

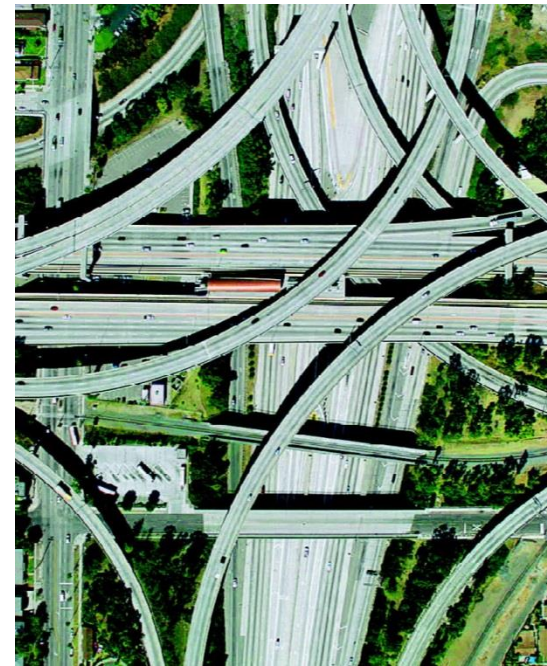


Praha, hotel Clarion
10. – 11. dubna 2013

Nástroje pro management multimediální sítě

T-COL2 / L2

Jiří Rott - Cisco



Agenda

Motivation

Medianet architecture framework

Media Monitoring

Perf.monitor, Mediatrace, IP SLA VO

Media Awareness

Metadata

UC client support

MSI, MSP

Resources

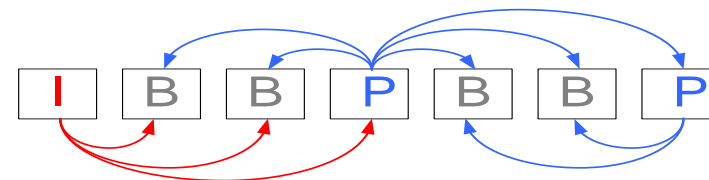


Video transport specific

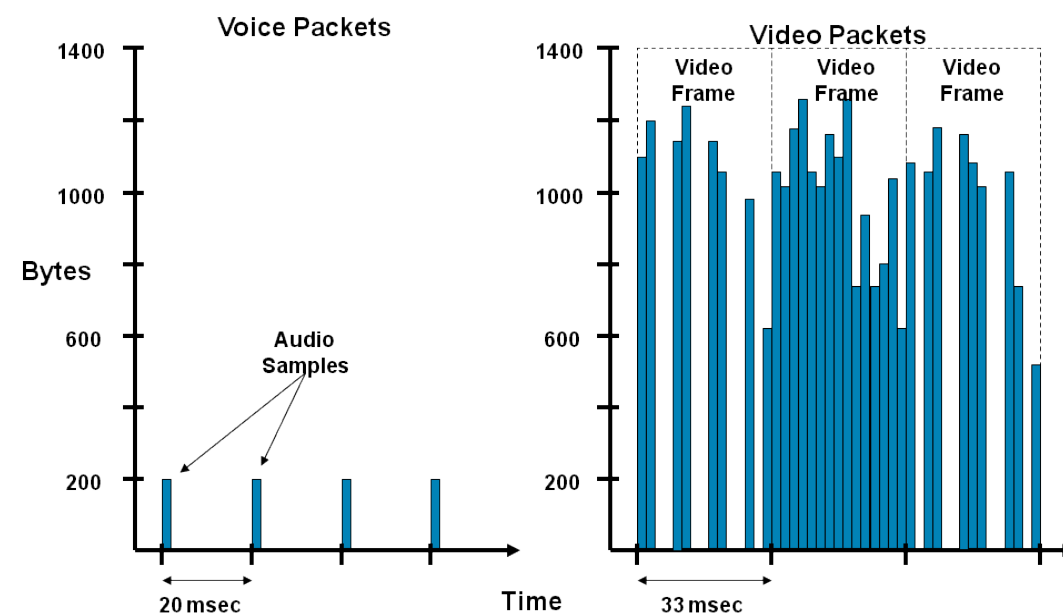
Different flow profile

Variable bit flow - burstiness

Extreme sensitivity to packet loss (compression ratios to 300:1)

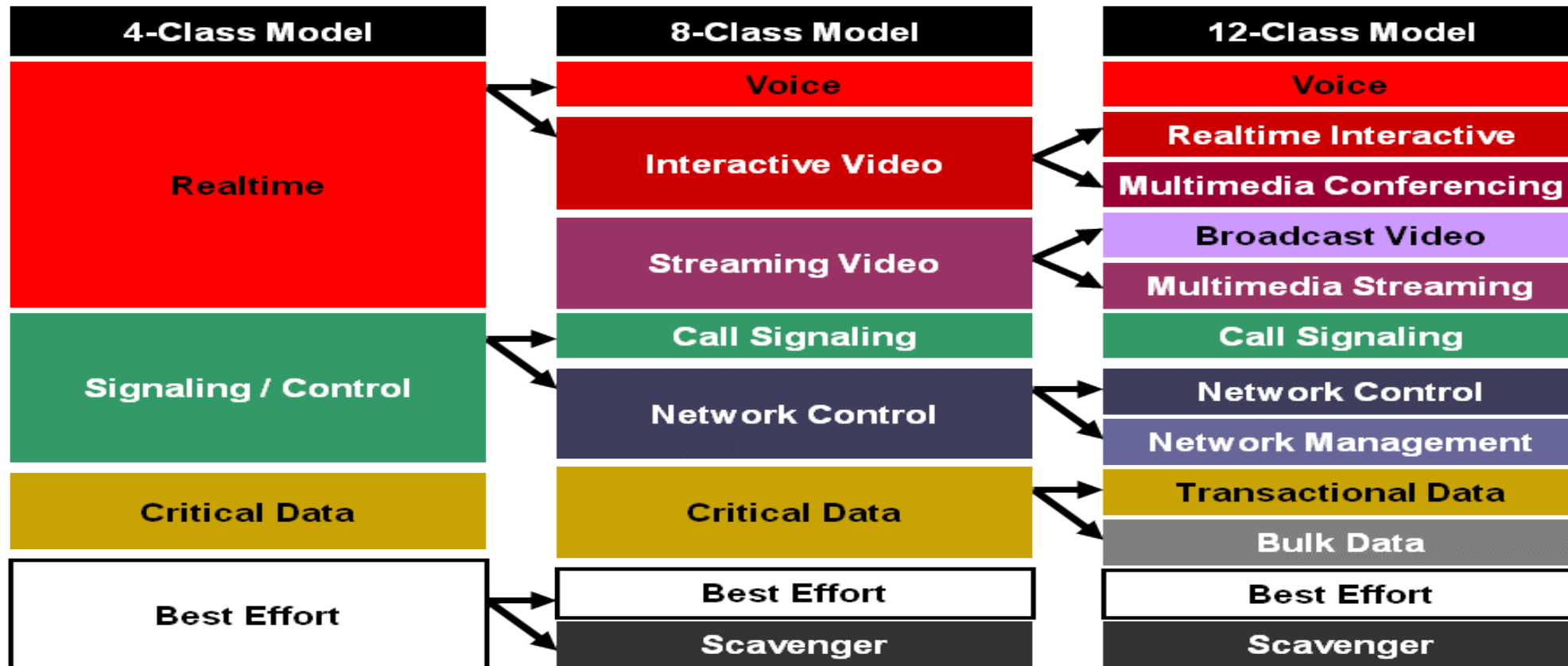


Application	Latency	Jitter	Loss (VoD)	Loss (Live)
Streaming Video	< 1000 ms	< 100 ms	< 0.1%	< 0.05%
Video Conferencing	< 150 ms	< 30 ms	NA	< 0.10%
TelePresence	< 150 ms	< 10 ms	NA	< 0.05%
Digital Signage	< 1000 ms	< 100 ms	< 0.1%	0%
IPTV	< 1000 ms	< 100 ms	< 0.1%	0%
Video Surveillance	< 1000 ms	< 100 ms	< 0.1%	< 0.05%



Quality guarantee?

- 1) QoS implementation (consistency)
LAN – marking
- 2) CAC implementation (best RSVP)



QoS Strategie



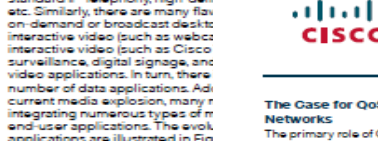
Medianet QoS Design Strategy

At-A-Glance

The Quality of Service Challenge for Medianets

Today there is a virtual explosion of media applications on the IP network with many different types of voice, video, and data applications. For example, standard IP Telephony, high-defi etc. Similarly, there are many flat on-demand or broadcast desk-to-interactive video (such as webcast interactive video (such as Cisco surveillance, digital signage, and video applications. In turn, there are number of data applications. Add current media explosion, many r integrating numerous types of r end-user applications. The evok applications are illustrated in Fig

Figure 1 Media Application Cor



The explosion of content and me and un-managed, as well as high collaboration applications, requi take a new look at their Quality of Without a clear strategy, the volu, today's media applications on th will exceed the ability of the net provision and manage.

Cisco Medianet QoS Desig

Each group of media application patterns and service level requi dedicated QoS class in order to service level requirements. Ther

make service level guarantees. This fundamental QoS requirement leads one to ask how many classes of media should be provisioned and how should these individual

requirements be provisioned and how should these individual

requirements be provisioned and how should these individual



Medianet Campus QoS Design

At-A-Glance

The Case for QoS in Medianet Campus Networks

The primary role of QoS in medianet campus networks is not to control latency or jitter (as it is in the WAN/VPN), but to manage packet loss. In GE/10GE campus networks, it takes only a few milliseconds of congestion to cause instantaneous buffer overruns resulting in packet drops. Medianet applications—particularly HD video applications—are extremely sensitive to packet drops, to the point where even 1 packet dropped in 10,000 is discernible by the end-user.

Classification, marking, policing, queuing, and congestion avoidance are therefore critical QoS functions that are optimally performed within the medianet campus network.

Four strategic QoS design principles that apply to campus QoS deployments include:

- Always perform QoS in hardware rather than software when a choice exists.
- Classify and mark applications as close to their sources as technically and administratively feasible.
- Police unwanted traffic flows as close to their sources as possible.
- Enable queuing policies at every node where the potential for congestion exists.

Medianet Campus QoS Design Considerations

There are several considerations that impact QoS designs within the medianet campus:

- Global Default QoS Setting
- Trust States and Conditional Trust
- Per-Port QoS, Per-VLAN QoS, Per-Port/Per-VLAN QoS
- Ingress QoS Models
- Egress QoS Models
- Ether-Channel QoS
- QoS Roles in a medianet campus
- AutoQoS

Global Default QoS Setting

On some platforms QoS is globally disabled by default (such as the Cisco Catalyst 3650/3750 and 6500). A fundamental first step is to globally enable QoS on these platforms.

Trust States

A switch port that is set to trust will accept and preserve either Layer 2 or Layer 3 packet markings. There are four static trust states with which a switch port may be configured:

- **Untrusted**—The default state with QoS enabled
- **Trust CoS**—Accepts Layer 2 802.1P CoS markings
- **Trust IP Precedence**—Accepts Layer 3 IP Precedence markings; largely deprecated
- **Trust DSCP**—Accepts Layer 3 DSCP markings; this is the most granular and flexible static state and thus the most utilized static trust state in medianet campus networks

Conditional Trust

Trust may also be extended dynamically, provided a successful condition has been met. In Cisco medianet campus networks this condition is a successful Cisco Discovery Protocol (CDP) negotiation between the access switch and the endpoints. Endpoints that can be extended conditional trust by Cisco Catalyst switches include Cisco IP phones, Cisco TelePresence Systems, Cisco IP Surveillance Cameras, and Cisco Digital Media Players. Conditional trust operation is shown in Figure 1.

