Cisco Catalyst C9800-CL Application Visibility and Control IOS-XE Rel 16.10

Revised: July 9, 2019

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).

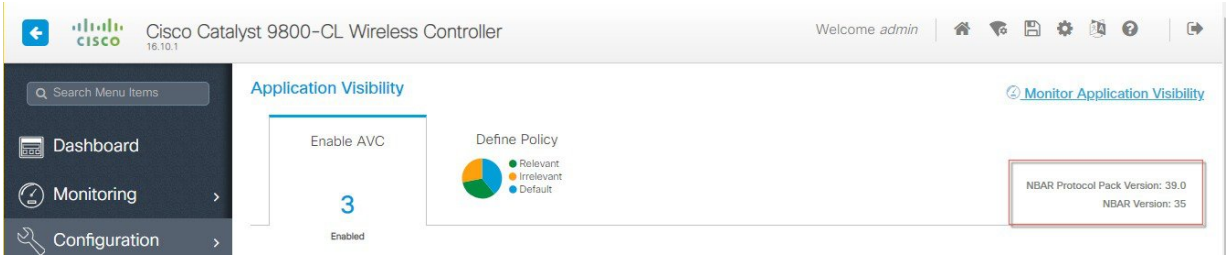
Complete list of the protocols supported in the release posted at the link below https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

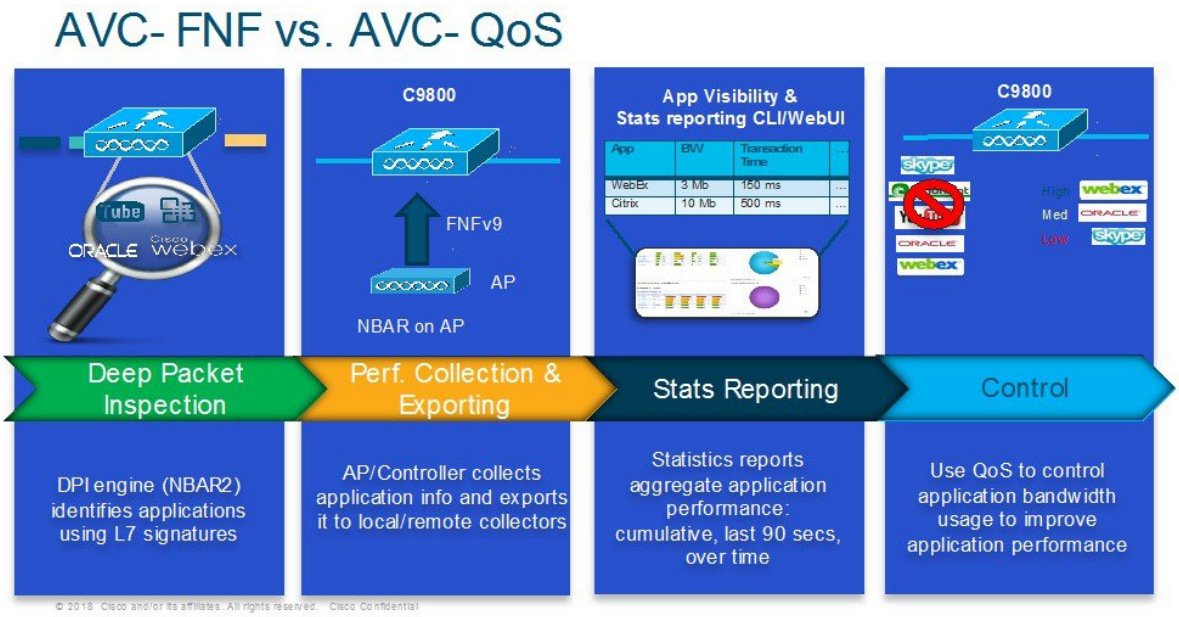
AVC-FNF Feature Summary on IOS XE 16.10

- NBAR on controller: NBAR engine v35, protocol pack v39.0
- NBAR on Wave-1 IOS APs: NBAR engine v23, Protocol Pack v14.0
- NBAR on Wave-2 COS APs: NBAR engine v35, Protocol Pack v33
- L2 & L3 roaming supported, L2 includes AP NBAR context transfer
- Application-based statistics reporting per WLAN and per client

- External FNFv9 collectors (PI, DNAC, third party)
- AVC Timeline
- Support for IOS (Wave 1) and ClickOS (Wave 2) APs
- WebUI, CLI, Netconf/Yang and SNMP support
- IPv4 and IPv6 traffic classification, no FNF support for IPv6 traffic flows on APs
- Support for all Cisco C9800 deployment modes
- IOS APs do not support AVC-FNF

	C9800	**W1 AP's**	**W2 AP's**
Local mode (Central switching)	Ipv4 Traffic : AVC Supported FNF Supported Ipv6 Traffic AVC Supported FNF Supported	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)	Not applicable	Ipv4 Traffic AVC Supported FNF Supported Ipv6 Traffic : AVC Supported FNF Supported	Ipv4 Traffic AVC Supported FNF Supported Ipv6 Traffic : AVC supported FNF not supported
Local mode (Fabric Mode)		Ipv4 Traffic AVC Supported FNF Supported Ipv6 Traffic : AVC Supported FNF Supported	Ipv4 Traffic AVC supported FNF supported Ipv6 Traffic : AVC supported FNF not supported





C9800 AVC-FNF Deployment Modes

C9800 IOS-XE 16.10 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)

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.

