Cisco Preferred Architecture for the Webex Video Mesh

Design Overview

March 2024

Contents

What's New in This Guide?

Table 1   Provides a historical list of updated and new topics added to this guide.

Date	Updated or New Topic	Update Details and Location
July 2021	Initial document publication	Initial release
March 2023	Throughout Document	Removed support for MM410v
March 2023	Hardware	Updated hardware options
March 2023	Capacity and Scale	Updated information
March 2023	Cascade Enablement	New configuration options
March 2023	Firewall	Updated to include new cascade port range
March 2023	QoS	New QoS port ranges
March 2023	GDM	Section added
March 2023	APIs	Section added
November 2023	Supported items	Webex App browser and Webex Suite Meetings Platform support
March 2024	Supported items	Updated supported Cisco Video devices. Added section on ThousandEyes support.

Preface

Cisco Preferred Architectures provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive, out-of-the-box, and built to scale with an organization as its business needs change. This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

Documentation for Cisco Preferred Architectures

- Cisco Preferred Architecture (PA) design overview guides help customers and sales teams select the appropriate architecture based on an organization's business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.
- Cisco Validated Design (CVD) guides provide details for deploying components within the Cisco Preferred Architectures. These guides support planning, deployment, and implementation (PDI).
- Cisco Collaboration Solution Reference Network Design (SRND) guide provides detailed design options for Cisco Collaboration. This guide should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

About This Guide

The *Cisco Preferred Architecture for the Webex Video Mesh* is for:

- Sales teams that design and sell collaboration solutions.

Customers and sales teams who want to understand the Webex Video Mesh architecture, its components, and general design best practices.

Readers of this guide should have a general knowledge of Cisco Voice, Video, and Collaboration products and a basic understanding of how to deploy these products.

This guide simplifies the design and sales process by:

- Recommending products in the Cisco Collaboration portfolio that are built for the enterprise and that provide appropriate feature sets for this market
- Detailing a collaboration architecture and identifying general best practices for deploying in enterprise organizations

For detailed information about configuring, deploying, and implementing this architecture, consult the related CVD documents on the Cisco Collaboration Preferred Architectures.

Introduction

The Webex Video Mesh is an extension of Webex Meetings that allows for local media processing of participant's video, audio, and content on the corporate network and dynamically creates cascade links to the Webex cloud joining all participants for a seamless meeting experience.

Technology Use Cases

The Cisco Preferred Architecture (PA) for the Webex Video Mesh delivers the benefit of keeping as much media local on the corporate network versus traveling out the Internet to Webex. This ability utilizes the corporate networks' quality of service configuration to enable a high-quality meeting for all participants connecting to the Video Mesh.

Benefits

- Quality and privacy: Local media processing improves the quality of audio, video, and data sharing and reduces Internet bandwidth consumption.

- Simplified resource planning: Transparent overflow to the cloud simplifies resource planning and solution sizing. Best of all, users get one seamless meeting experience, regardless of whether they are joining from devices or apps registered to the cloud or on-premises call control.

- Reduced operational overhead: Video Mesh offers a single management system, Control Hub, to provide cloud-based provisioning, usage metrics, and automated delivery of software updates.

- Security: Decreased open firewall ports when the Video Mesh node is deployed in the DMZ as it acts like a "Media proxy" for the meetings.

- Supports Webex Meetings

Available Services

The Video Mesh works in conjunction with Webex. It provides cloud-based services for media processing on the corporate network for collaboration devices and applications to use when attending Webex Meetings.

Webex App Modalities

The Webex App is a software client for mobile (iOS and Android) and Desktop (Windows and Mac) capable of multiple workloads connecting to different call control services using different media stacks to support various calling capabilities, features and call flows. Supported calling options in Webex are discussed in this article Webex | Supported Calling Options. The following nomenclature is used in this document going forward to delineate the various calling workloads in Webex App to differentiate the signaling and media stream requirements for identification and QoS classification:

Webex App

Webex App: This will refer to the native calling functionality for Webex App. It is used for Webex Space Meetings (meetings started from a Webex space), 1:1 calls to a Webex Account holder ("Call on Webex" calling option in Webex App) as well as SIP URI dialing. This is also the call functionality for Webex scheduled or Personal Room meetings for Webex Orgs enabled with Video Mesh Clusters or on the FedRamp program created prior to May 15th, 2021, or if Full-Featured Meetings has not been enabled or has been disabled. This workload was formerly accomplished with Webex Teams.

Webex App (FFM)

Webex App (FFM): Full-Featured Meetings is a feature enhancement to Webex App. When you start or join a Webex scheduled or Personal Room meeting from the Webex app, you get access to advanced features such as stage view, breakout sessions, reactions, Webex Assistant for Meetings (where available), and People Insights profiles. This is the default setting for Webex Meetings Orgs enabled after May 15th, 2021, unless the customer chose to opt out. All Webex Meetings Orgs enabled prior to May 15th, 2021, will have this feature enabled by default unless disabled for Video Mesh Cluster or on the FedRamp program.

Architecture

The Webex Video Mesh service allows for participants utilizing apps or hardware devices connecting to a Webex meeting to have local media processing. These devices can be registered to Webex or to an on-premises call control such as Cisco Unified Communications Manager and Cisco Expressway in this solution.

When a Webex meeting is started, each participant will connect to the meeting by either dialing the meeting SIP URI or clicking the green "Join" button on the app or device. The media will be routed to the local Video Mesh node cluster for local media processing of the video, audio, and content share for the meeting if the participant is on the corporate network or VPN'd into the corporate network. When the Video Mesh capacity is reached, the next participant on the corporate network will be automatically redirected to connect to the Webex cloud and attached to the Webex media resources.

Since there is a participant on the Webex cloud side of the meeting, whether it is an overflow participant or a participant joining from outside the corporate network, a cascade is created automatically from the Video Mesh cluster to the Webex meeting to join all the participants. Participants can then receive the audio, video, and content from any participant in the meeting. Figure 1 shows what this would look like for a single meeting with multiple different participants joining from the corporate network and remote participants joining to Webex from outside the organization.

Figure 1   Video Mesh Overview
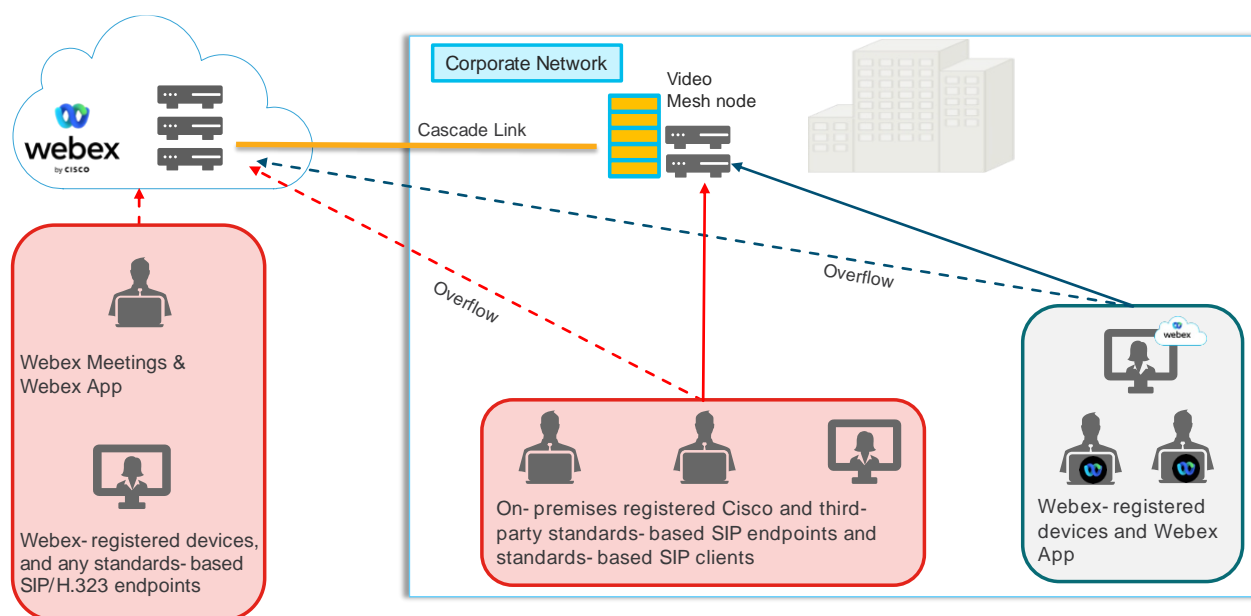
The Video Mesh software is installed as a single node or multiple nodes that are logically grouped together in a cluster. The cluster definition is created in the Control Hub and the nodes are placed in a cluster. A single cluster can have as little as one node or numerous nodes in a single cluster. There is not a hard limit to the number of nodes in a cluster or the number of clusters. In addition, an administrator can define multiple different clusters for their organization, but the physical location should be evaluated properly as it could have adverse consequences for bandwidth utilization and cluster selection predictability. For example, Cisco does not recommend having multiple clusters in the same city or region with very low latency from the clients. It is recommended to combine those nodes into a single larger cluster.

The cascade call flows are discussed in the cascade section for various scenarios to explain how signaling and media flows in the architecture.

The Video Mesh nodes can be placed inside the corporate network or in the DMZ. This decision normally comes down to the security policy of the organization and what traffic is allowed outbound from the LAN to the Internet.

Figure 2 shows a depiction of a common network with the Video Mesh nodes located either internally or in the DMZ. The Video Mesh nodes do not function like the Cisco Expressways and do not become firewall traversal devices. The Video Mesh nodes require a direct connection to the Internet and the Webex cloud. The administrators should decide ahead of the deployment whether they are going to deploy the Video Mesh node(s) inside the corporate network or in the DMZ, but not in both locations.

Figure 2   Video Mesh physical location
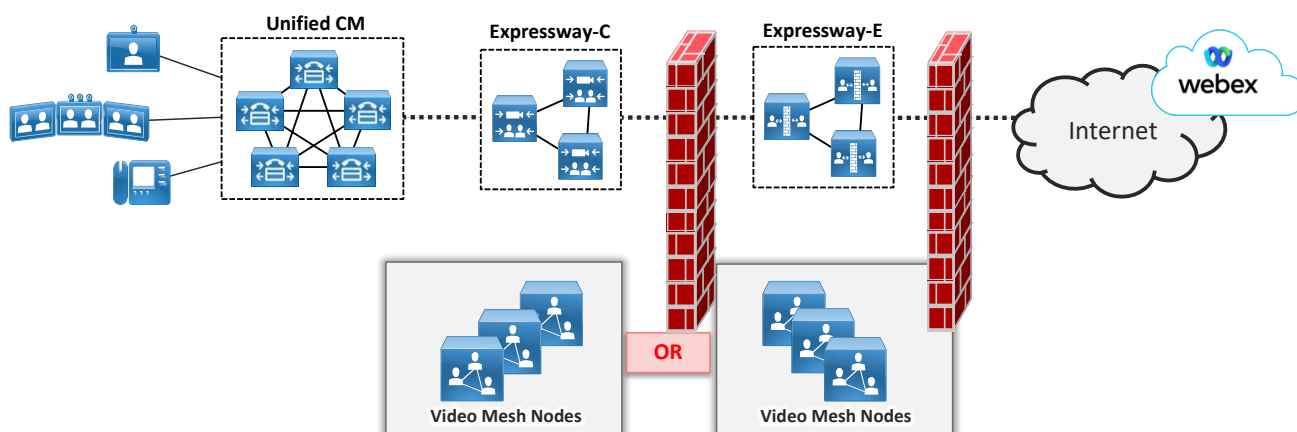
When thinking about deploying Video Mesh in the corporate network, it is good to understand what types of applications and devices can use Video Mesh. While the Video Mesh is very robust, it does not support all types of devices and meetings. The Video Mesh supports the following applications and devices when connecting to a Webex meeting.

- Any Webex registered Cisco Video device
    - Webex Share, SX, MX, DX, Room series and kits, Board series, Desk series
- Webex App (without the Full Featured Webex Experience toggle enabled, and Webex Suite Meetings Platform enabled)
    - Desktop or mobile
- Cisco Unified Communications Manager registered device
    - Video capable devices or applications such as the SX, MX, DX, Jabber, Webex Room, and Webex Desk series
    - Only uses a Video Mesh when calling a Webex scheduled or Webex Personal Room (PMR) meeting
- Cisco Video Communication Server or Expressway registered device
    - SIP or H.323 video endpoints. H.323 endpoints require Interworking.
    - Only uses a Video Mesh when calling a Webex scheduled or Webex Personal Room (PMR) meeting
- Webex App browser
    - web.webex.com

There are a few other devices and scenarios that do not use the Video Mesh node that should be taken into consideration when deploying the Video Mesh. The following do not use the Video Mesh for connecting to Webex meetings.

- Webex Calling IP phones
- Webex App with the Full Featured Webex Experience feature enabled

- Webex Meeting Desktop and Mobile application

- Call My Video System/SIP URI feature in the Webex account

  - Using this feature to call an on-premises registered video endpoint will not land the call on a Video Mesh node, the call will come back as a B2B call via the Expressways from Webex.

Hardware

The Video Mesh has two different software packages. These packages are only accessible from the Control Hub and can be located by going to Hybrid -> Video Mesh -> Settings. Once on that webpage, scroll down to the bottom of the webpage to see the download link for the two software options, "Full Software Image" and "Demo Software Image".

There are no licenses required to install the Video Mesh node specifically, but the Control Hub organization must have a meeting subscription for the Video Mesh to register to Webex.

Within the Full Software Image there are multiple deployment options during the installation process as seen in Figure 3.

- VMNLite

- CMS 1000

**Figure 3**   Video Mesh software options

The Cisco Meeting Server (CMS) 1000 and the 8-blade chassis, Cisco Meeting Server 2000 are supported hardware platforms from Cisco. The CMS 1000 hardware platform has a specific Video Mesh templates available to optimize the hardware resources available on each platform. The MM410v is a legacy hardware platform that cannot be purchased anymore and is not supported as a VMN platform now. The CMS 1000 or CMS 2000 are Cisco hardware platforms that can run either the Cisco Meeting Server software or Video Mesh software. These hardware platforms can be purchased

from Cisco. For more information on the CMS 1000 hardware specifications, click here and for more information on the CMS 2000, click here. The CMS1000 is the preferred hardware platform for use with the Video Mesh software.

The CMS 1000 and CMS 2000 hardware platforms allow for the full version of software or the VMNLite version to be installed on the hardware. The full version of software allows for all the capabilities that can be delivered for media processing based on the hardware platform's processing capabilities. This version allows for the optimum configuration to support any type of video endpoint connecting to the Video Mesh for a Webex meeting. The VMNLite is an optimized version for a specific set of participants, Webex registered video endpoints and the Webex App (without the Full Featured Webex Experience), to allow for greater scale for these types of participants versus the full version.

The VMNLite software will be installed multiple times on a CMS 1000 hardware platform and each installation is an individual Video Mesh. This combination of multiple VMNLite images on the CMS 1000 provides greater scale for all Webex registered participants. Co-residency of VMNLite VM with non VMNLite instances is not supported on the CMS 1000 and CMS 2000. Figure 4 shows a graphical representation of what it would be like to install VMNLite on a CMS 1000.

Figure 4   VMNLite on a CMS 1000

One instance of 70 vCPU VMN can be replaced with three instances of VMNLite on the same hardware.
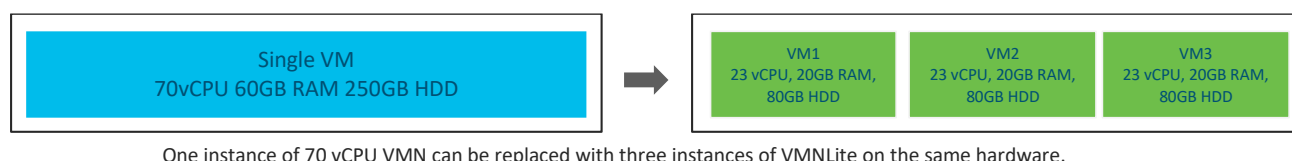
What is the difference between the VMNLite and the Full version? Historically in a traditional Multipoint Control Unit (MCU), there are functions within the software and hardware called transcoding and switching. Transcoding involves specialized video hardware that decodes the incoming video stream, manipulates the stream, and then re-encodes it before sending it on to the video endpoint. Switching does not require specialized video hardware but uses software instead. The incoming video and audio streams are copied and redirected to the correct video endpoints in the meeting, with no manipulation of the video stream. The transcoding process is more computational and requires more CPUs. The Video Mesh full version of software running on the CMS 1000 or CMS 2000 has both switching and large pool of resources for the transcoding process. If the corporate environment has many SIP based endpoints, then use the Full version and not the VMNLite. VMNLite is optimized for switching, which is used by the Webex App (without the Full Featured Webex Experience) along with the Webex registered endpoints and has a very minor number of resources dedicated to transcoding. Organizations can run any combination of Full version and VMNLite VMNs in the same cluster or in different clusters. When deciding which image to deploy consider the types of devices and applications being used in the network to install the proper image(s), VMNLite or Full version.

Cisco sells the CMS1000 hardware platform and the CMS 2000 hardware platform. The CMS 2000 is an 8-blade chassis, and each blade is a CMS 1000. The CMS 2000 can be designed to have local resources, CPU, RAM, and hard disk per blade or can use NFS storage for the chassis versus local disk per blade. NFS storage for a CMS 2000 requires peak IOPs (input/output operations per second) to be 300 IOPs. Additionally, the customer can run the Video Mesh images on their own hardware. The requirements for running Videos Mesh on CMS hardware or spec-based are in Table 2.

Table 2   System and Platform Requirements for the Video Mesh Node Software in a Production Environment.

Platform	Specifications	Notes
Cisco Meeting Server 1000	• 72vCPUs • 60GB main memory • 80GB local hard disk space	
Cisco Meeting Server 2000	• 72vCPUs • 60GB main memory • 80GB local hard disk space	• Each blade must be a complete Cisco Meeting Server 1000 with dedicated CPU, RAM and hard drives per blade.
	OR	
	• 72vCPUs • 60GB main memory • 80GB of NFS storage	• Each blade must have dedicated CPU and RAM. • Peak IOPs (input/output operations per second) for NFS storage is 300 IOPS.
Specification based configuration	• 2.6 GHz Intel Xeon E5-2600v3 or later processor • 72vCPUs • 60GB main memory • 80GB local hard disk space	• Each Video Mesh virtual machine must have dedicated CPU, RAM and hard drives.
	OR	
	• 2.6 GHz Intel Xeon E5-2600v3 or later processor • 72vCPUs • 60GB main memory • 80GB of NFS storage	• Each Video Mesh virtual machine must have CPU and RAM reserved for itself. • Peak IOPs (input/output operations per second) for NFS storage is 300 IOPS.

The Video Mesh software does not run on bare metal and requires a hypervisor layer. Video Mesh supports VMware software and use 2 vCPUs for the hypervisor software, version 6.5 or higher. In addition, hyperthreading needs to be enabled.

There is another version of the Video Mesh software that can be installed known as the Demo version. This version is available for organizations that would like to try out the functionality in a lab environment only and get an understanding of the product before putting a VMNLite or Full Software Image Video Mesh into production. The Demo version of the software requires a smaller number of vCPUs as it is designed to be used in a lab environment only. The demo version of software has the following requirements.

- 14vCPUs (12 for Video Mesh Node, 2 for ESXi)

- 8 GB main memory

- 20 GB local hard disk space

- 2.6 GHz Intel Xeon E5-2600v3 or later processor

While the Demo version is great for a lab there are other limitations to this version of software to be aware of when using it:

- No Cisco TAC support

- Cannot be upgraded to a full software version or VMNLite

- 90-day trial license

Software Installation

The Video Mesh software has a simple installation and configuration process. In fact, there is an EZ configuration wizard to assist the administrator with getting the node up and operational. More complexity will be introduced with integrating with different call control systems. This will be covered later in the Registration and Integration section.

As shown in Figure 5, first, the software will need to be downloaded from the Control Hub and installed on top of the VMWare hypervisor layer. This requires that the administrator install a new OVF template and point to the downloaded Video Mesh software image.
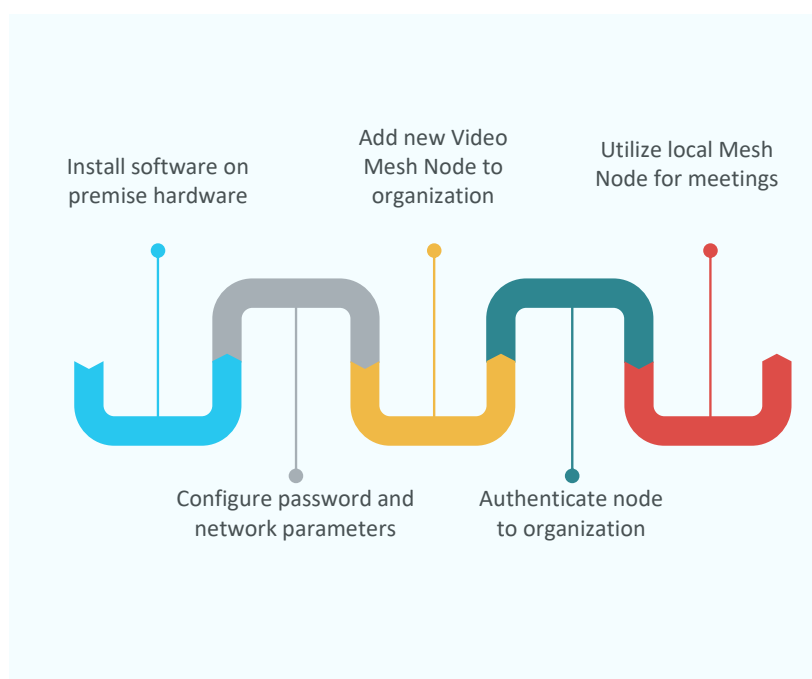
Once the Video Mesh software is installed on top of the VMware software, it requires basic network configurations such as IP address, mask, gateway, DNS and NTP server to be functional from a connectivity standpoint. The Video Mesh node will get a DHCP address at boot up, but it is recommended to change it to a static IP address and create a DNS A record for each node in the organization.

