ManageEngine
Powering IT ahead

CISCO

QoS Design and Validation for Enterprise Networks

Cisco and ManageEngine Joint Webinar on designing and validating Quality of Service policies in Enterprise Networks

Ken Briley
Technical Lead, Cisco Systems

Don Thomas Jacob
Technical Marketing Engineer, ManageEngine

ZOHO

About ManageEngine

ManageEngine

Network	Servers & Applications	Desktop	ServiceDesk	Windows Infrastructure	Event Log & Compliance	Security
Network Monitoring	Server Monitoring	Desktop Management	Helpdesk	Active Directory	Windows Event Logs	Vulnerability Analysis
NetFlow Analysis	Application Perf Monitoring	Asset Management	ITIL Service Desk	SQL Server	Syslog Management	Patch Management
Network Config Mgmt	End User Experience	Remote Control	Software License Tracking	Exchange Server	Firewall Log Analyzer	Password Management

ManageEngine is an IT management vendor focused on bringing a complete IT management portfolio to all types of enterprises

Webinar Agenda

- Introduction to QoS
  - What is QoS
  - The Need for QoS
- QoS in detail - Ken Briley, Technical Lead, Cisco Systems.
- QoS reports in ManageEngine NetFlow Analyzer

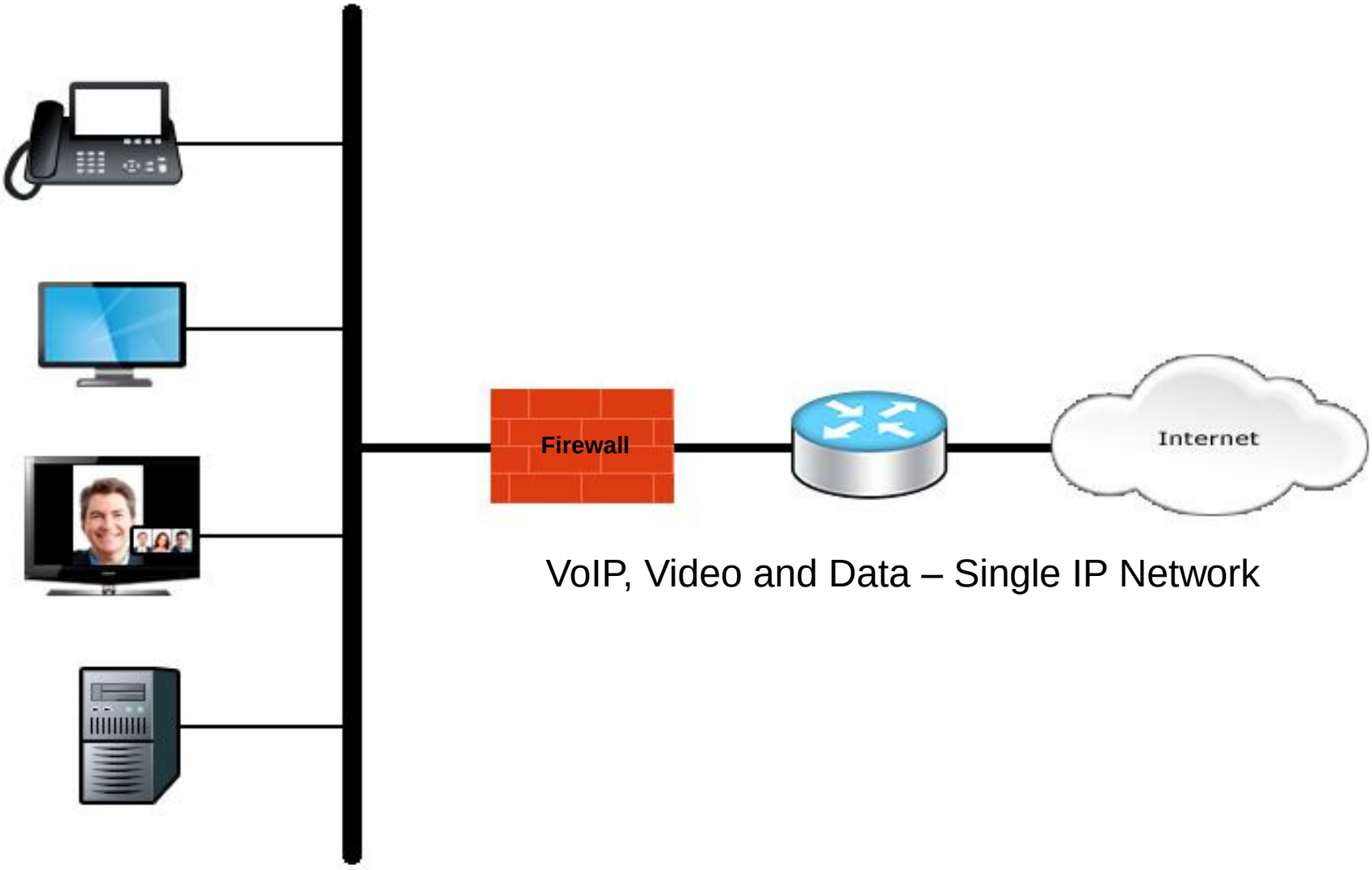
What is QoS

What is QoS

- Variety of traffic traverses the network
- You may have preference for certain type of traffic over the other – eg. ‘Business Critical’ vs ‘Other Traffic’
- A method to Optimize and Prioritize traffic on the network based on your key objectives
- Ensures delivery of business critical & delay sensitive applications at all times

The Need for QoS

Converged networks



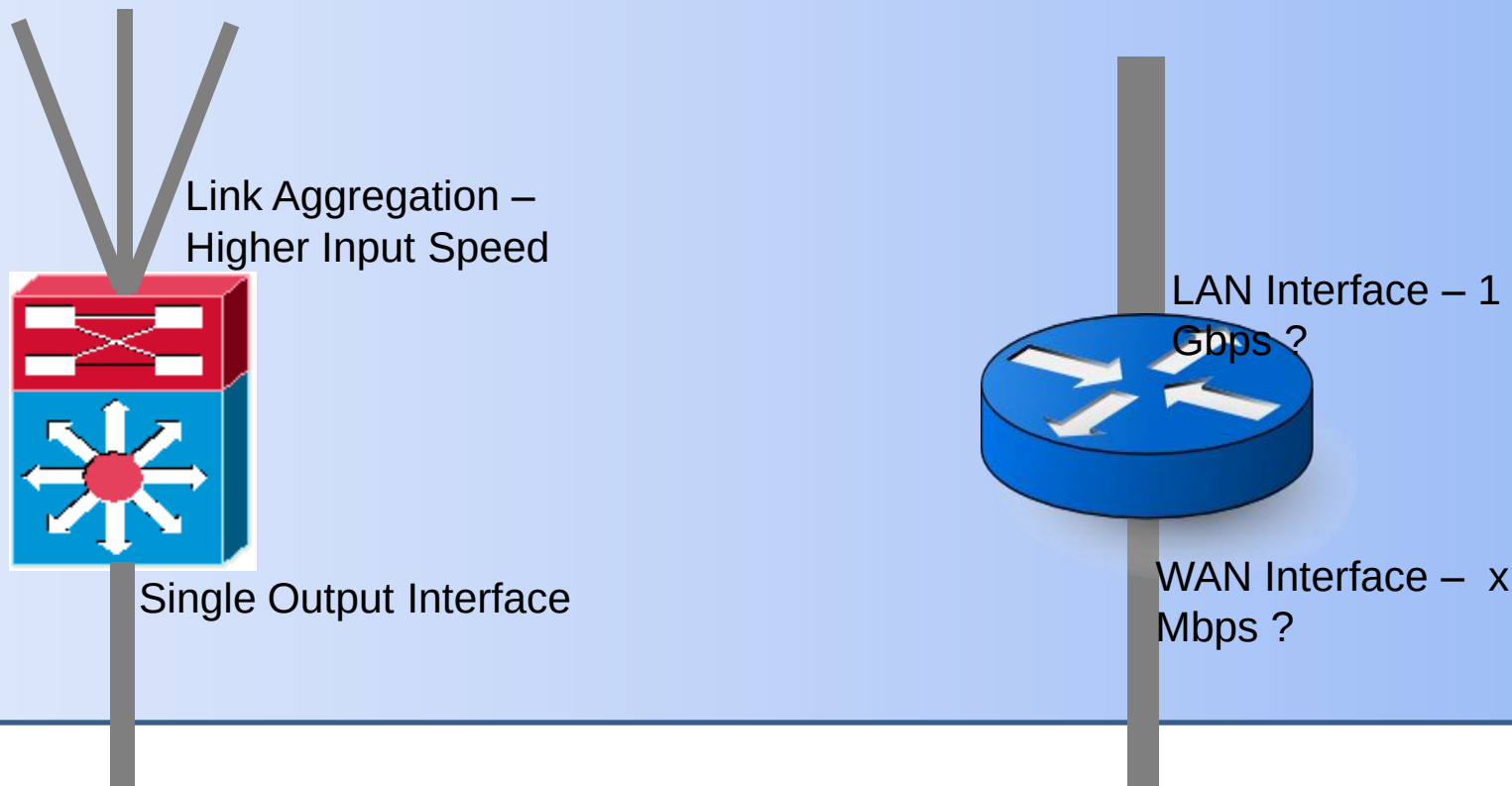
VoIP, Video and Data – Single IP Network

Converged networks

- Different traffic types: Data, Voice, Video - Same IP network
- All traffic comes under the Best Effort: Equal chance of being delivered or dropped
- Business Critical Applications fight with applications that should have fallen under lesser priority
- App segregation through QoS for priority treatment

Congestion Points

- IP Networks are bound to have Congestion Points
  - LAN to WAN connections: High Speed to Low Speed
  - Multiple Input Links (Aggregation) to Single Output Link

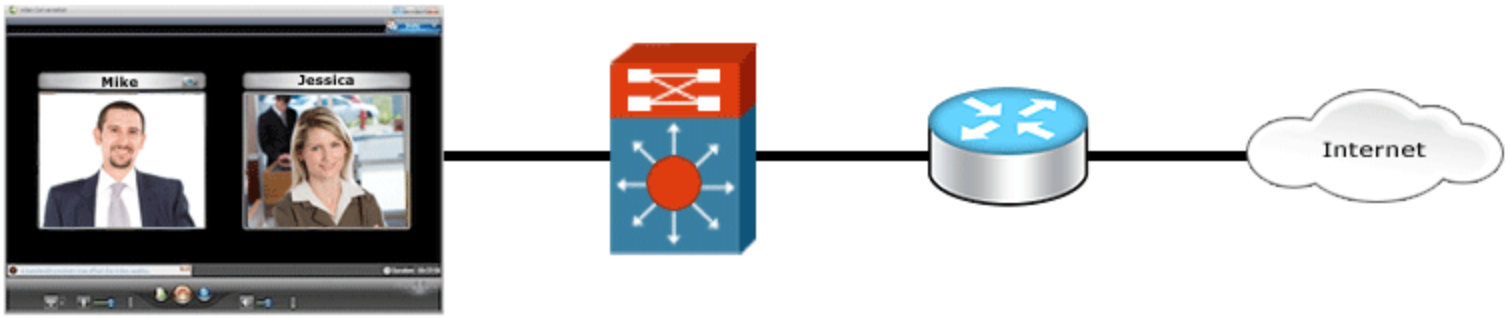


Congestion Points

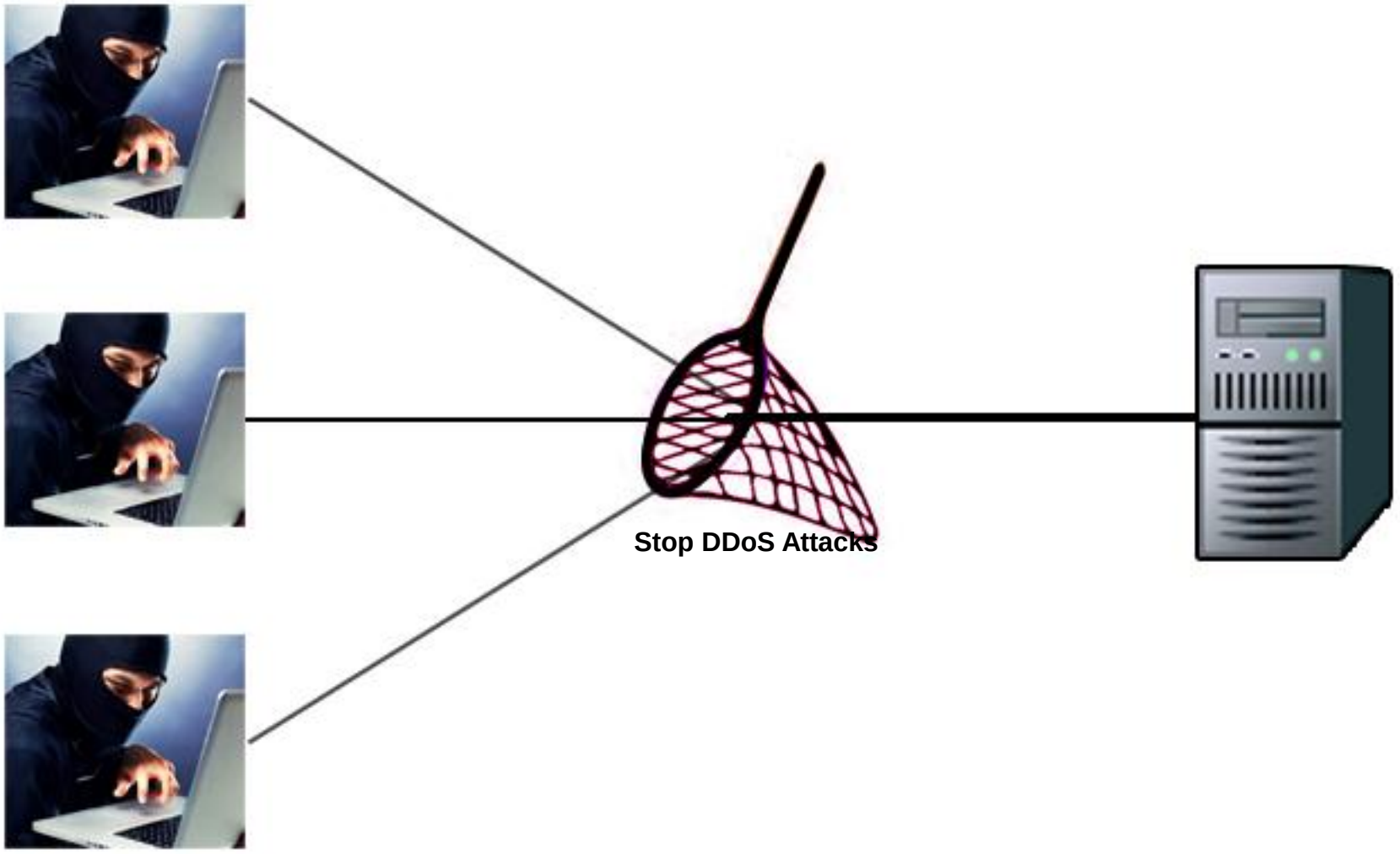
- IP Networks are bound to have Congestion Points
  - LAN to WAN connections: High Speed to Low Speed
  - Multiple Input Links (Aggregation) to Single Output Link
- Traffic can get dropped in such scenarios
- Have control on what data is dropped and where and how it is dropped

Delay Sensitive Application Delivery

- Increased usage of IP based Voice and Video for business communication
- IP based Media Traffic: Sensitive to delay and packet loss
- Ensure Delay-Sensitive applications get priority as and when needed



