Deployment Guide

Next Generation Enterprise WAN

Video Deployment Guide

October, 2011

NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR NABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R).

Next Generation Enterprise WAN Video Deployment Guide.

Contents

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

screen font	Terminal sessions and information in the displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Nonprinting characters, such as passwords, are in angle brackets.
< >	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note: Notes contain helpful suggestions or references to material not covered in the manual.

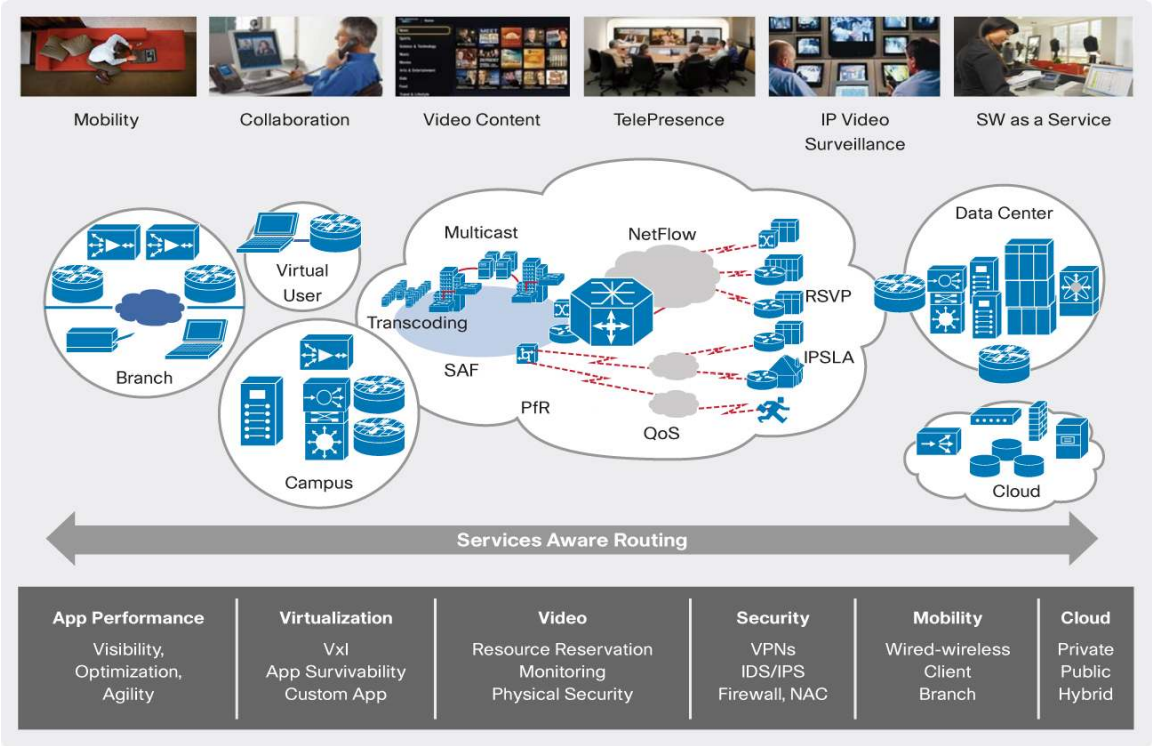
Caution: Cautions indicate that in this situation, you might do something that could result in equipment damage or loss of data.

Warning: Warnings indicate a potential situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.

Related Documentation

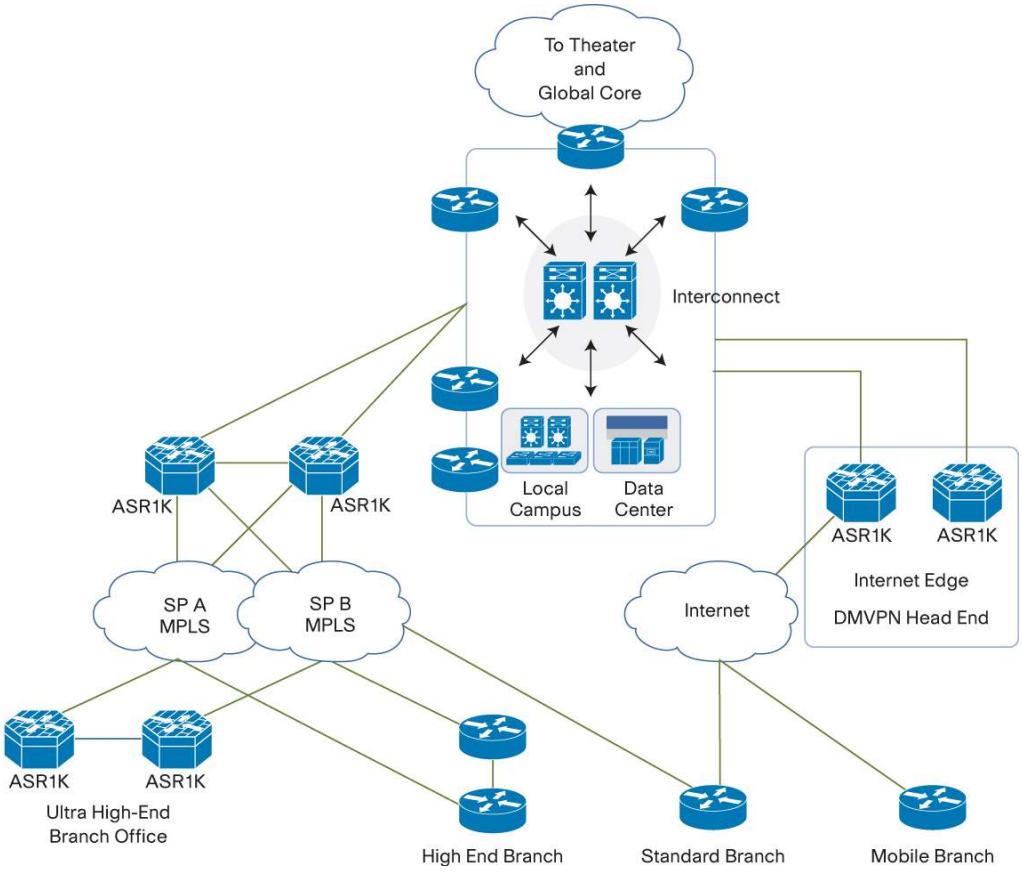
For additional information on Next Generation Enterprise WAN, refer to the following documents.

NGEW Architecture Overview



Enterprise networks must adapt to meet new and evolving business requirements. With the introduction of cloud services (private, public, or hybrid) pose new challenges to current enterprise network designs. With a more distributed workforce, the proliferation of bandwidth intensive video enabled endpoints, and the consolidation of servers into a few centralized locations requires networks to carry more traffic, with increase efficiencies, while demanding the same or a high level of performance and availability.

The Cisco Next Generation Enterprise WAN (NGEW) is a Cisco, end-to-end architecture, which provides foundation building blocks for next-generation enterprise networks. The hierarchical design provides the scalability required by large enterprise, which can be extended and replicated throughout multiple regions and theaters. This consistency leads to ease of deployment, maintenance and troubleshooting.