Figure 1 Conditional Trust Operation



Per-Port QoS

When a QoS policy is applied on a per-port basis, it is attached to a specific physical switch port and is active on all traffic received on that specific port (only). Figure 2 illustrates port-based QoS.

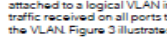
Figure 2 Port-Based QoS



Per-VLAN QoS

When a QoS policy is applied on a per-VLAN basis, it is attached to a logical VLAN interface and is active on all traffic received on all ports that are currently assigned to the VLAN. Figure 3 illustrates VLAN-based QoS.

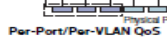
Figure 3 VLAN-Based QoS



Per-Port/Per-VLAN QoS

When a QoS policy is applied on a Per-Port/Per-VLAN basis, it is attached to specific VLAN on a trunked port and is active on all traffic received from that specific VLAN from that specific trunked port (only). Figure 4 illustrates Per-Port/Per-VLAN-based QoS.

Figure 4 Per-Port/Per-VLAN-Based QoS



Ingress QoS Models

There are many options for an administrator to choose from for ingress QoS models, as shown in Figure 5.

Medianet QoS Design Strategy

At-A-Glance

- **bandwidth queue with DSCP-based Weighted-Random Early Detect (DSCP-WRED) enabled.** Admission to this class should be controlled; additionally, traffic in this class may be subject to policing and re-marking. Example applications include Cisco Unified Personal Communicator, Cisco Unified Video Advantage, and the Cisco Unified IP Phone 7985G.
- **Multimedia Streaming**—This service class is

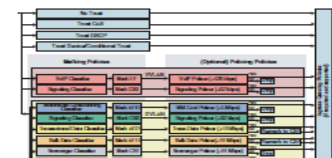
- **enabled on this class, as OAM traffic should not be dropped** (if this class is experiencing drops, then the bandwidth allocated to it should be re-provisioned). Example traffic includes SSH, SNMP, Syslog, etc.
- **Transactional Data (or Low-Latency Data)**—This service class is intended for interactive, "foreground" data applications ("foreground" refers to applications from which users are expecting a response via the network—in order to continue with their tasks;

permitted on enterprise networks, as long as resources are always available for business-critical voice, video, and data applications. However, as soon as the network experiences congestion, this class is the first to be penalized and aggressively dropped. Traffic in this class should be marked CS1 and should be provisioned with a minimal bandwidth queue that is the first to starve should network congestion occur. Example traffic includes YouTube, Xbox Live/360

Medianet Campus QoS Design

At-A-Glance

Figure 5 Ingress QoS Models



The three most utilized ingress QoS models for medianet campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Egress QoS Models

Cisco Catalyst switches perform queuing in hardware and as such are limited to a fixed number of queues. The nomenclature used to describe these queuing structures is IPxQyT, where:

- **IP** represents a strict priority queue
- **xQ** represents a number of non-priority queues
- **yT** represents a number of drop-thresholds per non-priority queue

No fewer than four hardware queues would be required to support medianet QoS policies in the campus; the following queues would be considered a minimum:

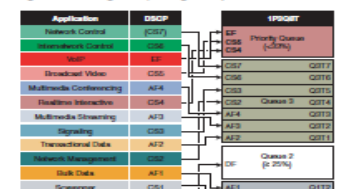
- Realtime queue (RFC 3248 EF PHB)
 - Guaranteed bandwidth queue (RFC 2597 AF PHB)
 - Default queue (RFC 2474 DF PHB)
 - Bandwidth constrained queue (RFC 3682 PDB or "scavenger" service)
- Additionally, the following bandwidth allocations are recommended for these queues:
- Realtime queue should not exceed 33% BW
 - Default queue should be at least 25% BW
 - Bulk/scavenger queue should not exceed 5% BW
- Given these minimum queuing requirements and bandwidth recommendations, the following application classes can be mapped to the respective queues:

For more details, see Medianet Campus QoS Design 4.0: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html.

- Voice, broadcast video, and realtime interactive may be mapped to the realtime queue (per RFC 4594)
- Network/internetwork control, signaling, network management, multimedia conferencing, multimedia streaming, and transactional data can be mapped to the guaranteed bandwidth queue. Congestion avoidance mechanisms, such as WRED, can be enabled on this class; furthermore, if configurable drop thresholds are supported on the platform, these may be enabled to provide intra-queue QoS to these application classes, in the respective order they are listed (such that control plane protocols receive the highest level of QoS within a given queue)
- Bulk data and scavenger traffic can be mapped to the bandwidth-constrained queue and congestion avoidance mechanisms can be enabled on this class. If configurable drop thresholds are supported on the platform, enabling them provides intra-queue QoS to drop scavenger traffic ahead of bulk data
- Best effort traffic can be mapped to the default queue; congestion avoidance mechanisms can be enabled on this class

An Egress Queuing Example Model

An egress queuing example based on these design considerations is shown in Figure 6.



Ether-Channel QoS

On some platforms ingress QoS policies (such as DSCP trust) are applied on the logical Port-Channel interface; however, on all platforms egress QoS policies (such as

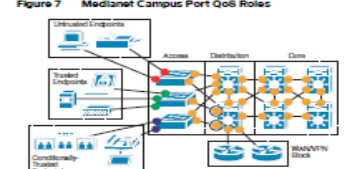
queuing policies) are always applied to the physical port member interfaces.

QoS Roles in a Medianet Campus

Access edge switch ports have the most variation in QoS policy roles and these will vary depending on the type of endpoint to which these are connecting.

For all switch-to-switch links the only QoS policies that are required are DSCP trust (on ingress) and queuing (on egress). QoS roles in a medianet campus network are shown in Figure 7.

Figure 7 Medianet Campus Port QoS Roles



- **Untrusted Endpoint Port QoS:**
 - Trust CoS
 - Trust IP Precedence
 - Trust DSCP
- **Trusted Endpoint Port QoS:**
 - Trust CoS
 - Trust IP Precedence
 - Trust DSCP
- **Conditionally-Trusted Endpoint Port QoS:**
 - Conditional Trust with Trust CoS
 - Conditional Trust with Trust DSCP

AutoQoS

On some Catalyst switching platforms Cisco has already updated and expanded the functionality of its AutoQoS feature to automatically provision QoS best practice designs for voice, IP-based video applications (such as IP Video Surveillance, Cisco TelePresence, conferencing applications, and streaming video applications), as well as for multiple types of data applications. On some switch platforms, an administrator can automatically provision these best practice designs via a single interface-level command that corresponds to the endpoint to which the switch port is connecting.

Copyright © 2011 Cisco Systems, Inc. All rights reserved. Cisco Confidential

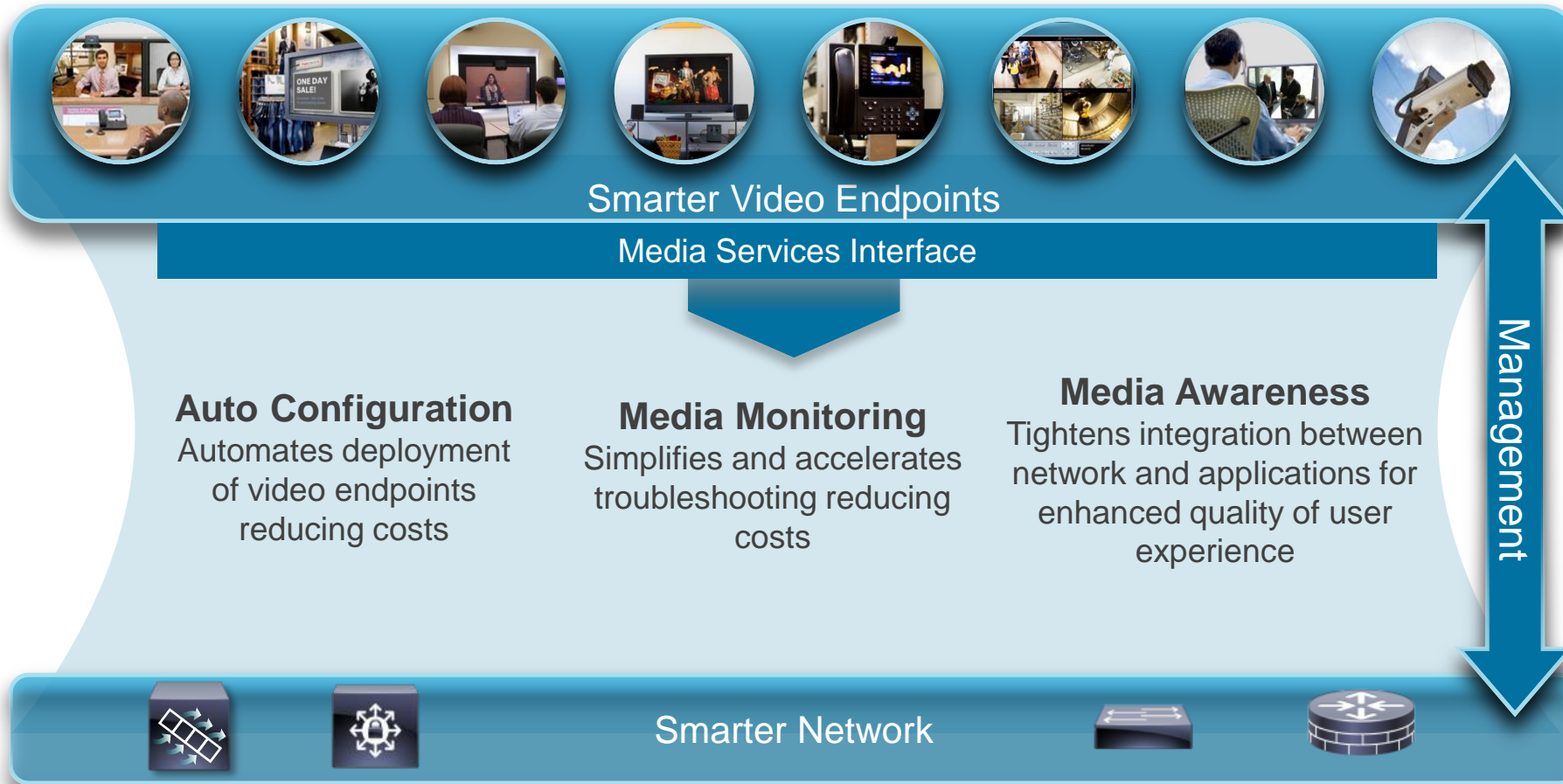
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qosmrn.pdf>