Mitigate DoS attacks

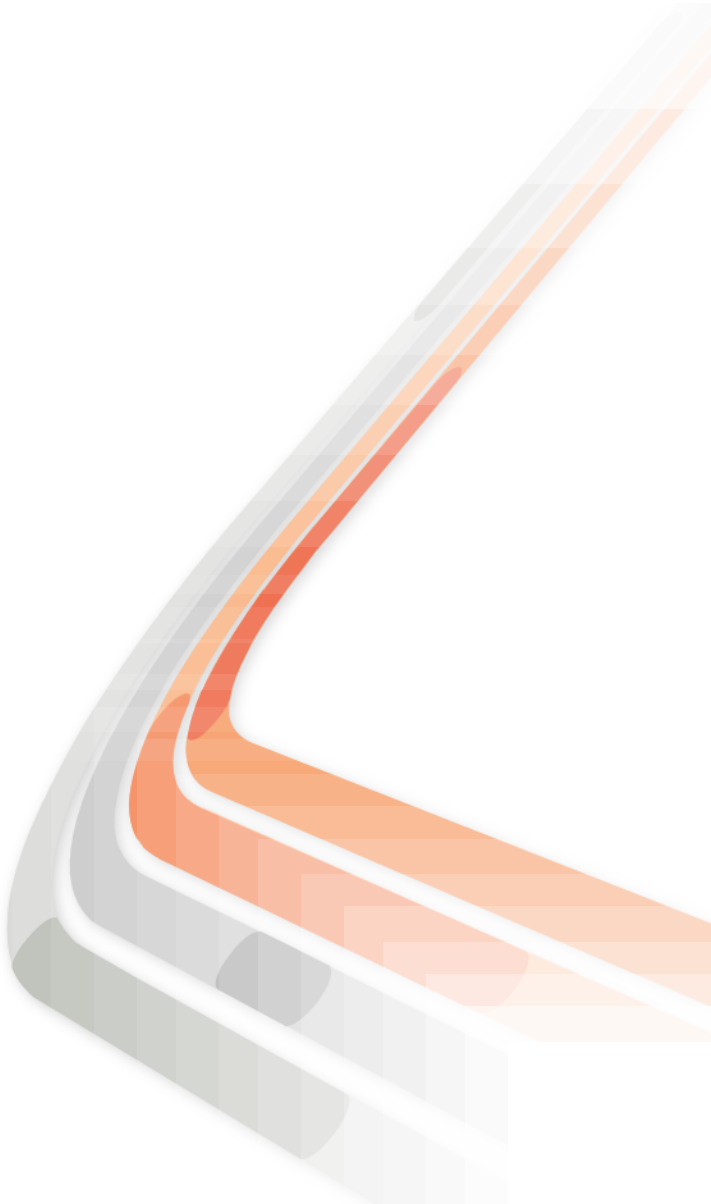


Mitigate DoS attacks

- DoS Attack - Consume resources to deny legitimate service requests
- Resource regulation ensures a resource is not over utilized by a single type of traffic
- Putting non-business applications in Scavenger Class prevents resource utilization in case of actual DoS attack
- Cisco CAT 6500 supports Microflow policing: Police traffic for each port/VLAN on a per flow basis

QoS in Detail

Enterprise QoS Design



Agenda

- Why QoS?
- QoS Design Considerations
  - Classification and Marking
  - Policing
  - Queueing
- Application Control
  - Campus
  - WAN
- Visibility and Monitoring QoS

Why QoS?
Business and Technical Drivers

- New Applications and Business Requirements
  - Explosion of Video Apps
  - Impact of HD
  - Blurring of Voice/Video/Data application boundaries
- New Standards and RFCs
  - RFC 4594
- New Platforms and Technologies
  - New Switches, Supervisors, Linecards, features, syntax

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp60730

New Business Requirements

Why Video?

A picture is a thousand words, Video says it all

"In person" experience

64% of communication is non-verbal[1]

One third of the human cortex is dedicated to vision[2]

[1]Kandola, Pearn "*The Psychology of Effective Business Communications in Geographically Dispersed Teams",* Cisco Systems, September 2006

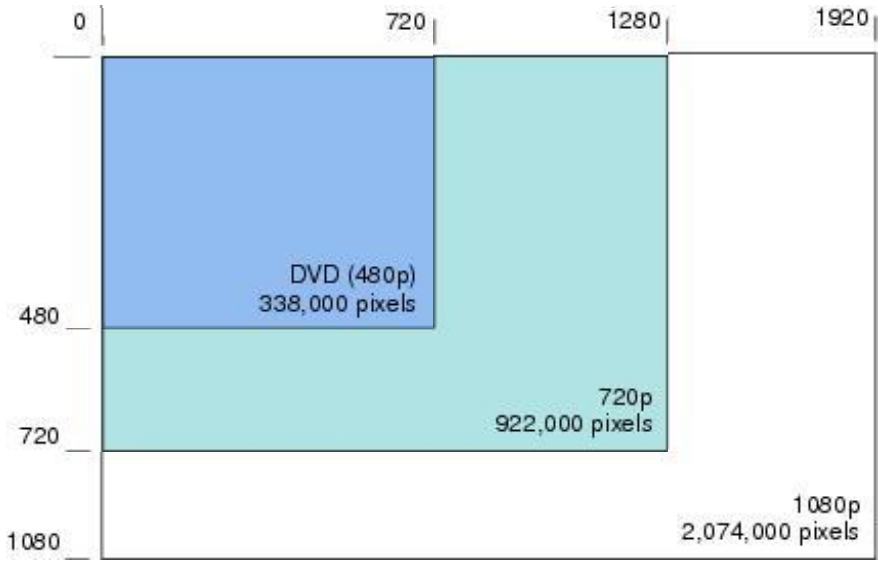
[2]Vision Group Research, FMRIB, University of Oxford, UK

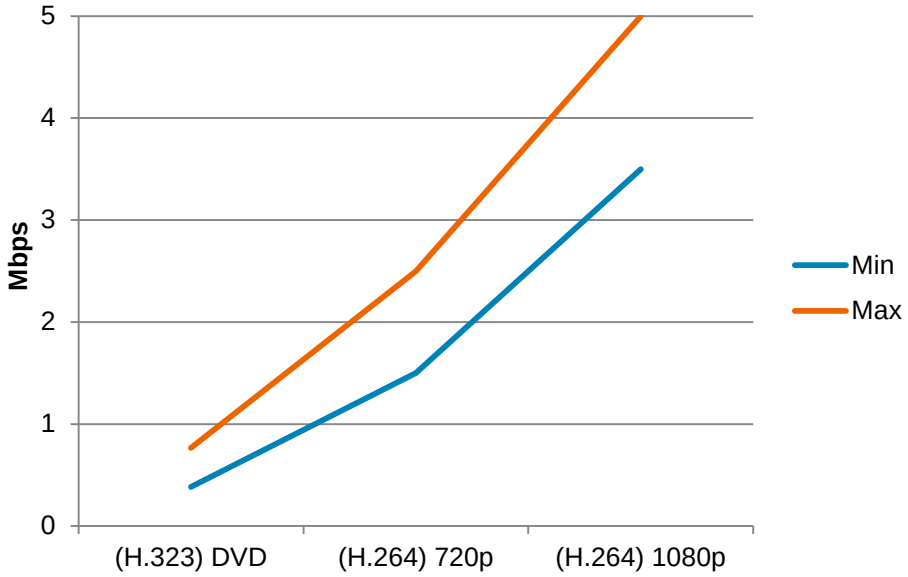
New Business Requirements
Cisco Visual Networking Index Findings

- **Global IP traffic will quadruple from 2009 to 2014.**
- **Global Internet video traffic will surpass global peer-to-peer (P2P) traffic by the end of 2010**. For the first time since 2000, P2P traffic will not be the largest Internet traffic type.
- **The global online video community will surpass 1 billion users by the end of 2010**.
- **Internet video is now over one-third of all consumer Internet traffic, and will approach 40 percent of consumer Internet traffic by the end of 2010**, not including the amount of video exchanged through P2P file sharing.
- **The sum of all forms of video (TV, video on demand, Internet, and P2P) will exceed 91 percent of global consumer traffic by 2014**
- **Advanced Internet video (3D and HD) will increase 23-fold between 2009 and 2014**. By 2014, 3D and HD Internet video will comprise 46 percent of consumer Internet video traffic.
- **Video communications traffic growth is accelerating**. Video communications traffic will increase sevenfold from 2009 to 2014.
- **Real-time video is growing in importance**. By 2014, Internet TV will be over 8 percent of consumer Internet traffic, and ambient video will be an additional 5 percent of consumer Internet traffic.
- **Video-on-demand (VoD) traffic will double every two and a half years through 2014**. Consumer IPTV and CATV traffic will grow at a 33 percent CAGR between 2009 and 2014.

http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.html

New Application Requirements
The Impact of HD on the Network





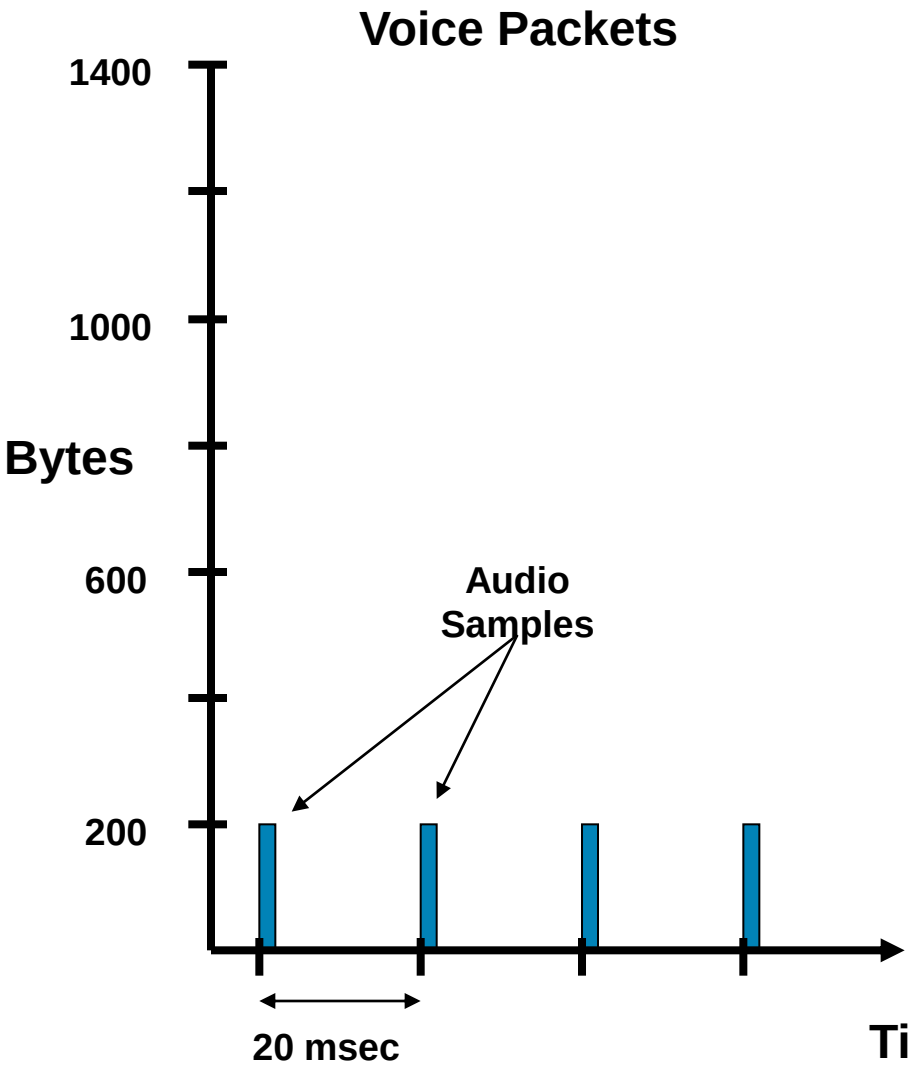
- User demand for HD video has a major impact on the network

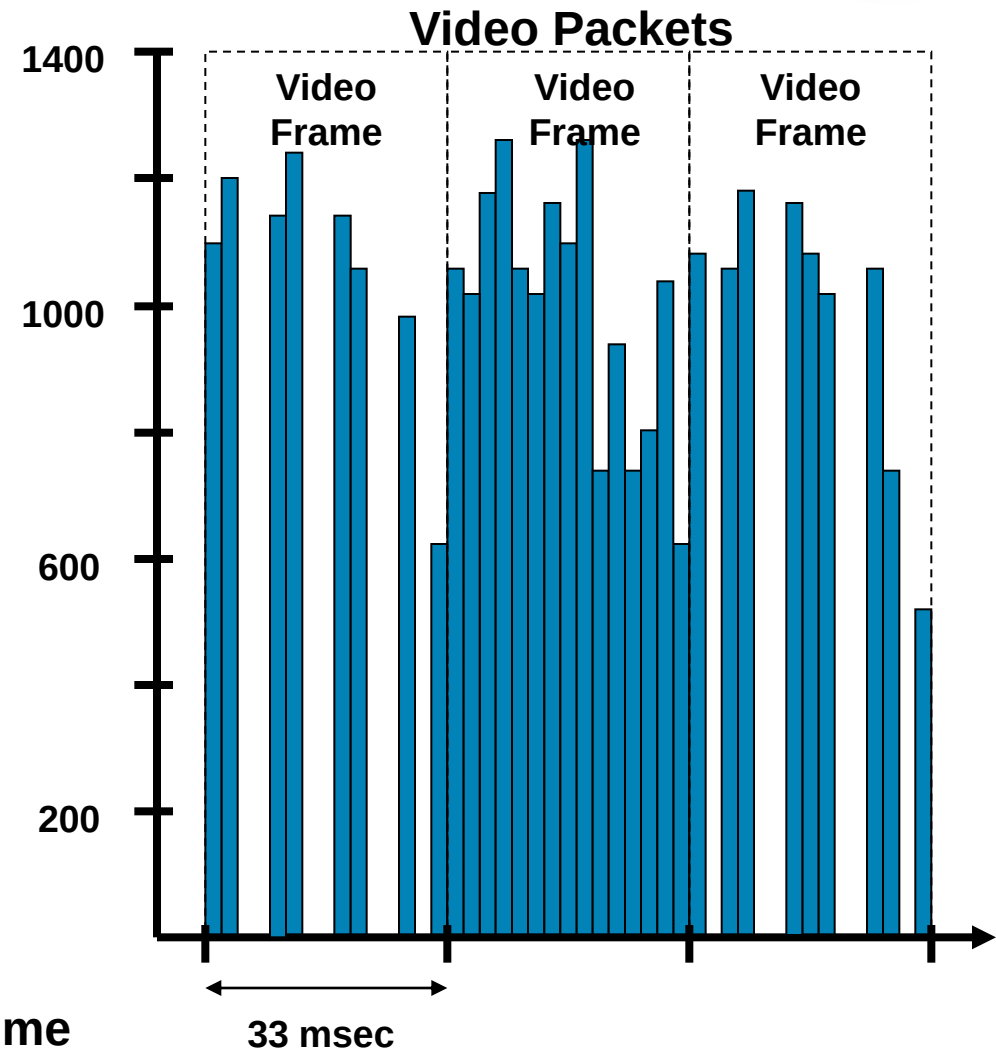
  (H.264) 720p HD video requires twice as much bandwidth as (H.323) DVD

