

*TOMORROW starts here.*



Cisco *live!*

# Utilising Network Intelligence for Collaboration and Real Time Media

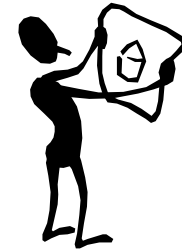
BRKUCC-2058

Aamer Akhter

Distinguished Engineer

# Agenda

- What is Medianet?
- Application Traffic Patterns and Demands
- Media Monitoring
- Media Awareness
- Summary



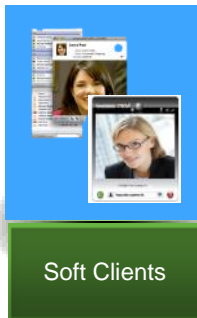
# What is Video Collaboration?

WebEx



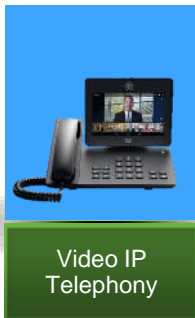
Web Conferencing

Jabber



Soft Clients

DX650  
CP-99xx  
CP-89xx



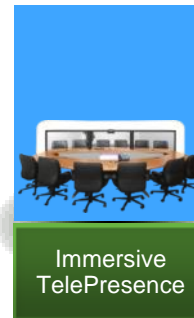
Video IP Telephony

EX90  
SX20  
TC Endpoints



Desktop/ Room Video Conferencing

1xxx,3xxx Series  
TX Series



Immersive TelePresence

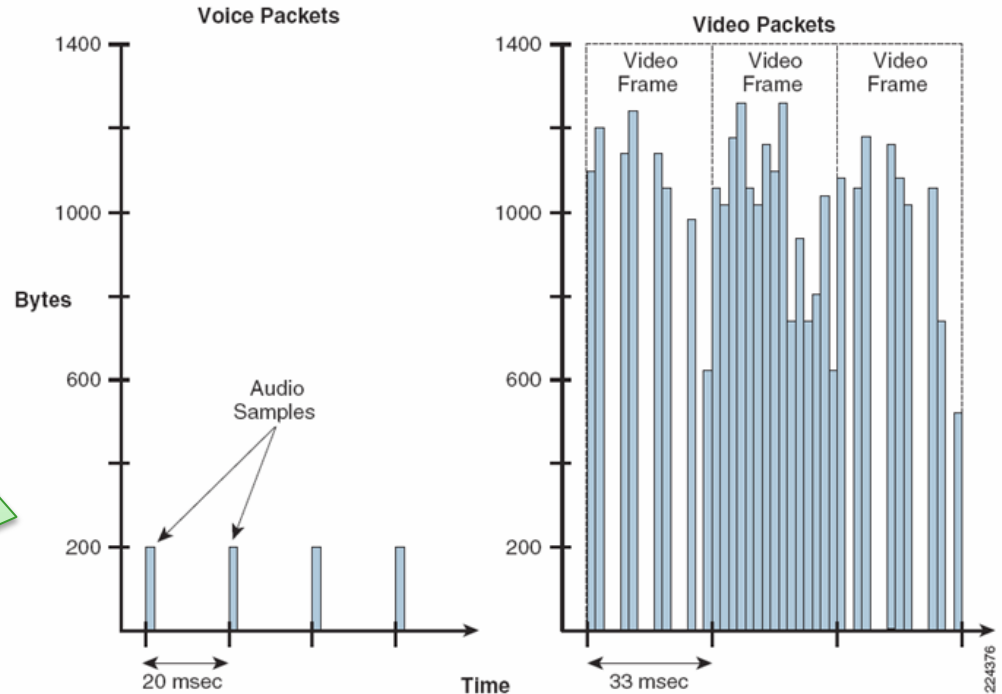


## Collaborative Rich Media Traffic Patterns

# But Video is Not Voice

- Traffic profile is very different
- Variable Bit Rate
- More data on the wire

**32 to 209  
times  
the  
bandwidth**



# Video Application Bandwidth

Video requirements continue to grow

## WebEx

- VoIP: 30-40 kbps, Desktop Share: 40 kbps, Video: 220 Kbps<sup>1</sup>
- HQ Video (360p 1.5Mbps, 180p 0.5 Mbps) Min 300k

## Video IP Telephony

- E20 128 kbps – 1152 kbps
- CP-99xx 256 kbps – 1024 kbps

## Soft Clients

- CUVA 460 kbps
- MOVI 384 kbps – 2 Mbps

## Desktop Video Conferencing

- 384 kbps – 6 Mbps

## TelePresence

- 1.5 Mbps – 24+ Mbps

# Network Requirements of Video Collaboration Apps

|                       | One Way Latency | Jitter   | Loss    |
|-----------------------|-----------------|----------|---------|
| Desktop Share (WebEx) | < 1000 ms       | < 100 ms | < 0.05% |
| Video Conferencing    | < 150 ms        | < 30 ms  | < 0.10% |
| TelePresence          | < 150 ms        | < 10 ms  | < 0.05% |
| IP Telephony          | < 150 ms        | < 30 ms  | < 0.10% |
| VC Soft Clients       | < 150 ms        | < 30 ms  | < 0.10% |

## Media Synchronisation

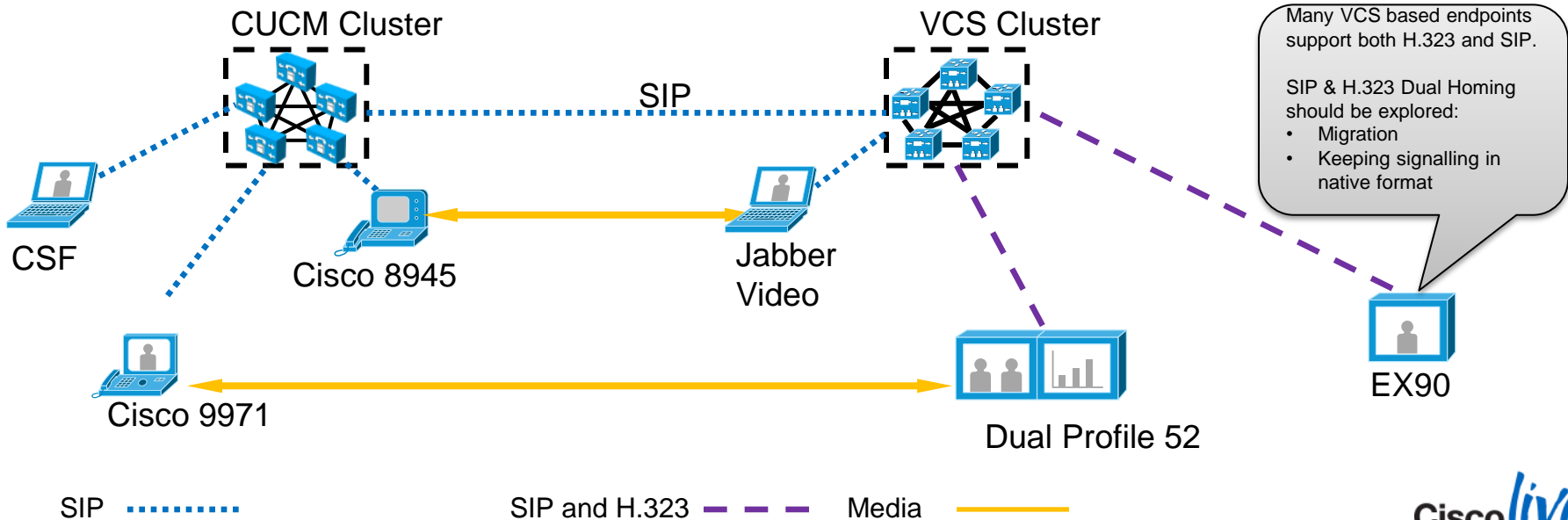
|  |           |
|--|-----------|
| audio + discrete info (slide show):    | < 1000 ms |
| audio + pointed objects w/ narration:  | < 200 ms  |
| Lip Sync: audio advance over video:    | < 30 ms   |
| Lip Sync: audio delay following video: | < 100 ms  |



# Point to Point Video Conferencing

Intra-Company, SIP to SIP

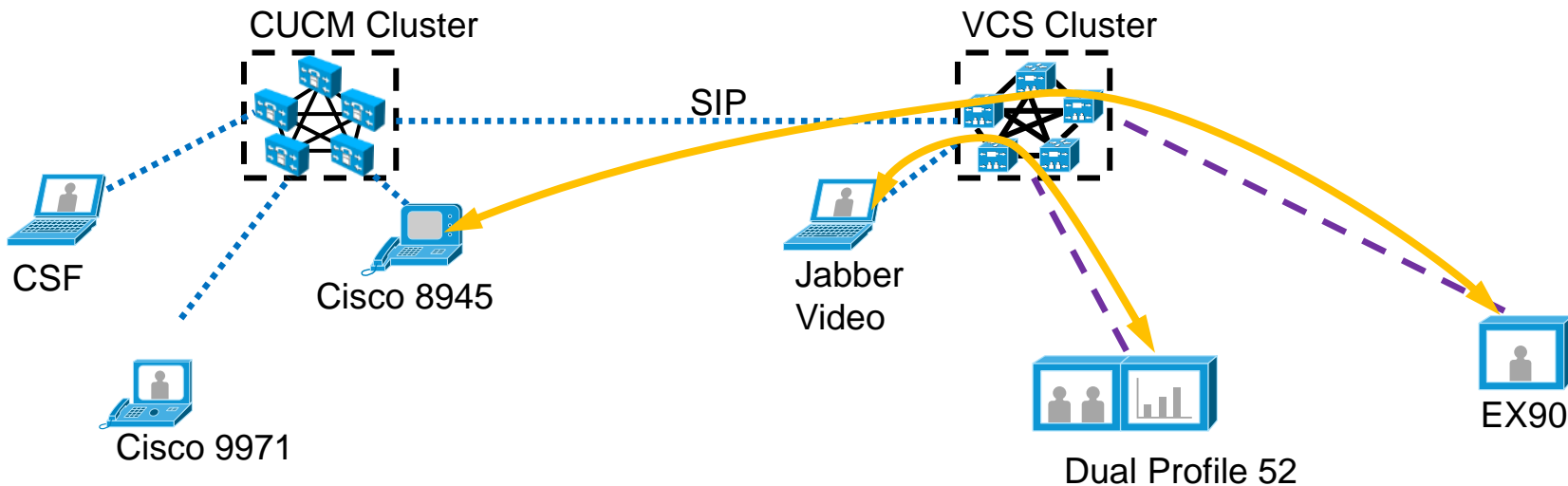
- **Call Signalling** may traverse multiple servers
  - No Signalling Protocol Interworking Required
- **Media Flows** Directly between Terminating Endpoints



# Point to Point Video Conferencing

Intra-Company, SIP/H.323 interworking

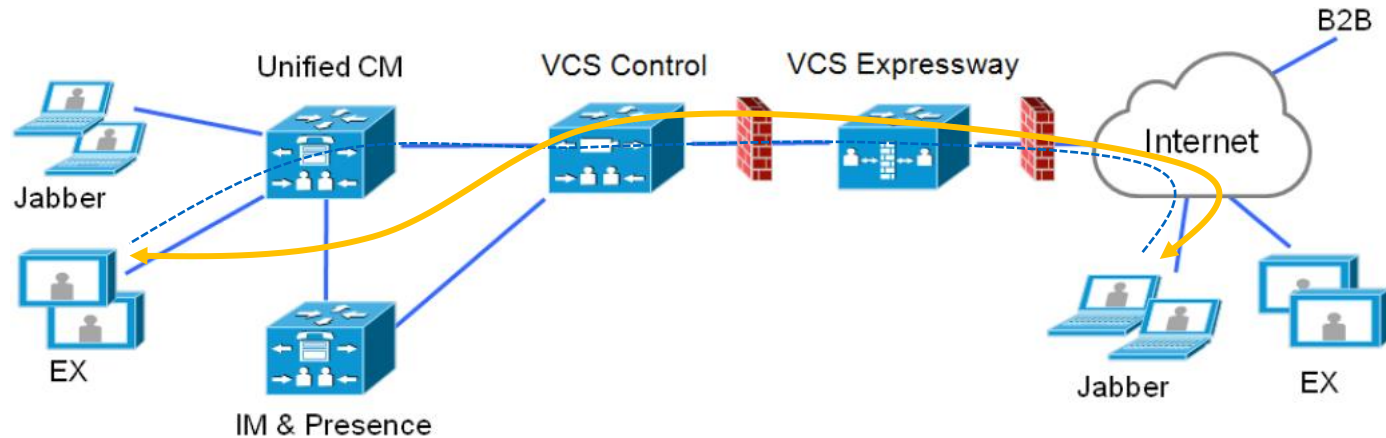
- **Call Signalling** may traverse multiple servers
- **Media Flows through the VCS** (which performs media translation)
  - Because of media anchoring, geographical location of the VCS is Important



SIP ..... H.323 ..... SIP and H.323 - - - Media ———

# Expressway Based Remote Access

- **Call Signalling** will traverse multiple servers as signalling crosses from outside to inside the enterprise and to the CUCM
- **Media Flows through the Expressway and VCS towards media end systems**
  - Because of media anchoring, geographical location of the VCS is Important

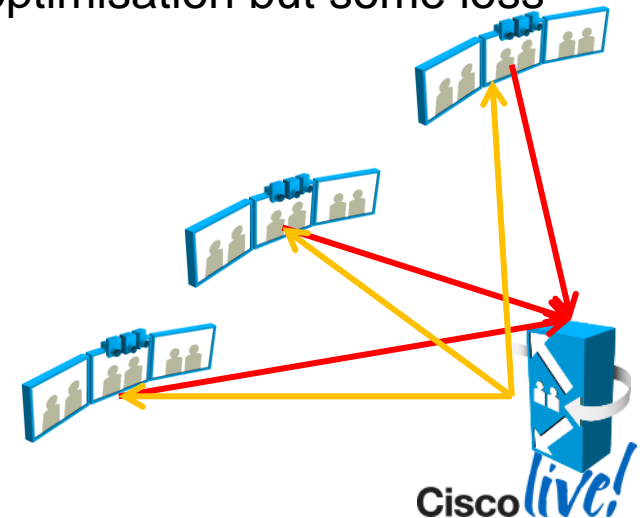


SIP ..... H.323 ..... SIP and H.323 - - - Media ———

# Multipoint Video Conferencing

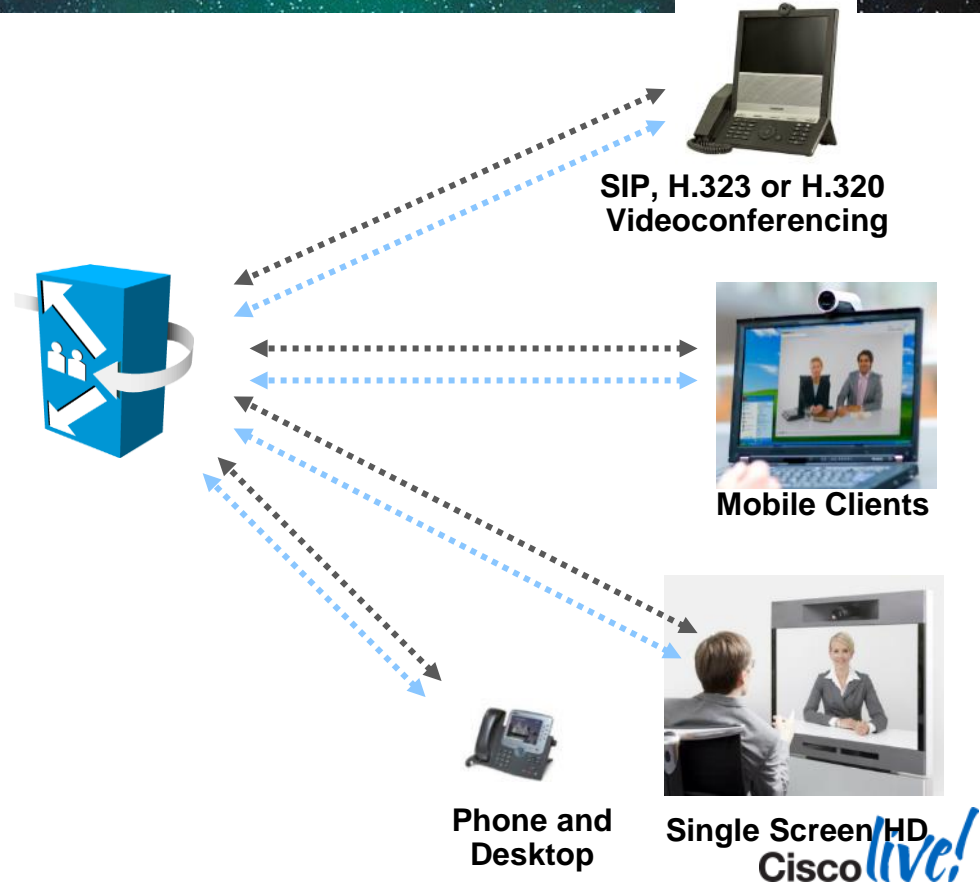
- Multiple solutions to enable multipoint conferencing.
- Participants send their audio/video stream to centralised device (MCU/CTMS)
- Device selects, possibly re-encodes, and retransmits audio/video to participants
- Cascading a possibility for some MCUs (better BW optimisation but some loss of functionality)

| Device                                      | Usage                                     |
|---|---|
| Cisco TelePresence Multipoint Switch (CTMS) | Immersive Cisco TelePresence multi-party  |
| TelePresence Server                         | Active-Presence & Transcoded TelePresence |
| Virtual TelePresence Server                 | Virtualised TelePresence Server           |
| TelePresence MCU                            | Multipoint Transcoded Video Conferencing  |
| Multi-site on certain endpoints             | Adhoc multipoint conferencing             |



