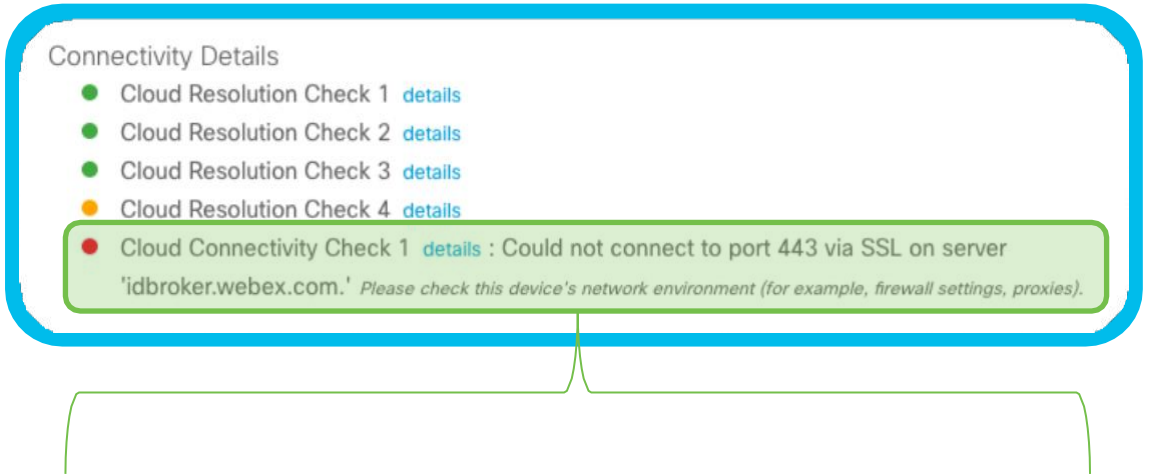
1. DNS Resolution
2. TCP Connectivity
3. Bandwidth

7 testing destinations

1.	idbroker.webex.com	Webex authentication and identity services
2.	identity.webex.com	Webex authentication and identity services
3.	hercules-a.wbx2.com	Microservice for hybrid management containers/registration
4.	index.docker.io	Container software repository
5.	registry-1.docker.io	Container software repository
6.	calliope-a.wbx2.com	Microservice for the media umbrella
7.	cme-junctionbox-apdx2-006-apdx2-public.wbx2.com	WebSocket connection point for Cloud media node and Video Mesh

Connectivity Checking





Typical causes:

1. Firewall blocking the traffic
2. Proxy not allowing traffic to the specific domain

Cisco Webex Network Requirements

Understanding Alarms

This node cannot complete a required download for an upgrade to succeed.

System Time on Video Mesh Node is Out of Sync

Webex Video Mesh SIP calling is not working correctly.

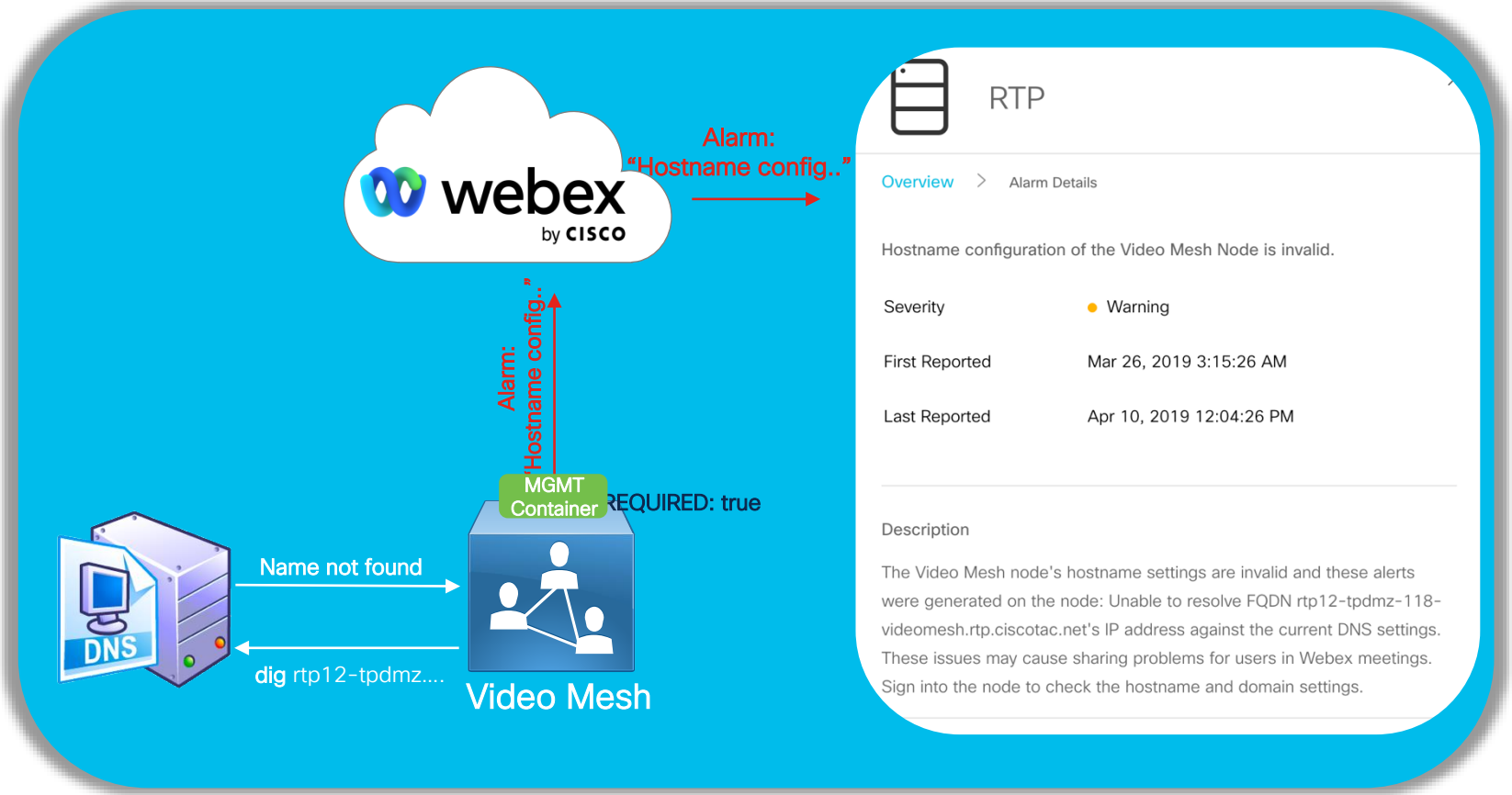
NTP configuration of the Video Mesh Node is invalid

Experienced problem connecting to Cisco Webex Cloud services

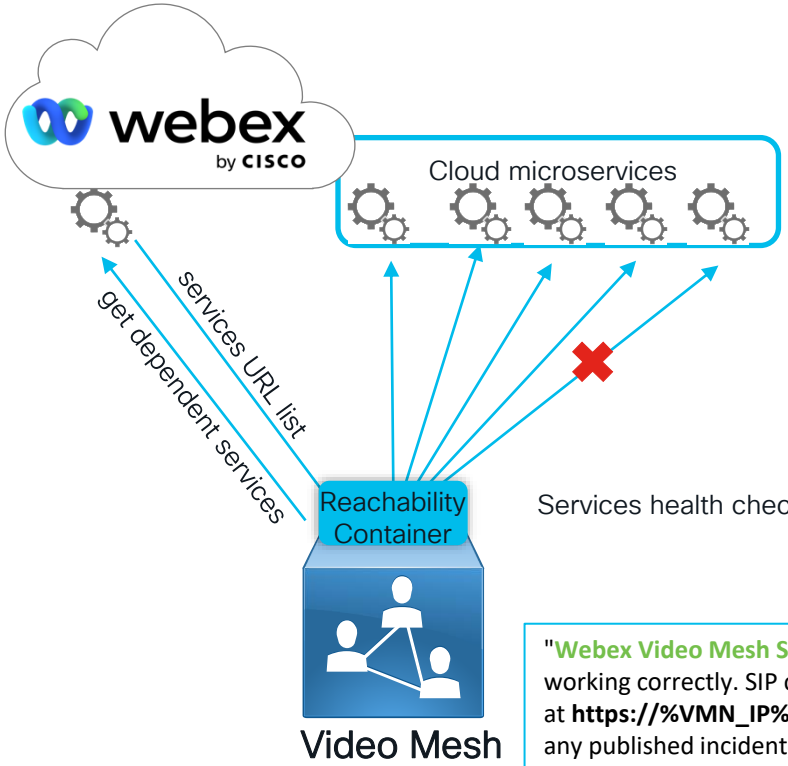
Hostname configuration of the Video Mesh Node is invalid

DNS configuration of the Video Mesh Node is invalid

Control Hub: Alarm Details



Calling Alarm Deep Dive



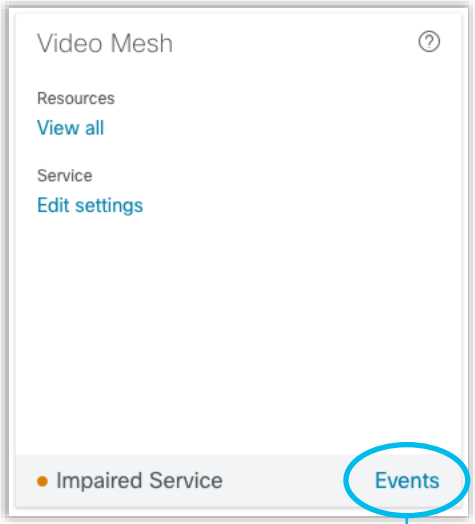
Cisco Webex Network Requirements

URLs	Code
Media URL	CAL
Auth URL	CI
Websocket URL	JB
Auth URL	CIS
Signaling URL	LOC
Reachability URL	RCH

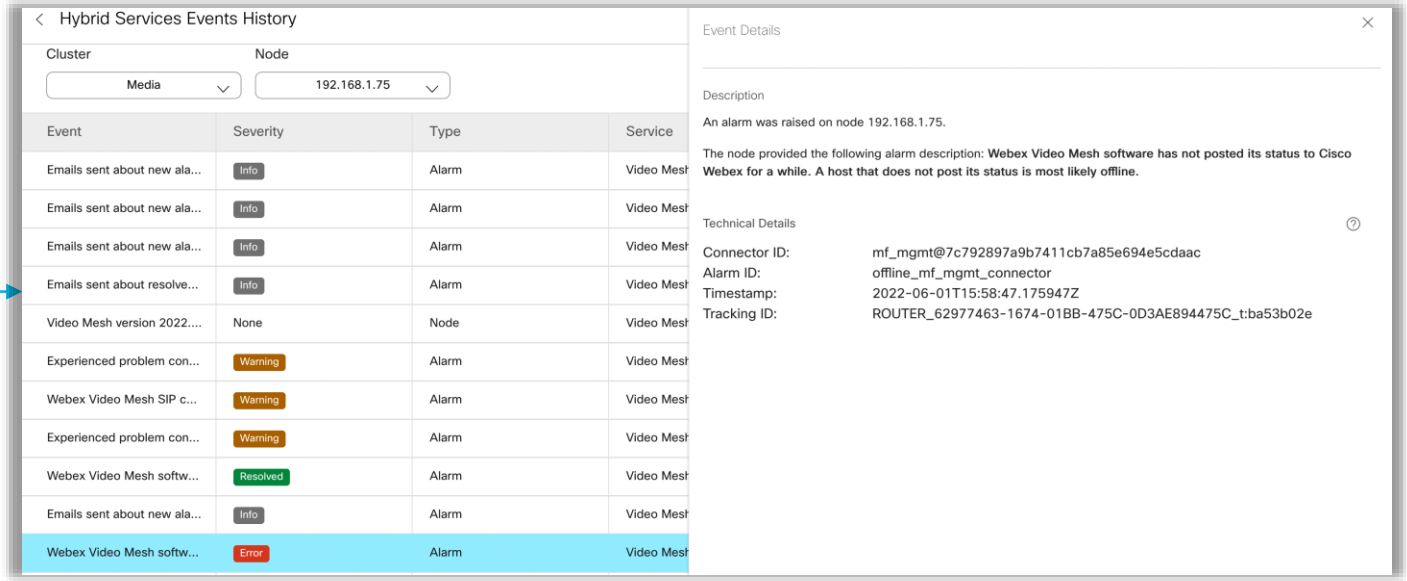
Defines which service URL failed

"**Webex Video Mesh SIP calling is not working correctly.**","description":"Webex Video Mesh SIP calling is not working correctly. SIP calls may overflow to the cloud or fail. Please check network connectivity to the cloud at **https://%VMN_IP%** and Cisco Webex status at https://status.ciscospark.com. If this problem persists without any published incident, go to https://admin.webex.com, click your admin username, and then click Feedback to open a case for further investigation **Error codes: LOC**"}

Webex Control Hub Events



- Provides records of events and historical changes to your Video Mesh nodes
- Variety of events and severities supported
- Filtering by cluster, node, and since (timeframe) are supported

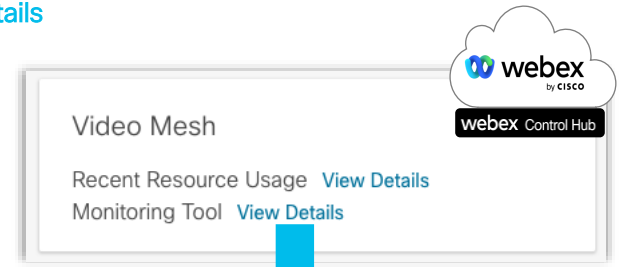


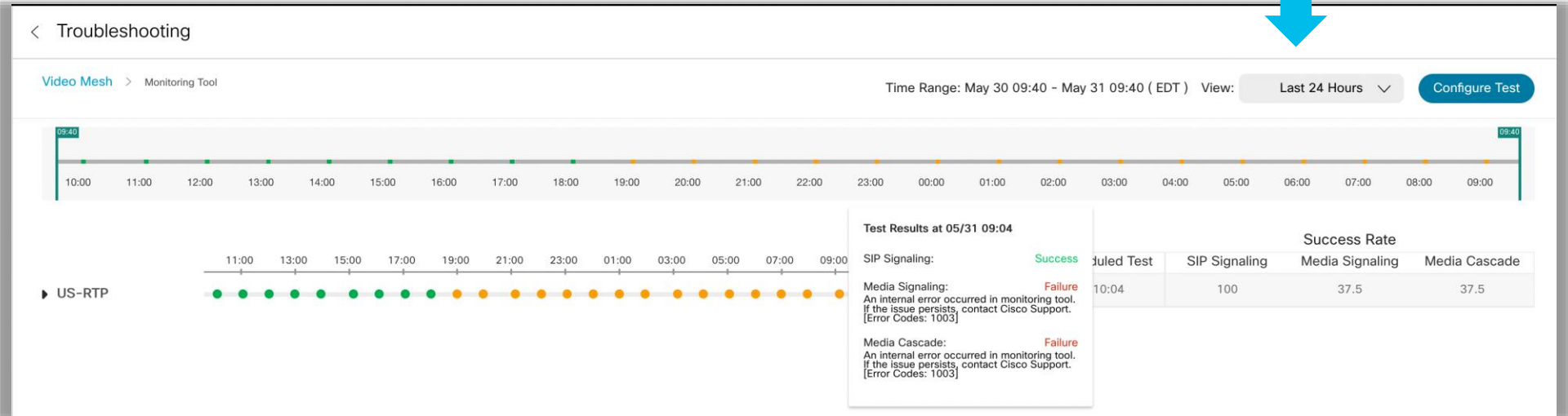
Media Health Monitoring

*Note: Test takes **2 minutes** to complete*

- Three synthetic tests are run:
  1. SIP Signaling
  2. Media Signaling
  3. Media Cascade
- Configure Hourly or Run immediately