<http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qoscampusaag.html>

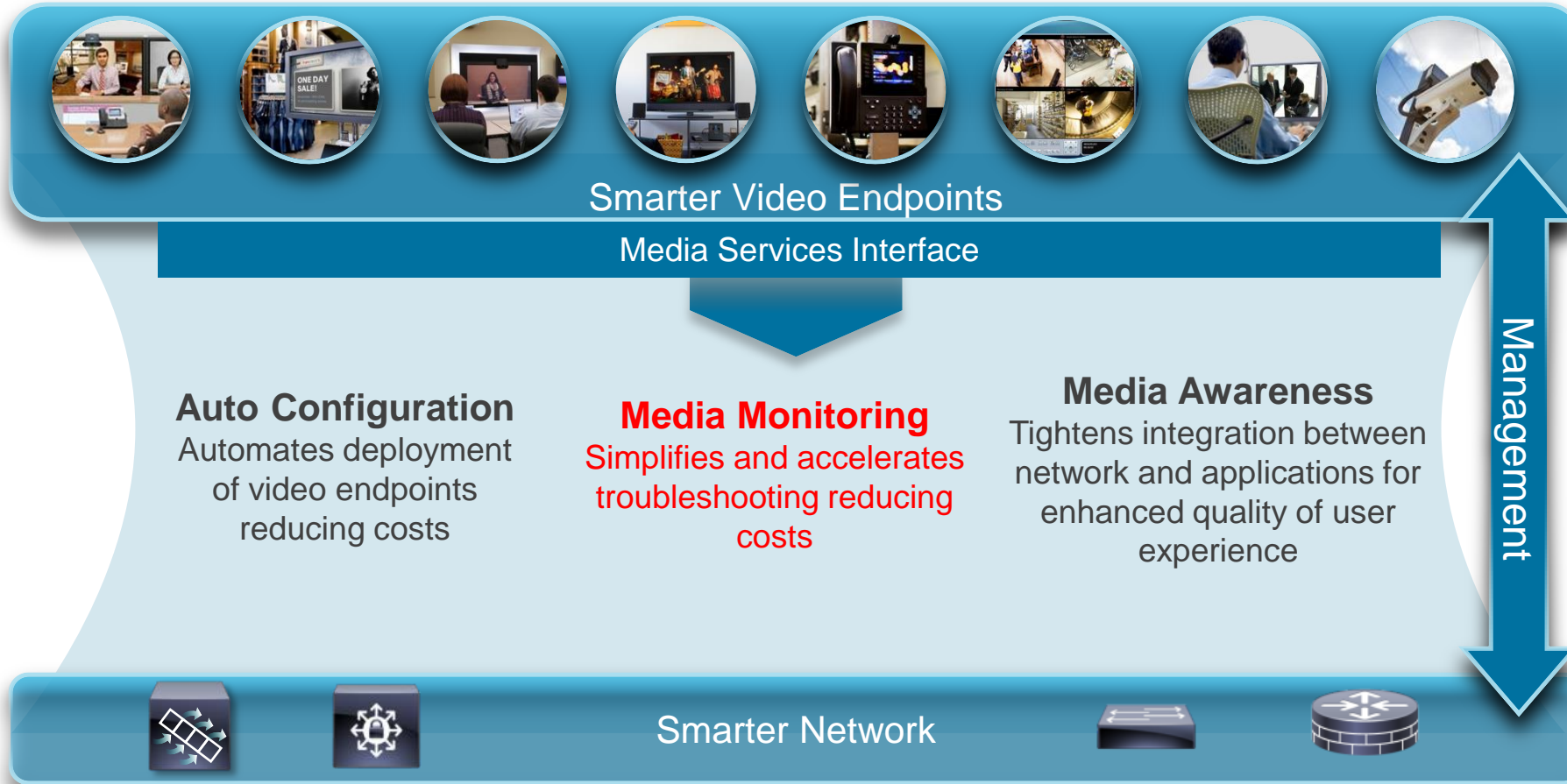
Medianet



How Medianet Helps?



How Medianet Helps?



Performance monitor



IOS Performance Monitor

Router/Switch native RTP and TCP analysis

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

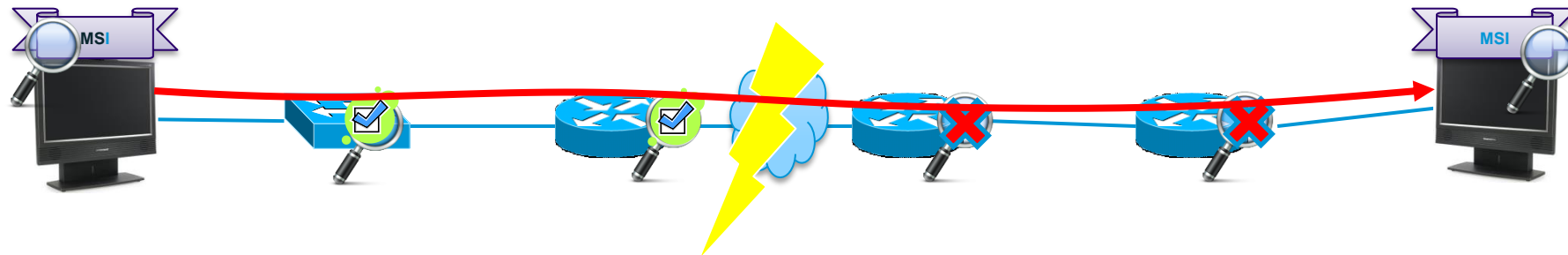
Cross-network synchronized time windows for measurement

same 30 second (default) intervals measured

Metrics can be **tested against thresholds** to **trigger actions**

Multi-level Alarm Raise/Clear, SNMP Traps, Syslog, Embedded scripts, Automatic Mediatrace, PfR

NetFlow and MIB interfaces



```
flow record type performance-monitor default-rtp:
```

```
Description:          VM default RTP record
```

```
No. of users:         4
```

```
Total field space:   98 bytes
```

```
Fields:
```

```
match ipv4 protocol
```

```
match ipv4 source address
```

```
match ipv4 destination address
```

```
match transport source-port
```

```
match transport destination-port
```

```
match transport rtp ssrc
```

```
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 counter packets dropped
```

```
collect timestamp interval
```

```
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
```

Perf-mon: flow records

Allows operator to select which metrics to collect

Based on Flexible NetFlow

Pre-packaged flow records

- *default-rtp*
- *default-tcp*

Perf-mon: simple inline configuration

Can **apply directly on interface**

Limited to **single class**



```
Interface FastEthernet0/0
service-policy type performance-traffic inline input
match dscp cs5 ef af41
flow monitor inline
  record default-rtp
  react 1 transport-packets-lost-rate
  threshold value gt 10.00
  alarm severity error
  action syslog
```

Metrics Available via Performance Monitor

IOS 15.1(3)T

PM 2.0 - IOS 15.2(2)T extension

Additional audio/video metrics
More emphasis on TCP metrics

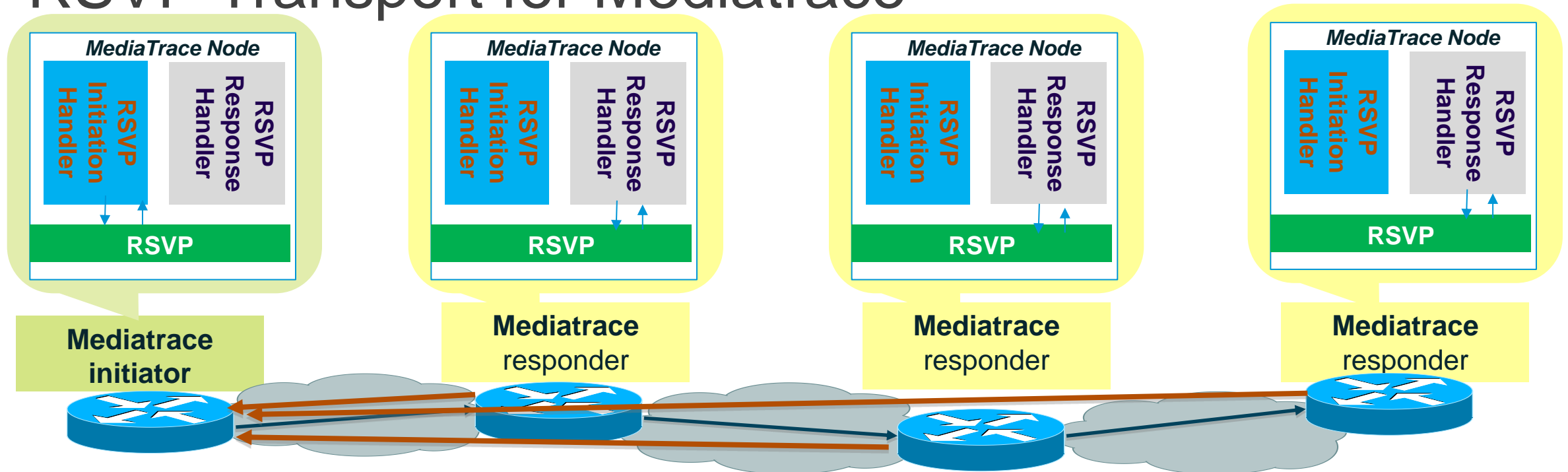
Metric/Data Value	Protocol
RTP payload type	RTP
IPv6 support	(all new and existing metrics)
Flexible NetFlow (FNF) field imports	all
TCP Max Segment Size	TCP
TCP min/max/avg Window Size	TCP
Out of order bytes	RTP
Out of order packets	RTP

Metric/Data Value	Protocol
transport rtp ssrc	RTP
application media packets counter (long)	All
application media bytes counter (long)	All
application media bytes rate	All
application media packet rate	All
transport packets lost counter	RTP
transport packets expected counter	RTP
transport packets lost rate	RTP
counter bytes rate	All
transport event packet-loss counter	TCP, RTP
transport round-trip-time	TCP
transport rtp jitter maximum	RTP
transport rtp jitter minimum	RTP
transport rtp jitter mean	RTP
application media packets rate variation	IP-CBR
application media event	-
counter packets dropped	All

Mediatrace



RSVP Transport for Mediatrace



MediaTrace (Dynamic Video monitoring), an application to dynamically monitor media-flows for Medianet uses **RSVP** as a **transport protocol**

RSVP traverses same path as media

RSVP can provide route-change notification to Mediatrace if there is any re-routing of the flow on a RSVP-aware node

Note : Switch L2 mode add :**ip rsvp snooping**

Mediatrace components

Requestor

End video system, NMS, same node as initiator, remote router/switch

Initiator – include data

Responder – send data back to initiator

Different types of data requests

Hops – hop discovery

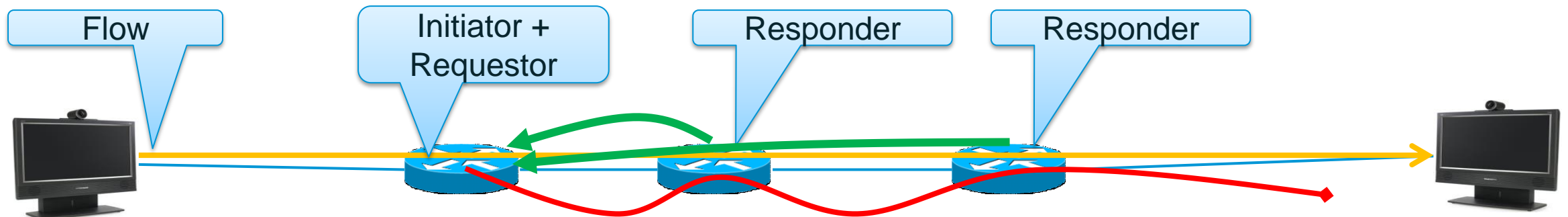
System – system information

Performance monitor – runs perf-mon, and collects data

Multiple configuration possibilities

Poll – simplest config , runs from IOS (wo level15)

Session – allow periodical repeated requests and history



Mediatrace type 1

Mediatrace hops poll

- identify L2 and L3 nodes

initiator# **mediatrace poll path-specifier source 10.10.130.2 destination 10.10.132.2 hops**

Started the data fetch operation.

Waiting for data from hops.

This may take several seconds to complete...

Data received for **hop 1**

Data received for **hop 2**

Data fetch complete.