# Traditional Video Conferencing MCU

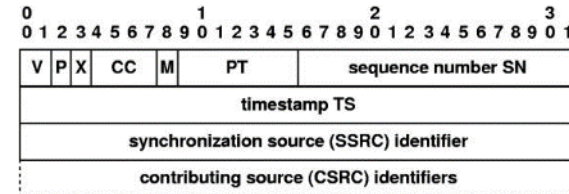
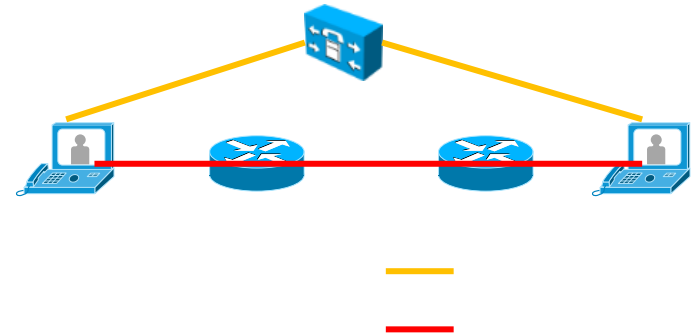
- Endpoints send audio and video towards central MCU
- MCU
  - Receives, blends/selects media and transmits
    - Mixes audio
    - Transcodes video to match receiving endpoint capabilities
  - Performs interop between devices
  - May operate in screen switching or composite modes
- MCUs are placed at:
  - High WAN bandwidth connected sites
  - Balancing end to end latency



# Traffic Details

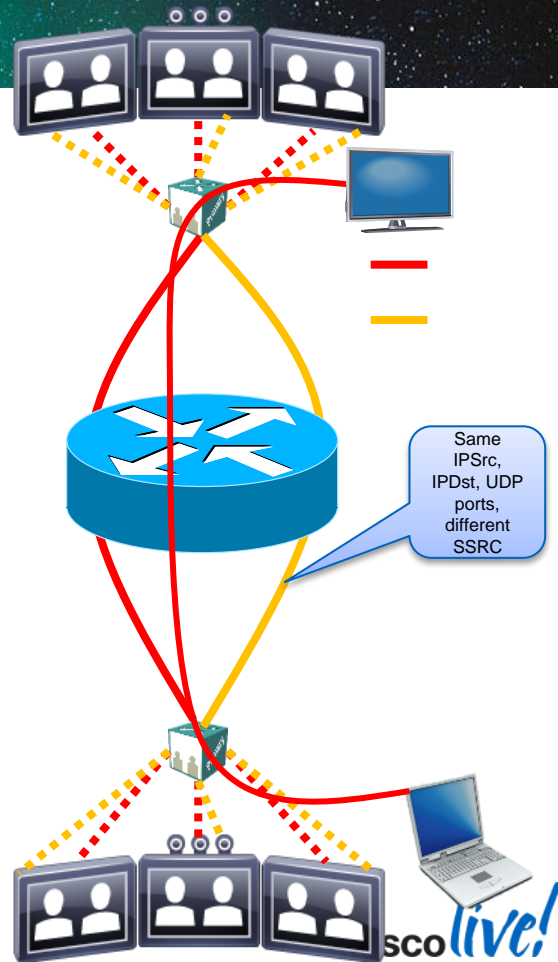
## IP Telephony and Video Conferencing

- IP Telephony and video conferencing almost always use RTP
  - RTP (RFC3550) over UDP
- RTP header provides
  - Sequencing
  - Timestamp
  - Payload types
  - Multiplexing of different media
- RTCP (RTP UDP port + 1) provides
  - Reporting
  - Control channel



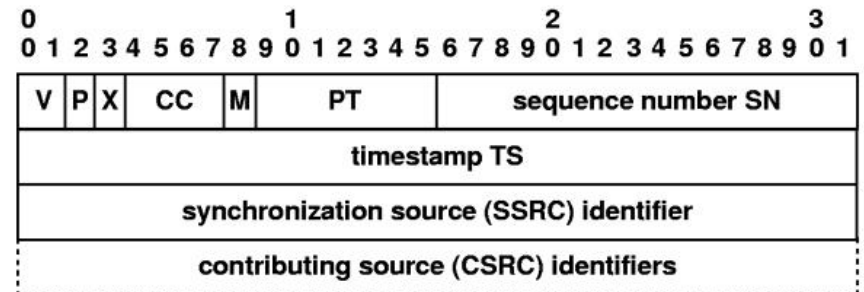
# RTP and Media Types

- Each media stream (audio, video, desktop share, etc.) is a unique SSRC
- Implementation specific: multiple SSRCs of same media type might be multiplexed together (same IPsrc, IPdst, UDP protocols)
- CTS:
  - 1 Audio UDP flow (multiple audio channels)
  - 1 Video UDP Flow (multiple channels)



# RTP Payload Types

- RTP Payload Type (PT) field designates type of media
- Divided into static (mostly legacy audio) and dynamic.
  - <http://www.iana.org/assignments/rtp-parameters>
- Dynamic range (96-127) PT communicated via signalling (SIP, H.323)
  - Identifying video can become a challenge.

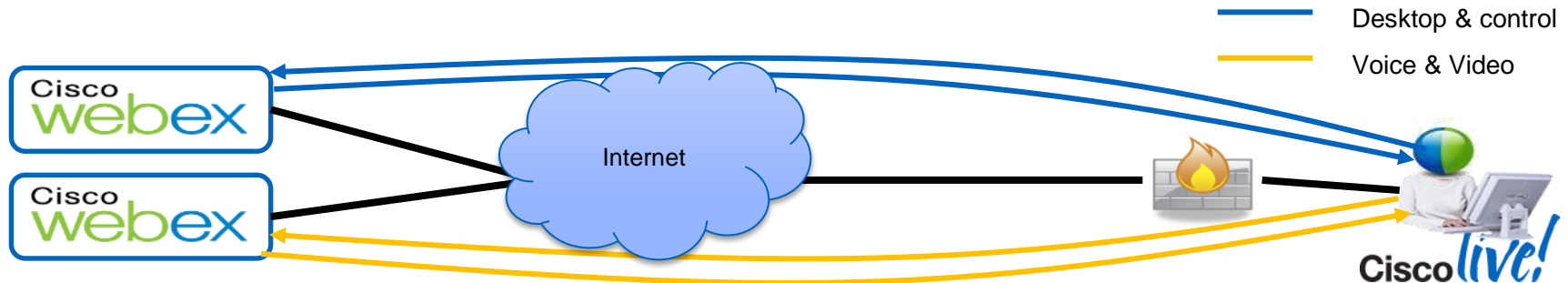




# WebEx Traffic Details

## Traditional WebEx Meeting Centre

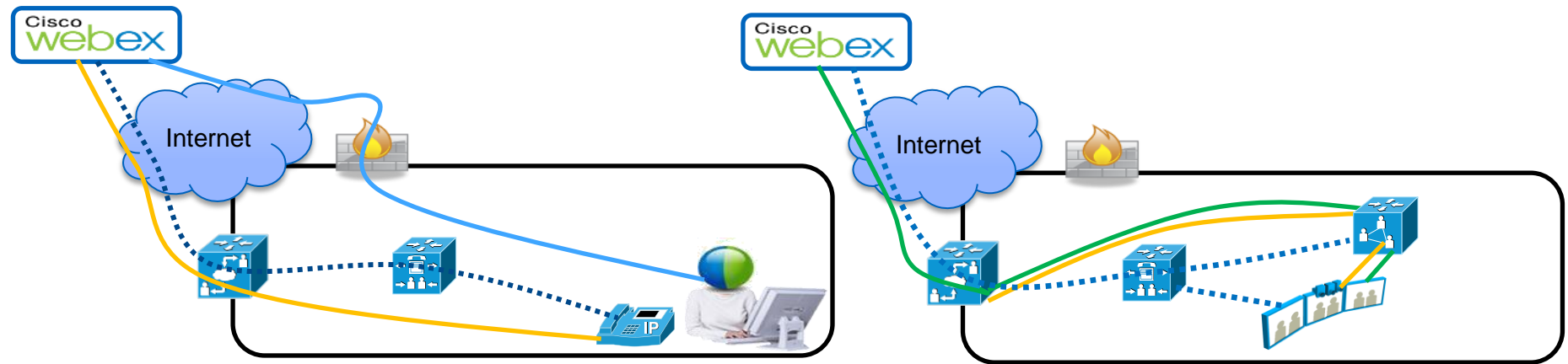
- Total of five flows Five flows used in WebEx meeting centre
  - Data flow (Application/Desktop Share, File Share, Presentation Share, etc.)
  - Control Flow (Backend signalling)
  - Video flow (Live Web Cam video), can be UDP or HTTPS
  - Audio flow (VoIP Audio), can be UDP or HTTPS
  - Streaming flow (Streaming Video), can be UDP or HTTPS
- Audio is commonly handled via PSTN vs. integrated with client
- UDP Video is an option but uncommon (firewall traversal issues) but bandwidth wise, most efficient



# WebEx Meeting Centre

## Cloud Connected Audio (CCA) and WebEx One Touch

- Cloud Connected Audio allows for native IP integration with enterprise VoIP system vs. PSTN traversal.
- SIP trunk between WebEx DC and Enterprise for carrying VoIP
- WebEx with TelePresence provides integration between Enterprise Video Conferencing and WebEx participants
- SIP trunk between WebEx DC and Enterprise for carrying voice & video.



SIP ..... RTP Voice — RTP Video — Desktop —

BRKUC-2058

© 2014 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Cisco *live!*

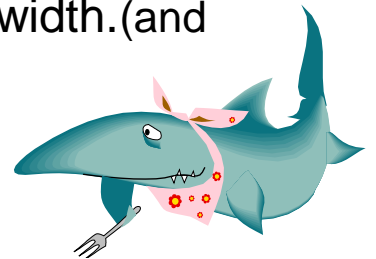
# Video Requests Come From All Over



# What Does Video Mean to You?



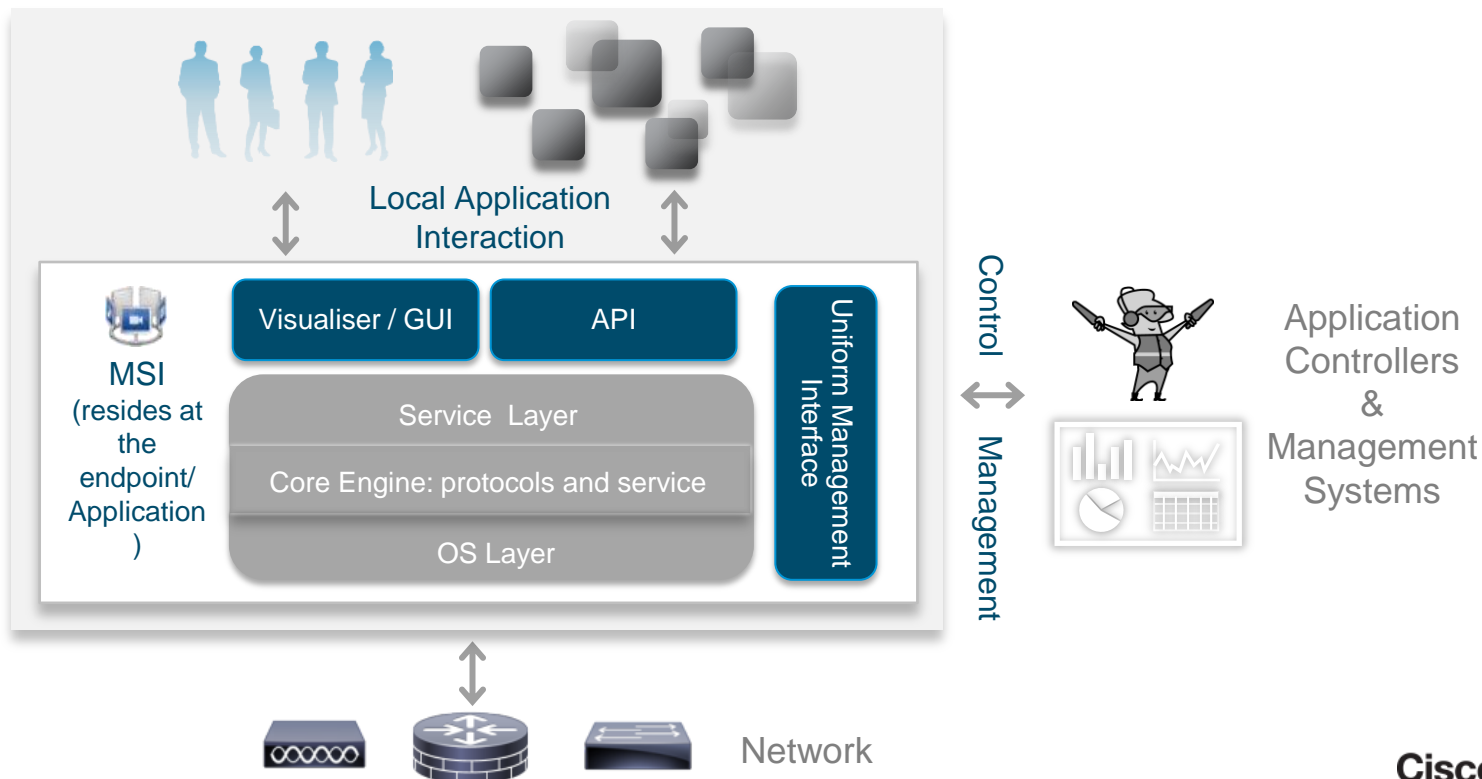
- New SLAs from application groups regarding rich media applications.
  - SPs: Medianet is tooling the enterprise to validate these SLAs!
- Video is bandwidth hungry  
Need tools, features to understand and manage this bandwidth.(and maybe more bandwidth)
- Video is sensitive to network conditions.  
Greater pressure to detect and resolve problems quickly.



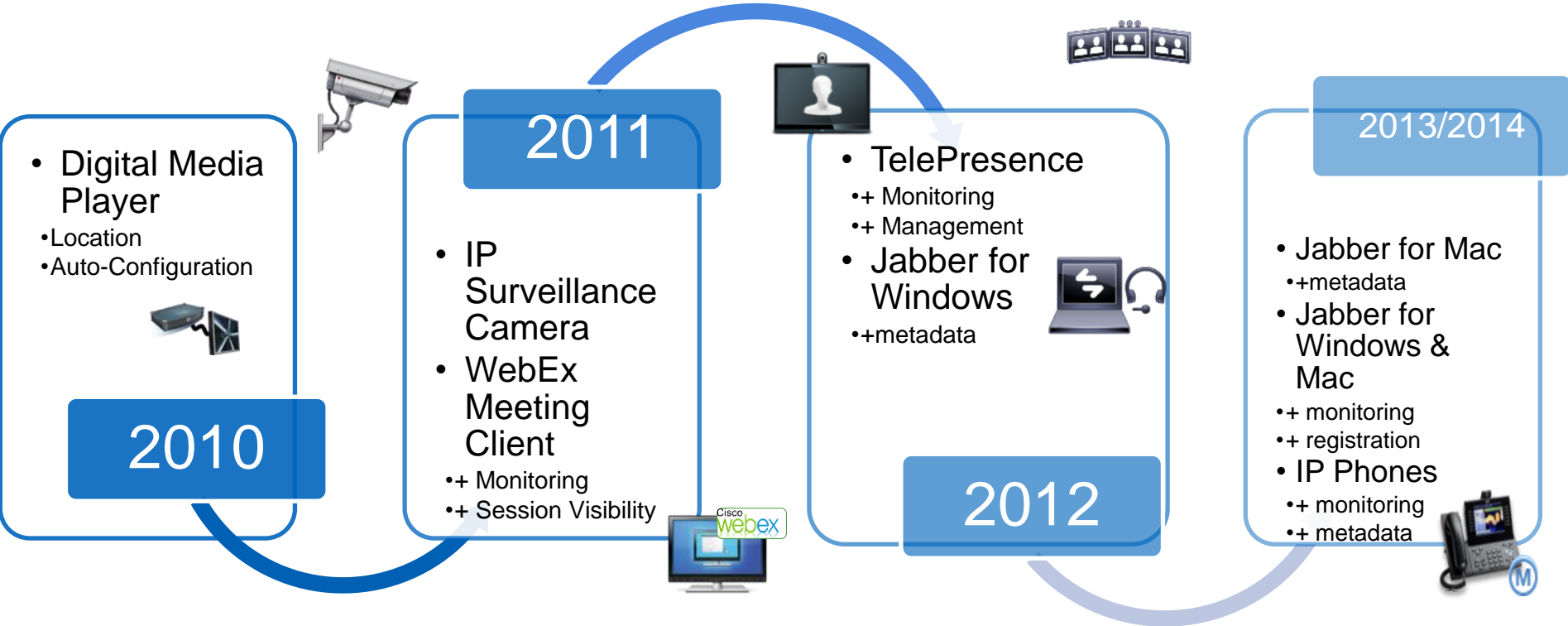
Cisco *live!*

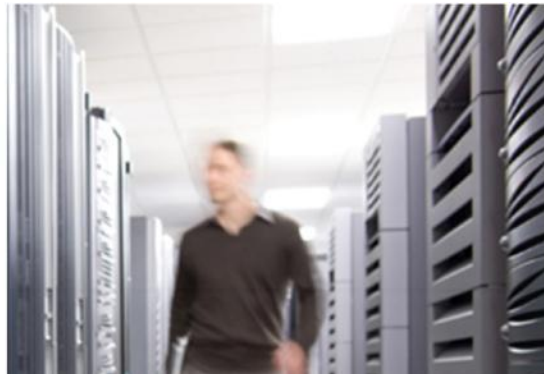
# Media Services Interface (MSI)

