Cisco live!

What You Make Possible

TOMORROW starts here.

cisco

Application Visibility and Control in Enterprise WAN

BRKRST-2030

TOMORROW starts here.

Managing Growing Applications in Today's Network

Understand the traffic pattern to control congestion

Accurately identify users of critical resources

Managing Growing Applications in Today's Network

Assess the traffic condition

Control the rate of traffic

Find the most optimal path

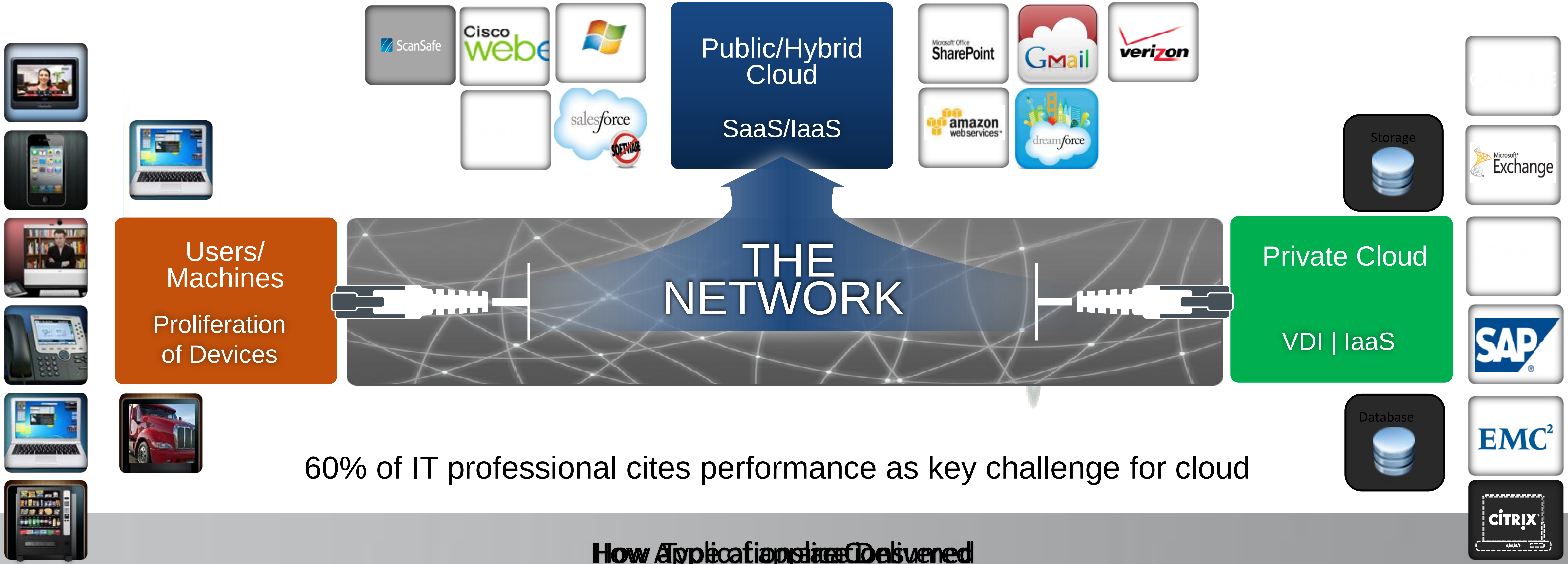
Agenda

- Why we need Application-awareness in Enterprise WAN?
- What is AVC?
- AVC Technologies
  - Application Recognition (NBAR2)
  - Performance Monitoring (FNF, ART, MMON)
  - Management Tool
  - Control (QoS, PfR)
- AVC and WAAS
- Conclusion

Why Application Visibility and Control in Enterprise WAN?

Business and IT are Changing Like Never Before

Drastic Change in Application Type, Delivery, and Consumption



60% of IT professional cites performance as key challenge for cloud

How Applications are Delivered

New User Behaviour and New Trends

Network Need to Evolve to Support These Transitions

Application complexity increases

Identify growing applications using more than just port number

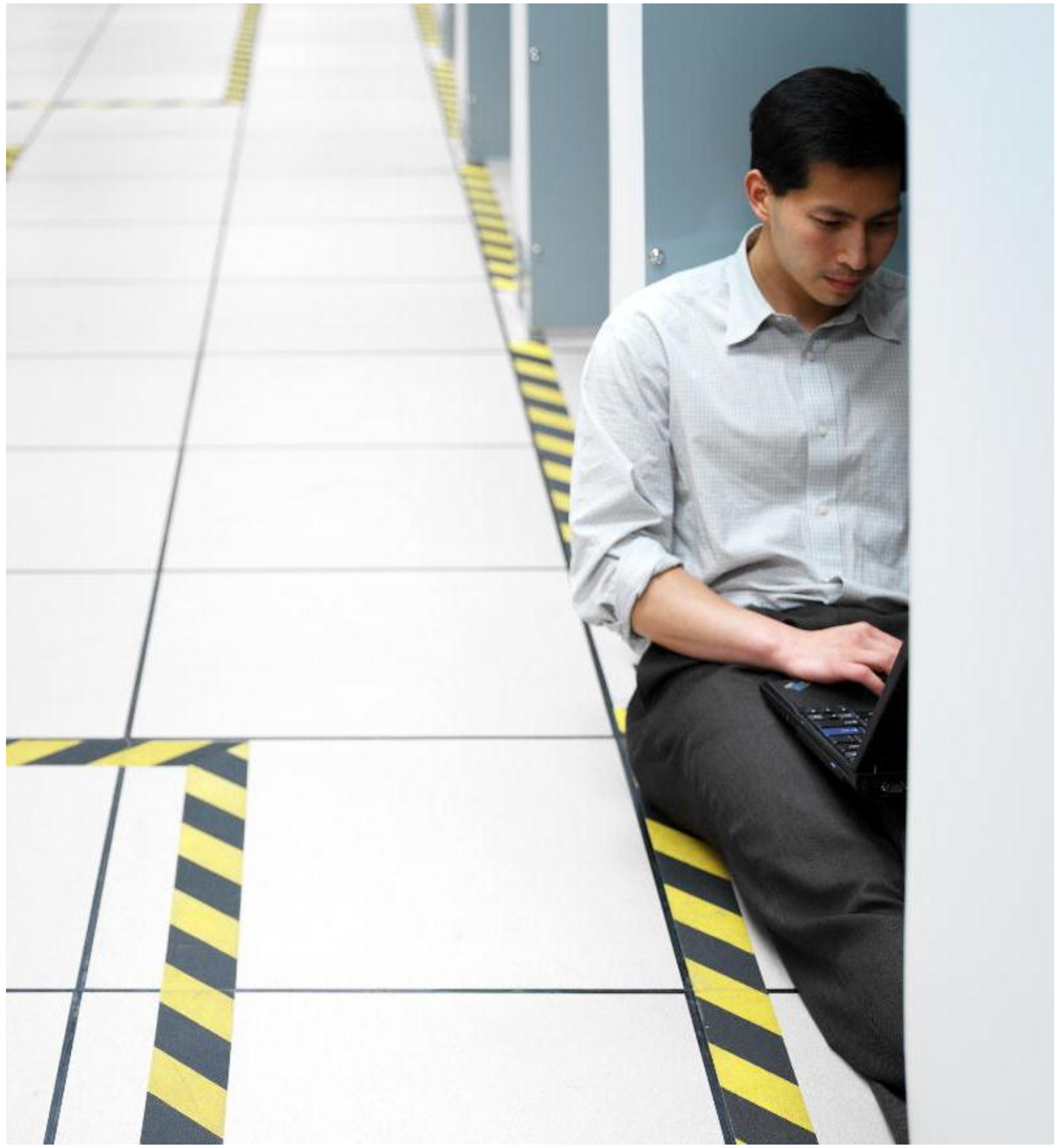
Cloud and Virtualisation centralise application delivery

Understand application performance from end users perspective

Multiple entities involved in delivering applications

Problem isolation to minimise downtime and business impact

How Can My Network Infrastructure Help Me?



Granularly identify the applications

Maximise use of available resources

Understand the network condition and capacity

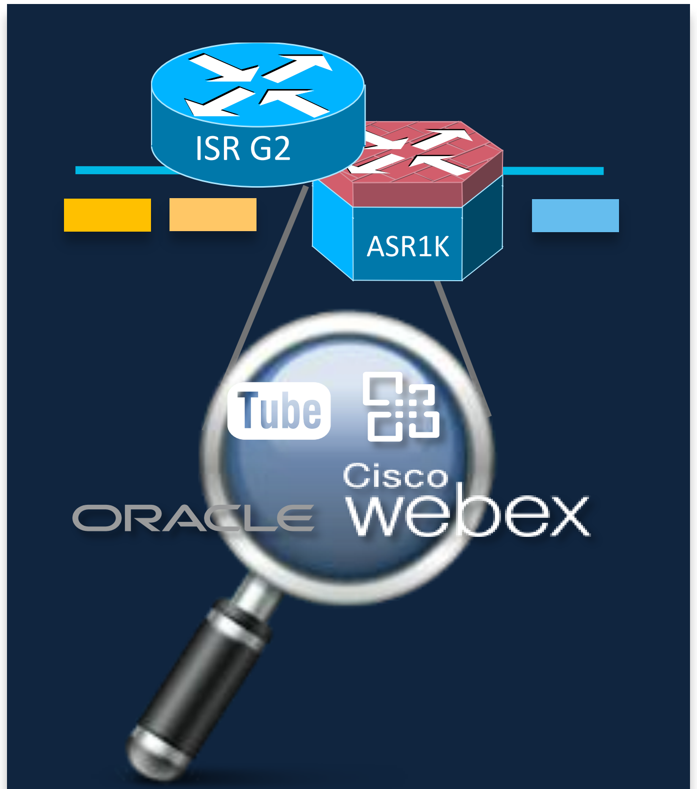
Understand the user experience

Control unwanted traffic

Deliver consistent performance to critical applications

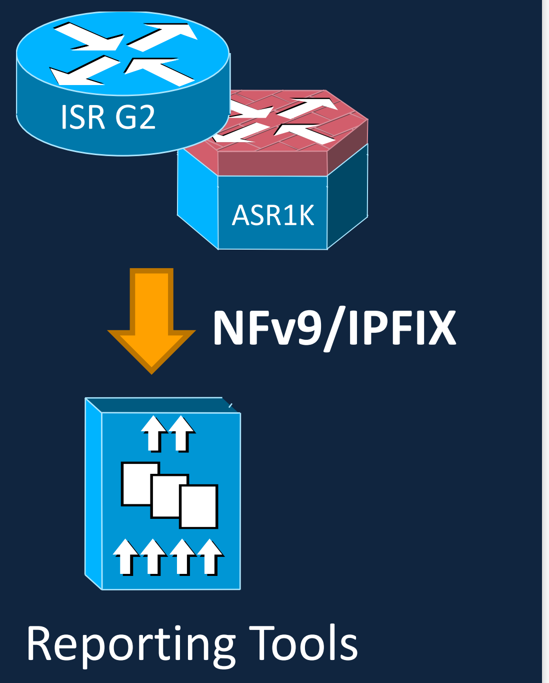
What is Application Visibility and Control (AVC)?

Application Visibility and Control for WAN – How it work?



Application Recognition

Identify applications using DPI



Perf. Collection & Exporting

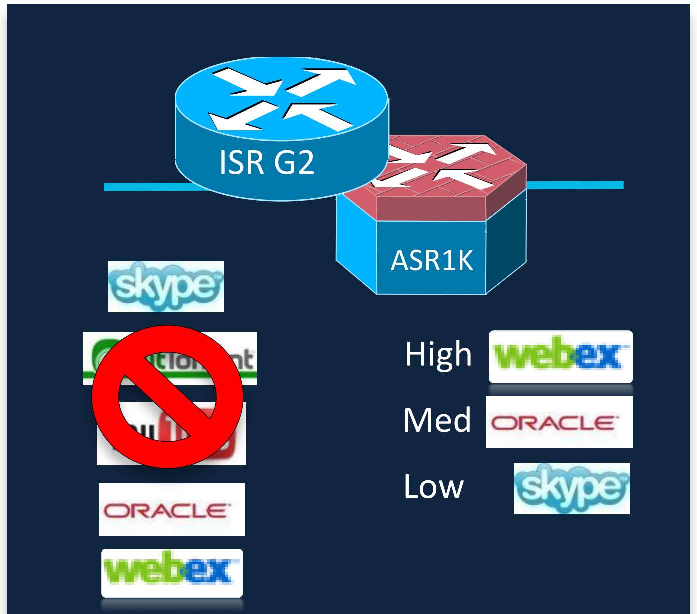
ISR G2 & ASR collect application bandwidth and response time metrics, and export to management tool

App Visibility & User Experience Report

App	BW	Transaction Time	…
WebEx	3 Mb	150 ms	…
Citrix	10 Mb	500 ms	…

Management Tool

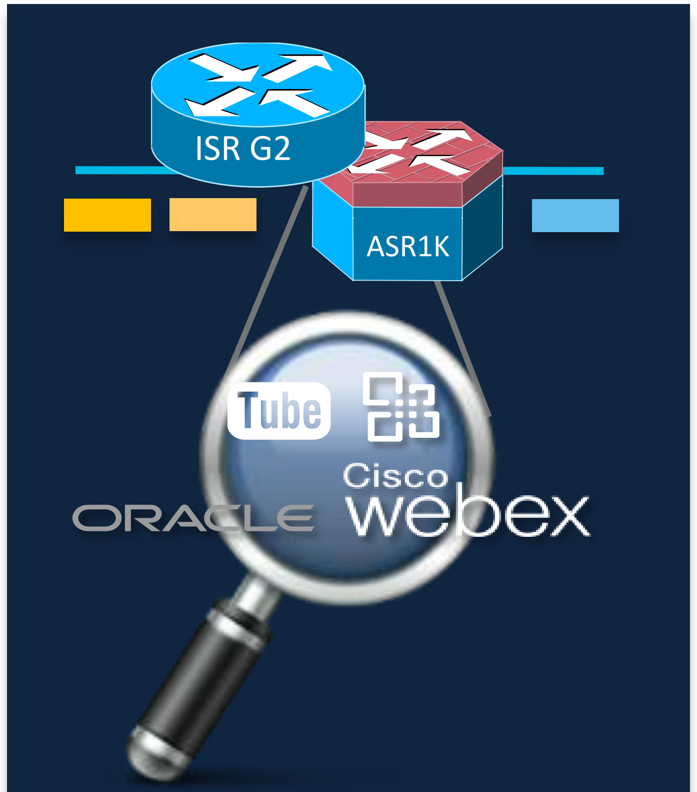
Advanced reporting tool aggregates and reports application performance



Control

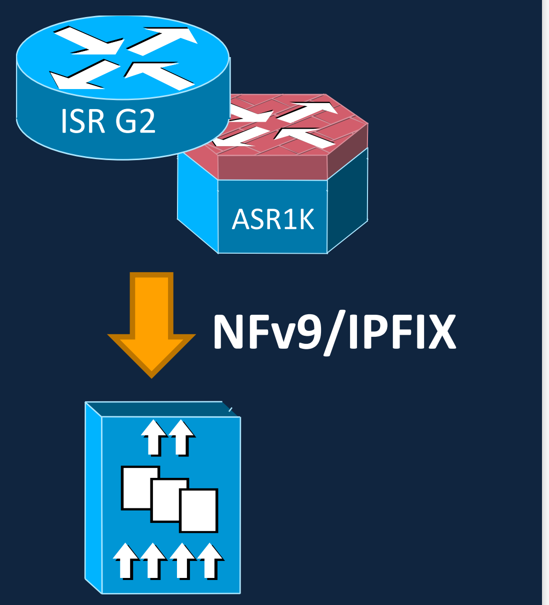
Control application usage in the network to maximise application performance

Application Visibility and Control for WAN – Enable Technologies



Application Recognition

- NBAR2



Reporting Tools

Perf. Collection & Exporting

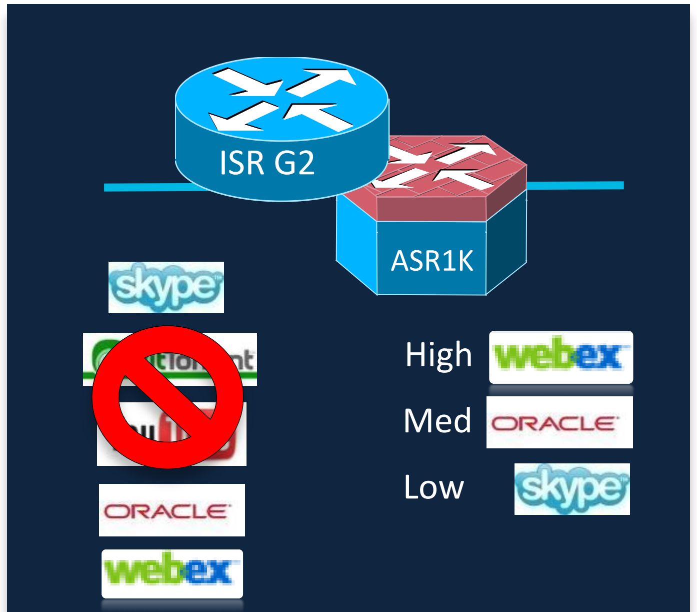
- FNF
- ART
- MMON

App Visibility & User Experience Report

App	BW	Transaction Time	…
WebEx	3 Mb	150 ms	…
Citrix	10 Mb	500 ms	…

Management Tool

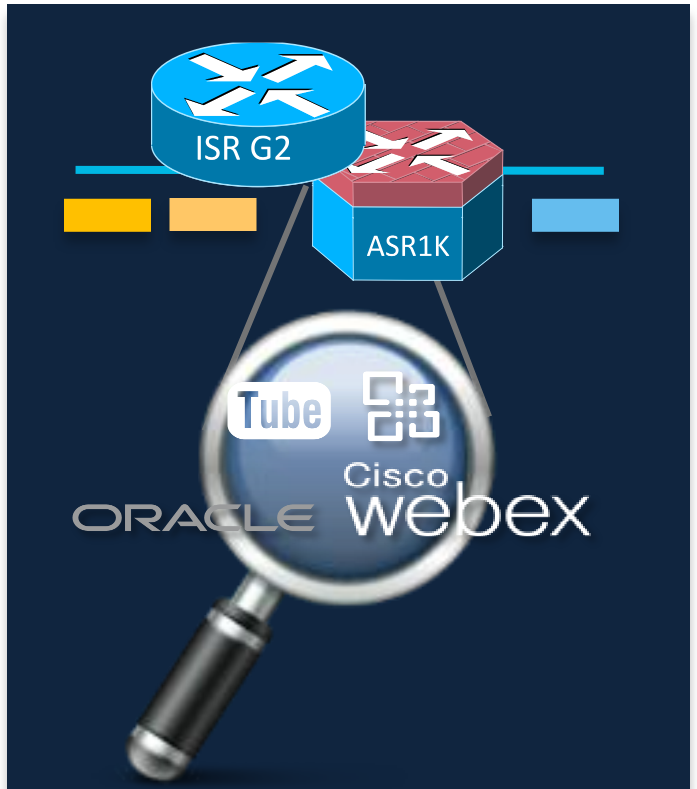
- Cisco Prime Infrastructure
- 3rd Party



Control

- QoS
- PfR

AVC Technologies



Application Recognition

Identify applications using DPI

Application Recognition

What is an Application?

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

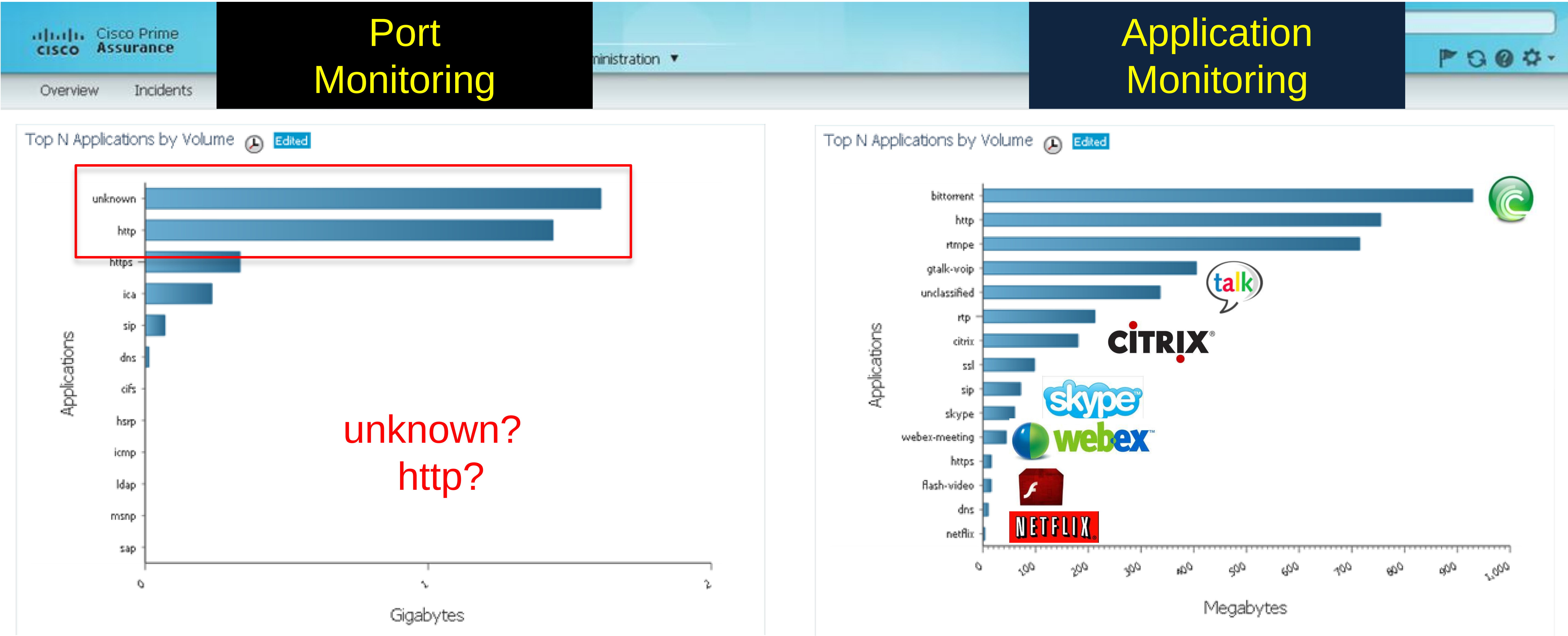
Are these applications?

Or just ports?

What about these?

webex
Rhapsody
Gmail by Google BETA
YouTube
McAfee
skype
Microsoft Exchange
Google talk BETA
Microsoft Office Live Meeting
BitTorrent
iTunes
Windows Server Update Services
Microsoft Office SharePoint Server 2007
salesforce.com

What is Really in Your Network?



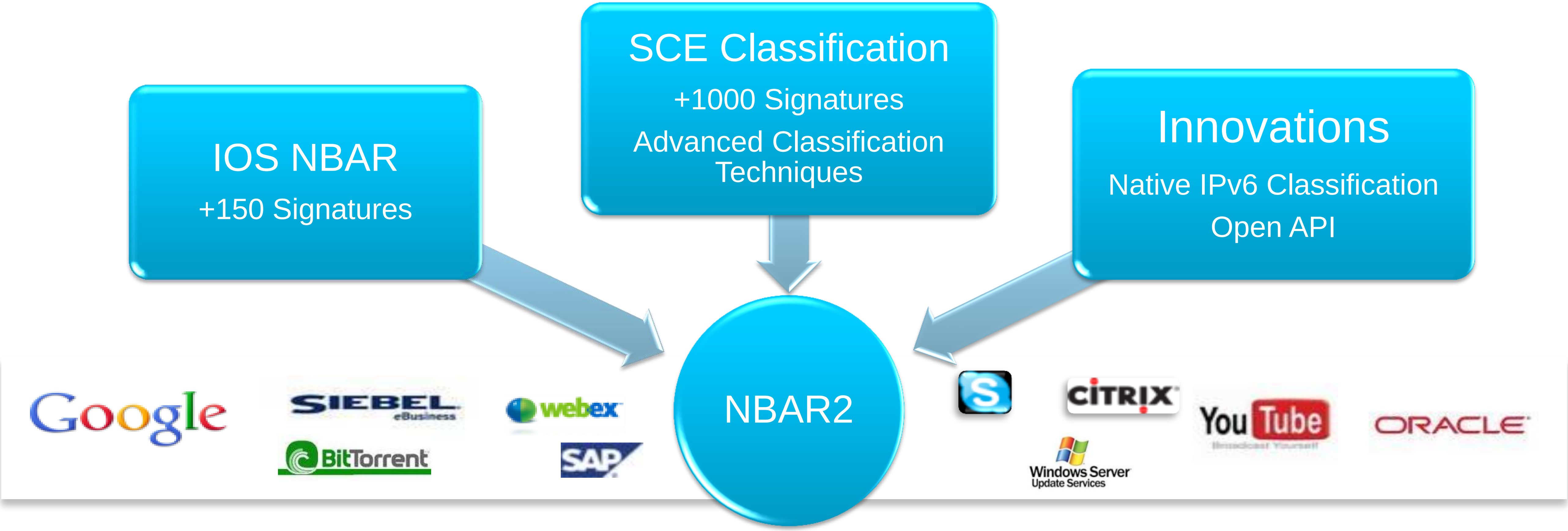
Port Monitoring

Application Monitoring

unknown?
http?

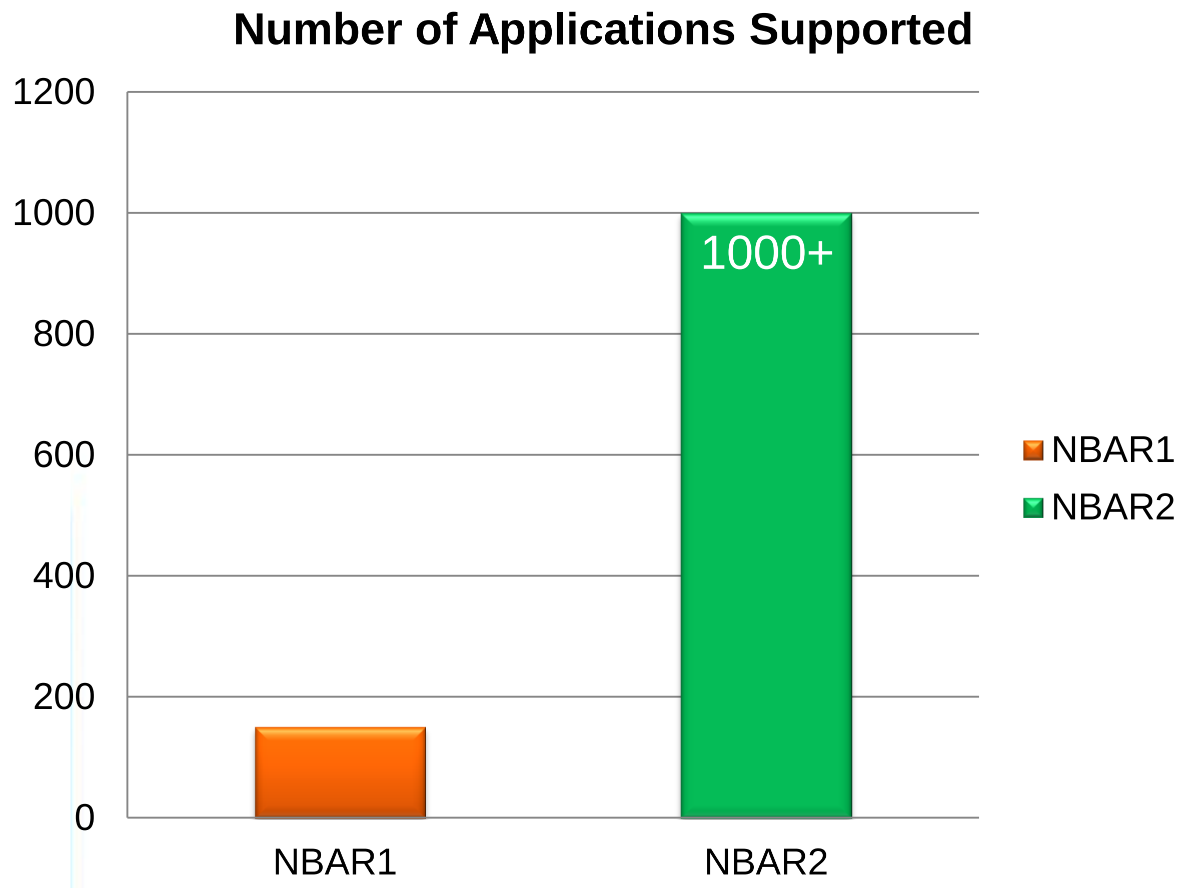
ISR G2: 15.2(2)T1
ASR1K: 3.4S

Next Generation NBAR (NBAR2)



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

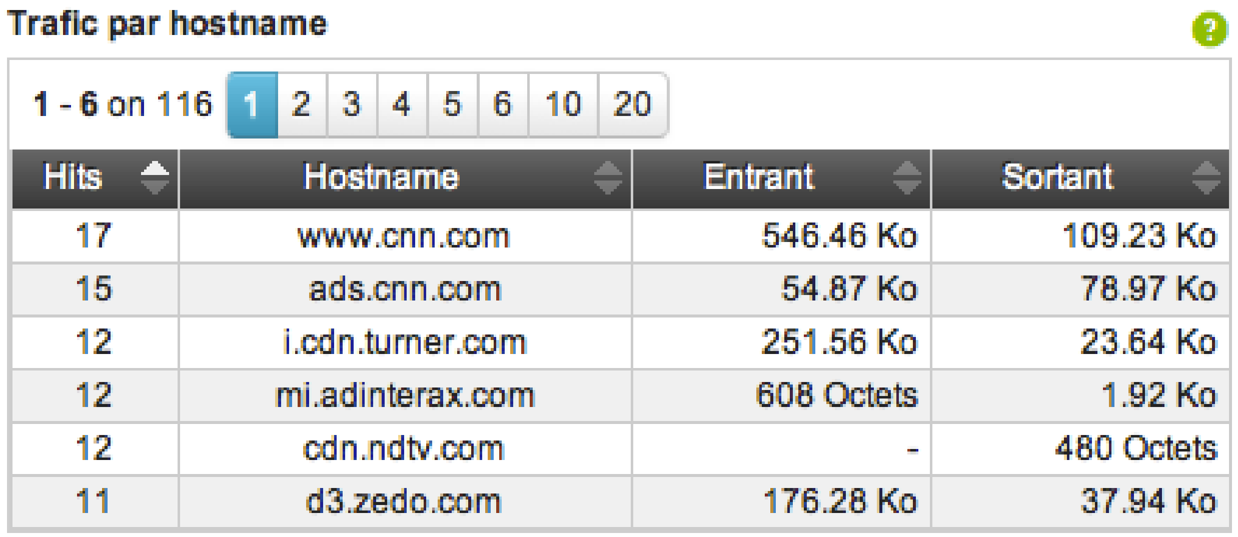
NBAR2 Highlight



Domain name

URI

Browser Type

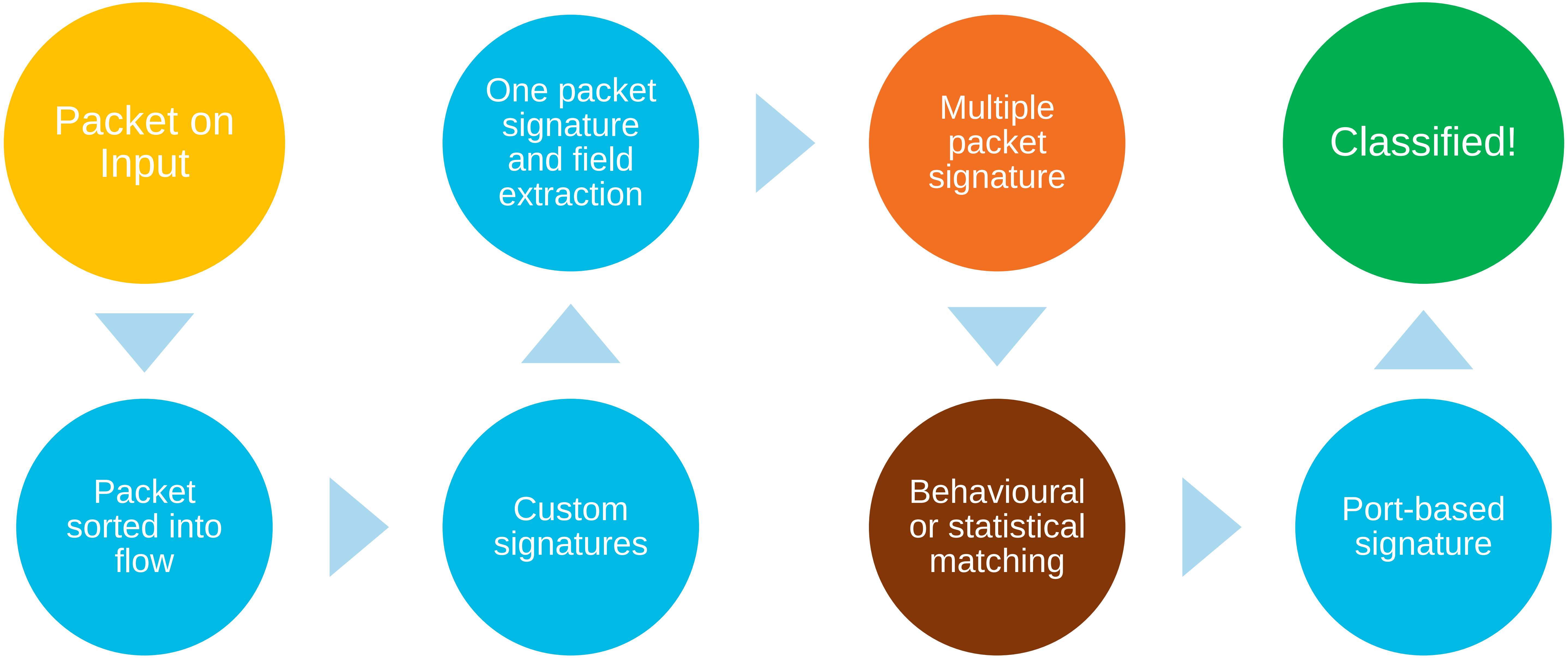

Trafic par hostname

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

- More than 1000 applications support and growing
- Detect applications regardless of port they are running

- Field Extraction – collect application specific information in addition to identify applications
- Sub-port Classification – match parameters of the applications

NBAR2 Classification Engine



Packet on Input

Packet sorted into flow

Custom signatures

One packet signature and field extraction

Multiple packet signature

Behavioural or statistical matching

Port-based signature

Classified!