  (H.264) 1080p HD video requires twice as much bandwidth as (H.264) 720p

New Applications Requirements

VoIP vs. HD Video—At the Packet Level



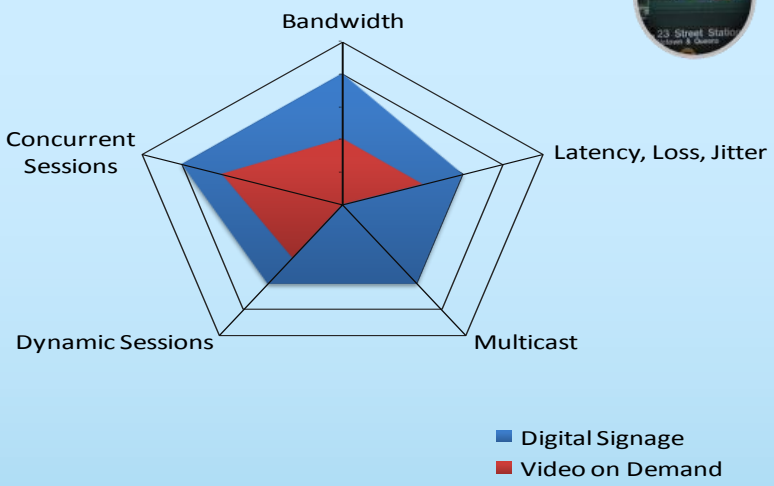


Time

New Application Requirements

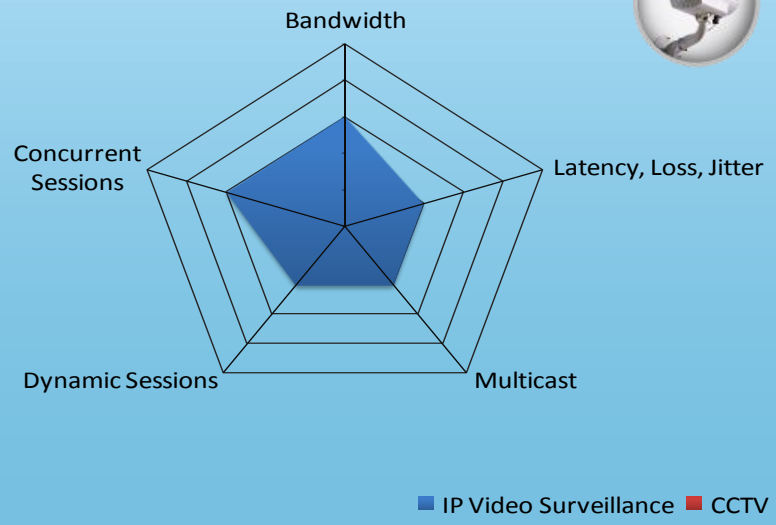
Provisioning for Video: One Size Does Not Fit All

Streaming Digital Media

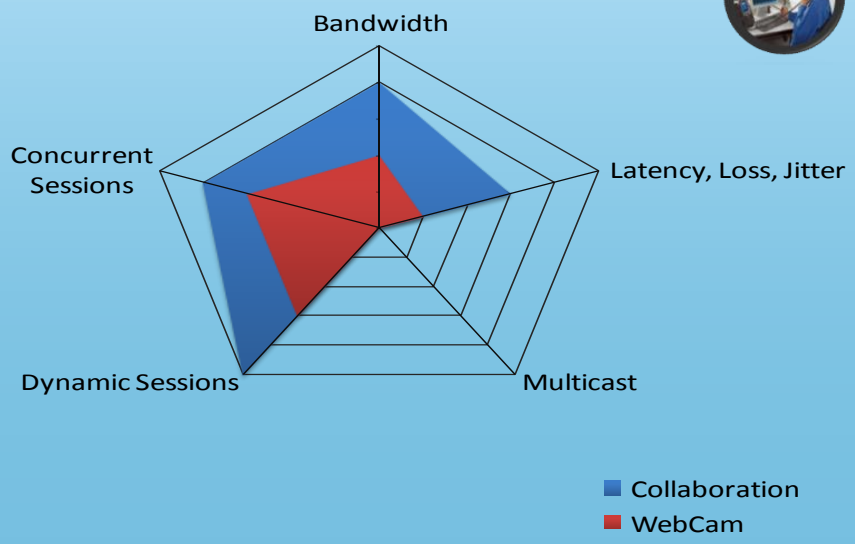


Telepresence

IP Video Surveillance

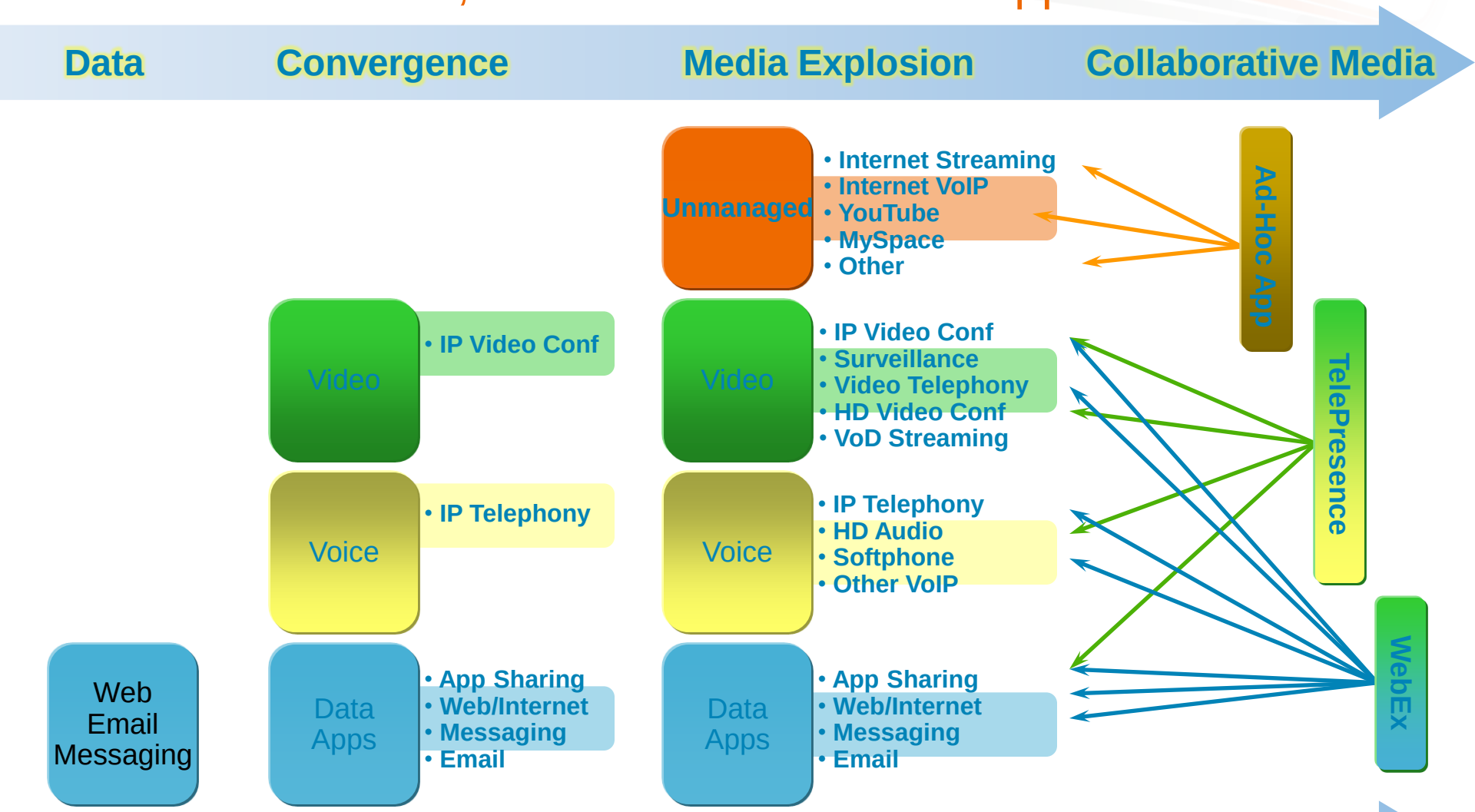


Desktop Collaboration



New Application Requirements

Trends in Voice, Video and Data Media Applications



New Standards and RFCs

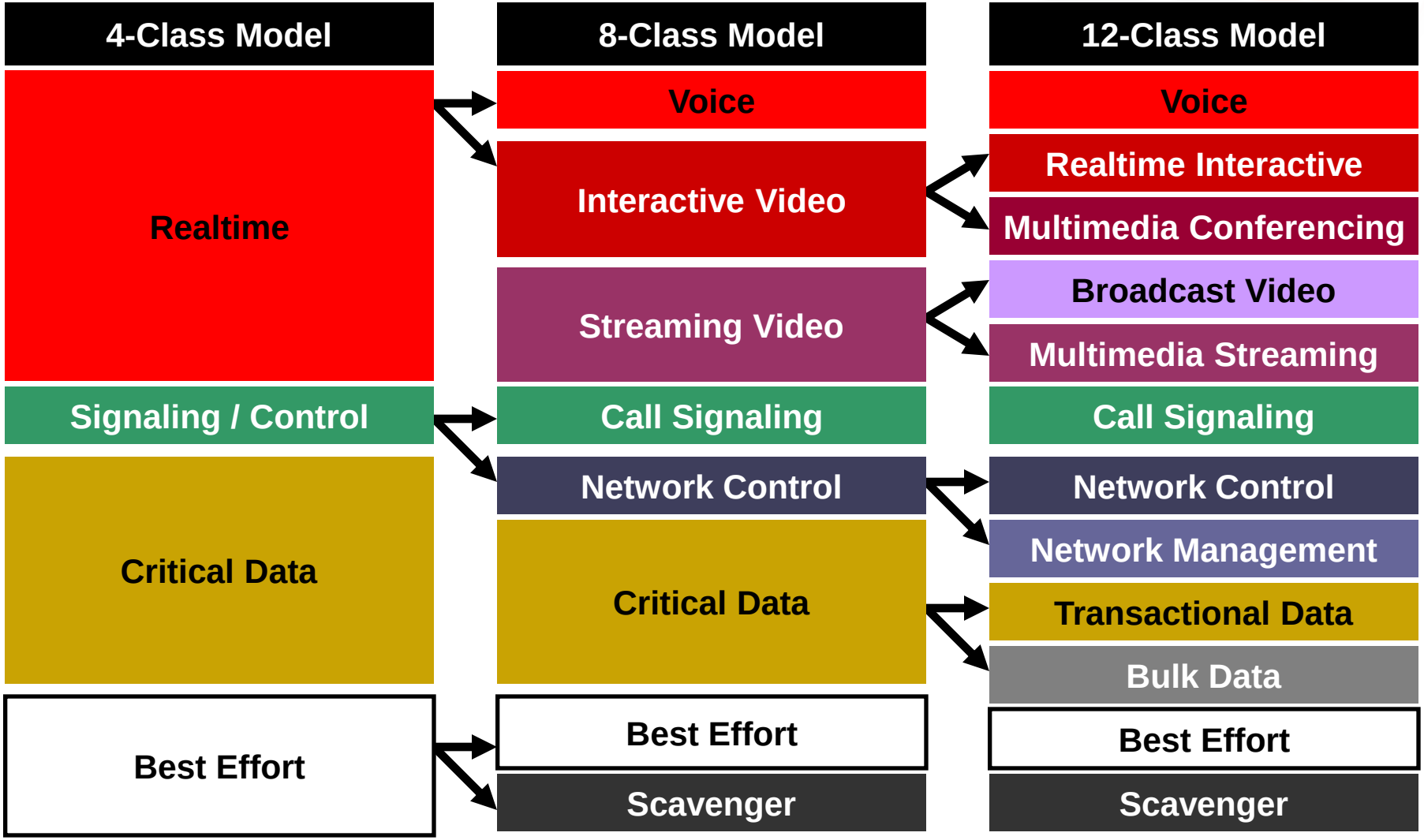
Cisco Medianet DiffServ QoS Recommendations (RFC 4594-Based)

Application Class	Per-Hop Behavior	Admission Control	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	Required	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Unified Personal Communicator, WebEx
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
Bulk Data	AF1		BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue (Deferential)	YouTube, iTunes, BitTorent, Xbox Live

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61104

Evolving Business Requirements

Business Requirements Will Evolve and Expand over Time

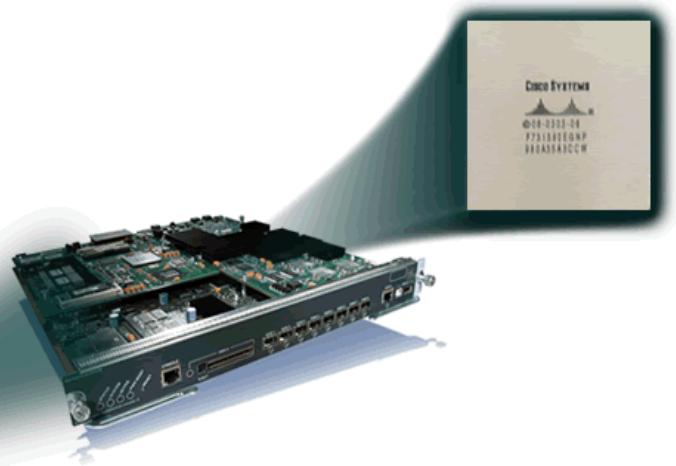


http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61135

QoS Design Considerations

Classification and Marking
How Should It Be Done?

QoS is implemented in Hardware on the Catalyst switching platforms. Depending on the platform, Qos functions may be split across the Supervisor and linecards



QoS features and capabilities could have dependencies on the specific forwarding engine and/or Linecard hardware versions

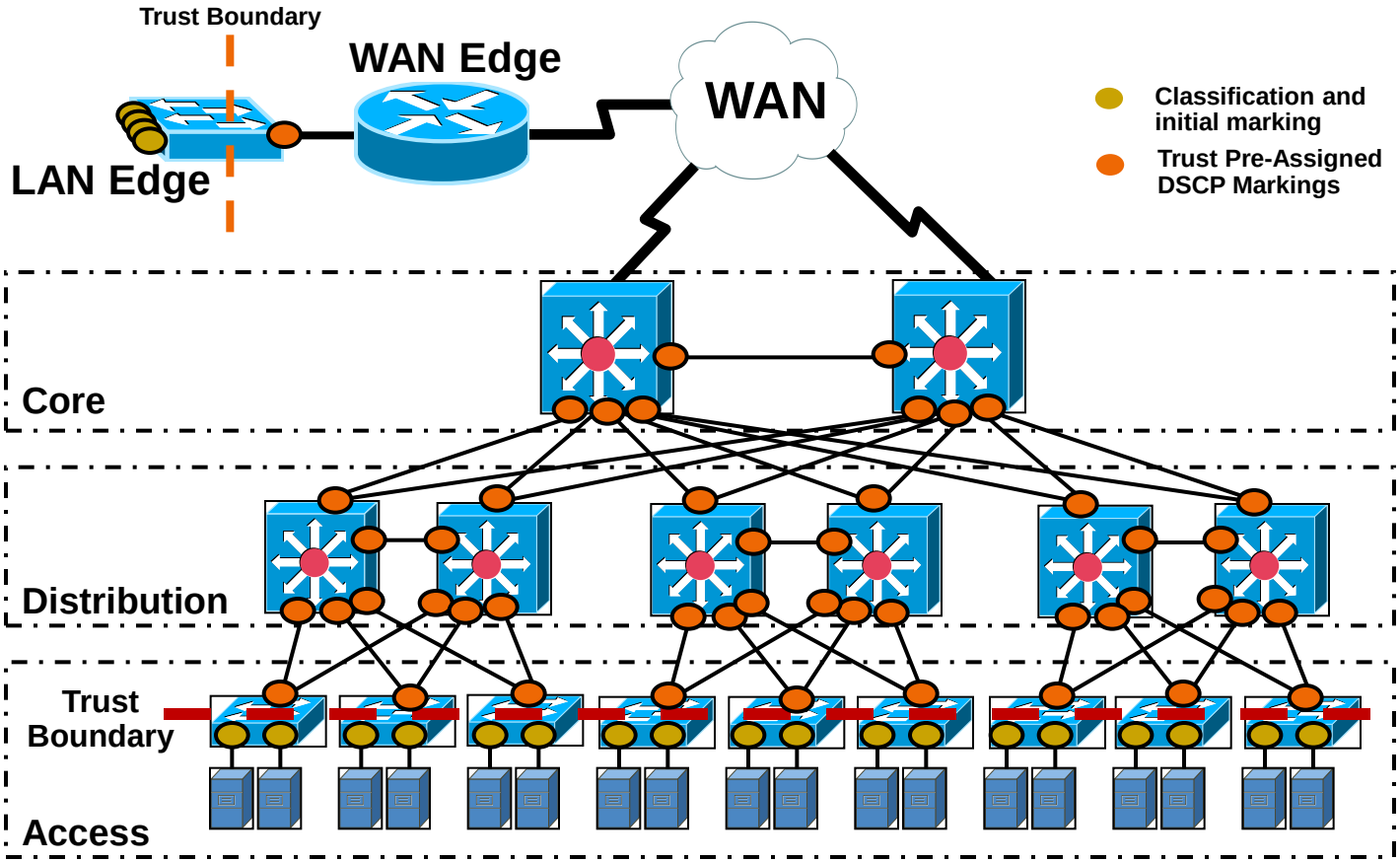
Classification and Marking

Where Should It Be Done?

