Medianet Overview

Aamer Akhter / aa@cisco.com
Medianet Program

Apr 1, 2014

What is Medianet?

Medianet is:

- An architecture for successful deployment of multiple media and business applications
- Medianet is NOT a product, SKU, or a single feature.

Medianet solutions include:

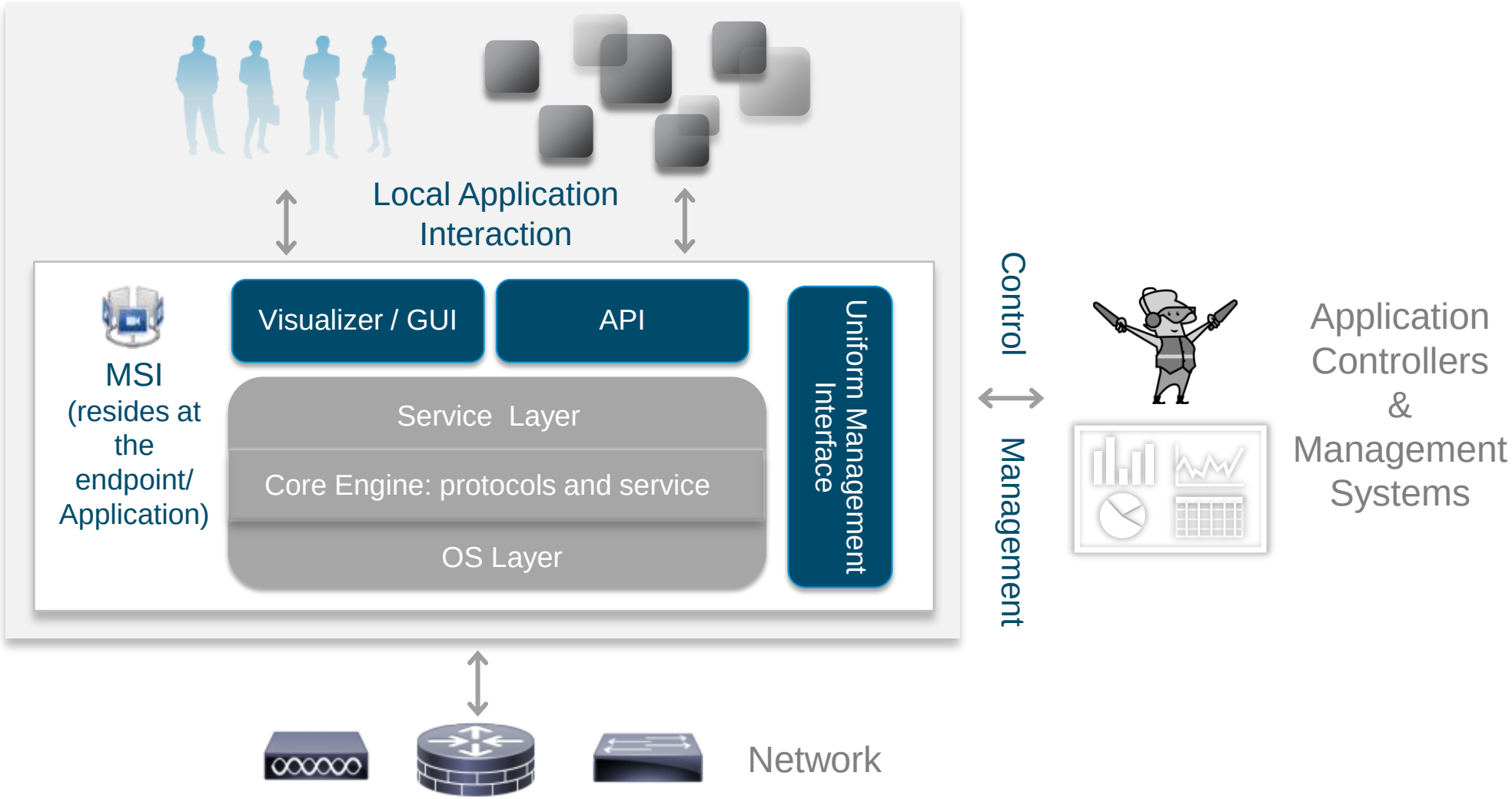
- Automatic, plug & play deployment
- Media performance monitoring, troubleshooting and capacity planning
- Media Awareness for bandwidth management
- End system awareness

Medianet solutions:

- Include compliant products and features in both Smart Endpoints/Applications and Smart Network Infrastructure
- DO NOT REQUIRE an entirely end-to-end Cisco network with medianet enabled in every hop

Media Services Interface (MSI)

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



MSI on Endpoints

- Digital Media Player
  - •Location
  - •Auto-Configuration

2010

2011

- IP Surveillance Camera
- WebEx Meeting Client
  - •+ Monitoring
  - •+ Session Visibility

- TelePresence
  - •+ Monitoring
  - •+ Management
- Jabber for Windows
  - •+metadata

2012

2013/2014

- Jabber for Mac
  - •+metadata
- Jabber for Windows
  - Local DSCP marking

MSI on TelePresence Hard Endpoints

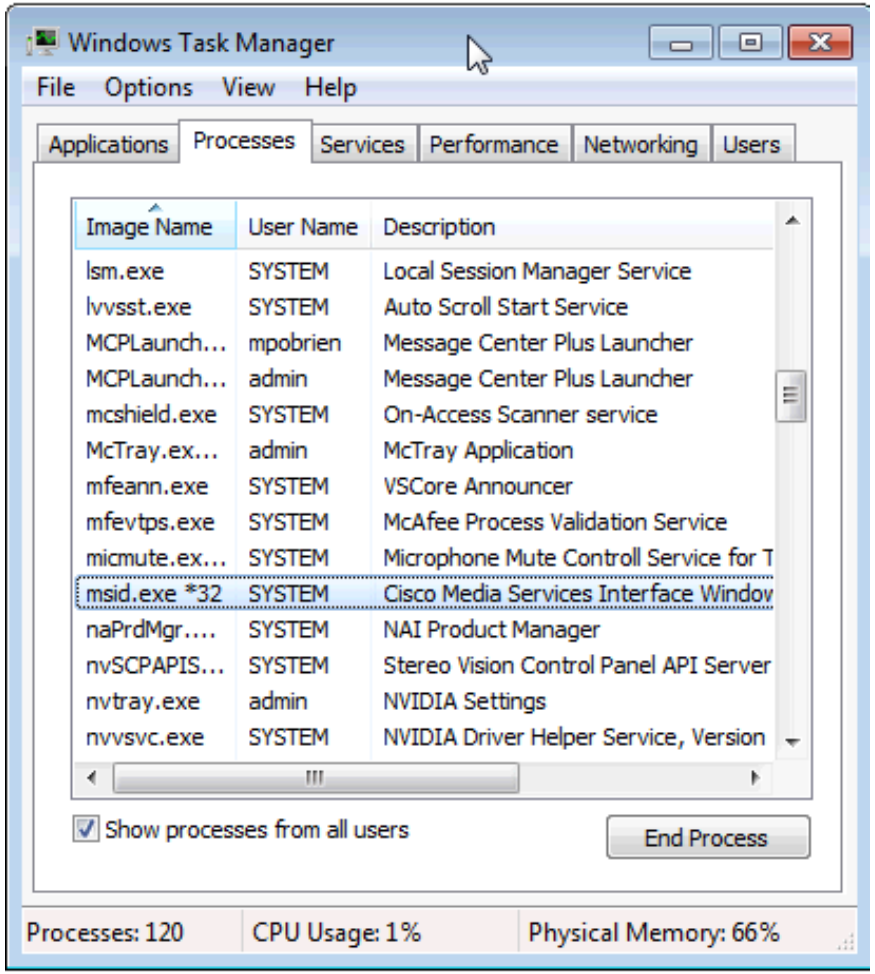
- Embedded in SW install
- EX, C, MX, SX with TC6.0+ and TE6.0+

  MSI http(s) username/password authentication synchronized with web/CLI

- TX, CTS500-32 TX6.0+

  MSI http(s) username/password authentication uses ‘misuser’ / ‘cisco’

MSI on Soft Client



MSI running as a service in Windows platforms

MSI Soft Platforms: Windows, MacOS

MSI Applications: Jabber (9.0(1)), WebEx (WBS28)

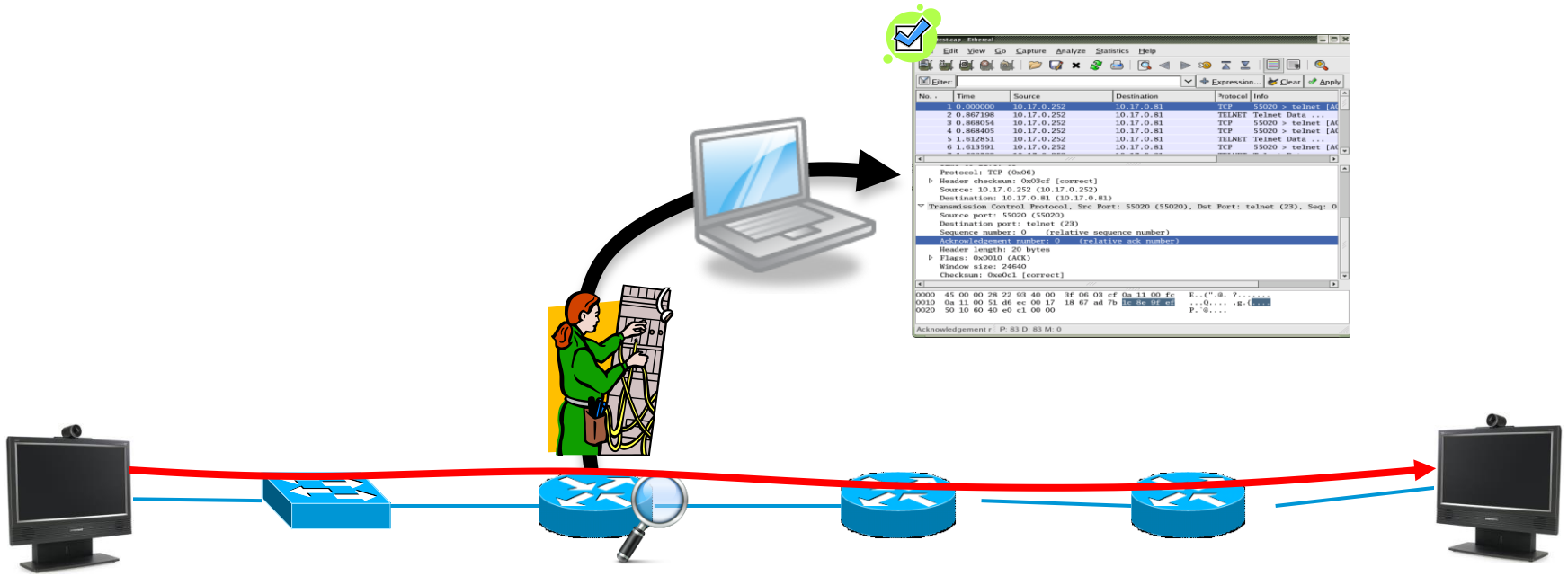
Coming soon to: Apple iOS and Android

Note: MSI needs to be explicitly installed on Windows/MacOS

Performance Monitor

Life with Dedicated Protocol Analyzers

- Wireshark and other protocol analyzers 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.

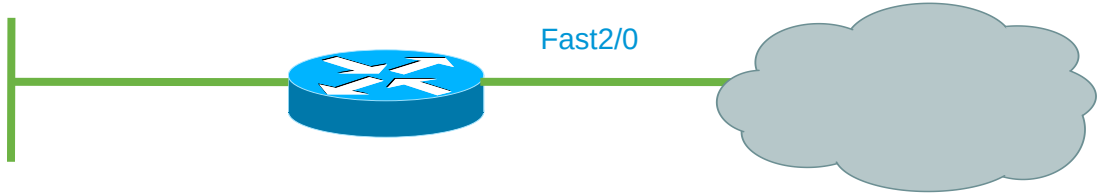


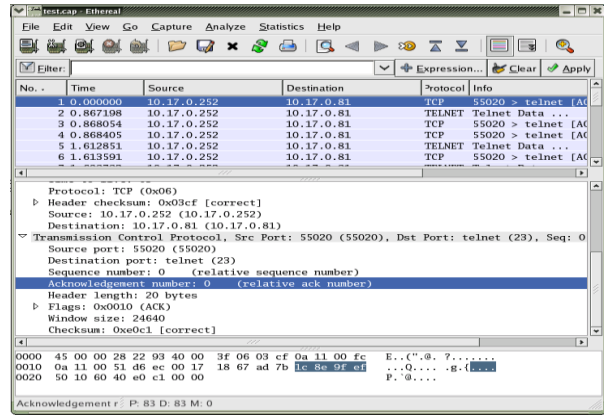
IP Traffic Export, Capture & Analyze

- Capture packets locally to buffer on router
- Store to flash, USB, FTP, TFTP for analysis in protocol analyzer

  IOS XE Cat 4k Sup 7E & Sup 7L-E (XE 3.3.0 SG) include built in Wireshark decode capability
- Capture does not add traffic to network

```
LY-2851-8(config)#ip traffic-export profile test mode capture
LY-2851-8(config)#int fast 2/0
LY-2851-8(config-if)#ip traffic-export apply test

LY-2851-8#traffic-export interface fast2/0 start
LY-2851-8#traffic-export interface fast2/0 stop
LY-2851-8#traffic-export interface fast2/0 copy ftp://10.17.0.252/images/test.cap
```