Cross-Platform SDK for integrating Applications with the network & Management Systems



# MSI on Endpoints



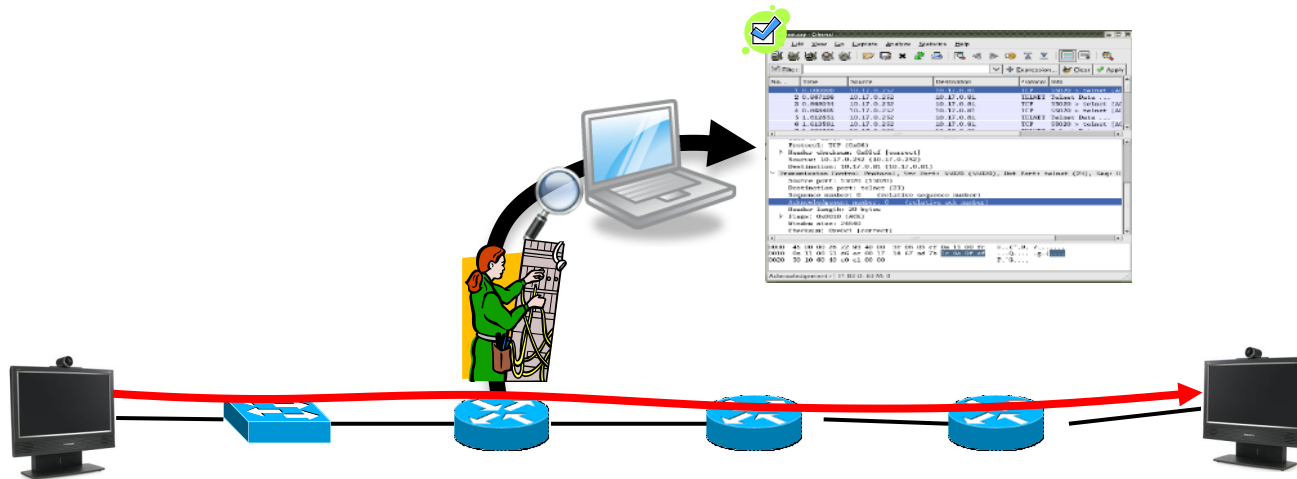


# Media Monitoring

# Dedicated Protocol Analysers



- Wireshark and other protocol analysers are great
  - Detailed analysis for variety of protocols at deep level
- Dedicated probes are expensive to deploy pervasively
  - Operator has to make difficult judgment calls on where the problem is going to be– before it happens
- Can be challenging after the fact- need on-site trained personnel.



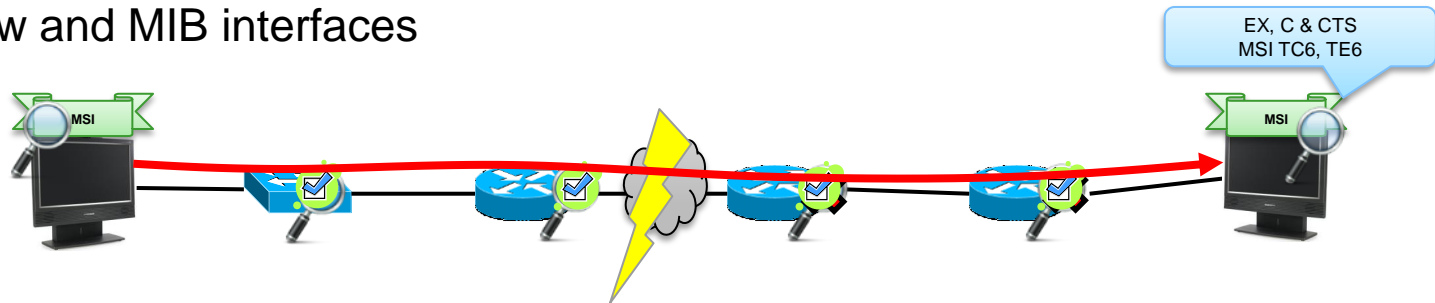


# Network Performance Monitor

Router/Switch native RTP and TCP analysis

Nov 2010  
15.1(3)T

- Network nodes are able to discover & validate **RTP, TCP** and **IP-CBR** traffic on hop by hop basis
- **À la carte metric (loss, latency, jitter etc.) selections**, applied on operator selected sets of traffic
- Allows for **fault isolation** and network span validation
- Cross-network synchronised time windows for measurement
  - same 30 second (default) intervals measured
- Per-application threshold and altering.
- NetFlow and MIB interfaces



# Perf-mon: Wide Applicability



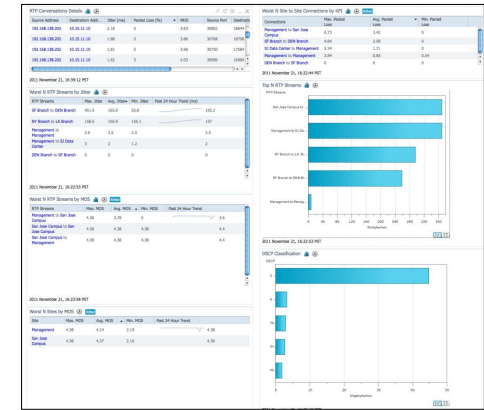
- Tested with:
  - Cisco EX90, MXP1700, Cisco TelePresence (1xxx, 3xxx), CUVA, CP-9971, CP-7985, CP-7960 (audio only), MS Lync, Avaya, Polycom
  - Cisco Video Surveillance Cameras, WebEx (HTTPS), IPTV (VLC)
  - Just plain web transactions (wget)



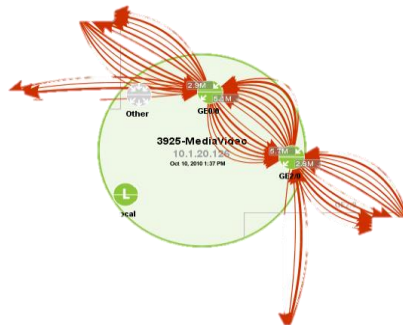
# Performance Monitor Management

More info: CDN Partners Page:  
<http://developer.cisco.com/web/mnests/partners>

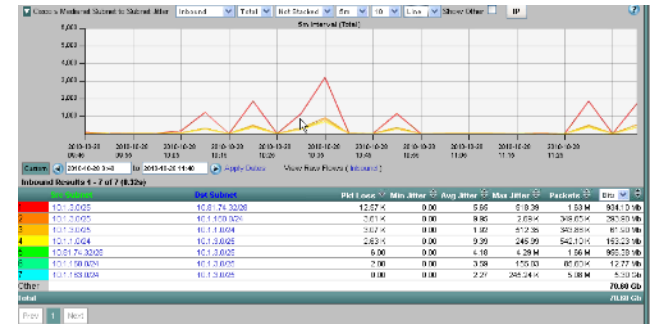
| Application  | Type        | Network, Endpoint/MSI |
|--|-------------|-----------------------|
| Cisco <b>Prime Infrastructure</b> w/Assurance License (includes configuration) | Network     | N                     |
| Cisco <b>Prime Collaboration Assurance</b>                                     | Application | N,E                   |
| ActionPacked <b>LiveAction</b> (configuration also planned)                    | Network     | N,E                   |
| Plixer <b>Scrutinizer</b>  | Network     | N                     |
| SevOne <b>SevOneNMS</b>  | Network     | N                     |
| CA/NetQoS <b>UCM</b>   | Application | N                     |
| ManageEngine <b>NetFlow Analyzer</b>   | Network     | N                     |
| Sonoco <b>ICMyNet</b>  | Network     | N                     |
| <b>14+ NMS application vendors engaged!</b>                                    |             |                       |



Cisco Prime Infra



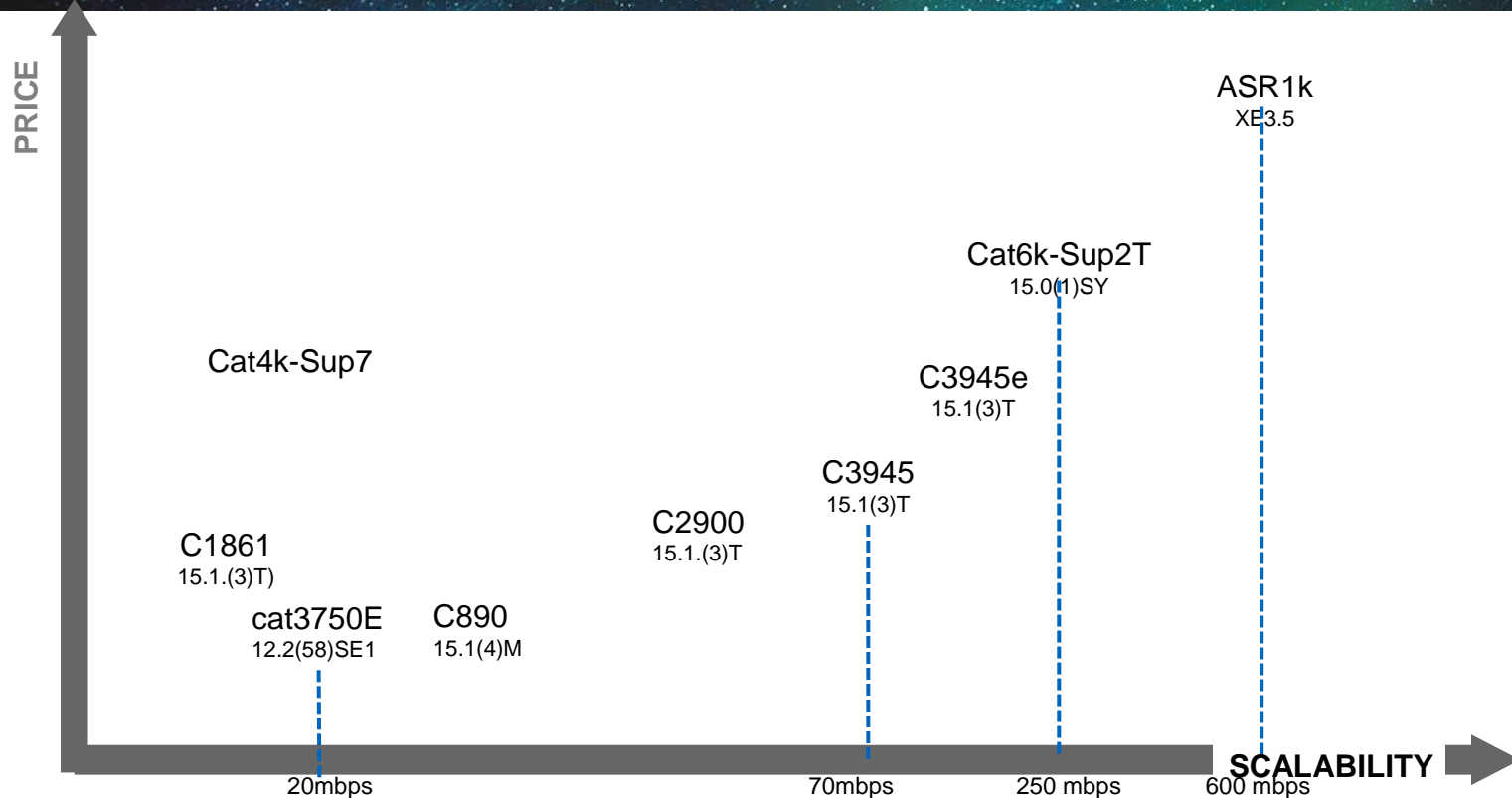
ActionPacked



Plixer  
Cisco Public

# Platform Wide Scalability

## Performance Monitor

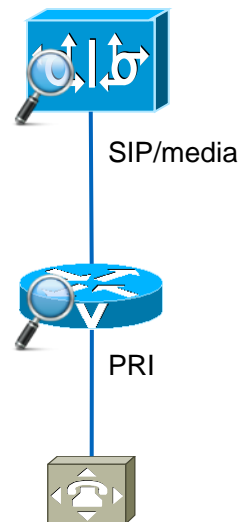


# Audio Quality Metrics (AQM) on CUBE

- AQM provides deeper insight into the media flows that are processed by the CUBE / Voice gateways

ISRG2, c8xx 15.3(3)M  
ASR1k (coming soon)

- Available via MIB, CDR and performance monitor



# Example Configuration

## AQM performance monitor

- 'media monitoring' configuration under 'voice service voip' or dial-peer
  - Controls generation of metrics on CUBE/VG
- To export via NetFlow, regular performance monitor configuration – just include the AQM fields
- MIB  
CISCO-VOICE-DIAL-CONTROL-MIB

```
voice service voip
  media monitoring [num] persist
! num is number of channels used to monitor
  media statistics
! delay calc, MOS etc
```

OR

```
dial-peer voice [tag] voip
  media monitoring
```

```
!
flow record type performance-monitor aqm
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect application voice number called
collect application voice number calling
...
```

Regular performance monitoring configuration continues

# Video Quality Metrics (VQM) on ISR G2

- VQM deeper insight into the video flows (H.264) that are crossing routers
- ISRG2, c8xx 15.3(3)M
- Available via performance monitor



# Example Configuration

## VQM performance monitor

- 'no shut' under 'video monitoring' global config.
- To export via NetFlow, regular performance monitor configuration – just include the AQM fields

```
video monitoring
  maximum-sessions 10
  no shutdown

flow record type performance-monitoring vqm-rec
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match transport rtp ssrc
  collect application video resolution [ width | height ] last
  collect application video frame rate
  collect application video payload bitrate [ average | fluctuation ]
  collect application video frame [ I | STR | LTR | super-P | NR ] counter
  frames
  collect application video frame [ I | STR | LTR | super-P | NR ] counter
  packets [lost]
  collect application video frame [ I | STR | LTR | super-P | NR ] counter
  bytes
  collect application video frame [ I | STR | LTR | super-P | NR ] slice-
  quantization-level
  collect application video eMOS compression [ network | bitstream ]
  collect application video eMOS packet-loss [ network | bitstream ]
  collect application video frame percentage damaged
  collect application video scene-complexity
  collect application video level-of-motion
  collect transport rtpsequence-number [ last ]
```

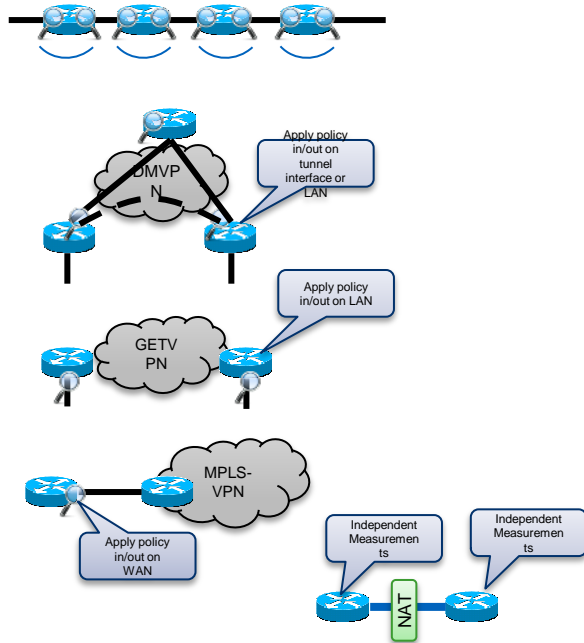


# End System (MSI) performance monitor

- MSI provides insight into
  - end system and application state
  - transmit and receive media statistics
- Information available via REST interface
- Ability to set thresholds and notifications
- Monitoring capability coming soon to Jabber for Windows



# Performance Monitor: Deployment

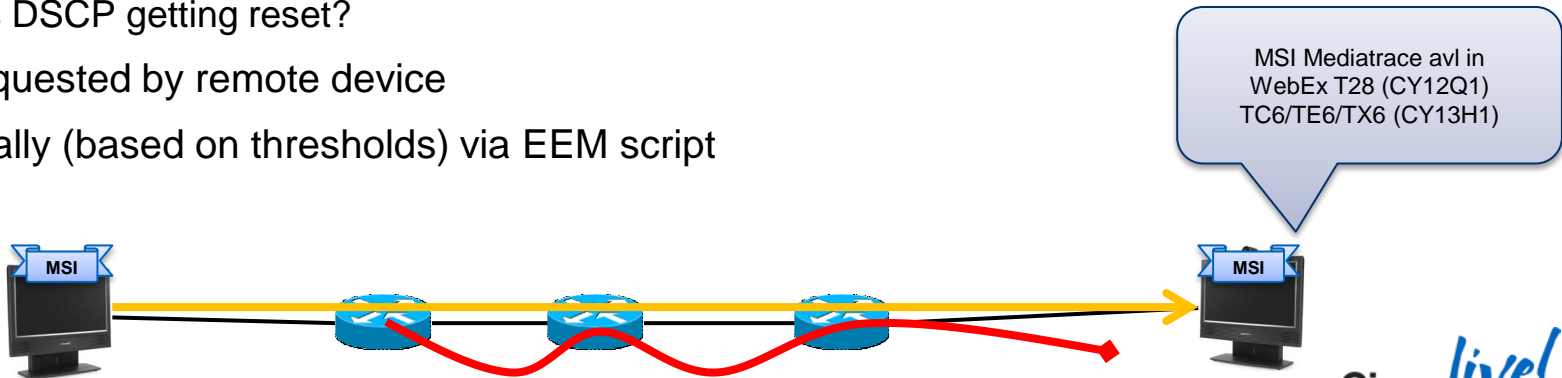


- Enable pervasively (if possible)
  - More monitoring points, the better the data
- Applications:
  - VoIP, WebEx, TelePresence, Desktop Video Conferencing (Cisco EX/MXP, Polycom, etc), Skype, Microsoft MOC/Lync
  - Any TCP traffic: Oracle, SAP, HTTP(s)
- Scenarios:
  - Remote sites without local IT staff
  - Telecommuter / cisco virtual office
  - WAN edge
    - DMVPN – tunnel interface
    - GETVPN – LAN interface
  - Mutation (NAT, SBC, etc.) – will require correlation

# Dynamic Monitoring with Mediatrace

Let mediatrace do the walking for you!

