Application Note

LiveAction®

Cisco Application Visibility and Controls (AVC) and Next Generation NBAR (NBAR2)

Contents

Introduction

Use this application note to use Cisco's Application Visibility and Control (AVC) to monitor and manage application performance metrics.

Cisco's Application Visibility and Control (AVC) technology leverages existing technologies such as NBAR2 in order to properly classify traffic types traversing the network infrastructure. With AVC, the aggregated flow destined to an application server can be measured from end to end. This allows the network to reach a higher level of application awareness and in turn collect performance metrics on said applications. With this data, the network administrator can act on the classified traffic in order to properly prioritize and control flow through QoS policies.[1]

With LiveNX 2.5 and greater, users can leverage the high network visibility provided by AVC and NBAR2, and perform active response to monitored traffic classes and flows. This application note provides instructions on enabling AVC and NBAR2 capabilities, within the context of the LiveNX software. A use case scenario will also be covered, outlining how LiveNX can be used to identify and analyze critical business traffic along with unwanted applications on the network. LiveNX's feature rich QoS functionality will then be utilized to mitigate the offending traffic by means of a policing policy incorporating Cisco's NBAR classification.

Next Generation NBAR (NBAR2)

NBAR2 is Cisco's latest generation of NBAR, providing a greater level of traffic classification based on its Deep Packet Inspection (DPI) engine. With over 1000 application signatures, and constantly updated protocol packs, NBAR2 has an added benefit to further identify and match multiple applications based on groups. For example, POP3, SMTP, MS Exchange, IMAP, and Gmail fall under the 'email' group.[2]

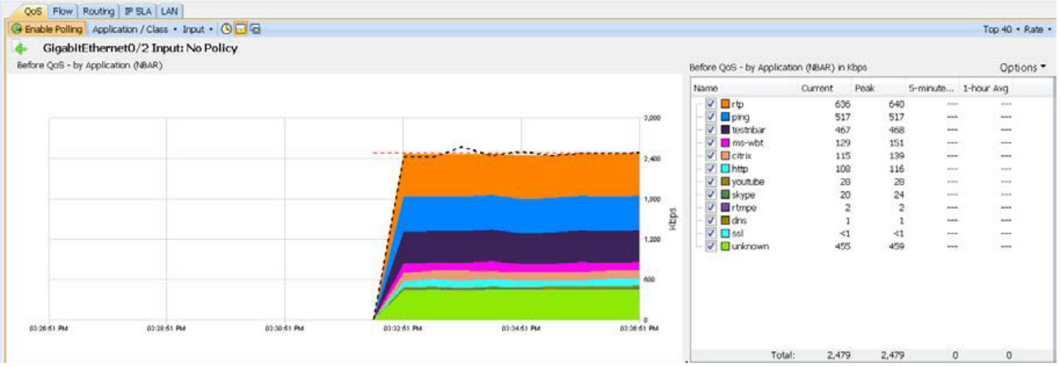
Use of NBAR2 extends to AVC as it provides the application recognition portion of the technology. With NBAR2 we can determine the exact traffic type as it traverses the router.

[1] http://www.cisco.com/en/US/prod/routers/application_visibility_control.html

[2] http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6616/qa_c67-697963.html

Instead of only showing HTTP or HTTPS traffic, we can peek into the actual nature of the web traffic. The following example displays the current and peak traffic rates of YouTube and Skype, both NBAR2 supported protocols according to:

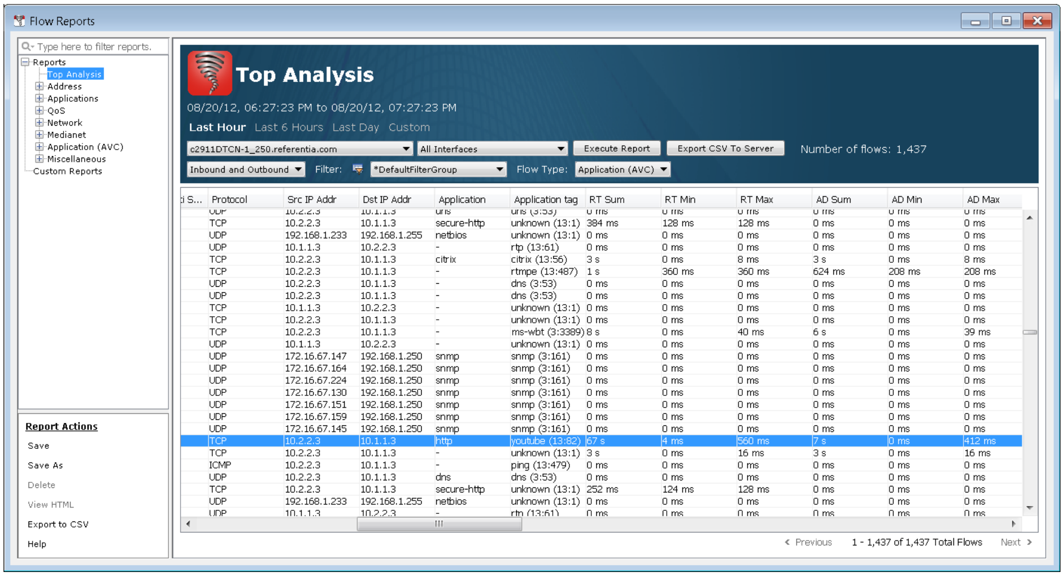
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6558/ps6616/product_bulletin_c25-627831.html



Before QoS - by Application (NBAR) in Kbps

Name	Current	Peak	5-minute...	1-hour Avg
☑ rtp	636	640	---	---
☑ ping	517	517	---	---
☑ tostribar	467	468	---	---
☑ ms-wbt	129	151	---	---
☑ citrix	115	139	---	---
☑ http	108	116	---	---
☑ youtube	28	28	---	---
☑ skype	20	24	---	---
☑ rtmpe	2	2	---	---
☑ dns	1	1	---	---
☑ ssl	<1	<1	---	---
☑ unknown	455	459	---	---
Total:	2,479	2,479	0	0

By opening up the LiveNX Flow Report, we can see the Application Tag used by AVC, derived from the NBAR2 DPI Engine. The following example shows YouTube assigned to 13:82.



08/20/12, 06:27:23 PM to 08/20/12, 07:27:23 PM

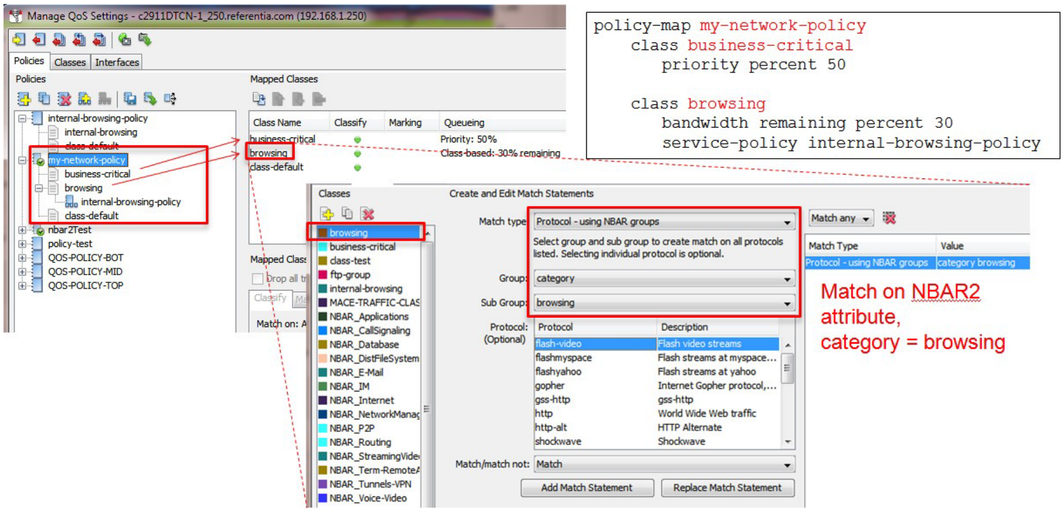
c2911DTCN-1_250.referentia.com | All Interfaces | Number of flows: 1,437

Inbound and Outbound | Filter: *DefaultFilterGroup | Flow Type: Application (AVC)

i S...	Protocol	Src IP Addr	Dst IP Addr	Application	Application tag	RT Sum	RT Min	RT Max	AD Sum	AD Min	AD Max
	UDP	10.2.2.3	10.1.1.3	dns	dns (3:53)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	TCP	10.2.2.3	10.1.1.3	secure-http	unknown (13:1)	384 ms	128 ms	128 ms	0 ms	0 ms	0 ms
	UDP	192.168.1.233	192.168.1.255	netbios	unknown (13:1)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	10.1.1.3	10.2.2.3	-	rtp (13:61)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	TCP	10.2.2.3	10.1.1.3	citrix	citrix (13:56)	3 s	0 ms	8 ms	3 s	0 ms	8 ms
	TCP	10.2.2.3	10.1.1.3	-	rtmpe (13:487)	1 s	360 ms	360 ms	624 ms	208 ms	208 ms
	UDP	10.2.2.3	10.1.1.3	-	dns (3:53)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	10.2.2.3	10.1.1.3	-	dns (3:53)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	TCP	10.1.1.3	10.2.2.3	-	unknown (13:1)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	TCP	10.2.2.3	10.1.1.3	-	unknown (13:1)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	TCP	10.2.2.3	10.1.1.3	-	ms-wbt (3:3389)	8 s	0 ms	40 ms	6 s	0 ms	39 ms
	UDP	10.1.1.3	10.2.2.3	-	unknown (13:1)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	172.16.67.147	192.168.1.250	snmp	snmp (3:161)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	172.16.67.164	192.168.1.250	snmp	snmp (3:161)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	172.16.67.224	192.168.1.250	snmp	snmp (3:161)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	172.16.67.130	192.168.1.250	snmp	snmp (3:161)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	172.16.67.151	192.168.1.250	snmp	snmp (3:161)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	172.16.67.159	192.168.1.250	snmp	snmp (3:161)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	172.16.67.145	192.168.1.250	snmp	snmp (3:161)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	67 s	4 ms	560 ms	7 s	0 ms	412 ms
	TCP	10.2.2.3	10.1.1.3	-	unknown (13:1)	3 s	0 ms	16 ms	3 s	0 ms	16 ms
	ICMP	10.2.2.3	10.1.1.3	-	ping (13:479)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	10.2.2.3	10.1.1.3	dns	dns (3:53)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	TCP	10.2.2.3	10.1.1.3	secure-http	unknown (13:1)	252 ms	124 ms	128 ms	0 ms	0 ms	0 ms
	UDP	192.168.1.233	192.168.1.255	netbios	unknown (13:1)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms
	UDP	10.1.1.3	10.2.2.3	-	rtp (13:61)	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms

1 - 1,437 of 1,437 Total Flows

LiveNX also allows full NBAR2 QoS control on Cisco routers both on a per-application level and also at the higher group level as we discussed earlier. T he following screenshots show an example where a network engineer is using the “browsing” group in his or her QoS classification. The “browsing” group includes applications such as flash-video, flash myspace, flash yahoo, http, shockwave and others. Taking advantage of Cisco’s NBAR2 grouping feature vastly reduces the complexity and verbosity of the router configuration.



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

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

Manage QoS Settings - c2911DTCN-1_250.referentia.com (192.168.1.250)

Policies

- internal-browsing-policy
  - internal-browsing
  - class-default
- my-network-policy
  - business-critical
  - browsing
    - internal-browsing-policy
  - class-default
- nbar2Test
- policy-test
- QOS-POLICY-BOT
- QOS-POLICY-MID
- QOS-POLICY-TOP

Mapped Classes

Class Name	Classify	Marking	Queueing
business-critical	●		Priority: 50%
browsing	●		Class-based: 30% remaining
class-default	●		

Classes: browsing, business-critical, class-test, ftp-group, internal-browsing, MACE-TRAFFIC-CLAS, NBAR_Applications, NBAR_CallSignaling, NBAR_Database, NBAR_DistFileSystem, NBAR_E-Mail, NBAR_IM, NBAR_Internet, NBAR_NetworkManag, NBAR_P2P, NBAR_Routing, NBAR_StreamingVide, NBAR_Term-RemoteA, NBAR_Tunnels-VPN, NBAR_Voice-Video

Create and Edit Match Statements

Match type: Protocol - using NBAR groups

Select group and sub group to create match on all protocols listed. Selecting individual protocol is optional.

Group: category

Sub Group: browsing

Protocol: (Optional)

Protocol	Description
flash-video	Flash video streams
flashmyspace	Flash streams at myspace...
flashyahoo	Flash streams at yahoo
gopher	Internet Gopher protocol,...
gss-http	gss-http
http	World Wide Web traffic
http-alt	HTTP Alternate
shockwave	Shockwave

Match/match not: Match

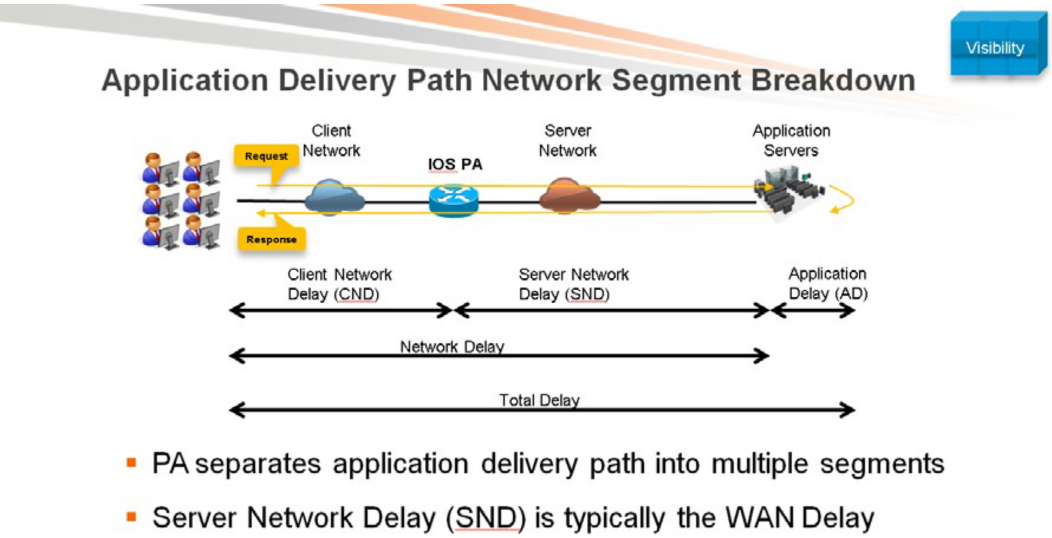
Match any

Match Type	Value
Protocol - using NBAR groups	category browsing

Match on NBAR2 attribute, category = browsing

Application Visibility and Control (AVC)

AVC provides intermediary network devices a look at various performance metrics from a client-server perspective. By means of AVC NetFlow, these values can easily be used to determine the performance of the client-side network, the server-side network, and the actual processing time of the application server.[3]

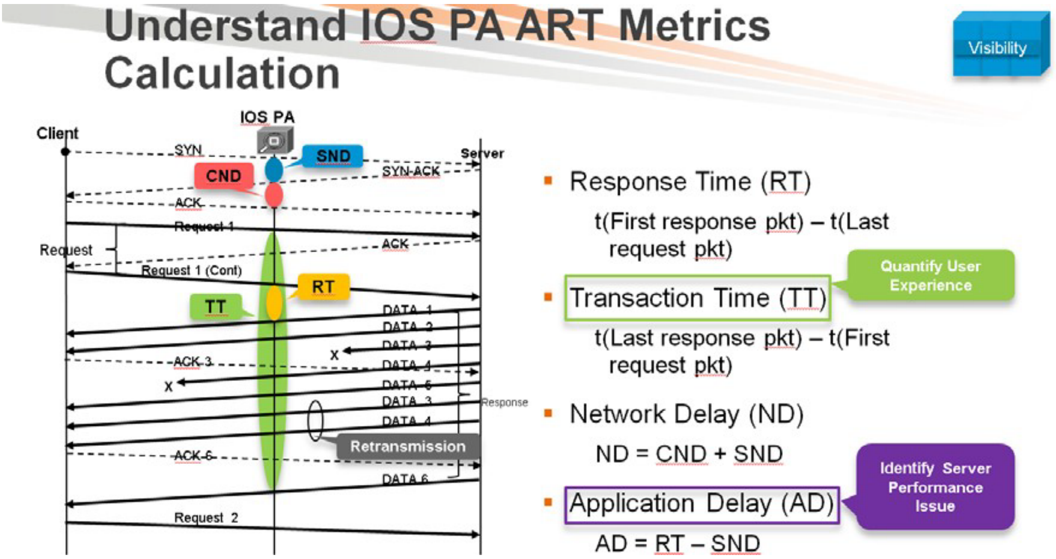


Application Delivery Path Network Segment Breakdown

- PA separates application delivery path into multiple segments
- Server Network Delay (SND) is typically the WAN Delay

The main difference between AVC as a flow mechanism, over Traditional NetFlow and Flexible NetFlow, is the fact that it primarily utilizes 4 out of the 5-tuple information typically associated with flow data. With AVC, we are only concerned with the source IP address, destination IP address, IP protocol, and destination port. The source port was omitted in order to reduce the overall number of individual flows to process by aggregating similar sessions into one AVC flow. Data provided by AVC are typically associated with sum totals, averages, and min/max values.[3]

[3] Kangwarn Chinthammit, BRKRST-2065 Application Visibility Control, Cisco Live US 2012, June 2012



Understand IOS PA ART Metrics Calculation

Visibility

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

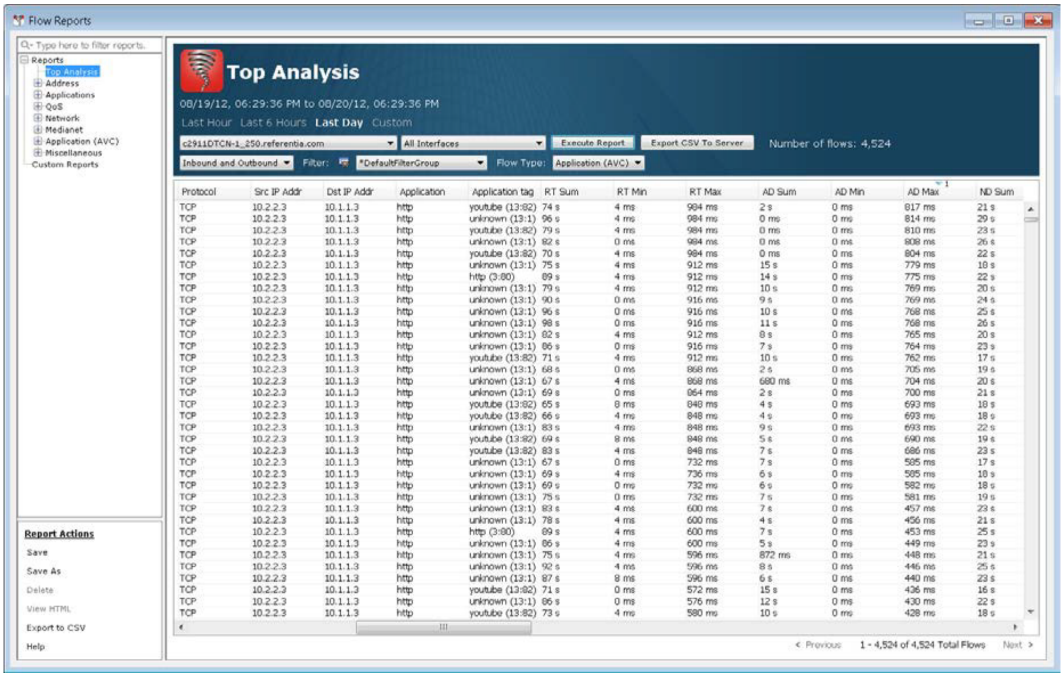
Quantify User Experience

Identify Server Performance Issue

To fully understand AVC, we have to take a look at other performance metric fields and the methods for which they are calculated. Using the standard Three-Way Handshake, we can see where the Application Response Time (ART) values are derived from.

LiveNX uses the very same information to populate the AVC flow list on each supported network device in the topology. The following is only a short list of fields that can be viewed in the real-time device view and through the flow report section:

AD Sum	Application Delay Summation of all sessions in AVC flow AD
Min/Max	Application Delay Minimum/Maximum value in AVC flow
ND Sum	Network Delay Summation of all sessions in AVC flow
ND Min/Max	Network Delay Minimum/Maximum value in AVC flow
CND Sum	Client Network Delay Summation of all sessions in AVC flow
CND Min/Max	Client Network Delay Minimum/Maximum value in AVC flow
SND Sum	Server Network Delay Summation of all sessions in AVC flow
SND Min/Max	Server Network Delay Minimum/Maximum value in AVC flow



08/19/12, 06:29:36 PM to 08/20/12, 06:29:36 PM

c2911DTCN-1_250.referentia.com | All Interfaces | Number of flows: 4,524

Inbound and Outbound | Filter: *DefaultFilterGroup | Flow Type: Application (AVC)

Protocol	Src IP Addr	Dst IP Addr	Application	Application tag	RT Sum	RT Min	RT Max	AD Sum	AD Min	AD Max	ND Sum
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	74 s	4 ms	984 ms	2 s	0 ms	817 ms	21 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	96 s	4 ms	984 ms	0 ms	0 ms	814 ms	29 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	79 s	4 ms	984 ms	0 ms	0 ms	810 ms	23 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	82 s	0 ms	984 ms	0 ms	0 ms	808 ms	26 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	70 s	4 ms	984 ms	0 ms	0 ms	804 ms	22 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	75 s	4 ms	912 ms	15 s	0 ms	779 ms	18 s
TCP	10.2.2.3	10.1.1.3	http	http (3:80)	89 s	4 ms	912 ms	14 s	0 ms	775 ms	22 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	79 s	4 ms	912 ms	10 s	0 ms	769 ms	20 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	90 s	0 ms	916 ms	9 s	0 ms	769 ms	24 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	96 s	0 ms	916 ms	10 s	0 ms	768 ms	25 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	98 s	0 ms	916 ms	11 s	0 ms	768 ms	26 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	82 s	4 ms	912 ms	8 s	0 ms	765 ms	20 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	86 s	0 ms	916 ms	7 s	0 ms	764 ms	23 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	71 s	4 ms	912 ms	10 s	0 ms	762 ms	17 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	68 s	0 ms	868 ms	2 s	0 ms	705 ms	19 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	67 s	4 ms	868 ms	680 ms	0 ms	704 ms	20 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	69 s	0 ms	864 ms	2 s	0 ms	700 ms	21 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	65 s	8 ms	848 ms	4 s	0 ms	693 ms	18 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	66 s	4 ms	848 ms	4 s	0 ms	693 ms	18 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	83 s	4 ms	848 ms	9 s	0 ms	693 ms	22 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	69 s	8 ms	848 ms	5 s	0 ms	690 ms	19 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	83 s	4 ms	848 ms	7 s	0 ms	686 ms	23 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	67 s	0 ms	732 ms	7 s	0 ms	585 ms	17 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	69 s	4 ms	736 ms	6 s	0 ms	585 ms	18 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	69 s	0 ms	732 ms	6 s	0 ms	582 ms	18 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	75 s	0 ms	732 ms	7 s	0 ms	581 ms	19 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	83 s	4 ms	600 ms	7 s	0 ms	457 ms	23 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	78 s	4 ms	600 ms	4 s	0 ms	456 ms	21 s
TCP	10.2.2.3	10.1.1.3	http	http (3:80)	89 s	4 ms	600 ms	7 s	0 ms	453 ms	25 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	86 s	4 ms	600 ms	5 s	0 ms	449 ms	23 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	75 s	4 ms	596 ms	872 ms	0 ms	448 ms	21 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	92 s	4 ms	596 ms	8 s	0 ms	446 ms	25 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	87 s	8 ms	596 ms	6 s	0 ms	440 ms	23 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	71 s	0 ms	572 ms	15 s	0 ms	436 ms	16 s
TCP	10.2.2.3	10.1.1.3	http	unknown (13:1)	86 s	0 ms	576 ms	12 s	0 ms	430 ms	22 s
TCP	10.2.2.3	10.1.1.3	http	youtube (13:82)	73 s	4 ms	580 ms	10 s	0 ms	428 ms	18 s

1 - 4,524 of 4,524 Total Flows

Supported Platforms[4]

Cisco Integrated Services Routers (ISR) Generation 2

Platform	IOS	License
Cisco ISR 3900/2900/1900	15.2(4)M1	Data

Cisco Aggregation Services Routers (ASR)

Platform	IOS	License
ASR 1000	IOS XE 3.8S (FCS: December 2012)	Data

For the latest information regarding Cisco AVC, visit: *http://www.cisco.com/go/avc*

AVC Minimum IOS Configurations

The minimum set of configurations for AVC consists of two parts. First, the flow exporter, flow record and flow monitor must be configured for MACE (Measurement, Aggregation, and Correlation Engine). Second, NBAR must be configured for protocol-discovery. An example is shown below.

```
!Configure flow exporter for the LiveNX server
flow exporter LIVENX
destination 172.16.67.141
transport udp 2055
template data timeout 15
option interface-table
option application-table timeout 20

!Configure MACE flow record
flow record type mace MACE-RECORD
```

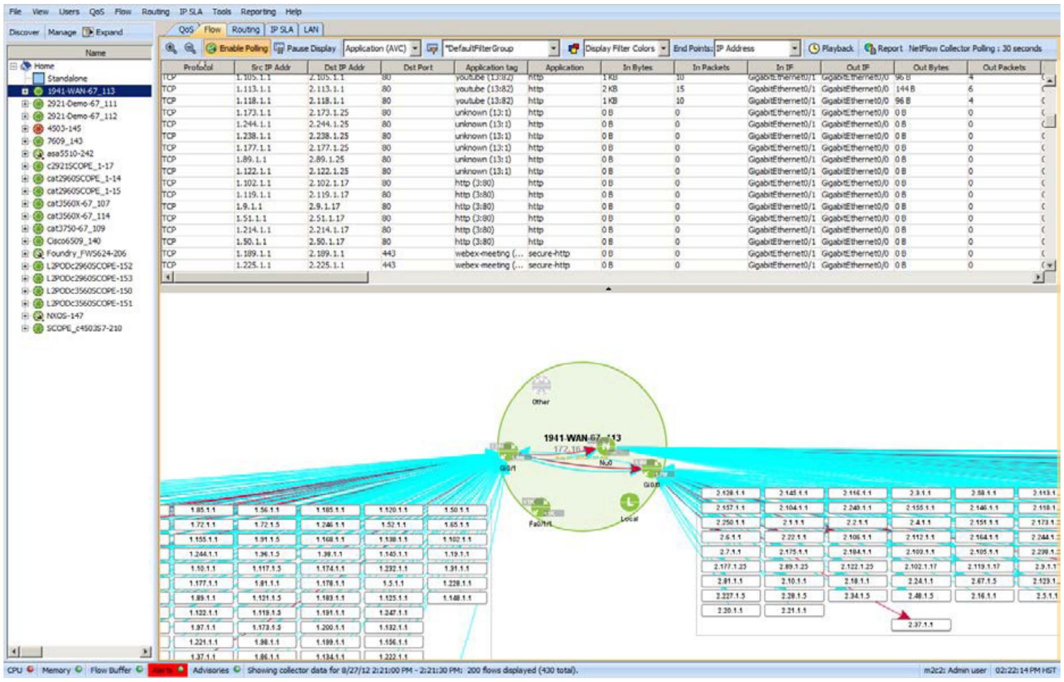
[4] http://www.cisco.com/en/US/prod/collateral/routers/ps9343/qa_c67-695977.html

```
collect ipv4 dscp
collect interface input
collect interface output
collect application name
collect counter client bytes
collect counter server bytes
collect counter client packets
collect counter server packets
collect art all

!
!Configure MACE flow monitor
flow monitor type mace MACE-MONITOR
record MACE-RECORD
exporter LIVENX

!
!Configure access-list and class-map for classification
!of traffic. This example, has a wide open ACL.
!This can be fine tuned for only traffic of interest.
ip access-list extended MACE-ACL
permit IP any any

class-map match-any MACE-TRAFFIC-CLASS
match access-group name MACE-ACL
!
!Configure MACE policy-map and apply flow-monitor action to thepolicy-map
policy-map type macemace_global
class MACE-TRAFFIC-CLASS
flow monitor MACE-MONITOR

!
!Enable mace and nbar protocol-discovery on monitored interfaces
!note that ip nbar protocol-discovery may be applied through LiveNX
!during the add device process. Enable mace on the WAN edge interface.
interface gig 0/1
description <WAN-EDGE-INTERFACE>
ip nbar protocol-discovery
mace enable
```

AVC Monitoring

AVC data may be monitored in LiveNX in four ways: device view, system view, alerts, and reports.

Device View



Protocol	Src IP Addr	Dst IP Addr	Dst Port	Application tag	Application	In Bytes	In Packets	In IF	Out IF	Out Bytes	Out Packets
TCP	1.105.1.1	2.105.1.1	80	youtube (13:82)	http	1 KB	10	GigabitEthernet0/1	GigabitEthernet0/0	96 B	4
TCP	1.113.1.1	2.113.1.1	80	youtube (13:82)	http	2 KB	15	GigabitEthernet0/1	GigabitEthernet0/0	144 B	6
TCP	1.118.1.1	2.118.1.1	80	youtube (13:82)	http	1 KB	10	GigabitEthernet0/1	GigabitEthernet0/0	96 B	4
TCP	1.173.1.1	2.173.1.25	80	unknown (13:1)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.244.1.1	2.244.1.25	80	unknown (13:1)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.238.1.1	2.238.1.25	80	unknown (13:1)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.177.1.1	2.177.1.25	80	unknown (13:1)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.89.1.1	2.89.1.25	80	unknown (13:1)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.122.1.1	2.122.1.25	80	unknown (13:1)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.102.1.1	2.102.1.17	80	http (3:80)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.119.1.1	2.119.1.17	80	http (3:80)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.9.1.1	2.9.1.17	80	http (3:80)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.51.1.1	2.51.1.17	80	http (3:80)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.214.1.1	2.214.1.17	80	http (3:80)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.50.1.1	2.50.1.17	80	http (3:80)	http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.189.1.1	2.189.1.1	443	webex-meeting (...	secure-http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0
TCP	1.225.1.1	2.225.1.1	443	webex-meeting (...	secure-http	0 B	0	GigabitEthernet0/1	GigabitEthernet0/0	0 B	0

Application (AVC)

*DefaultFilterGroup

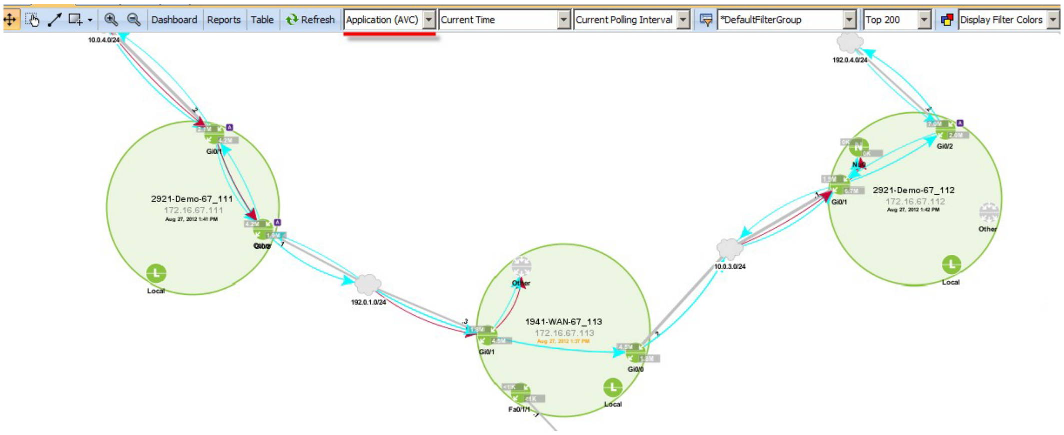
End Points: IP Address

NetFlow Collector Polling : 30 seconds

Showing collector data for 8/27/12 2:21:00 PM - 2:21:30 PM; 200 flows displayed (430 total).

The device view provides a real-time table of the AVC flows with a graphical view of the sources, endpoints, and transit interfaces for the traffic. The flow type selection drop-down menu may be used to display only AVC flow records.

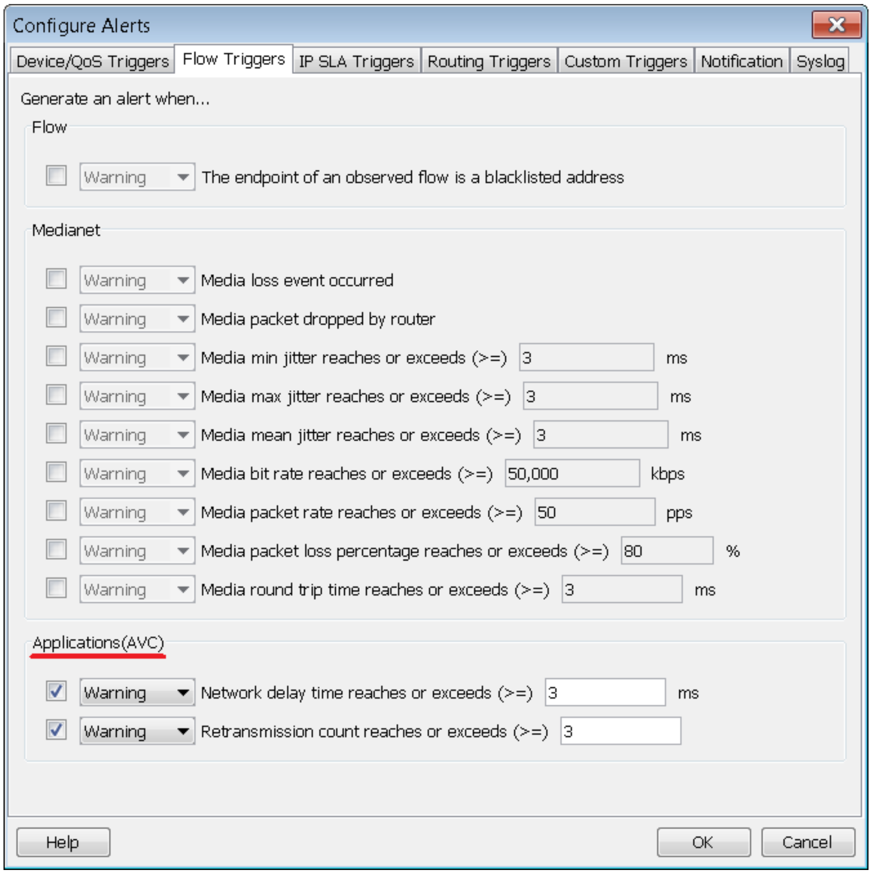
System View



The system view maps end-to-end traffic flows across your LiveNX topology. The flow type selection drop-down menu may be used to display only AVC.

Alerts

AVC alerts may be configured in Tools->Configure Alerts to increase visibility of network delay or retransmission events.



Generate an alert when...

Flow

□ Warning The endpoint of an observed flow is a blacklisted address

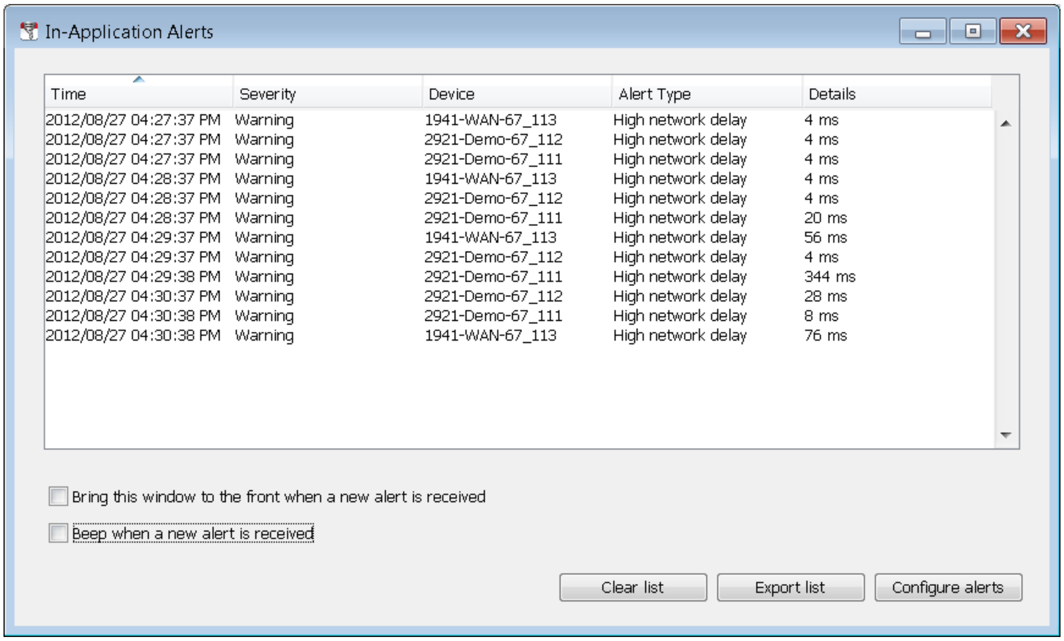
Medianet

□ Warning Media loss event occurred
□ Warning Media packet dropped by router
□ Warning Media min jitter reaches or exceeds (>=) 3 ms
□ Warning Media max jitter reaches or exceeds (>=) 3 ms
□ Warning Media mean jitter reaches or exceeds (>=) 3 ms
□ Warning Media bit rate reaches or exceeds (>=) 50,000 kbps
□ Warning Media packet rate reaches or exceeds (>=) 50 pps
□ Warning Media packet loss percentage reaches or exceeds (>=) 80 %
□ Warning Media round trip time reaches or exceeds (>=) 3 ms

Applications(AVC)

☑ Warning Network delay time reaches or exceeds (>=) 3 ms
☑ Warning Retransmission count reaches or exceeds (>=) 3

Triggered alerts are visible in the In-Application Alerts window.

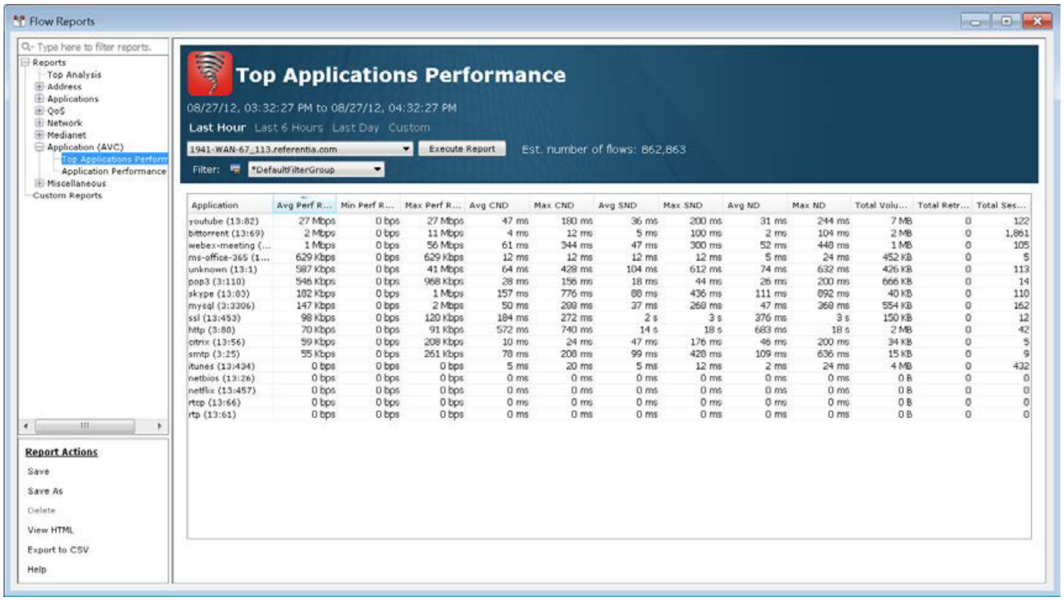


Time	Severity	Device	Alert Type	Details
2012/08/27 04:27:37 PM	Warning	1941-WAN-67_113	High network delay	4 ms
2012/08/27 04:27:37 PM	Warning	2921-Demo-67_112	High network delay	4 ms
2012/08/27 04:27:37 PM	Warning	2921-Demo-67_111	High network delay	4 ms
2012/08/27 04:28:37 PM	Warning	1941-WAN-67_113	High network delay	4 ms
2012/08/27 04:28:37 PM	Warning	2921-Demo-67_112	High network delay	4 ms
2012/08/27 04:28:37 PM	Warning	2921-Demo-67_111	High network delay	20 ms
2012/08/27 04:29:37 PM	Warning	1941-WAN-67_113	High network delay	56 ms
2012/08/27 04:29:37 PM	Warning	2921-Demo-67_112	High network delay	4 ms
2012/08/27 04:29:38 PM	Warning	2921-Demo-67_111	High network delay	344 ms
2012/08/27 04:30:37 PM	Warning	2921-Demo-67_112	High network delay	28 ms
2012/08/27 04:30:38 PM	Warning	2921-Demo-67_111	High network delay	8 ms
2012/08/27 04:30:38 PM	Warning	1941-WAN-67_113	High network delay	76 ms

□ Bring this window to the front when a new alert is received
□ Beep when a new alert is received

Reports

LiveNX can report on the performance of all applications or one particular application of interest.



08/27/12, 03:32:27 PM to 08/27/12, 04:32:27 PM

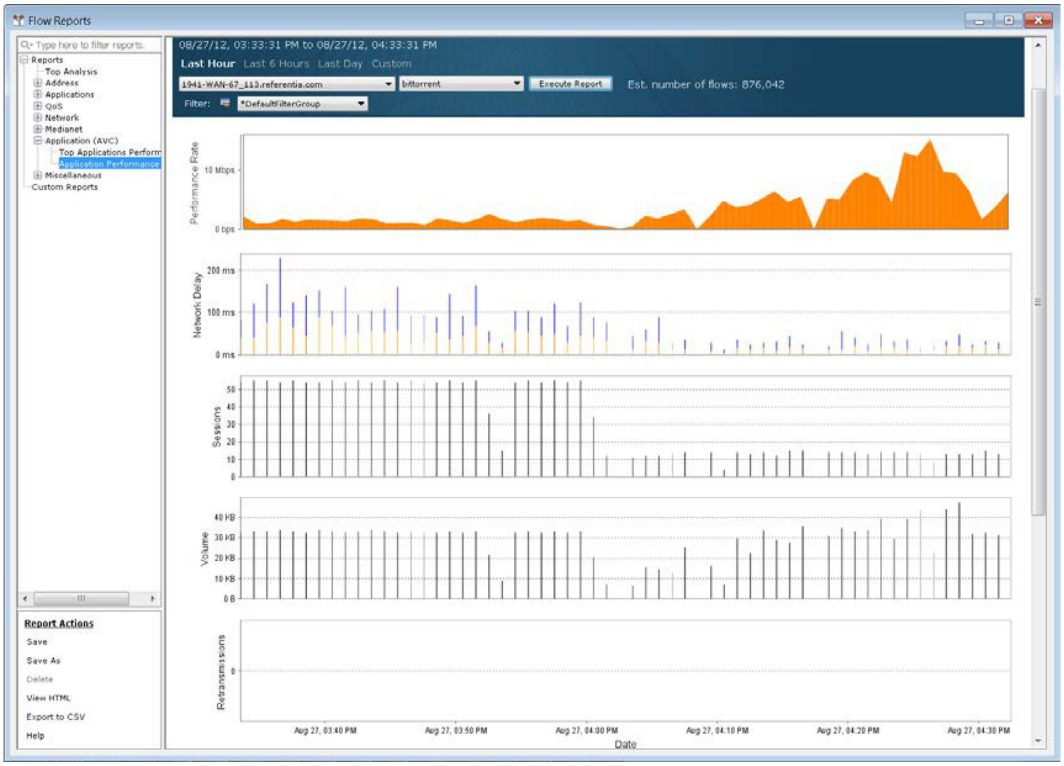
1941-WAN-67_113.referentia.com

Est. number of flows: 862,863

Filter: *DefaultFilterGroup

Application	Avg Perf R...	Min Perf R...	Max Perf R...	Avg CND	Max CND	Avg SND	Max SND	Avg ND	Max ND	Total Volu...	Total Retr...	Total Ses...
youtube (13:82)	27 Mbps	0 bps	27 Mbps	47 ms	180 ms	36 ms	200 ms	31 ms	244 ms	7 MB	0	122
bittorrent (13:69)	2 Mbps	0 bps	11 Mbps	4 ms	12 ms	5 ms	100 ms	2 ms	104 ms	2 MB	0	1,861
webex-meeting (...	1 Mbps	0 bps	56 Mbps	61 ms	344 ms	47 ms	300 ms	52 ms	448 ms	1 MB	0	105
ms-office-365 (1...	629 Kbps	0 bps	629 Kbps	12 ms	12 ms	12 ms	12 ms	5 ms	24 ms	452 KB	0	5
unknown (13:1)	587 Kbps	0 bps	41 Mbps	64 ms	428 ms	104 ms	612 ms	74 ms	632 ms	426 KB	0	113
pop3 (3:110)	546 Kbps	0 bps	968 Kbps	28 ms	156 ms	18 ms	44 ms	26 ms	200 ms	666 KB	0	14
skype (13:83)	182 Kbps	0 bps	1 Mbps	157 ms	776 ms	88 ms	436 ms	111 ms	892 ms	40 KB	0	110
mysql (3:3306)	147 Kbps	0 bps	2 Mbps	50 ms	288 ms	37 ms	268 ms	47 ms	368 ms	554 KB	0	162
ssl (13:453)	98 Kbps	0 bps	120 Kbps	184 ms	272 ms	2 s	3 s	376 ms	3 s	150 KB	0	12
http (3:80)	70 Kbps	0 bps	91 Kbps	572 ms	740 ms	14 s	18 s	683 ms	18 s	2 MB	0	42
citrix (13:56)	59 Kbps	0 bps	208 Kbps	10 ms	24 ms	47 ms	176 ms	46 ms	200 ms	34 KB	0	5
smtp (3:25)	55 Kbps	0 bps	261 Kbps	78 ms	208 ms	99 ms	428 ms	109 ms	636 ms	15 KB	0	9
itunes (13:434)	0 bps	0 bps	0 bps	5 ms	20 ms	5 ms	12 ms	2 ms	24 ms	4 MB	0	432
netbios (13:26)	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0 B	0	0
netflix (13:457)	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0 B	0	0
rtcp (13:66)	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0 B	0	0
rtp (13:61)	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0 B	0	0

The Top Applications Performance report displays in tabular form the performance metrics for all AVC applications for the device during the reporting time frame. A network administrator can drill down to an application of interest by right-clicking a row on the table or by launching an Application Performance report and selecting the appropriate application.



08/27/12, 03:33:31 PM to 08/27/12, 04:33:31 PM

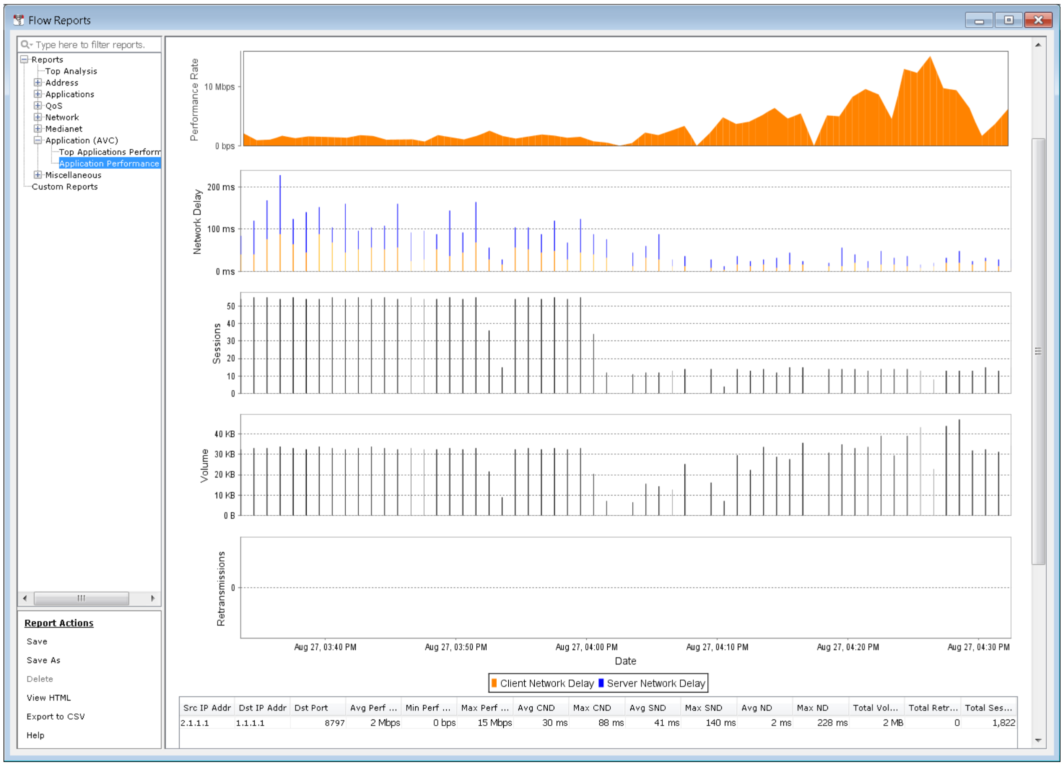
1941-WAN-67_113.referentia.com

bittorrent

Est. number of flows: 876,042

Filter: *DefaultFilterGroup

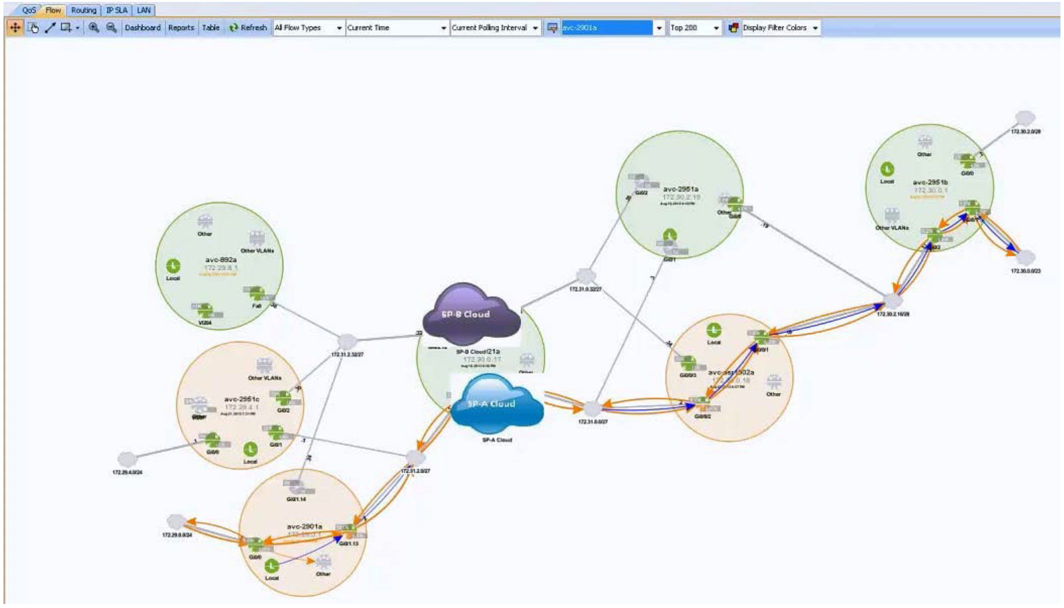
The Application Performance report plots performance metrics for one application over time. The flow entries for the application are shown in a table at the bottom of the Application Performance report. To drill down to the Top Analysis report for a specific flow entry, right-click on the table and select “View flow data.”



Src IP Addr	Dst IP Addr	Dst Port	Avg Perf ...	Min Perf ...	Max Perf ...	Avg CND	Max CND	Avg SND	Max SND	Avg ND	Max ND	Total Vol...	Total Retr...	Total Ses...
2.1.1.1	1.1.1.1	8797	2 Mbps	0 bps	15 Mbps	30 ms	88 ms	41 ms	140 ms	2 ms	228 ms	2 MB	0	1,822

AVC and NBAR2 Use Case Scenario[5]

This scenario revolves around a user experiencing degradation of critical business application performance due to BitTorrent utilizing a bulk of the WAN-edge bandwidth. With the help of LiveNX, and Cisco's AVC and NBAR2 technologies, we will walk through the steps to troubleshoot and resolve the performance issue affecting the network.

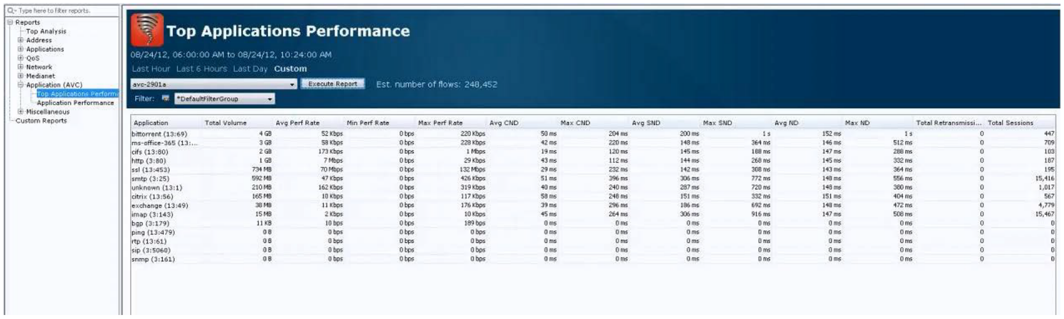


The current topology outlines the flow path between two sites, traversing a simulated Service Provider network. The majority of the scenario will focus on the avc-2901a router (bottom-left circle).

[5] Kangwarn Chinthammit, Technical Marketing Engineer, Troubleshoot and Resolve Application Performance with Cisco AVC and LiveAction, August 2012.

We begin with identifying the overall performance data of the top applications:

1. Right-click the device and select Flow, followed by Flow Report.
2. Under the Application (AVC) selector, choose Top Applications Performance.



Top Applications Performance

08/24/12, 06:00:00 AM to 08/24/12, 10:24:00 AM

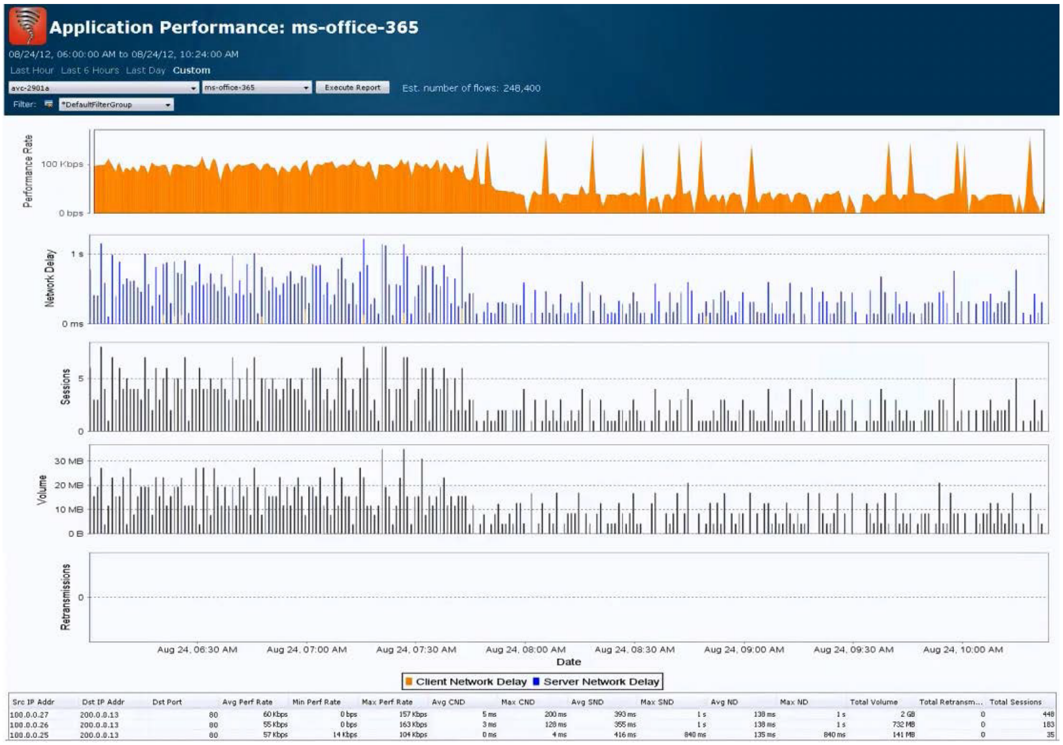
Est. number of flows: 248,452

Application	Total Volume	Avg Perf Rate	Min Perf Rate	Max Perf Rate	Avg CND	Max CND	Avg SND	Max SND	Avg ND	Max ND	Total Retransmissi...	Total Sessions
bittorrent (13:69)	4 GB	52 Kbps	0 bps	220 Kbps	50 ms	204 ms	200 ms	1 s	152 ms	1 s	0	447
ms-office-365 (13:...	3 GB	58 Kbps	0 bps	228 Kbps	42 ms	220 ms	148 ms	364 ms	146 ms	512 ms	0	709
cifs (13:80)	2 GB	173 Kbps	0 bps	1 Mbps	19 ms	120 ms	145 ms	188 ms	147 ms	288 ms	0	103
http (3:80)	1 GB	7 Mbps	0 bps	29 Kbps	43 ms	112 ms	144 ms	268 ms	145 ms	332 ms	0	187
ssl (13:453)	734 MB	70 Mbps	0 bps	132 Mbps	29 ms	232 ms	142 ms	308 ms	143 ms	364 ms	0	195
smtp (3:25)	592 MB	47 Kbps	0 bps	426 Kbps	51 ms	396 ms	306 ms	772 ms	148 ms	556 ms	0	15,416
unknown (13:1)	210 MB	162 Kbps	0 bps	319 Kbps	40 ms	240 ms	287 ms	720 ms	148 ms	380 ms	0	1,017
citrix (13:56)	165 MB	10 Kbps	0 bps	117 Kbps	58 ms	248 ms	151 ms	332 ms	151 ms	404 ms	0	567
exchange (13:49)	38 MB	11 Kbps	0 bps	176 Kbps	39 ms	296 ms	186 ms	692 ms	148 ms	472 ms	0	4,779
imap (3:143)	15 MB	2 Kbps	0 bps	10 Kbps	45 ms	264 ms	306 ms	916 ms	147 ms	508 ms	0	15,467
bgp (3:179)	11 KB	10 bps	0 bps	189 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0	0
ping (13:479)	0 B	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0	0
rtp (13:61)	0 B	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0	0
sip (3:5060)	0 B	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0	0
snmp (3:161)	0 B	0 bps	0 bps	0 bps	0 ms	0 ms	0 ms	0 ms	0 ms	0 ms	0	0

Here we see that the Total Volume of BitTorrent is greater than our mission-critical application, Microsoft Office 365. Depending on how saturated the WAN link is, this could impact the users' application experience. While this view is useful in identifying aggregate and average performance metrics, another option is to use view the data over time.

- Right-click on the desired application and select **View data over time**.

With the Microsoft Office 365 AVC flow selected, it is possible to see the reduction of the Performance Rate at approximately 8:00AM on August 24. The Performance Rate is the user's perceived performance of the selected application, defined as (Layer 7 Traffic Volume) / (Transaction Time). In this case, Microsoft Office 365's traffic volume is reduced due to BitTorrent's heavy network saturation resulting in a lower performance rate. Conversely, if an increase in delay were to be introduced into the path then the Transaction Time would also increase, causing a reduction in the overall performance rate.



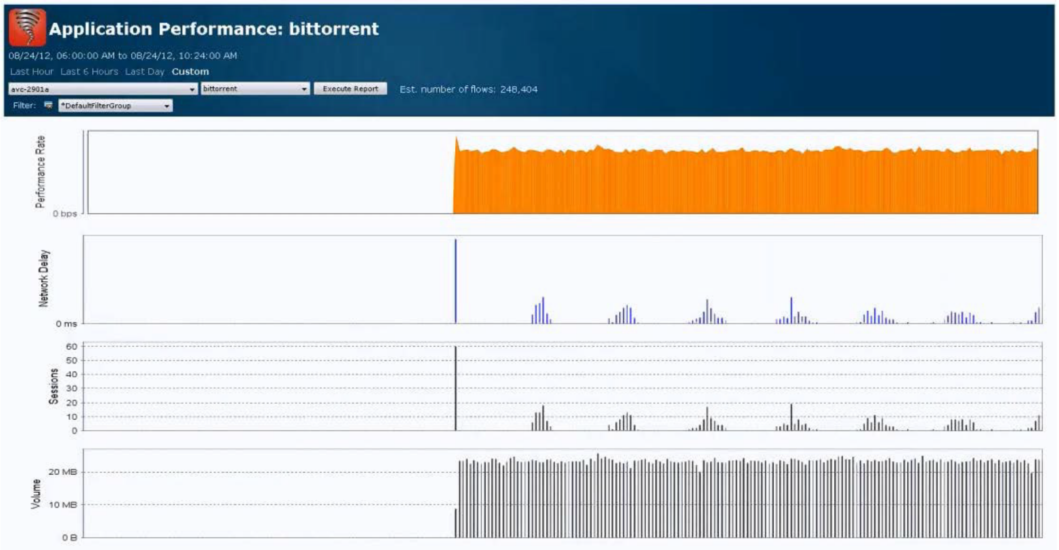
Application Performance: ms-office-365

08/24/12, 06:00:00 AM to 08/24/12, 10:24:00 AM

Est. number of flows: 248,400

Src IP Addr	Dst IP Addr	Dst Port	Avg Perf Rate	Min Perf Rate	Max Perf Rate	Avg CND	Max CND	Avg SND	Max SND	Avg ND	Max ND	Total Volume	Total Retransm...	Total Sessions
100.0.0.27	200.0.0.13	80	60 Kbps	0 bps	157 Kbps	5 ms	200 ms	393 ms	1 s	138 ms	1 s	2 GB	0	448
100.0.0.26	200.0.0.13	80	55 Kbps	0 bps	163 Kbps	3 ms	128 ms	355 ms	1 s	138 ms	1 s	732 MB	0	183
100.0.0.25	200.0.0.13	80	57 Kbps	14 Kbps	104 Kbps	0 ms	4 ms	416 ms	840 ms	135 ms	840 ms	141 MB	0	35

Now we take a look at BitTorrent's Application Performance Report. The sharp increase in performance rate notes the start of the offending application around the same time that Microsoft Office 365 starts degrading.



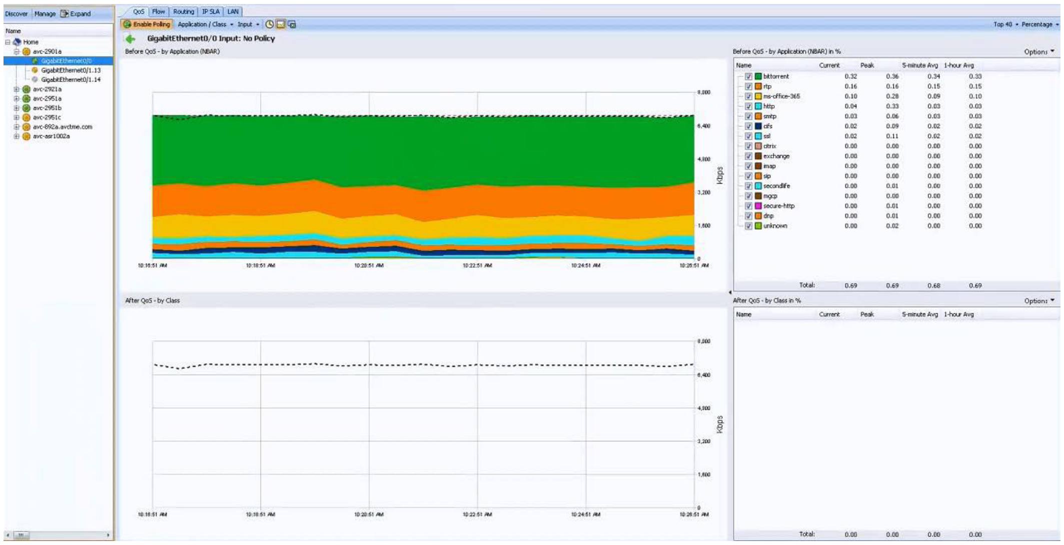
Application Performance: bittorrent

08/24/12, 06:00:00 AM to 08/24/12, 10:24:00 AM

avc-2901a | bittorrent | Est. number of flows: 248,404

Filter: *DefaultFilterGroup

With that information in mind, we move into LiveNX's real-time data provided by the QoS interface view. NBAR2 is currently performing its DPI functionality and is identifying BitTorrent as the top application entering the GigabitEthernet0/0 interface on the router, squelching all other traffic types.



GigabitEthernet0/0 Input: No Policy

Before QoS - by Application (NBAR) in %

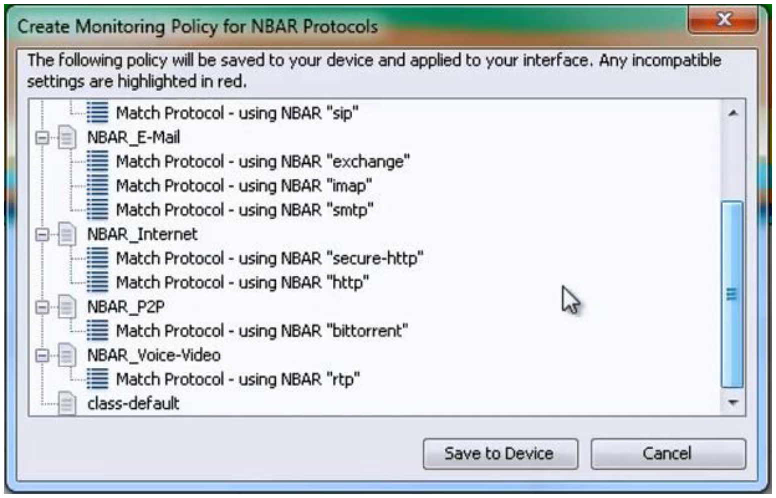
Name	Current	Peak	5-minute Avg	1-hour Avg
☑ 🟩 bittorrent	0.32	0.36	0.34	0.33
☑ 🟧 rtp	0.16	0.16	0.15	0.15
☑ 🟨 ms-office-365	0.10	0.28	0.09	0.10
☑ 🟦 http	0.04	0.33	0.03	0.03
☑ 🟧 smtp	0.03	0.06	0.03	0.03
☑ 🟦 cifs	0.02	0.09	0.02	0.02
☑ 🟦 ssl	0.02	0.11	0.02	0.02
☑ 🟫 citrix	0.00	0.00	0.00	0.00
☑ 🟫 exchange	0.00	0.00	0.00	0.00
☑ 🟫 imap	0.00	0.00	0.00	0.00
☑ 🟧 sip	0.00	0.00	0.00	0.00
☑ 🟦 secondlife	0.00	0.01	0.00	0.00
☑ 🟫 mgcp	0.00	0.00	0.00	0.00
☑ 🟪 secure-http	0.00	0.01	0.00	0.00
☑ 🟧 dnp	0.00	0.01	0.00	0.00
☑ 🟩 unknown	0.00	0.02	0.00	0.00
Total:	0.69	0.69	0.68	0.69

After QoS - by Class in %

Name	Current	Peak	5-minute Avg	1-hour Avg
Total:	0.00	0.00	0.00	0.00

In order to reduce the effects of BitTorrent on the network, a policing policy will be applied on GigabitEthernet0/0 – which also happens to be the interface closest to the source of the traffic. The simplest way to accomplish this is to create a monitoring policy based on the already known NBAR2 protocols.

1. Right-click on the graph which contains the protocols to monitor.
2. Select **Create monitoring policy for NBAR protocols**.
3. Save the configuration into the device.



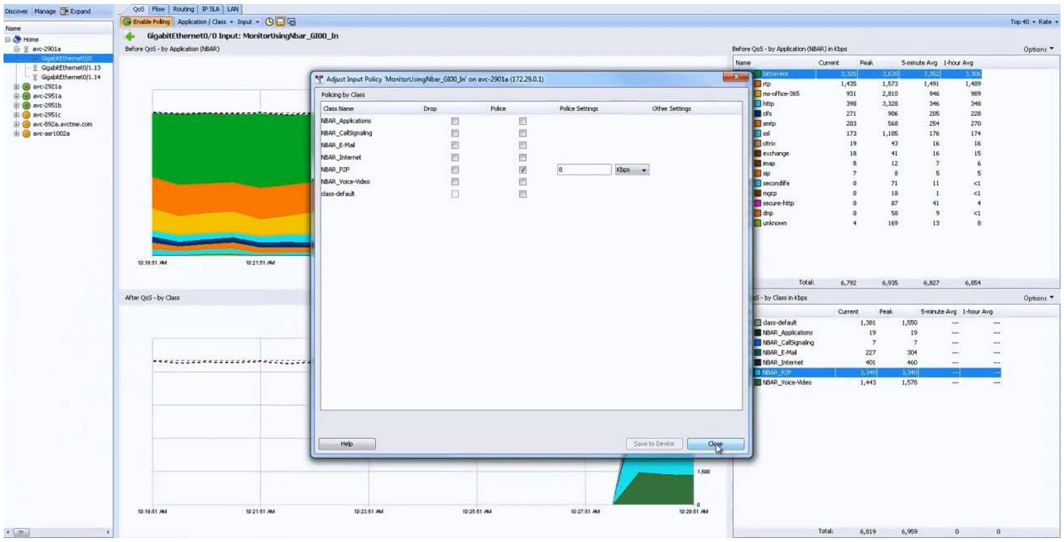
Create Monitoring Policy for NBAR Protocols

The following policy will be saved to your device and applied to your interface. Any incompatible settings are highlighted in red.

- Match Protocol - using NBAR "sip"
- NBAR_E-Mail
  - Match Protocol - using NBAR "exchange"
  - Match Protocol - using NBAR "imap"
  - Match Protocol - using NBAR "smtp"
- NBAR_Internet
  - Match Protocol - using NBAR "secure-http"
  - Match Protocol - using NBAR "http"
- NBAR_P2P
  - Match Protocol - using NBAR "bittorrent"
- NBAR_Voice-Video
  - Match Protocol - using NBAR "rtp"
- class-default

LiveNX will automatically create the policy and apply it on the interface. (Note: this policy can also be fine-tuned to meet the network engineer's needs.) Soon, the After QoS – by Class graph will become populated by a class-based view on the matched traffic types. While it is labeled as "MonitorUsingNbar_GI00_In", we can quickly apply a policing action on the class-map by right-clicking the QoS class and selecting Adjust Input QoS.

The following window will prompt us with the ability to Police a particular class and set a specified policing value. Keep in mind that 8Kbps is the lowest value possible for policing. While we could select Drop, BitTorrent is notorious for adapting to evade classification, when completely dropped. Policing on the other hand will greatly reduce the performance of BitTorrent, while preventing it from invoking its evasion algorithm.



GigabitEthernet0/0 Input: MonitorUsingNbar_GI00_In

Adjust Input Policy 'MonitorUsingNbar_GI00_In' on avc-2901a (172.29.0.1)

Policing by Class

Class Name	Drop	Police	Police Settings	Other Settings
NBAR_Applications	□	□		
NBAR_CallSignaling	□	□		
NBAR_E-Mail	□	□		
NBAR_Internet	□	□		
NBAR_P2P	□	☑	8 Kbps	
NBAR_Voice-Video	□	□		
class-default	□	□		

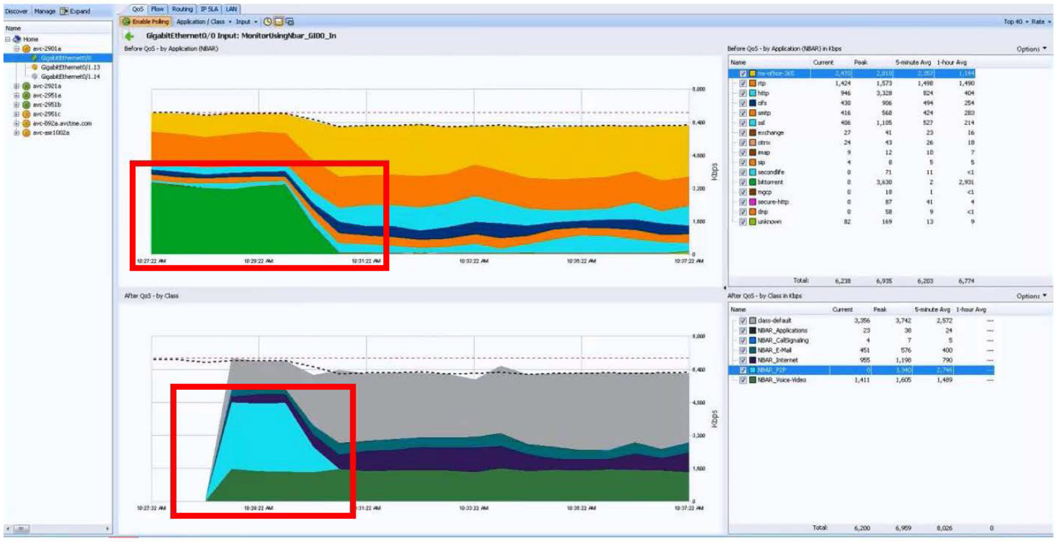
Before QoS - by Application (NBAR) in Kbps

Name	Current	Peak	5-minute Avg	1-hour Avg
bittorrent	3,326	3,630	3,352	3,306
rtp	1,435	1,573	1,491	1,489
ms-office-365	931	2,810	946	989
http	398	3,328	346	348
cifs	271	906	205	228
smtp	203	568	254	270
ssl	173	1,105	176	174
citrix	19	43	16	16
exchange	18	41	16	15
imap	8	12	7	6
sip	7	8	5	5
secondlife	0	71	11	<1
mgcp	0	18	1	<1
secure-http	0	87	41	4
dnp	0	58	9	<1
unknown	4	169	13	8
Total:	6,792	6,935	6,827	6,854

oS - by Class in Kbps

	Current	Peak	5-minute Avg	1-hour Avg
class-default	1,381	1,550	---	---
NBAR_Applications	19	19	---	---
NBAR_CallSignaling	7	7	---	---
NBAR_E-Mail	227	304	---	---
NBAR_Internet	401	460	---	---
NBAR_P2P	3,340	3,340	---	---
NBAR_Voice-Video	1,443	1,578	---	---
Total:	6,819	6,959	0	0

The end result is a greatly reduced traffic count for BitTorrent, as shown by the "Before QoS – by Application (NBAR)" and "After QoS – by Class" interface graphs.



GigabitEthernet0/0 Input: MonitorUsingNbar_GI00_In

Before QoS - by Application (NBAR)

After QoS - by Class

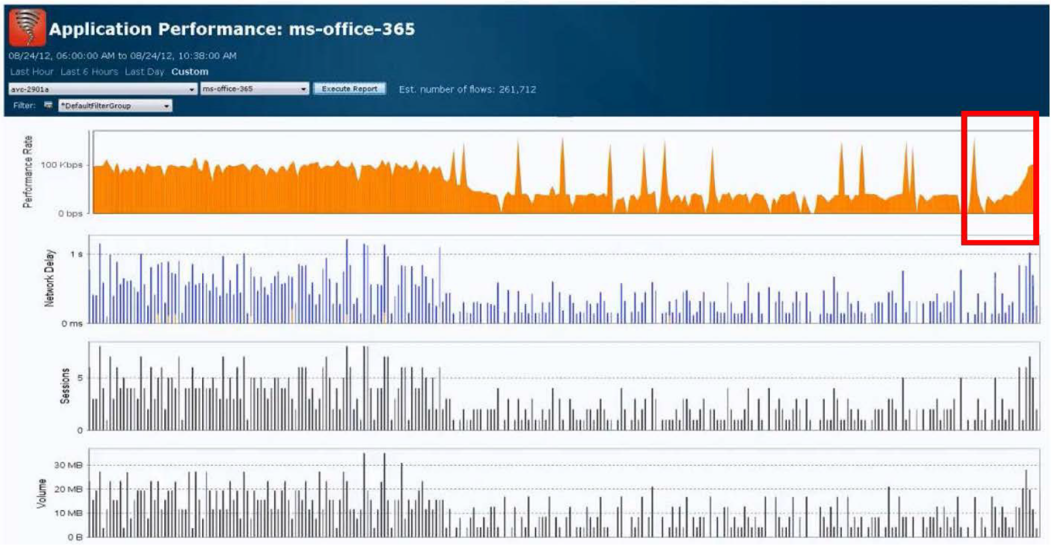
Before QoS - by Application (NBAR) in Kbps

Name	Current	Peak	5-minute Avg	1-hour Avg
☑ ms-office-365	2,470	2,810	2,357	1,144
☑ rtp	1,424	1,573	1,498	1,490
☑ http	946	3,328	824	404
☑ cifs	430	906	494	254
☑ smtp	416	568	424	283
☑ ssl	406	1,105	527	214
☑ exchange	27	41	23	16
☑ citrix	24	43	26	18
☑ imap	9	12	10	7
☑ sip	4	8	5	5
☑ secondlife	0	71	11	<1
☑ bittorrent	0	3,630	2	2,931
☑ mgcp	0	18	1	<1
☑ secure-http	0	87	41	4
☑ dnp	0	58	9	<1
☑ unknown	82	169	13	9
Total:	6,238	6,935	6,203	6,774

After QoS - by Class in Kbps

Name	Current	Peak	5-minute Avg	1-hour Avg
☑ class-default	3,356	3,742	2,572	---
☑ NBAR_Applications	23	38	24	---
☑ NBAR_CallSignaling	4	7	5	---
☑ NBAR_E-Mail	451	576	400	---
☑ NBAR_Internet	955	1,198	790	---
☑ NBAR_P2P	0	3,340	2,746	---
☑ NBAR_Voice-Video	1,411	1,605	1,489	---
Total:	6,200	6,959	8,026	0

We can also verify the AVC performance values through the previously gleaned reports, which display a rise in Microsoft Office 365's overall performance rate.



Application Performance: ms-office-365

08/24/12, 06:00:00 AM to 08/24/12, 10:38:00 AM

avc-2901a | ms-office-365 | Est. number of flows: 261,712

Filter: *DefaultFilterGroup

With this use-case scenario we can see how network administrators and engineers can utilize LiveNX and Cisco's AVC functionality to completely understand application traffic on the network and also take the appropriate steps to optimize business critical applications.