Different Ways to Use NBAR2

1. Discover applications going across interfaces
   - ip nbar protocol-discovery CLI
2. Match applications or groups of applications in QoS class-map to take action, i.e. shape, police, remark
   - match protocol CLI in QoS class-map
3. With Flexible Netflow (FNF) or other performance reporting features to report application name
   - match or collect application name CLI

NBAR2 Sub-port Classification

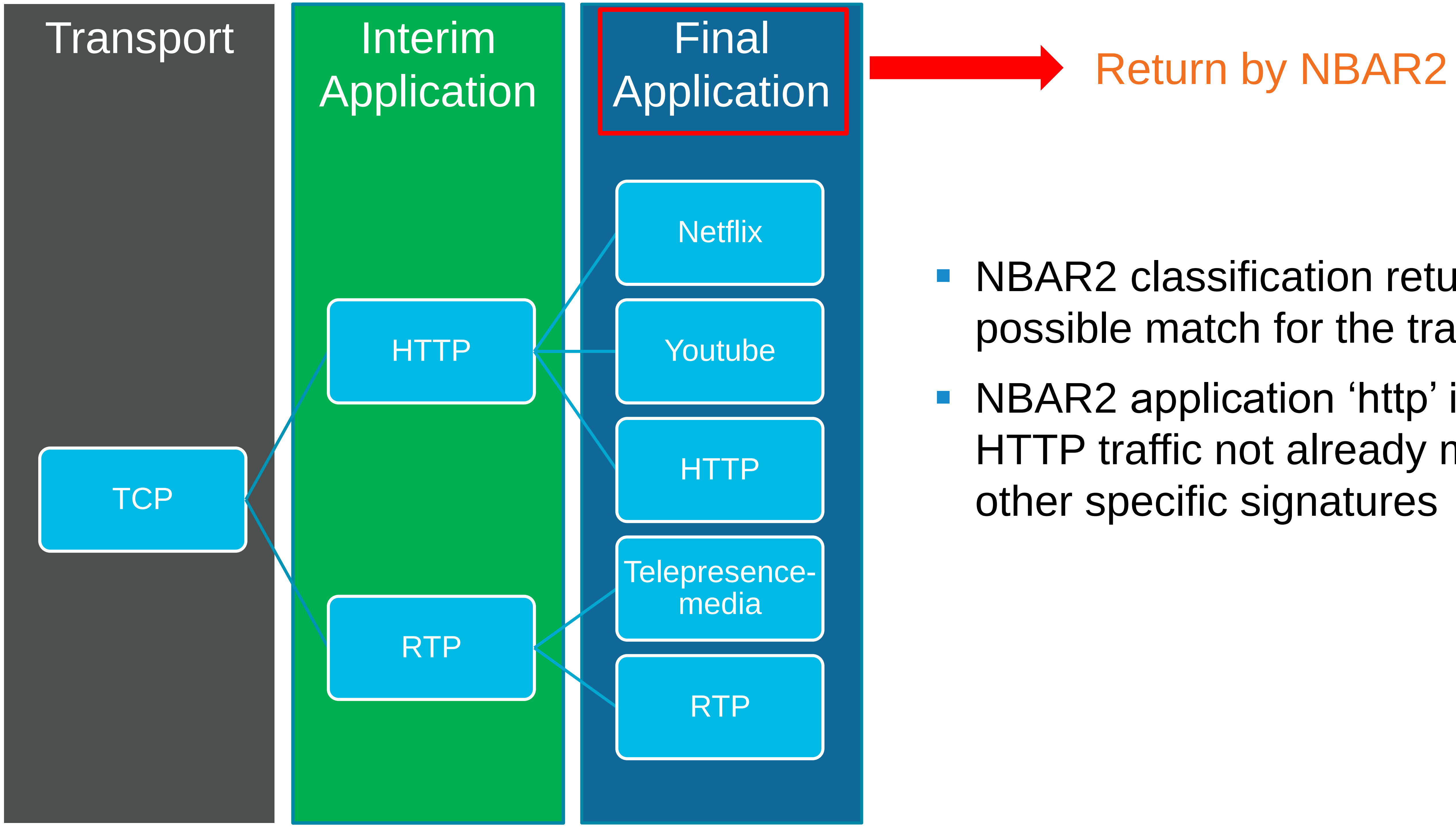
- Allows finer grained classification of traffic based on additional application level characteristics
  - http url, host, mime, User Agent and other fields
    - e.g. “match protocol http url *cisco.com*” matches http traffic to and from cisco.com
  - rtp payload-type
    - e.g. “match protocol rtp video” matches rtp video traffic
  - citrix ica-tag, app
    - e.g. “match protocol citrix ica-tag 0” matches citrix traffic with ica-tag 0

How to identify which NBAR2 sub-port classification is available?

```
router#show ip nbar parameter subclassification

 Protocol         Parameter            Parameter type
 ---------        ----------           ---------------
 share-point      Blog                 enum
 share-point      Document             enum
 share-point      Admin                enum
 share-point      Calendar             enum
 vnc              file-transfer        enum
 edonkey          search-file-name     regexp
 edonkey          file-transfer        regexp
 edonkey          text-chat            regexp
 rtp              payload-type         multi
 rtp              video                enum
 rtp              audio                enum
 webex-meeting    payload-type         multi
 webex-meeting    video                enum
 webex-meeting    audio                enum
 kazaa2           file-transfer        regexp
 gnutella         file-transfer        regexp
 fasttrack        file-transfer        regexp
 citrix           app                  regexp
 citrix           ica-tag              integer
 http             mime                 regexp_url
 http             content-encoding     regexp_url
 http             location             regexp_url
 (..snip..)
```

```
router(config)#class-map share-point
router(config-cmap)#match protocol share-point ?
  Admin     Match Administrator related actions
  Blog      Match Blog related actions
  Calendar  Match Calendar related actions
  Document  Match File Download and Upload
```

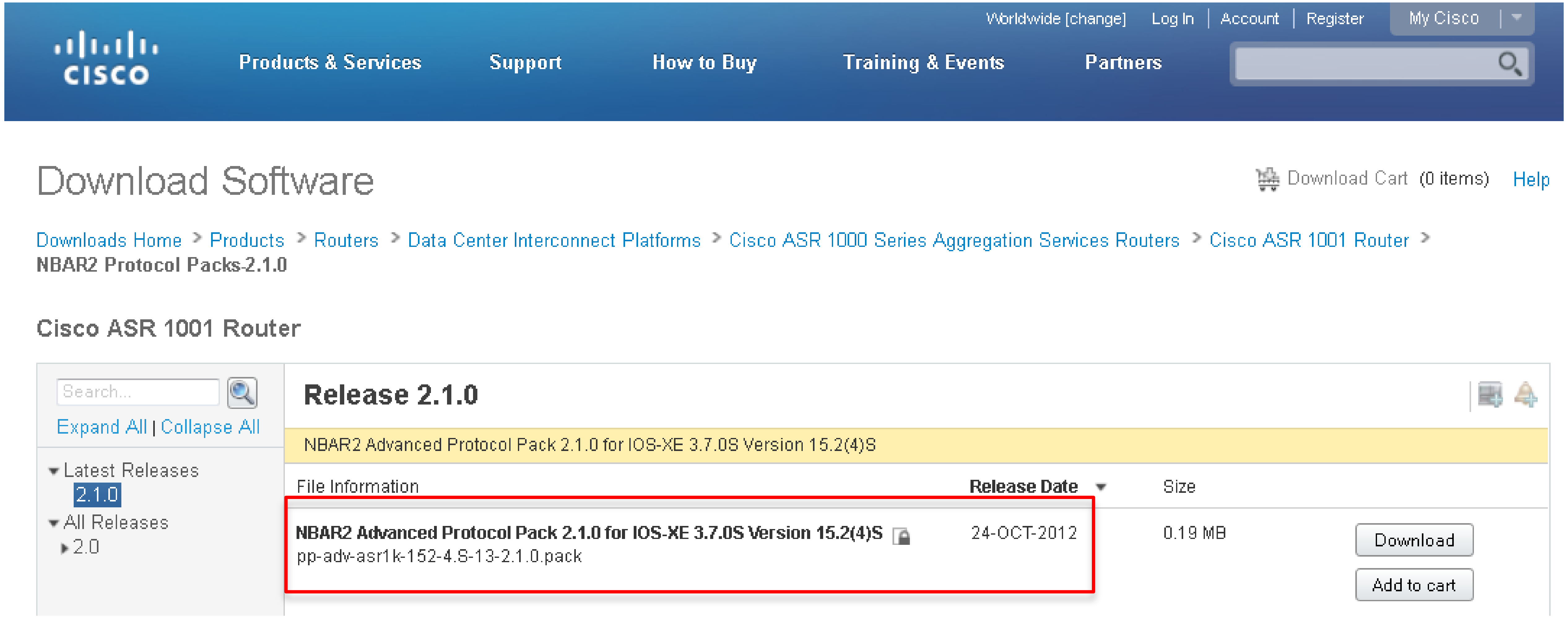
NBAR2 Classification Behaviour



- NBAR2 classification returns the best possible match for the traffic
- NBAR2 application ‘http’ includes only HTTP traffic not already matched by other specific signatures

NBAR2 Protocol Pack

ISR G2: 15.2(4)M2
ASR1K: 3.7S



Download Software

Download Cart (0 items) Help

Downloads Home > Products > Routers > Data Center Interconnect Platforms > Cisco ASR 1000 Series Aggregation Services Routers > Cisco ASR 1001 Router > NBAR2 Protocol Packs-2.1.0

Cisco ASR 1001 Router

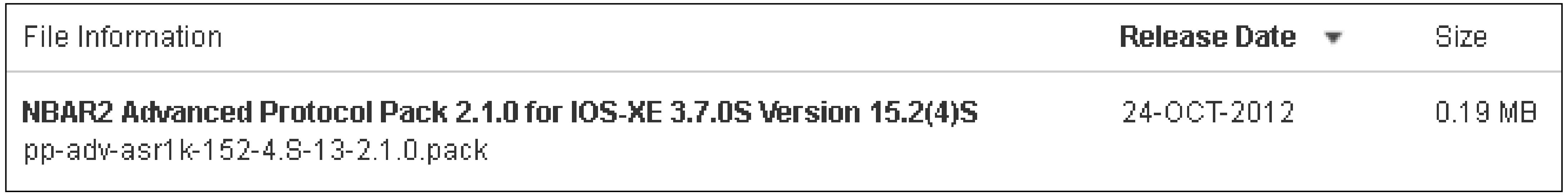
Release 2.1.0

NBAR2 Advanced Protocol Pack 2.1.0 for IOS-XE 3.7.0S Version 15.2(4)S

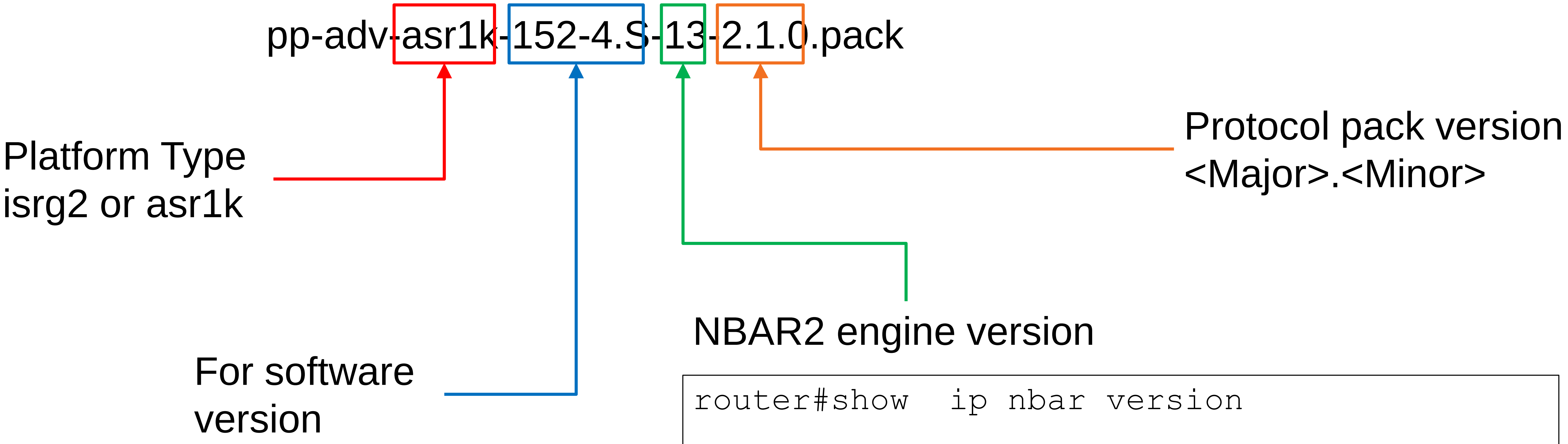
File Information	Release Date	Size	
NBAR2 Advanced Protocol Pack 2.1.0 for IOS-XE 3.7.0S Version 15.2(4)S pp-adv-asr1k-152-4.S-13-2.1.0.pack	24-OCT-2012	0.19 MB	Download Add to cart

- 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

Protocol Pack Explanation



File Information	Release Date ▾	Size
NBAR2 Advanced Protocol Pack 2.1.0 for IOS-XE 3.7.0S Version 15.2(4)S pp-adv-asr1k-152-4.S-13-2.1.0.pack	24-OCT-2012	0.19 MB



pp-adv-asr1k-152-4.S-13-2.1.0.pack

Platform Type
isrg2 or asr1k

For software
version

NBAR2 engine version

Protocol pack version
<Major>.<Minor>

```
router#show  ip nbar version

NBAR software version: 13

(..snip..)
```

NBAR2 Protocol Pack Upgrade Process

Step 1: Download Protocol Pack from CCO and place on router flash

```
router#dir bootflash:pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
Directory of bootflash:/pp-adv-asr1k-15.2(04)S-13-1.1(0).pack

48785  -rw-      188131   Sep 6 2012 21:24:52 -07:00  pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
```

Step 2: Configure NBAR2 to use Protocol Pack on flash

```
router#(config)#ip nbar protocol-pack flash:pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
```

Step 3: Validate that new protocol pack is active

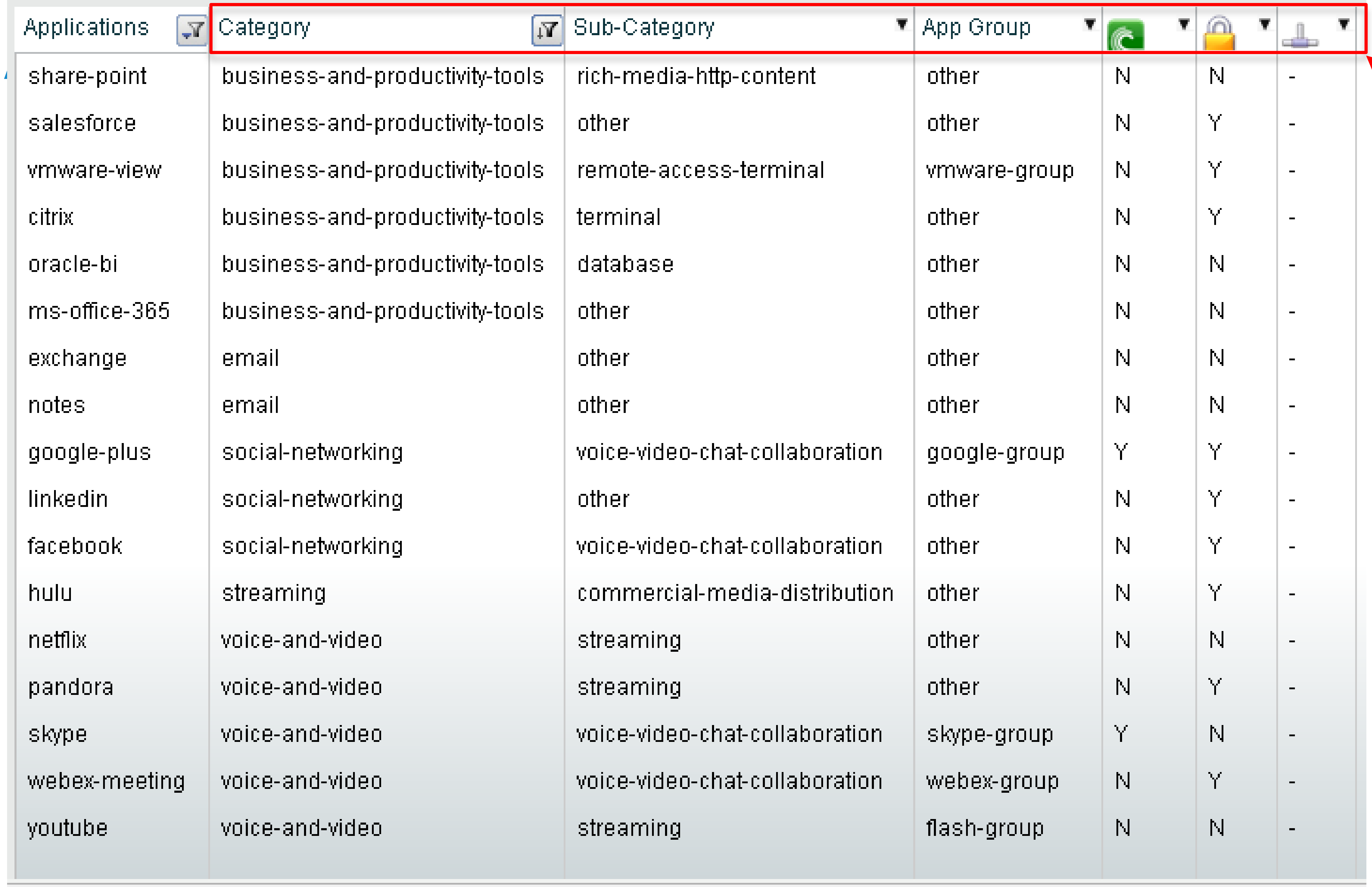
```
router#show ip nbar protocol-pack active

ACTIVE protocol pack:
Name:                             Advanced Protocol Pack
Version:                          3.0
Publisher:                        Cisco Systems Inc.
File:                             flash:pp-adv-asr1k-15.2(04)S-13-1.1(0).pack
```

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

Example: Applications and NBAR2



Applications	Category	Sub-Category	App Group		🔒	
share-point	business-and-productivity-tools	rich-media-http-content	other	N	N	-
salesforce	business-and-productivity-tools	other	other	N	Y	-
vmware-view	business-and-productivity-tools	remote-access-terminal	vmware-group	N	Y	-
citrix	business-and-productivity-tools	terminal	other	N	Y	-
oracle-bi	business-and-productivity-tools	database	other	N	N	-
ms-office-365	business-and-productivity-tools	other	other	N	N	-
exchange	email	other	other	N	N	-
notes	email	other	other	N	N	-
google-plus	social-networking	voice-video-chat-collaboration	google-group	Y	Y	-
linkedin	social-networking	other	other	N	Y	-
facebook	social-networking	voice-video-chat-collaboration	other	N	Y	-
hulu	streaming	commercial-media-distribution	other	N	Y	-
netflix	voice-and-video	streaming	other	N	N	-
pandora	voice-and-video	streaming	other	N	Y	-
skype	voice-and-video	voice-video-chat-collaboration	skype-group	Y	N	-
webex-meeting	voice-and-video	voice-video-chat-collaboration	webex-group	N	Y	-
youtube	voice-and-video	streaming	flash-group	N	N	-

NBAR2 Attributes

List of all NBAR2 Attributes and Values

For Your Reference

NBAR2 Category	NBAR2 Sub-category	NBAR2 Application Group		P2P Technology	Encrypted	Tunnel
browsing	authentication-services	apple-talk-group	skype-group	n	n	n
business-and-productivity-tools	backup-systems	banyan-group	smtp-group	y	y	y
email	client-server	bittorrent-group	snmp-group	unassigned	unassigned	unassigned
file-sharing	commercial-media-distribution	corba-group	sqlsvr-group			
gaming	control-and-signalling	edonkey-emule-group	stun-group			
industrial-protocols	database	fasttrack-group	telepresence-group			
instant-messaging	epayement	flash-group	tftp-group			
internet-privacy	file-sharing	fring-group	vmware-group			
layer2-non-ip	inter-process-rpc	ftp-group	vnc-group			
layer3-over-ip	internet-privacy	gnutella-group	wap-group			
location-based-services	license-manager	gtalk-group	webex-group			
net-admin	naming-services	icq-group	windows-live-messanger-group			
newsgroup	network-management	imap-group	xns-xerox-group			
obsolete	network-protocol	ipsec-group	yahoo-messenger-group			
other	other	irc-group				
trojan	p2p-file-transfer	kerberos-group				
voice-and-video	p2p-networking	ldap-group				
	remote-access-terminal	netbios-group				
	rich-media-http-content	nntp-group				
	routing-protocol	npmp-group				
	storage	other				
	streaming	p2p-file-transfer				
	terminal	pop3-group				
	tunnelling-protocols	prm-group				
	voice-video-chat-collaboration	skinny-group				

How to Determine NBAR2 Attributes

- What applications are in sub-category voice-video-chat-collaboration?

Attribute type

```
router#show ip nbar attribute sub-category voice-video-chat-collaboration
  aol-messenger              AOL Messenger Text Chat
  aol-protocol               America OnLine protocol
  bnet                       bnet
  cisco-phone                Cisco IP Phones and PC-based Unified Communicators
  conference                 chat
  cooltalk                   Internet telephony tool
(..snip)
```

Attribute name

- What are the values of all attributes of application webex-meeting?

```
router#show ip nbar protocol-attribute webex-meeting
           Protocol Name :  webex-meeting
                category :  voice-and-video
            sub-category :  voice-video-chat-collaboration
       application-group :  webex-group
          p2p-technology :  p2p-tech-no
                  tunnel :  tunnel-no
               encrypted :  encrypted-yes
```

Application name

Pre-defined Attributes

How to Reassign NBAR2 Application Attributes

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

Configure NBAR attribute-map and associate with a particular application using attribute-set

```
router(config)#ip nbar attribute-map payroll_custom_attr
router(config-attribute-map)#attribute category business-and-productivity-tools
router(config-attribute-map)#attribute encrypted encrypted-yes
router(config-attribute-map)#exit
router(config)#ip nbar attribute-set my_payroll payroll_custom_attr
```

NBAR2 Application

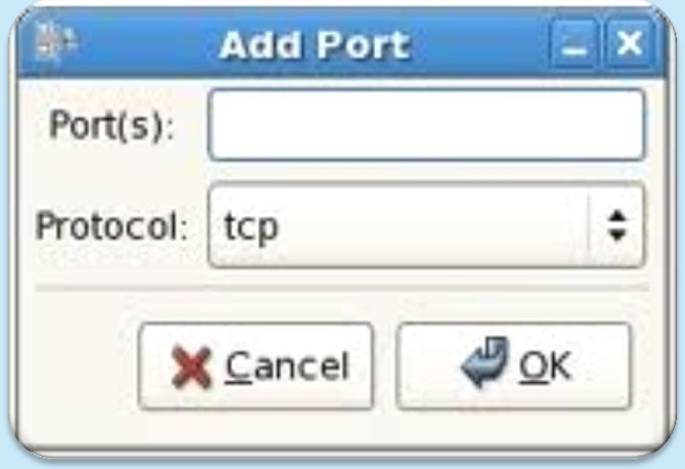
Before: Default, Pre-assigned attributes

```
router#show ip nbar protocol-attribute
my_payroll
           Protocol Name :  my_payroll
                category :  other
            sub-category :  other
       application-group :  other
          p2p-technology :  p2p-tech-unassigned
                  tunnel :  tunnel-unassigned
               encrypted :  encrypted-unassigned
```

After: Reassigned attributes using attribute-map

```
router#show ip nbar protocol-attribute
my_payroll
           Protocol Name :  my_payroll
                category :  business-and-
productivity-tools
            sub-category :  other
       application-group :  other
          p2p-technology :  p2p-tech-unassigned
                  tunnel :  tunnel-unassigned
               encrypted :  encrypted-yes
```

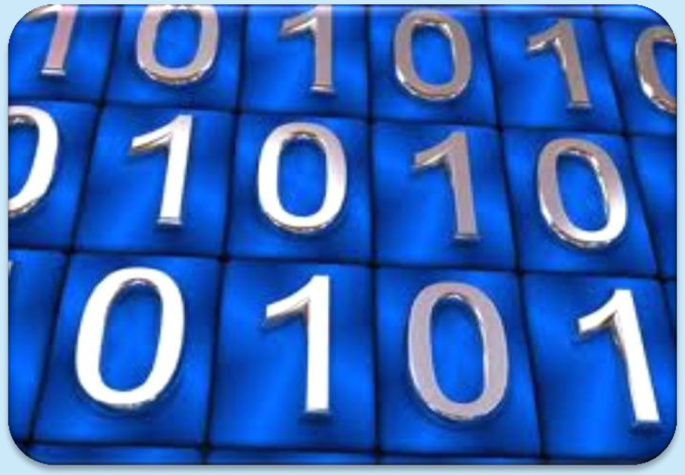
Define Your Own Application in NBAR2



Add Port

Port(s):

Protocol: tcp



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

New

- URI regex
- Host regex

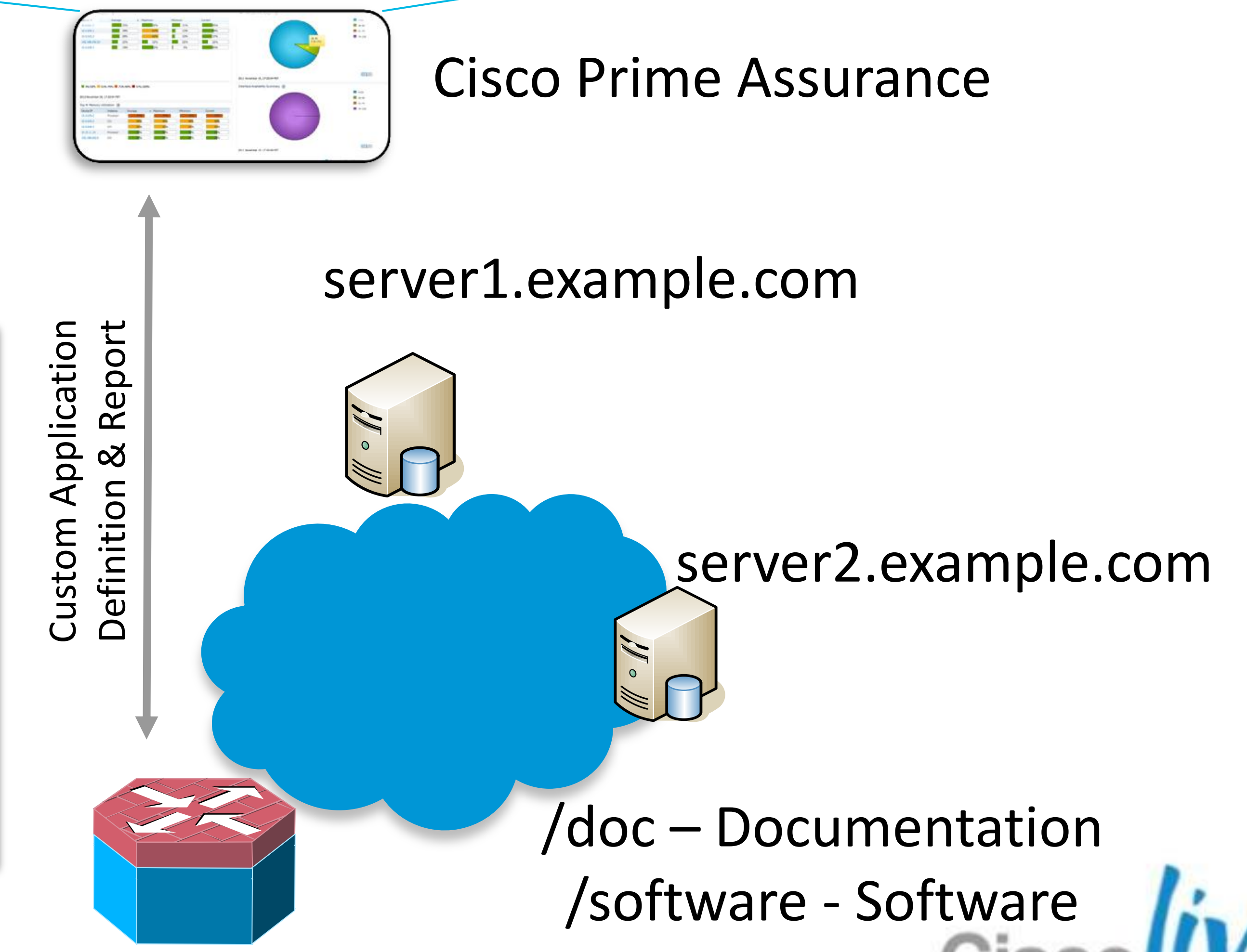
NBAR2 Custom Application Enhancement

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

- Today: NBAR supports custom app by port or values in payload
- New: Custom application match on HTTP URL
- Custom application match on HTTP URL and/or Host

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



Custom App Selector ID

```
router(config)#ip nbar custom my_payroll http host
               server1.example.com id 60001
router(config)#ip nbar custom my_doc_mgmt http url doc
               host server2.example.com id 60002
router(config)#ip nbar custom my_software_rep http url
               software host server2.example.com id 60003
```

ISR G2: Future
ASR1K: 3.8S

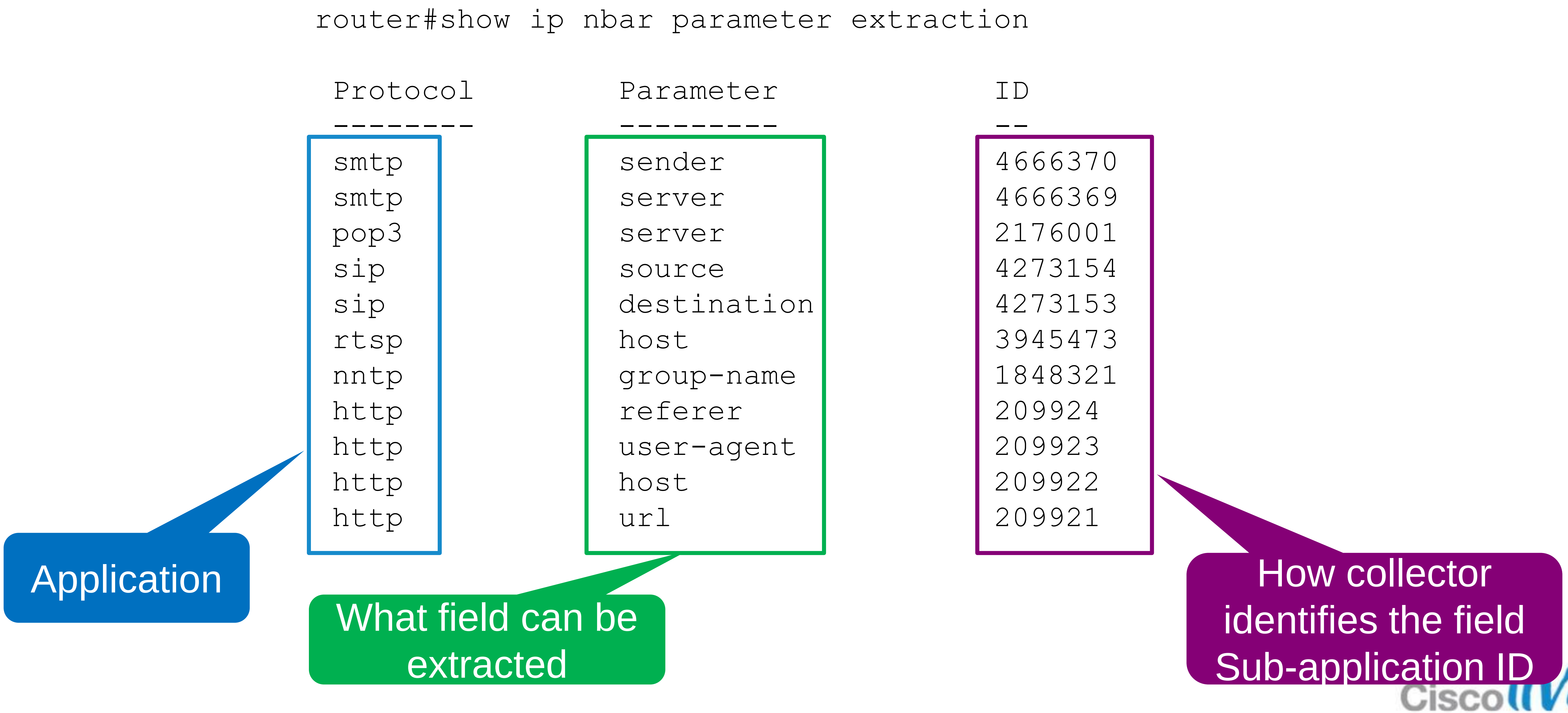
NBAR2 Field Extraction Support

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

NBAR2 Field Extraction Support

How to determine what fields can be extracted from application and export



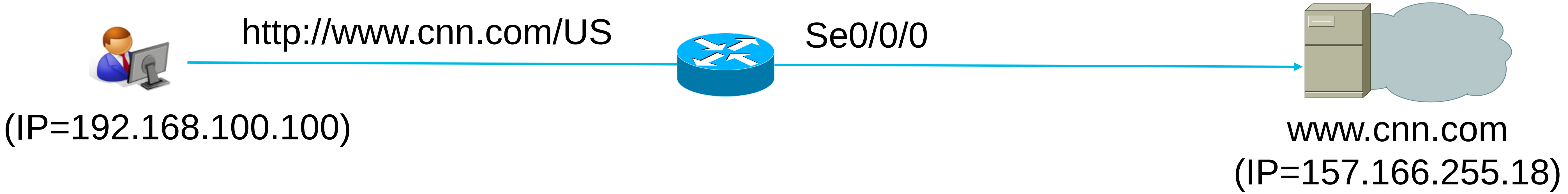
```
router#show ip nbar parameter extraction

 Protocol         Parameter             ID
 --------         ---------             --
 smtp             sender                4666370
 smtp             server                4666369
 pop3             server                2176001
 sip              source                4273154
 sip              destination           4273153
 rtsp             host                  3945473
 nntp             group-name            1848321
 http             referer               209924
 http             user-agent            209923
 http             host                  209922
 http             url                   209921
```

Application

What field can be extracted

How collector identifies the field Sub-application ID

Example: HTTP Field Extraction



collect application http url

collect application http host

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/
```

NBAR2 Resources ASR1000

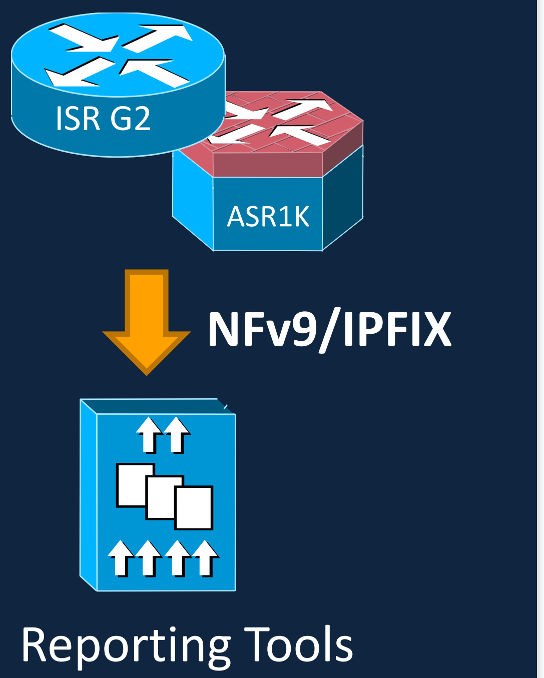
```
router# show ip nbar resources flow
NBAR flow statistics
        Maximum no of sessions allowed : 1000000
        Maximum memory usage allowed   : 367001 KBytes
        Active sessions                : 0
        Active memory usage            : 43712 KBytes
        Peak session                   : 1223
        Peak memory usage              : 43712 Kbytes

router(config)# ip nbar resources flow max-session <number of sessions>
router(config)# ip nbar resources protocol max-session <link age in
                multiple of system link age (secs.)>
```

- A syslog is generated if the number of active flows exceed the limit

Determine CPU Utilisation

- Find the CPU utilisation
  - **ISR G2:** show proc cpu
  - **ASR1K:** show platform hardware qfp active datapath utilisation summary