- Mediatrace discovers and queries L2 and L3 nodes along a flow's path
- Gathers system resource, interface and flow specific (perf-mon) stats
  - For performance monitor: dynamically configures monitoring policy (if needed) 5-tuple + intervals etc. match static policy).
- Consolidates information into a single screen
- Allows for easy comparisons of device behaviour
  - Which interface dropping packets?
  - Where is DSCP getting reset?
- Can be requested by remote device
- Automatically (based on thresholds) via EEM script



# Mediatrace Perf-Mon Poll

- **Mediatrace perf-mon poll**
  - Flow specific statistics
- Performance-monitor policy automatically configured (if needed) along path, then flow data collected
- Fixed field-sets for RTP and TCP flow analysis
- Mediatrace 2.0 removes requirement of Layer-4 ports in mediatrace request.

```
VXR-AA0310#mediatrace poll path-specifier source  
10.1.160.3 destination 10.1.3.3 perf-monitor
```

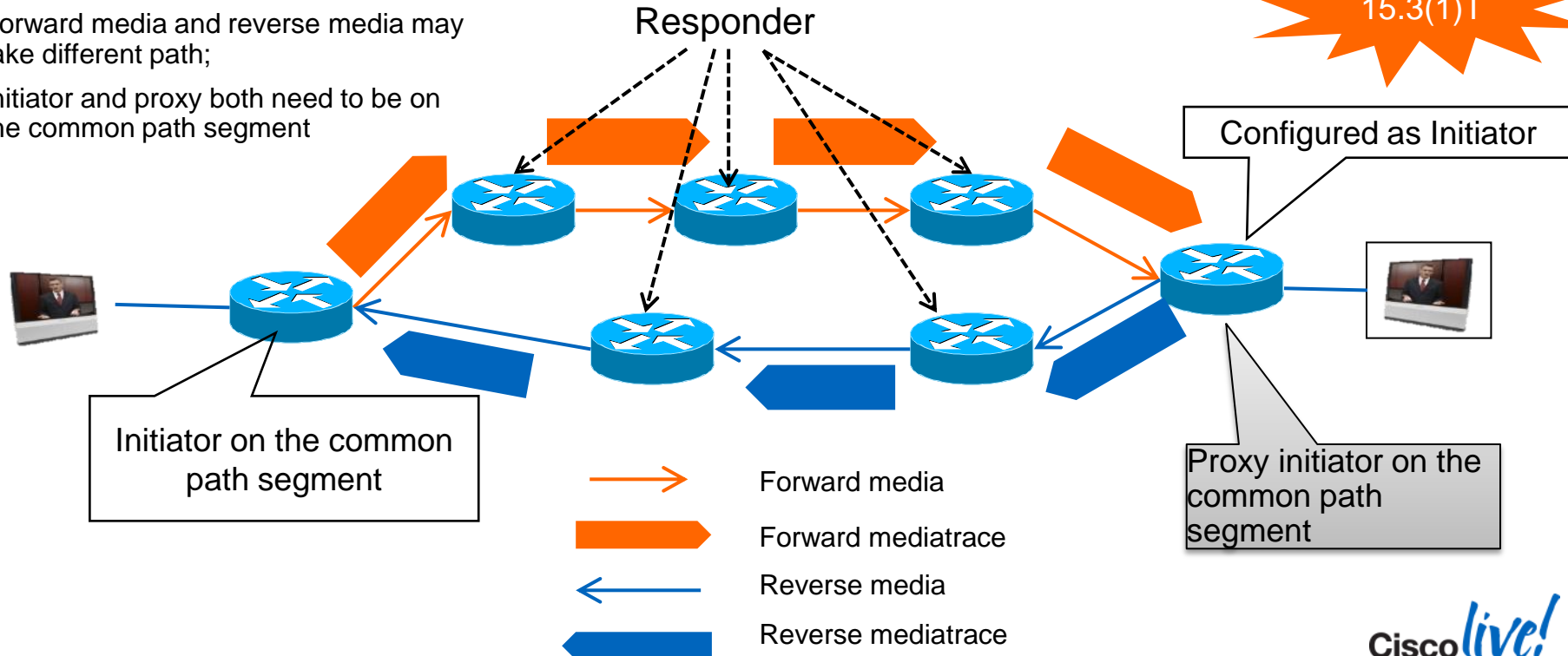
```
Started the data fetch operation.  
Waiting for data from hops.  
This may take several seconds to complete...  
Data received for hop 0  
Data received for hop 1  
Data received for hop 2  
Data fetch complete.  
Results:  
...  
Mediatrace Hop Number: 0 (host=VXR-AA0310, ttl=255)  
...  
Mediatrace Hop Number: 1 (host=3845-AA0216, ttl=250)  
Metrics Collection Status: Success  
Reachability Address: 10.1.162.2  
Ingress Interface: Fa0/0/0  
Egress Interface: Fa0/0/1  
Metrics Collected:  
Flow Sampling Start Timestamp: 01:30:42  
Loss of measurement confidence: FALSE  
Media Stop Event Occurred: FALSE  
IP Packet Drop Count (pkts): 0  
IP Byte Count (Bytes): 207398  
IP Packet Count (pkts): 898  
IP Byte Rate (Bps): 6913  
Packet Drop Reason: 0  
IP DSCP: 34  
IP TTL: 57  
IP Protocol: 17  
Media Byte Rate Average (Bps): 6314  
Media Byte Count (Bytes): 189438  
Media Packet Count (pkts): 898  
RTP Interarrival Jitter Average (usec): 6677  
RTP Packets Lost (pkts): 0  
RTP Packets Expected (pkts): 893  
RTP Packet Lost Event Count: 0  
RTP Loss Percent (%): 0.00
```

# Reverse Mediatrace

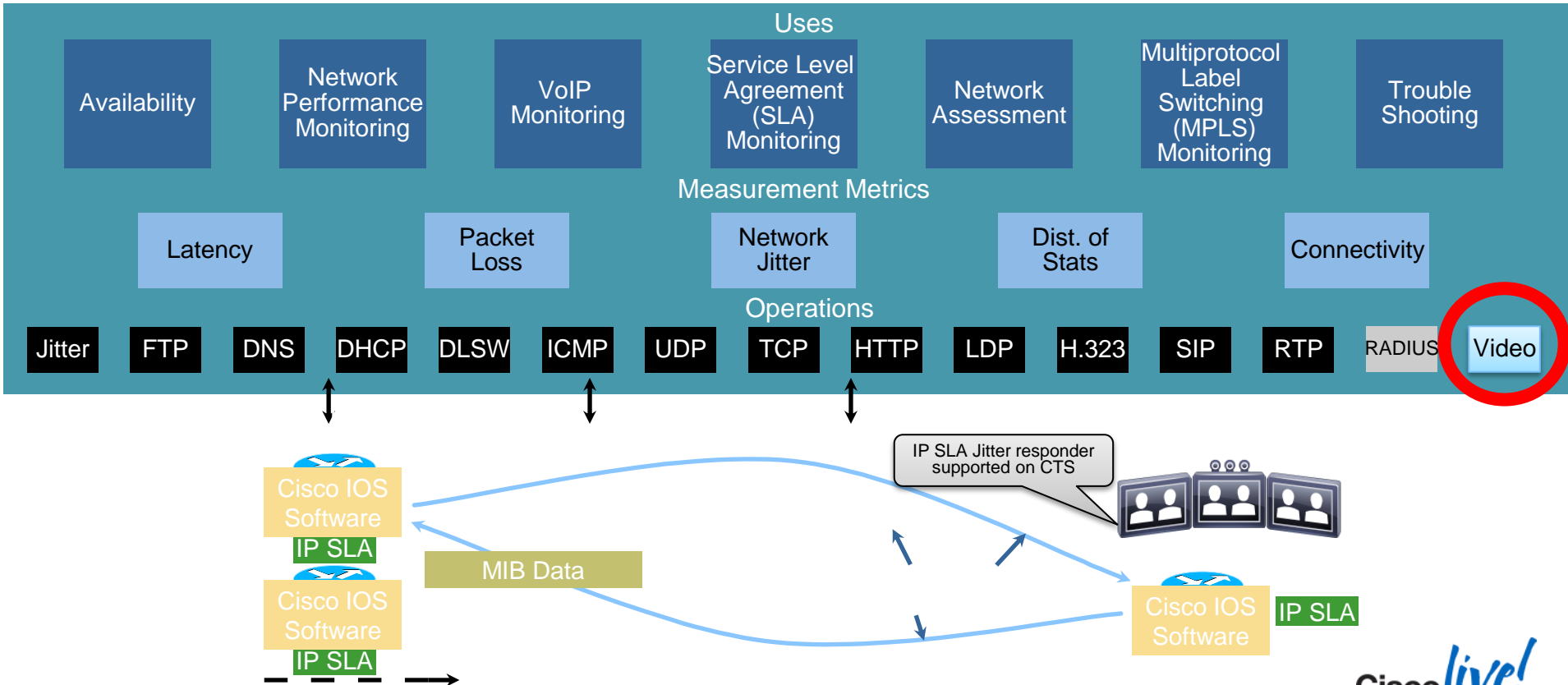
## Exploring the destination to source path

Forward media and reverse media may take different path;

Initiator and proxy both need to be on the common path segment



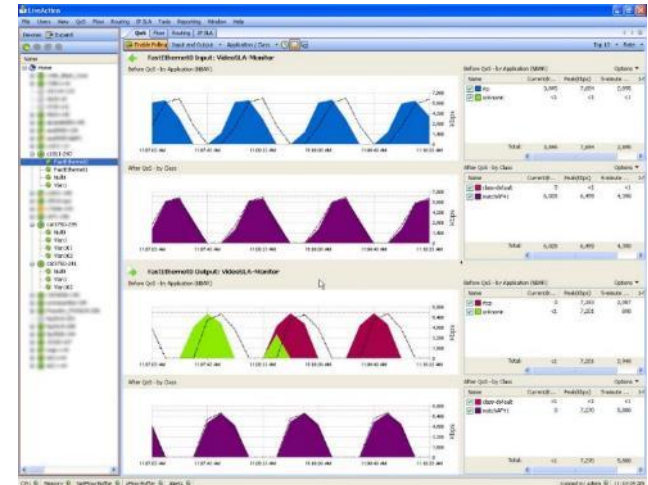
# IP SLA: Synthetic Traffic Measurements



# IPSLA Video Operation Embedded Traffic Simulator

Released  
March  
2012  
12.2(52)SE1

- IPSLA known in industry for jitter, ICMP, etc. probes
- Most probes measure experience without affecting user traffic (hopefully)
- Need traffic to **stress test** network
- IPSLA VO provides
  - Realistic representation of arbitrary video (RTP) traffic
    - Packet sizes, burstiness, traffic rate, etc.
  - pre-packaged profiles:
    - IPTV, Video Surv, CTS
    - Extensible via data file
  - Custom profile generation from packet capture



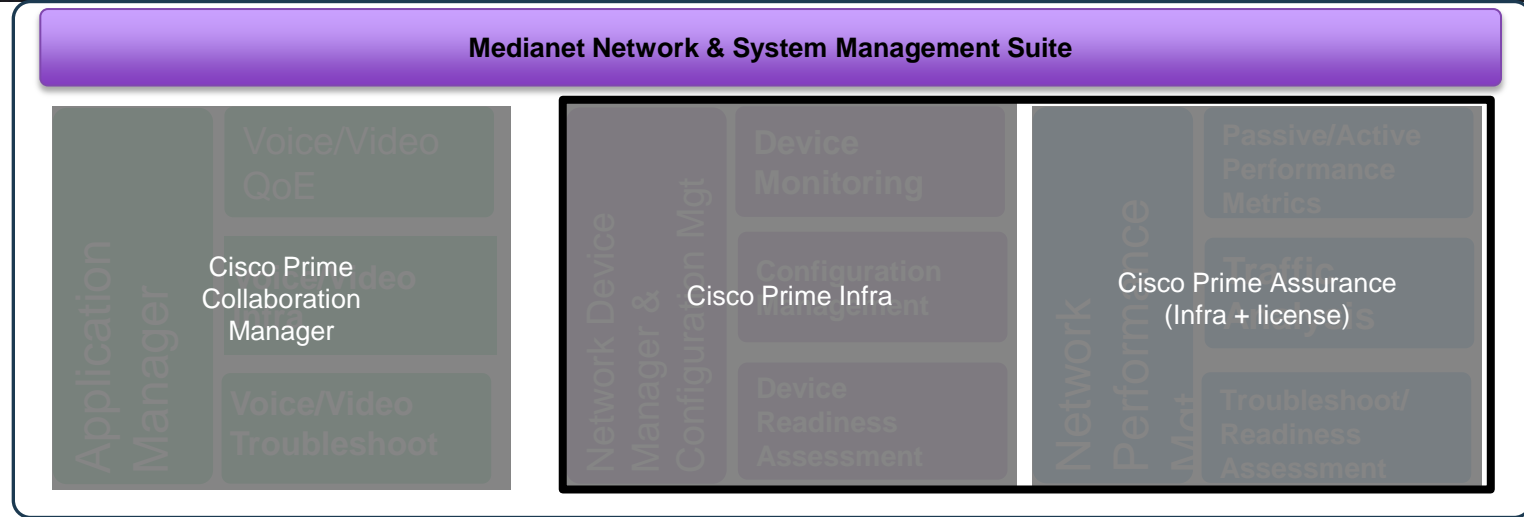
# Demo of Endpoint Monitoring Management

Cisco Prime Collaboration Manager (CPCM)