Troubleshooting > Status > Monitoring Tool: View Details

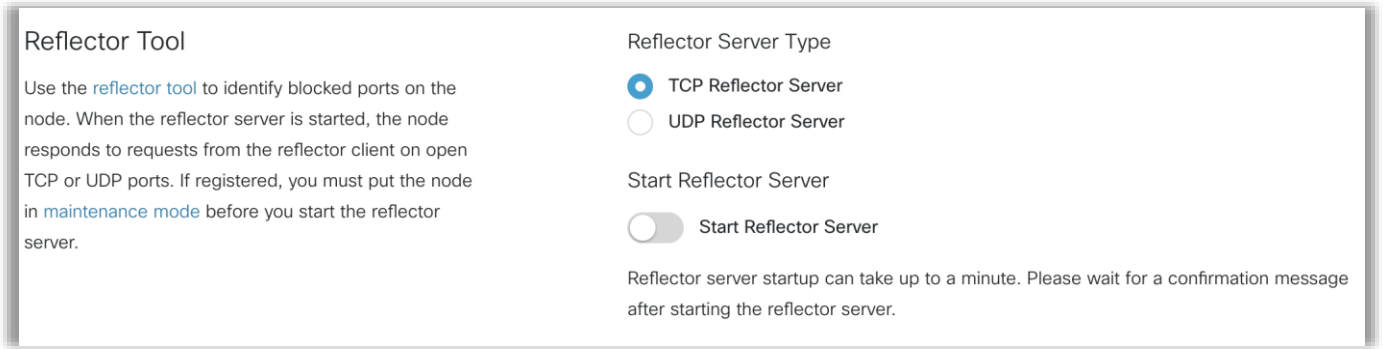




Reflector Tool

- Check ports from a client to VMN
  - QoS or non QoS enabled Video Mesh Nodes.
- Python Script run off of a client device (PC or
- Version 2.7 or higher of Python is required
- Script download location:
  - https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/mediaservice/deployment/qos/reflectorClient.zip

```
# +1 at the end to make the port inclusive.
non_qos_udp_ports_list = [5004] + list(range(34000, 34999+1))
non_qos_tcp_ports_list = [5004, 5060, 5061]
qos_udp_ports_list = [5004] + list(range(52500, 59499+1)) + list(range(63000, 64667+1))
qos_tcp_ports_list = [5004, 5060, 5061]
verify_port_list = []

def usage():
    print ("""Usage:
      --ip and --protocol are mandatory.
      If start-port is specified, end-port is considered mandatory. If no starting port is
      By default, tool checks for QoS ports unless --non-qos option is specified.
      Default QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 52500-59499 and 63
      Default non QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 34000-34999.
      To verify single port, both start and end port should be the required port to verify
      Examples:
      Below run is to verify non-qos ports using an input port range:
        python reflectorClient.py --ip <hmn-ip-address> --protocol <udp/tcp> --start-port
      Below run in to verify default qos ports:
        python reflectorClient.py --ip <> --protocol <udp/tcp>""")
```



Reflector Tool

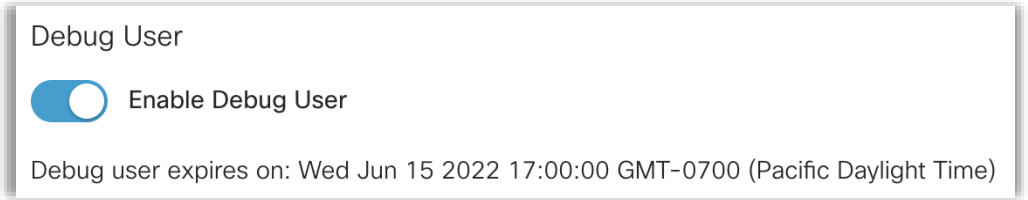
```
PSTOJANO-M-C58L:downloads paulstojanovski$ python reflectorClient.py --ip 192.168.1.84 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
 [------------------------------>] 100.00%  Success/Failed/Total: 3/0/3
##############################
No ports are blocked for tcp in ['5004', '5060-5061']
##############################
Exiting Reflector Client tool...

PSTOJANO-M-C58L:downloads paulstojanovski$ python reflectorClient.py --ip 192.168.1.84 --protocol udp
Please wait while verifying udp for ports: ['5004', '52500-59499', '63000-64667'] ...
 [------------------------------>] 100.00%  Success/Failed/Total: 8669/0/8669
##############################
No ports are blocked for udp in ['5004', '52500-59499', '63000-64667']
##############################
Exiting Reflector Client tool...

PSTOJANO-M-C58L:downloads paulstojanovski$ python reflectorClient.py --ip 192.168.1.84 --protocol udp
Please wait while verifying udp for ports: ['5004', '52500-59499', '63000-64667'] ...
 [----------->                    ] 38.76%  Success/Failed/Total: 0/3360/8669
```

What to supply TAC?

- Webex Conference ID or Meeting Number
- Detailed Description of the Problem
  - *Webex App users in the San Jose office are not using the Video Mesh node in our Bay Area cluster.*
- User(s) e-mail IDs that are impacted
- Webex Organization name
- Video Mesh node name, IP, and cluster name
- What types of clients/devices are connecting to the Video Mesh node
  - On Premise SIP Devices
  - Webex-registered clients/devices
  - 3rd party clients

Debug User

- Each Video Mesh Node has a built-in debug user account *(mfusion)*
- This account is used by TAC in special troubleshooting situations
- Account must be enabled through VMN Web interface *(Troubleshooting menu)*
- Account duration is 2 days
- Encrypted hash must be supplied to TAC to ge

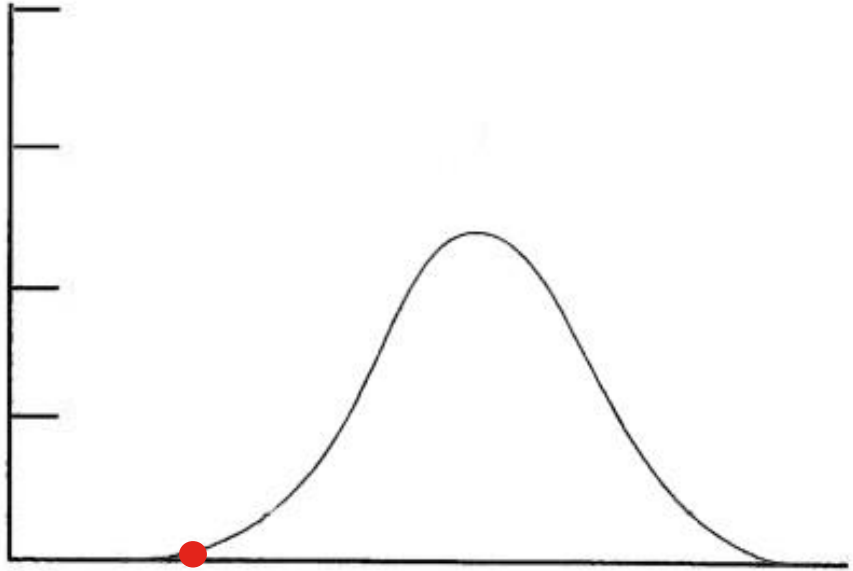


Building a Troubleshooting Baseline

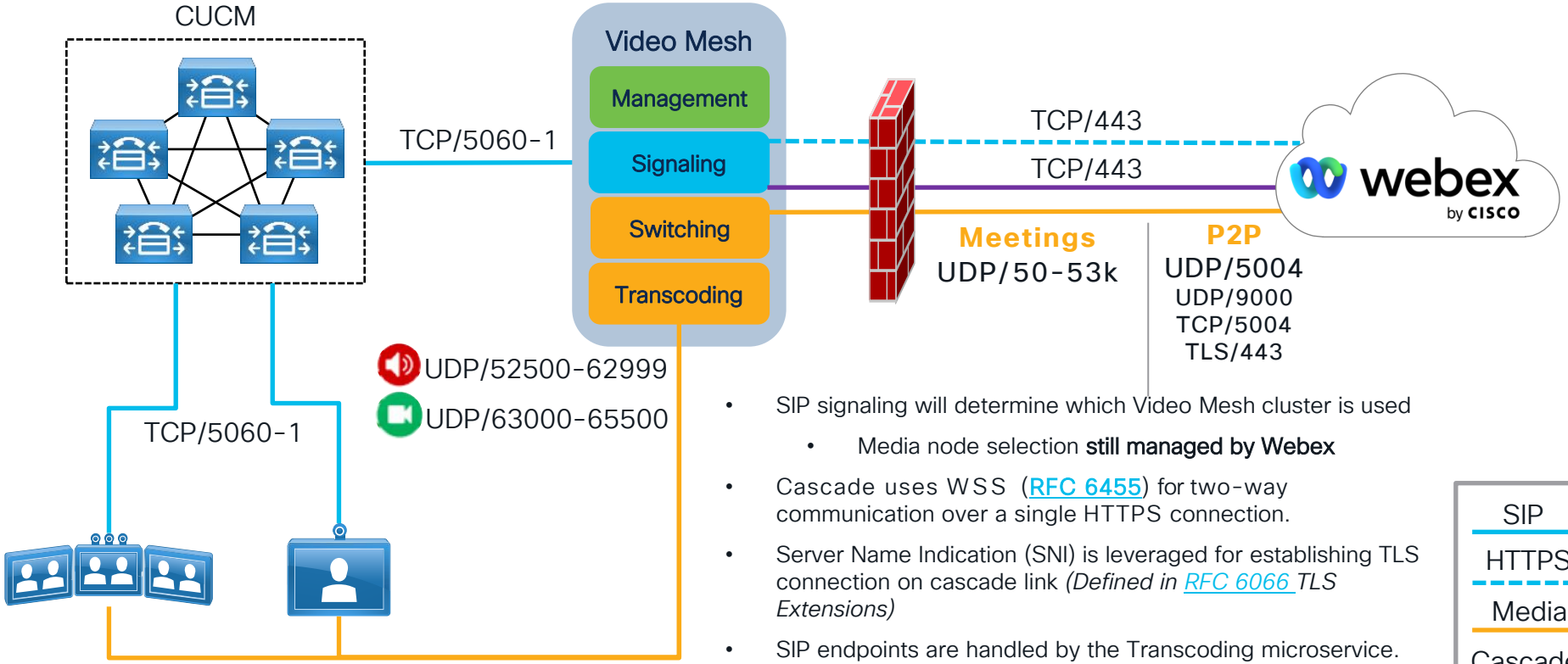
cisco Live!

Developing a Baseline

- Critical to understand how a product / solution works
- Understanding the baseline allows us to easily see deviations
- Requires some upfront investment but leads to quicker resolution



Video Mesh SIP-based Signaling/Media Paths

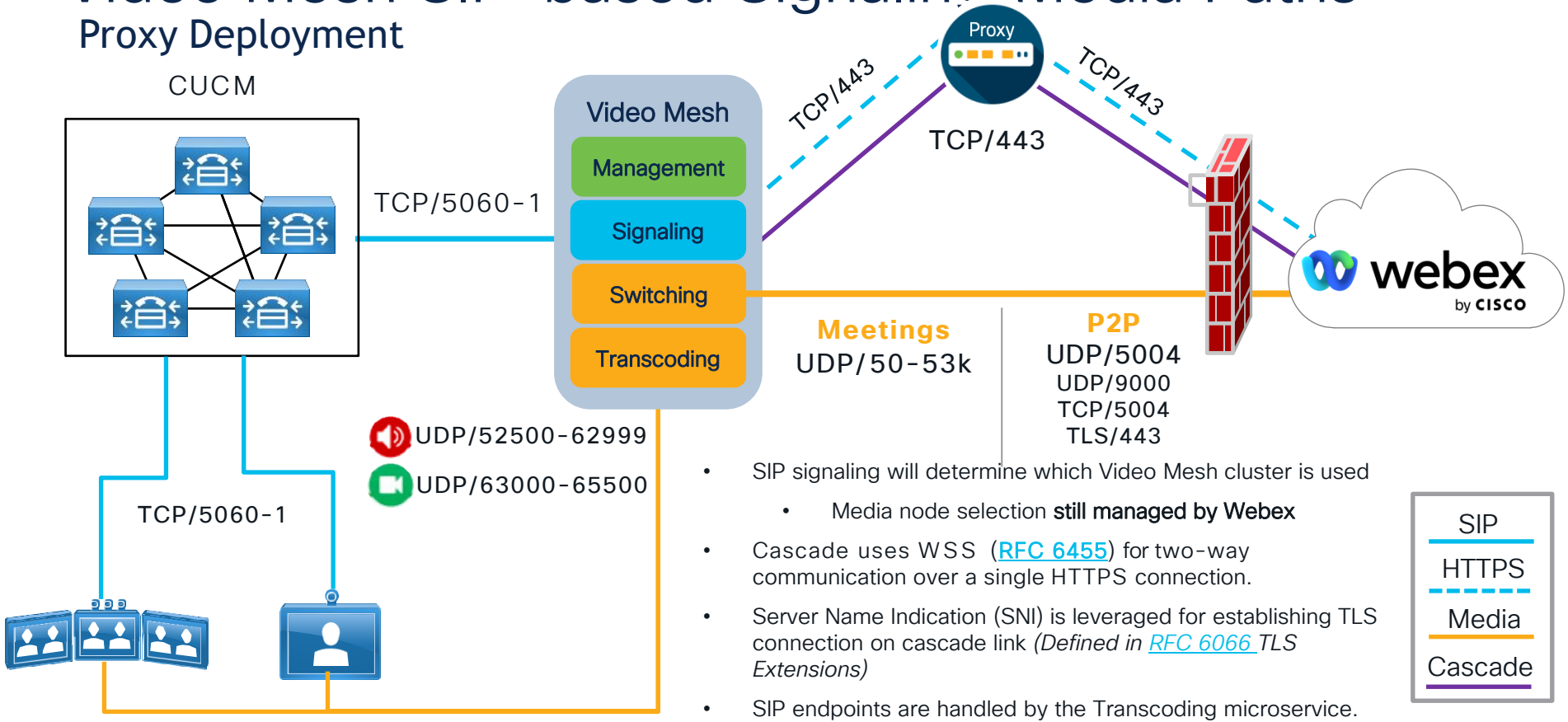


- SIP signaling will determine which Video Mesh cluster is used
  - Media node selection **still managed by Webex**
- Cascade uses WSS (RFC 6455) for two-way communication over a single HTTPS connection.
- Server Name Indication (SNI) is leveraged for establishing TLS connection on cascade link *(Defined in RFC 6066 TLS Extensions)*
- SIP endpoints are handled by the Transcoding microservice.
  - Allows for all participants to be multi-stream capable.

