TOMORROW starts here.

cisco

Cisco live!

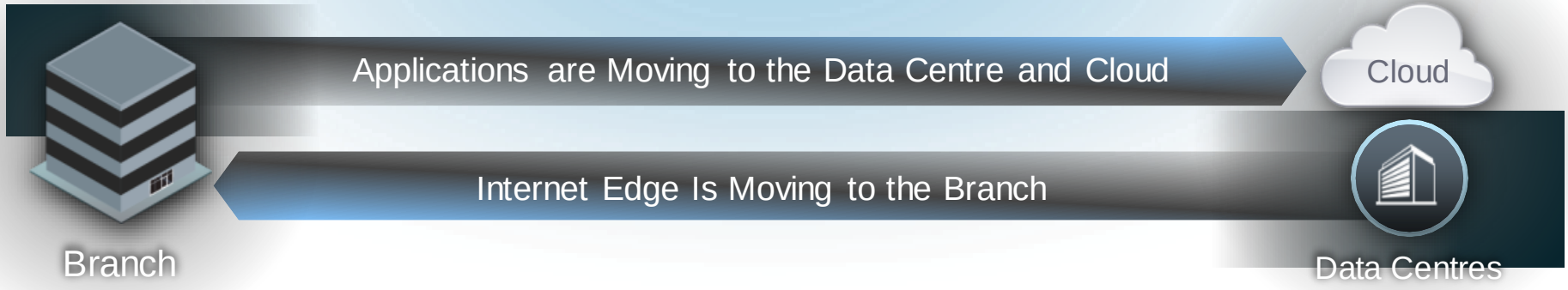
Application Visibility and Control in Enterprise WAN

BRKRST-2030

Liad Ofek
Manager, Technical Marketing – Application Experience Services
Enterprise Networking Group
Cisco

Cisco live!

Emerging Branch Demands
The Application Landscape Is Changing



Pressures on the WAN

Cloud

50% of CIOs Expect to Operate via the Cloud by 2015

Mobility

6X More Mobile Data Traffic by 2015

Fat Apps

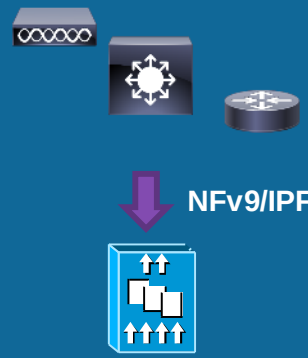
2/3 Of Mobile Traffic will be Video

What is Application Visibility and Control (AVC)

What is Needed

Application Recognition

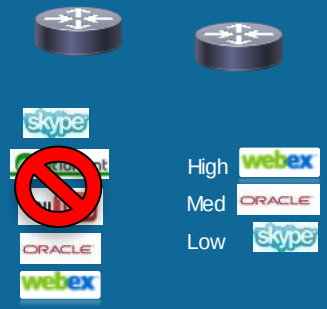
Identify applications using L3 to L7 information



Reporting Tools

Perf. Collection & Exporting

Collect application performance metrics, and export to management tool



Control

Control application network usage to improve application performance

App Visibility & User Experience Report

App	BW	Transaction Time	..
SAP	3M	150 ms	..
Sharepoint	10M	500 ms	..

Management Tool

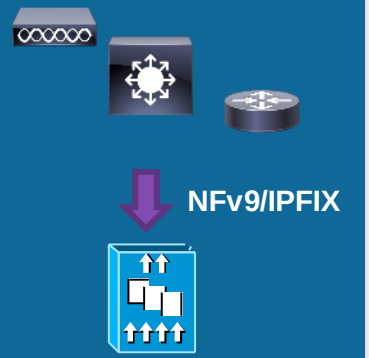
Advanced reporting tool aggregates and reports application performance

What is Application Visibility and Control (AVC)

Enabled Technologies

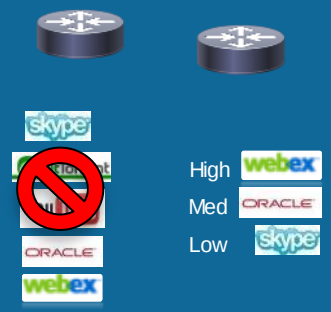
Application Recognition

- NBAR2
- Metadata



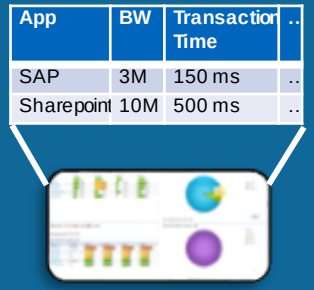
Perf. Collection & Exporting

- Unified Monitoring
  - Traffic Statistics
  - Response Time
  - Voice/Video Monitoring
  - URL Collection



Control

- QoS (w/ NBAR2)
- PfR



Management Tool

- Cisco Prime Infrastructure
- 3rd Party Tools




Discover - Classification

What is An Application?

HTTP	80
FTP	20/21
POP3	110
IMAP	143
HTTPS	443
SMTP	25

Are these applications?

Or just ports?

What about these?

Global Application ID

- Global Application Id: a unique Id per application reported of all DPI engines in Cisco
  - IOS ISR, IOS-XE ASR1k, Network Analysis Module, IOS Firewall
- A Cisco proprietary format, based on
  - On a L3 protocol, i.e. the IANA protocol type
  - On a L4 protocol, i.e. the IANA well known ports
  - On a L2 protocol, i.e. the Ethertype
  - On a L7 application/protocol: proprietary assignments (NO IANA registry for L7)
- Going to the IETF with this application id encoding
  - "Export of Application Information in IPFIX", RFC 6759

Global Application ID

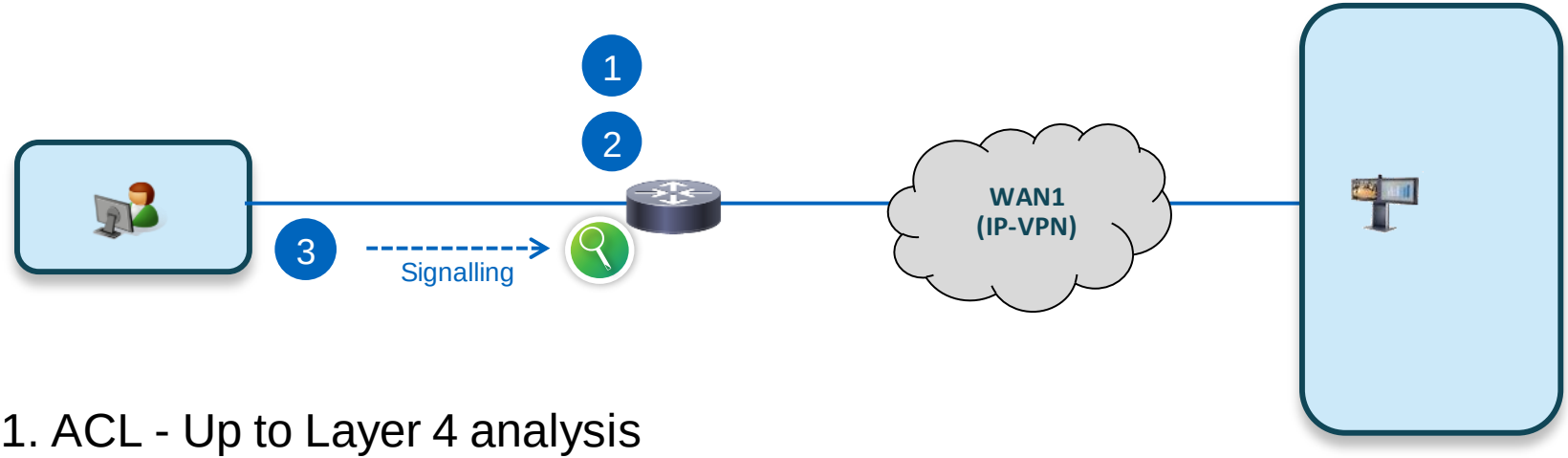
- NBAR2 Application ID Format (4 bytes)


```
router#show flow exporter option application table

Engine: cisco (CISCO_L7_GLOBAL, ID: 13)

appID   Name                  Description
-----   ----                  -----------
13:495  ms-office-365         Microsoft Office 365
13:497  ms-update             Microsoft Update Service
3:80    http                  world wide web

(..snip..)
```

```
router#show flow exporter option application
engines
Engine: prot (IANA_L3_STANDARD, ID: 1)
Engine: port (IANA_L4_STANDARD, ID: 3)
Engine: NBAR (NBAR_CUSTOM, ID: 6)
Engine: cisco (CISCO_L7_GLOBAL, ID: 13)
```

```
router#sh ip nbar protocol-id ms-office-365

Protocol Name              id            type
---------------------------------------------
ms-office-365             495           L7 STANDARD

router#
```

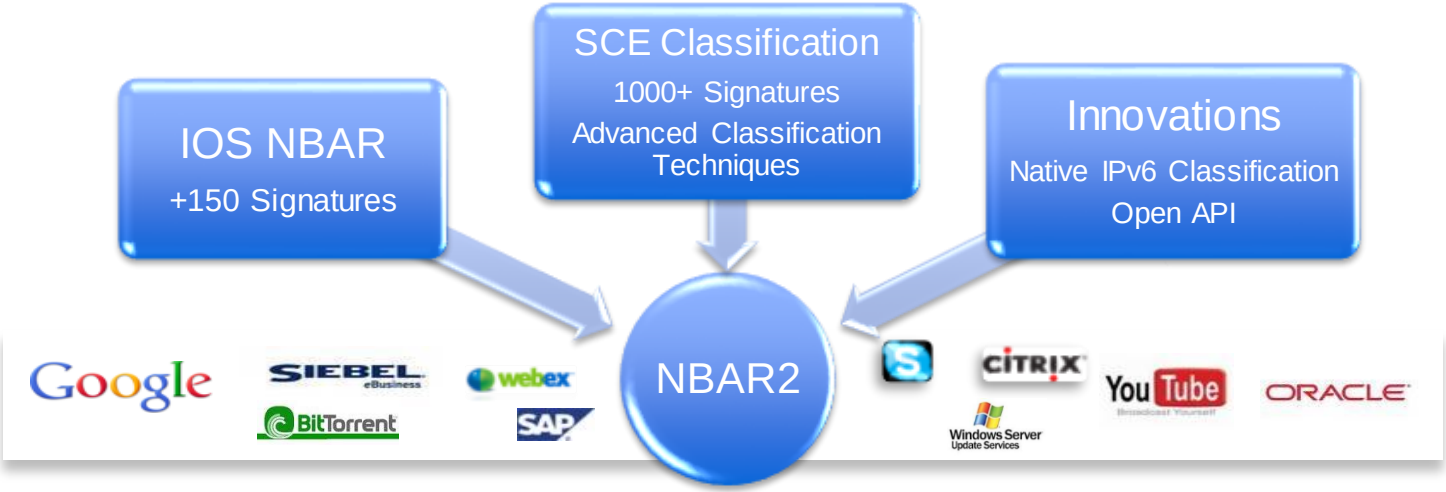
Application Recognition in Enterprise



- 1. ACL - Up to Layer 4 analysis
- 2. Deep Packet Inspection - Up to the application level
- 3. Metadata - Interact with application to go deeper into the end user flows

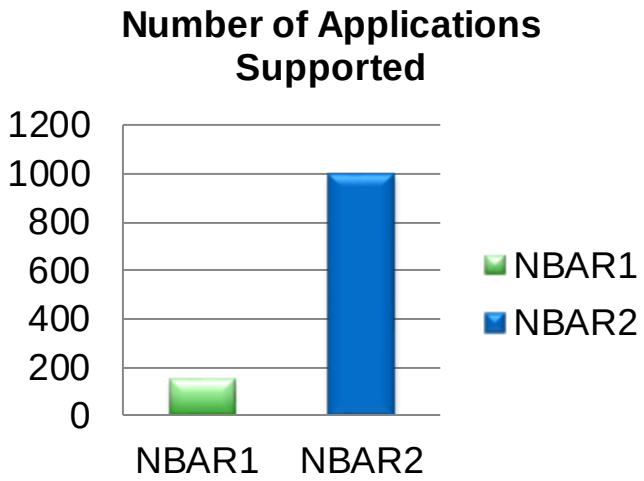
Deep Packet Inspection
Next Generation NBAR (NBAR2)

ISR G2: 15.2(2)T1
ASR1K: 3.4S



- New DPI engine provides Advanced Application Classification and Field Extraction Capabilities from SCE
- Protocol Pack allows adding more applications without upgrading or reloading IOS

NBAR2 Highlight



- More than 1000 applications support and growing
- Categorisation to simplify application management
- In-service signature update through Protocol Pack

HTTP URI

HTTP Hostname

Browser Type

Trafic par hostname

1 - 6 on 116 | 1 | 2 | 3 | 4 | 5 | 6 | 10 | 20

Hits	Hostname	Entrant	Sortant
17	www.cnn.com	546.46 Ko	109.23 Ko
15	ads.cnn.com	54.87 Ko	78.97 Ko
12	i.cdn.turner.com	251.56 Ko	23.64 Ko
12	mi.adinterax.com	608 Octets	1.92 Ko
12	cdn.ndtv.com	-	480 Octets
11	d3.zedo.com	176.28 Ko	37.94 Ko

- Field Extraction – collect application specific information in addition to identify applications
- NBAR2 sub-classification features - Dynamic payload types, SSL sub classification, PCoIP sub classification etc.

Simplify Application Management with NBAR2
Attributes

- NBAR2 attribute provides grouping of similar types of applications
- Use attributes to report on group of applications or to simplify QoS classification
- 6 pre-defined attributes per application (can be reassigned by users)

Category	First level grouping of applications with similar functionalities
Sub-category	Second level grouping of applications with similar functionalities
Application-group	Grouping of applications based on brand or application suite
P2P-technology?	Indicate application is peer-to-peer
Encrypted?	Indicate application is encrypted
Tunneled?	Indicate application uses tunnelling technique

Grouping Apps for Reporting and Classification

For Your Reference

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | root

Home | Design | Deploy | Operate | Report | Administration | Workflows

Applications and Services

Application Server Management

Services

- All Applications
- browsing
- business-and-productivity-tools
- email
- file-sharing
- gaming
- industrial-protocols
- instant-messaging
- internet-privacy
- layer3-over-ip
- location-based-services
- net-admin
- newsgroup
- obsolete
- other
- social-networking
- trojan
- voice-and-video

All Applications

Selected 0 | Total 1381

Edit | Delete | Create | Service | Deploy | Undeploy | View Jobs | Show All

Application Name	Business...	Category	Sub Category	P2P	Tunnel	Encrypted
001myapp	No	other	other	Unassigned	Unassigned	Unassigned
3com-amp3	No	other	other	Unassigned	Unassigned	Unassigned
3com-tsmux	No	obsolete	other	Unassigned	Unassigned	Unassigned
3gpp2-a10-pkts	No	other	other	Unassigned	Unassigned	Unassigned
3gpp2-a10-ubs	No	other	other	Unassigned	Unassigned	Unassigned
3gpp2-a11	No	other	other	Unassigned	Unassigned	
3pc	No	layer3-over-ip	other	Unassigned		
802-1ad	No	other	other	Unassigned	Unassigned	
802-1ah	No	other	other	Unassigned	Unassigned	
914c/g	No	net-admin	remote-access-terminal	No	No	No
9pfs	No	net-admin	storage	No	No	No
aarp	No	other	other	Unassigned	Unassigned	Unassigned
acap	No	net-admin	network-management	No	No	No
acas	No	other	other	Unassigned	Unassigned	Unassigned
accessbuilder	No	other	other	Unassigned	Unassigned	Unassigned
accessnetwork	No	other	other	Unassigned	Unassigned	Unassigned
acp	No	other	other	Unassigned	Unassigned	Unassigned
acr-nema	No	industrial-protocols	other	No	No	No
active-directory	No	net-admin	network-management	No	No	No
activesync	No	business-and-productivity-tools	client-server	No	No	Yes
adobe-connect	No	business-and-productivity-tools	remote-access-terminal	No	No	Yes
adtech-test	No	other	other	Unassigned	Unassigned	Unassigned
aed-512	No	obsolete	other	Unassigned	Unassigned	Unassigned
afpovertcp	No	business-and-productivity-tools	backup-systems	No	No	No
afs3	No	other	other	Unassigned	Unassigned	Unassigned

NBAR2 Attributes

Workflow Status 0 0 0 | Support Cases | Alarm Browser | Alarm Summary 0 0 0

ISR G2: 15.2(4)M2
ASR1K: 3.8S

Define Your Own Application in NBAR2

Port

- TCP or UDP
- 16 static ports per application
- Range of ports (1000 maximum)

Payload

- Search the first 255 bytes of TCP or UDP payload
- ASCII (16 characters)
- Hex (4 bytes)
- Decimal (1-4294967295)
- Variable (4 bytes Hex)

HTTP URL

- URI regex
- Host regex

L3/4 Based Definition Coming in XE 3.12

ISR G2: 15.2(4)M2
ASR1K: 3.8S

NBAR2 Custom Application Enhancement

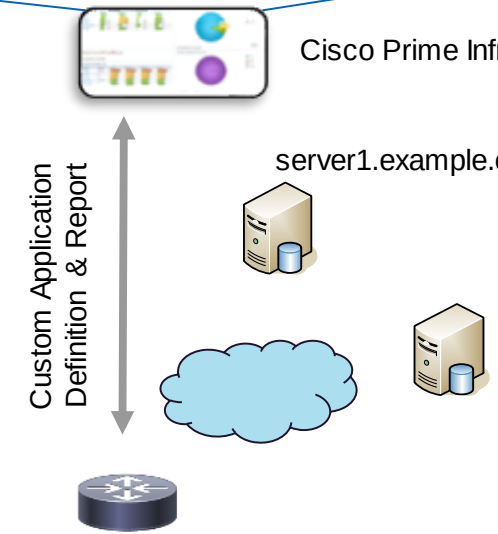
- Custom application match on HTTP URL and/or Host

```
ip nbar custom 001-payroll http host
server1.example.com id 60001

ip nbar custom 002-doc http url doc
host server2.example.com id 60002

ip nbar custom 003-soft http url
software host server2.example.com id
60003
```

Custom App Selector ID

Custom Enterprise Application

Custom App	Server	URI	BW	Resp. Time
My Payroll	server1.example.com	-	2M	100ms
My Doc. Mgmt.	server2.example.com	/doc	1M	250ms
My Software Rep.	server2.example.com	/software	5M	30sec