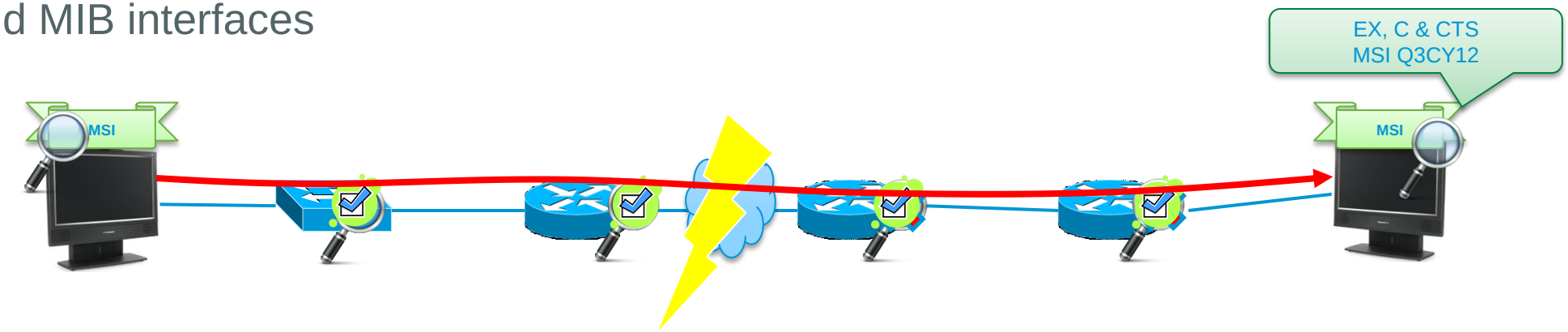


Performance Monitor

Router/Switch/Endpoint 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 synchronized 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, Polycom, Avaya, MS Lync, Cisco TelePresence (1xxx, 3xxx), CUVA, Jabber, MOVI, CP-9971, CP-7985, CP-7960 (audio only),

  Cisco Video Surveillance Cameras, WebEx (HTTPS), IPTV (VLC)

  Just plain web transactions (wget)







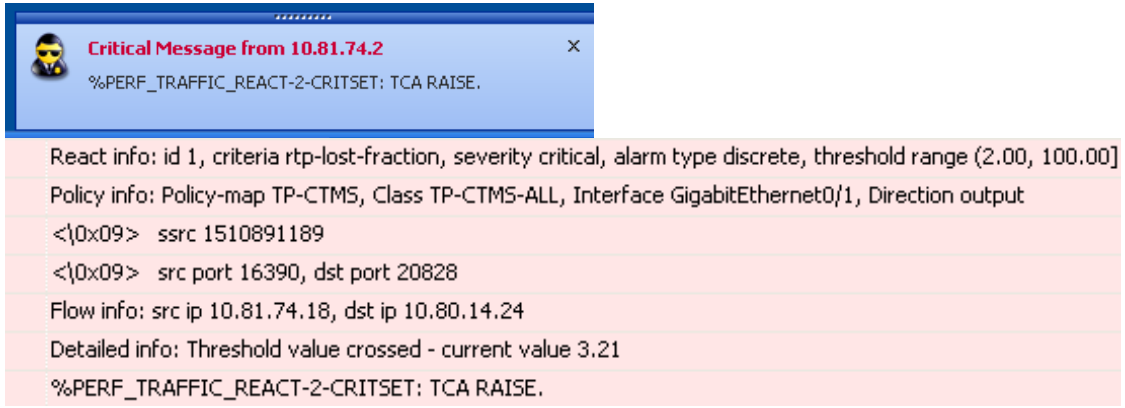


Thresholds & Alerts

- Metrics can be tested against thresholds to trigger actions

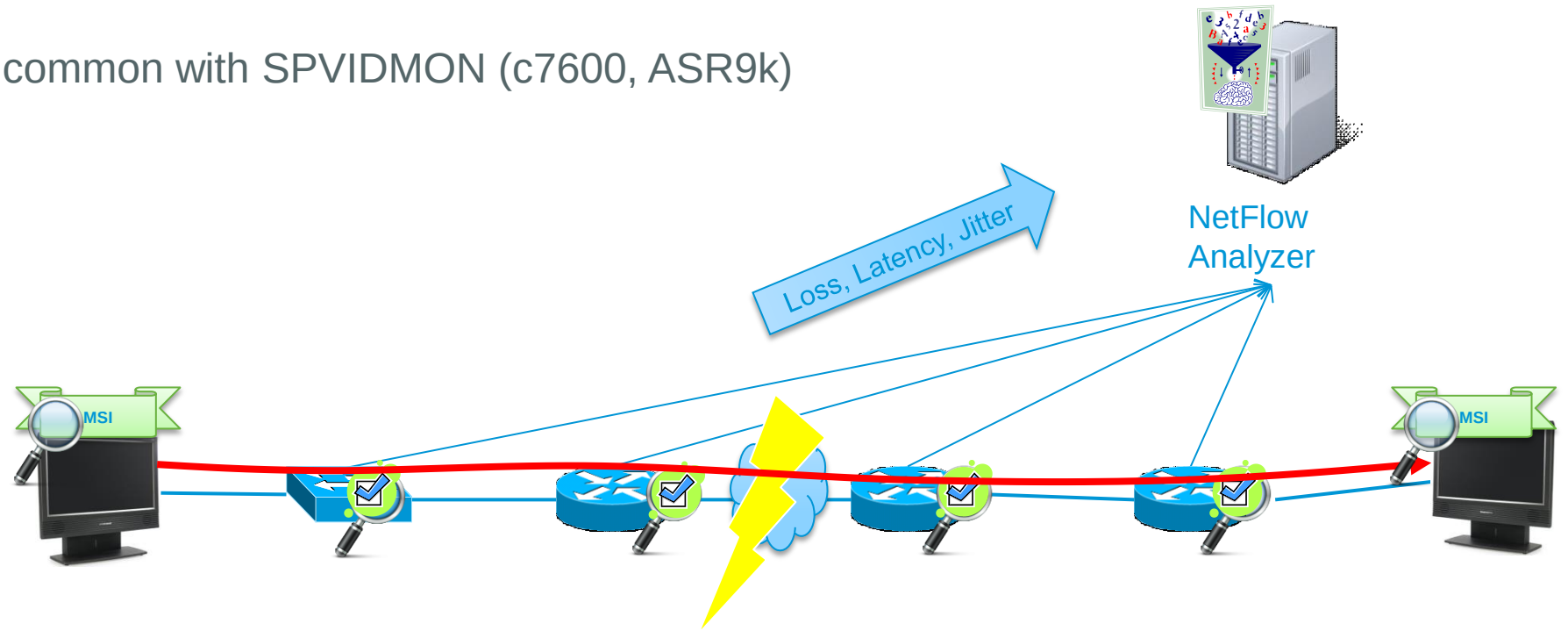
  Multi-level Alarm Raise/Clear, SNMP Traps, Syslog

SyslogWatcher



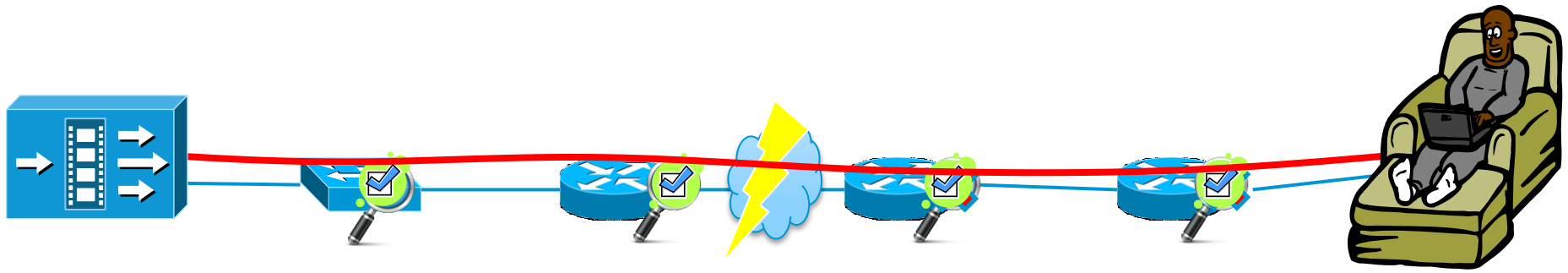
Reports - NetFlow & MIB

- NetFlow based metrics export from network
  - Can be based on flows, or aggregations of flows, etc.
  - Variety of uses: capacity planning, troubleshooting, baselining, etc.
- Historical interval (going back default 5 min) reports available on box via WSMA, MIB, mediatrace, and CLI
- MIB common with SPVIDMON (c7600, ASR9k)



Perf-Mon: TCP/HTTP Streaming

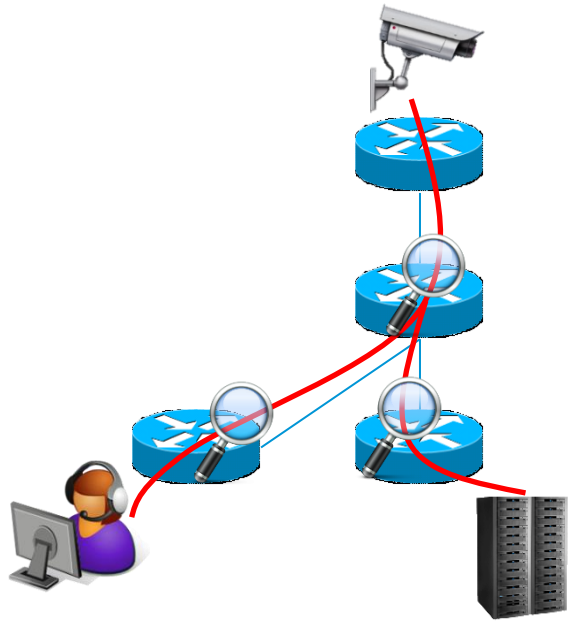
- Silverlight, Flash/RTMP, WebEx, etc all rely on TCP/HTTP based transport
- TCP level analysis allows for transport health metrics that help in issue notification & fault isolation.
  - Nodal level: TCP loss, out of order, packet/bit rate, window size
  - Session level: round-trip-time
- MSI on server/client allows for more detailed analysis.



Multicast Traffic & Performance Monitor

RTP Encapsulated Multicast Traffic

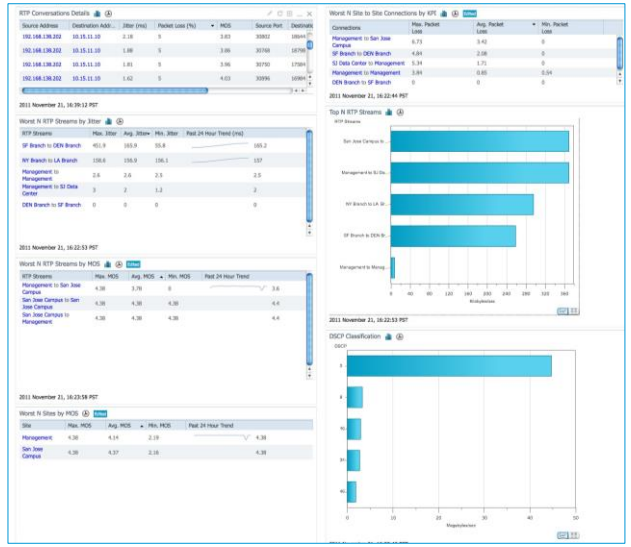
- RTP measurements applicable for unicast and multicast
- Examples of Applications
  - Video Surveillance
  - Digital Video Broadcasts (ETV/IPTV)
  - Streaming Video (WMV)
- Non-RTP: Constant Bit Rate monitoring and presence monitoring



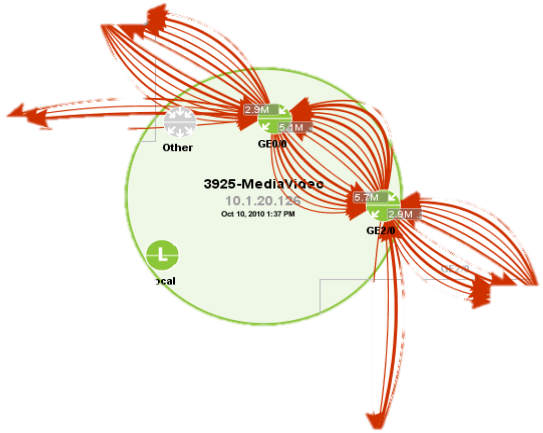
More info: CDN Partners Page:
http://developer.cisco.com/web/mnets/partners

Performance Monitor Management

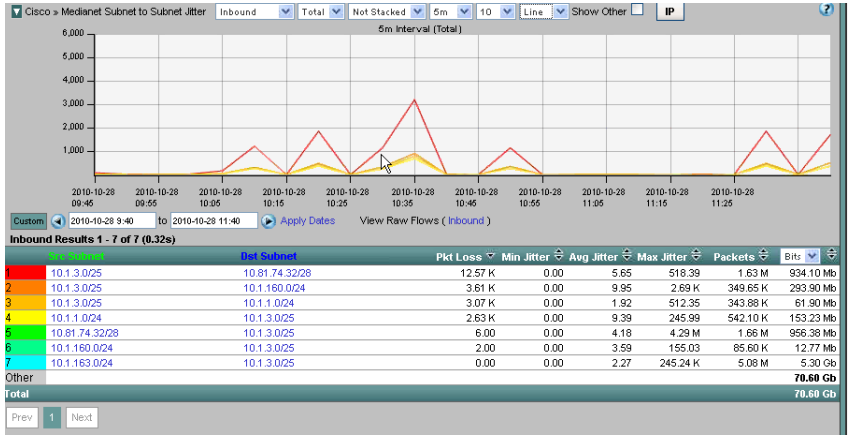
Application	Type	Network, Endpoint/MSI
Cisco Prime Infrastructure w/Assurance License (includes configuration)	Network	N
Cisco Prime Collaboration Assurance	Application	N,E
ActionPacked LiveAction (configuration also planned)	Network	N,E
Plixer Scrutinizer	Network	N
SevOne SevOneNMS	Network	N
CA/NetQoS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