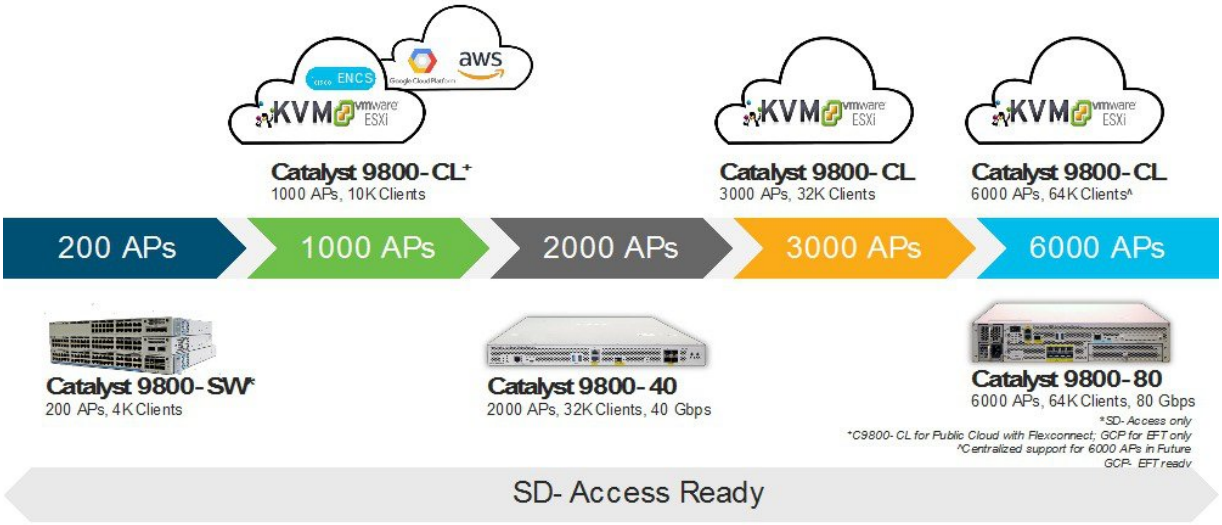
Flexible Netflow v9 records exporter is introduced. New Netflow v9 is sending 15 different data records (as defined in RFC 3954) to the External 3rd Party Netflow collector such as Stealthwatch and others. Support for the Enhanced Flow Record Data Export was added on the C9800.

- 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
- TOS-DSCP Value

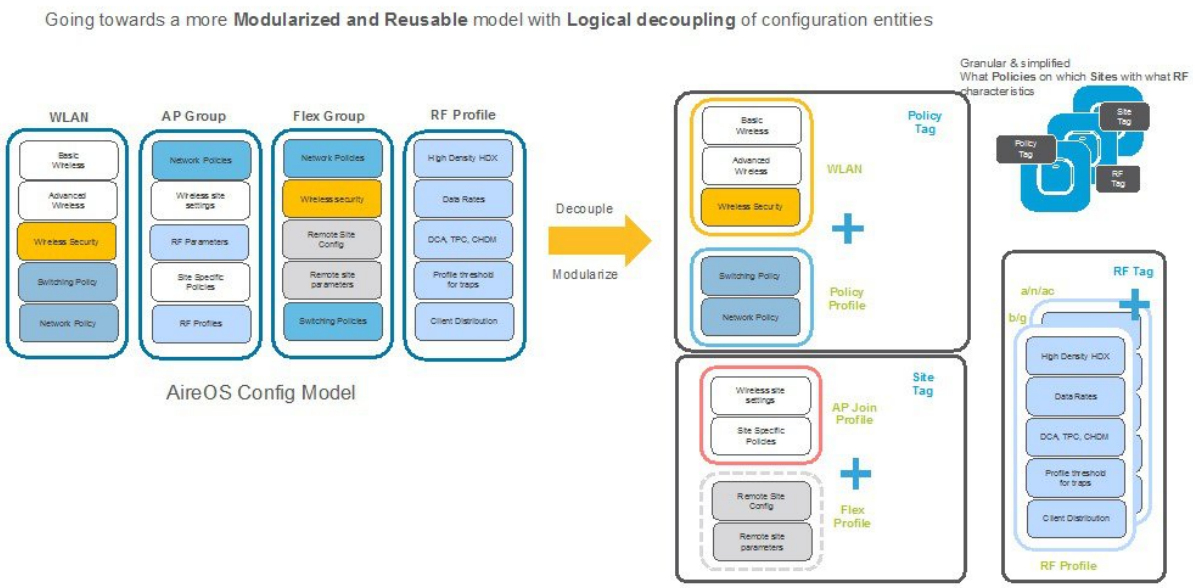
C9800 AVC-FNF Supported Platforms

- C9800
- Flex and Local modes: C9800
- APs
- Flex mode supports IOS (Wave-1) APs
- Flex and Fabric modes support COS (Wave-2) APs
- 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
- Local and Flex Central modes support all C9800 supported APs