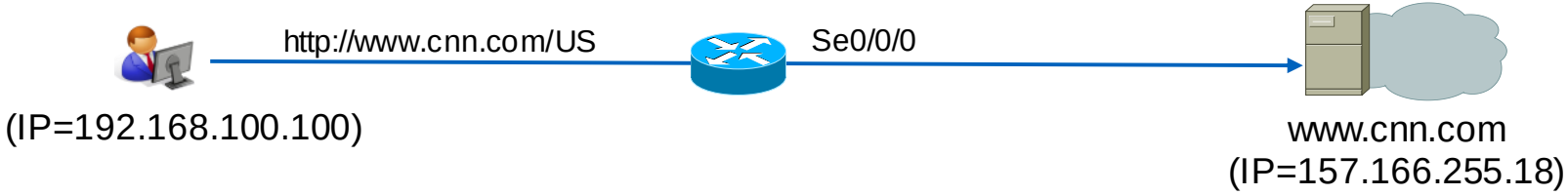
- All the NBAR commands are under “ip nbar…” it is completely unrelated to the IP version.
- Custom application attribute value is set to ‘other’ and ‘unassigned’ by default

NBAR2 Field Extraction
Overview

- Ability to look into specific applications for additional field information
- NBAR2 extracted fields from HTTP, RTP, PCOIP, etc… for QoS configuration
- HTTP Header Fields
- Eases classification of voice and video traffic
  - VoIP, streaming/real time video, audio/video conferencing, Fax over IP
  - Distinguishes between RTP packets based on payload type and CODECS
- Some extracted fields within Flexible NetFlow and Unified Monitoring

NBAR2 Field Extraction

HTTP Example



- Ability to extract information from HTTP message

collect application http host

collect application http url

collect application http user-agent

collect application http referer

```
GET /weather/getForecast?time=37&&zipCode=95035 HTTP/1.1
Host: svcs.cnn.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0)
Gecko/20100101 Firefox/14.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.cnn.com/US/
```

ISR G2: 15.2(4)M2 (*)
ASR1K: 3.8S

NBAR2 Field Extraction Support

Ability to extract certain fields out of protocol for reporting

Protocol Fields	Length	FNF Configuration Syntax
HTTP URL	*	collect application http url
HTTP Host	50	collection application http host
HTTP User-agent	200	collection appllication http user-agent
HTTP Referer	*	collect application http referer
RTSP Host	50	collection application rtsp host-name
SMTP Server	50	collect application smtp server
SMTP Sender	50	collect application smtp sender
POP3 Server	50	collect application pop3 server
NNTP Group Name	50	collect application nntp group-name
SIP Source Domain	50	collect application sip source
SIP Destination Domain	50	collect application sip destination

(*) ISR-G2: URL and Host

Sub Classification
NBAR RTP Payload Type Classification

- Eases classification of voice and video traffic
  - VoIP, streaming/real time video, audio/video conferencing, Fax over IP
- Distinguishes between RTP packets based on payload type and CODECS
- New in PP 7.0
  - audio/video parameters will match not only if the PT is in the known static range of audio or video, but also if it's in the dynamic range
- Future: audio/video granularity will be not a sub-classification but an actual protocol, so the report will show it well.

CODEC	Payload Type
G.711 (Audio)	0 (mu-law) 8 (a-law)
G.721 (Audio)	2
G.722 (Audio)	9
G.723 (Audio)	4
G.728 (Audio)	15
G.729 (Audio)	18
H.261 (Video)	31
MPEG-1 (A/V) MPEG-2 (A/V)	14 (Audio), 32 (Video), 33 (A-V)
Dynamic	96–127

```
Router(config-cmap)# match protocol rtp ?
 audio                    match voice packets
 payload-type             match an explicit PT (Payload Type)
 video                    match video packets
```

NBAR2 Field Extraction
Sub-application ID Format

- NBAR2 Sub-application ID Format (variable length)

```
flow record MYRECORD
 collect application http host
```

4 bytes	2 bytes	Variable length
NBAR App ID	**Sub App ID**	**Extracted Value**
0x03000050	0x3402	www.cisco.com

Extracted value

NBAR Sub-application ID – from show ip nbar parameters extraction and sub-application-table option template. Only take the last two bytes, 0x3402 = HTTP Host

NBAR Application ID, i.e. 0x03000050 = HTTP

NBAR2 and Encrypted Traffic

Overview

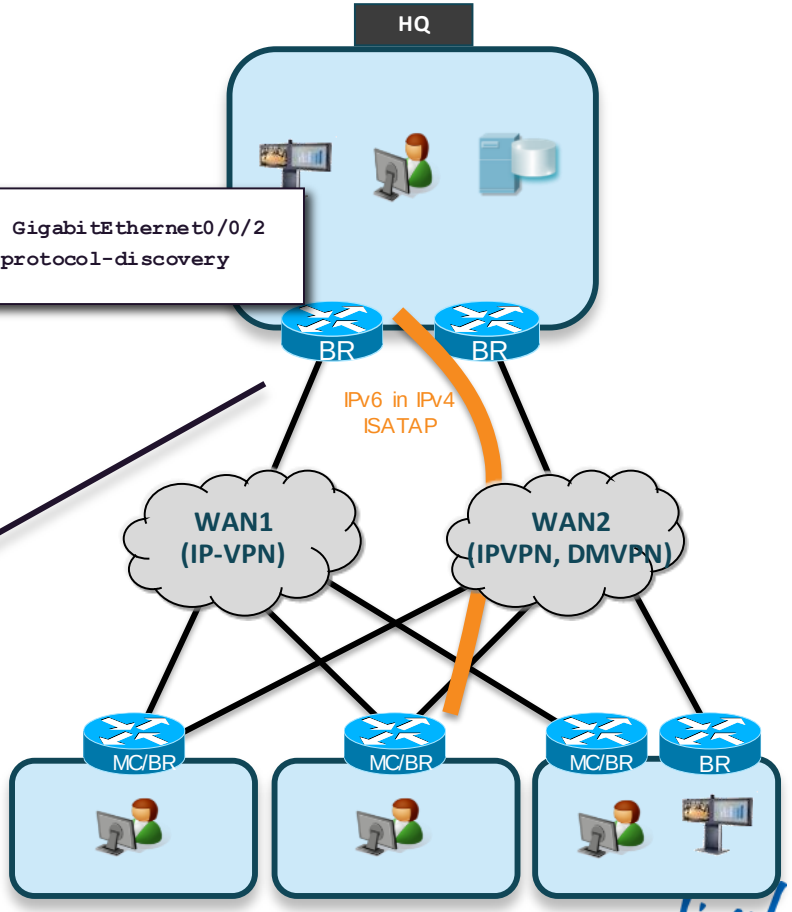
70+

- With heuristics based classification, NBAR can classify 70+ encrypted applications.

Protocol Discovery
IPv4 and IPv6 Classification

- Discover application protocols transiting an interface, and populate CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- Supports both input and output traffic
- Stateful application classification for IPv6 in IPv4 traffic
- Detection of IPv6 in IPv4 traffic (ISATAP, Teredo,6to4,..)

```
interface GigabitEthernet0/0/2
 ip nbar protocol-discovery
```




```
With IPv6 tunnel inspection turn ON, NBAR classifies
this flow as "HTTP"

interface Gi1/1
  ip nbar classification tunneled-traffic ?
             ipv6inip Tunnel type ISATAP, 6to4 and 6RD
             teredo   Tunnel type TEREDO
```

How NBAR2 can be Used

- Protocol Discovery – “ip nbar protocol-discovery” CLI
  - Discovers and provides real time statistics on applications
  - IPv4 and IPv6 supported
  - IPv6 in IPv4 tunnel inspection
  - Accounting: per-interface, per-application, bi-directional statistics: Bit rate (bps), Packet counts and Byte counts
  - Information available in the CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- Invoke ‘match protocol’ CLI in C3PL/MQC (class-map) CLI
  - Application optimisation
  - Used in a number of different IOS functions (QoS, performance monitor, IOS FW)
- With Flexible NetFlow (regardless of QoS)
  - Invoke ‘match|collect application name’ fields in flexible netflow (FNF)
  - Application name/ID is included in NetFlow export reports

NBAR2 – Regular Updates

In-service Application Definition Update

PPX (Major)
- protocols~ 10
- updates and fixes

1M →

PPX.1 (Minor)
- Bug fixes
- small updates

1M →

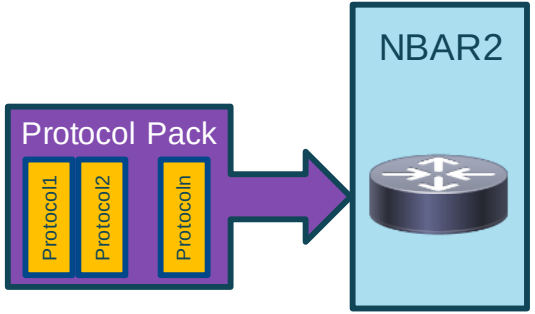
PPY (Major)
- Protocols~10
- updates and fixes

1M →

PPY.1 (Minor)
- Bug fixes
- small updates

PP 7.1 Available

- Advanced Protocol Pack
  - Includes all supported Protocols / Applications
  - Support Traffic categorisation and Attributes
  - Available (as Default protocol pack) in DATA image
  - Periodic releases and Offers SLA
- Useful Pointers:



Protocol Library

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Protocol List and Version support

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6616/product_bulletin_c25-627831.html

NBAR2 Protocol Pack
Example

For Your Reference

Download Software

Download Cart (0 items) [+] Feedback Help

Downloads Home > Products > Routers > WAN Aggregation and Internet Edge Routers > Cisco ASR 1000 Series Aggregation Services Routers > Cisco ASR 1002-X Router > **NBAR2 Protocol Packs-7.1.0**

Cisco ASR 1002-X Router

Search...

Expand All | Collapse All

- Latest Releases
  - 7.1.0
  - 6.2.0
  - 7.0.0
  - 6.1.0
- All Releases
  - 7.1
  - 7.0
  - 6.2
  - 6.1
  - 6.0
  - 5.1
  - 5.0
  - 4.0
  - 3.1
  - 3.0
  - 2.0

Release 7.1.0

Release Notes for 7.1.0 | Add Device | Add Notification

File Information	Release Date	Size	
NBAR2 Advanced Protocol Pack 7.1.0 for IOS-XE 3.9.0S Version 15.3(2)S pp-adv-asr1k-153-2.S-15-7.1.0.pack	21-OCT-2013	0.25 MB	Download Add to cart Publish
NBAR2 Advanced Protocol Pack 7.1.0 for IOS-XE 3.10.0S Version 15.3(3)S pp-adv-asr1k-153-3.S-16-7.1.0.pack	21-OCT-2013	0.25 MB	Download Add to cart Publish

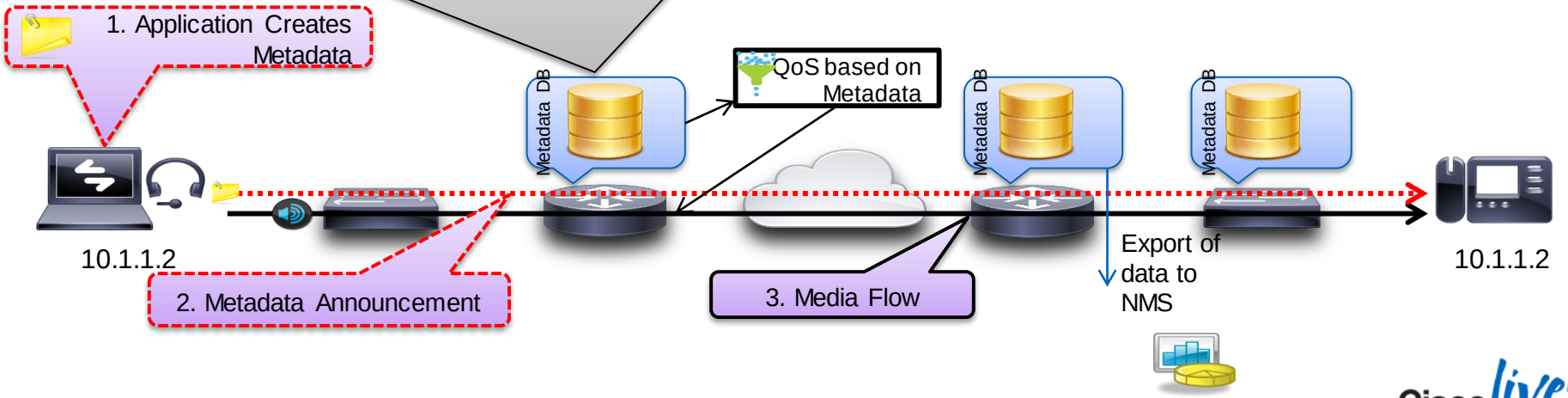
- Add new applications recognised by NBAR2 without IOS upgrade or router reload
- New protocol pack is published every two months on CCO
- Single IOS CLI to enable the protocol pack

Flow Metadata Principles

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






Performance Collection

Performance Collection & Exporting
What is it?

- **Integrated** performance monitoring available for different type of applications and use cases

Performance Collection

Voice and Video Performance
(Media Monitoring)

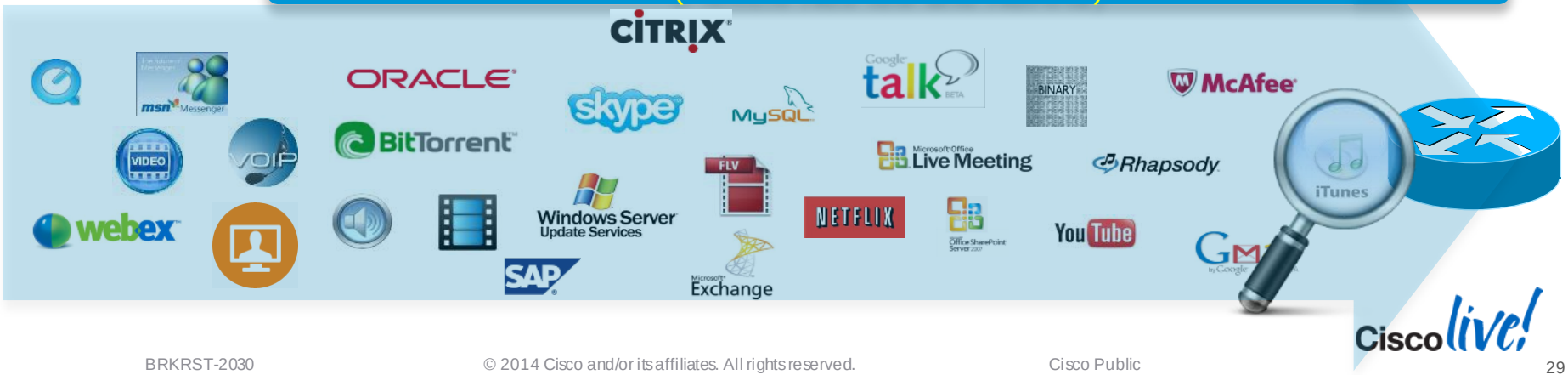
30% of bandwidth is voice and video

Critical Applications Performance
(Application Response Time)

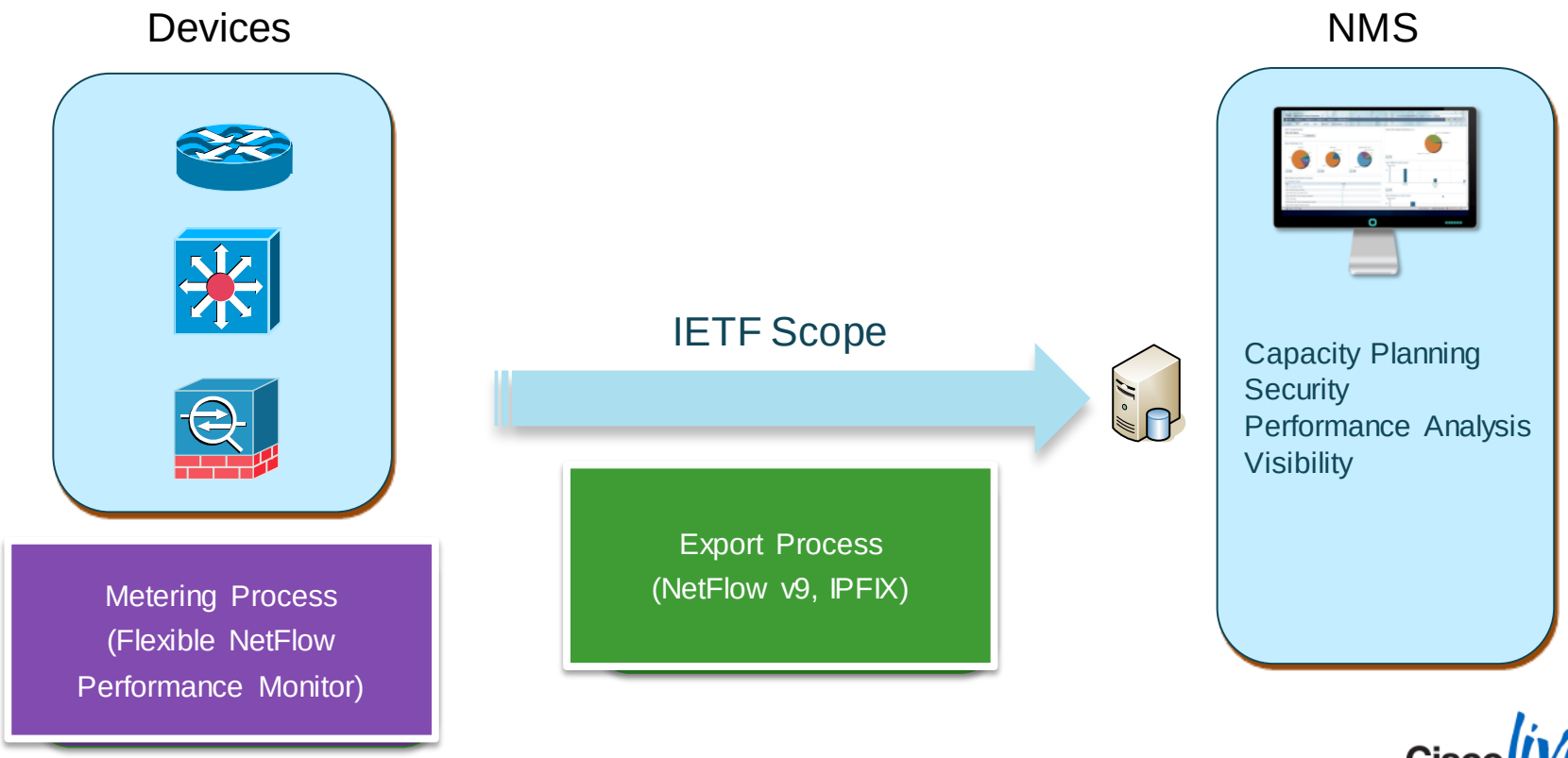
40% of bandwidth is critical applications