Cisco Prime Infra



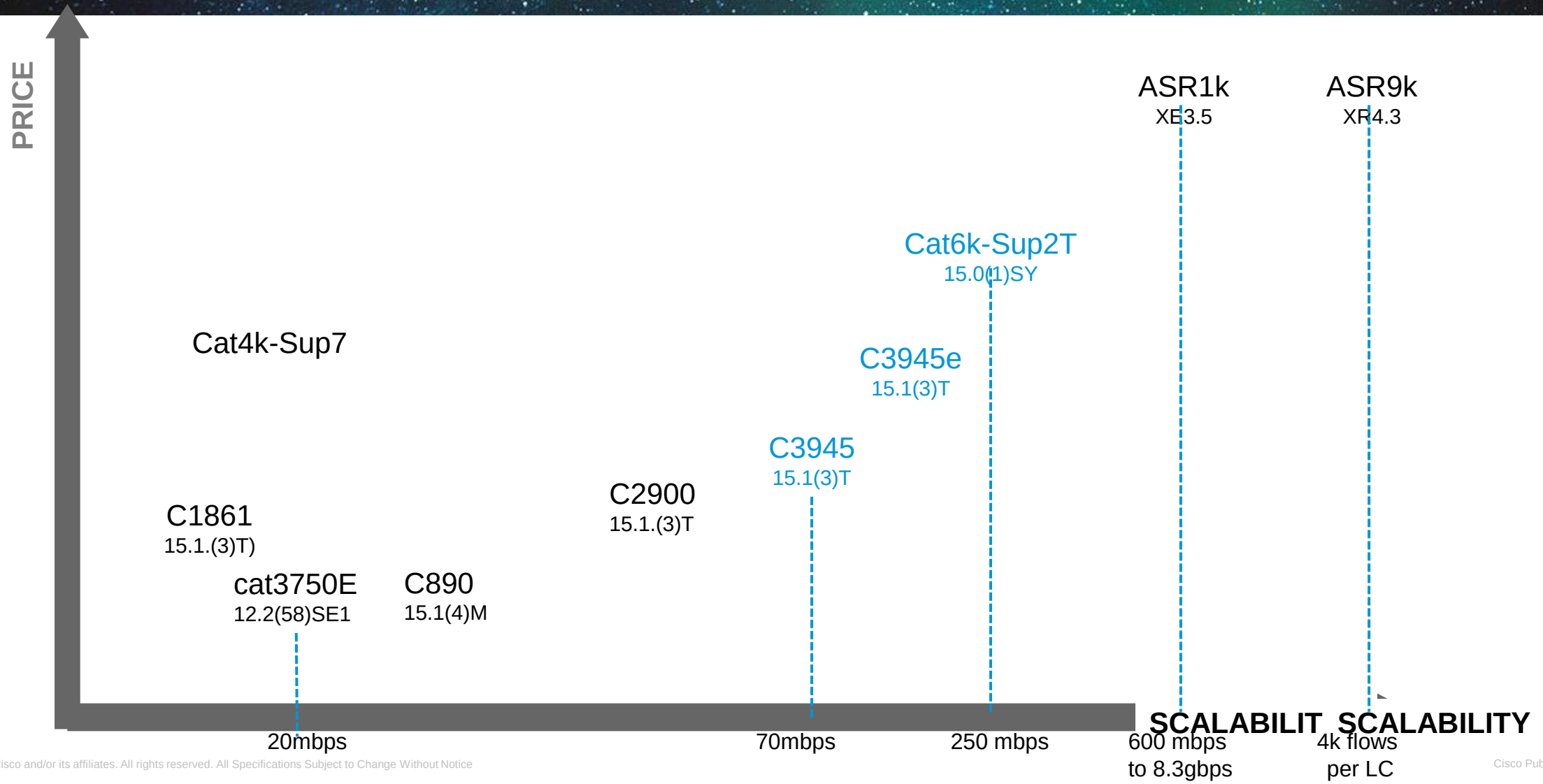
ActionPacked



Plixer

Platform Wide Scalability

Performance Monitor

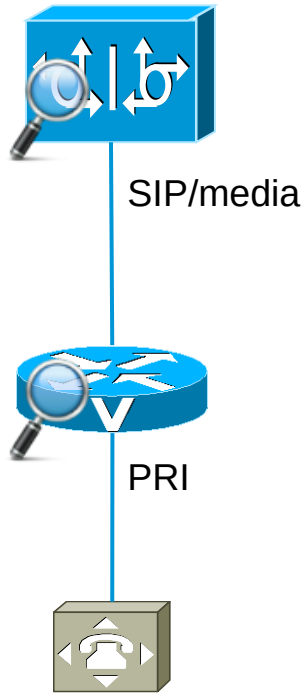


Audio Quality Metrics (AQM) on CUBE

- 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 ]
```

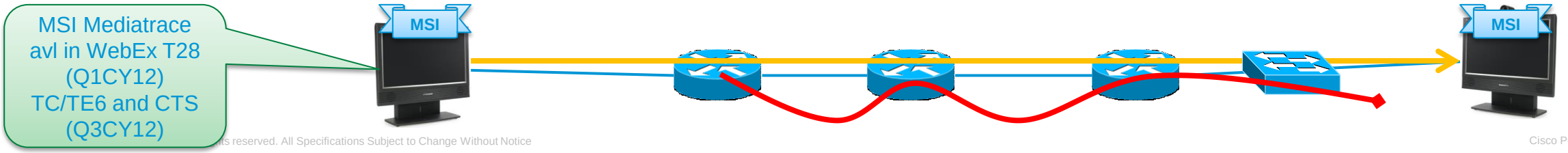
Mediatrace

Dynamic Monitoring with Mediatrace

Released Nov 2010 15.1(3)T

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 behavior
  - 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

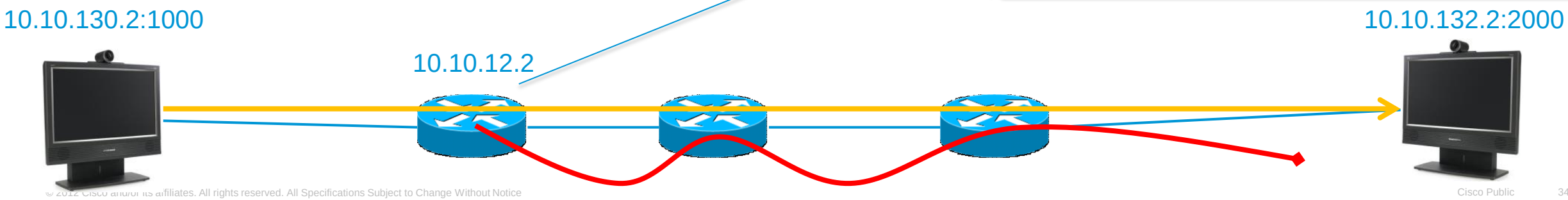
- Mediatrace perf-mon poll

  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
```

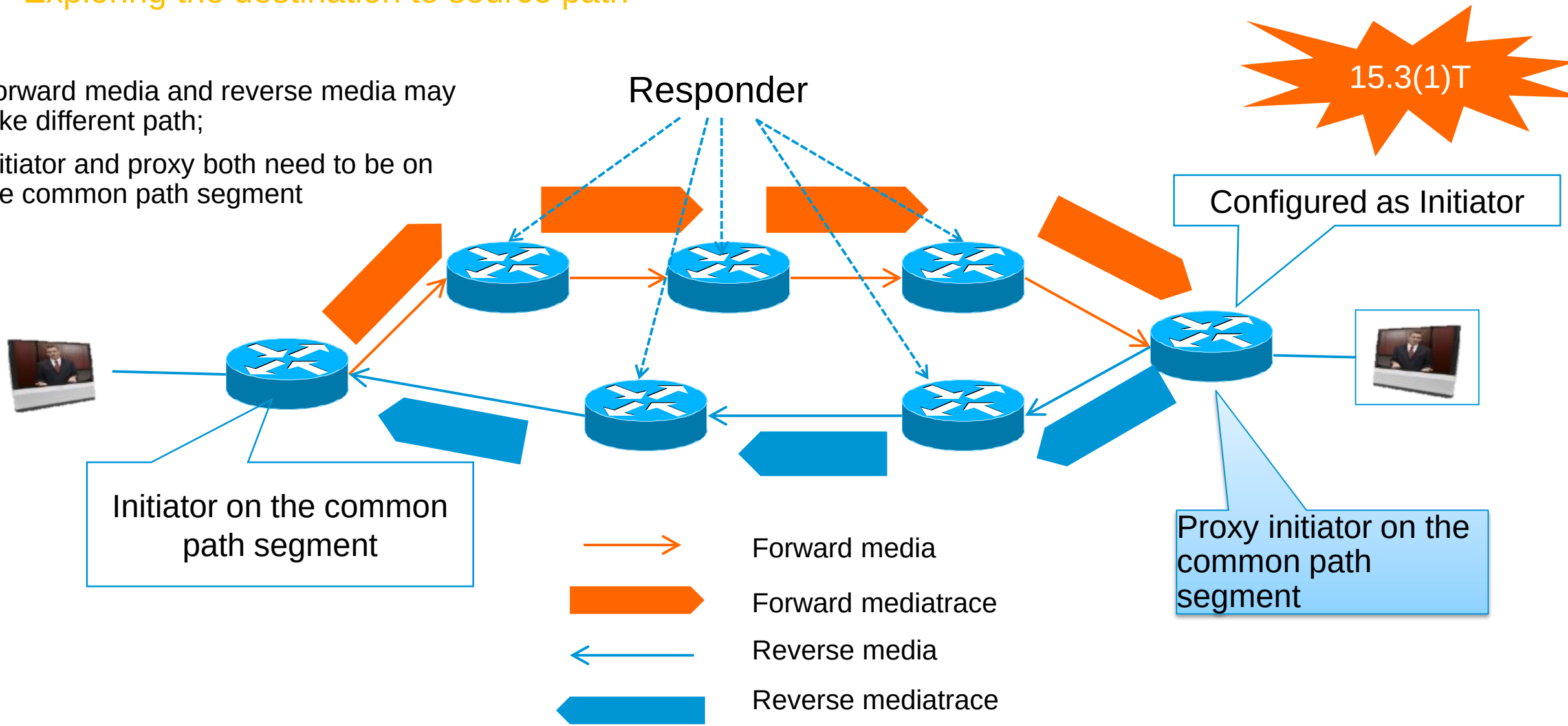


Reverse Mediatrace

Exploring the destination to source path

Forward media and reverse media may take different path;

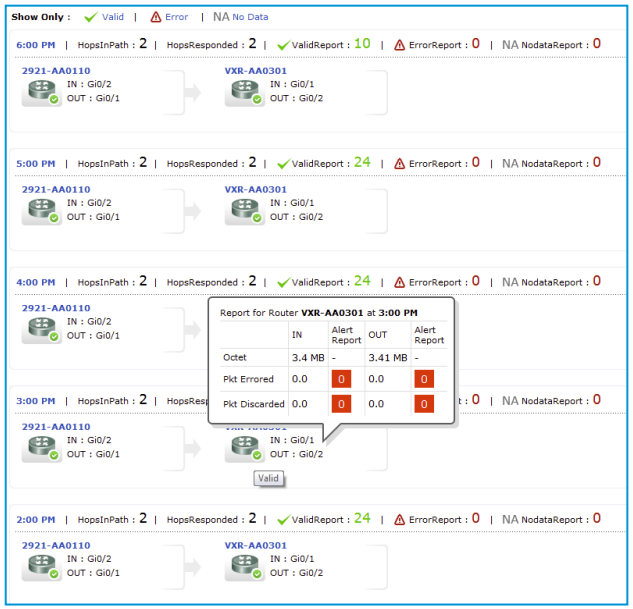
Initiator and proxy both need to be on the common path segment



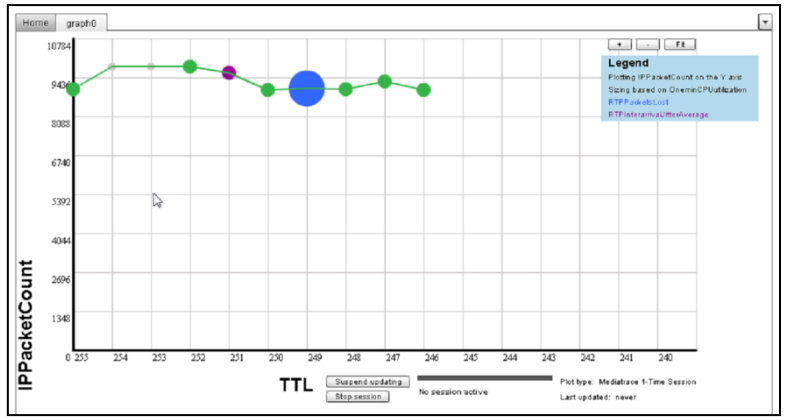
Network Management and Mediatrace

Cisco Prime Collaboration Assurance
Cisco Prime Infrastructure (Assurance license on top of Cisco Prime Infra)
ActionPacked LiveAction
ManageEngine NetFlow Analyzer

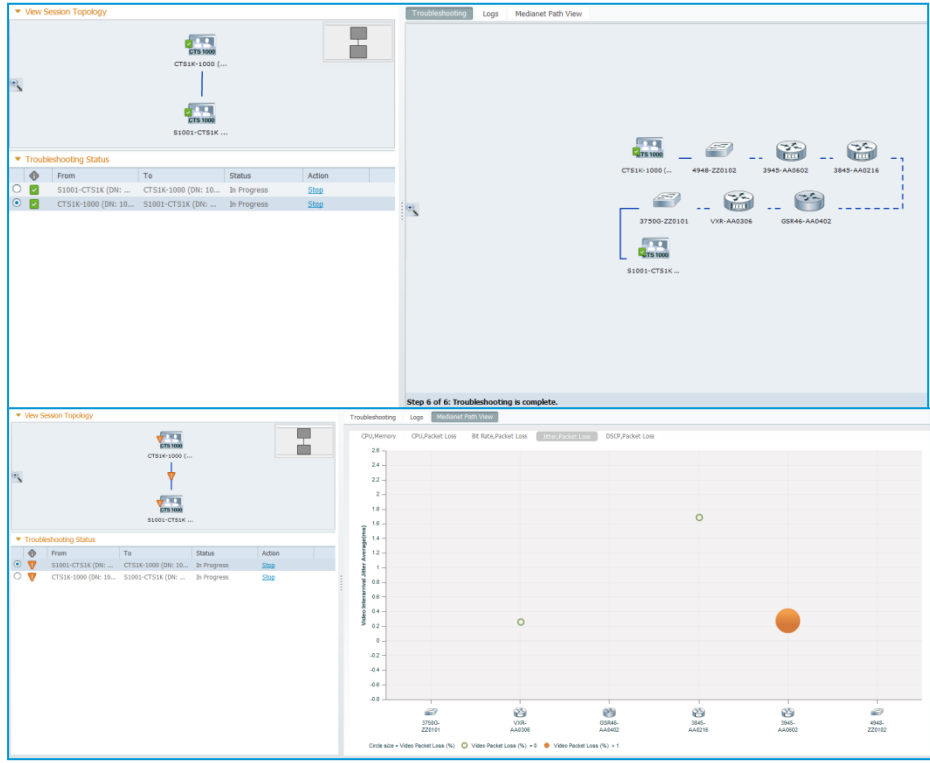
- Mediascope project (free open source)
  http://medianet.soureforge.net