```
router#show platform hardware qfp active datapath utilization summary
  CPP 0:                         5 secs        1 min        5 min       60 min
Input:      Total (pps)              13           17           16           17
                  (bps)           14168        40872        21528        24072
Output:     Total (pps)              12           17           16           16
                  (bps)           15440        48728        29640        32144
Processing: Load (pct)                0            0            0            0
```



Perf. Collection & Exporting

ISR G2 & ASR collect application bandwidth and response time metrics, and export to management tool

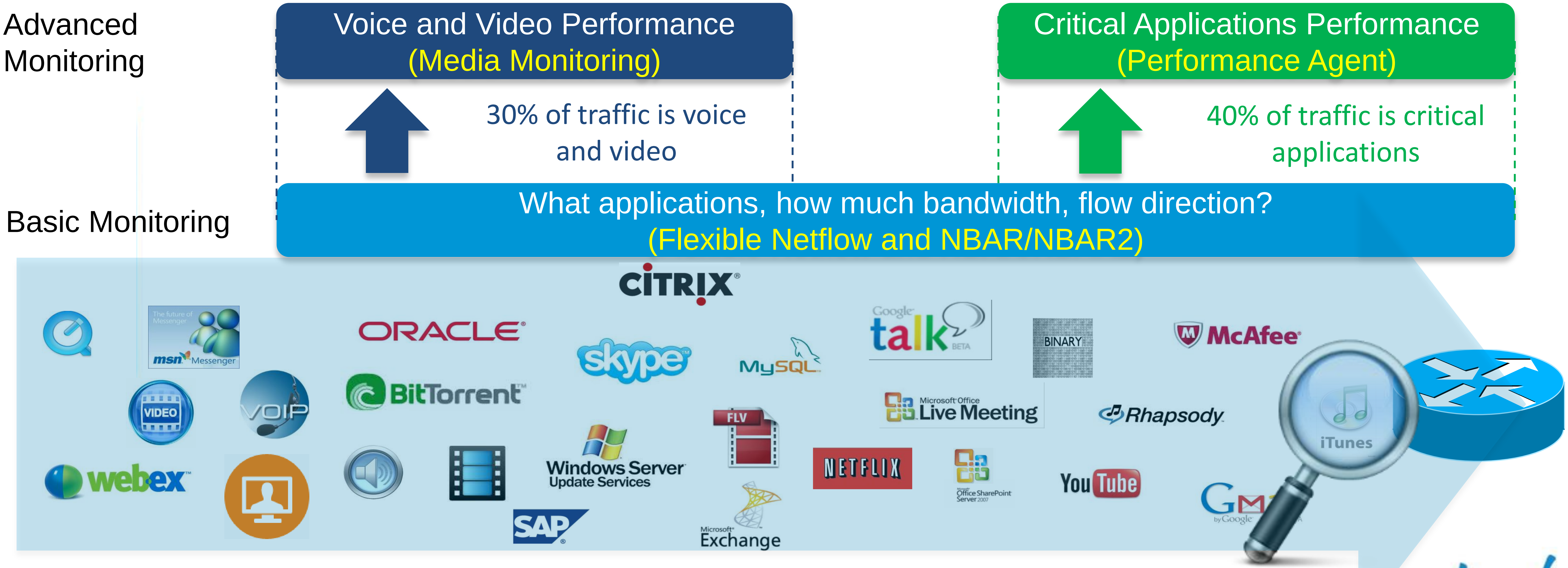
Performance Collection & Exporting

Performance Collection & Exporting – What is it?

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

Advanced Monitoring

Basic Monitoring



Voice and Video Performance
(Media Monitoring)

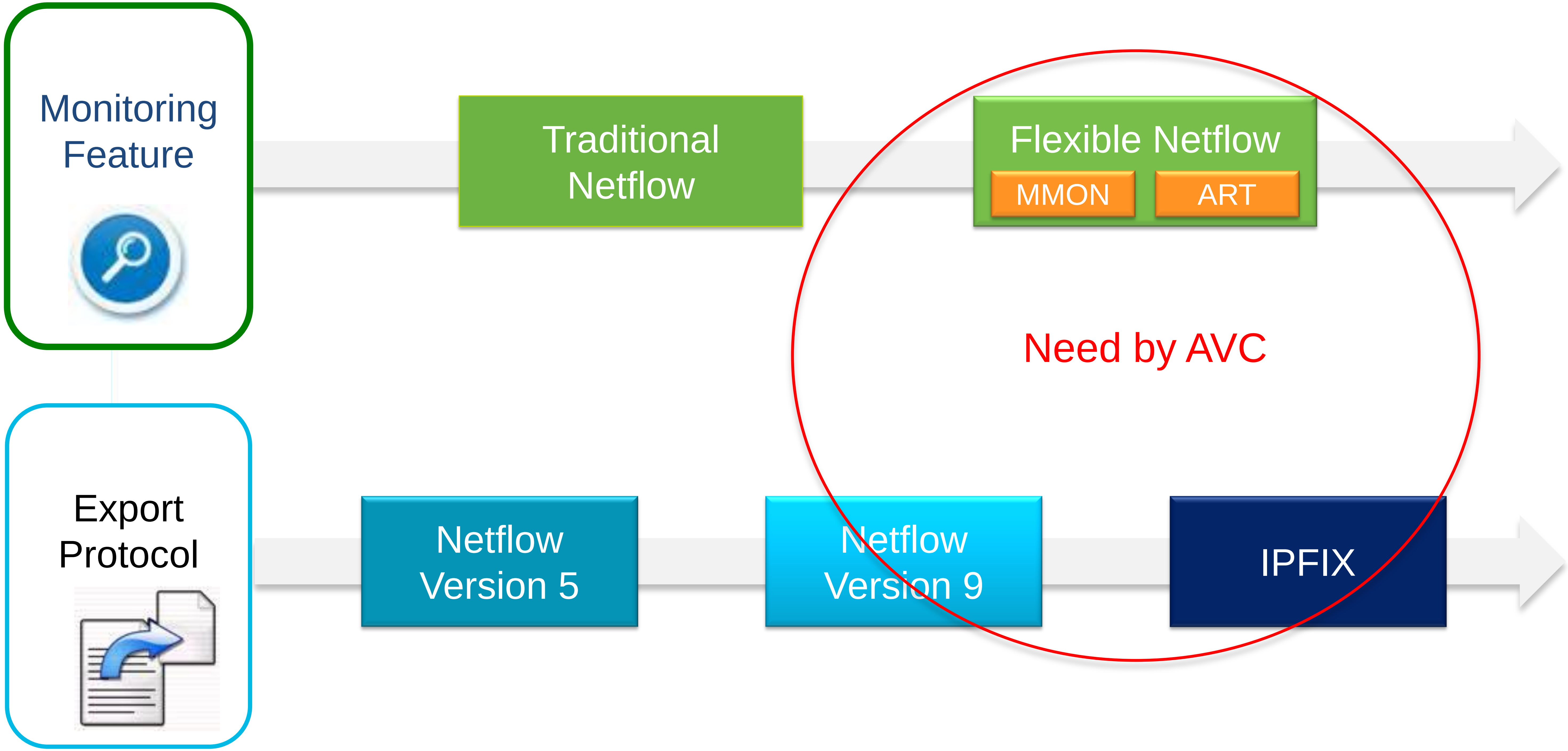
30% of traffic is voice and video

Critical Applications Performance
(Performance Agent)

40% of traffic is critical applications

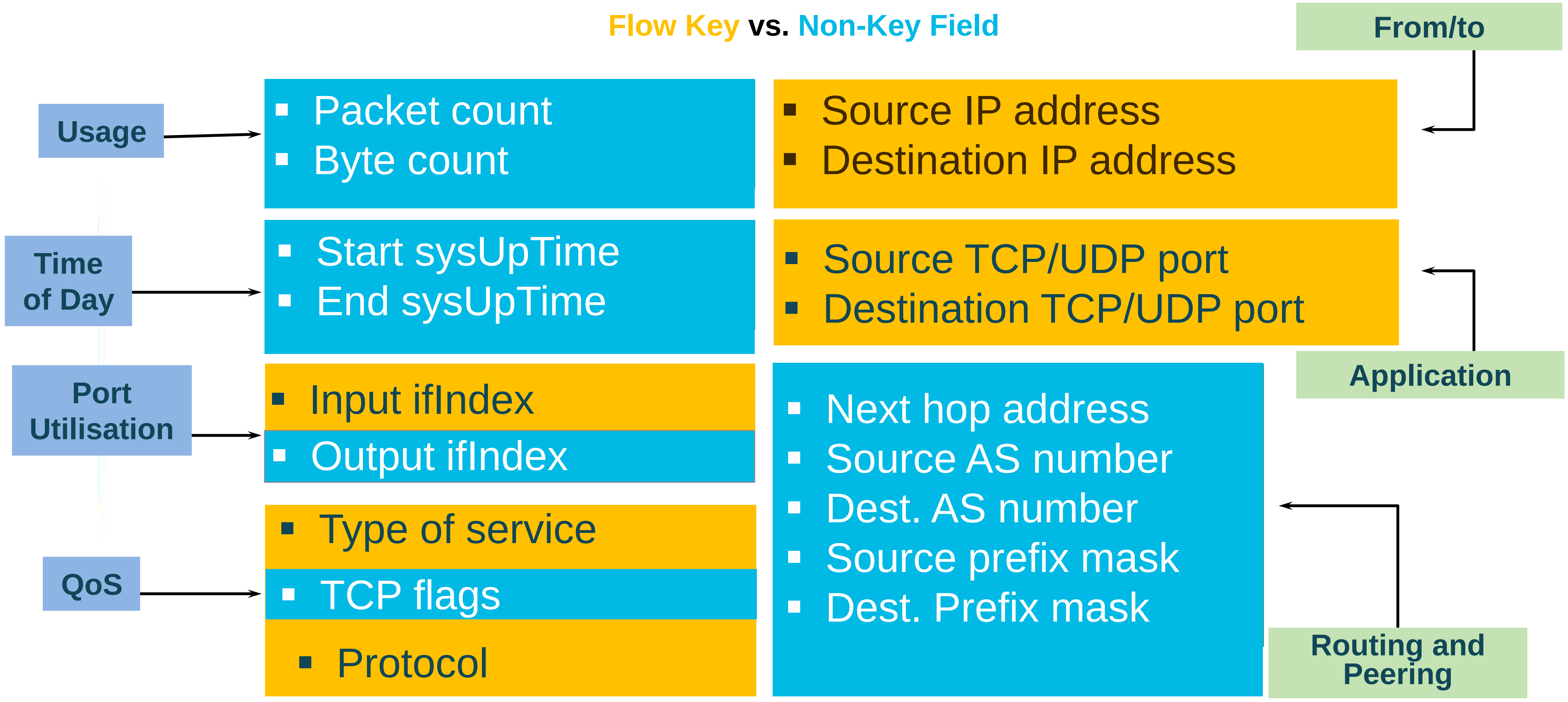
What applications, how much bandwidth, flow direction?
(Flexible Netflow and NBAR/NBAR2)

Performance Collection & Exporting Components



Traditional NetFlow

Version 5: Good Information, But Not Enough for Today Applications



Flow Key vs. Non-Key Field

Usage

- Packet count
- Byte count

Time of Day

- Start sysUpTime
- End sysUpTime

Port Utilisation

- Input ifIndex
- Output ifIndex

QoS

- Type of service
- TCP flags
- Protocol

From/to

- Source IP address
- Destination IP address

Application

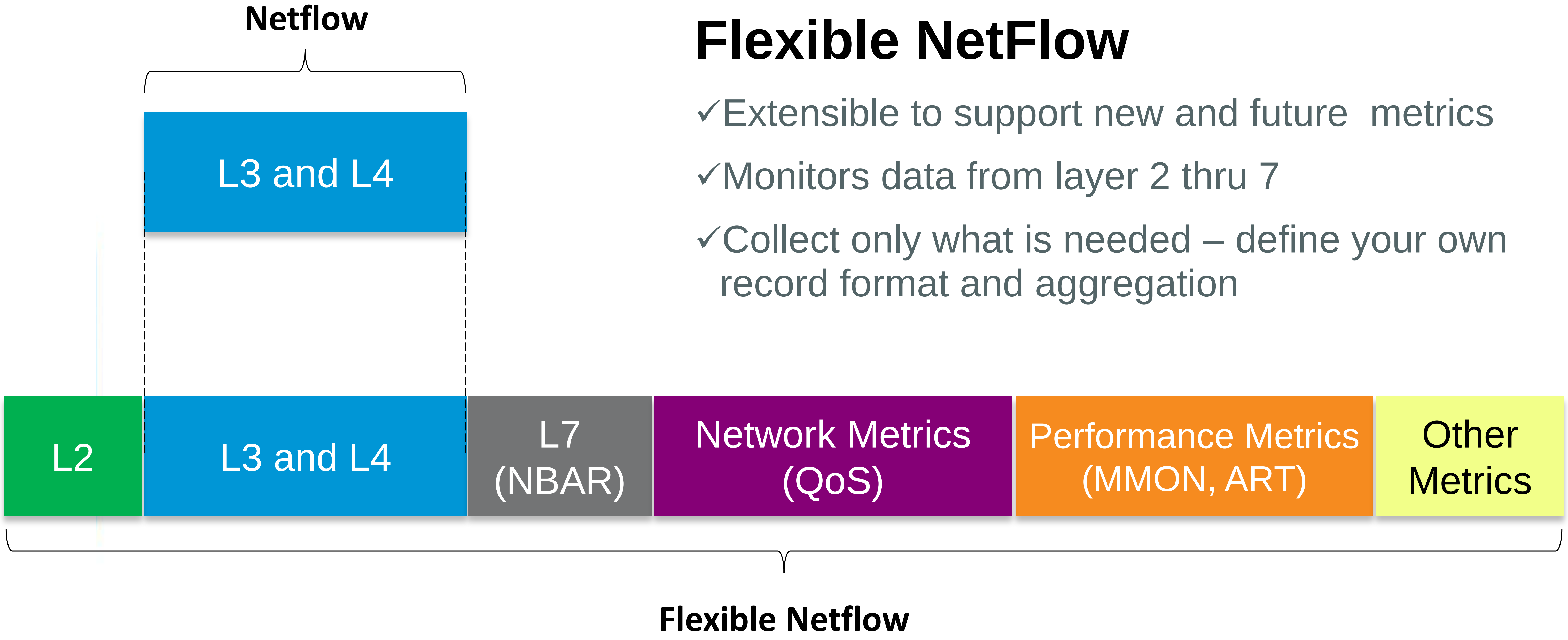
- Source TCP/UDP port
- Destination TCP/UDP port

Routing and Peering

- Next hop address
- Source AS number
- Dest. AS number
- Source prefix mask
- Dest. Prefix mask

- Collect layer 3 to 4 information. Static and not extensible

Gaining Full Visibility with Flexible Netflow



Flexible NetFlow

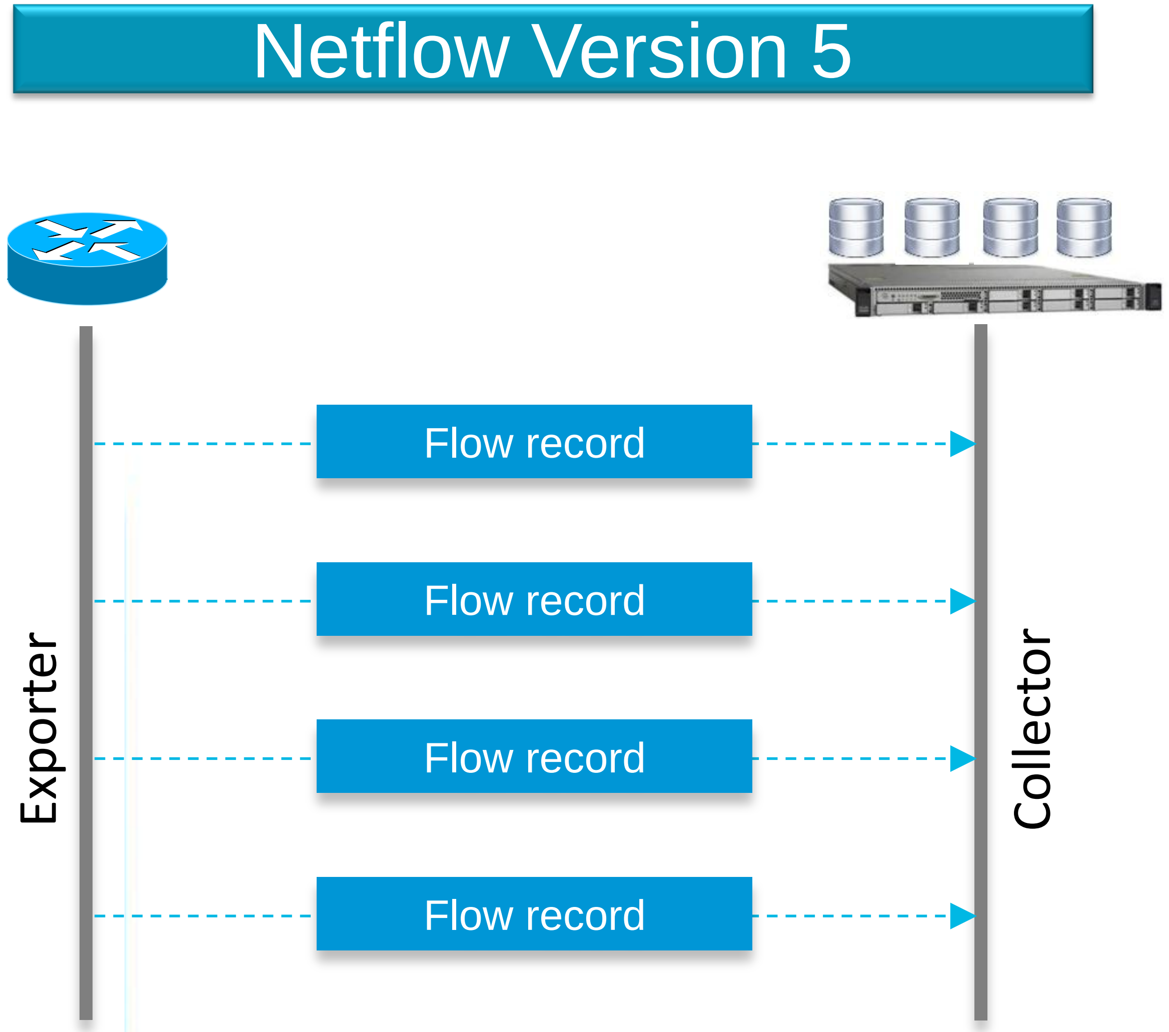
✓Extensible to support new and future metrics

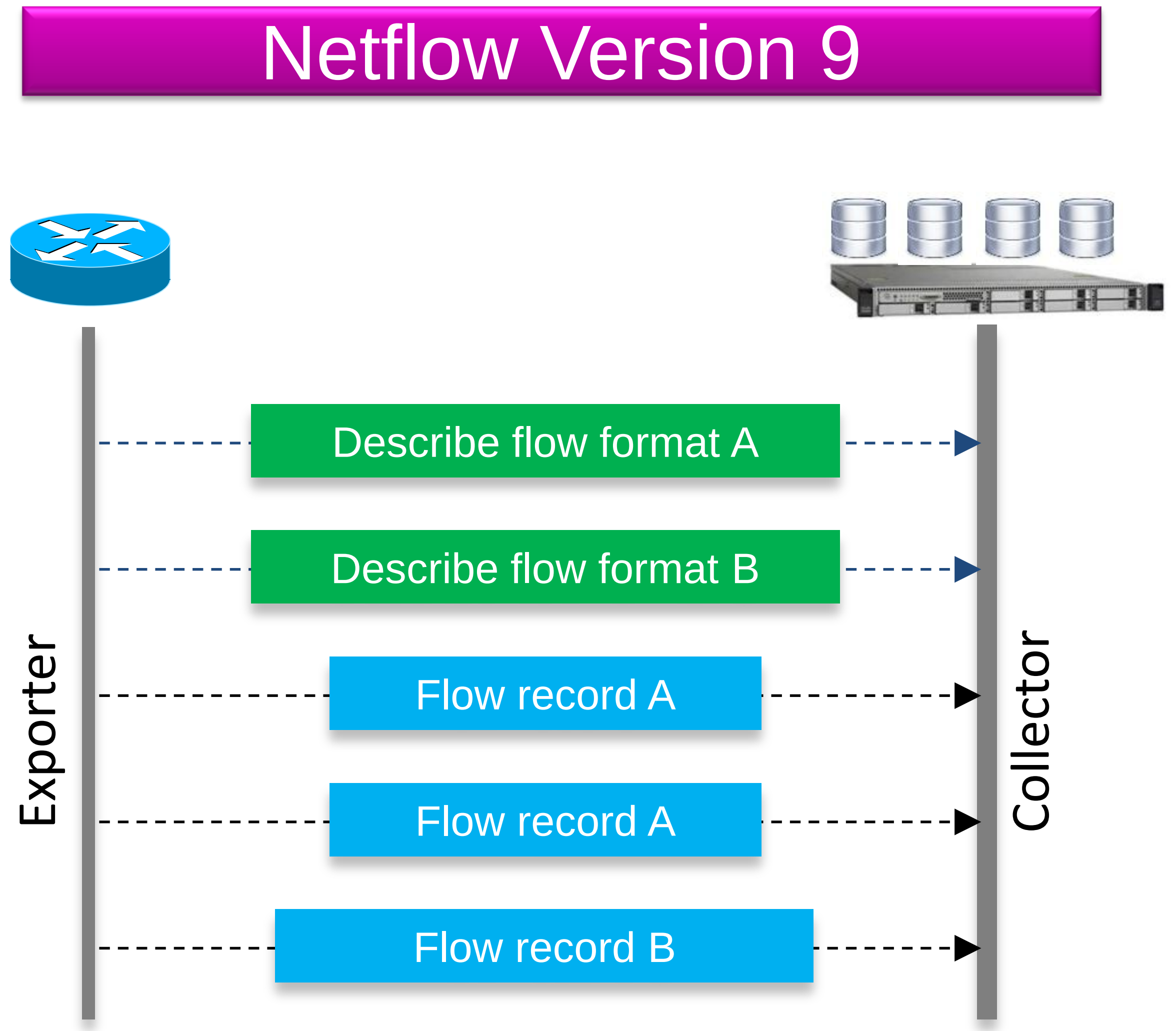
✓Monitors data from layer 2 thru 7

✓Collect only what is needed – define your own record format and aggregation

Netflow to FNF Migration Guide:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/ps6965/white_paper_c11-545581.html

Flexible & Extensible Flow Export Format with Netflow v9





- Fixed number of fields (18 fields)

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

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

Flexible Netflow Concept

Set of fields which identify unique entry to track

Define which information to collect

FNF Cache

Keyed Fields				Non-Keyed Fields			
Src IP	**Dst IP**	**App ID**	**…**	**Pkt**	**Byte**	**Input If**	**…**
1.1.1.1	2.2.2.2	0x10		10	2000	Fa0/0	
1.1.1.1	3.3.3.3	0x10		9	10000	Fa0/0	
2.2.2.2	1.1.1.1	0x10		15	15000	Fa0/1	
3.3.3.3	4.4.4.4	0x11		20	2000	Fa0/1	
1.1.1.1	2.2.2.2	0x20		10	500	Fa0/0	

Example: Tracking Traffic Flow with FNF

2 1

Key Fields	
Source IP	1.1.1.1
Destination IP	2.2.2.2
Destination port	80
Layer 3 Protocol	TCP - 6
TOS Byte	0
Non-key Fields	
Length	1250

- Create new entry in cache when key fields are unique
- Otherwise, update the non-key fields, i.e. packet count, byte count

2 1

Key Fields	
Source IP	3.3.3.3
Destination IP	4.4.4.4
Destination port	443
Layer 3 Protocol	TCP - 6
TOS Byte	0
Non-key Fields	
Length	519

Key fields

Non-key fields

FNF Cache After Packet 1

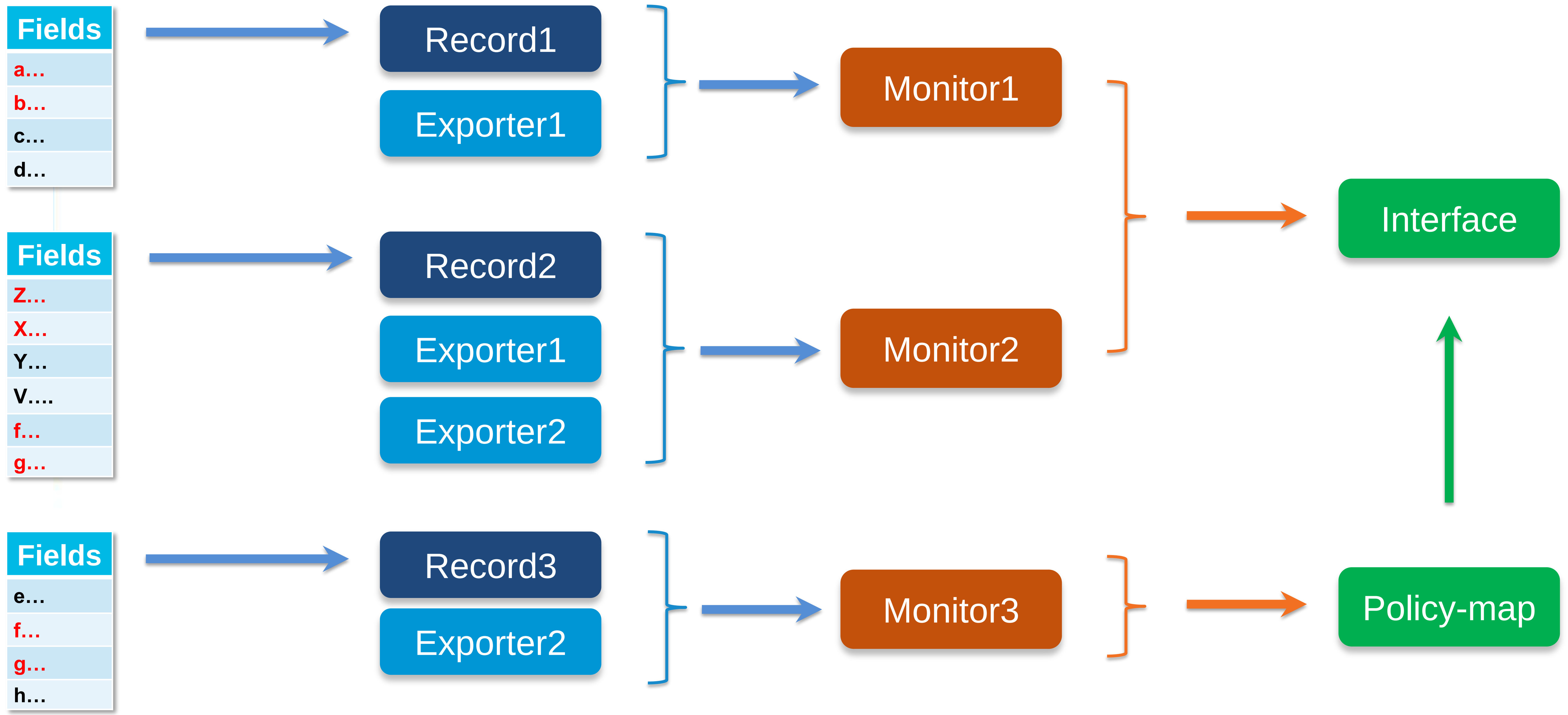
Source IP	Dest. IP	Dest Prt	Protocol	TOS	…	Bytes
1.1.1.1	2.2.2.2	80	6	0	…	11250

FNF Cache After Packet 2

Source IP	Dest. IP	Dest Prt	Protocol	TOS	…	Bytes
3.3.3.3	4.4.4.4	443	6	0	…	519
1.1.1.1	2.2.2.2	80	6	0	…	11250

Flexible NetFlow

Structure of Monitoring Components



Flexible Netflow Configuration on Interface

1 What metrics do I collect?

```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes
```

2 Where to export the flow record?

```
Router(config)# flow exporter my-exporter
Router(config-flow-exporter)# destination 1.1.1.1
```

3 What is my monitor context?

```
Router(config)# flow monitor my-monitor
Router(config-flow-monitor)# exporter my-exporter
Router(config-flow-monitor)# record my-record
```

4 Which interface to monitor?

```
Router(config)# interface s3/0
Router(config-if)# ip flow monitor my-monitor input
```

Flexible NetFlow Configuration on Policy-map

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

```
flow record RECORD-FNF
 match ipv4 source address
 match ipv4 destination address
 match application name
 match ipv4 dscp
!
flow monitor MONITOR-FNF
 record RECORD-FNF
!
policy-map MYPOLICY
 class Critical
  flow monitor MONITOR-FNF
!
interface eth0/0
 service-policy out MYPOLICY
!
```

```
show flow mon <fnf_mon> cache

 IPV4 SRC   IPV4 DST    APP NAME       DSCP
 ========   ========    ========       ====
 10.0.1.1   10.0.1.2    nbar  sqlnet   0x12
 10.0.1.1   10.0.1.2    nbar  citrix   0x12
 10.0.1.1   10.0.1.2    nbar  FTP      0xA
```

- Allow filter traffic to monitor – not possible if attach to interface directly
- Utilise QoS policy to filter traffic
- In ASR1K, support by policy-map type performance-monitor

FNF Option Template Provides Dynamic Information Update

- Available only with Flexible Netflow
- Device updates collector with information, e.g.
  - NBAR2 Application Name
  - Interface List
  - QoS policy name

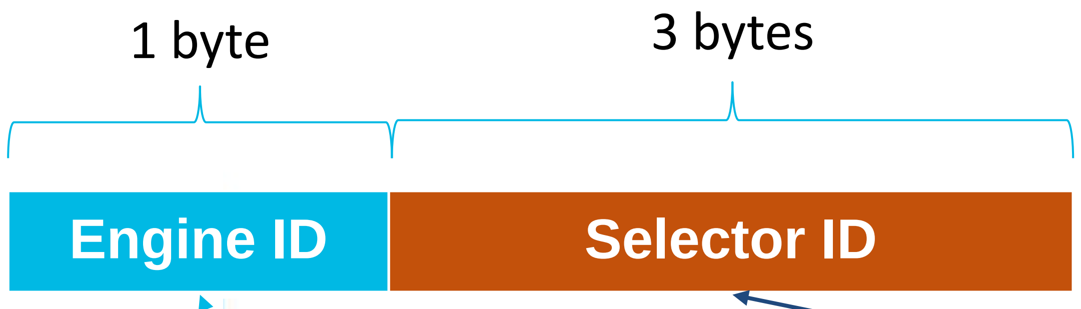
```
flow exporter my-collector
 destination 10.35.89.59
 source GigabitEthernet0/0/1
 transport udp 2055
 option interface-table timeout 3600
 option sampler-table timeout 3600
 option application-table timeout 3600

router#show flow exporter my-collector templates
Flow Exporter my-collector:
  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  |
  ---------------------------------------------------
```

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
interface-table	Interface SNMP ifIndex to name mapping
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

Flexible Netflow Application ID Format

Application ID is populated by NBAR2 (4 bytes)



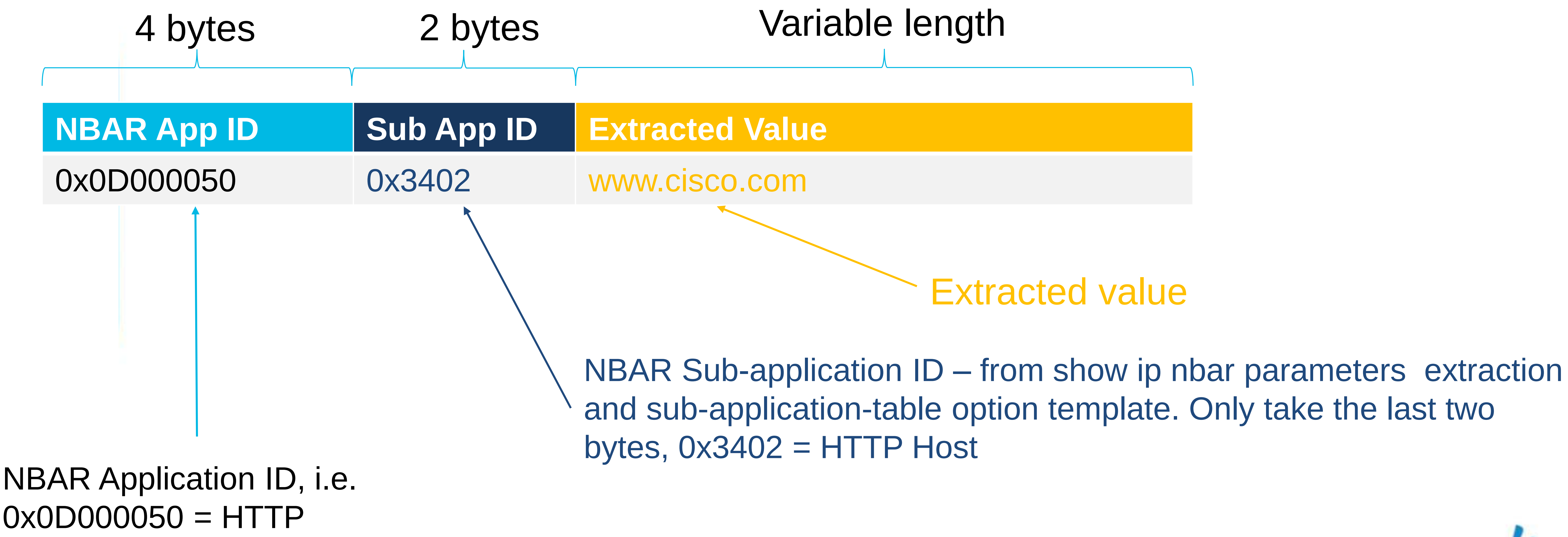
```
router#show flow exporter option application table

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

(..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)
```

Flexible Netflow Sub-application ID Format

Sub-application ID is populated by NBAR2 (variable length)

```
collect application http host
```



4 bytes	2 bytes	Variable length
NBAR App ID	Sub App ID	Extracted Value
0x0D000050	0x3402	www.cisco.com

Extracted value

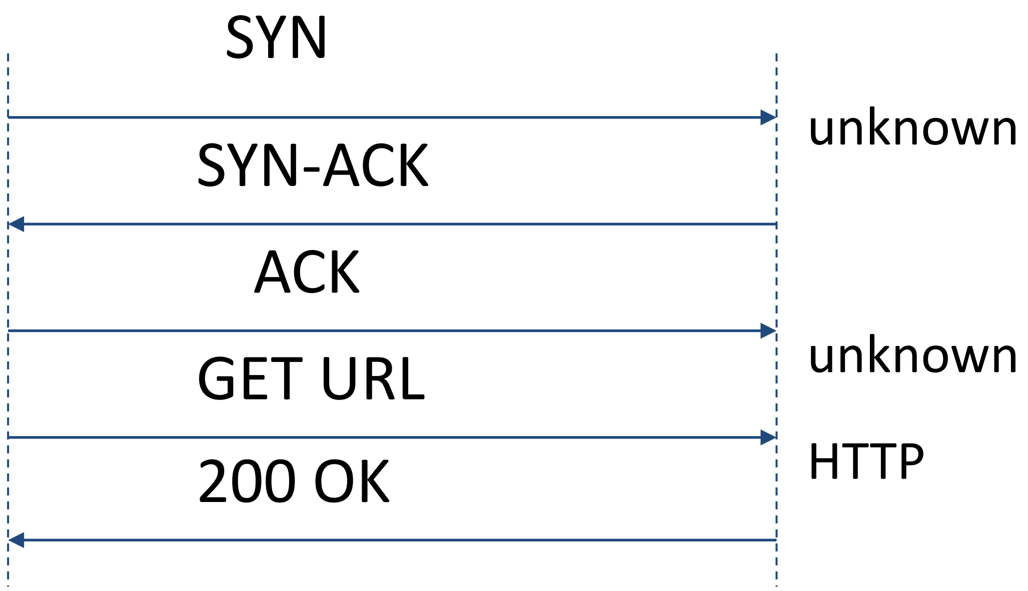
NBAR Sub-application ID – from show ip nbar parameters extraction and sub-application-table option template. Only take the last two bytes, 0x3402 = HTTP Host

NBAR Application ID, i.e.
0x0D000050 = HTTP

ISR G2: Future
ASR1K: 3.4S

FNF Accurate Accounting

```
router(config)# flow record <app_record>
router(config-flow-record)# match application name [account-on-resolution]
```



SYN

unknown

SYN-ACK

ACK

unknown

GET URL

HTTP

200 OK

- Cache the counters/timers in the flow table until the flow classified, as NBAR2 might take multiple packets for the classification
- Until application is classified – “application name” is set to “unknown”
- When the flow is classified, it starts accounting in the FNF cache and add the counters cached in the flow table

Interface	App.ID	Packets
Eth0	Unknown	2
Eth0	HTTP	1

Interface	App.ID	Packets
Eth0	HTTP	3

ISR G2: Future
ASR1K: 3.4S

FNF Connection Based Sampling

```
router(config)# sampler <sampler-name>
router(config-sampler)# mode {deterministic|random} 1 out-of <value M>
router(config-sampler)# granularity {packet (default) | connection}
```

- Goal: reduce the number of exported flow per monitor

  Example: NBAR on the Internet interface => will still get the most popular web sites

- Granularity configuration option allows accounting 1 out of N flows for a specific monitor
- For each monitor instance, all packets belonging to the same sampled flow will be recorded by FNF

FNF End of Flow Transaction

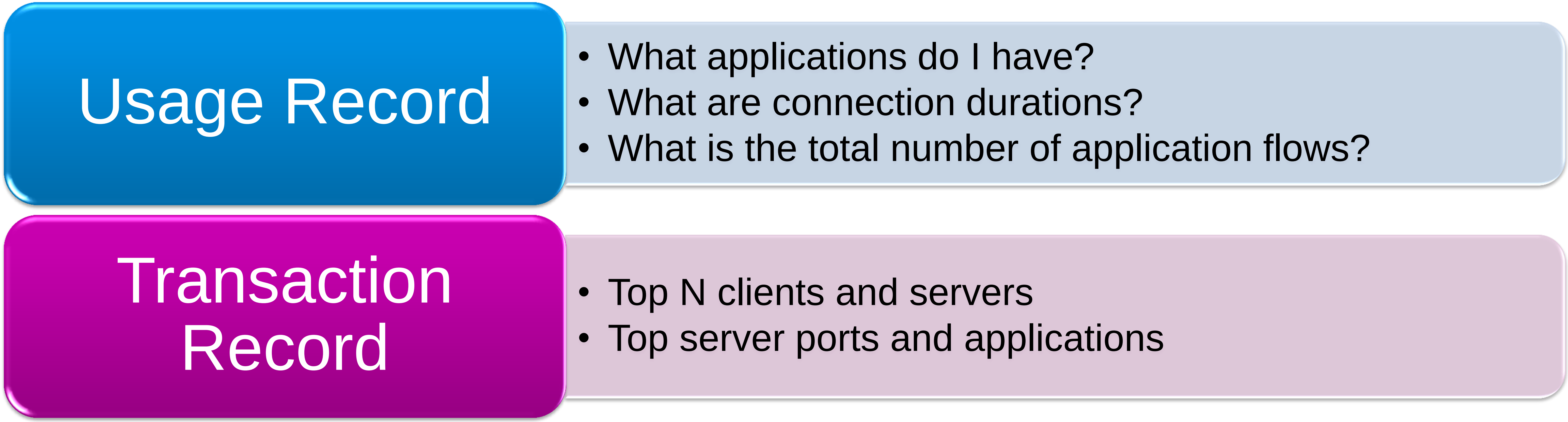
ISR G2: Future
ASR1K: 3.4S

```
router(config)# flow monitor <monitor-name>
router(config-flow-monitor)# cache timeout event transaction-end
```

- Usually FNF record expiration is based on timeouts
- A transaction based export is added:
  - To send the record close to the time the transaction/flow ended
  - To detect true flow termination (no based on a pause in the connection)
  - The timeout could be different per application
  - Ability to reduce the collector load by sending only one record on flow end

Sample AVC Monitoring

Discovery Application Bandwidth Usage and Top Talkers



Usage Record

- What applications do I have?
- What are connection durations?
- What is the total number of application flows?

Transaction Record

- Top N clients and servers
- Top server ports and applications

- User guide http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/xe-3s/cfg-avc-xe.html

Configure NBAR2 and FNF for ASR1K AVC

For Your Reference

Usage Records

```
flow record input-usage-record
 match interface input
 match flow direction
 match application name account-on-resolution
 collect interface output
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection new-connections
 collect connection sum-duration
flow record output-usage-record
 match interface output
 match flow direction
 match application name account-on-resolution
 collect interface input
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect connection new-connections
 collect connection sum-duration
```

Report connection count and total duration

Transaction Records