SIP
HTTPS
Media
Cascade

Video Mesh SIP-based Signaling/Media Paths

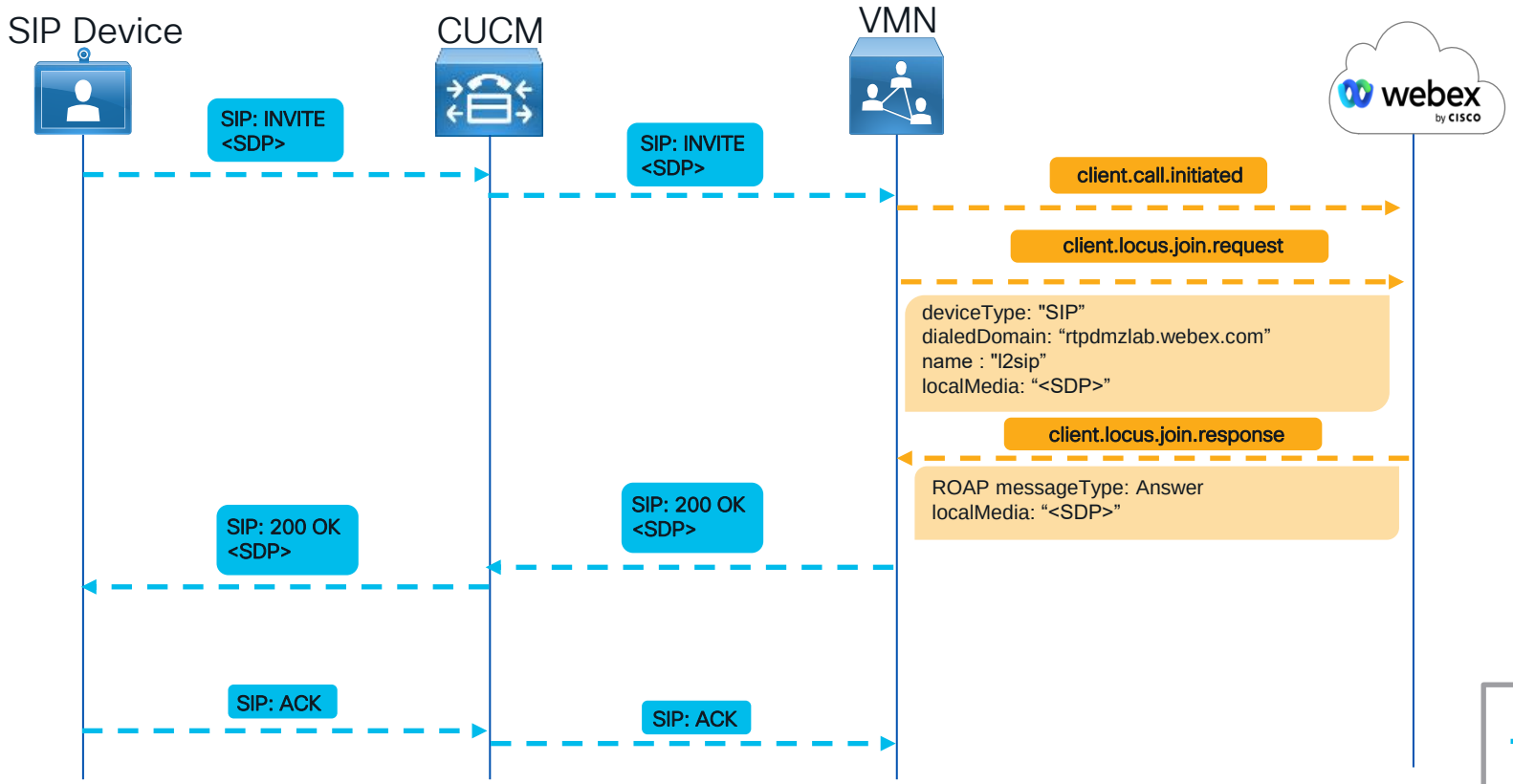
Proxy Deployment



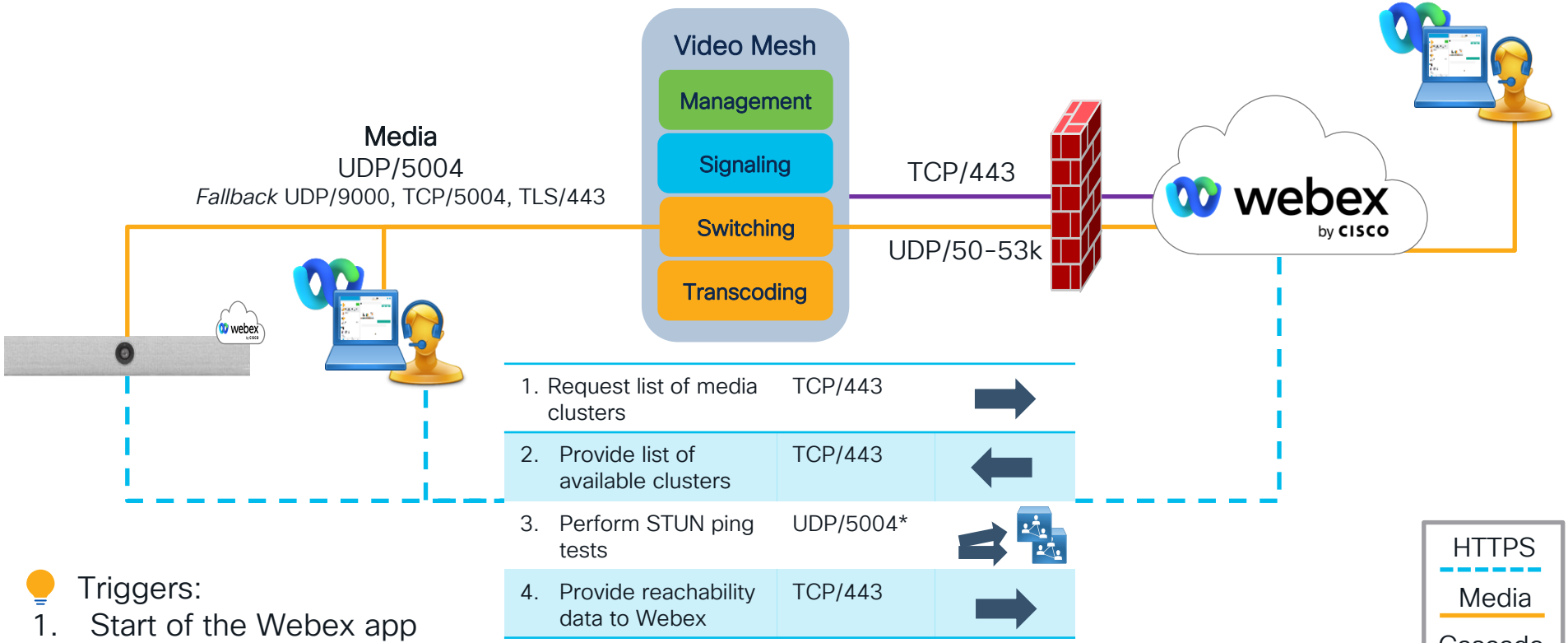
- SIP signaling will determine which Video Mesh cluster is used
  - Media node selection **still managed by Webex**
- Cascade uses WSS (RFC 6455) for two-way communication over a single HTTPS connection.
- Server Name Indication (SNI) is leveraged for establishing TLS connection on cascade link *(Defined in RFC 6066 TLS Extensions)*
- SIP endpoints are handled by the Transcoding microservice.
  - Allows for all participants to be multi-stream capable.

SIP
HTTPS
Media
Cascade

SIP Baseline Call into Video Mesh



Video Mesh Webex App-based Signaling/Media Paths



Triggers:

1. Start of the Webex app
2. Network event change
3. Cache expiry (2 hours)

Webex App Client Log

Cluster Discovery Initialization

Triggers:
1. Start of the Webex App
2. Network event change
3. Cache expiry (2 hours)

2019-05-01T18:44:32.787Z <Debug> [0x700005e3b000] MediaManager.cpp:62 networkChanged:Network has changed
2019-05-01T18:44:32.787Z <Debug> [0x700005e3b000] MediaManager.cpp:1610 performReachabilityCheck:Performing reachability Check
2019-05-01T18:44:32.787Z <Debug> [0x700005e3b000] MediaManager.cpp:2082 clearReachabilityData:Clearing reachability data
2019-05-01T18:44:32.787Z <Info> [0x700005e3b000] MediaManager.cpp:1647 getClusterInfoAndPerfromStunTrace:About to get Cluster information from Orpheus
2019-05-01T18:44:32.788Z <Debug> [0x700005e3b000] TelephonyAdapter.cpp:2182 locusRequest:Locus request: https://calliope-a.wbx2.com/calliope/api/discovery/v1clusters
TrackingId: OSX_97c6e74a-980f-4b40-afa4-7612ad914ac3_12

Webex App Client Log

Available Clusters (Video Mesh clusters)

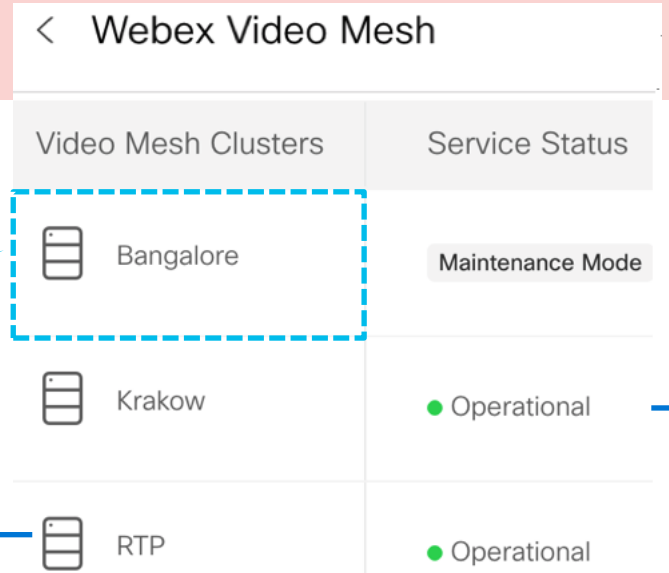
Company Name

RTP DMZ Test Lab Environment

Organization ID

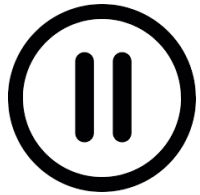
b522e1f2-553f-49a8-af80-9285a5d7f38e

2019-05-01T18:44:33.306Z <Debug> [0x700005e3b000] TelephonyAdapter.cpp:851 logPrivateData:LOCUS_DTO: **RestResponse**:
{"clusterClasses":{"hybridMedia":["b522e1f2-553f-49a8-af80-9285a5d7f38e.krakow.*",
"b522e1f2-553f-49a8-af80-9285a5d7f38e.rtp.*"]



Why was the **Bangalore** cluster not included?

Reachability Check Optimization



Challenge:

1) An organization could have a large number of Video Mesh clusters
   - Cluster reachability testing could take up to 15 seconds

2) A given user could start their client and place a call before a cluster reachability test has concluded

Solution:

- Implement an **optimized reachability check** that performs one reachability check to at minimum **one cluster in each cluster class**.
  - Cluster classes *(hybridMedia, ocpCloud, publicCloud)*
  - Returned resulted labled as “EarlyResult”
  - Other clusters will be tested if the client has time to continue

Webex App “WME” Client Log

Reachability Testing (Video Mesh **EarlyResult** clusters)

2020-08-09T16:56:18.704Z <Debug> [0x70000403a000] MediaManager.cpp:2106 operator():Response received from Orpheus
2020-08-09T16:56:18.704Z <Debug> [0x70000403a000] MediaManager.cpp:2146 performTraceServers:Calling WME to perform Stun Trace of Clusters

2020-08-09T16:56:18.708Z <Info> [0x113610dc0] WME:0 :[MediaSession] CTraceServer::createContextList, cluster name = 8ad51c16-13ad-43e8-a390-2f653ff28e99.emea.* cid_1 this=0x7fe51b4e0c90

2020-08-09T16:56:18.709Z <Info> [0x70000d3a0000] WME:0 :[UTIL] CCmConnectorUdpT::Connect, connect() successful. addr=192.168.1.83 port=5004 fd=37 this=0x7fe51b5e7090

2020-08-09T16:56:18.709Z <Info> [0x70000d3a0000] WME:0 :[UTIL] CCmTransportBase::SetTos2Socket, SetOption(IP_TOS) IPPROTO_IPV successful **nTos=0** this=0x7fe51d8d3e00

2020-08-09T16:56:18.761Z <Info> [0x70000d3a0000] WME:0 :[UTIL] CCmConnectorTcpT::Connect_i,

Webex App “WME” Client Log

Round-trip-delay results (Video Mesh **EarlyResult** clusters)

2020-08-09T16:56:18.809Z <Debug> [0x70000d3a0000]
WMETraceServerSink.cpp:60 OnTraceServerEarlyResult:OnTraceServerEarlyResult:
0 Result :

{"8ad51c16-13ad-43e8-a390-2f653ff28e99.emea.*”:
{"clusterUsability":{"usable":"true"},"tcp":{"latencyInMilliseconds":"20","reachable":"true"},"udp":{"latencyIn
Milli seconds":"26","reachable":"true"}}}

The Webex App determined the following:

1. EMEA Video Mesh cluster was chosen from the hybridMedia cluster class
2. EMEA Video Mesh cluster is usable, reachable, and is reporting 26 milliseconds of UDP latency

Webex App Client Log

Available Clusters (Cloud media clusters)

2020-08-09T16:56:18.704Z <Debug> [0x70000403a000] TelephonyAdapter.cpp:926 logPrivateData:LOCUS_DTO: **RestResponse**:
{"clusterClasses":{"hybridMedia":["8ad51c16-13ad-43e8-a390-2f653ff28e99.emea.*","8ad51c16-13ad-43e8-a390- 2f653ff28e99.useast.*"]
...
"ocpCloud":["alhrm.alhrm.*","wjfk.wjfk.*","asfom.asfom.*","aiadm.aiadm.*","anrtm.anrtm.*","asinm.asinm.*"
,"wsyd.wsyd.*","wams2.wams2.*","wdfw2.wdfw2.*","afram.afram.*"],
"publicCloud":["squared.asinm.*","squared.afram.*","salhrm.salhrm.*","saiadm.saiadm.*","squared.asydm.* ","squared.aiadm.*","sagrum.sagrum.*","squared.asfom.*"]},

ocpCloud	Region
lhr	Europe
jfk	United States
sfo	Europe
iad	United States
nrt	APAC
sin	APAC
syd	Australia

publicCloud	Region
sin	Asia
fra	Europe
lhr	Europe
Iad	United States
syd	Australia
gru	South America
sfo	United States

Webex App “WME” Client Log

Reachability Testing (Cloud media clusters)

2019-05-01T19:00:12.841Z <Debug> [0x70000591d000] MediaManager.cpp:1651 operator():Response received from Orpheus
2019-05-01T19:00:12.841Z <Debug> [0x70000591d000] MediaManager.cpp:1691 performTraceServers:Calling WME to perform Stun Trace of Clusters

2020-08-09T16:56:18.708Z <Info> [0x113610dc0] WME:0 :[MediaSession] CTraceServer::createContextList, cluster name = asinm.asinm.* cid 1 this=0x7fe51b4e0c90

2020-08-09T16:56:19.044Z <Info> [0x70000d3a0000] WME:0 :[UTIL] CCmDns6Manager::AsyncResolve, aHostName=external-media17.public.asinm-b-2.prod.infra.webex.com
2020-08-09T16:56:19.087Z <Info> [0x70000d3a0000] WME:0 :[UTIL] CCmDnsManager::DoGetHostByName_I, Get IPv4 addr: 170.133.176.44 for host: external-media17.public.asinm-b-2.prod.infra.webex.com
2020-08-09T16:56:19.088Z <Info> [0x70000d3a0000] WME:0 :[UTIL] CCmConnectorTcpT::Connect_i, addr=170.133.176.44 port=5004 laddr=0.0.0.0 lport=0 fd=37 this=0x7fe52080c220
2020-08-09T16:56:19.240Z <Info> [0x70000d3a0000] WME:0 :[UTIL] CCmConnectorUdpT::Connect, connect() successful. addr=170.133.176.44 port=5004 fd=45 this=0x7fe51b770da0
.....

Webex App Client Log

Round-trip-delay results (Cloud media clusters)

2020-08-09T16:56:30.723Z <Debug> [0x70000d3a0000]
WMETraceServerSink.cpp:21 OnTraceServerResult:OnTraceServerResult: 0 Result:

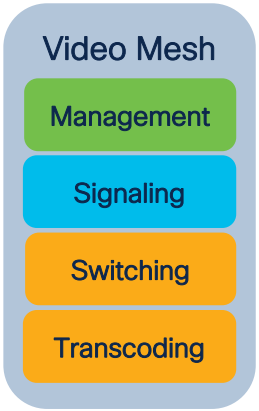
"asinm.asinm.*":{"clusterUsability":{"usable":"true"},
"tcp":{"latencyInMilliseconds":"446","reachable":"true"}
,
"udp":{"latencyInMilliseconds":"271","reachable":"true"
},
"xtls":{"latencyInMilliseconds":"414","reachable":"true"
}},

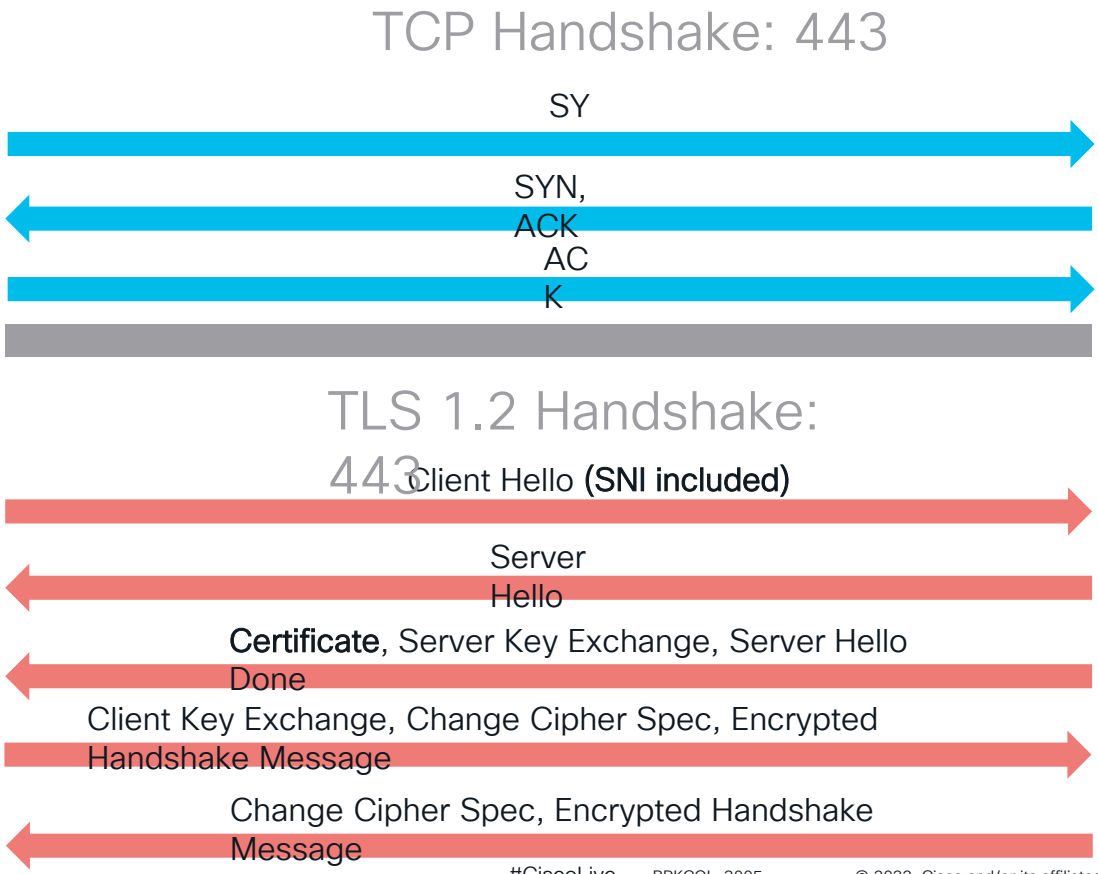
"afram.afram.*":{"clusterUsability":{"usable":"true"},"tcp":{"latencyInMilliseconds":"167","reachable":"true"},"udp":{"lat
encyInMilliseconds":"119","reachable":"true"},"xtls":{"latencyInMilliseconds":"169","reachable":"true"}}

"aiadm.aiadm.*":{"clusterUsability":{"usable":"true"},"tcp":{"latencyInMilliseconds":"38","reachable":"true"},"udp":{"lat
encyInMilliseconds":"35","reachable":"true", "},"xtls":{"latencyInMilliseconds":"39","reachable":"true"}}

- All three clusters are usable and reachable.
- The Webex App is based in the US so results favor the US-based (iad) media cluster.
- If no hybridMedia nodes were available, the media node in aiadm would be preferred.