Traffic Statistics

What applications, how much bandwidth, flow direction?
(Flexible NetFlow and NBAR2)



Performance Monitoring
Foundation Overview



Foundation: Metering Process

NetFlow Key Fields vs Non-key Fields

Key Fields	Packet 1
Source IP	1.1.1.1
Destination IP	2.2.2.2
Source port	23
Destination port	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Non-key Fields	**Packet 1**
Length	1250

- IPv4 and IPv6 support
- Key fields are unique per flow record (match statement)
- Non-key fields are attributes or characteristics of a flow (collect statement)
- If packet key fields are unique, new entry in flow record is created
  - First packet of a flow will create the Flow entry using the Key Fields"
  - Remaining packets of this flow will only update statistics (bytes, counters, timestamps)
- Otherwise, update the non-key fields, i.e. packet count

Key Fields	Packet 2
Source IP	3.3.3.3
Destination IP	4.4.4.4
Source port	80
Destination port	22079
Layer 3 Protocol	TCP - 6
TOS Byte	0
Non-key Fields	**Packet 2**
Length	519

NetFlow Cache After Packet 1

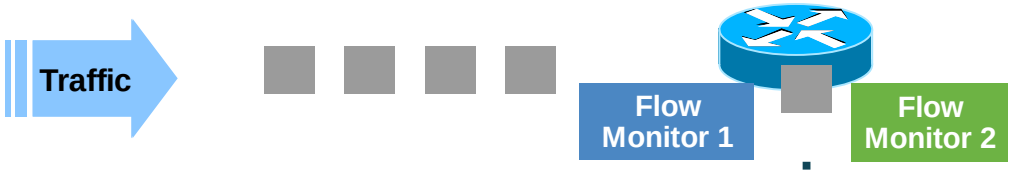
Source IP	Dest. IP	Dest. I/F	Protocol	TOS	…	Pkts
1.1.1.1	2.2.2.2	E1	6	0	…	11000

NetFlow Cache After Packet 2

Source IP	Dest. IP	Dest. I/F	Protocol	TOS	…	Pkts
3.3.3.3	4.4.4.4	E1	6	0	…	50
1.1.1.1	2.2.2.2	E1	6	0	…	11000

Foundation: Metering Process

Multiple Monitors with Unique Key Fields



Key Fields	Packet 1
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source Port	23
Destination Port	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Non-Key Fields
Packets
Bytes
Timestamps
Next Hop Address

Key Fields	Packet 1
Source IP	3.3.3.3
Destination IP	2.2.2.2
Input Interface	Gi0/1
SYN Flag	0

Non-Key Fields
Packets
Timestamps

Traffic Analysis Cache

Source IP	Dest. IP	Source Port	Dest. Port	Protocol	TOS	Input I/F	…	Pkts
3.3.3.3	2.2.2.2	23	22078	6	0	E0	…	1100

Security Analysis Cache

Source IP	Dest. IP	Input I/F	Flag	…	Pkts
3.3.3.3	2.2.2.2	Gi0/1	0	…	11000

Foundation: Metering Process

Cache Types

Normal

- Similar to today's NetFlow
- More flexible active and inactive timers: one second minimum

Immediate

- Flow accounts for a single packet
- Desirable for real-time traffic monitoring, DDoS detection, logging
- Desirable when only very small flows are expected (ex: sampling)
- Caution: may result in a large amount of export data

Permanent

- To track a set of flows without expiring the flows from the cache
- Entire cache is periodically exported (update timer)
- After the cache is full (size configurable), new flows will not be monitored
- Uses update counters rather than delta counters

Synchronised

- Exports on a regular basis
- Used by ART and Media

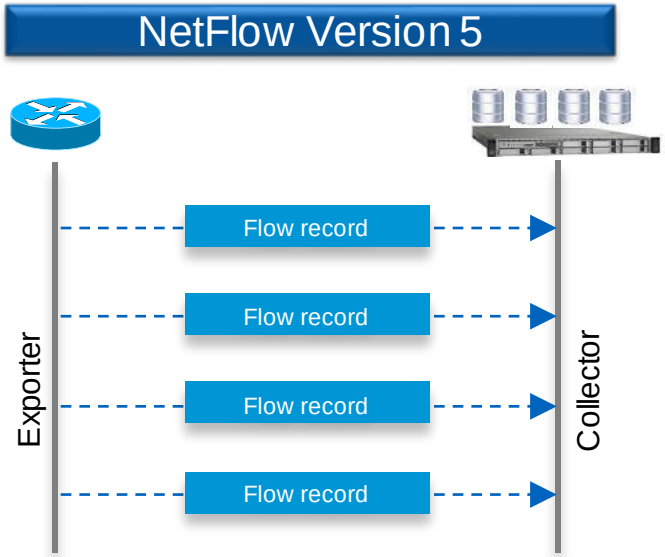
Transaction-End

- A transaction is a set of logical exchanges between endpoints
- Generates the record in the NetFlow cache at the end of a transaction.

Foundation: Exporting Process

NetFlow v9 and IPFIX

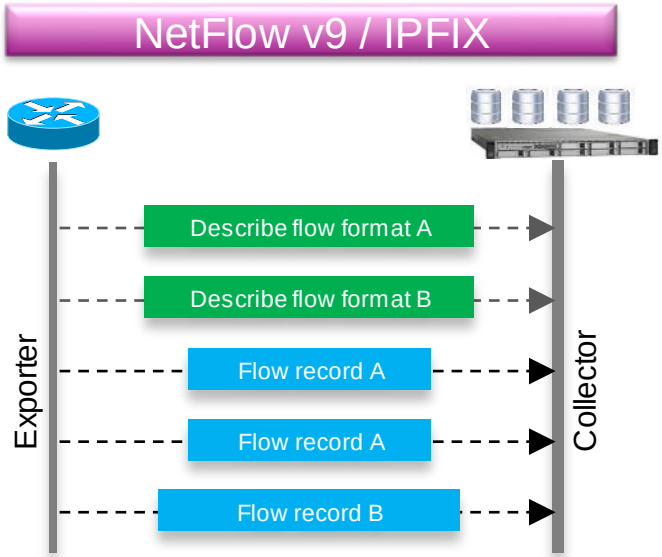
Static Flow Export Format



- Fixed number of fields (18 fields)

  e.g. source/destination IP & port, input/output interfaces, packet/byte count, ToS

Flexible & Extensible Flow Export Format



- Users define flow record format
- Flow format is communicated to collector

Foundation: Exporting Process
Option Templates

- Use for exporting non-traffic related information to netflow collector or reporting tools.
- Available only with Flexible NetFlow

```
flow exporter MYEXPORTER
 destination 10.35.89.59
 source GigabitEthernet0/0/1
 transport udp 2055
 option interface-table timeout 300
 option sampler-table timeout 300
 option application-table timeout 300
```

```
router#show flow exporter MYEXPORTER templates
Flow Exporter insight:
  Client: Option options interface-table
  Exporter Format: NetFlow Version 9
  Template ID    : 256
  Source ID      : 6
  Record Size    : 104
  Template layout
  ----------------------------------------------------
  |       Field            |  Type | Offset |  Size  |
  ----------------------------------------------------
  | v9-scope system        |     1 |      0 |      4 |
  | interface input snmp   |    10 |      4 |      4 |
  | interface name         |    82 |      8 |     32 |
  | interface description  |    83 |     40 |     64 |
  ----------------------------------------------------
```

Foundation: Exporting Process
Available Option Template

Option Template	Definition
application-table	NBAR Application ID to name mapping
application-attributes	Application attributes definition per application
c3pl-class-table	QoS class-map ID to name mapping
c3pl-policy-table	QoS policy-map ID to name mapping
exporter-stats	Exporter Statistics Option
interface-table	Interface SNMP ifIndex to name mapping
Sampler-table	Export Sampler Option
sub-application-table	NBAR Sub-application ID to name mapping
vrf-table	VRF ID to name mapping
queue-id (hidden)	Queue index and queue drop information

Note: Check the IOS release for exact support

What do we want to Monitor?

Application Traffic Stats	Conversation Traffic Stats	URL Visibility	Application Response Time	Media Performance
Filters • DNS/DHT	Filters • Remaining traffic not included in other filters	Filters • HTTP Traffic	Filters • Selected TCP Applications	Filters • RTP Applications
• Traffic statistics per application	• Traffic statistics per application, client and server	• Sample traffic statistics, TCP performance and host/URL data per connection	• Traffic statistics and TCP performance metrics per application, client and server	• Traffic statistics and media performance metrics per application, client and server

We Need More Metrics with Flexible NetFlow

Bytes, Packets, Routing Info (L3 to L4) — FNF

Application ID (L3 to L7) — + NBAR2

Performance Metrics (e.g. MMON, ART)

Network Metrics (e.g. QoS)

Derived Metrics (e.g. URL Hit count)

Other Metrics (e.g. PfR)

Unified Monitoring

Network latency

Response Time

Jitter

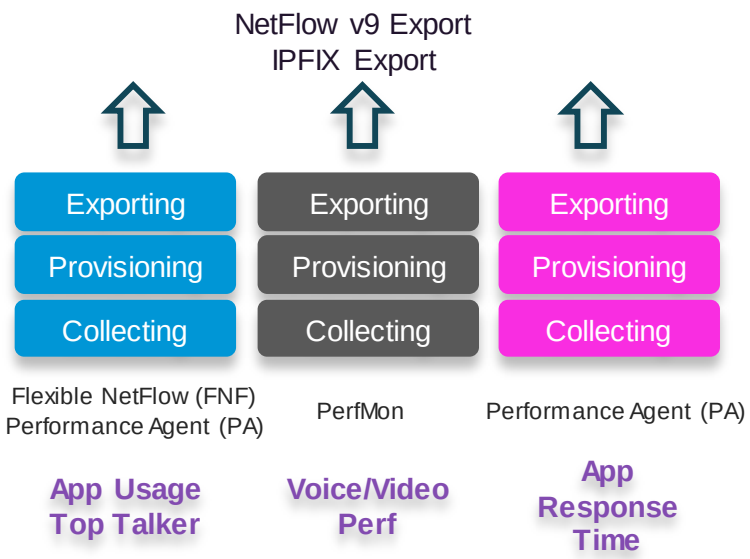
QoS policy/class-map

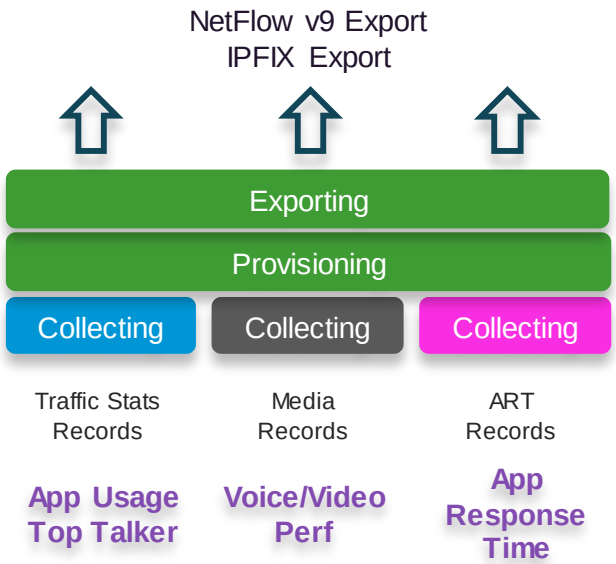
Retransmission

Evolving to Unified Monitoring

NEW

Now Available on IOS and IOS-XE





- Certain metrics available for certain features. Multiple features to configure
- Separate provisioning
- This was the current model for IOS

- All metrics are available within single feature
- Single provisioning
- This is the current model for IOS XE
- This is new in IOS – 15.4(1)T

Unified Monitoring

Metric Mediation Agent (MMA) – Overview

Prime Infrastructure

Partners

Export NetFlow v9 or IPFIX

Metrics Data

Traffic

Application Recognition (NBAR2)

Deep Packet Inspection Engine identifying +1000 applications

Metric Collection (MMA)

Correlation, Aggregation, Alerts
Flexible NetFlow

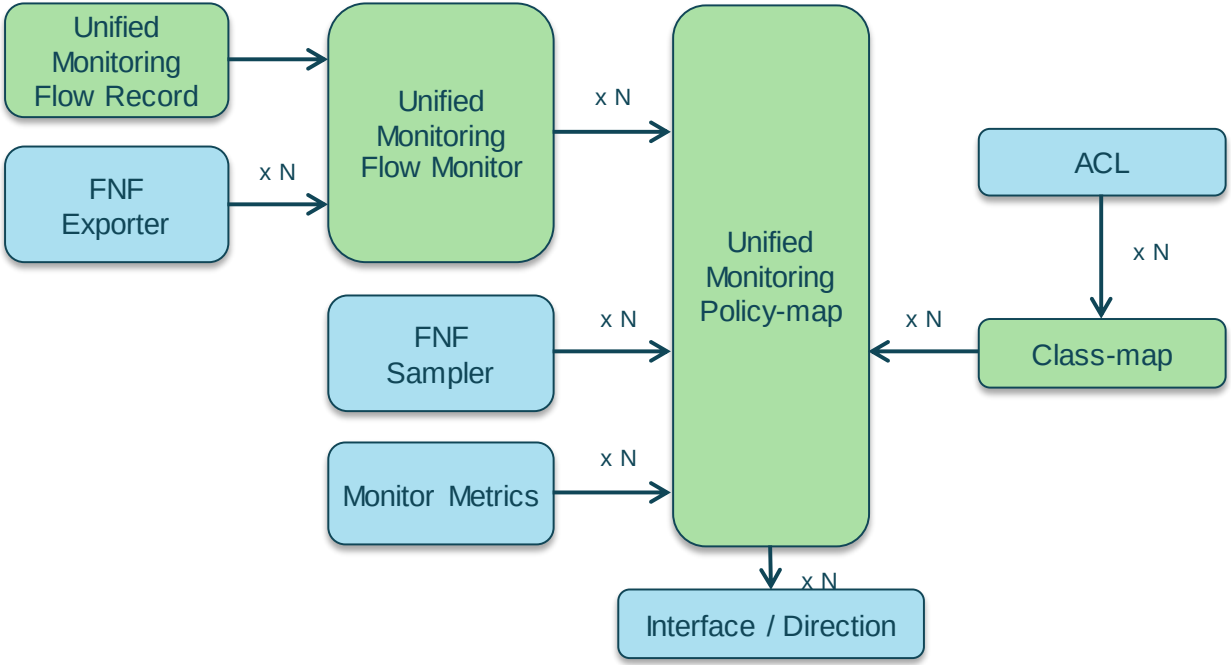
Metric Providers
Traffic Statistics
Application Response Time
Media Performance
URL Collection

Control (QoS)

Application Priorisation
Application Bandwidth Management

Unified Monitoring
Metric Mediation Agent (MMA) – Provisioning

- Flexible, single monitoring policy for voice/video, application, traffic discovery
- Match traffic to monitor using L3, L4, or L7 information
- IPv4 and IPv6 supported
- Collect only relevant information for each traffic type
- Per traffic type sampling



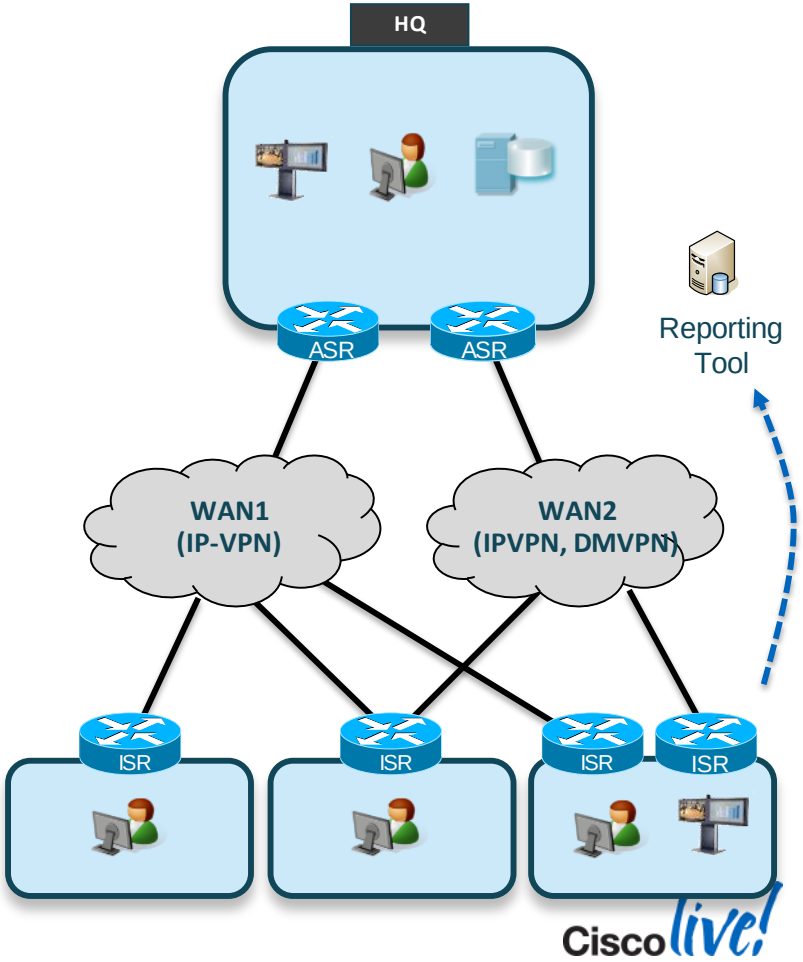
1. Traffic Statistics
Application Usage

Key Features

- Feature to collect and export network information and statistics
- Flexibility in defining fields and flow record format
- NBAR2 Integration
  - Examines data from Layers 3 thru 7
  - Utilises Layers 3 and 4 plus packet inspection for classification
  - Stateful inspection of dynamic-port traffic
- IOS: FNF, PA or MMA
- IOS-XE: FNF or MMA
- Export: NFv9 or IPFIX

Benefits

- Visibility into application usage
- Monitors data in Layers 2 thru 7
- Capacity Planning
- Top-N applications
- Top-N clients and servers