Results:

Data Collection Summary:

Request Timestamp: 22:47:56.788 PST Fri Oct 29 2010

Request Status: Completed

Number of hops responded (includes success/error/no-record): 2

Number of hops with valid data report: 2

Number of hops with error report: 0

Number of hops with no data record: 0

Detailed Report of collected data:

Number of Mediatrace hops in the path: 2

Mediatrace Hop Number: **1** (host=responder1, ttl=254)

Reachability Address: 10.10.12.3

Ingress Interface: Gi0/1

Egress Interface: Gi0/2

Mediatrace Hop Number: **2** (host=responder2, ttl=253)

Reachability Address: 10.10.34.3

Ingress Interface: Gi0/1

Egress Interface: Gi0/2

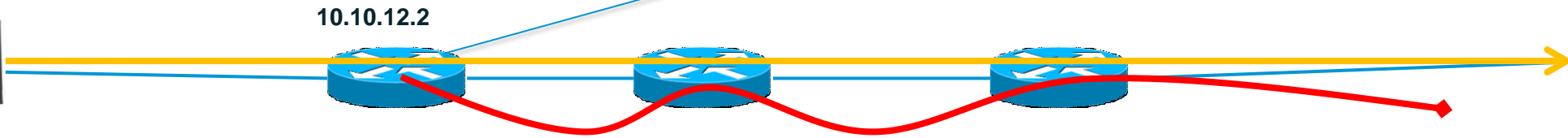
10.10.130.2:1000



10.10.12.2



10.10.132.2:2000



Mediatrace type 2

Preconfigured profile

mediatrace session- system profile

session 2, repeated after 60 sec

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

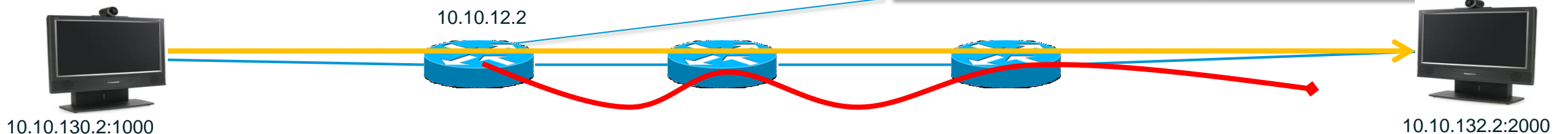
Pkts discarded at Ingress (pkts): 0

Pkts discarded at Egress (pkts): 0

Ingress i/f speed (mbps): 1000.000000

Egress i/f speed (mbps): 1000.000000

Note: data removed for readability



Mediatrace type 3

Preconfigured profil

mediatrace session-perf-mon

```
initiator#show mediatrace session stats 1
```

```
Session Index: 1
```

```
...
```

```
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:
```

```
Flow Sampling Start Timestamp: 23:45:56
```

```
Loss of measurement confidence: FALSE
```

```
Media Stop Event Occurred: FALSE
```

```
IP Packet Drop Count (pkts): 0
```

```
IP Byte Count (Bytes): 6240
```

```
IP Packet Count (pkts): 60
```

```
IP Byte Rate (Bps): 208
```

```
Packet Drop Reason: 0
```

```
IP DSCP: 0
```

```
IP TTL: 57
```

```
IP Protocol: 17
```

```
Media Byte Rate Average (Bps): 168
```

```
Media Byte Count (Bytes): 5040
```

```
Media Packet Count (pkts): 60
```

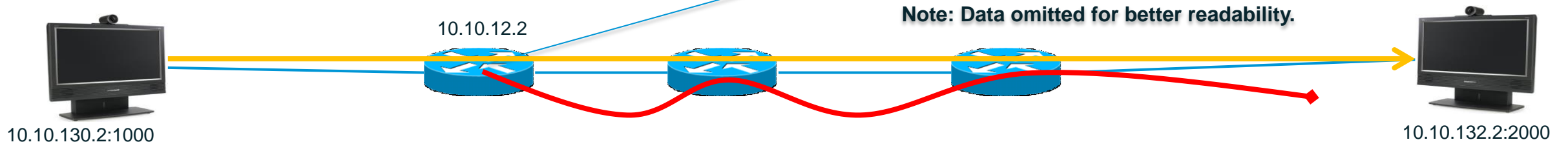
```
RTP Interarrival Jitter Average (usec): 3911
```

```
RTP Packets Lost (pkts): 0
```

```
RTP Packets Expected (pkts): 60
```

```
RTP Packet Lost Event Count: 0
```

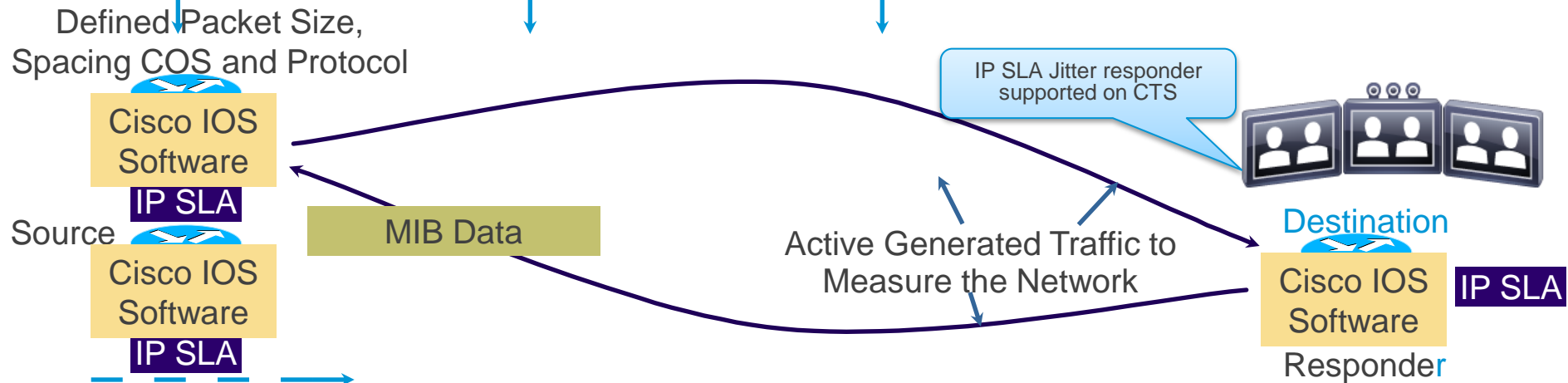
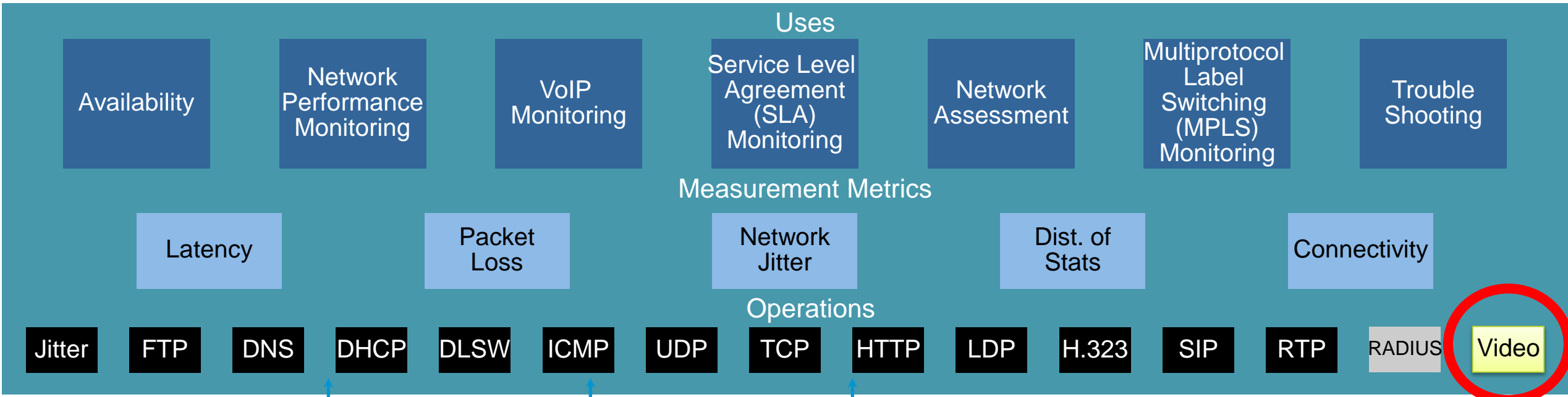
```
RTP Loss Percent (%): 0.00
```



IP SLA VO



IP SLA: Synthetic Traffic Measurements















IPSLA Video Operation Embedded Traffic Simulator

IPSLA VO support:

Platform	Sender Requirements	Responder Requirements	Starting from Image	License Requirements (Sender and Responder)
Cisco Catalyst 3K Series	No platform-specific requirement	No platform-specific requirement	12.2(58)SE2	IPBase/IPBase
Cisco Catalyst 4K Series	SUP-7E, SUP-7LE	SUP-7E, SUP-7LE, SUP-6E	15.1(1)G	IPBase/IPBase
Cisco ISR G2 Series	PVDM3 available on 2900, 3900 platforms	No DSP requirement; 1900, 2900, 3900, series	15.2(2)T	UCk9/IPbase




IPSLA VO profiles

Profile vs platform:

Platform/Profile	TelePresence	IP Television (IPTV)	IP Video Surveillance Camera (IPVSC)	Cisco Phone
Cisco Catalyst 3K Series	 <i>* =modeled after an older version of codec</i>		 <i>* =modeled after an older version of codec</i>	
Cisco Catalyst 4K Series				
Cisco ISR G2 Series			 <i>!=using custom profile</i>	

IPSLA VO custom profiles

Custom profiles:

Platform	Support for Custom Profile	Mechanism
Cisco Catalyst 3K Series		Custom Profile Generator
Cisco Catalyst 4K Series		
Cisco ISR G2 Series		Configure profile parameters using Cisco IOS CLI and MIBs

Custom profiles on ISR G2

Custom profiles parameters:

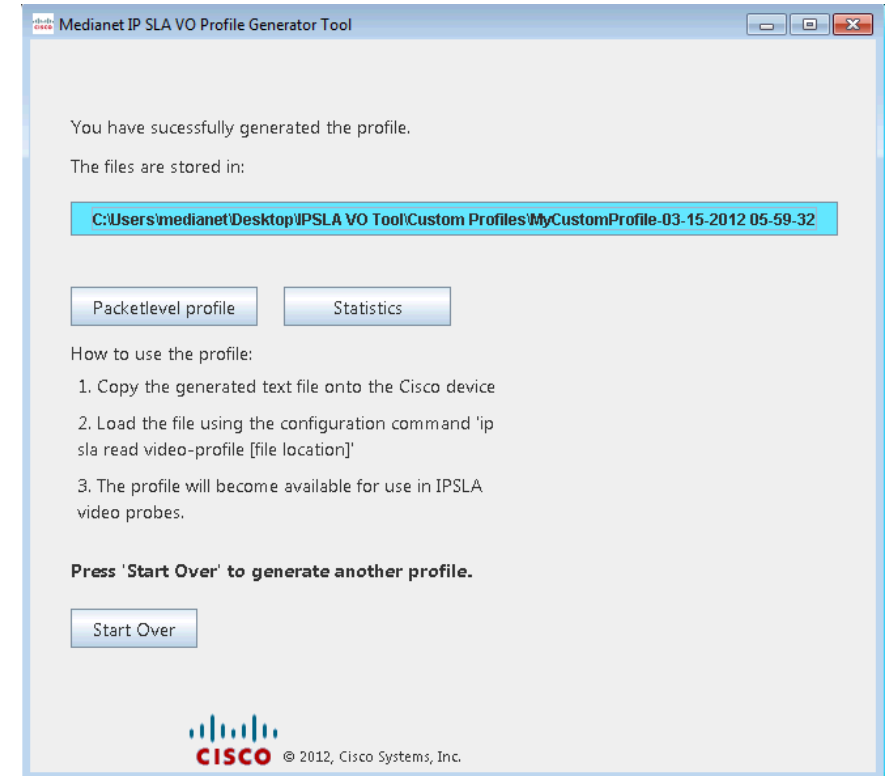
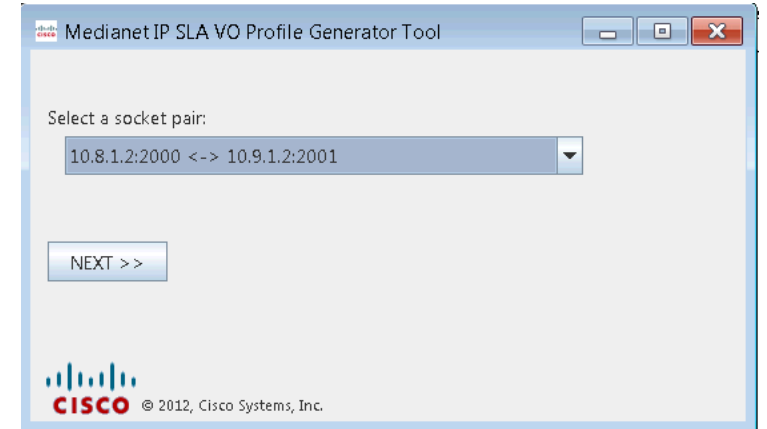
Mandatory Parameters	Endpoint type (CTS, CP-9900 or custom) Maximum bit rate (up to 4 Mbps) Frame rate (up to 30 fps) Resolution (up to 1080p) Codec (e.g. H.264 Baseline) Video contents
Optional Parameters	Rate-control averaging window size I-frame max size I-frame refresh interval RTP average size per packet Encoder jitter buffer control