```
flow record tr-record
 match connection transaction-id
 collect ipv4 version
 collect ipv4 protocol
 collect ipv4 source address
 collect ipv4 destination address
 collect transport source-port
 collect transport destination-port
 collect interface input
 collect interface output
 collect flow direction
 collect flow sampler
 collect counter bytes long
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
 collect flow end-reason
 collect connection initiator
```

Tracking unique transaction

Correlate bi-direction flows belong to the same session

AVC Performance on ASR1K

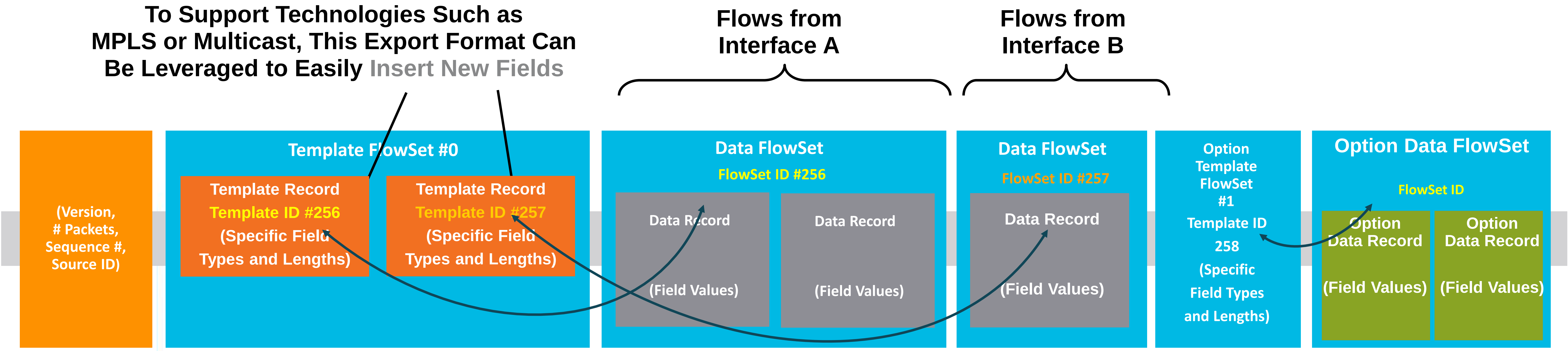
ASR1000 ESP data plane forwarding module	Max BW [Gbps]	Max PPS [MPPS]	Max IP Flows [M]	Max CPS [KF/S]	Typical L7 BW [Gbps]
ESP5	5	TBD	0.75	TBD	2.5
ESP10	10	3.5	1.65	150	5
ESP20	20	5	3.5	200	10
ESP40	20	5	3.5	200	10

- Typical ISP Traffic used
- NBAR2: no CPU impact on the RP but only an impact on ESP CPU
- Transaction Record is sampled 1 out-of 1000 connections

Flexible Netflow Terminology

For Your Reference

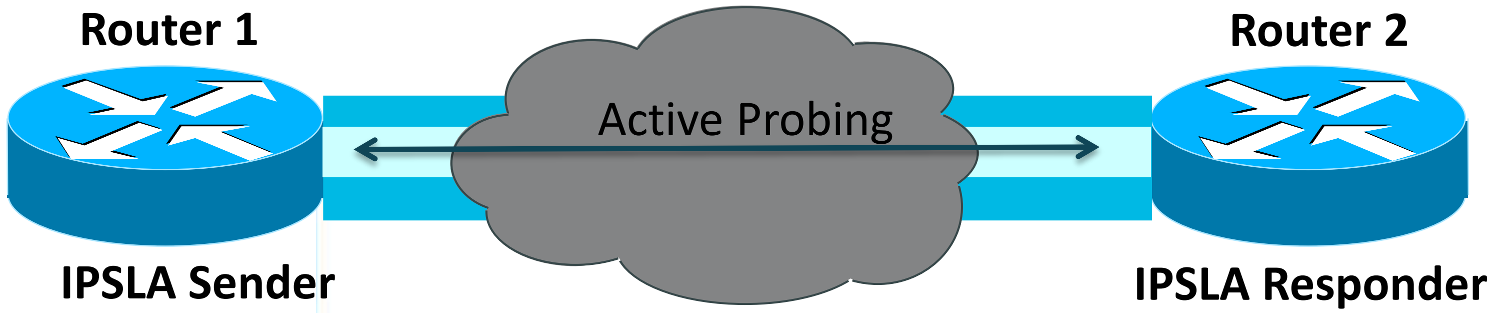
Templates and FlowSets



- Template Records: Building blocks
  - Template Record Type: Defines the structure & interpretation of fields in a Flow Data Record
  - Options Template Record Type: Defines the structure and interpretation of fields in an Options Data Record
- Data Records:
  - provides information about an IP flow or an event that exists on the device
  - Matching ID numbers are the way to associate template to the data records
- FlowSets:
  - Template FlowSet and Data FlowSet
  - Aggregation of different templates and data

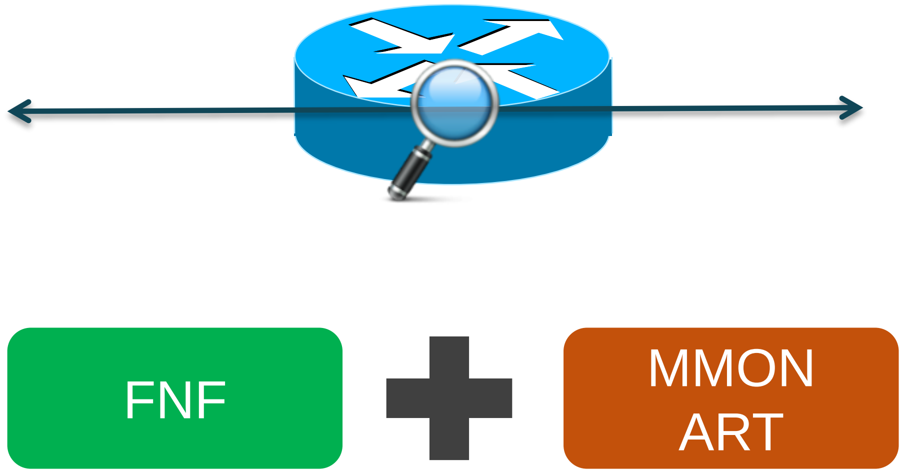
Active or Passive Monitoring

Active Monitoring



- Generate synthetic traffic into the network
- Require IOS responder for advanced monitoring types

Passive Monitoring



- Inspect traffic to measure performance metrics
- Performance metrics available only when there is traffic

When Users Complain About Application

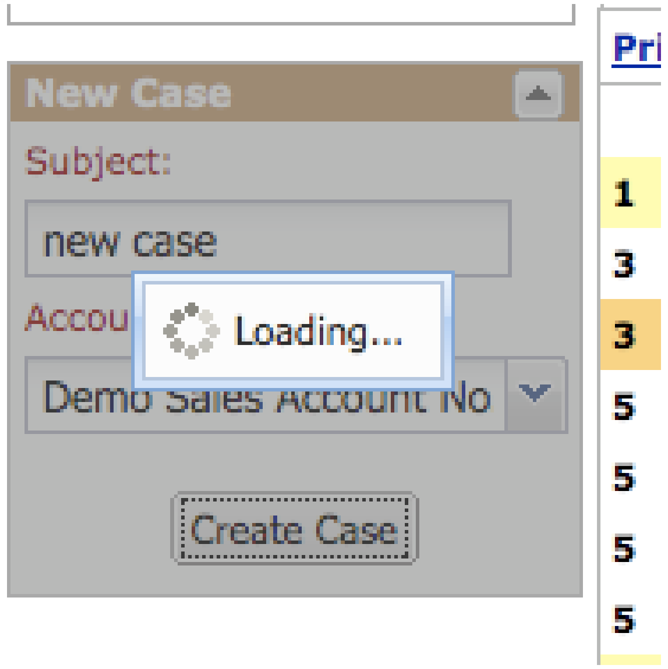
What the users see

What network admins see

What can happen

Your network is so slow I cannot get any work done today

End Users



New Case

Subject:

new case

Accou

Loading...

Demo Sales Account No

Create Case

Pri

1
3
3
5
5
5
5

I do not see anything wrong

ping – OK
show ip route - OK
traceroute - OK
show interface - OK

Network Admin

Increased Latency

WAN Problem

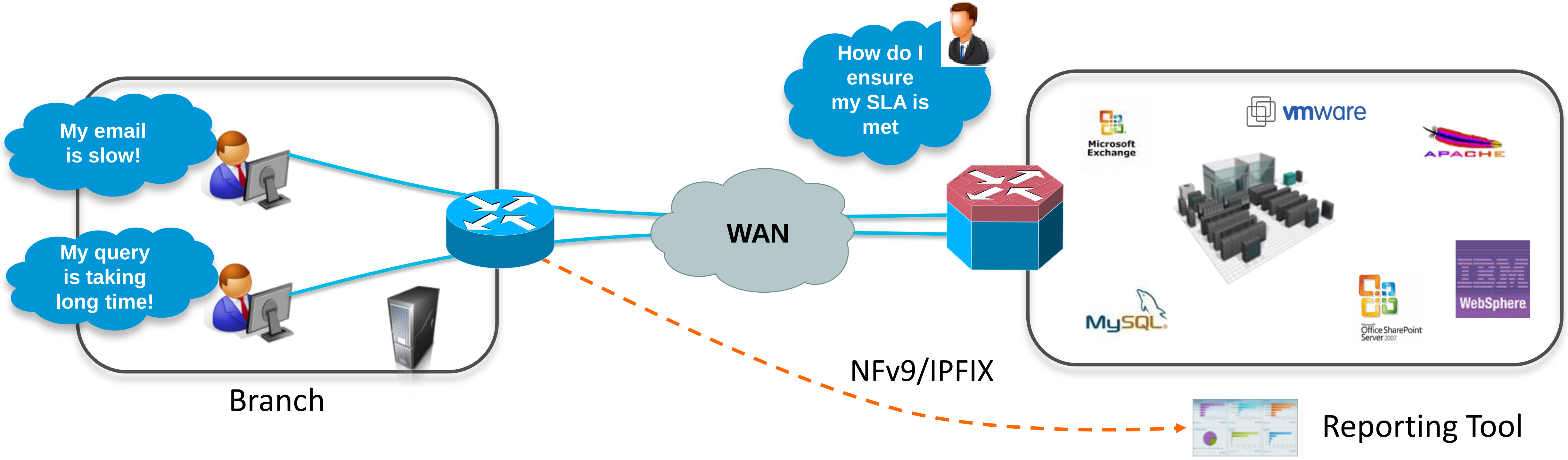
Application Problem

Server Problem

User Problem

Application Response Time (ART) Measurement

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



Key Features

27 Application Response Time (ART) Metrics

Interact with NBAR2 for Application ID and field extraction information

In ISR G2, provide by Performance Agent (PA)

In ASR1K, ART is part of unified monitoring

Benefits

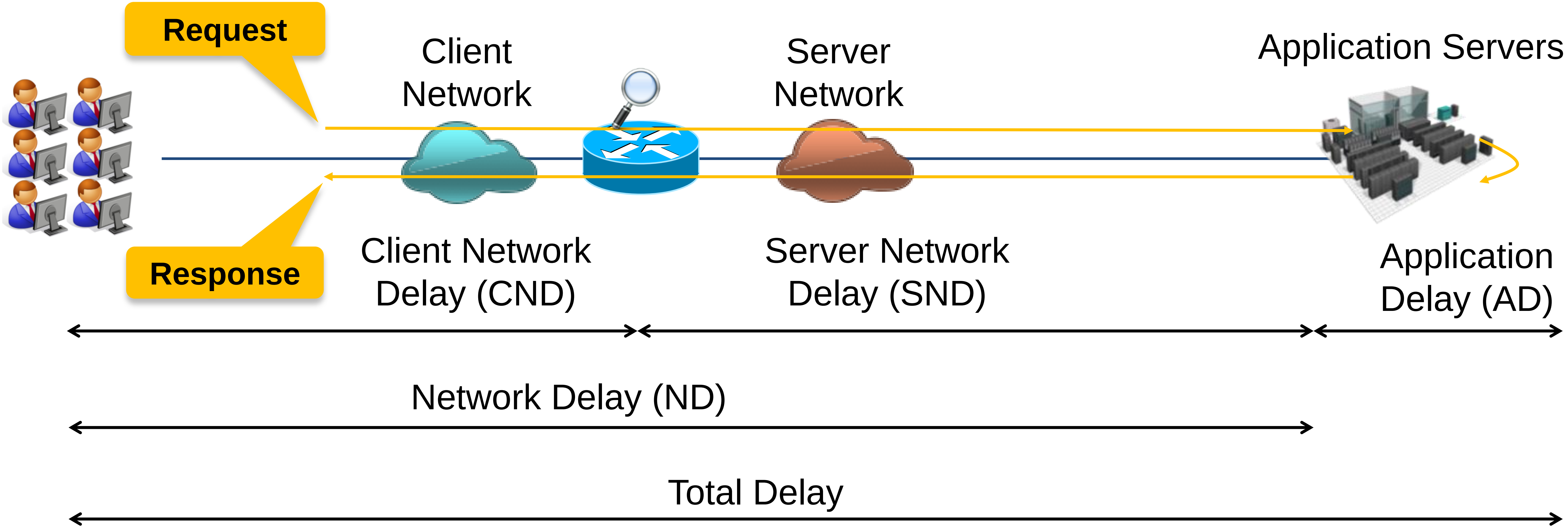
Visibility into application usage and performance

Quantify user experience

Troubleshoot application performance

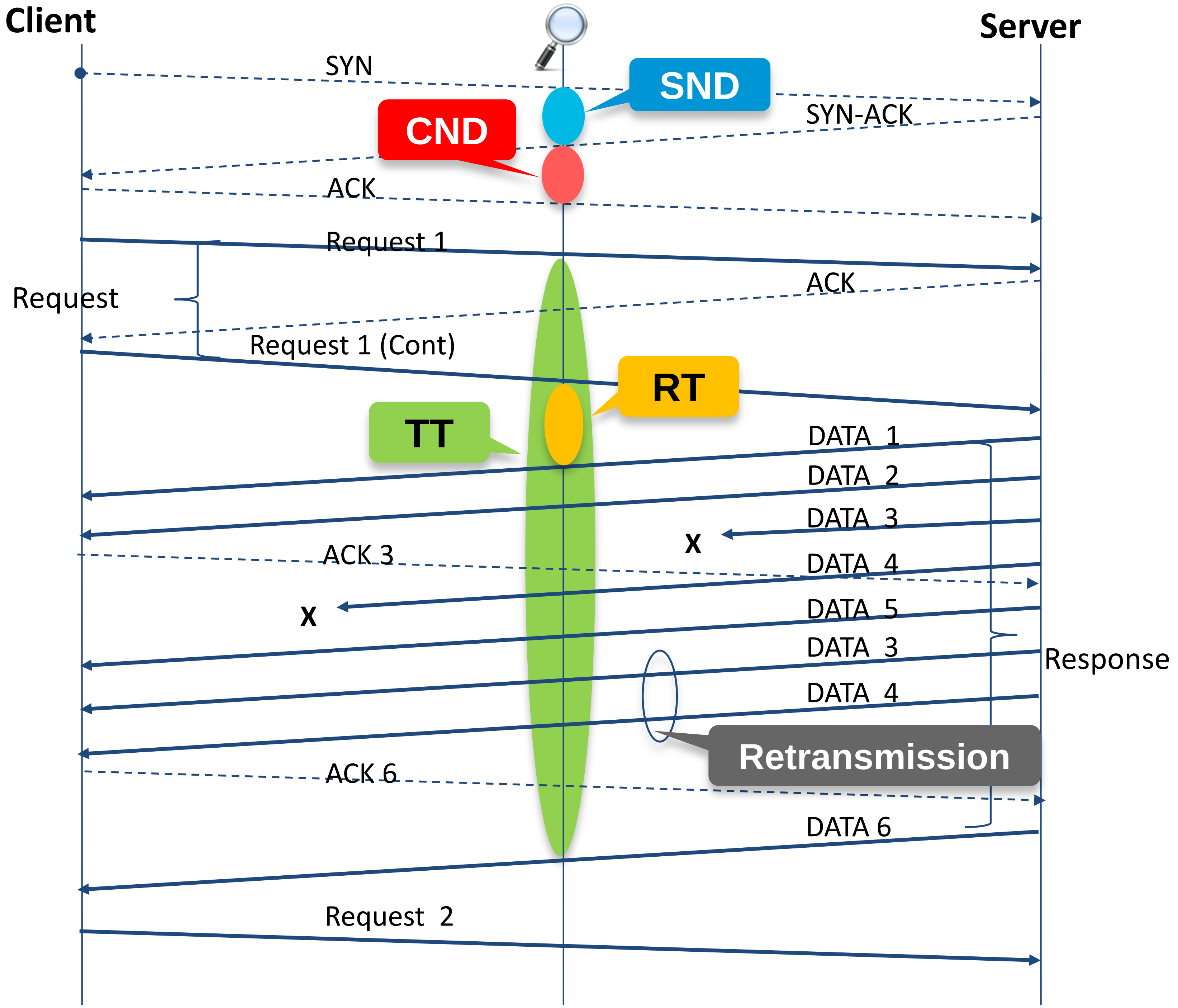
Track service levels for application delivery

Application Delivery Path Network Segment Breakdown



- Separate application delivery path into client and server segments
- Server Network Delay (SND) approximates WAN Delay
- Latency per application

Understand ART Metrics Calculation



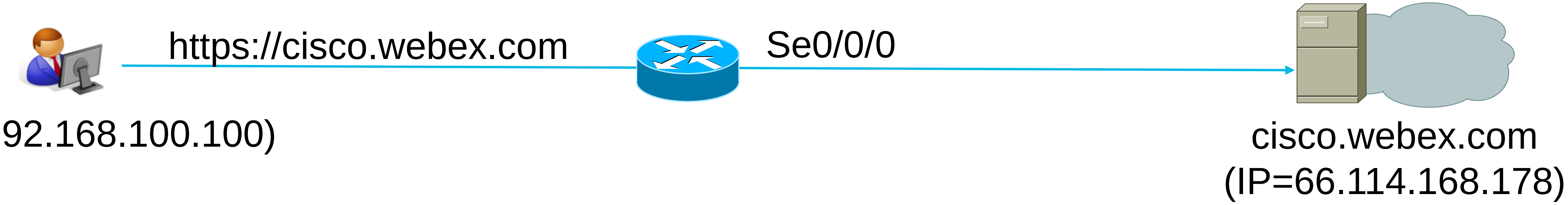
- Response Time (RT)
  - t(First response pkt) – t(Last request pkt)
- Transaction Time (TT)
  - t(Last response pkt) – t(First request pkt)
- Network Delay (ND)
  - ND = CND + SND
- Application Delay (AD)
  - AD = RT – SND

Quantify User Experience

Quantify User Experience

Identify Server Performance Issue

ART & NBAR/NBAR2 Interaction



- ‘collect application name’ exports application ID field to reporting tool

Flow Record

Without NBAR

Src IP	Dst IP	Dst Port	App ID	Resp Time	…
192.168.100.100	66.114.168.178	443	0	100	

With NBAR

Src IP	Dst IP	Dst Port	App ID	Resp Time	…
192.168.100.100	66.114.168.178	443	0x0D00019E	100	

Indicate this is webex application

List of Metrics Supported by IOS PA on ISR G2

For Your Reference

Traditional FNF Metrics

- Application ID (from NBAR2)
- Client/Server Bytes
- Client/Server Packets
- Source MAC Address
- Input/Output Interface
- IP DSCP

WAAS Express Metrics

- Input/Output Bytes
- WAAS Connection Mode
  - TFO, TFO/LZ, TFO/DRE, TFO/LZ/DRE
- Input/Output DRE Bytes
- Input/Output LZ Bytes

ART Metrics

- CND - Client Network Delay (min/max/sum)
- SND – Server Network Delay (min/max/sum)
- ND – Network Delay (min/max/sum)
- AD – Application Delay (min/max/sum)
- Total Response Time (min/max/sum)
- Total Transaction Time (min/max/sum)
- Number of New Connections
- Number of Late Responses
- Number of Responses by Response Time
  - (7-bucket histogram)
- Number of Retransmissions
- Number of Transactions
- Client/Server Bytes
- Client/Server Packets

List of ART Metrics Supported on ASR1K

For Your Reference

ART Metrics

- CND - Client Network Delay (min/max/sum)
- SND – Server Network Delay (min/max/sum)
- ND – Network Delay (min/max/sum)
- AD – Application Delay (min/max/sum)
- Total Response Time (min/max/sum)
- Total Transaction Time (min/max/sum)
- Number of New Connections
- Number of Late Responses
- Number of Responses by Response Time
  - (7-bucket histogram)
- Number of Retransmissions
- Number of Transactions
- Client/Server Bytes
- Client/Server Packets

ART Configuration Differences – ISR G2 and ASR1K

For Your Reference

Key Differences	ISR G2	ASR1K
Flow record type	Type mace	Type performance-monitor
Monitoring policy	Type mace with mandatory name mace_global	Type performance-monitor
Number of policies supported	One	Multiple
Attachment to interface	Mace enable	Service-policy type performance-monitor applied to both in and out direction
Key fields	Pre-defined, static 4-tuple (source/destination IP, destination port, protocol type)	Flexible as defined by users

ART Configuration Steps

	1 What metric to collect	2 Where to export info	3 Create monitoring context	4 Filter what to monitor	5 Attach the monitor to policy	6 Attach policy to interface
ISR G2	Create flow record type mace	Define flow exporter	Create flow monitor type mace	Create class-map and policy-map type mace	Attach flow monitor type mace to policy	Configure mace enable on interface
ASR1K	Create flow record type performance-monitor	Define flow exporter	Create flow monitor type performance-monitor	Create class-map and policy-map type performance-monitor	Attach flow monitor type performance-monitor to policy	Attach service-policy type performance-monitor to interface in both directions

Application Usage and Performance

IOS PA Example

For Your Reference

Export With option templates

```
flow exporter PA-EXPORTER
 destination 10.151.1.131
 source loopback0
 transport udp 9991
 option interface-table timeout 300
 option application-table timeout 300
```

Record for PA

```
flow record type mace PA-RECORD
 collect ipv4 dscp
 collect interface input
 collect interface output
 collect application name
 collect counter client bytes
 collect counter server bytes
 collect counter client packets
 collect counter server packets
 collect art all
 ! URI collection needs ipfix export
 <collect application http uri statistics>
 <collect application http host>
 collect policy qos classification hierarchy
 collect policy qos queue drops
```

Flow monitor

```
flow monitor type mace PA-MONITOR
 record PA-RECORD
 exporter PA-EXPORTER
```

Define the traffic to monitor

```
ip access-list extended all-traffic-acl
 permit ip any any
!
class-map match-any all-traffic
 match access-group name all-traffic-acl
!
```

```
policy-map type mace mace_global
 class all-traffic
  flow monitor PA-MONITOR
```

Apply on the interface

```
interface Serial0/0/0
 ip nbar protocol-discovery
 mace enable
```

For Your Reference

Application Performance

ASR1K Example

Export With option templates

```
flow exporter ART-EXPORTER
 destination 10.151.1.131
 source loopback0
 transport udp 9991
 export-protocol ipfix
 option interface-table timeout 300
 option application-table timeout 300
```

ART Record

```
flow record type performance-monitor ART-RECORD
 match routing vrf input
 match ipv4 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 ipv4 dscp
 collect interface input
 collect interface output
 collect flow sampler
 collect connection initiator
 collect connection new-connections
 collect connection sum-duration
 collect connection delay response to-server sum
 collect connection server counter responses
```

```
 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
 collect connection client counter packets retransmitted
 collect connection delay network client-to-server sum
 collect connection delay application sum
 collect connection delay response client-to-server sum
 collect connection transaction duration sum
 collect connection transaction counter complete
 collect connection server counter bytes long
 collect connection server counter packets long
 collect connection client counter bytes long
 collect connection client counter packets long
```

Flow monitor

```
flow monitor type mace ART-MONITOR
 record ART-RECORD
 exporter ART-EXPORTER
 cache entries 35000
 cache timeout synchronized 60
```

For Your Reference

Application Performance (Cont.)

ASR1K Example

Define the traffic to monitor

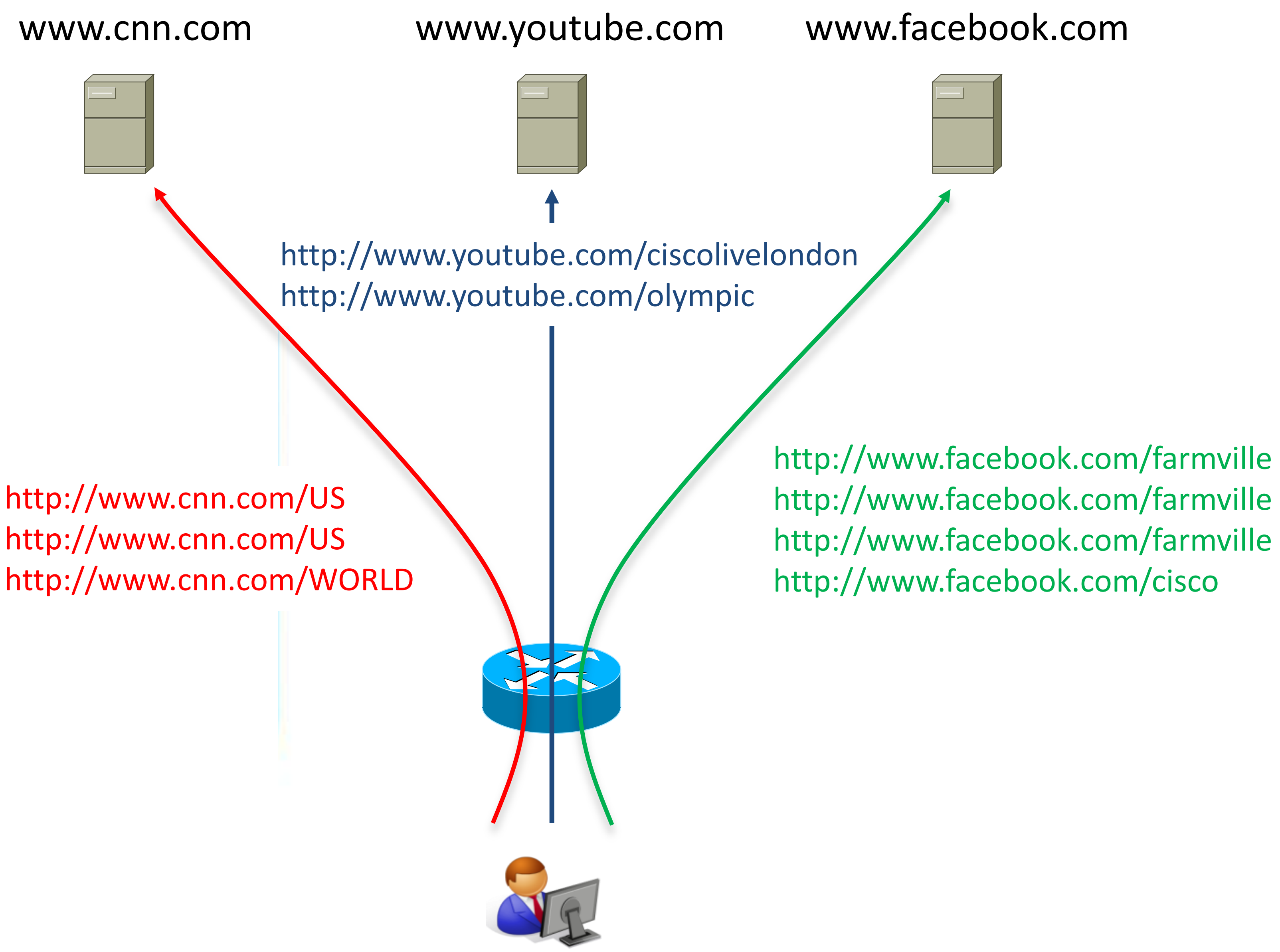
```
ip access-list extended tcp-traffic-acl
 permit tcp any any
!
class-map match-any tcp-traffic
 match access-group name tcp-traffic-acl
!
```

```
policy-map type performance-monitor ART-POLICY
 class tcp-traffic
  flow monitor ART-MONITOR
```

Apply on the interface

```
interface Serial0/0/0
 service-policy type performance-monitor input ART-POLICY
 service-policy type performance-monitor output ART-POLICY
```

Top Domain and URL Hit Count Report


www.cnn.com
www.youtube.com
www.facebook.com
http://www.youtube.com/ciscolivelondon
http://www.youtube.com/olympic
http://www.cnn.com/US
http://www.cnn.com/US
http://www.cnn.com/WORLD
http://www.facebook.com/farmville
http://www.facebook.com/farmville
http://www.facebook.com/farmville
http://www.facebook.com/cisco

- Provide web browsing activity report
  - Most visited web site
  - Most visited URL per site

Field Name	Field ID	Value
application http host	45003	www.cnn.com
application http uri statistics	42125	US\02WORLD\01
art count new connections	9282	3

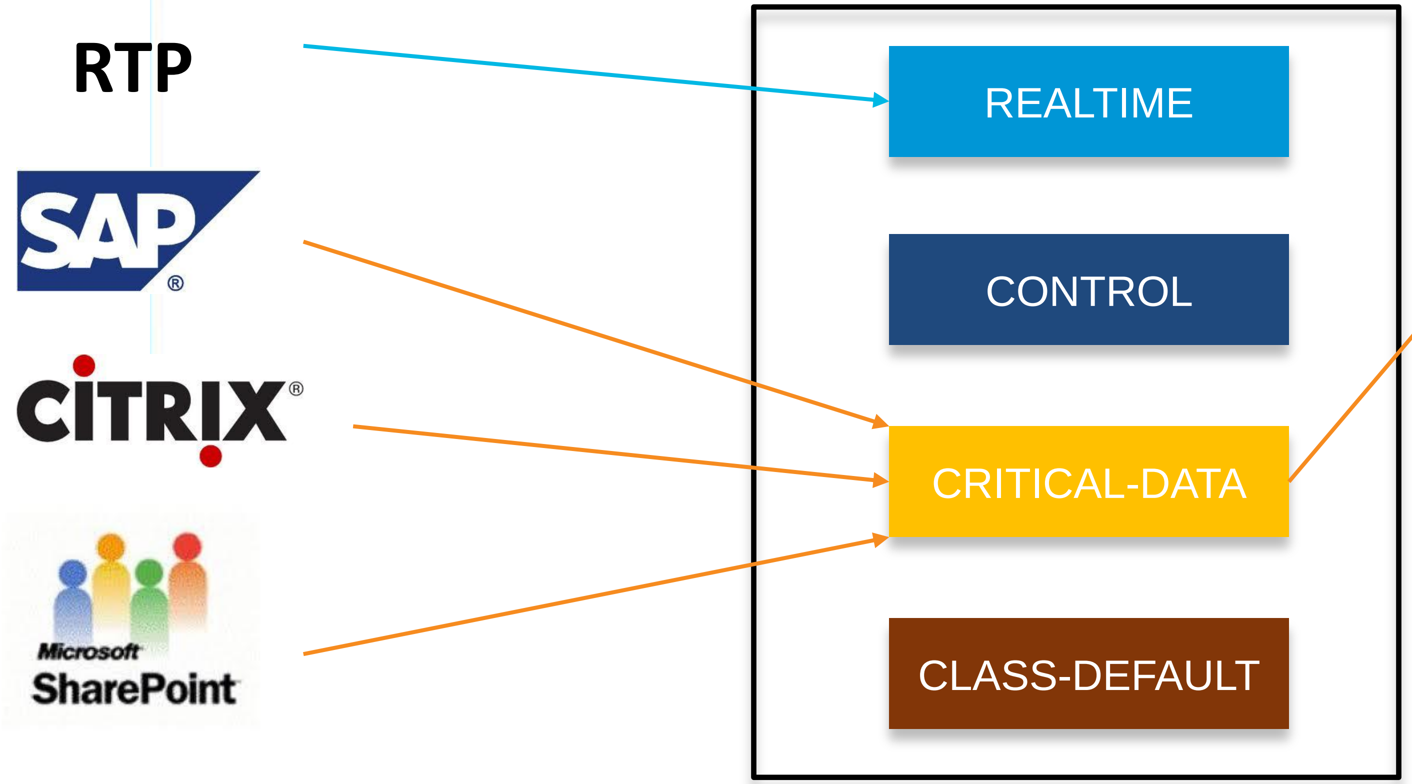
QoS Class-ID, Queue Drops and Queue Hierarchy

IOS-XE 3.9
15.2(4)M2 phase 1
15.3(1)T phase 2

Export with FNF

- Accurately report application class of service
  - Which QoS class my WebEx application falls into
- Correlate application performance problem with network congestion
  - How many queue drops do I have for my SAP application

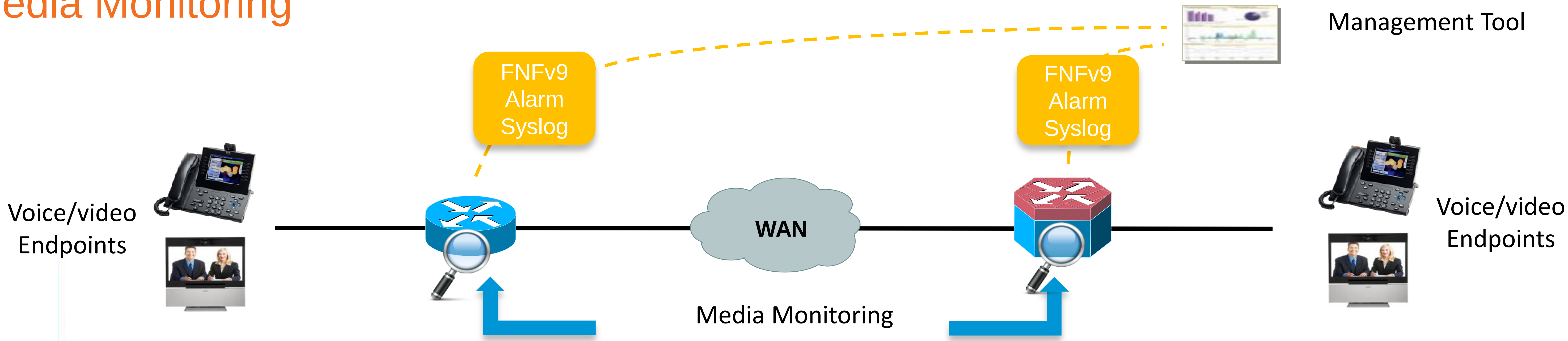
```
Policy-map QoS_Policy
 class REALTIME
  priority percent 33
 class CONTROL
  bandwidth percent 7
 class CRITICAL-DATA
  bandwidth percent 35
```



Field Name	Field ID	Value
policy qos classification hierarchy	41000	QoS_Policy|CRITICAL-DATA
application id	96	SAP
policy qos queue index	42128	3

Monitor Voice and Video Performance

Media Monitoring



Key Features

Monitor media performance metrics, i.e. jitter, loss

Integrate with NBAR2 to identify applications

Setting threshold and generating alert/alarm

Standard FNFv9 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

Medianet Performance Monitoring Metrics

Default RTP

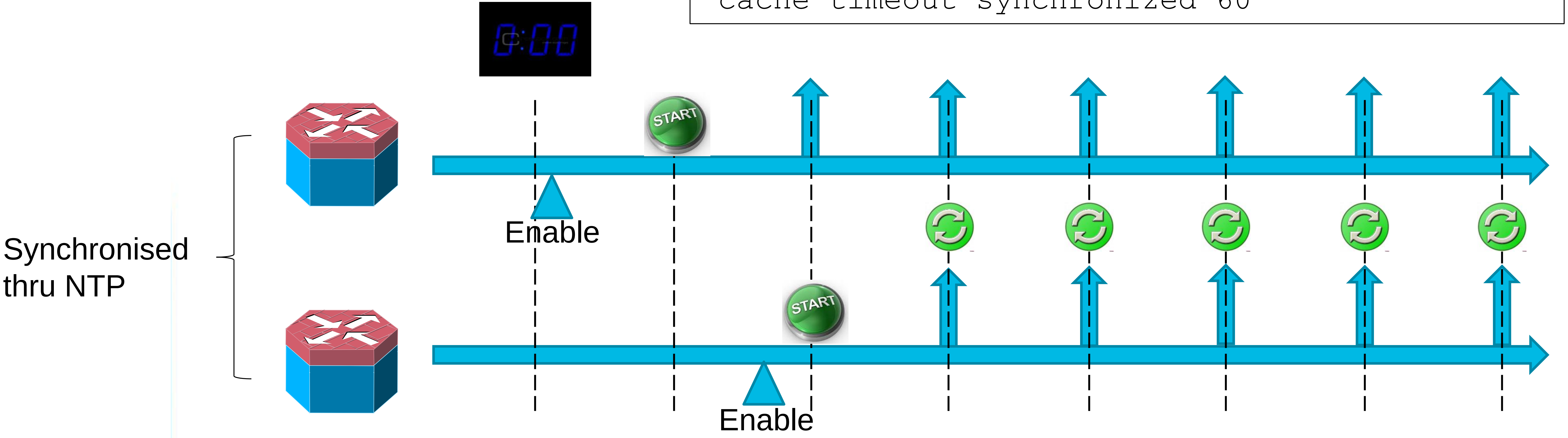
```
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport rtp ssrc
collect routing forwarding-status
collect ipv4 dscp
collect ipv4 ttl
collect transport packets expected counter
collect transport packets 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 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
```

Default TCP