The configuration of the network settings can be done via the CLI, by initiating an SSH command to the device, VMWare console, or by going to the Video Mesh webpage, https://<Video_Mesh_ip_address_or_fqdn>/setup.

Now that the Video Mesh node has IP connectivity, the node first needs to register to a Webex org before it can be used. This registration process requires access to the Control Hub and Video Mesh node from the administrator's PC or Mac. The following steps are done during this process:

- Registration process starts from the Control Hub by adding a new node.
- Control Hub redirects to the Video Mesh node.
- Video Mesh node runs a series of connectivity checks.
- Customer administrator gives permission to register the device.
- Redirect back to Video Mesh node with an encrypted token.
- Video Mesh node checks account represented by the token for correct rights.
- Video Mesh node uses the token to create a unique machine account.
- Video Mesh node uses the machine account to register to the Webex organization.
- Registration is complete.

Figure 5   Video Mesh Installation Process

Once the Video Mesh is registered, the Control Hub will change its state to installing as it checks for any updates to any of the docker containers. Normally there is a software update, and this will take a several minutes to upgrade and then the node is available to handle calls for a Webex meeting.

Installing a single node via the GUI is perfectly fine, but if you are deploying multiple nodes this may not be the most efficient use of time. Cisco provides a way to programmatically deploy the Video Mesh nodes with the organization. This process involves creating a CSV file of the common parameters needed to be configured: username, password, IP address, mask, gateway hostname, DNS, NTP, etc. This file is used for input to the python script that runs and utilizes the Ovftool API provided by VMware. More information on the scripts can be found here.

When deploying a Video Mesh node, it can only be part of a single Webex organization, it cannot be registered to multiple different Webex organization and is not a multitenant node. Additionally, the Video Mesh node requires at least 10Mbps of upload and download speed on the Internet link to operate properly.

Capacity and Scale

The Video Mesh can be deployed on different hardware platforms from Cisco, the CMS 1000 and the CMS 2000. The deployed hardware along with the resolution of the meeting, 1080p or 720p, the types of devices or clients connecting to the meeting, the number of participants joining from the Webex cloud, and the overall topology of the meeting will all affect the capacity of each node. Each meeting is different and dynamic requiring different amounts of CPU to process all the video, audio and content for the local and remote participants at all different times in the meeting. Cisco provides general guidance on the capacity of a node as seen in Table 3 for the Full software version and Table 4 for the VMNLite software version.

Table 3   Full Version capacity

Scenario	Resolution	Participant capacity
Meetings with only Webex App participants	720p	100–130*
Meetings and 1-to-1 calls with only Webex App participants	720p	60–100*
Meetings with only SIP participants	720p	70–80*
Meetings with only SIP participants	1080p	30–40*
Meetings with Webex App and SIP participants	720p	75–110*

* Use these numbers as general guidance.

Table 4 VMNLite capacity

Scenario	Resolution	Participant capacity with 3 VMNLite nodes on a CMS 1K server
Meetings with only Webex App participants	720p	250–300*
Meetings and 1-to-1 calls with only Webex App participants	720p	175–275*

* Use these numbers as general guidance.

When sizing a node, it is best to use the conservative numbers and monitor the utilization in Control Hub to evaluate if more capacity is needed. The key charts in the Control Hub to monitor are the Redirects and Overflows. These are discussed in the Control Hub section of the document.

Registration and Integration

The Video Mesh is available as a media resource to different endpoints and applications for a Webex meeting. These endpoints and applications can be registered to Webex, Cisco Unified Communications Manager, or the Video Communications Server and the Expressway products. Depending on the registration point, additional configuration and considerations are needed. More details are provided in the following sections.

Cloud Registration

Cisco video endpoints registered to Webex along with the Webex App (without the Full Featured Webex Experience) can find the Video Mesh nodes automatically when doing a 1:1 meeting or a multi-participant Webex meeting. There is a process built into the software called "Cluster Reachability" that will perform a latency test to the Video Mesh cluster(s) on the corporate network and to the cloud Webex media resources. At the point of startup, network change, or cache expiration which is every 2 hours, the video endpoint or application will ask Webex for a list of media resources that are candidates for the video endpoint or application to use as a media resource. The Webex service will provide the video endpoint or application a list of clusters and a randomly selected node in each cluster. The video endpoint or application will do a STUN Ping test to each randomly selected node and record the information. These results are used to figure out which clusters are reachable from the video endpoint or application when joining a meeting. Figure 6 shows an example of the Webex App (without the Full Featured Webex Experience) log showing the reachability results to the "hq_sydney" cluster in that organization. The application can reach the cluster node, represent by "reachable: true", for TCP and UDP along with displaying the latency in milliseconds for the STUN Ping test for each protocol. The preferred connection for media is UDP.

Figure 6   Cluster reachability results

Reachability to clusters (Video Mesh Clusters) ────────── Cluster Name

35a15b0a-0ef1-4029-9f63-a7c54df5df59.hq_sydney.*":

{"clusterUsability":{"usable":"true"},"tcp":{"latencyInMilliseconds":"90","reachable":"true"},"udp":{"latencyInMilliseconds":"88","reachable":"true"}},
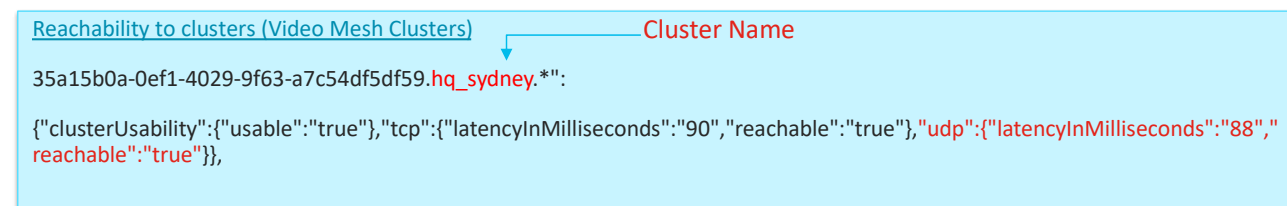
Once the video endpoint or application has the media resources, it can now utilize them when joining a Webex meeting. The Webex registered endpoint or Webex App (without the Full Featured Webex Experience) will use this information to ask a Webex service which media resource to use for the meeting. The Webex service chooses the Video Mesh cluster to use based on the cluster reachability results. It will choose the closest node to the device or application unless there are not enough media resources in that cluster. If the test results failed in the cluster reachability test, the cluster will not be considered. The Webex service will use the on-premises clusters before any Webex media resources in the cloud. For example, if the corporation has 3 clusters, US, Italy, and Australia, the Webex device or Webex App (without the Full Featured Webex Experience) will try to use all three of those clusters before going to any of the publicly available Webex cloud media resources. This is true in all cases, except for one case, where a cloud media resource could be used before a Video Mesh cluster on the corporate network. This situation happens when there is a vast distance between the Webex device or Webex App (without the Full Featured Webex Experience) and the corporate Video Mesh clusters. The device or application will use the cloud node instead of internal Video Mesh nodes if the round-trip timer (RTT) >= 250ms to the Video Mesh node and cloud node's RTT is 20% less (200ms or less) than the internal Video Mesh clusters. This mechanism is not configurable and happens dynamically.

Cisco On-Premises Call Control Integration

The Video Mesh nodes can be integrated into the Cisco on-premises call control applications such as Unified Communications Manager and Video Communication Server or Expressway. This integration allows for non-cloud registered devices to utilizes the Video Mesh for Webex meetings. This integration is not dynamic and does not use the cluster reachability concept discussed earlier, instead it relies upon SIP call routing. In Unified Communications Manager this is accomplished via a SIP trunk configuration or in the case of a Video Communications Server or Expressway a Neighbor Zone is used. These call control specific configurations route the meeting request in SIP signaling to the Video Mesh node. In the call control integration architecture, the administrator can use either call control, both of which route SIP requests but it is not recommended to use both Unified Communications Manager and Video Communication Server/Expressway with Video Mesh at the same time. Figure 7 shows how the on-premises call control can connect either the SIP trunk or the Neighbor Zone to the Video Mesh node(s).

Figure 7 Integration mechanisms
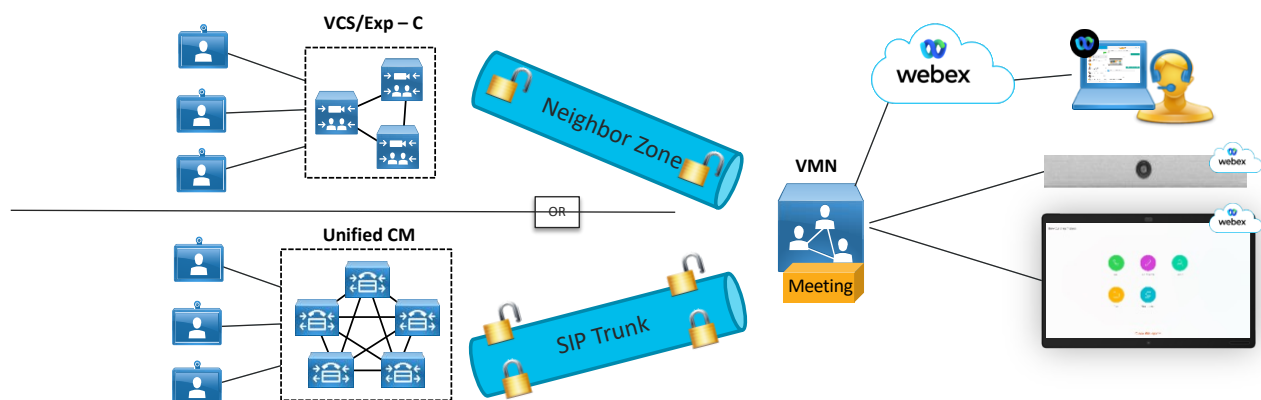
Unified Communications Manager Integration

The Unified Communications Manager integration utilizes the SIP trunk functionality to make a secure, port 5061 or unsecure, port 5060 connection to the Video Mesh node. This configuration will allow Unified Communications Manager endpoints that dial a Webex meeting to use the SIP trunk to connect to the Video Mesh node and keep the media local between the endpoint and the Video Mesh node.

To configure this integration, the following needs to be done for an unsecure SIP trunk configuration:

- Create a SIP Profile for the Video Mesh trunk
  - Modify Early Offer Support to "Best Effort (no MTP inserted)"
  - Make sure SIP Options Ping is Enabled (default setting)
- Create a new non-secure SIP Trunk Security Profile
  - Use default settings
- Create a new SIP Trunk
  - Name the trunk
  - IPv4 or FQDN of the Video Mesh
  - Destination Port - 5060
  - Add the non-secure Video Mesh SIP Trunk Security Profile
  - Add the Video Mesh SIP Profile
  - Run On All Active Unified Communications Manager Nodes

- Calling and Connecting Party Info Format
  - Deliver URI and DN in connected party, if available.

To create a secure SIP trunk using TLS on port 5061, the below additional criteria need to be met prior to the configuration:

- Unified Communications Manager needs to be in Mixed Mode.

- Certificate Management between Unified Communications Manager and the Video Mesh nodes.

- All Video Mesh nodes must be enabled with a secured trunk in the organization.

- Endpoints must use encrypted connections to the Video Mesh. Endpoints running without encrypted connections to the Video Mesh will fail unless a secondary path exists such as a SIP trunk to the firewall traversal Expressways to reach Webex.

- The Control Hub needs the Media Encryption toggle enabled along and the Trusted SIP Sources need to be defined. The Trusted SIP Sources are the Unified Communications Manager publishers and subscribers.

For the secure SIP trunk configuration in Unified Communications Manager configuration, the following steps will be needed:

- Create a SIP Profile for the Video Mesh
  - Modify Early Offer Support to "Best Effort (no MTP inserted)"
  - Make sure SIP Options Ping is Enabled (default setting)

- Create a new secure SIP Trunk Security Profile
  - Device Security mode: Encrypted
  - Incoming and outgoing: TLS
  - X.509 Subject Name
  - SIP V.150 Outbound SDP Offer Filtering: Use Default Filter

- Create a new SIP Trunk
  - Enable sRTP Allowed
  - Run On All Active Unified Communications Manager Nodes
  - Calling and Connecting Party Info Format
    - Deliver URI and DN in connected party, if available.
  - Destination Address
  - Destination Port - 5061
  - Add the secure Video Mesh Trunk Security Profile
  - Add the Video Mesh SIP Profile

For secure setup, the administrator needs to successfully complete a TLS handshake to establish two-way trust between the Unified Communications Manager and the Video Mesh node(s). In combination with the secure trunk configuration, this allows encrypted SIP signaling traffic and SRTP media in corporate network from the trusted Unified Communications Managers to land on trusted Video Mesh nodes. In a clustered environment, the administrator must install CA and server certificates on each Video Mesh node individually.

After the SIP trunk is established, proper call routing needs to be setup so that a device that dials to the corporation's Webex meeting site, *sitename.webex.com*, are routed to the SIP trunk pointing to the Video Mesh node(s). The *sitename*

is the unique name for the Webex site per organization. Media traffic from the endpoint device will go directly from the device to the Video Mesh.

Video Communication Server (VCS) or Expressway

Video Mesh can also integrate with the Video Communication Server (VCS) or Expressway call control. In either case the inside device or "C" (core), or the external device "E" (edge), can setup a neighbor zone to the Video Mesh node. To configure this integration the following needs to be done.

- Create a neighbor zone for the Video Mesh Node

    o Port 5060 (TLS port 5061 is not supported)

    o Add the Video Mesh IP address or FQDN in the peer IP address

- Create a search rule for Video Mesh Node calls

Cascade Enablement

While having an integration to a Cisco call control is an option and very common, there needs to be a configuration change on the Control Hub to enable the Video Mesh to create a media cascade to Webex. The media cascade allows the connection of media from the on-premises Video Mesh node(s) to the Webex meeting so all participants can see the video, audio, and content shared in the meeting. More will be discussed in a later section around cascades and cascade flows, but one parameter needs to be changed from the default setting to allow cascades to happen. Within Control Hub, under the meeting site's Common Settings, the Media Resource Type of the Cloud Collaboration Meeting Room Options needs to change from "Cloud" (the default) to "Video Mesh". Figure 8 shows the enablement option screen. This change from "Cloud" to "Video Mesh" is important because that tells the Webex meeting that it will accept media cascades from the Video Mesh into the meeting and that participants can land on the Video Mesh nodes for any meeting. If this is left to the default setting (Cloud) then a media cascade will not be established, and all participants of the meeting will join the Webex meeting in the cloud and not use the Video Mesh node.

Figure 8   Cascade Enablement

But what if there is a Webex meeting hosted by another organization that has not changed this parameter? Well in that scenario even though the administrator has installed Video Mesh nodes and the administrator has configured the site's Media Resource Type to "Video Mesh", the local Video Mesh nodes will not be utilized because the Webex meeting is hosted by an external organization with their Media Resource Type set to Cloud. To negate the meeting participants from going to the Webex cloud media resources and use the corporate Video Mesh nodes, an additional setting needs to be enabled. The "Prefer Video Mesh for All External Webex Meetings" is a global Video Mesh setting that will allow the participants of any externally hosted Webex meeting to use the Video Mesh nodes in the network, assuming they have capacity to support the participant, no matter what the host's Media Resource Type is set to. In Figure 9, if the toggle is enabled, this will utilize the corporate Video Mesh nodes even when the host Webex meeting site has the Media Resource Type set to Cloud. Cisco recommends all Video Mesh customers to enable this toggle.

**Figure 9**   Prefer Video Mesh for All External Webex Meetings
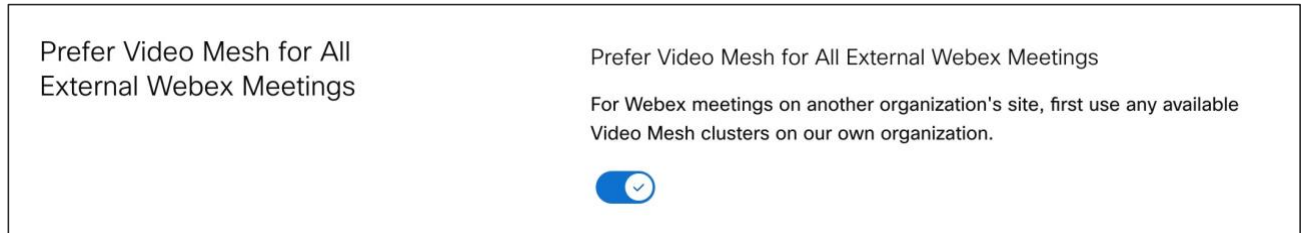
DMZ deployment

The Video Mesh node can be deployed inside the internal network or in the DMZ. Either deployment is supported and may be dictated by the security policy of the organization. For example, there may be a policy where the internal devices are not allowed to have direct Internet access without terminating on a device in the DMZ, such as the Video Mesh.

The Video Mesh node supports a deployment in the DMZ and Figure 10 shows an example of a DMZ deployment architecture.

Figure 10   DMZ architecture
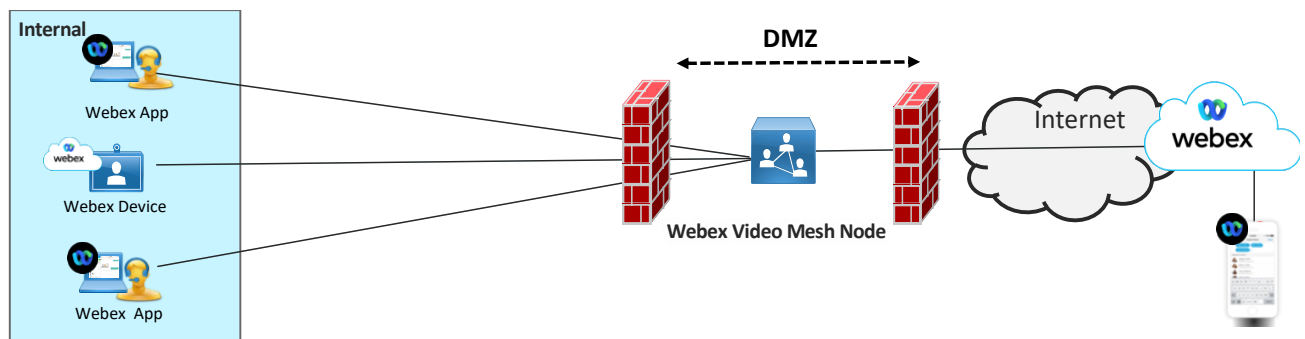
The following are key considerations when deploying a Video Mesh node in the DMZ.

- External media does not traverse the internal network.

- All media for internal participants goes to the DMZ.

- Meets security requirement policies disallowing direct media connections to the Internet from the internal network.

When deploying a Video Mesh node or cluster in the DMZ there is the ability for the admin to setup the Video Mesh node with a single or dual network interface card configuration. The secondary interface which is the outside interface is disabled by default and will need to be enabled via the CLI or the Video Mesh webpage interface. In a cluster of Video Mesh nodes, all network interfaces must be setup the same way, either single NIC or dual NIC, not a combination of both. The Video Mesh does support NAT and PAT. Additionally, Cisco provides a list of Webex resources so the firewall administrator can permit the traffic from the Video Mesh nodes to the Webex resources needed for the meeting. Refer to the following article when configuring the firewall for outbound traffic from the Video Mesh node https://help.webex.com/en-us/WBX264/How-Do-I-Allow-Webex-Meetings-Traffic-on-My-Network - id_135011.

In the DMZ, when enabling the secondary interface, this interface is the outside interface and is used for external communication to the Webex services. The internal interface is used for internal media connection, command line interface (CLI), webpage interface, and SIP communications from Unified Communications Manager or VCS/Expressway call controls. The secondary interface is used for cascade signaling and media, WebSocket connections and any HTTPs traffic to Webex. Figure 11 shows a diagram of the internal and secondary interfaces used with a dual NIC configuration in the DMZ.