A logical starting point is the Regional WAN, where all branch locations connect through various access technologies, such as wireless (3G/4G), DSL, and MPLS, to the highly scalable aggregation routers at the Enterprise Interconnect. The Enterprise Interconnect is the location where traffic from regional WAN is aggregated to the In-theater and global WAN cores. In addition, the Enterprise Interconnect links all the other components of NGEW including local Data Centers and Campus, as well as Enterprise Edge which is the demarcation point between enterprise networks and any external network service (e.g. Internet, Cloud, Voice).

Within the NGEW Regional WAN module, NGEW defines four branch designs

- **Mobile Branch** - Single tier, single WAN link, mobile with minimal redundancy
- **Standard Branch** - Single tier, dual WAN links providing redundancy for link failures
- **High-end Branch** - Dual tier, dual WAN links providing maximum redundancy for both device and link failures
- **Ultra High-end Branch** - Based on the High-end Branch with increased capacity and higher availability

In addition to providing advanced routing functionality, one of the primary design goals of NGEW is to build a network foundation that can reliably support new applications and services including those in the Cisco Borderless Network - Application Velocity, Medianet, IPv6, and Mobility. Customers will benefit from investing in Cisco network design that has gone through rigorous testing, and scales to support new applications and services to address their continuously evolving business requirement.

Video Business Overview

Multiple researches indicate video traffic is growing at a very rapid rate. Today workforces are more distributed, however the need for face-to-face communication is still required to maintain collaboration and productivity. Interactive video is expanding from conference room based video such as TelePresence to desktop and mobile video. The proliferation of video-enabled mobile devices put additional requirements for the network to support communications among video enabled endpoints with varying capabilities.

This is creating concern that networks may not be ready to support additional traffic demands, combined this with the requirement to evaluate, monitor, and troubleshoot video deployment, may delay enterprise video deployment and impact business growth. WAN bandwidth is a high re-occurring cost and thus limited, to ensure efficient use of resources requires an intelligent routing and video termination resource in the branch. In addition, the enterprise needs to ensure the video traffic does not impact its self and can coexist with the business critical applications and services.

Cisco NGEW enables the deployment of **medianet** features providing enterprises a number of tools to evaluate, monitor, and troubleshoot video deployment. Branch videoconference resource provides a local videoconference bridge to reduce the amount of video traffic that needs to traverse the WAN link. The 12-class QoS policy along with proper provisioning protects latency sensitive voice and video traffic, while maximizing throughput for business critical applications.

Video Technology Overview

Medianet

A medianet is an end-to-end network architecture comprised of intelligent technologies and devices in a platform optimized for the delivery of rich-media experiences. Medianet has the following characteristics.

- **Media-aware:** Can detect and optimize different media and application types (TelePresence, video surveillance, desktop collaboration, and streaming media) to deliver the best experience
- **Endpoint-aware:** Automatically detects and configures media endpoints
- **Network-aware:** Can detect and respond to changes in device, connection, and service availability

With the increasing adoption of new video and rich-media applications, medianet technologies become critical to address challenges associated with the transmission of video and rich media over the network, including ensuring predictability, performance, quality, and security.

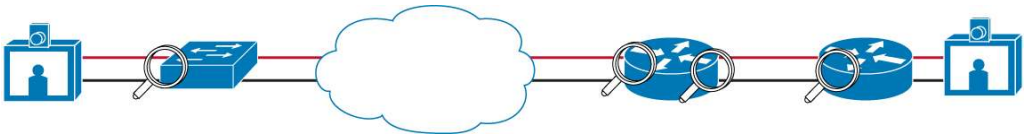
By accelerating deployment of applications, minimizing complexity and ongoing operational costs, and helping to scale the infrastructure for the best quality of experience (QoE), medianet technologies helps to address these challenges.

Cisco Media Monitoring

Cisco Media Monitoring, one of the capabilities provided by medianet, provides monitoring and troubleshooting capabilities for video traffic. There are two features within Cisco Media Monitoring that are implemented in NGEW.

- **Cisco Performance Monitor**, with ActionPacked! LiveAction for monitoring
- **Mediatrace**, with Cisco Collaboration Manager for monitoring

Cisco Performance Monitor



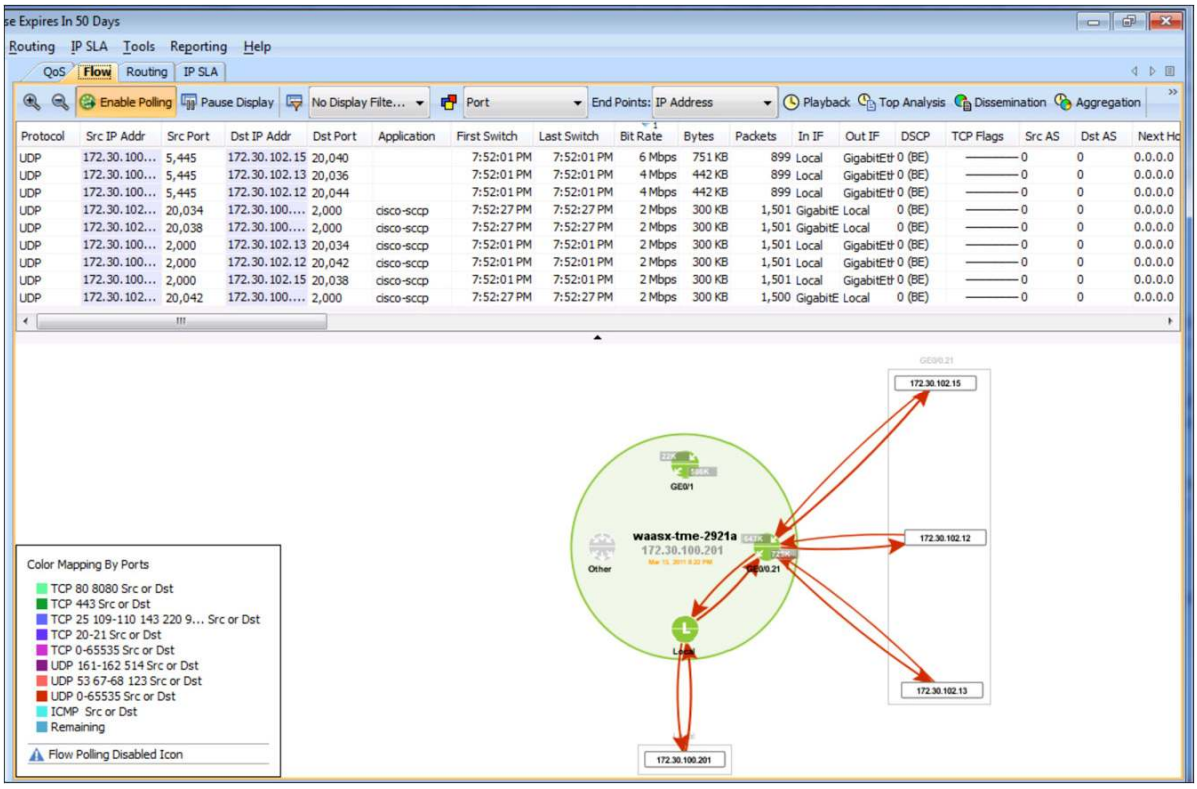
Cisco Performance Monitor allows routers to monitor the media streams as they flow through, and capture important performance metrics such as jitter, latency, DSCP value, and packet loss.