For Your Reference

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | root

Home | Design | Deploy | Operate | Report | Administration | Workflows

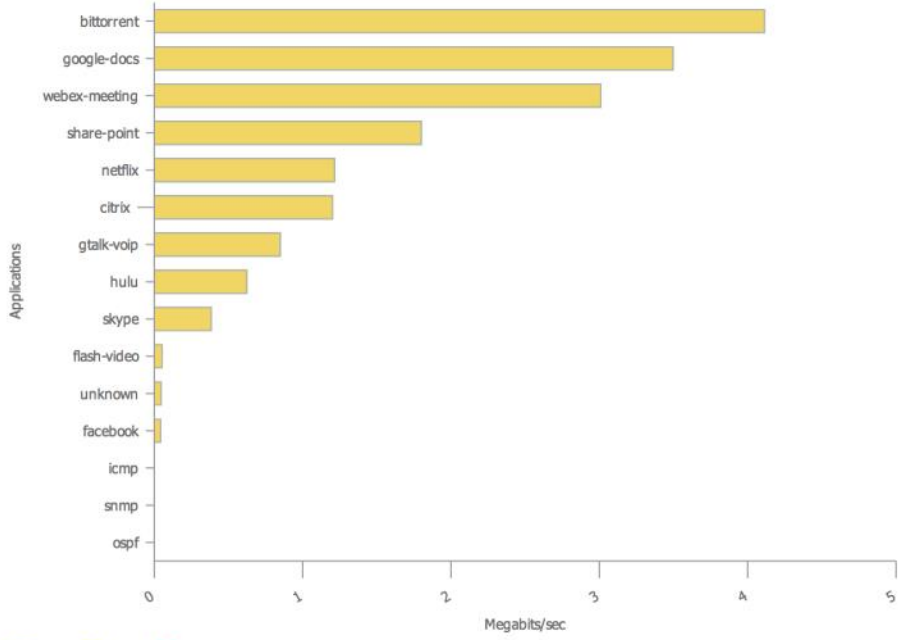
Overview | Incidents | Performance | Detail Dashboards

Site | Device | Interface | Application | Voice/Video | End User Experience | WAN Optimization | Demo Stats | Demo Perf

Top N Applications (with AVC)

Edited

Rate | Volume



Traffic | Wireless | Wired

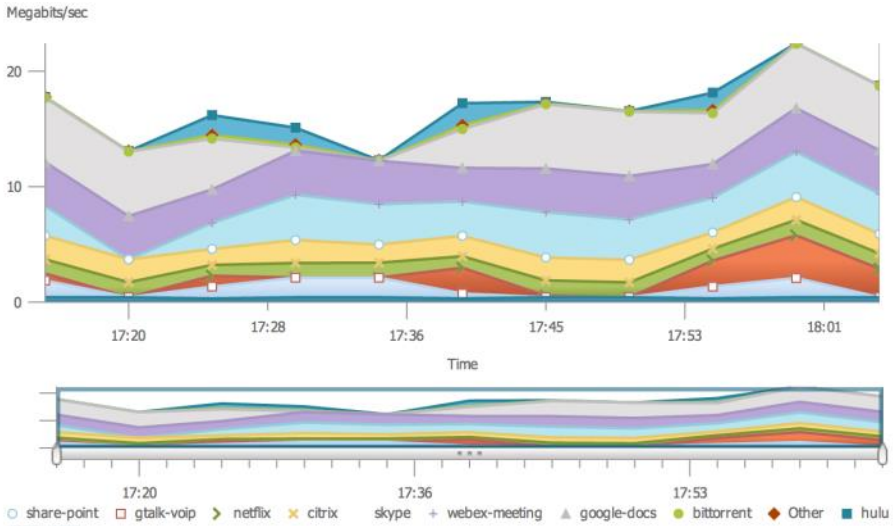
2013 April 02, 18:09:53 CEST

Top Application Traffic Over Time (with AVC)

Edited

Applications | Application Categories

Rate | Volume



2013 April 02, 18:10:04 CEST

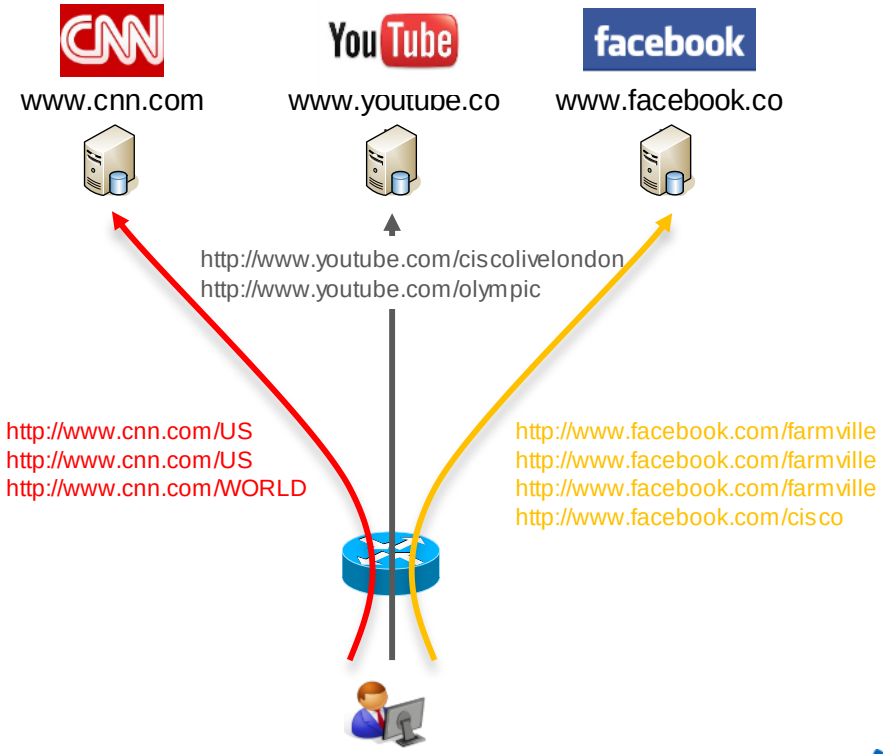
2. URL Collection
Top Domain, hit counts

Key Features

- Provide web browsing activity report
- Standard IPFIX export
- IOS: PA or MMA
- IOS-XE: MMA
- Utilise IPFIX Format which is extensible

Benefits

- Visibility into top domains
- Monitors data in Layers 2 thru 7
- Most visited web site
- Most visited URL per site
- How many hits for a particular domain – extracted from HTTP request message



Top Domain and URL Hit Count Report

Field Extraction Details – ISR-G2 with Performance Agent

ISR-G2: 15.2(4)M2

Field Name	Field ID	Description	Value
application http host	45003	Host name	www.cnn.com
application http uri statistics	42125	List of URI	US\02WORLD\01
art count new connections	42050	Number of new connections	3

- Supported in Performance Agent (PA)
- Provide as a concatenated string that collects the hit count for first level URI and domain.
- Details:
  - ISR-G2: PA will collect and export URI and hit-count in the format “uri:count::uri:count.....”.
  - The delimiters colon (:) and double colon (::) are written here just for the demonstration of the format. The actual delimiter would be NULL (\0)
  - URI and count is always represented in binary format using fixed length 2bytes.
  - The URI being collected and exported is limited to the first ‘/’.

Top Domain and URL Hit Count Report

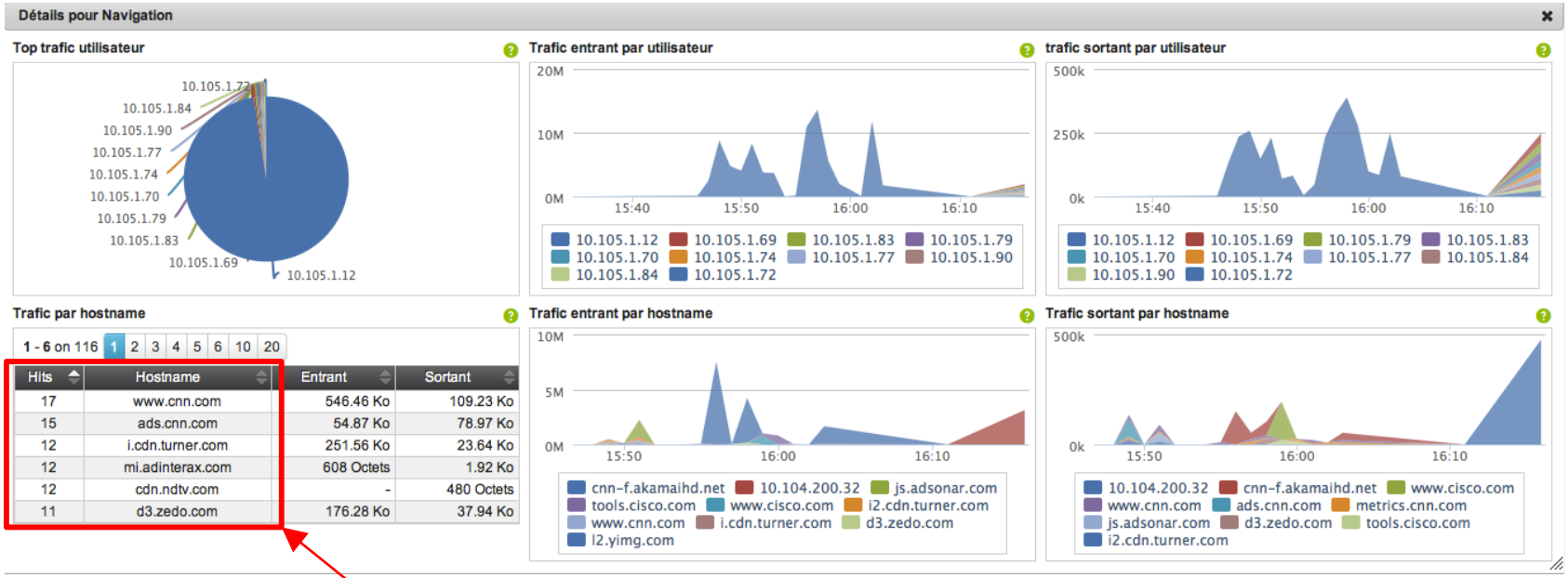
Field Extraction Details – ASR1k/ISR-G2 with Unified Monitoring

ASR1k: XE 3.8S
ISR-G2: 15.4(1)T

Field Name	Field ID	Sub Application	Description	Value
application http host	45003	0x3402	Host name	www.cnn.com
application http url	45003	0x3401	URI	US
application http uri statistics	42125	-	List of URI	US\02WORLD\01

- Pre XE3.10 (Unified Monitoring)
  - Only URL and Host are supported.
  - In a typical configuration it should be exported using a connection/transaction records with export on transaction-end. So hit count =1, each URL is exported on a different record.
  - We will target to have nested monitors with structured data to export such metric with associated info (for example to add bytes/packets/art per URI and not only hits).
- XE3.10, XE3.11 (Unified Monitoring)
  - URI statistic field Supported
  - Allowed only in connection/transaction records so the hit-count is always 1.
  - The reason for adding this field is to limit the URL size.
- Post 3.11 (Unified Monitoring)
  - We will target to have nested monitors with structured data to export such metric with associated info (for example to add bytes/packets/art per URI and not only hits).

Example: URL Hit Count Report



How many hits for a particular domain – extracted from HTTP request message

Courtesy of LivingObjects

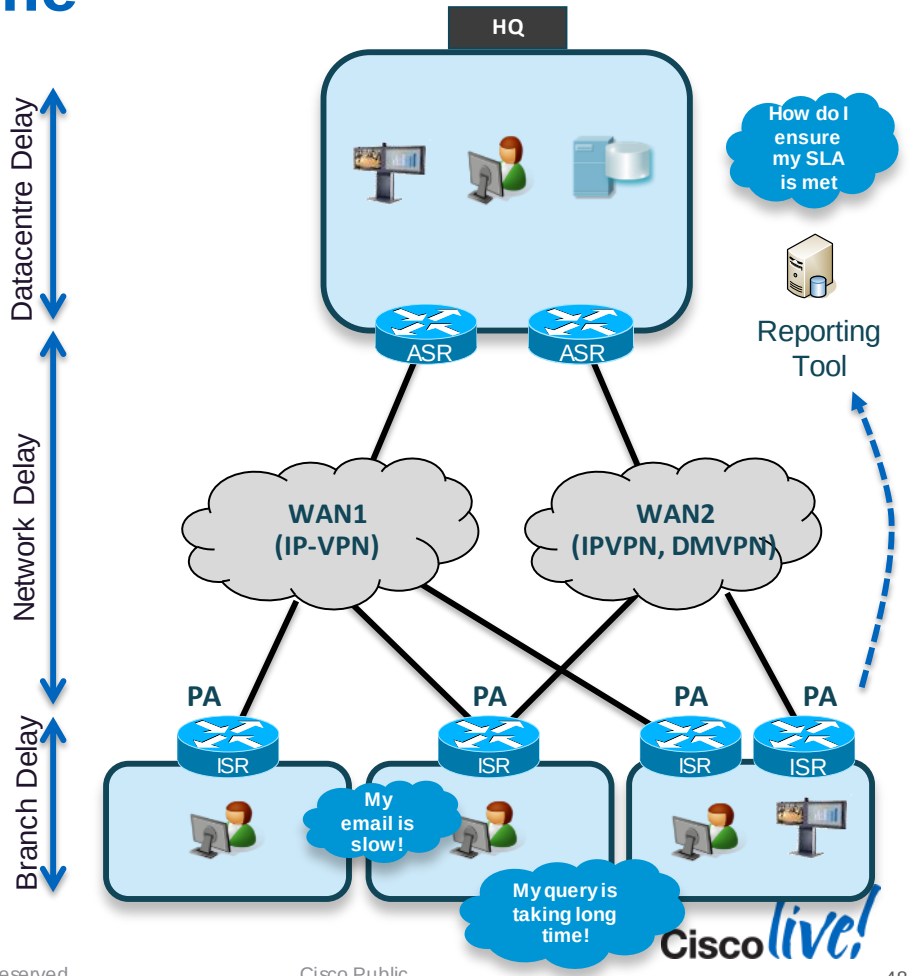
3. Application Response Time
Measurement

Key Features

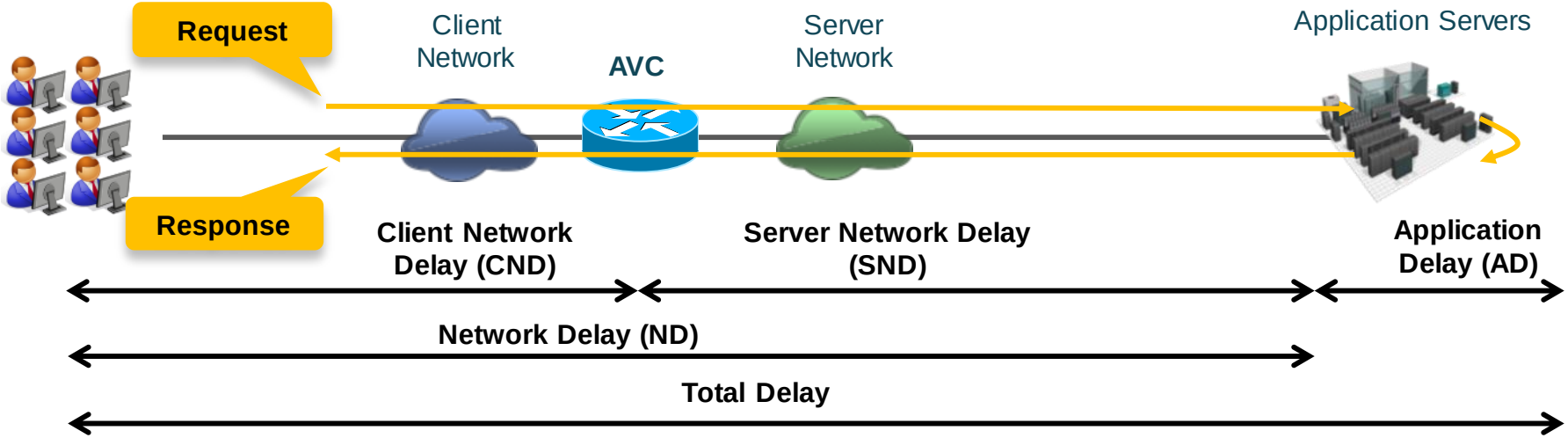
- 27 Application Response Time (ART) Metrics
- Interact with NBAR2 for Application ID
- IOS: PA or MMA
- IOS-XE: MMA
- Export: NFv9 and IPFIX export

Benefits

- Visibility into application usage and performance
- Quantify user experience
- Troubleshoot application performance
- Track service levels for application delivery

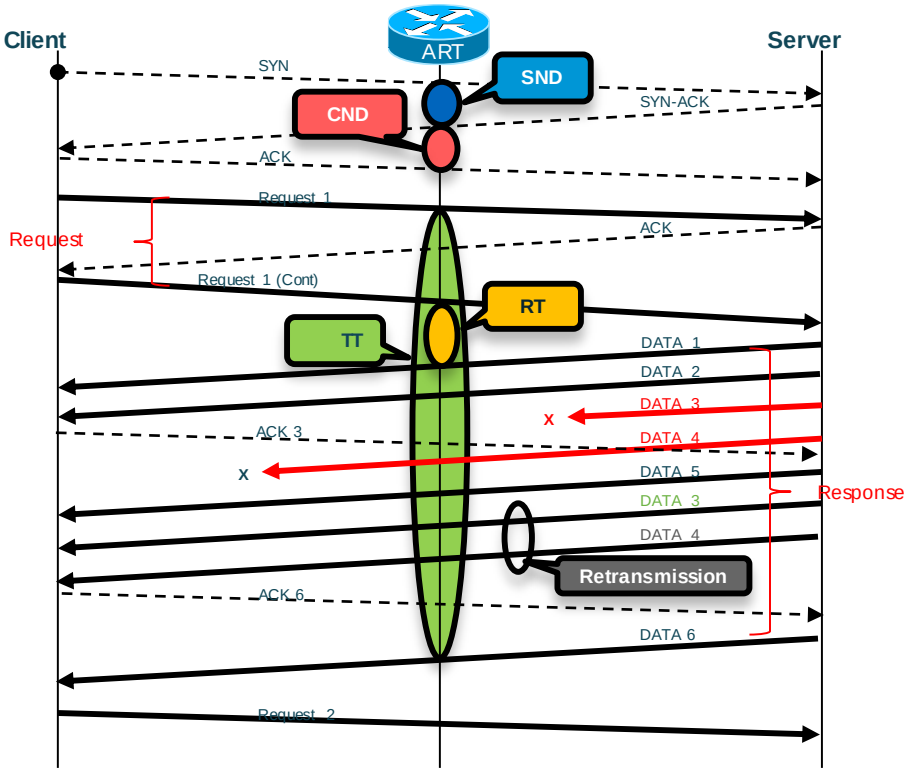


Application Response Time
Network Path Segments



- Application response time provides insight into application behaviour (network vs server bottleneck) to accelerate problem isolation
- Separate application delivery path into multiple segments
- Server Network Delay (SND) approximates WAN Delay
- Latency per application