Figure 11 Services on the Video Mesh node in a Dual NIC configuration
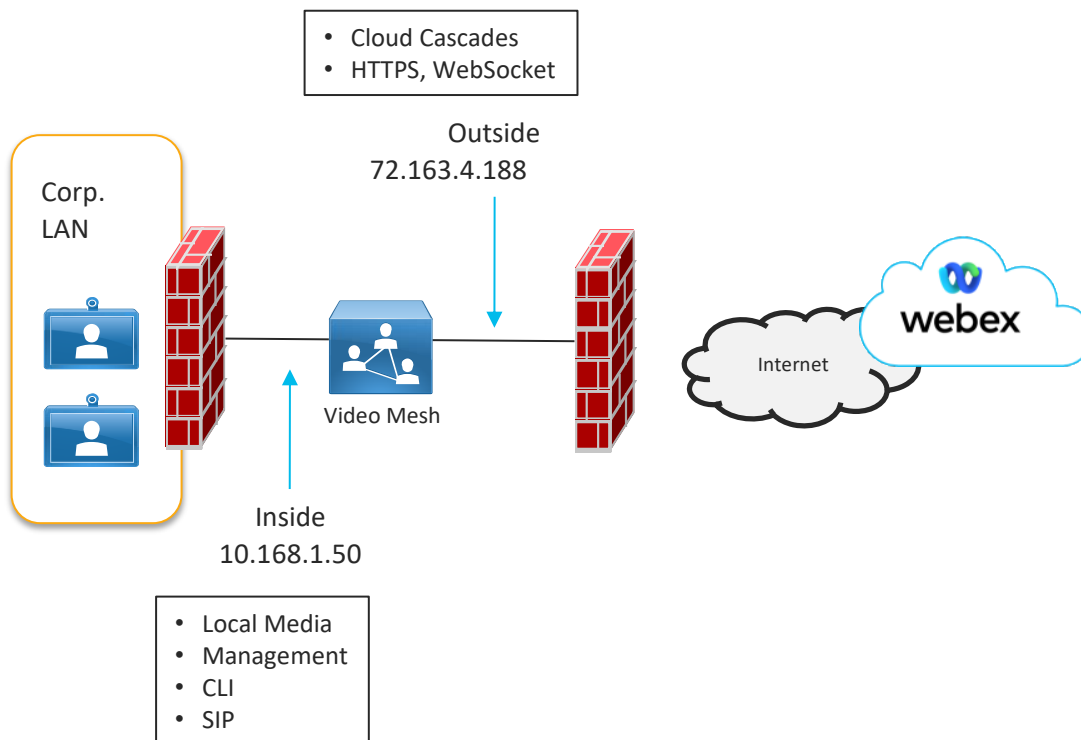
Within the CLI or Video Mesh webpage there is the ability for the administrator to configure the route rules of the Video Mesh. This allows the flexibility of the configuration to meet the needs of the network administrator for the DMZ deployment. Figure 12 shows an example of adding routes to the route rules on the Video Mesh webpage.

Figure 12 Managing Routing Rules

Proxy Server Considerations

Some organizations may use a proxy server as part of their infrastructure, The Video Mesh works with both transparent and explicit proxies supporting both inspecting and non-inspecting modes.

Cisco officially supports the following proxy solutions that can integrate with the Video Mesh nodes.

- Cisco Web Security Appliance (WSA) for transparent proxy
- Squid for explicit proxy

While support has been established with WSA and Squid, the Video Mesh proxy functionality should work with most major proxy vendors. For an explicit proxy or transparent inspecting proxy, the proxy server needs to decrypt the traffic, thus a copy of the proxy's root certificate must be uploaded to the Video Mesh node trust store.

The Video Mesh supports the following explicit proxy and authentication type combinations:

- No authentication with http and https
- Basic authentication with http and https
- Digest authentication with https only
- NTLM authentication with http only

From a signaling traffic flow perspective, the administrator can route HTTPs TCP 443 traffic to the proxy as illustrated in Figure 13.

Figure 13   Proxy Server Integration
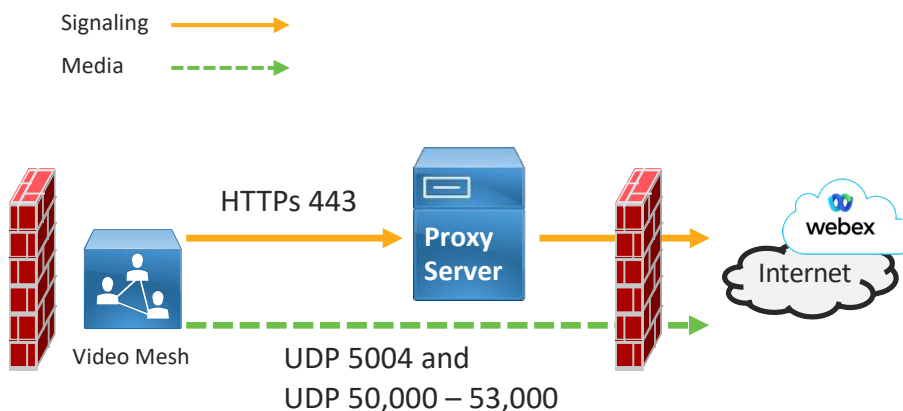
Firewall Requirements

Whether the Video Mesh is deployed in the internal network or located in the DMZ, firewall ports will need to be opened to allow for proper communication between the Video Mesh nodes and Webex. If this is not done properly, different aspects of the Video Mesh functionality will fail.

The Video Mesh will use HTTPs 443 for communicating with a variety of Webex services for things such as registration, health checks, and signaling. It will also use HTTPs 443 for WebSocket communications when creating a cascade. UDP is Cisco's preferred transport protocol for media, and Cisco strongly recommends using only UDP to transport media. The Video Mesh also supports TCP as a transport protocol for media as a fallback for 1:1 meetings only, but this is not recommended in production environments as the connection orientated nature of this protocol can seriously affect media quality over unmanaged or lossy networks such as the Internet. Table 5 shows the requirements needed in the firewall for cascades from the Video Mesh to Webex to be establish. Notice in Table 5 that there are two ranges of media destination

ports for cascades. The Video Mesh uses destination ports UDP 5004 and UDP 50,000 – 53,000. The UDP 5004 destination port is used for 1:1 meetings where one participant is on the Video Mesh node and called another participant that is located on the Webex cloud media resources. The UDP 50,000 – 53,000 range is used for all multiparty Webex meetings. This range, UDP 50,000 – 53,000 does not have any fallback ports and must be opened for the Video Mesh to connect the media cascade to Webex. Table 5 is not a complete list of ports and destinations for all functions of the Video Mesh.

Table 5   Cascade connection requirements

Type	Source	Source Port	Transport Protocol	Destination URL	Destination Port
Signaling	Video Mesh Node	Ephemeral	Default - TCP	*.wbx2.com	443 444
Media (Default – QoS enabled)	Video Mesh Node	Audio – 52500 – 62999 Video – 63000 – 65500 Content – 63000 – 65500	Default – UDP Fallback – TCP (only possible to 5004) (TCP is not recommended to use.)	*.webex.com *.wbx2.com	5004 50000 - 53000
Media	Video Mesh Node	34000 – 34999	Default – UDP Fallback – TCP (only possible to 5004) (TCP is not recommended to use.)	*.webex.com *.wbx2.com	5004

With the dynamic nature of a cloud offering like Webex that allows for expansion while growing and optimization with different cloud providers, it is recommended to reference the Webex Services article, https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Services, to ensure the firewall is setup with the latest URLs, IP subnets, and ports for proper communications of all services.

QoS

As shown in Figure 14 and Figure 15, the Video Mesh can support QoS markings for ingress and egress traffic. The QoS toggle is enabled by default but can be turned off via the Control Hub under the Video Quality section of the Video Mesh settings. When QoS is disabled, it will change the default source ports to 34000 - 34999 for audio 🔊, video 🎥, and content sharing 🖥 and native marking of all the traffic to AF41. By default, with QoS enabled, audio is using source ports 52500-62999 and marking the audio traffic as EF. Video and content share are using source ports 63000-65500 and marking the video and content traffic as AF41. The native marking of the traffic by the Video Mesh node is fixed and cannot be adjusted by the administrator but if another marking is desired, then remarking in the network is an option.

Figure 14   Port Usage QoS Enabled (Default)
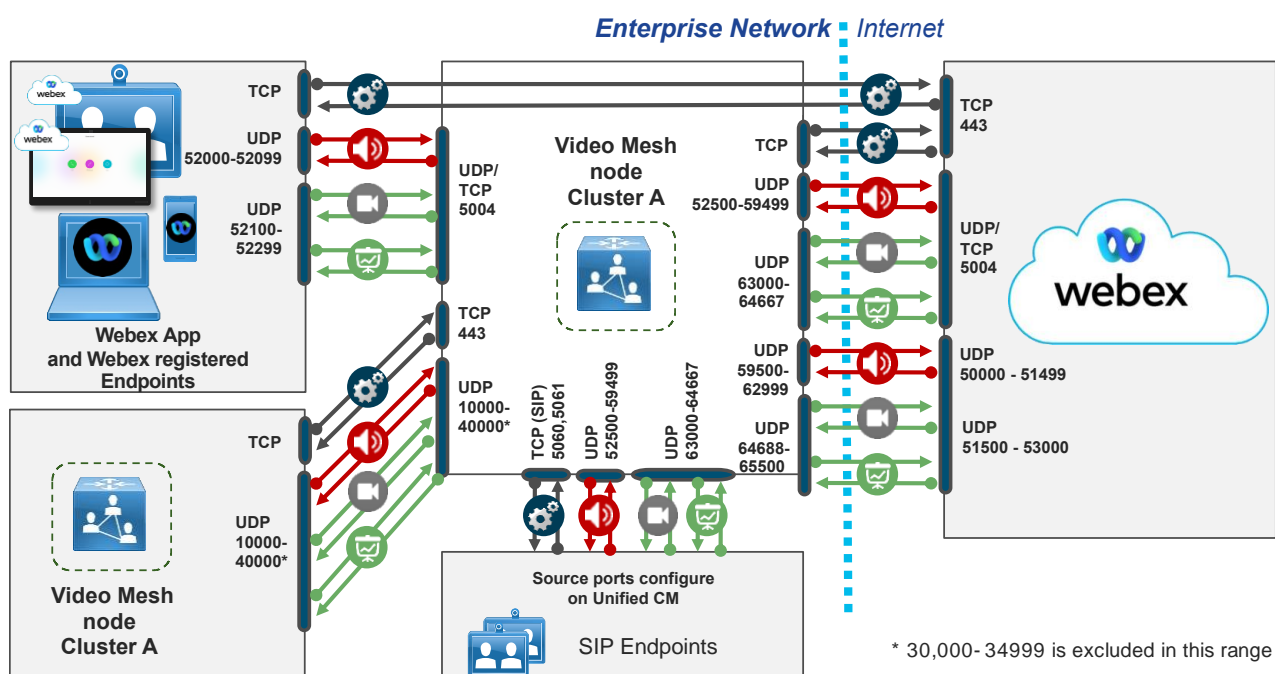
Note: A DMZ Video Mesh cluster may want to turn off QoS to limit the number of ports to open through the firewall.

Figure 15   Native Marking QoS Enabled

- *30,000- 34999 is excluded in this range.
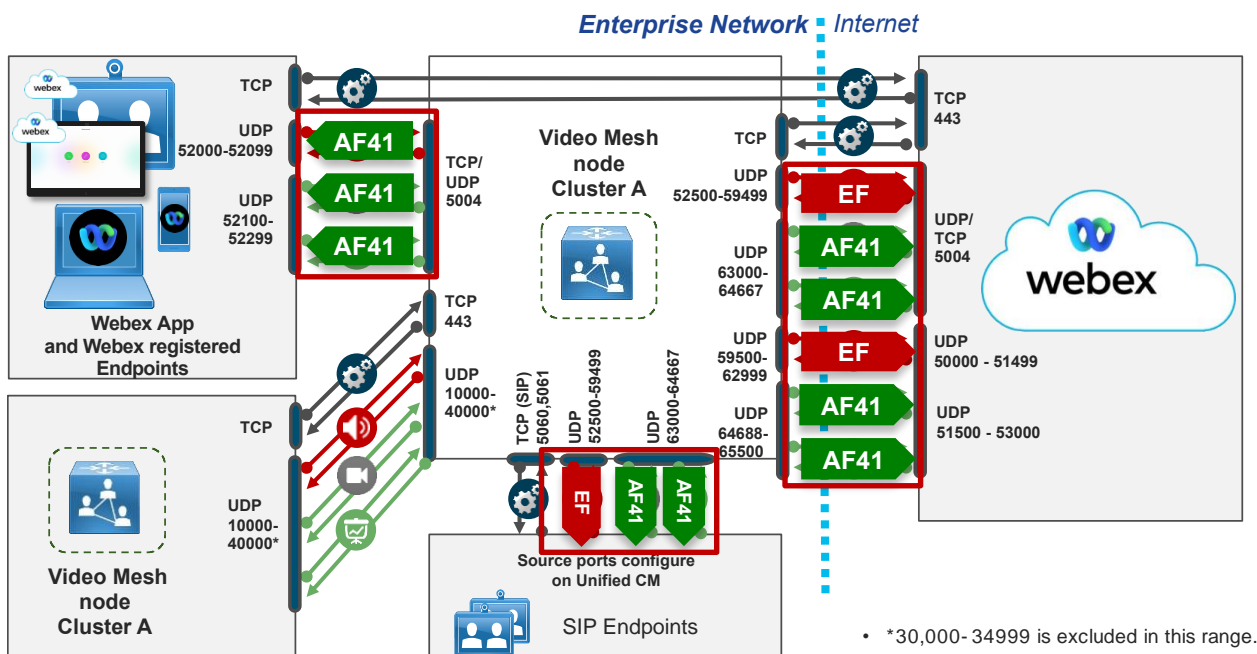
Cisco does provide a mechanism to test the ports for QoS and non-QoS configuration. Within the Video Mesh there is a "Reflector Server" option that can be enabled. When this is enabled on the Video Mesh, the administrator needs to download the python script from Cisco's website: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/mediaservice/deployment/qos/reflectorClient.zip, and run it on a PC or Mac. Inside this script the administrator can test all the ports from the source device to the Video Mesh. Figure 16 shows an example of the script and the options available to be run by the administrator while performing the tests.

Figure 16   Reflector Client

```
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 specified, default ports are verified for connectivity.
    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 63000-64667.
    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 52000 --end-port 52501 --non-qos
    Below run in to verify default qos ports:
      python reflectorClient.py --ip <> --protocol <udp/tcp>""")
```

1080p Resolution

The Video Mesh node can support many different resolutions depending on the endpoint connected. Most commonly 1080p and 720p are used. If the Webex App (without the Full Featured Webex Experience) or Webex registered endpoint is participating in a meeting on the Video Mesh, then the Video Mesh will process 1080p or 720p by default from those systems, assuming they have these capabilities. But if the video endpoint is registered to an on-premises call control such as Unified Communications Manager, then it is recommended to enable the 1080p toggle in the Control Hub Video Mesh global settings. This toggle will enable the Video Mesh to send and receive 1080p, main speaker video, from that SIP endpoint assuming the SIP video endpoint has this capability enabled and advertising 1080p to the Video Mesh. Additionally, when turning this on, check that Unified Communications Manager is configured to allow that SIP video endpoint to send 1080p resolution to the meeting. Video resolution for Unified Communications Manager registered endpoints is determined by the region settings bandwidth. Figure 17 shows an example of two Unified Communications Manager registered devices sending 1080p main video for a Webex meeting.

**Figure 17**   SIP 1080p Main Video with toggle enabled
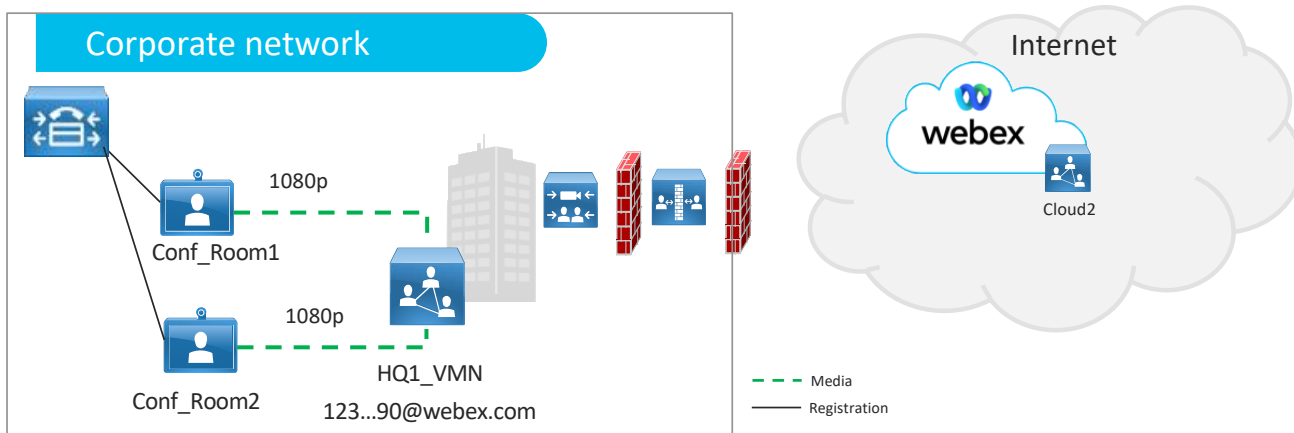
Call Flows

Cascades

The concept of a cascade is a signaling and media connection from the Video Mesh node to Webex to create a single meeting where all the video, audio, and content is seen by the participants independent of where they are connected to the meeting, either on the Video Mesh or to Webex directly. Within the media cascade, it needs to provide the relevant audio, video, and content streams to the remote side, so they are displayed properly on that device.

In a simple example where all the participants have the same layout on their device as shown in Figure 18, the media streams from the active speaker, the Webex App (without the Full Featured Webex Experience) with the yellow person and yellow dotted lines, needs to be sent to all the participants so it can be displayed in the large window on their screen. The other participants are not speaking so lower resolution video streams need to be sent to the other participants so they can be displayed in the smaller windows of the layout.

Figure 18   Main Video only
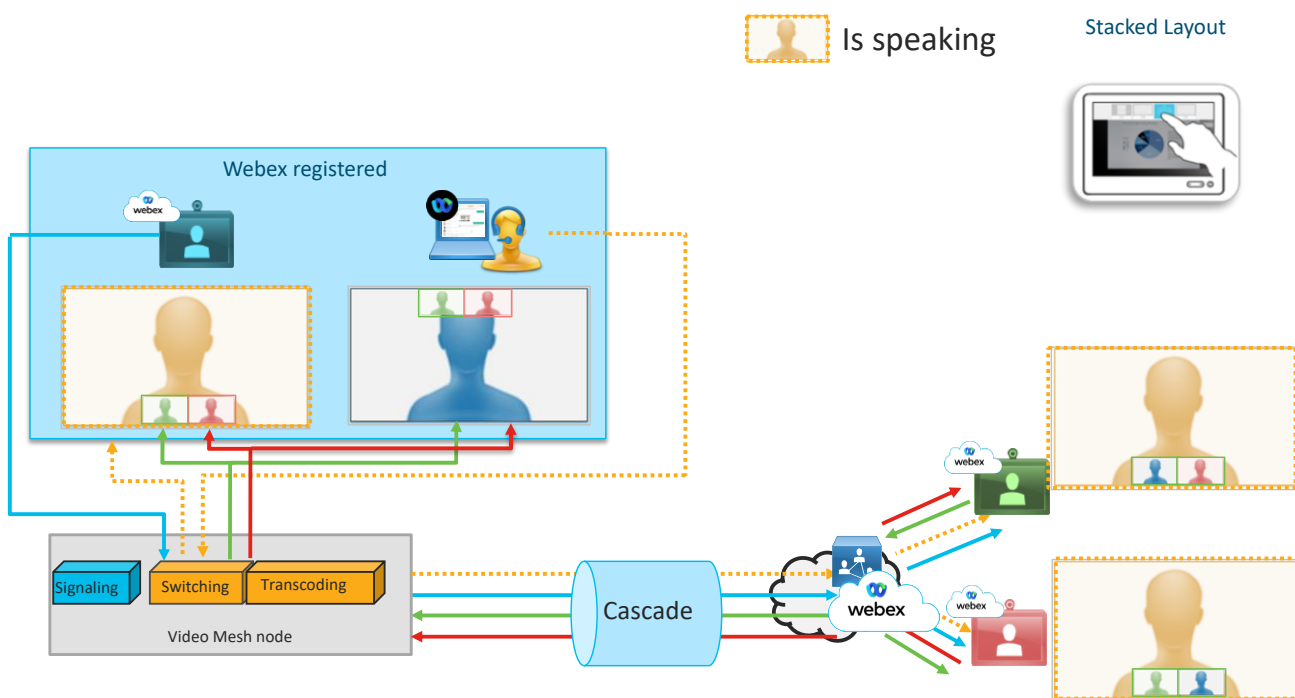
This same concept will hold true if the active speaker decides to send a PowerPoint slide to assist in the delivery of their content. In this case, shown in Figure 19, the layout will change for each participant requiring different resolutions of the video streams to be sent across the cascade to fulfill the layout on the different participants.