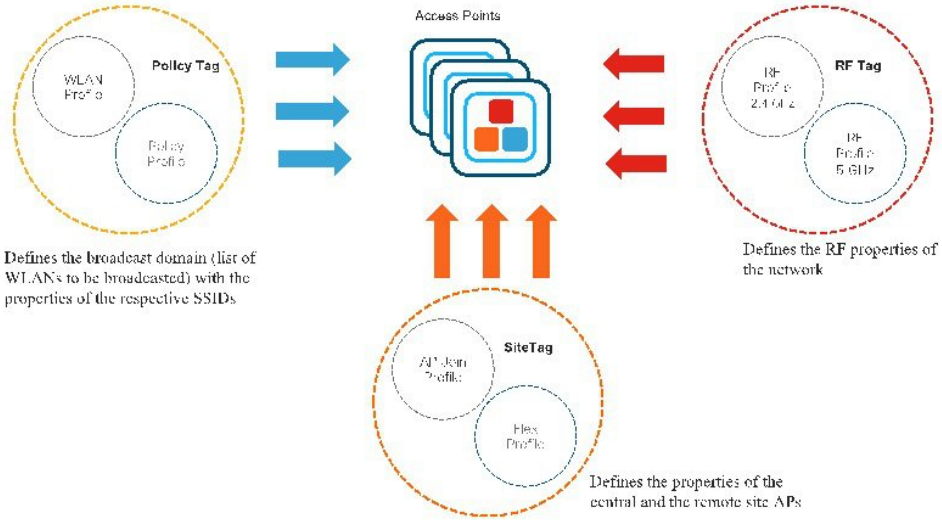
Catalyst 9800 Series – AP and Client Support



AireOS vs C9800 Config Model



Cisco 9800 Catalyst Wireless Config Model

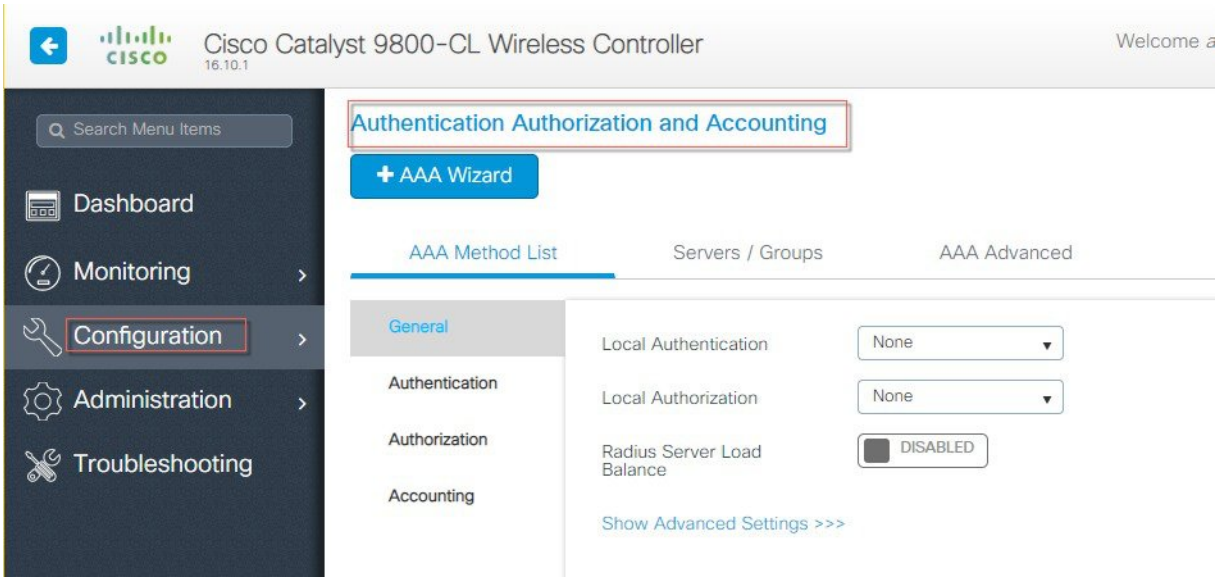


C9800 -CL Basic AAA Configuration-Day1

To perform CL basic AAA configuration for Day 1 perform the following steps:

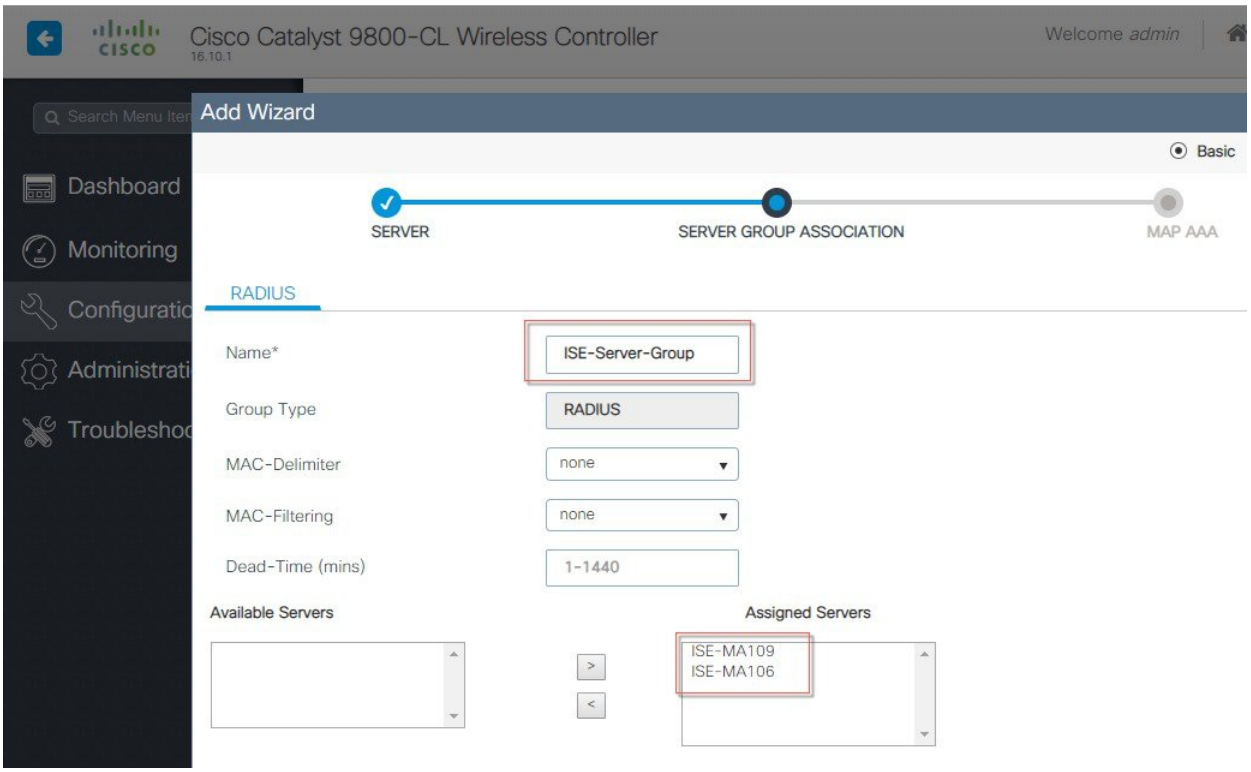
Procedure

Step 1 Login to C9800 and from the controller main menu navigate to **Configuration** > **AAA Wizard** and configure the following:



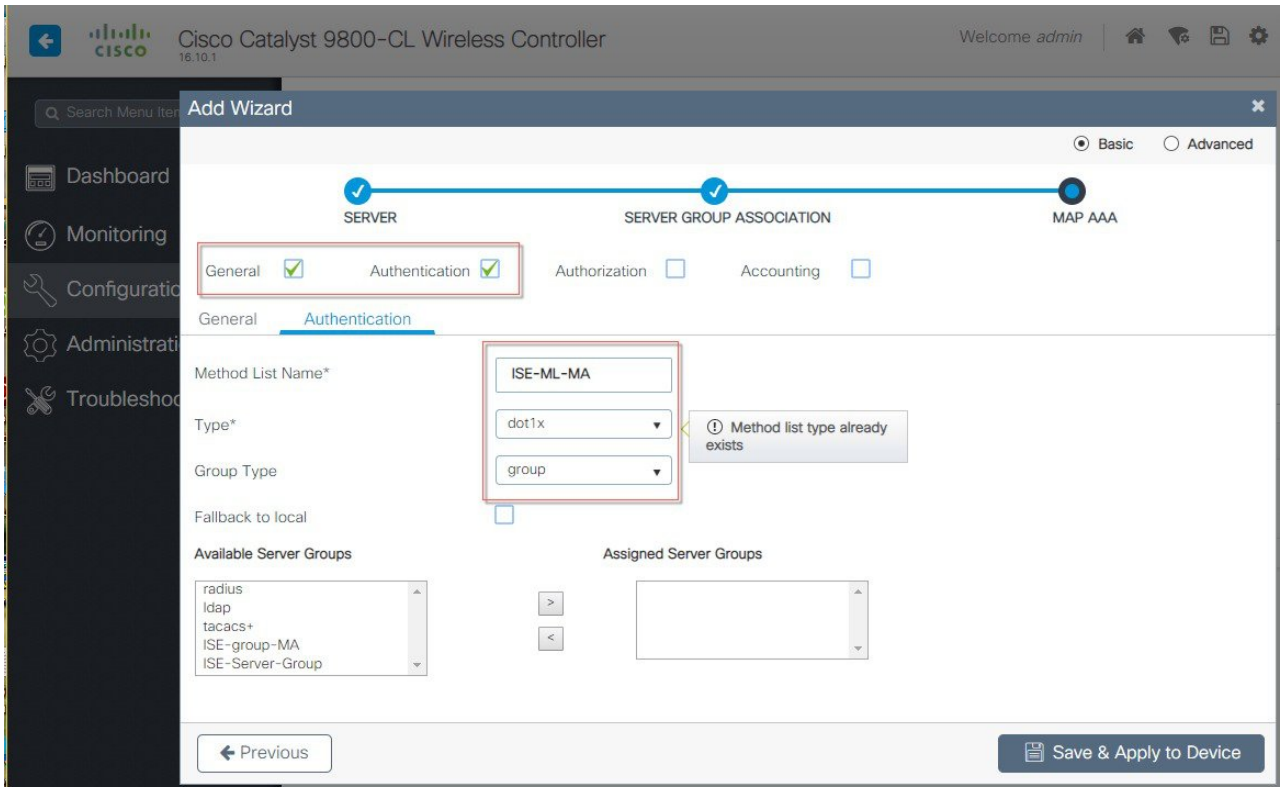
Server: **Name**= ISE, **Server Address**, Shared Secret and click **Next**.