Administrator can also set up performance metrics threshold, i.e. jitter, RTP packet loss. Once the performance metrics exceeds the threshold values, a syslog or SNMP traps are generated to notify the network administrators of potential issue.

The flow performance metrics are exported in Flexible Netflow v9 format, and can be consumed by external monitoring tool, i.e. ActionPacked! LiveAction, Plixer Scrutinizer, CA NetQoS, SevOne.

ActionPacked! LiveAction

ActionPacked! LiveAction (http://actionpacked.com/products/overview) is a monitoring software that can be used to analyze and display netflow records generated by Cisco Performance Monitor. It will display all the streams currently tracked by Cisco Performance Monitor, and their performance metrics, such as bit rate, jitter, RTP loss rate, etc. It also stores a history of these performance metrics, which can be replayed when troubleshooting the problems. Below chart shows the streams from 3 videophones doing conferencing through a videoconference bridge.



Mediatrace

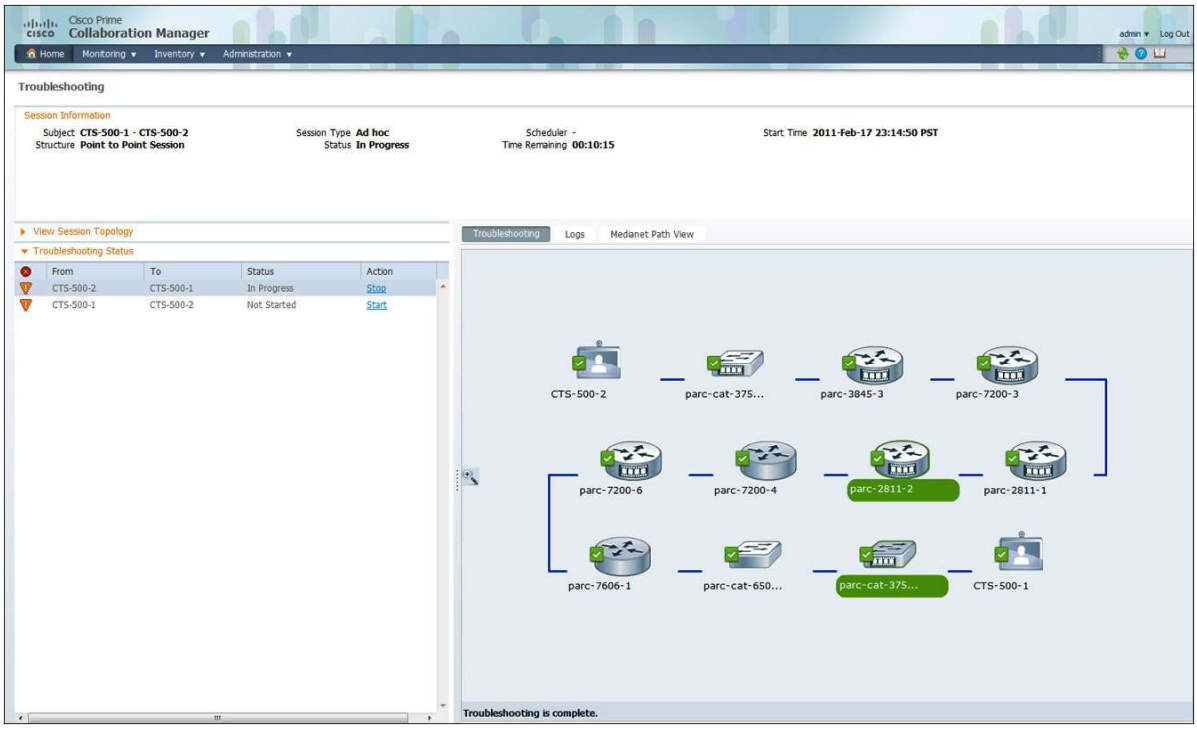
Mediatrace provides the capability to troubleshoot the media performance issue on the fly. Mediatrace can be initiated on-demand or at regular interval. Initiator of the mediatrace can request different types of mediatrace profiles, which provide information and statistics such as, media path, input and output interfaces, system resource, and performance metrics for all the devices along the media path. Below describes all the available mediatrace profiles and metric types.

Profile	Metric type	Use for
system	cpu	Collecting CPU of devices along media path
	memory	Collecting memory of devices along media path
	intf	Collecting input/output interfaces of devices along media path
perf-monitor	Rtp	Collecting RTP metrics
	tcp	Collecting TCP metrics

Cisco Collaboration Manager can be used to initiate mediatrace and display the trace results.

Cisco Collaboration Manager

Cisco Collaboration Manager 1.0 is a service assurance product targeted at managing Cisco Collaboration Services. The current release supports Cisco TelePresence devices.



Cisco Collaboration Manager provides the following functionalities.

- End-to-end visibility of video collaboration services, including end-user quality of experience.
- Real-time monitoring capabilities for all sessions, endpoints, application managers, call processors, and devices that reside in an Enterprise video collaboration network.
- Troubleshooting information in near real-time. It identifies whether the problems are at video application endpoints or in a network segment.
- Immediate access to critical fault information and performance statistics. It minimizes the effort required to isolate, classify, and correlate service-affecting outages, at lower operational costs.
- Ability to identify video collaboration quality degradations to the specific devices and/or interfaces that causes them.

Branch Videoconference

A videoconference bridge brings together three or more callers from a variety of video endpoints. This capability is traditionally provided in a MCU at the headquarter location. When majority of conference participants are located at the branch, each participant's video traffic is sent to the MCU in headquarter, which provides video mixing, and then is sent back to the branch. This creates significant amount of traffic on the enterprise WAN.

With branch videoconference support in ISR-G2, PVDM3 modules, which can be controlled by CUCM or CUCME, are used to provide local video mixing functionality. Traffic from branch participants are mixed locally before it is sent across the WAN, thus significantly reduce the bandwidth usage on the enterprise WAN. ISR-G2 branch videoconference support both ad-hoc and meet-me conferences.

In ad-hoc conferences, a participant on a phone call initiates a videoconference by adding another participant. In an ad-hoc conference, the videoconference bridge supports up to a maximum of eight conferees.

In meet-me conferences, callers dial a designated number that has been designated as a Videoconference bridge. Callers on supported video phones are connected to the conference bridge as video conferees. In a meet-me conference, the videoconference bridge supports up to 16 conferees.

The videoconference bridge can operate in two modes.