Figure 19   Content Sharing
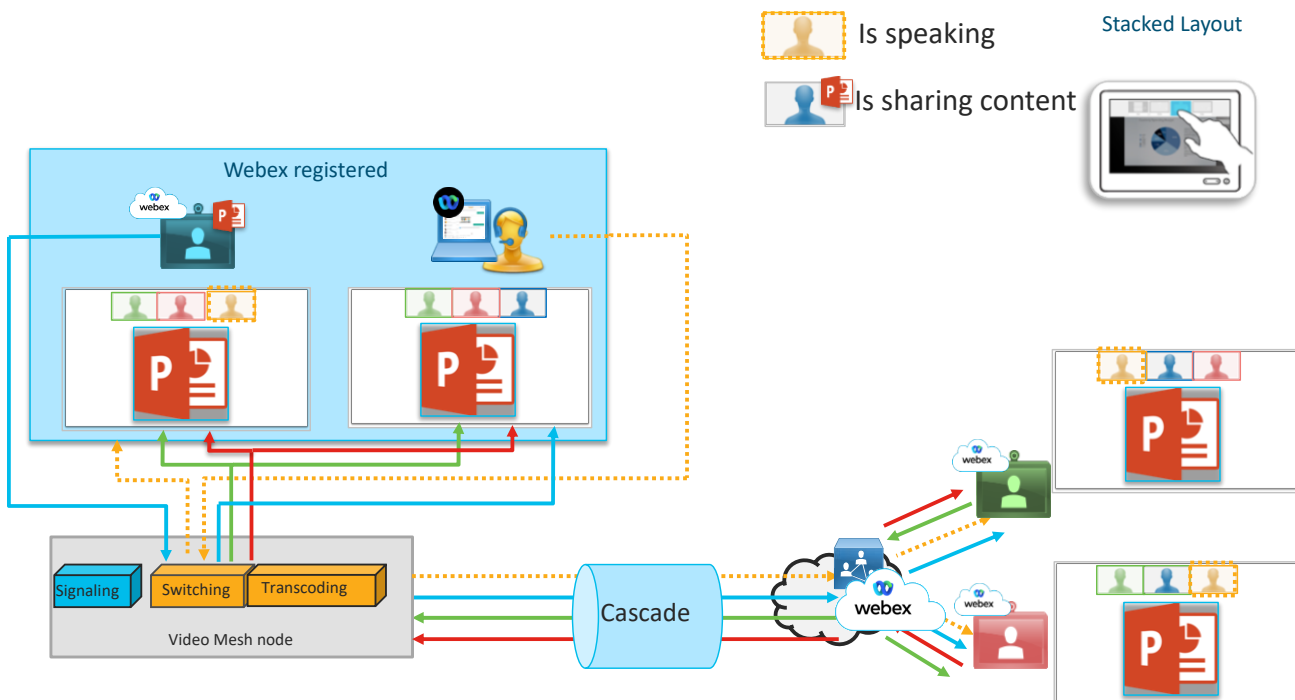
The different video endpoints will now send a lower resolution video stream of the speaker as the requirements on the remote side is for a small window because the main portion of the screen is being used for the PowerPoint slide. In addition, the content channel will now be actively sending media from the source video device to all the devices in the meeting, whether locally on the Video Mesh or remotely on Webex.

In general Cisco video endpoints can send 3 or 4 different video streams ranging from 180p to 1080p, but that will be dependent on the capability of each video endpoint. Depending on the layout requirements of the remote side, a single video endpoint can send multiple resolutions of their main video or speaker video, to meet the requirements of the other participants. Additionally, a single content stream can be sent along with multiple audio streams. The architecture is designed this way to give the best user experience on the device in the meeting.

The Video Mesh cascade is a per meeting cascade and will be established if a single participant is connected to Webex's media resources in the cloud for that meeting. The cascade is always initiated from the Video Mesh to Webex. Each cascade will send streams for the main speaker video, audio, and content to the remote side. These streams are bi-directional across the cascade. Within each cascade, there can be up to 25 sources where a source is the device that is creating the data streams that are being sent. For example, if a Desk Pro is in the meeting connected to the Video Mesh, it will be a source. If a DX80 is connected to that same meeting, it will be another source. Based on the capabilities of the Desk Pro, or DX80, they can send multiple different main speaker video streams to the remote side at various resolutions, for example, 1080p, 360p, and 180p, if they are required for the layout presentation on the Video Mesh or to a Webex connected participant. Figure 20 illustrates an example of a meeting with multiple different participants speaking, no content shared, and devices on the left side connected to the Video Mesh and the devices on the right side connected to Webex. This figure shows an example of what streams and resolutions might be sent across the cascade from the Video Mesh to Webex at that point in time in the meeting.

Figure 20   Main Video with multiple layout example – Video Mesh to Webex
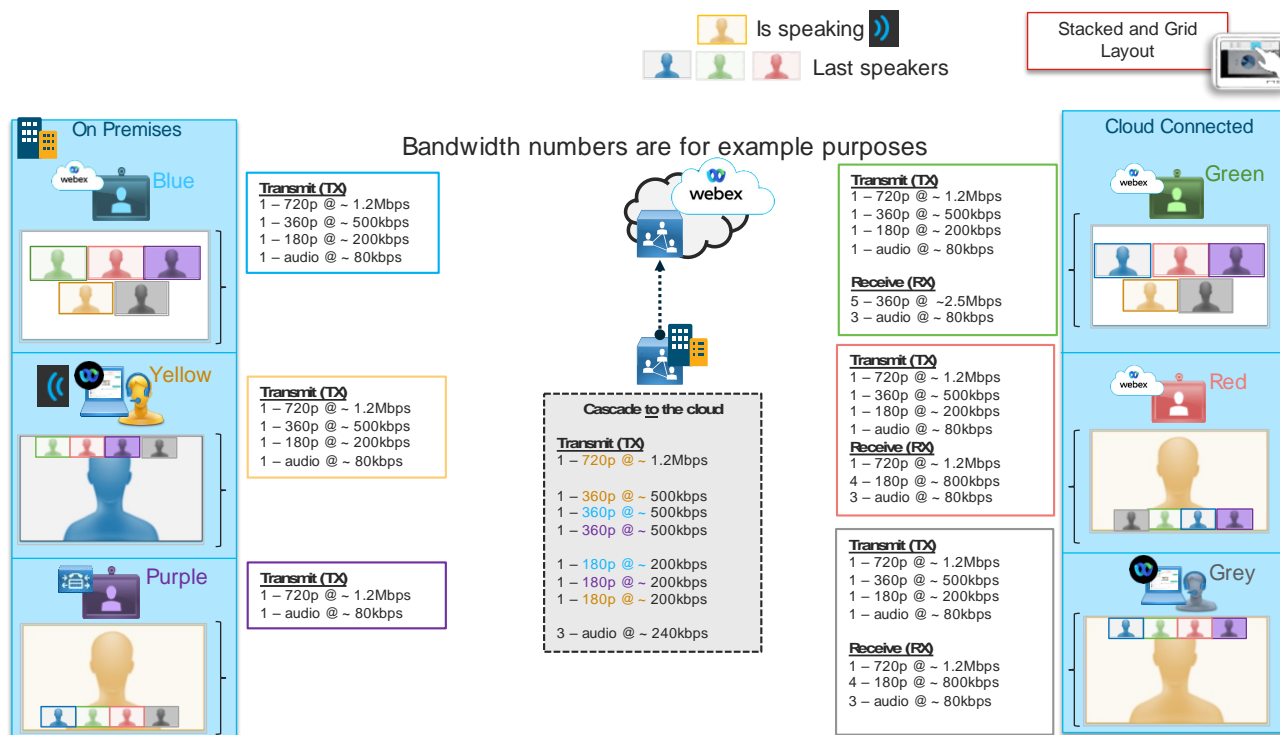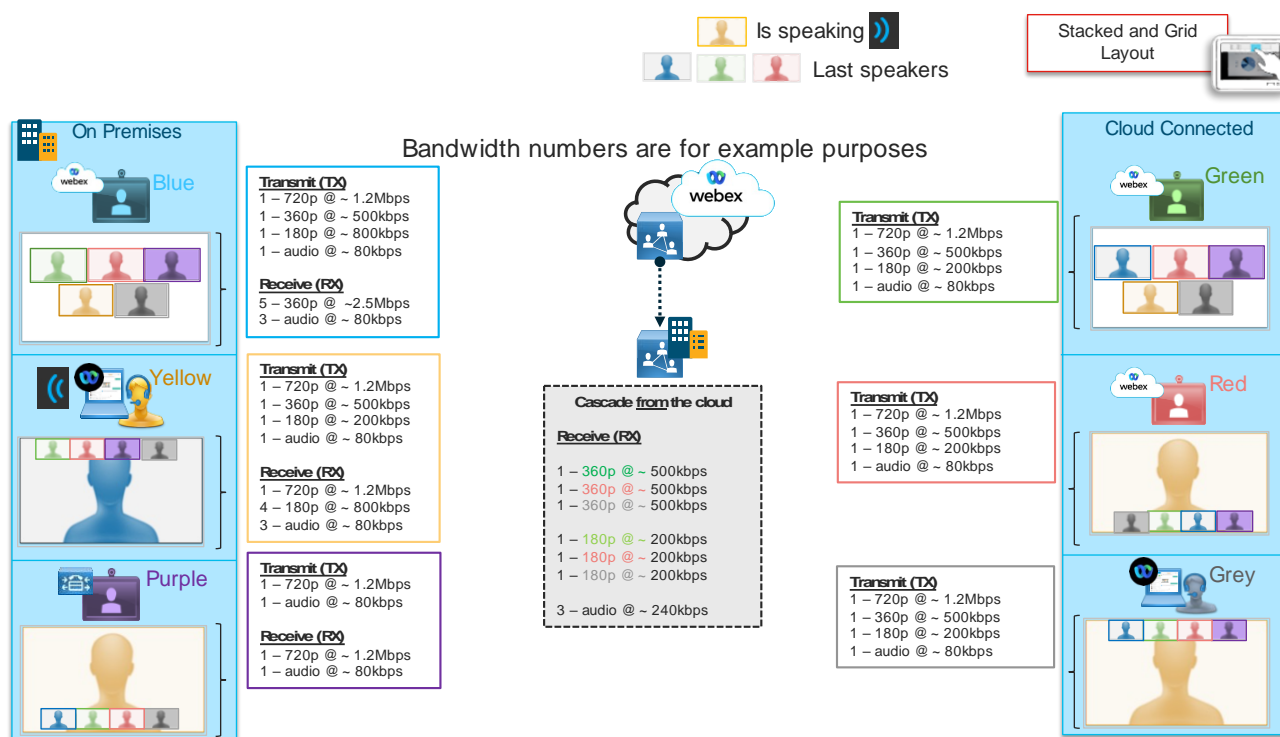

Figure 21 shows an example of the same scenario with the media streams from the Webex to the Video Mesh. These streams are needed from Webex to meet the layout requirements of the Video Mesh participants.

Figure 21   Main Video with multiple layout example - Webex to Video Mesh

These cascades are a per meeting cascade, so it is common to see multiple cascades happening at a single time from a Video Mesh node to Webex. The Control Hub has a report that allows for the administrator to view the activity around the cascades by going to Analytics -> Video Mesh -> Bandwidth tab. Within this tab there are key performance indicators, KPIs, of the overall cascade bandwidth for a given time frame. Figure 22 is an example of the KPIs.

Figure 22   Bandwidth KPIs
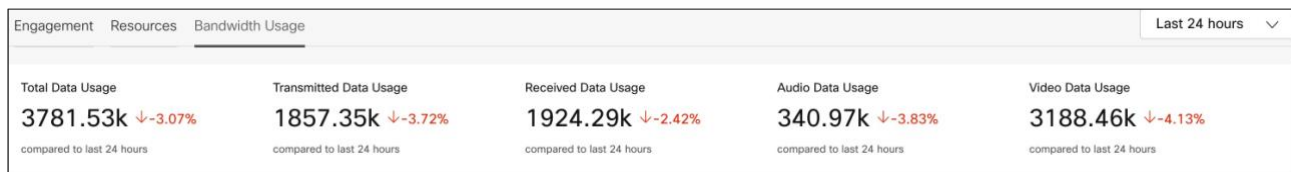
Additionally, on that page there are three other graphs that illustrate the

- Total cascade data used by the cluster for the selected period of time.

- Total distribution of cascade data, both transmit and receive, over a selected period of time.

- Total distribution of data across all media streams, audio, video and share in a selected period of time.

Figure 23 shows an example of the total distribution of data across all media streams charts that can be used by the administrator to do analysis.

Figure 23   Total Cascaded Data by Stream
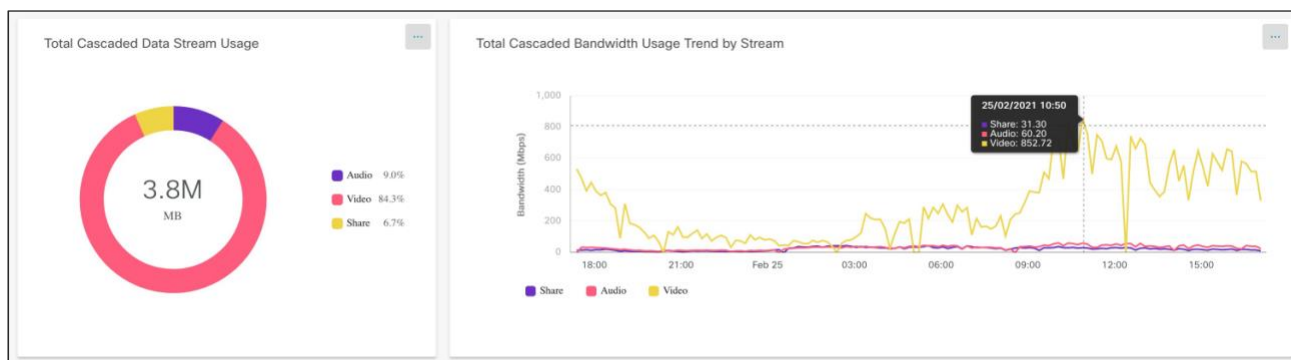
These charts should be monitored to see the cascade bandwidth being utilized by the Video Mesh nodes, but if this is a new installation how do you plan for bandwidth needed?   With the nature of the meeting requirements, the cascade bandwidth will change throughout the call. In addition, each meeting has different layout requirements which will dictate the number of streams needed. With that, Cisco has evaluated historical data in a 3-month timeframe from our larger Video Mesh customers with many meetings per day that include cascades. This information tells us that about 12mbps is a good estimate to use for a per meeting cascade calculation for capacity planning. The cascade bandwidth number will be different in each organization due to meeting participants and meeting requirements. Additionally, the cascade bandwidth per stream can reach up to 20mbs for main video plus the single content stream and audio streams. The cascade bandwidth is not configurable by the administrator.

Each Video Mesh cluster in an organization should be deployed at main locations or datacenters with direct Internet access. Deploying Video Mesh clusters in many locations, including small locations, is not a good practice because the bandwidth savings gained by having a Video Mesh could be lessened or negated if the locations have very few video enabled devices or applications. It may be better for the video enabled devices or Webex App (without the Full Featured

Webex Experience) to connect to a centralized Video Mesh cluster or go directly to Webex. Regional or centralized Video Mesh clusters are recommended deployments, and it is always best to start with a few clusters and grow as needed.

Multisite call flows

The Webex architecture with Video Mesh provides a hub and spoke architecture for cascades. The hub is Webex, and the spokes are the Video Mesh clusters in the corporate network. Each cascade has signaling and media streams to Webex. In Figure 24, this corporation has 3 locations, Singapore, New York, and London with video participants in each location that will need to connect to the Video Mesh cluster in New York. In this case the participants in red all dial into the same meeting and will be routed across the network to the Video Mesh node in New York. Since all participants are on-premises and the Video Mesh node has capacity to host those participants, a cascade is not needed.

Figure 24   Centralized Video Mesh cluster – Centralized Internet Access
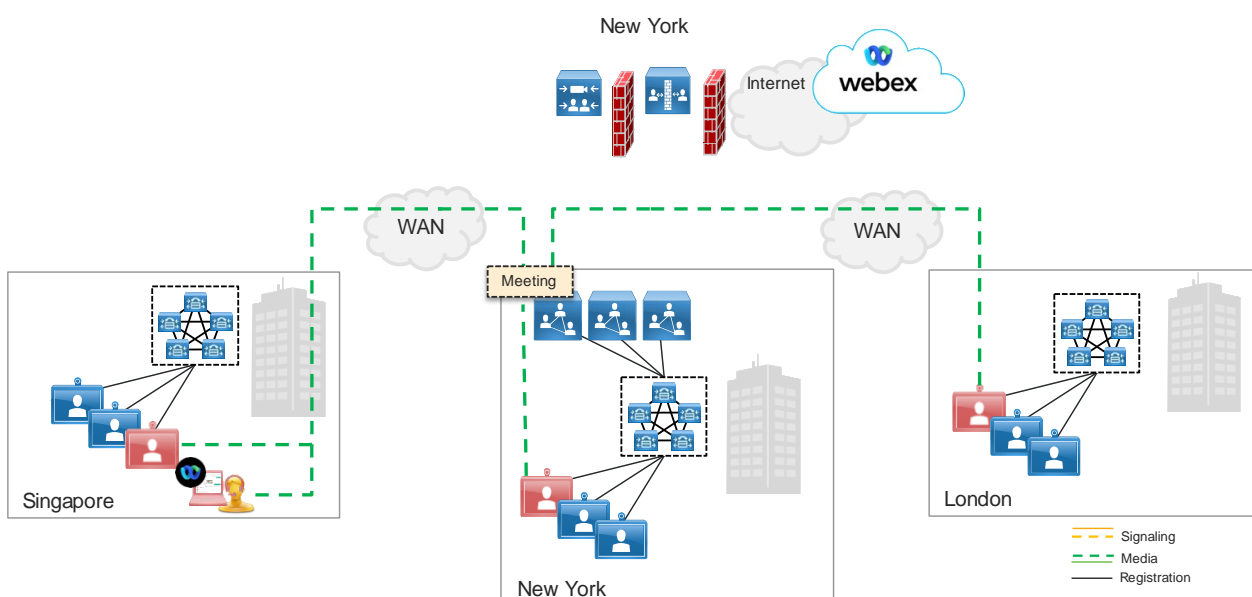
When a participant joins the meeting from outside the corporate network such as from a Webex App in a café, then that participant will join Webex, and a cascade will be created from the Video Mesh cluster in New York to Webex. The cascade link does not use the firewall traversal mechanism or the Cisco Expressways, as the Video Mesh cluster needs direct access to the Internet to connect to Webex. Figure 25 shows the cascade to join the external participant to the meeting.

Figure 25   External Participant - Centralized Video Mesh cluster – Centralized Internet Access
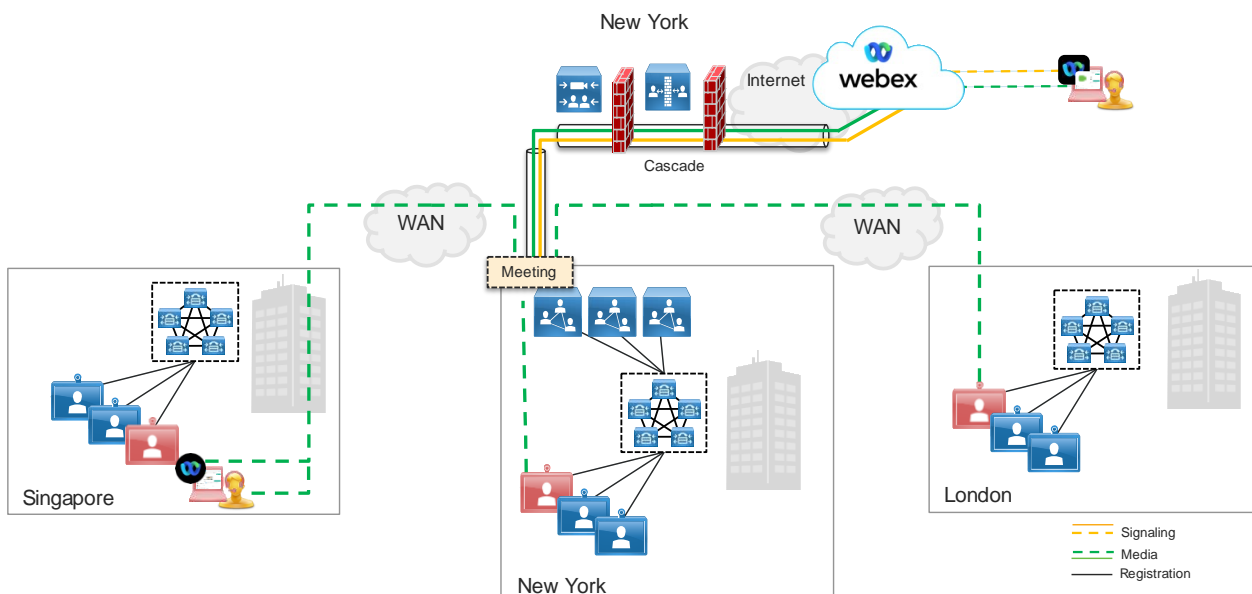

As organizations grow, they will add additional Video Mesh clusters to regionalize the traffic to an in-region Video Mesh cluster. In Figure 26 the Singapore location has deployed a new Video Mesh cluster and, using the same scenario where all the participants in red are joining the same meeting, a new cascade flow will happen. The hub, in this case, is Webex and the spokes are the Singapore and New York Video Mesh clusters. Since each location has a participant connected to the in-region Video Mesh cluster, each cluster will have its own cascade link to Webex to join all the participants.