```
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect routing forwarding-status
collect ipv4 dscp
collect ipv4 ttl
collect transport round-trip-time
collect transport event packet-loss counter
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect counter bytes rate
collect timestamp interval
collect application media bytes counter
collect application media packets rate
collect application media event
collect monitor event
collect transport round-trip-time min
collect transport round-trip-time max
collect transport round-trip-time sum
collect transport round-trip-time samples
```

Synchronised Cache Type

```
flow monitor type performance-monitor ART-tool
 cache timeout synchronized 60
```

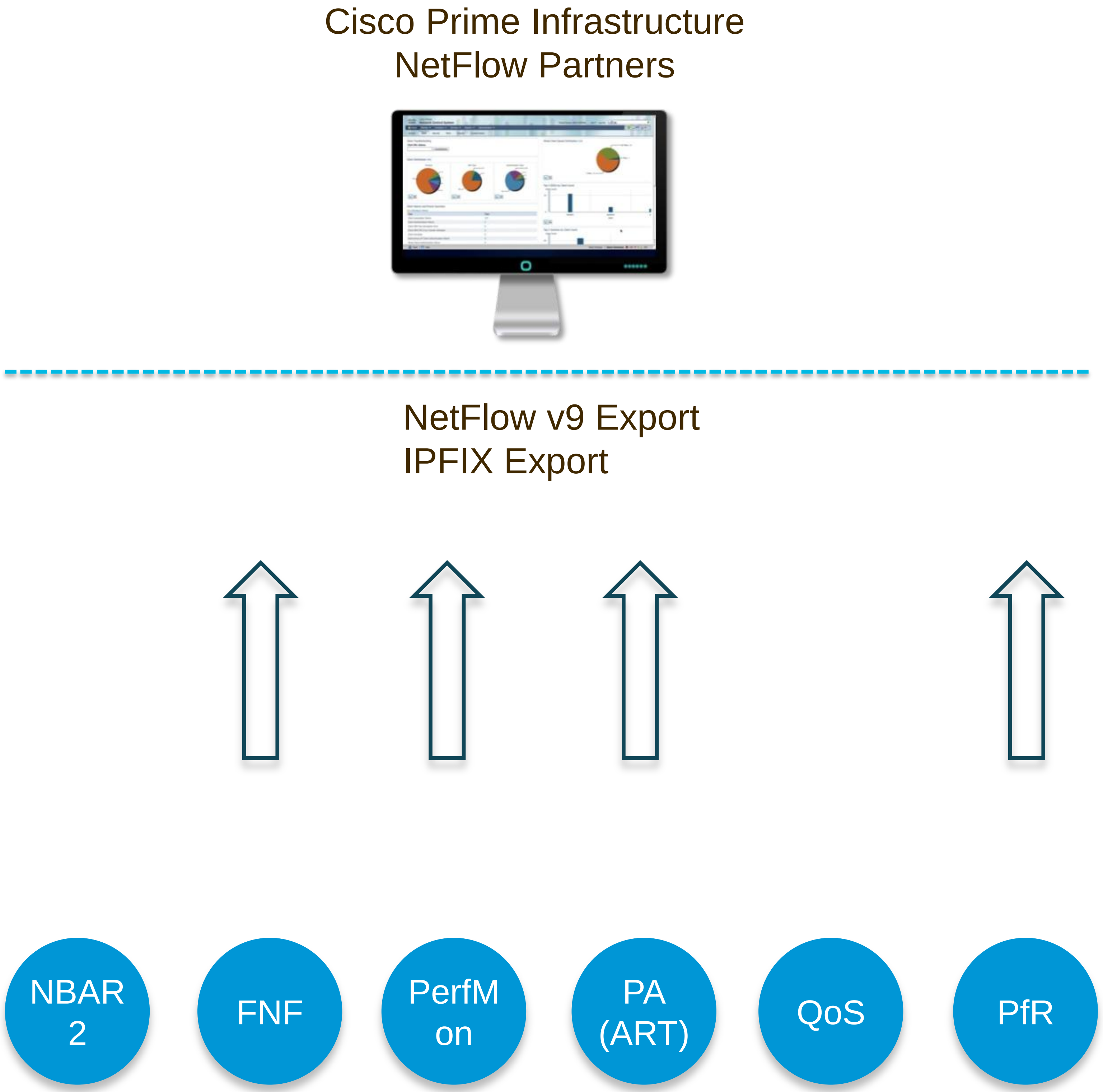


- Compare latency metric require same collection period across all devices
- Configure cache type ‘synchronised’ turn on this behaviour
- All devices require time synchronisation
- All devices start collection and export from top of the hour

AVC 1.0

Where are we today?

- Different provisioning models
- Duplication of metrics
- Inconsistent features
- Inconsistent show o/p
- Less functionality more confusion



Cisco Prime Infrastructure
NetFlow Partners

NetFlow v9 Export
IPFIX Export

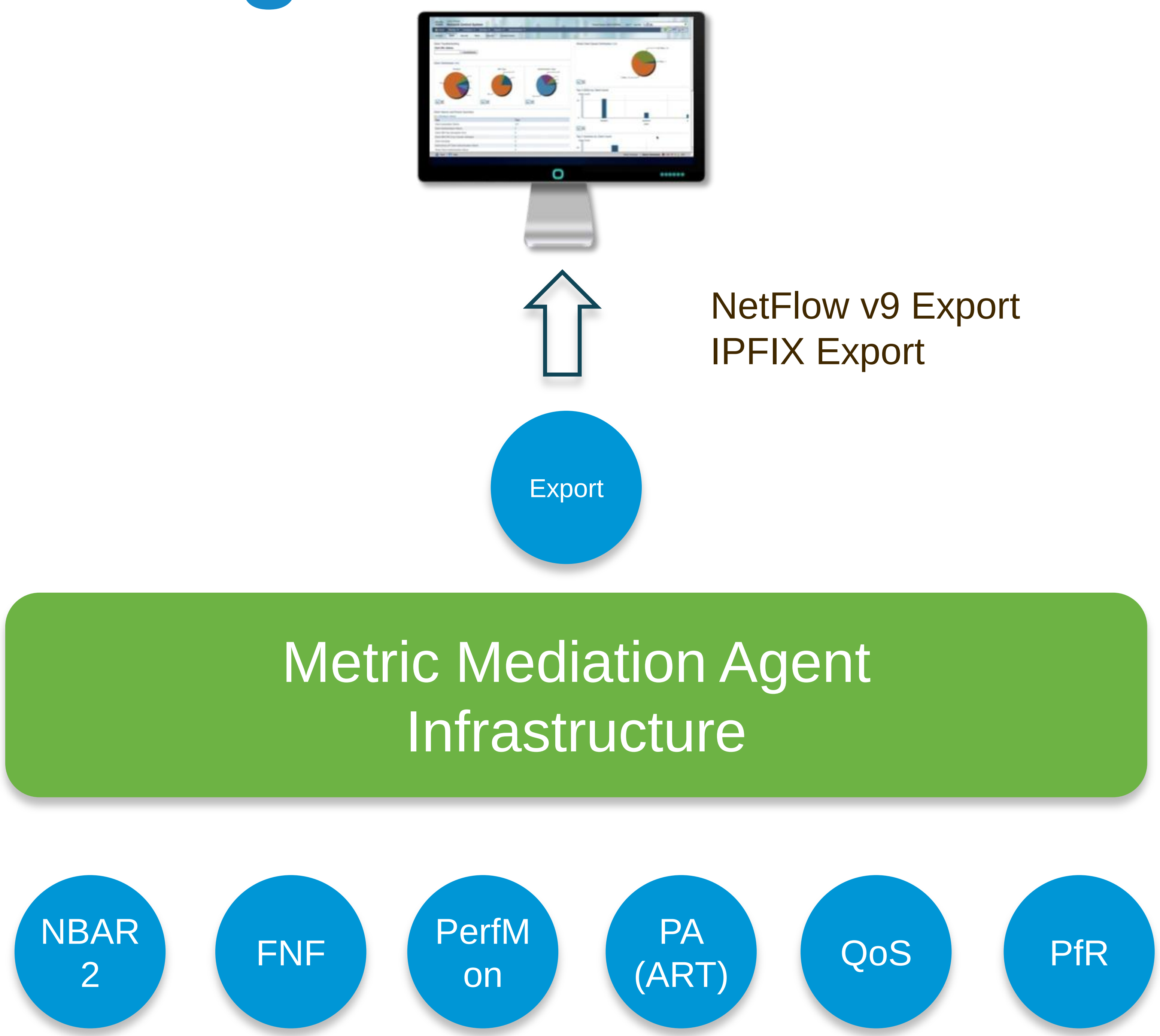
ISR G2: Future
ASR1K: 3.8S

AVC 2.0 – Unified Monitoring

Introduce Metric Mediation Agent (MMA)

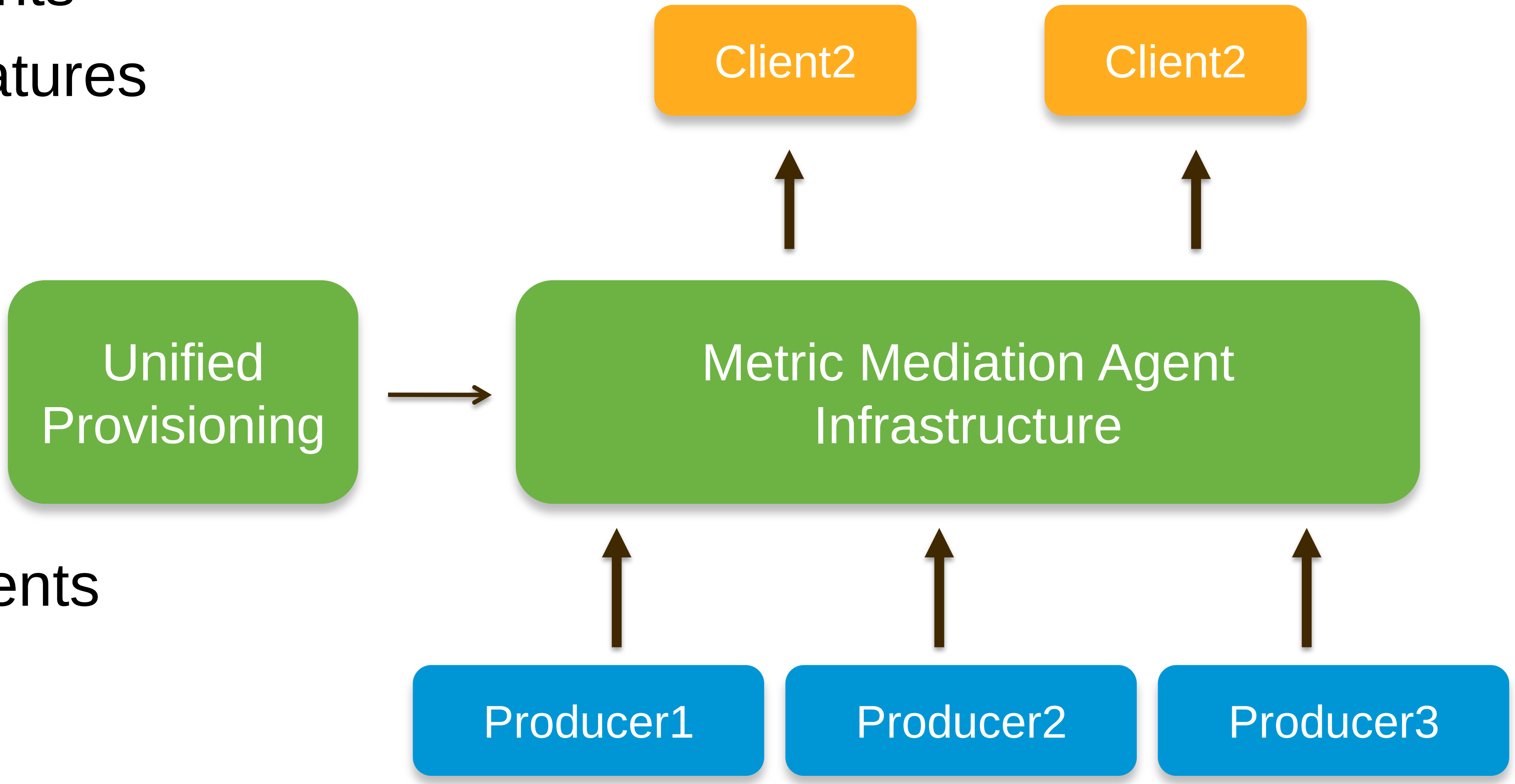
- Consistency in monitoring look-and-feel across features.
- Consistency in monitoring across platforms
- Consistency in managing monitoring data
- Enhance monitoring experience by consolidating feature statistics
- Enhance, use of monitoring data for data analysis, trending capacity planning and even auto configuration.
- Consistent semantics for each metric

Cisco Prime Infrastructure
NetFlow Partners



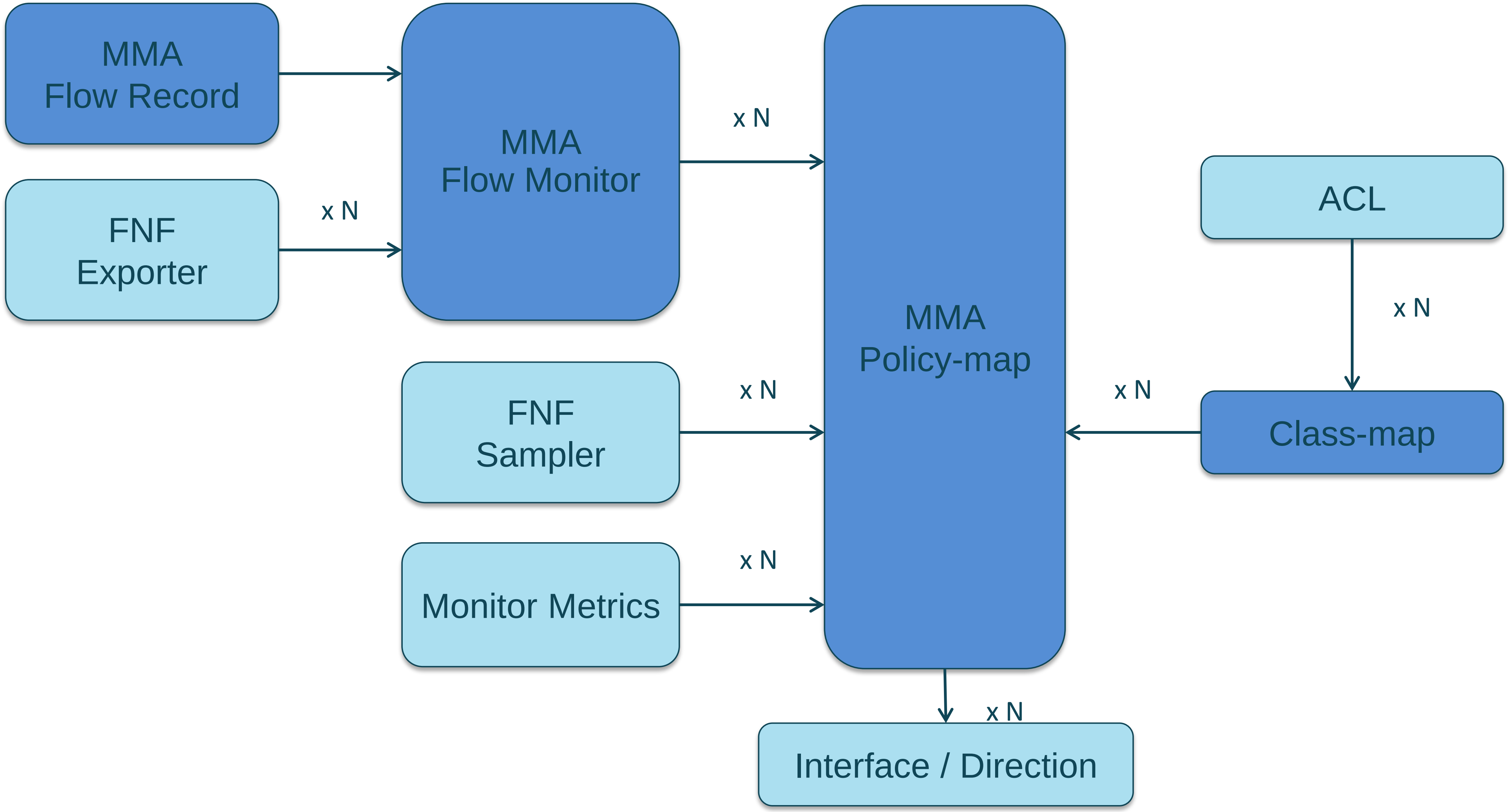
MMA – Service Provided

- Database for historical stats for clients
- Class and flow correlation for all features
- Data Manager supports stats aggregation and complex query
- Threshold monitoring and alert
- Common stats export (V9, SNMP, ConnectedApp API)
- Integration with other infra components
  - ConnectedApps
  - EEM
  - eEdge



MMA – Unified Provisioning

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



Performance Monitoring

Single Flow Record Type

Media Monitoring

- RTP SSRC
- RTP Jitter (min/max/mean)
- Transport Counter (expected/loss)
- Media Counter (bytes/packets/rate)
- Media Event
- Collection interval
- TCP MSS
- TCP round-trip time

Application Response Time

- CND - Client Network Delay (min/max/sum)
- SND – Server Network Delay (min/max/sum)
- ND – Network Delay (min/max/sum)
- AD – Application Delay (min/max/sum)
- Total Response Time (min/max/sum)
- Total Transaction Time (min/max/sum)
- Number of New Connections
- Number of Late Responses
- Response Time Histogram
- Number of Retransmissions
- Number of Transactions
- Client/Server Bytes
- Client/Server Packets

Other Metrics

- L3 counter (bytes/packets)
- Flow event
- Flow direction
- Client and server address
- Source and destination address
- Transport information
- Input and output interfaces
- L3 information (TTL, DSCP, TOS, etc.)
- Application information (from NBAR2)
- Monitoring class hierarchy

- All performance metrics are consolidated into one flow record type performance-monitor

AVC Pre-defined Flow Records

Traffic Statistics

- Application Usage per client IP/subnet/site
- Top clients per application

Application Response Time

- Per-application end-to-end latency
- Application response time & transaction time
- Application processing time
- Top conversation per application

Media Performance

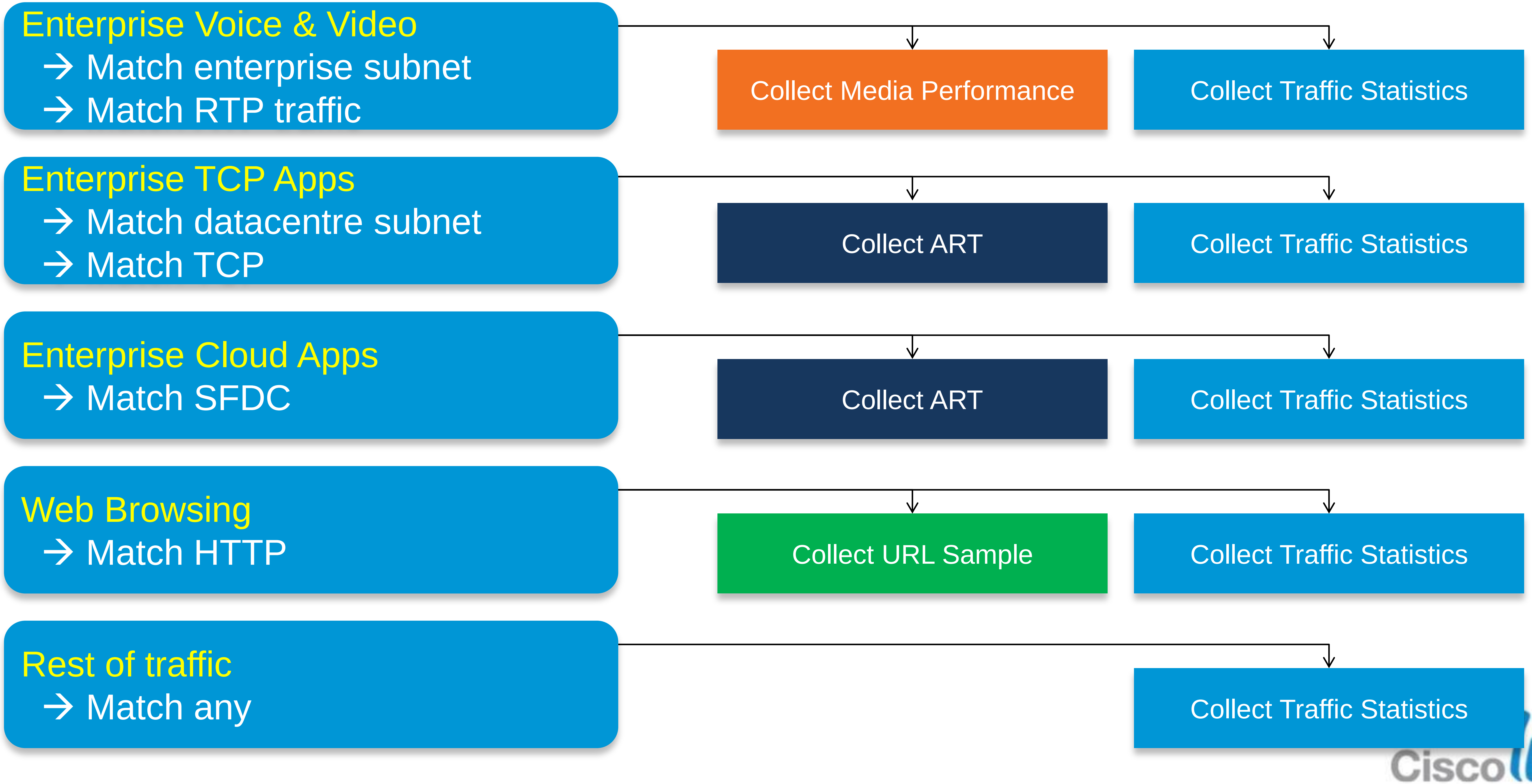
- Per-stream jitter and packet loss
- RTP conversations

URL Visibility

- Most visited web-site
- Per-URL application response time

AVC Sample Monitoring Policy

AVC Monitoring Policy



Enterprise Voice & Video
→ Match enterprise subnet
→ Match RTP traffic

Collect Media Performance

Collect Traffic Statistics

Enterprise TCP Apps
→ Match datacentre subnet
→ Match TCP

Collect ART

Collect Traffic Statistics

Enterprise Cloud Apps
→ Match SFDC

Collect ART

Collect Traffic Statistics

Web Browsing
→ Match HTTP

Collect URL Sample

Collect Traffic Statistics

Rest of traffic
→ Match any

Collect Traffic Statistics

Unified Monitoring Policy

AVC 1.0 – FNF, PA, Perfmon

Flexible NetFlow

```
flow record FNF-RECORD
 match ipv4 source address
 match ipv4 destination address
 match application name
 collect counter bytes long
  (..)
!
flow monitor FNF-MONITOR
  (..)
!
interface Gi0/0/1
 ip flow monitor FNF-MONITOR input
 ip flow monitor FNF-MONITOR output
```

Flow byte-count, interface, etc.

Perfmon

```
flow record type performance-monitor
medianet-record
 match ipv4 source address
 collect transport rtp-jitter
  (..)
!
flow monitor type performance-monitor
medianet-mon
  (..)
!
policy-map type performance-monitor
medianet
 class rtp-traffic
  flow monitor medianet-mon
!
interface Gi0/0/1
 service-policy type performance-monitor
input medianet
 service-policy type performance-monitor
output medianet
```

Voice/video RTP metrics, jitter, etc.

Performance Agent

```
flow record type mace mace-record
 collect art all
  (..)
!
flow monitor type mace ios-pa
  (..)
!
policy-map mace_global
 class http-traffic
  flow monitor type mace ios-pa
!
interface Gi0/0/1
 mace enable
!
```

App. Response Time, etc.

Unified Monitoring Policy

AVC 2.0 – MMA

Policy-driven monitoring – what to monitor, what to collect in single policy

Define Flow Records

```
flow record type performance-monitor rtp-record
 match ipv4 source address
 match ipv4 destination address
 match application name
 collect transport rtp-jitter
 (..)
flow record type performance-monitor art-record
 match ipv4 source address
 match ipv4 destination address
 match application name
 collect art all
 (..)
```

Flow byte-count, interface.
Voice/video RTP metrics, jitter.
App. Response Time, etc.

Define Flow Monitors

```
flow monitor type performance-monitor rtp-mon
 (..)
flow monitor type performance-monitor app-mon
 (..)
```

Filter what traffic to monitor