Understand IOS ART Metrics Calculation



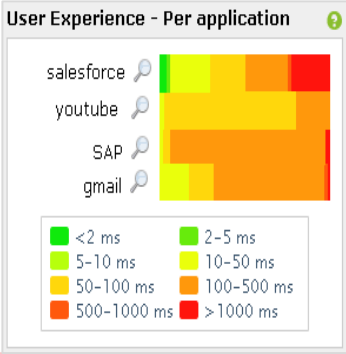
Network Delay (ND)	ND = CND + SND
Response Time (RT)	t(First response pkt) – t(Last request pkt)
Transaction Time (TT)	t(Last response pkt) – t(First request pkt)
Application Delay (AD)	AD = RT – SND

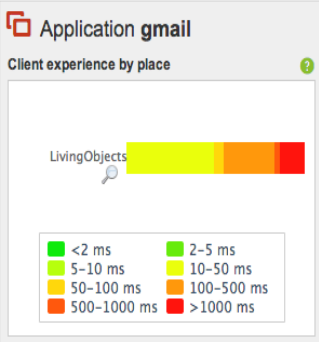
Quantify User Experience

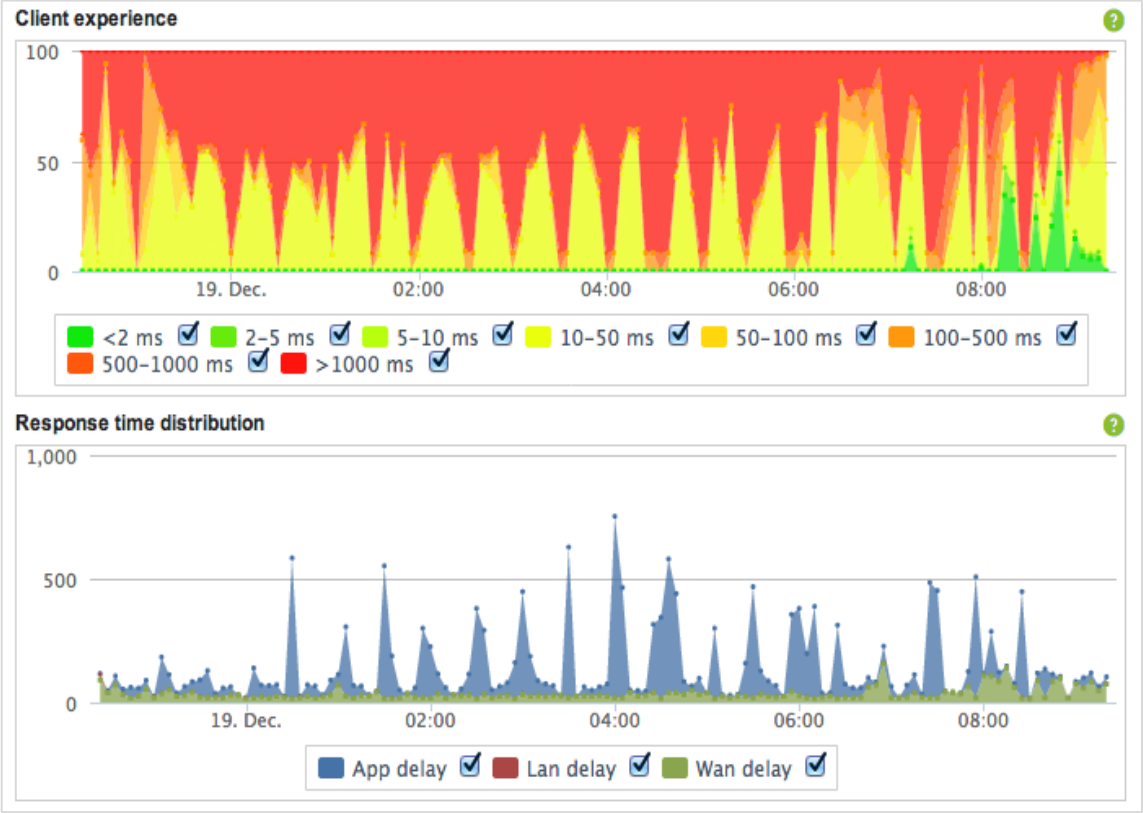
Identify Server Performance Issue

Application Response Time
Measurement

For Your Reference







Screenshots: courtesy LivingObjects

For Your Reference

https://10.9.2.1/webacs/loginAction.do?action=login&flashVersion=9.0.124.0&hasCorrectFlashVersion=true&product=wcs#pa

Cisco Internal | perso | Medianet | AVC | IWE | Cisco Europe | Visibility | Employee Landi... | Directory

Cisco Prime Infrastructure – My...

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | root

Home | Design | Deploy | Operate | Report | Administration | Workflows

Overview | Incidents | Performance | Detail Dashboards

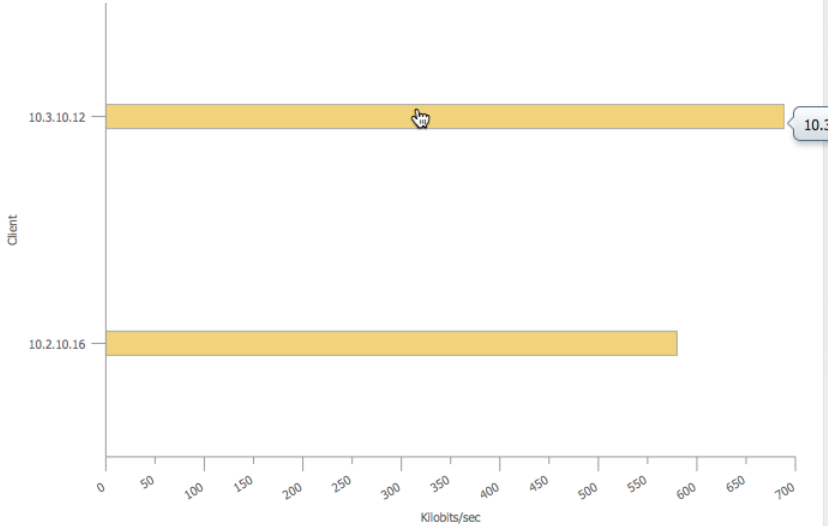
Filters | *Application: youtube | *Time Frame: Past 6 Hours | Network Aware | Site: All | Go

Top N Clients

Edited

Client | User

Rate | Volume



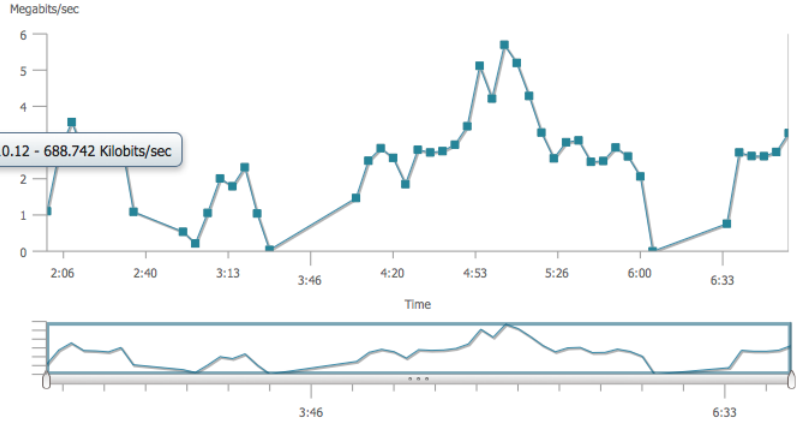
Traffic | Wireless | Wired

2013 March 19, 14:03:06 UTC

Top N Servers

Application Traffic Analysis

Rate | Volume



2013 March 19, 14:03:08 UTC

Application Server Performance

Application Server	Site	Application	Avg. Server Response Time (ms)	Max. Server Response Time (ms)	Analysis
74.125.224.39	Unassigned	youtube	67	109	
74.125.170.147	Unassigned	youtube	45	85	
74.125.224.37	Unassigned	youtube	35	84	
74.125.170.110	Unassigned	youtube	74	74	

Workflow Status 0 0 0 | Support Cases | Alarm Browser | Alarm Summary 16 1 142

For Your Reference

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | root

Home | Design | Deploy | Operate | Report | Administration | Workflows

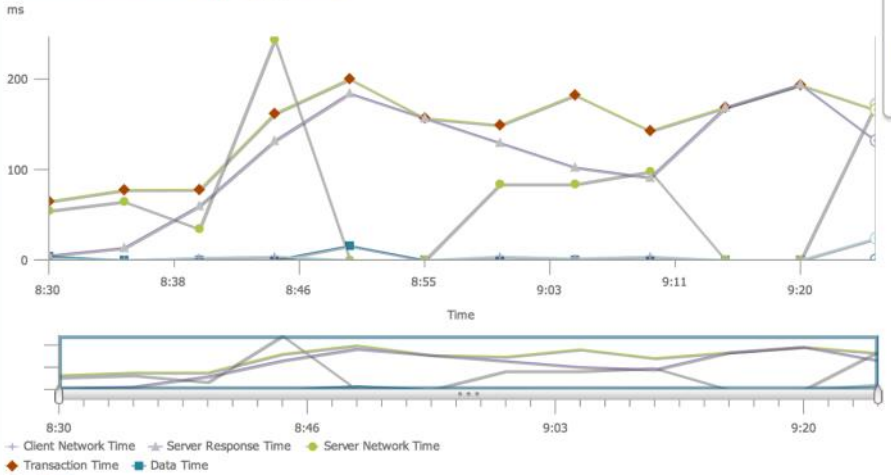
Overview | Incidents | Performance | Detail Dashboards

Site | Device | Interface | Application | Voice/Video | End User Experience | WAN Optimization | AVC Stats | AVC Perf | AVC URLs | test

Filters: Application http | Site Branch3 | Go

Application ART Analysis

Edited



2013 March 19, 16:29:27 UTC

Time: 09:25:00 3/19/2013 (PDT)

Value(s) are ms

Client Network Time:	24
Server Response Time:	132
Server Network Time:	172
Transaction Time:	166.22
Data Time:	0

Edited

			Maximum Transacti...	Average Transactio...	Art Analysis
		http	176	176	Show Analysis
		http	193	146	Show Analysis
		http	258	46	Show Analysis
10.3.10.15		http	184	15	Show Analysis
10.3.10.17		http	0	0	Show Analysis

2013 March 19, 16:29:27 UTC

Worst N Sites by ART Metrics

Edited

Selected Metric : Transaction Time

Site	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)
Datacenter	http	55705	22479
Unassigned	http	55705	6344
Branch1	http	9202	1957
Branch4	http	5572	1532
Branch5	http	6938	585

Workflow Status 0 0 0 | Support Cases | Alarm Browser | Alarm Summary 20 1 125

QoS Visibility

QoS Class-ID, Queue Drops and Queue Hierarchy

Applied Policy Map

```
policy-map P1
 class C1
  shaping average 16000000
  service-policy child
```

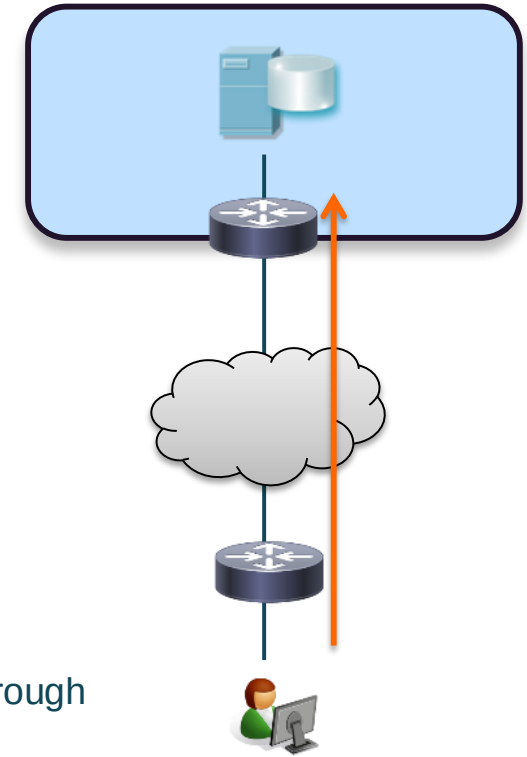
```
policy-map child
 class C11
  bandwidth remaining percent 10
 class C12
  bandwidth remaining percent 70
 class class-default
  bandwidth remaining percent 20
```

```
class-map match-all C1
  match any
class-map match-all C11
  match ip dscp ef
class-map match-all C12
  match ip dscp cs2
```

In the Flow Record,
collect policy qos class hierarchy
collect policy qos queue drops

Flow	Hierarchy	Queue id
Flow 1	P1, C1, C11	1
Flow 2	P1, C1, C11	1
Flow 3	P1, C1, C12	2

Queue id	Queue packet drops
1	100
2	20



- For each flow, the class hierarchy and queue drops can now be exported through NetFlow
- Class-ID to Name mapping provided through separate Option Templates

4. Media Monitoring

Monitor Voice and Video Performance

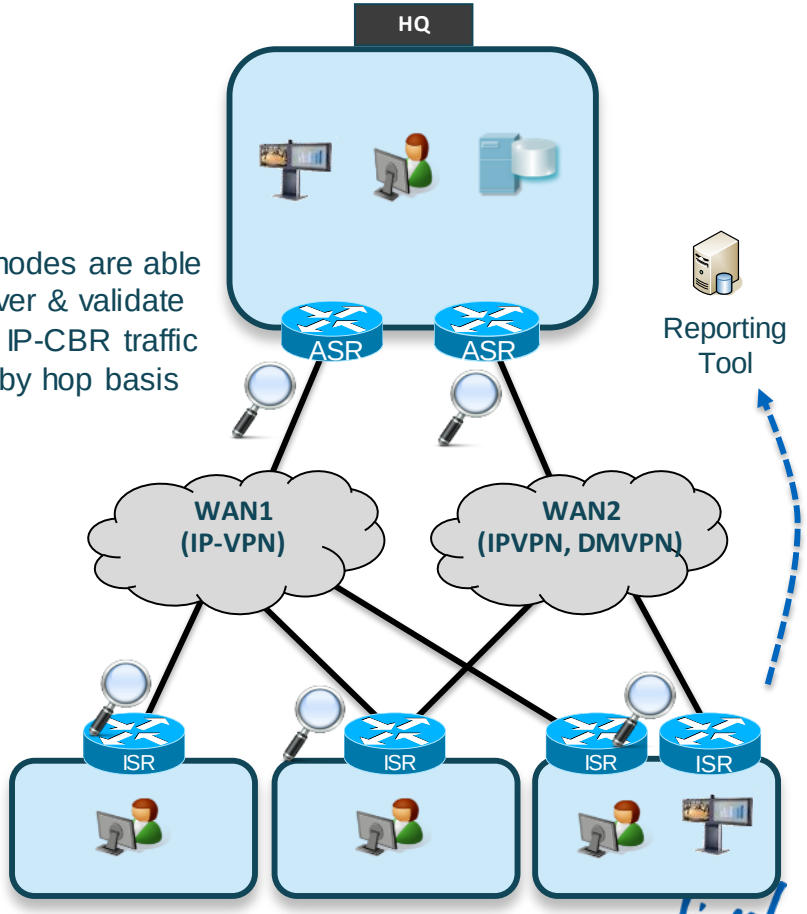
Key Features

- Monitor media performance metrics, i.e. jitter, loss
- Integrate with NBAR2 to identify applications
- Setting threshold and generating alert/alarm
- IOS: PerfMon or MMA
- IOS-XE: MMA
- Export: NFv9 or IPFIX export

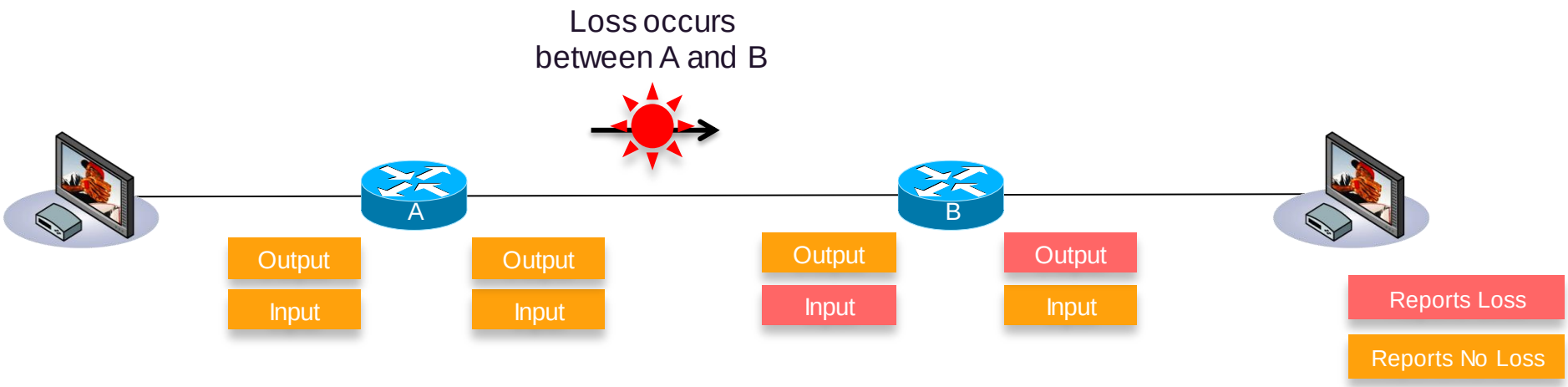
Benefits

- Real-time monitoring of voice and video performance across network
- Accelerate troubleshooting – identify what, where, when is the problem
- Proactive troubleshooting
- Validate SLA

Network nodes are able to discover & validate RTP and IP-CBR traffic on hop by hop basis



Performance Monitor
Understand RTP metrics



- RTP packet drops on the WAN interface (input) or on the LAN interface (output).
- Synchronisation source identifier (SSRC) to distinguish between different audio and video channels if they share the same UDP session (TP).
- RTP jitter values
- RTP payload type gives you an idea of the kind of media in an RTP stream

Media Performance Metrics

For reference, below is the record definition we use in current profile for Media (input):

Key Fields

```
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
match routing vrf output
match interface output
```