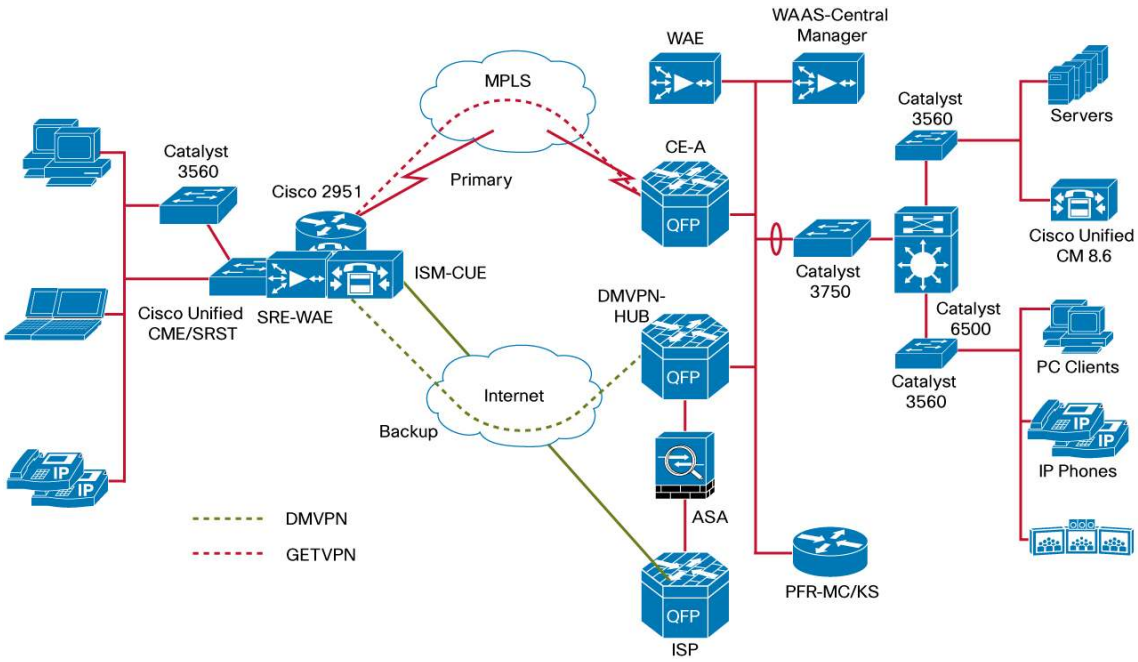
- **Homogenous mode:** This is when all the endpoints can have the same video format (same video codec, resolution, frame rate, etc.). This service requires all the video endpoints to have the same video capability.
- **Heterogeneous mode:** This format allows mixing endpoints with different video formats. This requires significant DSP resource and requires PVDM3-128.

Deploying Video in NGEW

In the current phase of NGEW, video support is implemented in standard and high-end branch. In both branch profiles, end-to-end QoS ensures video traffic is guaranteed sufficient bandwidth. Performance Routing (PfR) is configured to re-route video traffic if the primary path cannot provide the level of service required for video.

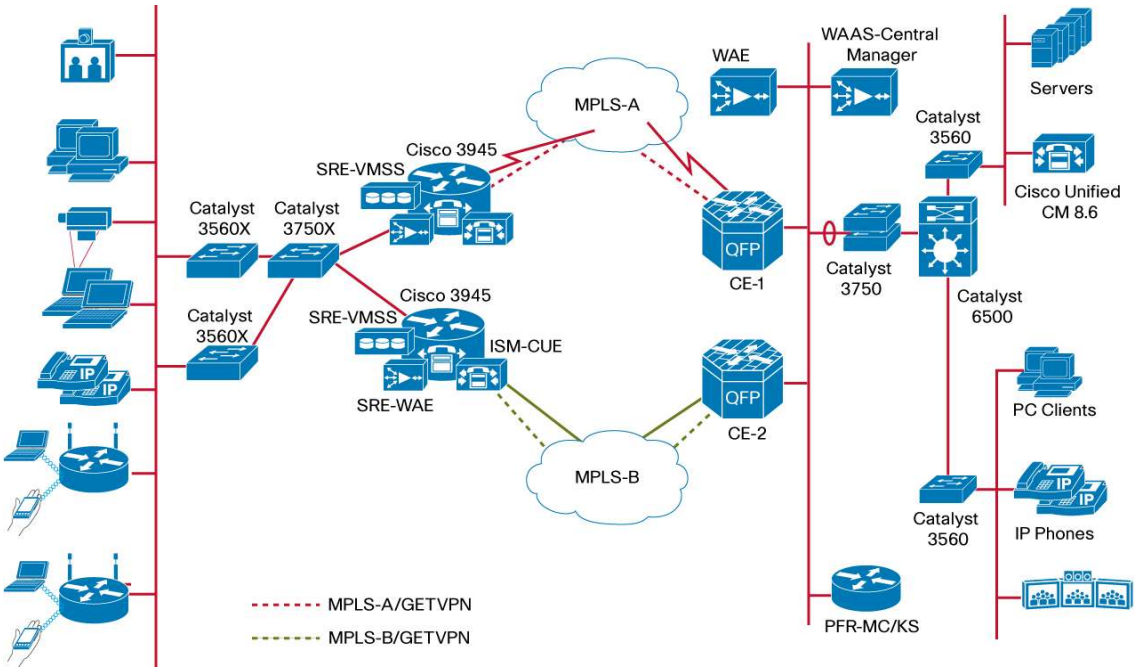
Video support in mobile and ultra high-end branch will be supported in future phase.

Figure 1. Standard Branch Design



In the standard branch design, a Cisco 2951 is deployed and equipped with 3 x PVDM3-256 for videoconferencing. Cisco Unified Call Manager Express is configured on the branch router with SIP trunk to the Cisco Unified Call Manager cluster in the Head Quarter.

Figure 2. High-end Branch Design



In the high-end branch design, additional redundancy and availability is achieved by deploying two 3945s configured with HSRP. Each 3945 is equipped with 4 x PVDM3-256 to support videoconferencing. DSP resources from both routers are added to Media Resource Group (MRG) in CUCM which allows DSP resources from both routers to be used simultaneously. Redundancy is provided by dual tier design of redundant routers and redundant WAN links. The High-end branch design utilizes the Cisco Unified Call Manager cluster at the head quarter for call control.

Video Implementation Overview

In the above two NGEW branch designs (standard and high-end), video traffic is monitored end-to-end. This is achieved by enabling Cisco Performance Monitor on the switches and WAN routers, which send performance statistics to 3rd party tool, ActionPacked! LiveAction. WAN routers are also configured with performance threshold for the syslog to be generated when the video quality degrades. This allows network administrator to monitor ongoing video deployment and be notified when the video performance degrades beyond acceptable value.

Once the problem is detected, network administrator can use Cisco mediatrace to collect performance metrics that impact video quality from all the devices along the media path. This allows network administrator to identify potential device(s) causing video quality degradation.

Branch video conferencing capability is enabled on ISR-G2 to locally mix video traffic from branch participants, which reduces WAN bandwidth usage during videoconference.

Implementation Steps

Cisco Performance Monitor

Enable Cisco Performance Monitor on the Router

Use the following procedures to enable Cisco Performance Monitor for video traffic.