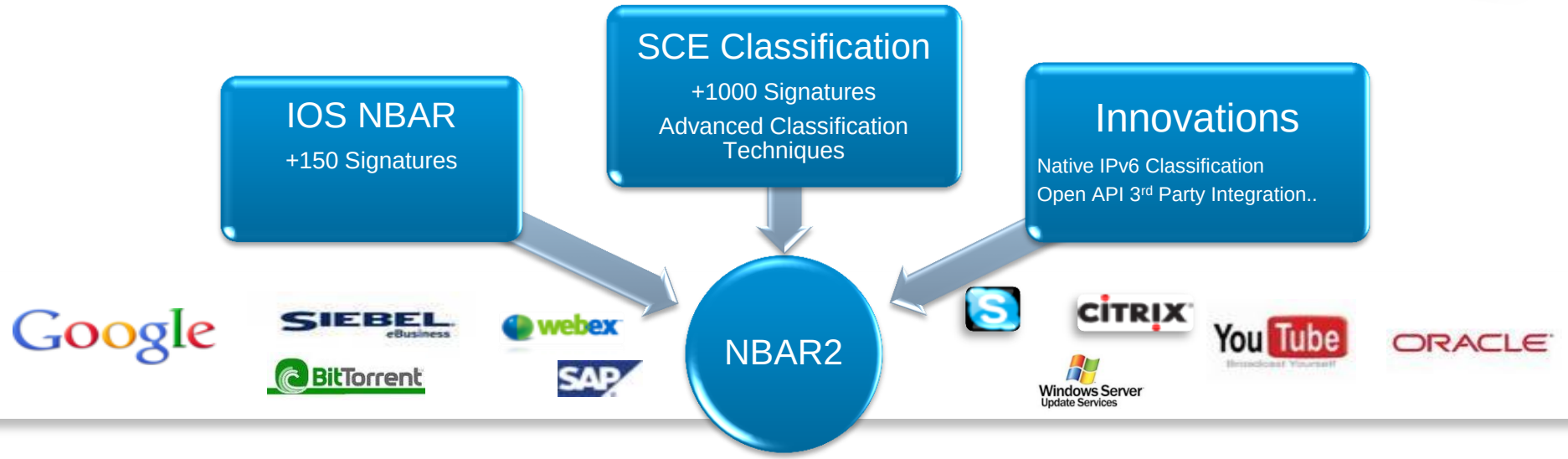
Classification and marking should be performed as close as technically feasible to the sources so that prioritization may be implemented at congestion points throughout the network; DSCP should be used wherever possible…

Subsequent points in the network can now "trust" the marked values and queue based on these baseline values outlined below

Classify and mark traffic at the physical port or VLAN, Queue on uplinks to Distribution

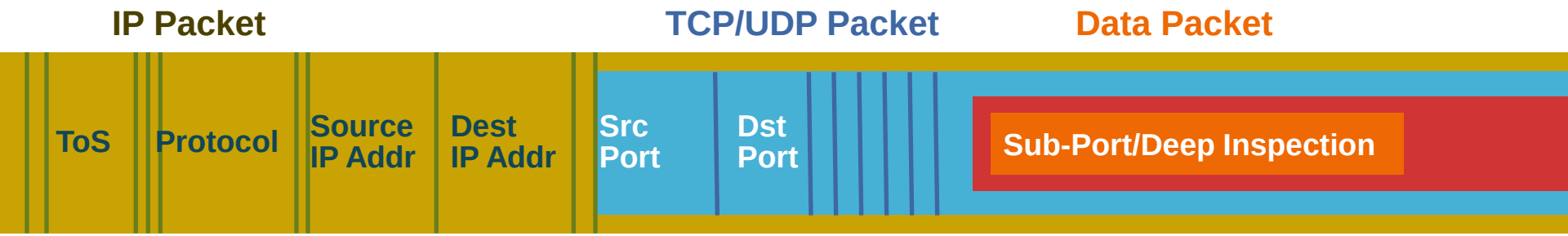


Next Generation NBAR (NBAR2)



- New DPI component which provide Advanced Application Classification and Field Extraction Capabilities taken from SCE
- Backward compatibility to preserve existing NBAR investments
- In-service field upgradable Protocol Definition – no IOS upgrade required

NBAR is the Engine, Still need a Driver



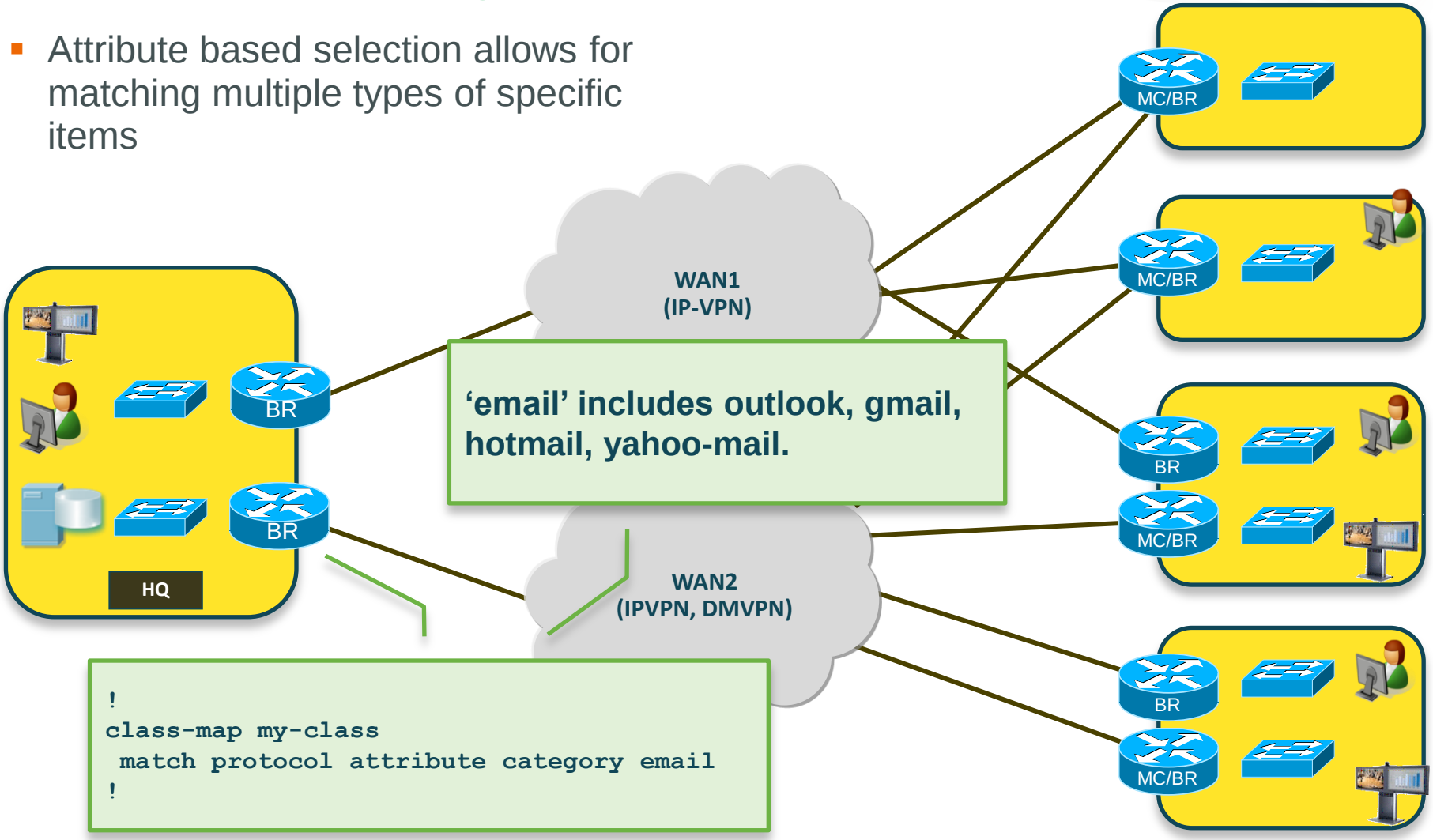
- Multiple methods to use the engine, depending on need.
- Enable NBAR Protocol Discovery at interface level
  - All traffic is classified based on protocol.
    Results (packets, bytes, application) are available via CLI and MIB
- Invoke ‘match protocol’ CLI in C3PL/MQC (class-map) CLI
  - Used in a number of different IOS functions (QoS, performance monitor, IOS FW)
  - Results vary depending on IOS function used
- Invoke ‘application name/ID’ fields in flexible netflow (FNF)
  - Application name/ID is included in NetFlow export reports

NBAR2

Simplified Policies using Attributes

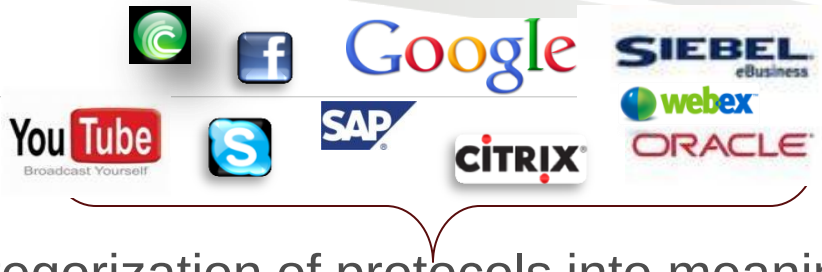
15.2(2)T1
XE 3.4.0S

- Attribute based selection allows for matching multiple types of specific items



NBAR2 - Traffic Categorization by attribute

For Your Reference



Categorization of protocols into meaningful terms
Simplification of control configuration and report aggregation

Categories	Sub-Categories	Application-Group	P2P-technology	Tunnel	Encrypted
file-sharing	client-server	ftp-group	n	n	n
browsing	other	other	y	y	y
net-admin	routing-protocol	ipsec-group	unassigned	unassigned	unassigned
other	tunneling-protocols	imap-group			
internet-privacy	network-management	irc-group			
instant-messaging	voice-video-chat-collaboration	kerberos-group			
email	authentication-services	ldap-group			
newsgroup	database	sqlsvr-group			
voice-and-video	naming-services	netbios-group			
business-and-productivity-tools	terminal	nntp-group			
industrial-protocols	streaming	pop3-group			
gaming	p2p-networking	snmp-group			
obsolete	p2p-file-transfer	tftp-group			
trojan	control-and-signaling	fasttrack-group			
layer3-over-ip	inter-process-rpc	gnutella-group			
location-based-services	remote-access-terminal	skinny-group			
layer2-non-ip	network-protocol	edonkey-emule-group			
	commercial-media-distribution	bittorrent-group			
	rich-media-http-content	smtp-group			
	license-manager	windows-live-messanger-group			
	epayement	yahoo-messenger-group			
	storage	flash-group			
	backup-systems	skype-group			
	one-click-hosting	corba-group			

DiffServ QoS Recommendations (RFC 4594-Based)

How Should Traffic Be Marked?

Application Class	Per-Hop Behavior	Admission Control	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	Required	(Optional) PQ	Cisco TelePresence™
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Unified Personal Communicator
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	Cisco WebEx®™ / MeetingPlace® / ERP Apps
Bulk Data	AF1		BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue (Deferential)	YouTube, iTunes, BitTorent, Xbox Live

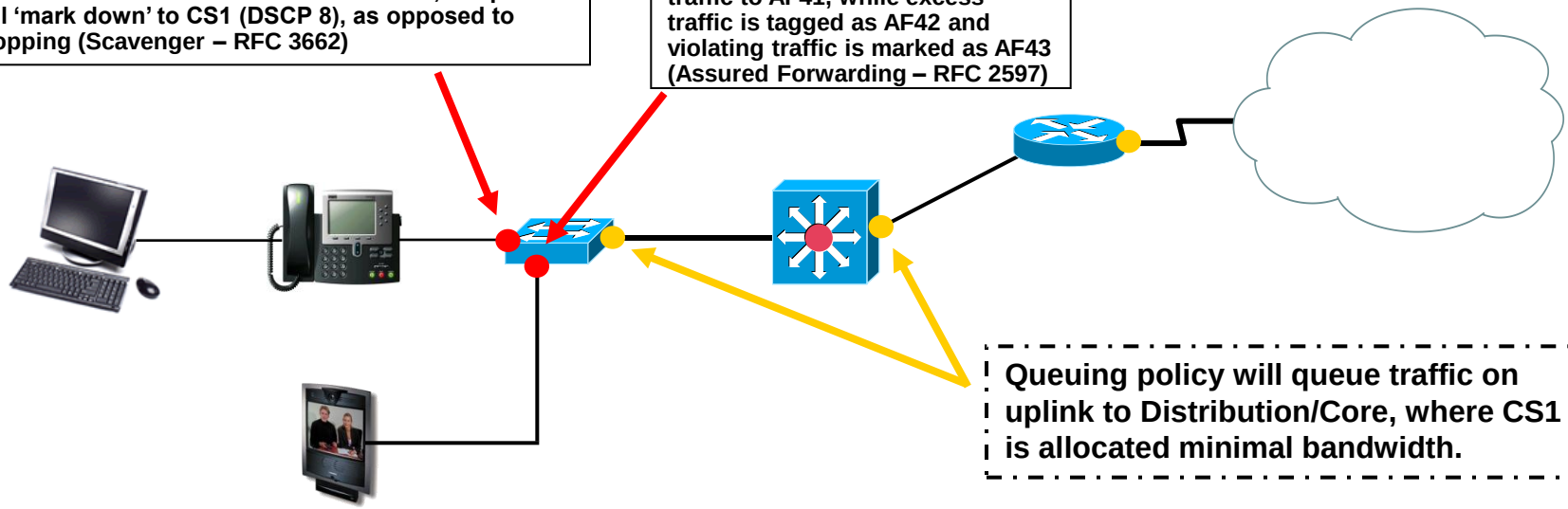
Policing Design Principles
Where and How Should Policing Be Done?

Policing shall be applied as close to the traffic source as possible; in general, policing should be applied at the access layer of the network at the "Trust Boundary" during the initial classification and marking process; policing policies can be configured to drop offending traffic, or they can be configured to mark down excess traffic, specifying a different PHB or method of treatment

Ingress policy includes a policer for voice bearer traffic, based on the codec type and the number of concurrent calls. Excess traffic is dropped by the policer.

Ingress policy includes a policer for data traffic. A baseline value is used. Traffic conforming to the policer is marked as 0. For excess traffic, the policer will 'mark down' to CS1 (DSCP 8), as opposed to dropping (Scavenger – RFC 3662)

Ingress policy for video conferencing marks conforming traffic to AF41, while excess traffic is tagged as AF42 and violating traffic is marked as AF43 (Assured Forwarding – RFC 2597)



Queuing Design Principles
Where Should It Be Done?