Non-Key Fields

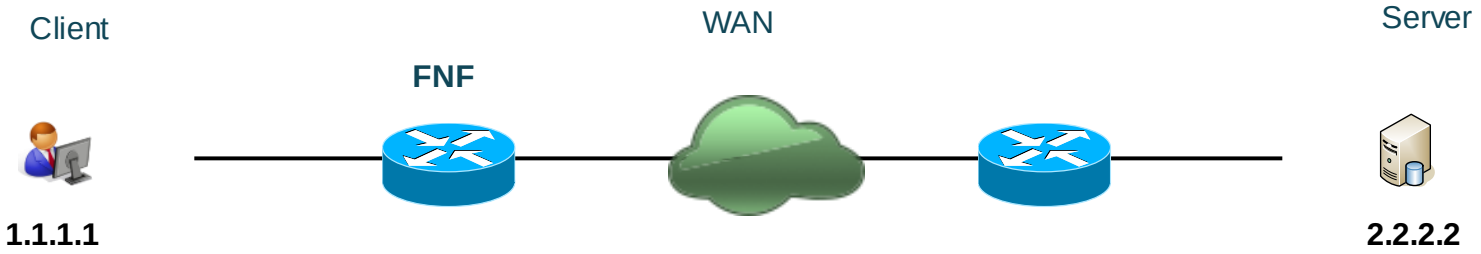
```
collect routing vrf input
collect interface input
collect application name
collect ipv4 dscp
collect datalink source-vlan-id
collect connection initiator
collect counter packets
collect counter bytes long
collect connection new-connections
collect ipv4 ttl
collect transport rtp payload-type
collect transport rtp jitter mean sum
collect transport rtp jitter maximum
collect transport packets lost counter
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

Performance Monitoring (MMA)

Implementation and Configuration

- CLI – Define your own records, monitors, class-maps and policy-map
- Prime Infrastructure 2.0
- CLI – Use ezPM with Cisco pre-defined profiles

Key Fields
Src/Dest IP vs Connection



Key Fields

match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port

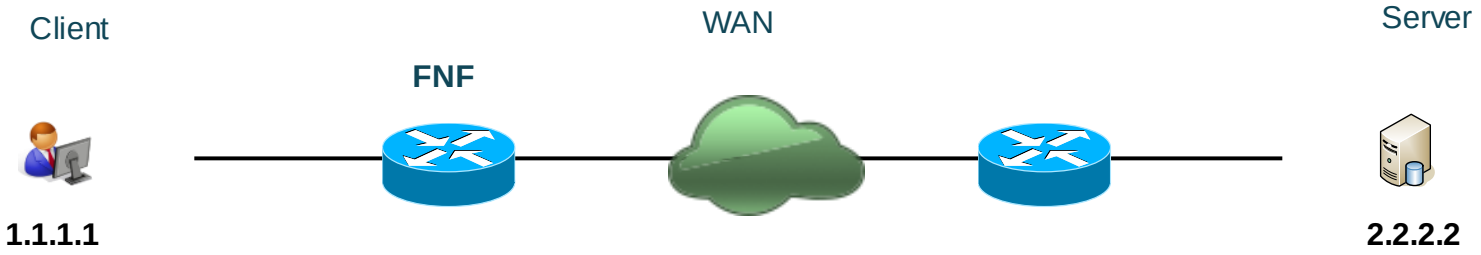
or

Key Fields

match connection client ipv4 address
match connection server ipv4 address
<match connection client transport port>
match connection server transport port

Client port can be omitted (don't provide much info)

Key Fields
Src/Dest IP vs Connection



Dir from client to server

- Source IP = 1.1.1.1, Dest IP = 2.2.2.2
- Client IP = 1.1.1.1, Server IP = 2.2.2.2

Dir from server to client

- Source IP = 2.2.2.2, Dest IP = 1.1.1.1
- Client IP = 1.1.1.1, Server IP = 2.2.2.2

- When using the src/dst fields, each direction creates a different record since the key is different. 2 records are created for each flow.
- When using the client/server fields, both directions results with the same key therefore one bi-dir record is created. 1 record is created for each flow.

Configuration Samples

- Conversation Traffic Stats for IPv4 and IPv6
- Application Response Time for IPv4 and IPv6
- Media Performance for IPv4 and IPv6

Unified Monitoring Policy
Conversation Traffic Stats

For Your Reference

```
flow record type performance-monitor my-visibility-conv_ts_ipv4
 description ezPM record
 match routing vrf input
 match ipv4 protocol
 match application name account-on-reso
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match services waas segment account-on
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect connection new-connections
 collect connection sum-duration
 collect connection server counter byte
 collect connection server counter pack
 collect connection client counter byte
 collect connection client counter pack
 collect services waas passthrough-reas

 [SNIP]
```

```
flow record type performance-monitor my-visibility-conv_ts_ipv6
 description ezPM record
 match routing vrf input
 match ipv6 protocol
 match application name account-on-resolution
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect ipv6 dscp
 collect connection new-connections
 collect connection sum-duration
 collect connection server counter bytes long
 collect connection server counter packets long
 collect connection client counter bytes long
 collect connection client counter packets long
 collect services waas passthrough-reason

 [SNIP]
```

Unified Monitoring Policy
Conversation Traffic Stats

For Your Reference

```
flow monitor type performance-monitor my-visibility-conv_ts_ipv4
 record my-visibility-conv_ts_ipv4
 cache entries 156250
 cache timeout synchronized 60
!
```

```
flow monitor type performance-monitor my-visibility-conv_ts_ipv6
 record my-visibility-conv_ts_ipv6
 cache entries 156250
 cache timeout synchronized 60
!
```

Unified Monitoring Policy
Application Response Time

For Your Reference

```
flow record type performance-monitor my-visibility-art_ipv4
 description ezPM record
 match routing vrf input
 match ipv4 protocol
 match application name account-on-reso
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match services waas segment account-on
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect connection delay response to-s
 collect connection server counter resp
 collect connection delay response to-s
 collect connection delay network to-se
 collect connection delay network to-cl

[SNIP]
```

```
flow record type performance-monitor my-visibility-art_ipv6
 description ezPM record
 match routing vrf input
 match ipv6 protocol
 match application name account-on-resolution
 match connection client ipv6 address
 match connection server transport port
 match connection server ipv6 address
 match services waas segment account-on-resolution
 collect datalink source-vlan-id
 collect ipv6 dscp
 collect connection delay response to-server sum
 collect connection server counter responses
 collect connection delay response to-server histogram late
 collect connection delay network to-server sum
 collect connection delay network to-client sum

[SNIP]
```

Unified Monitoring Policy
Application Response Time

For Your Reference

```
flow monitor type performance-monitor my-visibility-art_ipv4
 record my-visibility-art_ipv4
 cache entries 56250
 cache timeout synchronized 60
```

```
!
flow monitor type performance-monitor my-visibility-art_ipv6
 record my-visibility-art_ipv6
 cache entries 56250
 cache timeout synchronized 60
!
```

Unified Monitoring Policy

Media Performance

For Your Reference

```
flow record type performance-monitor my-visibility-media_ipv4_in
 description ezPM record
 match routing vrf input
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match transport rtp ssrc
 match interface input
 collect datalink source-vlan-id
 collect ipv4 dscp
 collect ipv4 ttl
 collect transport packets lost cour
 collect transport rtp jitter maximu
 collect application name
 collect connection new-connections
 collect transport rtp payload-type
 collect transport rtp jitter mean s

[SNIP]
```

```
flow record type performance-monitor my-visibility-media_ipv6_in
 description ezPM record
 match routing vrf input
 match ipv6 protocol
 match ipv6 source address
 match ipv6 destination address
 match transport source-port
 match transport destination-port
 match transport rtp ssrc
 match interface input
 collect datalink source-vlan-id
 collect ipv6 dscp
 collect ipv6 ttl
 collect transport packets lost counter
 collect transport rtp jitter maximum
 collect application name
 collect connection new-connections
 collect transport rtp payload-type
 collect transport rtp jitter mean sum

[SNIP]
```

Unified Monitoring Policy

Media Performance

For Your Reference

```
flow monitor type performance-monitor my-visibility-media_ipv4_in
 record my-visibility-media_ipv4_in
 cache entries 4000
 cache timeout synchronized 60
 history size 10
```

```
flow monitor type performance-monitor my-visibility-media_ipv6_in
 record my-visibility-media_ipv6_in
 cache entries 4000
 cache timeout synchronized 60
 history size 10
```

Unified Monitoring Policy

Class Maps

For Your Reference

```
class-map match-all my-visibility-conv_ts_ipv4
 match protocol ip
!
class-map match-all my-visibility-conv_ts_ipv6
 match protocol ipv6
!
class-map match-all my-visibility-art_ipv4
 match access-group name my-visibility-art_ipv4_tcp
!
class-map match-all my-visibility-art_ipv6
 match access-group name my-visibility-art_ipv6_tcp
!
class-map match-any my-visibility-media_app
 match protocol telepresence-media
 match protocol rtp
!
class-map match-all my-visibility-media_ipv4_in
 match access-group name my-visibility-media_ipv4_udp
 match class-map my-visibility-media_app
!
class-map match-all my-visibility-media_ipv4_out
 match access-group name my-visibility-media_ipv4_udp
 match class-map my-visibility-media_app
!
```

Define the Traffic you are interested in.
The Performance Monitors will be applied appropriately

Unified Monitoring Policy

Policy Maps

For Your Reference

```
policy-map type performance-monitor my-visibility-in
 class my-visibility-art_ipv4
  flow monitor my-visibility-art_ipv4
 class my-visibility-art_ipv6
  flow monitor my-visibility-art_ipv6
 class my-visibility-media_ipv4_in
  flow monitor my-visibility-media_ipv4_in
 class my-visibility-media_ipv6_in
  flow monitor my-visibility-media_ipv6_in
 class my-visibility-conv_ts_ipv4
  flow monitor my-visibility-conv_ts_ipv4
 class my-visibility-conv_ts_ipv6
  flow monitor my-visibility-conv_ts_ipv6
```

Apply the Performance Monitors to the appropriate class and then aplply the policy on the interface

AVC Configuration
Prime Infrastructure

- Enable AVC with just ON/OFF button
- With Cisco Prime Infrastructure 2.0

Cisco Prime Infrastructure

Home | Design | Deploy | Operate | Report | Administration | Workflows

Feature Design | Monitor Configuration | Configuration Groups | Shared Policy Objects

Templates
- Features and Technologies
  - Application Visibility
    - AV Configuration
  - Controller
  - Interfaces
  - Network Analysis Module
  - Security
  - WAN Optimization
- CLI Templates
- Composite Templates
- My Tags
- My Templates

Validation Criteria
*Device Type: Routers
OS Version:

Template Detail
*Apply to Interface Role: LAN-DATA

Traffic Statistics
On
IPs, Subnets: Any IPv4
Applications: ANY
Advanced Options

HTTP URL Visibility
On
IPs, Subnets: Any IPv4
Applications: Flash Yahoo, Flash Video, Gmail, Flash Myspace, RealMedia Traffic
Advanced Options

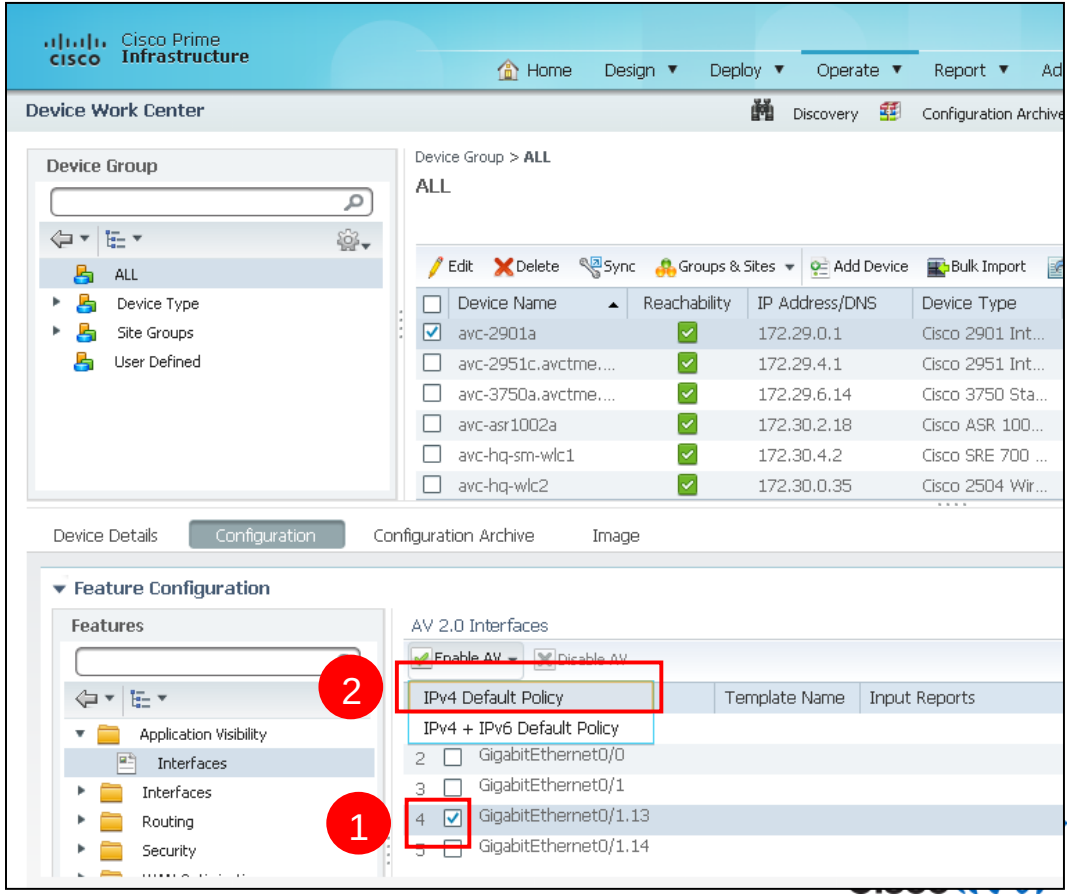
Application Response Time
On
IPs, Subnets: Any IPv4
Applications: Any TCP
Advanced Options

Voice/Video Metrics
On
IPs, Subnets: Any IPv4
Applications: Real-time Transport P..., Telepresence Media

Save as New Template | Cancel

AVC Configuration
Prime AVC One-Click

- Enable AVC in one-click
  - One device at a time
- Two simple steps
  1. Select interface(s)
  2. Enable



AVC Configuration
ezPM

IOS-XE: 3.10
IOS 15.4(1)T

Monitor Name	Default Traffic Classification
Application-Response-Time (ART)	All TCP
URL	HTTP applications
Media	RTP applications over UDP
Conversation-Traffic-Stats	Remaining traffic not matching other classifications
Application-Traffic-Stats	DNS and DHT

- Enable AVC and enable flexibility:
  - Configuring exporters
  - Enable / Disable various traffic-monitors (a.k.a tools)
  - For each traffic-monitor, override some default parameters (IPv4/6, Ingress/Egress, traffic to which the monitor is applied, cache size..)

IOS-XE: 3.10
IOS 15.4(1)T

ezPM

```
! User defined ezPM context
performance monitor context my-visibility profile application-experience
 exporter destination 10.10.10.10 source GigabitEthernet0/0/1
 traffic-monitor all
!
! Attach the context to the interface
interface GigabitEthernet0/0/2
 performance monitor context my-visibility
!
```

- Equivalent to ~650 lines of configuration
- Records/Monitors/Class-maps/Policy-map pre-defined

Summary – AVC Monitoring for IOS

Implementation Options

What to Monitor	Option1 What to Configure	Option2 What to Configure	Option3 What to Configure New – IOS 15.4(1)T
Application Usage, Top Talkers	Flexible NetFlow	Performance Agent	Performance Monitor (traffic-stats)
Application Response Time	Performance Agent	Performance Agent	Performance Monitor (application-response-time)
Voice & Video Performance	Media Monitor	Media Monitor	Performance Monitor (media)

Summary – AVC Monitoring for IOS-XE

Implementation Options

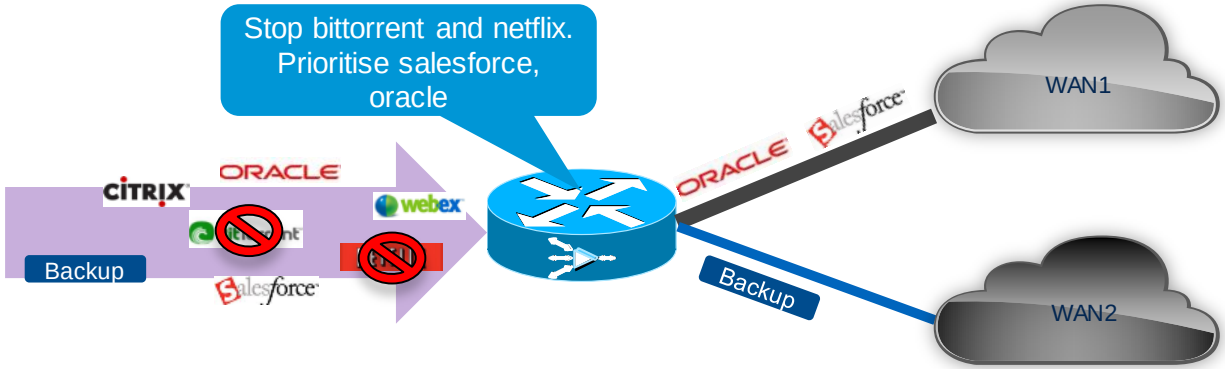
What to Monitor	Option1 What to Configure	Option2 What to Configure
Application Usage, Top Talkers	Flexible NetFlow	Performance Monitor (traffic-stats)
Application Response Time	Performance Monitor (application-response-time)	Performance Monitor (application-response-time)
Voice & Video Performance	Performance Monitor (media)	Performance Monitor (media)




CONTROL
QoS and Performance Routing (PfR)

Maximise Application Performance

Controls application bandwidth usage and selects optimal path



Application-aware QoS

Identify 1000+ applications using NBAR2 and control bandwidth with Cisco industry leading QoS

Limit unwanted traffic and prioritise critical applications

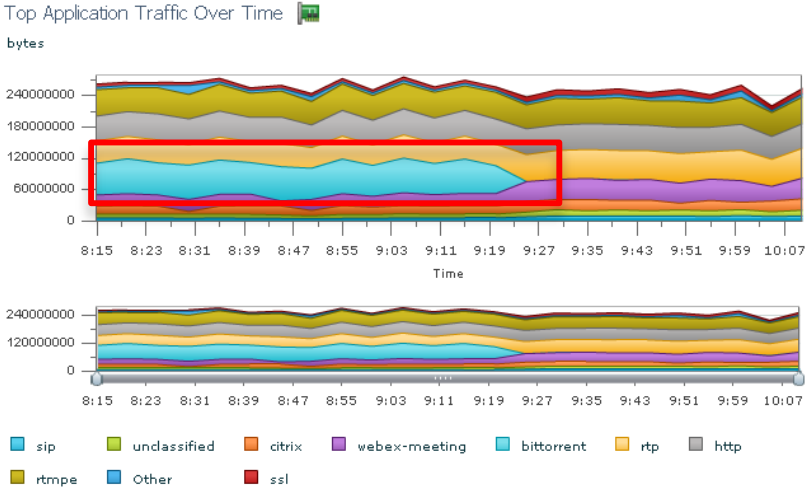
Intelligent Path Selection

Deliver critical applications over the path which can meet application performance requirement using PfR

Automatic load share to maximise bandwidth use on available links

Example: Stop P2P Applications with AVC

After apply control policy