# Enterprise Medianet Network & System Management



Mediatrace  
IPSLA VO  
MSI  
IOS Perf Monitor

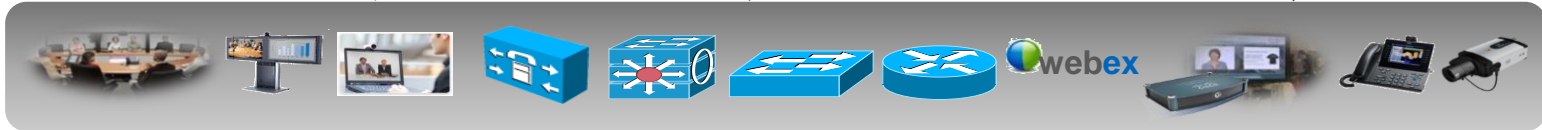


Configuration  
Uptime

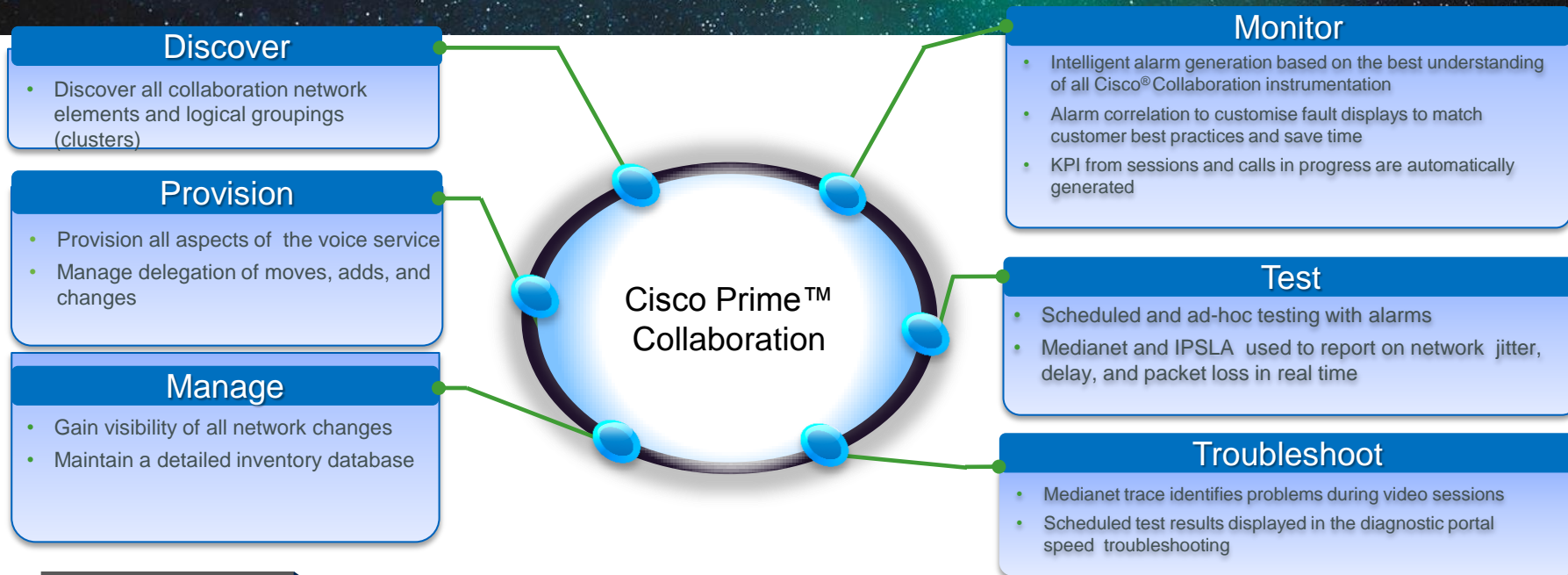
IPSLA VO  
Mediatrace



NetFlow, NBAR, NAM  
IOS Perf mon, CBQoS



# Prime Collaboration: Lifecycle Management



- Single product for all collaboration lifecycle needs
- Simplification and automation of many day-to-day tasks

# Cisco Prime Collaboration Diagnostic Testing

## Phone Tests

- Call hold
- Call forward
- Call park
- Call conference
- Call transfer
- Call test

## Synthetic Tests

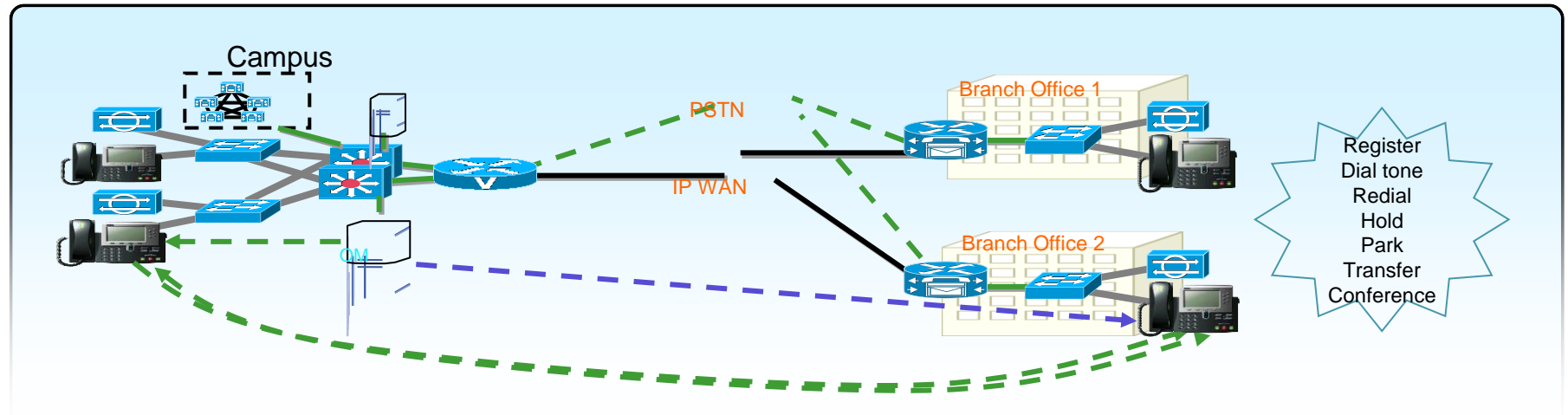
- Phone registration
- End-to-end call
- TFTP download
- Dial tone
- Emergency call
- Message waiting indicator

## Phone Status Test

- IPSLA ping
- Verifies reachability

## Node-to-node testing

- Ping and ping-path echo
- UDP echo
- UDP jitter for voice over IP
- Gatekeeper registration delay



# Cisco Prime Assurance 2.1 for Enterprise

Interactive & Customisable Dashboards

End-User/Application/  
Network views

Monitoring, Config,  
Threshold templates

FNF Coll & Reporting

Alarms/Events Browser

**Assurance**

**Collaboration**

**Network  
Infrastructure**

**Data Centre**

Multi-NAM Management

WAN Optimisation Views

OOB Reports & APIs

ART/Traffic/RTP Analysis

End-point management

PA

Medianet  
Performance Monitor

NetFlow & NBAR

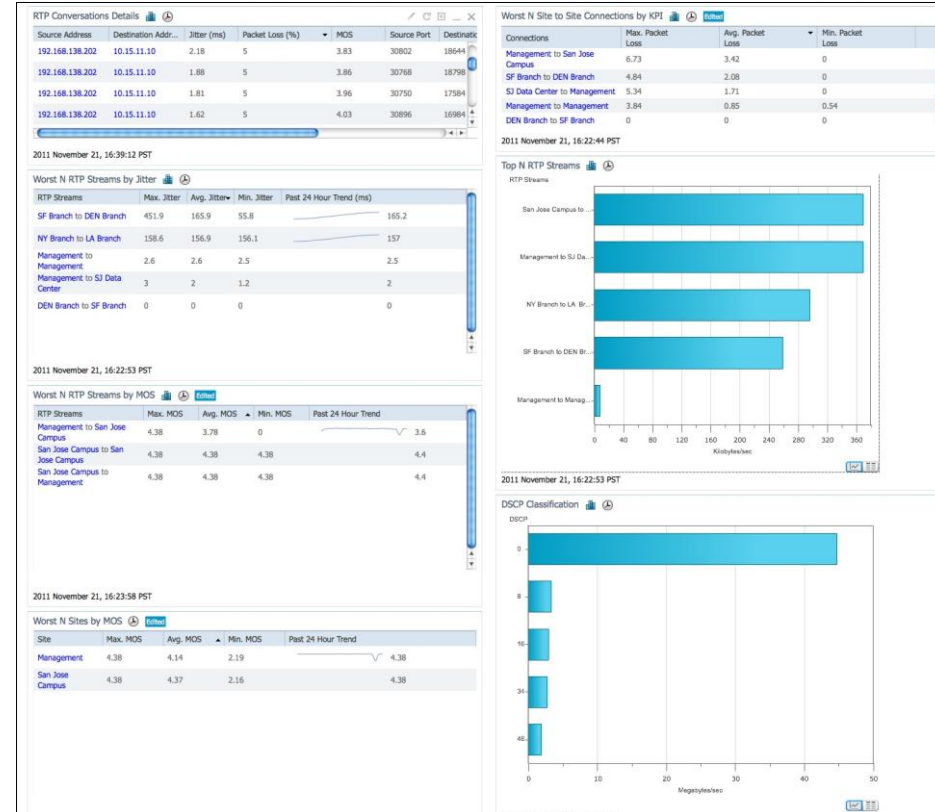
SNMP  
(IF, CBQoS)

Packets

Events

# Prime Assurance: Voice/Video Dashboard

- DSCP Classification
- RTP Conversations Details
- Top N RTP Streams
- Voice Call Statistics
- Worst N RTP Streams by Jitter
- Worst N RTP Streams by Packet Loss
- Worst N RTP Streams by MOS
- Worst N Sites by MOS
- Worst N Site to Site Connection KPI





# Application Awareness



## Flow Attributes



## Classification / Marking



## QoS Enforcement

- Have traditionally been implicit

Application implied by IP address, UDP port range, application name (with DPI), maybe even DSCP (overloading of DSCP)

- Reality is that applications have rich set of flow attributes:

Audio / video

Scheduled / ad-hoc

Soft-client / hard client

Internal / External party

- Marking may be arrived at via various methods:

End system DSCP trust

ACL based on port ranges

DPI/NBAR

Metadata etc.

- Traffic is groomed into DSCP marking
- Recommendation is along RFC4594 lines

- QoS enforcement is based on DSCP groomed traffic

- Multiple DSCP values may map to the same QoS class

- Number of QoS classes may change across the network (campus, SP WAN-edge, etc.).

- Generally cookie-cutter configurations across network with distinctions:

Network HW capability

SP service plan, etc.

**Cisco** *live!*

Video  
Application  
Marking  
RFC 4594 DSCP  
Markings

| Application Class       | PHB  | Admission Control | Congestion Management & Congestion Avoidance | Video Applications                              |
|-------------------------|------|-------------------|--|---|
| VoIP Telephony          | EF   | Required          | Priority Queue (PQ)                          |   |
| Broadcast Video         | CS5* | Required          | (Optional) PQ                                | Enterprise TV / IPVS                            |
| Real-Time Interactive   | CS4  | Required          | (Optional) PQ                                | High End Video Conferencing                     |
| Multimedia Conferencing | AF41 | Required          | BW Queue + DSCP WRED                         | Video Telephony / Conferencing                  |
| Multimedia Streaming    | AF31 | Recommended       | BW Queue + DSCP WRED                         | VoDs  |
| Network Control         | CS6  |                   | BW Queue                                     |   |
| Call-Signaling          | CS3* |                   | BW Queue                                     |   |
| OAM                     | CS2  |                   | BW Queue                                     |   |
| Transactional Data      | AF21 |                   | BW Queue + DSCP WRED                         | WebConferencing                                 |
| Bulk Data               | AF11 |                   | BW Queue + DSCP WRED                         |   |
| Best Effort             | DF   |                   | Default Queue + RED                          |   |
| Scavenger               | CS1  |                   | Min BW (Deferential) Queue                   | YouTube / Xbox Live / iTunes / BitTorrent/ etc. |



# How Many Classes of Service Do I Need?

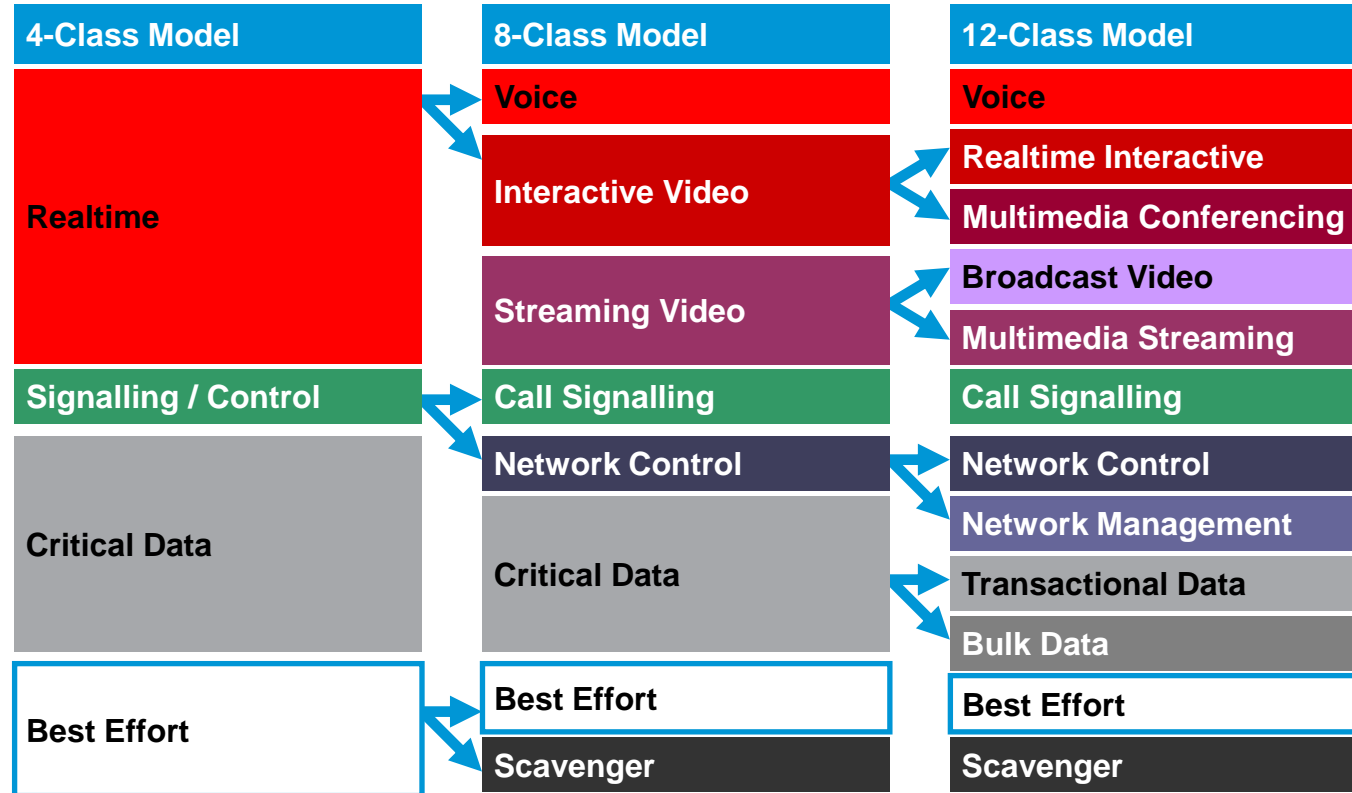
Service Provider Plans

Capability of network devices

How much time do you have?

---

But always try to mark traffic along RFC4594 lines.



Requirements



# Soft Client Classification Methods

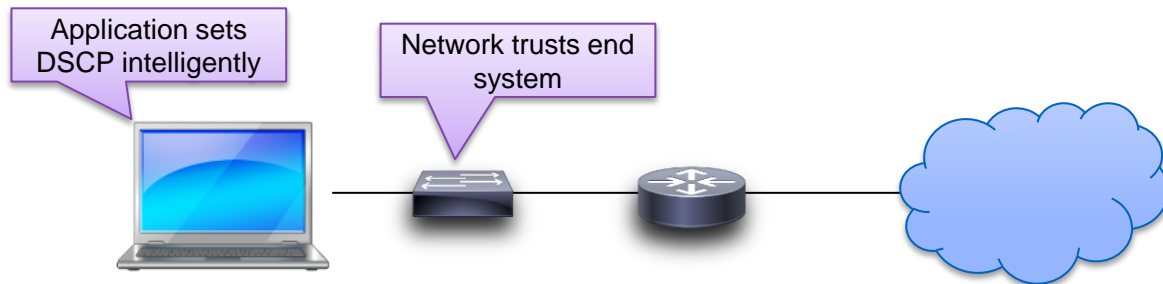
## DSCP set directly by application on end system

### Pro:

- straightforward. If it works.
- Application has flexibility to use different DSCP values

### Con:

- Generally PC is not a trusted device. Possible exceptions strictly managed PC, access port implements policer to limit overage/abuse. Need to work with network team to extend DSCP trust boundary.
- DSCP context is controlled by application vs. network
- Not an option for Windows Vista, Win7, Win8. Needs registry tweak in Win XP



# Soft Client Classification Methods

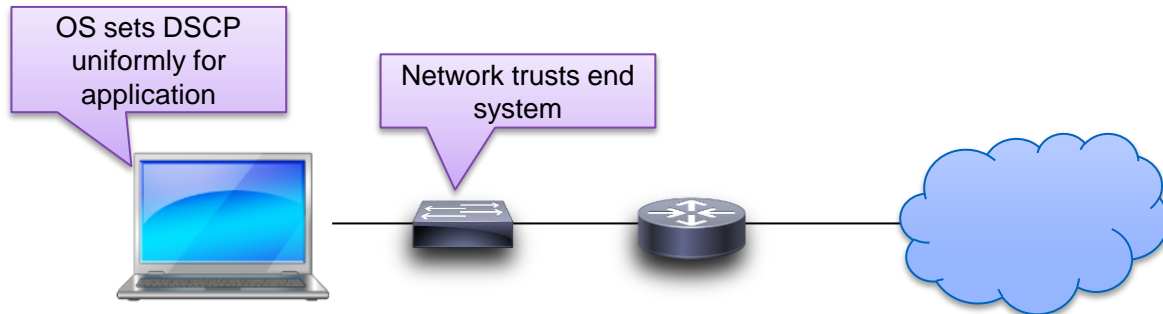
## DSCP set by OS (Windows Group Policy Object - GPO)

### Pro

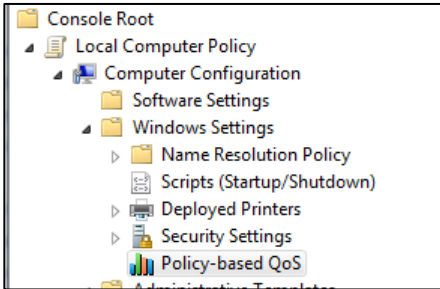
- Works for Windows Vista, Win7, Win8
- Centralised Administration of Policies (Windows AD)

### Con:

- Unable to differentiate amongst some flows created by application (media types)
- Generally PC is not a trusted device. Possible exceptions strictly managed PC, access port implements policer to limit overage/abuse. Need to work with network team to extend DSCP trust boundary.
- GPO is Windows specific



# Windows Group Policy Object (GPO)



Windows Group Policy Object (GPO) allows for the QoS control (policer, DSCP marking) of traffic. Based on application name, URL, IP address, IP protocol and L4 port numbers

Policy-based QoS

Create a QoS policy  
A QoS policy applies a Differentiated Services Code Point (DSCP) value, throttle rate, or both to outbound TCP, UDP, or HTTP response traffic.