Step 1. Configure flow exporter

Below defines a flow exporter named **vm_exporter1**, specifies the server (LiveAction) address and port, and optionally specifies the source interface from which the export data will be sent. Under destination and transport, specify the IP address of the LiveAction server address and port respectively.

```
flow exporter vm_exporter1
 destination 40.40.193.251
 source GigabitEthernet0/1.195
 transport udp 2055
```

Step 2. Configure flow monitor to tie the flow exporter and flow record together. There are already two default flow record, **default-rtp** and **default-tcp**. For simplicity, use default flow record.

```
flow monitor type performance-monitor vm_monitor1
 record default-rtp
 exporter vm_exporter1
```

Step 3. Configure class-map to specify the traffic to monitor

This is done using Cisco C3PL class-map which is configured the same way as QoS class-map. The traffic can be matched using ACL, DSCP, or NBAR. Example below uses ACL to specify the traffic to be monitored.

```
ip access-list extended rtp-udp-acl
 permit udp 40.40.0.0 0.0.255.255 40.40.0.0 0.0.255.255
!
class-map match-any video-class
 match access-group name rtp-udp-acl
```

Step 4. Specify the performance monitoring policy

Below creates a performance monitoring policy named **video-mon** and attach the class **video-class** created in previous step. There are a number of additional parameters that can be specified.

- Specify the **flow monitor** used for monitoring this traffic class. In this case, it is the flow monitor created in step 3, **vm_monitor1**.
- Specify the **monitor parameters**. Below shows the sampling period of 10 seconds and only keep the history of the last 5 samples.
- Specify the **monitor metric**. Two options are available, **rtp** or **ip-cbr**. Below shows that RTP traffic with payload type 96 @ 48 KHz and payload type 112 @ 90 KHz are monitored.
- Specify the **react** parameters. This allows setting threshold and action. Below will make the system generate syslog with the critical severity when average jitter of RTP stream exceeds 3000 microseconds.

```
policy-map type performance-monitor video-mon
 class video-class
   flow monitor vm_monitor1
   monitor parameters
    interval duration 30
    history 5
   monitor metric rtp
    clock-rate 96 48000
    clock-rate 112 90000
   react 525 rtp-jitter-average
    threshold value gt 3000
    alarm severity critical
    action syslog
```

Step 5. Apply the performance monitoring to the interface

It is recommended that, at the edge, the policy is applied to interface on the WAN.

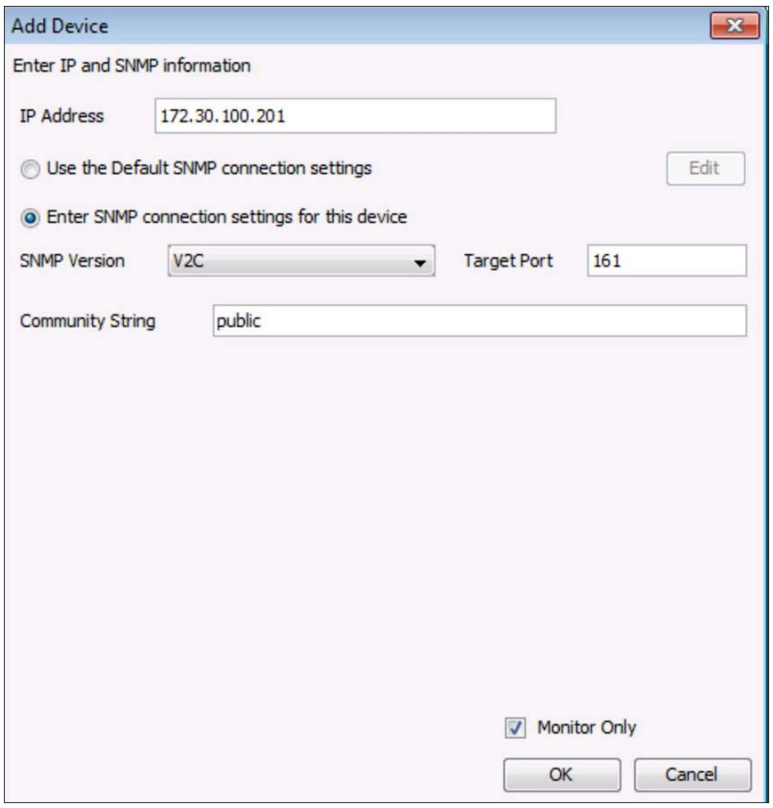
```
interface GigabitEthernet0/0.21
 description Ethernet WAN to MPLS
 service-policy type performance-monitor input video-mon
 service-policy type performance-monitor output video-mon
```

Add Device to LiveAction

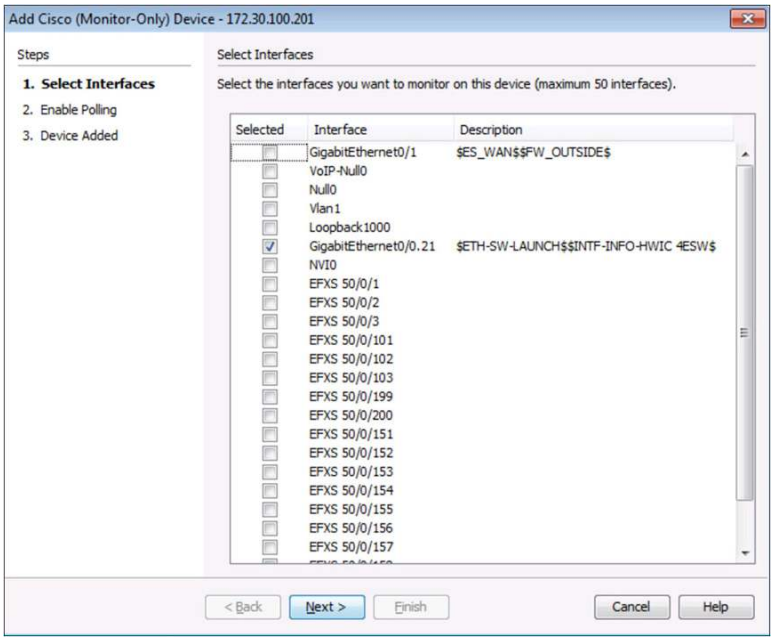
Step 1. Enable SNMP on the router. This is required for LiveAction to communicate with the router. Below example uses community string **public** for **read-only** privilege.

```
snmp-server community public RO
```

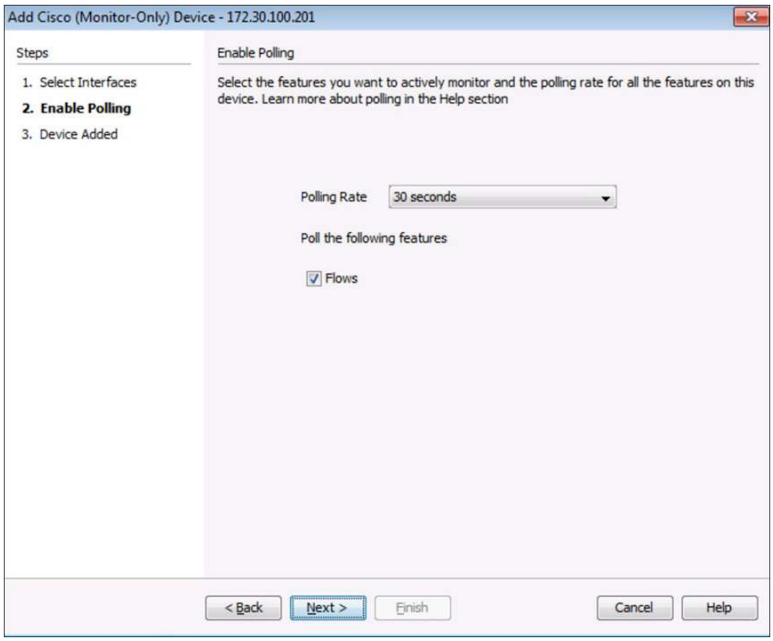
Step 2. From the LiveAction main menu, select **File->Add Device**. The IP address specified must match the source address specified in the flow exporter. Make sure the checkbox **Monitor Only** is checked.



