Advanced Accounting & Performance Management with NBAR

BRKNMS-3007

Marisol Palmero

Cisco Networkers 2007

HOUSEKEEPING

- We value your feedback, don’t forget to complete your online session evaluations after each session and complete the Overall Conference Evaluation which will be available online from Friday.
- Visit the World of Solutions on Level -01!
- Please remember this is a ‘No Smoking’ venue!
- Please switch off your mobile phones!
- Please remember to wear your badge at all times including the Party!
- Do you have a question? Feel free to ask them during the Q&A section or write your question on the Question form given to you and hand it to the Room Monitor when you see them holding up the Q&A sign.

Session Abstracts

- This advanced session covers the principle of Cisco’s Network Based Application Recognition(NBAR), with a focus on accounting and performance management:

  NBAR is a device instrumentation feature in Cisco IOS® that is capable of inspecting packets up to the payload, resulting in application specific traffic statistics. The session discusses the theory, background, requirements, performance impact, and deployment scenarios, for example security analysis and traffic classification. In addition, the relationship with related features, such as QoS, NetFlow, IP SLA, and others will be addressed. It also offers an overview of management applications that support NBAR.

- The topic is relevant for network planners and administrators of both Enterprises and Service Providers that need application-specific traffic statistics. Attendees should be familiar with IP and SNMP fundamentals.

This Session Is (Not) About

+ Business case for application recognition
+ In-depth explanation of NBAR
+ Brief overview of NBAR partners applications
+ Level 3 session

– Accounting and performance management applications
– Everything you ever wanted to know about QoS, NetFlow, SNMP, IP SLA

- Suggested additional sessions

  Advanced NetFlow Deployment (BRKNMS -3006)

  Advanced Network Performance Measurement with Cisco IOS® IP SLA (BRKNMS -3004)

  Introduction to QoS (RST-1501)

  Cisco IOS® Application Optimization (APP-1205)

Agenda

- What Is the Business Case? How to Approach It?
- What Are the Nuts and Bolts of NBAR?
- How to Compare Multiple Features?
- What Did We Cover?
- What's Left?

Acknowledgment to Ralf Wolter

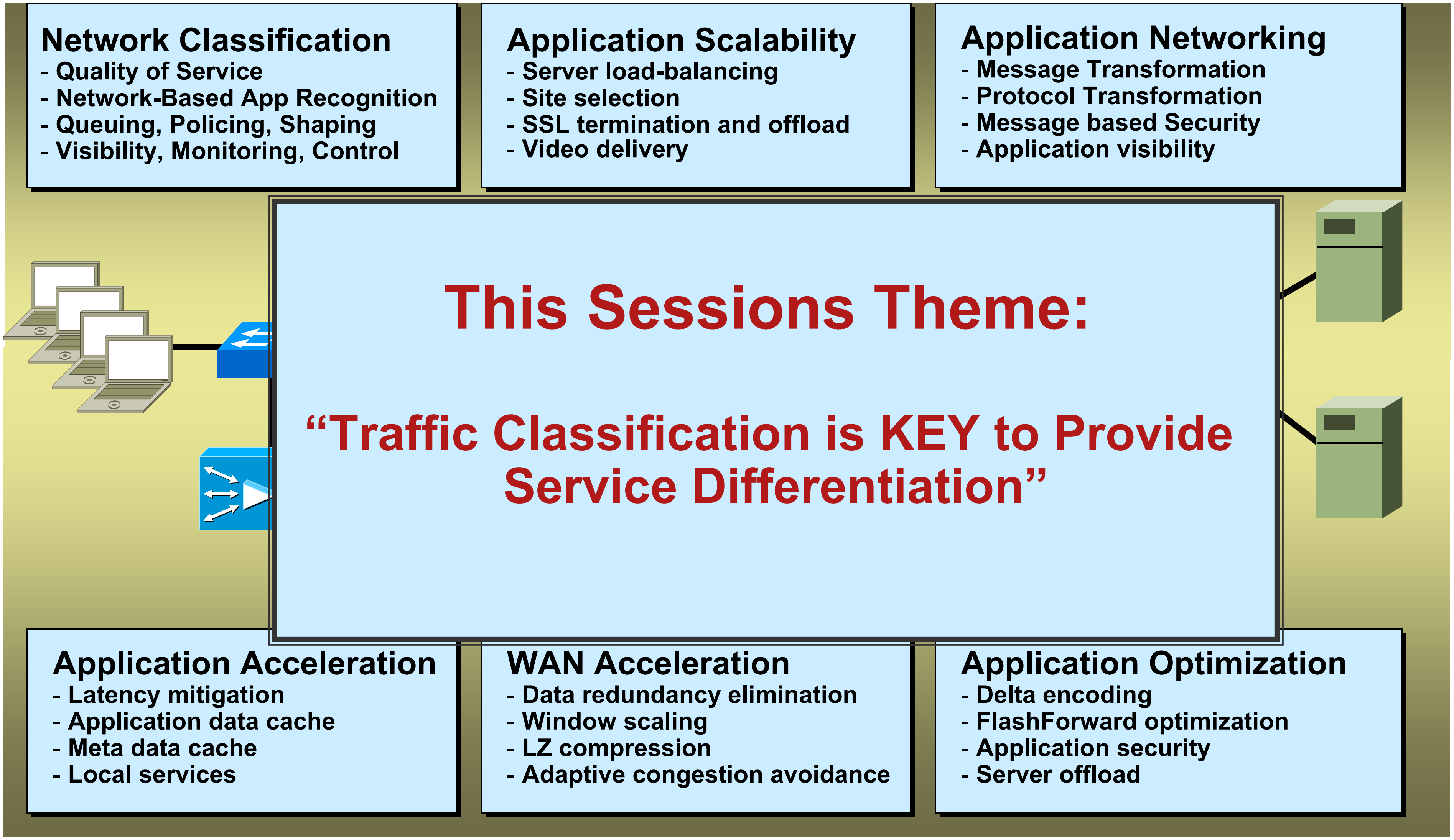
Agenda

- What Is the Business Case? How to Approach It?
- What Are the Nuts and Bolts of NBAR?
- How to Compare Multiple Features?
- What Did We Cover?
- What's Left?

Business Requirements

- How do I track which applications run on my network and what is their resources consumption?
- How do I know if users are accepting application usage policies?
- How much bandwidth should I assign to different QoS classes?
- How do I account for application resource utilization?
- How do I effectively plan to allocate and deploy applications (e.g., VoIP) most efficiently?

The Big Picture: Application Optimization Infrastructure



Network Classification
- Quality of Service
- Network-Based App Recognition
- Queuing, Policing, Shaping
- Visibility, Monitoring, Control

Application Scalability
- Server load-balancing
- Site selection
- SSL termination and offload
- Video delivery

Application Networking
- Message Transformation
- Protocol Transformation
- Message based Security
- Application visibility

This Sessions Theme:

“Traffic Classification is KEY to Provide Service Differentiation”

Application Acceleration
- Latency mitigation
- Application data cache
- Meta data cache
- Local services

WAN Acceleration
- Data redundancy elimination
- Window scaling
- LZ compression
- Adaptive congestion avoidance

Application Optimization
- Delta encoding
- FlashForward optimization
- Application security
- Server offload

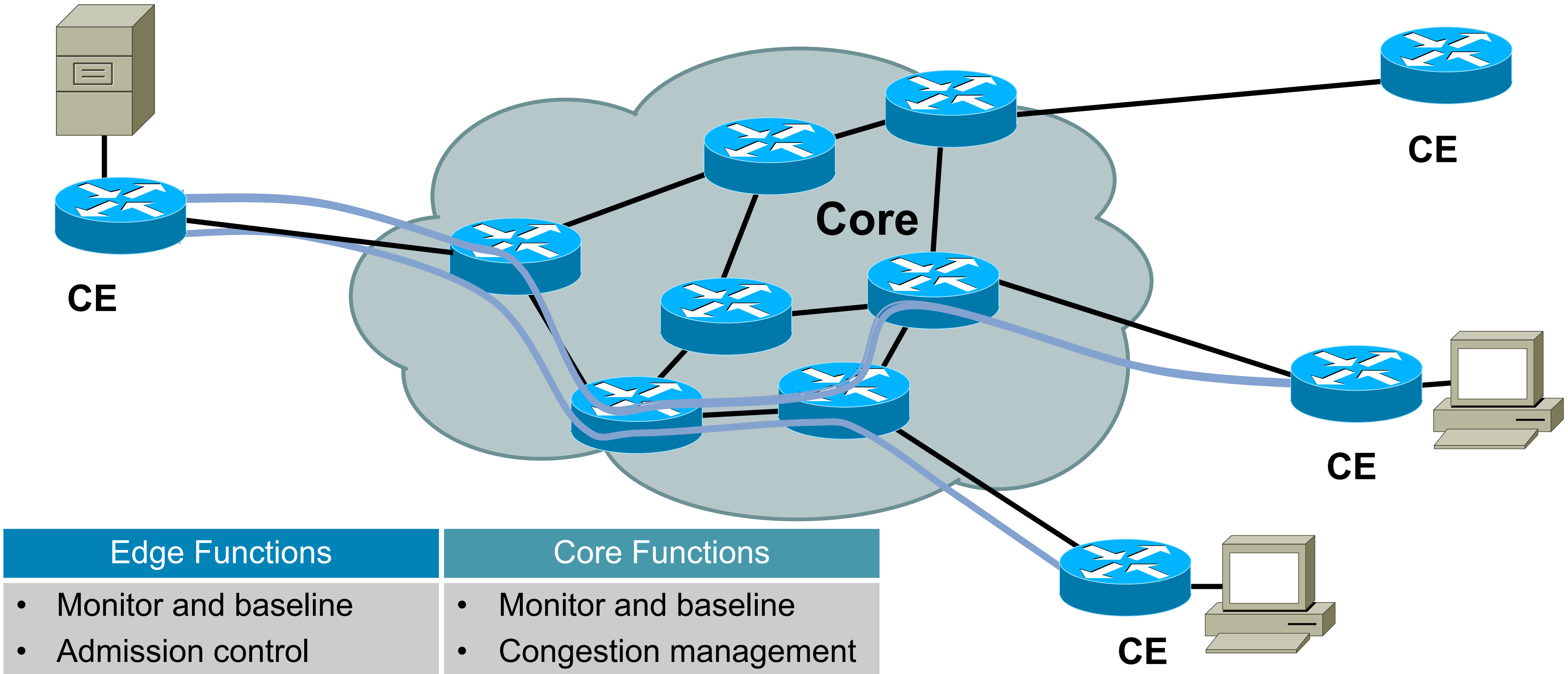
How to Identify Applications?

Application/Protocol	How to Identify?
VoIP	UDP TOS = 5
IPVC	TOS = 4
H.323	TCP Port = 1719 , 1720 and TOS = 3
IPv6 Multicast	Format Prefix (FP) = 1111 1111
VOD	TCP Port 507

Details for Accounting Collection:

- Layer three protocol type (e.g., TCP)
- Protocol port number (e.g., port 80 for http, port 23 for telnet)
- ToS byte/DSCP
- Server IP address (as a specific example)
- Traffic volume details (packets, bytes)
- Time of day (start/stop timestamp, duration)
- Data packet inspection (in some cases)

Five Use Cases: Bandwidth Monitoring, Allocation, and Verification



Edge Functions

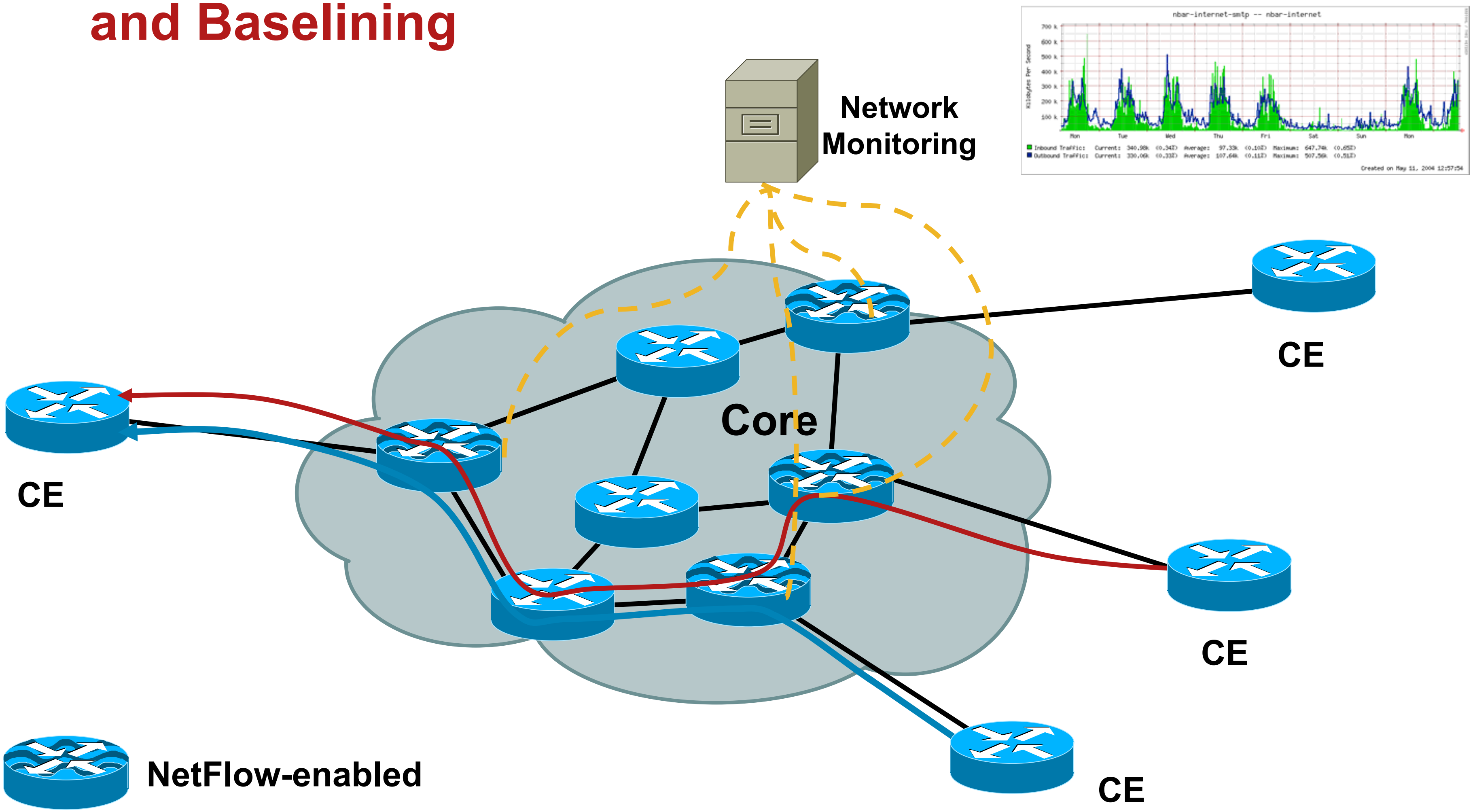
- Monitor and baseline
- Admission control
- Bandwidth provisioning
- Classification
- Marking/remarking
- Traffic shaping
- Rate limiting

Core Functions

- Monitor and baseline
- Congestion management
- Traffic engineering
- Low-latency queuing

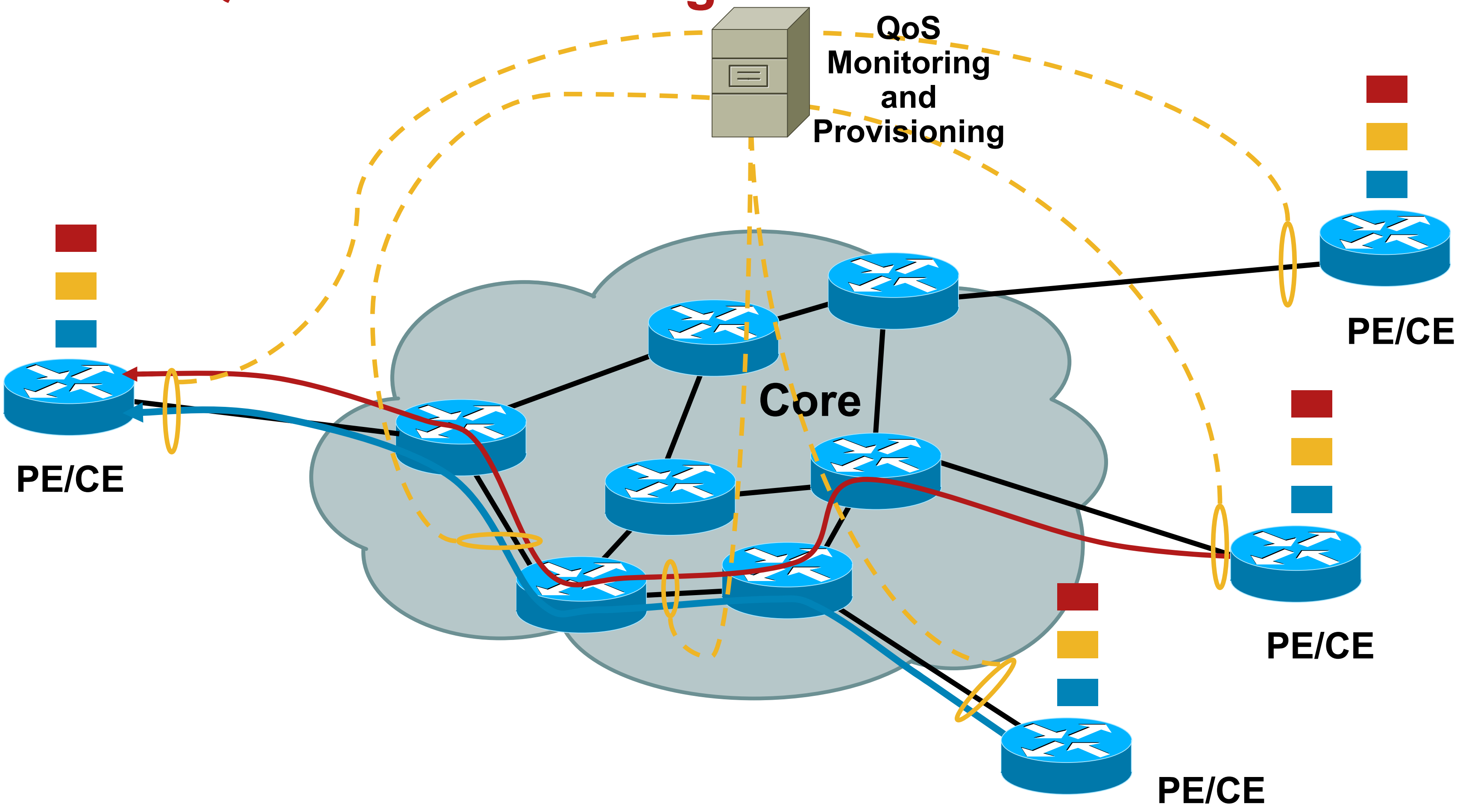
Use Case 1: Bandwidth Monitoring

Proposal: NetFlow-Based Network Monitoring and Baselining


nbar-internet-smtp -- nbar-internet
Kilobytes Per Second
700 k
600 k
500 k
400 k
300 k
200 k
100 k
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Mon
🟩 Inbound Traffic: Current: 340.98k (0.34%) Average: 97.33k (0.10%) Maximum: 647.74k (0.65%)
🟦 Outbound Traffic: Current: 330.06k (0.33%) Average: 107.64k (0.11%) Maximum: 507.56k (0.51%)
Created on May 11, 2004 12:57:54
Network Monitoring
Core
CE
CE
CE
CE
CE
NetFlow-enabled

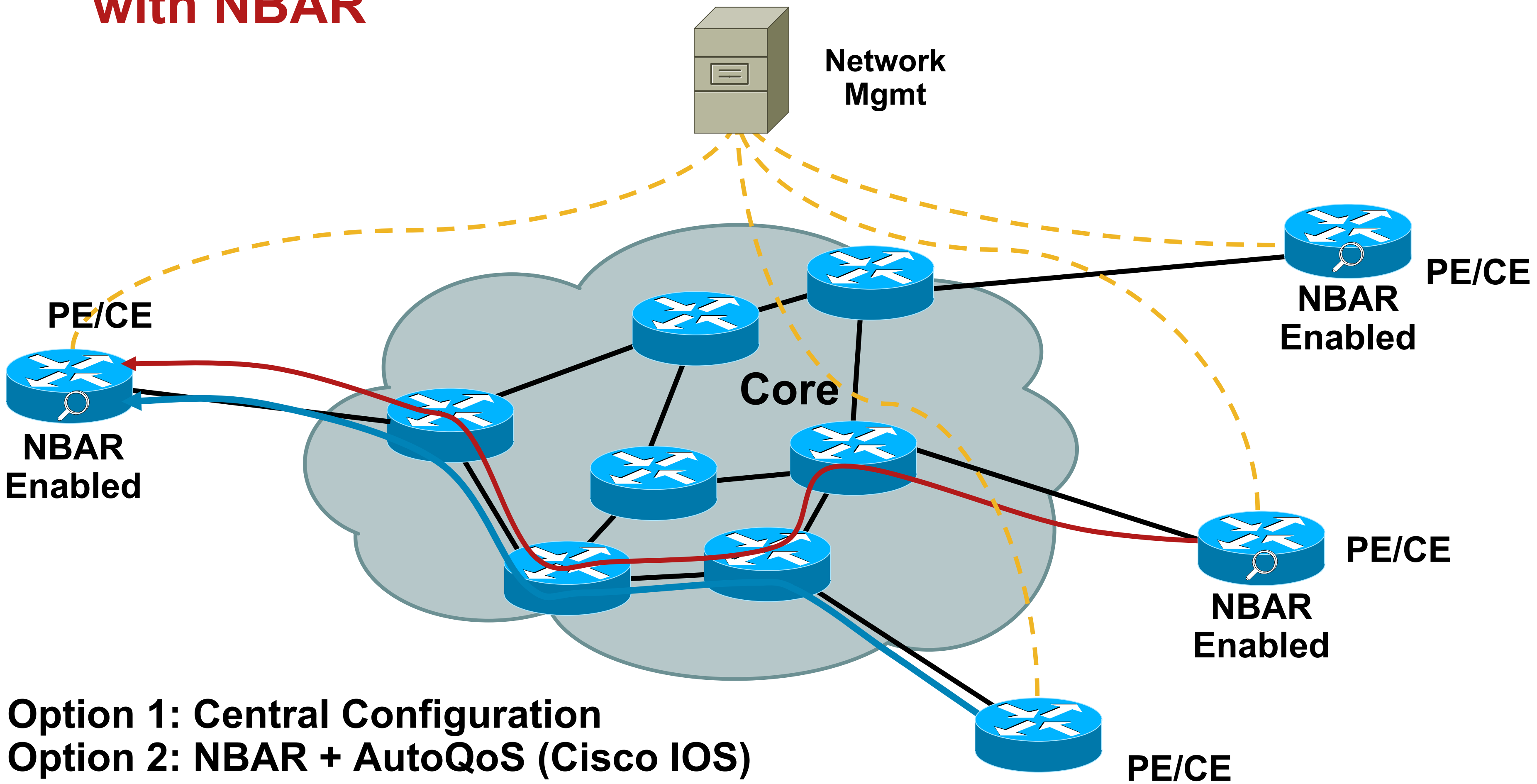
Use Case 2: Static Bandwidth Allocation

Proposal: Static QoS Configuration Based on CB-QoS-MIB Monitoring



Use Case 3:
Static BW Allocation per Application

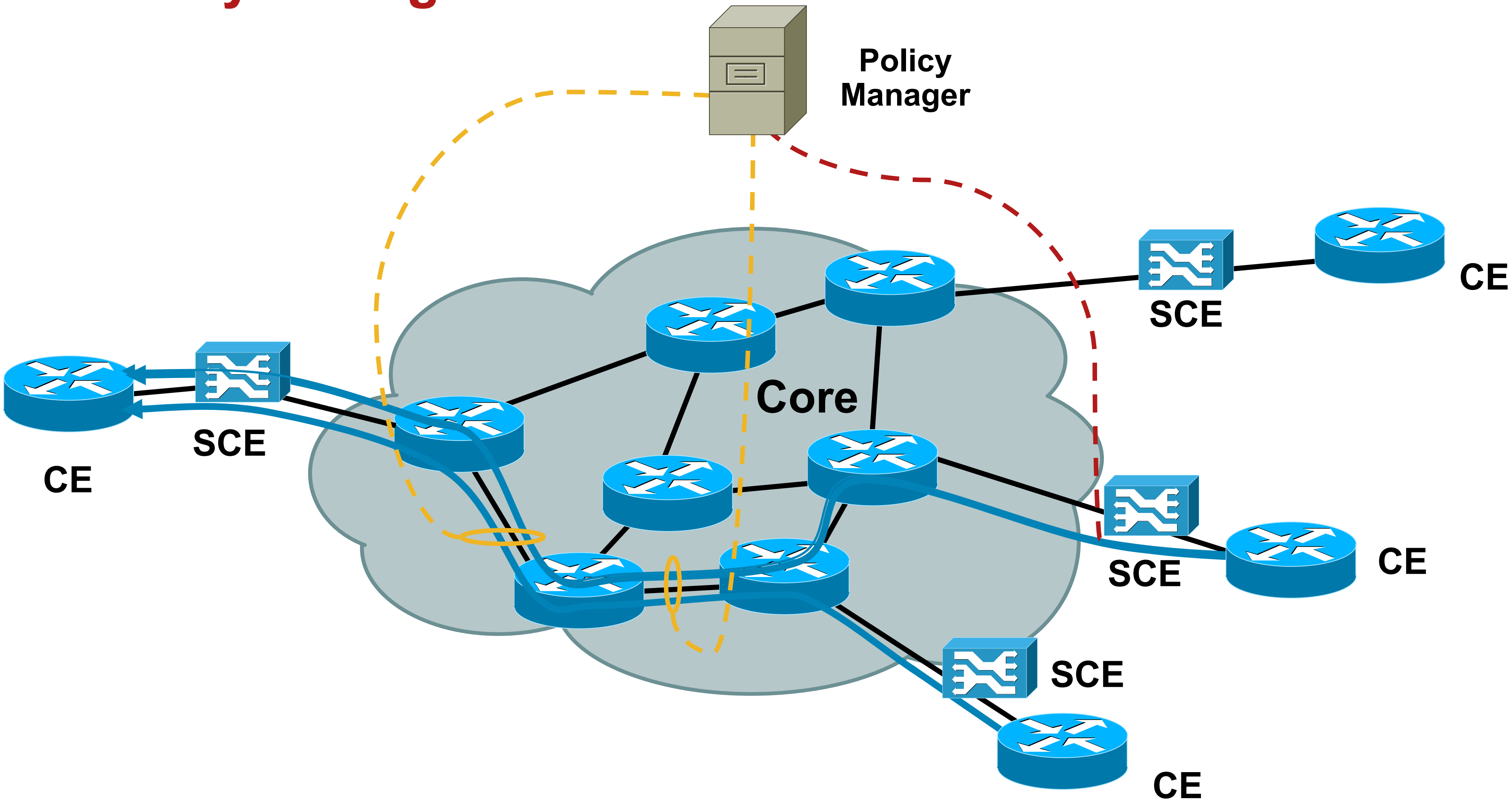
Proposal: Static Application-QoS Classification with NBAR



Option 1: Central Configuration
Option 2: NBAR + AutoQoS (Cisco IOS)