Queuing should be performed wherever there may be potential for congestion (even if a rare occurrence), ensuring consistency between Campus/WAN/VPN networks…

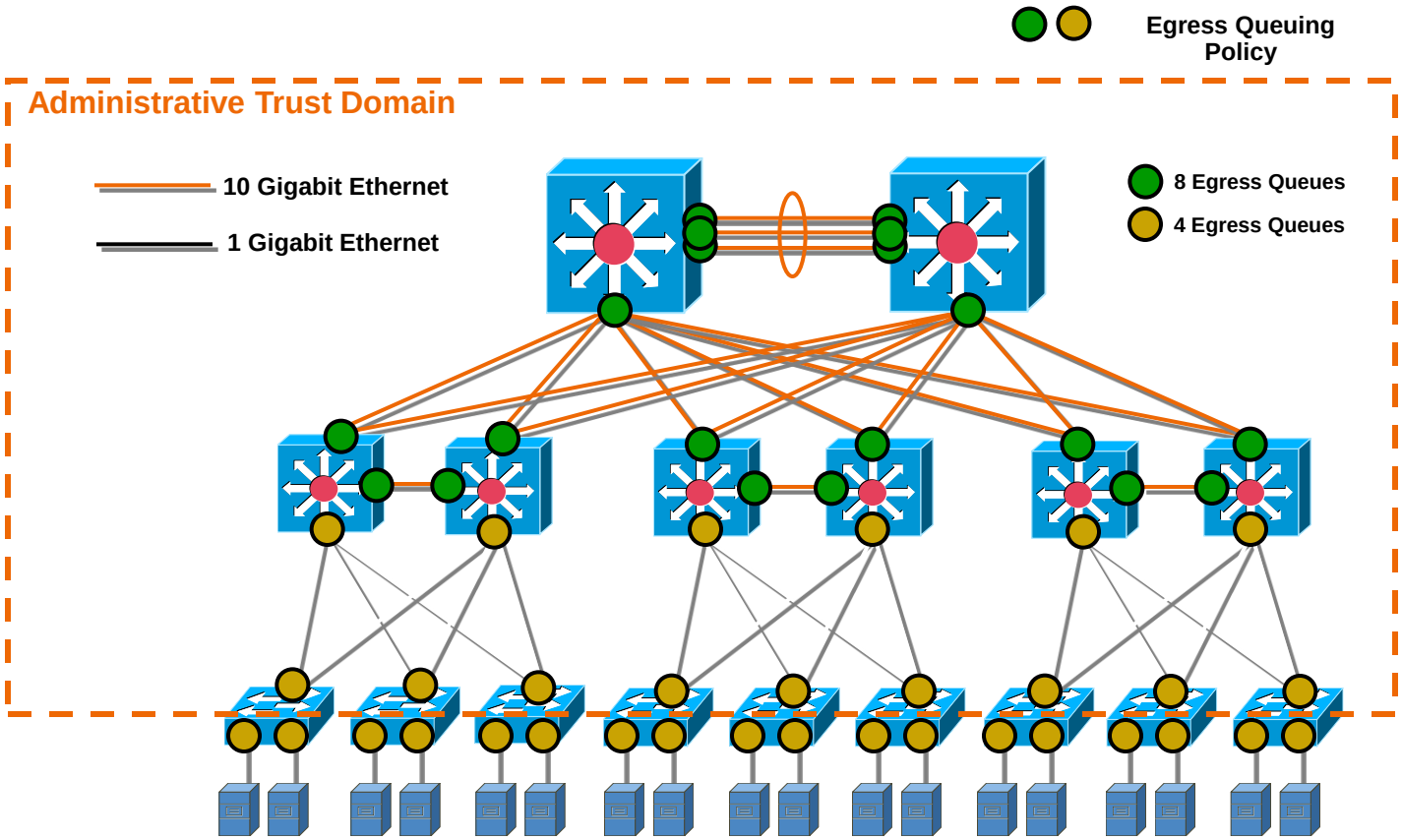
Recommended Guidelines:

1) **25% minimum allocated to Best Effort (BE) Class**

2) **Priority Queue (PQ) given maximum of 33%**

3) **Scavenger should be provisioned with a minimal bandwidth allocation ~ 5%**

4) **Congestion Avoidance enabled on select TCP flows in non-PQ**

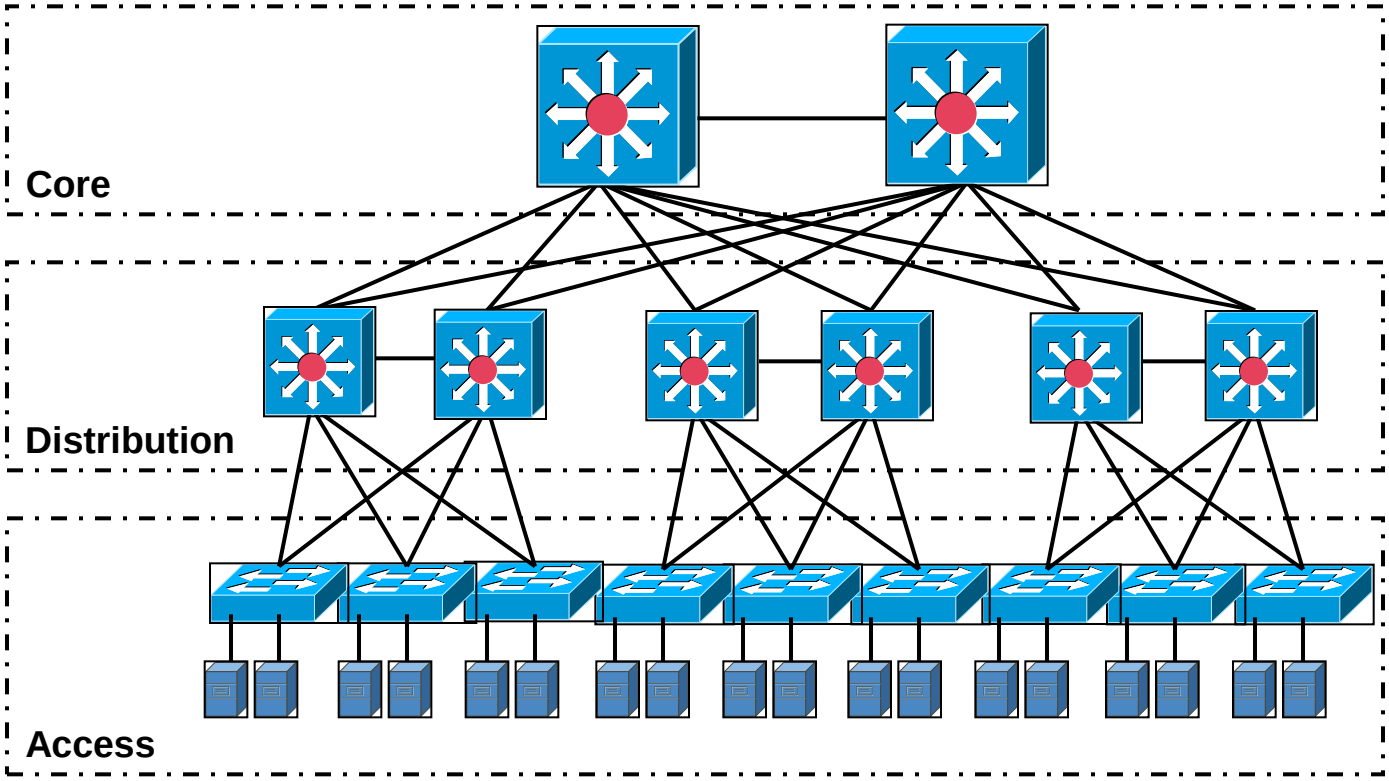


Campus QoS Considerations
Typical Campus Oversubscription Ratios

Campus networks are always designed with oversubscription in mind to take advantage of the bursty nature of traffic and the assumption that not all users are requiring bandwidth simultaneously…

Typically 4:1 Ratio

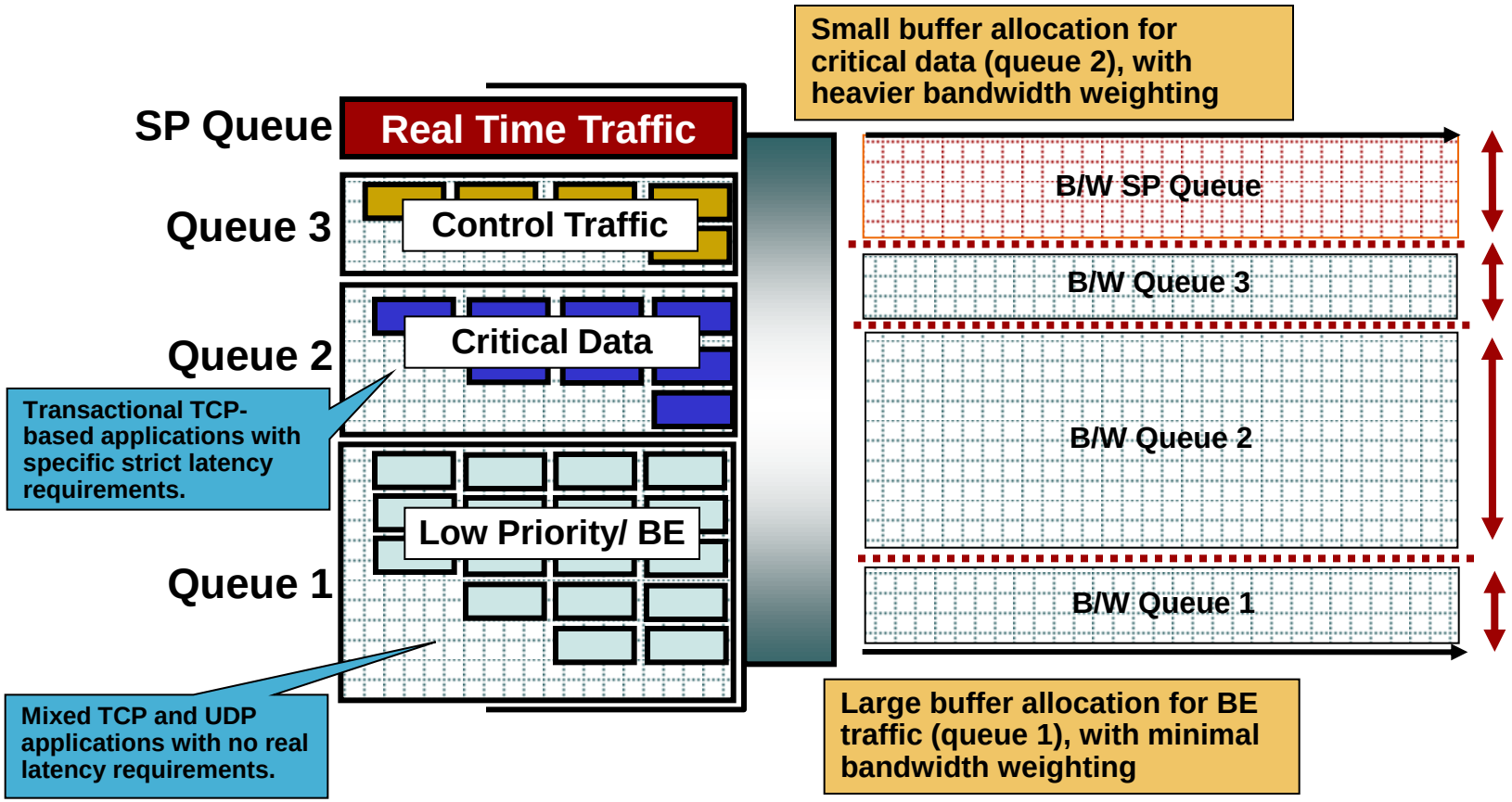
Typically 20:1 Ratio



Campus QoS Design Considerations

Allocating Buffer Capacity

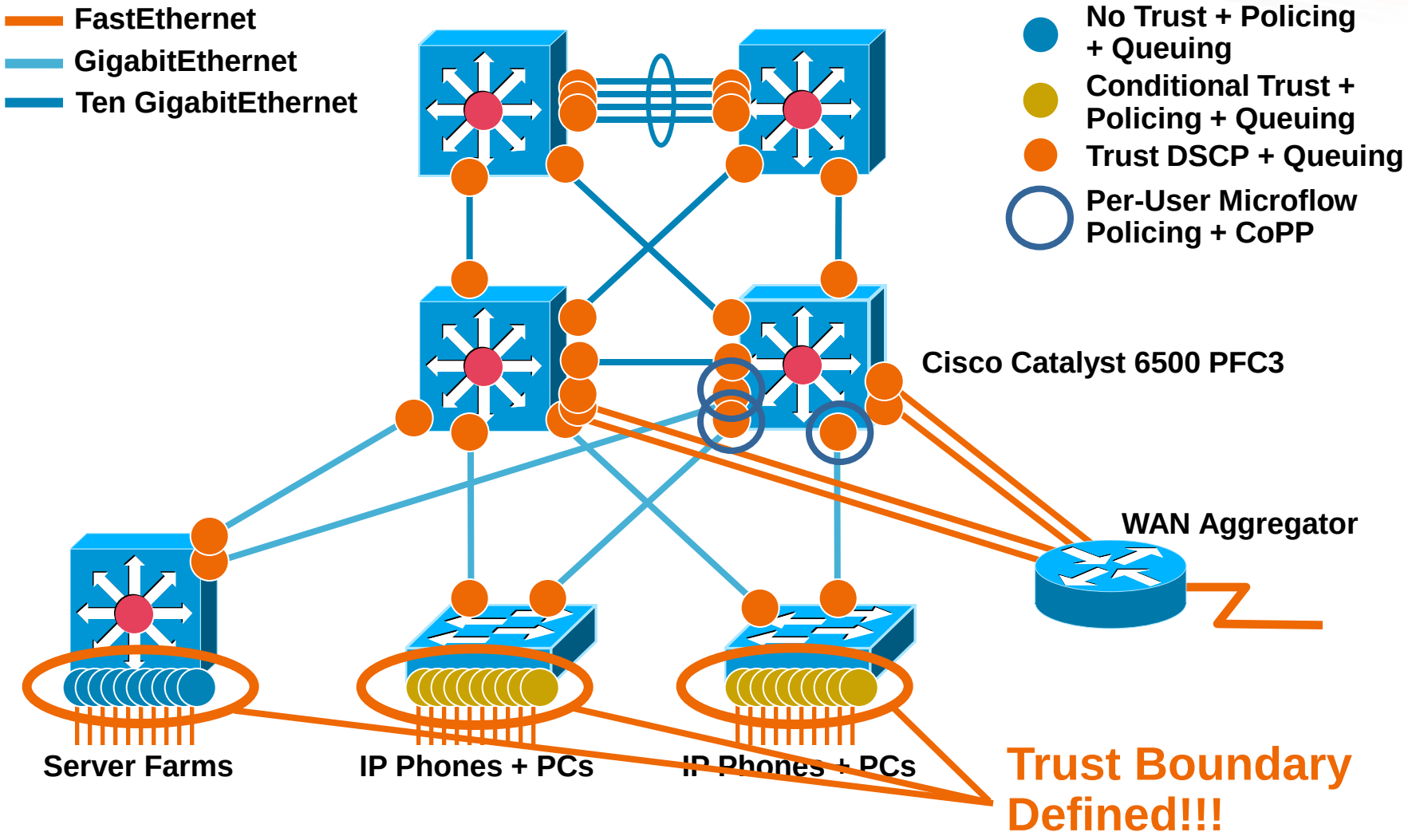
Each port has a finite amount of memory that is specifically reserved for buffering traffic during times of contention. Although the total amount of buffer capacity for egress traffic may be fixed for a given port, how that memory is distributed amongst the queues is configurable.



***Allocating more memory to a given queue can increase packet latency, which could impact application performance.

Campus QoS Considerations

Where Is QoS Required Within the Campus?