```
class-map match-any bittorrent
 match protocol attribute sub-category p2p-file-transfer
 match protocol bittorrent-networking
 match protocol dht
policy-map drop-bittorrent
 class bittorrent
  police 8000 conform-action drop  exceed-action drop  violate-action drop
interface GigabitEthernet0/0/0
 service-policy input drop-bittorrent
 service-policy output drop-bittorrent
```

Performance Routing
Intelligent Path Control

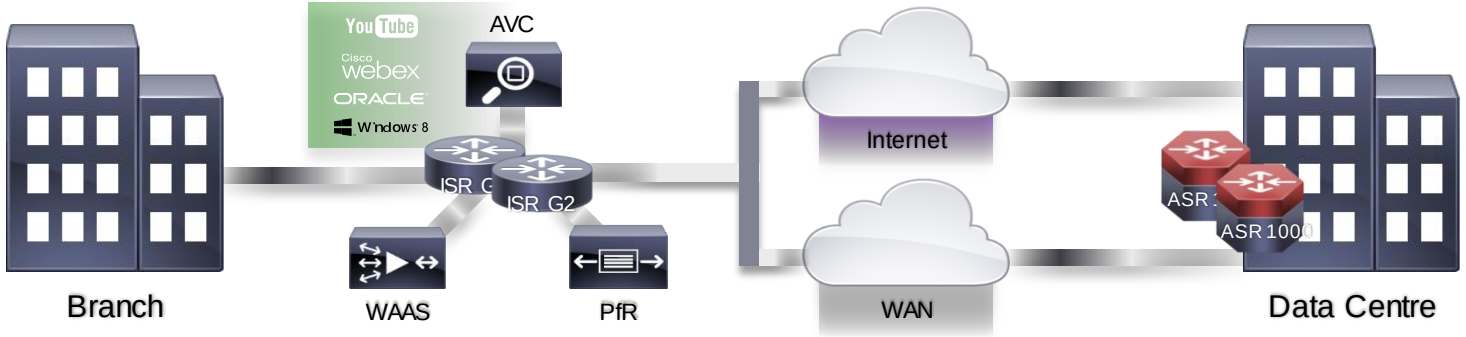
- Lower WAN Costs
  - Increasing use of Internet based WAN
- Full Utilisation of expensive WAN bandwidth
  - Efficient distribution of traffic based upon load, circuit cost and path preference

- Improved Application Performance

  Per application best path based on delay, loss, jitter measurements

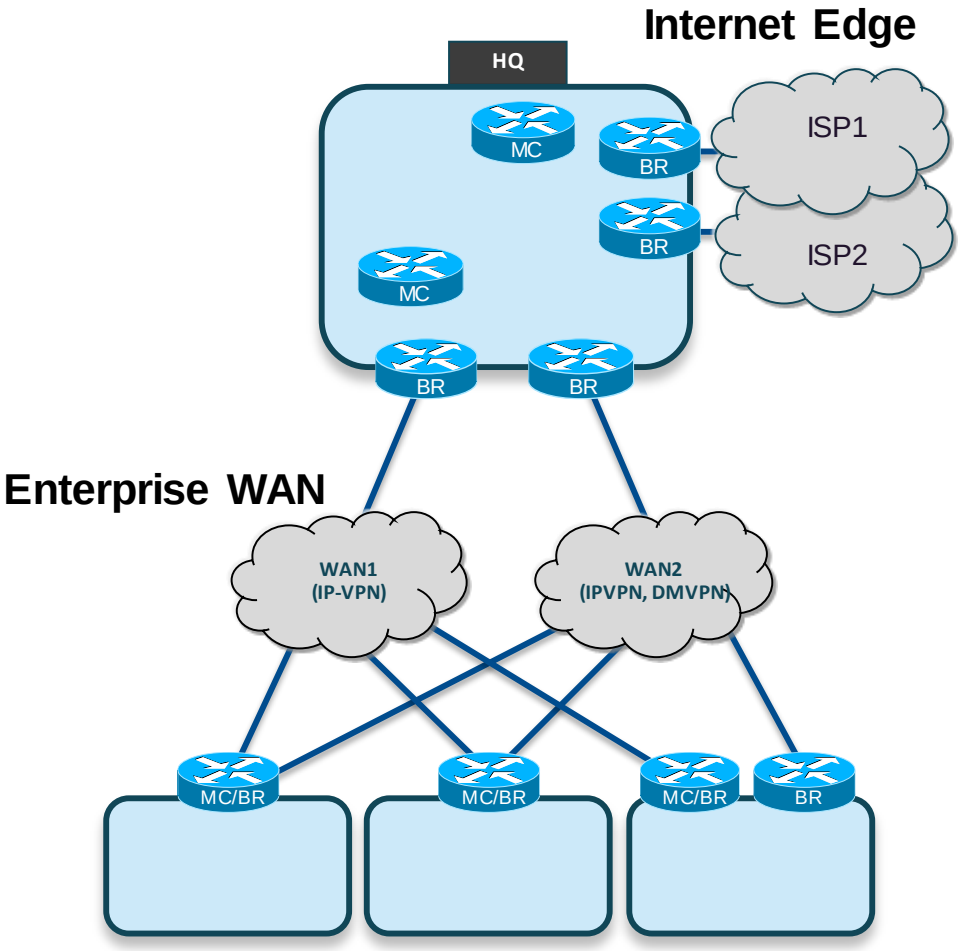
- Increased Application Availability

  Protection from carrier black holes and brownouts



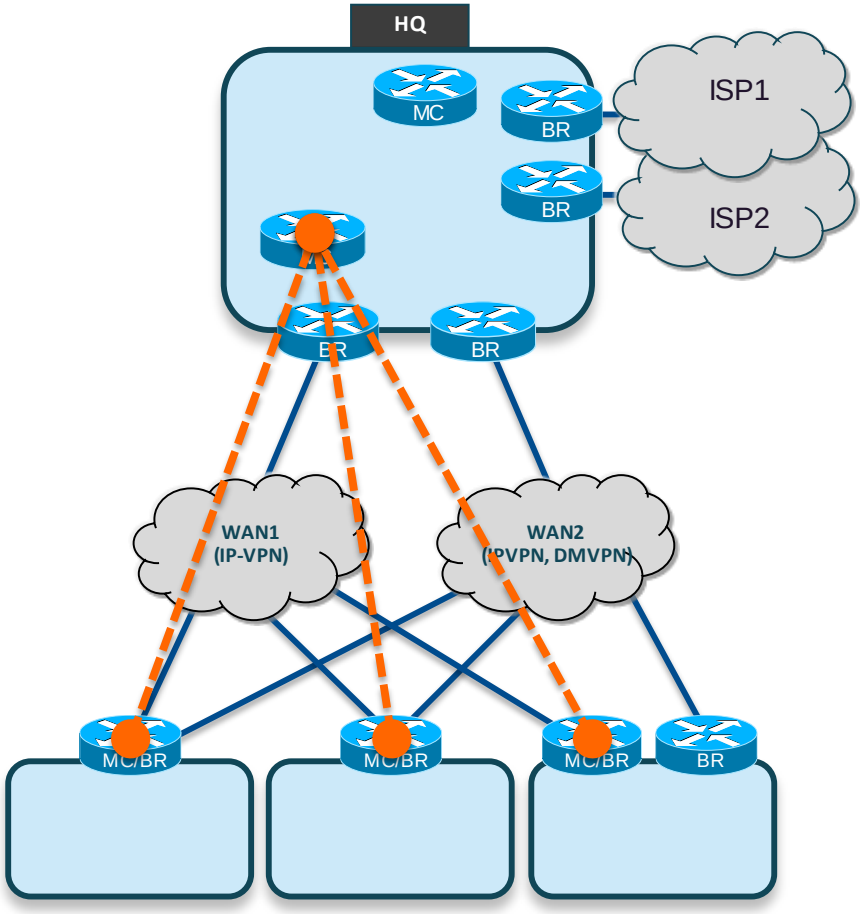
Performance Routing
Topologies

- IPv4 only (IPv6 support future)
- MC on all sites – Distributed Model
- MC controls local BRs only
- Optimise by:
  - Reachability, Loss,
  - Delay, Jitter, MOS,
  - Throughput, Load, and/or $Cost



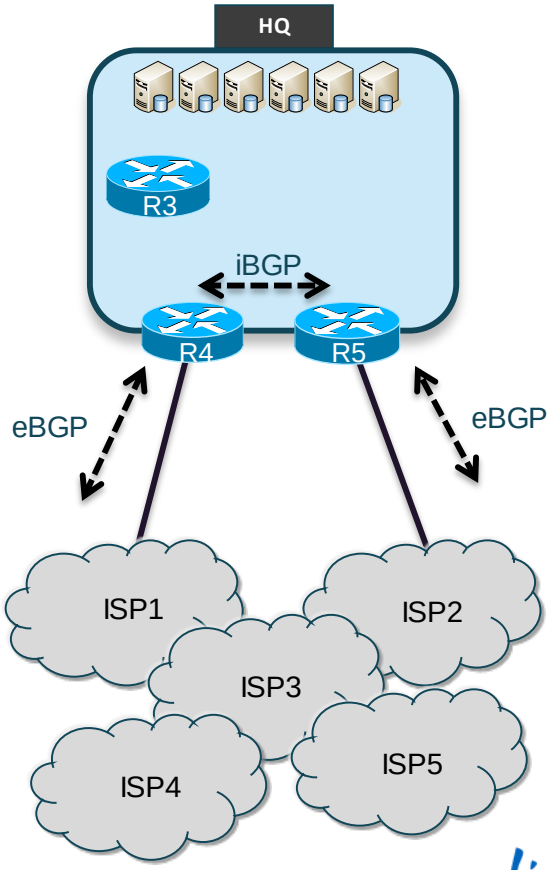
Performance Routing
Peering & Discovery

- Enterprise Domain
- Multisite MC Peering Framework
- MC to MC Peering Framework can be used to exchange policies, services and feedback
- Remote Site Discovery
  - Automatic discovery of branch routers
  - Simplifies Configuration – prefix and target discovery
  - Probing Efficiency – sharing of probe data across policies
  - Enhance PfR – remote site bandwidth discovery



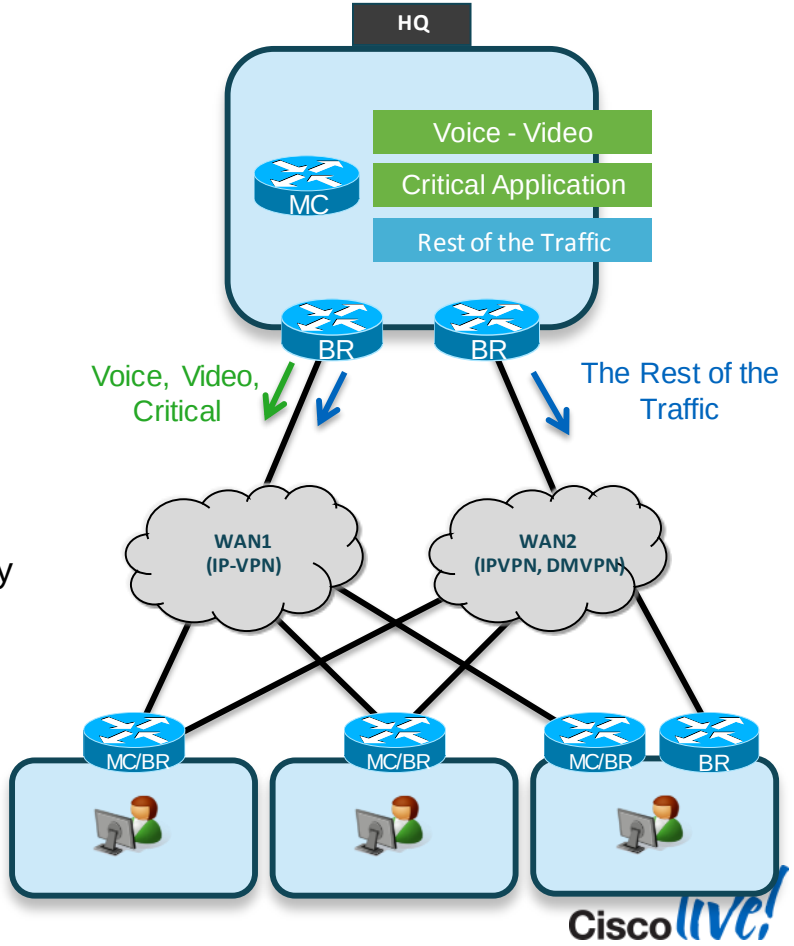
Automatic Traffic Engineering

- Problem Statement
  - Ingress/Egress path are under/over utilised
  - Maximise bandwidth utilisation (uplinks with different BW)
- Solution: PfR used to load balance the traffic
  - New default policies based on load-balancing
  - Cisco ASR1k is typical BR/MC with BR terminating WAN connections
  - BGP routing
    - BRs must be iBGP peers
    - Default routing **or**
    - Partial routes **or**
    - Full routes



Enterprise WAN Use Case
Blackout and Brownout

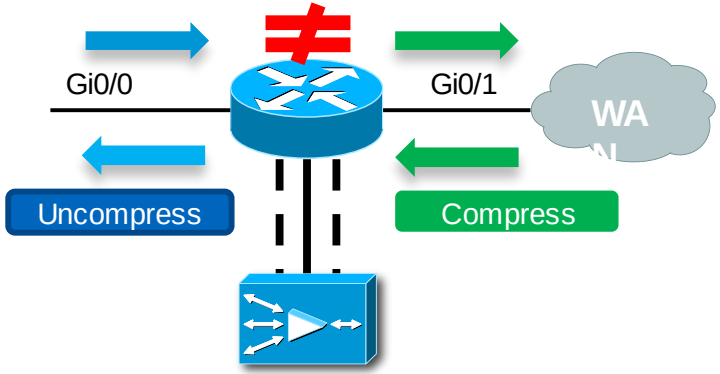
- Problem Statement
  - Recent carrier routing problem cause a network outage (Blackout).
  - Fluctuating performance over the WAN is causing intermittent application problems (Brownout)
  - Secondary/Backup WAN path under utilised
- Solution: PfR Application based optimisation
  - Protect Voice and Video traffic:
    - primary path, check delay, loss, jitter – fallback secondary
  - Protect Business Applications:
    - primary path, check loss, utilisation – fallback secondary
  - Best effort Applications – Maximise bandwidth utilisation:
    - load balanced across SPs or use the secondary path






WAAS

Traffic Visibility Through FNF with WAAS
Overview



Before WAAS

- Ingress FNF on all interfaces is sufficient
  - LAN in traffic = WAN out traffic
  - WAN In traffic = LAN out traffic

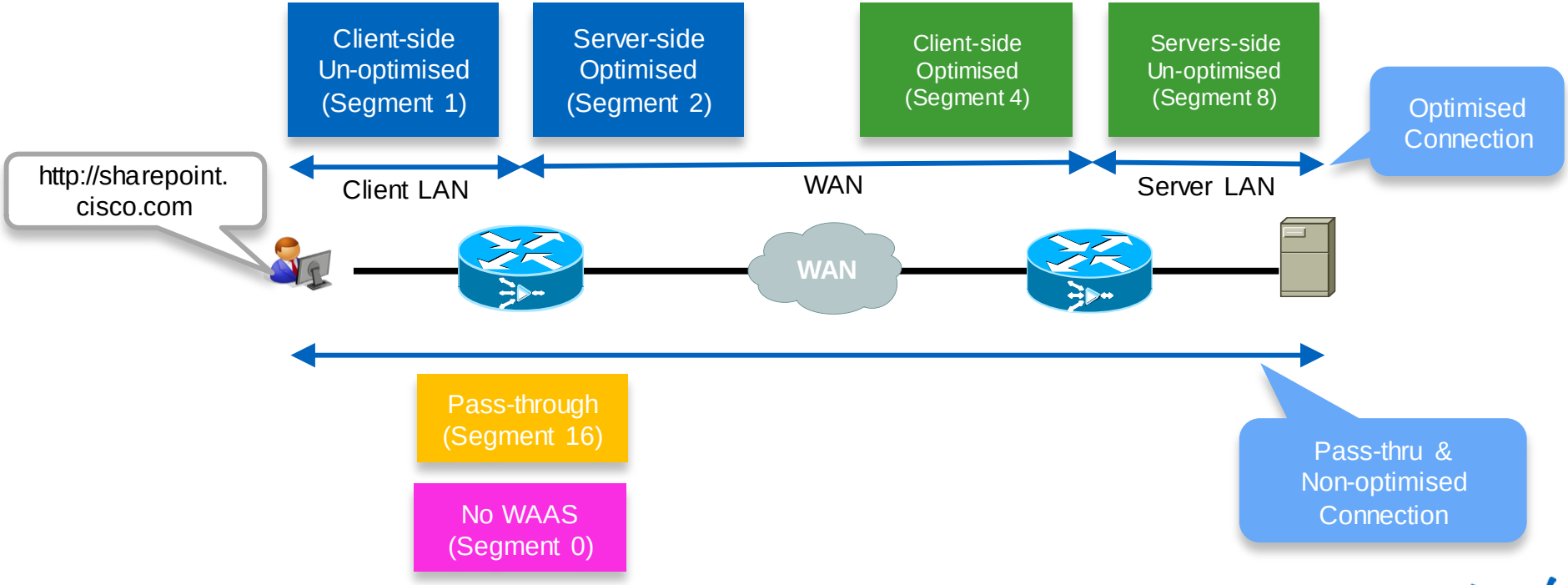
After WAAS (with offpath redirection)

- Ingress FNF on all interfaces will give wrong results

  LAN in traffic > WAN out traffic

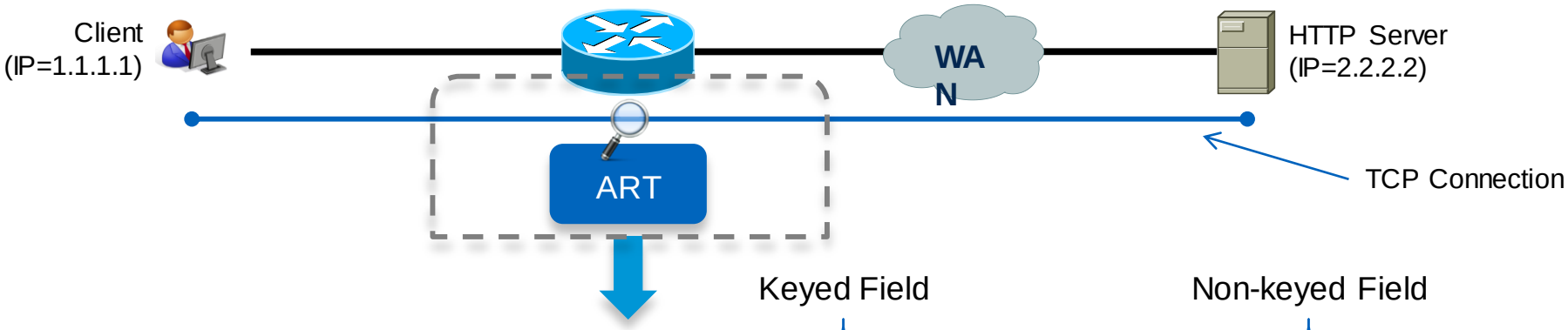
  LAN out traffic > WAN in traffic
- WAAS requires FNF on both ingress and egress of the same interfaces

WAAS Segment



PA Monitoring & Export without WAAS

Overview

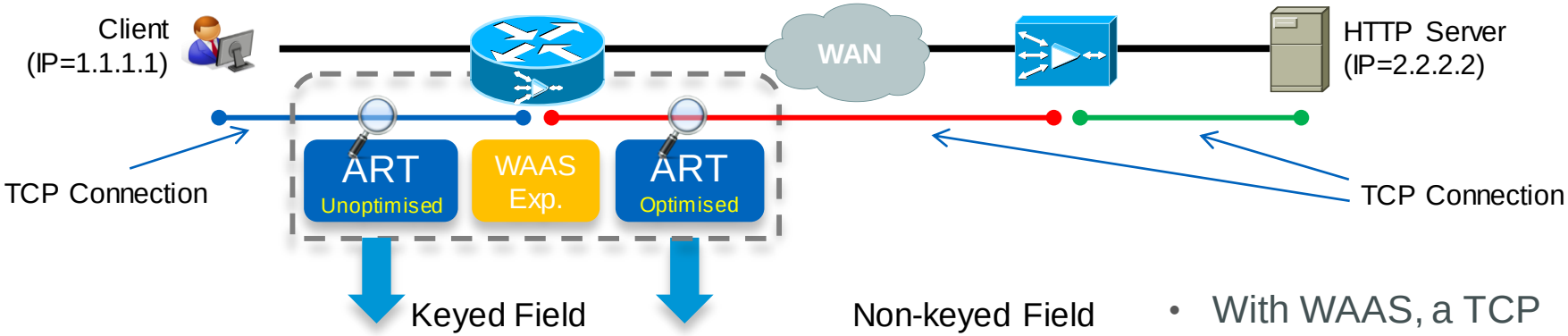


Segment ID	Src IP	Dst IP	Dst Port	Protocol Type	Resp Time	..
0 or 16	1.1.1.1	2.2.2.2	80	6 (TCP)	100	

- Without WAAS, there is only **one** TCP segment seen by the router
- Segment ID of 0 indicates no WAAS
- Segment ID of 16 indicates pass-through

PA Monitoring & Export with WAAS Express

Overview

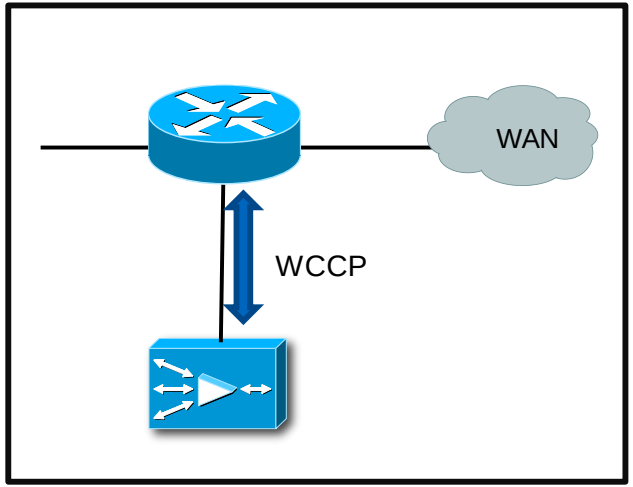


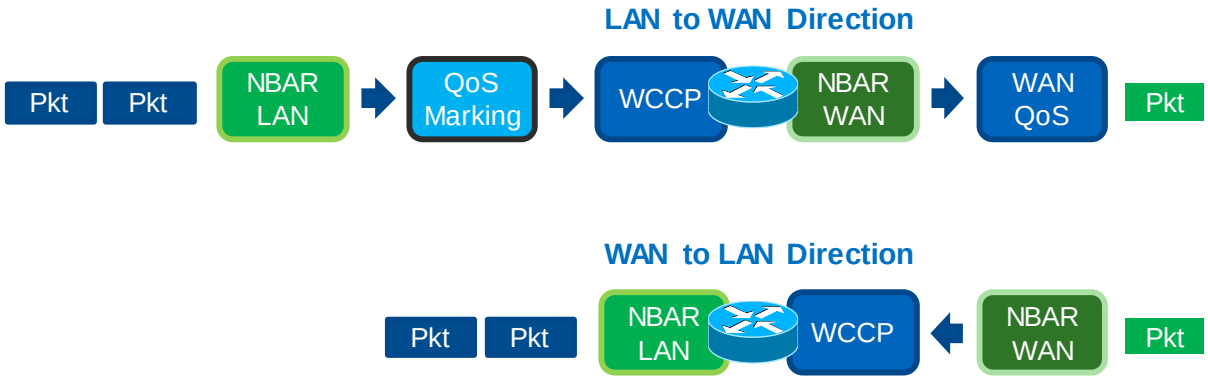
Segment ID	Src IP	Dst IP	Dst Port	Protocol Type	Resp Time	..
1	1.1.1.1	2.2.2.2	80	6 (TCP)	10	
2	1.1.1.1	2.2.2.2	80	6 (TCP)	100	

- With WAAS, a TCP connection between client and server is split into 3 TCP connections

- With WAAS Express, ART monitors both Un-optimised and Optimised segments
- Each device (branch and headend) exports two records per TCP connection

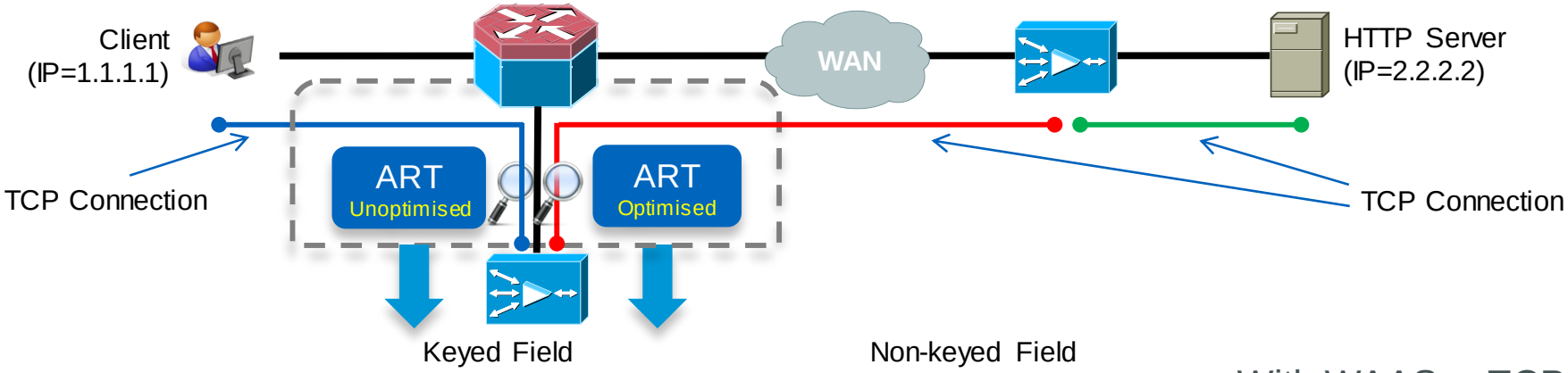
WAN Optimisation Packet Path with WCCP





- Need to decide where is the best place to run NBAR
- Running NBAR on the WAN side is not desirable because NBAR will see compressed traffic
- Where should I run NBAR if I want application-aware QoS when WAAS is present?

ART Monitoring & Export with AppNav in ASR1K



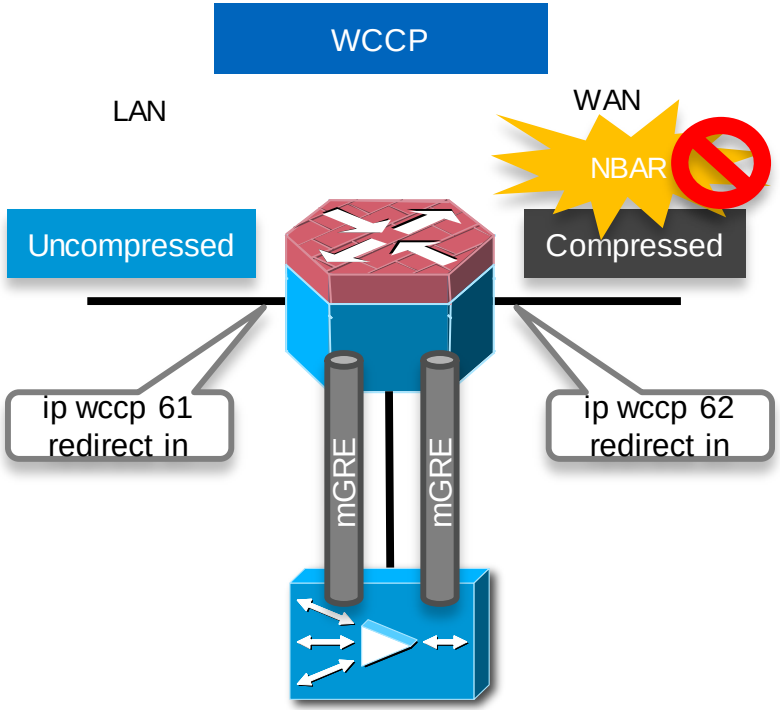
Segment ID	Src IP	Dst IP	Dst Port	Protocol Type	Resp Time	..