Server Group Association: **Name**=ISE-Server-Group, From **Available Servers** select ISE, click '**>**' to assigned list, and click **Next**.



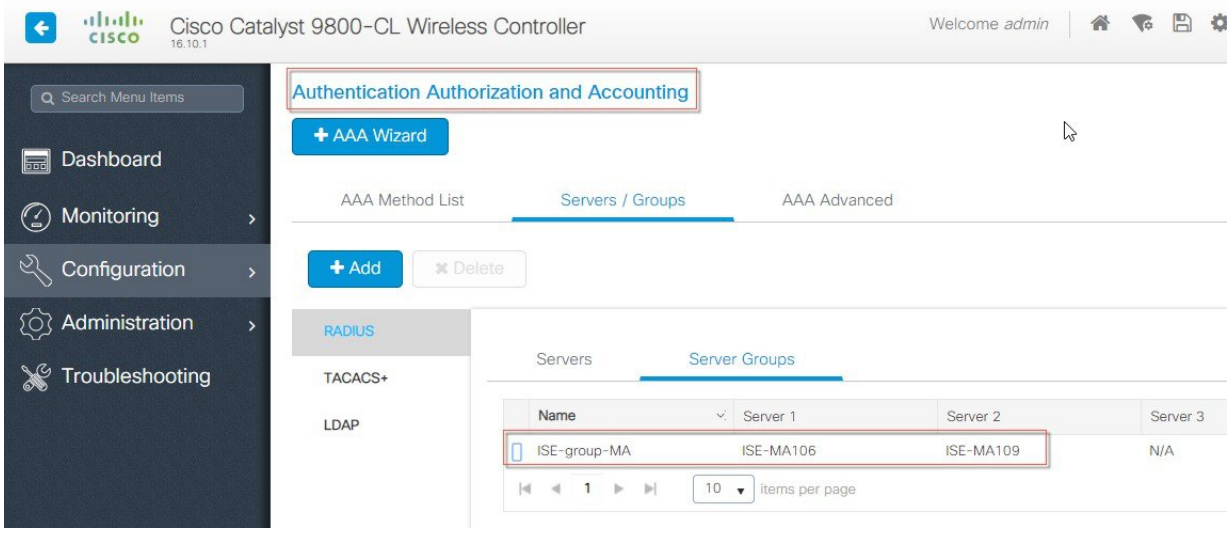
Step 2 To MAP AAA, select Authentication and **Method List Name**=ISE-ML, **Type**=dot1x, under 'Available Server Groups' Select 'ISE-Server-Group' and **Save & Apply button**.

See examples of AAA configuration in the screen shots below:



Step 3 Choose **Configuration** > **AAA**>**Servers/Groups** to list the configured AAA servers.

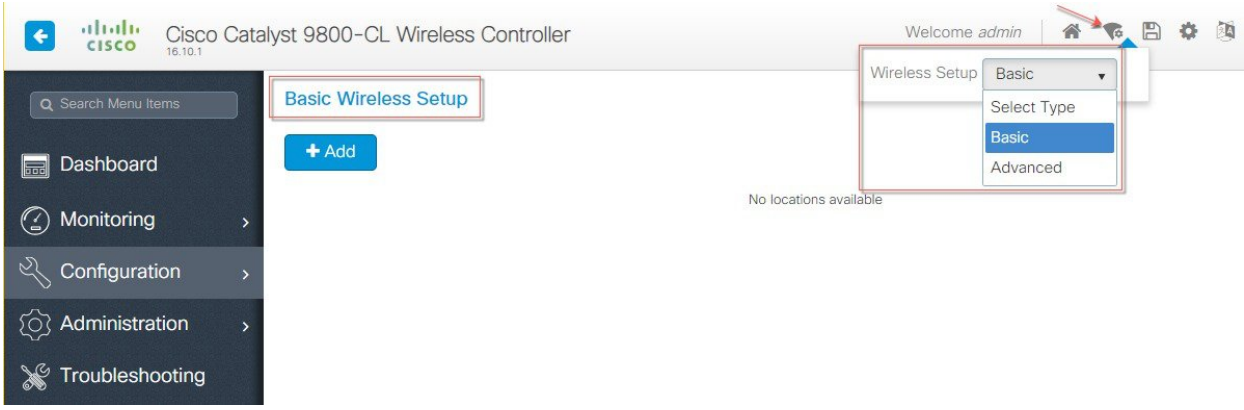
Example is as shown below:



C9800-CL Basic WLAN configuration-Day1

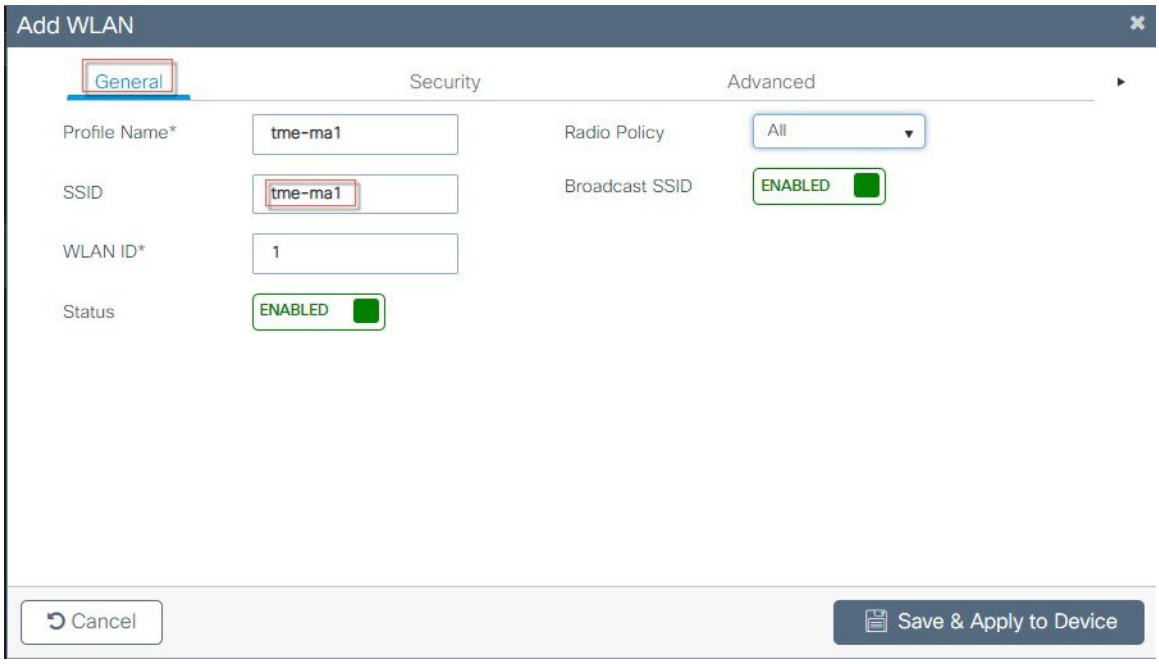
To perform C9800-CL basic WLAN configuration for Day 1, perform the following steps:

Step 4 Login to C9800 and from the controller main menu go to **Configuration** > **Wireless Basic Setup**.

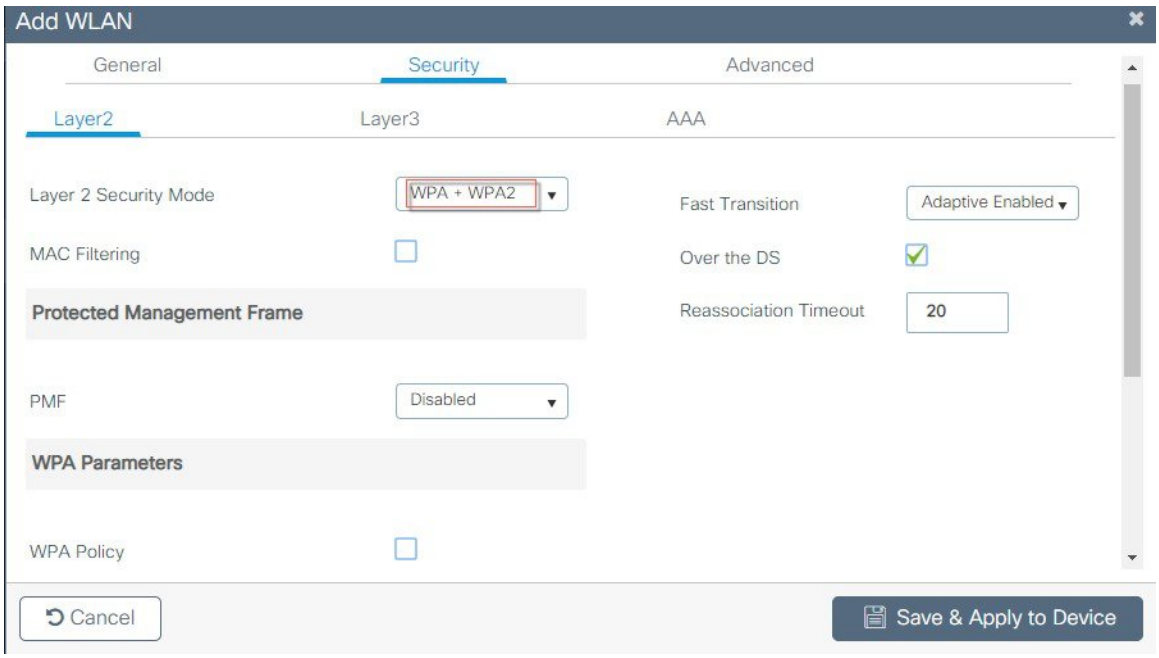


Configure **Location Name** and **Location type** as shown in the example below:

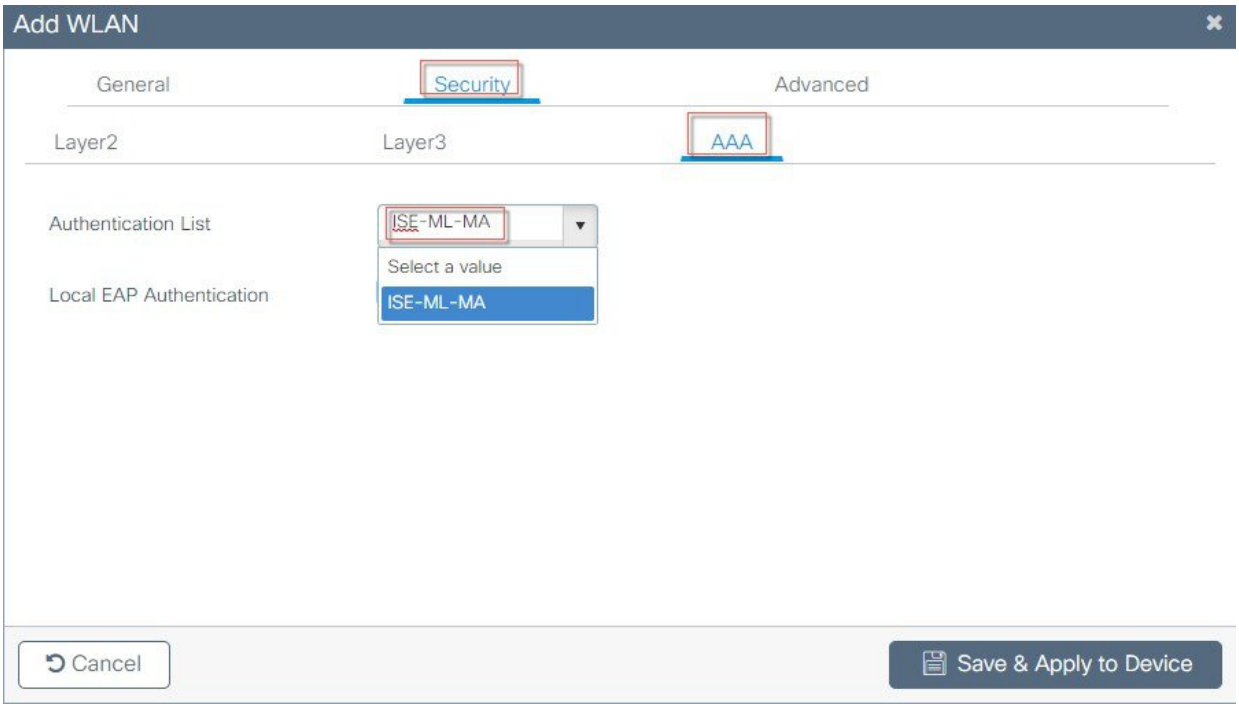
Next, click on ADD-WLAN to configure a new SSID and enable it.



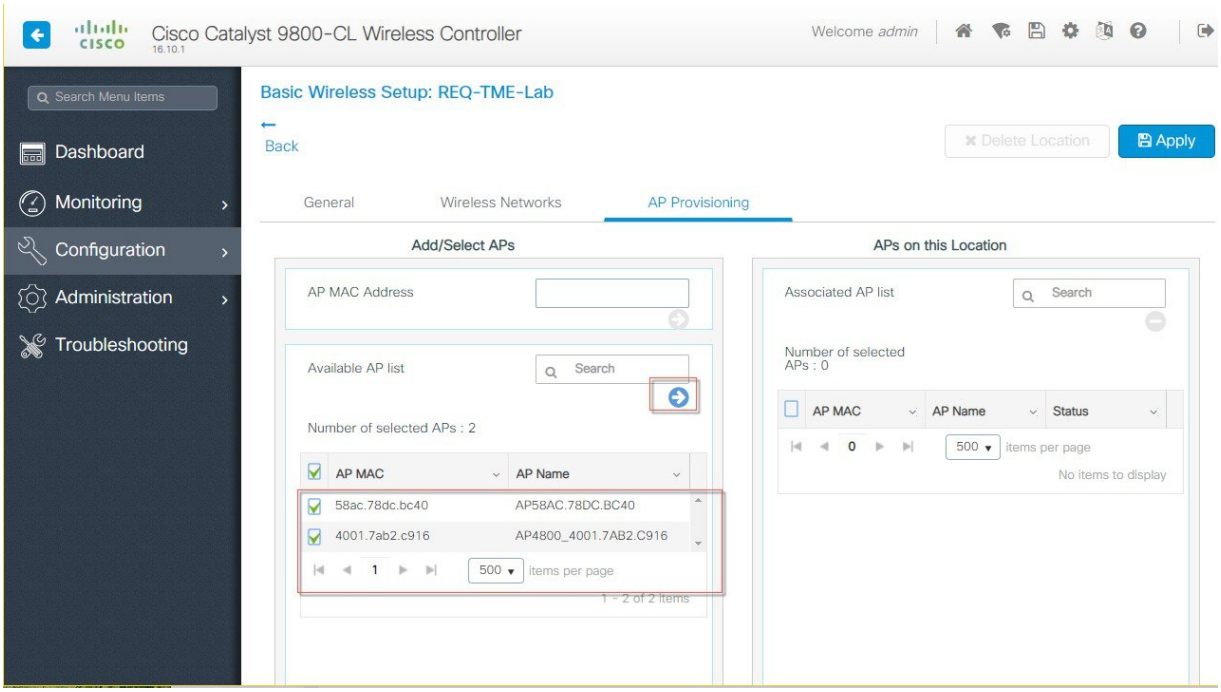
Configure security parameters of the selected WLAN.