```
policy-map type performance-monitor avc
 class rtp-traffic
  flow monitor rtp-mon
 class tcp-app
  flow monitor app-mon
 (..)
!
interface Gi0/0/1
 service-policy type performance-monitor input avc
 service-policy type performance-monitor output avc
```

Performance Collection & Exporting Summary –

ISR G2 vs ASR1K

Export (NFv9 and IPFIX)	IOS (ISR G2)	IOS XE (ASR1K)
Collect Application Name (NBAR2)	✓	✓
Flexible Netflow on Interface	✓	✓
Policy-based Flexible Netflow	✓	✓
Field Extraction Report	✗	✓
URL Hit Count	✓	✗
Media Monitoring (MMON)	✓	✓
TCP Performance (ART)	✓	✓
QoS Class Hierarchy Report	✓	✗
Unified Monitoring Policy (MMA)	✗	✓

- Data is as of IOS 15.2(4)M2 and IOS XE 3.8S

Cisco Prime Infrastructure (PI)

3rd Party Network Management

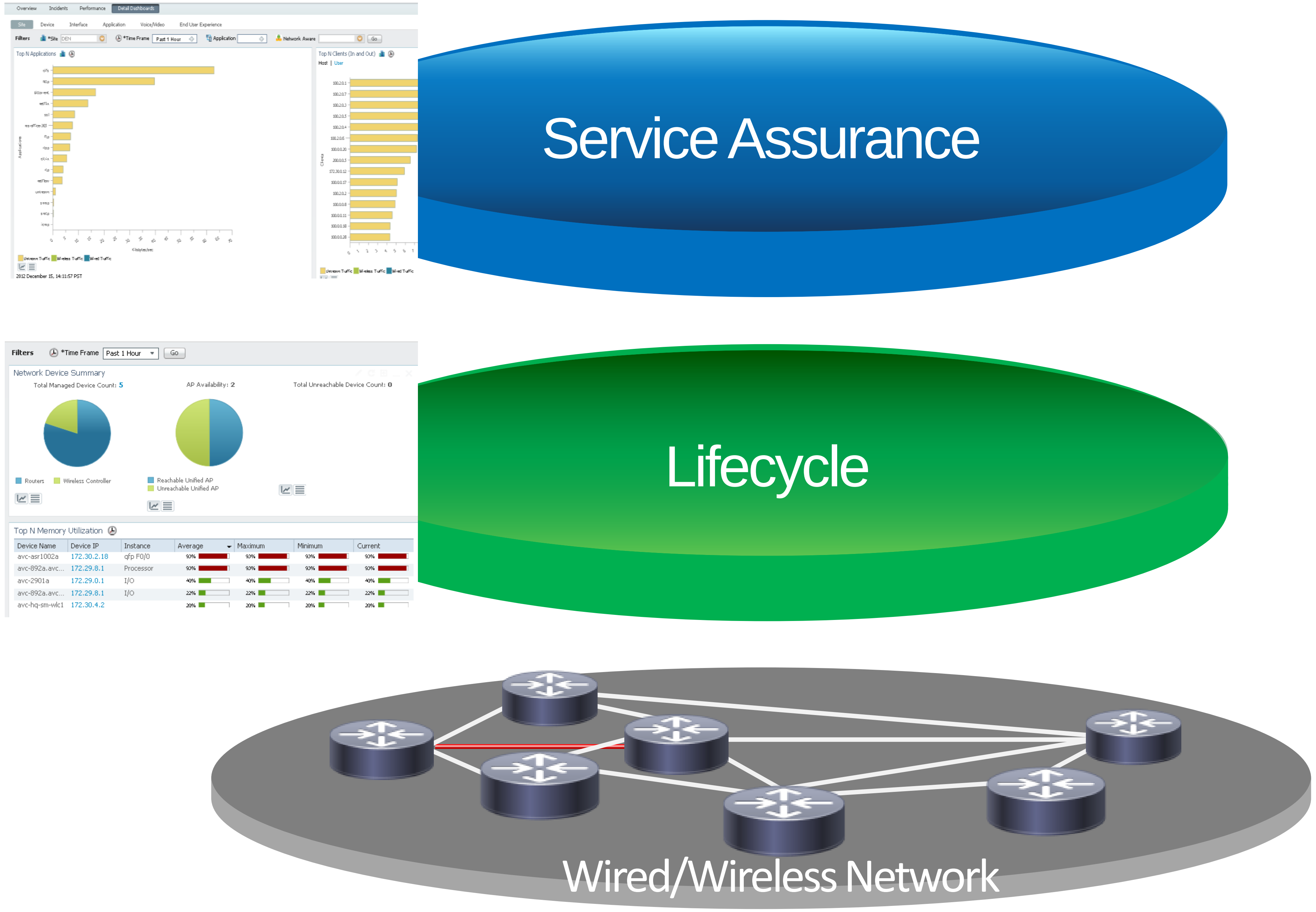
App Visibility &
User Experience Report

App	BW	Transaction Time	…
WebEx	3 Mb	150 ms	…
Citrix	10 Mb	500 ms	…

Management Tool

Advanced reporting tool aggregates and reports application performance

Cisco Prime Infrastructure



2012 December 15, 14:11:57 PST

Filters *Time Frame Past 1 Hour Go

Top N Memory Utilization

Device Name	Device IP	Instance	Average	Maximum	Minimum	Current
avc-asr1002a	172.30.2.18	qfp F0/0	93%	93%	93%	93%
avc-892a.avc...	172.29.8.1	Processor	93%	93%	93%	93%
avc-2901a	172.29.0.1	I/O	40%	40%	40%	40%
avc-892a.avc...	172.29.8.1	I/O	22%	22%	22%	22%
avc-hq-sm-wlc1	172.30.4.2		20%	20%	20%	20%

- ✓ Accelerate Troubleshooting
- ✓ Proactive monitoring and resolution of network issues
- ✓ Visibility into application and voice traffic

- ✓ One Management for all wired and wireless devices
- ✓ Day 1 device support
- ✓ Single pane of glass view and manage into the entire network

Assurance

Improve Enterprise Operational Excellence

Network Performance

- ✓ Network Availability and Performance polling with Event/Alarm generation
- ✓ Custom MIB polling
- ✓ Network Traffic Analysis & Reporting
- ✓ Data and flow collection: NetFlow, MMON, ART, NBAR2, SPAN

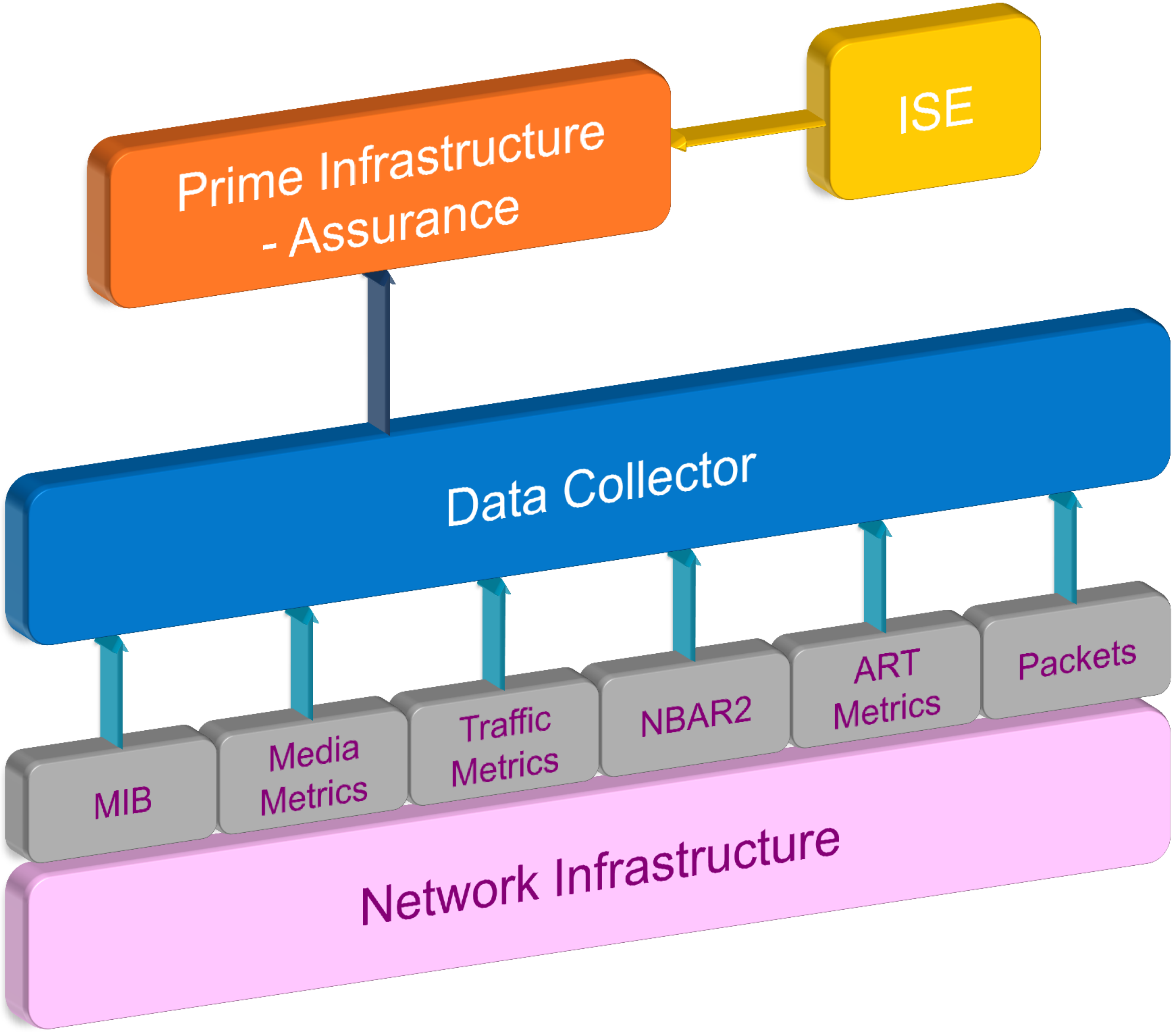
Visibility

- ✓ End-to-end application performance (Visibility and Response Time)
- ✓ Voice and Video Quality of Experience (Media trace and users voice troubleshooting)
- ✓ Packet level debugging and troubleshooting

End User Experience

- ✓ Users Wired/Wireless experience - Applications, bandwidth utilisation and voice quality experience by user's end points
- ✓ Optimised Business critical application delivery
- ✓ WAN Optimisation ROI

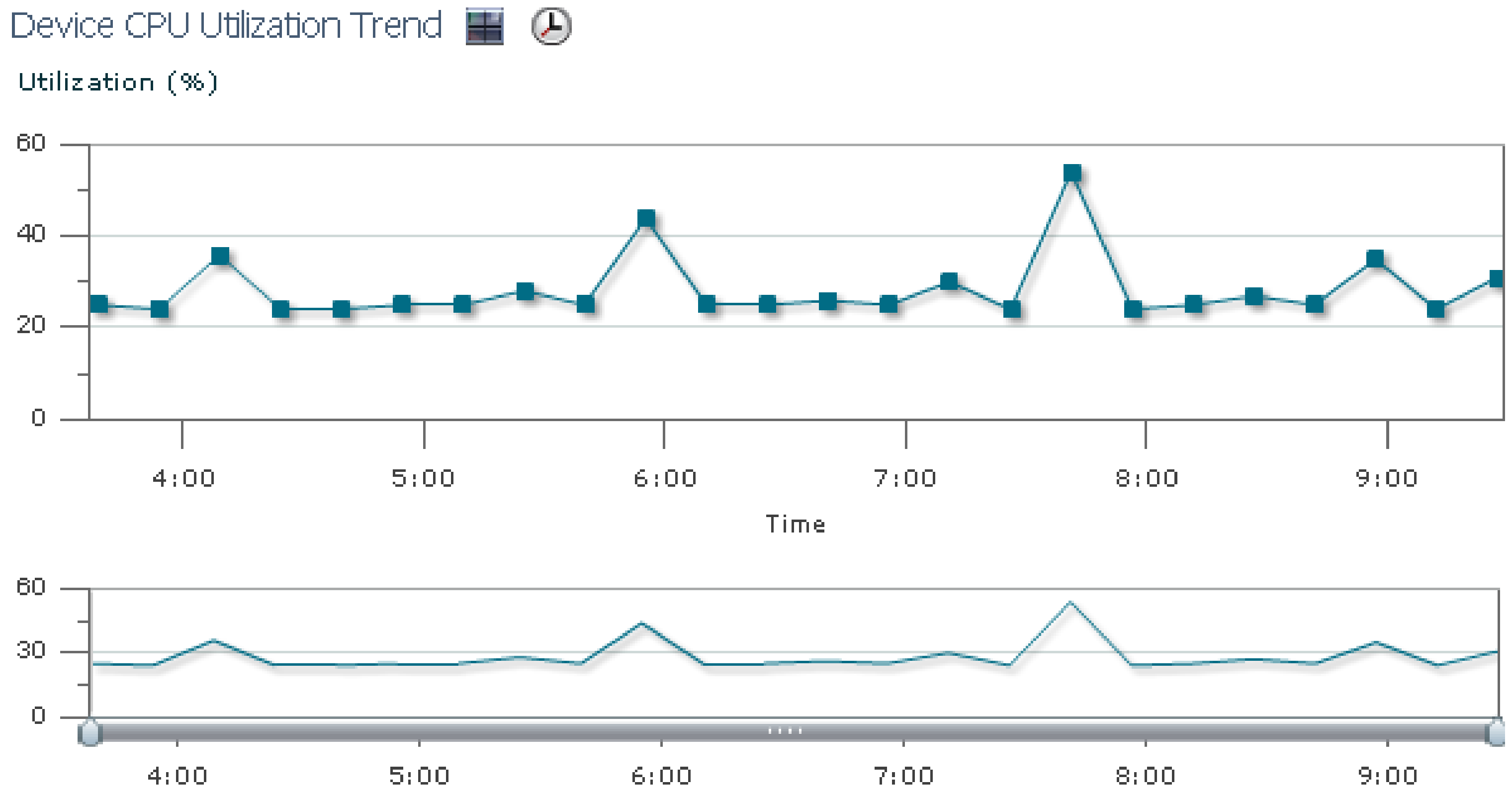
Cisco Prime Infrastructure – Assurance



- Configuration of AVC features*
- Network Monitoring
- Service Monitoring
- Reporting and Trends
- Multi-NAM Manager
- Packet and Flows Analysis
- Application Response Time
- Voice and Video Metrics
- Distributed SNMP and Netflow Collection

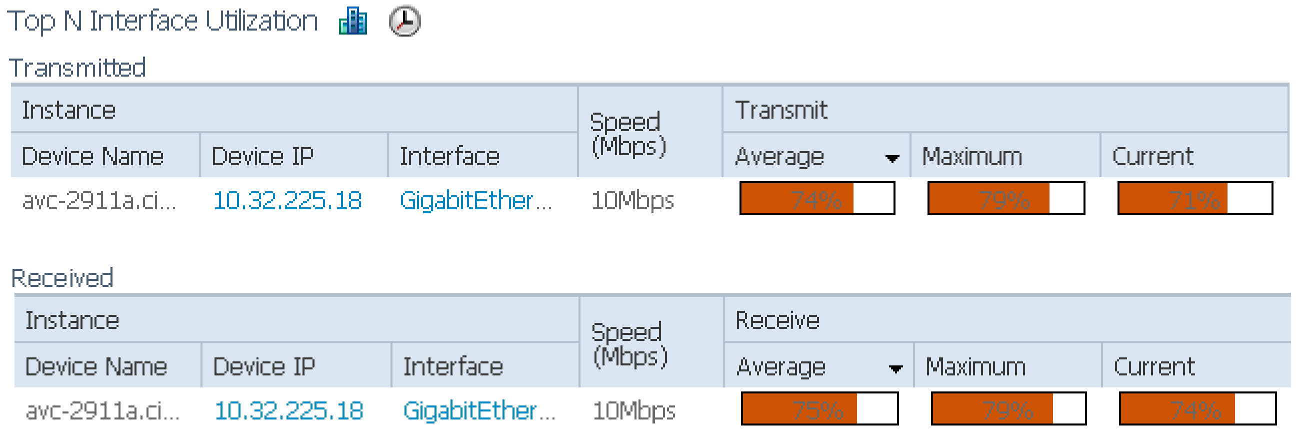
Cisco Prime Infrastructure

Monitor Infrastructure Performance



CPU and Memory

- Polling of Infrastructure Information through SNMP



Top N Interface Utilization

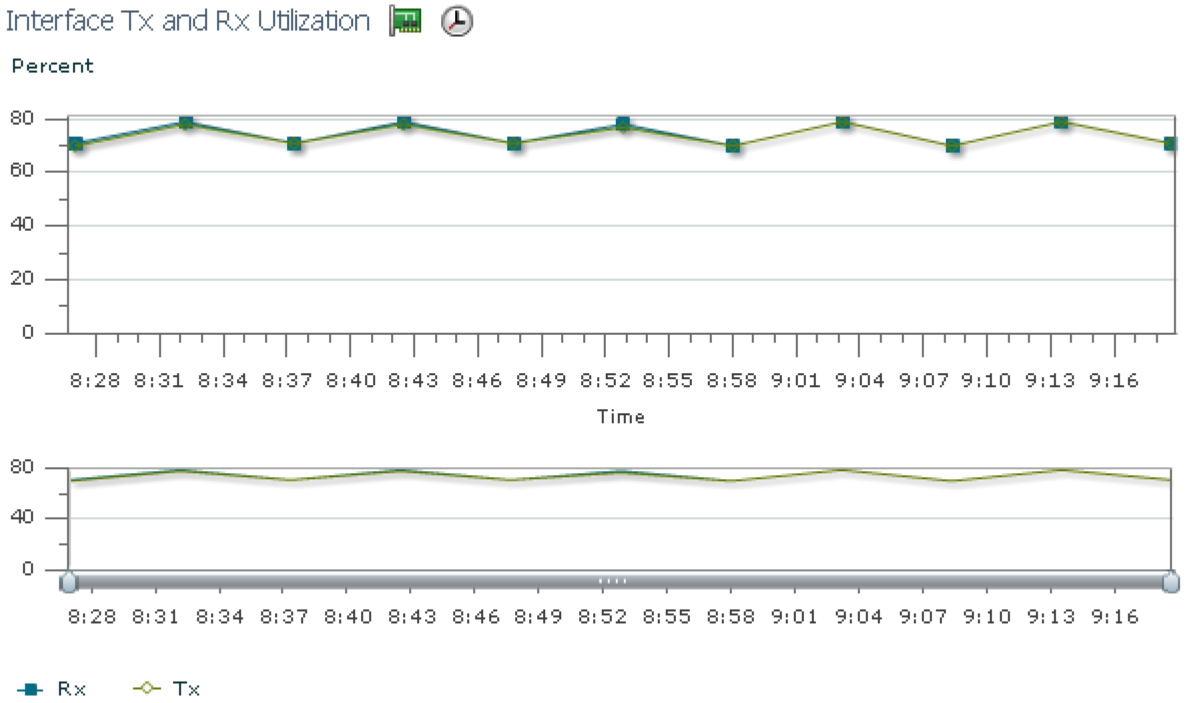
Transmitted

Instance			Speed (Mbps)	Transmit		
Device Name	Device IP	Interface		Average	Maximum	Current
avc-2911a.ci...	10.32.225.18	GigabitEther...	10Mbps	74%	79%	71%

Received

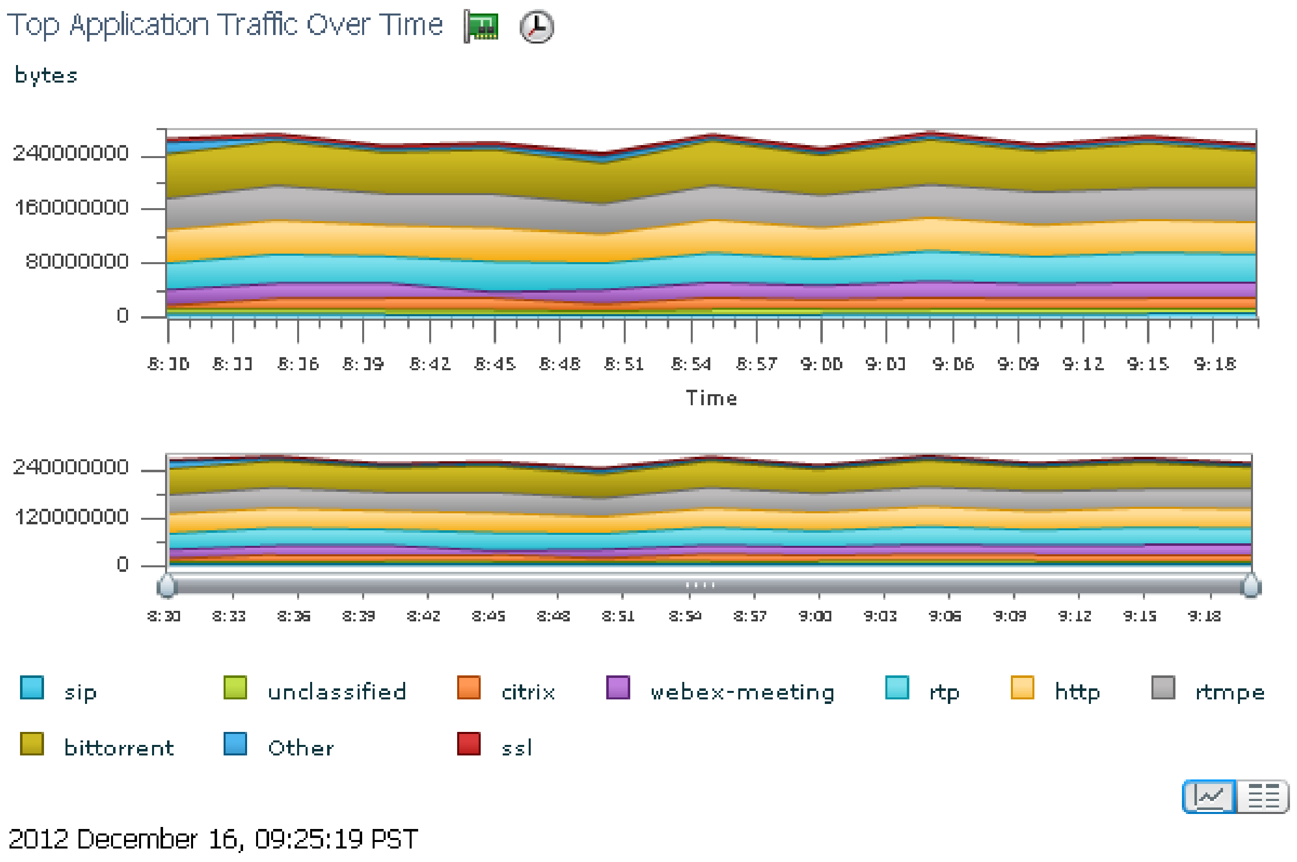
Instance			Speed (Mbps)	Receive		
Device Name	Device IP	Interface		Average	Maximum	Current
avc-2911a.ci...	10.32.225.18	GigabitEther...	10Mbps	75%	79%	74%

Interface Utilisation



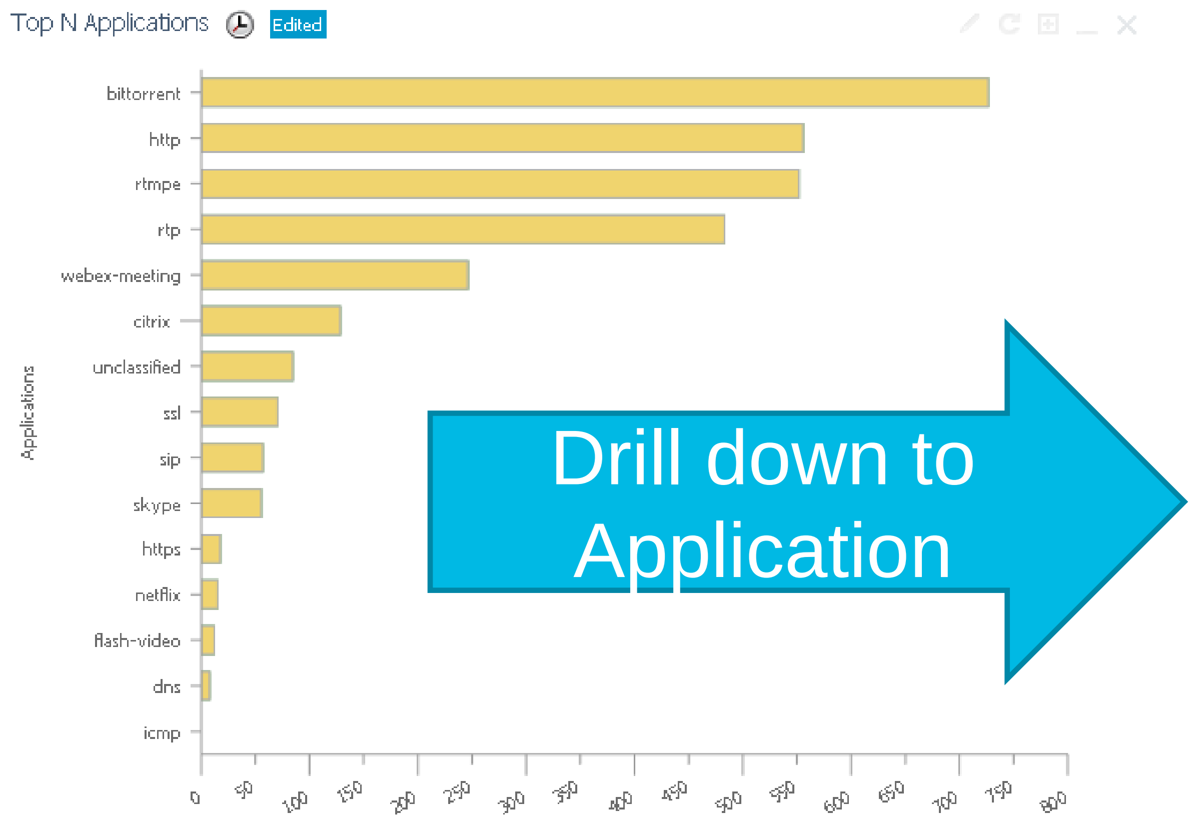
Cisco Prime Infrastructure

Monitor Application Usage



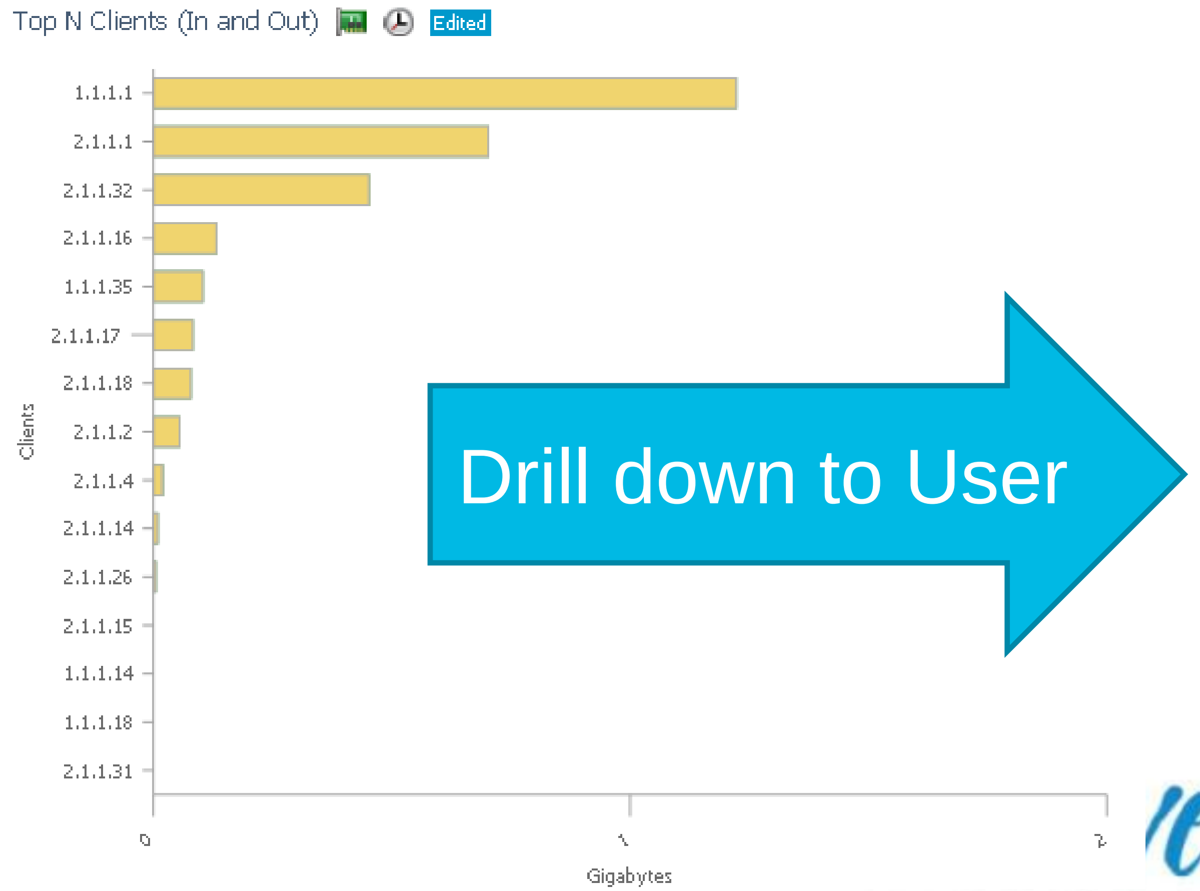
2012 December 16, 09:25:19 PST

Application over Time



Drill down to Application

Top Applications & Top Talkers

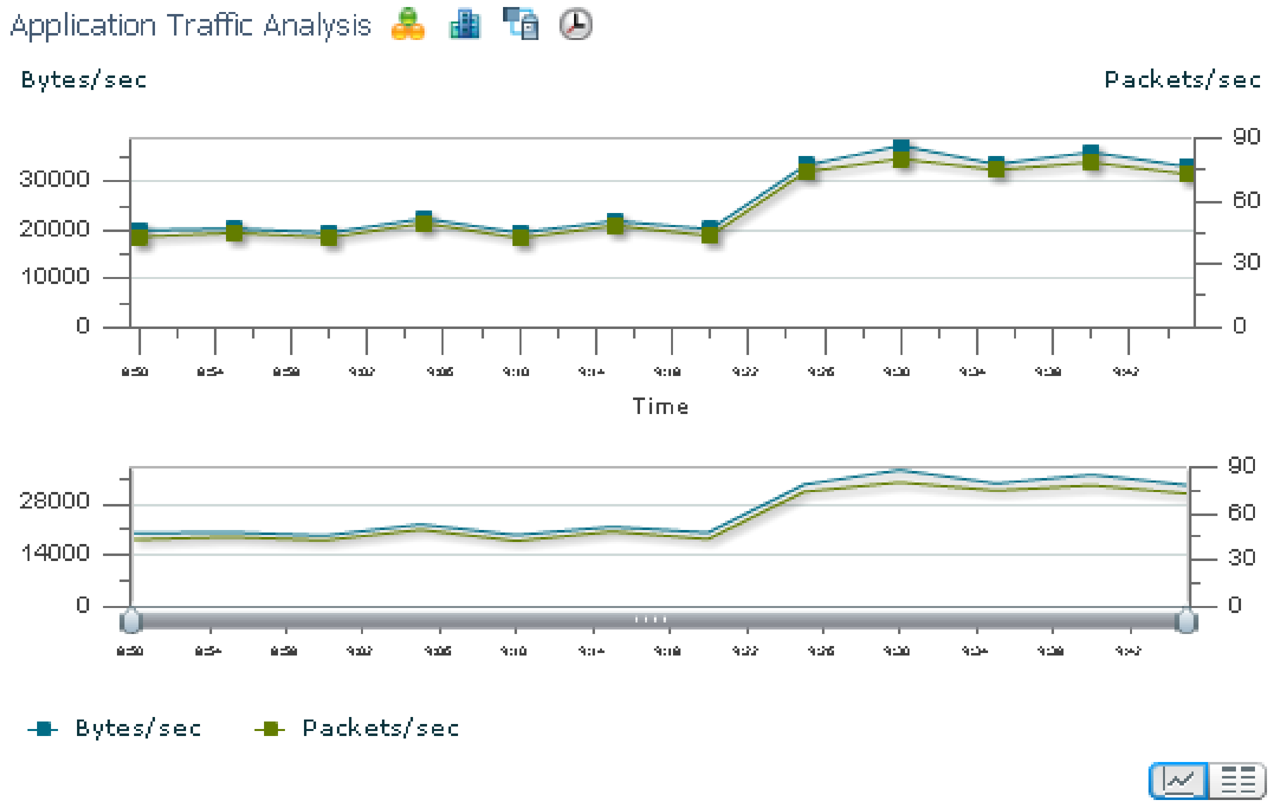


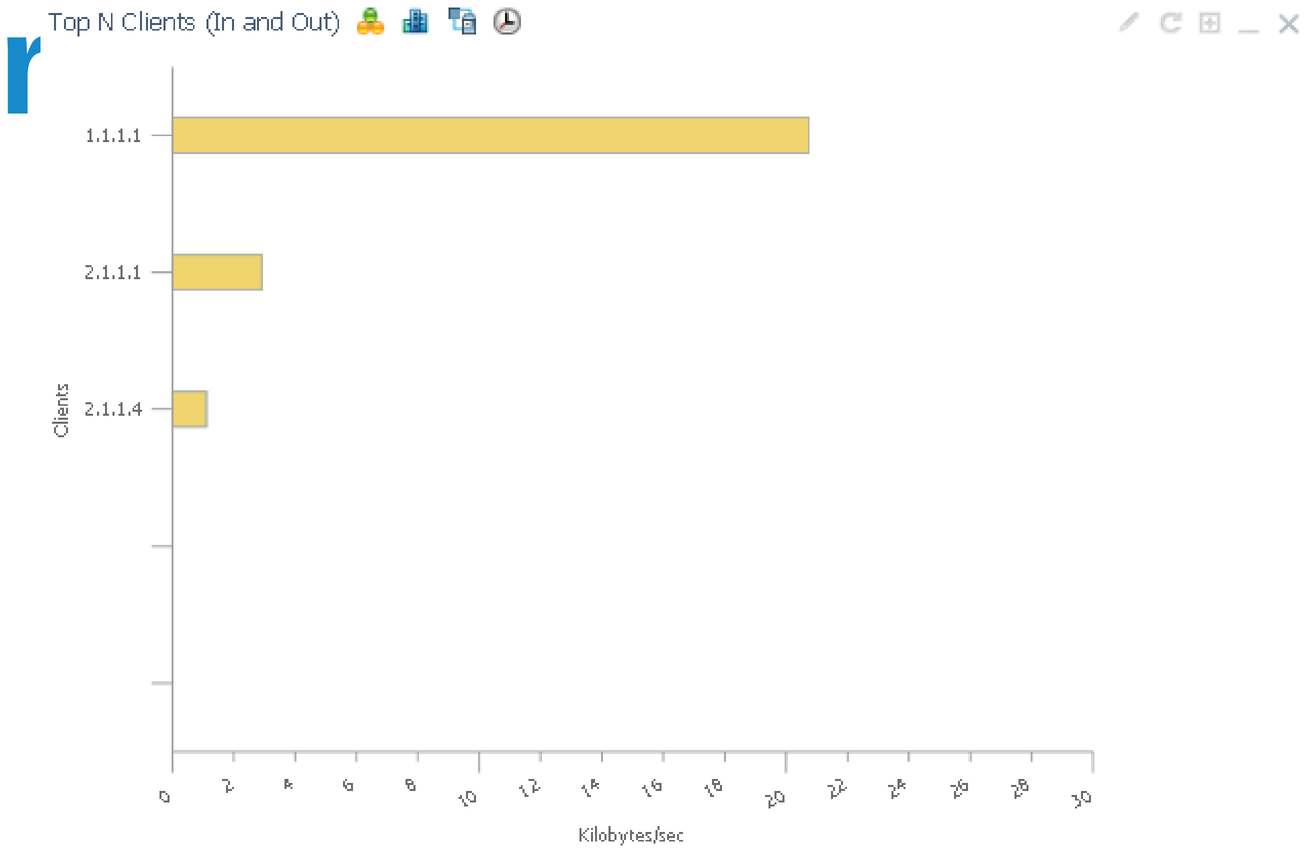
Drill down to User

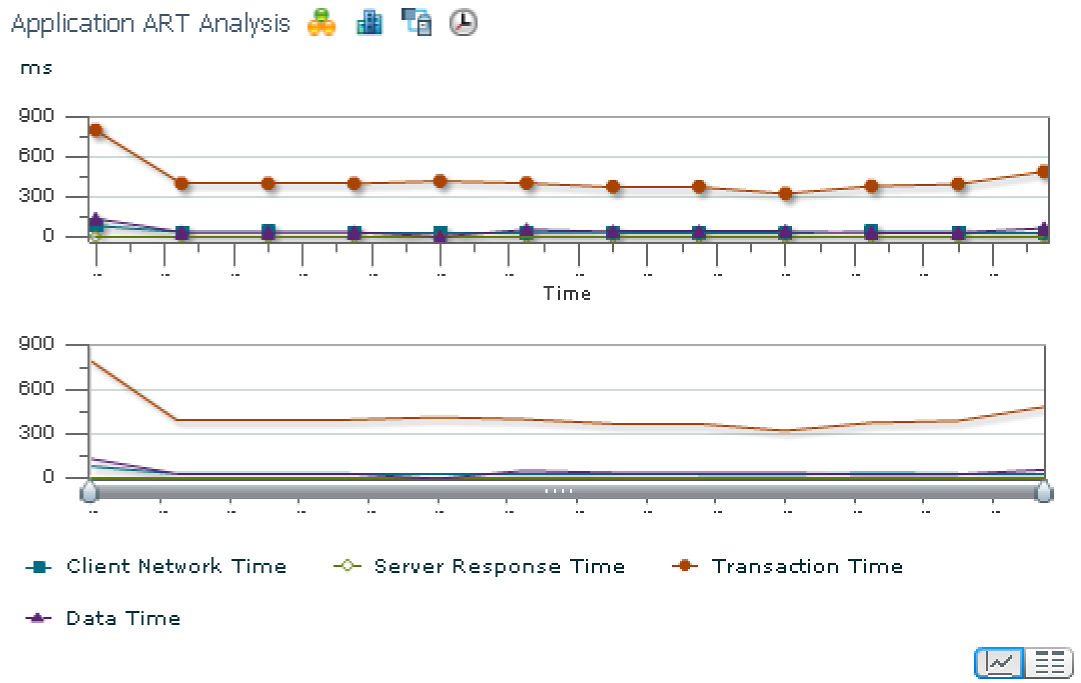
- Drill down to specific interface or site to see application usage and top talkers

Cisco Prime Infrastructur

Application Performance View

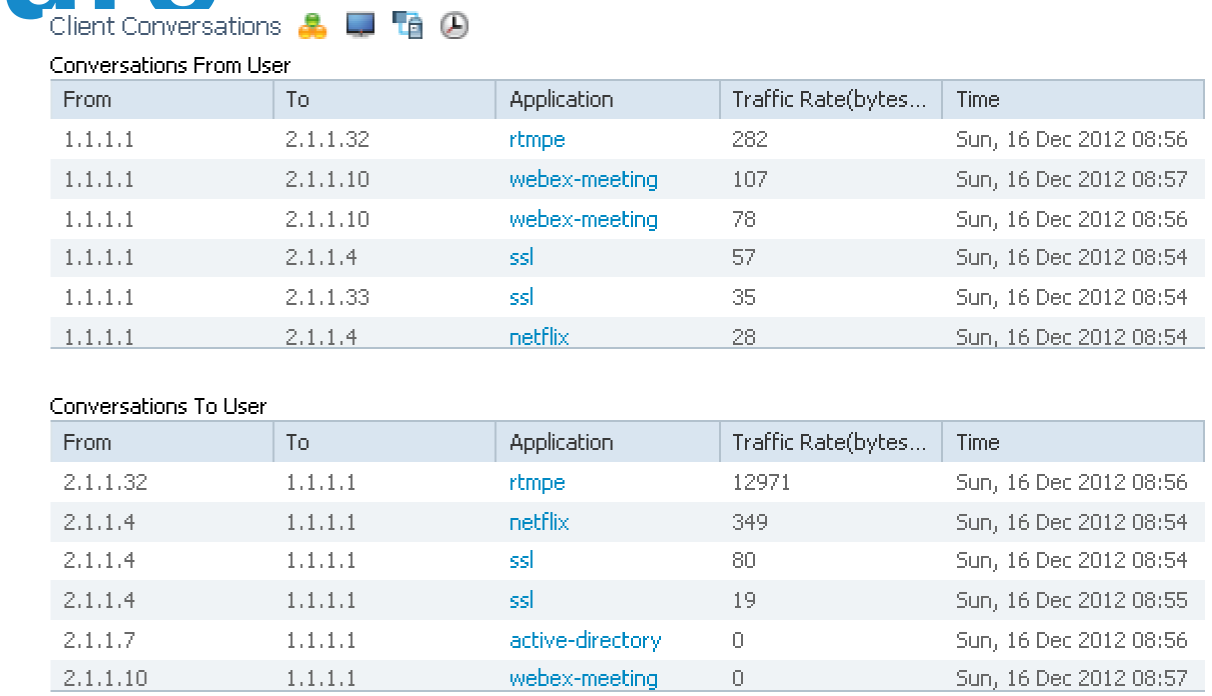






Cisco Prime Infrastructure

End User View



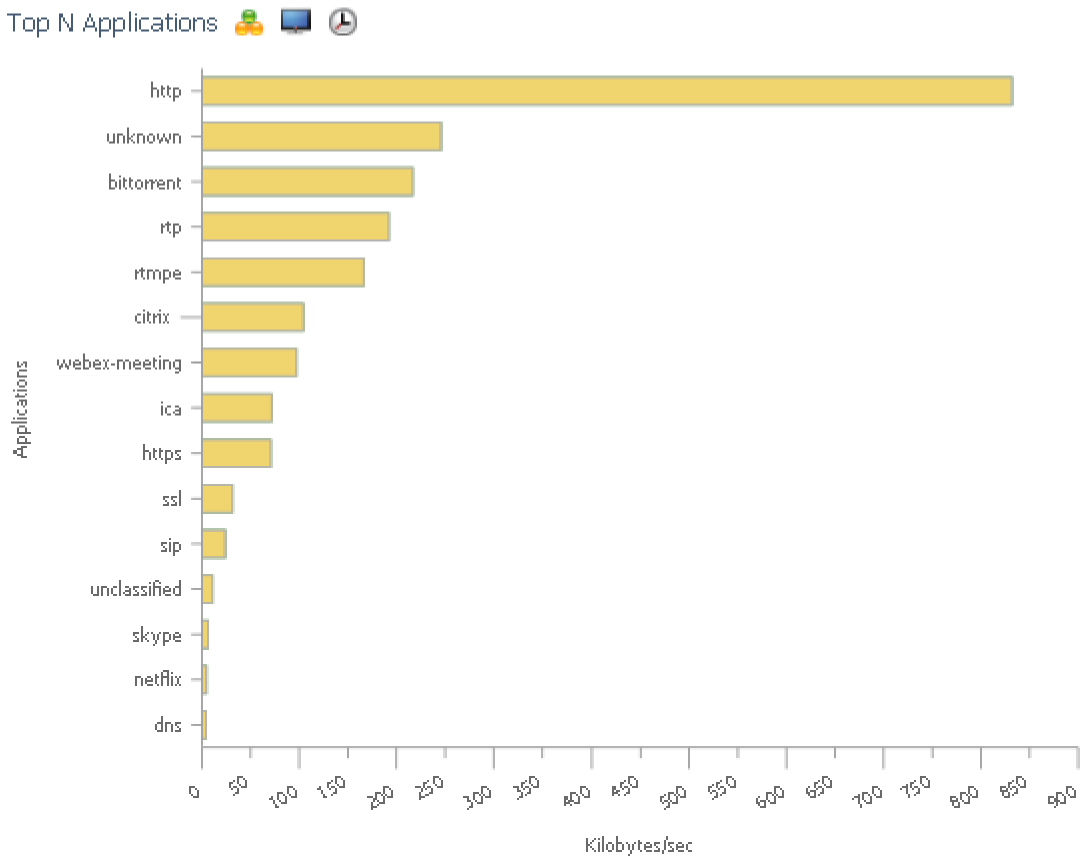
Client Conversations

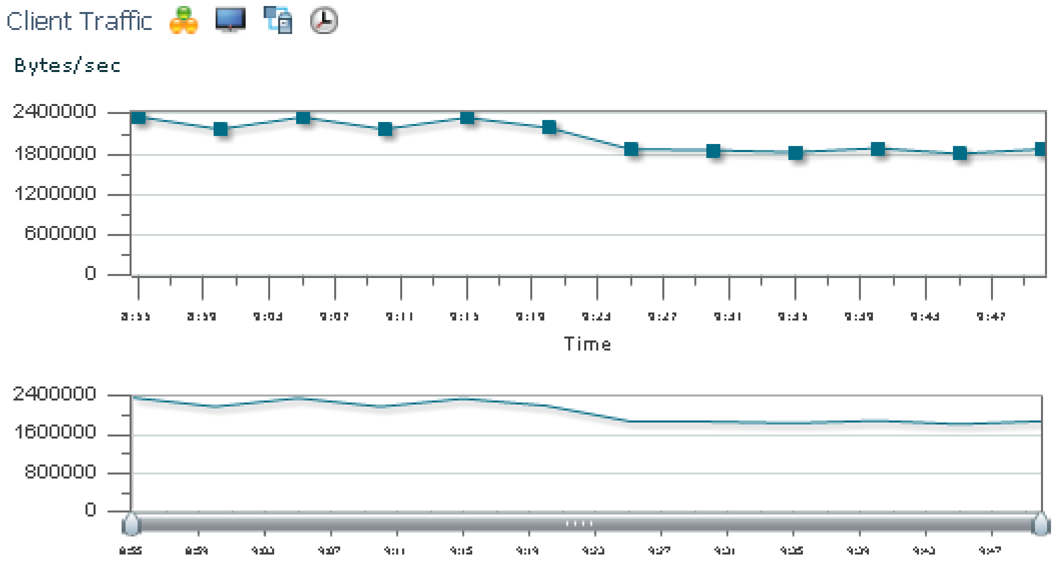
Conversations From User

From	To	Application	Traffic Rate(bytes...	Time
1.1.1.1	2.1.1.32	rtmpe	282	Sun, 16 Dec 2012 08:56
1.1.1.1	2.1.1.10	webex-meeting	107	Sun, 16 Dec 2012 08:57
1.1.1.1	2.1.1.10	webex-meeting	78	Sun, 16 Dec 2012 08:56
1.1.1.1	2.1.1.4	ssl	57	Sun, 16 Dec 2012 08:54
1.1.1.1	2.1.1.33	ssl	35	Sun, 16 Dec 2012 08:54
1.1.1.1	2.1.1.4	netflix	28	Sun, 16 Dec 2012 08:54

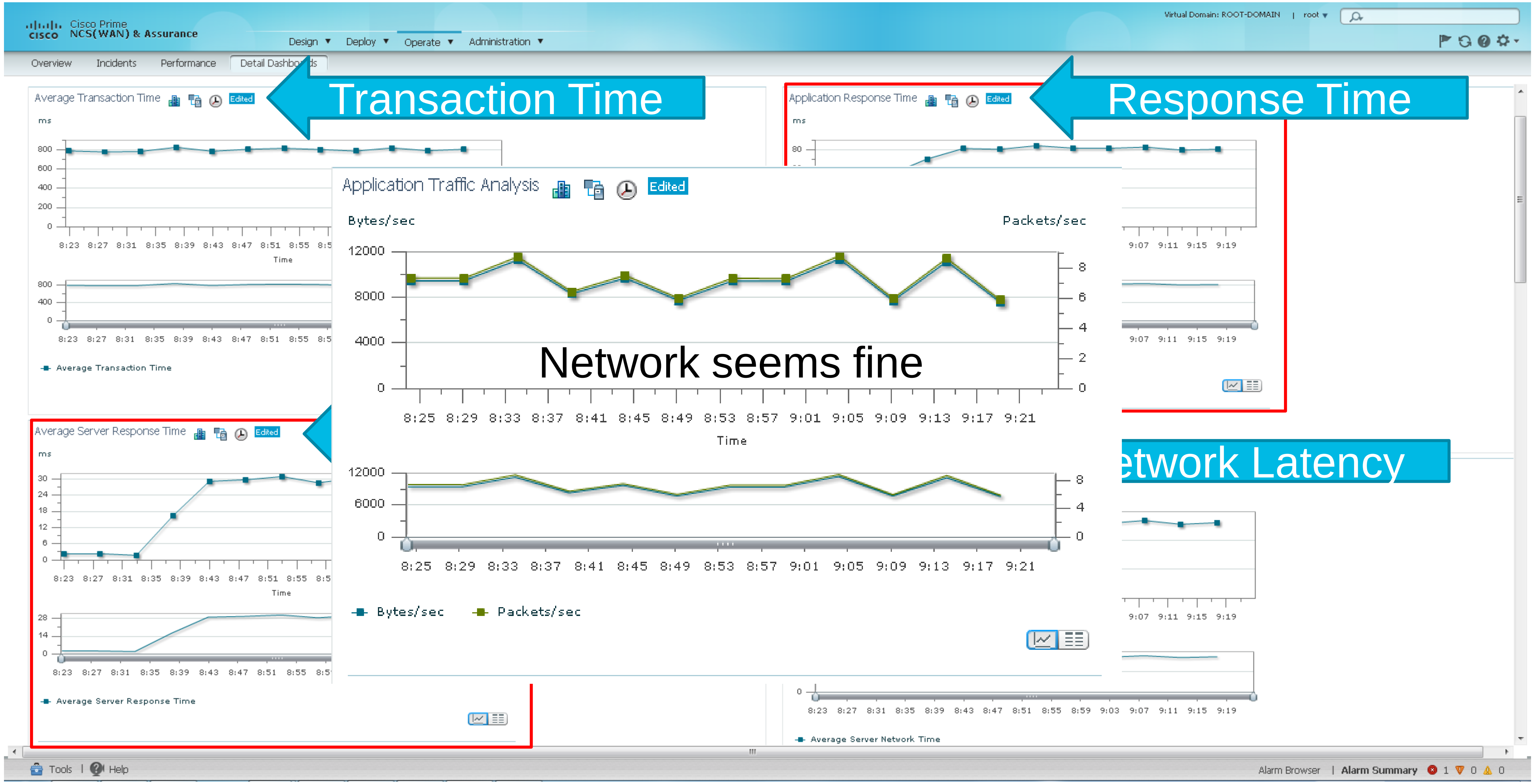
Conversations To User

From	To	Application	Traffic Rate(bytes...	Time
2.1.1.32	1.1.1.1	rtmpe	12971	Sun, 16 Dec 2012 08:56
2.1.1.4	1.1.1.1	netflix	349	Sun, 16 Dec 2012 08:54
2.1.1.4	1.1.1.1	ssl	80	Sun, 16 Dec 2012 08:54
2.1.1.4	1.1.1.1	ssl	19	Sun, 16 Dec 2012 08:55
2.1.1.7	1.1.1.1	active-directory	0	Sun, 16 Dec 2012 08:56
2.1.1.10	1.1.1.1	webex-meeting	0	Sun, 16 Dec 2012 08:57





1. Detect Application Server Problem



Transaction Time

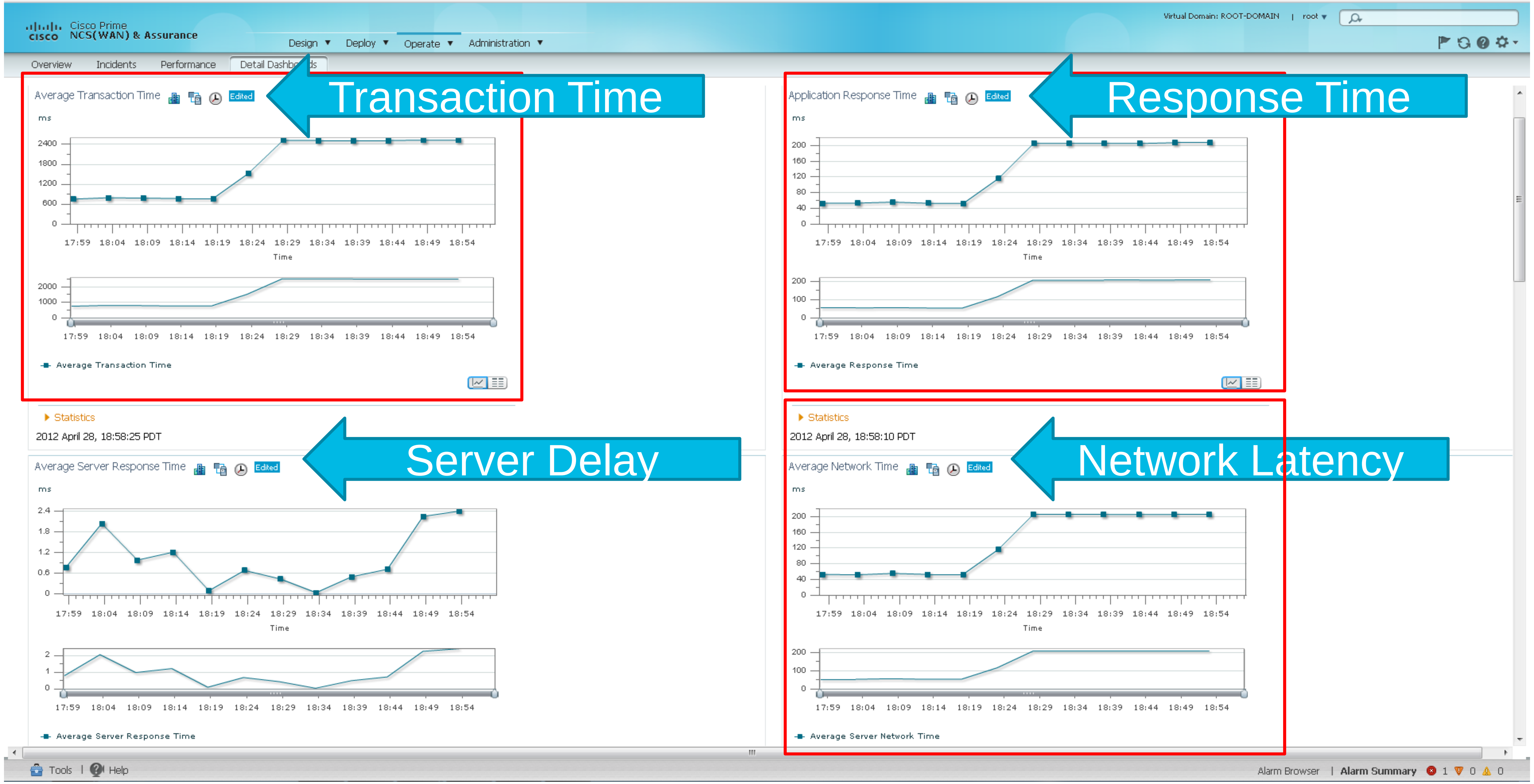
Response Time

Network seems fine

Network Latency

- End user experience is impacted because application is slow

2. Detect Network Latency Increase Per Application



Statistics

2012 April 28, 18:58:25 PDT

Statistics

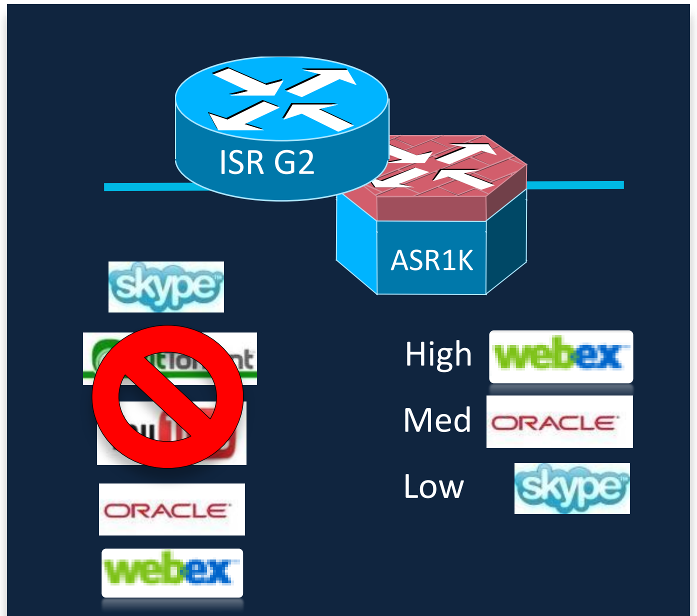
2012 April 28, 18:58:10 PDT

- Increased network latency impacts response time and transaction ti

Cisco Prime Infrastructure and 3rd Party

Vendor		NBAR2	Field Extraction	URL Hit Count	MMON	ART	PfR	QoS Class	QoS GUI
Cisco Prime Infrastructure v2.0	IOS	☑			☑	☑	☑		
	XE	☑	☑		☑	☑	☑		
ActionPacked LiveAction v2.6	IOS	☑			☑	☑	☑	☑	☑
	XE				☑		☑		
Plixer Scrutiniser	IOS	☑			☑	☑	☑		
	XE				☑		☑		
Living Objects	IOS	☑		☑		☑			
	XE								
Insight Reporter v4.0	IOS	☑				☑			
	XE	☑	☑						

And more in the pipeline ..



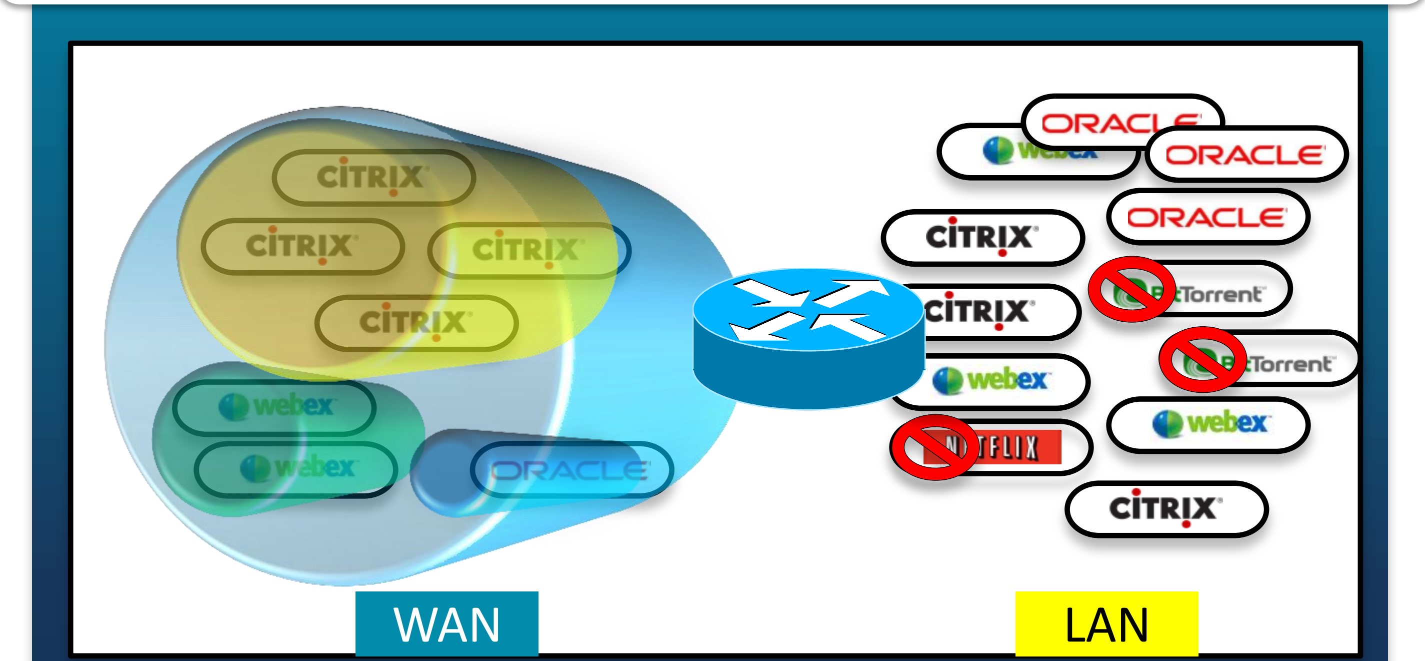
Control

Control application usage in the network to maximise application performance

Quality of Service (QoS) Performance Routing (PfR)

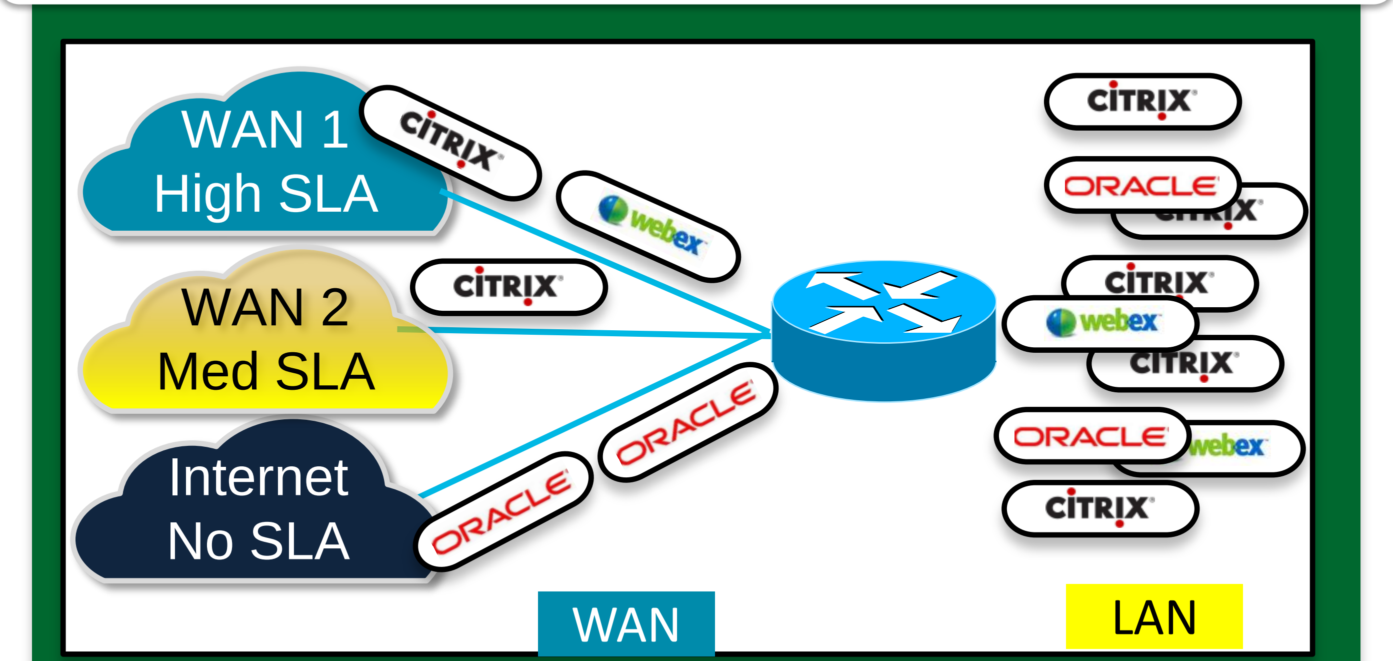
AVC Control Options

Application Bandwidth Control



- Guarantee bandwidth to protect critical applications from network congestion
- Provide low latency to delay sensitive applications
- Stop or limit unwanted applications from usin WAN resources

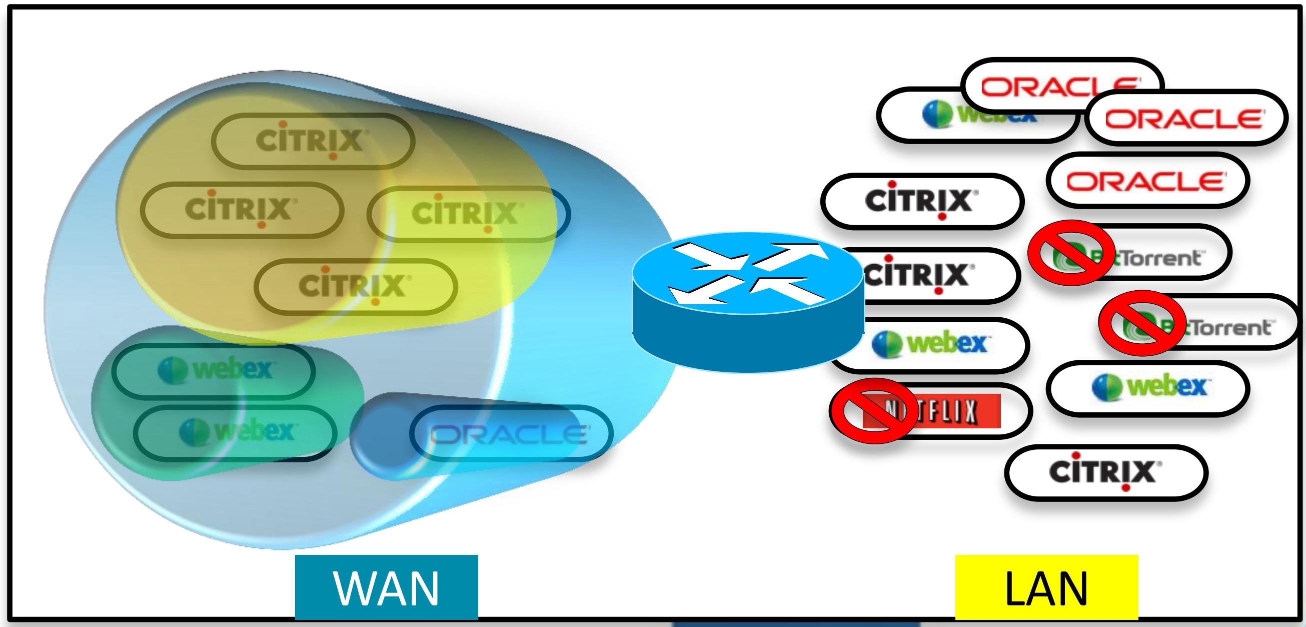
Application Path Control



- Application routing based-on real-time performance Information
- Intelligent load sharing provides resiliency and fully utilises all available WAN resources
- Improve performance of voice, video, and critical applications

Application Bandwidth Control

QoS



The Role of QoS for Control

Guarantee Bandwidth
- Bandwidth action

Limit Max Bandwidth
- Police action

Minimise Latency
- Priority action

Change Flow Properties
- Set action, i.e. set dscp

Reduce Burst
- Shape action

How to use NBAR2 Attributes in QoS Class-map

For Your Reference

- Match on protocol (application) or pre-defined attributes