1	1.1.1.1	2.2.2.2	80	6 (TCP)	10	
2	1.1.1.1	2.2.2.2	80	6 (TCP)	100	

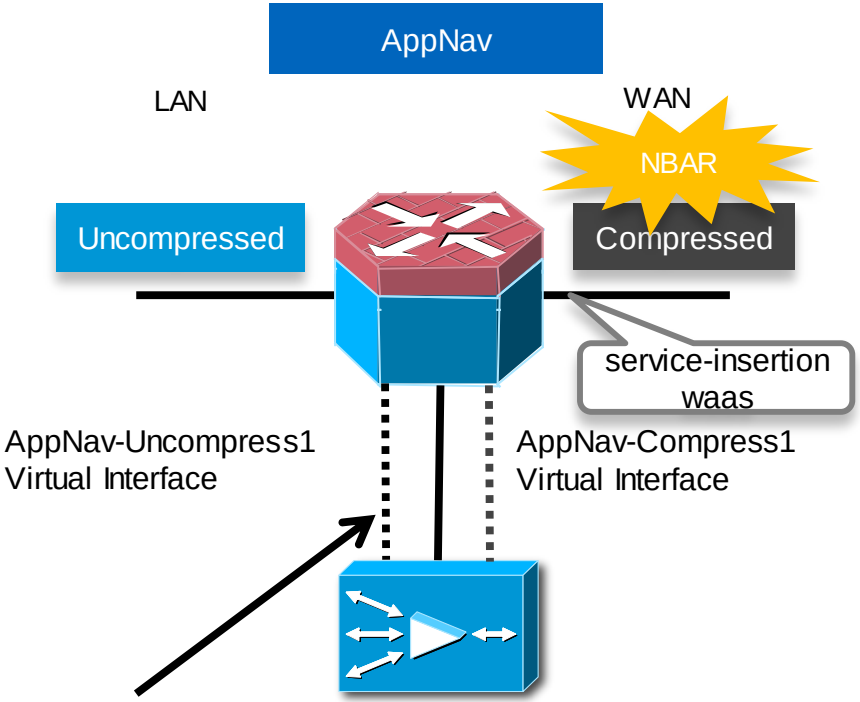
- With WAAS, a TCP connection between client and server is split into 3 TCP connections

- AppNav creates two logical interfaces, *AppNav-Uncompress* and *AppNav-Compress*
- ART monitors traffic on the AppNav logical interfaces and export two records

How AppNav Address NBAR2 & WAAS Interop?

Overview





If NBAR is enabled on WAN interface, and WAAS is enabled, automatically run NBAR on Uncompress Virtual Interface




Performance Tests

IOS Platforms – Traffic Profiles

- Stateful Traffic profile with enterprise branch application mix
- Throughput is measured as NDC (No Drop Connection)
- Average packet size: 390 bytes
- 30% of BW is upload, 70% of BW is download

Applications	% Bandwidth
VoIP g.729 (~28 Kbps)	10%
H.264 CIF Video (312 Kbps)	20%
Oracle	2.8%
Citrix ICA	3%
HTTP Applications	30%
HTTP Browsing (32K)	10%
HTTPS	10%
MS Exchange	5%
Streaming Video (160K and 250K)	5%
SMTP	2%
POP3	2%
DNS	0.2%

IOS Platforms – Test Configurations

	Config A Application aware QoS (without reporting)	Config B Application aware QoS (with reporting)	Config C Application Performance metrics
NBAR2	Yes	Yes	Yes
FNF – Traffic Usage	No	Yes	Yes
TCP Performance metrics (ART)	No	No	Yes
Media Monitoring	No	No	Yes
NBAR2 based QoS	Yes	Yes	Yes

IOS Platforms – Test Results

G2 Platform	A	B	C
	Throughput (Mbps)	Throughput (Mbps)	Throughput (Mbps)
3945e	705	351	184
3925e	428	253	151
3945	268	114	71
3925	225.3	92	60.8
2951	162	75	48
2921	112	53	37
2911	87	40	32
2901	81	41	25.6
1941	78	41	28

IOS-XE Platforms – Traffic Profiles

- Stateful Traffic profile with enterprise application mix modified for WAN aggregation
- Throughput measured @ 90% data plane CPU
- Average packet size: 550 bytes

Applications	% Bandwidth
VoIP g.729 (~28 Kbps)	3%
H.264 CIF Video (312 Kbps)	20%
Oracle	2.8%
Citrix ICA	3%
HTTP Applications	22%
HTTP Browsing (32K)	22%
HTTPS	10%
MS Exchange	3%
Streaming Video (160K and 250K)	5%
SMTP	0.5%
POP3	0.5%
DNS	0.2%

IOS-XE Platforms – Test Configurations

	Config A Application QoS	Config B Application QoS + App Usage	Config C Application QoS + App Usage + App Performance
NBAR2	Yes	Yes	Yes
HQoS (with NBAR2)	Yes	Yes	Yes
Traffic stats flow records in unified monitoring	No	Yes	Yes
ART flow records in unified monitoring	No	No	Yes
Media flow records in unified monitoring	No	No	Yes

IOS-XE Platforms – Test Results

XE Platform	A	B	C
	Throughput (Gbps)	Throughput (Gbps)	Throughput (Gbps)
4451-X	1.4	0.9	0.7
ASR1001	4.1	2.4	2.1
ESP5	5.0	1.4	1.2
ESP10	10.0	2.8	2.5
ESP20	20.0	5.6	4.9
ESP40	23.8	4.9	4.7
Kingpin	17.7	12.4	10.9
ESP100	64.8	14.3	8.2




Conclusion

AVC Network Management – What is Available?

AVC Cisco Developer Network Site: http://developer.cisco.com/web/avc

Vendor		NBAR2	Field Extraction	URL Hit Count	MMON	ART	PfR	QoS Class	Multi-tenant
Cisco Prime Infrastructure 2.0	IOS	☑			☑	☑			
	XE	☑	☑		☑	☑			
ActionPacked LiveAction V3.x	IOS	☑			☑	☑	☑	☑	
	XE	☑ (MIBs)			☑	☑	☑	☑	
Plixer Scrutiniser	IOS	☑			☑	☑	☑		
	XE				☑		☑		
Living Objects	IOS	☑		☑		☑			☑
	XE			☑		☑			☑
InfoVista SDM 3.3 5View 6.3	IOS	☑				☑			☑
	XE								
Insight v4.0	IOS	☑				☑			☑
	XE	☑	☑						☑

Key Takeaway

What can AVC do for me?	How?
Identify various applications in my network	NBAR2 uses DPI to identify 1000+ applications
Collect traffic information and performance metrics without hardware probe	Embedded monitoring exports information in standard NFv9 or IPFIX format
Provide data for proactive monitoring and troubleshooting	Both Cisco Prime Infrastructure and 3rd party are supported
Tune my network to improve application performance	Application-aware QoS leveraging NBAR2 to identify applications – PfR Path Control

Technical References

- Application Visibility and Control
  - http://www.cisco.com/go/avcportal
  - http://www.cisco.com/go/pfr
- Docwiki.cisco.com
  - AVC: http://docwiki.cisco.com/wiki/AVC:Home
  - PfR: http://docwiki.cisco.com/wiki/PfR:Home
- AVC Solution Guide for IOS-XE
  - http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_xe3_8/avc_soln_guide_iosxe3_8.html
  - http://www.cisco.com/en/US/docs/ios/solutions_docs/avc/ios_xe3_9/avc_soln_guide_iosxe3_9.html
  - http://www.cisco.com/en/US/partner/docs/ios/solutions_docs/avc/ios_xe3_10/avc_config.html
- NBAR
  - http://www.cisco.com/en/US/partner/docs/ios/ios_xe/qos/configuration/guide/clsfy_traffic_nbar_xe.html
- AVC Cisco Developer Network (CDN)
  - http://developer.cisco.com/web/avc




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
- 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

CISCO™