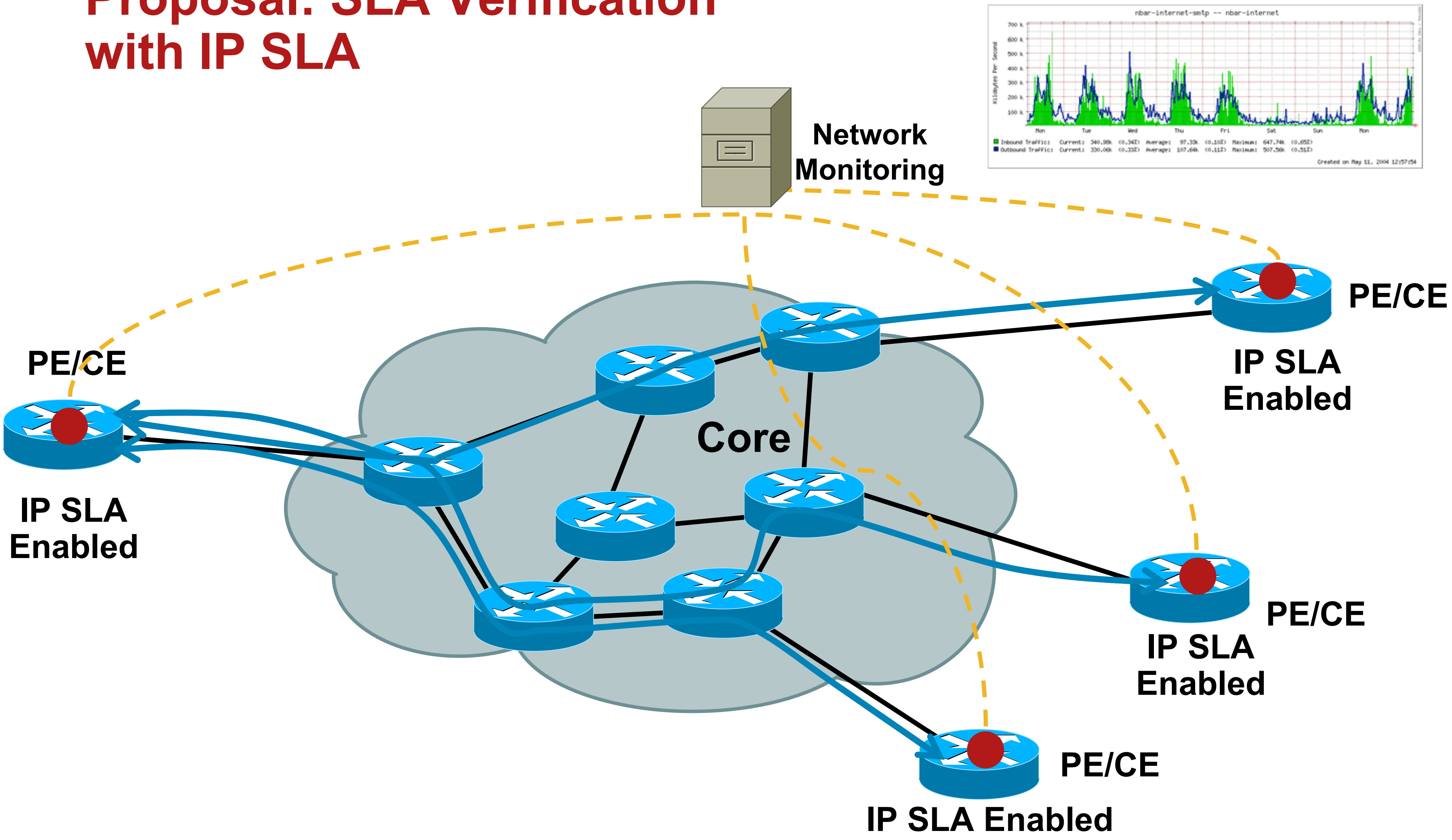
Use Case 4:
Dynamic Bandwidth Allocation

Proposal: Dynamic Configuration with SCE and Policy Manager



Use Case 5:
Pro-Active Service Monitoring

Proposal: SLA Verification with IP SLA


nbar-internet-smtp -- nbar-internet
Kilobytes Per Second
700 k
600 k
500 k
400 k
300 k
200 k
100 k
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Mon
Inbound Traffic: Current: 340.98k (0.34%) Average: 97.33k (0.10%) Maximum: 647.74k (0.65%)
Outbound Traffic: Current: 330.06k (0.33%) Average: 107.64k (0.11%) Maximum: 507.56k (0.51%)
Created on May 11, 2004 12:57:54
Network Monitoring
Core
PE/CE
IP SLA Enabled
PE/CE
IP SLA Enabled
PE/CE
IP SLA Enabled
PE/CE
IP SLA Enabled

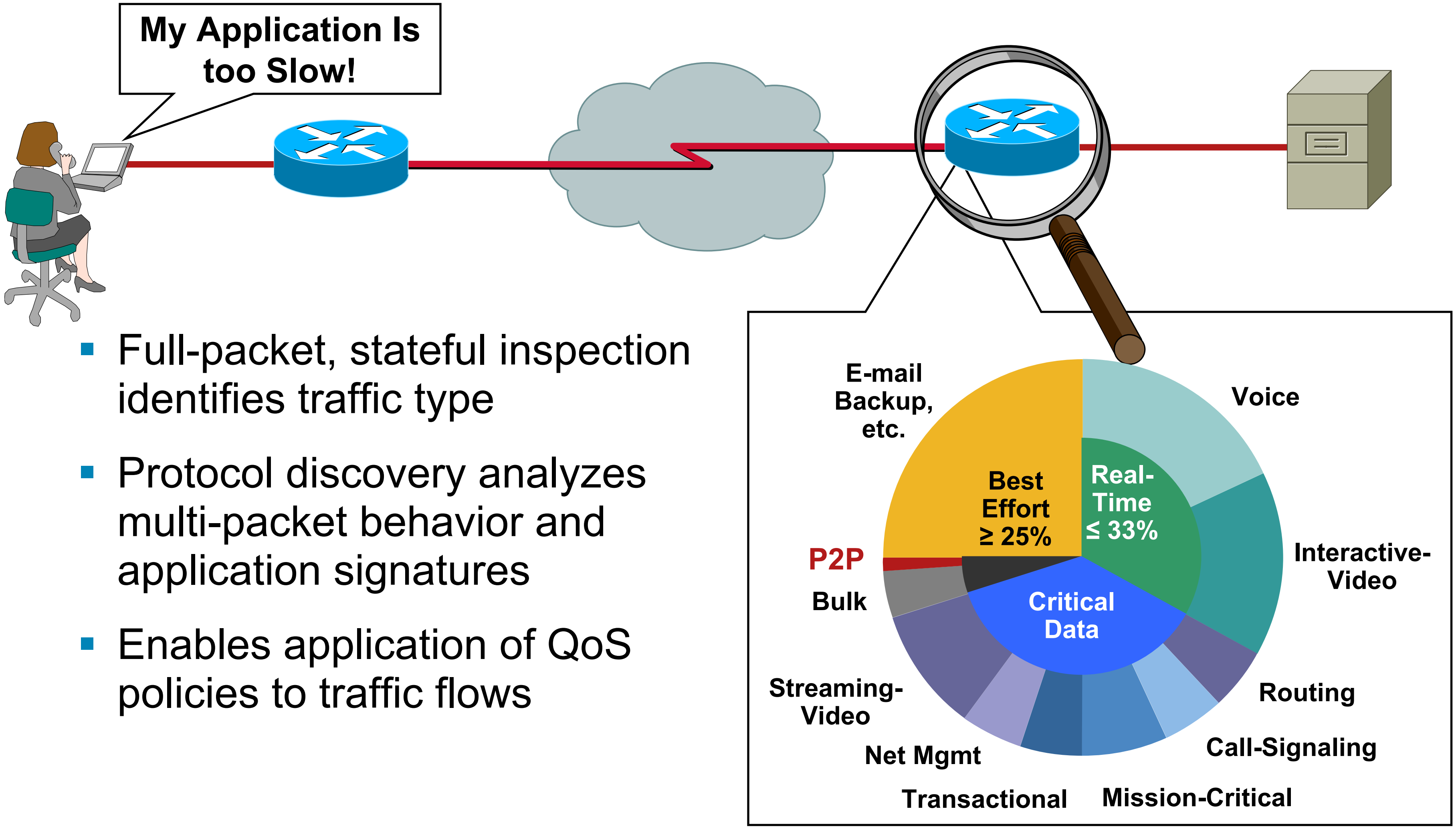
Five Use Cases: Bandwidth Monitoring, Allocation, and Verification

Function	Cisco IOS Software Feature				Appliance
	NBAR	CB-QoS-MIB	NetFlow	IP SLA	SCE
Device Monitoring	X	X	X		X
Network Monitoring				X	
Baselining	X	X	X	X	X
Static Configuration	X				X
Dynamic Configuration					X
SLA Verification				X	
Passive Measurement	X	X	X		X
Active Measurement				X	

Agenda

- What Is the Business Case? How to Approach It?
- What Are the Nuts and Bolts of NBAR?
- How to Compare Multiple Features?
- What Did We Cover?
- What's Left?

NBAR Overview



Link Utilization

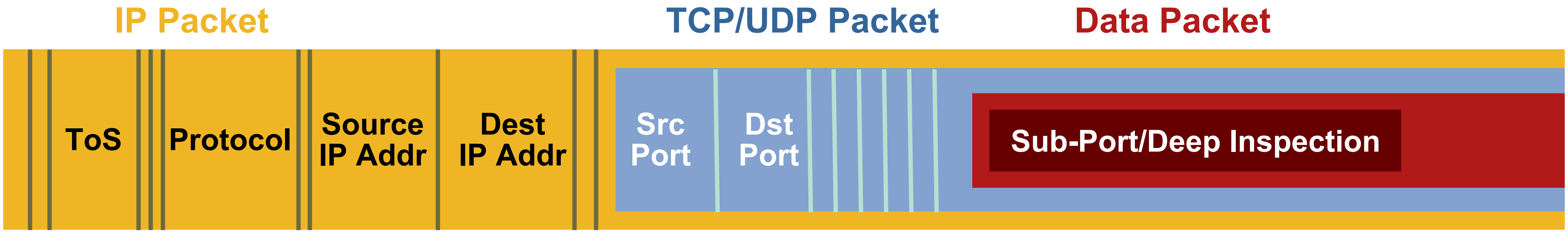
- Full-packet, stateful inspection identifies traffic type
- Protocol discovery analyzes multi-packet behavior and application signatures
- Enables application of QoS policies to traffic flows

NBAR Principles

- Network-Based Application Recognition classifies traffic by protocol (Layer 4–7)
- Protocol discovery analyzes application traffic patterns in real time and discovers which applications are running on the network
- NBAR supports Cisco IOS QoS features to apply application-level QoS policies
  - Guaranteed bandwidth with Class-based Weighted Fair Queuing (CBWFQ)
  - Policing and limiting bandwidth
  - Marking (ToS or IP DSCP)
  - Drop policy with weighted random early detection (WRED)
- Accounting functionality is provided by the NBAR "protocol discovery" feature

NBAR: Full-Packet Inspection

Stateful and Dynamic Inspection



- Identifies over 90 applications and protocols
  TCP and UDP port numbers
  - Statically assigned
  - Dynamically assigned during connection establishment
- Non-TCP and non-UDP IP protocols
- Data packet inspection for matching values
- Header classification and data packet inspection

NBAR: Two Modes of Operation

- Protocol discovery per interface
  - Protocol discovery discovers and provides real time statistics on applications
  - Per-interface, per-protocol, bi-directional statistics
    - Bit rate (bps)
    - Packet counts
    - Byte counts
- Modular QoS traffic classification
  - Policing function for “unwanted” protocols
  - “match protocol” command

NBAR Modes of Operation
CLI Examples

- Protocol discovery per interface

```
(config-if)#ip nbar protocol-discovery
```

- Modular QoS traffic classification

```
(config)#class-map [match-any|match all] myProt
(config-cmap)#match protocol custom-01
```

- Example:

```
class-map match-all http-s
  match protocol http host *www.yahoo.com*
  match protocol http mime *html*
  match protocol http s-header-field *Netscape-Enterprise*
```

NBAR Prerequisites and Limitations

- Previously CEF had to be enabled (solved!)
- NBAR takes place before post operations
- Maximum 24 concurrent URLs, hosts, or MIME type matches
- IP v4 traffic only
- Matching beyond the first 400 bytes in a packet payload was not supported initially; Cisco IOS 12.3(7)T removed this restriction and NBAR now supports full payload inspection
- Custom protocol traffic can only inspected the first 255 bytes of the payload
- “Multiple Matches” feature is limited to the first 4 bytes of the payload

NBAR: Unsupported Features

- Multicast
- MPLS-labeled packets
- IPv6
- virtual TCP reassembly, VPR (virtual packet reassembly)
- Pipelined persistent HTTP requests
- URL/host/MIME classification with secure HTTP (encrypted traffic)
- Asymmetric flows with stateful protocols

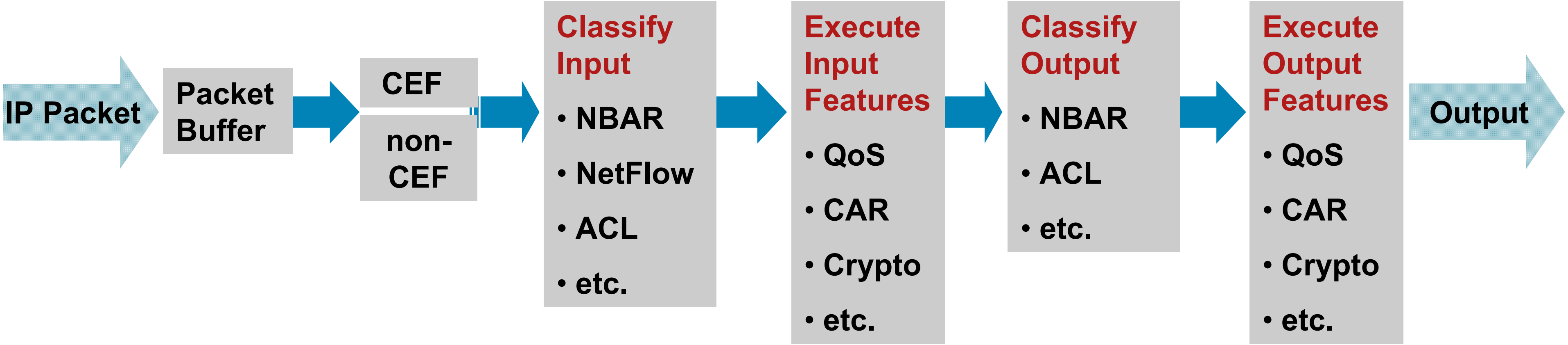
NBAR: Main Supported Platforms

Cisco IOS Release		
12.4T	12.4 Mainline	12.2S
Cisco 800 above 871	Cisco 800 above 831	Cisco 7200
Cisco 1700	Cisco 1700	Cisco 7301
Cisco 1800	Cisco 1800	Cisco 7304-NPE
Cisco 2600XM	Cisco 2600XM	
Cisco 2800	Cisco 2800	
Cisco 3600	Cisco 3600	
Cisco 3700	Cisco 3700	
Cisco 3800	Cisco 3800	
Cisco 7200	Cisco 7200	
Cisco 7301	Cisco 7301	
	Cisco 7500 with VIP2-50 or above	

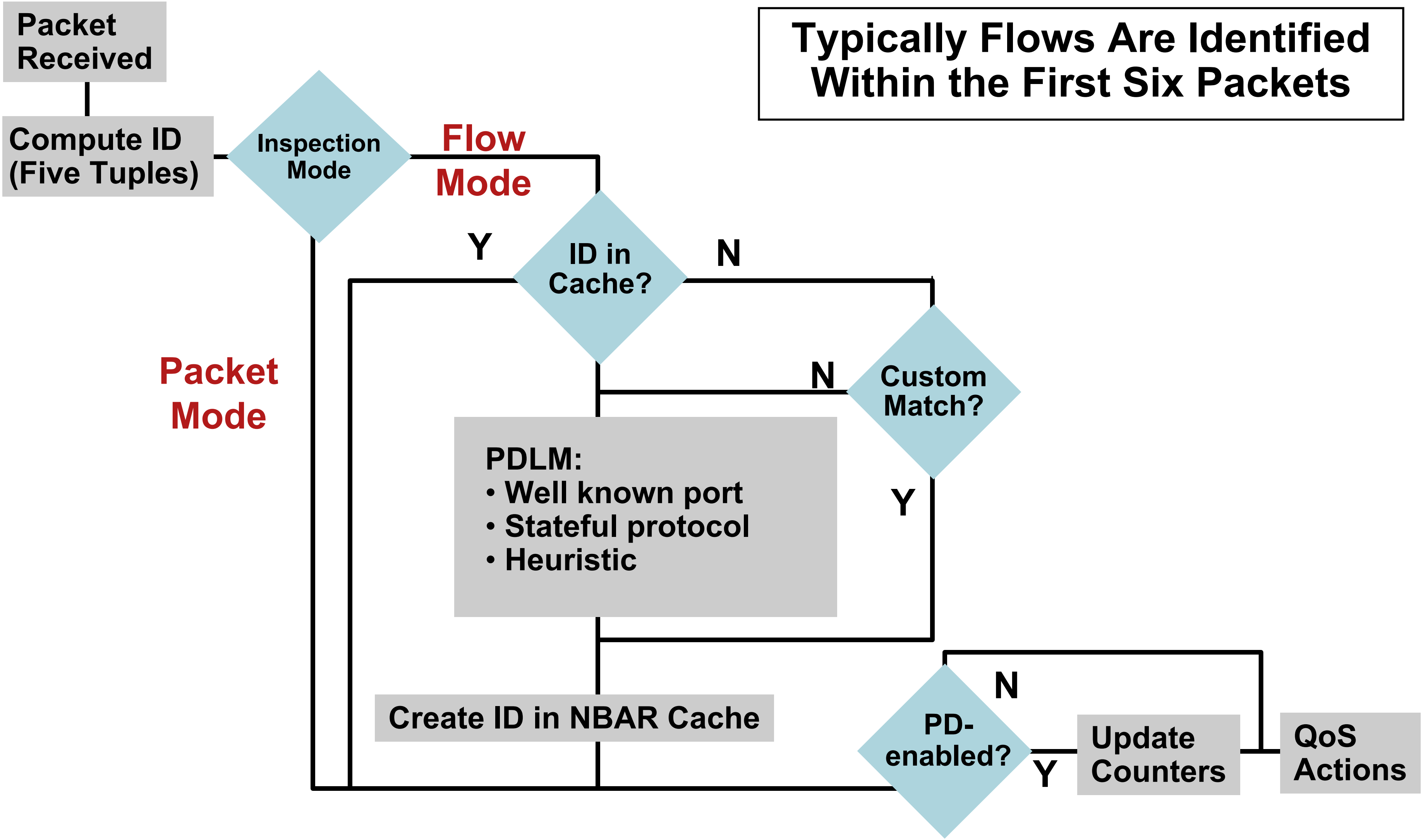
Cisco Catalyst® 6000 (sup32-PISA)/Cisco 7600

- SUP1/SUP1a/SUP2: software-based implementation
- SUP32: hardware-based with SUP32-PISA. Also supports the Flexwan, Enhanced Flexwan & SIP-200
- SUP720: SIP-200, FlexWAN and enhanced FlexWAN interfaces (software-based implementation)
- Also supported on the Multiprocessor WAN Application Module (MWAM) (6*7200 on a board)

NBAR in the Router’s Forwarding Path



NBAR—Processing Packets



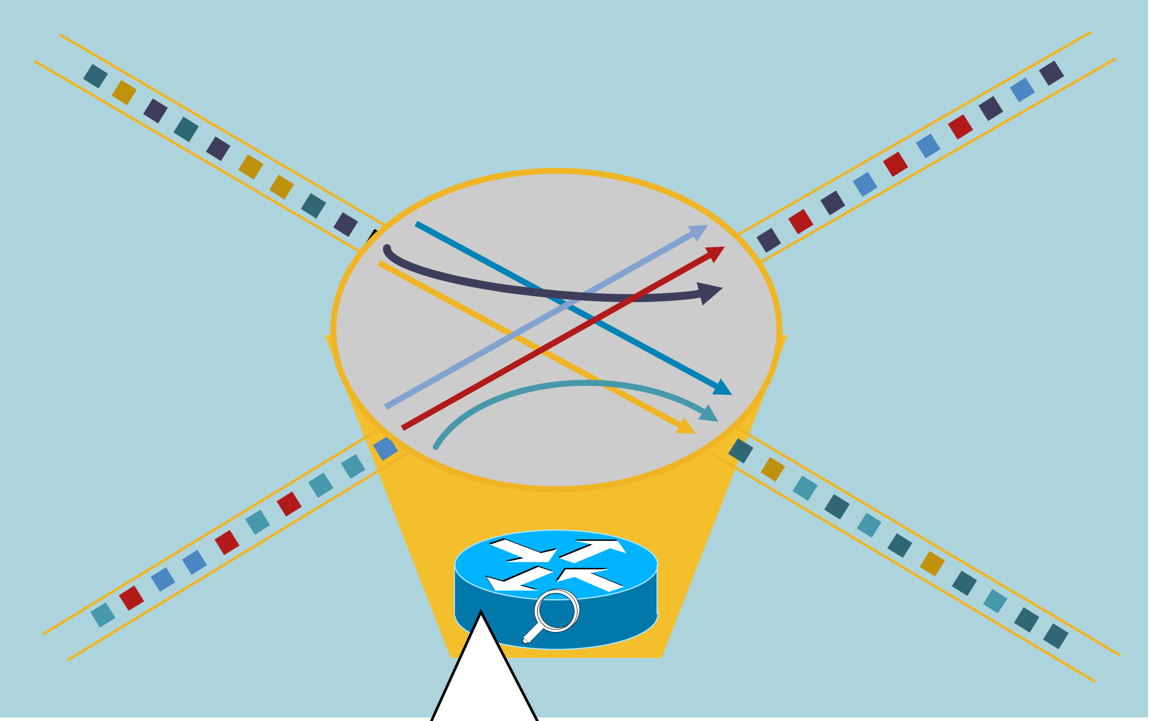
Typically Flows Are Identified Within the First Six Packets

NBAR Flow-based Analysis

Five Tuples Define a Flow Within the PDLM

1. Source IP address
2. Destination IP address
3. Source port
4. Destination port
5. L3 protocol type

A Flow Is Unidirectional!



NBAR Protocol Statistics CLI/MIB

NBAR Resources

- Flow concept is required for stateful inspection
  150 bytes per flow; 1 MB DRAM = 5,000 flows
- Flow cache: track for state changes, e.g. a control flow starts a data channel (e.g., FTP download starts on other port numbers)

```
Router(config)#ip nbar resources [flow-idle-time]
  [initial-memory] [max-memory]

    <10-86400> max-idle time (in seconds). Default=30s

    <100-8000> Initial memory (in kBytes). Default: 1 MB

    <0-2000>   Amount of memory to expand by (in kBytes)
```

NBAR Protocol Discovery

- Configure traffic statistics collection for all protocols known to NBAR
- Discover application protocols transiting an interface
- Supports both input and output traffic
- Can be applied with or without a service policy

```
(config-if)#ip nbar protocol-discovery
```

```
Router# show ip nbar protocol-discovery [interface
interface-spec][stats {byte-count|bit-rate|packet-
count}][protocol protocol-name| top-n number}]
```

NBAR Protocol Discovery Example

```
router# show ip nbar protocol-discovery interface FastEthernet 6/0

  FastEthernet6/0
                   Input                           Output
  Protocol         Packet Count                    Packet Count
                   Byte Count                      Byte Count
                   5 minute bit rate (bps)         5 minute bit rate (bps)
  -----------      ------------------------        ------------------------
  http             316773                          0
                   26340105                        0
                   3000                            0
  pop3             4437                            7367
                   2301891                         339213
                   3000                            0
  snmp             279538                          14644
                   319106191                       673624
                   0                               0
  ftp              8979                            7714
                   906550                          694260
                   0                               0
  …
  Total            17203819                        151684936
                   19161397327                     50967034611
                   4179000                         6620000
```

NBAR Top-N Statistics

```
Router#show ip nbar protocol-discovery top-n 5
Serial0/0
              Input                    Output
Protocol      Packet Count             Packet Count
              Byte Count               Byte Count
              5 minute bit rate (bps)5 minute bit rate (bps)
  ---------- ------------------------ ------------------------
  custom-01        40565                        40565
                   2596160                      2596160
                   3000                         3000
  telnet           395                          75
                   28539                        6415
                   0                            0
  icmp             101                          100
                   7360                         6860
                   0                            0
  snmp             28                           0
                   1988                         0
                   0                            0
  netbios          9                            0
                   738                          0
                   0                            0
  unknown          205                          204
                   14976                        10404
                   0                            0
  Total            41304                        40944
                   2649809                      2619839
                   3000                         3000
```

- Top-N for all interfaces with NBAR protocol discovery enabled
- NBAR-PD- MIB provides Top-N for all interfaces where N can differ for each interface

NBAR Protocol Discovery MIB

- MIB functionality

    Enable/disable NBAR protocol discovery per interface

    Display the protocols/applications recognized by NBAR

    Key statistics are associated with each protocol, which can be used to define traffic classes and QoS policies

    A configurable protocol Top-N table

    Configure thresholds: report breaches and send notifications when these thresholds are crossed

    Configure notifications (traps) based on statistic thresholds

    Maintain a history table of all notification events (max. 5,000)

    Hysterisis mechanism stops multiple traps occurring for same breached threshold within a sample period