Figure 26   Regional Video Mesh clusters – Centralized Internet
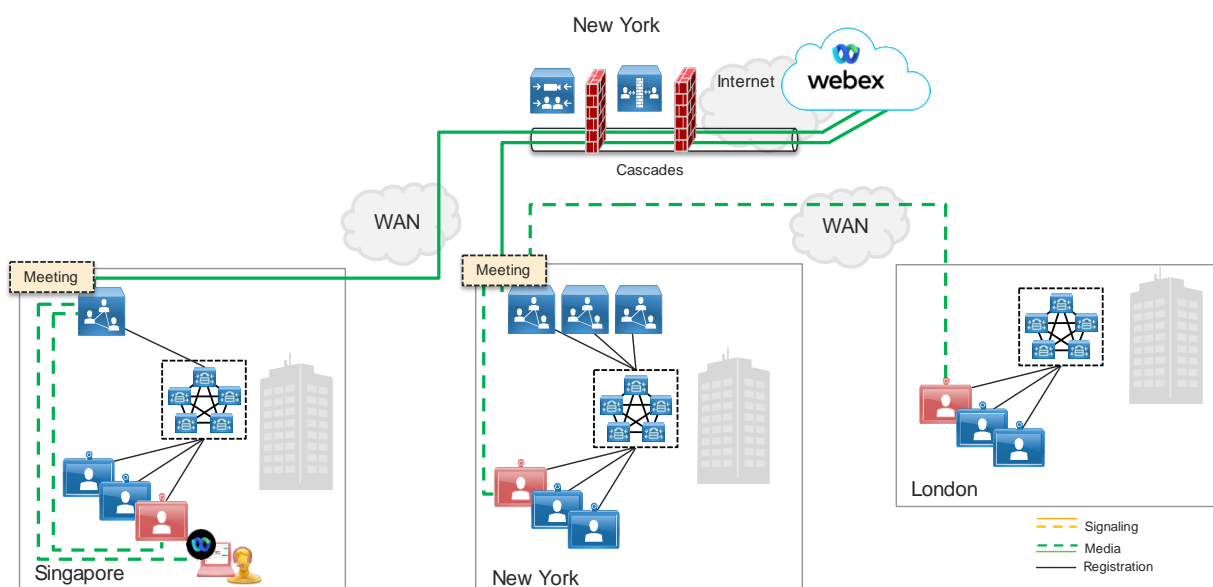
As the Singapore location grows, an enterprise may install a regional Internet connection to allow for better connectivity. In this case, the cascade path will change to use the Singapore Internet connection versus traversing the WAN to the previous Internet connectivity point in New York, as shown in Figure 26.

In Figure 27 the Singapore Video Mesh cluster will create a cascade through the Singapore Internet connection and the New York location will use the New York Internet connection to connect to Webex. Once both the cascades are established, the media will be transmitted to and from the local Video Mesh clusters to Webex and back.

**Figure 27**　Regional Video Mesh clusters – Local Internet
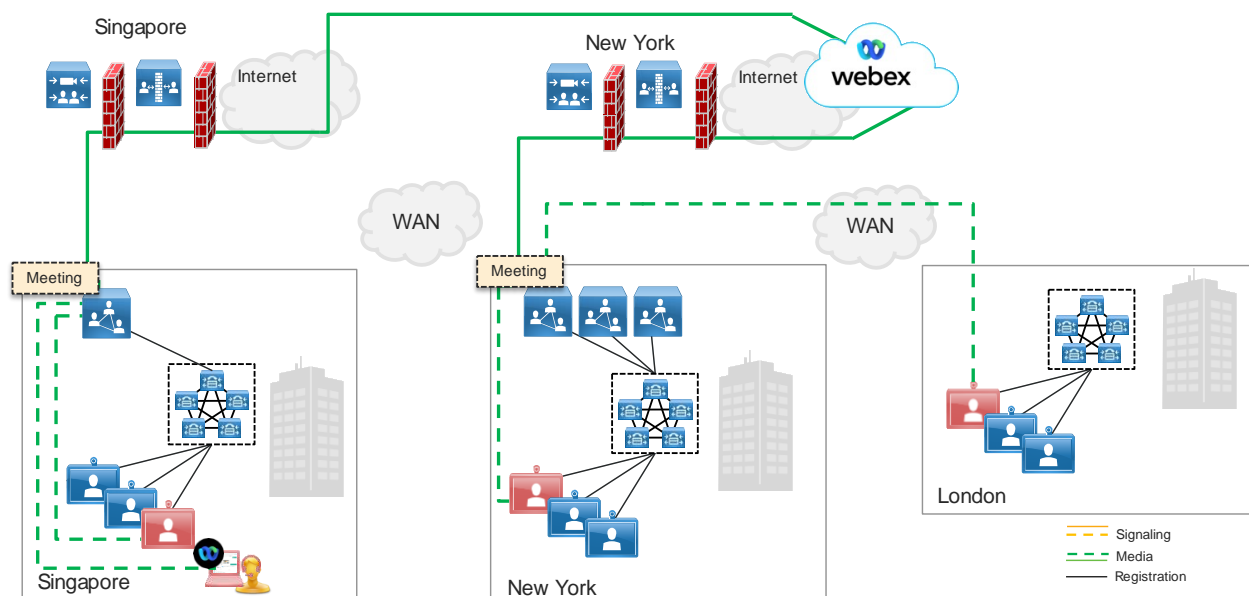
For Webex to accept cascade requests from the Video Mesh clusters, a setting needs to be enabled to allow this to happen. This setting shown in Figure 8, needs to be set to "Video Mesh". When this is enabled, this allows for the Video Mesh clusters from the host organization and any other participants organization to establish a cascade to Webex. Using the same configuration as the other examples, but in this case, Singapore was spun out and became a different company with a Webex site of "Singcorp.webex.com" while New York and London are part of the same company with a Webex site of "NYcorp.webex.com". When all the participants join the meeting, as shown in Figure 28, the cascades are allowed to be established for both companies.

Figure 28   Meeting Hosted on an external Webex site when Media Resource Type = Video Mesh
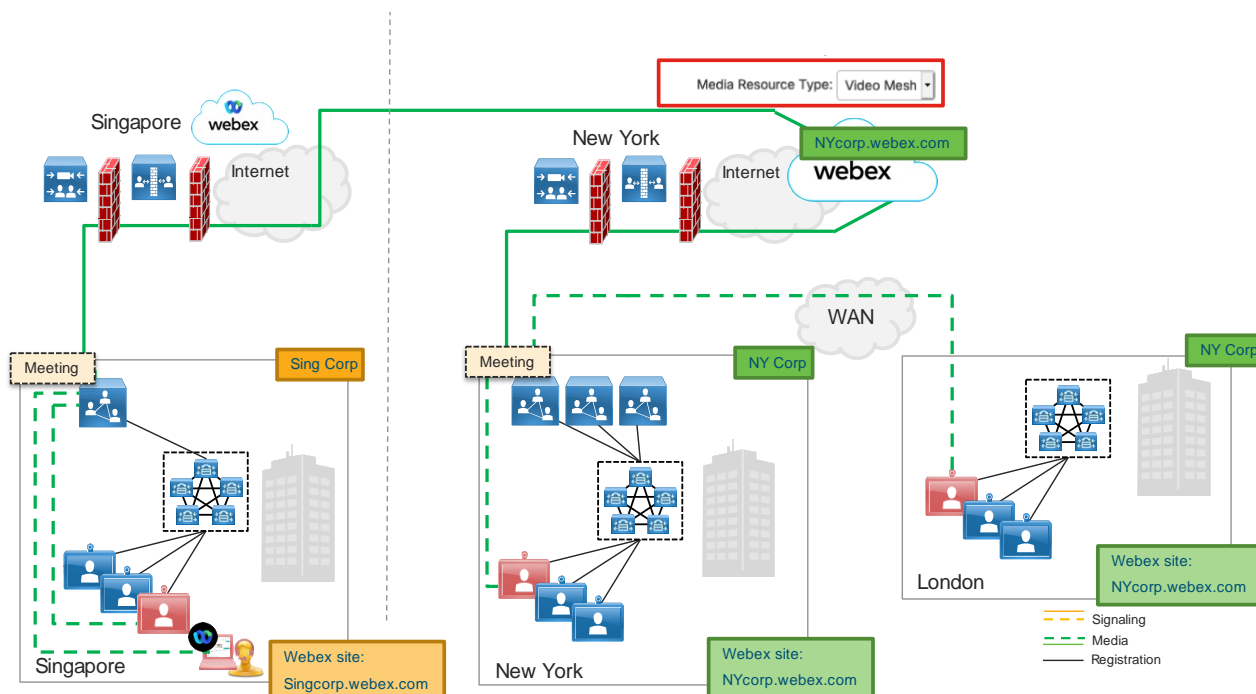
If the Media Resource Type setting in the Webex site's Collaboration Meeting Room (CMR) for the host site is set to the default "Cloud", then a cascade from any cluster is not allowed. This setting applies to the host organization and any external organizations causing all meeting participants to connect directly to Webex via the Internet connection and not use their Video Mesh clusters. Figure 29 shows the call flows for the participants in the meeting connecting to NYcorp.webex.com but not being able to use their Video Mesh nodes because of the Media Resource Type setting in the host site is set to "Cloud". In this scenario all participants from Singcorp or NYcorp will send the media to Webex and not use the Video Mesh nodes.

Figure 29   Meeting Hosted on an external Webex site when Media Resource Type = Cloud
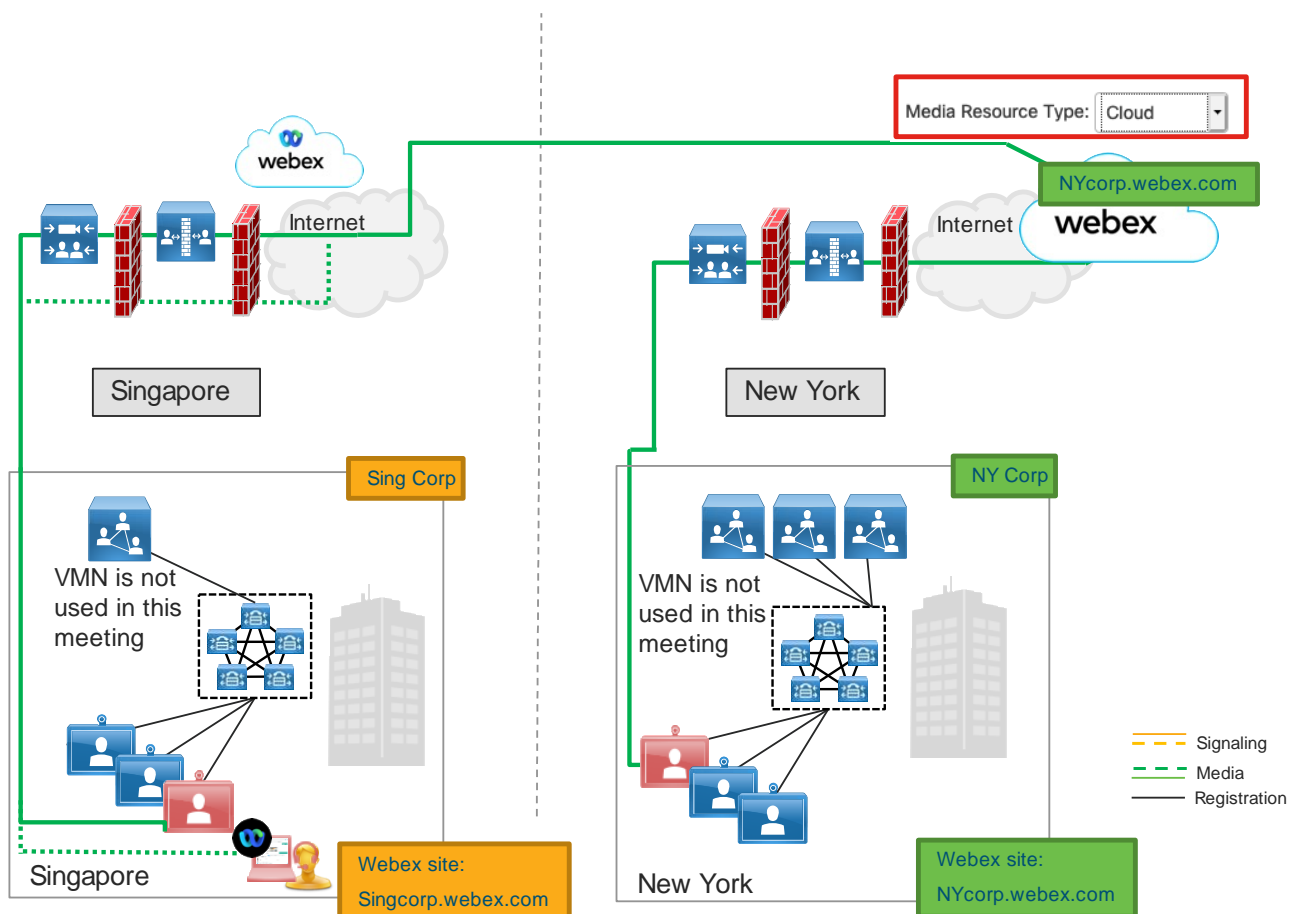
To allow the corporate Video Mesh clusters to be used independent of the Media Resource Type setting in the host site, the administrator can turn on the Prefer Video Mesh for All External Webex Meetings setting as shown in Figure 30. This Video Mesh global setting is recommended by Cisco to be enabled to allow the clients or devices to use the Video Mesh for all Webex meetings.

Figure 30   Prefer Video Mesh for All External Webex Meetings setting
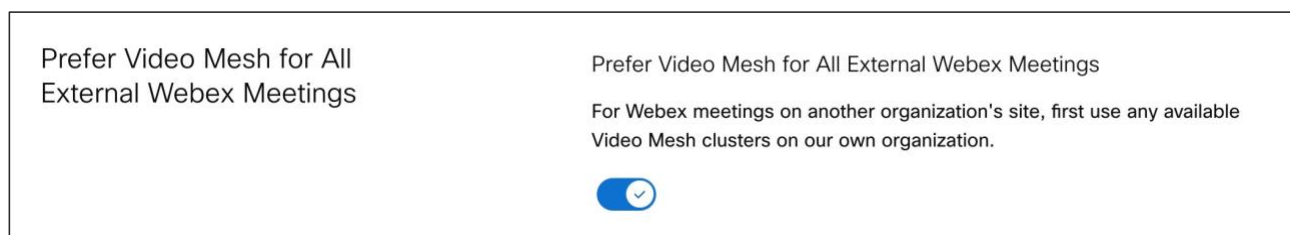
When considering the location of the Video Mesh clusters, there is an architecture that is not recommended and will cause suboptimal routing to the Video Mesh for Webex registered devices and the Webex App (without the Full Featured Webex Experience). This architecture is commonly seen when deploying two Video Mesh clusters into two datacenters with a very low latency links between the users and these datacenters. Cisco recommends that a single cluster be configured in Control Hub as opposed to two different clusters for better Video Mesh performance but based on network topology this may not be an option. In this unique scenario the Webex App (without the Full Featured Webex Experience) or Webex registered device performs the cluster reachability testing, and the results of the two Video Mesh clusters is

<=25ms difference. When the Webex orchestration service gets the cluster reachability results, it will make the conclusion that all the nodes in both clusters are available for the meeting because the latency is so close. This means any of the Video Mesh nodes in either cluster can be used for any meeting by the participants and the cluster designation in Control Hub is not considered. Figure 31 shows two clusters, New York – Primary Datacenter and New York – Backup Datacenter cluster. The backup cluster has one Video Mesh node, and the primary cluster has three Video Mesh nodes. When the participants want to join a meeting, they will be routed to any of the four nodes to host the meeting.

Additionally, Cisco does not support Video Mesh nodes across a WAN in a single cluster. The Video Mesh architecture is designed with all the Video Mesh nodes in a cluster to be in the same datacenter or LAN segment.

Figure 31   Low latency connection between the sites

| Device	RTT	Cluster
Webex App/Endpoint - HQ	22	Primary
Webex App/Endpoint - HQ	38	Backup
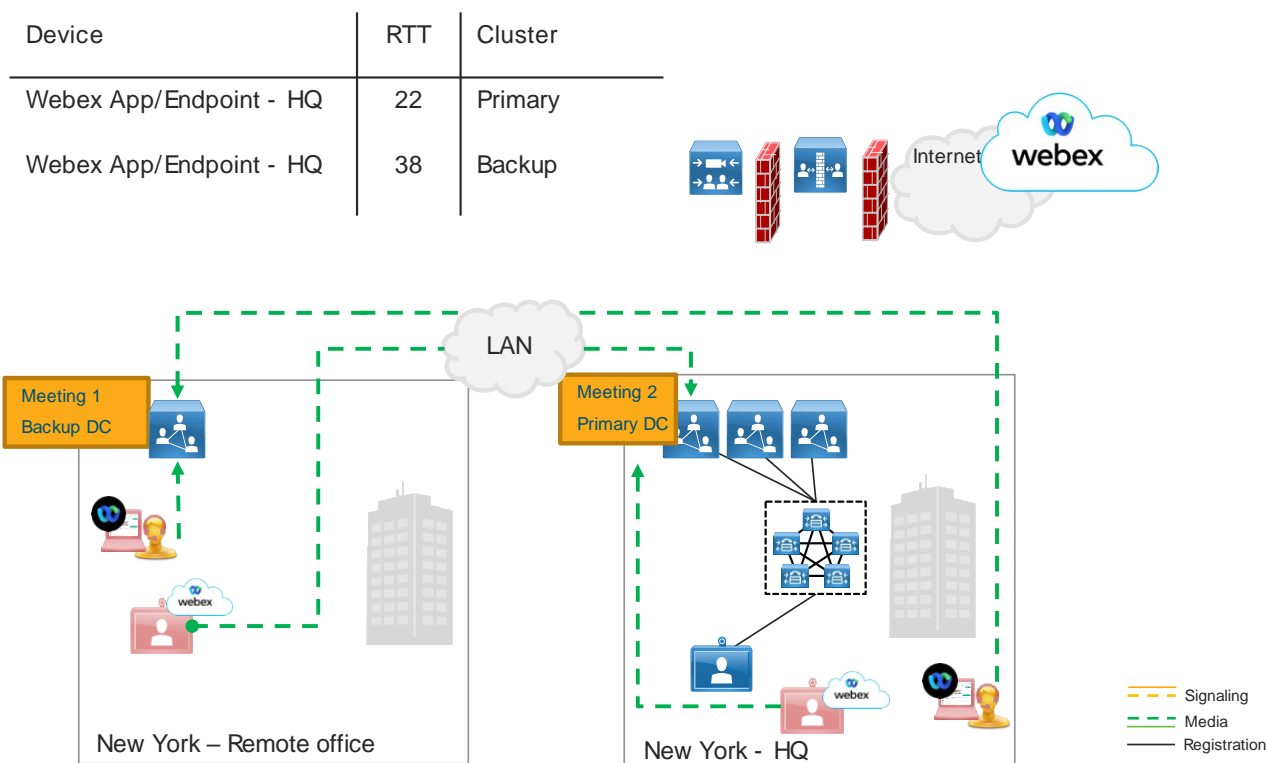
Point to Point call flows

The Video Mesh is a media resource available for Webex meetings. It is not a standalone bridge and always requires communication to Webex but does not always need to create cascades to Webex for all meetings. The Video Mesh can host meetings locally. For example, a meeting can be two participants in a point-to-point call or many participants in a meeting. Figure 32 shows an example where two cloud registered participants, a video device, and Webex App (without the Full Featured Webex Experience), are calling each other to meet. The media for each participant will be hosted on the Video Mesh and will not go directly between the participants.

Figure 32 Cloud registered point to point call

If the participants, Katie and Ben, were external to the corporate network but had a full tunnel VPN to the corporate network, then when Katie calls Ben, they use the Video Mesh nodes as show in Figure 33. If Katie and Ben are geographically far from Sydney, then backhauling the media traffic to the Video Mesh node might cause quality issues and it may be better to allow split tunneling to use the Webex cloud media resources.