Policy name:  
jabber-SIP

Specify DSCP Value:  
34

Specify Outbound Throttle Rate:  
1 kbps

[Learn more about QoS Policies](#)

< Back Next > Cancel

1

Policy-based QoS

This QoS policy applies to:

All applications

Only applications with this executable name:  
%ProgramFiles%\jabberVideo\jabberVideo.exe  
Example: application.exe or %ProgramFiles%\application.exe

Only HTTP server applications responding to requests for this URL:  
Include subdirectories and files

Example: http://myhost/training/ or https://\*/training/  
Example of non-standard TCP port: http://myhost:8080/training/ or https://myhost:\*training/

[Learn more about QoS Policies](#)

< Back Next > Cancel

2

Policy-based QoS

Specify the source and destination IP addresses.

A QoS policy can be applied to outbound traffic that is from a source or to a destination IP (IPv4 or IPv6) address or prefix. For HTTP response traffic, the destination IP address or prefix denotes the client(s) that issued the HTTP request.

This QoS policy applies to:

Any source IP address

Only for the following source IP address or prefix:

This QoS policy applies to:

Any destination IP address

Only for the following destination IP address or prefix:

Example for a host address: 1.2.3.4 or 3ffe:ffff::1  
Example for an address prefix: 192.168.1.0/24 or fe80::1234/48

[Learn more about QoS Policies](#)

< Back Next > Cancel

3

Policy-based QoS

Specify the protocol and port numbers.

A QoS policy can be applied to outbound traffic using a specific protocol, a source port number or range, or a destination port number or range.

Select the protocol this QoS policy applies to:  
TCP

Specify the source port number:

From any source port

From this source port number or range:

Specify the destination port number:

To any destination port

To this destination port number or range:  
5050  
Example for a port: 443  
Example for a port range: 137:139

[Learn more about QoS Policies](#)

< Back Finish Cancel

4

# Soft Client Classification Methods

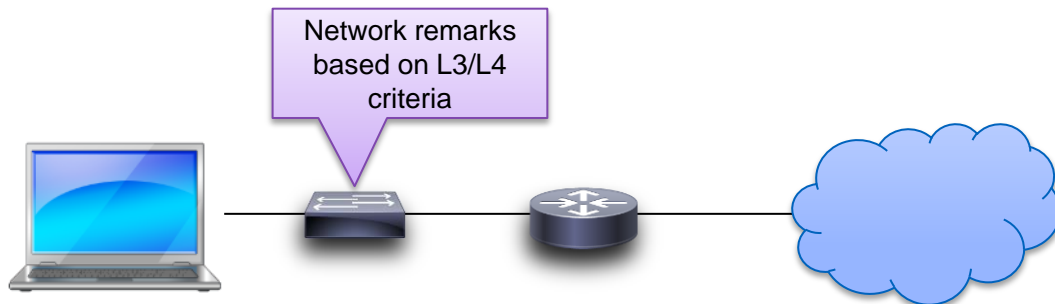
DSCP set by network based on understood UDP port ranges

Pro:

- Do not need to trust endpoint
- Straightforward access-list mapping

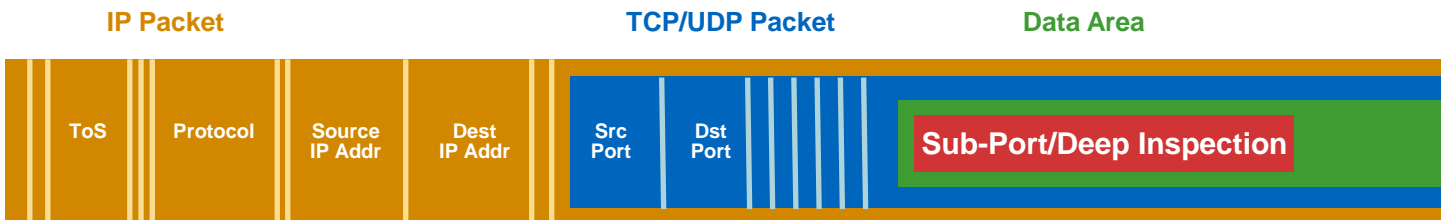
Con:

- Possible conflict on UDP ranges between different applications
- UDP port range may change based on SW rev, managed state etc.
- Context of application usage flow (media, usage etc.) not understood. Is it voice or video?



# NBAR: Full-Packet Inspection

- Stateful and Dynamic Inspection



- Used for intelligent policy (QoS, filtering, etc.) or reporting
- Identifies over 1200 applications and protocols TCP and UDP port numbers
  - Statically assigned
  - Dynamically assigned during connection establishment
  - RTP and RTP payload type identification, MS-Lync, gtalk-video, skype, etc.
  - Cisco TelePresence media and signalling supported in IOS 15.1(3)T
  - WebEx desktop-share/audio/video supported in 15.2(2)T
- Non-TCP and non-UDP IP protocols
- Data packet inspection for matching values

# Soft Client Classification Methods

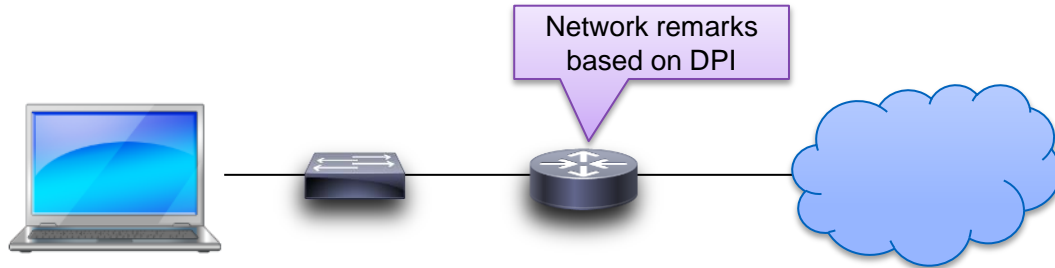
## DSCP set by network based on DPI (NBAR)

### Pro:

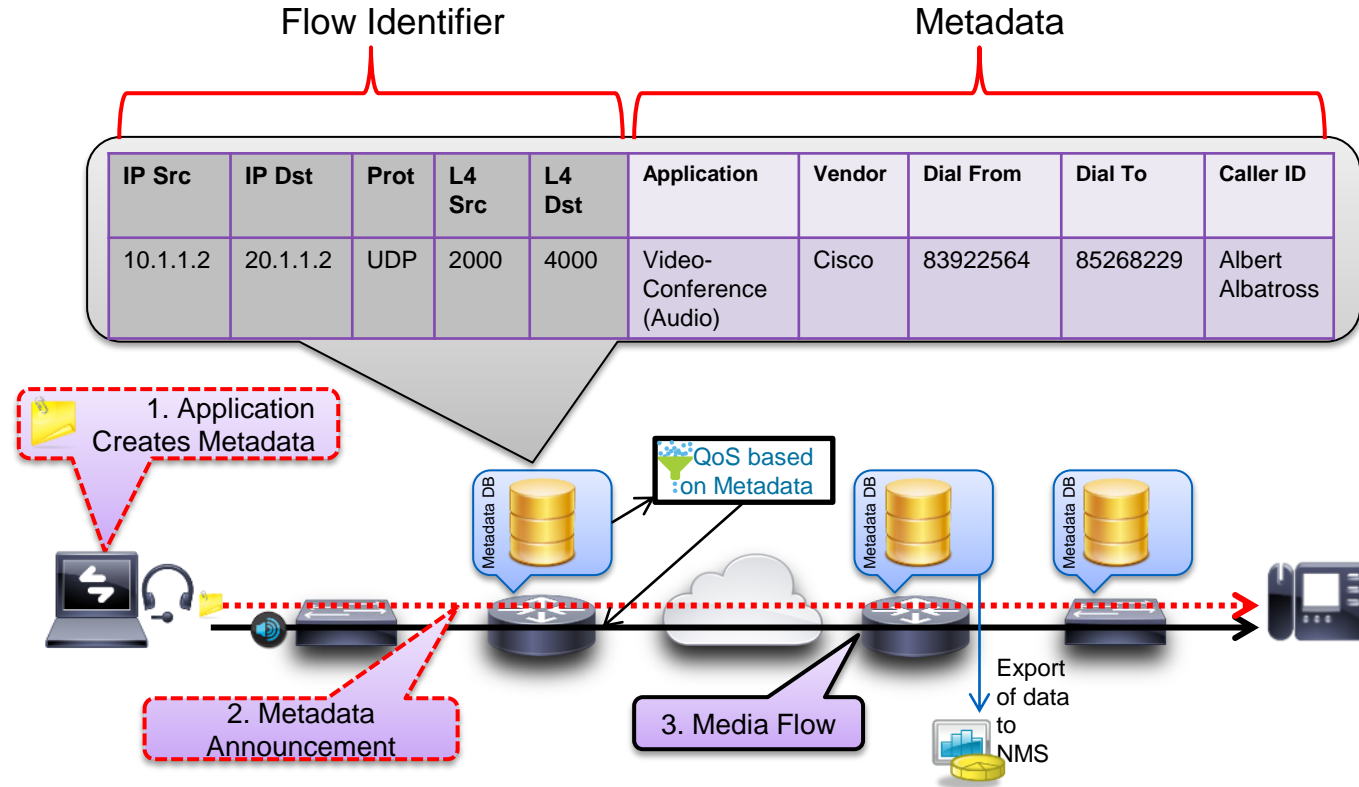
- Do not need to trust endpoint
- Simple configuration mapping

### Con:

- Challenged by encryption
- Context is based on what is visible / gleaned on the wire
- Network capability is on limited platforms (AP, ISRG2, ASR1k)



# Introducing Medianet Flow Metadata





# Soft Client Classification Methods

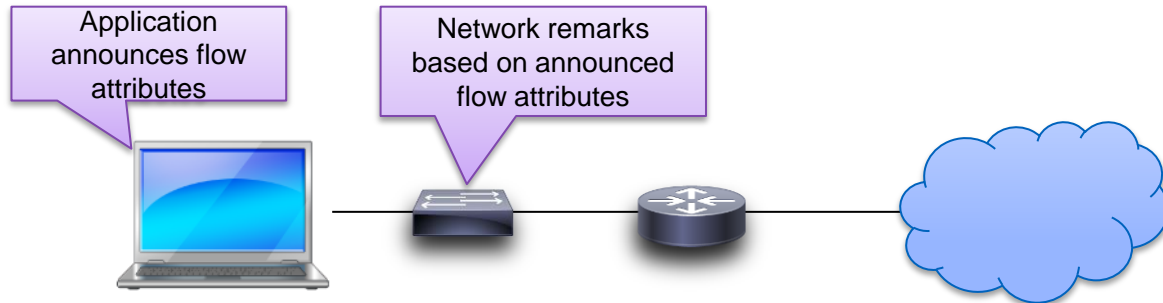
## MSI produced Metadata

### Pro:

- Separation between application context (metadata) and policy (based in network)
- Explicit signalling: no false positive or negatives
- Extremely granular information elements
- Simple network configuration mapping
- Lightweight- widely available across cisco network devices (cat4k, cat6k, ISRG2, ASR1k, cat3k (CY13Q4))

### Con:

- Need to have MSI deployed as well as network capability



# Examples of Metadata Classification

| Case  | IOS Configuration   |
|---|---|
| Software phone video conferencing (audio+video) | <pre>Class-map match-all &lt;video&gt;   Match application attribute device-class software-phone   Match application attribute media-type video Class-map match-all &lt;audio-in-video&gt;   Match application attribute device-class software-phone   Match application attribute media-type audio-video</pre> |
| Software phone audio only call (only audio)     | <pre>Class-map match-all &lt;audio-only&gt;   Match application attribute device-class software-phone   Match application attribute media-type audio</pre>  |
| Physical phone audio only call (only audio)     | <pre>Class-map match-all &lt;audio-only&gt;   Match application attribute device-class physical-phone   Match application attribute media-type audio</pre>  |
| WebEx Video                                     | <pre>Class-map match-all &lt;video &gt;   Match application webex-meeting   Match application match application attribute media-type video</pre>  |

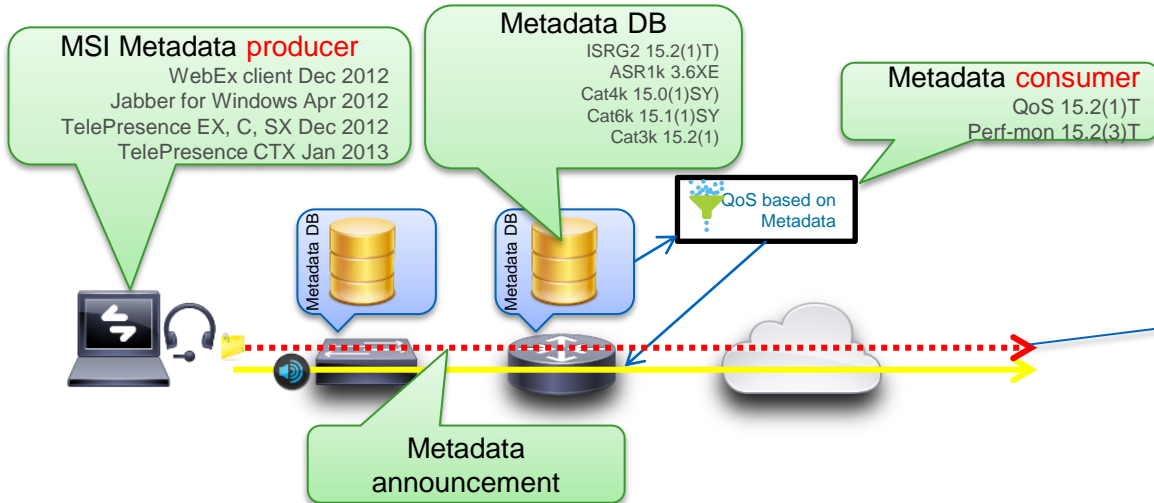
# Cisco IT: Identify and Classify Challenge

|  |   |  |  |                                      |
|--|---|--|--|--------------------------------------|
| <b>CP-9971</b>                                   | Video<br>NBAR: Payload type 97 or 126 <sup>1</sup><br>Voice<br>ACL: UDP/16384-32784 | Video<br>AF42<br>Voice<br>EF (Prec. 5) | CBWFQ<br>(384Kbps to 6Mbps) <sup>2</sup><br><br>LLQ (128K) | Medianet metadata<br>UDP port ranges |
| <b>Jabber, MOVI, Softphone</b>                   | ACL: UDP/14040-14240 and DSCP 37  | AF42                                   | CBWFQ<br>(384Kbps to 6Mbps)                                | Medianet metadata<br>UDP port ranges |
| <b>Tandberg C-Series<br/>(E20, EX-60, EX-90)</b> | ACL: UDP/2326-2485 and DSCP 35  | AF41                                   | CBWFQ<br>(768Kbps to 6Mbps)                                | Medianet metadata<br>UDP port ranges |
| <b>Tandberg MXP Series</b>                       | ACL: UDP/46000-49000 and DSCP 35  | AF41                                   | CBWFQ<br>(768Kbps to 6Mbps)                                | Medianet metadata<br>UDP port ranges |
| <b>MCU (Codian)</b>                              | ACL: UDP/49152-65535 and DSCP 35  | AF41                                   | CBWFQ<br>(384Kbps to 6Mbps)                                | Medianet metadata                    |
| <b>WebEx</b>                                     | TCP traffic based upon destination  | Default                                | In Progress  | Medianet metadata                    |
| <b>Cisco TelePresence System</b>                 | match protocol telepresence-media<br>match protocol telepresence-control            | CS4                                    | CBWFQ<br>(3.5 or 6.5 Mbps)                                 | Medianet metadata                    |
| <b>ALL<br/>Control and Signalling</b>            | ACL: SIP, SCCP, RADIUS, BFCP (TCP)<br>NBAR; RTCP                                    | 24 (Prec. 3)                           | LLQ (64Kbps)   | N/A                                  |