Step 3. Specify the interface to which the Cisco Performance Monitor policy is applied.



Step 4. Define the polling rate and check that flows are monitored. Note that the polling rate should match the **interval** setting in the monitoring parameters.



Mediatrace

Manually Enabled Mediatrace through CLI

Mediatrace can be used to troubleshoot media issues. The first release of Cisco Collaboration Manager supports only Cisco TelePresence endpoints. Running mediatrace for traffic from other endpoints is still supported through CLI. Below steps show how to enable mediatrace through CLI.

There are 4 components that consist of a mediatrace session

- **Mediatrace profile:** specify the type of mediatrace (system or perf-monitor)
- **Path specifier:** specify the path (source and destination address) of the mediatrace session
- **Flow specifier:** specify the flow (source and destination address and port) of the media flow to run mediatrace on. This is necessary only if the mediatrace profile used is of the type perf-monitor
- **Mediatrace session parameters:** specify the other parameters of the mediatrace session, i.e. interval to run mediatrace, timeout, history size

Step 1. Enable mediatrace responder on all devices

For mediatrace to be effective mediatrace responder should be enable on as many devices as possible.

```
mediatrace responder
```

Step 2. Configure **mediatrace profile**. There are two types of mediatrace profiles, **system** or **perf-monitor**, each with different metric types. Below example creates one system and one perf-monitor profiles.

```
!
! Create the system mediatrace profile for cpu metric
!
mediatrace profile system cpu1
 metric-list cpu
!
! Create the perf-monitor mediatrace profile for rtp metric
!
mediatrace profile perf-monitor rtp1
 metric-list rtp
```

Step 3. Configure **path specifier** which specifies the source and the destination of the media.

```
mediatrace path-specifier path1 destination ip 172.30.102.6
 source ip 172.30.0.1
```

Step 4. Configure **flow specifier** which is required only for mediatrace profile **perf-monitor**. Specify the media flow on which to run the trace.

```
mediatrace flow-specifier flow1
 source-ip 172.30.0.1 source-port 5004
 dest-ip 172.30.102.6 dest-port 1901
```

Step 5. Specify the **mediatrace session parameters**. The mediatrace can be initiated on-demand or at regular interval.

Below is session parameter for **on-demand** mediatrace session

```
mediatrace session-params sp_on_demand
 response-timeout 10
 frequency on-demand
 history data-sets-kept 5
```

Below is session parameter for **scheduled** mediatrace session. The config below shows a scheduled mediatrace session at 60 seconds interval.

```
mediatrace session-params sp_scheduled
 response-timeout 10
 frequency 60
 history data-sets-kept 5
```

Step 6. Create a mediatrace session which ties all the above components together.

Below is the mediatrace session that collects the perf-monitor profile metrics. Note that the flow specifier needs to be specified for the **perf-monitor** mediatrace profile.

```
mediatrace 1
 path-specifier path1
 session-params sp_on_demand
 profile perf-monitor rtp1 flow-specifier flow1
```

Below is the mediatrace session that collects the system profile metrics. Since the system profile only requires the path information, the flow specifier is not needed.

Step 7. Initiate the mediatrace. If the mediatrace session is associated with the session parameters that has frequency set to **on-demand**, run the following command from exec mode.

```
mediatrace poll session 1
```

If the session parameters have the frequency set to a number, start the mediatrace from the configuration mode. Below configuration will run the mediatrace session for duration of 1 hour, at one minute interval.

```
mediatrace schedule 2 lifetime 3600
mediatrace schedule 2 start-time now
```

Automatically Run Mediatrace using Cisco Collaboration Manager

The following steps are for enabling all the devices to be managed by Cisco Collaboration Manager, which can trigger on-demand mediatrace for Cisco TelePresenceTelePresence endpoints.

Step 1. Enable SNMP on the router. Note the RW community string needs to be specified as well as the RO community string. Below example uses community **private** and **public** for **read-write** and **read-only** privilege respectively.

```
snmp-server community private RW
snmp-server community public RO
```

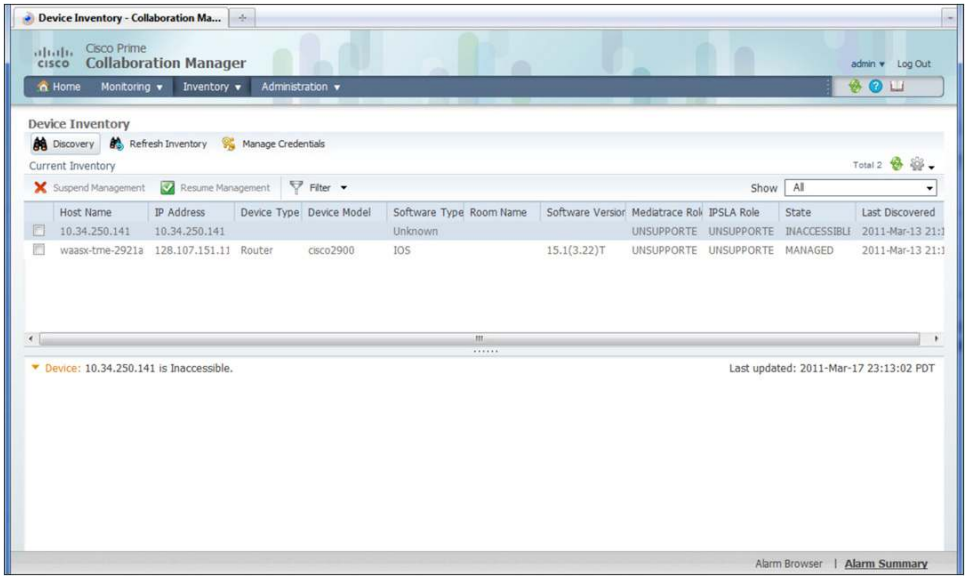
Step 2. Enable mediatrace and HTTP server to which the Cisco Collaboration Manager uses to communicate.

```
mediatrace responder
!
! Optionally specify the source of mediatrace
mediatrace initiator source-ip 10.5.10.1
!
username <cisco> privilege 15 secret <enable_password>
!
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
```