```
class-map match-any p2p-class
 match protocol attribute application-group bittorrent-group
 match protocol kazaa2
 match protocol attribute sub-category p2p-networking
```

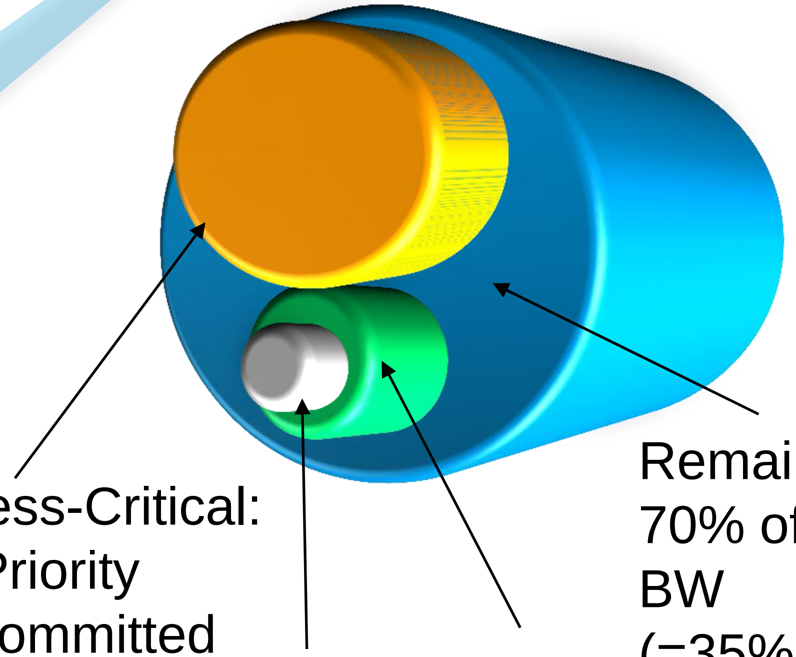
- I want to exclude Viber and Skype from **sub-category** voice-video-chat-collaboration

```
class-map match-any excluded-apps
 match protocol skype
 match protocol viber
class-map match-all voice-video-chat-app
 match protocol attribute sub-category voice-video-chat-collaboration
 match not class-map excluded-apps
```

Application-aware QoS

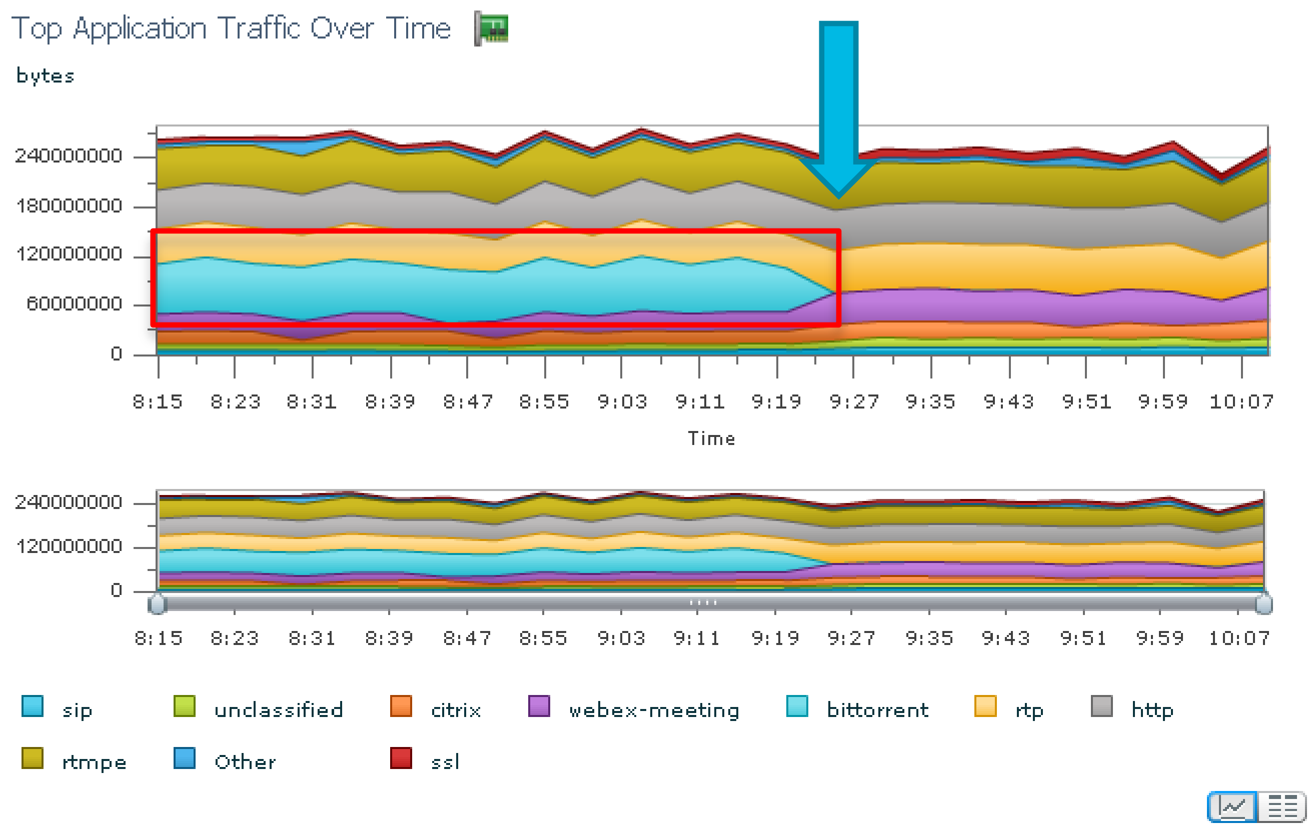
```
class-map match-all business-critical
        match protocol citrix
        match access-group 101

class-map match-any browsing
        match protocol attribute category browsing

class-map match-any internal-browsing
        match protocol http url "*myserver.com*"

policy-map internal-browsing-policy
        class internal-browsing
                bandwidth remaining percent 60

policy-map my-network-policy
        class business-critical
                priority percent 50

        class browsing
                bandwidth remaining percent 30
                service-policy internal-browsing-policy

interface Serial0/0/0
        service-policy output my-network-policy
```

Application	BW	Priority
Business Critical	Committed 50%	High
Browsing	30% (=15% of the line)	Normal
Internal Browsing	60% (Out of Browsing)	
Remaining	70% (=35% of the line)	Normal

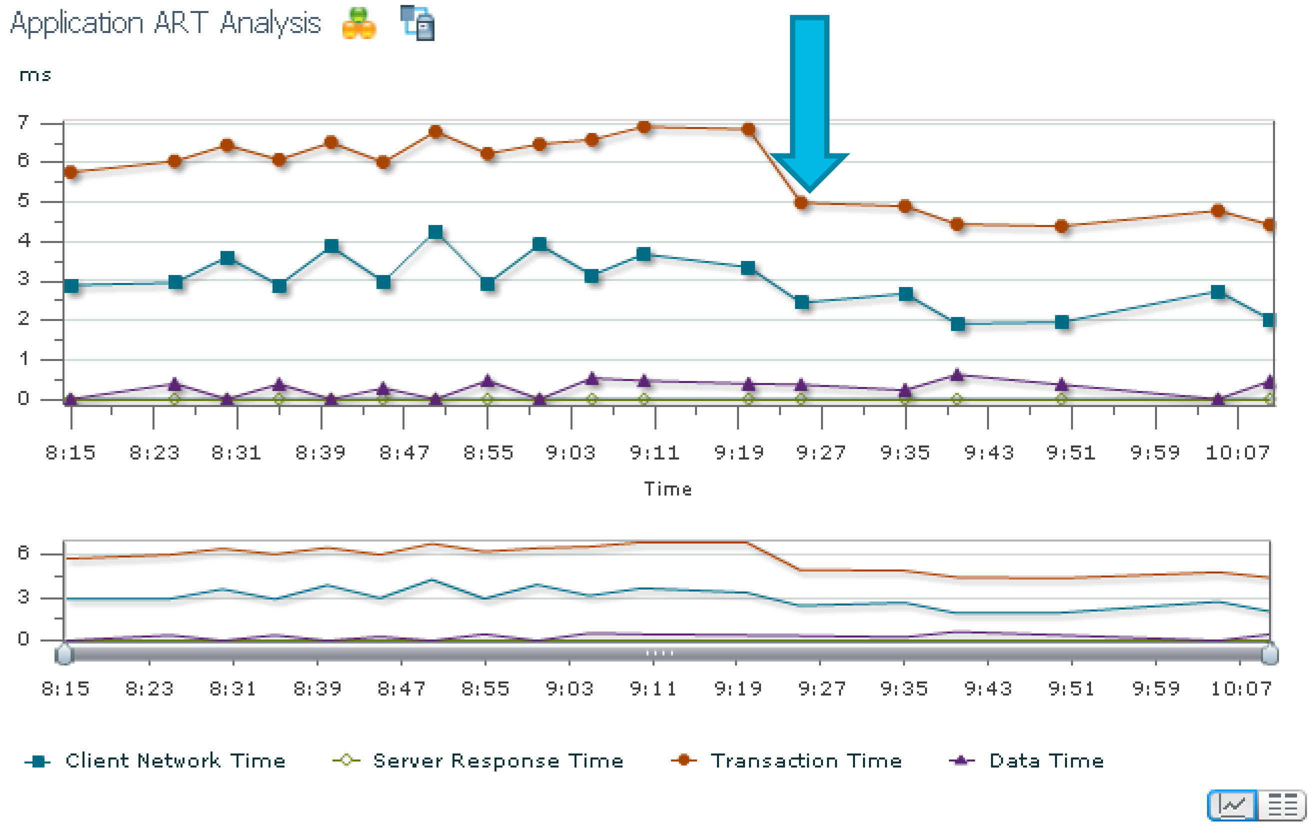


Example: Stop P2P Applications with AVC

Bandwidth Usage
After apply control policy

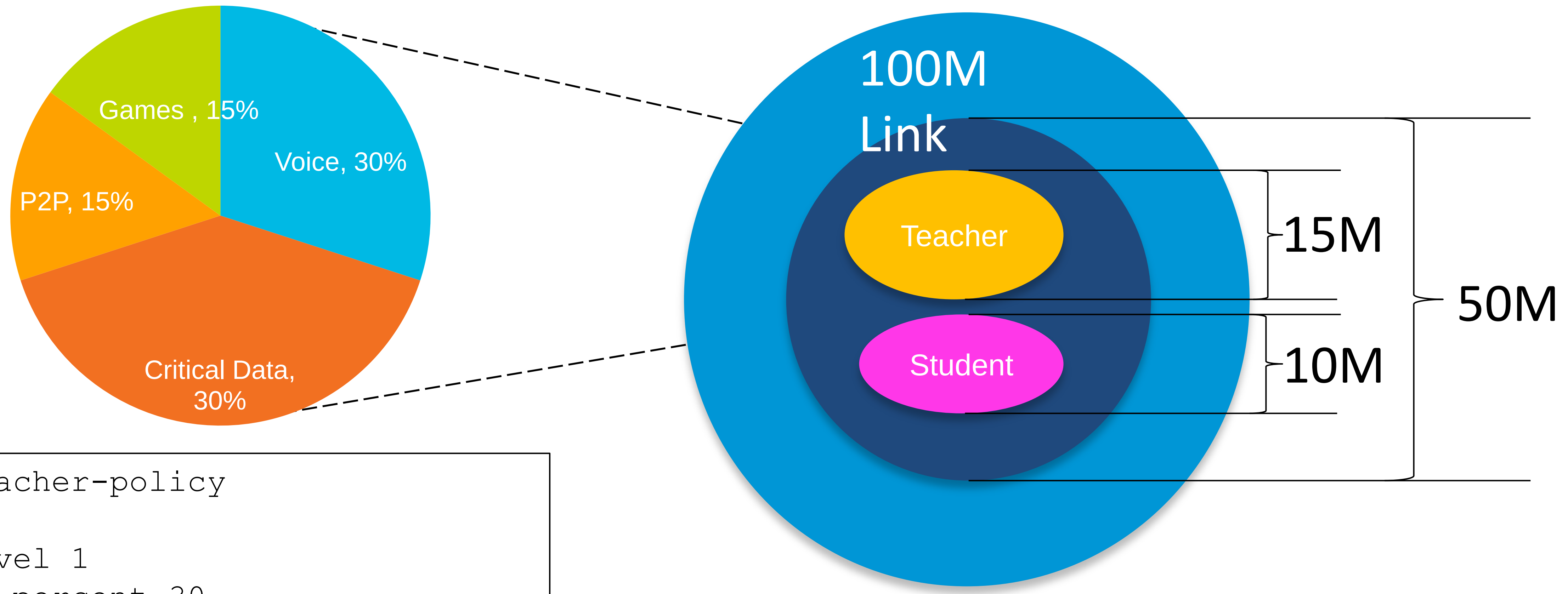


Critical Apps Performance
After apply control policy



```
class-map match-any p2p-app
 match protocol dht
 match protocol attribute sub-category p2p-file-transfer
policy-map control-policy
 class p2p-app
  police 8000 conform-action transmit exceed-action drop
```

How to Partition and Guarantee Application BW

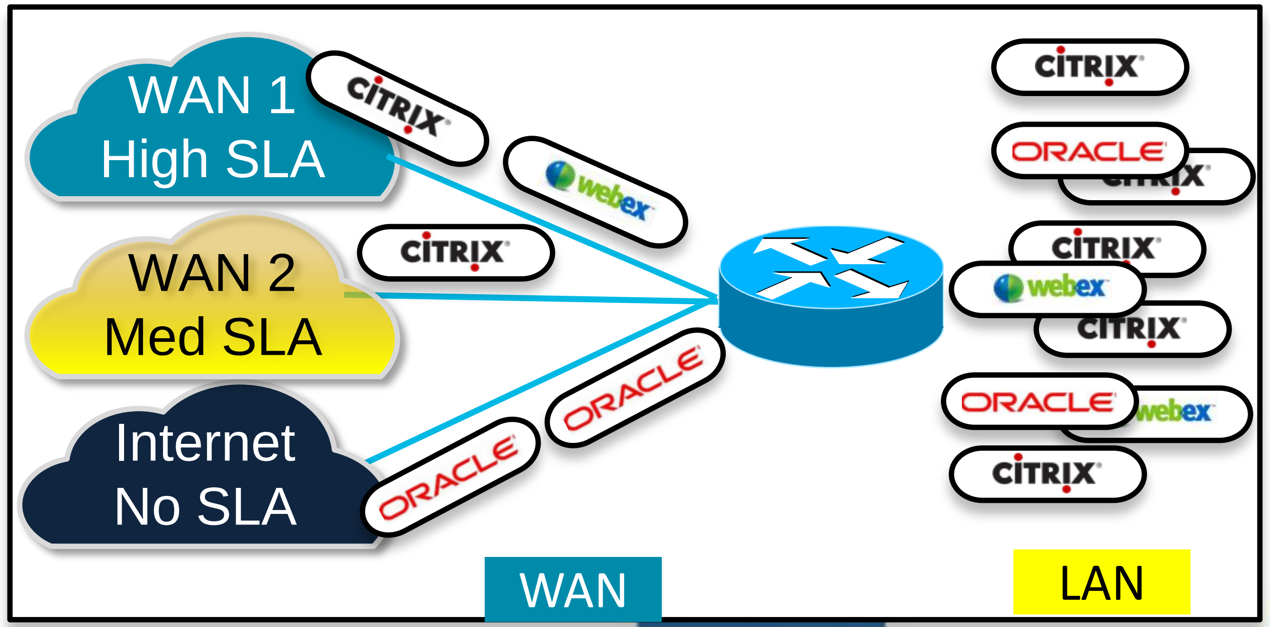


```
policy-map teacher-policy
 class voice
  priority level 1
  police rate percent 30
 class critical-data
  bandwidth percent 30
  fair-queue
 class games
  bandwidth percent 15
  fair-queue
 class p2p
  bandwidth percent 15
  fair-queue
 class class-default
  bandwidth percent 10
```