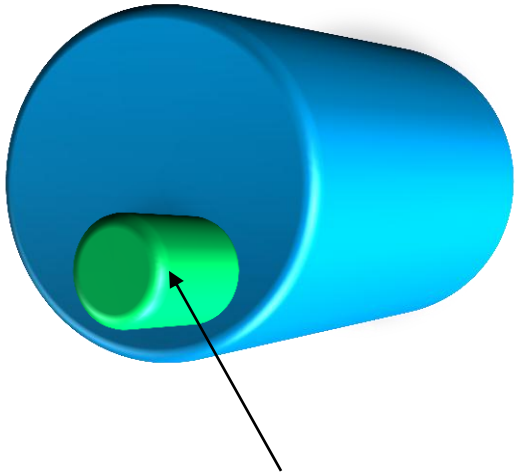


Application Control

Application Control for the Campus

```
ip access-list extended TRANSACTIONAL
permit tcp any any eq 443
permit tcp any any eq 1521
permit udp any any eq 1521

class-map match-all VVLAN-VOIP
      match ip dscp ef
class-map match-all TRANSACTIONAL
      match access-group name TRANSACTIONAL

policy-map Access-policy
  class VVLAN-VOIP
      set dscp ef
      police 128k bc 8000 conform-action transmit
            exceed-action drop

policy-map DVLAN-MARKING
  class TRANSACTIONAL
       set dscp af21

interface range GigabitEthernet 2/1-48
   switchport access vlan 10
    swtichport voice vlan 110
Vlan config 10
       service-policy input DVLAN-MARKING
Vlan config 110
        servic-policy input VVLAN-MARKING
```

Application	Policed	Marked
Transactional	NO	AF21
Voice Bearer	128kbps	EF, trusted



Voice Bearer policed to 128kbps

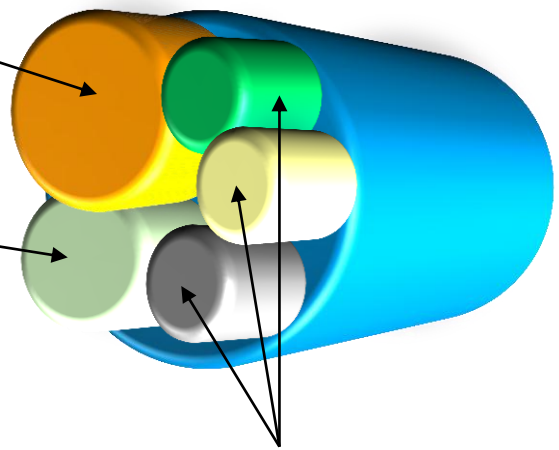
Application Control for the Campus

```
class-map match-any PRIORITY
  match dscp ef
  match dscp cs5
  match dscp cs4
class-map match-all TRANSACTIONAL
  match dscp af21 af22 af23
…

policy-map Egress-queueing
 class PRIORITY
  priority
 class CONTROL-MGMT
  bandwidth remaining percent 10
class MULTIMEDIA-STREAMING
  bandwidth remaining percent 10
  class TRANSACTIONAL
  bandwidth remaining percent 10
 class class-default
 bandwidth remaining percent 25
  dbl

interface range TenGigabitEthernet 1/1-2
service-policy output Egress-queueing
```

Application	Bandwidth	Priority
Priority	Policer limited	High
Control-MGMT	10 %	Normal
Multimedia-streaming	10%	Normal
Transactional	10%	Normal
Default	25%	Low

Priority traffic limited at edged via policers allocated up to 100%

Class Default 25% remaining

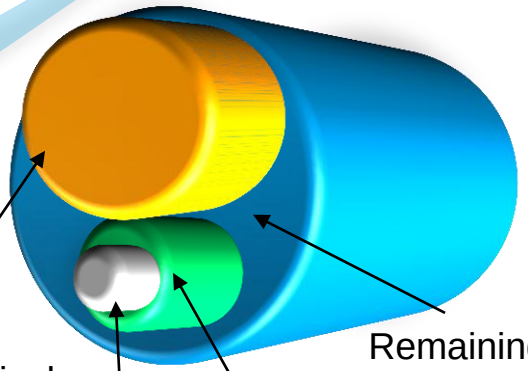


Control, Multimedia and Transactional each receive 10% remaining

Application-aware QoS WAN

```
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



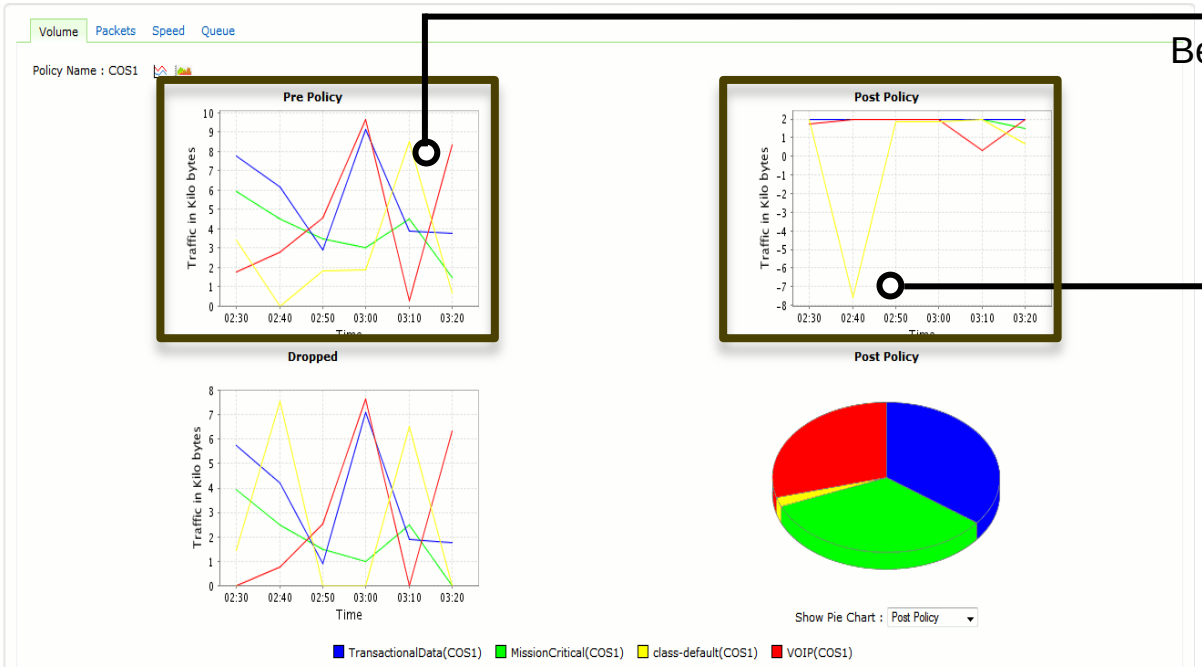
Business-Critical:
High Priority
50% committed

Internal-Browsing:
60% of Browsing

Browsing:
30% of Excess BW
(=15% of the line)

Remaining:
70% of Excess BW
(=35% of line)

Control Application Bandwidth Usage with QoS



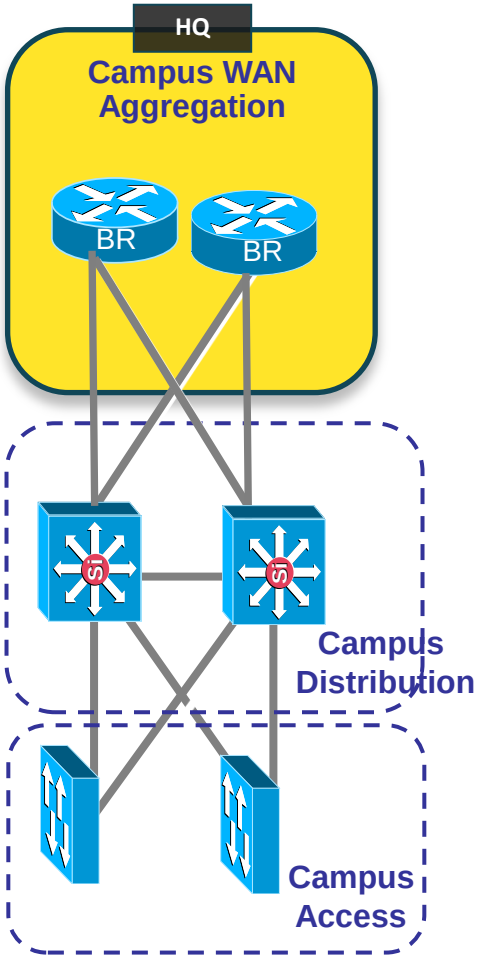
Before apply QoS control policy

After apply control policy

- NBAR2 is used to identify the application (match protocol in class-map)
- QoS actions include drop, re-prioritization of application in the QoS queue, re-mark DSCP/IP Precendence, police or shape the traffic rate using QoS MQC

Evolving QoS
Campus and Wan QoS alignment via MQC

- MLS command set is evolving into MQC
  - 6500/4500 now MQC based
- MQC construct (C3PL) leveraged in Performance Monitoring, IOS FW, eEdge…
- QoS is always on – no “mls QoS”
- Trust paradigm is replaced by implicit trust
- Explicit configuration of QoS parameters are required
- Unified CLI and provisioning language provide stronger QoS alignment



Monitoring QoS

Monitor

- Depth and scope of monitoring QoS varies
- Monitoring minimums should include trending link utilizations and packet drops
- Use Neflow to identify mismarked applications
- More powerful tools can collect traffic statistics from the class-based-QoS-MIB
- NBAR protocol discovery can be leveraged by applications to collect statistics and display them graphically
- Collecting lots of data is most useful if there are good backend tools to sort the data and flag issues such as high drop rates

SNMP MIB
Cisco-Class-Based-QoS-MIB

- Primary accounting mechanism for QoS:
  - Policing, classification, shaping, queuing, congestion avoidance
- Long-term QoS monitoring
  - Cisco QoS Policy Manager (QPM)
- Provides accounting for configured QoS policies
  - Does not inspect all packets for TOS/DSCP
- Provides equivalent statistics to “Show policy-map interface”
  - Counters can not be reset

Flexible Netflow

- Flexible Netflow is an opened standard to export network information and statistics
  - UDP-based transport
  - Flexibility in defining fields and flow record format
  - Opened protocol – can be analyzed by Cisco Prime, Insight, and other 3rd party reporting vendors
- Consist of data collection (flow monitor) and data export (flow export)
- Flexibility choosing fields to collect for exporting
- Can be used for collecting application based info and statistics along with other network information
- Can be utilized by other monitoring feature to export information (IOS Performance Agent, Medianet, PfR)

Configure a Flow Monitor

Configure the Exporter

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

Configure the Flow Record

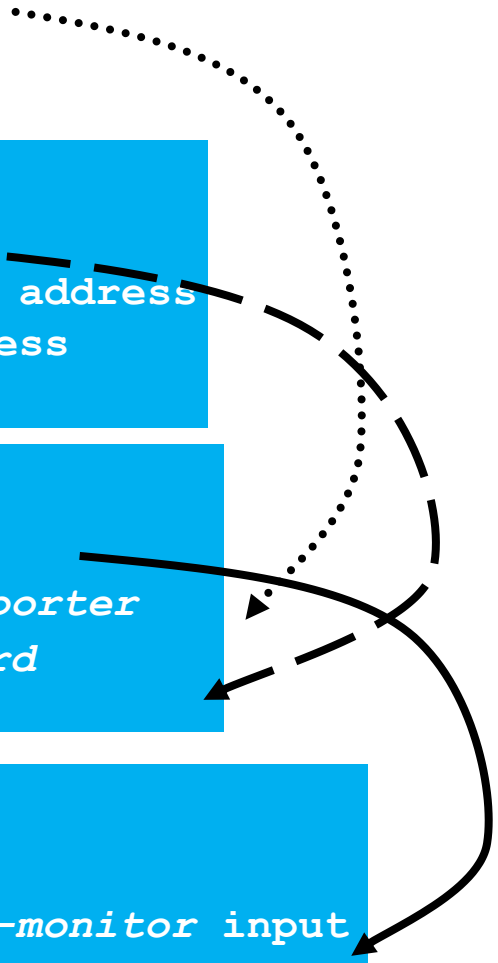
```
Router(config)#flow record my-record
Router(config-flow-record)#match ipv4 destination address
Router(config-flow-record)#match ipv4 source address
Router(config-flow-record)#collect counter bytes
```

Configure the Flow Monitor

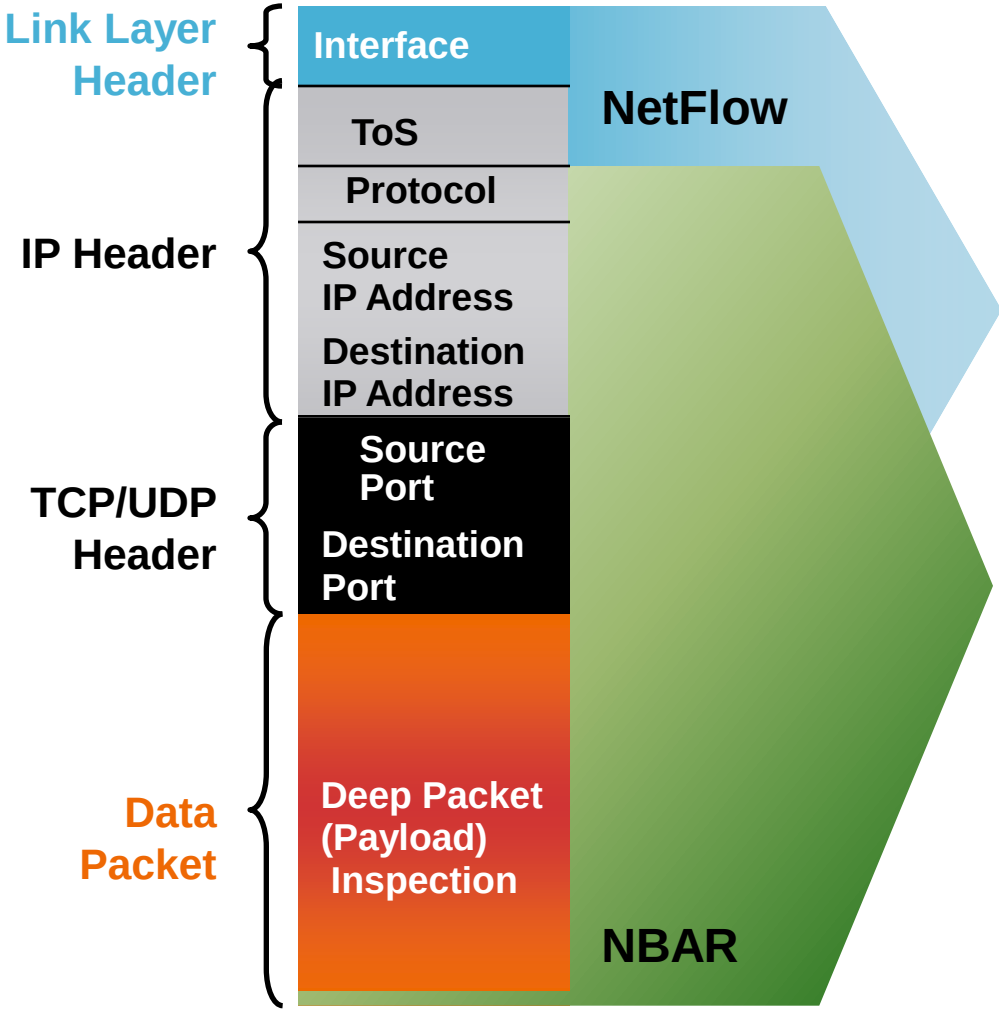
```
Router(config)#flow monitor my-monitor
Router(config-flow-monitor)#exporter my-exporter
Router(config-flow-monitor)#record my-record
```

Configure the Interface

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



NetFlow and NBAR Integration



NetFlow

- ✓ Monitors data in Layers 2 thru 4
- ✓ Determines applications by combination of Port or Port/IP Addressed
- ✓ Flow information who, what, when, where

NBAR

- ✓ Examines data from Layers 3 thru 7
- ✓ Utilizes Layers 3 and 4 plus packet inspection for classification
- ✓ Stateful inspection of dynamic-port traffic
- ✓ Packet and byte counts

Integrated Flexible NetFlow, NBAR and QoS

Trust boundary verification

```
router(config)# flow record fnf-QoS-record
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match application name
router(config-flow-record)# match ipv4 dscp
router(config-flow-record)# match flow class-id
router(config-flow-record)# collect counter bytes
router(config-flow-record)# collect counter packets
router(config)# flow monitor fnf_monitor
router(config-flow-monitor)# record fnf-QoS-record

router(config)# interface eth0/0
router(config-if)# ip flow monitor fnf-monitor output
```