1 Note: RTP payload inspection must be performed prior to ACL match

# Application (MSI) Generated Metadata

- Metadata protocol:** announces flow parameters and attributes to network nodes along a path
- Metadata flow DB:** maintains flow attribute information, and coordinates metadata producers/consumers.
  - Producer:** creates metadata information
  - Consumer:** utilises metadata information
- Nodes that do not support metadata will pass it silently



```

FF2205-4507#show metadata flow local-flow-id 5

To          From          Protocol
64.102.38.183  10.1.1.2      UDP

SPort      DPort      Ingress I/F          Egress I/F
24594      16384      Vlan605              n/a

Metadata Attributes :

Application Name      : cisco-phone
Application Tag       : 218103889 (cisco-phone)
Application Category  : voice-video
Application Sub Category : voice-video-chat-collaboration
Application Device Class : software-phone
Application Media Type : audio
End Point Model       : Jabber for Windows
Unknown Identifier (147) : [ 00 00 00 05 ]
Unknown Identifier (148) : [ 00 00 00 02 ]
Application Vendor    : Cisco Systems, Inc.
Application Version    : Jabber 9.0.0

Matched filters :

Direction: IN:
Direction: OUT:
    
```

# Medianet Metadata

## Metadata Created by Media Services Proxy (MSP)

- Devices that do not support MSI may be provided supplementary services by **Media Services Proxy (MSP)**
- MSP generate metadata from gleaning of signalling (SIP, H.323, RTSP, mDNS, etc)

```
3945-BB0208#show metadata flow local-flow-id 10

To          From          Protocol SPort  DPort
10.4.10.12  10.1.1.2      UDP      49222  14094

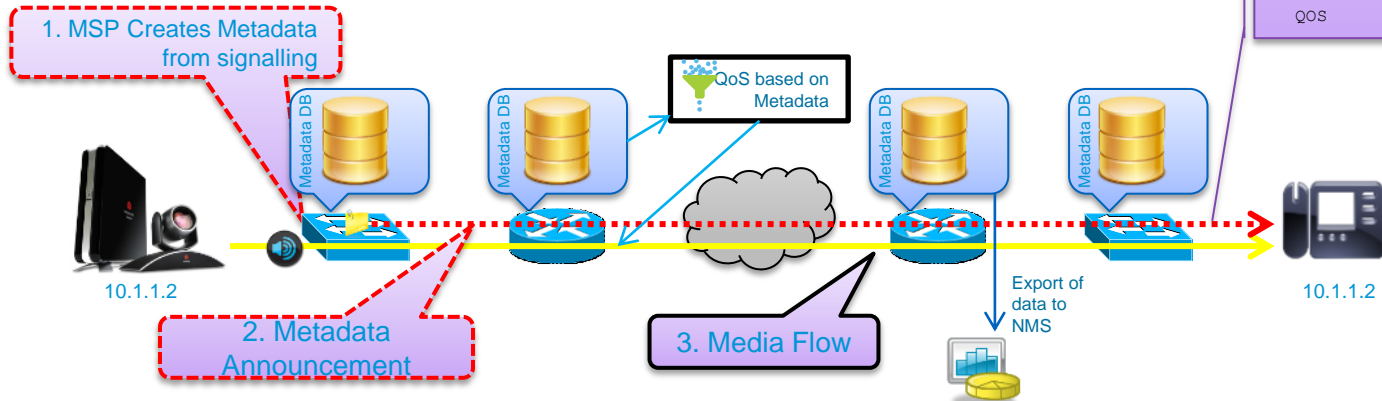
Ingress I/F      Egress I/F
GigabitEthernet0/1  GigabitEthernet1/0

Metadata Attributes :

Called URI      : 4103@cisco.com
Calling URI     :
vputtasu.office.6000@cisco.com
Application Name : rtp
Application Tag  : 218103869 (rtp)
Bandwidth       : 256
SDP Session ID  : 352800100
SIP User Name   : vputtasupolycom
Mime Type       : H264
Payload Type    : 109
Clock Frequency : 90000

Matched filters :

Direction: IN:
Direction: OUT:
QOS       : "metadata called-uri 4103@cisco.com"
```





## Examples of Deployment

# A Phased Approach to Monitoring

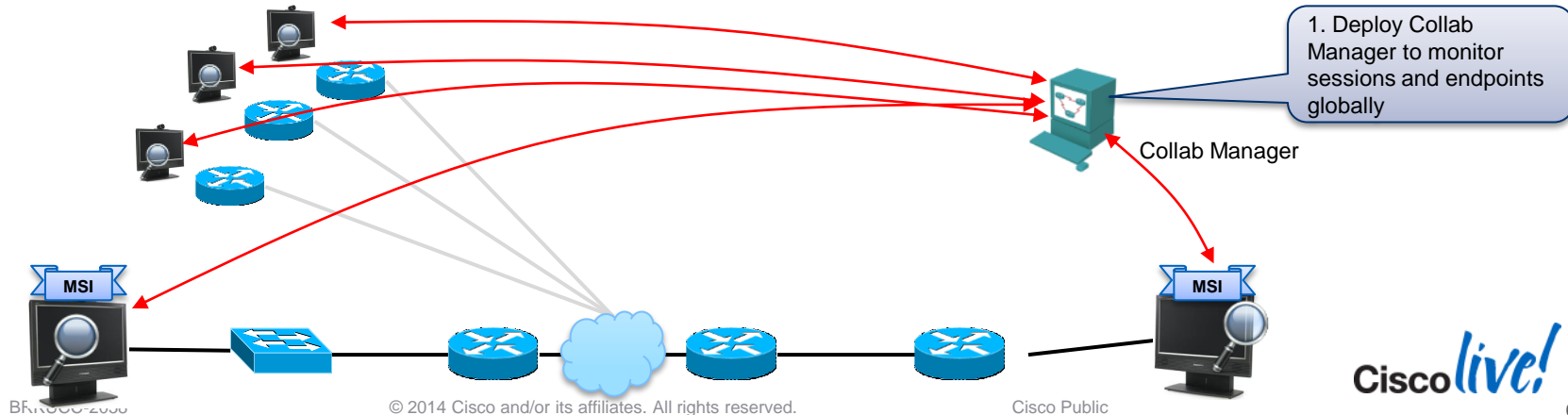
## For Cisco UC/ VC Applications

- Situation:

- Intermittent issues with voice/video quality. Operator wants to quickly discover and resolve issues to provide a stable SLA service.

1. Deploy Collaboration Manager to monitor phone and VC endpoints, 'over the top'

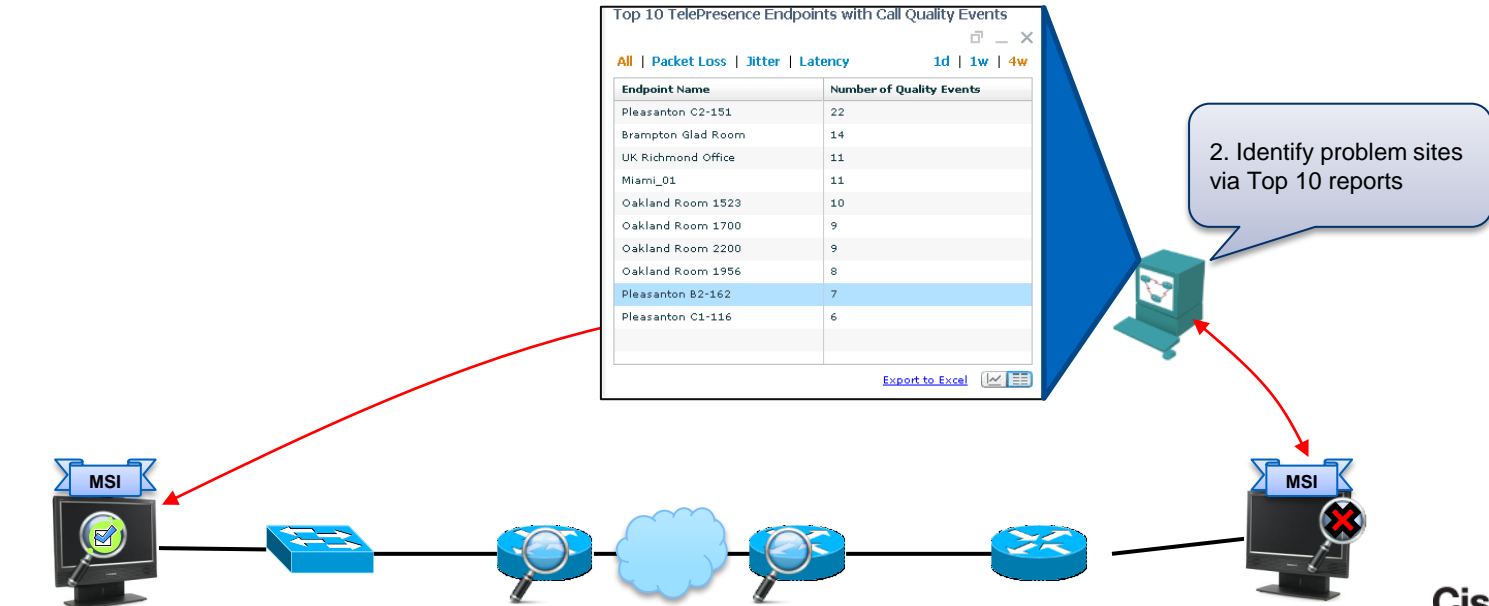
No network changes needed



# A Phased Approach to Monitoring

For Cisco UC/ VC Applications

2. Via CP Top 10 Reports, identify worst performing endpoints and sites.





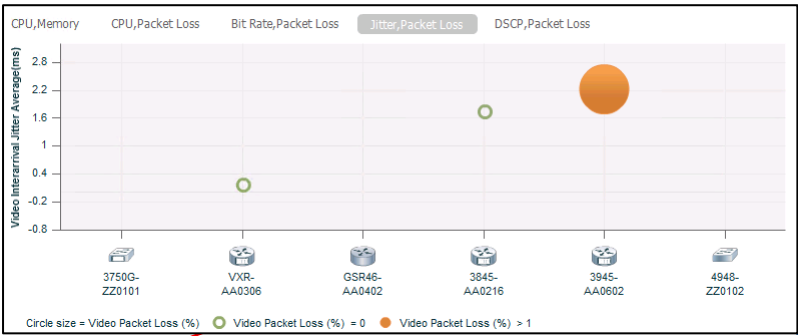
# A Phased Approach to Monitoring

## For Cisco UC/ VC Applications

If network write access unavl for collab manager, deploy for endpoint driven mediatrace.

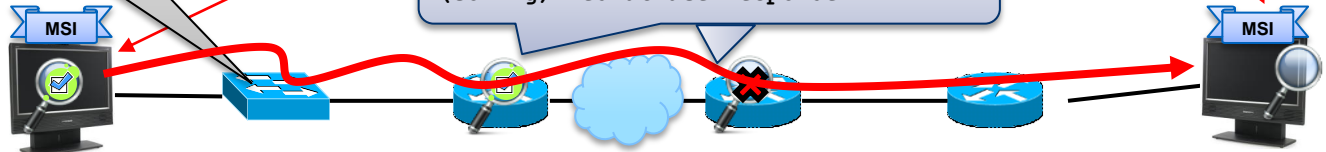
- 3. On identified jitter problem sites, enable performance monitor & mediatrace.
- 4. Localise problem using Collab Manager and Mediatrace

Depending on who controls the LAN / WAN. May need to deploy on switches vs. WAN routers.



3. Deploy performance monitor and mediatrace (config) mediatrace responder

4. Perform fault-isolation using mediatrace.



# Metadata Classification for Differentiated Quality of Service (1)

- Situation:

- Bandwidth contention between different forms of video applications. Application and network operators want to be able to manage bandwidth better to allow a more deterministic experience.
- **WebEx**: Desire to deploy high quality video (1.5 mbps) but concerned about bandwidth contention. Do not want desktop share or audio to be compromised.
- **Conference Room Video**: Highest level quality of video offered and expected.
- **Jabber based audio or audio/video**: Audio/Video telephony for the masses. Best effort service– audio more important than video.

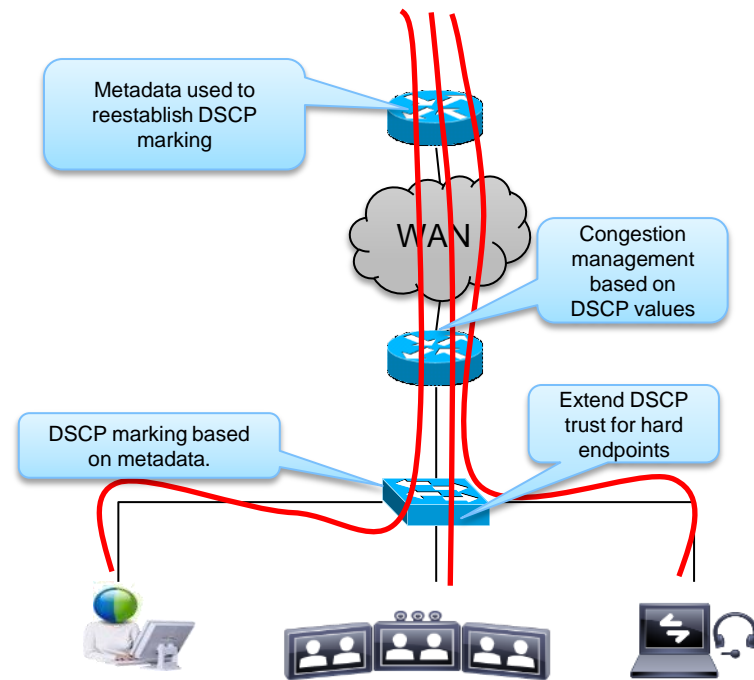
This is just one example.

Service delivery profiles differ across operators.



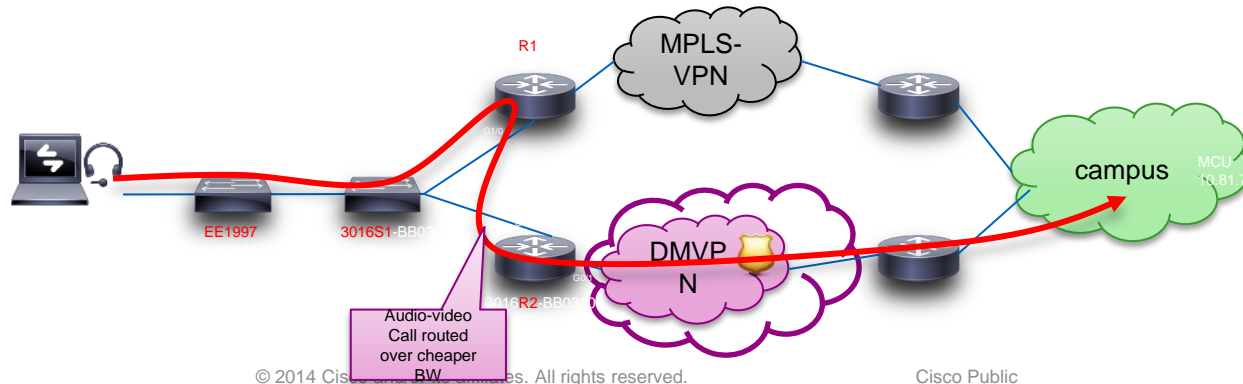
# Metadata Classification for Differentiated Quality of Service (2)

- Medianet Flow Metadata is used to drive classification.
  - Provides information to separate WebEx desktop share (AF21) from desktop video (DF)
  - DSCP Trust (CS4) is extended to CTS as it is a hard endpoint. However, metadata could be used for easier provisioning.
  - Jabber is identified as a soft client via metadata
    - Voice only calls are marked as EF
    - Voice and Video call media are marked as AF41.










# Metadata Classification for Intelligent Path Selection

- Situation:
  - Traditional MPLS-VPN bandwidth is expensive to justify for mass video usage. However, enterprise has cheaper broadband connections.
- Identify soft client originated video calls and route (via policy-based-routing) to cheaper path. Voice only soft-client calls remain on MPLS-VPN path.
- Use perf-mon and mediatrace to detect and monitor quality issues.