Figure 33 Cloud registered point to point call with VPN
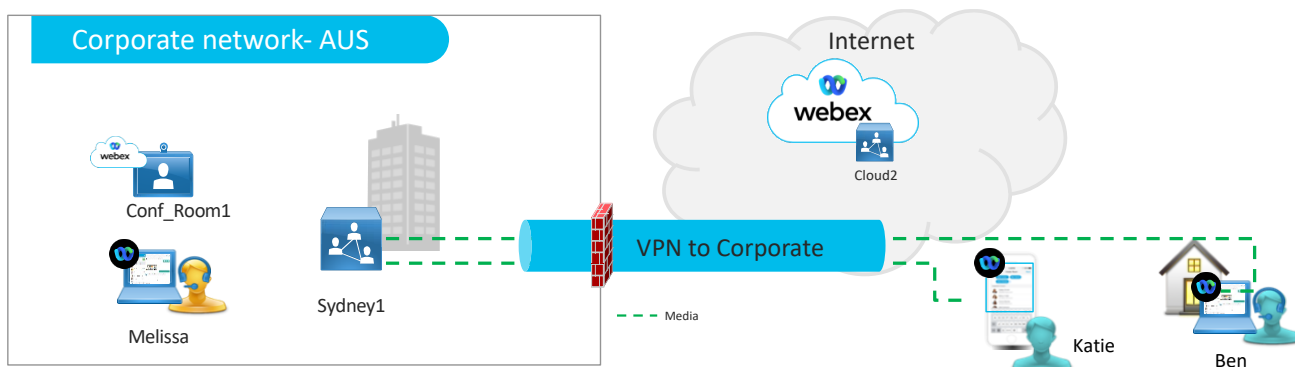
In another scenario, illustrated in Figure 34, a video endpoint, Conf_Room1, registered to an on-premises call control, Unified Communications Manager in this case but it could also be a VCS or Expressway-C, calls a Webex App (without the Full Featured Webex Experience) user Melissa. The media for the Conf_Room1 devices will utilize the firewall traversal mechanism of the Expressway products, like a business to business, B2B, call to reach Melissa on the Webex App (without the Full Featured Webex Experience). Conf_Room1 will not use the SIP trunk to the Video Mesh node because Unified Communications Manager's routing logic has *.sitename.webex.com and this is not a Webex meeting call. The Webex App (without the Full Featured Webex Experience) needs to utilize the Video Mesh for all media communications, if it is reachable, and will send its media there. If a local Video Mesh node is not available, then Melissa's media will go to the Webex resources directly and does not use the Expressway-C and Expressway-E firewall traversal.

Figure 34   On-Premises registered, and Webex App (without the Full Featured Webex Experience) point to point call
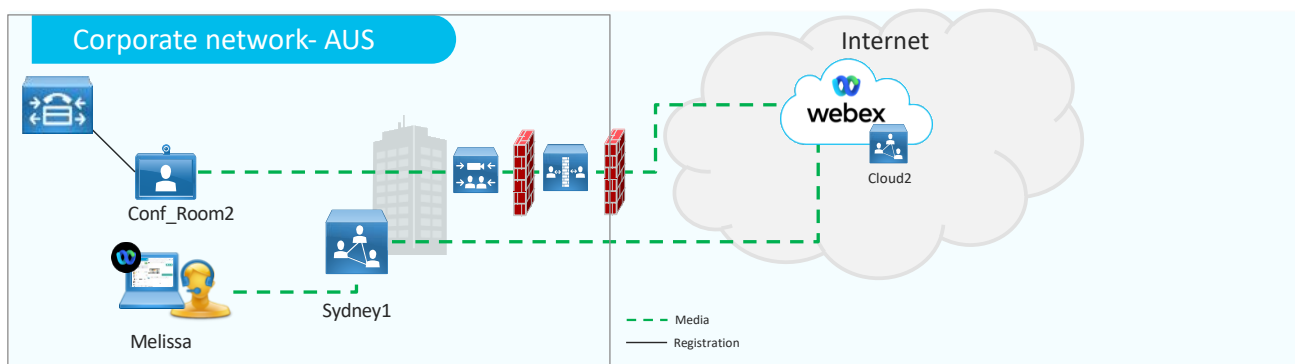

Globally Distributed Meetings

Video Mesh uses the globally distributed media (GDM) capabilities of Webex to achieve better media routing. To achieve optimal connectivity, Webex selects the nearest cloud media node to customer's network when performing Video Mesh cascades to Webex. Media then passes through the Webex backbone to interact with the Webex microservices for the meeting. This routing minimizes latency and keeps most of the traffic on the Webex backbone and off the Internet.

In Figure 35 the Webex site is hosted in the US, but the Video Mesh nodes are based in the Europe and Australia. Prior to GDM enablement, when a cascade connection was needed for the meeting, the cascades would use the Internet to connect to the US from Europe and Australia introducing potential issues affecting the quality. With GDM enabled, the Video Mesh nodes will find a Webex datacenter in that region and that Webex datacenter will be the termination point of the Video Mesh cascade. The discovery of the Webex datacenter and selection process happens dynamically and is enabled for all Webex sites.

Figure 35   GDM in a global meeting
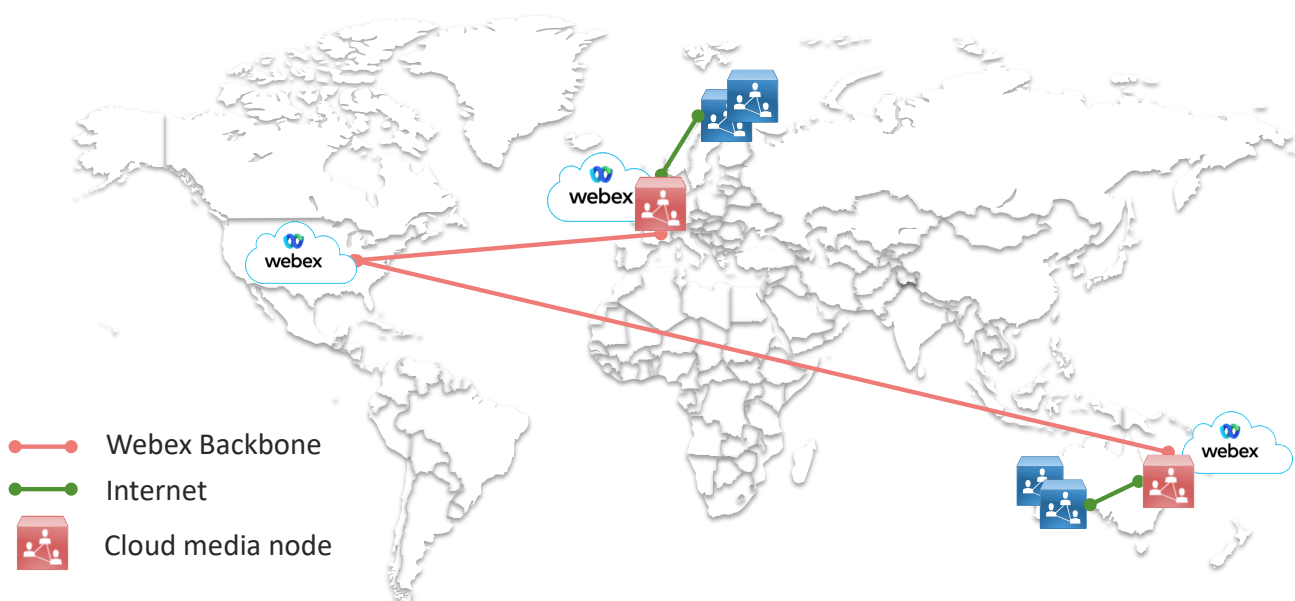
In some scenarios, GDM can keep cascade media in region. As shown in Figure 36, if a customer has the Webex site hosted in the London Webex datacenter and the Video Mesh nodes are in Spain and Italy, the Video Mesh cascades will terminate in one of the European Webex datacenters when connecting to the Webex Meeting.

Figure 36   GDM with an in region meeting
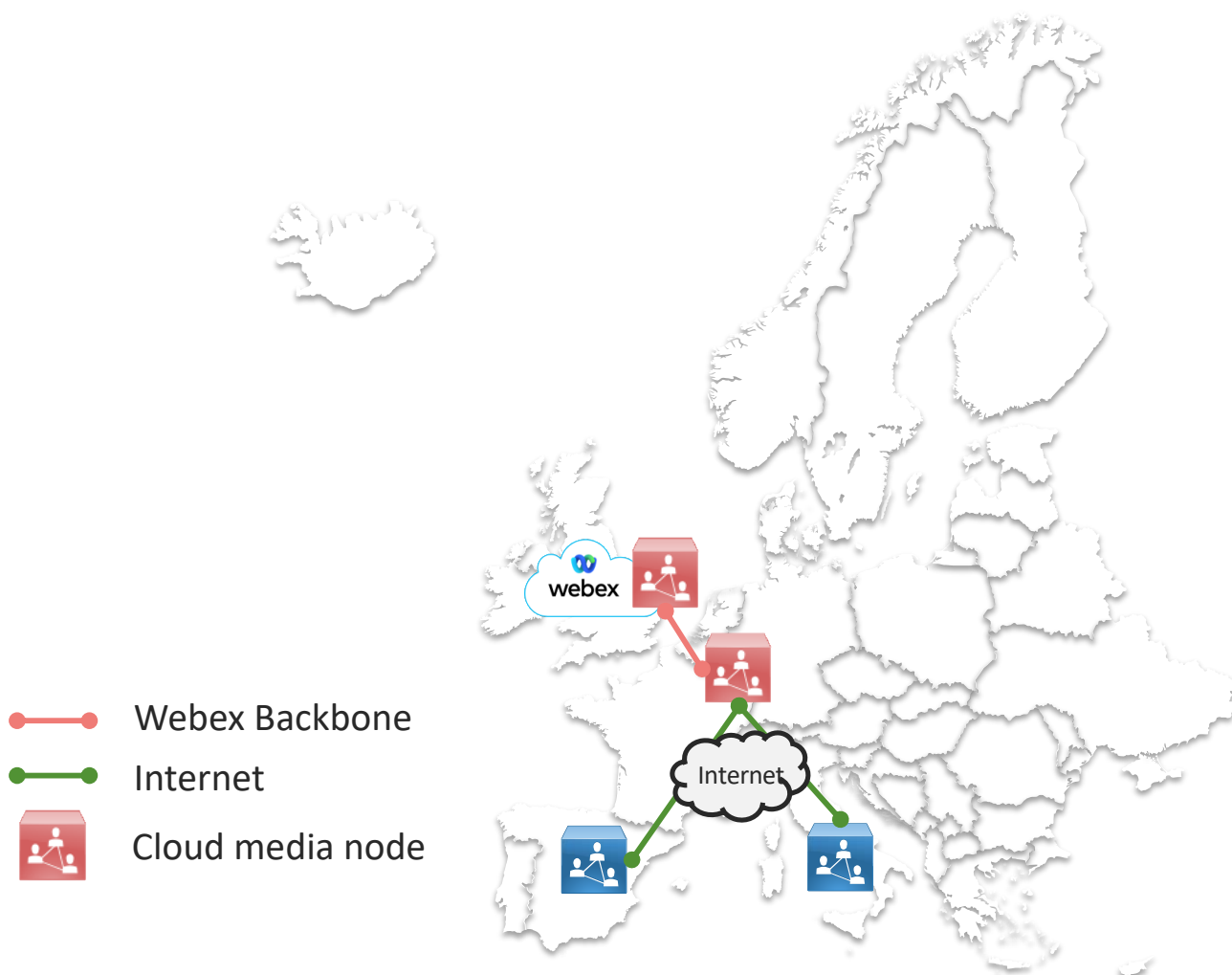
If the Video Mesh nodes are not cascading to a Webex datacenter in region, then the administrator can do a check to verify the Geo location. Cisco uses MaxMind as the GeoIP location provider and the administrator can verify that MaxMind correctly identifies the location of their public IP address to ensure efficient routing. Do the following steps to verify the Webex database is correct.

- https://ds.ciscospark.com/v1/region/<public IP address>

- Verify that the *countryCode* is appropriate in the response for the location of your submitted public IP address.

- If the location is incorrect, submit a request to correct the location of your public IP address to MaxMind at https://support.maxmind.com/geoip-data-correction-request/correct-a-geoip-location

Private Meetings

Cisco has another type of meeting for the Video Mesh that is different than the scheduled or adhoc meetings. The "Private Meeting (Video Mesh only)" session type in Webex will enable this meeting. This session type invokes a meeting where the architecture keeps the meeting media on the corporate network and does not extend it over the Internet to Webex. This will allow the meeting scheduler to have a meeting where all the media is on-premises. Some types of meetings that might require a Private Meeting session type could involve executive leadership, the corporate legal team, or research and development for example. The rest of the normal production meetings will still be using Webex.

As shown in Figure 37, the private meeting requirements specify that all participants be either on-premises in the corporate network or connected remotely via a full tunnel VPN connection for media to the corporate network to send and receive media to and from the Video Mesh private meeting. In other words, the attendees must be able to access the Video Mesh from the local network otherwise they will not be able to join this private meeting. When this meeting is active, the Video Mesh will not create a media cascade from the Video Mesh node to Webex; however, the Video Mesh still needs to communicate with Webex so signaling traffic for the cascade will be active during the private meeting. This type of meeting does not make the Video Mesh node a standalone bridge like Cisco Meeting Server, it simply eliminates any media cascading from the Video Mesh to Webex.

Figure 37   Private meetings overview

Devices and applications that are external to the corporate network maybe able to reach the private meeting depending on their connectivity. Table 6 shows the types of devices and situations that may or may not connect to a private meeting.
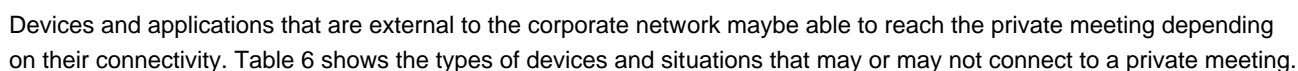
Table 6   Private Meeting Connectivity

Type	Supported
On-premises SIP device registered device to Unified CM or Expressway	Yes
On-premises Webex App (without the Full Feature Webex Experience) or Webex registered video device	Yes
Webex App (without the Full Feature Webex Experience) or devices using VPN (full tunnel)	Yes
Mobile and Remote Access (MRA) registered device	Yes
Webex App or Webex registered video device (no VPN)	No
Device or user not registered to the Webex Org hosting the private meeting	No
PSTN calls	No
Webex Meetings Desktop and Mobile app	No
Web.webex.com	No

Private Meetings requires that the device be registered to the meeting host's Webex organization and that any Webex App (without the Full Featured Webex Experience) user connecting to the private meeting be a member of the host Webex organization. This also applies to a Webex App (without the Full Featured Webex Experience) paired to the Webex registered device scenario, as both need to be part of the host Webex organization.

PSTN calls are considered off the corporate network and unsecure with unknown callers and will not be allowed to access a private meeting hosted on the Video Mesh.

Within a private meeting not all functionalities will be available to the users. This is due to where the functionality or microservices are located. The following functionality is not available because media needs to be sent to Webex to invoke those microservices to produce the action.

- 2-way whiteboarding
- Webex Meeting recordings (Network Based Recording – NBR)
- Webex Assistant
- Transcription and translation of the meeting
- Webex Breakout rooms

The private meeting feature is designed for a regional meeting to have the best quality results. This means that the private meeting can cascade between Video Mesh clusters on the corporate network. This is known as intercluster cascades. In Figure 38, the meeting spans across two different Video Mesh clusters, HQ and Remote. Each cluster has participants that join the meeting, and the cascade is formed dynamically connecting the two clusters together to pass the audio, video, and content to all participants. When planning for private meetings it is important to keep in mind the network path for potential intercluster cascades and ensure that potential paths do not impact the meeting quality. It is recommended to view this type of meeting as a regional meeting.

Figure 38   Intercluster cascade
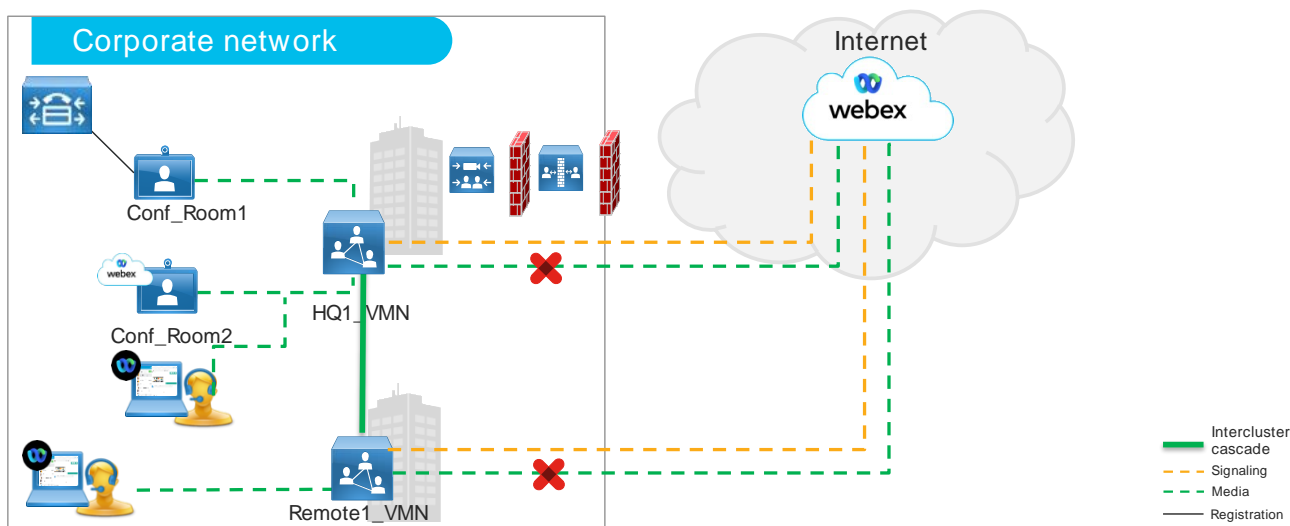
To schedule a private meeting, the private meeting session type needs to be enabled for the scheduling user in Control Hub. Once this entitlement is enabled for the user then that user can schedule a private meeting and invite any participant to the meeting. Scheduling the private meeting can be done several different ways. Table 7 shows the different means that are available to schedule a private meeting.

Table 7   Scheduling a private meeting

Scheduling Method	Supported
Webex Web Scheduler	Yes
Outlook with Productivity Tools	Yes
Webex Scheduler for M365	Yes
Webex Meetings XML API	Yes
Scheduled Space Meeting	Yes
Personal Meeting Room (PMR) scheduling	No
@webex scheduling	No
Webex App – In app scheduler	No

Finally, when configuring private meetings, there are two settings that can be enabled by the administrator to allow the private meeting functionality. In the Control Hub, within the Video Mesh Clusters global setting page, there is an org-wide Private Meeting toggle that will turn on the capabilities of scheduling a private meeting. When this toggle is enabled, anyone scheduling a space meeting will get a private meeting. This applies to all spaces in the organization. Figure 39

shows the toggle to enable private scheduled space meetings.

Figure 39   Scheduled Space Meeting - Private
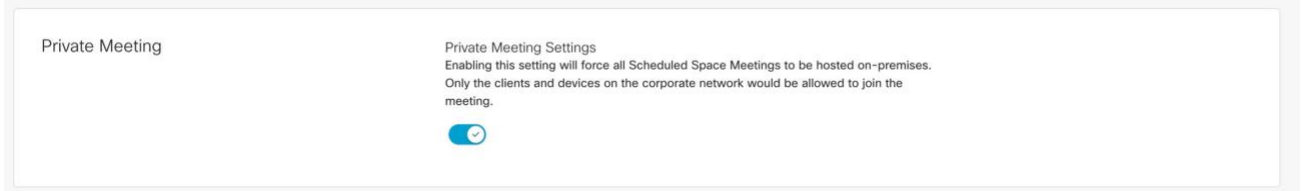
As shown in Figure 40 in the Video Mesh cluster settings, there is another toggle that will take a cluster and reserve it for private meetings only. It is recommended to have at least a single cluster for private meetings to guarantee resources are available for those participants to join a private meeting. If none of the clusters are enabled for private meetings, the private meeting will be started on the same Video Mesh nodes that are used for all other meetings.

Figure 40   Reserve cluster for Private Meetings only
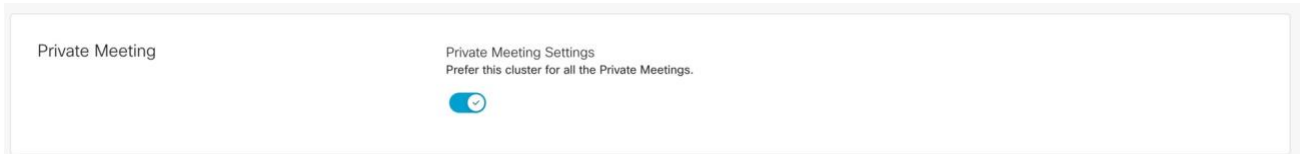
When a Video Mesh cluster is marked as private, it has a capacity limit equal to the capacity of the number of nodes in the cluster. If a participant of a private meeting tries to join a private meeting when the capacity of the private meeting cluster is reached, then that participant will be redirected to the other non-private clusters in the corporate network. This will continue until all the Video Mesh resources are full but will not overflow that participant to the cloud because this is a private meeting. When the participant lands on a non-private cluster, an intercluster cascade will be established between the non-private cluster and the private cluster to link all the participants together in the meeting.