```
show flow mon <app_mon> cache

IPV4 SRC   IPV4 DST    APP NAME       DSCP  Class-id
========   ========    ========       ====  ========
10.0.1.1   10.0.1.2    nbar ssh       0x20  Management
10.0.1.1   10.0.1.2    nbar telnet    0x20  Management
10.0.1.1   10.0.1.2    NBAR my-app    0x22  Transactional
```

Traffic | Application | Source | Destination | QoS | Conversation | Medianet | NBAR | CBQoS

Select : FNF NBAR | IN | OUT | Last 15 Minutes | From: 2012-03-12 17:36 | To: 2012-03-12 17:51

Resolve DNS | Group by None | Showing 1 to 50 | View per page 50

Src IP	Dst IP	Application	Src Port	Dst Port	Protocol	DSCP	Traffic
172.18.93.211	228.8.47.52	snmp	36511	161	UDP	AF1	2.23 MB
172.18.66.250	228.8.7.9	http	468	80	TCP	CS6	1.77 MB
172.18.78.232	66.8.47.52	Skype	52091	16	UDP	Default	1.06 MB
172.18.2.164	70.8.47.52	BitTorrent	49600	52091	UDP	Default	828.01 KB
172.18.4.62	232.0.1.10	unknown	0	0	UDP	Default	422.83 KB
172.18.2.101	192.168.24.158	netbios	137	137	UDP	CS1	48.12 KB

- Validate Policy configuration
- Troubleshoot incorrect or missing configurations
- Validate bandwidth allocations
- Isolate Rogue Application traffic

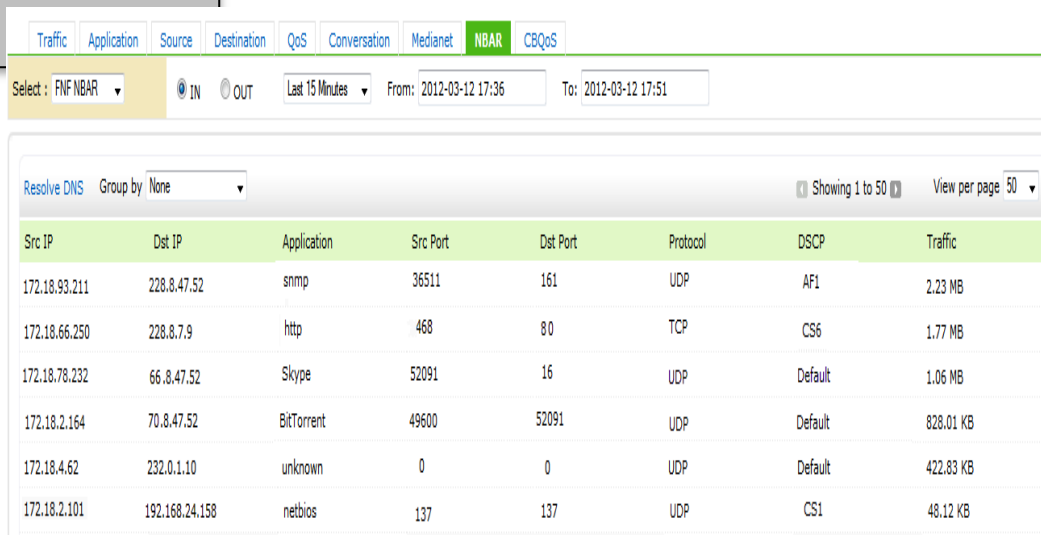
Integrated Flexible NetFlow, NBAR and QoS

Trust boundary verification

```
router(config)# flow record QoS-Record
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match application name
router(config-flow-record)# match ipv4 dscp
router(config-flow-record)# match flow class-id

router(config)# flow monitor Traffic-monitor
router(config-flow-monitor)# record QoS-Record

router(config)#policy-map fnf-NBAR-QoS
router(config-pmap)#class Critical
router(config-pmap-c)#flow Traffic-monitor

router(config)# interface eth0/0
router(config-if)# service-policy out fnf-NBAR-QoS
```

```
show flow mon <fnf_mon> cache

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

- Validate Policy configuration
- Troubleshoot incorrect or missing configurations
- Validate bandwidth allocations
- Isolate Rogue Application traffic

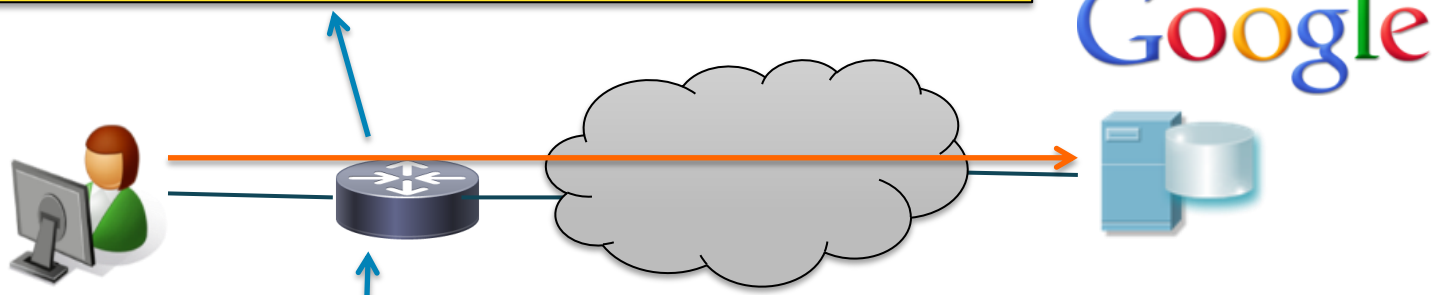


Flexible NetFlow
NBAR2 Integration – Field Extraction

15.3(1)M
IOS XE
3.7.0S

- NBAR extracts fields from flows and exposes it into Flexible NetFlow
- HTTP Fields (Hostname and URL) planned in 15.3(1)M and IOS XE 3.7.0S

```
show flow mon <app_mon> cache

IPV4 SRC ADDR    IPV4 DST ADDR   APP NAME       Hostname          URL… …
===============  ==============  =============  ================  ==========
10.0.1.1         10.0.1.2        nbar http    www.google.com    /news
```




```
router(config)# flow record HTTP_record
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match application name
router(config-flow-record)# match application http hostname
router(config-flow-record)# match application http URL
```

Integrated Flexible NetFlow, NBAR and QoS

```
3845-Pagent#sh flow monitor fnf-monitor cache
  Cache type:                               Normal
  Cache size:                               4096
  Current entries:                          2
  High Watermark:                           6

  Flows added:                              926
  Flows aged:                               924
    - Active timeout      ( 1800 secs)      0
    - Inactive timeout    (   15 secs)      924
    - Event aged                            0
    - Watermark aged                        0
    - Emergency aged                        0
```

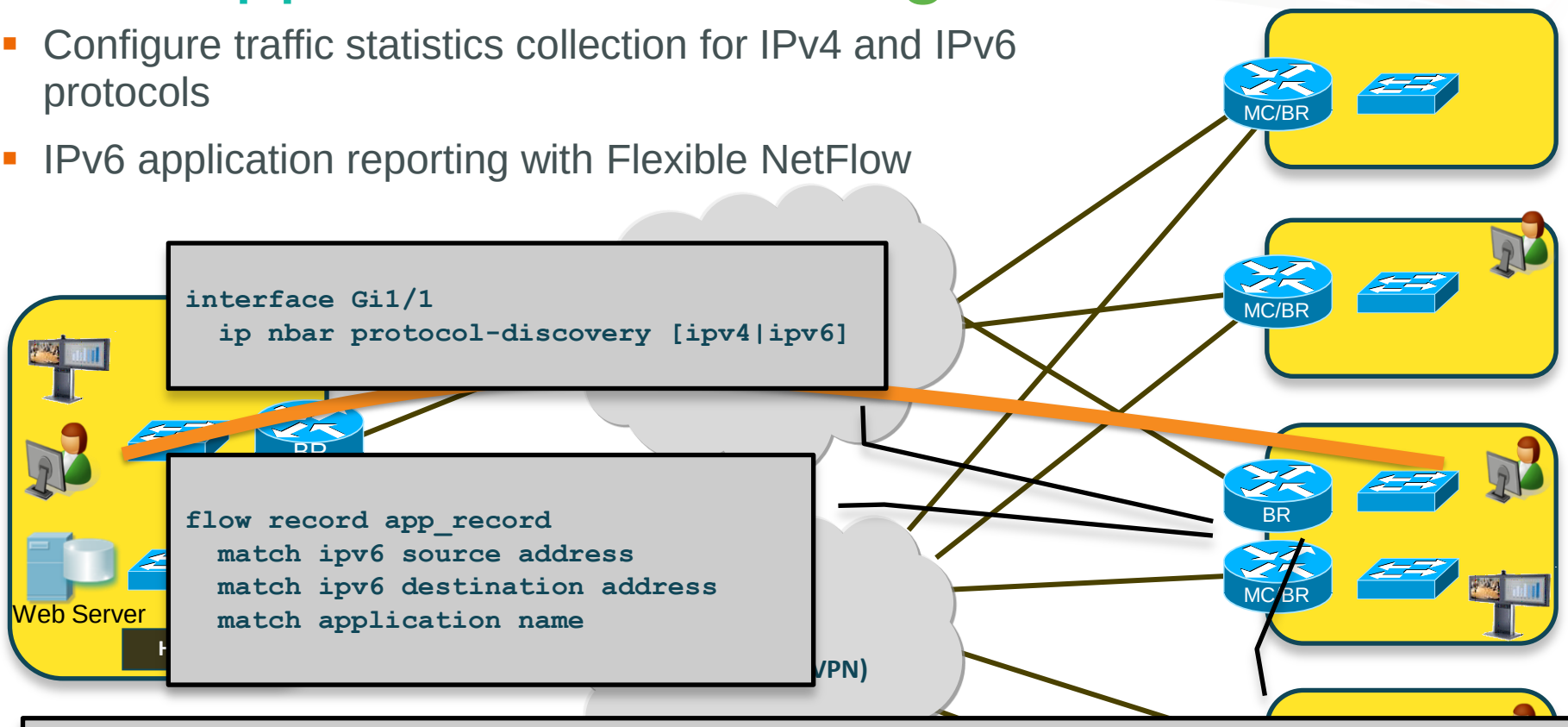
```
IPV4 SOURCE ADDRESS:          10.27.37.2
IPV4 DESTINATION ADDRESS:     10.27.37.9
IP TOS:                       0x70
IP DSCP:                      0x1C
APPLICATION NAME:             nbar telnet
CLASS-ID:                     management
counter bytes:                249
counter packets:              5

IPV4 SOURCE ADDRESS:          10.27.0.2
IPV4 DESTINATION ADDRESS:     10.27.37.9
IP TOS:                       0x00
IP DSCP:                      0x00
APPLICATION NAME:             nbar tftp
CLASS-ID                      class-default
counter bytes:                11868
counter packets:              24
```

NOTE:
TOS of 0x70 equates to 112 decimal
DSCP of 0x1C equates to 28 decimal
Ip telnet tos70

IPv6 Application monitoring

15.2(1)T1, IOS XE 3.3.0S

- Configure traffic statistics collection for IPv4 and IPv6 protocols
- IPv6 application reporting with Flexible NetFlow




```
interface Gi1/1
  ip nbar protocol-discovery [ipv4|ipv6]
```

```
flow record app_record
  match ipv6 source address
  match ipv6 destination address
  match application name
```

```
# sh flow monitor APPIPv6  cache format table

IPV6 SOURCE ADDRESS                      IPV6 DESTINATION ADDRESS                 APPL NAME
2A01:E35:8ABF:9510:FA1E:DFFF:FEE1:E789   2A01:E35:8ABF:9510:222:55FF:FEE6:BA98    http
```

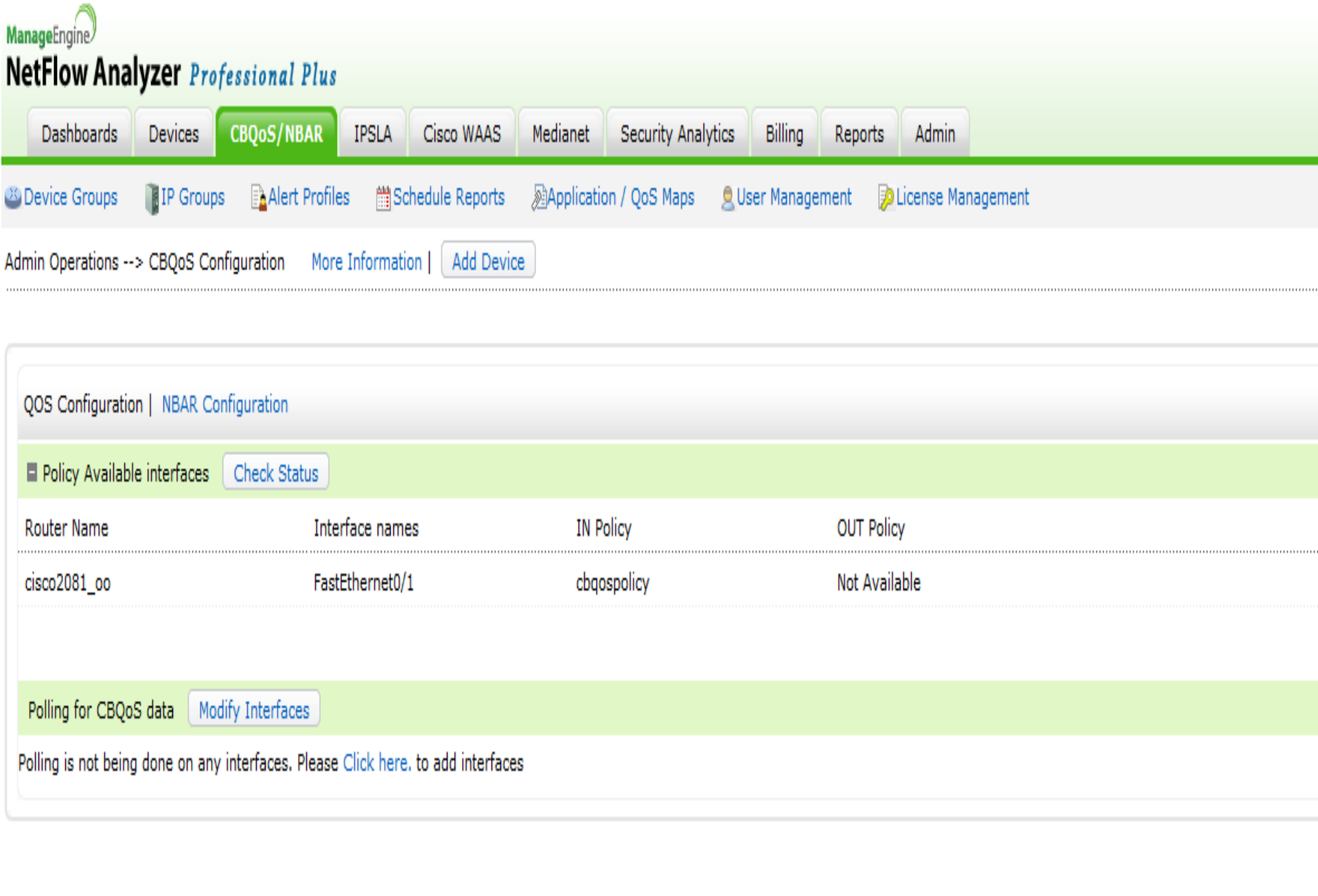
QoS Reports using ManageEngine NetFlow Analyzer

CISCO-CLASS-BASED-QOS-MIB

- SNMP query of CISCO-CLASS-BASED-QOS-MIB
  - Reports on Policy, Child-Policy and Class
  - Pre and Post Policy statistics
  - Volume, speed and utilization based drop value information
  - Match statement statistics for each class
  - View configuration of policies from product GUI

Validating QoS Performance

ManageEngine



Validating QoS Performance

ManageEngine

Device Groups | IP Groups | Alert Profiles | Schedule Reports | Application / QoS Maps | User Management | License Management | Search

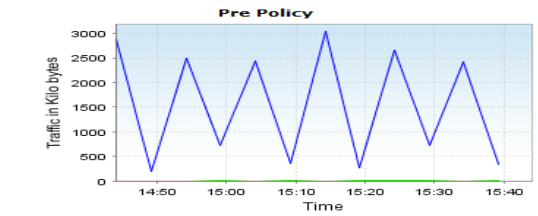
cisco2081_oo --> FastEthernet0/1 | Action(s) | More Reports | Dashboards

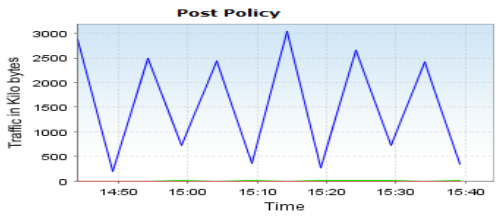
Traffic | Application | Source | Destination | QoS | Conversation | Medianet | NBAR | CBQoS