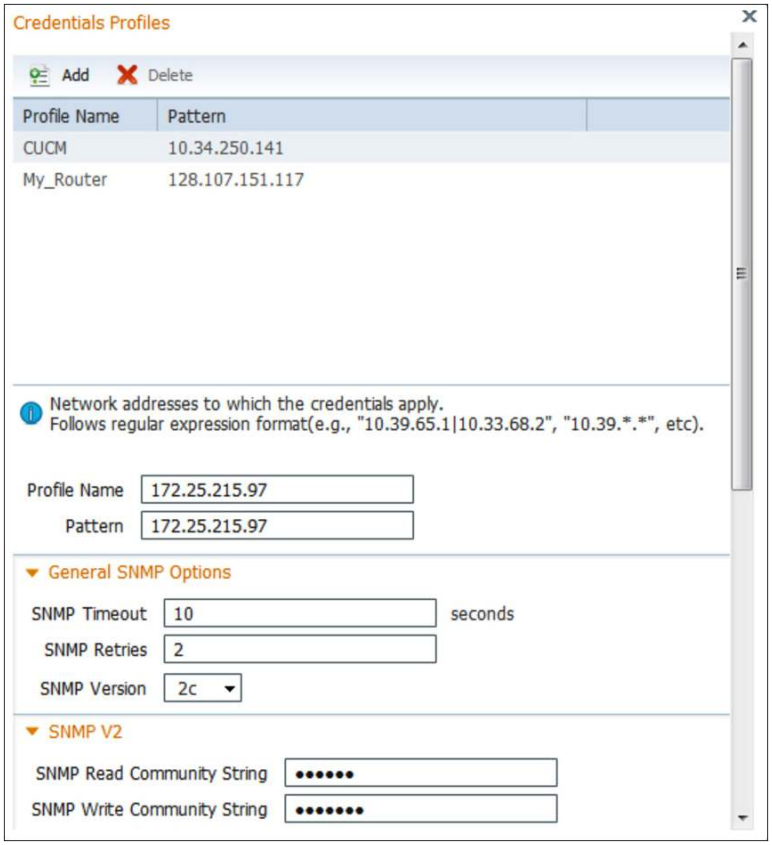
Step 3. Enable IOS WSMA agent. Below indicates that HTTP is used as transport protocol.

```
wsma agent exec profile wsma_listener_http
wsma agent config profile wsma_listener_http
!
wsma profile listener wsma_listener_http
 transport http
```

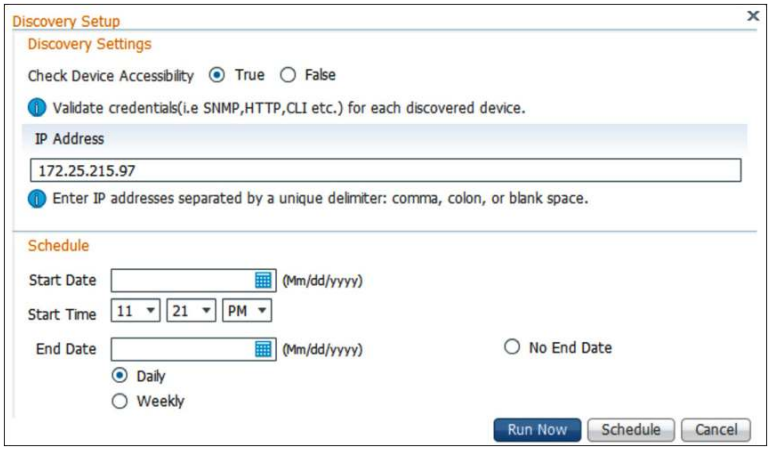
Step 4. Login to the Collaboration Manager. Note that Cisco Collaboration Manager does not support Microsoft Internet Explorer. Use Mozilla Firefox to run Cisco Collaboration Manager. From the main menu, select **Inventory -> Device Inventory**. Click on **Manage Credentials** button.



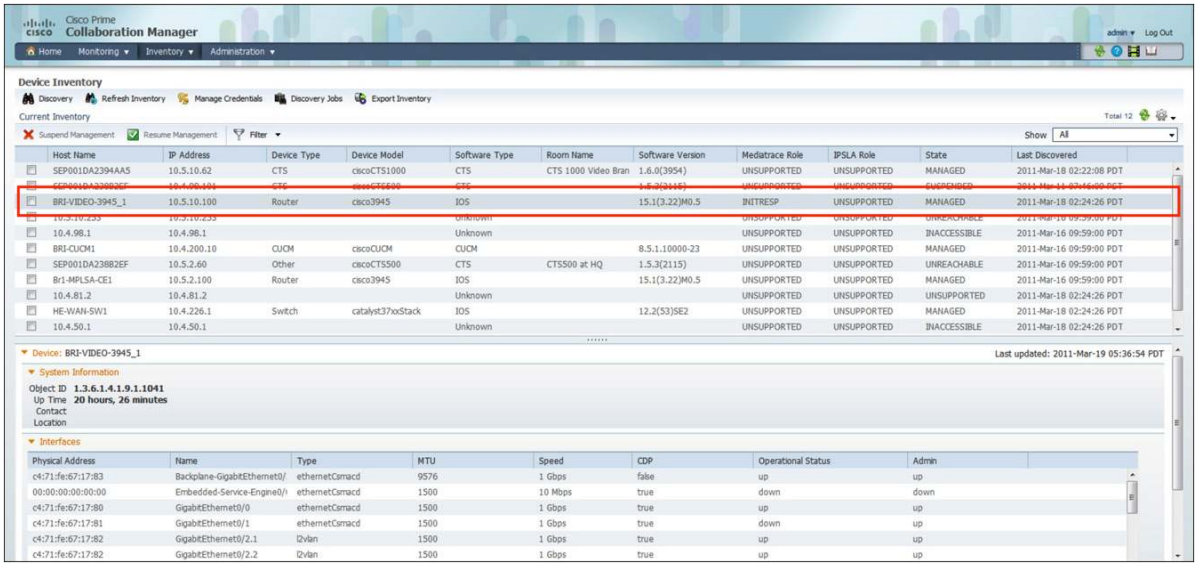
Step 5. Provide the login information under CLI and HTTP sections, and the matching SNMP community string.



Step 6. Specify the IP address that match the pattern provided in the previous step. Click **Run Now**.



Step 7. Below show the inventory table after discovery. Added router device state should show **MANAGED**. This device is now managed by Cisco Collaboration Manager.



Branch Videoconferencing Bridge

In standard branch, CUCME which is deployed at the branch router also controls videoconferencing resources. CUCME has SIP trunk to CUCM cluster at the HQ. In high-end branch, centralized CUCM controls videoconferencing resources at the branch.

Create Videoconference Bridge on the Branch Router

This step is the same for both standard and high-end branches.