Understanding the Cascade signaling





Understanding the Cascade signaling

TLS Handshake

tcp.stream eq 335

No.	Time	Source	Destination	Protocol	Length	Src Port	Dst Port	SNI	Info
204344	13:17:21.203008	192.168.1.75	23.89.10.17	TCP	76	41110	443		41110 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1186002932 TSecr=0 WS=256
204358	13:17:21.240369	23.89.10.17	192.168.1.75	TCP	76	443	41110		443 → 41110 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1380 SACK_PERM=1 TSval=3738918315 TSe
204359	13:17:21.240423	192.168.1.75	23.89.10.17	TCP	68	41110	443		41110 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1186002970 TSecr=3738918315
204360	13:17:21.240866	192.168.1.75	23.89.10.17	TLSv1.2	304	41110	443	homer0.wdfwm-a-9.prod.infra.webex.com	Client Hello
204380	13:17:21.277995	23.89.10.17	192.168.1.75	TCP	68	443	41110		443 → 41110 [ACK] Seq=1 Ack=237 Win=65024 Len=0 TSval=3738918353 TSecr=1186002970
204381	13:17:21.280032	23.89.10.17	192.168.1.75	TLSv1.2	2804	443	41110		Server Hello
204382	13:17:21.280032	23.89.10.17	192.168.1.75	TLSv1.2	555	443	41110		Certificate, Server Key Exchange, Server Hello Done

Client Hello

```
Extension: server_name (len=42)
    Type: server_name (0)
    Length: 42
  Server Name Indication extension
      Server Name list length: 40
      Server Name Type: host_name (0)
      Server Name length: 37
      Server Name: homer0.wdfwm-a-9.prod.infra.webex.com
```

*Client Hello contains the **RFC 6066** Server Name Indication TLS extension*

Server Hello

Certificate, Server Key Exchange, Server Hello Done

```
Extension (id-ce-subjectAltName)
    Extension Id: 2.5.29.17 (id-ce-subjectAltName)
  GeneralNames: 3 items
    > GeneralName: dNSName (2)
    > GeneralName: dNSName (2)
    > GeneralName: dNSName (2)
      dNSName: homer0.wdfwm-a-9.prod.infra.webex.com
```

Webex media server cert SAN matches the name in the Client Hello SNI extension

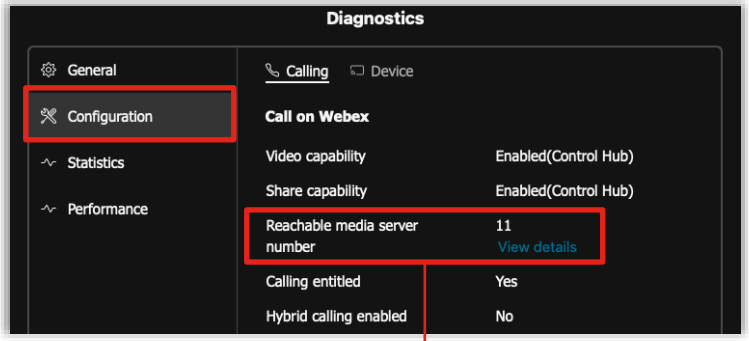
Video Mesh

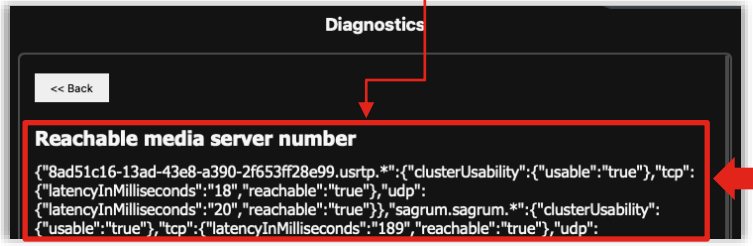
- Management
- Signaling
- Switching
- Transcoding

webex by CISCO

Webex App Diagnostics

1. From the Webex App select Help > Health Checker
2. Click Diagnostics in the right-hand corner

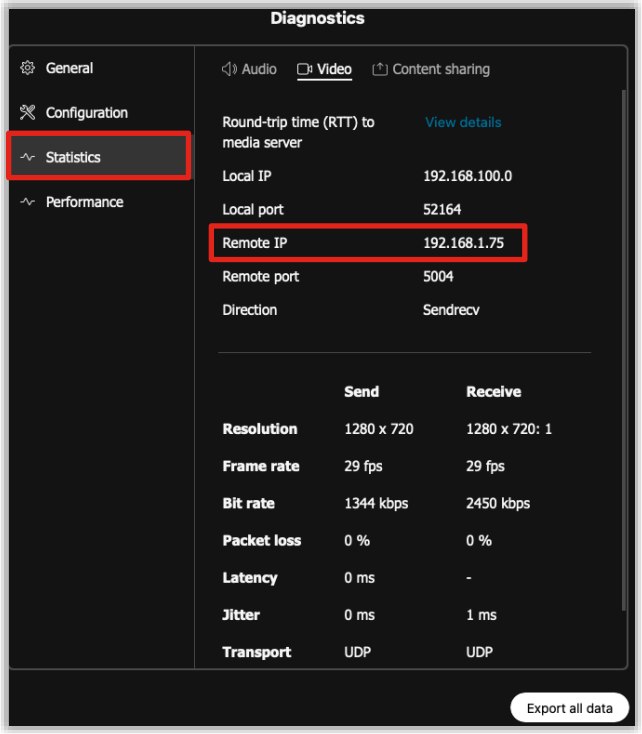




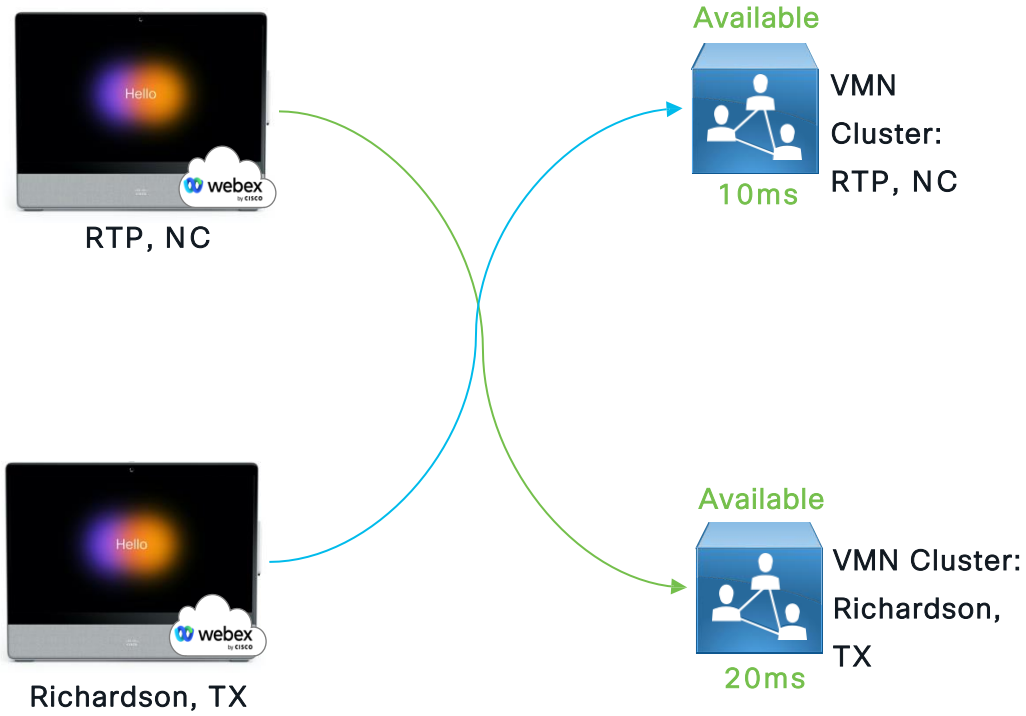
JSON formatted response to help understand if a VMN should have been chosen

TIP

Quickly determine if you've connected to your Video Mesh



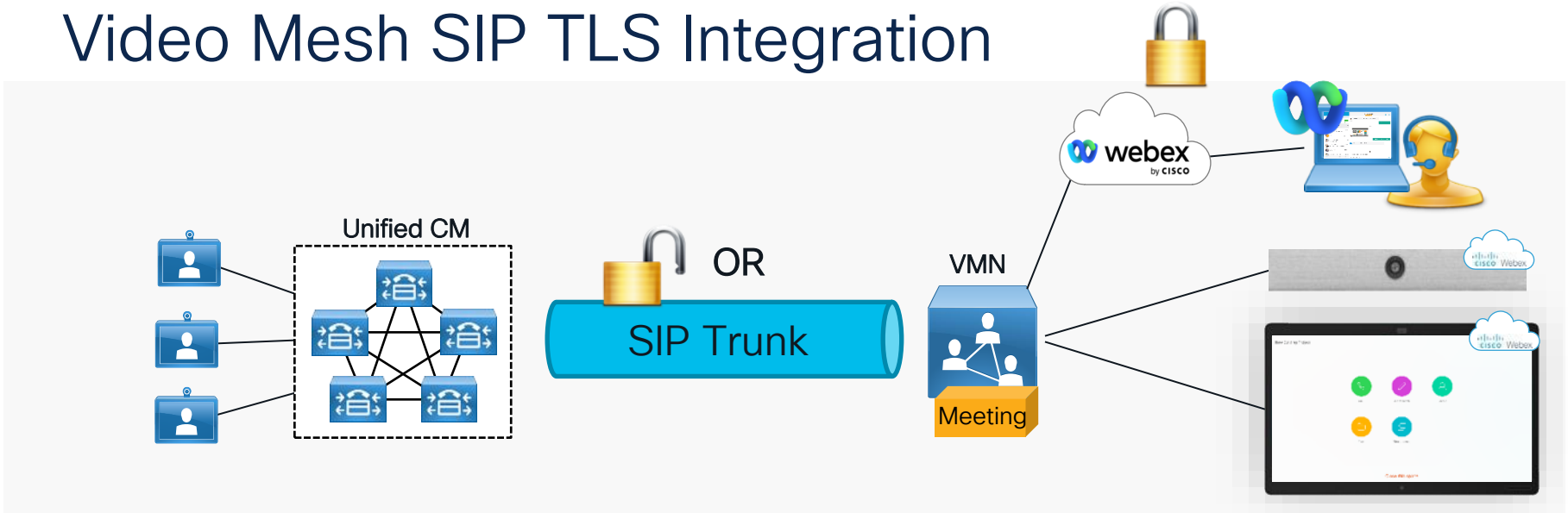
Randomized Cluster Selection



- Two cluster Video Mesh design
- Cluster reachability is under 25ms
- If reachability under 25ms node selection is randomized

Troubleshooting Deployments

Video Mesh SIP TLS Integration



Solution Requirements:

- CUCM must be running version **11.5.(1) SU3 or later**
- CUCM must be running in **Mixed mode**.
- Certificates must be **exchanged** between VMN(s) and CUCM node(s)
- All CUCM registered endpoints **must be encrypted**. *(non-encrypted endpoints overflow to Cloud)*

*Note: TLS Integration **not supported** for Expressway*

Video Mesh TLS Certificate Requirements

CUCM

- SIP Trunk Security Profile
  - **x509 Subject Name** must include **Common Name** of Video Mesh Node(s)
- Video Mesh Root CA must be added as a Call Manager trust

VMN

- Video Mesh certificate must be signed by a Root CA
- CUCM Root CA must be added to Video Mesh Trust Store
  - Root CA can be internal or external

Control Hub

- Media Encryption must be on
  - Defined globally
- SIP Trusted Sources:
  - Defined at cluster level
  - Must match the **Common Name** value of CUCM certificate(s)

Common SIP TLS Integration Failures

When troubleshooting TLS failures on Video Mesh leverage:

- CUCM SDL traces
- Video Mesh logs (l2sip.log)
- Packet Captures

l2sip/l2sip.log

C=US, Common Names and SANs: [rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net]
2019-05-02 20:11:01.677 UTC(+0000) INFO [TLSMessageChannelThread-39] c.c.w.s.s.s.t.UntrustedSipSourcesCache UntrustedSipSourcesCache.java:41 - New untrusted sip source added to cache. New size: 1, New certificate: Subject: L=RTP12,ST=North Carolina,CN=rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net,OU=TAC,O=Cisco,C=US, Common Names and SANs: [rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net]

2019-05-02 20:11:01.693 UTC(+0000) WARN [TLSMessageChannelThread-39] c.c.w.s.l.s.logger.L2SipStackLogger L2SipStackLogger.java:317 - gov.nist.javax.sip.stack.TLSMessageChannel.run (TLSMessageChannel.java:537) [A problem occured while Accepting connection]
SSLHandshakeException: java.security.cert.CertificateException: Client certificate Subject: L=RTP12,ST=North Carolina,CN=rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net,OU=TAC,O=Cisco,C=US, Common Names and SANs: [rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net] from host address /192.168.1.21:56216 failed certificate validation.
Caused by: CertificateException: Client certificate Subject: L=RTP12,ST=North Carolina,CN=rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net,OU=TAC,O=Cisco,C=US, Common Names and SANs: [rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net] from host address /192.168.1.21:56216 failed certificate validation.
...
Caused by: CertificateException: Hostname validation failed for certificate Subject: L=RTP12,ST=North Carolina,CN=rtp12-tpdmz-118-

rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net

Common SIP TLS Integration Failures

When troubleshooting TLS failures on Video Mesh leverage:

- CUCM SDL traces
- Video Mesh logs (l2sip.log)
- Packet Captures

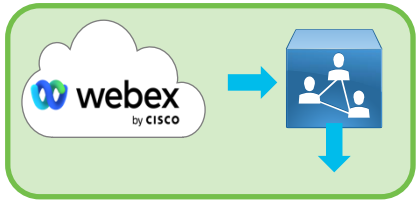

```
▼ Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1007
    Certificates Length: 1004
  ▼ Certificates (1004 bytes)
      Certificate Length: 1001
    ▼ Certificate: 308203e5308202cda00302010202107f65f7b08fae967bc3... (id-at-localityName=RTP12,id-at-stateOrProvinceName=North Carolina,id-at-commonName=rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net
```

tcp.port==5061 && ip.addr==192.168.1.21 && ip.addr==192.168.1.84

No.	Time	Source	Destination	Protocol	Length	S Port	D Port	Info
5223	2019-05-02 20:12:02.924664	192.168.1.21	192.168.1.84	TLSv1…	1547	45668	5061	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Messag
5228	2019-05-02 20:12:02.924729	192.168.1.84	192.168.1.21	TCP	68	5061	45668	5061 → 45668 [ACK] Seq=18671 Ack=1609 Win=33024 Len=0 TSval=1204374776 TSecr=1381218646
5246	2019-05-02 20:12:02.931471	192.168.1.84	192.168.1.21	TLSv1…	75	5061	45668	Alert (Level: Fatal, Description: Certificate Unknown)

```
Frame 5246: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 192.168.1.84, Dst: 192.168.1.21
▶ Transmission Control Protocol, Src Port: 5061, Dst Port: 45668, Seq: 18671, Ack: 1609, Len: 7
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Unknown)
      Content Type: Alert (21)
      Version: TLS 1.2 (0x0303)
      Length: 2
    ▼ Alert Message
        Level: Fatal (2)
        Description: Certificate Unknown (46)
```

Common SIP TLS Integration Failures



Video Mesh: l2sip/l2sip.log

2019-05-02 18:34:19.004 UTC(+0000) INFO [qtp1243171897-64] c.c.w.s.diagnostics.WebSequenceUtil WebSequenceUtil.java:111 - Unknown ->+ L2SIP: [PUT] **/v1/ecp/trustedSipSources**

2019-05-02 18:34:19.006 UTC(+0000) INFO [qtp1243171897-64] c.c.w.s.s.sip.tls.L2SipTrustManager L2SipTrustManager.java:163 - Setting **trustedSipSources**: [**rtp12-tpdmz-118-ucmpub.rtp.ciscotac.com**]

2019-05-02 18:34:19.019 UTC(+0000) INFO [qtp1243171897-64] c.c.w.s.diagnostics.WebSequenceUtil WebSequenceUtil.java:126 - L2SIP ->- Unknown: [200 OK] **/v1/ecp/trustedSipSources**

SIP TLS Configuration

⚠ This setting is done at the cluster level and is not available until you enable media encryption for your entire organization under the Video Mesh settings.