ManageEngine



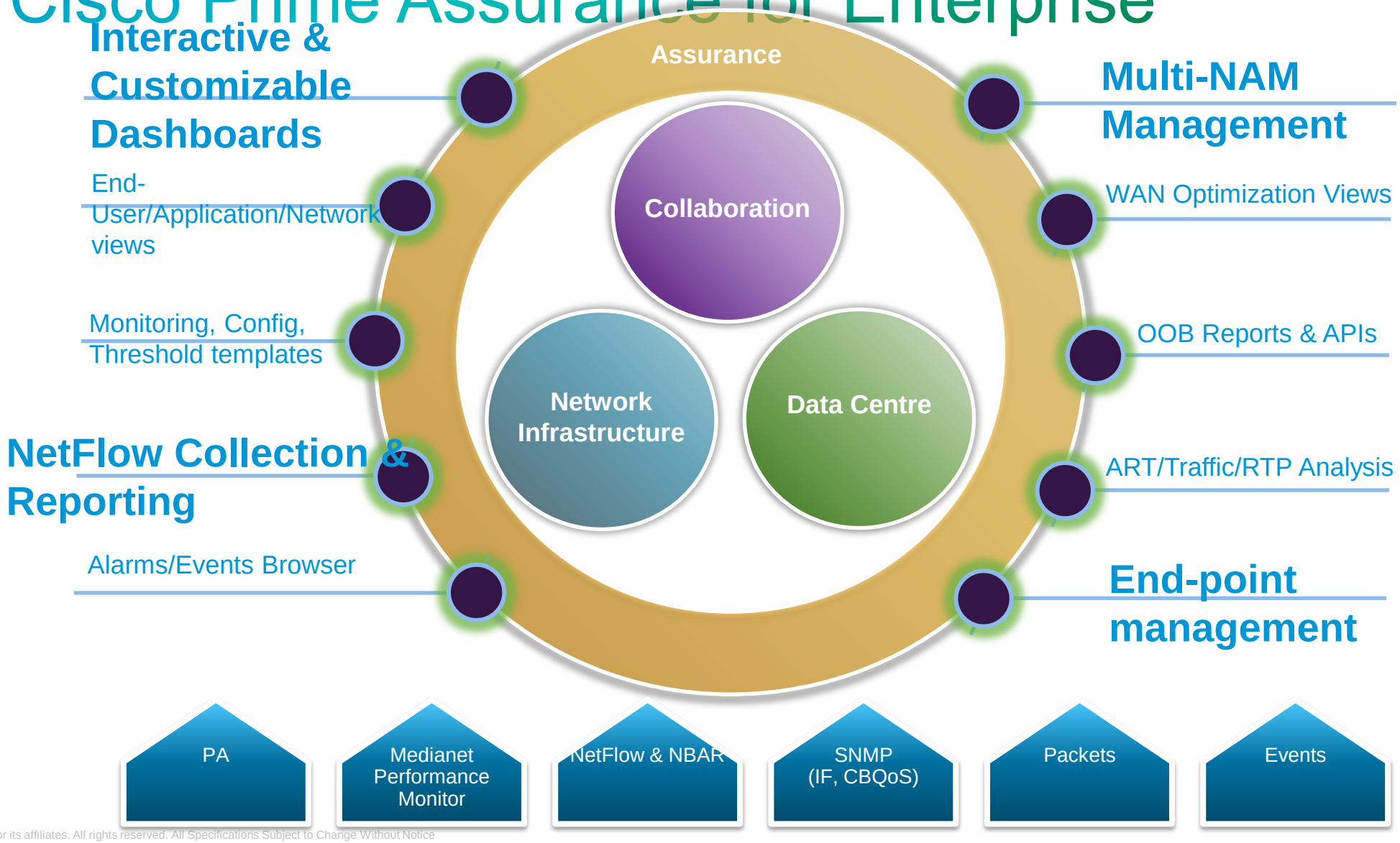
mediascope



Cisco Prime Collaboration

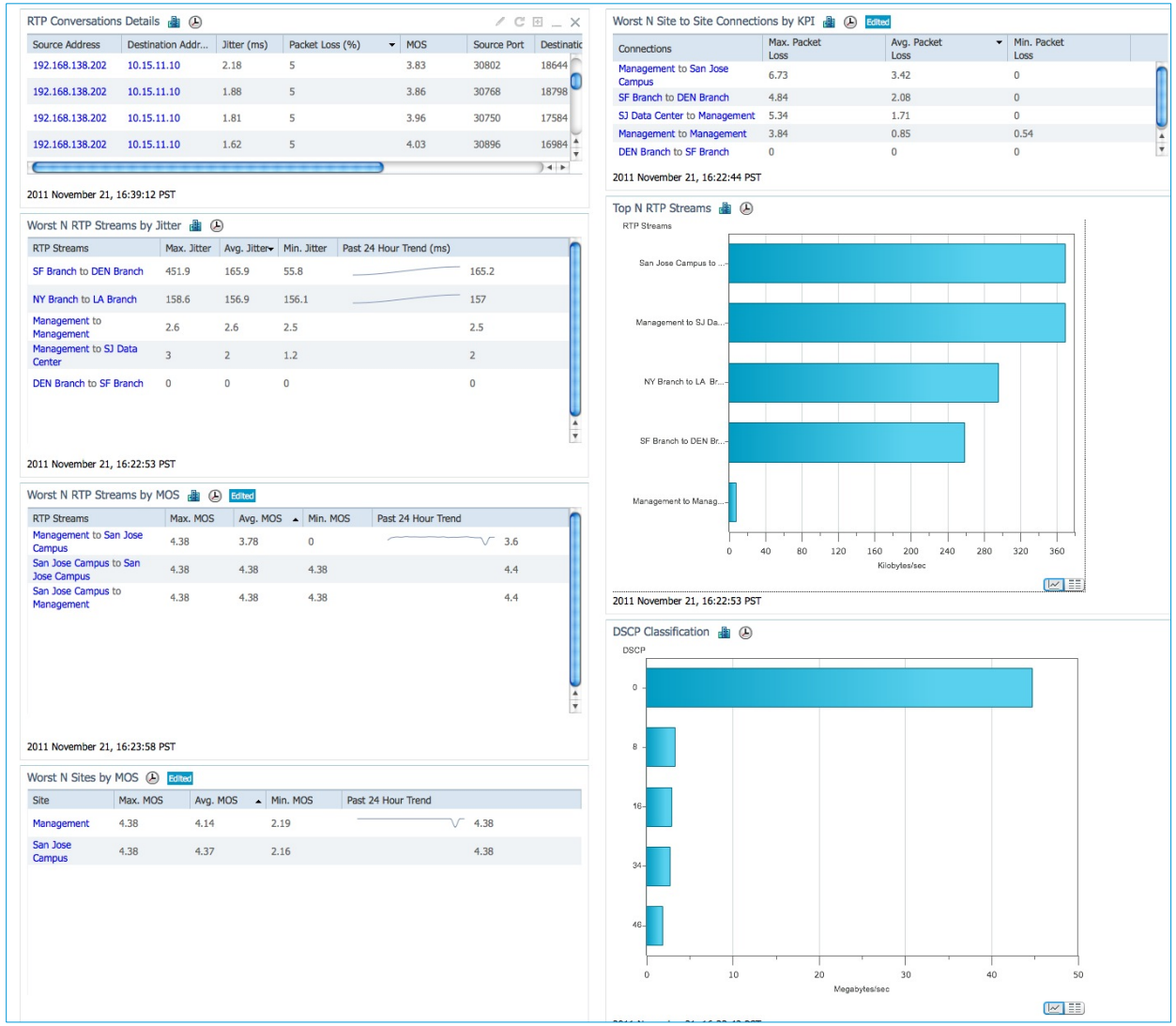
More info: CDN Partners Page: http://developer.cisco.com/web/mnets/partners

Cisco Prime Assurance for Enterprise



Prime Assurance: Voice/Video Dashboard

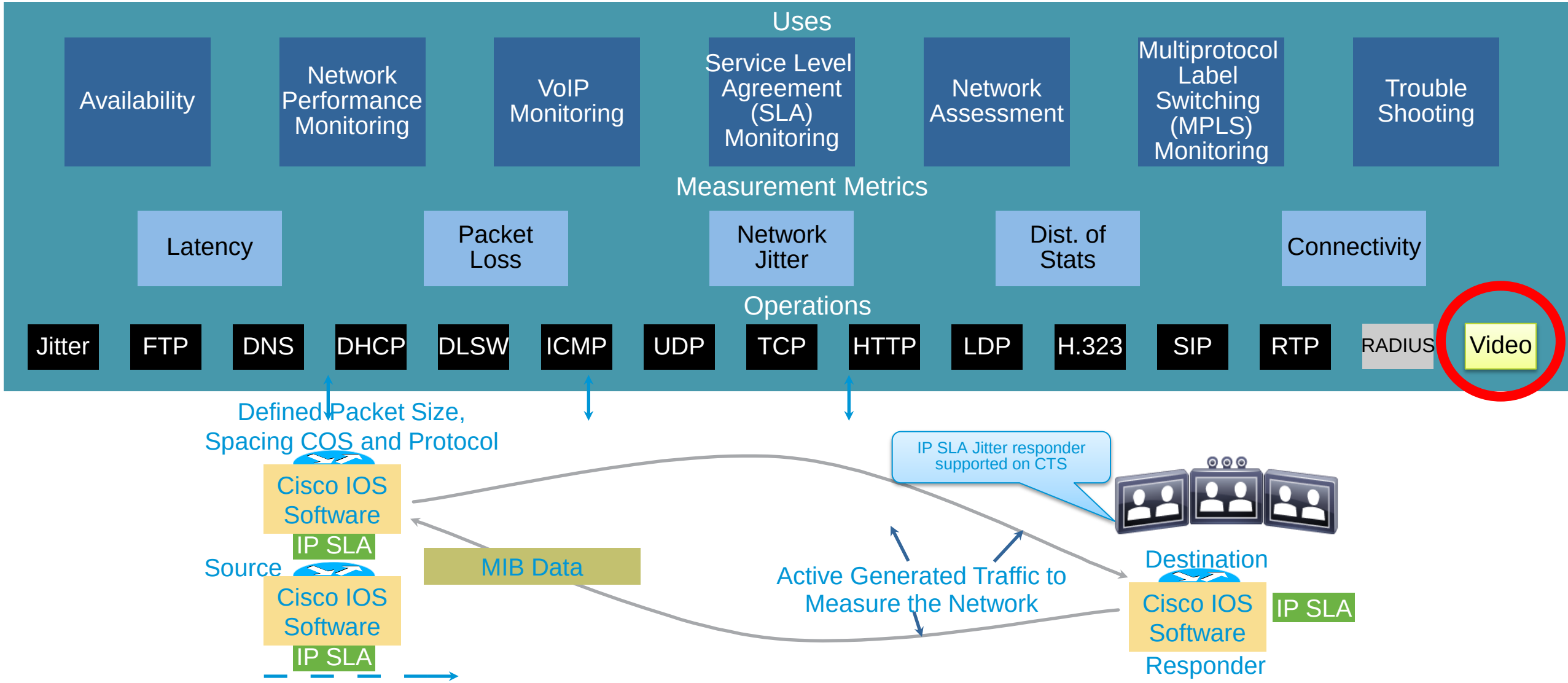
- DSCP Classification
- RTP Conversations Details
- Top N RTP Streams
- Voice Call Statistics
- Worst N RTP Streams by Jitter
- Worst N RTP Streams by Packet Loss
- Worst N RTP Streams by MOS
- Worst N Sites by MOS
- Worst N Site to Site Connection KPI



Synthetic Traffic

IPSLA Video Operation

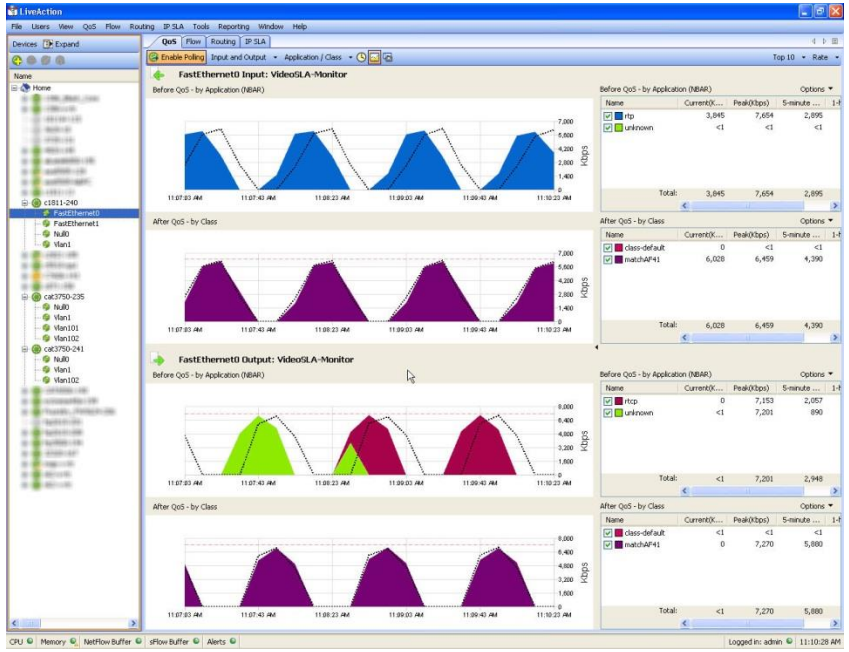
IP SLA: Synthetic Traffic Measurements



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

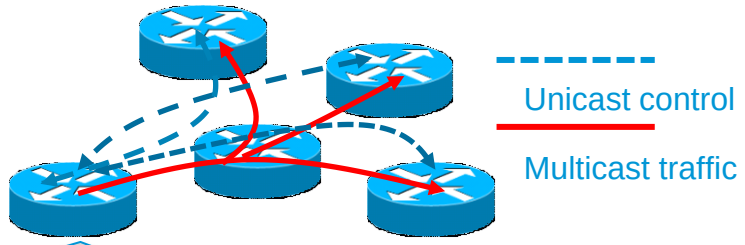


ActionPacked

IPSLA Multicast Support

Aug 2012

- IPSLA Multicast available: 15.2(4)M (Aug2012)
  - One Way Delay (NTP req)
  - One Way Jitter
  - Packet Loss
- Configuration is on IP SLA Sender
  - Have to specify each responder explicitly in endpoint-list
  - Responder becomes mcast receiver, IGMPv3 (G) and (S,G) behavior
- ISRG2, ISR4451X, ASR1k, CSR1000v, cat4k(sup7/6), c7600
- IPSLA VO Roadmap item

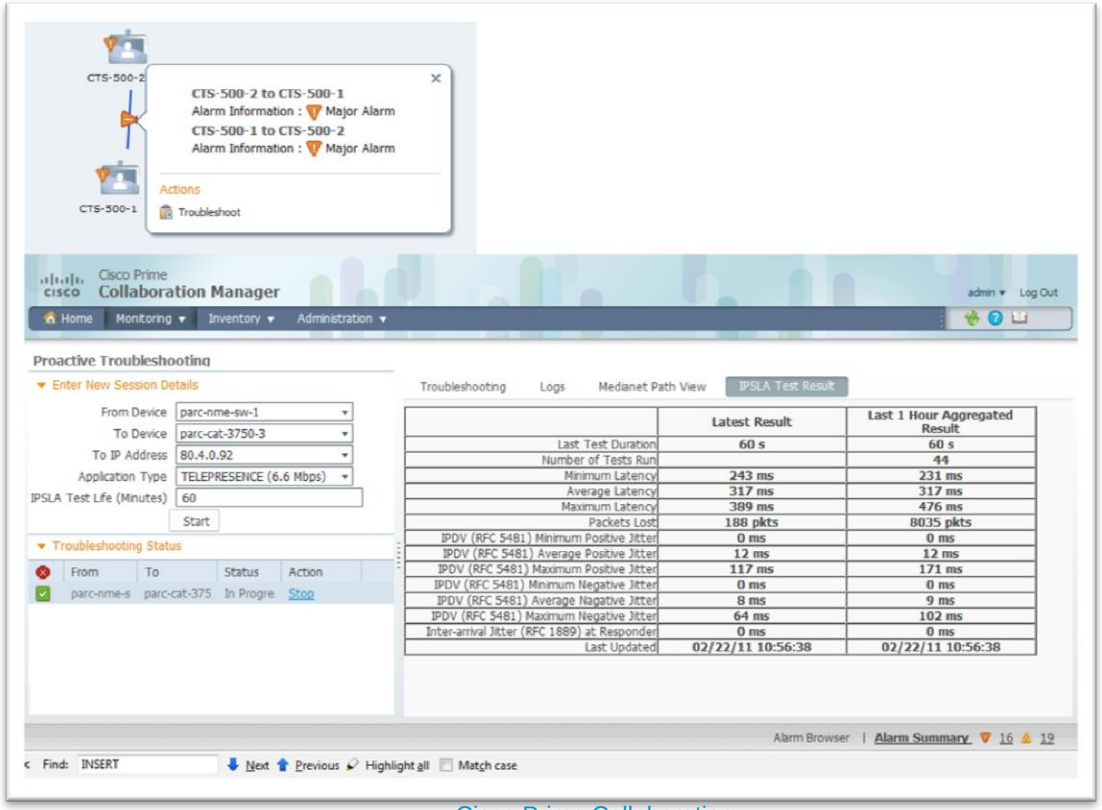



```
SLAsender(config)#ip sla endpoint-list type ip mylist
 ip-address 172.16.1.2,172.17.1.2 port 3800
SLAsender(config)#ip sla 1
 udp-jitter 224.1.1.1 4000 endpoint-list mylist source-ip 172.16.1.1 source-port 4500 num-packets 100 interval 25
```

Network Management for IPSLA VO

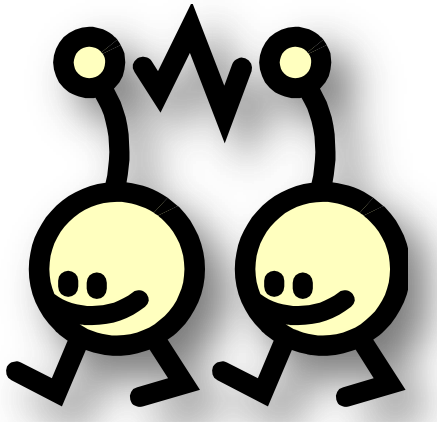
Application	Type
Cisco Prime Collaboration	Application
Cisco Prime LMS 4.1	Network
Cisco Prime Performance Manager 1.0.3	Network
ActionPacked LiveAction (configuration also planned)	Network
SevOne SevOneNMS	Network
14+ NMS application vendors engaged!	

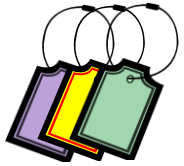
More info:
Cisco Prime LMS: cisco.com/go/lms
Cisco Prime CM: cisco.com/go/primecollaboration
Cisco Prime Performance Manager:
http://www.cisco.com/en/US/products/ps11715
CDN Partners Page:
http://developer.cisco.com/web/mnets/partners



Cisco Prime Collaboration Manager (IPSLA VO)

Media Awareness





Flow Attributes

- 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

Classification / Marking

- 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

- 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.

Video Application Marking

RFC 4594 DSCP Markings

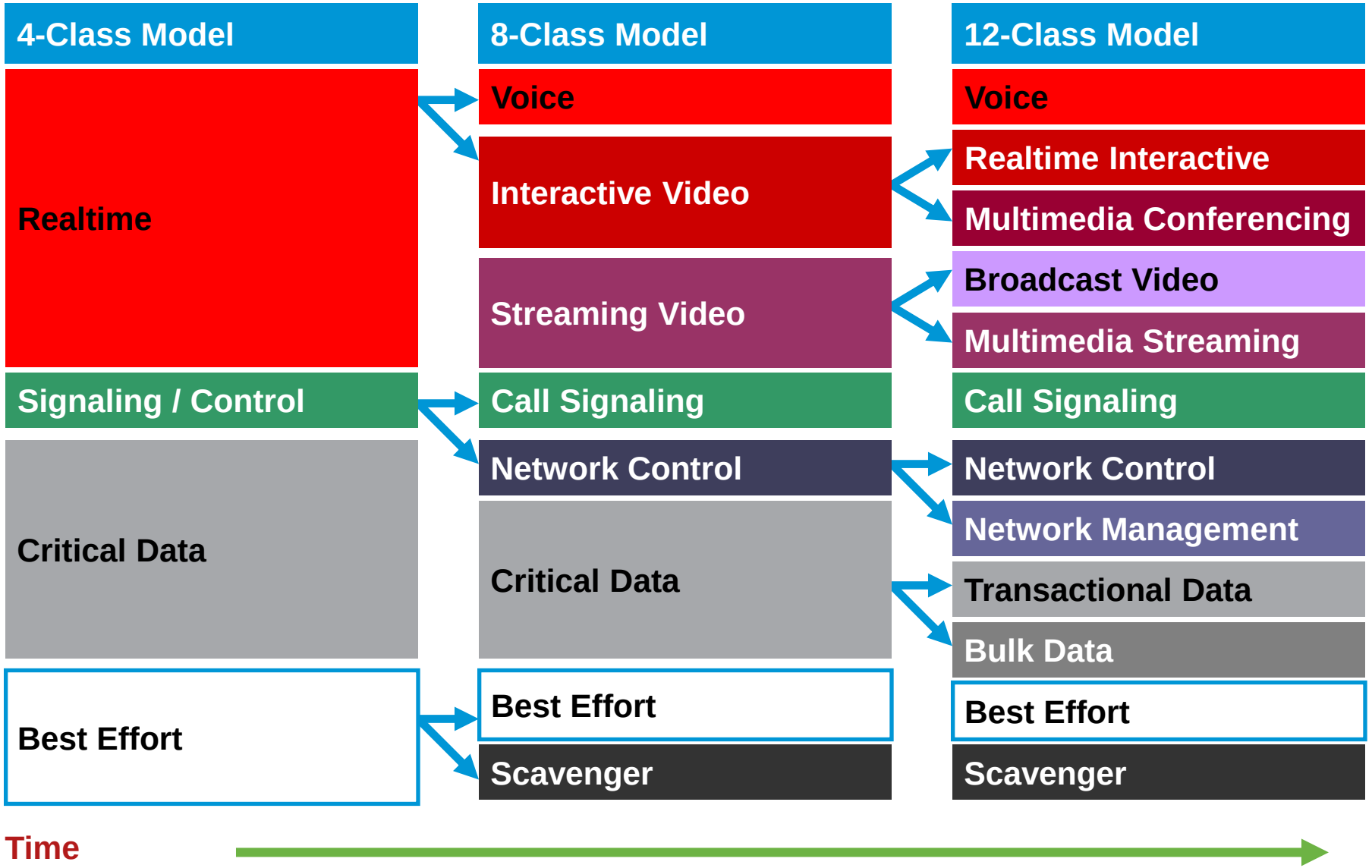
Application Class	PHB	Admission Control	Congestion Management & Congestion Avoidance	Video Applications
VoIP Telephony	EF	Required	Priority Queue (PQ)	
Broadcast Video	CS5*	Required	(Optional) PQ	Enterprise TV / IPVS
Real-Time Interactive	CS4	Required	(Optional) PQ	High End Video Conferencing
Multimedia 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)lQueue	YouTube / Xbox Live / iTunes / BitTorent/ etc.

How Many Classes of Service Do I Need?

Service Provider Plans

Capability of network devices

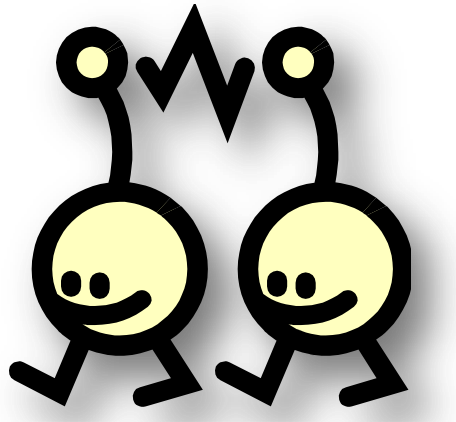
But always try to mark traffic along RFC4594 lines.



Defining Application Awareness

‘Application Awareness’ is…

A collection of techniques to detect different types of endpoints, media and application types (TelePresence, video surveillance, desktop collaboration and streaming media) in order to deliver the best experience.



Why Media Awareness?

Example Policies		Example Use Cases
	QoS	• Prioritize Voice & Video • Protect Business Critical Applications
	Monitoring	• Troubleshooting • SLA
	Routing	• Avoid Bandwidth upgrade by leverage the backup path • Protect Business Critical Applications
	Security	• Access Control • Firewall traversal

Soft Client Classification Methods

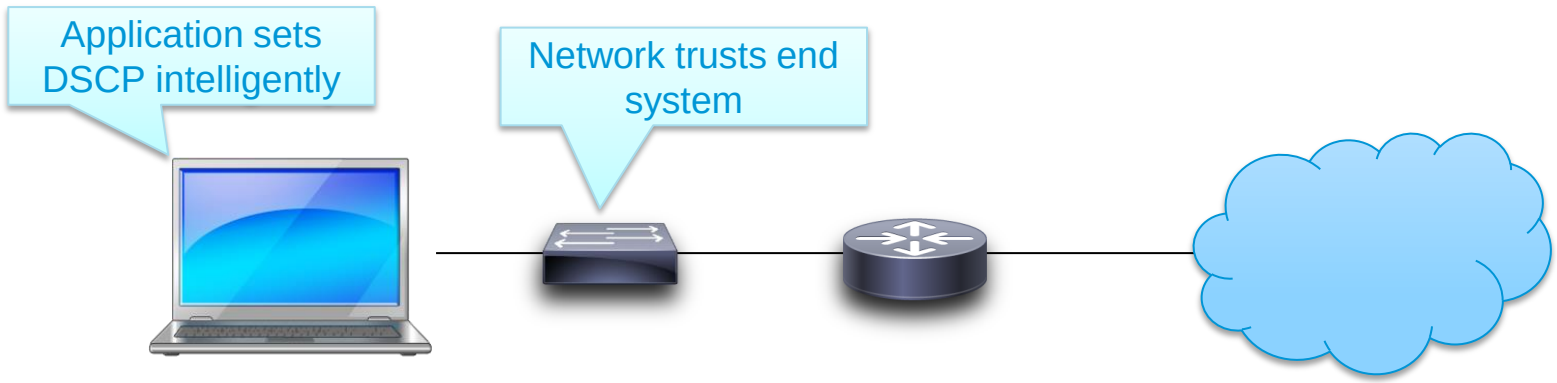
DSCP set directly by application on end system

Pro:

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

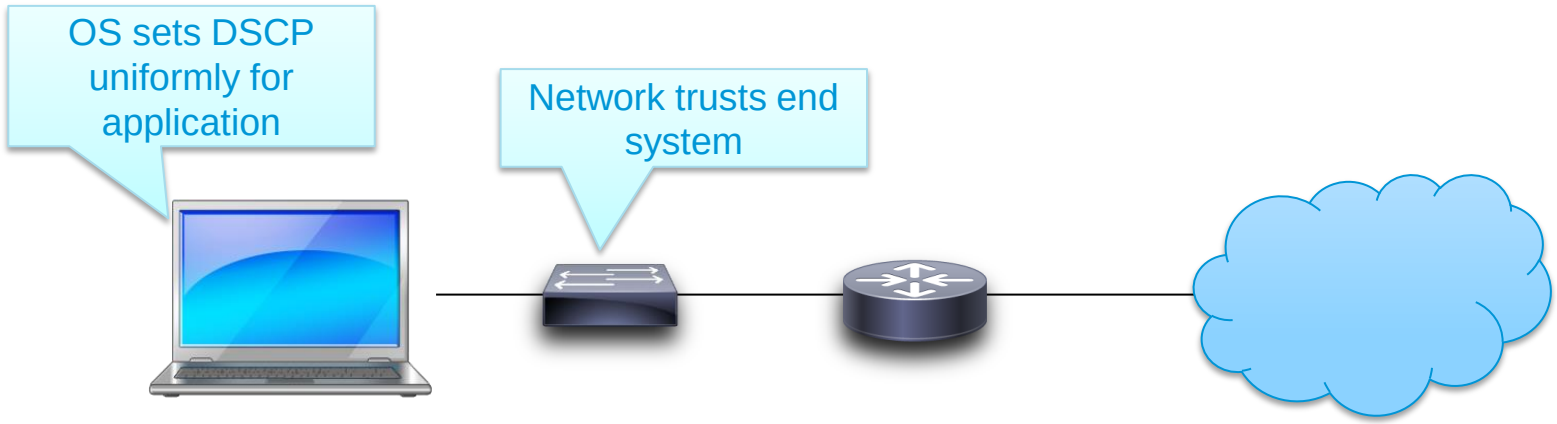
Con:

- 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

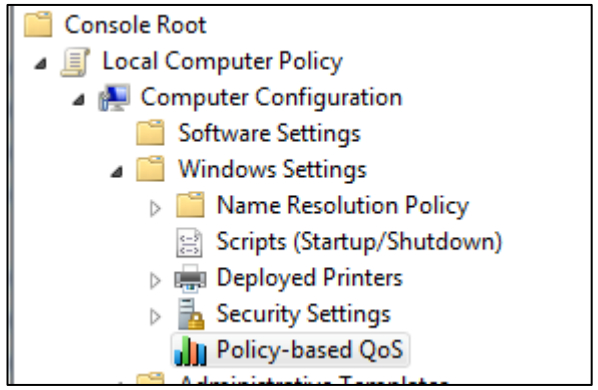


Soft Client Classification Methods

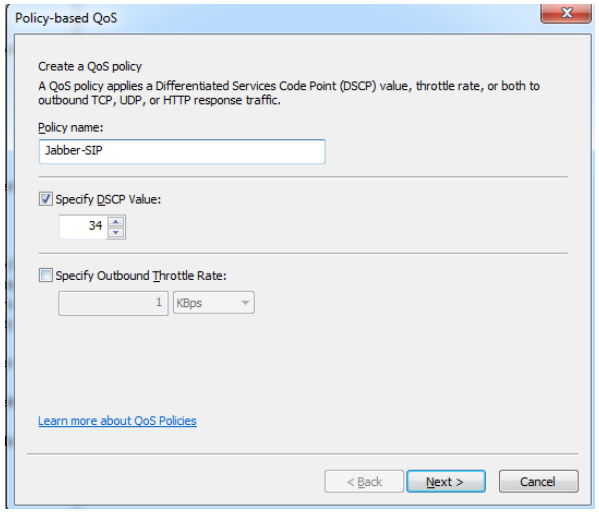
DSCP set by OS (Windows Group Policy Object - GPO)	Pro • Works for Windows Vista, Win7, Win8 • Centralized Administration of Policies (Windows AD)
	Con: • Unable to differentiate amongst some flows created by application (media types) • Generally PC is not a trusted device. Possible exceptions strictly 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



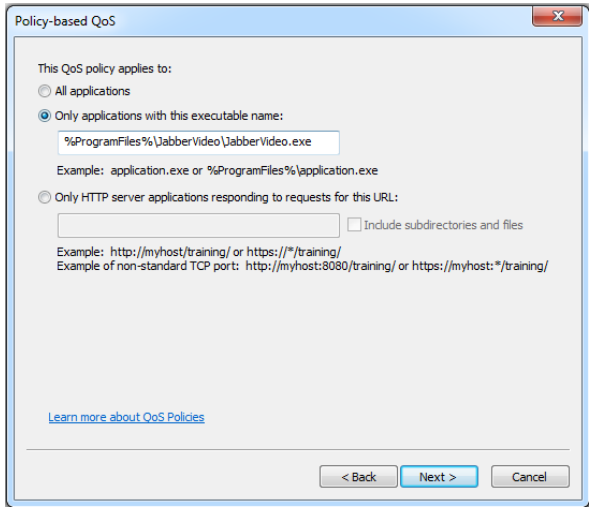
Windows Group Policy Object (GPO)



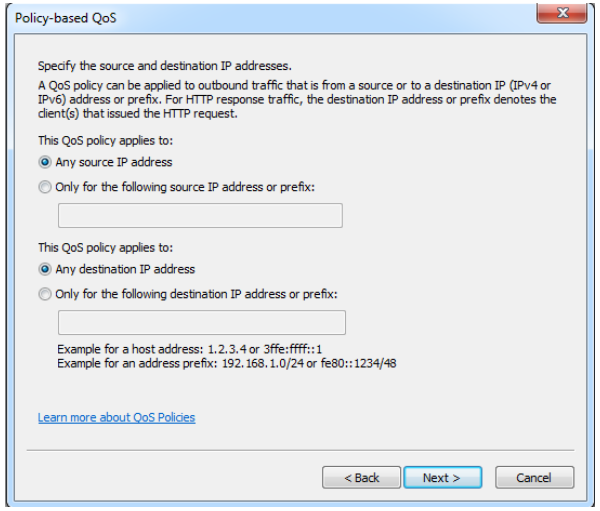
Windows Group Policy Object (GPO) allows for the QoS control (policer, DSCP marking) of traffic.
Based on application name, URL, IP address, IP protocol and L4 port numbers



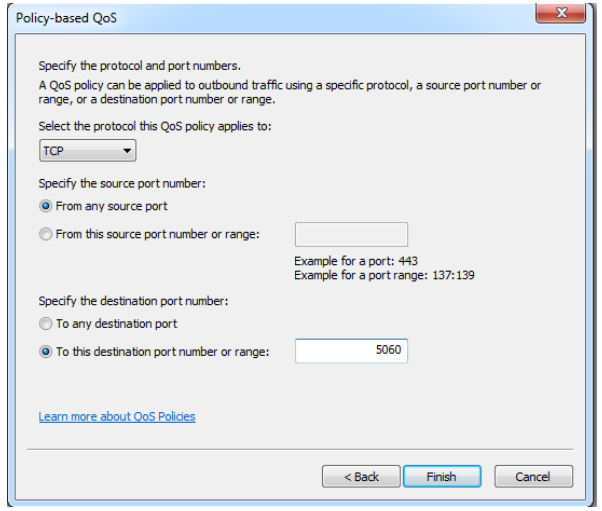
1



2



3



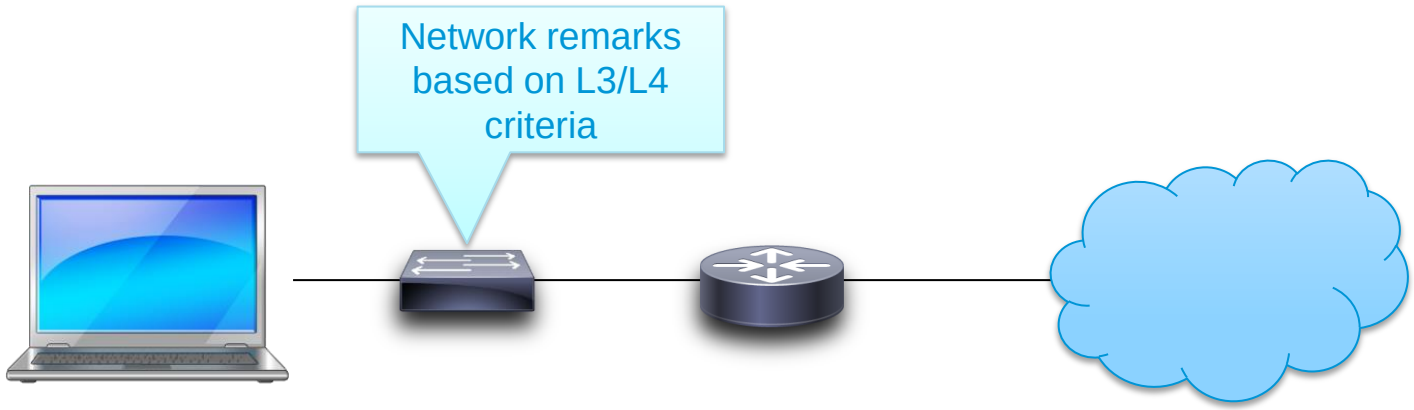
4

Soft Client Classification Methods

DSCP set by network based on understood UDP port ranges

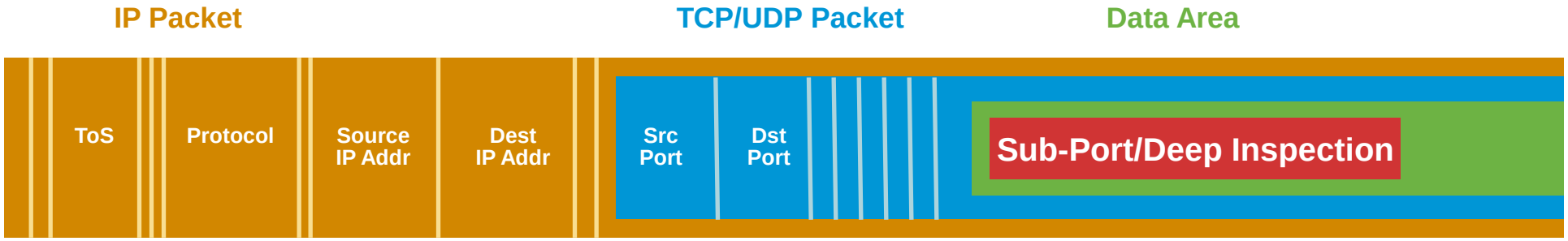
Pro:
- Do not need to trust endpoint
- Straightforward access-list mapping

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



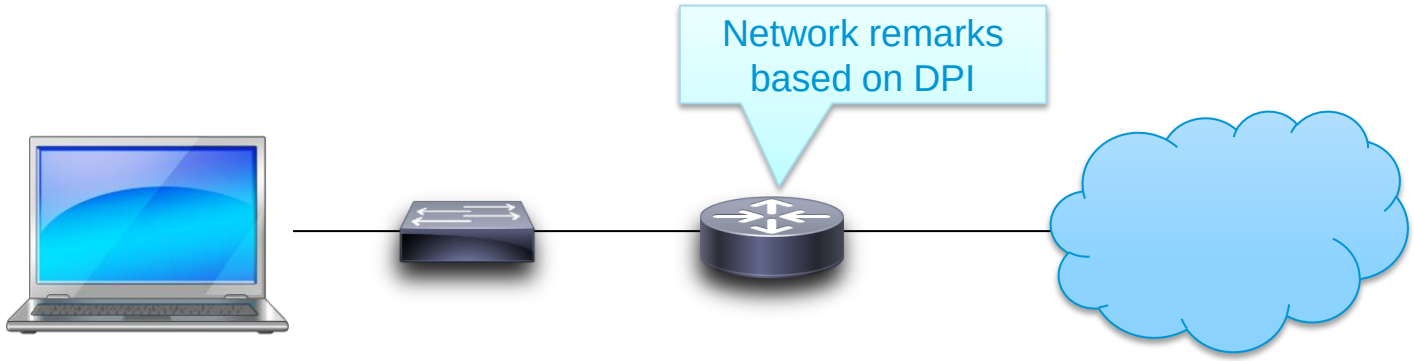
- Used for intelligent policy (QoS, filtering, etc.) or reporting
- Identifies over 1200 applications and protocols TCP and UDP port numbers
  - Statically assigned
  - Dynamically assigned during connection establishment
  - RTP and RTP payload type identification, MS-Lync, gtalk-video, skype, etc.
  - Cisco TelePresence media and signaling 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

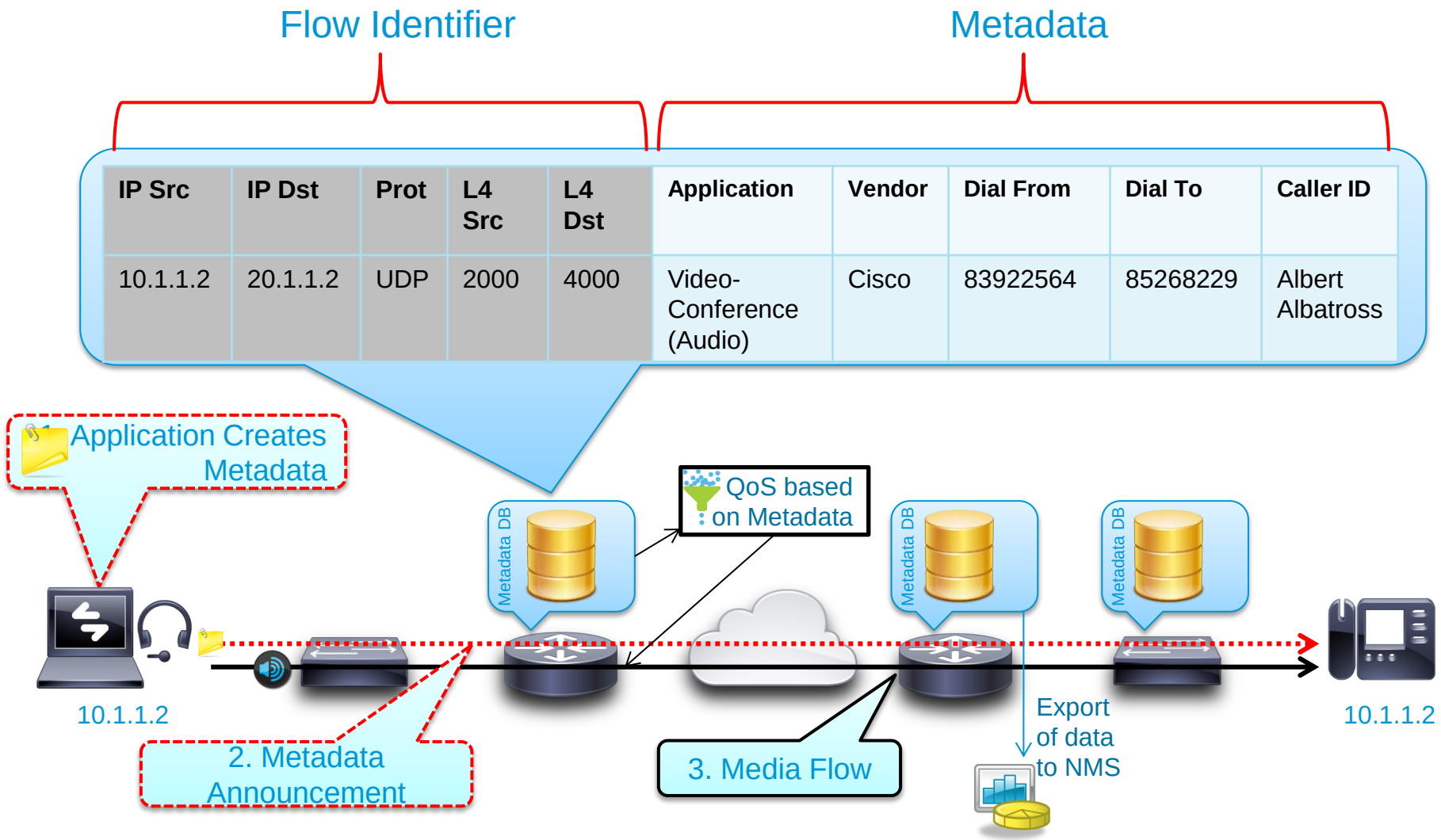
DSCP set by network based on DPI (NBAR)