Customized profile IP SLA VO - 3k

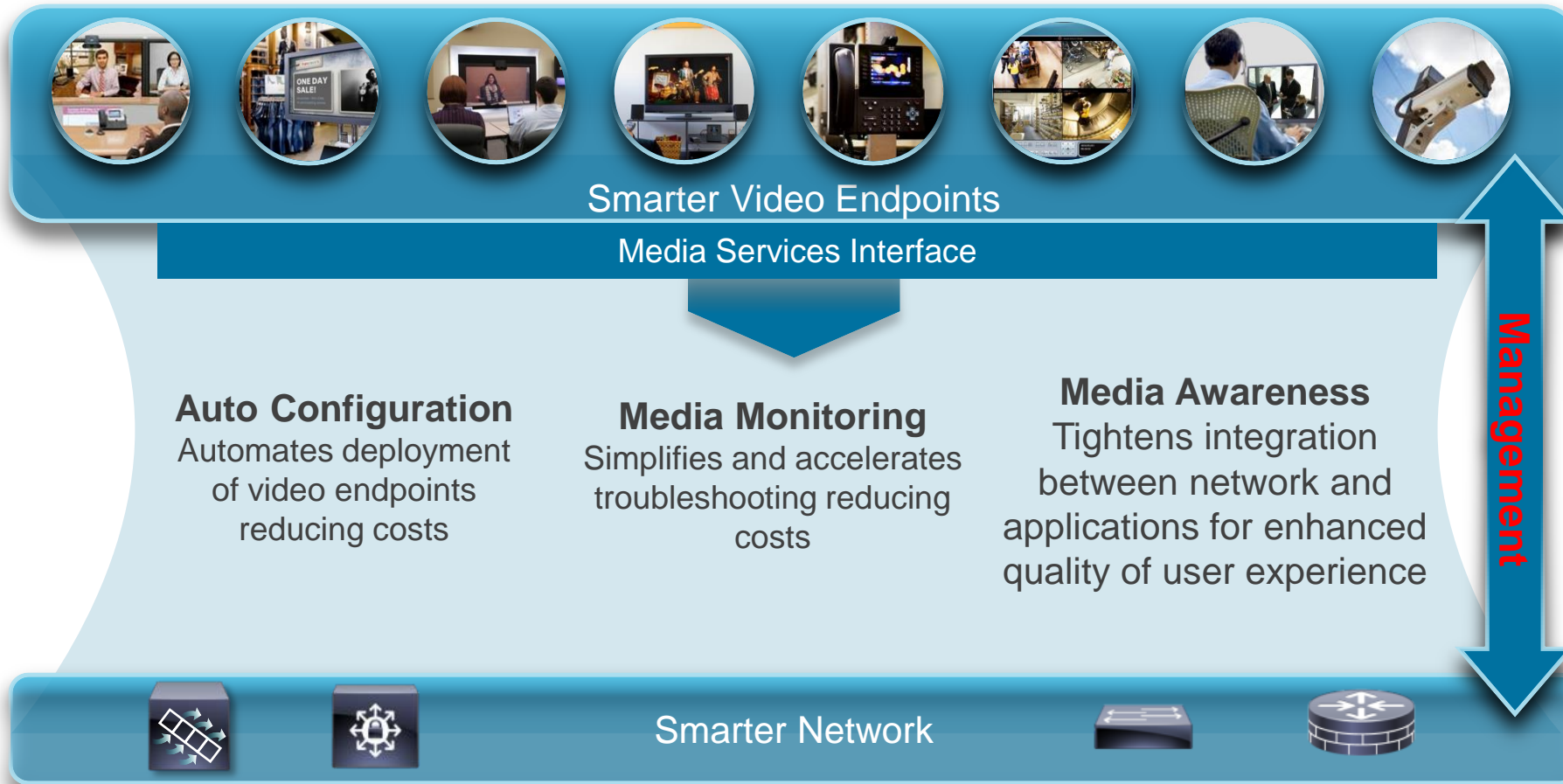
IP SLA VO allow to generate video profile

Procedure:

- 1) save .pcap data 9 (at least 30 sec)
- 2) download from <http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html#~design> (part tools)
- 3) install ipslavo.exe
- 4) download .pcap and select socket pair
- 5) generate „text“ and „stat“ files
- 6) copy „text“ file into Cisco device
- 7) load file by „ip sla read video-profile“ command
- 8) use it as normal IP SLA VO profile



How Medianet Helps?



Management Solutions



Cisco Prime LAN Management Solution

- Medianet Readiness Assessment
- Medianet “plug-in” provides workflows for provisioning autoconfiguration and location settings and tracking of medianet endpoints
- More info: <http://cisco.com/go/lms>



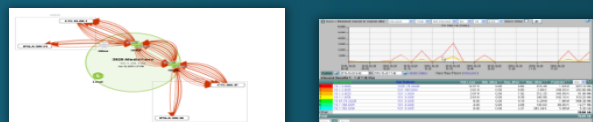
Cisco Prime Assurance Manager

- End-to-end proactive, network based monitoring, troubleshooting & analysis of application traffic
- Supports a variety of sources including performance monitor
- More info: <http://www.cisco.com/go/pam>



Cisco Prime Collaboration Manager

- Supports timely end-to-end visibility and isolation of video-related issues for TelePresence & Tandberg sessions
- Provides deeper network path visibility with mediatrace
- More info: <http://www.cisco.com/go/cpcm>



CDN Partner Tools

- Tools from other vendors supporting medianet features.
- More info: <http://developer.cisco.com/web/mnts/partners>

Cisco Prime Collaboration Manager

Network based Mediatrace Enablement (configuration)

Device Role	Configuration	Purpose
Mediatrace Initiator	<pre>username <username> priv 15 secret <username_enable_password> ! ip http server ip http authentication local ip http timeout-policy idle 60 life 86400 requests 10000 ! wsma agent exec profile wsma_listener_http wsma agent config profile wsma_listener_http ! wsma profile listener wsma_listener_http transport http</pre>	WSMA
	<pre>mediatrace initiator [source-interface source-ip] <int ip></pre>	Mediatrace
Mediatrace Responder (Initiator is also a responder)	<pre>mediatrace responder</pre>	Mediatrace
Performance Monitor	<pre>service-policy type performance-monitor inline input flow monitor inline record default-rtp</pre>	Perf-Mon
IPSLA	<pre>IPSLA responder</pre>	IPSLA

Media Monitoring Interfaces



Performance Monitor

- Flexible NetFlow V9
- MIB
- REST for MSI



Mediatrace

- Web Services Management Agent (WSMA)
- REST for MSI
- MIB (new!)



IPSLA Video Operation

- MIB

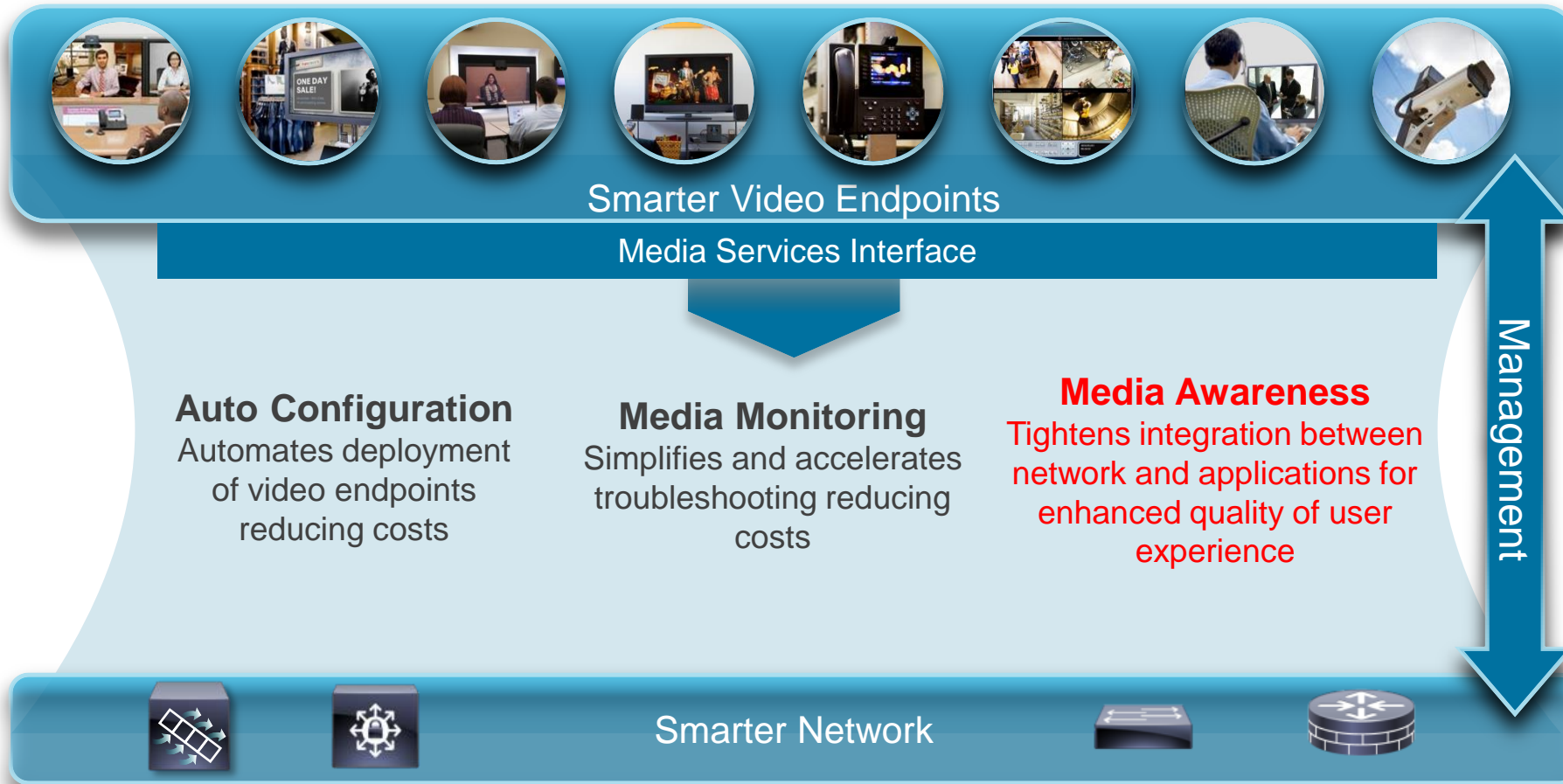
Find more @ <http://developer.cisco.com/web/mnets/resources>

Medianet Systems Management IVT Program Guidelines:
<http://developer.cisco.com/web/mnets/partners>

Ukázka Cisco Prime Collaboration Manager



How Medianet Helps?