- Introduced in Cisco IOS 12.2 (15) T

NBAR Protocol Discovery MIB Tables

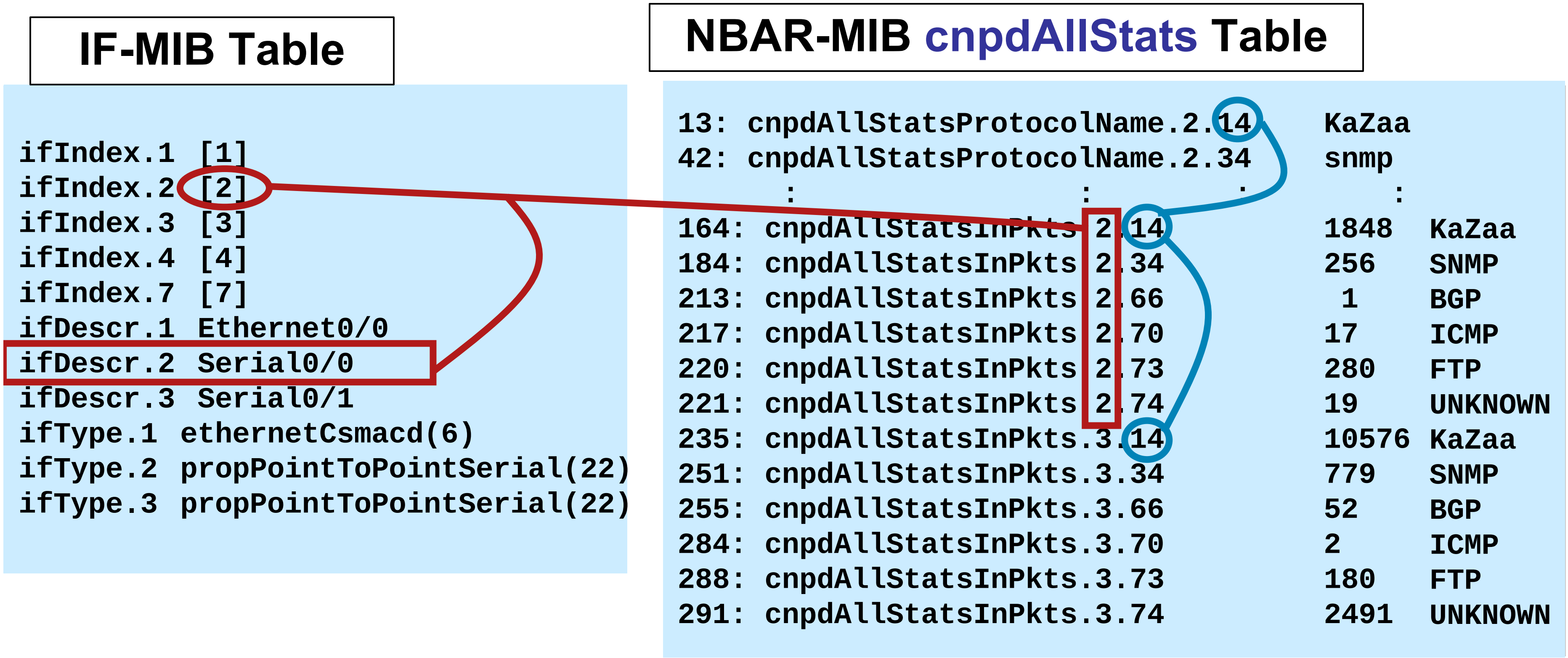
Table	Description	SNMP Access
cnpdSupportedProtocols	List of all supported protocols	Read-only
cnpdAllStats	All NBAR statistics per interface	Read-only
cnpdTopNstats	Top-N table statistics	Read-only
cnpdThresholdhistory	History of falling rising events	Read-only
cnpdStatus	Enable or disable NBAR per interface, including time-stamp	Read-write
cnpdTopNconfig	Configure top-N table by interface	Read-write
cnpdThresholdconfig	Protocol threshold configuration	Read-write
cnpdNotificationsconfig	Enable traps	Read-write
cnpdMIBNotifications	Rising or falling events	N/a

MIB Description

- Statistics table
  - A per interface list of protocols and applications (byte-count, packet-count and bit-rate statistics)
  - List updates regularly
  - At a glance view of the application traffic on each interface—with no configuration required
- Top-N statistics table
  - Select interface, sample period and the statistic used to base the table on
  - 1,024 top-N tables can exist across all interfaces in total
  - Tables are ordered by which application is using the most bandwidth
  - Monitor applications that use the highest bandwidth per interface

NBAR Protocol Discovery MIB: Example

- Indexed by interface and protocol
- In/out bytes, packets, and bit rate
- All protocols per interface listed
- Protocols not discovered: per interface count = 0



IF-MIB Table

```
ifIndex.1  [1]
ifIndex.2  [2]
ifIndex.3  [3]
ifIndex.4  [4]
ifIndex.7  [7]
ifDescr.1  Ethernet0/0
ifDescr.2  Serial0/0
ifDescr.3  Serial0/1
ifType.1  ethernetCsmacd(6)
ifType.2  propPointToPointSerial(22)
ifType.3  propPointToPointSerial(22)
```

NBAR-MIB cnpdAllStats Table

```
13: cnpdAllStatsProtocolName.2.14    KaZaa
42: cnpdAllStatsProtocolName.2.34    snmp
      :                 :        :         :
164: cnpdAllStatsInPkts.2.14         1848   KaZaa
184: cnpdAllStatsInPkts.2.34         256    SNMP
213: cnpdAllStatsInPkts.2.66          1     BGP
217: cnpdAllStatsInPkts.2.70         17     ICMP
220: cnpdAllStatsInPkts.2.73         280    FTP
221: cnpdAllStatsInPkts.2.74         19     UNKNOWN
235: cnpdAllStatsInPkts.3.14         10576  KaZaa
251: cnpdAllStatsInPkts.3.34         779    SNMP
255: cnpdAllStatsInPkts.3.66         52     BGP
284: cnpdAllStatsInPkts.3.70         2      ICMP
288: cnpdAllStatsInPkts.3.73         180    FTP
291: cnpdAllStatsInPkts.3.74         2491   UNKNOWN
```

NBAR Protocol Discovery MIB: Thresholds and Traps

- Set thresholds on individual protocols on an interface, or on a statistic regardless of protocol

  Thresholds for any combination of supported protocols/and or all protocols

- Configurable statistic types

  Interface in, out and sum

  Bytes, packets, and bit rate

- Information is stored for prolonged period of time if the threshold is breached

- Notification (trap) is generated and sent with a summary of threshold information

NBAR Protocol Discovery MIB: Notification Example

Binding #1: sysUpTimeInstance * (timeticks) 0 days 03h:17m:14s.19th**

System up time when notification occurred

Binding #2: snmpTrapOID.0 * (oid) cnpdThresholdFallingEvent**

Monitored protocol was above but has now fallen below configured threshold for this interface.

Note for each ThresholdRisingEvent there will be a ThresholdFallingEvent

Binding #3: cnpdThresholdConfigIfIndex.1 * (int32) 3 [3]**

Ifindex.3 Serial0/1

Binding #4: cnpdThresholdConfigStatsSelect.1 * (int32) bitRateSum(3)**

Monitoring Serial0/1 (inbound + outbound)bit rate

Binding #5: cnpdThresholdHistoryValue.1 * (int32) 1**

serial0/1 (inbound+ outbound) bit rate = 1b/s

Binding #6: cnpdThresholdConfigFalling.1 * (int32) 5**

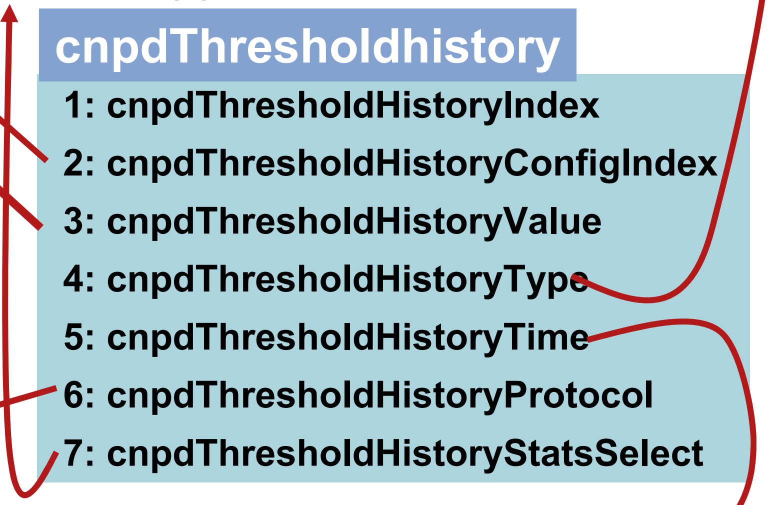
Configured falling threshold for

(inbound+ outbound)bit rate = 5 b/s

Binding #7: cnpdThresholdHistoryProtocol.1 * (int32) 33**

Protocol monitored 33 = Telnet

Binding #8: cnpdThresholdHistoryTime.1 * (timeticks) 0 days 03h:17m:14s.18th**



cnpdThresholdhistory

1: cnpdThresholdHistoryIndex
2: cnpdThresholdHistoryConfigIndex
3: cnpdThresholdHistoryValue
4: cnpdThresholdHistoryType
5: cnpdThresholdHistoryTime
6: cnpdThresholdHistoryProtocol
7: cnpdThresholdHistoryStatsSelect

NBAR Protocol Discovery MIB:
Traffic Classification and Real-Time Statistics

- Automatically uses all PDLMs

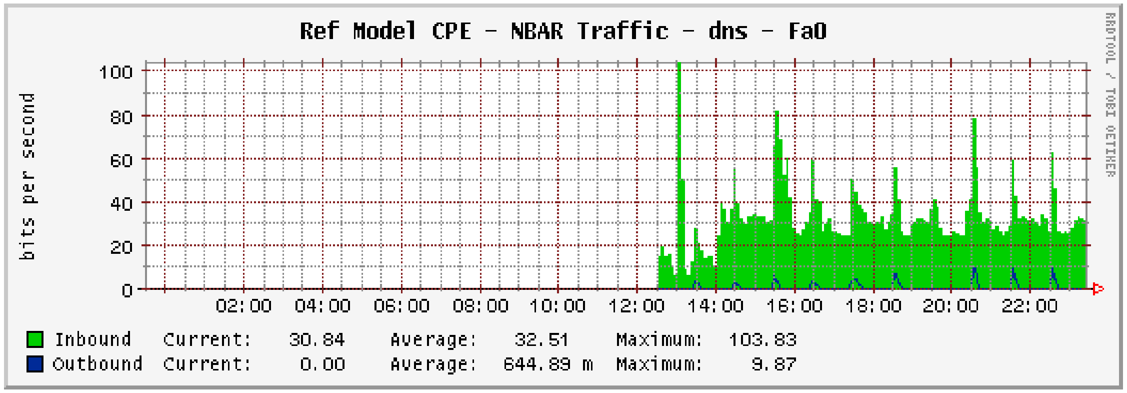
  Run protocol discovery instead of specifying individual protocols

- Provides statistics per application, per interface via SNMP

  Bit rate (bps)

  Packet counts

  Byte counts



NBAR Protocol Discovery MIB Availability

- All platforms that currently support NBAR
- Introduced at 12.2(15)T
- Cisco IOS documentation
  http://cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455984.html

NBAR Traffic Classification Commands

- Configuration commands

```
match protocol
ip nbar custom
ip nbar pdlm
ip nbar port-map
ip nbar resources
```

To modify or redefine the port numbers in use by the router

- Show commands

```
show ip nbar version
show ip nbar port-map
show ip nbar pdlm
show ip nbar protocol-discovery
```

To confirm the port numbers in use by the router

NBAR Configuration of Traffic Classification

Enable Protocol Discovery

```
router(config)# interface FastEthernet 0/1
router(config-if)# ip nbar protocol discovery
```

Define Traffic Match

```
router(config)# class-map match-all MyTraffic
router (config-cmap)# match protocol gnutella file-transfer “*”
router (config-cmap)# match protocol gnutella file-transfer “*.mpeg”
```

Option to Create a Policy

```
router(config)# policy-map MyPolicy
router(config-pmap)# class MyTraffic
router(config-pmap-c)#
router(config-pmap-c)# set dscp 1
router(config-pmap-c)# set ip precedence 5
router(config-pmap-c)# police rate percent 50
```

Apply Policy

```
router(config)# interface FastEthernet 0/1
router(config-if)# service-policy output MyPolicy
```

Defining a class-map: Traffic Match Options

```
Router(config)#class-map match-all nbar_test
Router(config-cmap)#match ?
        access-group           Access group
        any                    Any packets
        class-map              Class map
        cos                    IEEE 802.1Q/ISL class of service
        destination-address    Destination address
        discard-class          Discard behavior identifier
        dscp                   Match DSCP in IP(v4) and IPv6 packets
        fr-de                  Match on Frame-relay DE bit
        fr-dlci                Match on fr-dlci
        input-interface        Select an input interface to match
        ip                     IP specific values
        mpls                   MPLS specific values
        not                    Negate this match result
        packet                 Layer 3 Packet length
        precedence                      Match Precedence in IP(v4) packets
        protocol               Protocol
        qos-group                       Qos-group
        source-address         Source address
```

Enables NBAR

NBAR “clear” Command

- Clear all counters

```
router# clear ip nbar
    Clear all NBAR Protocol Discovery statistics? [yes]: n
    NBAR packet capture is not enabled
    NBAR state-graph tracing is not enabled
    Port statistics for unclassified packets is not turned on
```

- Clear counters at a specific interface

```
router# clear ip nbar protocol-discovery interface gi 0/0
    Clearing NBAR Protocol Discovery statistics on
    GigabitEthernet0/0
    Proceed? [yes]: yes
```

NBAR PDL and PDLM

- PDLM (Protocol Description Language Module), the heart of the NBAR engine
- PDL (native): part of the Cisco IOS image (show ip nbar version)
- PDLM (non-native extensions): download from CCO
  PDLMs become PDLs in the next release (show ip nbar pdlm)
- PDLMs are separated files that add quick support for new protocols and applications
- PDLM are loaded from flash memory, usually no reboot
- Do not require an Cisco IOS upgrade; exception: Skype with Cisco IOS 12.4(4)T (no PDLM)
- PDLM size ~ 100kB (e.g., http 115kB)
- To load a PDLM to a router

  http://www.cisco.com/cgi-bin/tablebuild.pl/pdlm
- No proactive notification of new PDLM

NBAR PDLM Configuration

- CLI “match protocol” displays the protocols that NBAR supports

```
Router(config)#class-map match-all nbar_test
Router(config-cmap)#match protocol ?
 …
 bittorrent    bittorrent
 …
 citrix        Citrix Systems Metaframe 3.0
 …
 directconnect Direct Connect Version 2.0
 …
…
```

All protocols listed, even if added as PDLM

NBAR PDLM Show and Load Command

```
Router# show ip nbar version
   *Feb 21 16:06:17.363: %SYS-5-CONFIG_I: Configured from
   console by console version

   NBAR software version: 6


   …

   14 napster          Mv: 3
   15 fasttrack        Mv: 2
   16 gnutella         Mv: 3, Nv: 2; disk1:gnutella.pdlm
   17 kazaa2           Mv: 7
```

Added with a PDLM

To load the PDLM
to the router

```
Router(config)# ip nbar pdlm device:pdlm-name
```

NBAR Supported Protocols

Enterprise Applications	Security and Tunneling	Network Mail Services	Internet
Citrix ICA	GRE	IMAP	FTP
PCAnywhere	IPINIP	POP3	Gopher
Novadigm	IPsec	Exchange	HTTP
SAP	L2TP	Notes	IRC
Routing Protocols	MS-PPTP	SMTP	Telnet
BGP	SFTP	Directory	TFTP
EGP	SHTTP	DHCP/BOOTP	NNTP
EIGRP	SIMAP	Finger	NetBIOS
OSPF	SIRC	DNS	NTP
RIP	SLDAP	Kerberos	Print
Network Management	SNNTP	LDAP	X-Windows
ICMP	SPOP3	Streaming Media	Peer-to-Peer
SNMP	STELNET	CU-SeeMe	BitTorrent
Syslog	SOCKS	Netshow	Direct Connect
RPC	SSH	Real Audio	eDonkey/eMule
NFS	Voice	StreamWorks	FastTrack
SUN-RPC	H.323	VDOLive	Gnutella
Database	RTCP	RTSP	KaZaA
SQL*NET	RTP	MGCP	WinMX
MS SQL Server	SIP	Signaling	
	SCCP/Skinny	RSVP	
	Skype		

PDLM Details: Protocol Matches

With PDLMs

edonkey.pdl, gnutella.pdl, napster.pdl, rtp.pdl, skype.pdl, sunrpc.pdl, bittorrent.pdl, exchange.pdl, netshow.pdl, rtsp.pdl, sqlnet.pdl, tftp.pdl, citrix.pdl, fasttrack.pdl, http.pdl, rcmd.pdl, rtspplayer.pdl, vdolive.pdl, custom.pdl, kazaa2.pdl, realaudio.pdl, winmx.pdl, directconnect.pdl, ftp.pdl, mgcp.pdl, rtcp.pdl, skinny.pdl, streamwork.pdl,

Port or Protocol ID Matched

egp, gre, icmp, eigrp, h323, sip, ipinip, ipsec, ospf, bgp, cuseeme, dhcp, dns, finger, gopher, secure-http, imap, secure-imap, irc, secure-irc, kerberos, l2tp, ldap, secure-ldap, sqlserver, netbios, nfs, nntp, secure-nntp, notes, ntp, pcanywhere, pop3, secure-pop3, pptp, rip, rsvp, smtp, snmp, socks, ssh, syslog, telnet, secure-telnet, secure-ftp, xwindows, printer, novadigm

Recently Added PDLMs

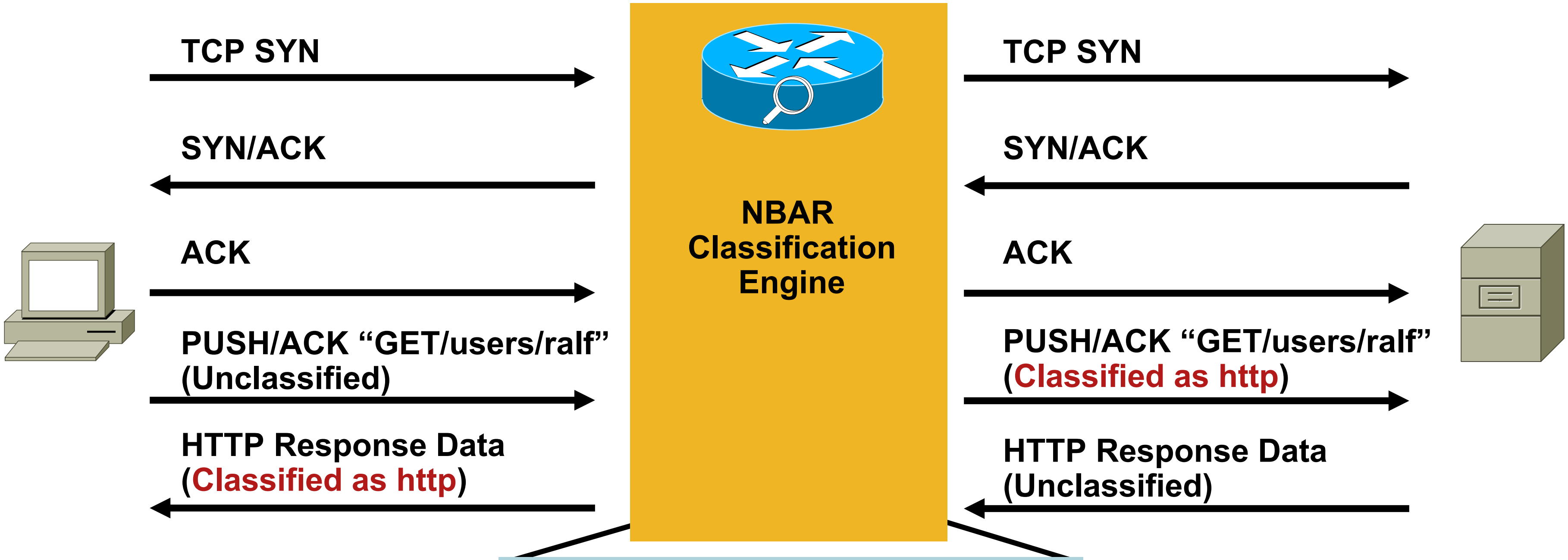
- Peer-to-peer traffic
  - WinMX
  - eDonkey and eMule
  - BitTorrent
  - Gnutella update
  - DirectConnect
  - Skype (v1) 12.4(4)T
- User-defined custom classification
  - HTTP header field classification 12.3(11)T
  - Multiple matches per port 12.4(2)T

- Corporate applications
  - Citrix ICA priority packet tagging
  - SAP
  - Client—application server
  - Client—message server
  - App server—app server

- Protocols
  - Real-Time Streaming Protocol (RTSP)
  - Session Initiation Protocol (SIP)
  - Skinny
  - Media Gateway Control Protocol (MGCP)
  - Real Time Control Protocol (RTCP)
  - Layer 2 Tunneling Protocol (L2TP)

Cisco software download: NBAR packet description language modules
www.cisco.com/pcgi-bin/tablebuild.pl/pdlm

NBAR PDLM Example: HTTP



TCP SYN

SYN/ACK

ACK

PUSH/ACK "GET/users/ralf"
(Unclassified)

HTTP Response Data
(Classified as http)

NBAR
Classification
Engine

TCP SYN

SYN/ACK

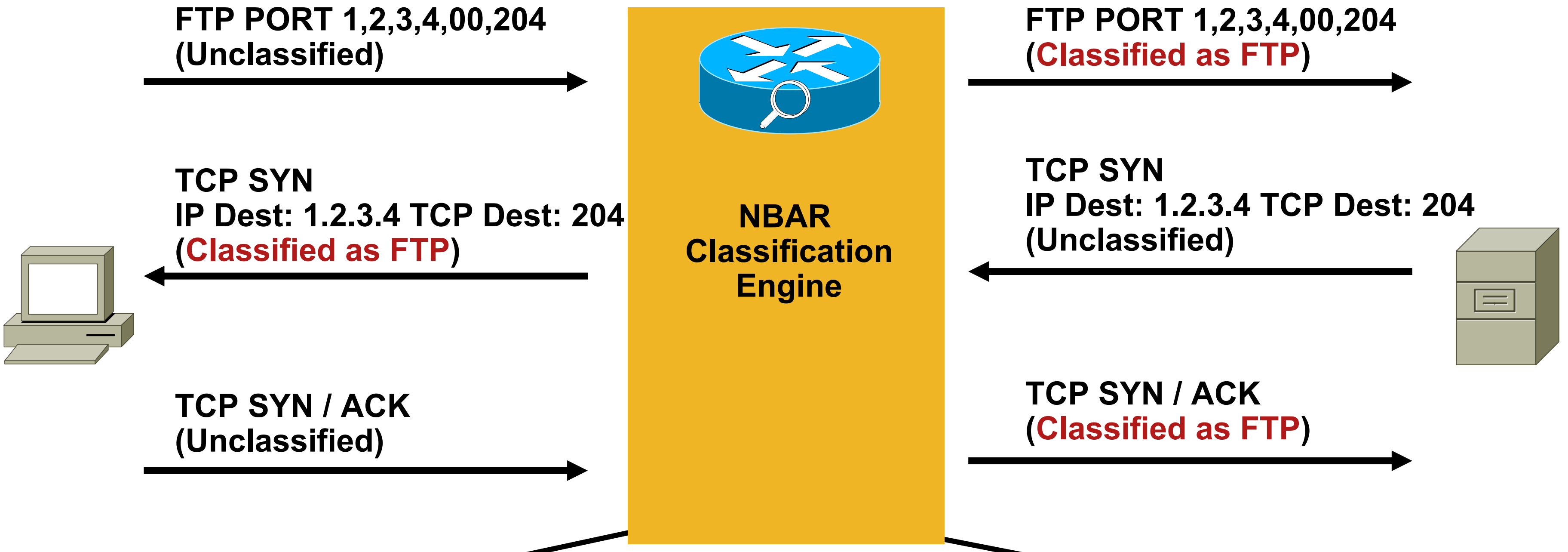
ACK

PUSH/ACK "GET/users/ralf"
(Classified as http)

HTTP Response Data
(Unclassified)

```
class-map nbar_http_url_ralf
 match protocol http url "/users/ralf"
!
policy-map policy_ralf
 class nbar_http_url_ralf
  set precedence 7
!
interface FastEthernet1/0
 service policy input policy_ralf
 service policy output policy_ralf
```

NBAR PDLM Example: FTP



FTP PORT 1,2,3,4,00,204
(Unclassified)

TCP SYN
IP Dest: 1.2.3.4 TCP Dest: 204
(Classified as FTP)

TCP SYN / ACK
(Unclassified)

NBAR
Classification
Engine

FTP PORT 1,2,3,4,00,204
(Classified as FTP)

TCP SYN
IP Dest: 1.2.3.4 TCP Dest: 204
(Unclassified)

TCP SYN / ACK
(Classified as FTP)

1. Recognize FTP command “PORT”
2. Listen for the server to open a new TCP connection to 1.2.3.4:204
3. Supports both active and passive FTP

NBAR PDLM Example: Citrix Priority Packet Tagging

Virtual Channel Priorities		
Priority	ICA Bits (decimal)	Sample Virtual Channels
High	0	Video, mouse, and keyboard screen updates
Medium	1	Program neighborhood, clipboard, audio mapping, and license management
Low	2	Client common equipment (COM) port mapping, client drive mapping
Background	3	Auto client update, client printer mapping, and original equipment manufacture (OEM) channels

Configure class maps that classify Citrix ICA traffic by ICA tag:

```
class-map match-any Citrix-high-medium-low
      match protocol citrix ica-tag “0”
      match protocol citrix ica-tag “1”
      match protocol citrix ica-tag “2”
class-map Citrix-background
      match protocol citrix ica-tag “3”
```

Peer-to-Peer File Sharing

Top Four File-Sharing Applications

File-Sharing Application	% of File-Sharing Traffic
eDonkey	51%
BitTorrent	34%
FastTrack/Kazaa	10%
Gnutella	6%

Video Files Made up 61% of Volume

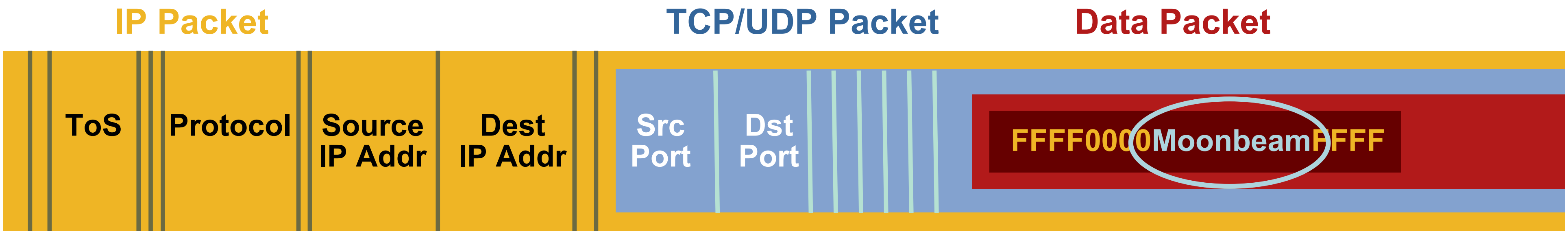
Source: CacheLogic, August 30, 2005

“NeoModus Direct Connect” PDLM

- Direct Connect is a peer-to-peer (P2P) software application that facilitates audio, video, and image file-sharing between clients; it provides complete distributed file-searching and file-sharing with other peers
- The “Direct Connect” native PDL adds support for Direct Connect to Cisco IOS Software; an NBAR PDLM for Direct Connect is also available for use on earlier versions of Cisco IOS software
- Cisco IOS 12.4T

  http://www.cisco.com/en/US/partner/products/ps6441/prod_bulletin09186a00804a8728.html#wp1064474

NBAR User-Defined Custom Application Classification



IP Packet

ToS

Protocol

Source IP Addr

Dest IP Addr

TCP/UDP Packet

Src Port

Dst Port

Data Packet

FFFF0000MoonbeamFFFF

- Used for static TCP/UDP port-based applications that are not supported in NBAR PDLMs
- Up to ten custom applications can be added
- Each custom application can have max. 16 TCP and 16 UDP ports mapped
- Statistics appear in the Protocol Discovery

```
Router(config)#ip nbar port-map custom-01 ?
     tcp   TCP ports
     udp   UDP ports
```

- Custom protocol traffic can only be inspected for the first 255 bytes of the payload

NBAR User-Defined Custom Application Classification Example

```
ip nbar custom lunar_light
  8 ascii Moonbeam tcp
  range 2000 2999
```

Name—Name the match criteria up to 24 characters >> lunar_light

Offset—Specify the beginning byte of string or value to be matched in the data packet, counting from zero for the first byte >> Skip first 8 bytes

Format—Define the format of the match criteria ASCII, hex or decimal >> ascii

Value—Should match with the value in the packet If ASCII, up to 16 characters >> Moonbeam

[Source or destination port]—Optionally restrict the direction of packet inspection; defaults to both directions if not specified >> [source | destination]

TCP or UDP— Indicate the protocol encapsulated in the IP packet >> tcp

Range or selected port number(s) "range" with start and end port numbers, up to 1,000 one to sixteen individual port numbers >> Range 2000 2999

```
class-map solar_system

match protocol lunar_light

policy-map astronomy
  class solar_system
  set ip dscp AF21

interface Serial1

service-policy output astronomy
```

NBAR User-Defined Custom Application Multiple Matches Per Port

- “Multiple Matches Per Port” increases flexibility of user-defined application recognition

```
ip nbar custom name [offset [format value]] [variable field-
name field-length] [source|destination] [tcp | udp] [range
start end | port-number]
```

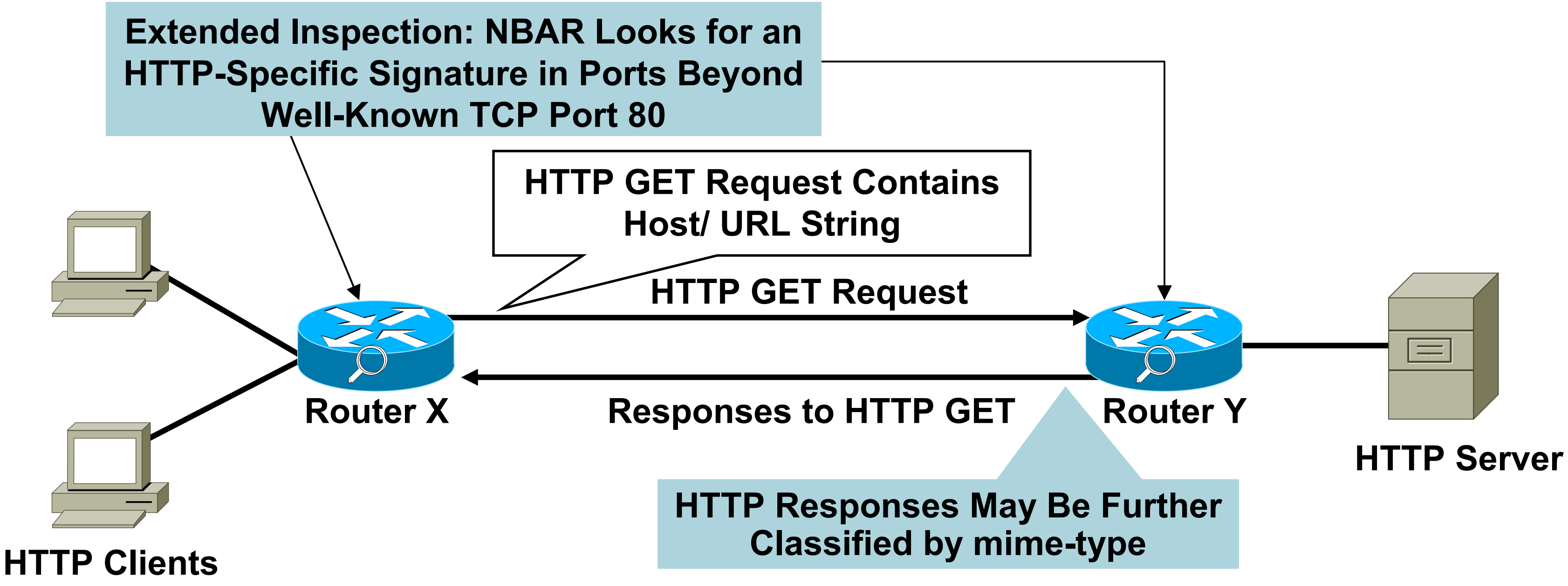
- Example: identify UDP packets with a destination port of 3000 and "0x56" in the seventh byte of the payload

```
ip nbar custom virus_home 7 hex 0x56 dest udp 3000
```

Note: “Multiple Matches” feature is limited to the first 4 bytes of the payload;

Successor: Flexible Packet Matching (FPM)

NBAR HTTP Classification



Extended Inspection: NBAR Looks for an HTTP-Specific Signature in Ports Beyond Well-Known TCP Port 80

HTTP GET Request Contains Host/ URL String

HTTP GET Request

Responses to HTTP GET

HTTP Responses May Be Further Classified by mime-type

```
router(config-cmap)#match protocol http ?
     Host         host-name-string  – Match Host Name
     URL          url-string        – Match URL String
     Mime         MIME-type         – Match MIME Type
```

NBAR HTTP Header Fields

- NBAR can classify traffic using HTTP header fields
- Client to server request header fields:

  User-Agent, Referrer, From

- Response messages (server to client) header fields:

  Server, Location, Content-Base, Content-Encoding

- All HTTP fields

c-header-field	*Client general Header Field*
host	*Server Host Name*
mime	*Match MIME Type*
s-header-field	*Server general Header Field*
url	*Match URL String*

- Example

```
match protocol http c-header-field *Mozilla/4.0*
match protocol http s-header-field *http://www.cisco.com/go/nbar*
```

- Added in 12.3(11)T

HTTP Requests Payload Inspection
Example: Assign ebay Traffic Precedence=5

```
router(config)# class-map match-all ebay-class
router(config-cmap)# match protocol http url "*ebay*"

router(config)# policy-map ebay-policy
router(config-pmap)# class ebay-class
router(config-pmap-c)# set ip precedence 5

router(config)# interface FastEthernet0/0
router(config-if)# ip nbar protocol-discovery
router(config-if)# service-policy input ebay-policy
```

HTTP Requests Payload Inspection
Example: Assign ebay Traffic Precedence=5

```
router#sh policy-map interface fast0/0
 FastEthernet0/0
 Service-policy input ebay-policy
  Class-map ebay-class (match-all)
   636 packets, 99322 bytes
   5 minute offered rate 0 bps, drop rate 0 bps
   Match protocol secure-http
   QoS Set
    ip precedence 5
     Packets marked 636
  Class-map class-default (match-any)
   21374 packets, 3102730 bytes
   5 minute offered rate 0 bps, drop rate 0 bps
   Match any
```

NBAR RTP Payload Type Classification

- Eases classification of voice and video traffic

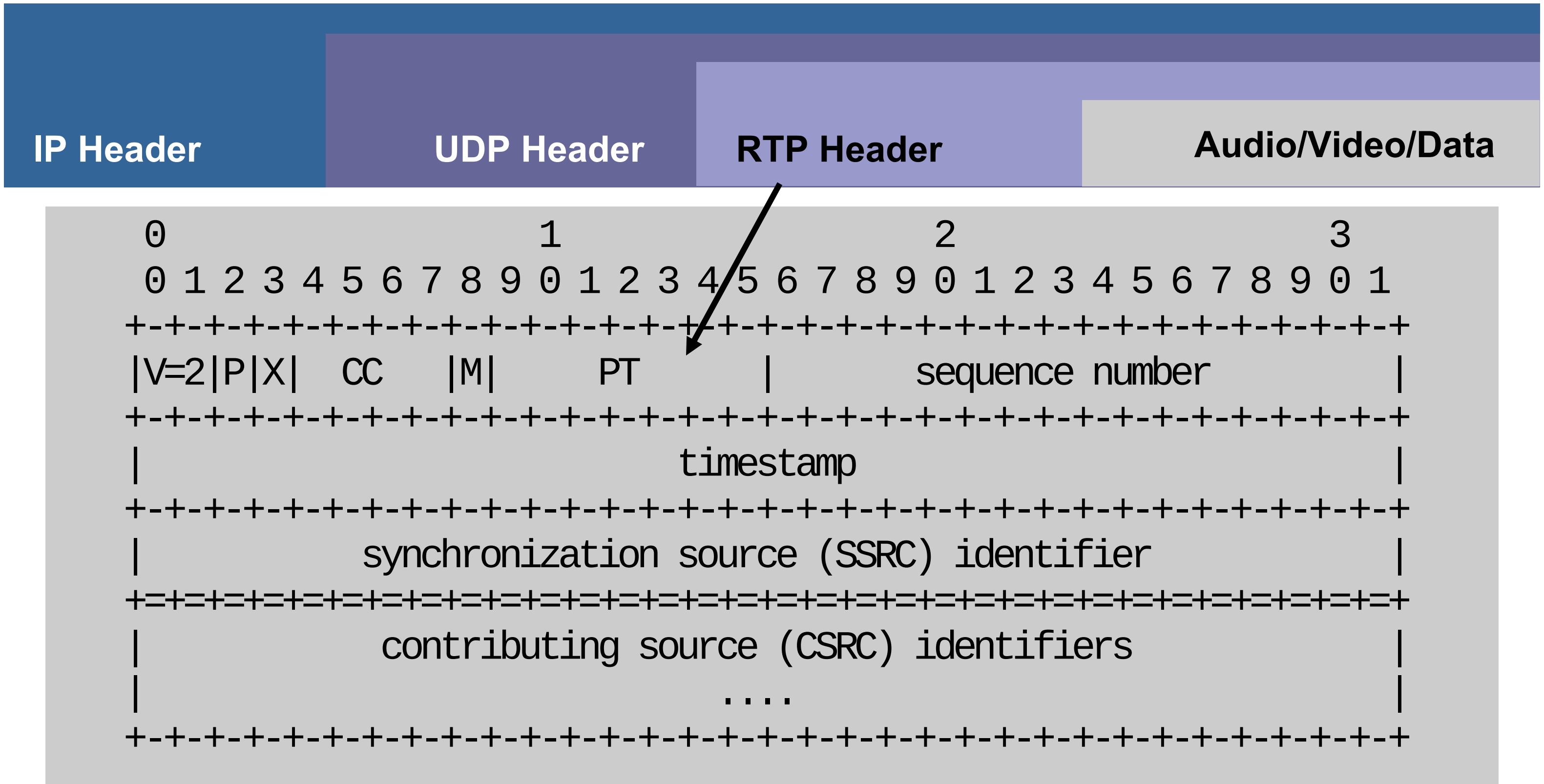
  VoIP, streaming/real time video, audio/video conferencing, Fax Over IP

- Distinguishes between RTP packets based on payload type and CODECS
- Removes dependencies on UDP Port Range and DSCP markings

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

NBAR Real-Time Transport Protocol Payload Classification

Stateful Identification of Real Time Audio and Video Traffic, Differentiation on the Basis of Audio and Video Codecs



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V=2|P|X|  CC   |M|     PT      |       sequence number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           timestamp                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           synchronization source (SSRC) identifier            |
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
|            contributing source (CSRC) identifiers             |
|                             ....                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- **Real-Time Transport Protocol (RTP)—RFC 1889**
- **RTP profile for audio and video conferences with minimal control—RFC 1890**

NBAR RTP Payload Classification Configuration

```
match protocol rtp [audio | video |
                    payload-type payload-string]
```

audio: Specifies matching by payload-type values 0-23
video: Specifies matching by payload-type values 24-33
payload-type: Specifies matching by payload-type value, for
more granular matching than audio or video provide
payload-string: A string specifying the payload-type values

- Example

NBAR to match RTP traffic with the payload-types 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 64

```
match protocol rtp payload-type "0, 1, 4 - 0x10,
10001b - 10010b, 64“
```

- Cisco IOS 12.2(8)T and 12.1(11b)E

NBAR-NAT Integration and Real Time Streaming Protocol (RTSP)

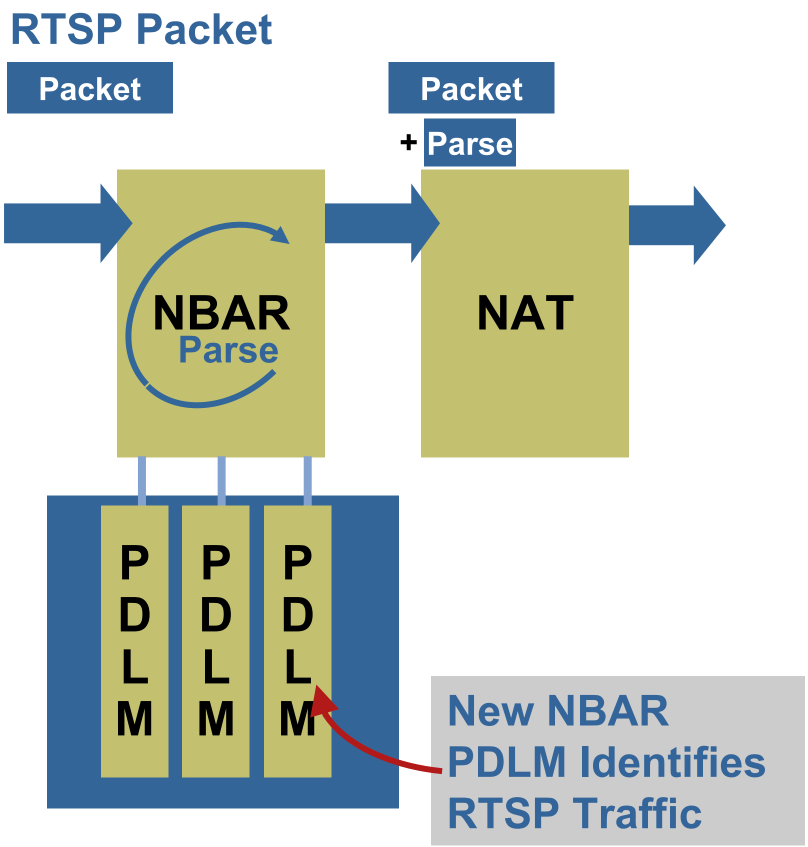
- NBAR provides Network Address Translation (NAT) with Real Time Streaming Protocol (RTSP) and MGCP
- NBAR parses the RTSP payload and translates the embedded address and port
- RTSP-based applications can run in NAT's Port Address Translation (PAT) configuration mode
- RTSP-based applications include

  RealSystem G2 by RealNetworks

  Windows Media Services (WMS) by Microsoft

  QuickTime by Apple

  IP/TV® by Cisco
- Cisco IOS 12.3(7)T

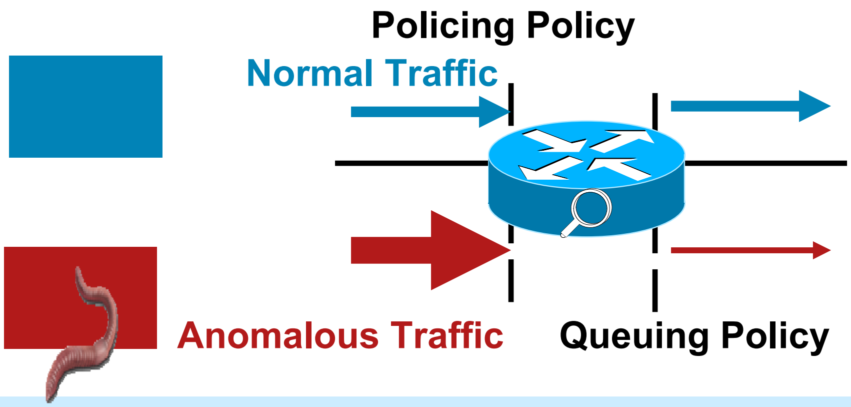


CLI Example for NAT, RTSP

- *ip nat service rtsp port port-number*
  (well known port number: TCP (UDP) 554)
- *show ip nat statistics*
- *show ip nat translations*
- http://cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802043f7.html

```
Router (config)# ip nat service rtsp port 80
```

NBAR Scenario: Identify Security Attacks
Rate-Limit Anomalous Traffic



```
Router(config)# class-map match-any MyVirusMap
     Router(config-cmap)# match protocol http url "*default.ida*"
     Router(config-cmap)# match protocol http url "*cmd.exe*"
     Router(config-cmap)# match protocol http url "*root.exe*“

Router(config)# policy-map MyVirusPolicy
     Router(config-pmap)# class MyVirusMap
     Router(config-pmap-c)# set dscp 1
     Router(config-pmap-c)#police 1000000 31250 31250 conform-action drop
     exceed-action drop violate-action drop

Router(config)# interface serial 0/0
     Router(config-if)# service-policy input MyVirusPolicy
```

NBAR Scenario: Identify Security Attacks Policing Anomalous Traffic

```
Router#show policy-map interface serial 0/0
Serial0/0
Service-policy input: MyVirusPolicy

Class-map: MyVirusMap (match-any)
        5 packets, 300 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: protocol http url "*default.ida*"
        5 packets, 300 bytes
        5 minute rate 0 bps
        Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
        Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
        police:
        1000000 bps, 31250 limit, 31250 extended limit
        conformed 5 packets, 300 bytes; action: drop
        exceeded 0 packets, 0 bytes; action: drop
        violated 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map: class-default (match-any)
        5 packets, 300 bytes
        5 minute offered rate 0 bps, drop rate 0 bps
        Match: any
```

How to Identify “unclassified” Traffic

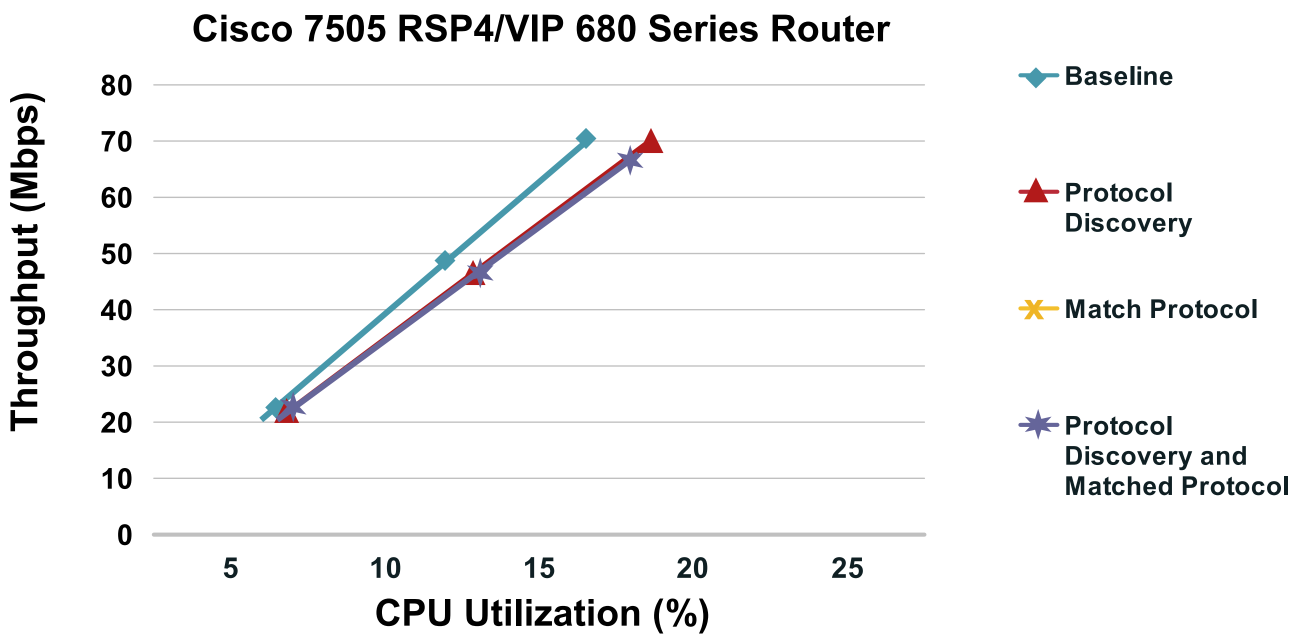
```
Router# show ip nbar unclassified-port-stats

Port Statistics for unclassified packets is not turned on.

Router# debug ip nbar unclassified-port-stats
```

```
Router# debug ip nbar filter destination_port tcp <#>

Router# debug ip nbar capture a b c d
  a: number of bytes (40-512)
  b: number of starting packets to capture (after TCP SYN)
  c: number of final packets to capture
  d: number of total packets to capture
```

The Debug IP NBAR Commands Should Be Enabled Only Under Carefully Controlled Circumstances!

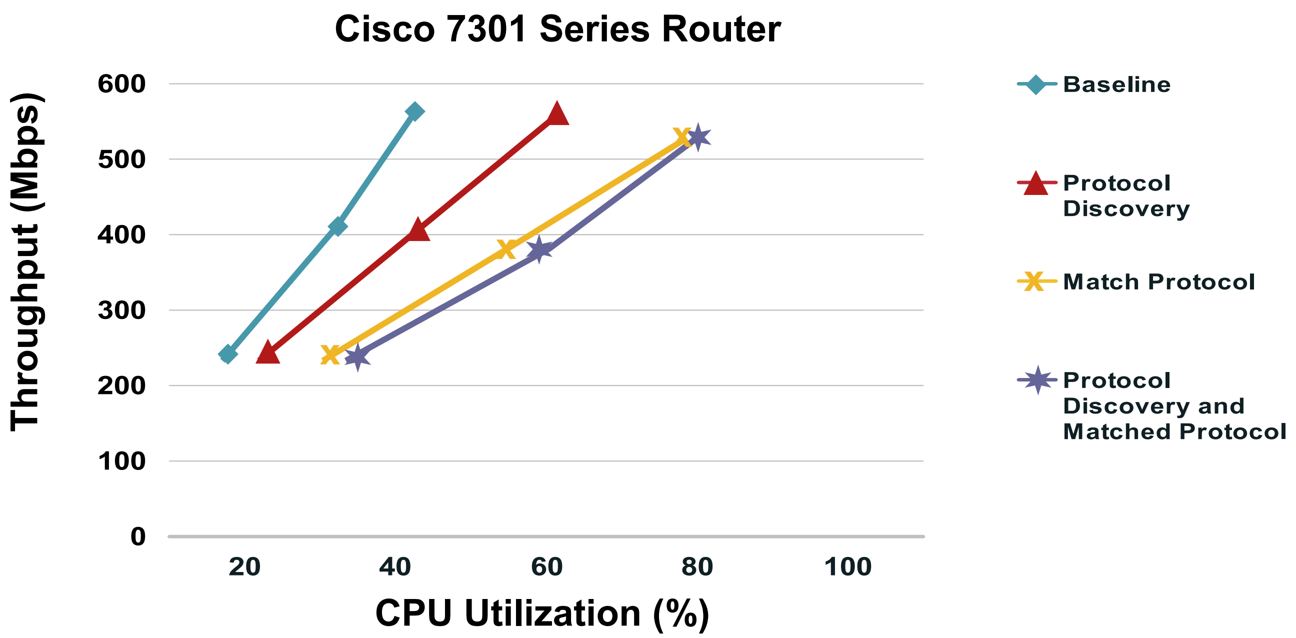
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a0080094ac5.shtml

NBAR Performance Test: 7505



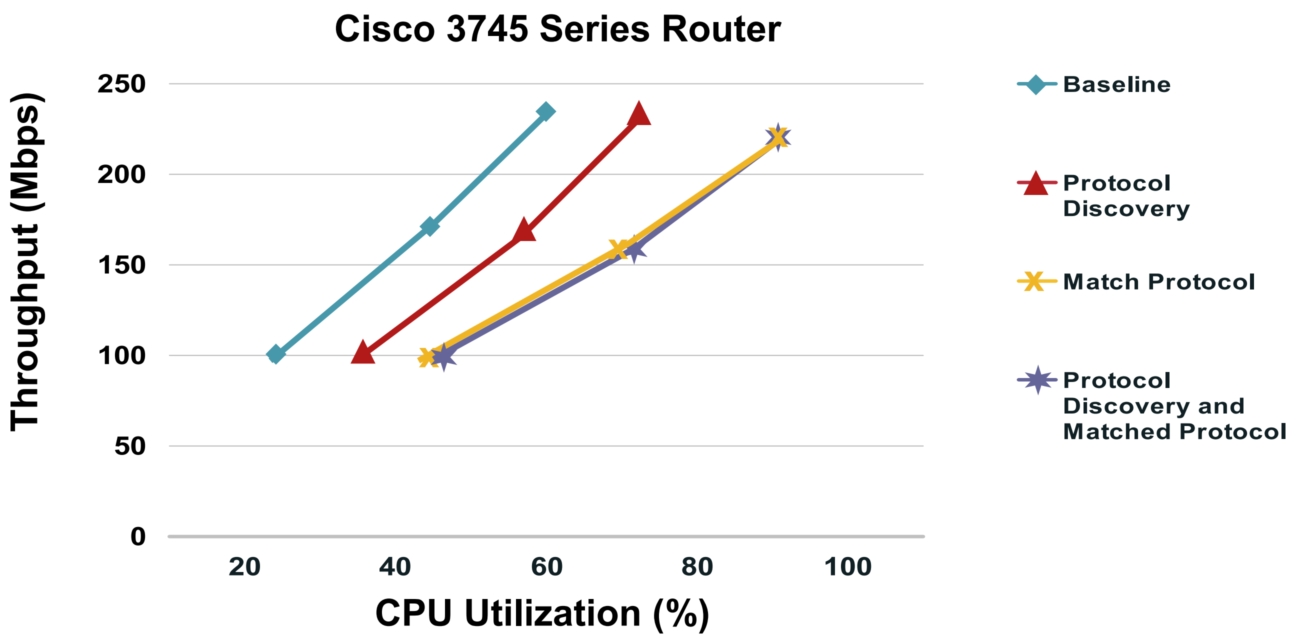
Difference Between Baseline and:						
	Protocol Discovery		Match Protocol		Protocol Discovery and Match Protocol	
	CPU Δ	Throughput Δ%	CPU Δ	Throughput Δ%	CPU Δ	Throughput Δ%
60% NDR	3	0	2	4.7	2	4.7
40% NDR	2	0	2	0	2	0
20% NDR	1	0	1	0	1	0

NBAR Performance Test: 7301



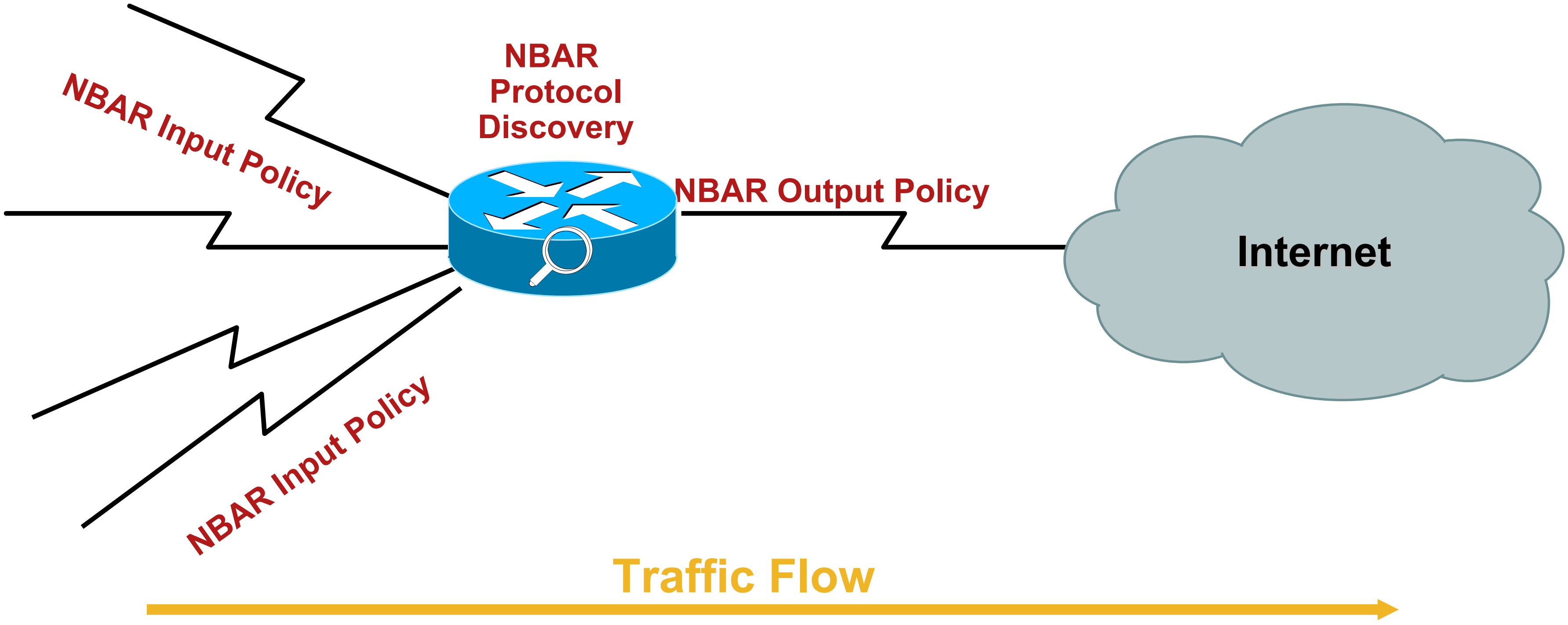
	Difference Between Baseline and:					
	Protocol Discovery		Match Protocol		Protocol Discovery and Match Protocol	
	CPU Δ	Throughput Δ%	CPU Δ	Throughput Δ%	CPU Δ	Throughput Δ%
60% NDR	19	0	53	3.57	53	4.6
40% NDR	11	0	39	0.12	41	0.13
20% NDR	8	0	23	0	23	0

NBAR Performance Test: 3745



	Difference Between Baseline and:					
	Protocol Discovery		Match Protocol		Protocol Discovery and Match Protocol	
	CPU Δ	Throughput Δ%	CPU Δ	Throughput Δ%	CPU Δ	Throughput Δ%
60% NDR	12	0	32	3.4	32	5.1
40% NDR	12	0	25	0	25	0
20% NDR	9	0	16	0	17	0

NBAR Deployment: Ingress-Egress Considerations



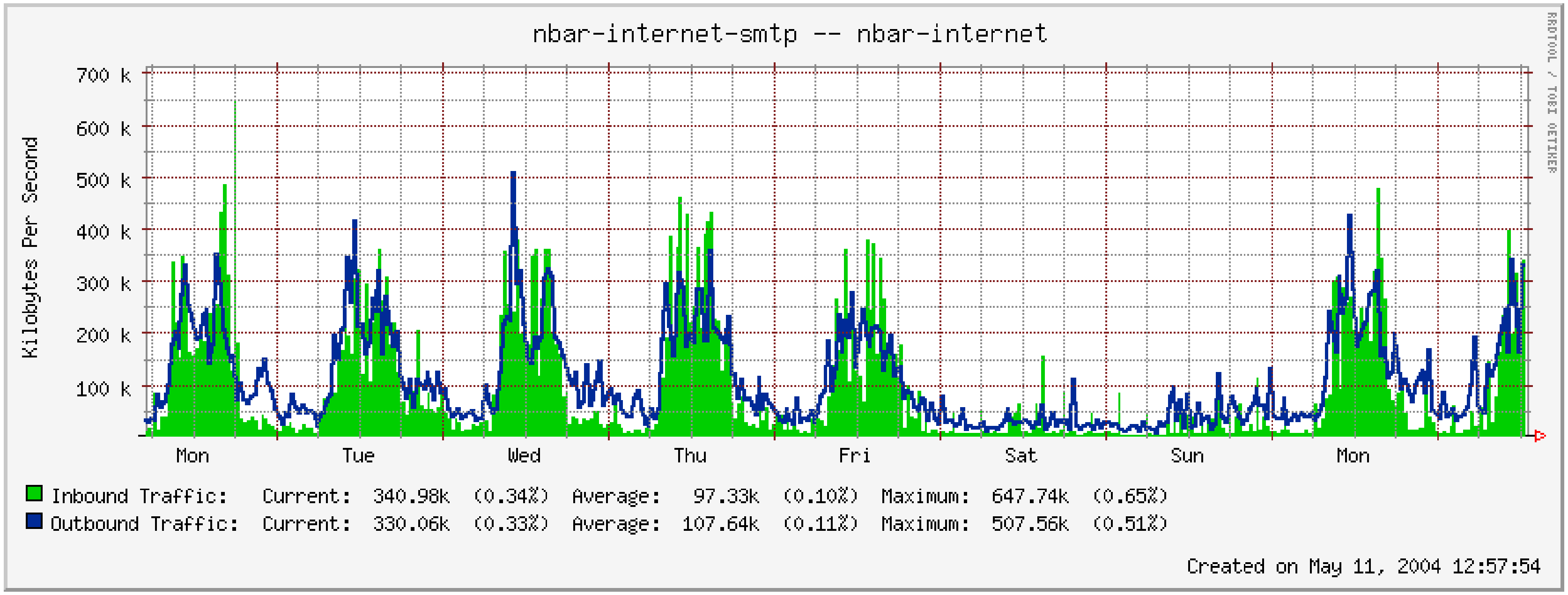
NBAR input policy:	ingress traffic only
NBAR output policy:	egress traffic only
NBAR protocol discovery:	ingress and egress traffic

MRTG—NBAR Support

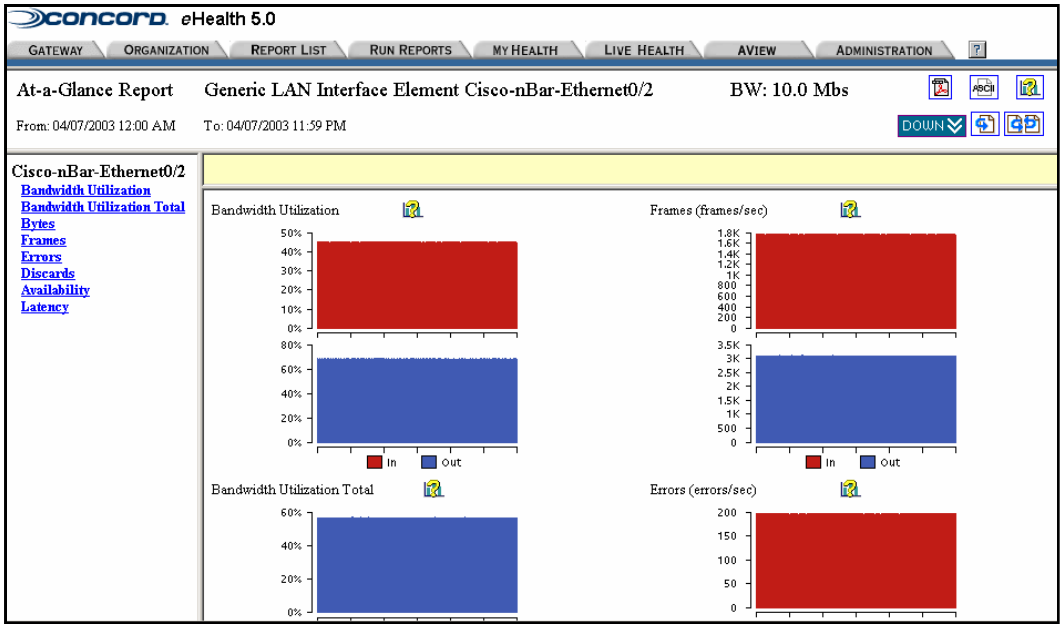
MRTG
MULTI ROUTER TRAFFIC GRAPHER

MRTG Graphing Support for NBAR

- http://www.eatworms.org.uk/cacti/cisco-nbar.php
- http://vermeer.org/display_doc.php?doc_id=6
- http://www.somix.com/products/denika_nbar.php



CA Unicenter (Concord)— NBAR Support



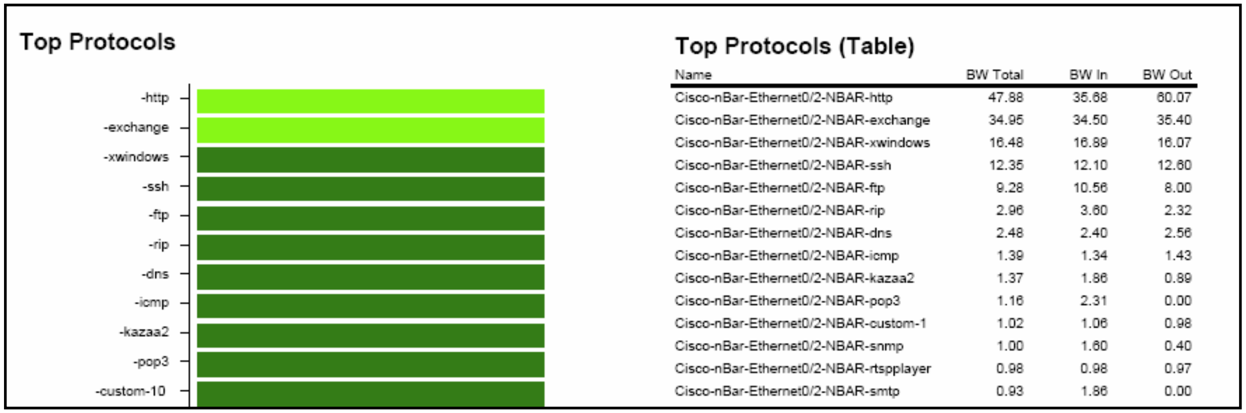
At-a-Glance Report Generic LAN Interface Element Cisco-nBar-Ethernet0/2 BW: 10.0 Mbs

From: 04/07/2003 12:00 AM To: 04/07/2003 11:59 PM

Cisco-nBar-Ethernet0/2

- Bandwidth Utilization
- Bandwidth Utilization Total
- Bytes
- Frames
- Errors
- Discards
- Availability
- Latency

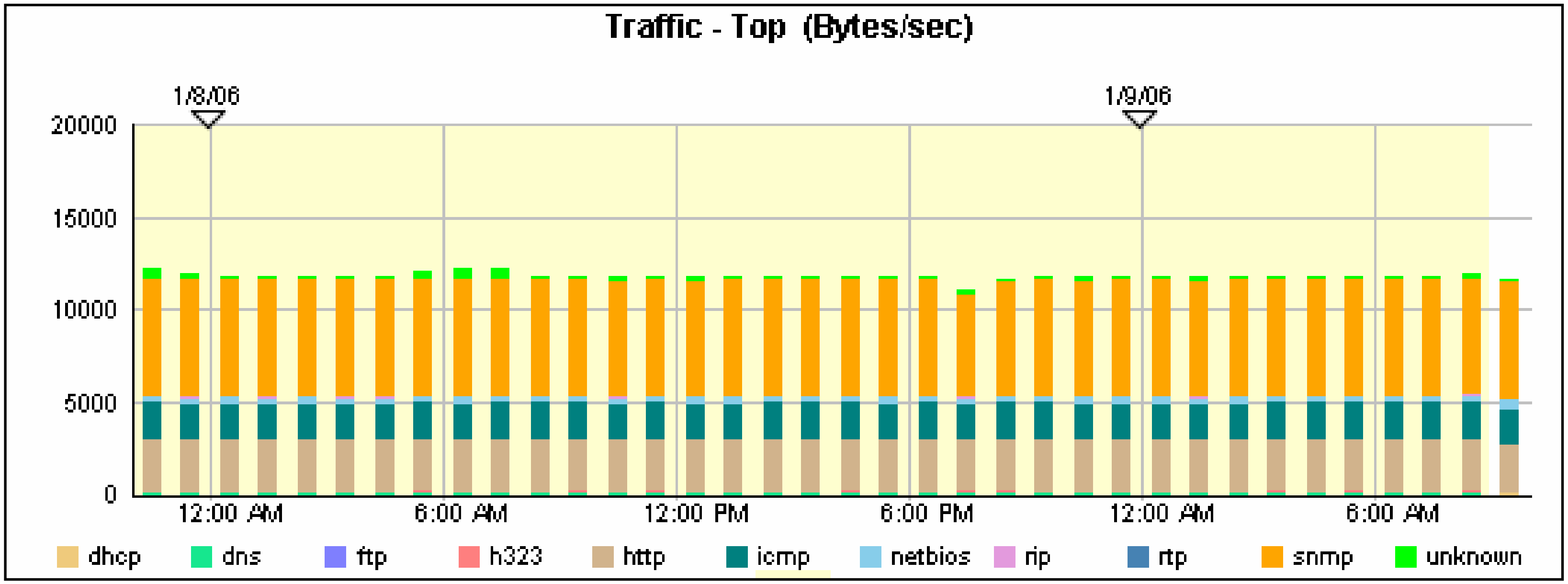
NBAR PD Drilldown

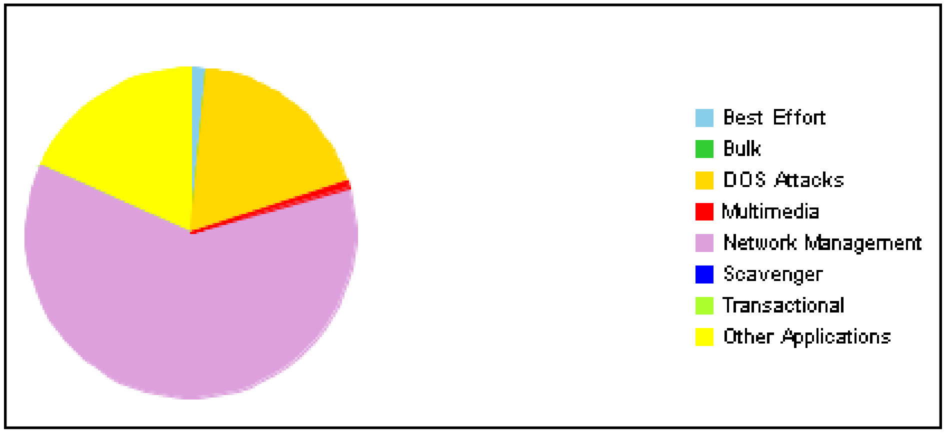


Top Protocols (Table)

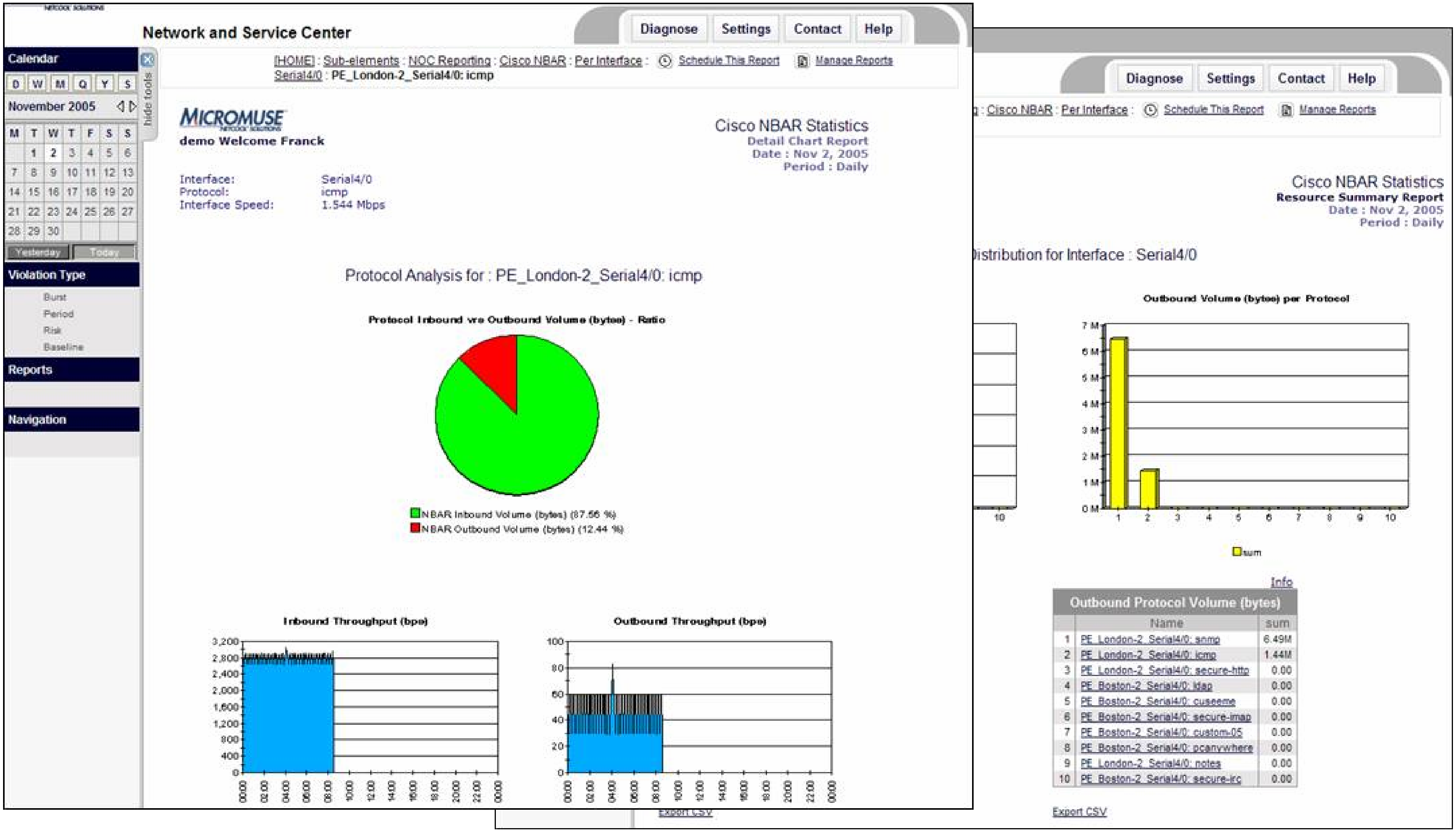
Name	BW Total	BW In	BW Out
Cisco-nBar-Ethernet0/2-NBAR-http	47.88	35.68	60.07
Cisco-nBar-Ethernet0/2-NBAR-exchange	34.95	34.50	35.40
Cisco-nBar-Ethernet0/2-NBAR-xwindows	16.48	16.89	16.07
Cisco-nBar-Ethernet0/2-NBAR-ssh	12.35	12.10	12.60
Cisco-nBar-Ethernet0/2-NBAR-ftp	9.28	10.56	8.00
Cisco-nBar-Ethernet0/2-NBAR-rip	2.96	3.60	2.32
Cisco-nBar-Ethernet0/2-NBAR-dns	2.48	2.40	2.56
Cisco-nBar-Ethernet0/2-NBAR-icmp	1.39	1.34	1.43
Cisco-nBar-Ethernet0/2-NBAR-kazaa2	1.37	1.86	0.89
Cisco-nBar-Ethernet0/2-NBAR-pop3	1.16	2.31	0.00
Cisco-nBar-Ethernet0/2-NBAR-custom-1	1.02	1.06	0.98
Cisco-nBar-Ethernet0/2-NBAR-snmp	1.00	1.60	0.40
Cisco-nBar-Ethernet0/2-NBAR-rtspplayer	0.98	0.98	0.97
Cisco-nBar-Ethernet0/2-NBAR-smtp	0.93	1.86	0.00

InfoVista—NBAR Support





Micromuse—NBAR Support



demo Welcome Franck

Cisco NBAR Statistics
Detail Chart Report
Date : Nov 2, 2005
Period : Daily

Interface:	Serial4/0
Protocol:	icmp
Interface Speed:	1.544 Mbps

Protocol Analysis for : PE_London-2_Serial4/0: icmp

Cisco NBAR Statistics
Resource Summary Report
Date : Nov 2, 2005
Period : Daily

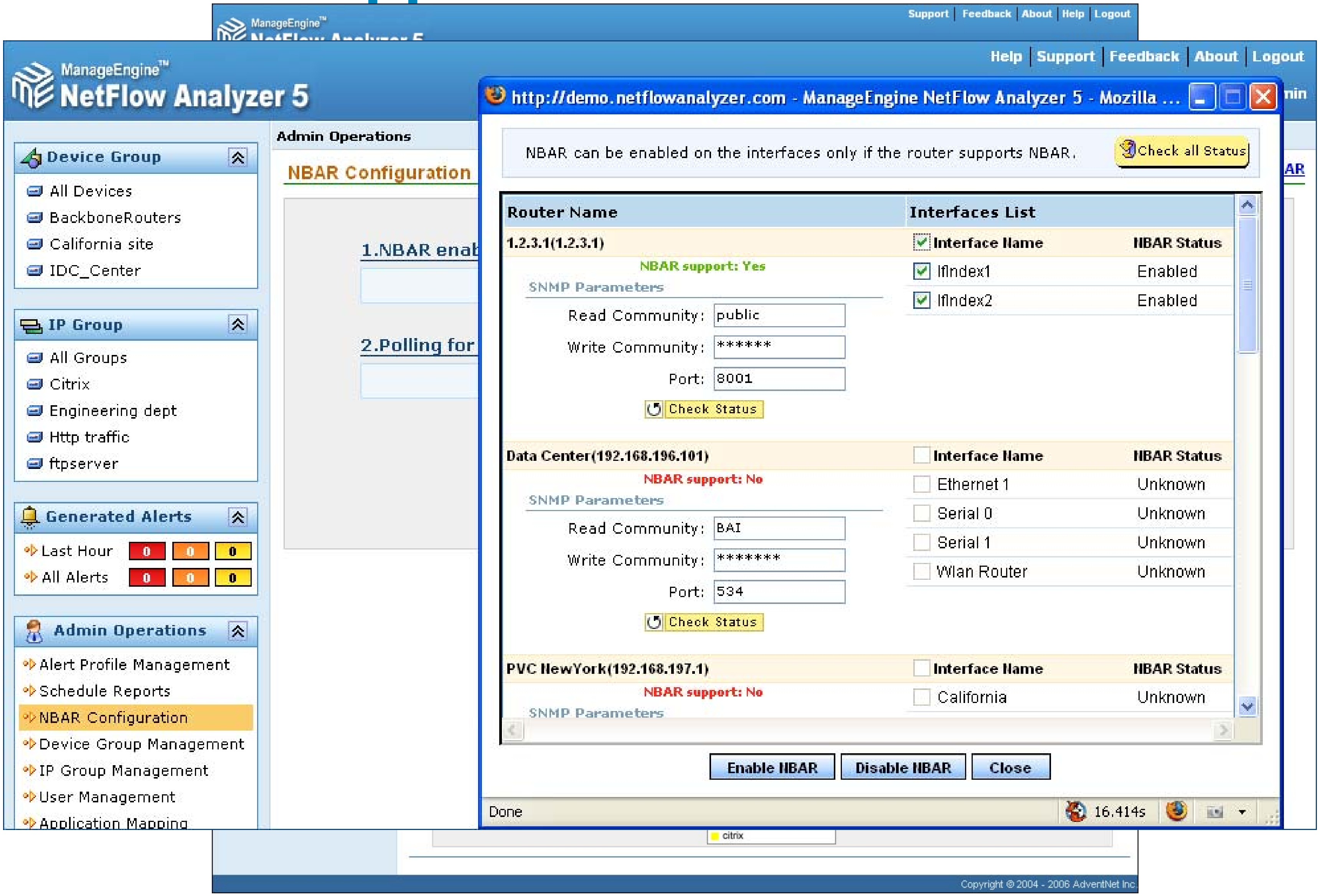
istribution for Interface : Serial4/0

Outbound Protocol Volume (bytes)		
	Name	sum
1	PE_London-2_Serial4/0: snmp	6.49M
2	PE_London-2_Serial4/0: icmp	1.44M
3	PE_London-2_Serial4/0: secure-http	0.00
4	PE_Boston-2_Serial4/0: ldap	0.00
5	PE_Boston-2_Serial4/0: cuseeme	0.00
6	PE_Boston-2_Serial4/0: secure-imap	0.00
7	PE_Boston-2_Serial4/0: custom-05	0.00
8	PE_Boston-2_Serial4/0: pcanywhere	0.00
9	PE_London-2_Serial4/0: notes	0.00
10	PE_Boston-2_Serial4/0: secure-irc	0.00

Export CSV

AdventNet NetFlow Analyzer—NBAR Support

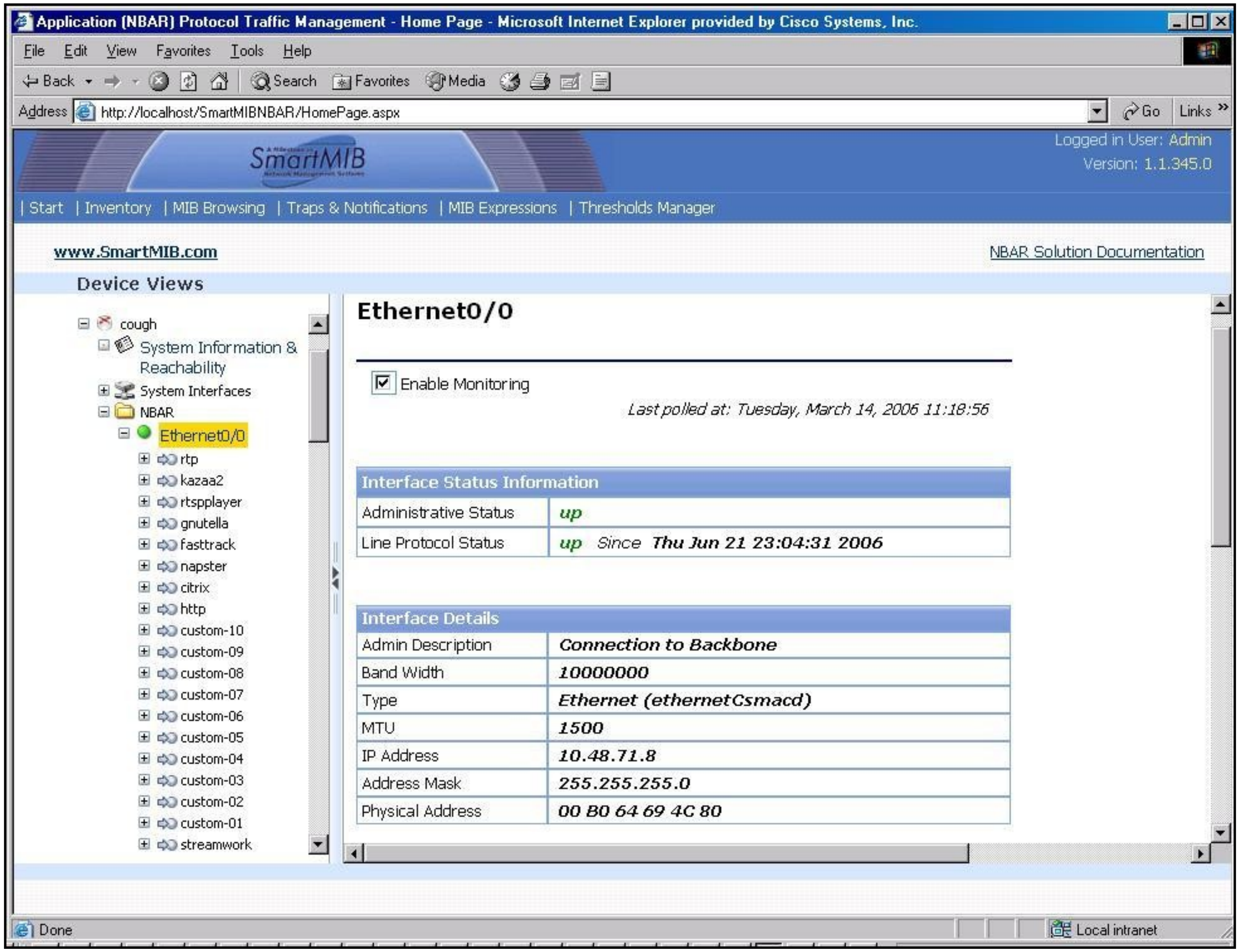
AdventNet
Excellence Matters



NBAR can be enabled on the interfaces only if the router supports NBAR.

Router Name		Interfaces List	
1.2.3.1(1.2.3.1)		☑ Interface Name	NBAR Status
NBAR support: Yes		☑ IfIndex1	Enabled
SNMP Parameters		☑ IfIndex2	Enabled
Read Community:	public		
Write Community:	******		
Port:	8001		
Data Center(192.168.196.101)		□ Interface Name	NBAR Status
NBAR support: No		□ Ethernet 1	Unknown
SNMP Parameters		□ Serial 0	Unknown
Read Community:	BAI	□ Serial 1	Unknown
Write Community:	*******	□ Wlan Router	Unknown
Port:	534		
PVC NewYork(192.168.197.1)		□ Interface Name	NBAR Status
NBAR support: No		□ California	Unknown
SNMP Parameters			

SmartMIB—NBAR Support


Application (NBAR) Protocol Traffic Management - Home Page - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/SmartMIBNBAR/HomePage.aspx
Go Links
SmartMIB
Logged in User: Admin
Version: 1.1.345.0
| Start | Inventory | MIB Browsing | Traps & Notifications | MIB Expressions | Thresholds Manager
www.SmartMIB.com
NBAR Solution Documentation
Device Views
cough
System Information & Reachability
System Interfaces
NBAR
Ethernet0/0
rtp
kazaa2
rtspplayer
gnutella
fasttrack
napster
citrix
http
custom-10
custom-09
custom-08
custom-07
custom-06
custom-05
custom-04
custom-03
custom-02
custom-01
streamwork
Done
Local intranet

Ethernet0/0

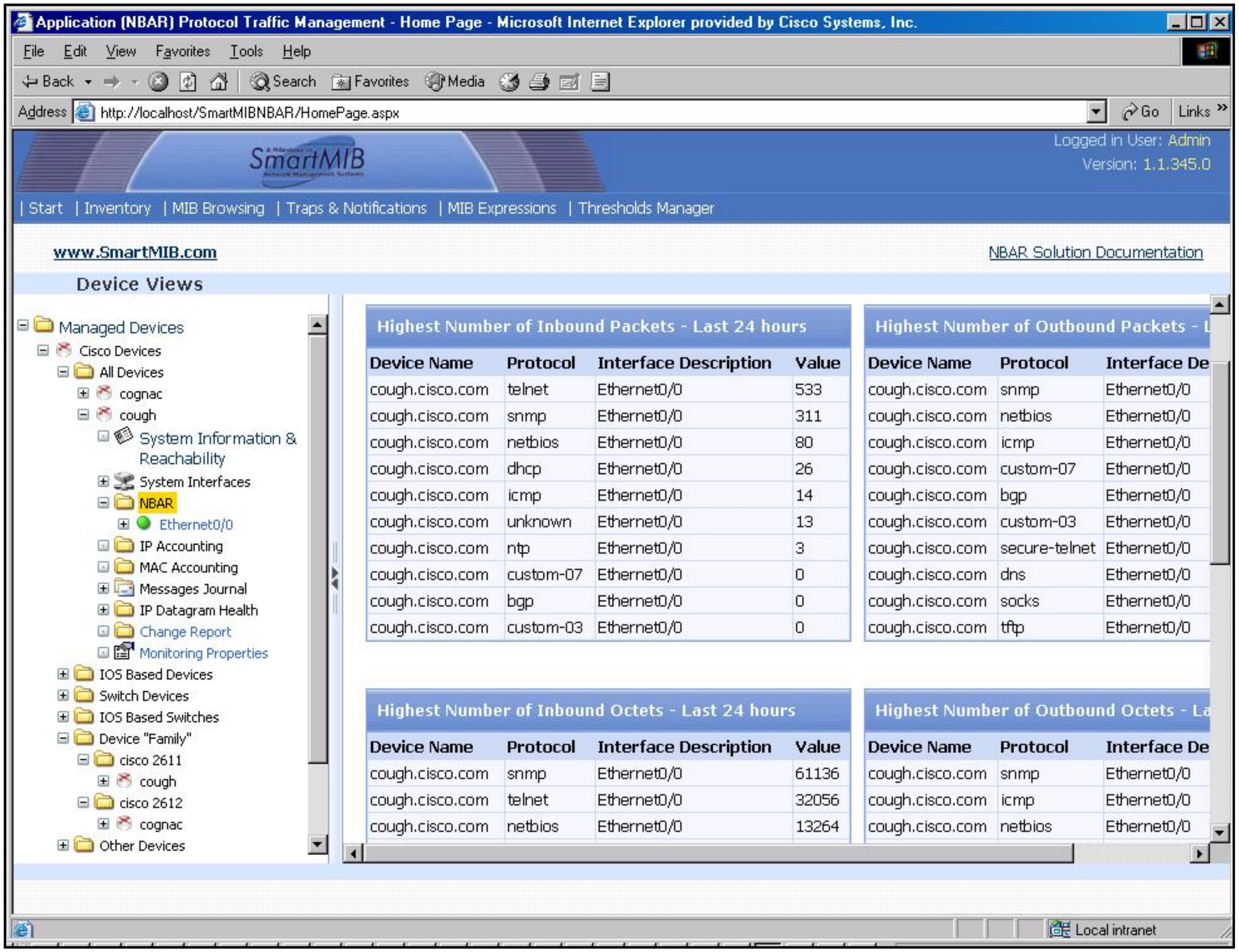
☑ Enable Monitoring

Last polled at: Tuesday, March 14, 2006 11:18:56

Interface Status Information	
Administrative Status	*up*
Line Protocol Status	*up Since* **Thu Jun 21 23:04:31 2006**

Interface Details	
Admin Description	**Connection to Backbone**
Band Width	**10000000**
Type	**Ethernet (ethernetCsmacd)**
MTU	**1500**
IP Address	**10.48.71.8**
Address Mask	**255.255.255.0**
Physical Address	**00 B0 64 69 4C 80**

SmartMIB—NBAR Support


Application (NBAR) Protocol Traffic Management - Home Page - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
SmartMIB
| Start | Inventory | MIB Browsing | Traps & Notifications | MIB Expressions | Thresholds Manager
Local intranet

Address: http://localhost/SmartMIBNBAR/HomePage.aspx

Logged in User: Admin
Version: 1.1.345.0

www.SmartMIB.com

NBAR Solution Documentation

Device Views

- Managed Devices
  - Cisco Devices
    - All Devices
      - cognac
      - cough
        - System Information & Reachability
        - System Interfaces
        - NBAR
          - Ethernet0/0
        - IP Accounting
        - MAC Accounting
        - Messages Journal
        - IP Datagram Health
        - Change Report
        - Monitoring Properties
    - IOS Based Devices
    - Switch Devices
    - IOS Based Switches
    - Device "Family"
      - cisco 2611
        - cough
      - cisco 2612
        - cognac
    - Other Devices

Highest Number of Inbound Packets - Last 24 hours

Device Name	Protocol	Interface Description	Value
cough.cisco.com	telnet	Ethernet0/0	533
cough.cisco.com	snmp	Ethernet0/0	311
cough.cisco.com	netbios	Ethernet0/0	80
cough.cisco.com	dhcp	Ethernet0/0	26
cough.cisco.com	icmp	Ethernet0/0	14
cough.cisco.com	unknown	Ethernet0/0	13
cough.cisco.com	ntp	Ethernet0/0	3
cough.cisco.com	custom-07	Ethernet0/0	0
cough.cisco.com	bgp	Ethernet0/0	0
cough.cisco.com	custom-03	Ethernet0/0	0

Highest Number of Outbound Packets - L

Device Name	Protocol	Interface De
cough.cisco.com	snmp	Ethernet0/0
cough.cisco.com	netbios	Ethernet0/0
cough.cisco.com	icmp	Ethernet0/0
cough.cisco.com	custom-07	Ethernet0/0
cough.cisco.com	bgp	Ethernet0/0
cough.cisco.com	custom-03	Ethernet0/0
cough.cisco.com	secure-telnet	Ethernet0/0
cough.cisco.com	dns	Ethernet0/0
cough.cisco.com	socks	Ethernet0/0
cough.cisco.com	tftp	Ethernet0/0

Highest Number of Inbound Octets - Last 24 hours

Device Name	Protocol	Interface Description	Value
cough.cisco.com	snmp	Ethernet0/0	61136
cough.cisco.com	telnet	Ethernet0/0	32056
cough.cisco.com	netbios	Ethernet0/0	13264

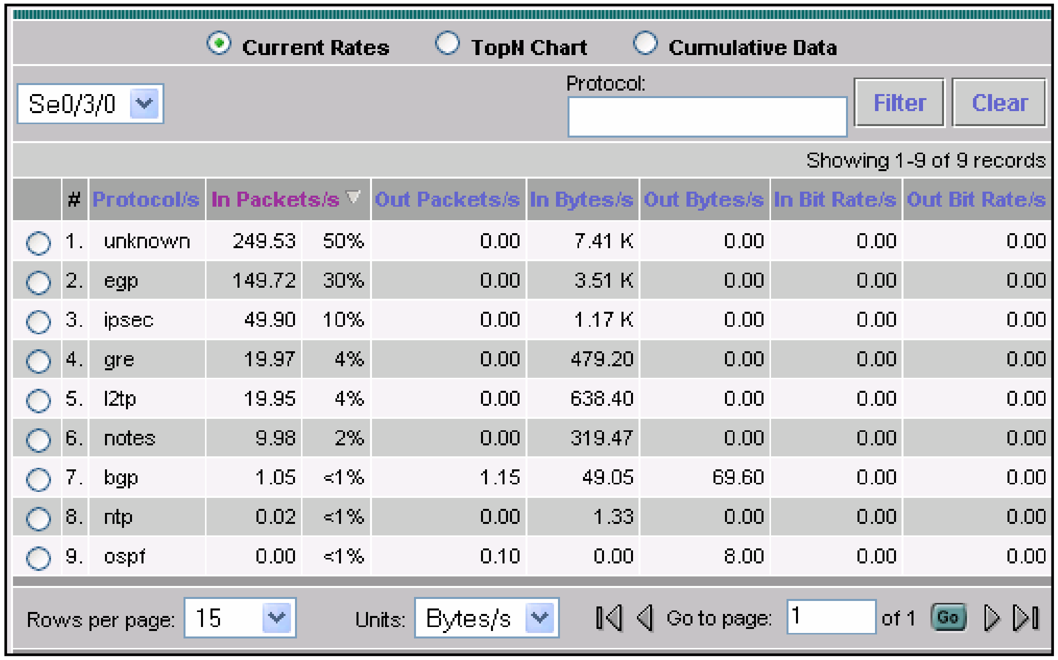
Highest Number of Outbound Octets - La

Device Name	Protocol	Interface De
cough.cisco.com	snmp	Ethernet0/0
cough.cisco.com	icmp	Ethernet0/0
cough.cisco.com	netbios	Ethernet0/0

Cisco NAM—NBAR Support

NAM Uses SNMP to:

- Enable Protocol discovery on device interfaces
- Report on applications discovered by NBAR



● Current Rates ○ TopN Chart ○ Cumulative Data

Se0/3/0

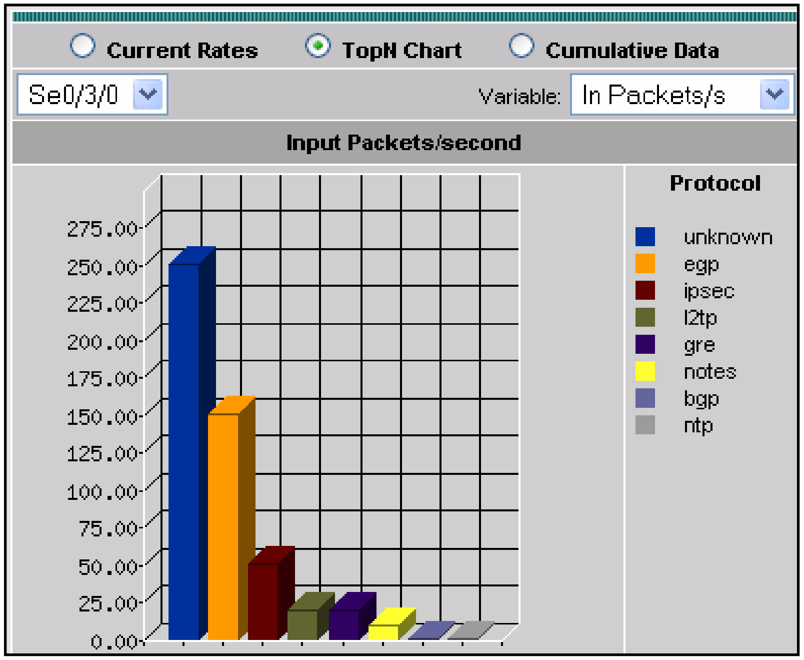
Protocol:

Filter Clear

Showing 1-9 of 9 records

	#	Protocol/s	In Packets/s		Out Packets/s	In Bytes/s	Out Bytes/s	In Bit Rate/s	Out Bit Rate/s
○	1.	unknown	249.53	50%	0.00	7.41 K	0.00	0.00	0.00
○	2.	egp	149.72	30%	0.00	3.51 K	0.00	0.00	0.00
○	3.	ipsec	49.90	10%	0.00	1.17 K	0.00	0.00	0.00
○	4.	gre	19.97	4%	0.00	479.20	0.00	0.00	0.00
○	5.	l2tp	19.95	4%	0.00	638.40	0.00	0.00	0.00
○	6.	notes	9.98	2%	0.00	319.47	0.00	0.00	0.00
○	7.	bgp	1.05	<1%	1.15	49.05	69.60	0.00	0.00
○	8.	ntp	0.02	<1%	0.00	1.33	0.00	0.00	0.00
○	9.	ospf	0.00	<1%	0.10	0.00	8.00	0.00	0.00

Rows per page: 15 Units: Bytes/s Go to page: 1 of 1 Go

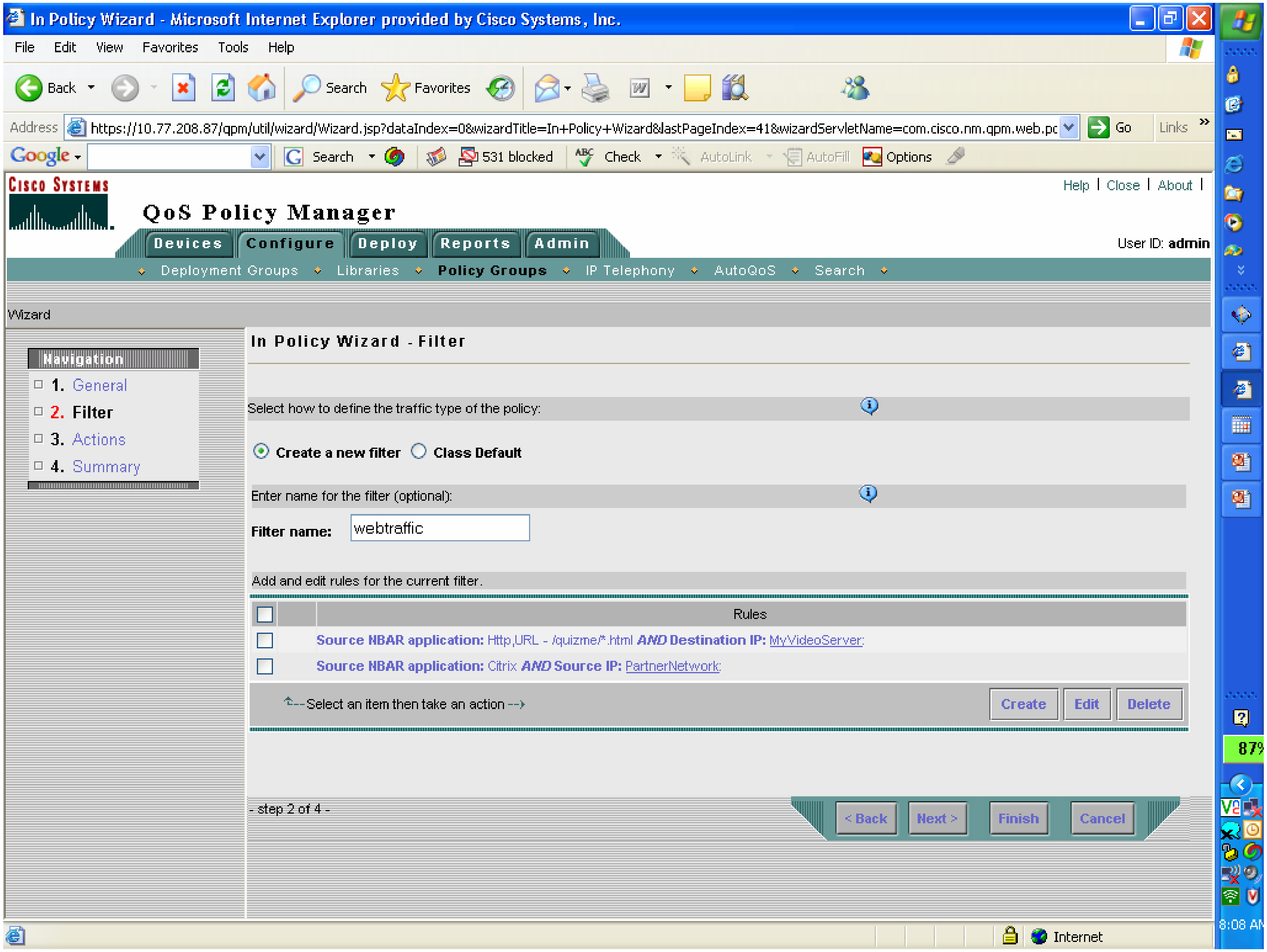


○ Current Rates ● TopN Chart ○ Cumulative Data

Se0/3/0 Variable: In Packets/s

Input Packets/second

CiscoWorks QoS Policy Manager (QPM)—NBAR Support


In Policy Wizard - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.77.208.87/qpm/util/wizard/Wizard.jsp?dataIndex=0&wizardTitle=In+Policy+Wizard&lastPageIndex=41&wizardServletName=com.cisco.nm.qpm.web.pc
Go Links
Google Search 531 blocked Check AutoLink AutoFill Options
Cisco Systems
Help | Close | About |
QoS Policy Manager
Devices Configure Deploy Reports Admin
User ID: admin
Deployment Groups Libraries Policy Groups IP Telephony AutoQoS Search
Wizard
Navigation
1. General
2. Filter
3. Actions
4. Summary
Create Edit Delete
< Back Next > Finish Cancel
Internet
8:08 AM
87%

In Policy Wizard - Filter

Select how to define the traffic type of the policy:

● Create a new filter ○ Class Default

Enter name for the filter (optional):

Filter name: webtraffic

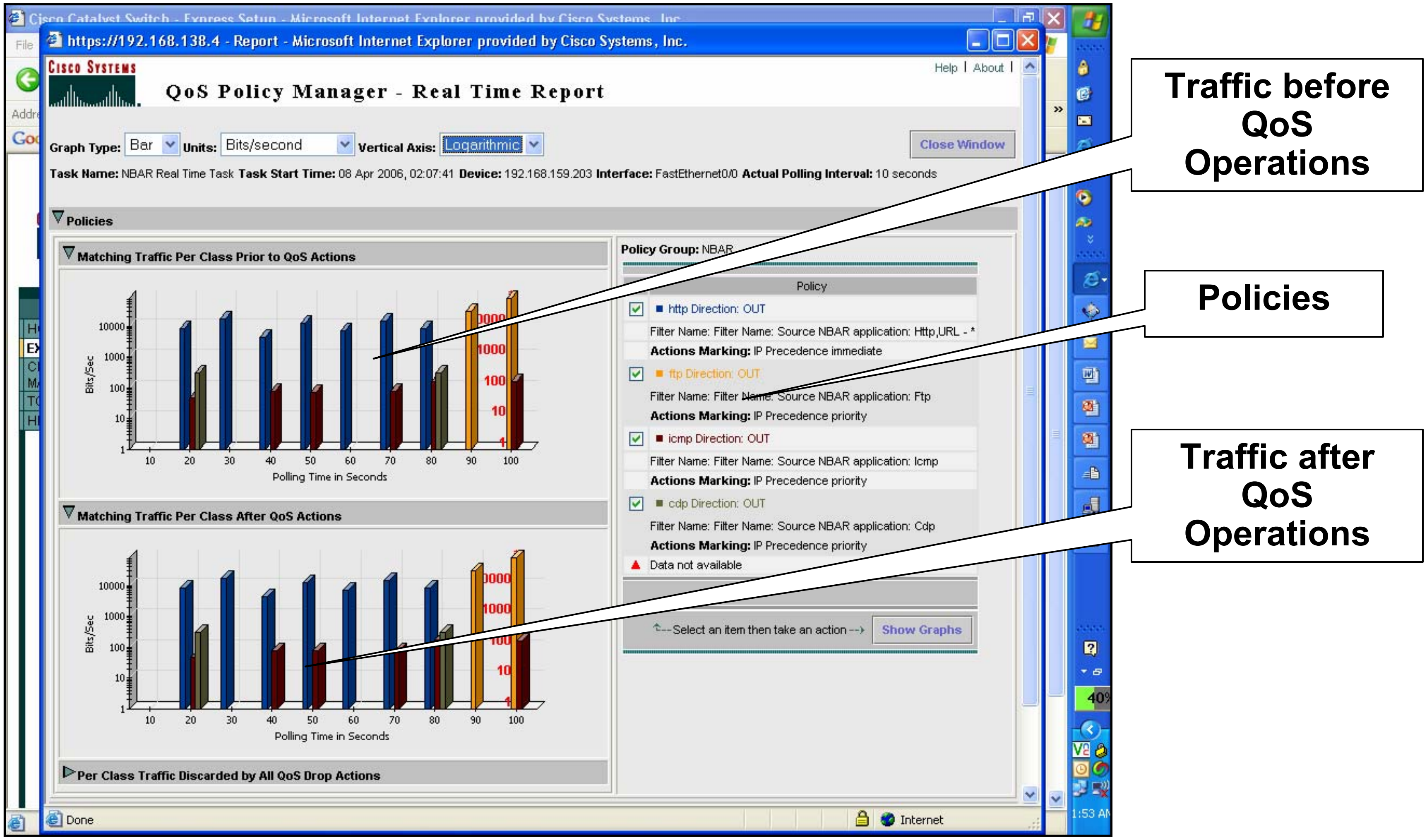
Add and edit rules for the current filter.

□	Rules
□	**Source NBAR application:** Http,URL - /quizme/*.html ***AND*** **Destination IP:** MyVideoServer;
□	**Source NBAR application:** Citrix ***AND*** **Source IP:** PartnerNetwork;

←-Select an item then take an action -->

- step 2 of 4 -

CiscoWorks QoS Policy Manager (QPM)— NBAR Support



https://192.168.138.4 - Report - Microsoft Internet Explorer provided by Cisco Systems, Inc.

QoS Policy Manager - Real Time Report

Graph Type: Bar Units: Bits/second Vertical Axis: Logarithmic

Task Name: NBAR Real Time Task Task Start Time: 08 Apr 2006, 02:07:41 Device: 192.168.159.203 Interface: FastEthernet0/0 Actual Polling Interval: 10 seconds

Policy Group: NBAR

	Policy
☑	■ http Direction: OUT
	Filter Name: Filter Name: Source NBAR application: Http,URL - *
	Actions Marking: IP Precedence immediate
☑	■ ftp Direction: OUT
	Filter Name: Filter Name: Source NBAR application: Ftp
	Actions Marking: IP Precedence priority
☑	■ icmp Direction: OUT
	Filter Name: Filter Name: Source NBAR application: Icmp
	Actions Marking: IP Precedence priority
☑	■ cdp Direction: OUT
	Filter Name: Filter Name: Source NBAR application: Cdp
	Actions Marking: IP Precedence priority
▲	Data not available

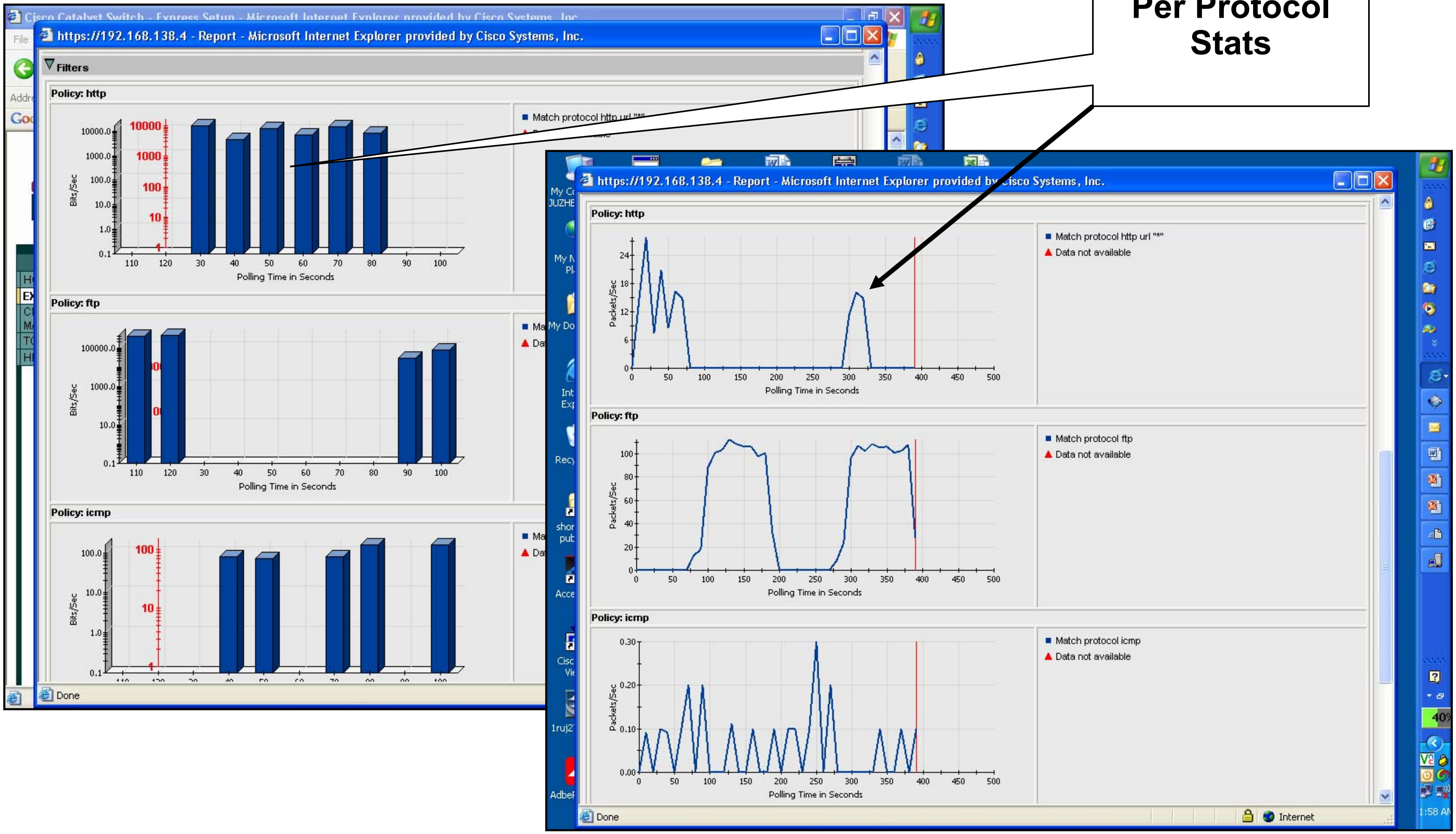
Cisco Catalyst Switch - Express Setup - Microsoft Internet Explorer provided by Cisco Systems, Inc.
CISCO SYSTEMS
Help | About |
Close Window
Policies
Matching Traffic Per Class Prior to QoS Actions
Bits/Sec
10000
1000
100
10
1
10 20 30 40 50 60 70 80 90 100
Polling Time in Seconds
Matching Traffic Per Class After QoS Actions
Per Class Traffic Discarded by All QoS Drop Actions
Select an item then take an action
Show Graphs
Done
Internet

Traffic before QoS Operations

Policies

Traffic after QoS Operations

CiscoWorks QoS Policy Manager (QPM)— NBAR Support


Cisco Catalyst Switch - Express Setup - Microsoft Internet Explorer provided by Cisco Systems, Inc.
https://192.168.138.4 - Report - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Filters
Policy: http
Bits/Sec
Polling Time in Seconds
Match protocol http url "*"
Policy: ftp
Policy: icmp
Done
https://192.168.138.4 - Report - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Policy: http
Packets/Sec
Polling Time in Seconds
Match protocol http url "*"
Data not available
Policy: ftp
Match protocol ftp
Data not available
Policy: icmp
Match protocol icmp
Data not available
Done
Internet

Per Protocol Stats

NBAR: Possible Applications

	NBAR
Network Monitoring	(X)
Network Planning	X
Security Analysis	X
Application Monitoring	X
User Monitoring	
Traffic Engineering	
Peering Agreement	
Usage-based Billing	(X)
Destination-sensitive Billing	

Many Features Act on Traffic

- Many features need to understand network traffic
  - Quality of Service
  - Security
  - Broadband
  - NetFlow
  - Routing
  - … and many others
- Issue: Each feature might take a unique approach
  - Different configuration command syntax
  - Unnecessary complexity for customers

Agenda

- What Is the Business Case? How to Approach It?
- What Are the Nuts and Bolts of NBAR?
- How to Compare Multiple Features?
- What Did We Cover?
- What's Left?

NBAR Versus Access Control List (ACL)

ACL:

- Classify static port protocols
- Provide an easy way for blocking traffic
- Less CPU overhead (pre-compiled ACLs)
- No monitoring function (CLI only)

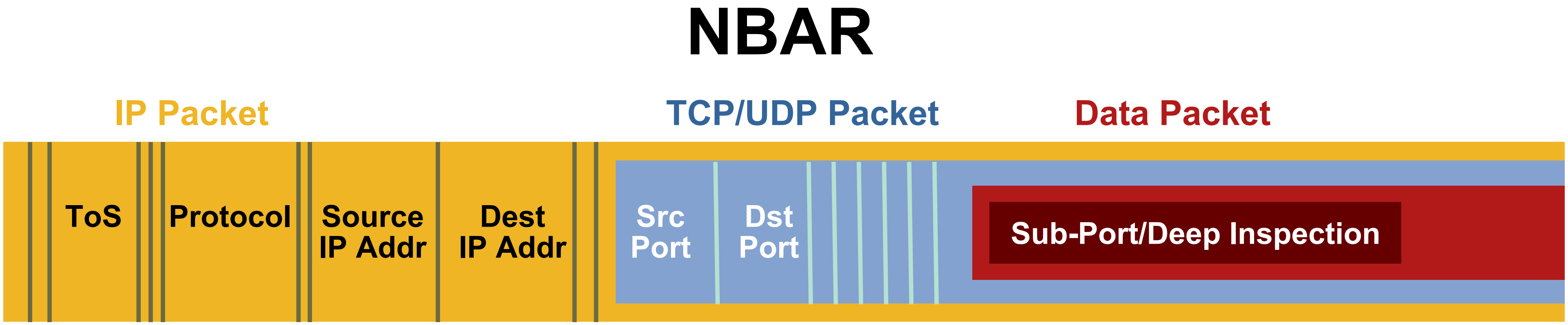
NBAR:

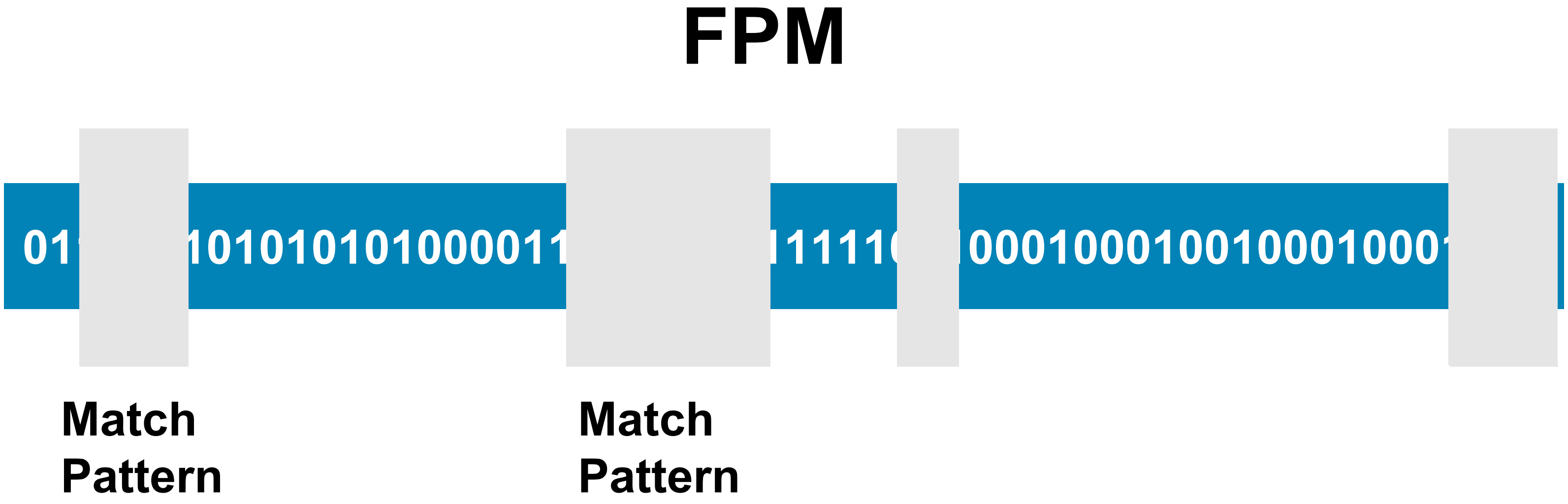
- Classify static and dynamic port protocols
- Provide an easy way for prioritizing traffic
- Monitoring function
- MIB support
- Higher CPU impact
- Max. 16 ports per protocol

Introducing Flexible Packet Matching (FPM)

- FPM was developed to identify virus signatures anywhere in the packet and flow
- A match statement defines signatures and every packet is inspected and dropped, if a match occurs
- Ability to match on arbitrary bits of a packet at arbitrary depth (offset) in the packet
- Allows Layer 2–Layer 7 stateless classification and match capability
- Gives the possibility to identify attacks on legitimate ports—for example an attack on port 80
- Introduced in Cisco IOS 12.4(4)T
- Cisco 871 Series, 1700, 1800, 2600 (2600XM, 2691), 3700, 3800, 7200, and 7301 Series Routers.
- FPM will be accelerated in HW with Sup32-PISA at a speed of up to 2Gbps

NBAR Versus Flexible Packet Matching (FPM)



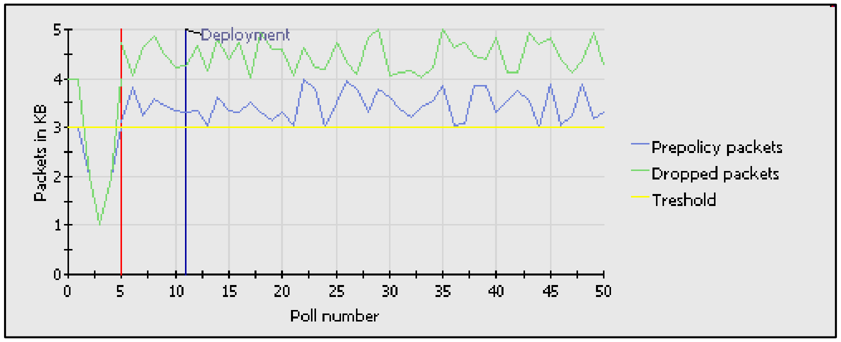


Cisco Class-Based QoS MIB

- NBAR Protocol-Discovery-MIB monitors traffic recognized by PDLMs
- Cisco Class-based QoS MIB provides statistics for all MQC “match” operation
- Statistics include summary counts (bits/bytes/packets), rates pre-policy (input), and post-policy (output)
- Features monitored includes queueing, traffic-shaping, packet-marking, random-detection, etc.
- Monitors QoS statistics on interfaces and subinterfaces
- ciscoCBQosMIB

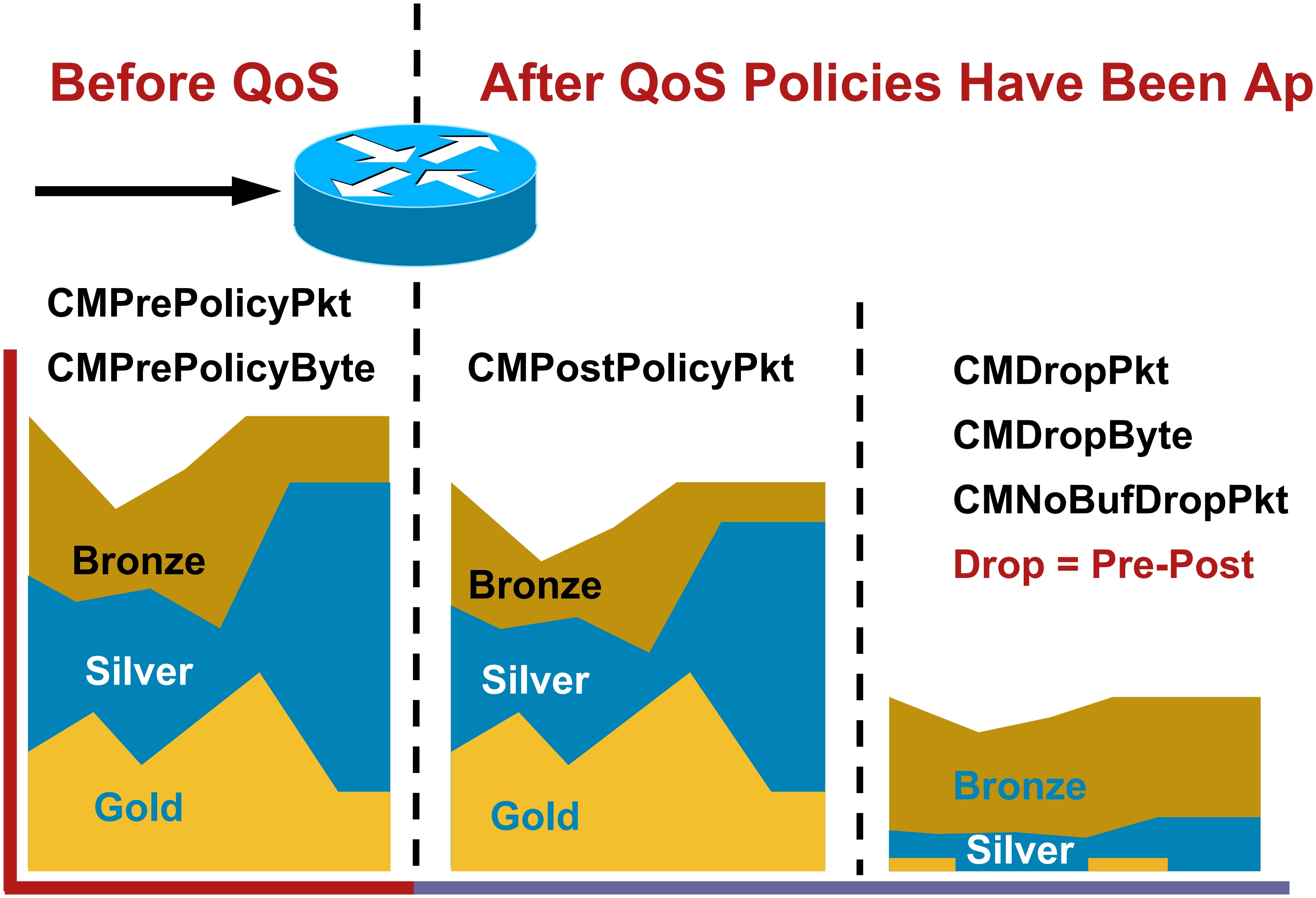
CBQoS MIB

```
1 : cbQosServicePolicy
2 : cbQosInterfacePolicy
3 : cbQosFrameRelayVCPolicy
4 : cbQosATMPVCPolicy
5 : cbQosObjects

6 : cbQosPolicyMapCfg
7 : cbQosClassMapCfg
8 : cbQosMatchStmtCfg
9 : cbQosQueueingCfg
10: cbQosREDCfg
11: cbQosREDClassCfg
12: cbQosPoliceCfg
13: cbQosTSCfg
14: cbQosSetCfg

15: cbQosClassMapStats
16: cbQosMatchStmtStats
17: cbQosPoliceStats
18: cbQosQueueingStats
19: cbQosTSStats
20: cbQosREDClassStats
```



ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CLASS-BASED-QOS-MIB.my

Cisco Class-Based-QoS MIB
Class-Map Stats Table (cbQosCMstats)



Before QoS

After QoS Policies Have Been Applied

CMPrePolicyPkt

CMPrePolicyByte

CMPostPolicyPkt

CMDropPkt

CMDropByte

CMNoBufDropPkt

Drop = Pre-Post

MQC Configuration and CB-QoS-MIB

1. Define traffic classes with MQC

```
class-map match-all my_default_class
 match ip dscp default
class-map match-all my_CS1_class
 match ip dscp cs1
…
```

cbQosClassMapCfg

cbQosMatchstmtCfg

2. Create a service policy by associating a class to a policy

```
policy-map mypolicy
    class my_default_class
    class my_CS1_class
   …
```

cbQosPolicyMapCfg

cbQosPoliceCfg

3. Attach a service policy to an interface

```
interface Ethernet0/0
    service-policy [input|output] mypolicy
```

4. Show policy statistics

```
show policy-map interface
```

cbQosPoliceStats
cbQosClassMapStats
cbQosMatchstmtStats

NBAR and AutoQoS

- Cisco IOS AutoQos feature has two flavors

  1. AutoQoS for VoIP: one stage mechanism, creates pre-defined policy maps for voice traffic

  2. AutoQoS Enterprise

     I) Turn on the discovery mode and gather traffic statistics
     (config-if)# "auto discovery qos"

     II) A policy map is created based on the detected traffic with suggested bandwidth settings per class

     Two modes

     "Trusted mode" in case DSCP has been set correct

     "Untrusted mode" discovers applications by leveraging NBAR

- Introduced in 12.3 T

Cisco AutoQoS for Enterprise

Traffic Class	DSCP
IP Routing	CS6
Interactive Voice	EF
Interactive Video	AF41
Streaming Video	CS4
Telephony Signaling	CS3
Transaction/Interactive	AF21
Network Management	CS2
Bulk Data	AF11
Best Effort	0
Scavenger	CS1

Procedure

1. **Invoke "auto discovery qos" on the applicable link**

   Use "show auto discovery qos" to view data collection in progress

2. **Automatically configure the link with "auto qos" command**

   Use "show auto qos" to display the QoS policy settings deployed

3. **Use “auto discovery trust” in the core if DSCP values are already assigned at the edge**

Cisco AutoQoS: Discovery in Progress

```
router# show auto discovery qos

AutoQoS Discovery enabled for applications
 Discovery up time: 2 days, 55 minutes
 AutoQoS Class information:
 Class VoIP:
 Recommended Minimum Bandwidth: 517 Kbps/50% (PeakRate)
 Detected applications and data:
 Application/    AverageRate    PeakRate   Total
 Protocol      (kbps/%)      (kbps/%)   (bytes)
 rtp audio     76/7        517/50    703104
 Class Interactive Video:
 Recommended Minimum Bandwidth: 24 Kbps/2% (AverageRate)
 Detected applications and data:
 Application/    AverageRate    PeakRate   Total
 Protocol      (kbps/%)      (kbps/%)   (bytes)
 rtp video     24/2        5337/52    704574
 Class Transactional:
 Recommended Minimum Bandwidth: 0 Kbps/0% (AverageRate)
 Detected applications and data:
 Application/    AverageRate    PeakRate   Total
 Protocol      (kbps/%)      (kbps/%)   (bytes)
 citrix        36/3        74/7    30212
 sqlnet        12/1        7/<1    1540
```

Cisco AutoQoS: Suggested Policy

```
Suggested AutoQoS Policy for the current uptime:
 !
 class-map match-any AutoQoS-Voice-Et3/1
 match protocol rtp audio
 !
 class-map match-any AutoQoS-Inter-Video-Et3/1
 match protocol rtp video
 !
 class-map match-any AutoQoS-Signaling-Et3/1
 match protocol sip
 match protocol rtcp
 !
 class-map match-any AutoQoS-Transactional-Et3/1
 match protocol citrix
 !
 class-map match-any AutoQoS-Bulk-Et3/1
 match protocol exchange

policy-map AutoQoS-Policy-Et3/1
 class AutoQoS-Voice-Et3/1
 priority percent 1
 set dscp ef
 class AutoQoS-Inter-Video-Et3/1
 bandwidth remaining percent 1
 set dscp af41
 class AutoQoS-Signaling-Et3/1
 bandwidth remaining percent 1
 set dscp cs3
```

Recommended Policy Is Based on AutoDiscovery Statistics

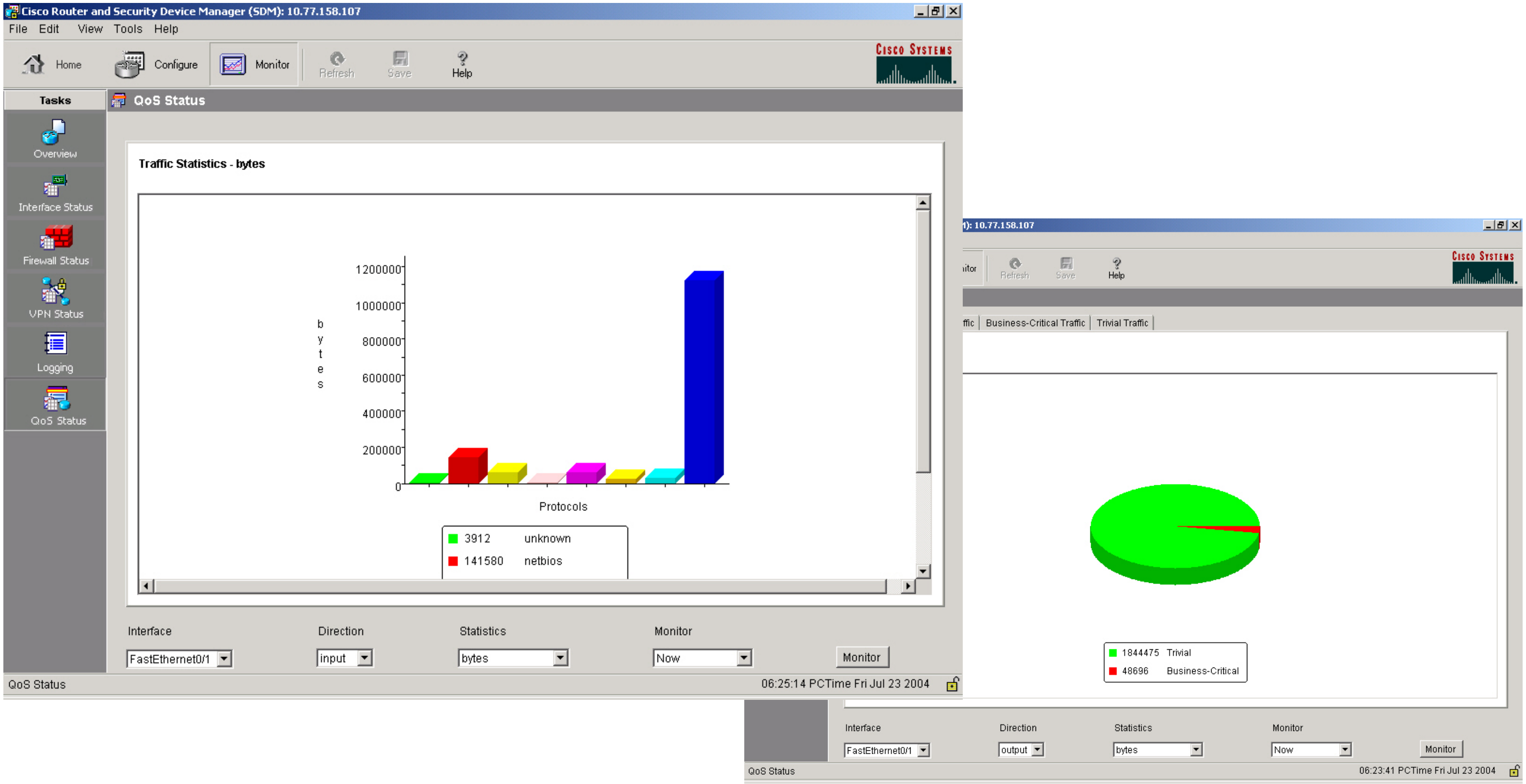
Options

- Continue AutoDiscovery (policy may change)
- Copy and change the policy (offline)

```
. . .
 class AutoQoS-Transactional-Et3/1
 bandwidth remaining percent 1
 random-detect dscp-based
 set dscp af21
 class AutoQoS-Bulk-Et3/1
 bandwidth remaining percent 1
 random-detect dscp-based
 set dscp af11
 class class-default
 fair-queue
```

Cisco Router and Security Device Manager (SDM)

GUI for Device Configuration and Monitoring



Cisco Router and Security Device Manager (SDM): 10.77.158.107

QoS Status

Traffic Statistics - bytes

🟩 3912	unknown
🟥 141580	netbios

Interface: FastEthernet0/1 · Direction: input · Statistics: bytes · Monitor: Now

QoS Status — 06:25:14 PCTime Fri Jul 23 2004

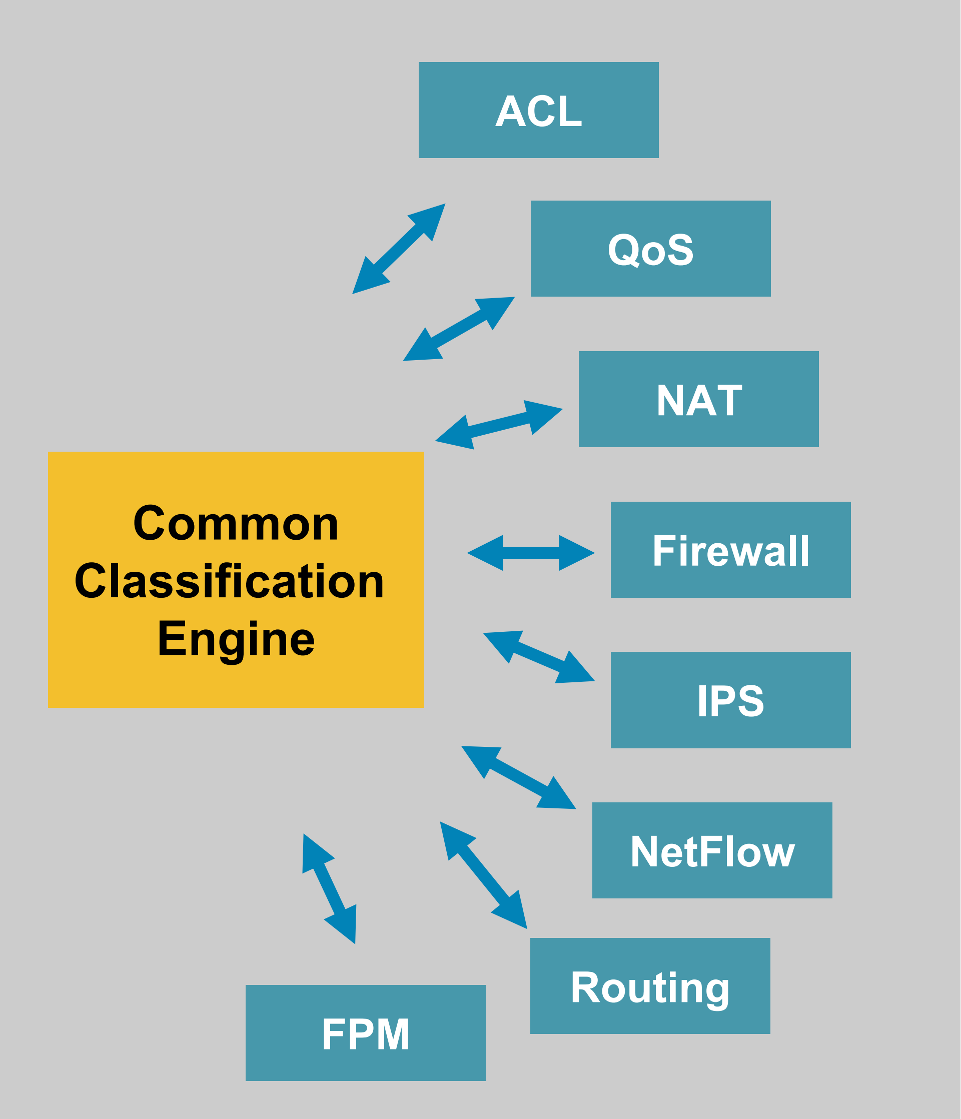
🟩 1844475	Trivial
🟥 48696	Business-Critical

Interface: FastEthernet0/1 · Direction: output · Statistics: bytes · Monitor: Now

QoS Status — 06:23:41 PCTime Fri Jul 23 2004

Future Direction for Cisco IOS Traffic Classification

- Traffic classification for multiple client services in a high volume, distributed environment
- Unified configuration language
- Uniform provisioning across platforms



SCE vs. NBAR

SCE (Cisco Service Control Engine 1000/2000 Series):

- Objective: special purpose appliance for application recognition and monitoring / usage analysis
- Stateful deep packet inspection
- Multi-gigabit analysis and control
- Subscriber and application awareness
  (in conjunction with a Policy Manager)
- Dynamic bandwidth control
- Sold separately

NBAR:

- Objective: Integrated application recognition feature within Cisco IOS
- Stateful deep packet inspection
- Static bandwidth control
- Included in IOS license

Cisco Traffic Anomaly Detector vs. NBAR

Traffic Anomaly Detector:

- Objective: identify traffic anomalies and *unknown* attacks
- Special purpose appliance/blade for anomaly detection
- Granular, per-connection state analysis of all packets
- Session-state context recognizes validated session traffic
- Detects and defeats complex DDoS attacks and per-flow deviations
- Sold separately

NBAR:

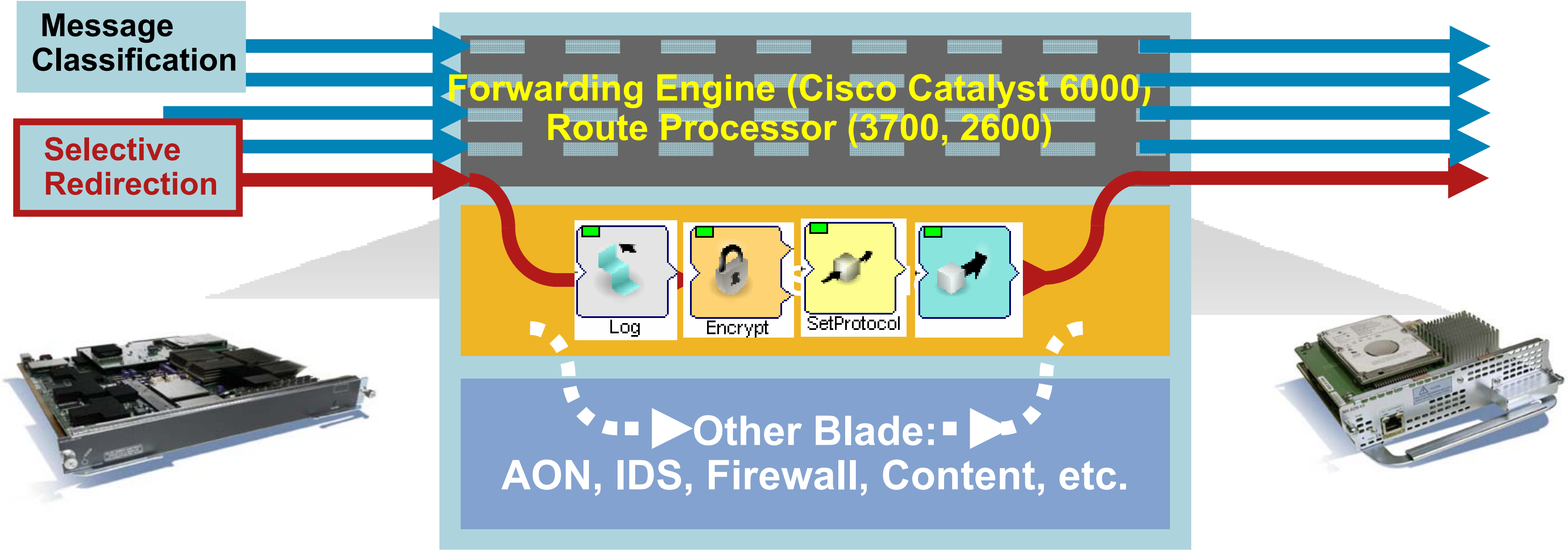
- Objective: Block *known* virus/p2p/attacks
- Integrated feature within Cisco IOS
- Stateful deep packet inspection
- Static bandwidth control
- Included in IOS license

Traffic Anomaly Detector XT 5600

Traffic Anomaly Detector Module

NBAR and AON

- **NBAR monitors all traffic**
- **Only “relevant” traffic is sent to AON blade**


Message Classification
Selective Redirection
Forwarding Engine (Cisco Catalyst 6000)
Route Processor (3700, 2600)
Log
Encrypt
SetProtocol
Other Blade:
AON, IDS, Firewall, Content, etc.

IP SLA vs. NBAR

IP SLA:

- Objective: SLA verification
- Synthetic measurement (active)
- Measures per class of service
- Application agnostic
- Emulates some applications only (DNS, DHCP, http, RTP)
- Monitor and define thresholds for response time, jitter, delay, …
- IP SLA router can sit outside of the traffic path (Shadow router)
- Low CPU impact

NBAR:

- Objective: Application Recognition
- Observed measurement (passive)
- Deep packet inspection; application recognition, packet load inspection
- Monitor and define thresholds for bandwidth usage per application
- NBAR router needs to be in the traffic path
- Medium to high CPU impact

NetFlow vs. NBAR

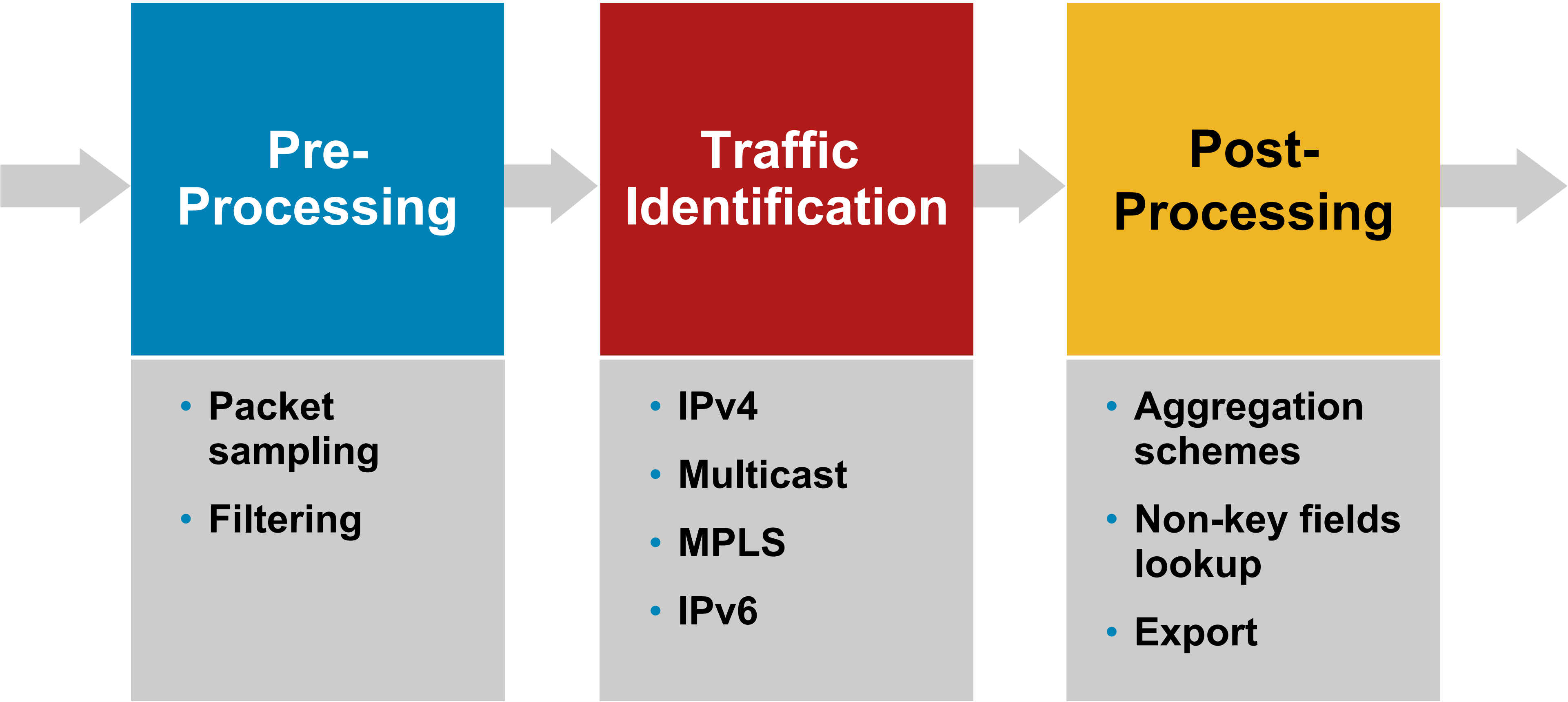
NetFlow:

- Integrated IOS functionality
- Monitors observed traffic
- Flow concept only
- Layer 2–4
- Push and pull (MIB) mode
- NetFlow export (push mode) provides more granular reporting functions (e.g. for billing)
- Flexible NetFlow offers user-defined flows
- Monitoring function only
- Medium to high CPU impact

NBAR:

- Integrated IOS functionality
- Monitors observed traffic
- Flow and packet concept for collection
- Layer 3–7
- Pull (MIB) mode only
- Fixed flow definition
- PDLMs for application and protocol specification
- Classify static and dynamic port protocols
- Monitoring function and traffic classification
- Medium to high CPU impact

NetFlow Processing Order



Pre-Processing

- Packet sampling
- Filtering

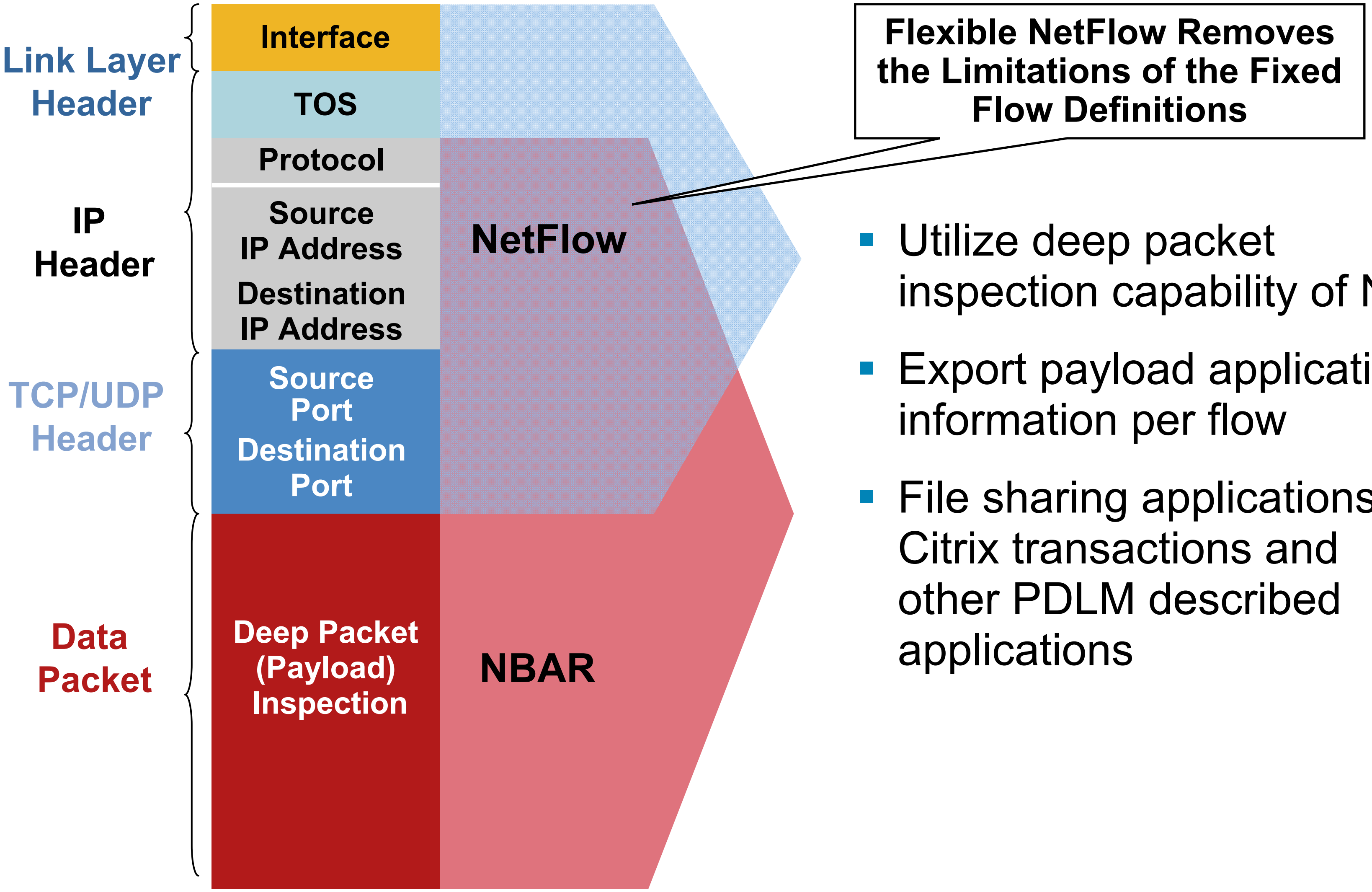
Traffic Identification

- IPv4
- Multicast
- MPLS
- IPv6

Post-Processing

- Aggregation schemes
- Non-key fields lookup
- Export

Future: NetFlow and NBAR



- Utilize deep packet inspection capability of NBAR
- Export payload application information per flow
- File sharing applications, Citrix transactions and other PDLM described applications

References

http://www.cisco.com/go/nbar

http:// www.cisco.com/go/netflow

http:// www.cisco.com/go/qos

- White Paper

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tqos_c/part_05/qsnbar1.htm#wp75985

- **Cisco Networking Integration with the Citrix ICA Protocol, www.support.citrix.com/**

  Document ID: CTX104475, July 2004, 17 pages

Agenda

- What Is the Business Case? How to Approach It?
- What Are the Nuts and Bolts of NBAR?
- How to Compare Multiple Features?
- What Did We Cover?
- What's Left?

Summary

- NBAR is a powerful feature to identify applications in the network
- NBAR is the vehicle for multiple other traffic classification features in Cisco IOS Software
- New protocols are constantly added
- NBAR deployment should be planned carefully
- Stay tuned for more ☺

This Sessions Theme:

“Traffic Classification is KEY to Provide Service Differentiation”

Mapping Technologies to Other Sessions

Session	Technology
Introduction to SNMP and MIBs Getting the Right Events from Network Elements	**SNMP**
Advanced NetFlow Usage	**NetFlow**
Performance Measurement with Cisco Devices	**NBAR, RMON, ART, CB-QoS MIB**
Introduction to Network Performance Measurement Advanced Network Performance Measurement	**IP SLA**

Agenda

- What Is the Business Case? How to Approach It?
- What Are the Nuts and Bolts of NBAR?
- How to Compare Multiple Features?
- What Did We Cover?
- What's Left?

Roadmap

- New PDLM´s:

  Skype 2.0/2.5

  Exchange 2003

  Winny

- Programmable IP Services Accelerator (Sup32-PISA) in Cat6k

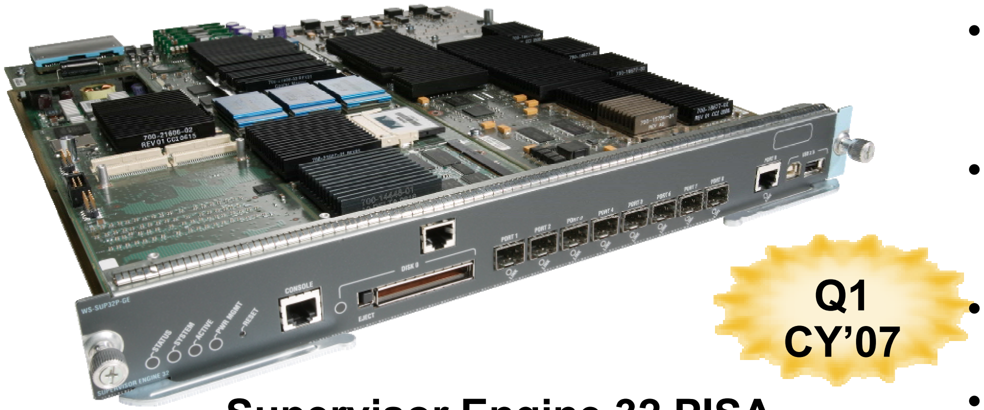
  Provides acceleration on NBAR and FPM for Layer 3 IPv4 Unicast packets.

  Performance 2Gbps

  Incorporate full Sup32 functionality

  Target Routed Access and Wan Edge deployments

Overview
Supervisor Engine 32 PISA



Q1 CY’07

Supervisor Engine 32 PISA
8x10GE Uplinks + 1x 10/100/100

Q2 CY’07

Supervisor Engine 32 PISA
2x10GE Uplinks + 1x 10/100/100

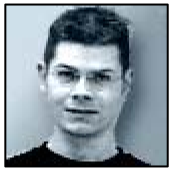
- Application awareness and classification – NBAR @ Multigigabit Speeds
- Flexible Packet Matching @ Multigigabit Speeds
- Deep Packet Inspection (Up to 4096 bytes)
- Programmable Architecture with the ability to seamlessly add new protocols and services
- IPv4 and IPv6 in hardware
- Advanced Multicast and MPLS Services
- Full Redundancy with NSF/SSO
- Enhanced Manageability (Embedded Event Manager, ERSPAN, Netflow)
- Comprehensive Security and QoS

Meet the Experts
Management & Operations

- Benoit Claise
  Distinguished Service Engineer

- Bruno Klauser
  Consulting Systems Engineer

- Emmanuel Tychon
  Technical Marketing Engineer



- Ralph Droms
  Technical Leader

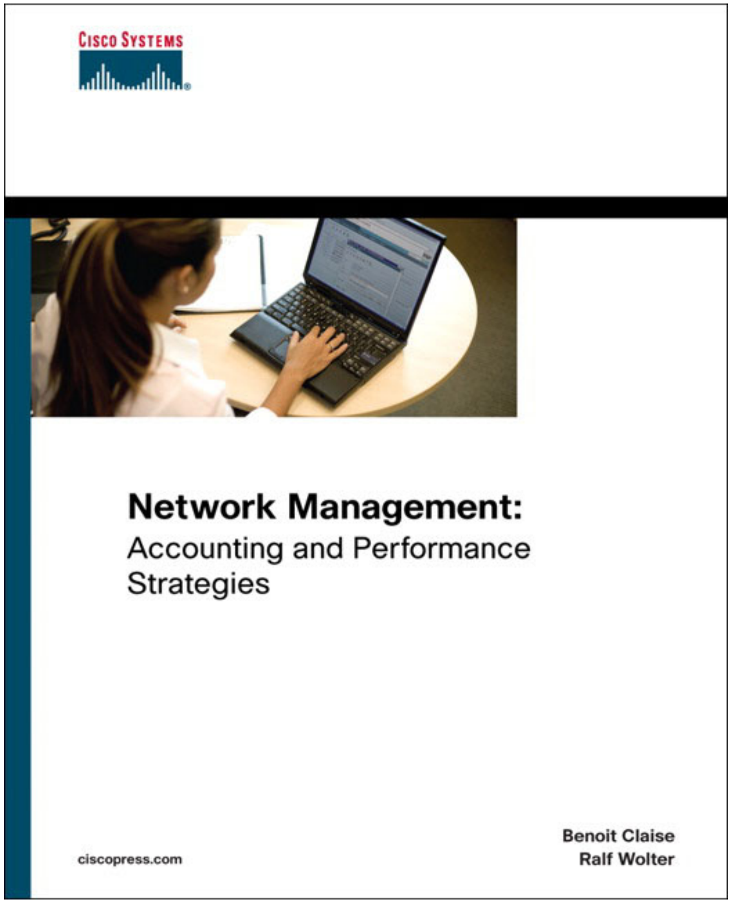
- Stephen Mullaney
  Technical Marketing Engineer

- Stuart Parham
  Consulting Systems Engineer

Recommended Reading

BRKNMS - 3007

- Network Management: Accounting and Performance Strategies (Jul 07)



Available in the Cisco Company Store

What is left?

Q and A

Management & Operations Sessions

Session Number	Session Title
BRKBBA -2005	NMS for Carrier Ethernet and Broadband Aggregation
BRKNMS -2001	Security of NM Systems in the Miscreant Economy
BRKNMS -2002	Managing Cisco IOS -XR Software
BRKNMS -2009	Unified Communication key factors for successful management
BRKNMS -2010	Managed Service Management
BRKNMS -2011	Data Sources and Tools provided by Cisco for ITIL Processes
BRKNMS -3003	Getting the Right Events from Network Elements
BRKNMS -3004	Adv. Network Performance Measurement with Cisco IP SLA
BRKNMS -3005	Name and Address Management with DNS and DHCP
BRKNMS -3006	Advanced NetFlow Deployment
BRKNMS -3007	Adv. Accounting and Performance Management with NBAR
BRKNMS -3008	Ethernet -OAM

Appendix

Ralf´s addings

- 1. FE channel supported only VLAN 1? see Tim's email, according to it the limitation is gone, however I'd like you to verify it in your lab!

To open a bug on this, see email and ST with Michael Ott

- 2. create slide that lists all supported interfaces FR, ATM, p2p, logical/physical - there was quite a number of questions related to it!

There is no such list created: with so many interfaces available in cisco platforms no-one has gone to the trouble of testing them all. Propose to do something in regards…

- 3. IPmc not supported as the traffic goes through a separate switching path (internally in IOS) - is this still the case?

Not supported. In the roadmap but no high priority

- 4. Add 6500 NBAR hardware feature card (contact Michael for details)

[mhelin]hardware accelerated nBAR on the 6k, best to check with Hasan Sairaj - who is the PM on the 6k side that owns the PISA blade. You may also work with TME Aurelie Fontaney. Support will not be before networkers´07

- 5. Can OER+NBAR be combined, maybe by using the "custom" feature?

[rahulpl]Not yet. 12.5 PI1 >> CSCsg56146

- 6. How to identify IGMP, IGRP traffic? Not done via pdlm
- 7. General roadmap and new PDLMs -> Michael

Got the roadmap, but Michael do not want to publish it! Adding one slide on this.

Applicability: Mapping Technologies to Applications

Scenario	Technology
Network Monitoring	NetFlow, BGP PA
Network Planning and Traffic Engineering	NetFlow, BGP PA
Application Monitoring	NBAR, RMON, ART
User Monitoring	AAA, NetFlow
QoS/CoS Monitoring	CB-QoS MIB, IP Acc., IP SLA
Security Analysis	NetFlow, IP Accounting
Peering and Transit Agreements	SNMP, NetFlow, BGP PA, IP Accounting
Time and Usage-based Billing	AAA, NetFlow, RMON
Destination and Source-sensitive Billing	BGP PA, NetFlow
VoIP Accounting	MIBs, AAA

Which Traffic Is Counted? From the Router’s Point of View

	Destined	Originated	Transit
SNMP MIBs	X	X	X
RMON, SMON			X
IP Accounting			X
IP Accounting Precedence			X
IP Accounting MAC			X
NBAR	X	X	X
BGP Policy Accounting		X	X
AAA	X		
NetFlow	(X)	(X)	X

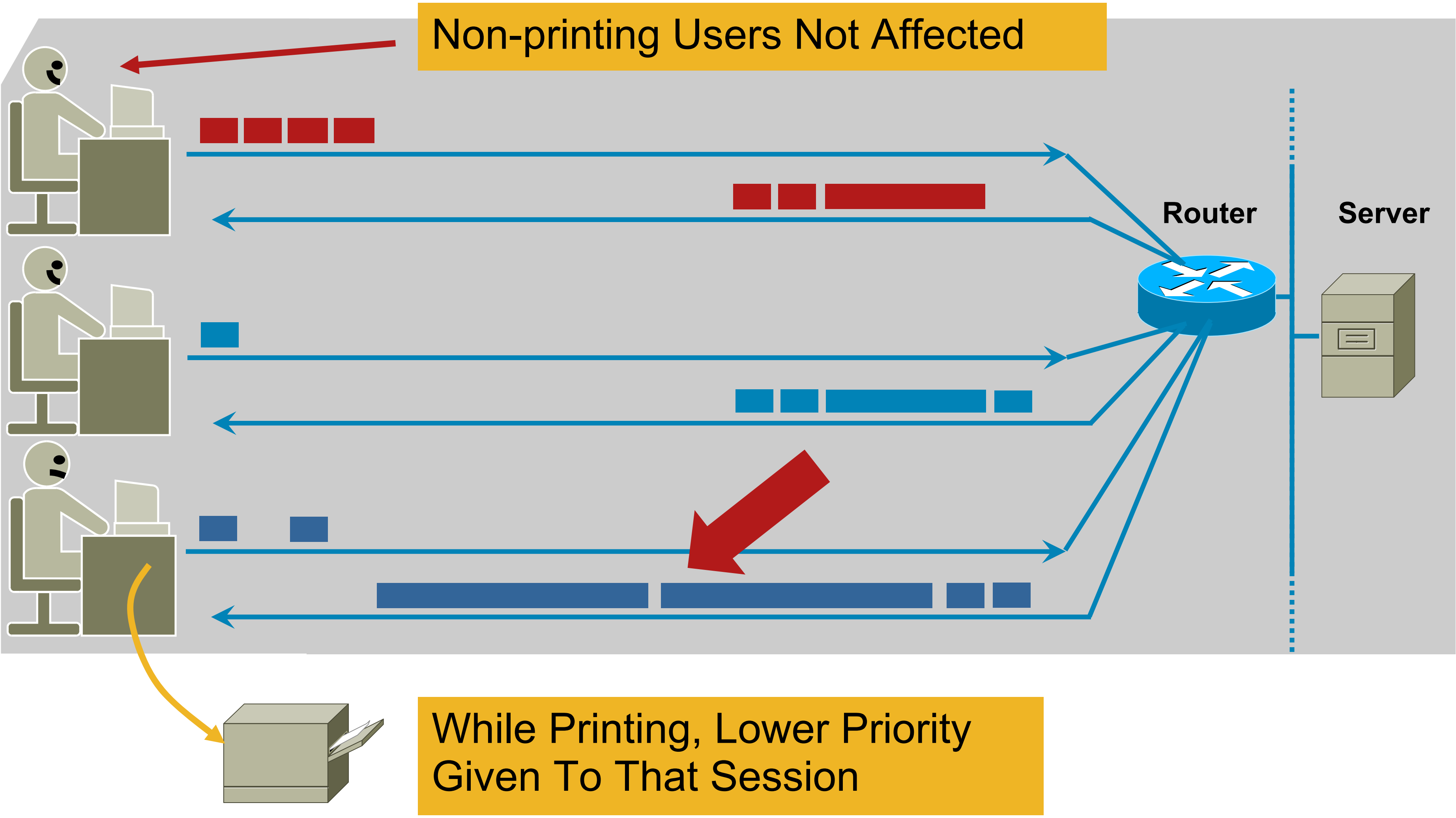
What Is the Capture Direction?

	Incoming	Outgoing	NA
SNMP MIBs	X	X	
RMON, SMON			X
IP Accounting		X	
IP Accounting Precedence	X	X	
IP Accounting MAC	X	X	
NBAR	X	X	
BGP Policy Accounting	X	X	
AAA	X	X	
NetFlow	X	(X)	

Can the Results Be Retrieved by SNMP?

	SNMP
SNMP MIBs	X
RMON, SMON	X
IP Accounting	X
IP Accounting Precedence	X
IP Accounting MAC	X
NBAR	X
BGP Policy Accounting	X
AAA	(X)
NetFlow	(X)

Managing Congestion with QoS Policies Based on Citrix ICA Virtual Channel Priorities



Non-printing Users Not Affected

While Printing, Lower Priority Given To That Session

How to Rate-Limit Citrix Print Traffic

1. Configure *class maps* that classify Citrix ICA traffic by ICA tag

```
     class-map match-any Citrix-high-medium-low
                match protocol citrix ica-tag “0”
                match protocol citrix ica-tag “1”
                match protocol citrix ica-tag “2”
     class-map Citrix-background
                match protocol citrix ica-tag “3”
```

2. Create a *policy map* that allocates bandwidth for traffic matched by the *class ma*

```
     policy-map Citrix-traffic
                class Citrix-high-medium-low
                  bandwidth percent 20
                class Citrix-background
                        bandwidth percent 5
                        police cir 128000
                               conform-action transmit
                               exceed-action drop
```

Assign 20% as minimum BW

Assign 5% as minimum BW

Transmit now if traffic within the 128kbps limit

Limit bits-per-second to 128 kbps (e.g., on 1.5 Mbps T1 link)

Drop now (TCP will retransmit later) if above limit

3. Assign the *policy map* to the router interface(s) *licy*

```
     Interface Serial 0/0
       service-policy output Citrix-traffic
```

Apply the policy-map to outbound traffic