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

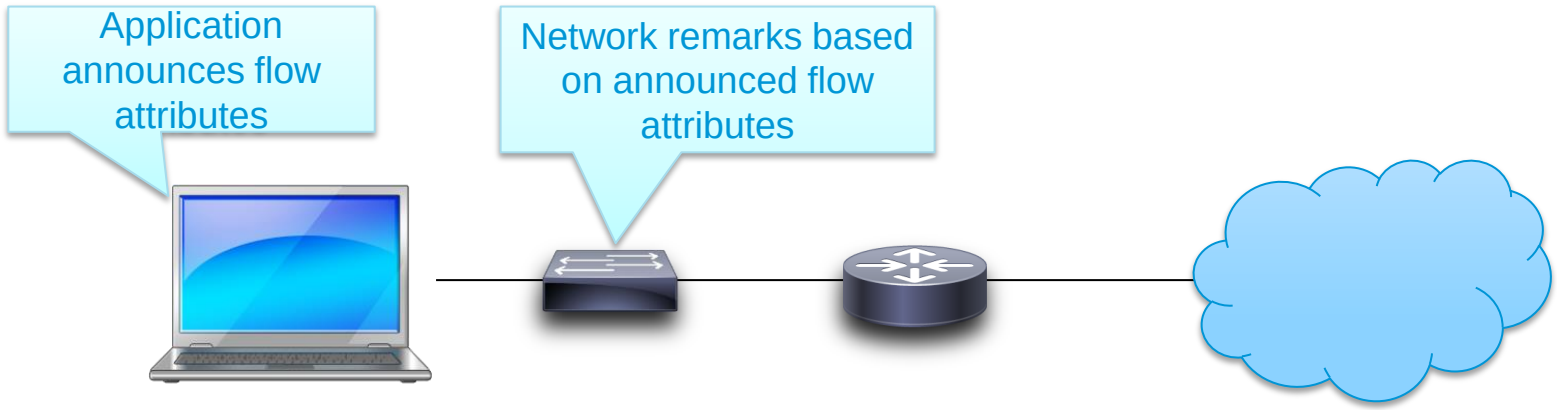
MSI produced Metadata

Pro:

- Separation between application context (metadata) and policy (based in network)
- Explicit signaling: 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



Reverse Metadata

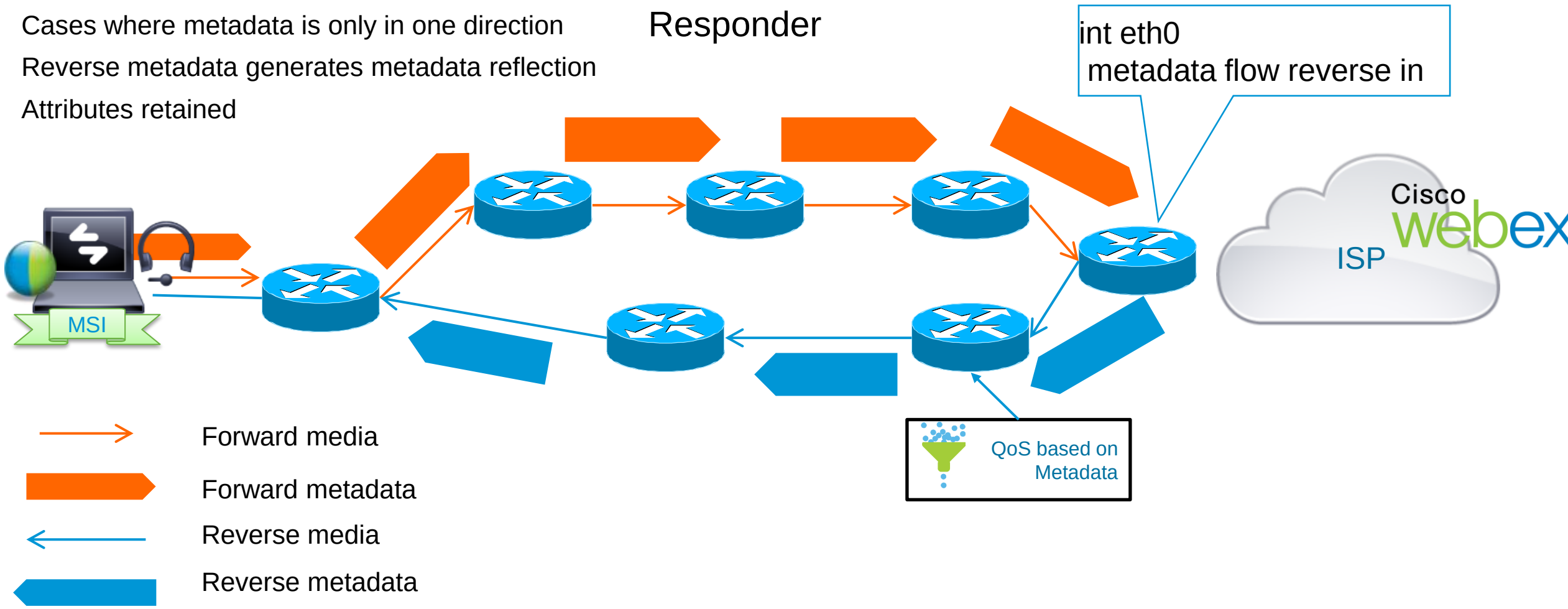
Making single sided metadata bi-directional

15.4(1)T

Cases where metadata is only in one direction

Reverse metadata generates metadata reflection

Attributes retained



Examples of Metadata Classification

Case	IOS Configuration

Software phone video conferencing (audio+video)	`Class-map match-all <video>`
	`  Match application attribute device-class software-phone`
	`  Match application attribute media-type video`
	`Class-map match-all <audio-in-video>`
	`  Match application attribute device-class software-phone`
	`  Match application attribute media-type audio-video`

Software phone audio only call (only audio)	`Class-map match-all <audio-only>`
	`  Match application attribute device-class software-phone`
	`  Match application attribute media-type audio`

Physical phone audio only call (only audio)	`Class-map match-all <audio-only>`
	`  Match application attribute device-class physical-phone`
	`  Match application attribute media-type audio`

WebEx Video	`Class-map match-all <video >`
	`  Match application webex-meeting`
	`  Match application match application attribute media-type video`

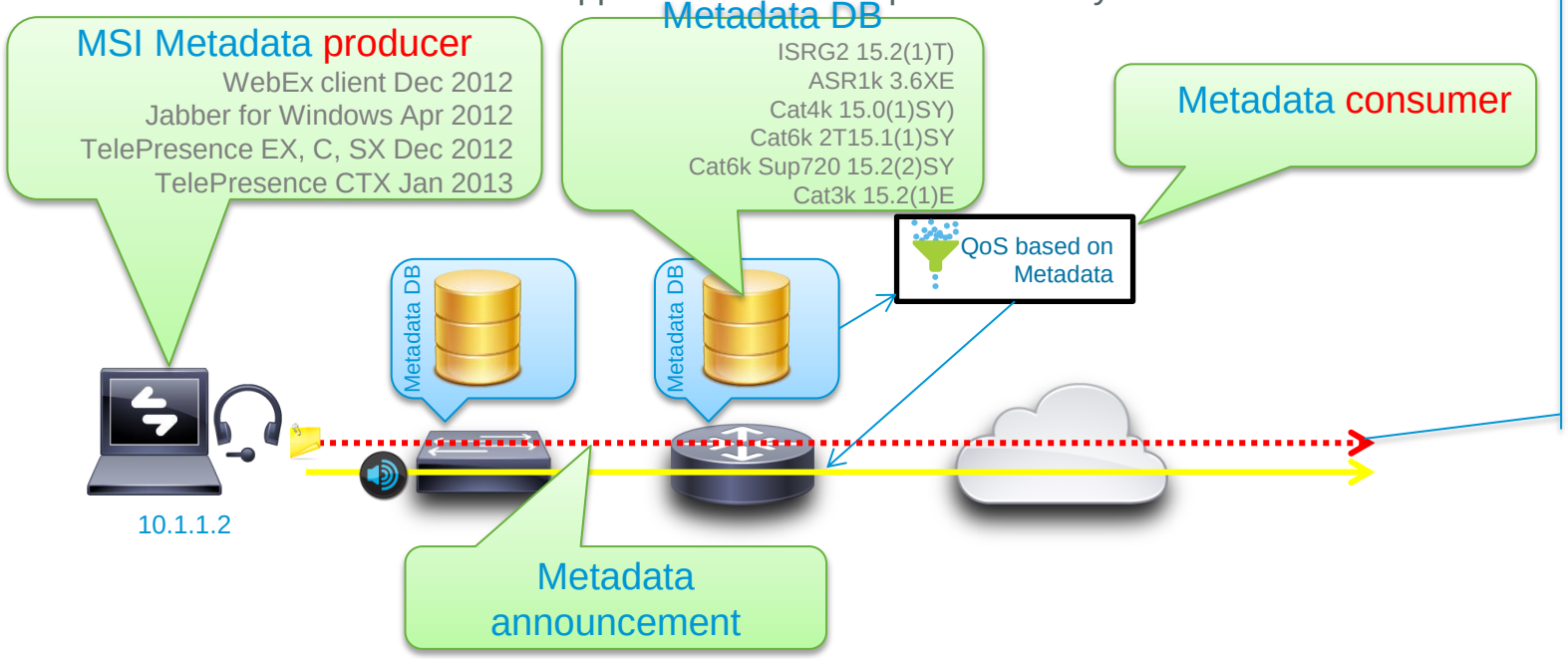
Cisco IT: Identify and Classify challenge

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

1. Note: RTP payload inspection must be performed prior to ACL match
2. 6Mbps is the maximum video queue size on a CVO router

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: utilizes metadata information
- Nodes that do not support metadata will pass it silently



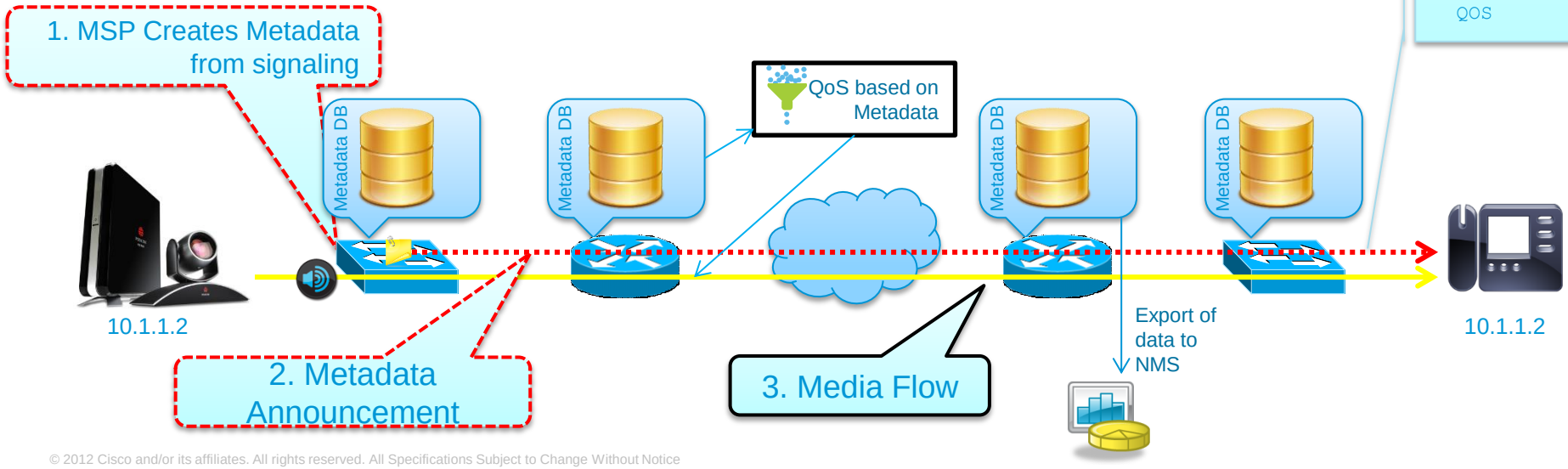

```
FF2205-4507#show metadata flow local-flow-id 5

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:
```