Media Awareness



DSCP Values Remarked

- OS (e.g. Windows) remarks traffic
- Security Policy: Do not trust DSCP markings from general purpose computers
- Limited SP DSCP values

Window remarks traffic even though the application correctly sets the DSCP values

Jabber/MSI generates metadata

Voice: set QoS policy

DSCP remarked for SP

Service Provider supports limited DSCP values

Private MPLS and GETVPN

QoS Policy driven by metadata

Security Policy: Network does not trust any laptop or PC, remarks all traffic to best effort

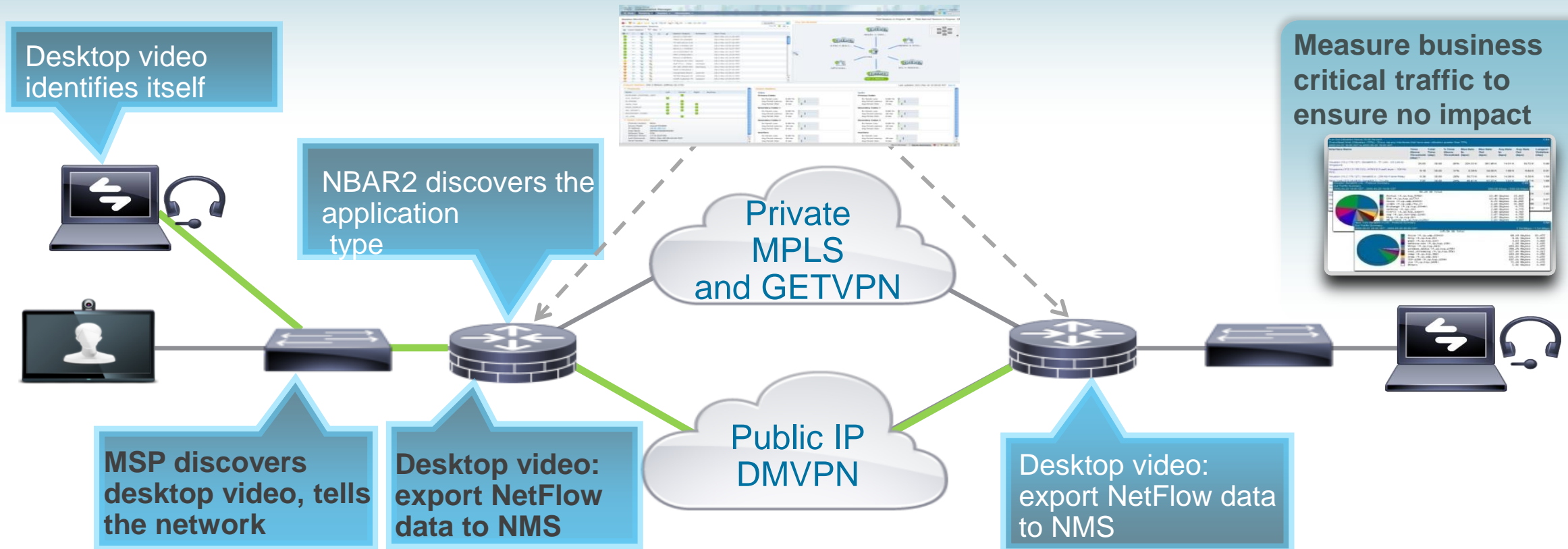
Public IP DMVPN

Traffic remarked back to enterprise values



What Applications are running on your Network?

- Network discovers application type and start monitoring important traffic
- Application attributes exported via Flexible NetFlow that can be visualized by network management systems



Are you using your backup link?

Determination of path based on Metadata Attributes

- Videoconferencing traffic has stringent SLA -> MPLS
- Desktop video traffic is best effort -> DMVPN

Desktop video identifies itself



Desktop video: route traffic to DMVPN



Videoconferencing identifies itself

VC traffic: route traffic to MPLS

Private MPLS and GETVPN

Public IP DMVPN



Application Awareness Methods

How?	Mechanisms	Technologies
Network figures it out	Implicit – Deep Packet Inspection (control signaling protocols for the establishment of sessions, packet headers and payload)	Network Based Application Recognition (NBAR/NBAR2) Media Services Proxy (MSP)
Endpoint/Application directly tells the network what type of applications	Explicit – Endpoint/Application signals to the network	Flow Metadata
Network administrator configures the network	Static configuration	ACLs

Introducing Medianet Flow Metadata

Flow Identifier

Metadata

IP Src	IP Dst	Prot	L4 Src	L4 Dst	Application	Vendor	Dial From	Dial To	Caller ID
10.1.1.2	20.1.1.2	UDP	2000	4000	Video Conference (Audio)	Cisco	83922564	85268229	Albert Albatross

1. Application Creates Metadata



10.1.1.2

2. Metadata Announcement



QoS based on Metadata



3. Media Flow



Export of data to NMS



10.1.1.2

Medianet Flow 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

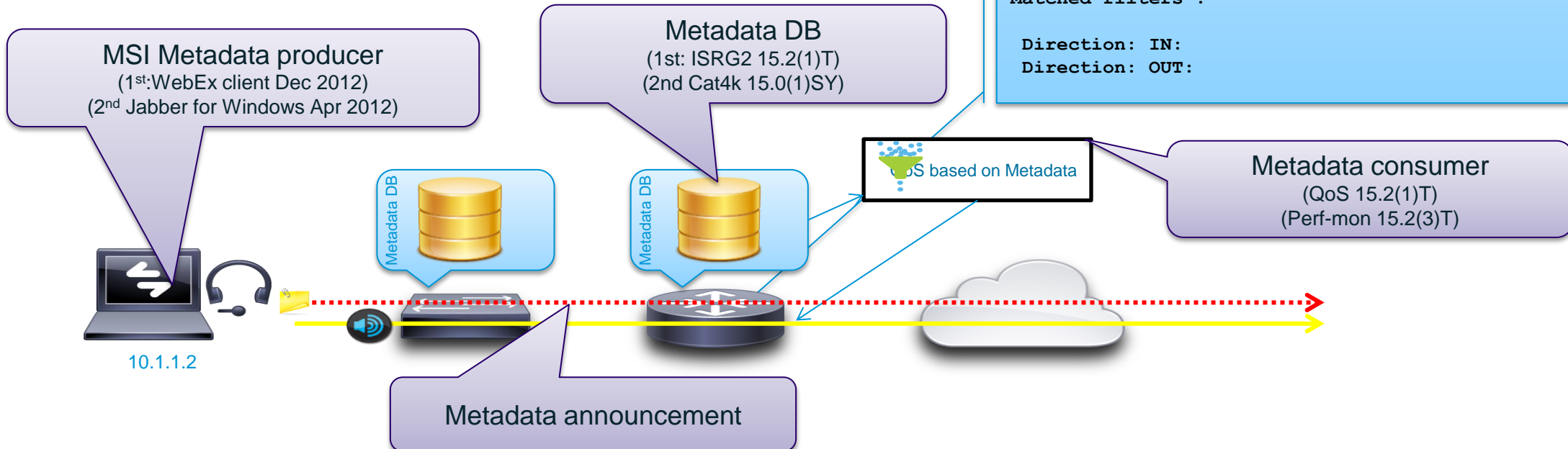
SPort  DPort  Ingress I/F          Egress I/F
24594  16384  Vlan605                n/a
```

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:
```



Metadata – Show Commands

Detailed information about a Flow with attributes

```
router#sh metadata flow local-flow-id 2
To          From          Protocol SPort   DPort   Ingress I/F      Egress I/F
2.2.2.2     1.1.1.1       UDP      3000    30001   Ethernet1/0     Ethernet1/1

Metadata attributes :
Application Vendor      : Cisco Systems
End Point Model        : CTS 3000
Application Name       : rtp
Application Tag        : 218103869 (rtp)
Bandwidth              : 4000
Application Media Type : video
SDP Session ID        : 97388383462821
Mime Type              : H.264
Payload Type           : 96
Clock Frequency       : 22050
SSRC                   : 56
Global Session Id     : 8D44C3FAF803-11E0-91F0-00E0184DFDEA-00000038-00000000
```

Metadata attributes

IOS
15.1(1)SG

match application value	Description
cisco-phone	Cisco IP Phones and PC-based Unified Communicators
citrix	Citrix
h323	H323 protocol
jabber	Jabber Protocol
rtp	Real time protocol
rtsp	Real Time Streaming Protocol
sip	Session Initiation Protocol
telepresence-control	telepresence-control stream
telepresence-data	telepresence data stream
telepresence-media	telepresence media (voice/Video)
vmware-view	VMWARE view
webex-data	WebEX Data
webex-meeting	WebEX Meeting
webex-streaming	WebEX Streaming
xmpp-client	XMPP Client

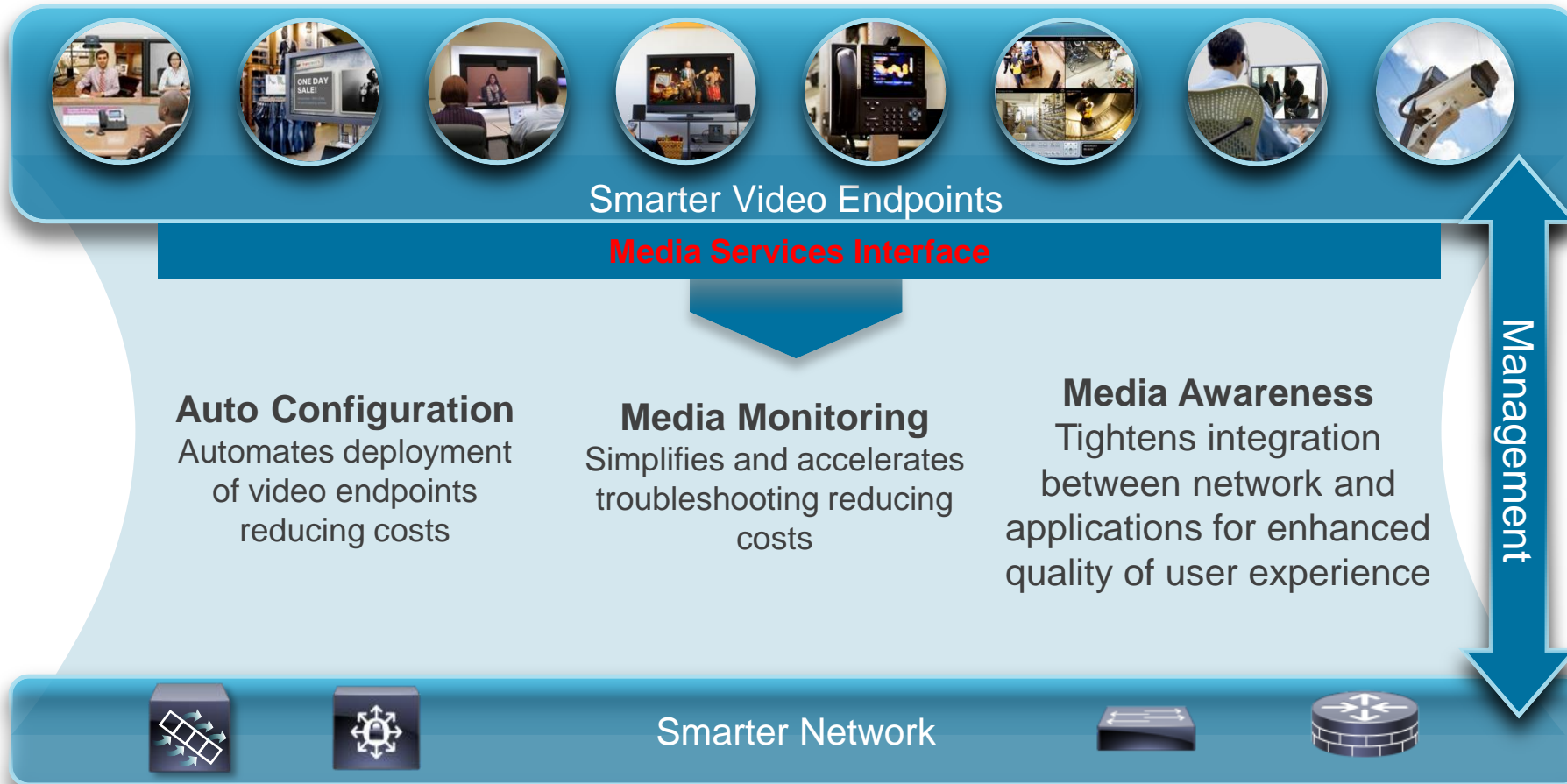
match application vendor value
Axis Communications AB
Cisco Systems, Inc.
Polycom, Inc.
Robert Bosch GmbH
Sony

Metadata attributes – cont.