To get insight on private meeting utilization within the organization, the Control Hub Analytics reports under the Engagement and Resources tab have three separate graphs showing the number of call joins to a private or non-private meeting, the number of private meetings in a cluster, and maximum call distribution of private meetings by cluster. These reports will not show up in Control Hub Analytics until a private meeting has been completed.
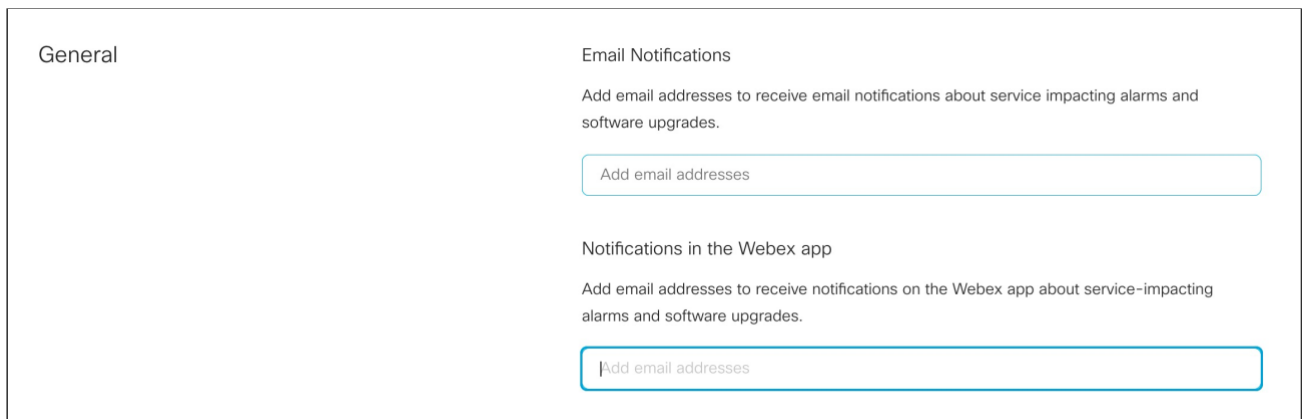
Video Mesh in the Control Hub

The Control Hub is the management portal for the Webex portfolio and within the webpages the Video Mesh has several areas of post-installation that are important for the administrators. It is recommended that each administrator do the following in Control Hub:

- Place an email in the configuration page to receive notifications within the Webex App or email about Video Mesh alarms.

- Enable one Video Mesh node in every cluster for the Video Mesh Monitoring Tool.

- Monitor the Video Mesh Analytics to plan for increased capacity in the future.

To enable alarm notification to be received in the Webex App or by email, the administrator needs to add an email address in the following settings: Hybrid -> Video Mesh card -> Settings. Figure 41 shows the configuration areas inside the Video Mesh settings on the Control Hub.

Figure 41 Notifications Setup

The information provided in the notification is based on the Video Mesh Events in the Control Hub. These events provide records of events and historical changes to the Video Mesh nodes such as DNS issues, NTP issues, communication issues to Webex, upgrades scheduled and completed, and many more. There are different levels of severity on each event that are classified on the webpage with labels such as Error, Warning, Resolved, and Info. The information presented in the Control Hub can be filtered by node and timeframe. Figure 42 shows an example of the type of information that can be seen in the events log.

Figure 42   Video Mesh Events
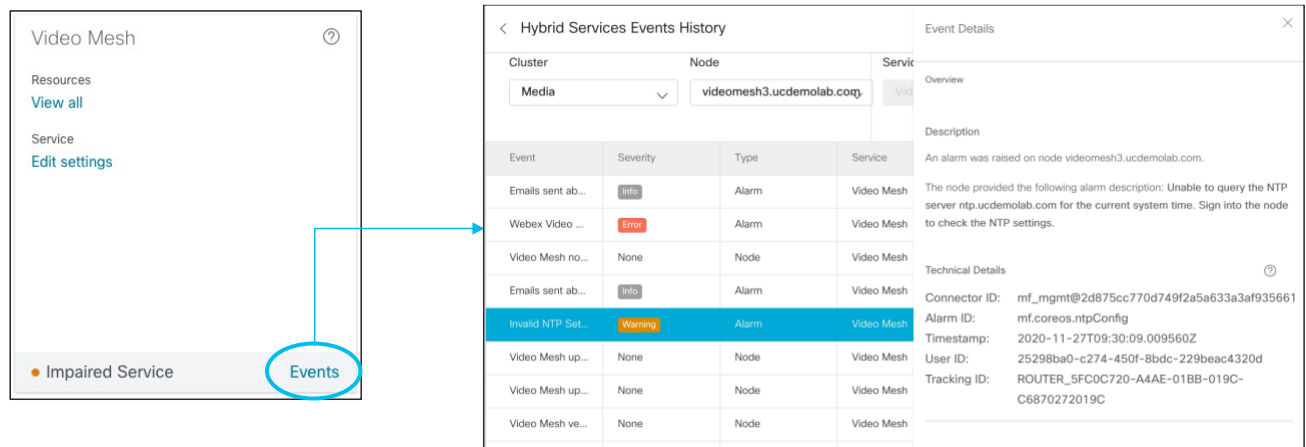
The Video Mesh Monitoring Tool can engage a Webex call simulator available on every Video Mesh node. It is recommended to enable this tool on at least one Video Mesh node in every cluster and can be accessed by going to: Troubleshooting -> Video Mesh in the Control Hub. When the tests are performed by the Video Mesh, it will check the SIP signaling, media signaling and media cascade, detecting failures to increase the mean time to resolution by the administrator. These tests are performed every 6 hours but have an option for the administrator to run them at any point in time. If the Video Mesh node has active calls going on, the service will intelligently skip the scheduled tests because active calls are happening on that Video Mesh node. Also running the Video Mesh Monitoring Tool does not impact the participant capacity of the Video Mesh. Within the Control Hub webpage, the administrator can see a historical view displaying the results for the last 24 hours or last 7 days. Figure 43 shows an example of what is displayed on the Video Mesh Monitoring Tool.

Figure 43   Video Mesh Monitoring Tool
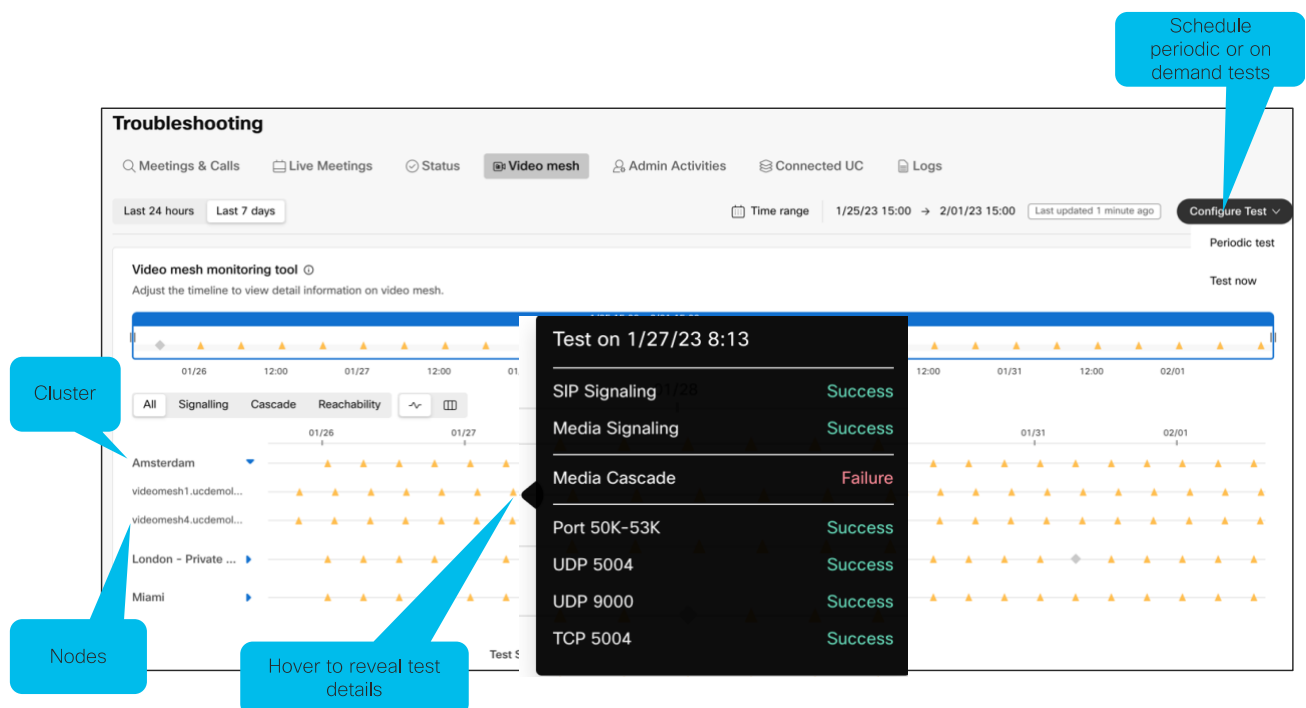
The Control Hub Analytics has a webpage "Video Mesh" that is specific to the Video Mesh analytics. This page is broken down into four sections, "Live Monitoring", "Engagement", "Resources", and "Bandwidth Usage" with a simple view of Key Performance Indicators (KPI) at the top of the webpage. Within each tab there are two columns, on the left a circle or bar graph and on the right is a trend graph is shown. Each graph can save data into PNG, JPG, PDF, CSV or XLS formats. The data can be selected for a specific element, and each appropriate graph will be updated with the selected node or cluster information only. When viewing the chart timelines, they are dependent on the selection of the data timeline.

- Last 24 hours - Changes the horizontal access to every 10 minutes

- Last 7 days - Changes the horizontal access to every 1 hour

- Last 30 days - Changes the horizontal access to every 3 hours

- Last 90 days - Changes the horizontal access to every 8 hours

The Video Mesh Analytics page refreshes every 10 minutes.

Each tab, "Live Monitoring", "Engagement", "Resources", and "Bandwidth Usage" focus on different aspects of data around the Video Mesh. The Live Monitoring tab focuses on the cluster availability, resource utilization, overflow, redirect and bandwidth trends over the last 4 hour or the last 24 hour period. The Engagement tab focuses on the number of participants that connect to the Video Mesh, the number that connect to Webex and the number of participants that overflowed to the cloud for a Webex Meetings. This includes multi-party and 1:1 meetings that utilized the Video Mesh. In addition, the Engagement charts provide information on the types of devices per call leg used in those meetings as shown in Figure 44.

Figure 44   Call Legs by Endpoint type
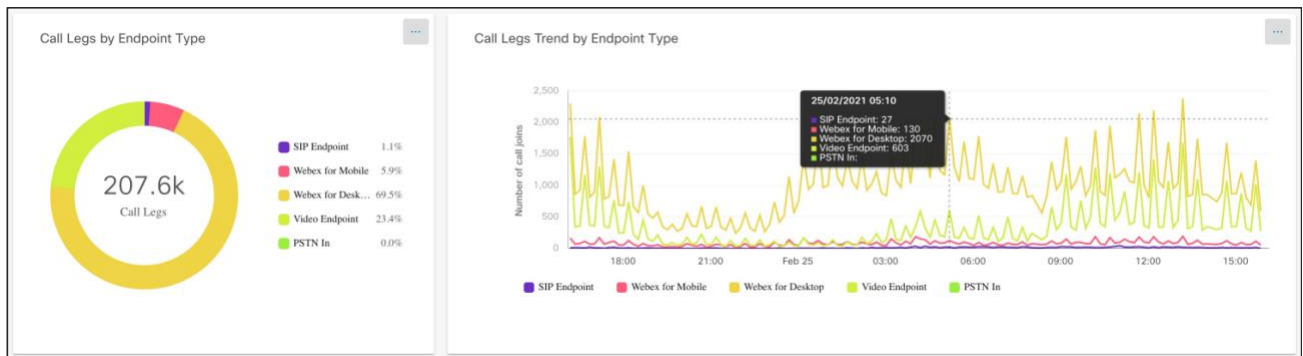
The Resources tab focuses on the Video Mesh cluster availability, call overflows and call redirects. Call overflows are when the Video Mesh clusters in the organization cannot handle a request from a participant to join a meeting. At that time instead of ending the call attempt, the Video Mesh will have the participant sent to Webex to use Webex's meeting resource to join the meeting. The Call Overflow Analytics will provide a count of the number of overflows, when it happened, and a reason for the overflow. Figure 45 shows an example of an overflow that happened 5 times because there were not enough resources available on the Video Mesh cluster.

Figure 45   Overflow to Cloud Details

Call redirects are the process when a single Video Mesh cluster has reached capacity and is unable to accept another call or participant and will redirect the request to another Video Mesh cluster on the corporate network. This normally happens when the original Video Mesh cluster needs additional nodes installed. Figure 46 shows an example of the redirect information available in the resource webpage.

Figure 46   Call Redirect Details

The Bandwidth Usage tab provides information on the cascade bandwidth usage per cluster, the bandwidth used per data type, transmit and receive, and the bandwidth used per data stream, audio, video, and content. Figure 47 shows an example of the bandwidth used in a cascade per data stream.

Figure 47   Total Cascaded Data Stream Usage
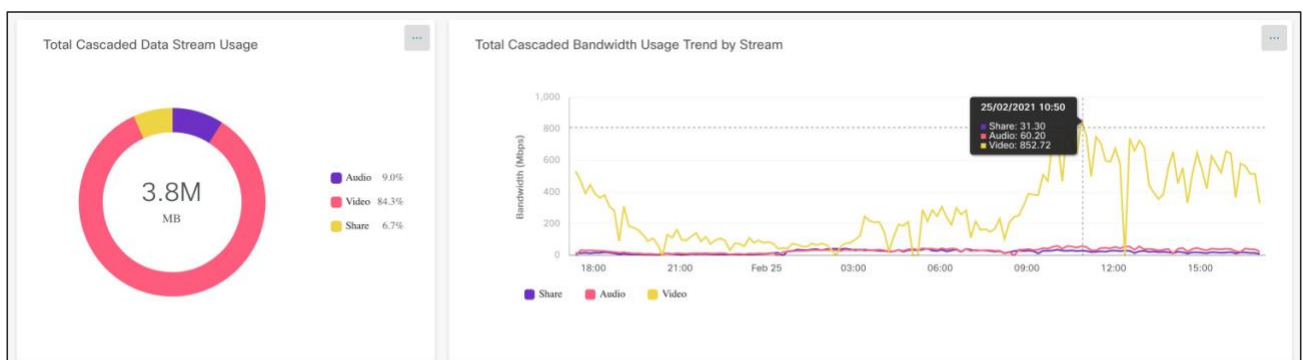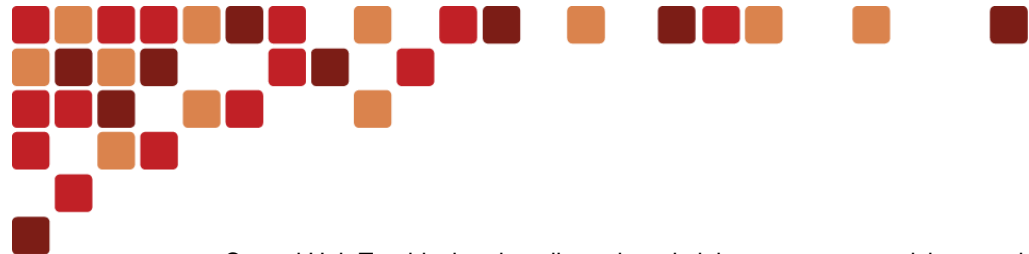
Control Hub Troubleshooting allows the administrator to see participant activity, audio, video and device utilization as well to help identify issues. One of the many pieces of information that is available is the media node that a participant is utilizing for that meeting. The media node can be a Webex datacenter or a Video Mesh node in the corporate network. The media node is visible by clicking on a participant and looking inside the *Equipment and Networks* information box located on the top right-hand side of the webpage. If the participant is using the corporate Video Mesh node then *VMS:Cluster_Name: Node_Name* is displayed, but if the participant is using a Webex datacenter it will show the location of the datacenter only. Figure 48 shows an example of the participant utilizing a corporate Video Mesh node where the Video Mesh cluster name in Control Hub is "Tampa" and the specific Video Mesh node being used is "videomesh1.ucdemolab.com". In some instance there may be multiple nodes that are displayed. In this scenario an internal cascade was made in the Video Mesh cluster to connect the participants into the same meeting. This cascade is done automatically by Webex and is not configurable. When this scenario happens *VMS:Cluster_Name: Secondary_Node:Host_Node* will be displayed in the *Equipment and Networks* information box located on the top right-hand side of the participants troubleshooting webpage. Figure 49 displays the Cluster_Name as "blr_test", the Secondary_Node as "blrecp5.cisco.com" and the Host_Node as 10.196.6.16.

This article on help.webex.com explains all the other capabilities and insights available within the troubleshooting page.

Figure 48   Troubleshooting showing a Video Mesh node being used by participant.
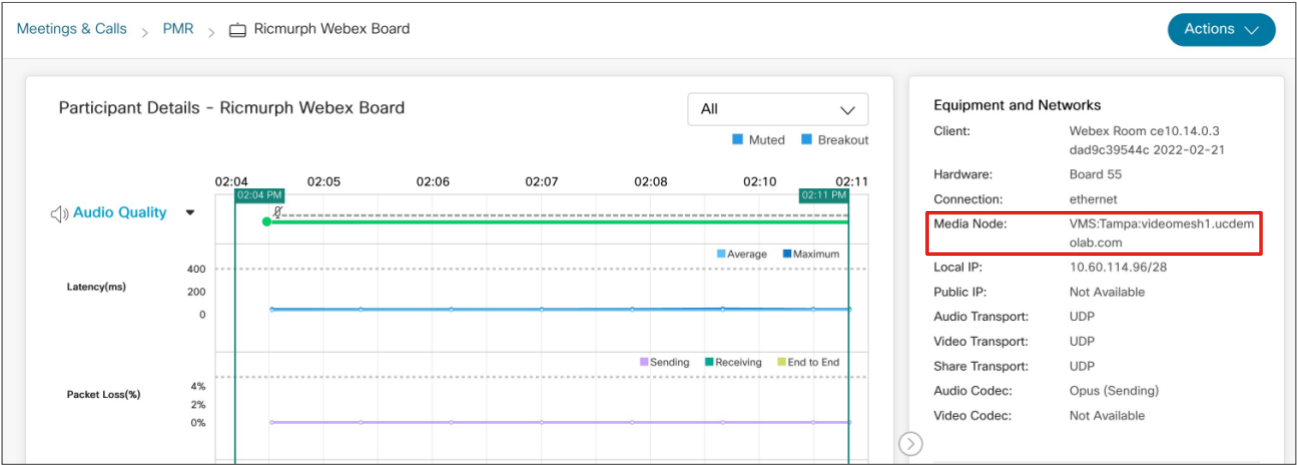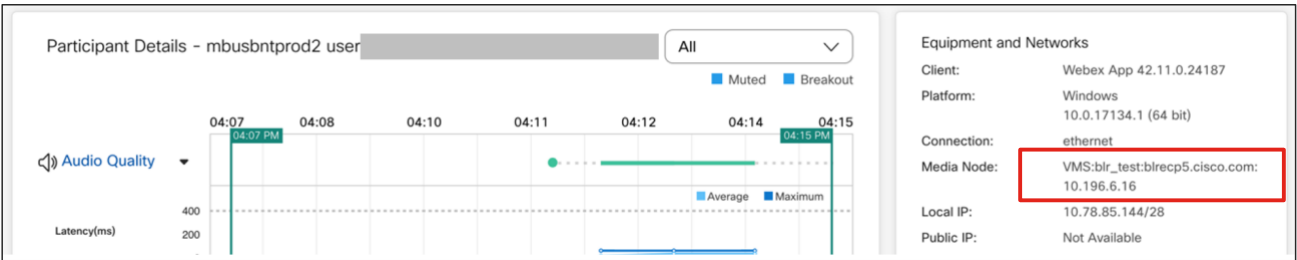

Figure 49   Troubleshooting showing a Video Mesh node that cascaded in the cluster to join all the participants

ThousandEyes

The Video Mesh platform has integrated a ThousandEyes Enterprise Agent into the platform, enabling the administrator to perform end-to-end monitoring across the network. This integration equips the administrator with a wide array of network monitoring tests, opening visibility into many areas of the network path. Issues anywhere along a customer's network infrastructure can be narrowed down and diagnosed with greater precision, improving the efficiency of their deployment.

After the Video Mesh nodes have been registered in ThousandEyes, the administrator can perform the following tests in the ThousandEyes portal.

- Network Test – Agent to Agent
- SIP Server Test
- RTP Stream Test
- Webex HTTP Server URL Test
- Authoritative Webex DNS Server Test

More information about this integration can be found in the Video Mesh configuration guide.