Network Generated 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 signaling (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"
```



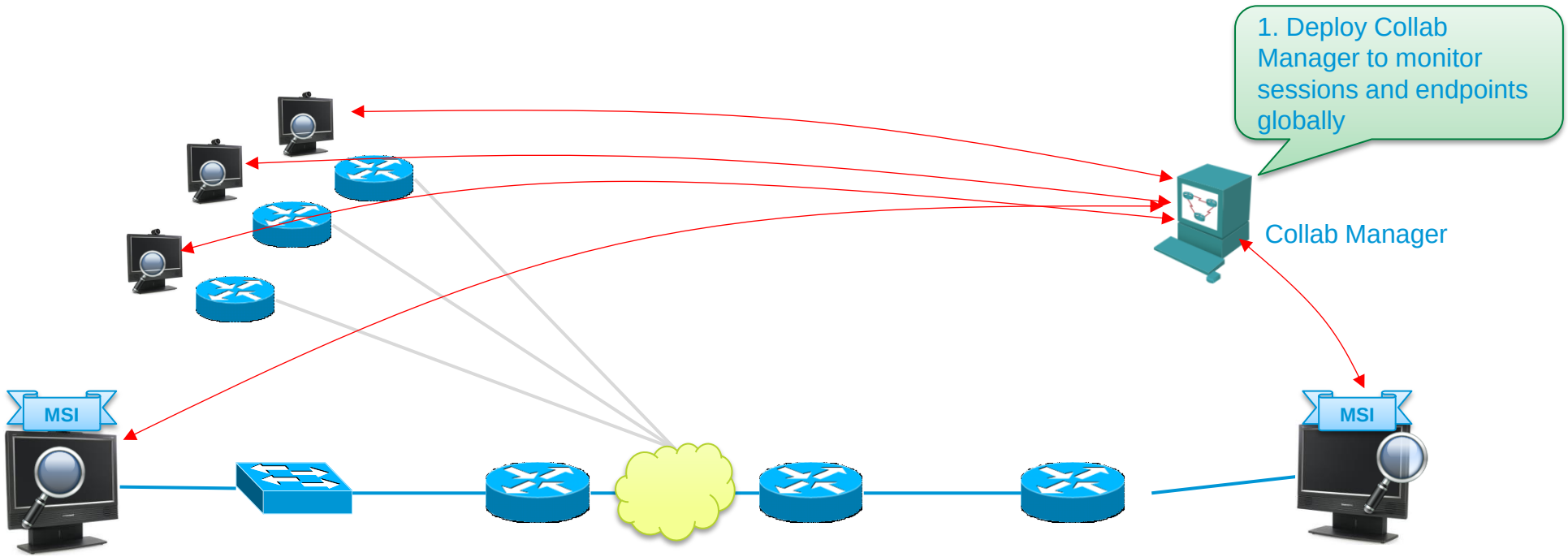
Examples of Deployment

A Phased Approach to Monitoring
For Cisco UC/ VC Applications

Situation:

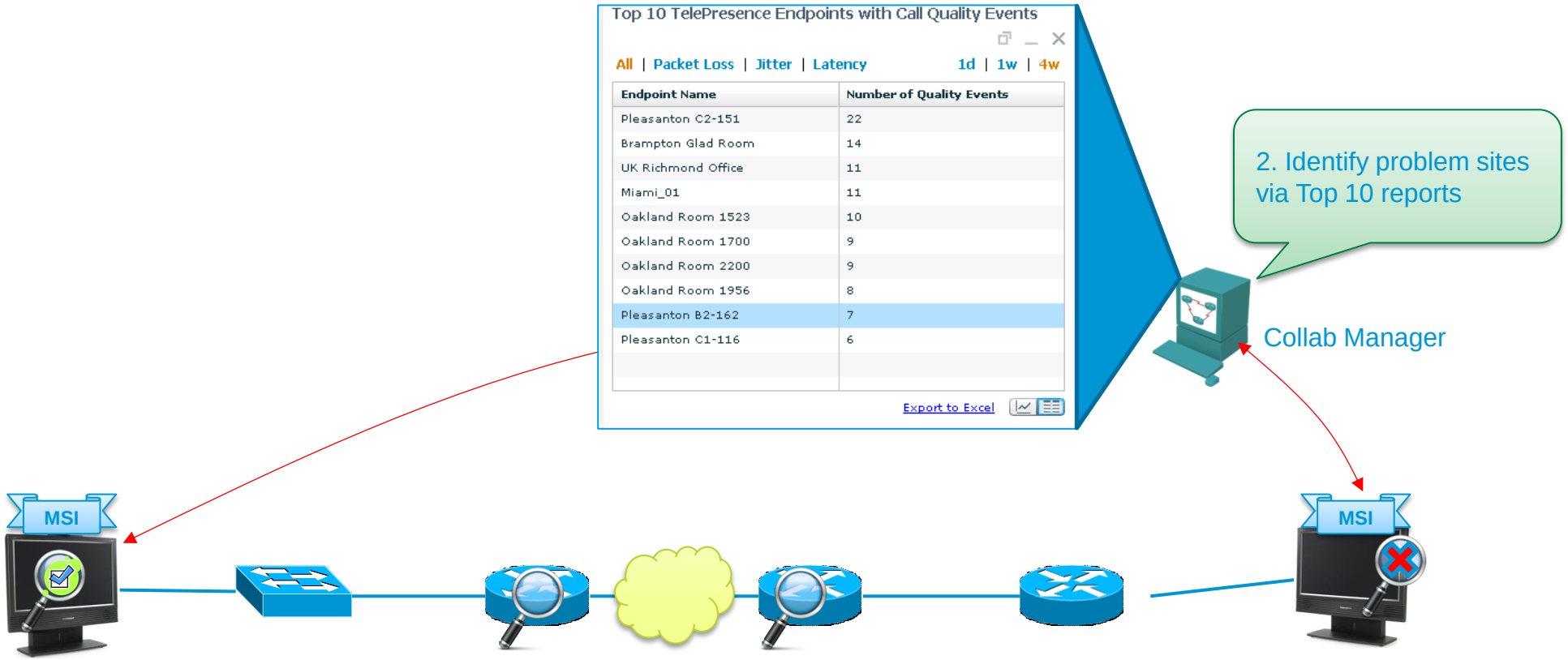
Intermittent issues with voice/video quality. Operator wants to quickly discover and resolve issues to provide a stable SLA service.

1. Deploy Collaboration Manger to monitor phone and VC endpoints, ‘over the top’
   No network changes needed.



A Phased Approach to Monitoring

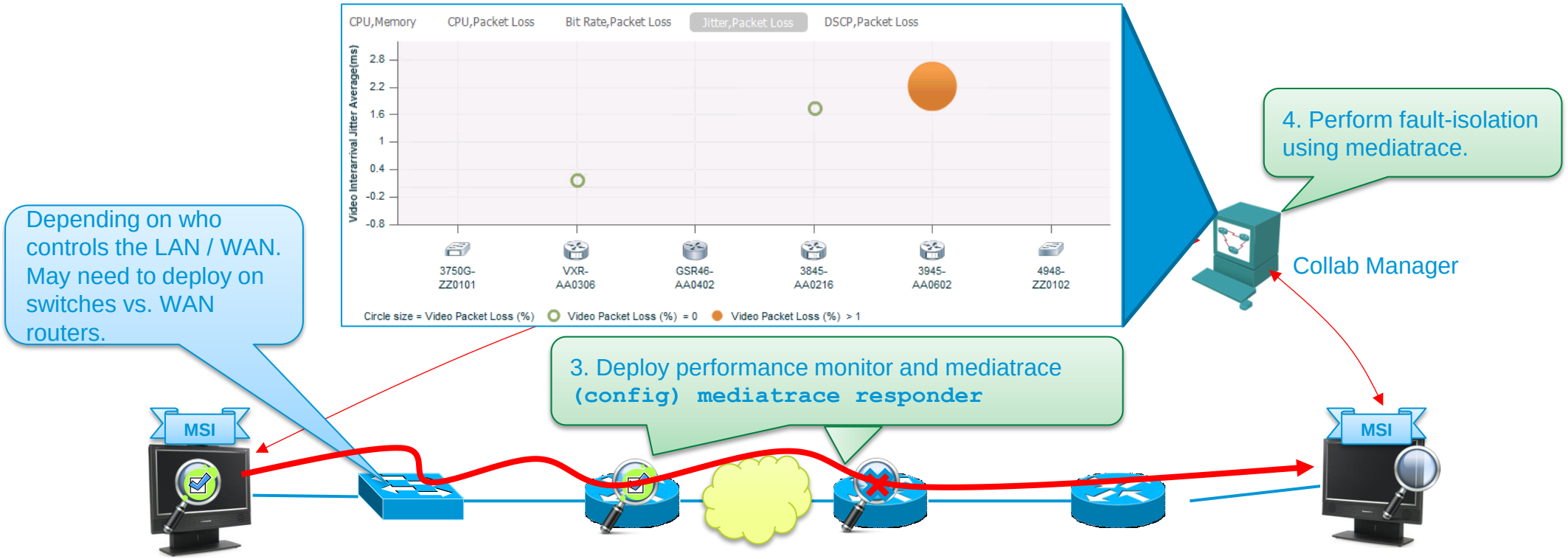
2. Via CP Top 10 Reports, identify worst performing endpoints and sites.



A Phased Approach to Monitoring

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

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

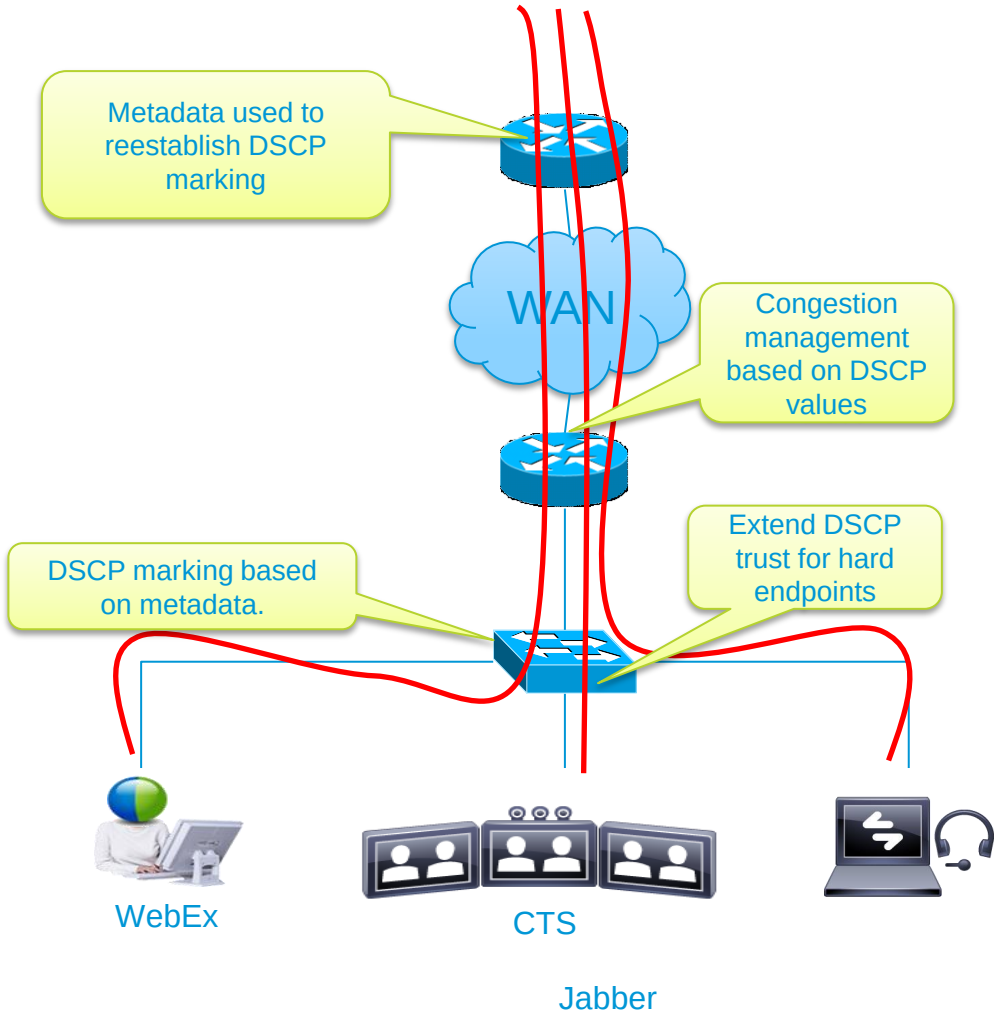

WebEx


CTS


Jabber

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.

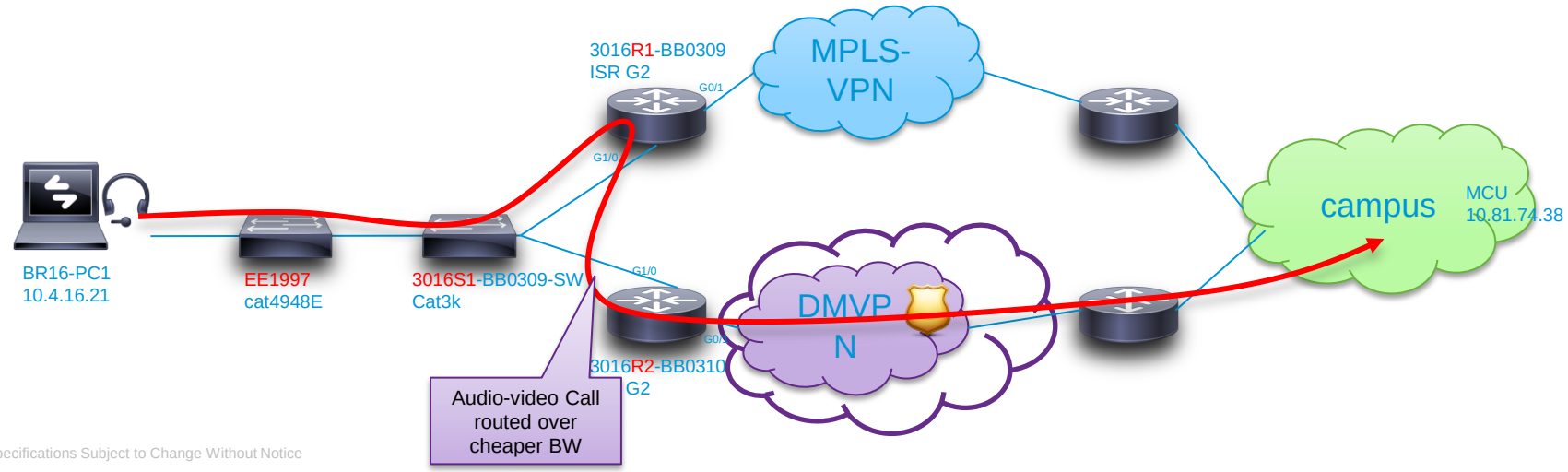


Metadata Classification for Intelligent Path Selection

- 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.



Additional 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
- Medianet Data sheet (includes SW version numbers): http://www.cisco.com/en/US/prod/collateral/routers/ps10536/data_sheet_c78-612429.html
- Medianet Knowledge Base - http://www.cisco.com/go/medianetkb
- Medianet Support forum -https://supportforums.cisco.com/community/etc/medianet
- SRND http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_medianet.html
- Medianet Blogs - http://blogs.cisco.com/tag/medianet/
- Cisco Developer Network for Medianet -http://developer.cisco.com/web/mnets

Thank you.