# Medianet Feature Availability

- Autoconfiguration
- Media Monitoring
- Media Awareness
- Media Services Proxy

|  |  |  |   |  |   |   |
|--|--|--|---|--|---|---|
| <br><b>WBS29.SP32</b><br><span style="color: blue;">✓</span> 1H2012 | <br><b>Digital Media Player 4310G/4400</b><br><span style="color: yellow;">✓</span> | <br><b>4300/4500 Series HD Box Cameras</b><br><span style="color: yellow;">✓</span> | <br><b>Jabber for Windows</b><br><span style="color: blue;">✓</span> 1H2012<br><span style="color: black;">✓</span> 2H2012 | <br><b>VXI</b><br><span style="color: blue;">✓</span> 2H2012<br><span style="color: black;">✓</span> 2H2012 | <br><b>TP CTS</b><br><span style="color: blue;">✓</span> 2H2012<br><span style="color: black;">✓</span> 2H2012 | <br><b>TP C &amp; Ex Series</b><br><span style="color: blue;">✓</span> 2H2012<br><span style="color: black;">✓</span> 2H2012 |
|--|--|--|---|--|---|---|

## Network Management



## Media Services Interface

- Auto Configuration:**
- Auto smart ports
  - Location

- Media Monitoring:**
- Performance monitor
  - Mediatrace
  - IPSLA VO

- Media Awareness:**
- Media Services Proxy
  - Flow Metadata

Cisco Prime:  
 Collaboration Manager 1.1  
 LMS 4.1  
 Cisco Prime Assurance Manager 1.1

|  |   |   |  |  |   |   |
|--|---|---|--|--|---|---|
| <br><b>Cisco ISR G2 2900/3900 Series</b><br><span style="color: magenta;">✓</span> Q1 2012<br><span style="color: blue;">✓</span> Q1 2012 | <br><b>Cisco ISR 880/890 Series</b><br><span style="color: blue;">✓</span> Q1 2012 | <br><b>Catalyst 2960S/2960 Series</b><br><span style="color: yellow;">✓</span> | <br><b>Catalyst 3750/3560 Series</b><br><span style="color: yellow;">✓</span> | <br><b>Catalyst 4500/4900 Series</b><br><span style="color: black;">✓</span> 1H2012<br><span style="color: magenta;">✓</span> 1H2012<br><span style="color: blue;">✓</span> 1H2012 | <br><b>Catalyst 6500/6500-E Series</b><br><span style="color: blue;">✓</span> 2H2012 | <br><b>Cisco ASR 1000 Series</b><br><span style="color: blue;">✓</span> 2H2012 |
|--|---|---|--|--|---|---|

## Medianet Readiness Assessment Service



# Medianet Summary

- Medianet is a solution that includes components within the end systems, network and management
- Medianet features assist in service validation, troubleshooting, and accelerate video application deployment
- Planning, Pre-Deployment
  - IPSLA VO, Performance-Monitor
- Troubleshooting
  - Performance Monitor, Mediatrace, CPCM, IPSLA VO
- Scalable Control and Policy
  - Media Service Proxy, Auto Smart Ports, Metadata



# Medianet @ Cisco Live Melbourne

Walk in Self Paced (WISP) Labs

- LABRST-2050  
Performance Monitor and Mediatrace Lab
  
- LABRST-2053  
Medianet Flow Metadata Lab

# Connect with Your Peers and Cisco

- Discuss business, IT, architecture, adoption and product topics with peers
  - Unified communications, collaboration applications, customer care, telepresence
- Interact with Cisco Product Managers, Technical Marketing Engineers and Services Consultants
- Learn about new product announcements
- Join the Collaboration User Group
  - Influence product direction
  - Access to Beta trials
    - Exclusive programs, advisory groups and briefings
  - Membership is free!

## Cisco Collaboration Community and User Group

The screenshot shows the Cisco Communities website for the Collaboration User Group. The header includes the Cisco logo, 'Cisco Communities', a 'Directory' dropdown, and a search bar. The main content area is titled 'Collaboration' and features several sections:

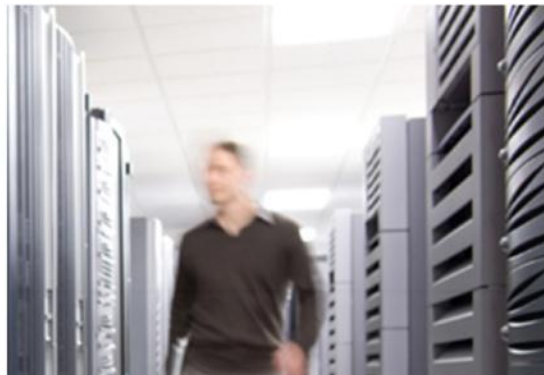
- Sign Up for Email Notifications:** A section for users to get email updates on new posts.
- Navigate to a Topic and Post:** A list of topics including 'Cisco Collaboration Virtual Launch Experience', 'Enterprise Social Software', 'Business Conversations and Sharing', 'Product Conversations and Sharing', 'Telepresence', 'Unified Communications', 'WebEx Meeting Applications', 'WebEx Connect', and 'Other'.
- Popular Tags:** A list of tags such as 'cisco\_collaboration\_virtual\_launch\_experience', 'collaboration\_user\_group', 'unified\_communications', 'virtual\_experience', and 'virtual\_launch\_experience'.
- Cisco Cius Announcement and Customer Stories:** A featured article with a video player and a 'Log into Community' button.
- About the Collaboration Community:** A section with a 'Log into Community' button.
- Collaboration User Group Dashboard:** A section for users to join the group, with a 'Join User Group How' button and a 'Log into Community' button.
- Click on each image to learn about user group benefits:** A row of images with captions: 'Beta and Early Field Trials', 'Technical Briefings', 'Virtual Office Hours', 'Feature Request Tool', 'Special Interest Groups', 'VIP Perks at Cisco Live', and 'Contact Center User Group'.

Visit the Collaboration Community and join the Collaboration User Group at:  
[www.cisco.com/go/joinconversation](http://www.cisco.com/go/joinconversation)



# Additional Medianet Resources

- Medianet on Cisco.com  
<http://www.cisco.com/go/medianet>
  - Autoconfiguration  
<http://www.cisco.com/go/autoconfiguration>
  - Media Monitoring  
<http://www.cisco.com/go/mediamonitoring>
  - MSI  
[http://www.cisco.com/en/US/solutions/ns340/ns857/ns156/ns1094/media\\_services\\_interface.html](http://www.cisco.com/en/US/solutions/ns340/ns857/ns156/ns1094/media_services_interface.html)
- Medianet Knowledge Base  
<http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html>
- Medianet Support Forum  
<https://supportforums.cisco.com/community/etc/medianet>
- Medianet Blogs  
<http://blogs.cisco.com/tag/medianet/>
- Cisco Developer Network for Medianet  
<http://developer.cisco.com/web/mnets>
- Cisco Prime Collaboration Manager  
<http://www.cisco.com/go/cpcm>
- Cisco TelePresence Management Suite  
<http://www.cisco.com/en/US/products/ps11338/>



Q & A

# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm



## Learn online with Cisco Live!

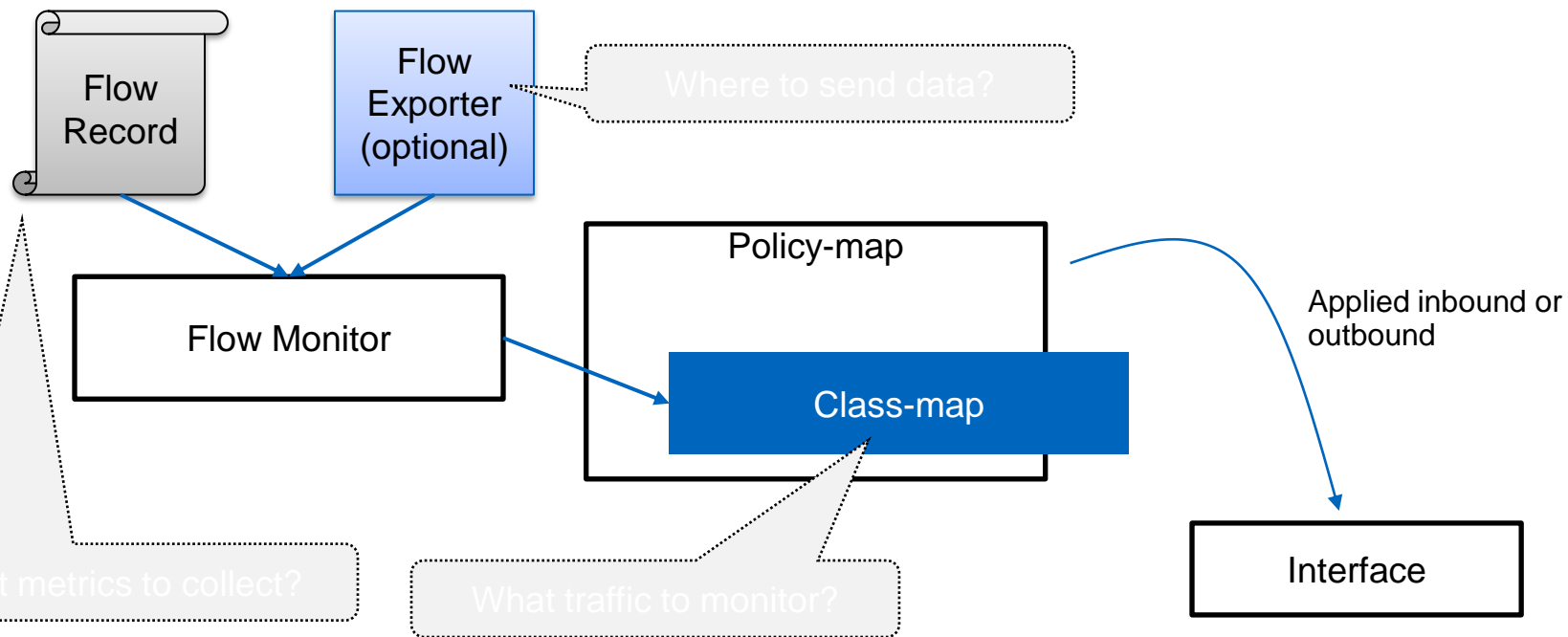
Visit us online after the conference for full access to session videos and presentations.

[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)



**CISCO**™

# Performance Monitor Configuration



# Example Configuration – Flow Record

- Flow Record defines what metrics to collect and how to collect them (just like in Flexible NetFlow configuration)
- Performance monitor introduces  
`flow record type performance-monitor`
- Match field types perform aggregation towards that field.
  - `le`  
`match ipv4 source address`  
`match ipv4 destination address`  
  
will create a unique entry per src-dst combinations
- Built-in ‘default-rtp’ and ‘default-tcp’ flow records

```
flow record type performance-monitor default-rtp-pt-name
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
match policy performance-monitor classification hierarchy
collect routing forwarding-status
collect ipv4 dscp
collect ipv4 ttl
collect transport packets expected counter
collect transport packets lost counter
collect transport packets lost rate
collect transport event packet-loss counter
collect transport rtp jitter mean
collect transport rtp jitter minimum
collect transport rtp jitter maximum
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect counter bytes rate
collect timestamp interval
collect application name
collect application media bytes counter
collect application media bytes rate
collect application media packets counter
collect application media packets rate
collect application media event
collect monitor event
collect transport rtp payload-type
```

# Example Configuration – Monitor

- Flow monitor pulls together the flow record, exporter, and specific cache management configurations (just like Flexible NetFlow)
- Special type of flow monitor  
flow monitor type performance-monitor
- (optional) Flow exporter configures how the NetFlow exporting is done
- Policy map specifies which traffic to monitor (via class-map), how to monitor (via monitor), and any per-class threshold crossing actions
- Typed policy-map (performance monitor)

```
flow exporter mn-campus-sampler
 destination 10.1.160.37
 source Loopback0
 transport udp 2055
 template data timeout 60
 option c3pl-class-table
 option c3pl-policy-table
 option interface-table
 option application-table
 option sub-application-table
 !
flow monitor type performance-monitor default-rtp-pt-name
 record default-rtp-pt-name
 exporter mn-campus-sampler
 cache timeout synchronized 10 export-spread 5
 history size 10
 !
policy-map type performance-monitor rtp-traffic-name
 class VOIP
  flow monitor default-rtp-pt-name
  react 1 transport-packets-lost-rate
  threshold value ge 1.00
  alarm severity error
  action syslog
 class VIDEO-CONF
  flow monitor default-rtp-pt-name
```

# Example Configuration – Interface Attachment

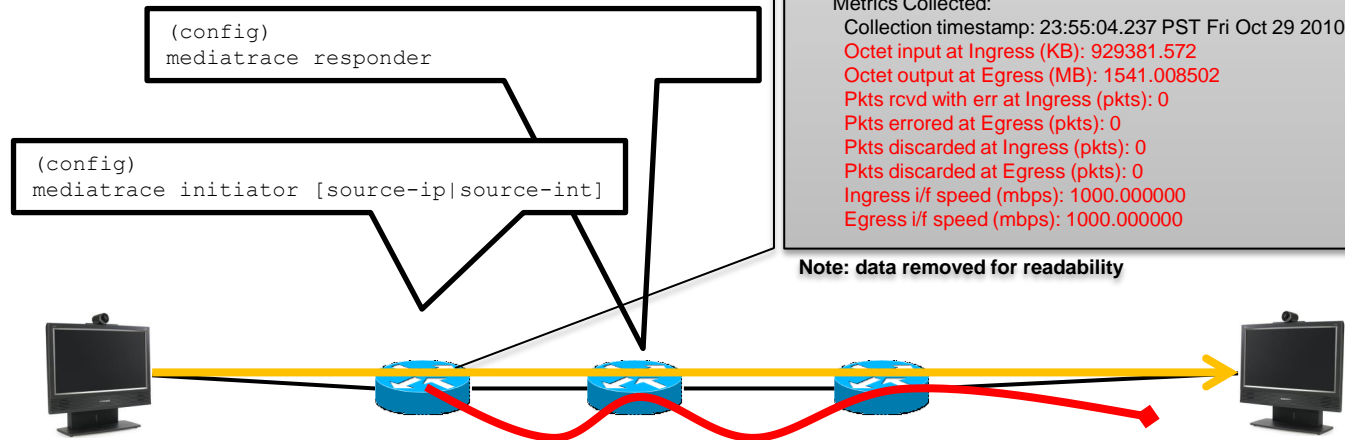
- Finally, policy map is applied to interface
- Note typed policy is used
- Direction of monitoring (input|output) selectable for some platforms

```
interface gigabitEthernet 0/1  
  service-policy type performance-monitor input rtp-traffic-name
```



# Mediatrace System Profile Session

- **Preconfigured mediatrace session- system profile**
  - session 2, 60 sec recurring (see notes for config)
  - Poll could also be used



```
initiator#show mediatrace session stats 2
Session Index: 2
Global Session Id: 86197709
Session Operation State: Active
Operation time to live: Forever
Data Collection Summary:
...
Detailed Report of collected data:
Last Route Change Timestamp:
Route Index: 0
Number of Mediatrace hops in the path: 2

Mediatrace Hop Number: 1 (host=responder1, ttl=254)
Metrics Collection Status: Success
Reachability Address: 10.10.12.3
Ingress Interface: Gi0/1
Egress Interface: Gi0/2
Mediatrace Hop Number: 2 (host=responder2, ttl=253)
Metrics Collection Status: Success
Reachability Address: 10.10.34.3
Ingress Interface: Gi0/1
Egress Interface: Gi0/2
Metrics Collected:
Collection timestamp: 23:55:04.237 PST Fri Oct 29 2010
Octet input at Ingress (KB): 929381.572
Octet output at Egress (MB): 1541.008502
Pkts rcvd with err at Ingress (pkts): 0
Pkts errored at Egress (pkts): 0
Pkts discarded at Ingress (pkts): 0
Pkts discarded at Egress (pkts): 0
Ingress i/f speed (mbps): 1000.000000
Egress i/f speed (mbps): 1000.000000
```

# MSI Mediatrace

- Initiate / delete a mediatrace from end system
- Responds to mediatrace
- Get a list of active mediatrace sessions, config, and status

Start mediatrace



Only 'mediatrace responder' needed in network



```
<MTReportPerRequest>
  <RequestTimestamp>*13:05:46.981 UTC Tue Nov 29 2011</RequestTimestamp>
  <RequestStatus>Completed</RequestStatus>
  <TotalHopResponded>4</TotalHopResponded>
  <HopsWithValidReport>3</HopsWithValidReport>
  <HopsWithErrorReport>0</HopsWithErrorReport>
  <HopsWithNoDataRecord>1</HopsWithNoDataRecord>
  <TotalMediatraceHops>4</TotalMediatraceHops>
  <MediatraceHop>
    <HopNum>0</HopNum>
    <HopName>joyzhang-mac-ubuntu11</HopName>
    <TTL>255</TTL>
    <MetricsCollectionStatus>Fail</MetricsCollectionStatus>
    <ReachabilityAddress>144.254.20.86</ReachabilityAddress>
    <IngressInterface>None</IngressInterface>
    <EgressInterface>eth1</EgressInterface>
  </MediatraceHop>
  <MediatraceHop>
    <HopNum>1</HopNum>
    <HopName>msit-rt1</HopName>
    <TTL>251</TTL>
    <MetricsCollectionStatus>Success</MetricsCollectionStatus>
    <ReachabilityAddress>10.51.40.193</ReachabilityAddress>
    <IngressInterface>Gi0/0</IngressInterface>
    <EgressInterface>Gi0/1</EgressInterface>
    <VMTCPMetrics>
      <FlowSamplingStartTimestamp>*13:10:00.000 UTC Tue Nov 29
2011</FlowSamplingStartTimestamp>
      <LossOfMeasurementConfidence>>false</LossOfMeasurementConfidence>
      <MediaStopEventOccurred>>false</MediaStopEventOccurred>
      <IPPacketDropCount>0</IPPacketDropCount>
      <IPByteCount>52</IPByteCount>
      <IPPacketCount>1</IPPacketCount>
      <IPByteRate>5</IPByteRate>
      <PacketDropReason>0</PacketDropReason>
      <IPDSCP>0</IPDSCP>
      <IPTTL>60</IPTTL>
      <MediaByteCount>0</MediaByteCount>
      <TCPConnectRoundTripDelay>4294967295</TCPConnectRoundTripDelay>
      <TCPLostEventCount>0</TCPLostEventCount>
    </VMTCPMetrics>
  </MediatraceHop>
</MTReportPerRequest>
</mt-report>
```



**CISCO** <sup>TM</sup>