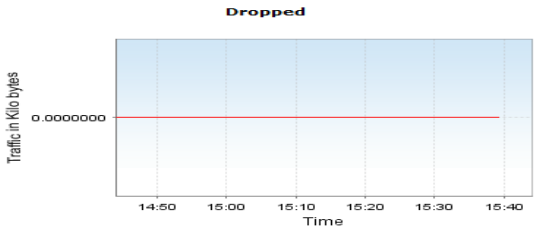
IN | OUT | Last Hour | From: 2012-01-18 14:44 | To: 2012-01-18 15:44

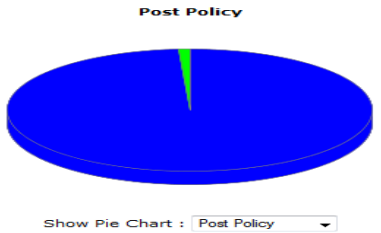
Volume | Packets | Speed | Queue

Policy Name : cbqosweb









Show Pie Chart : Post Policy

class-default(cbqosweb) Web(cbqosweb) snmp(cbqosweb)

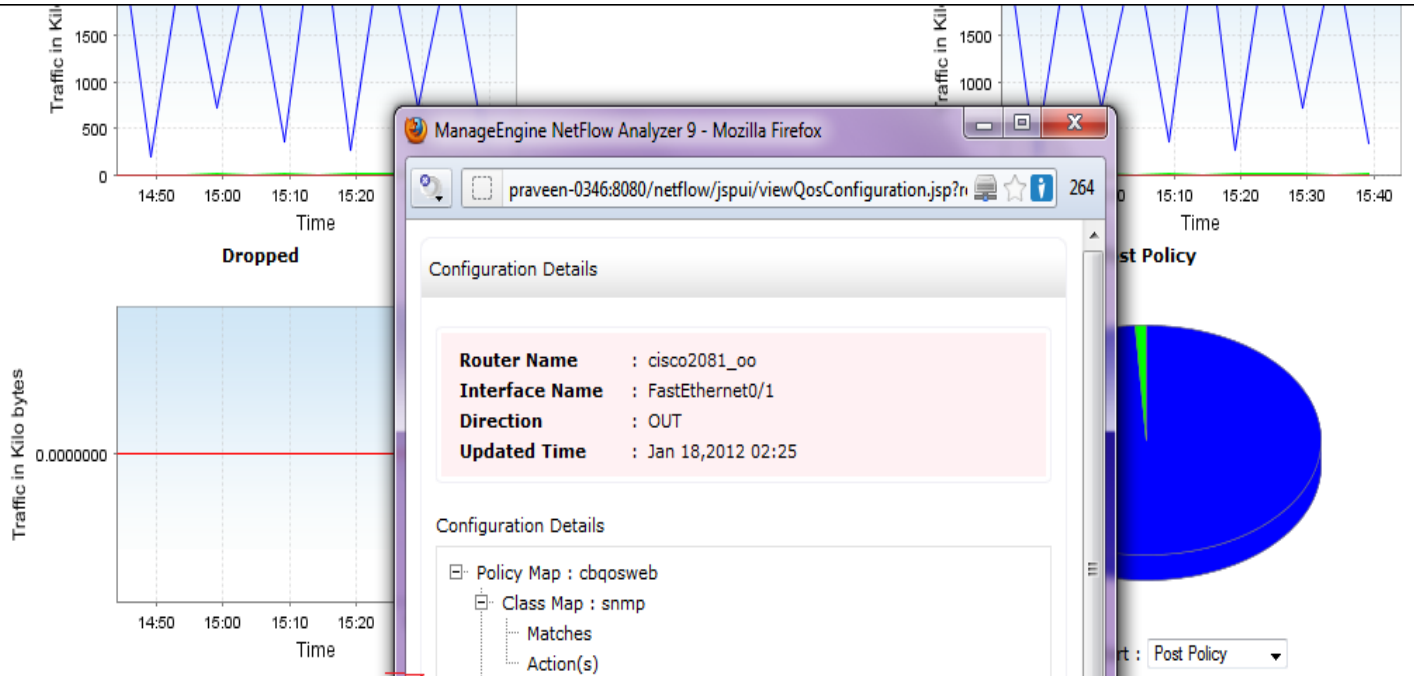
Parent Policy | View Configuration

cbqosweb

Class	Pre Policy	Dropped	% Dropped	Post Policy ▲	% Post Policy
class-default	18.54 MB	0.00	0.00%	18.54 MB	99.47%
Web	99.42 KB	0.00	0.00%	99.42 KB	0.53%
snmp	0.00	0.00	0.00%	0.00	0.00%
Total	18.63 MB	0.00		18.63 MB	

Validating QoS Performance

ManageEngine



ManageEngine NetFlow Analyzer 9 - Mozilla Firefox

praveen-0346:8080/netflow/jspui/viewQosConfiguration.jsp?r 264

Configuration Details

Router Name	: cisco2081_oo
Interface Name	: FastEthernet0/1
Direction	: OUT
Updated Time	: Jan 18,2012 02:25

Configuration Details

- Policy Map : cbqosweb
  - Class Map : snmp
    - Matches
    - Action(s)
  - Class Map : Web
    - Matches
      - Match protocol secure-http
      - Match protocol ftp
      - Match protocol smtp
      - Match protocol pop3
      - Match protocol http
    - Action(s)
  - Class Map : class-default
    - Matches
      - Match any
    - Action(s)

Parent Policy | View Configuration

cbqosweb

Class	Pre Policy	% Post Policy
class-default	18.54 MB	99.47%
Web	99.42 KB	0.53%
snmp	0.00	0.00%
Total	18.63 MB	

Child Policy

No child policy

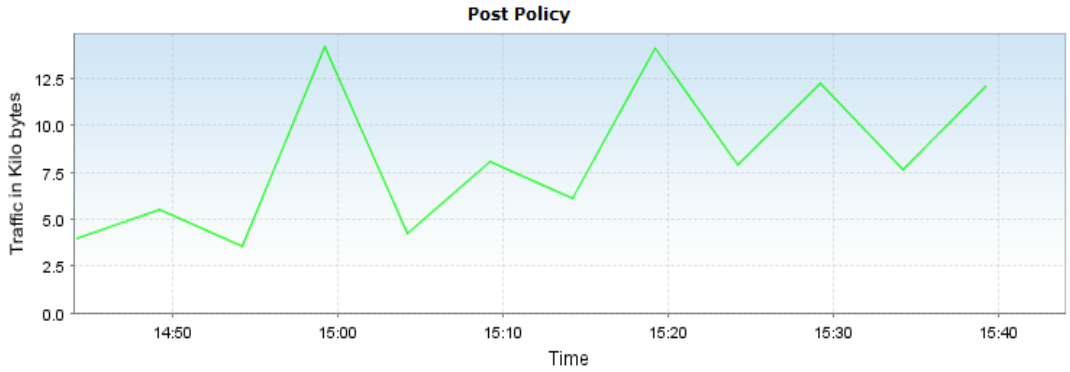
Validating QoS Performance

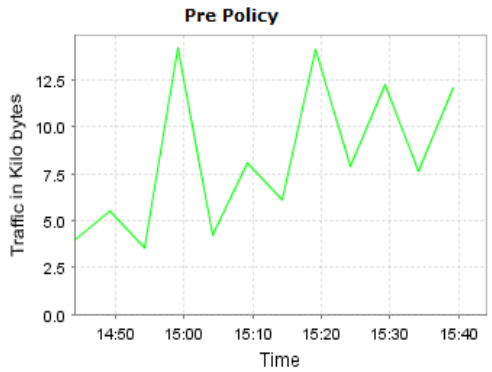
ManageEngine

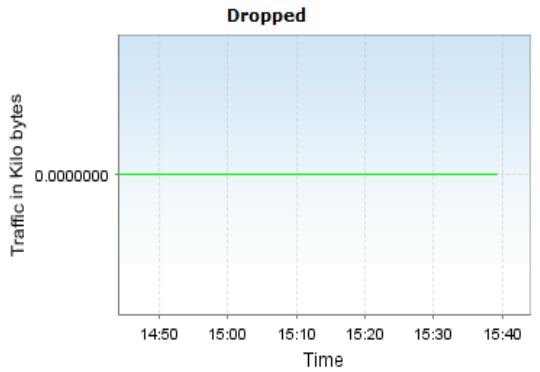
cisco2081_oo [FastEthernet0/1] --> qosOUT Start Time: Jan 18,2012 14:44 End Time: Jan 18,2012 15:44

Policy Name : cbqosweb

Class	Pre Policy	Dropped	Post Policy
Web	99.42 KB	0.00	99.42 KB







NetFlow

- NetFlow reports on Interface, IP Address, Application (Protocol & Port), DSCP, ToS, NextHop, TCP Flag, etc.
- Check if application conversations have the assigned DSCP markings
- NetFlow shows DSCP markings for each conversation – Reporting can be done for INGRESS or EGRESS

Validating QoS Performance

ManageEngine

172.18.95.215	172.18.255.255	netbios-dgm	138	138	UDP	CS1	207.05 KB
172.18.117.147	172.18.255.255	netbios-ns	137	137	UDP	Default	201.63 KB
172.18.95.239	172.18.255.255	netbios-ns	137	137	UDP	Default	201.31 KB
172.18.78.232	172.18.255.255	netbios-ns	137	137	UDP	Default	190.02 KB
172.18.97.44	224.0.0.251	mdns	5353	5353	UDP	Default	184.4 KB
172.18.181.20	224.0.0.251	mdns	5353	5353	UDP	Default	182.01 KB
172.18.83.253	172.18.255.255	netbios-ns	137	137	UDP	CS1	169.49 KB
172.18.99.193	172.18.255.255	netbios-ns	137	137	UDP	CS1	168.64 KB
172.18.78.223	224.0.0.251	mdns	5353	5353	UDP	Default	161.37 KB
172.18.98.192	224.0.0.251	mdns	5353	5353	UDP	Default	158.22 KB
172.18.99.17	224.0.0.252	llmnr	57754	5355	UDP	Default	155.91 KB
172.18.95.96	224.0.0.251	mdns	5353	5353	UDP	Default	154.65 KB
172.18.149.90	172.18.2.101	http	49849	80	TCP	Default	154.64 KB
172.18.2.185	172.18.255.255	netbios-ns	137	137	UDP	CS1	154.12 KB
172.18.99.134	172.18.255.255	netbios-ns	137	137	UDP	CS1	152.38 KB
172.18.2.183	172.18.255.255	netbios-ns	137	137	UDP	CS1	146.97 KB
172.18.2.182	172.18.255.255	netbios-ns	137	137	UDP	CS1	142.07 KB
172.18.0.1	224.0.0.18	VRRP_App	0	0	VRRP	Default	131.15 KB
172.18.97.229	239.255.255.250	ws-discovery	64402	3702	UDP	Default	123.15 KB
172.18.99.96	239.255.255.250	ws-discovery	64402	3702	UDP	Default	123.15 KB
172.18.158.66	224.0.0.251	mdns	5353	5353	UDP	Default	116.81 KB
172.18.8.12	172.18.255.255	netbios-ns	137	137	UDP	CS1	115.52 KB
172.18.96.242	224.0.0.251	mdns	5353	5353	UDP	Default	114.62 KB
172.18.98.99	224.0.0.251	mdns	5353	5353	UDP	Default	114.25 KB
172.18.97.236	224.0.0.251	mdns	5353	5353	UDP	Default	110.11 KB
172.18.51.3	172.18.255.255	netbios-ns	137	137	UDP	CS1	106.19 KB
172.18.99.24	172.18.255.255	netbios-ns	59359	137	UDP	CS1	104.75 KB
172.18.2.186	172.18.255.255	netbios-ns	137	137	UDP	CS1	102.57 KB
172.18.39.193	239.255.255.250	ssdp	1900	1900	UDP	Default	101.32 KB

Validating QoS Performance

ManageEngine

CS1	3.44 MB	7%

Application distribution for **CS1**

Application	Traffic	% Utilization
netbios-ns	2.41 MB	70%
netbios-dgm	1.02 MB	30%

CS6	103.81 KB	<1%

Application distribution for **CS6**

Application	Traffic	% Utilization
mdns	63.47 KB	61%
icmp	22.43 KB	22%
IGMP_App	17.78 KB	17%
telnet	120.00 Bytes	<1%

000010	91.61 KB	<1%

Application distribution for **000010**

Application	Traffic	% Utilization
Unknown_App	91.61 KB	100%

000111	10.08 KB	<1%

Application distribution for **000111**

Application	Traffic	% Utilization
icmp	10.08 KB	100%

000100	3.31 KB	<1%

Application distribution for **000100**

Application	Traffic	% Utilization
bootps	2.65 KB	80%
telnet	654.00 Bytes	20%

Validating QoS Performance

ManageEngine

Traffic | Application | Source | Destination | QoS | Conversation | Multicast | Medianet | NBAR | CBQoS | Security Events

Top DSCP IN Report - AF11 From: 2012-03-12 13:05 To: 2012-04-11 13:05 Back

Resolve DNS | Group by None Showing 1 to 43 View per page 100

Src IP	Dst IP	Application	Port	Protocol	DSCP	Traffic(16.34 GB)	Percent
72.[illegible].76	121.[illegible]	ssh	22	TCP	AF11	9.29 GB	57%
11.[illegible].210	121.[illegible]182.67	ESP_App	*	ESP	AF11	5.83 GB	36%
12.[illegible]	12[illegible]182.67	TCP_App	*	TCP	AF11	501.9 MB	3%
74.[illegible]	[illegible]182.67	pop3s	995	TCP	AF11	279.06 MB	2%
173.[illegible]	[illegible]182.112	https	443	TCP	AF11	76.49 MB	<1%
72.5[illegible]	[illegible]182.67	imaps	993	TCP	AF11	67.19 MB	<1%
204.[illegible]	[illegible]182.67	TCP_App	*	TCP	AF11	56.47 MB	<1%
98.1[illegible]	[illegible]182.76	TCP_App	*	TCP	AF11	55.86 MB	<1%
74.[illegible]	[illegible]182.67	ssh	22	TCP	AF11	30.56 MB	<1%
199.[illegible]	[illegible]182.77	http	80	TCP	AF11	16.57 MB	<1%
199.[illegible]	[illegible]182.76	http	80	TCP	AF11	15.76 MB	<1%
223.[illegible]	[illegible]182.67	TCP_App	*	TCP	AF11	14.99 MB	<1%
199.[illegible]	[illegible]182.76	https	443	TCP	AF11	12.34 MB	<1%
199.[illegible]	[illegible]182.67	https	443	TCP	AF11	12.1 MB	<1%
199.[illegible]	[illegible]182.67	https	443	TCP	AF11	11.7 MB	<1%
199.[illegible]	[illegible]182.76	https	443	TCP	AF11	11.52 MB	<1%
199.[illegible]	[illegible]182.77	https	443	TCP	AF11	11.38 MB	<1%
199.[illegible]	[illegible]182.77	https	443	TCP	AF11	11.31 MB	<1%
14[illegible]	[illegible]182.111	https	443	TCP	AF11	5.03 MB	<1%
22[illegible]	[illegible]182.67	TCP_App	*	TCP	AF11	4.42 MB	<1%
223.[illegible]	[illegible]182.67	TCP_App	*	TCP	AF11	3.11 MB	<1%
124.[illegible]	[illegible]182.112	https	443	TCP	AF11	2.88 MB	<1%
119.[illegible]	[illegible]182.111	https	443	TCP	AF11	2.18 MB	<1%
199.[illegible]	[illegible]182.67	http	80	TCP	AF11	1.8 MB	<1%

Questions?

Over 4000 enterprises worldwide uses ManageEngine NetFlow Analyzer for traffic analytics

NetFlow Analyzer: www.netflowanalyzer.com

TAC Team: netflowanalyzer-support@manageengine.com

Sales: sales@manageengine.com

NetFlow Analyzer Blogs: https://blogs.netflowanalyzer.com

User Forums: http://forums.netflowanalyzer.com

Thank you.