Trusted SIP sources

Enter the Common Name (CN) or any FQDNs that are present in the Subject Alternative Name on the CallManager certificate (typically the FQDN of the Unified CM). These entries are identified as trusted SIP sources and are allowed to send secure SIP calls to Webex Video Mesh.

rtp12-tpdmz-118-ucmpub.rtp.ciscotac.com × Enter the trusted SIP sources...

Certificate Settings

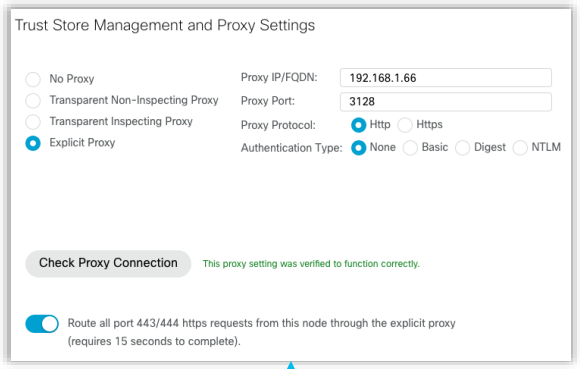
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

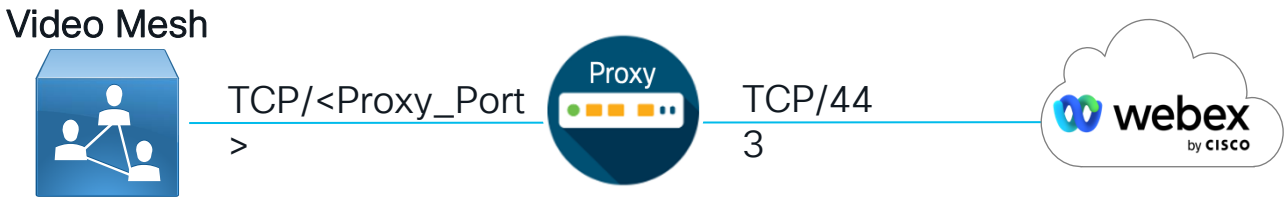
Certificate File Data

[
Version: V3
Serial Number: 7F65F7B08FAE967BC3A8A4A22C0FD0F5
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=RTP12, ST=North Carolina, CN=rtp12-tpdmz-118-ucmpub.rtp.ciscotac.net, OU=TAC, O=Cisco, C=US

≠

Proxy Deployments





Support Proxy Configurations:

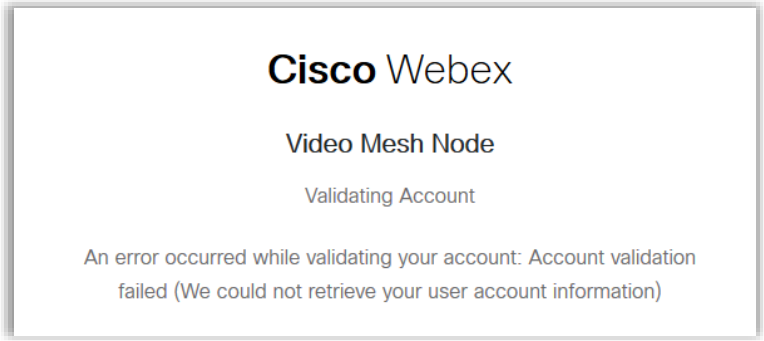
- No Proxy
- Transparent Non-Inspecting Proxy
- Transparent Inspecting Proxy
- Explicit Proxy
  - Auth: None/Basic/Digest/NTLM

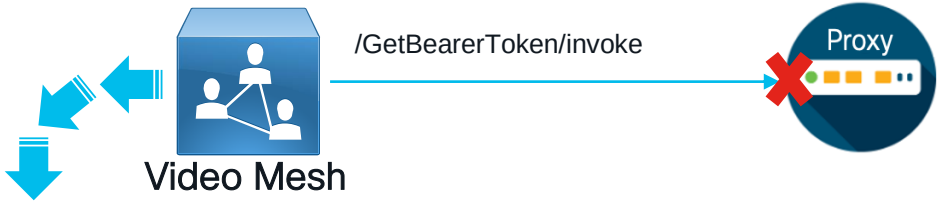
Domain	Purpose
*.docker.com	Original location for **Video Mesh container upgrades**
*.docker.io	Original location for **Video Mesh container upgrades**
.amazonaws.com	Future location for **Video Mesh container upgrades, log upload**
*.wbx2.com	Used for various services such as **metrics, node registration, cascade signaling**
*.webex.com	Used for **identity and authentication**

* Currently used in Federal environments

Initial Video Mesh Node Registration Failure

- The first phase of node registration includes obtaining a Bearer Token for the Video Mesh node.
- The Video Mesh uses this Bearer Token for machine account registration
- Bearer Token requested on behalf of the User Admin of the Org
- Requests are made to idbroker.webex.com
- Any blocking of the request will generate the following error message
  - 403/404/500/504 HTTP Errors
  - TCP Connection Refused/Wrong Port





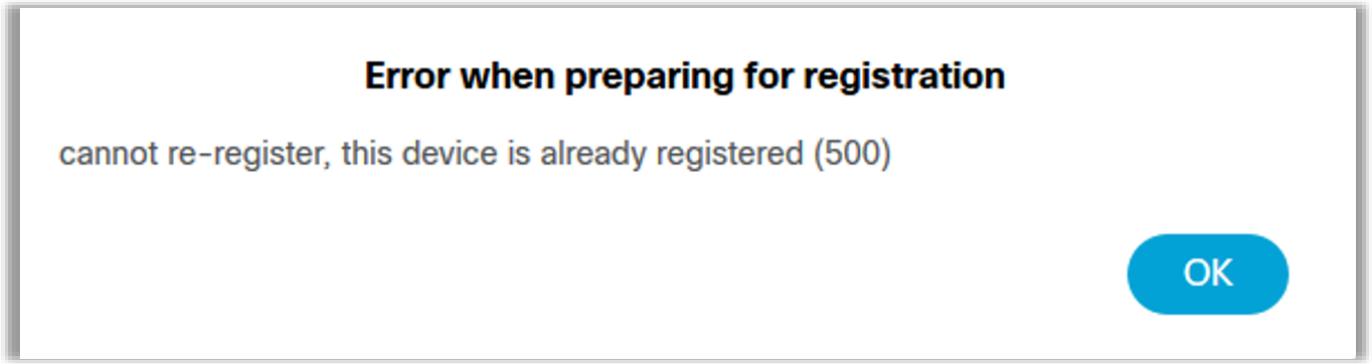
proxyadapter/all.log

2020-08-07 19:25:23,717 --- pws processing request... for url:https://idbroker.webex.com/idb/token/8ad51c16-13ad-43e8-a390-2f653ff28e99/v1/actions/GetBearerToken/invoke

2020-08-07 19:25:23,951 --- pws incoming proxyResponse:403/Proxy Unacknowledged

Initial Video Mesh Node Registration Stuck

- During initial Video Mesh node registration, you could encounter:

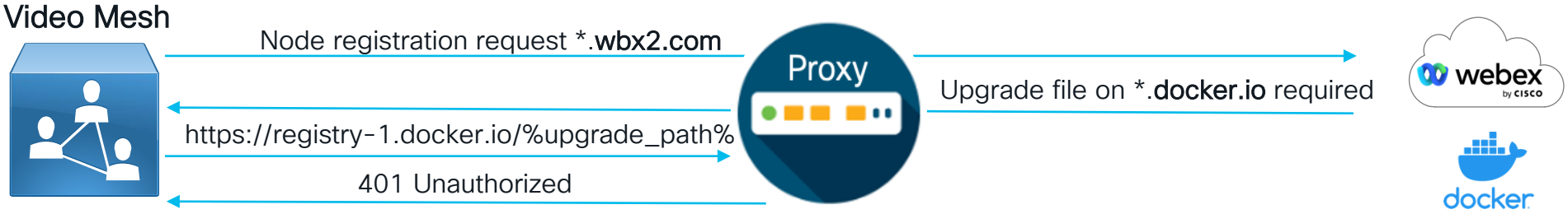


- Condition occurs when the following sequence of events are met:
  1. Initial registration fails due to proxy/firewall blocking the required Cloud domains
  2. Node is then removed from Control Hub
  3. Registration is re-attempted to the same Video Mesh node

Factory Reset required to recover

CSCvv30352
Local Deregister

Video Mesh Upgrade Failure
Symptom: Upgrade is stuck



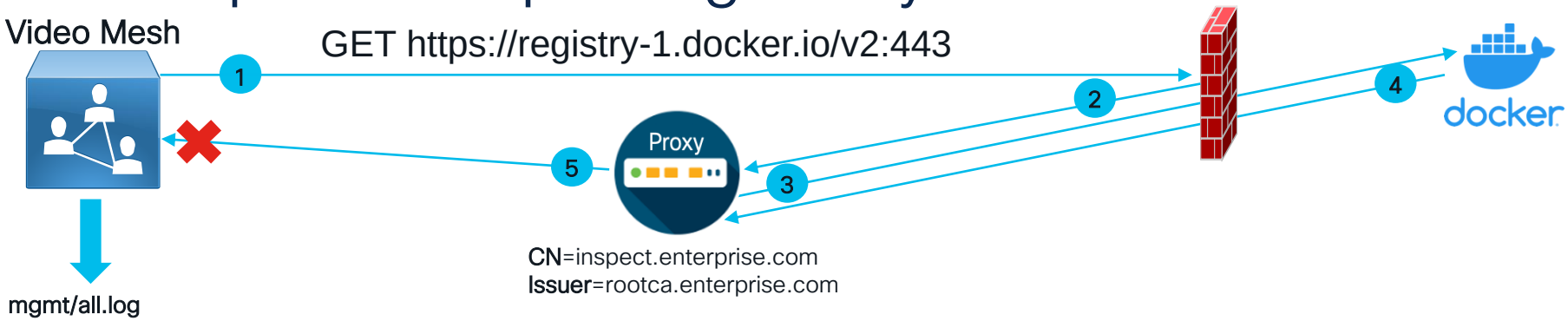
/proxyadapter/all.log

2020-07-14 00:38:19,478 --- pws processing request... for url:https://registry-1.docker.io/v2/ciscocitg/mfusionetcd/manifests/sha256:9645c8171560d850df2b9895e1ede7e56980ef96e03b5fa8d54240a4678bbd2f

2020-07-14 00:38:19,539 --- pws incoming proxyResponse:401/Unauthorized

{ "content-type": "application/json",
"docker-distribution-api-version": "registry/2.0",
"www-authenticate":
"Bearer
realm=\"https://auth.docker.io/token\",service=\"registry.docker.io\",scope=\"repository:ciscocitg/mfusionetcd:pull\",error=\"insufficient_scope\"",
"date": "Tue, 14 Jul 2020 00:38:19 GMT",
"content-length": "164",
"strict-transport-security": "max-age=31536000",
"cache-control": "proxy-revalidate",
"connection": "close",
"set-cookie": ["BCSI-CS-b12a1aad97a49d1e=1; Path=/"],
"proxy-support": "Session-based-authentication" }

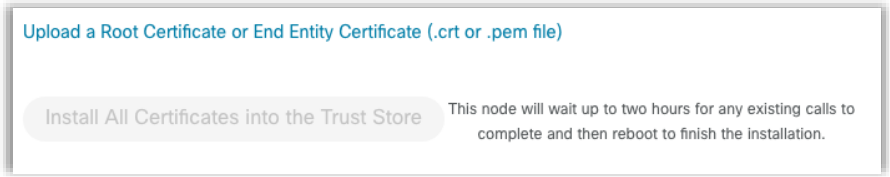
Transparent Inspecting Proxy



{"action":"PULL","config":
{"image":{"imageName":"index.docker.io/ciscocitg/mfusionetcd","imageTag":"2020.04.28.23m"},
"name":"mfusionetcd_2020.04.28.23m_cfg1.0","orgOrder":0,"runsOnCores":"2"},
"created":1593121489653,
"status":"FAILED","blockId":0,"blockTask":"REPLACE_IMAGE",
"blockOrigin":"replace container based on image tag/sha difference or cfg difference",
"started":1593121489657,
"failed":1593121489780,
"statusDetails":[{"error":"Error in docker pull (possible networking or docker daemon problem)",
"rawError":"**Error: (HTTP code 500) server error** - Get https://registry-1.docker.io/v2/: x509: certificate signed by unknown authority "}]}

Remediation Steps:

1. Upload Root CA certificate that signed the proxy to the VMN Trust store
2. Configure proxy to bypass Webex domains



Troubleshooting Meetings

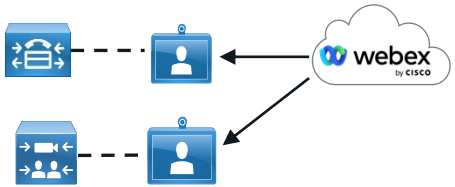
What's **Not** Supported?

- Webex Web App
  - https://web.webex.com

- Webex Full-Featured Meeting App

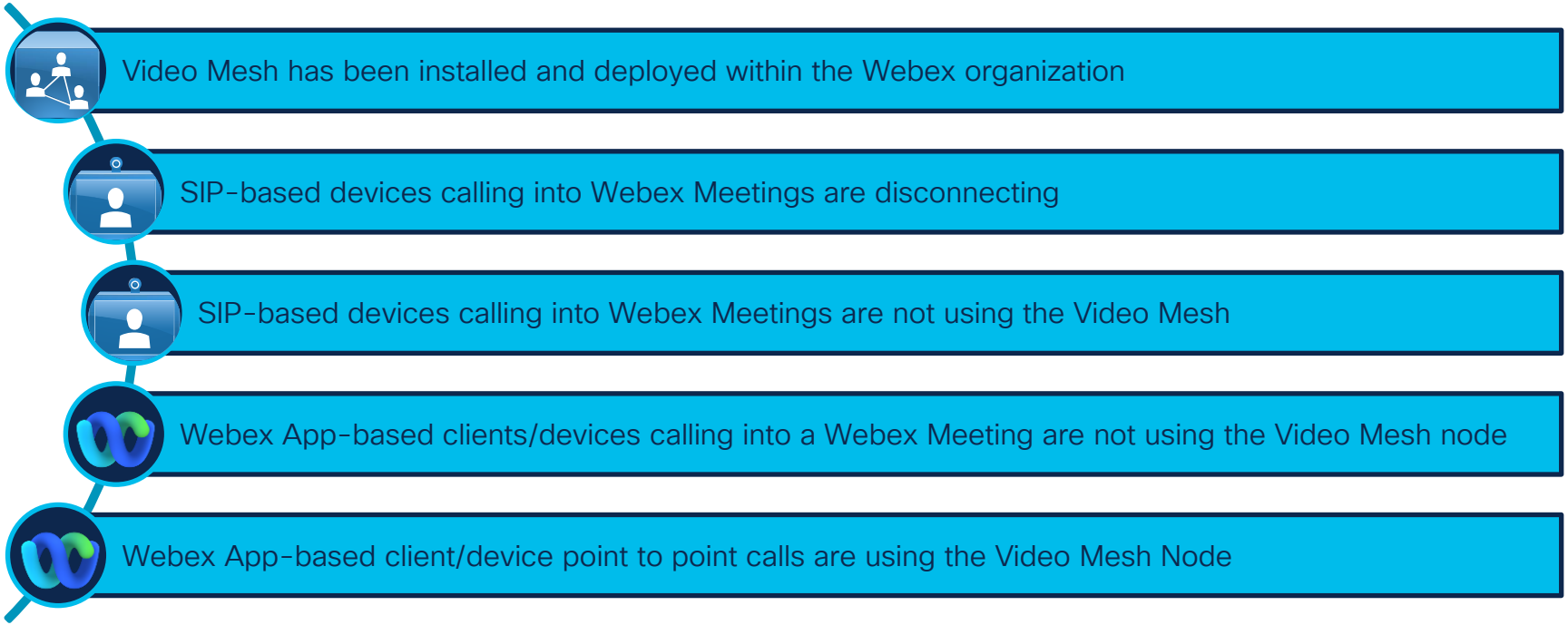
- Webex Calling registered phones

- Webex dialing back to SIP registered endpoints

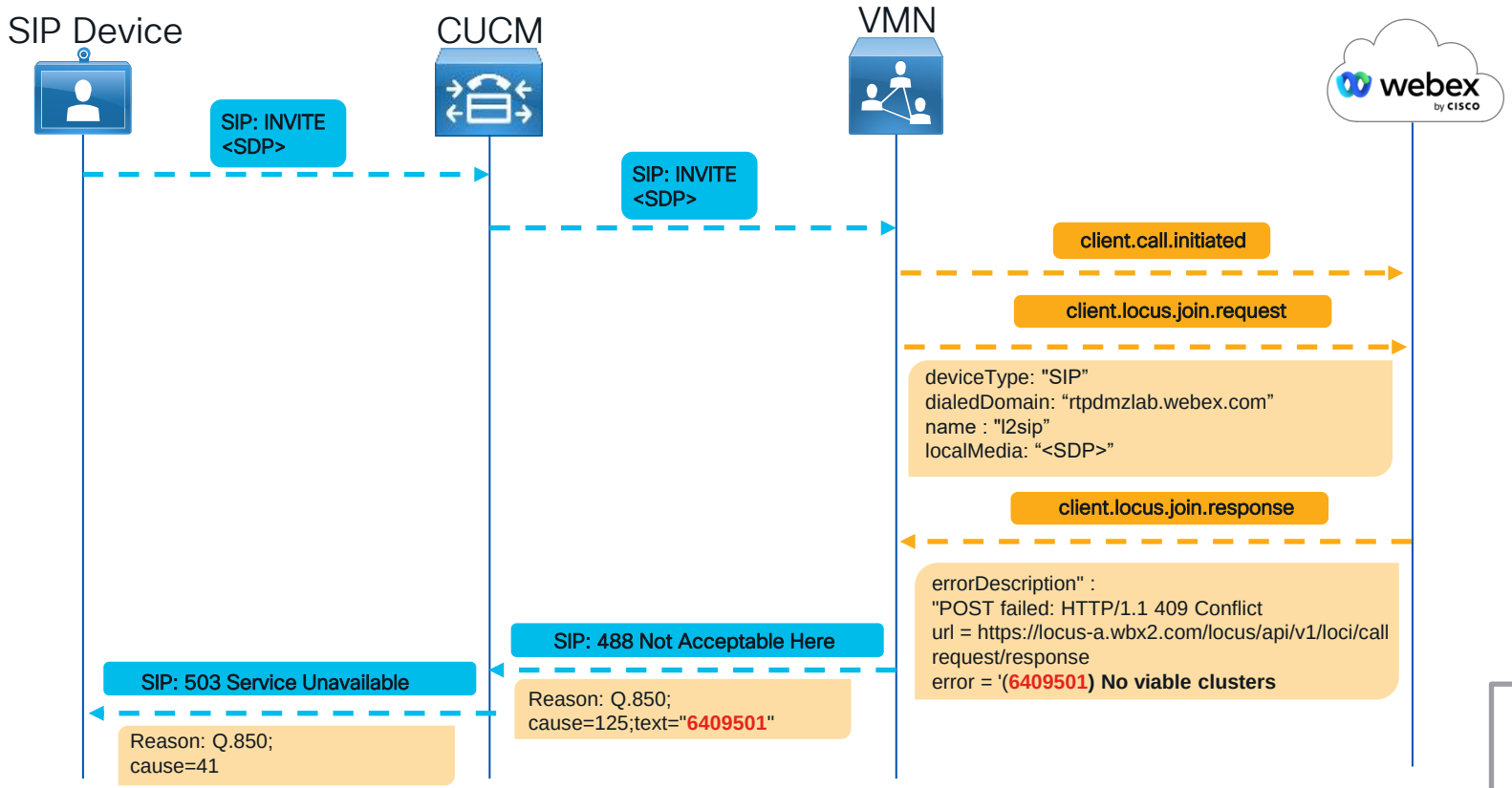


Video Mesh Node(s) Not Used

What our customers tell us



VMN Not Used: SIP Experience



VMN Not Used: Webex App Experience

/current_log.txt

2019-04-09T16:45:04.026Z <Debug> [0x70000e843000] MediaManager.cpp:1713 onTraceServersCompleted:In onReachabilityResultReady: earlyResult: 0, success: 1, traceResult: {"b522e1f2-553f-49a8-af80-9285a5d7f38e.rtp.*":{"clusterUsability":{"usable":"true"},"tcp":{"latencyInMilliseconds":"0","reachable":"true"},"udp":{"latencyInMilliseconds":"10","reachable":"true"}}

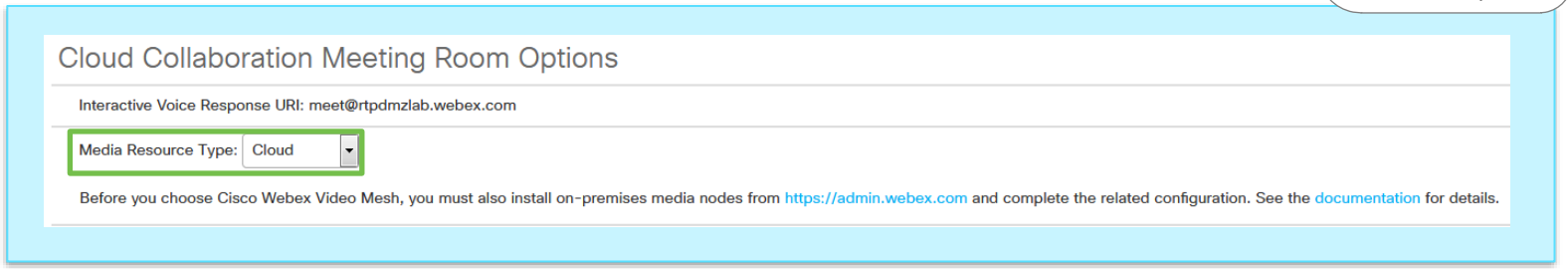
/media/current_log.txt

2019-04-09T16:45:12.929Z <Debug> [0x7000039f0000] ConnectionPeer.cpp:191 onCommandReceived:Received ipc::Command::Type::SetRemoteSdp

2019-04-09T16:45:12.929Z <Debug> [0x7000039f0000] ConnectionPeer.cpp:193 operator():Processing ipc::Command::Type::SetRemoteSdp

2019-04-09T16:45:12.933Z <Info> [0x10c60b5c0] WME:0 :[MediaSession] v=0
o=linus 0 1 IN IP4 207.182.171.147
s=-
c=IN IP4 207.182.171.147
b=TIAS:10128000

VMN Not Used: Resolution

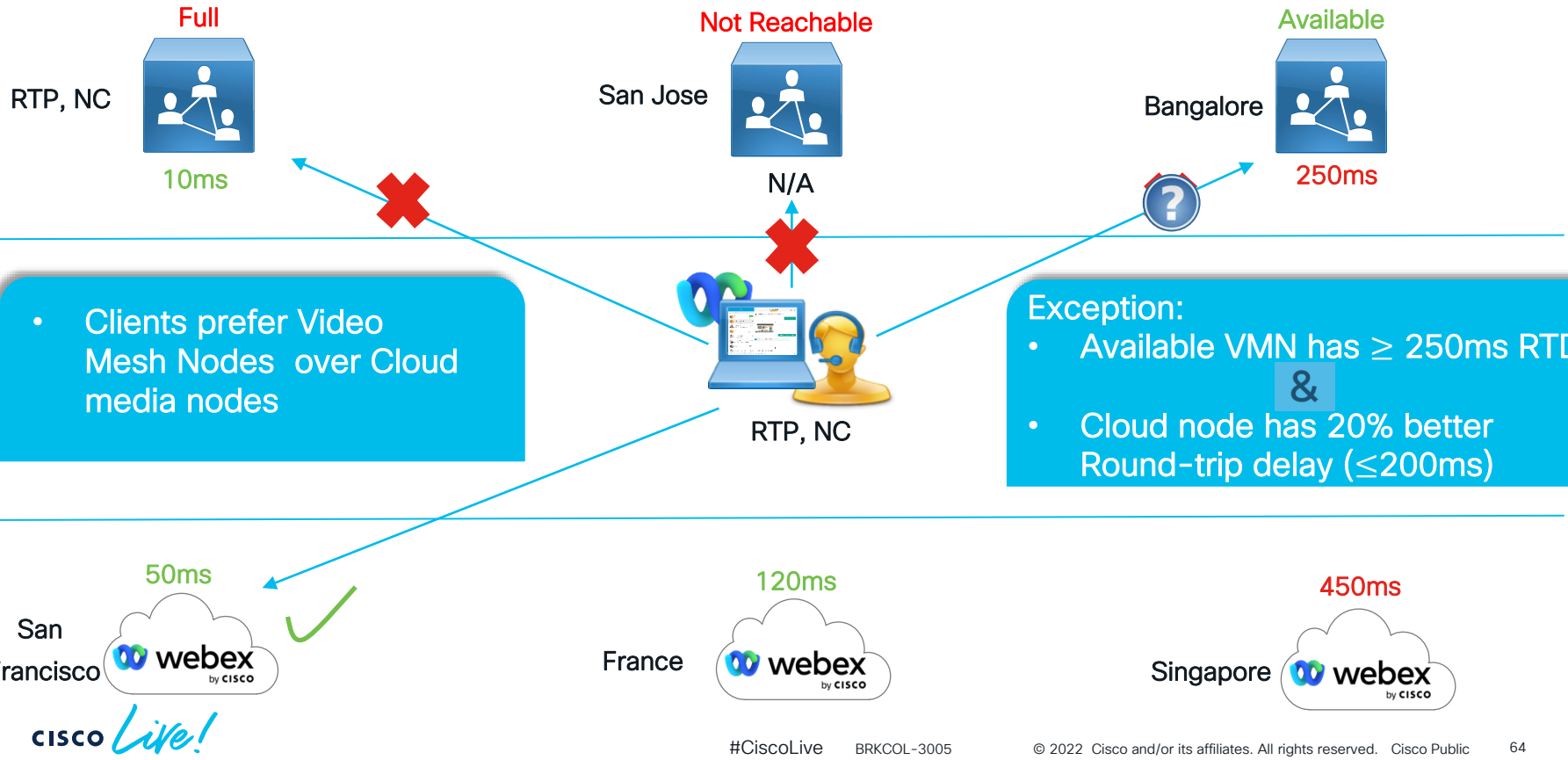


1. Login to Control Hub
2. Select **Services**
3. Select **Sites** under the *Meetings* card
4. Select the *Webex site* and choose **Configure Site**
5. Select the **Site Options**
6. Under the *Cloud Collaboration Meeting Room Options* select **Video Mesh** as the *Media Resource Type*.

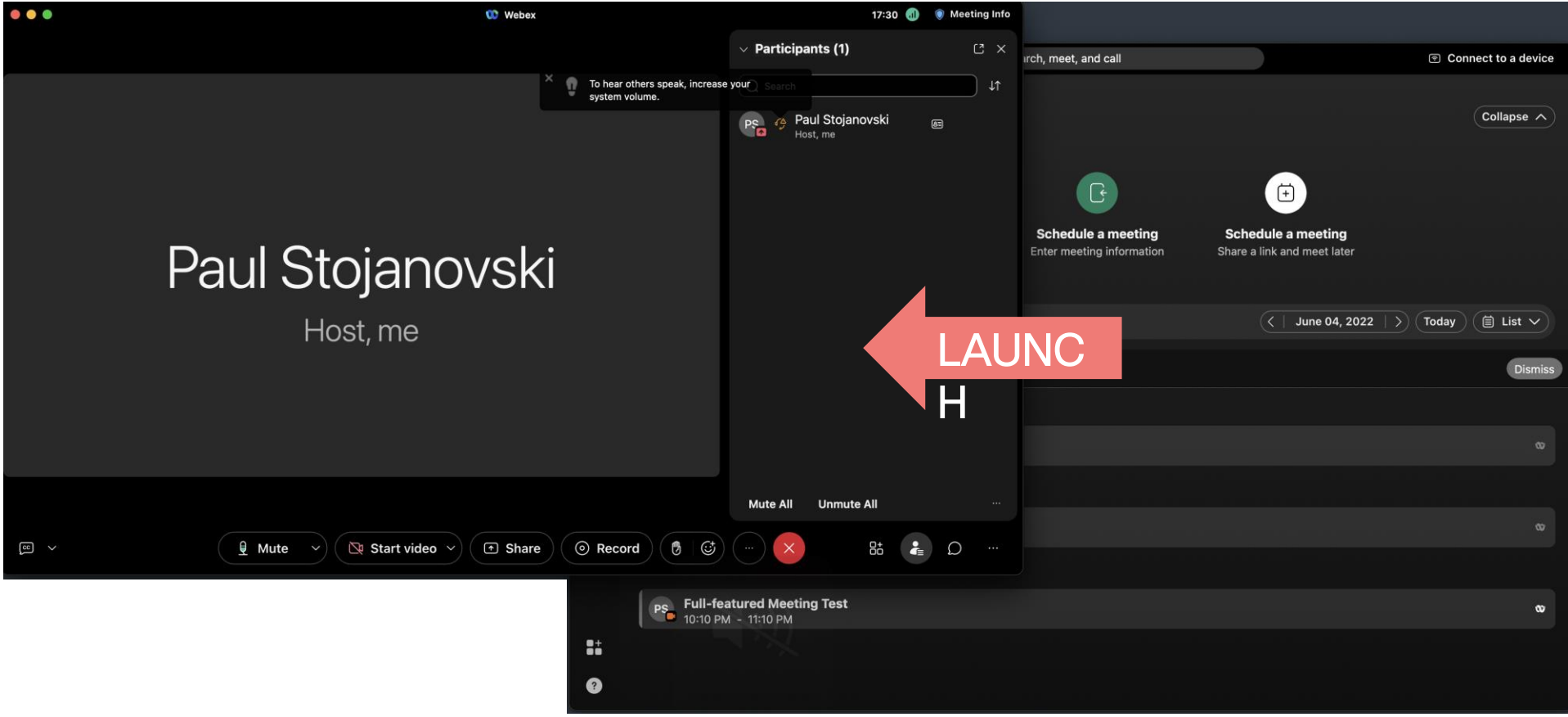
Other factors for why a Video Mesh is not used

1. The Video Mesh is:
   - Not reachable from client/device
   - Not usable (Maintenance mode, Offline)
   - At capacity
2. Misconfigured CUCM or Expressway call routing
3. SIP Trunk to Video Mesh is down
4. Video Mesh latency is 250ms and a Cloud-media node *(20% better)* has a lower RTT
5. Media Resource Type set to Cloud on the Webex Meeting site
   - Prefer Video Mesh for All External Webex Meetings set to False
6. Full-feature Meetings client or another unsupported client is being used

Excessive STUN Round-trip delay



Full Featured App Experience



Full-Featured Meeting App Log Analysis

```
2022-06-05T01:59:59.875Z <Info> [0x104780580] WebExCrossLaunch.cpp:2960
startWbxMeetingCommunicator:XLaunch
2022-06-05T01:59:59.876Z <Info> [0x104780580] WebExCrossLaunch.cpp:3004
startMeetingManagerSDK:XLaunch
2022-06-05T01:59:59.876Z <Info> [0x104780580] WebExCrossLaunch.cpp:3139
initMeetingManagerWrapper:XLaunch.
2022-06-05T02:01:21.762Z <Debug> [0x2b0573000] TelephonyService.cpp:9191
webexMeetingJoined:meetingIdentifier: 23444778179
2022-06-05T02:01:21.762Z <Info> [0x2b0573000] WebExCrossLaunch.cpp:1289
onMeetingJoined:XLaunch,
                23444778179
```

Indication that Full-Featured Meeting App is being used

Joined meeting number

Webex Split Meetings: Symptom

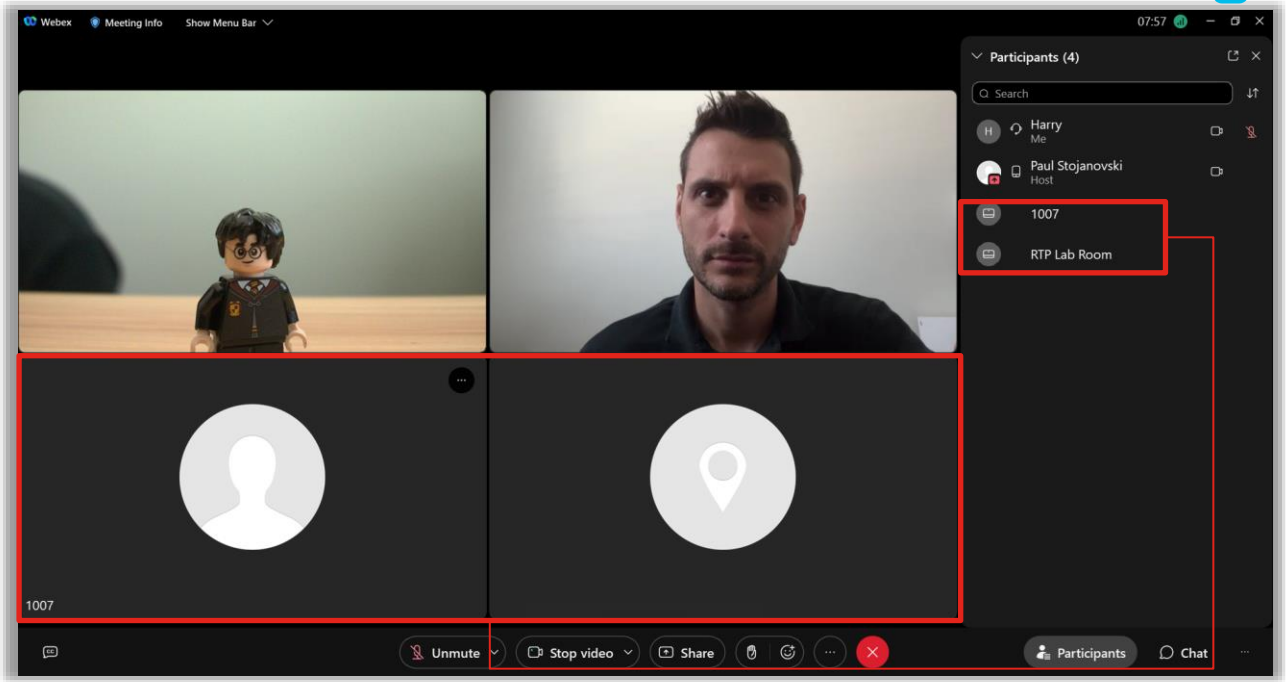
Okay....
So what now?

VMN-based participants see each other:

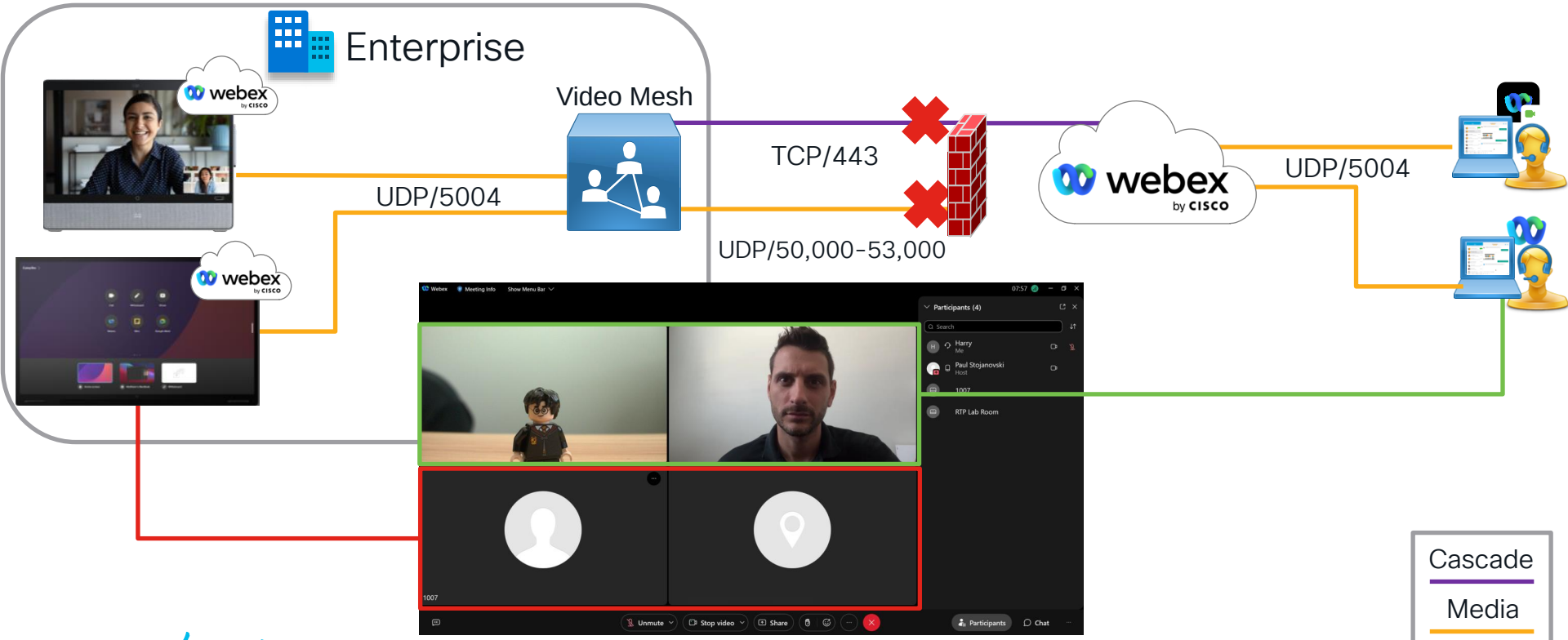
- Webex Devices
- Webex App
- SIP Clients

Cloud-based participants see each other:

- Webex Full-featured App
- Webex Devices
- Webex App



Consider the Cascade signaling and media paths

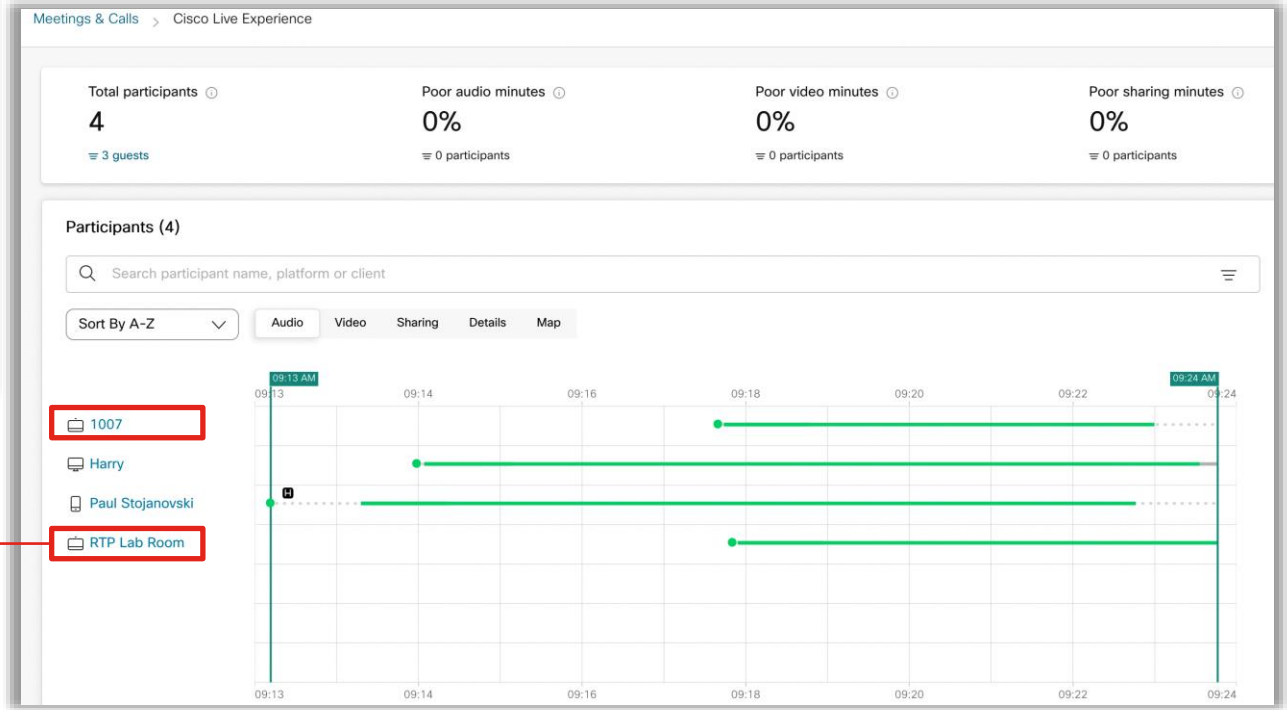


Leveraging Control Hub Troubleshooting

Equipment and Networks

Client:	Webex Room ce10.15.1.6 10270456893 2022-05-04
Hardware:	Board 55
Connection:	ethernet
Media Node:	VMS:US-RTP:192.168.1.75
Local IP:	192.168.3.240/28
Public IP:	Not Available
Audio Transport:	UDP
Video Transport:	UDP
Audio Codec:	Opus (Sending) Opus (Receiving)
Video Codec:	H.264 BP (Sending) H.264 BP (Receiving)

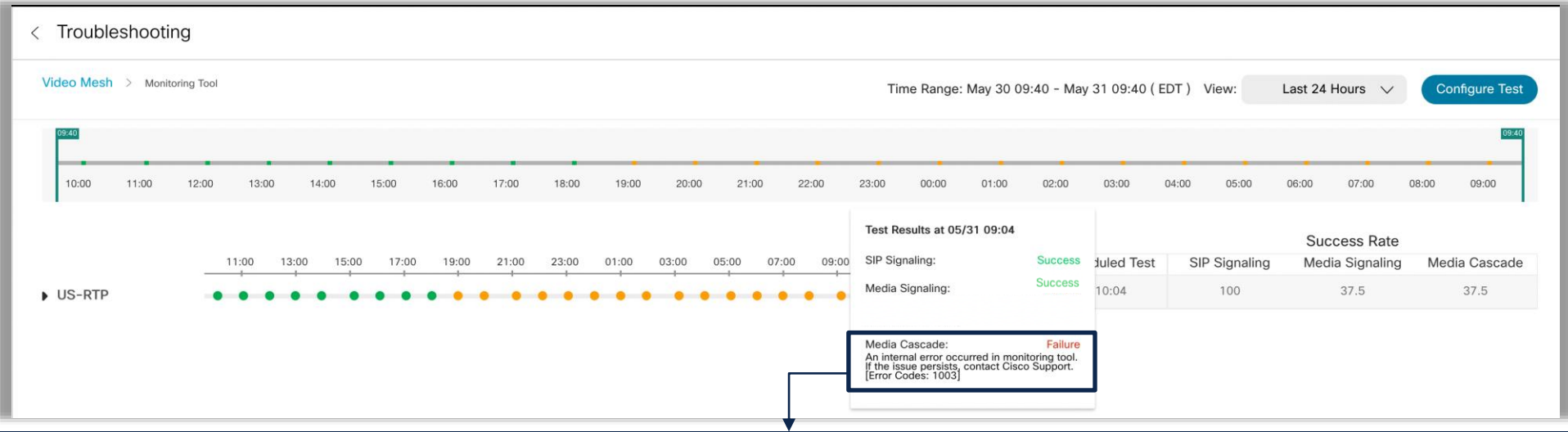
Troubleshooting > Meetings & Calls > Enter Conference Number



- Identify if all Devices or clients are joining the same Video Mesh
  - VMS:%Cluster_Name%:%Node%

Analyze Media Health Monitoring results

Troubleshooting > Status > Monitoring Tool

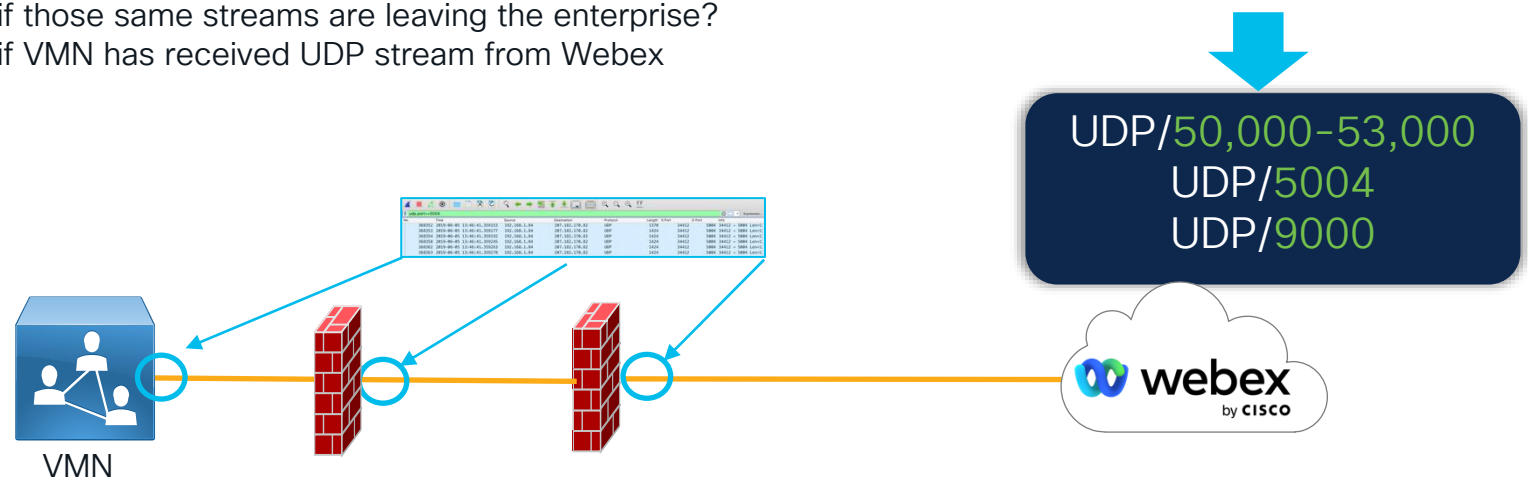


meetingshealth/wme.log

2022-06-01 13:13:54,350 INFO wme_logs: [nattool] this=0x2515940 [Audio], **1: PROG** 172.17.42.7:52024 (HO 1)-> **170.72.132.19:51030** (HO 1) UDP
2022-06-01 13:13:54,350 INFO wme_logs: [nattool] this=0x2515940 [Audio], **1: PROG** 172.17.42.7:52050 (HO 1)-> **170.72.132.19:5004** (HO 1) UDP
2022-06-01 13:13:54,350 INFO wme_logs: [nattool] this=0x2515940 [Audio], **2: SUCC** 172.17.42.7:52076 (HO 1)-> **170.72.132.19:9000** (HO 1) UDP

Structuring your troubleshooting

1. Run parallel packet captures from:
   - Video Mesh
   - Any firewall outside interface within the environment
2. Manually run the **Media Health Monitoring** tool
3. Leverage Video Mesh “meetingshealth/wme.log” to check the STUN tested **IP:Port** pair
4. Analyze the results
   - Determine if UDP traffic is being sent from the Video Mesh node outbound over our cascade media port range
   - Determine if those same streams are leaving the enterprise?
   - Determine if VMN has received UDP stream from Webex



Webex Split Meetings: Intermittent Issues
Webex IP Subnets for Media Services

- Cisco does not recommend restricting media to the Webex cloud by IP subnets
- For intermittent media issues ensure all IP subnet ranges for Webex media services are opened

IP subnets for media services			
18.230.160.0/25	20.108.99.0/24*	64.68.96.0/19	170.133.128.0/18
20.50.235.0/24*	23.89.0.0/16	66.114.160.0/20	173.39.224.0/19
20.53.87.0/24*	40.119.234.0/24*	66.163.32.0/19	173.243.0.0/20
20.57.87.0/24*	44.234.52.192/26	69.26.160.0/19	207.182.160.0/19
20.68.154.0/24*	52.232.210.0/24*	114.29.192.0/19	209.197.192.0/19
20.76.127.0/24*	62.109.192.0/18	150.253.128.0/17	210.4.192.0/20
		170.72.0.0/16	216.151.128.0/19

Note: Filtering Webex signaling traffic by IP address is not supported as the IP addresses used by Webex are dynamic and may change at any time. HTTP signaling traffic to Webex services can be filtered by URL/domain in your Enterprise Proxy server, before being forwarded to your firewall.

P2P Call Split Meeting

Cascade Signaling Failure

Webex Video Mesh Node

linus/rest.log

[2019-04-09 15:19:29,624] mc_proxy:create_cascade:1019[INFO] [TID None] - creating cascade device with peer_url wss://207.182.188.63:443/calliopews venue id a578f6ef-a5ea-3db5-b9ce-3dd4ed4b4561 peer id a578f6ef-a5ea-3db5-b9ce-3dd4ed4b4561__-1042559223613759903__b522e1f2-553f-49a8-af80-9285a5d7f38e.rtp.rtp12tpdmz118videomesh02rtpciscotacnet

[2019-04-09 15:19:29,648] mc_websocket_device:open_ws:64[INFO] [TID LINUS_8cca66c5-7d23-40b8-a30f-71709bc2fa6a_1-1] - Initializing

[2019-04-09 15:19:31,652] mc_websocket_device:_on_ws_proto_connect_error:141[INFO] [TID LINUS_8cca66c5-7d23-40b8-a30f-71709bc2fa6a_1-1] - error initializing websocket -> [Failure instance: Traceback (failure with no frames): <class 'twisted.internet.defer.CancelledError'>:

[[2019-04-09 15:19:31,656] mc_websocket_device:delete:78[INFO] [TID LINUS_8cca66c5-7d23-40b8-a30f-71709bc2fa6a_1-1] - Websocket device 0-98 delete, reason: web socket device create error

[2019-04-09 15:19:31,657] mc_device:delete:560[INFO] [TID LINUS_8cca66c5-7d23-40b8-a30f-71709bc2fa6a_1-1] - Device 0-98 delete, reason: web socket device create errorwebsocket connection to wss://207.182.188.63:443/calliopews

Case study

Case Study: Video Mesh Participants Drop Mid-Call

- **Original TAC Problem Description:**
  - *We had an issue with this meeting where two Videoconference systems randomly disconnected at around 9:15 AM ET*

- **Clarified TAC Problem Description:**
  - Intermittently video conference systems connected to any Video Mesh node across our geographic deployment will drop during core business hours.

Case Study: Video Mesh Participant Drops Mid-Call

TAC Observations:

- Issue was always reported between peak business hours 9-11AM EDT
- Video Mesh clusters were regionally deployed in US, EMEA, and APAC
- The node breakdown in those clusters were US1 (4), US2 (2), EMEA (2), and APAC (2)
- All regional traffic for Video Mesh would break out locally
- Participants in EMEA and APAC were landing on their local Video Mesh nodes
- Control Hub Diagnostics suggested a media disconnect on the Video stream

IF statements

- If this is a **media issue...**
- If media is **breaking out locally...**

THEN

*Why would this be happening across **all** Video Mesh nodes during **peak US business hours***

Case Study: Video Mesh Participant Drops Mid-Call

Webex Video Mesh Node

/linus/rest.log

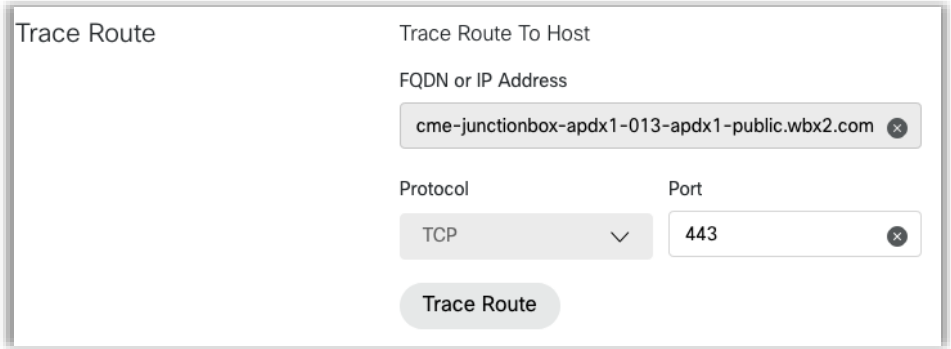
[2020-08-10 17:05:30,000] client:onOpenHandshakeTimeout:238[INFO] [TID None] - CJB_client: **onOpenHandshakeTimeout**, connection_id="ccdf5bd4-ebc5-4f6e-b30f-b1f25f2cb07d"
[2020-08-10 17:05:30,001] client:remove_and_build_missing_connections:1027[INFO] [TID None] - CJB_client: **Connection ccdf5bd4-ebc5-4f6e-b30f-b1f25f2cb07d is Failed**, prep_close="False"
[2020-08-10 17:05:30,002] client:fail:542[INFO] [TID None] - CJB_client: Connection **ccdf5bd4-ebc5-4f6e-b30f-b1f25f2cb07d** is failed, URL="**wss://cme-junctionbox-apdx1-013-apdx1-public.wbx2.com:443/calliopews**" args="()"
[2020-08-10 17:05:30,002] client:dropConnection:246[INFO] [TID None] - CJB_client: **dropConnection**, connection_id="**ccdf5bd4-ebc5-4f6e-b30f-b1f25f2cb07d**"
[2020-08-10 17:05:30,005] client:onClose:226[INFO] [TID None] - CJB_client: Websocket connection **ccdf5bd4-ebc5-4f6e-b30f-b1f25f2cb07d** Closed, clean="False", code="1006", reason="**connection was closed uncleanly (WebSocket opening handshake timeout (peer did not finish the opening handshake in time)**)"

This WebSocket connection represents the cascade link, not necessarily the media stream itself.

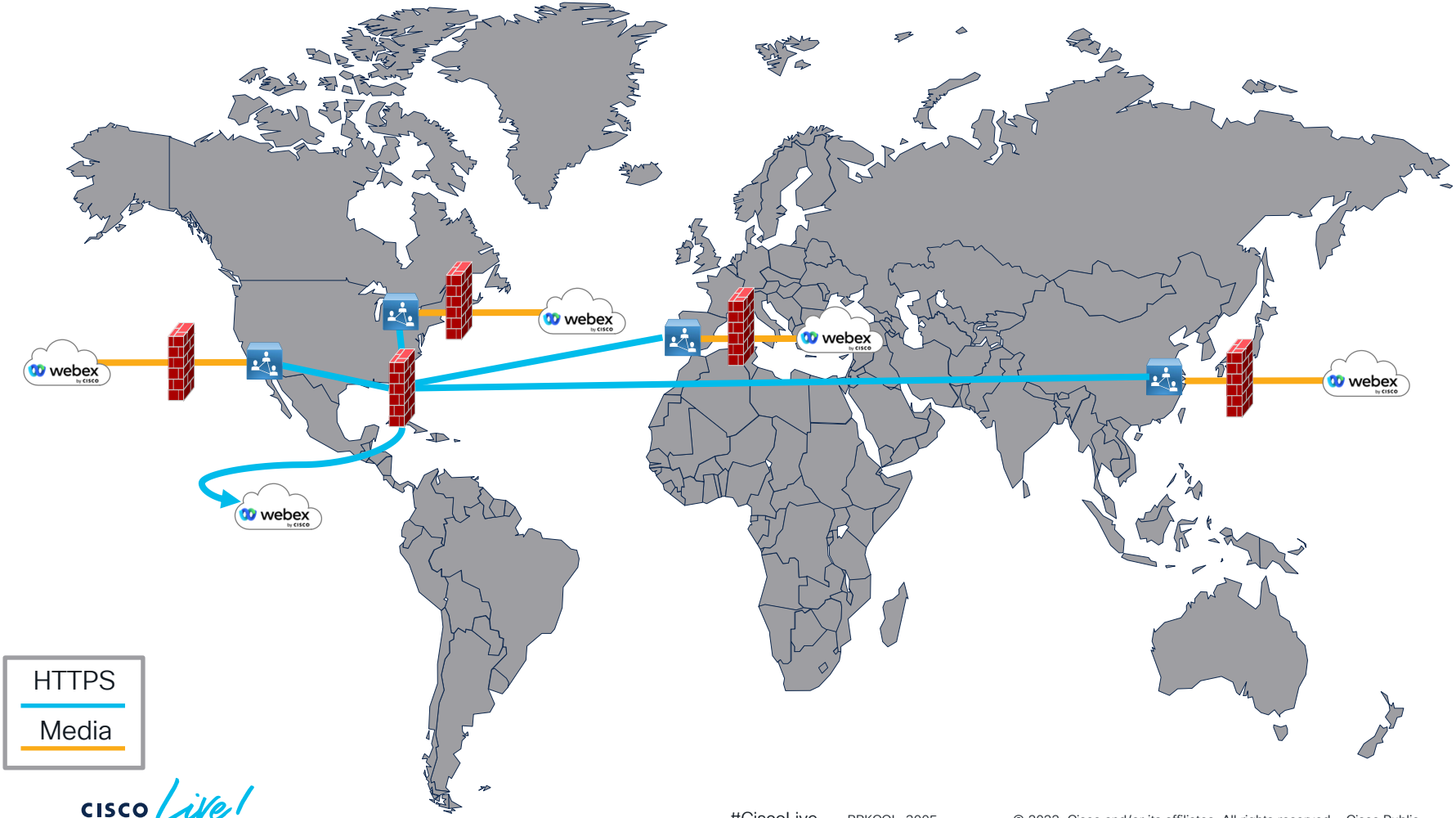
If the cascade failure persists for over 30 seconds the symptom is that the endpoint video will drop out

CE Endpoint reports this as KickedFromLocus Inactive

***r CallHistoryGetResult Entry 0 DisconnectCause: "KickedFromLocus (INACTIVE)"**
*r CallHistoryGetResult Entry 0 DisconnectCauseCode: 0
*r CallHistoryGetResult Entry 0 DisconnectCauseOrigin: Spark
*r CallHistoryGetResult Entry 0 DisconnectCauseType: RemoteDisconnect



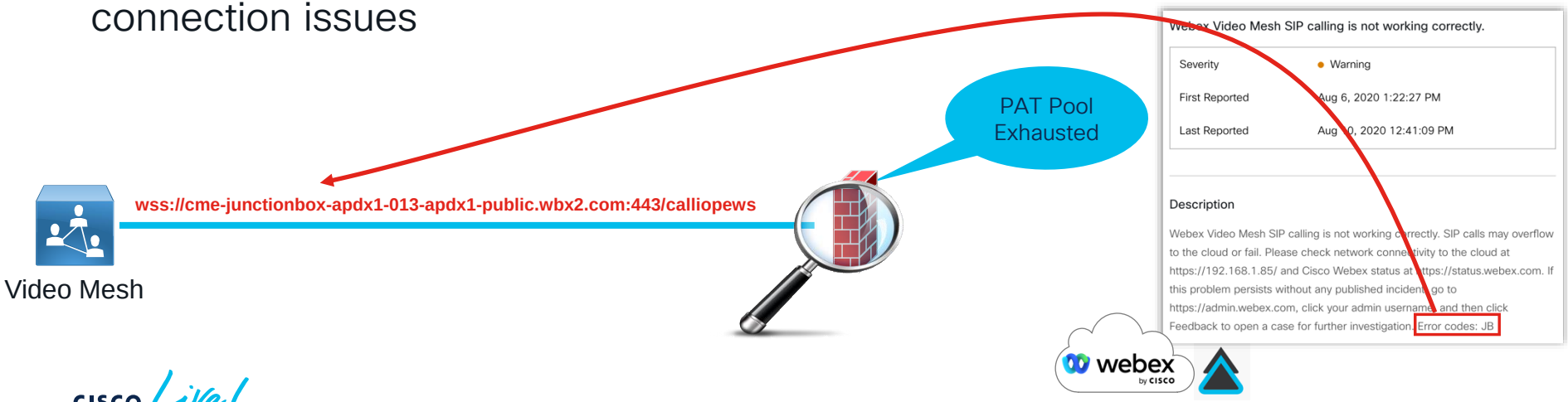
https://%VMN%/setup/#troubleshooting



Case Study: Video Mesh Participant Drops Mid-Call

Where did these findings leave us?

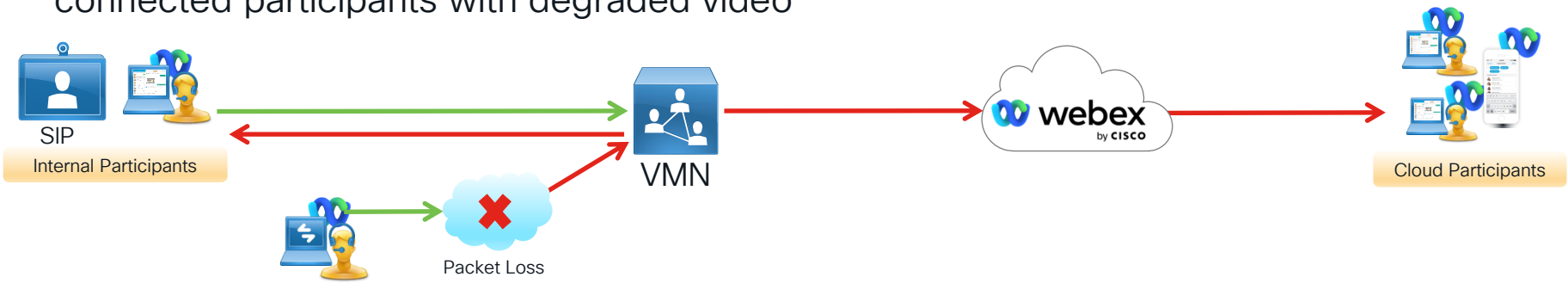
- This allowed us to narrow our focus onto the core data center
  - We validated that none of the Video Mesh nodes we're routing through proxy
  - We received a report that another Cloud application was experiencing connection issues



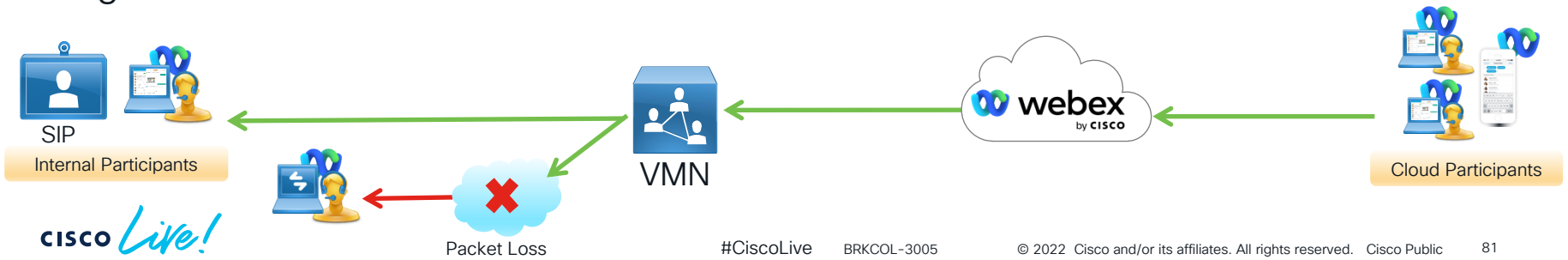
Isolating media issues

Media issues between internal participants and VMN

- All Video Mesh-connected participants and Cloud participants see some Video Mesh-connected participants with degraded video

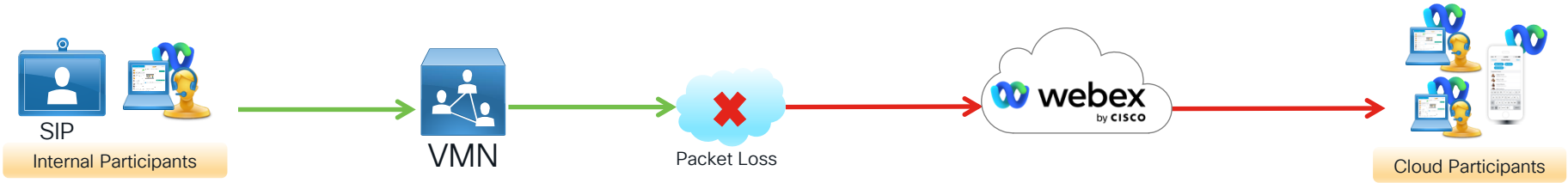


- Some Video Mesh participants see all Video Mesh and Cloud participants with degraded video

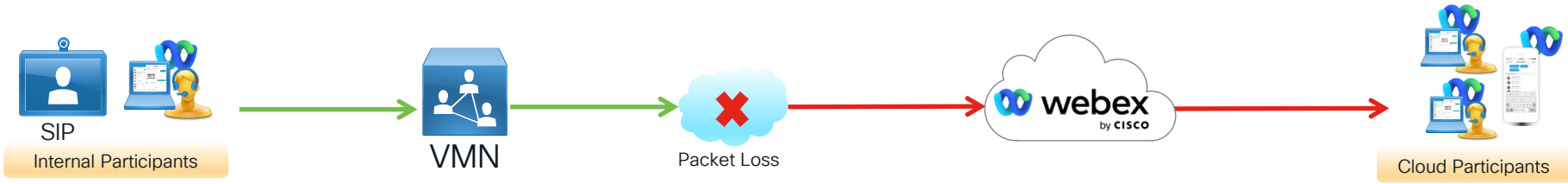


Media issues between Video Mesh and Webex

- All Cloud participants see all Video Mesh-connected participants with degraded video



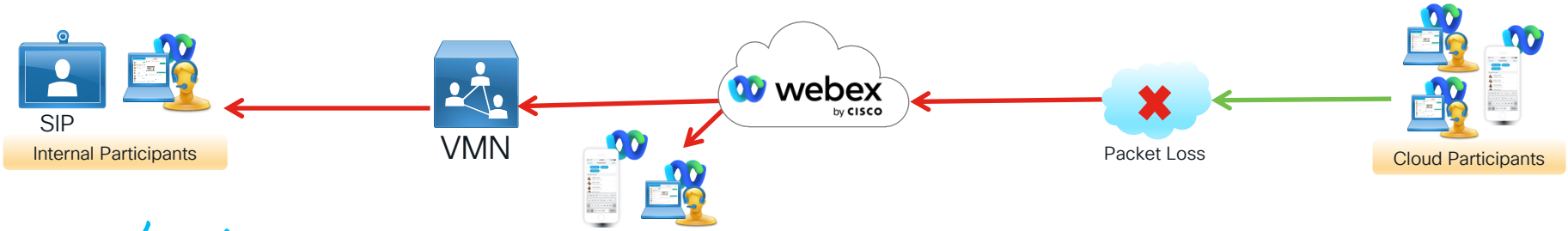
- All Video Mesh-connected participants see all Cloud participants with degraded video



Media issues between Webex and Cloud participants

- Some Cloud participants see all Video Mesh-connected participants with degraded video

- All Cloud and Video Mesh-connected participants some Cloud-connected participants with degraded video.



Conclusion

Troubleshooting Video Mesh

Mystery unraveled

1. Leverage Video Mesh **log and tooling** along with Control Hub **reports and analytics**

2. Understanding the Video Mesh **troubleshooting baseline** helps identify deviations

3. Remember the **common customer pitfalls** to avoid them in your environment

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

cisco Live!

Thank you


cisco Live!
ALL IN