Note that if the Video Mesh node is using a proxy configuration, then the ThousandEyes agent will not be able to work properly. This is a limitation in the solution currently.
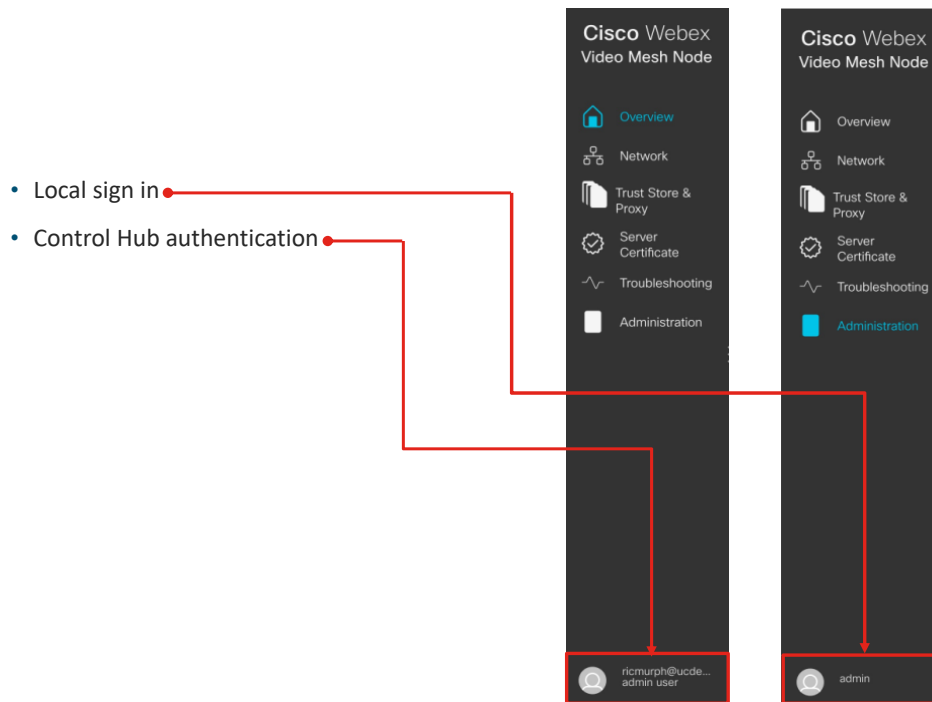
Video Mesh Webpage

While the Control Hub provides a lot of good analytics, the individual Video Mesh nodes provide additional capabilities that the administrator can utilize. The access to the Video Mesh node can be done directly by going to https://<Video_Mesh_Node_ip_address_or_fqdn>/setup using the admin login and password or directly from Control Hub by using the "Go to Node" option which uses the Control Hub authentication to login to the Video Mesh node. In order to use the Control Hub authentication to a Video Mesh, the user must be a full administrator in that Webex organization. This ability does not work for users that are functional, service or partner administrators. The "Go to Node" is located in the node settings in the cluster details page. Figure 50 shows the "Go to Node" option.

Figure 50   Go to Node
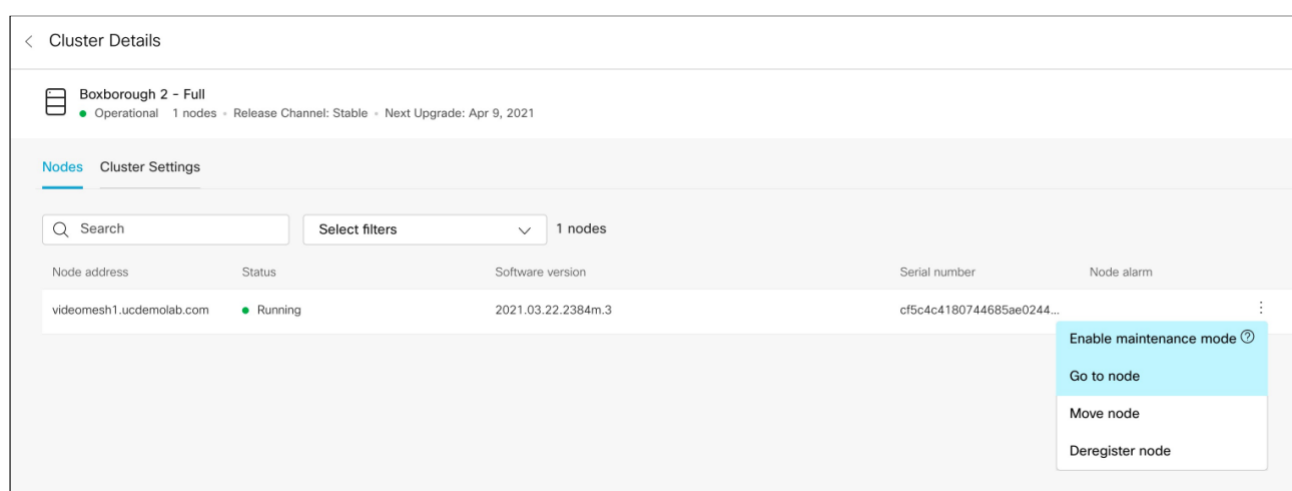
Once logged into the Video Mesh webpage it is easy to see the authentication mechanism used. Figure 51 shows a Control Hub administrator and local admin user login to the Video Mesh webpage.

Figure 51   Video Mesh Webpage authentication login

Once authenticated and logged into the Video Mesh, there are several tabs on the left side of the webpage: Overview, Network, Trust Store & Proxy, Server Certificate, Troubleshooting and Administration.

The Overview page provides information around the Video Mesh node such as

- Call Status
- Node Details
- Node Health
- Node Notifications
- Network Settings
- Registration Details
- Connectivity Checks

The call status is the number of calls or participants that are being hosted on that Video Mesh node at that time. It does not state the individual device or application, just a numerical value of the total call legs connecting. To see if a participant is using a Video Mesh in a meeting, this can be done in the Troubleshooting section of Control Hub for that particular meeting.

If the connectivity checks in the Connectivity Test boxes have anything besides "Pass" then the administrator is advised to hover the mouse pointer over the failed connection and utilize the information provided to figure out why that Video Mesh is unable to reach those external services required for the Video Mesh to function properly. Figure 52 shows the entire Overview page.

Figure 52   Overview Page
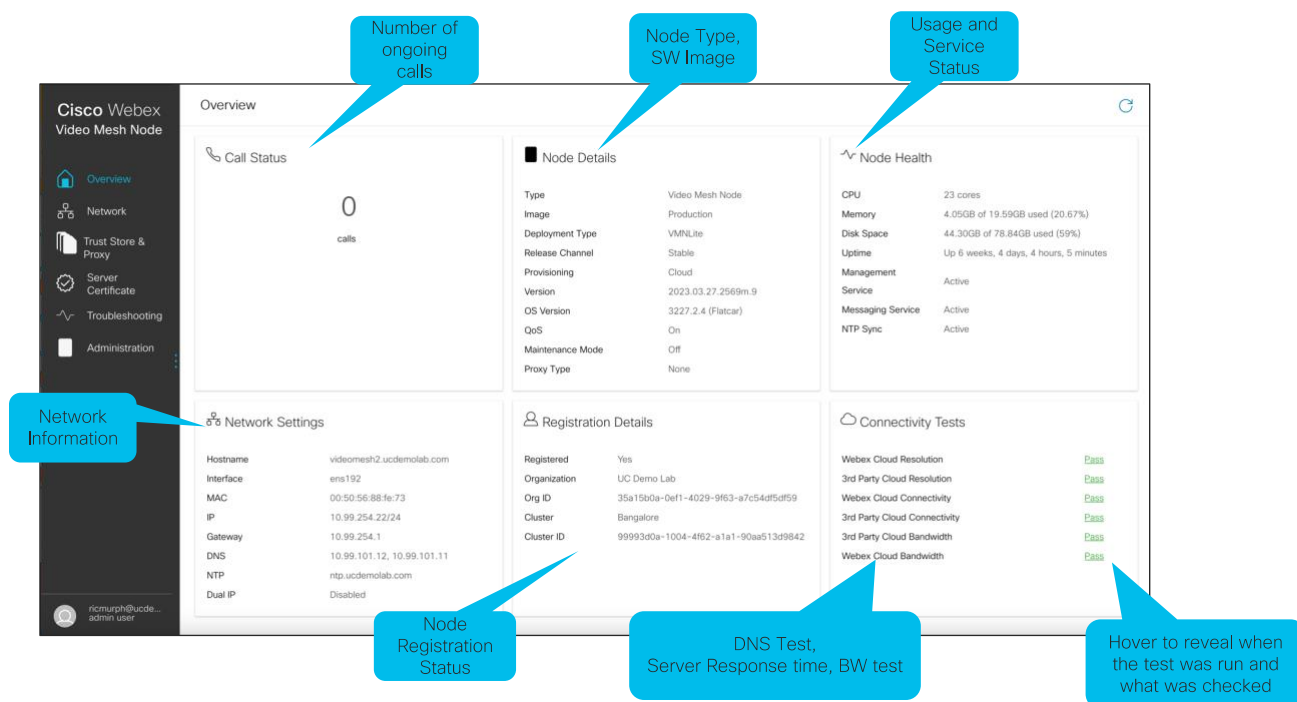
The Network webpage has the basic IP addressing information needed for the Video Mesh to communication on the primary and secondary NIC. This interface allows for the IP address, Mask, Gateway, DNS and NTP settings to be configured for either interface. In the Advanced tab there is also the ability for the administrator to change the default IP subnet used by the Video Mesh software for container-to-container communication. The default configuration is 172.17.42.0 - 172.17.42.63 but if this overlaps with any internal configuration, it can be changed after the Video Mesh is put into maintenance mode.

The Trust Store & Proxy webpage allows for the configuration to work with a Transparent, inspecting, or non-inspecting, and Explicit proxy. The Transparent inspecting proxy requires a certificate uploaded to the Video Mesh node with no http(s) configuration changes; however, the Video Mesh nodes need a root certificate so that they trust the proxy. Inspecting proxies are typically used by IT to enforce policies regarding which websites can be visited and types of content that are not permitted. This type of proxy decrypts all traffic, even https.

For Explicit proxy configuration the administrator configures the Video Mesh node with the proxy to use an authentication mechanism. To do this the administrator will need to know the proxy IP address and proxy listening port. Additionally, there are several different authentication types supported by the Video Mesh for an explicit proxy.

- **None**: for HTTP or HTTPs explicit proxies, no further authentication is required.
- **Basic**: for HTTP or HTTPs explicit proxies and used for an HTTP user agent to provide a username and password when making a request, and uses Base64 encoding
- **Digest**: for HTTPs explicit proxies only and used to confirm the identity of a user before sending sensitive information and applies a hash function on the username and password before sending over the network.
- **NTLM**: for HTTP only. Like Digest, NTLM is used to confirm the identity of a user before sending sensitive information. Uses Windows credentials instead of the username and password.

Figure 53 shows the explicit proxy page configuration mentioned above.

Figure 53   Explicit Proxy

The Server Certificate webpage allows the administrator to create a certificate signing request (CSR), upload a server certificate in .crt or .pem format, and upload a private key. This webpage would be utilized for proxy and secure communication configuration with Unified Communications Manager.

The Troubleshooting webpage has many different functions that will be useful to the administrator when trying to figure out issues relating to a Video Mesh. This webpage has the following functions.
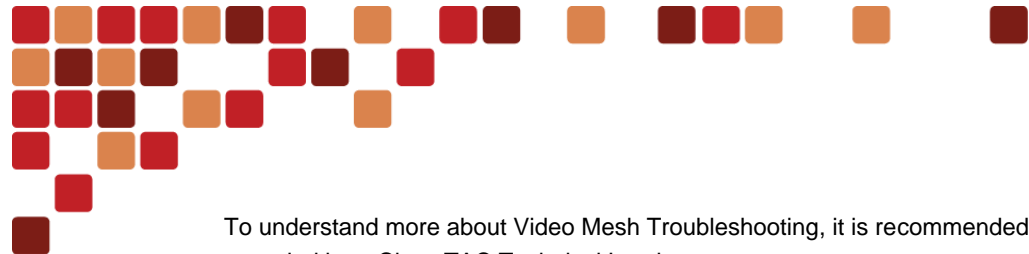
- Send Logs
- Packet Capture
- Ping
- Traceroute
- Check NTP server
- Reflector Tool
- Debug User

The Send Logs section of the webpage allows the administrator to download or send the Video Mesh logs to Cisco. Once the logs are sent to Cisco an upload identifier is shown that can be used for reference when communicating with Cisco TAC. If further packet capture is needed to troubleshoot the issue the Video Mesh can create a PCAP file with parameters, to limit the capture to a single interface, host, or port. The PCAP file has maximum size of 2 GB.

Ping, traceroute, and the NTP server check are standard tools to test connectivity or paths to a remote IP address or device.

The Reflector Tool was discussed in the QoS section and is used for port tests when QoS is enabled or disabled on the Video Mesh node. This setting enables the Reflector Tool on the Video Mesh.

It is recommended that the Debug User remain disabled and enabled only when advised by Cisco TAC.

To understand more about Video Mesh Troubleshooting, it is recommended to watch the following Cisco Live session recorded by a Cisco TAC Technical Leader.

Troubleshooting the Cisco Webex Video Mesh Solution – DGTL-BRKCOL-3002

- Event: 2020 Digital
- Speaker: Paul Stojanovski
- Available at: https://www.ciscolive.com/on-demand/on-demand-library.html?search=DGTL-BRKCOL-3002#/

The Administration webpage allows for the following functionality:

- Local Sign In
- Change Passphrase
- Change Password Expiry
- Maintenance Mode
- Reboot Node
- Shutdown Node
- Factory Reset
- External Logging

The Local Sign In toggle allows the administrator to disable the local "admin" user account access to the Video Mesh. This setting can be enabled along with the Control Hub authentication for access to the Video Mesh webpage by different accounts.

The admin password will expire 90 days after being set. This timeframe can be changed inside the Change Password Expiry to meet the password security policy of the organization. This setting allows for expiration of the admin password from 2 up to 365 days.

APIs

Application Programming Interface (API) are available for the Video Mesh that allow the developer to programmatically get a rich set of information and perform tasks relating the Video Mesh. The Video Mesh APIs can be categorized into these areas, provisioning, configuration updates, analytics and monitoring.

Provisioning APIs

The Video Mesh can be installed using the browser interface and this process works great for installing a few nodes, but it does not work well for larger number of nodes because of the amount of time and repetition required by the administrator to accomplish the installation. To install large number Video Mesh nodes it is recommended that the administrator evaluate using the Provisioning API script. This script is located on GitHub and when used, requires the administrator to have already downloaded the Video Mesh OVA file, created the config.json file, created the input_data or input_data_vcenter csv file that contains the Video Mesh parameters such as name, IP address, mask, gateway, DNS, NTP, hostname and more. This script will save time and allow for a simple programmatic way to deploy large numbers of Video Mesh nodes in the corporate network.
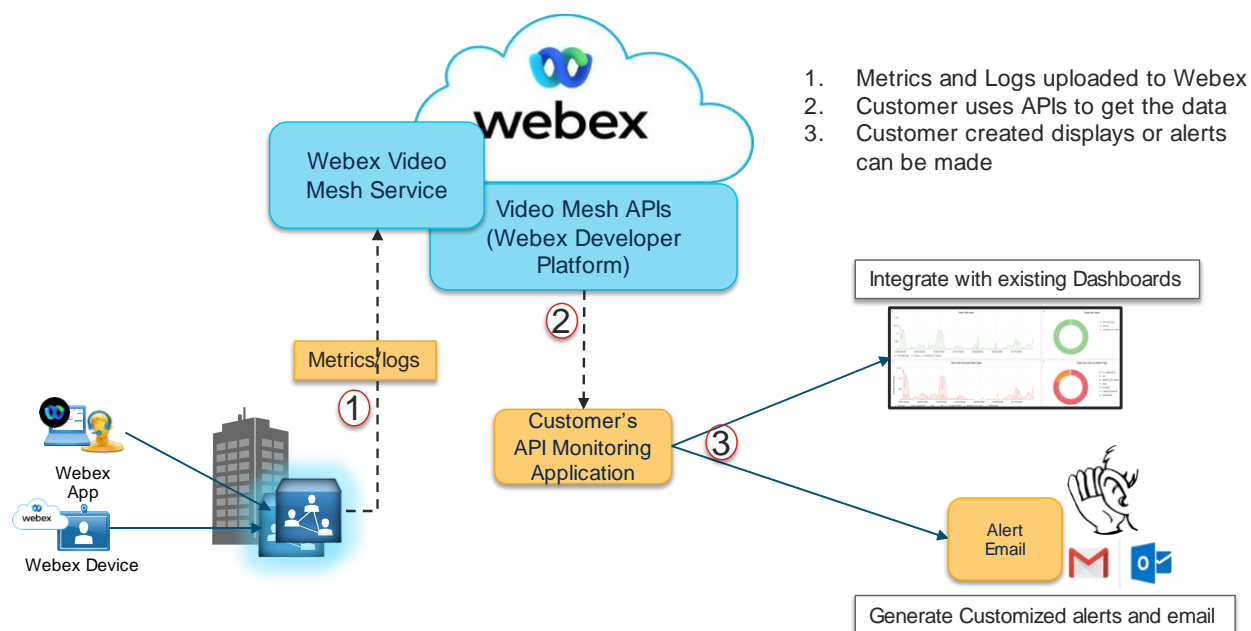
Configuration Updates

After the initial installation of the Video Mesh nodes there may be a requirement to update parameters such as DNS or NTP as the network changes. This would be a tedious task to do via the Video Mesh web interface but the Video Mesh offers Day 2 scripts for network parameters, passwords and certificates that the administrator can use to programmatically change settings.

Analytics and Monitoring APIs

The Video Mesh team has built an API framework that can be used to get information outside Control Hub so that the administrator can ingest the data into other tools for custom alerting or displaying the data within internal tools. Figure 54 shows the general flow of events to get the data.

Figure 54 API Framework

1. Metrics and Logs uploaded to Webex
2. Customer uses APIs to get the data
3. Customer created displays or alerts can be made

The Webex Developer Platform contains the information about the available Video Mesh APIs and the constructs of the API. If the administrator is not familiar with APIs the Webex developer platform allows the administrator to run the specific commands on their Video Mesh nodes to see the json results within the webpage. This gives the administrator the information that will be returned from the platform when using the Video Mesh APIs.

The Video Mesh APIs give the administrator a way to retrieve the same analytics and monitoring data that is displayed in the Control Hub Analytics page. Additionally, the APIs provide the ability for the administrator to trigger on-demand troubleshooting tests, like the Video Mesh Monitoring Tool, Network tests, and Reachability tests from the Webex Developer Portal or their own monitoring application which can help in quickly isolating and identifying the root cause of issues. The Video Mesh team has created an application shown in Figure 55 that is a simple example of how the APIs can be used to track organization data, retrieves and displays data such as Cluster Details, Cluster and Node Availability, Cluster Utilization, Call Redirects and Overflows, Media Health Monitoring and Reachability Test Results. This example is available on GitHub.

Figure 55 Sample client application
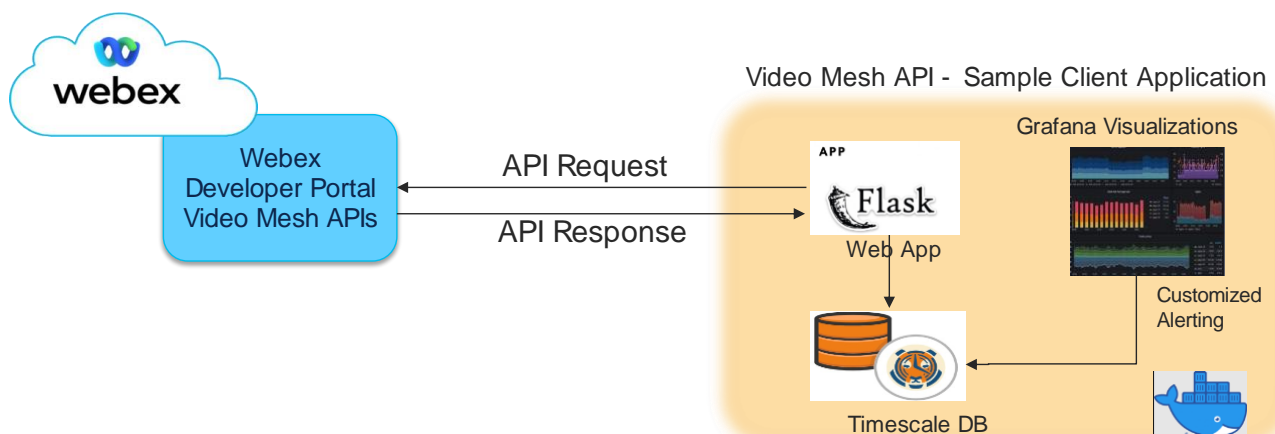
Conclusion

Three key points to keep in mind when deploying the Video Mesh:

1. Deploy Video Mesh nodes in the large campus sites with Internet connections. Start small and grow as needed.

2. Keep in mind the cascade path when placing a Video Mesh cluster in the architecture.

3. Continuously monitor the Video Mesh analytics, add more nodes and/or clusters based the observed traffic patterns, specifically watching the overflow and redirect alerts.

Reference Links

General Information

https://www.cisco.com/c/en/us/solutions/collaboration/webex-hybrid-services/webex-hybrid-media-service.html

Deployment Guide

http://www.cisco.com/go/video-mesh

Release Notes

https://help.webex.com/en-us/jgobq2/Cisco-Webex-Video-Mesh-Release-Notes

Network requirements

https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Teams-Services

Video Mesh Analytics

https://help.webex.com/en-us/n0rlwxe/Analytics-for-Your-Cloud-Collaboration-Portfolio#Cisco_Concept.dita_a07f1228-c4a7-445c-952a-e4d0f97cc23d

Video Mesh Cisco Validated Design (CVD)

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Collaboration/hybrid/pa_hybrid_vmn.pdf