Step 1. First, create the conference bridge resource on the branch router. The dsp-reservation is optional. Below configuration reserves 50% of DSP resource for audio conference, hence only 50% is left for videoconference.

```
voice-card 0
 ! Reserve 50% of DSP resource for voice conference
 voice-service dsp-reservation 50
 dsp services dspfarm
```

Step 2. Create the DSP farm profile for videoconferencing. Note the profile number 50 is created for homogenous conference. This means all the endpoints participating in the videoconferencing need to support the same video codec. This example below assumes that all endpoints can support H.264 CIF @ 15 fps.

```
dspfarm profile 50 conference video homogeneous
 codec g711ulaw
 codec g729abr8
 codec g729r8
 codec g729br8
 codec h264 cif frame-rate 15 bitrate 320kbps
 maximum sessions 2
 associate application SCCP
```

Step 3. Specify the local interface used for SCCP, and specify the CUCM address and version. Then, enable SCCP application on the branch router.

```
sccp local GigabitEthernet0/2.2
sccp ccm <CUCM or CUCME address> identifier 3 version 7.0
sccp
```

Step 4. Create the SCCP group and associate the CCM identifier created in step 3. The videoconference bridge will register with CUCM using the name specified below, VCB0471FE671782.

```
sccp ccm group 3
associate ccm 3 priority 1
! The name has to match what is configured in CUCM
associate profile 50 register VCB0471FE671782
```

Standard Branch Videoconference

The design for standard branch requires CUCME (Cisco Unified Call Manager Express) deployed at the branch, with SIP trunk to the CUCM (Cisco Unified Call Manager) cluster at the head quarter. The configuration of SIP trunk is not in the scope of this document.

Add Videoconference Bridge Resource to CUCME

Step 1. Enable the conference hardware in the CUCME.

```
telephony-service
 sdspfarm units 10
 ! Enable hardware based conference
 conference hardware
 max-conferences 4
```

Step 2. Create an ephone-dn and specify as meet-me or ad-hoc conference.

```
ephone-dn 57 octo-line
number 9AAA
conference ad-hoc video
!
ephone-dn 56 octo-line
number 9445
! Unlocked meetme number
conference meetme unlocked video
```

Step 3. Check the conference resource status by **show ephone-dn conference.**

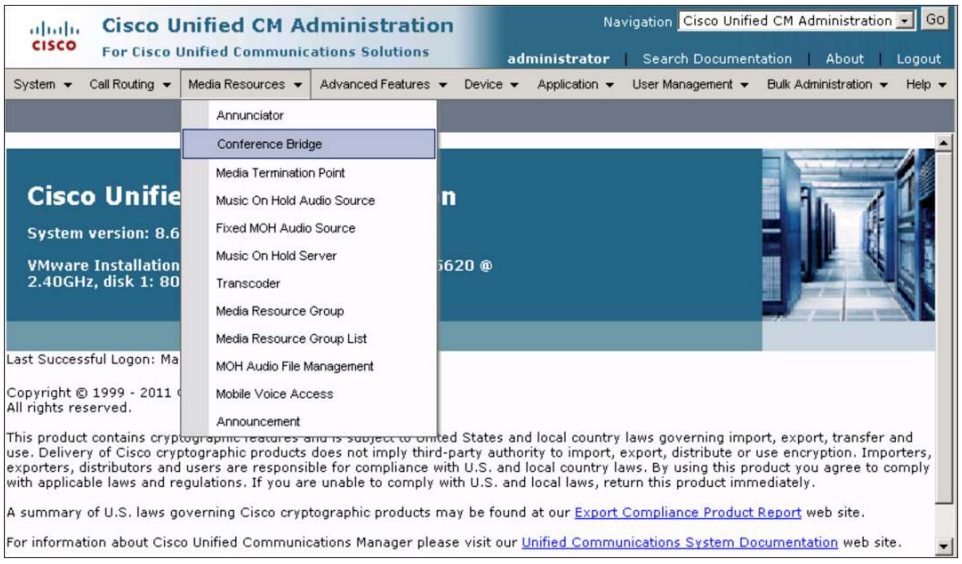
```
show ephone-dn conference
type         active inactive  numbers
=======================================
Ad-hoc Video    3       37     8001
DN tags: 151, 152, 153, 154, 155

Ad-hoc Video    0       40     8002
DN tags: 156, 157, 158, 159, 160

Meetme Video    0       16     9999
DN tags: 199, 200
All DN tags unlocked.
```

High-end Branch Videoconference

The design for high-end branch requires centralized CUCM controlling conference resources at the branch routers.

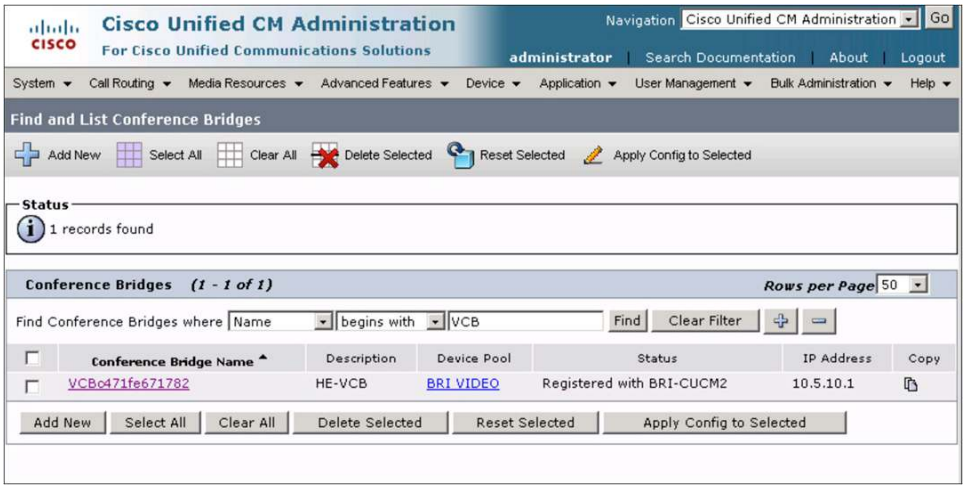
Add Videoconference Bridge Resource to CUCM

Step 1. Logon to the CUCM administration. From the main menu, select **Media Resources > Conference Bridge**.



Step 2. In page **Find and List Conference Bridges**, click **Add New**, which will bring you the next page where you can enter the conference bridge information. The Conference Bridge Name has to match what is configured in the SCCP group in the conference bridge. Below example has conference bridge name, **VCB0471FE671782**.

Step 3. The conference bridge status should show as **Registered**. The CUCM is ready to utilize the videoconference bridge resource.



Monitor the Videoconferencing Session

To monitor the current videoconference session, use **show telephone-service conference hardware detail video**. Below shows that an ad-hoc conference initiated by caller with DN 1003 is in progress, and there are 3 participants in the conference.

```
show telephony-service conference hardware detail video
Conference   Type             Active  Max  Peak    Master         MasterPhone
Last
                                                                  cur(initial)
================================================================================
============
8001         Ad-hoc Video          3     4     3    1003 phone3    6     (  6)
1002 phone2
```

```
  Conference parties (number:phone)
      1002 phone2 :5  (admin):Video
      1001 phone1 :4  (admin):Video
      1003 phone3 :6  (admin):Video
```

Product List

Role	Hardware/Software	Software Version
Standard Branch	Cisco 2951	15.1(4)M
	PVDM3-256	
High-end Branch	Cisco 3945	15.1(4)M
	PVDM3-256	
Headend Router	Cisco ASR1006	RLS 3.3
Cisco Performance Monitor Reporting	ActionPacked! LiveAction	2.0
Cisco Mediatrace Management Software	Cisco Collaboration Manager	1.0
Call Control	CUCM	8.6
	CUCME (embedded in IOS)	8.6

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-685567-00 10/11