match application attribute	values
category	business-productivity-tools voice-video
device-class	desktop-conferencing desktop-virtualisation physical-phone room-conferencing software-phone surveillance
media-type	audio control data video voice-video
sub-category	remote-access-terminal voice-video-chat-collaboration

match metadata	values	Description
cac status	admitted un-admitted	RSVP CSC status – eg: to assign different DSCP in QoS
called-uri	WORD (string)	Called entity in SIP/H323 calls
calling-uri	WORD (string)	Calling entity in SIP/H323 calls
device-model	WORD (string)	Device-ID of sender (eg: “phone-model”)
global-session-id	WORD (string)	String identifying all flow of a call-segment (eg: audio + video flows between endpoint and MCU)
multi-party-session-id	WORD (string)	String to identify all flows of a conference call

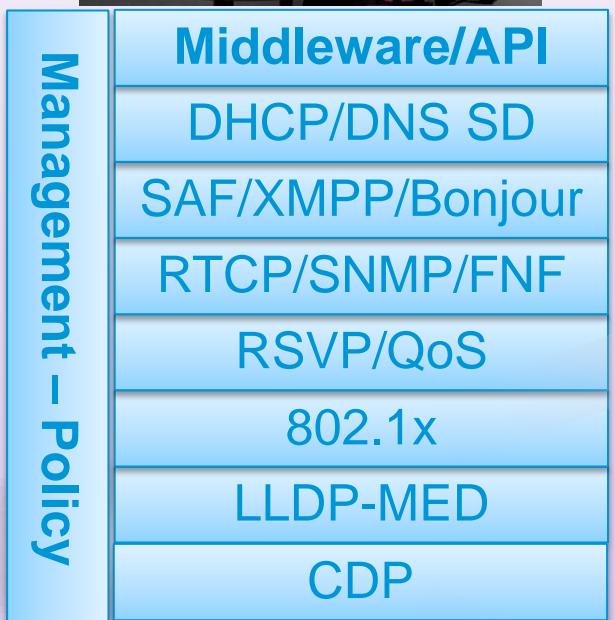
How Medianet Helps?



UC client support (Media Service Interface)



Media Service Interface



Medianet

- Media Services Interface (resides at the video endpoint):
- API
 - Middleware
 - Host Stacks / Protocols

Media Services Interface Deliverables



- MSI Reference implementation
- API SDK
- Simulation - Test environment
- Support - Documentation



Platform Portability Layer:
Win, Mac, embedded Linux, mobile OS

MSI on PCs

PC based Applications

(WebEx, **Jabber for Windows**)

- Separate download on CCO (yes, it's really 'MSI.msi'!)
 - Needs Administrator Rights
 - Runs as Windows Service
 - Shared by all MSI-aware applications
- MSI services enabled (eg. CDP)

Embedded Applications

(EX, C Series, CTS)

- Included in application SW install

```
3945-BB0206-sw#show cdp neighbors fast0/6 detail
```

```
-----  
Device ID: MEDIANET-SITE
```

```
Entry address(es):
```

```
  IPv6 address: FE80::E499:2FBE:56A3:663A(link-local)
```

```
  IP address: 10.4.9.12
```

```
Platform: MSI on Windows,
```

```
Capabilities: Host
```

```
Interface: FastEthernet0/6,
```

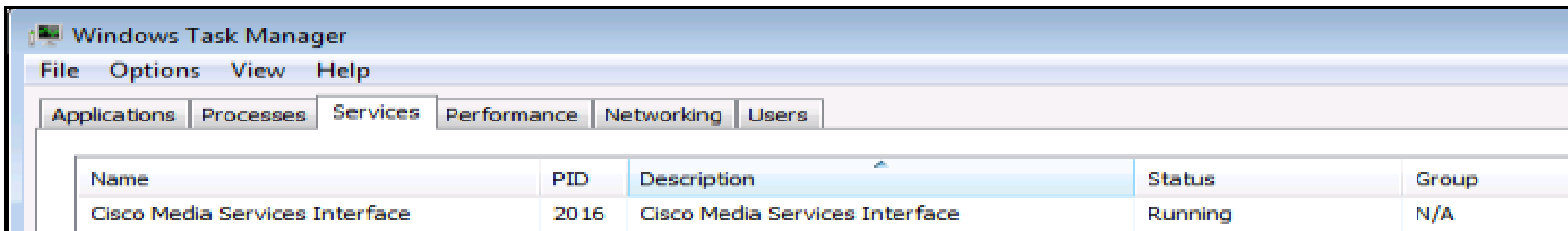
```
Port ID (outgoing port): Local Area Connection
```

```
Holdtime : 165 sec
```

```
Version :
```

```
Microsoft Windows Vista Business Edition (build 6000)
```

```
64 bit
```



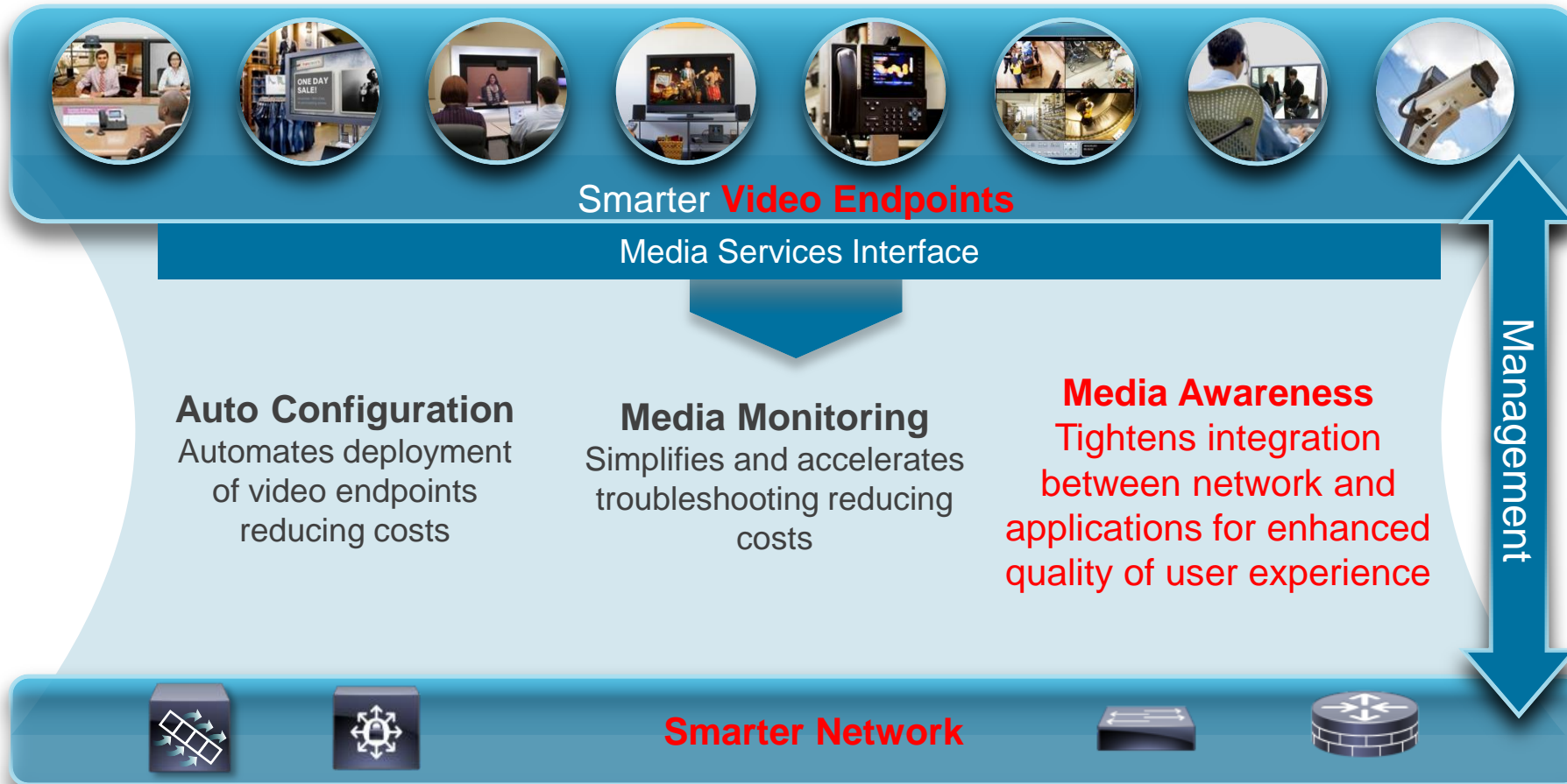
Endpoint and Network Points of Measurement

Metric	Metric	Routers/Switches	MSI
Layer 2	VLAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	MAC address	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IP	IP Address(s)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	DSCP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Transport	RTP - Loss	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	TCP – Loss	<input checked="" type="checkbox"/> (only loss event)	<input checked="" type="checkbox"/>
	TCP Round Trip Time	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	RTP Jitter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Media	Frame Discards	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Frame Repairs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Frame IDR Count	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Ukázka MSI, Metadata



How Medianet Helps?



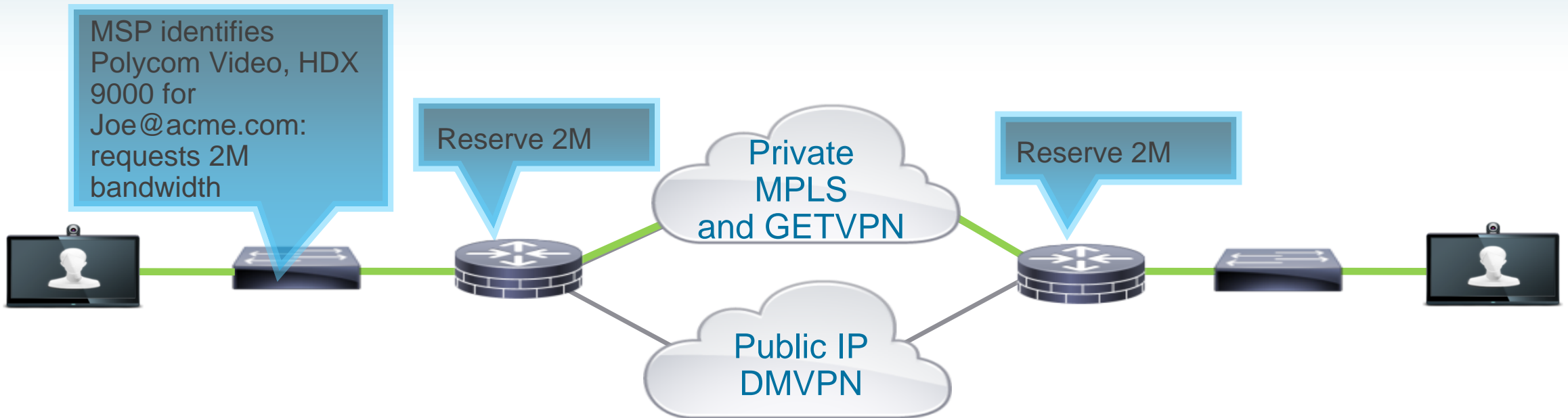
Media Service Proxy



Ensuring QoE

Network Discovers the Application and Reserves Bandwidth

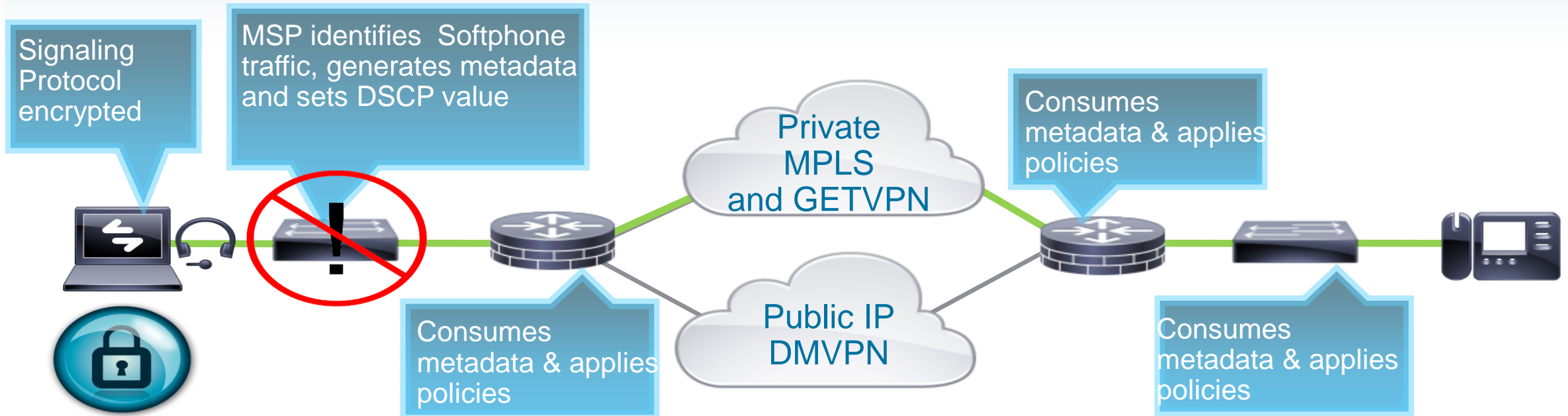
- MSP discovers Polycom Videoconferencing traffic
- MSP reserves network resources on behalf of the Polycom endpoint



Ensuring QoE

Network Discovers the Application and Assigns the DSCP values

- MSP identifies VoIP flows via SIP/SDP, H.225/H.245
- What if control signaling protocols are encrypted? Signals need to be visible!