```
policy-map HQoS_Parent_1
 class class-default
  shape average 50000000
   service-policy HQoS_Per_Branch
policy-map HQoS_Per_Branch
 class teacher
  shape average 15000000
   service-policy teacher-policy
 class student
  shape average 10000000
   service-policy student-policy
```

Application Path Control

PfR



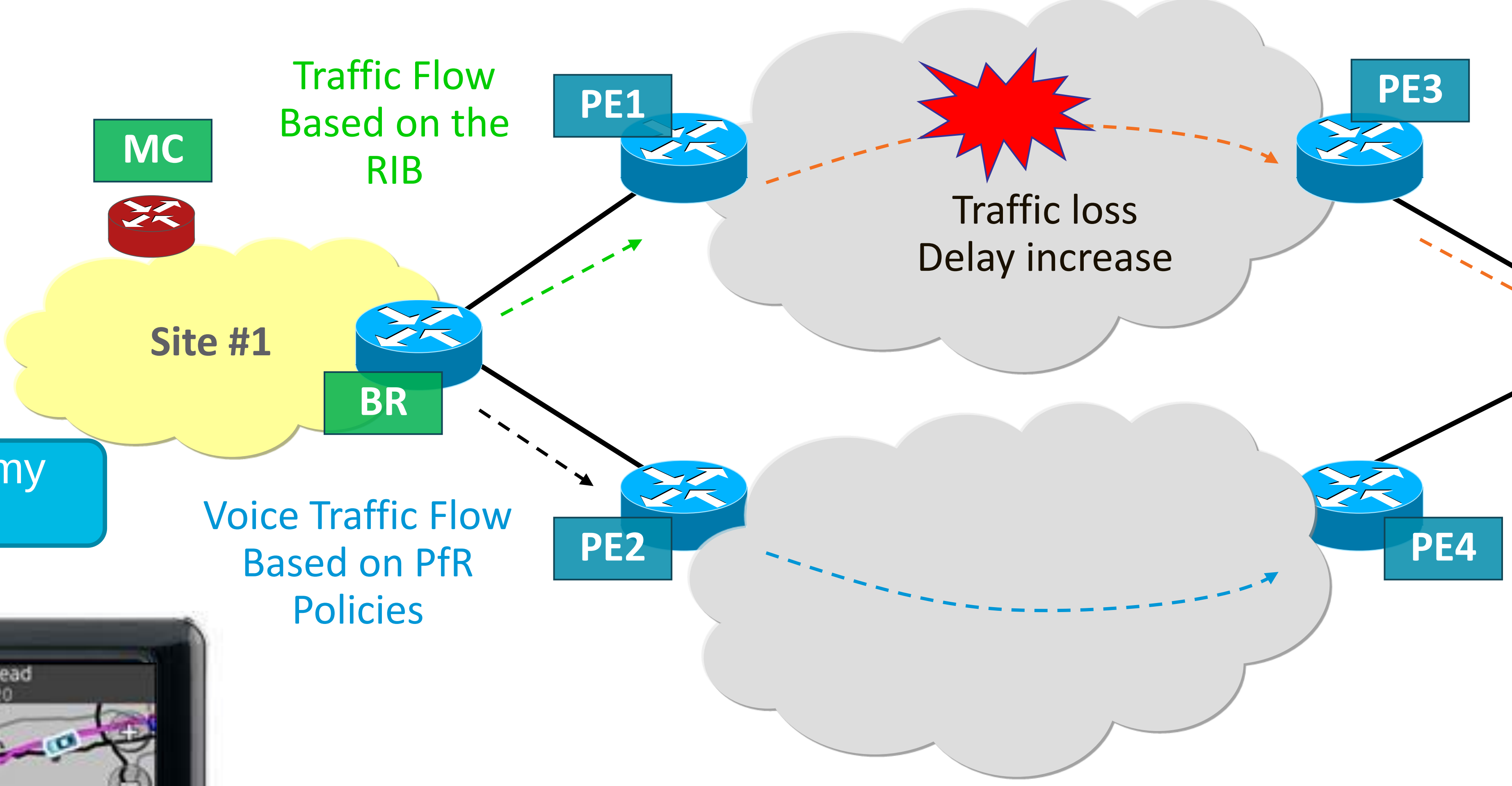
Control Application Path with PfR

- Per application load balancing and path selection beyond shortest path, i.e. link utilisation, latency, jitter, MOS

Route Preference

○ Faster Time
● Shorter Distance
○ Less Fuel
○ Off Road

Which way should I go


MC
Traffic Flow Based on the RIB
PE1
PE3
Traffic loss
Delay increase
Site #1
BR
Site #2
MC/BR
Voice Traffic Flow Based on PfR Policies
PE2
PE4

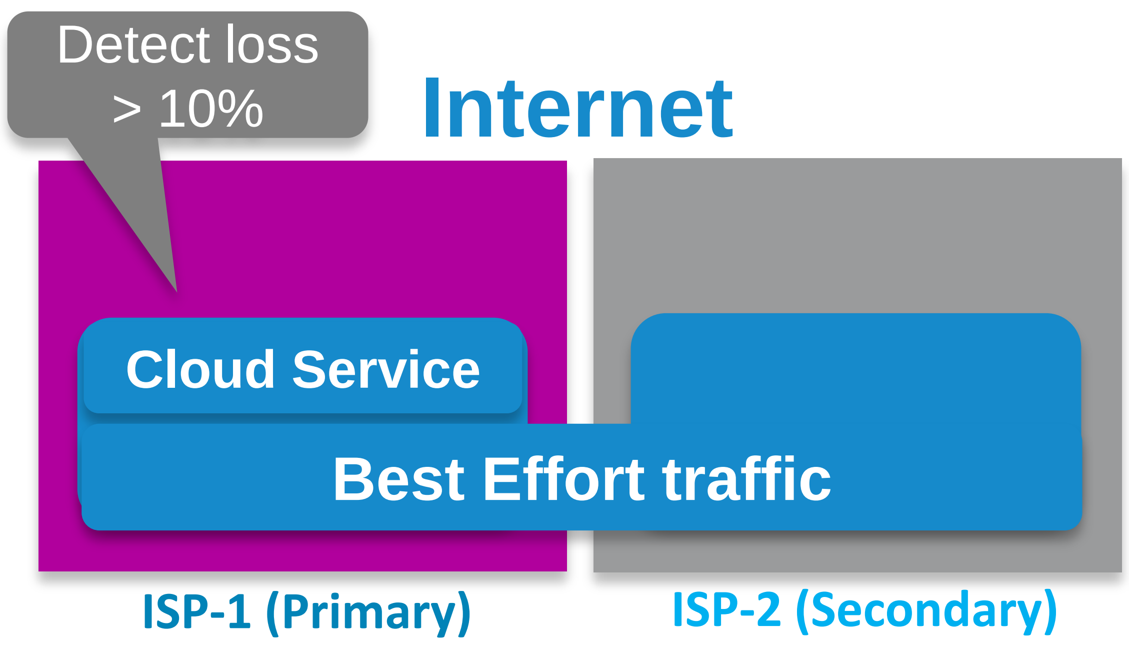
How is traffic on my route?

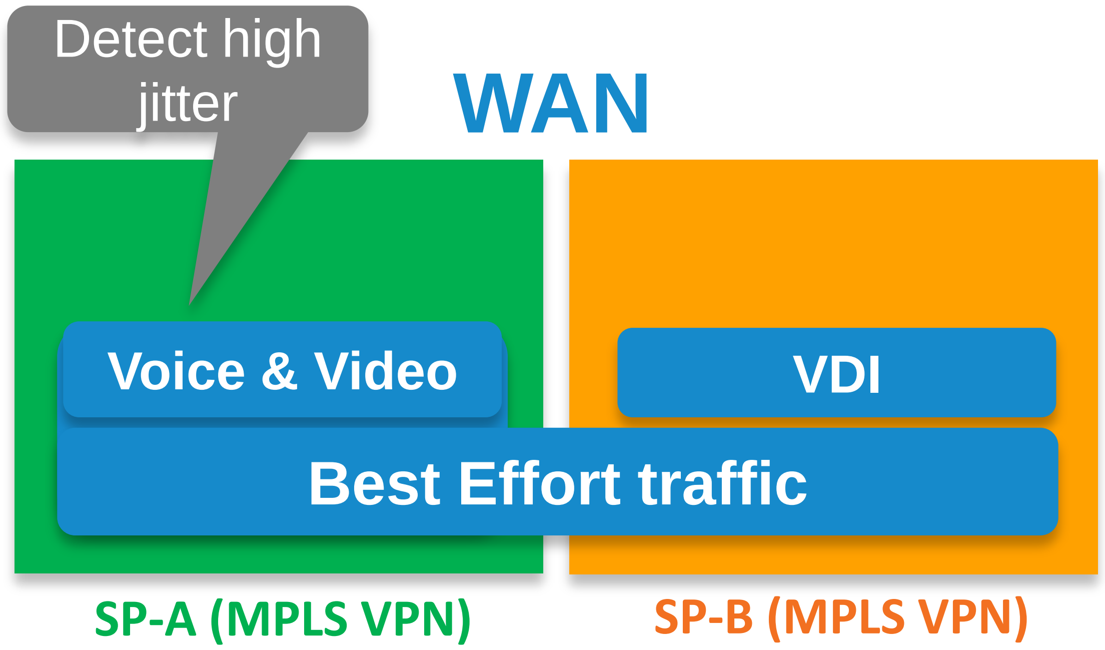
16 min delay 25 mi ahead
I-90 Westbound at US-20

- Collect real-time performance information for making path selection, i.e. route around congested link or network

PfR Use Case Examples

Protecting critical applications while maximising bandwidth utilisation





Cloud Service & Load Balancing Policy

- Protect business Cloud applications from Internet brownout, Loss <10%
- Cloud Service preferred path – ISP1
- Maximise all ISP bandwidth by load sharing all other Internet traffic

Multimedia & Critical Data Policy

- Protect voice and video quality, Latency < 200ms; Jitter < 30ms
- Protect VDI applications from brownouts, i.e. Loss < 5%
- Voice & Video preferred path SP-A
- VDI preferred path SP-B
- Maximise utilisation by load sharing

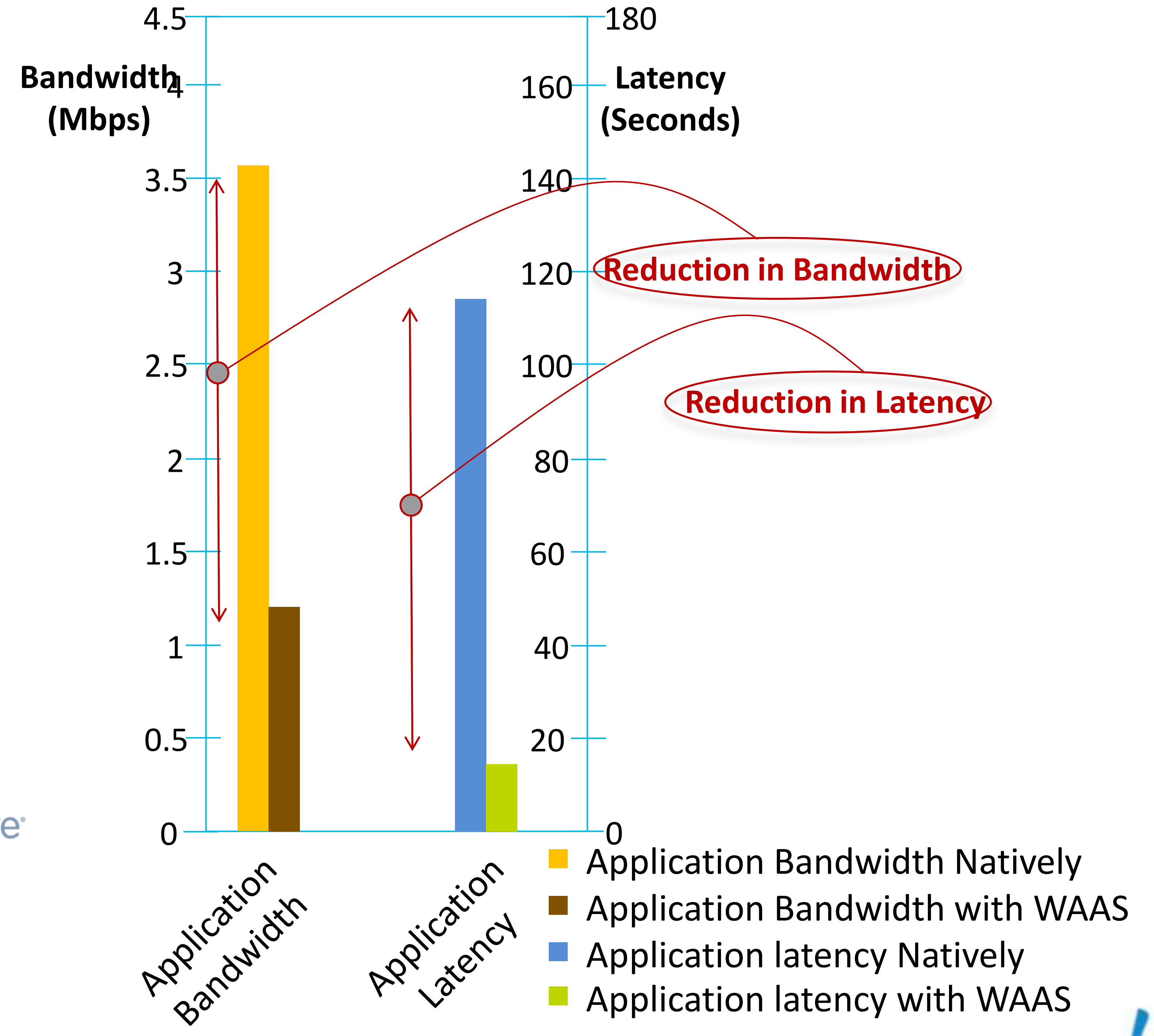
AVC & WAAS Design Consideration

Cisco WAAS

Enhancing User Experience and WAN Efficiency

Problem
- Application latency
- WAN Bandwidth inefficiencies

Solution
- Reduce load
  Data Redundancy Elimination, Compression, TCP optimsation
- Application Optimisation
  fewer protocol messages, Meta data caching, ...



Microsoft Office

Microsoft SharePoint

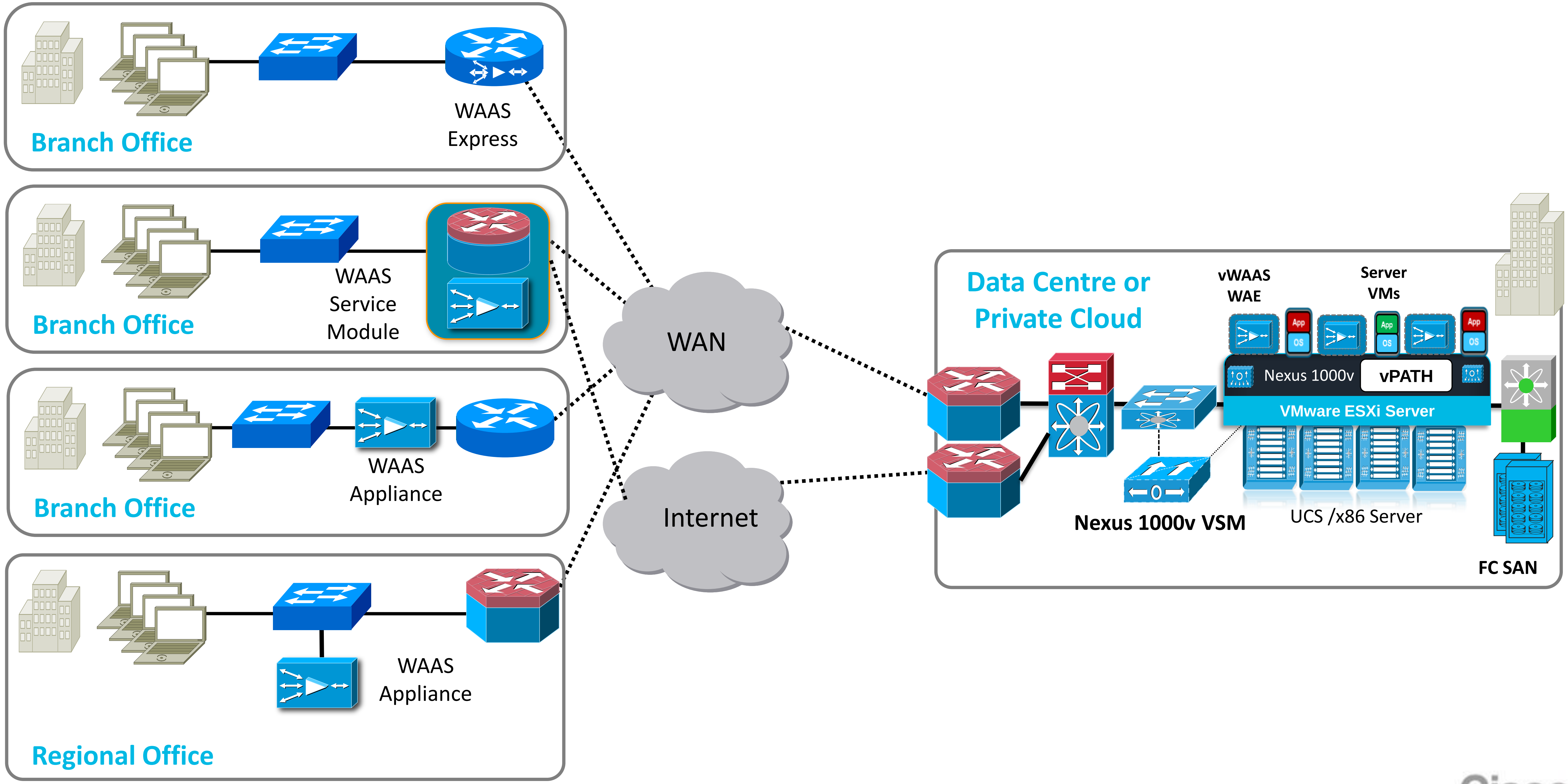
vmware

CITRIX

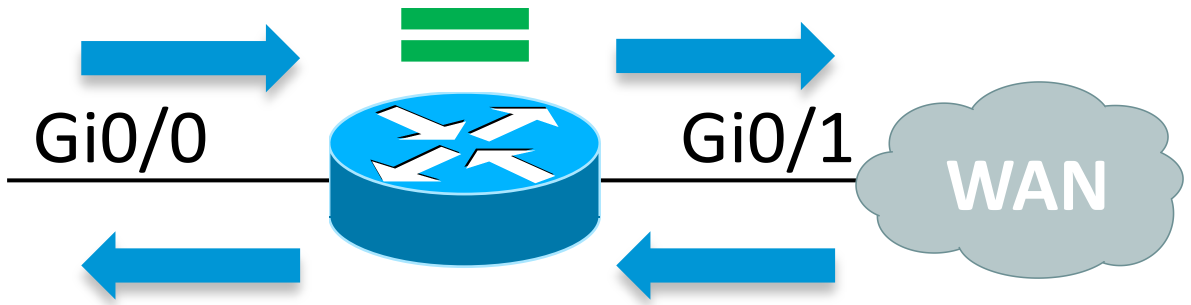
SAP

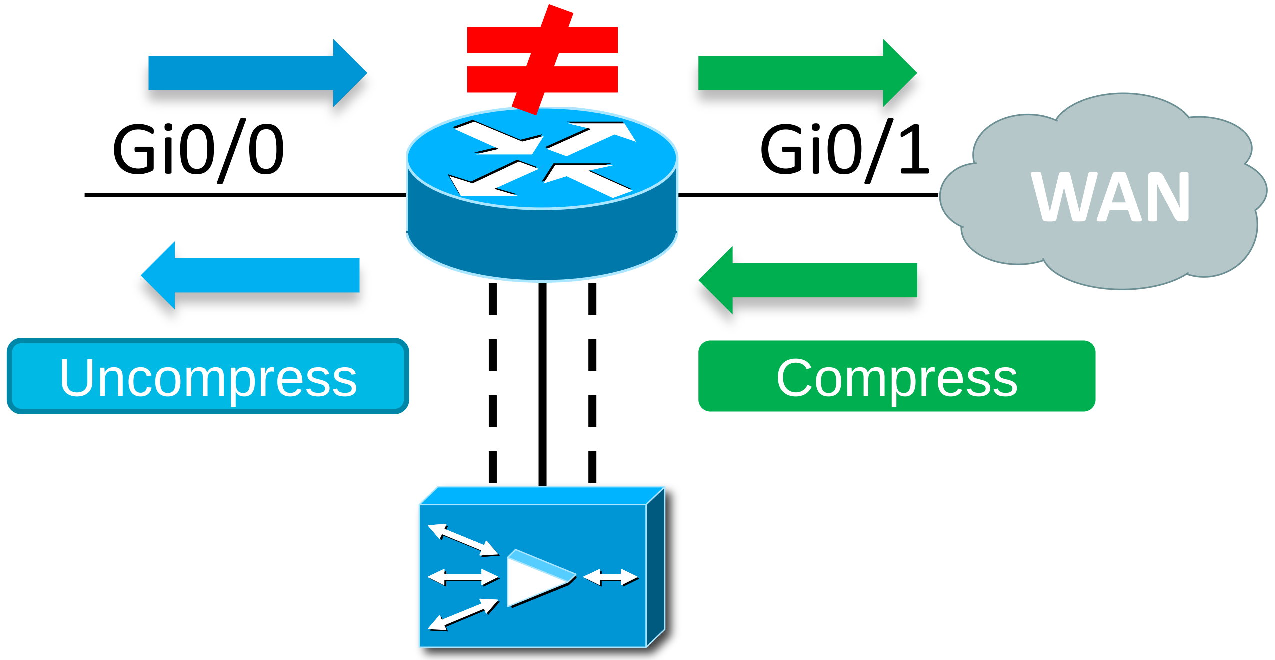
webex

Cisco WAAS: WAN Optimisation Solution



Traffic Visibility Through FNF with WAAS





Before WAAS

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

After WAAS (with offpath redirection)

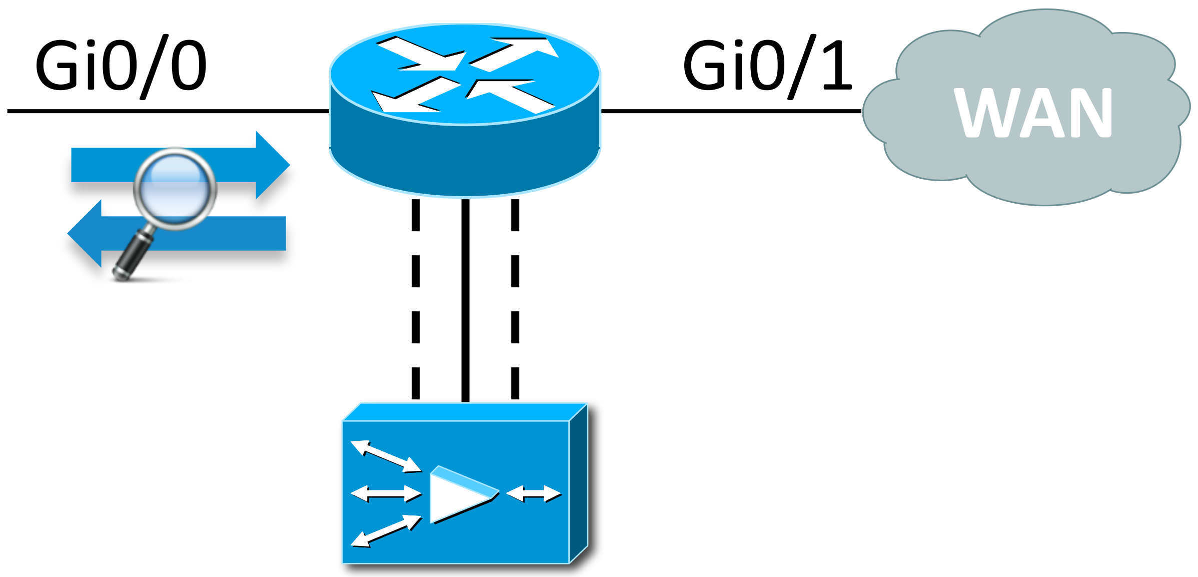
- Ingress FNF on all interfaces will give wrong results

  LAN in traffic > WAN out traffic

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

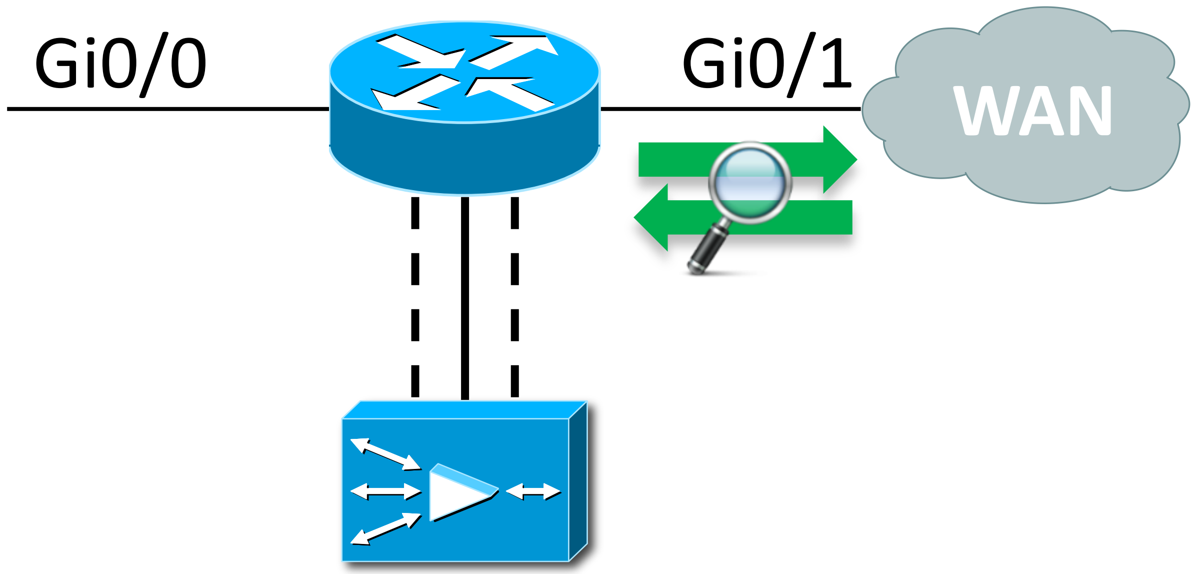
Traffic Visibility Through FNF with WAAS

Deployment Option



FNF Applied on the LAN

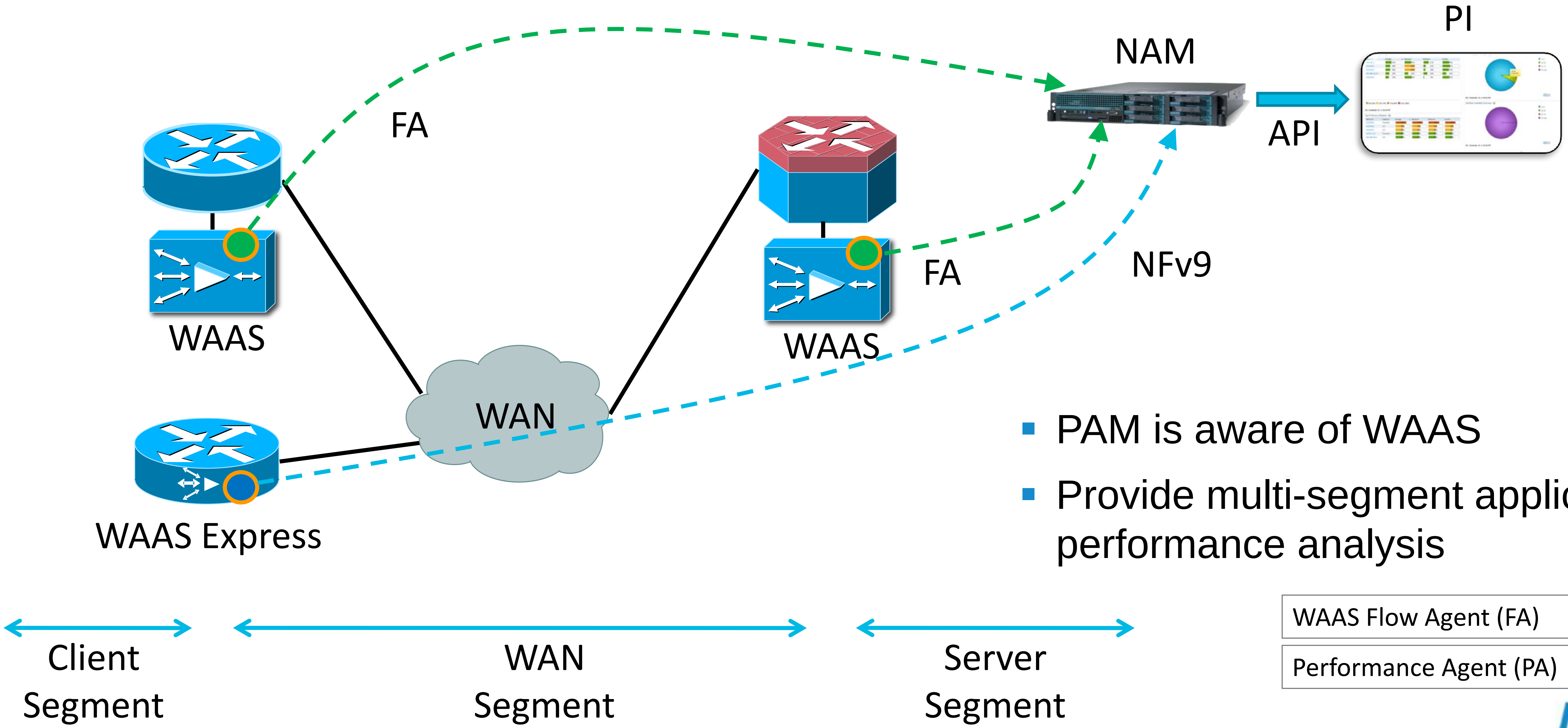
- Collect uncompressed traffic bandwidth and top talkers
- Allow NBAR2 to provide application name



FNF Applied on the WAN

- Collect compressed traffic bandwidth and top talkers
- Do not use NBAR2 on the WAN

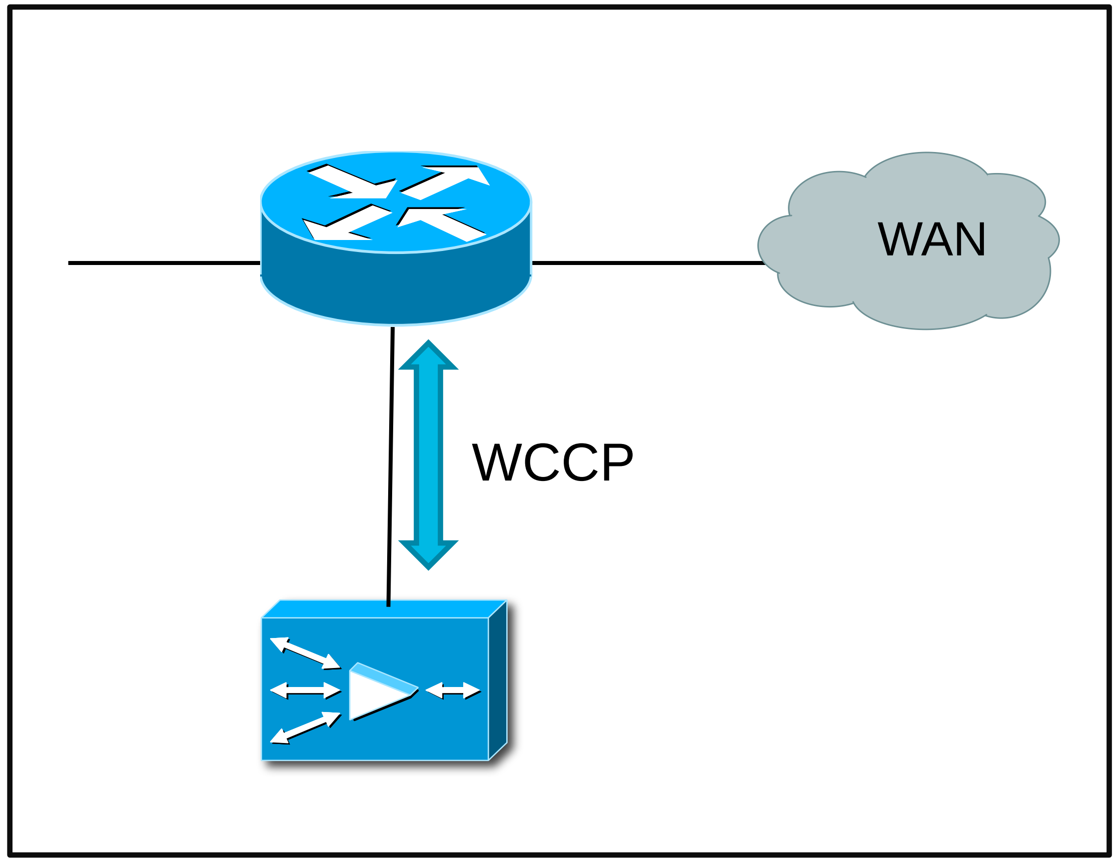
Monitor TCP Performance with WAAS Deployment

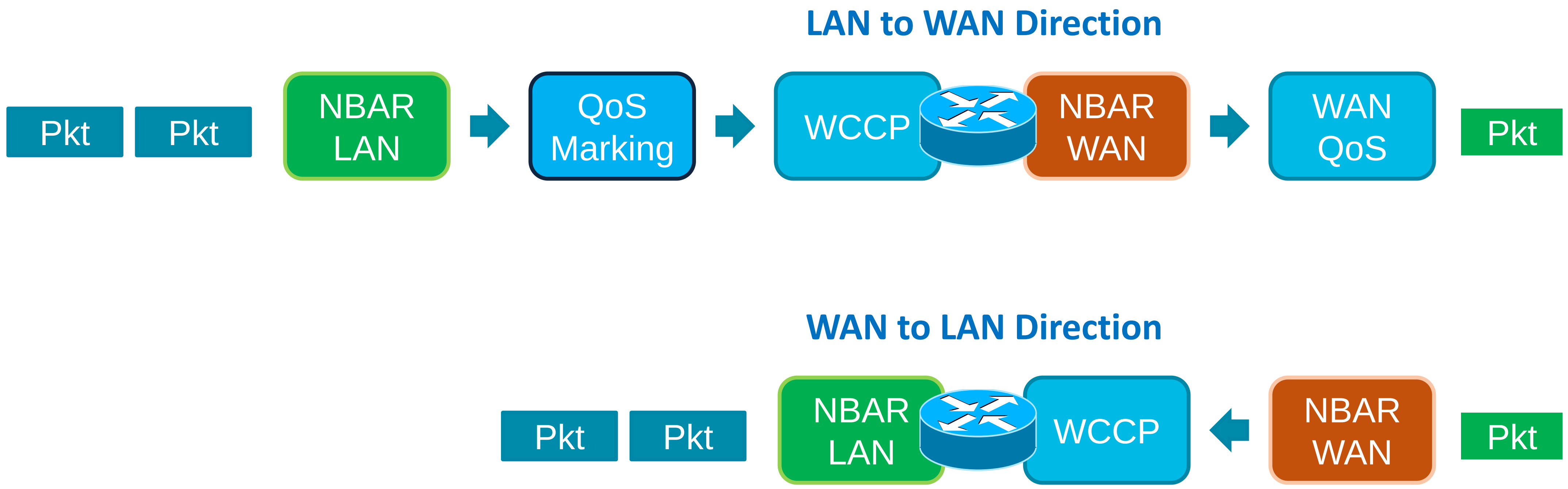


- PAM is aware of WAAS
- Provide multi-segment application performance analysis

WAAS Flow Agent (FA)	🟢
Performance Agent (PA)	🔵

WAN Optimisation Packet Path with WCCP





LAN to WAN Direction

Pkt → Pkt → NBAR LAN → QoS Marking → WCCP → NBAR WAN → WAN QoS → Pkt

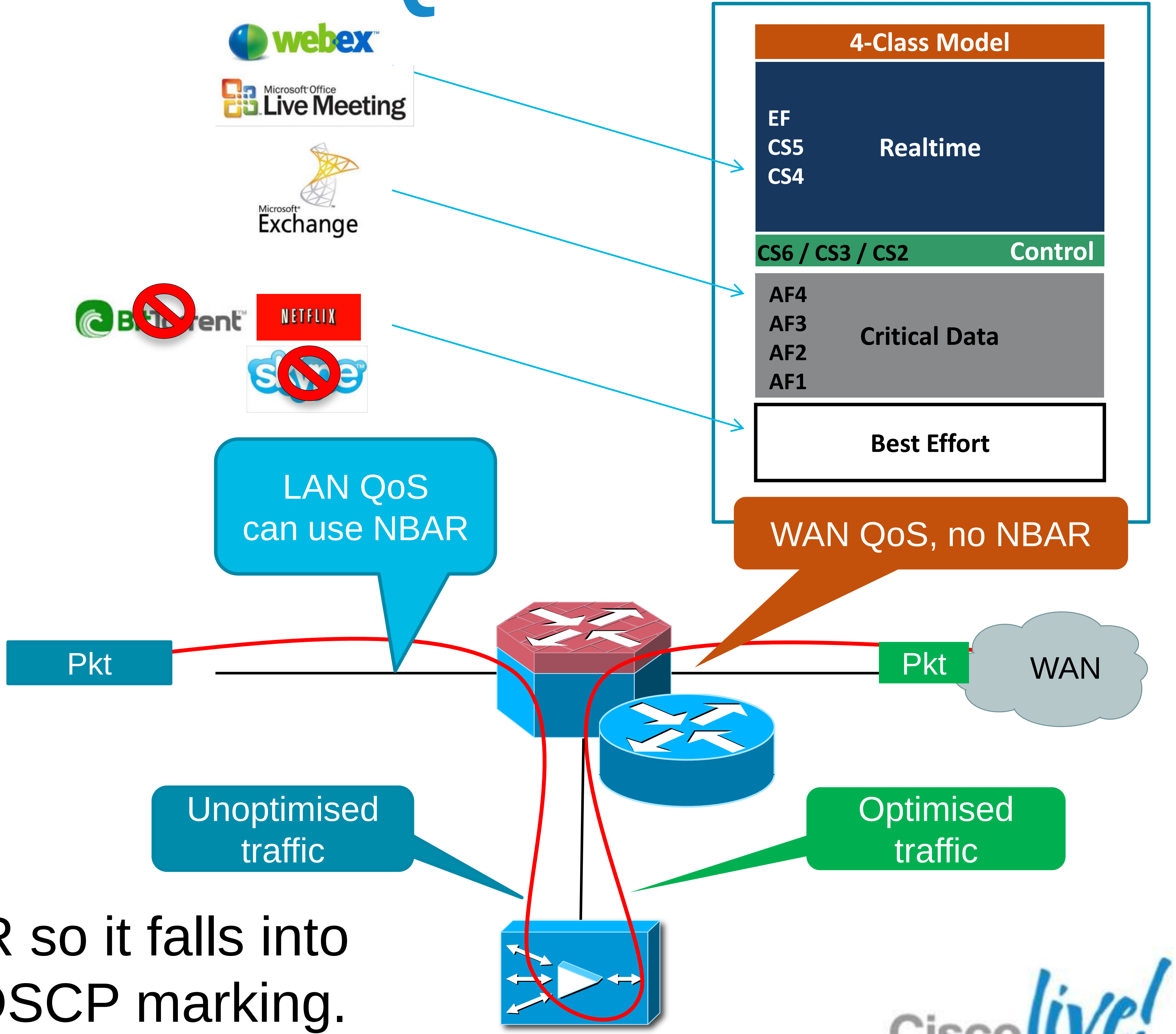
WAN to LAN Direction

Pkt ← Pkt ← NBAR LAN ← WCCP ← NBAR WAN ← Pkt

- 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?

Enabling Application-aware QoS with WAAS

```
class-map match-any cloud-collaboration-app
 match protocol webex-meeting
 match protocol livemeeting
class-map match-any enterprise-app
 match protocol exchange
class-map match-any recreational-app
 match protocol attribute sub-category streaming
class-map match-any unwanted-app
 match protocol skype
 match protocol attribute application-group
bittorrent-group
policy-map lan-remark
 class cloud-collaboration-app
  set dscp cs4
 class enterprise-app
  set dscp af41
 class recreational-app
  set dscp 0
 class unwanted-app
  drop
interface GigabitEthernet0/0
 service-policy input lan-remark
```



- Mark traffic on the LAN using NBAR so it falls into the right queue. WAAS preserves DSCP marking.

What you Need to Enable PfR + WAAS

- When WCCP session is established between router and WAAS, tunnel interfaces are created
- PfR requires defining ‘internal’ and ‘external’ interfaces

```
router#show tunnel groups
2 tunnel groups active
 WCCP : service group 317 in "Default", ver v2,
assgnmnt: mask-value set
   intf: Tunnel0, locally sourced
 WCCP : service group 318 in "Default", ver v2,
assgnmnt: mask-value set
   intf: Tunnel2, locally sourced
```

```
pfr master
 border 192.168.254.2 key-chain pfr-keychain
  interface GigabitEthernet0/2 external
   max-xmit-utilization percentage 80
   link-group secondary
  interface GigabitEthernet0/1.34 internal
  interface GigabitEthernet0/1.32 internal
  interface Tunnel0 internal
  interface Tunnel2 internal
```

Add both interfaces as PfR internal interfaces

Summary

Key Takeaways

- Classification
  - NBAR2 is the next generation DPI
  - Leave the application classification tasks to the network
- Monitoring and Traffic Analysis – FNF, MMON, and ART
  - Allow proactive monitoring and accelerate troubleshooting
  - Open export format – NFv9 and IPFIX
  - FNF: The monitoring foundation
  - MMON: Engine which provides native RTP Analysis (refer to as Medianet perf-mon)
  - ART: Engine which provides TCP Performance
- Management
  - Cisco Prime Infrastructure
  - 3rd Party Support starts and more is coming
- Control
  - NBAR2 makes QoS application-aware
  - Performance Routing (PfR)

So Far, You Have Seen…

- What is AVC and why it is important
- How do we make use of AVC to provide better visibility and control of applications in your network
- Deep dive of some of the technologies used by AVC

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 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 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww