Application Visibility and Control Deployment Guide for Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Amsterdam 17.1

First Published: March 12, 2020

Cisco Systems, Inc. www.cisco.com

Table of Contents

Application Visibility and Control

Application Visibility and Control (AVC) is the Cisco leading approach for deep-packet inspection (DPI) technology in wireless and wired products. AVC empowers users to a whole new level of traffic recognition and shaping through the Network Based Application Recognition engine (NBAR) and Quality of Service (QOS) mechanisms. The AVC feature supports Wireless products using a distributed approach that benefits from NBAR running on the Access Points (AP) or Controller whose goal is to run DPI and reports the results via Flexible Netflow (FNF) messages. The controller aggregates all reports and consumes them with show commands, WebUI or further Netflow export messages to external Netflow collectors such as Prime. Once the Application Visibility is established, the user can define Control rules with policing mechanisms at a client level.

AVC is a subset of the entire FNF package that can provide traffic information even when the deep packet inspection is disabled. FNF is a feature supported in wireless that relies on the Netflow enablement on the controller for all modes: centralized and flex.

Network Based Application Recognition (NBAR) provides application-aware control on a wireless network and enhances manageability and productivity. It also extends Cisco's Application Visibility and Control (AVC) as an end-to-end solution, which gives a complete visibility of applications in the network and allows the administrator to take some action on the same.

NBAR is a deep-packet inspection technology available on Cisco IOS based platforms, which supports stateful L4 - L7 classification. NBAR2 is based on NBAR and has extra requirements such as having a Common Flow Table for all IOS features which use NBAR. NBAR2 recognizes application and passes on this information to other features like QoS, NetFlow and Firewall, which can take action based on this classification.

The key use cases for NBAR are capacity planning, network usage base lining and better understanding of what applications are consuming bandwidth. Trending of application usage helps network admin to plan for network infrastructure upgrade, improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic.

NBAR Supported Feature

NBAR as a feature can perform the following tasks:

1. Classification–Identification of Application/Protocol.

2. AVC–Provides visibility of classified traffic and also gives an option to control the same using Drop or Mark (DSCP) action.

3. Flexible NetFlow–Updating NBAR stats to NetFlow collector like Cisco Prime Assurance Manager (PAM).

Complete list of the protocols supported in the release posted at the link below

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

AVC-FNF Feature Summary on IOS XE 17.1

- NBAR on controller: NBAR engine **v38**, protocol pack **v45**

- L2 & L3 roaming supported, L2 includes AP NBAR context transfer

- Application-based statistics reporting per WLAN and per client

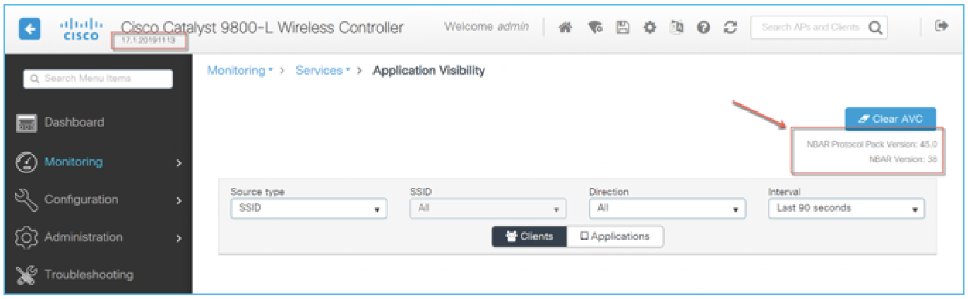
- External FNF collectors

- AVC Timeline

- Support for Wave-1 and Wave-2 APs. Fabric, Wave-2 only.
- WebUI, CLI, Netconf/Yang and SNMP support
- IPv4 and IPv6 traffic classification, FNF support for IPv6 traffic flows on Wave-2 APs only
- Support for all Cisco C9800 deployment modes

	C9800	W1 AP’s	W2 AP’s	WiFi 6 AP’s
Local mode (Central switching)	Ipv4 Traffic: AVC Supported FNF Supported Ipv6 Traffic : AVC Supported FNF Supported	Not applicable	Not applicable	Not applicable
Flex mode (Central switching)	Ipv4 Traffic: AVC Supported FNF Supported Ipv6 Traffic: AVC Supported FNF Supported	Not applicable	Not applicable	

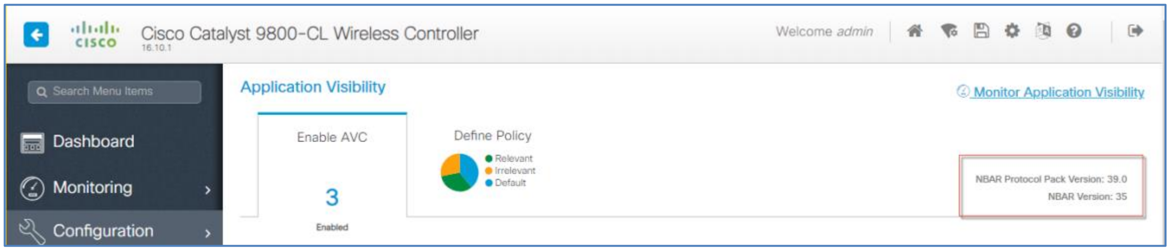
Flex mode (Local switching)	N/A	Ipv4 Traffic: AVC Supported FNF Supported Ipv6 Traffic: AVC Supported FNF Not supported	Ipv4 Traffic: AVC Supported FNF Supported Ipv6 Traffic: AVC Supported FNF supported	Ipv4 Traffic: AVC Supported FNF Supported Ipv6 Traffic: AVC Supported FNF supported
Local mode (Fabric Mode)		Ipv4 Traffic: AVC Not Supported FNF Not Supported Ipv6 Traffic: AVC Not Supported FNF Not Supported	Ipv4 Traffic: AVC Supported FNF Supported Ipv6 Traffic: AVC Supported FNF Supported	Ipv4 Traffic: AVC Supported FNF Supported Ipv6 Traffic: AVC Supported FNF Supported


Cisco Catalyst 9800-L Wireless Controller
17.1.20191113

Monitoring > Services > Application Visibility

NBAR Protocol Pack Version: 45.0
NBAR Version: 38

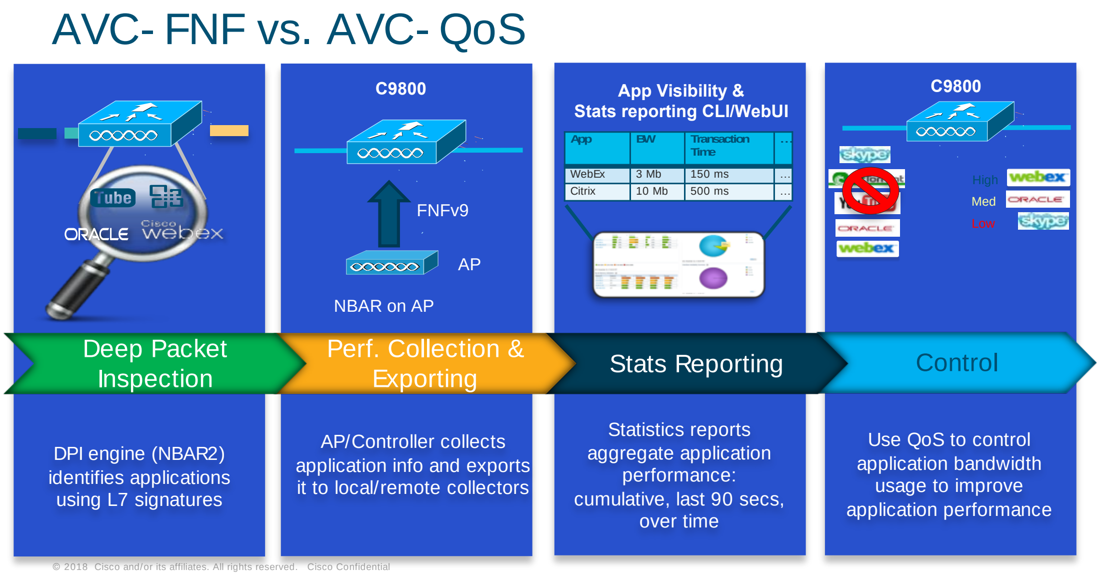
Source type: SSID
SSID: All
Direction: All
Interval: Last 90 seconds


Cisco Catalyst 9800-CL Wireless Controller
16.10.1

Application Visibility

Enable AVC: 3 Enabled

NBAR Protocol Pack Version: 39.0
NBAR Version: 35



AVC- FNF vs. AVC- QoS

App Visibility & Stats reporting CLI/WebUI

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

Deep Packet Inspection → Perf. Collection & Exporting → Stats Reporting → Control

DPI engine (NBAR2) identifies applications using L7 signatures

AP/Controller collects application info and exports it to local/remote collectors

Statistics reports aggregate application performance: cumulative, last 90 secs, over time

Use QoS to control application bandwidth usage to improve application performance

C9800 AVC-FNF Deployment Modes

C9800 IOS-XE 17.1 Supports 4 deployment modes

- Flex (a.k.a. “Local switching with APs in FlexConnect mode”
- Flex Central (a.k.a. “Central switching with APs in FlexConnect mode”)
- Local (a.k.a. “Central switching with APs in local mode”)
- Fabric (a.k.a. eCA DNA)

Flexible NetFlow Support

An IP traffic flow is a sequence of packets passing through a network device with common attributes like source and destination IP address & transport ports, direction, etc. Additional common attributes for wireless flow are SSID, AP MAC. These packets with common attributes are aggregated into flows and exported to the NetFlow Collectors. Prior to IOS-XE release 17.1, controller exported NetFlow data was not supported.

Starting with Cisco IOS XE 17.1.1, IPv6 flow monitor is supported on Wave 2 APs. Two flow monitors can be attached in a policy profile per direction (input and output) and per IP version (IPv4 and IPv6) in local (central switching) mode, whe NBAR runs on the controller. However, only one flow monitor is supported per direction (input and output) and per IP version (IPv4 and IPv6) in FlexConnect and Fabric modes on Wave 2 APs, when NBAR runs on the corresponding AP.

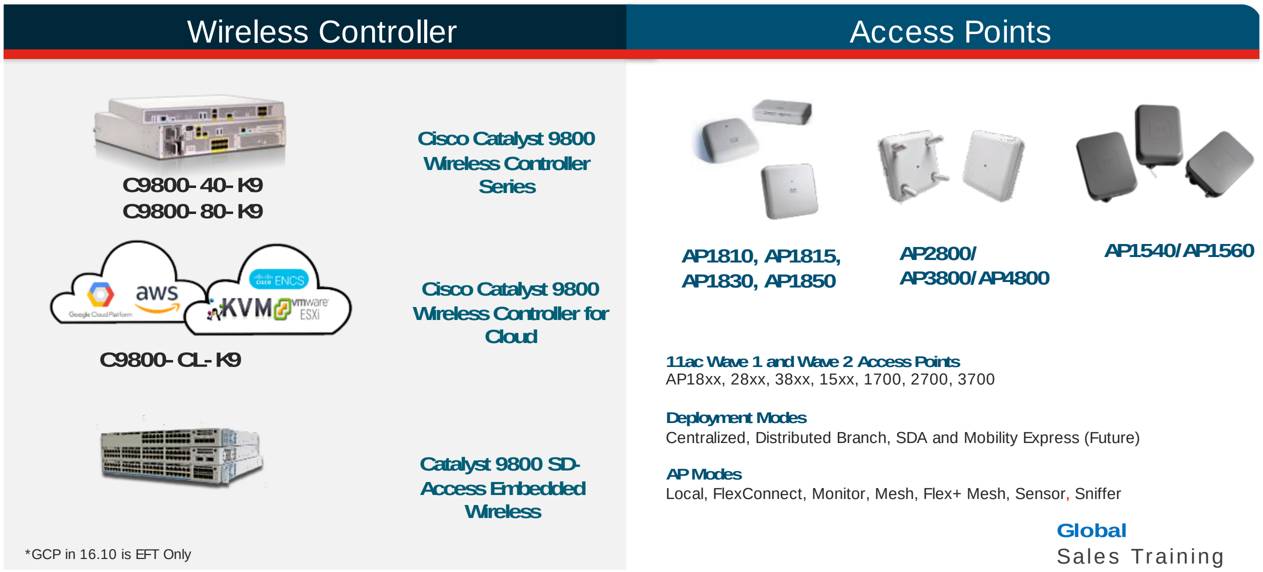
IPv4 and IPv6 Flexible Netflow records exporter is introduced in rel 17.1. FNF is sending 17 different data records (as defined in RFC 3954) to the External 3rd Party Netflow collector such as Stealthwatch and others. Support for the Enhanced Flow Record Data Export was added on the C9800.

- Application Tag
- Client Mac Address

- AP Mac address
- WlanID
- Source IP
- Dest IP
- Source Port
- Dest Port
- Protocol
- Flow Start Time
- Flow End Time
- Direction
- Packet count
- Byte count
- VLAN ID (Local mode) – Mgmt/Client
- TOS - DSCP Value

C9800 IPv4 and IPv6 AVC-FNF Supported Platforms

- C9800
- Flex and Local modes: C9800 APs
- Flex mode supports Wave-1 APs and WiFi 6 APs
- Flex and Fabric modes support Wave-2 and WiFi6 APs Only
- AP_1810W, AP_1810T, AP_1815W, AP_1815T, AP_1815I, AP_1815M, AP_1815TSN, AP_1815STAR, AP_1832I, AP_1852E, AP_1852I, AP_2802E, AP_2802I, AP_2802H, AP_3802E, AP_3802P, AP_3802H, AP_4800 and C9100 APs.
- Local, Fabric and Flex Central modes support all C9800 IOS-XE rel 17.1supported APs



Wireless Controller

C9800-40-K9
C9800-80-K9

Cisco Catalyst 9800 Wireless Controller Series

C9800-CL-K9

Cisco Catalyst 9800 Wireless Controller for Cloud

Catalyst 9800 SD-Access Embedded Wireless

*GCP in 16.10 is EFT Only

Access Points

AP1810, AP1815, AP1830, AP1850

AP2800/ AP3800/AP4800

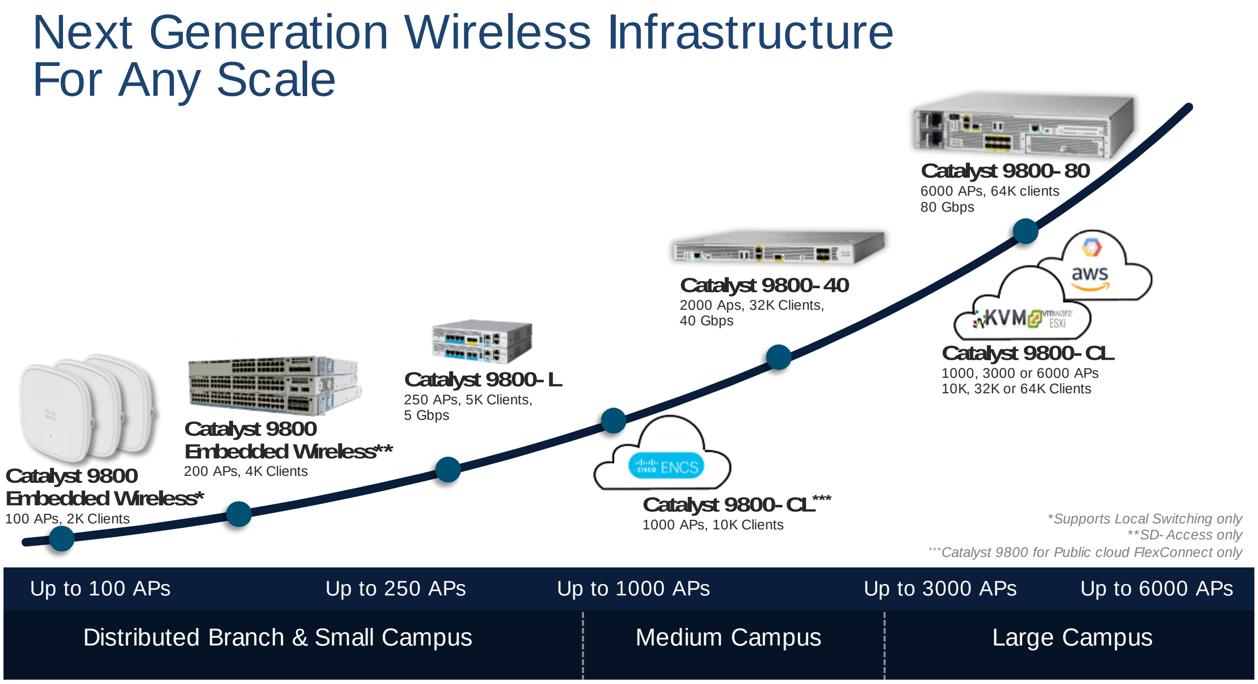
AP1540/AP1560

11ac Wave 1 and Wave 2 Access Points
AP18xx, 28xx, 38xx, 15xx, 1700, 2700, 3700

Deployment Modes
Centralized, Distributed Branch, SDA and Mobility Express (Future)

AP Modes
Local, FlexConnect, Monitor, Mesh, Flex+ Mesh, Sensor, Sniffer

Global
Sales Training



Next Generation Wireless Infrastructure For Any Scale

Catalyst 9800 Embedded Wireless*
100 APs, 2K Clients

Catalyst 9800 Embedded Wireless**
200 APs, 4K Clients

Catalyst 9800-L
250 APs, 5K Clients,
5 Gbps

Catalyst 9800-CL***
1000 APs, 10K Clients

Catalyst 9800-40
2000 Aps, 32K Clients,
40 Gbps

Catalyst 9800-CL
1000, 3000 or 6000 APs
10K, 32K or 64K Clients

Catalyst 9800-80
6000 APs, 64K clients
80 Gbps

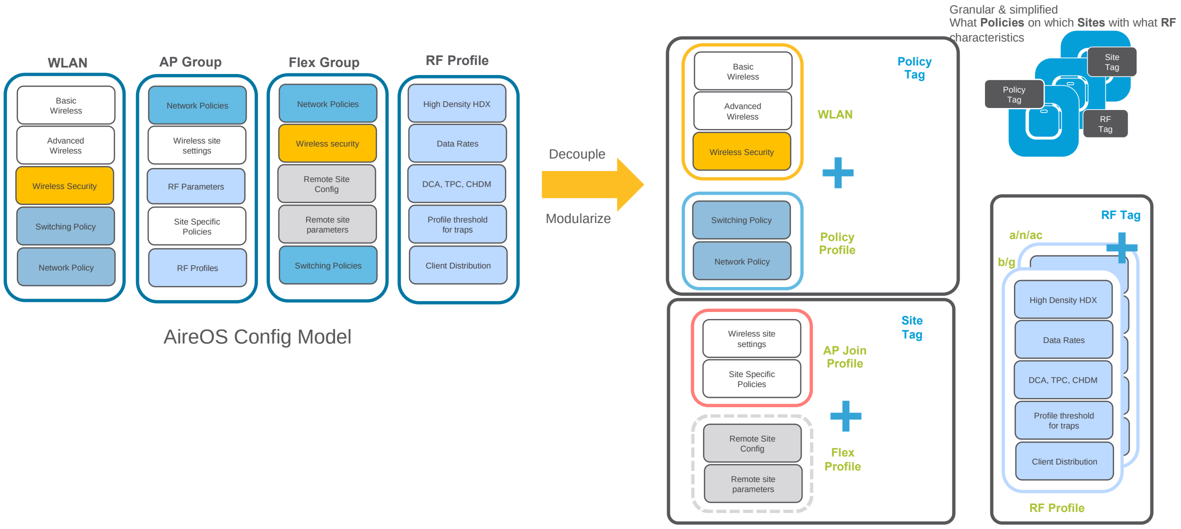
*Supports Local Switching only
**SD-Access only
***Catalyst 9800 for Public cloud FlexConnect only

Up to 100 APs | Up to 250 APs | Up to 1000 APs | Up to 3000 APs | Up to 6000 APs

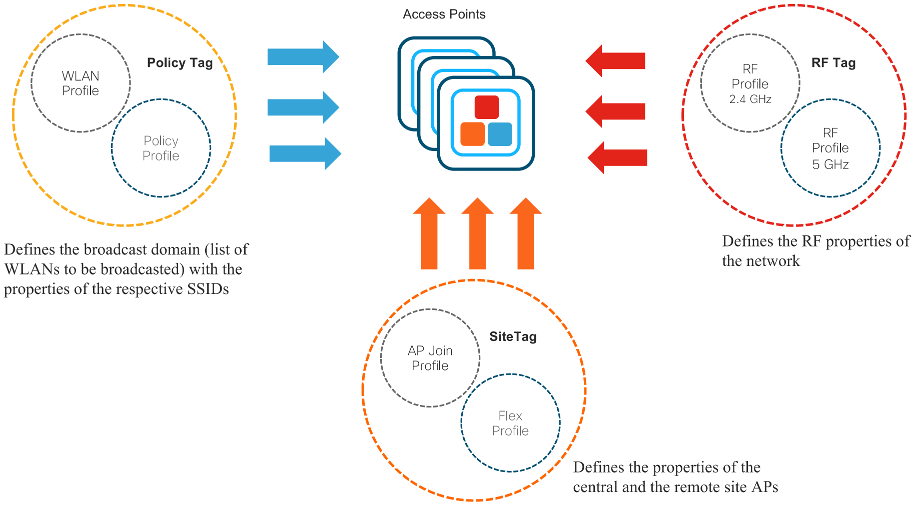
Distributed Branch & Small Campus | Medium Campus | Large Campus

AireOS vs. C9800 Config Model

Going towards a more **Modularized and Reusable** model with **Logical decoupling** of configuration entities



Cisco 9800 Catalyst Wireless Config Model



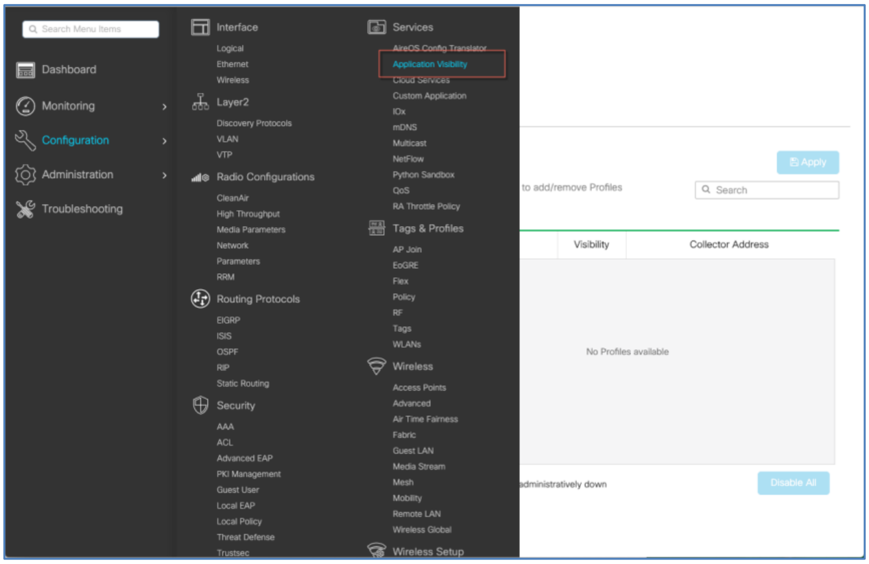
Defines the broadcast domain (list of WLANs to be broadcasted) with the properties of the respective SSIDs

Defines the RF properties of the network

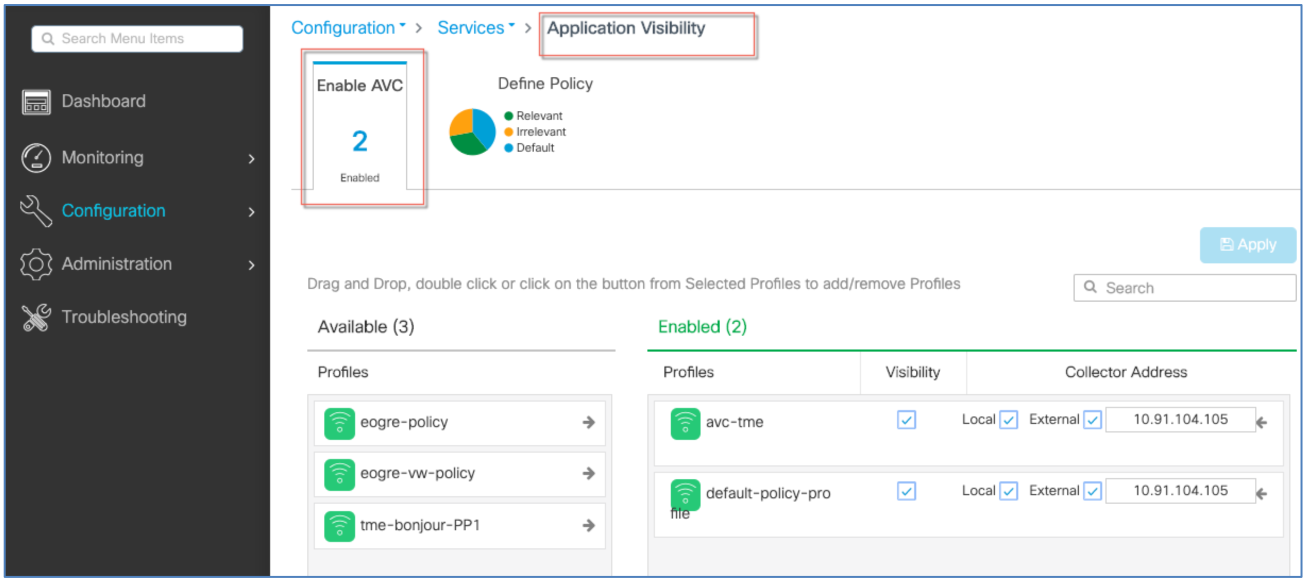
Defines the properties of the central and the remote site APs

C9800 AVC WLAN Configuration

Step 1: Login to C9800 and from the controller main menu go to Configuration > Services> Application Visibility



Select Configured WLANs and apply AV on them as shown in the example below, you may also select here local or external Netflow Collector



Drag and Drop, double click or click on the button from Selected Profiles to add/remove Profiles

Available (3)

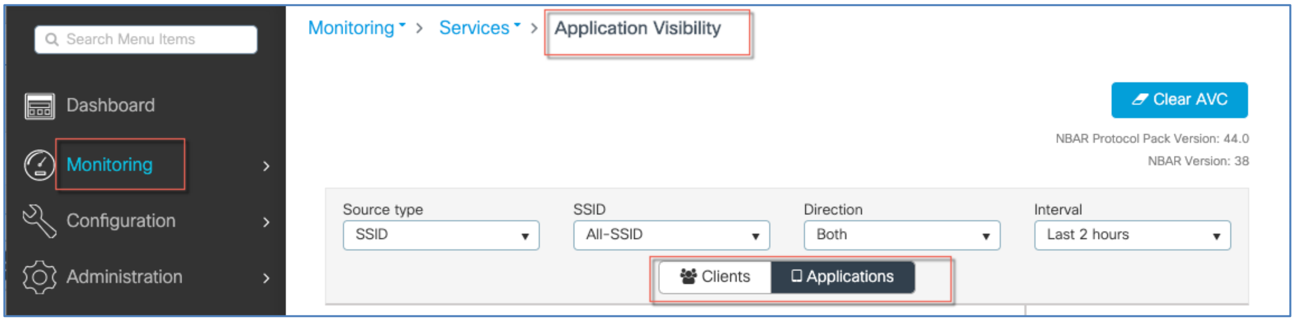
Profiles
eogre-policy
eogre-vw-policy
tme-bonjour-PP1

Enabled (2)

Profiles	Visibility	Collector Address
avc-tme	☑	Local ☑ External ☑ 10.91.104.105
default-policy-profile	☑	Local ☑ External ☑ 10.91.104.105

Step 2: Connect a client(s) to the one of the AVC enabled WLANs and pass traffic by browsing to different sites

then wait for few seconds and then go to C9800 main menu **Monitor > Application Visibility**

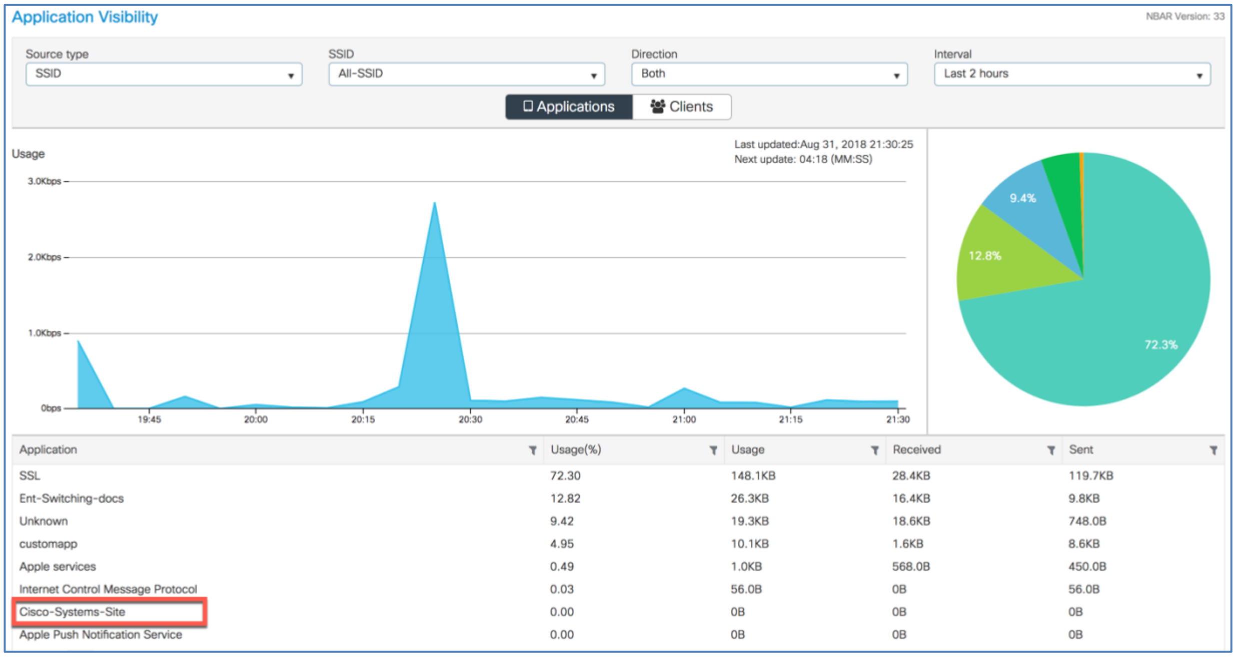


NBAR Protocol Pack Version: 44.0
NBAR Version: 38

Source type	SSID	Direction	Interval
SSID	All-SSID	Both	Last 2 hours

The page will show a graphical view of the all apps running on the network and monitored by the NBAR.

User can filter it through per SSID, direction and time interval (up to 48 hrs). User can see the apps which clients try to access.



Application Visibility

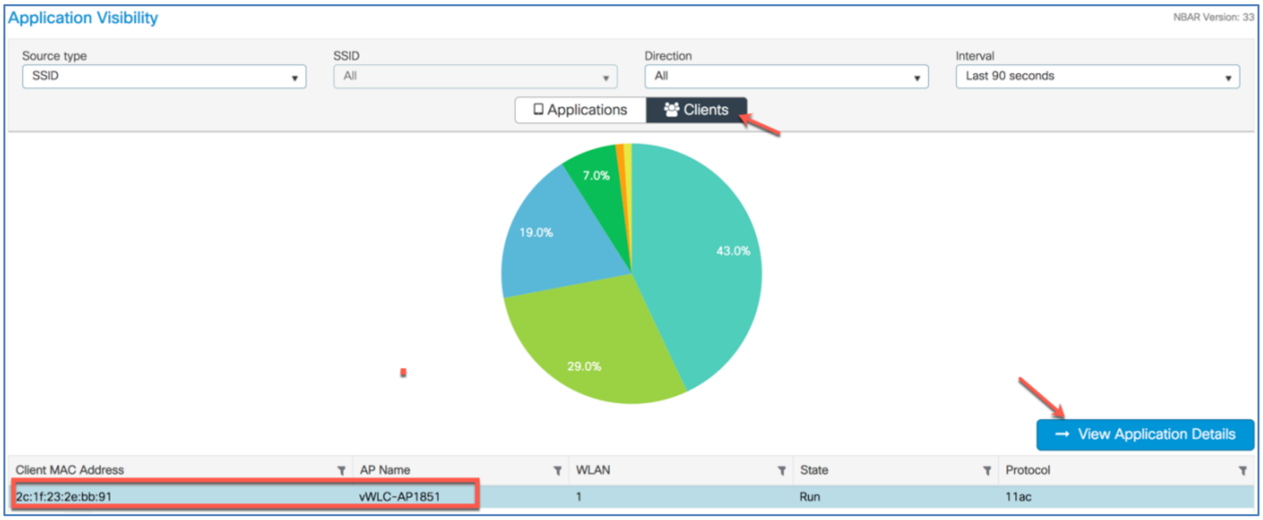
NBAR Version: 33

Source type: SSID
SSID: All-SSID
Direction: Both
Interval: Last 2 hours

Last updated:Aug 31, 2018 21:30:25
Next update: 04:18 (MM:SS)

Application	Usage(%)	Usage	Received	Sent
SSL	72.30	148.1KB	28.4KB	119.7KB
Ent-Switching-docs	12.82	26.3KB	16.4KB	9.8KB
Unknown	9.42	19.3KB	18.6KB	748.0B
customapp	4.95	10.1KB	1.6KB	8.6KB
Apple services	0.49	1.0KB	568.0B	450.0B
Internet Control Message Protocol	0.03	56.0B	0B	56.0B
Cisco-Systems-Site	0.00	0B	0B	0B
Apple Push Notification Service	0.00	0B	0B	0B

Similarly, per client AV stats can be seen - click on the Clients tab and select the client and click on **View Application Details** button



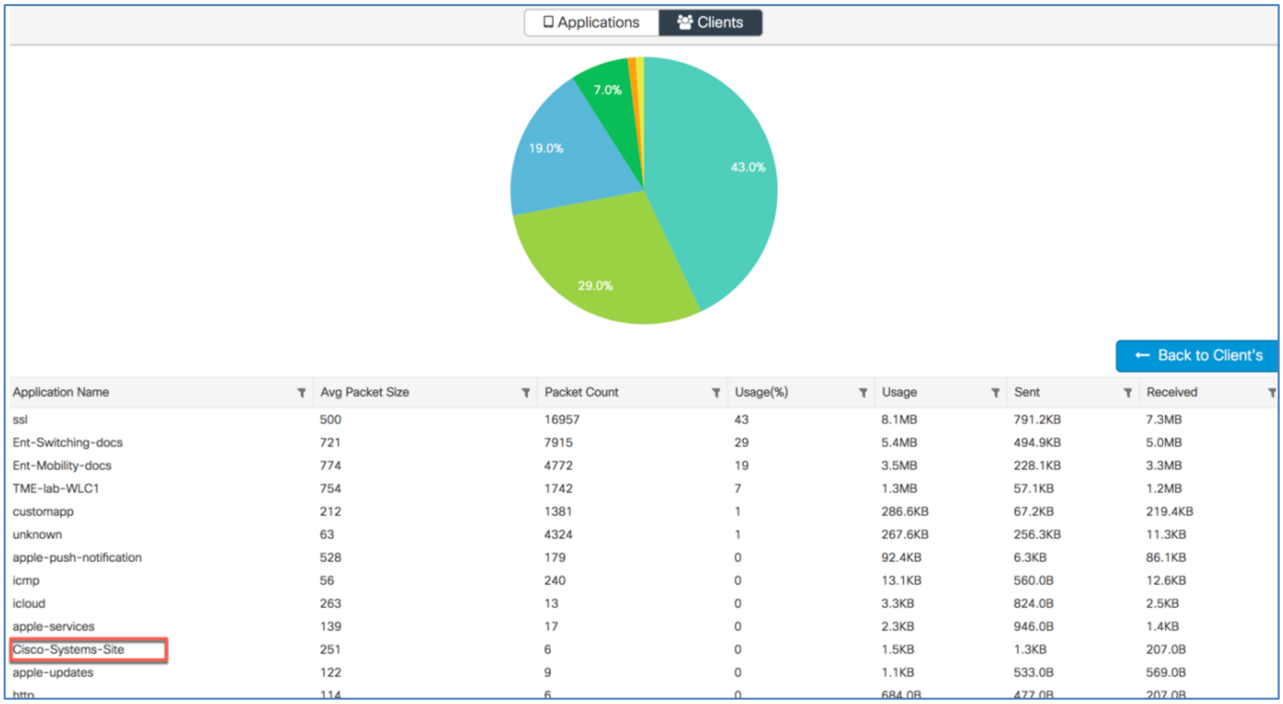
Application Visibility

NBAR Version: 33

Source type: SSID
SSID: All
Direction: All
Interval: Last 90 seconds

Client MAC Address	AP Name	WLAN	State	Protocol
2c:1f:23:2e:bb:91	vWLC-AP1851	1	Run	11ac

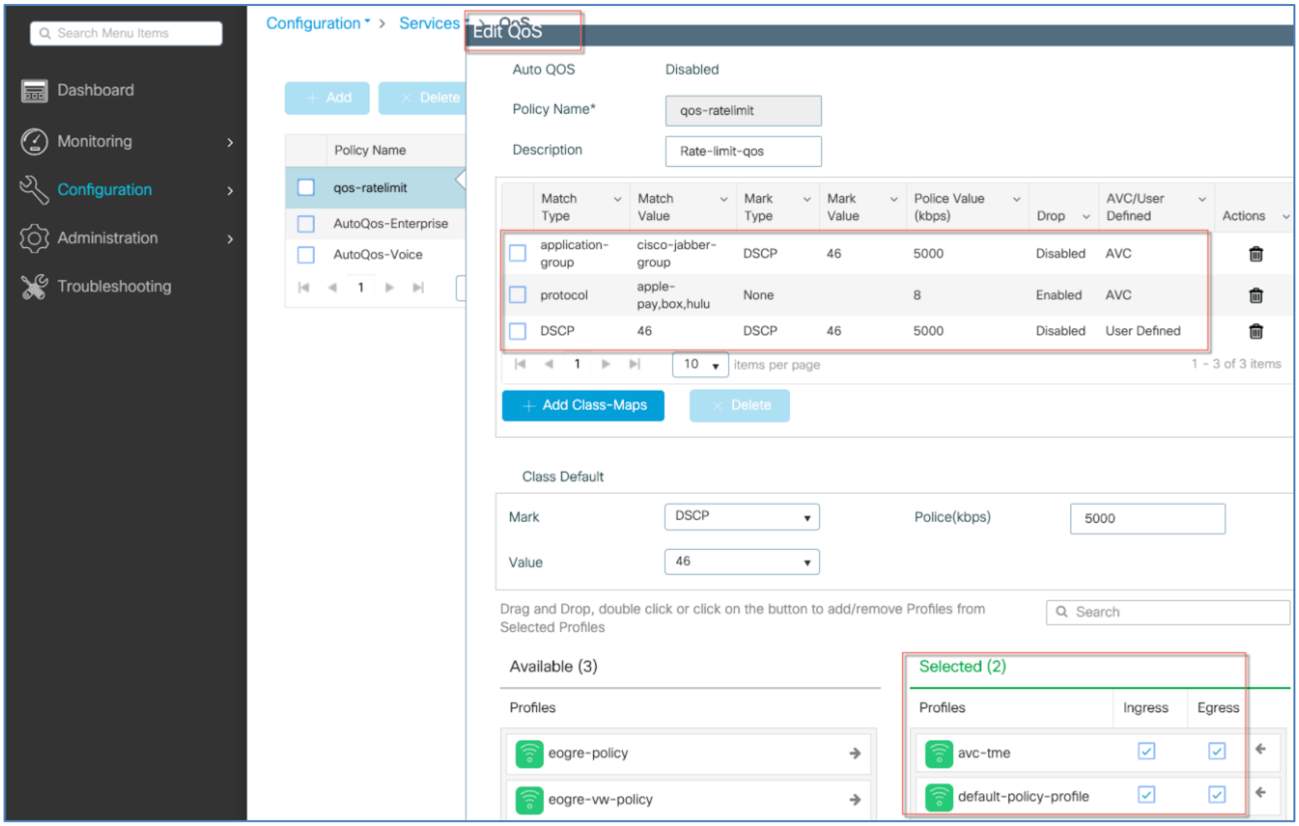
This will show all the apps usage in % graph and in tabular format which that client tried to access



Application Name	Avg Packet Size	Packet Count	Usage(%)	Usage	Sent	Received
ssl	500	16957	43	8.1MB	791.2KB	7.3MB
Ent-Switching-docs	721	7915	29	5.4MB	494.9KB	5.0MB
Ent-Mobility-docs	774	4772	19	3.5MB	228.1KB	3.3MB
TME-lab-WLC1	754	1742	7	1.3MB	57.1KB	1.2MB
customapp	212	1381	1	286.6KB	67.2KB	219.4KB
unknown	63	4324	1	267.6KB	256.3KB	11.3KB
apple-push-notification	528	179	0	92.4KB	6.3KB	86.1KB
icmp	56	240	0	13.1KB	560.0B	12.6KB
icloud	263	13	0	3.3KB	824.0B	2.5KB
apple-services	139	17	0	2.3KB	946.0B	1.4KB
Cisco-Systems-Site	251	6	0	1.5KB	1.3KB	207.0B
apple-updates	122	9	0	1.1KB	533.0B	569.0B
http	114	6	0	684.0B	477.0B	207.0B

Step 3**:** To control the applications (Mark, Drop or Rate limit) or the traffic - configure AVC with a QoS policy to Mark/Drop or Rate Limit an application. the YouTube application.

Go to **Configuration>Services>QoS and** Click on Add button and it will take you to QoS policy page



Auto QOS: Disabled

Policy Name*: qos-ratelimit

Description: Rate-limit-qos

	Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
□	application-group	cisco-jabber-group	DSCP	46	5000	Disabled	AVC	🗑
□	protocol	apple-pay,box,hulu	None		8	Enabled	AVC	🗑
□	DSCP	46	DSCP	46	5000	Disabled	User Defined	🗑

1 — 10 items per page — 1 - 3 of 3 items

Class Default

Mark: DSCP

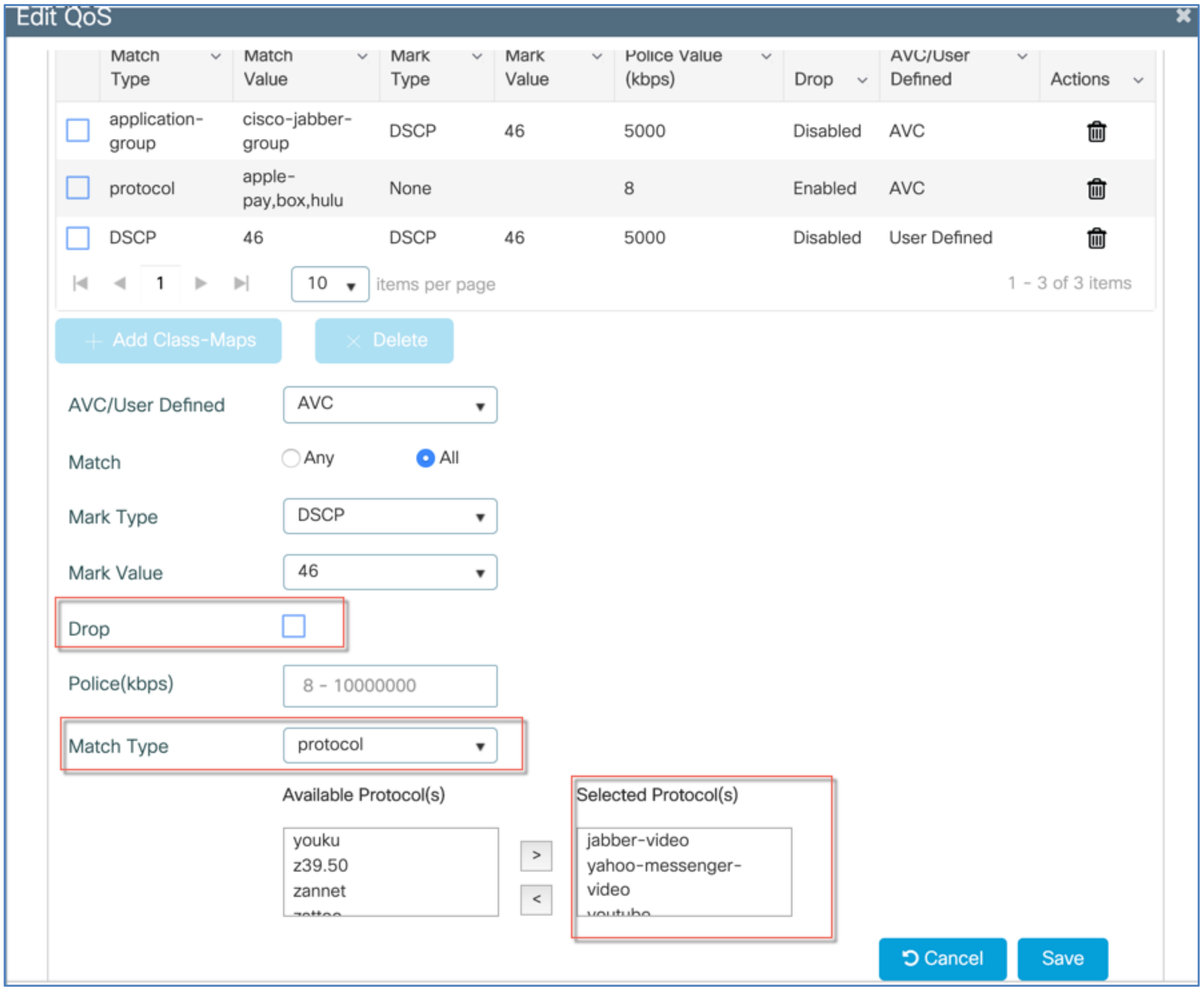
Police(kbps): 5000

Value: 46

Profiles	
eogre-policy	→
eogre-vw-policy	→

Profiles	Ingress	Egress	
avc-tme	☑	☑	←
default-policy-profile	☑	☑	←

In that Auto QoS page select a button **+Add Class_Maps,** and in that next page configure desired AVC options such as Mark DSCP value or Drop a specific Protocol as shown in the example below YouTube and Twitter are configured to be Dropped by the AVC policy



Edit QoS

	Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
□	application-group	cisco-jabber-group	DSCP	46	5000	Disabled	AVC	🗑
□	protocol	apple-pay,box,hulu	None		8	Enabled	AVC	🗑
□	DSCP	46	DSCP	46	5000	Disabled	User Defined	🗑

1 | 10 items per page | 1 - 3 of 3 items

AVC/User Defined: AVC

Match: ○ Any ● All

Mark Type: DSCP

Mark Value: 46

Drop: □

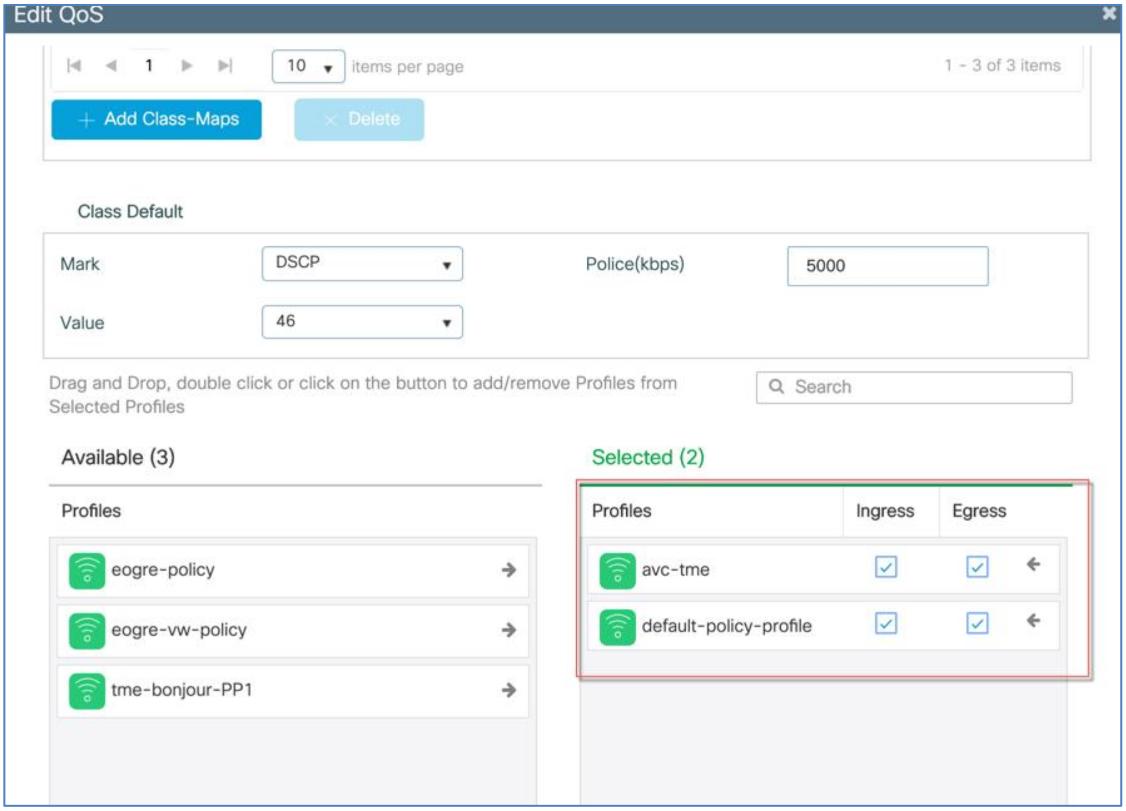
Police(kbps): 8 - 10000000

Match Type: protocol

Available Protocol(s): youku, z39.50, zannet, zattoo

Selected Protocol(s): jabber-video, yahoo-messenger-video, youtube

Next, select the WLAN profiles on which you want to apply this QoS policy. In the example below, we select two WLAN profiles we configured in the previous steps and applied the Ingress.



Edit QoS

Class Default

Mark: DSCP

Police(kbps): 5000

Value: 46

Drag and Drop, double click or click on the button to add/remove Profiles from Selected Profiles

Available (3)

Profiles
eogre-policy
eogre-vw-policy
tme-bonjour-PP1

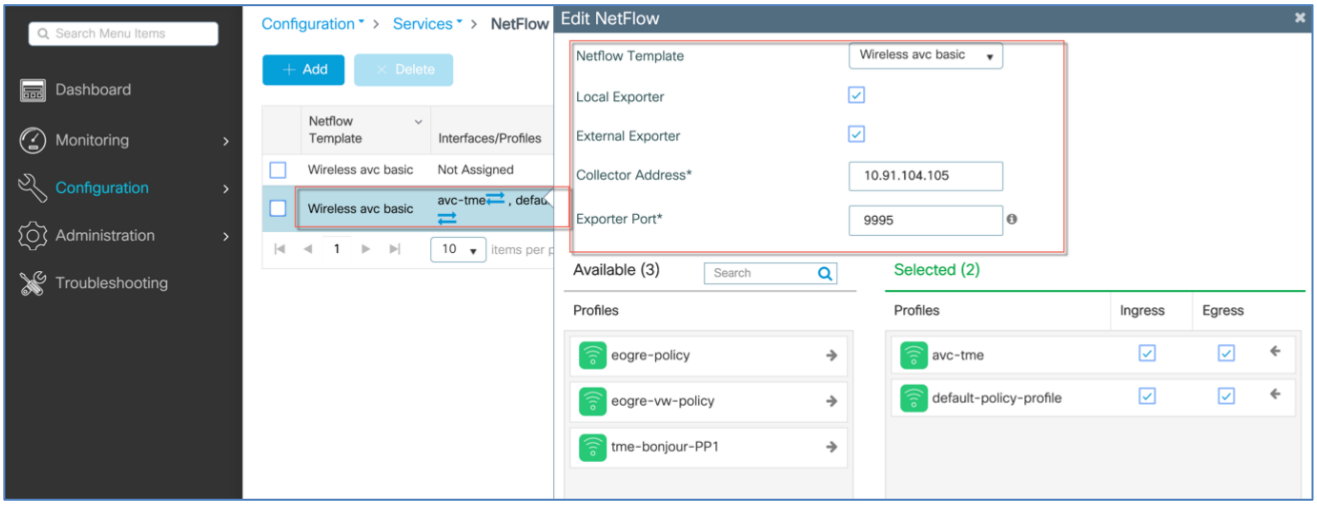
Selected (2)

Profiles	Ingress	Egress
avc-tme	☑	☑
default-policy-profile	☑	☑

Step 4 (Verification): Connect a client to one of the WLAN profiles configured above and try accessing different sites e.g. cisco.com and also try accessing YouTube and Twitter. The client should be able to browse to all sites except YouTube and Twitter, which are marked as dropped in the Configured QoS-policy.

Setting up a NetFlow collector

IOS-XE controllers support Netflow collectors such StealthWatch. Below are sample configurations of the Netflow collectors.



	Netflow Template	Interfaces/Profiles
□	Wireless avc basic	Not Assigned
□	Wireless avc basic	avc-tme, defau

Edit NetFlow

Netflow Template: Wireless avc basic

Local Exporter: ☑

External Exporter: ☑

Collector Address*: 10.91.104.105

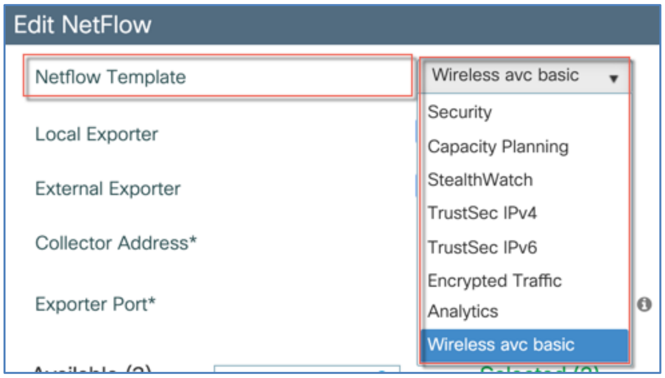
Exporter Port*: 9995

Available (3)

Profiles
eogre-policy
eogre-vw-policy
tme-bonjour-PP1

Selected (2)