Metadata for non-MSI Devices

Devices that do not support MSI may be provided supplementary services by **Media Services Proxy (MSP)**

MSP generates 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

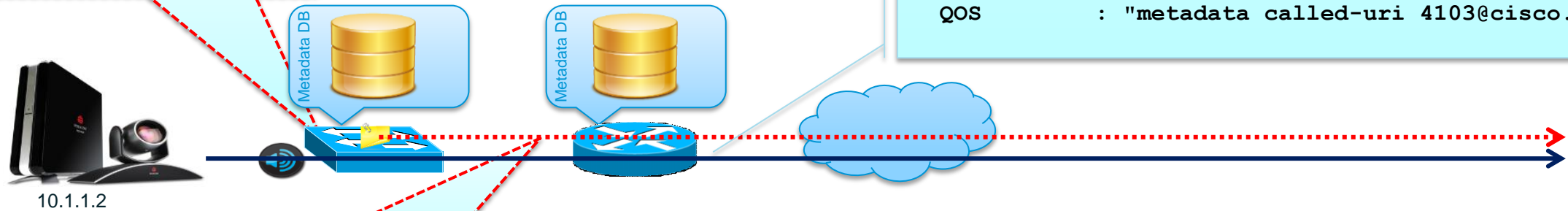
Metadata Attributes :

Called URI	:	4103@cisco.com
Calling URI	:	vputtasu.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"

MSP Creates Metadata from signaling



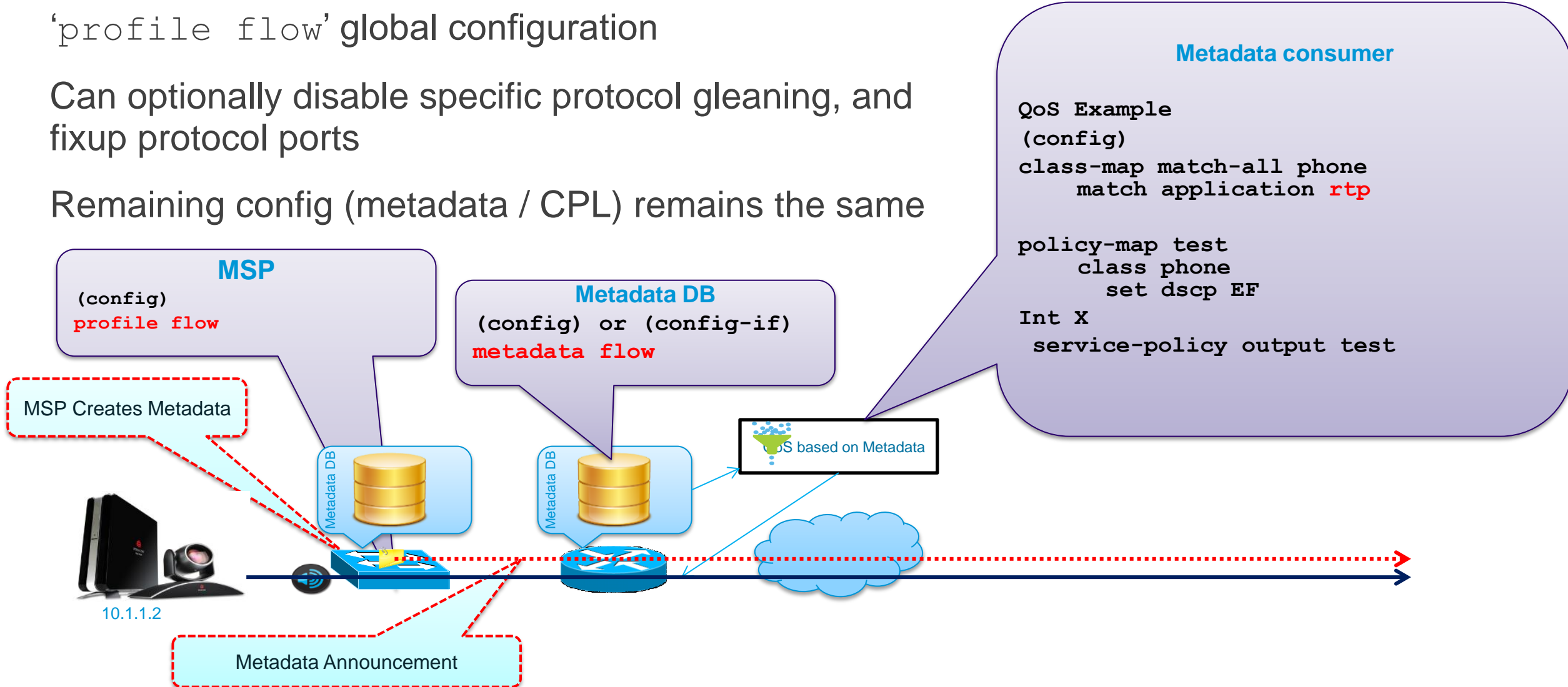
Metadata Announcement

Enabling MSP

'profile flow' global configuration

Can optionally disable specific protocol gleaning, and fixup protocol ports

Remaining config (metadata / CPL) remains the same



Compare and Contrast: MSI & MSP

Capabilities	MSI	MSP	Considerations
Auto discovery of the endpoint and auto configuration of the switch port	✓	✓	Limited to protocols (SIP, H323, mDNS, CDP, LLDP, SIP, DHCP) supported by MSP – surveillance cameras & collaboration endpoints
Location awareness on endpoints/ applications (learned from the network)	✓	✗	
Auto discovery of services by application	✓	✗	
Performance Monitoring on endpoint	✓	✗	Network can independently monitor traffic
Dynamic troubleshooting on endpoint – Mediatrace	✓	✗	
Identify the flow and apply the appropriate policies (e.g. QoS, monitoring, routing, etc.)	✓	✓	MSP recognizes the type of flow by gleaning a limited set of signaling protocols (RTSP, SDP, SIP, H.225, H.245) and they have to be visible to MSP
Application specific information sharing with the network	✓	✓	MSI can share any attributes with the network whereas MSP is limited to what is available from the signaling protocols
Resource reservation	✗	✓	MSP can reserve bandwidth on behalf of the endpoint
3 rd Party support	✓	✓	MSI licensing will be available in Q3CY2012

Metadata Producers



- Metadata producers create metadata announcements

Metadata producers may be anywhere along the flow path

Generally better to be at the source, or near the source

Producers	Notes	Platform/Release
MSI (application)	Direct application integration at source of flow, before flow even starts	WebEx, FR29SP32, Q1CY12 VXC, Q2CY12 CTS, Q3CY12 Tandberg, TC6/TE6, Q3CY12
NBAR (routers)	DPI used to create metadata attributes then share downstream	ISRG2 15.2(4)M Q3CY12 ASR1k,
MSP (routers & switches)	Light-weight DPI to create metadata attributes. Used locally or downstream	ISRG2 15.2(3)T Q2CY12 Catalyst 4k 15.1(1)SG Q3CY12

Metadata Consumers

What can use Metadata



Consumer	Function	Platform/Release
QoS / C3PL	QoS services (match, remark, WRED, shape etc)	ISRG2 15.2(3)T Q2CY12 ASR1k XE3.7 Q3CY12 Cat4k 15.1(1)SG Q3CY12 Cat6k/Sup2T MA2 Q4CY12
Flexible NetFlow (FNF)	Reporting of metadata attributes	ISRG2 15.2(4)M Q3CY12
Performance Monitoring		ISRG2 15.2(3)T Q2CY12 ASR1k XE3.7 Q3CY12
Policy Based Routing	Determination of path based on metadata attribute	ISRG2 Q4CY12

Medianet support



Medianet Feature Availability

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

 WBS29.SP32 ✓ 1H2012	 Digital Media Player 4310G/4400 ✓	 4300/4500 Series HD Box Cameras ✓	 Jabber for Windows ■ 1H2012 ■ 2H2012	 VXI ■ 2H2012 ■ 2H2012	 TP CTS ■ 2H2012 ■ 2H2012	 TP C & Ex Series ■ 2H2012 ■ 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

 Cisco ISR G2 2900/3900 Series ✓ Q1 2012 ✓ Q1 2012	 Cisco ISR 880/890 Series ✓	 Catalyst 2960S/2960 Series ✓	 Catalyst 3750/3560 Series ✓	 Catalyst 4500/4900 Series ✓ 1H2012 ✓ 1H2012 ✓ 1H2012	 Catalyst 6500/6500-E Series ■ 2H2012	 Cisco ASR 1000 Series ✓ ■ 2H2012
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Medianet Readiness Assessment Service

Conclusion

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

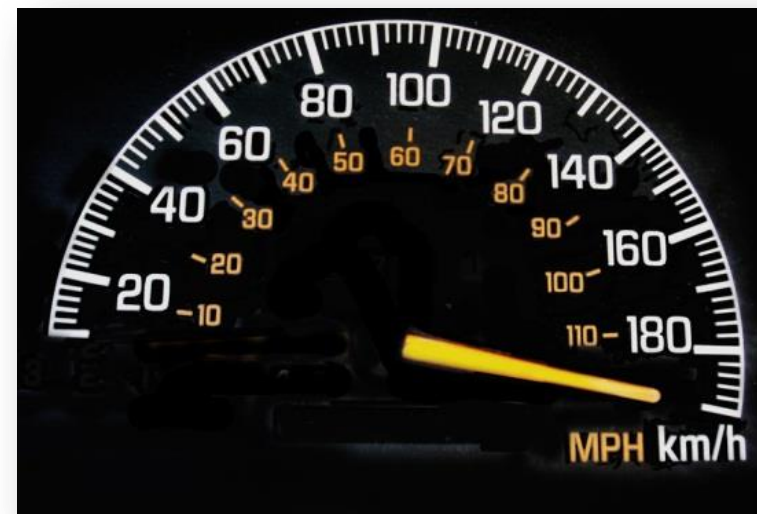
- IPSLA VO, Performance-Monitor

Troubleshooting

- Performance Monitor, Mediatrace, CPCCM, IPSLA VO

Scalable Control and Policy

- Media Service Proxy, Auto Smart Ports, Metadata, MSI



Kde najít informace?



Additional Medianet Resources

- **Medianet on Cisco.com:** **Part of SRND!**
<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 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>

Prosíme, ohodnotte
tuto přednášku.

Děkujeme za pozornost.