Profiles	Ingress	Egress
avc-tme	☑	☑
default-policy-profile	☑	☑



Edit NetFlow

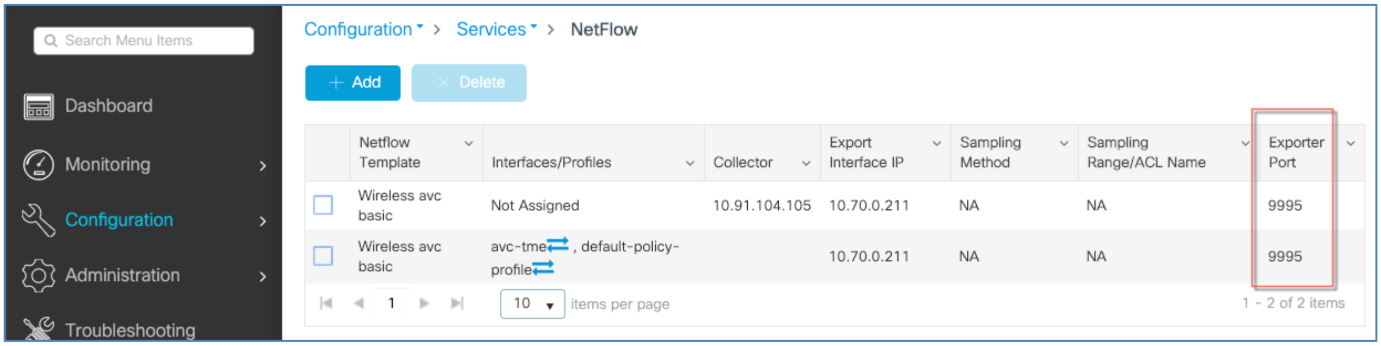
Netflow Template: Wireless avc basic

Local Exporter

External Exporter

Collector Address*

Exporter Port*

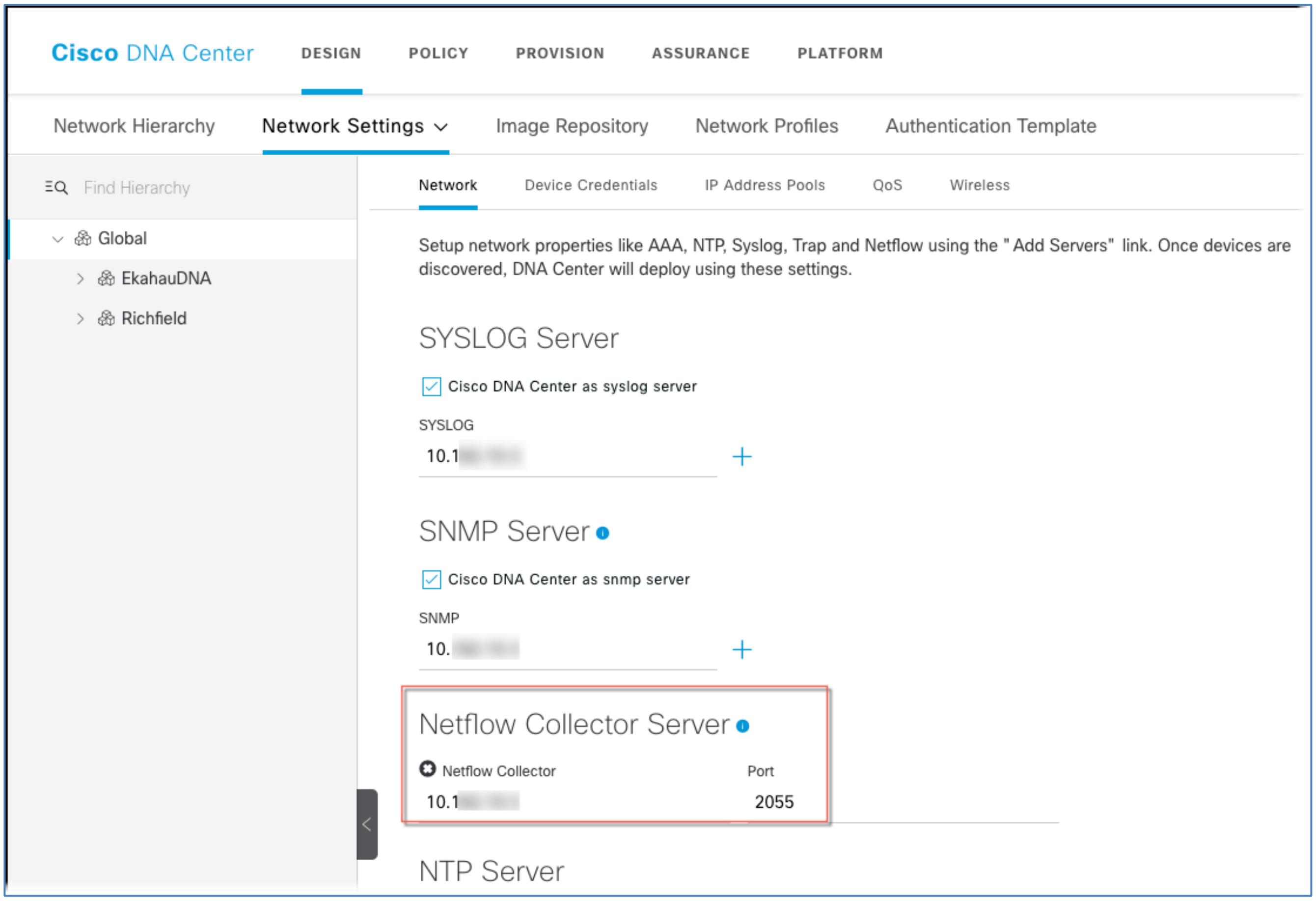


Configuration > Services > NetFlow

	Netflow Template	Interfaces/Profiles	Collector	Export Interface IP	Sampling Method	Sampling Range/ACL Name	Exporter Port
□	Wireless avc basic	Not Assigned	10.91.104.105	10.70.0.211	NA	NA	9995
□	Wireless avc basic	avc-tme⇄ , default-policy-profile⇄		10.70.0.211	NA	NA	9995

1 | 10 items per page | 1 - 2 of 2 items

Netflow collector services can be also setup on the DNA-C server as illustrated below.



Setup network properties like AAA, NTP, Syslog, Trap and Netflow using the " Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings.

SYSLOG Server

☑ Cisco DNA Center as syslog server

SYSLOG: 10.1[redacted]

SNMP Server

☑ Cisco DNA Center as snmp server

SNMP: 10.[redacted]

Netflow Collector Server

Netflow Collector: 10.1[redacted] Port: 2055

NTP Server

NBAR2 Protocol Pack Upgrade

- Allows to update the Protocol Pack (list of recognized protocols by NBAR engine) on the controller **only.** APs are not upgraded as of IOS-XE rel 17.1.
- Upgrade is seamless – no interruption of service is needed
- New protocols/applications show up after upgrade without reboot in AVC CLIs & WebUI
- New custom protocols / applications can be defined by the user

Step 1: Upload the protocol pack to the bootflash (example)

Apply - it takes about 10 sec before new flows can be classified but not interruption of service happens:

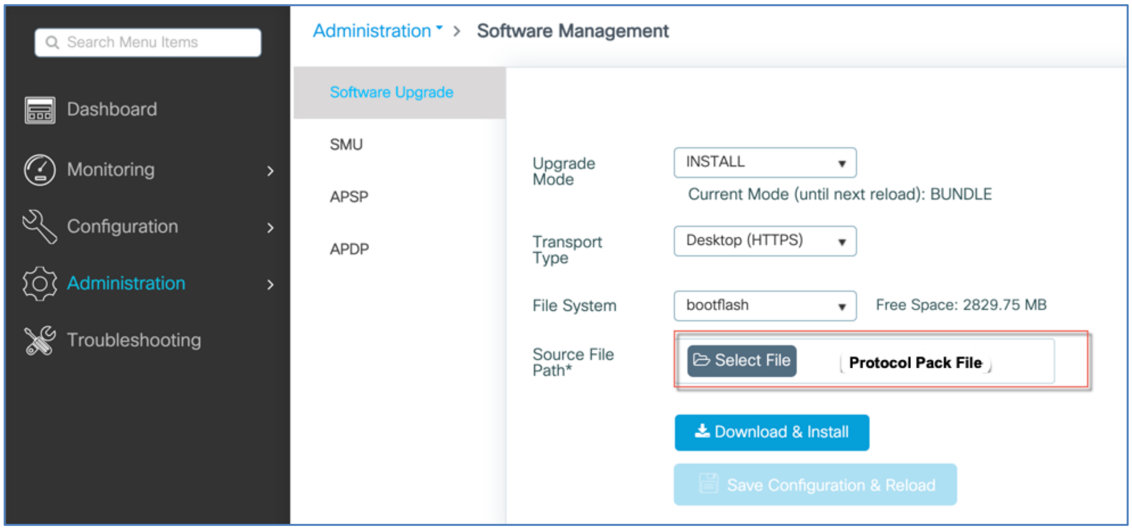
```
C9800#conf t
C9800(config)#ip nbar protocol-pack bootflash:<uploadppack>
```

Check the version:

```
C9800-MA1#show ip nbar protocol-pack active
```

```
Active Protocol Pack:
Name:                           Advanced Protocol Pack
Version:                        44.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:    38
State:                            Active
```

Same can be done from the WebUI interface



Upgrade Mode: INSTALL
Current Mode (until next reload): BUNDLE
Transport Type: Desktop (HTTPS)
File System: bootflash
Free Space: 2829.75 MB
Source File Path*: Protocol Pack File

NBAR Custom Apps Configuration

- After definition, it takes up to 10 seconds for the app to be ready in NBAR engine
- Only new flows will be classified with the newly defined apps

```
#imp nbar custom <app name> <rules>
```

Example to match a URL:

```
C9800(config)#ip nbar custom myappname http url http://internalwiki.cisco.com
```

C9800 -CL AVC CLI Commands

Stats show commands

```
show avc wlan <ssid> top <n> applications (upstream | downstream | aggregate)
show avc client <mac_addr> top <n> applications (upstream | downstream | aggregate)
show avc wlan <ssid> application <app_name> top <n>(upstream | downstream | aggregate)
show avc status wlan <ssid>
show controllers dot 0 wlan
Show ip nbar version
show avc nbar statistics
Show ip nbar protocol-pack active
show ip nbar protocol-discovery wlan <wlan profile name> [filtering options]

clear ip nbar protocol-discovery wlan <wlan profile name>
clear avc (wlan <ssid>| client <mac_addr>) stats
```

Minimal AVC CLI configuration

```
flow exporter fm-exp
  destination local
or Destination <hostname or A.B.C.D>
flow monitor fm-avc
  record wireless avc basic
  exporter fm-exp
  cache timeout active 60
wireless profile policy avc-policy-prof
  ipv4 flow monitor fm-avc input
  ipv4 flow monitor fm-avc output
  no shutdown
wireless tag policy avc-policy-tag
  wlan avc-wlan policy avc-policy-prof
wlan avc-wlan 1 avc-wlan-ssid
  no shutdown
ap <AP's ethernet mac>
  policy-tag avc-policy-tag
```

Minimum config for NBAR Protocol Discovery

Enable the NBAR Protocol Discovery in the default-policy-profile*:*

```
wireless profile policy default-policy-profile
  central association
  central switching
  ip nbar protocol-discovery
  vlan 70
  no shutdown
```

Related Documentation

Cisco C9800 Controller Information: https://software.cisco.com/download/home/286322605/type/282046477/release/Gibraltar-16.10.1

Complete list of the protocols supported in the release posted at the link below

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Legal Information

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco Copyright