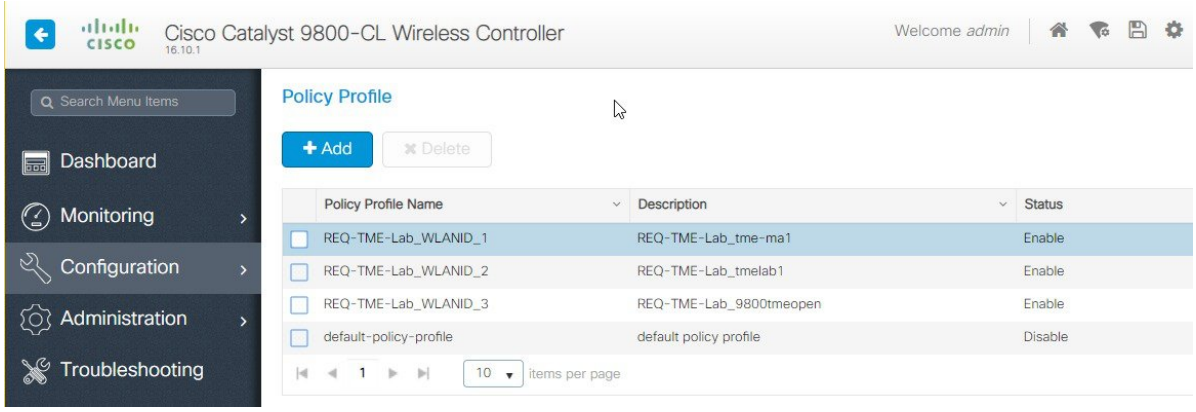
Step 5 Configure the AAA server that was setup in step 1.



Step 6 And final step would be to bind the configure WLAN to the selected APs in the specific Location.

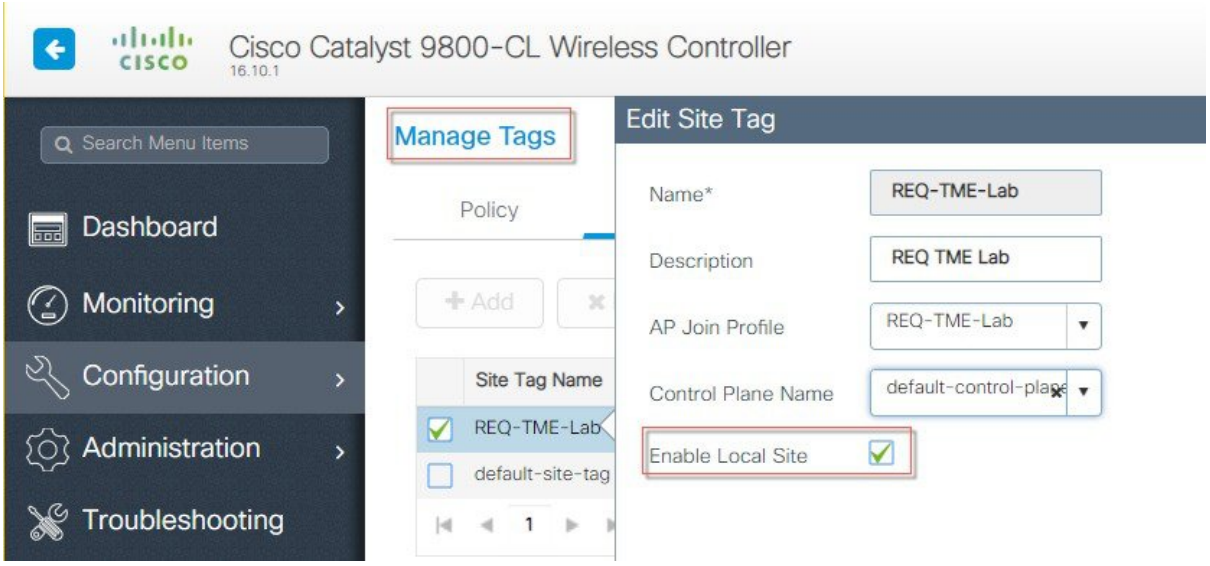


The above configured WLAN profiles can be seen now under Policy Profiles tab.



And also under the Configuration>Tags tab–make sure to enable the Local Site.

Step 7 Configure security parameters of the selected WLAN.

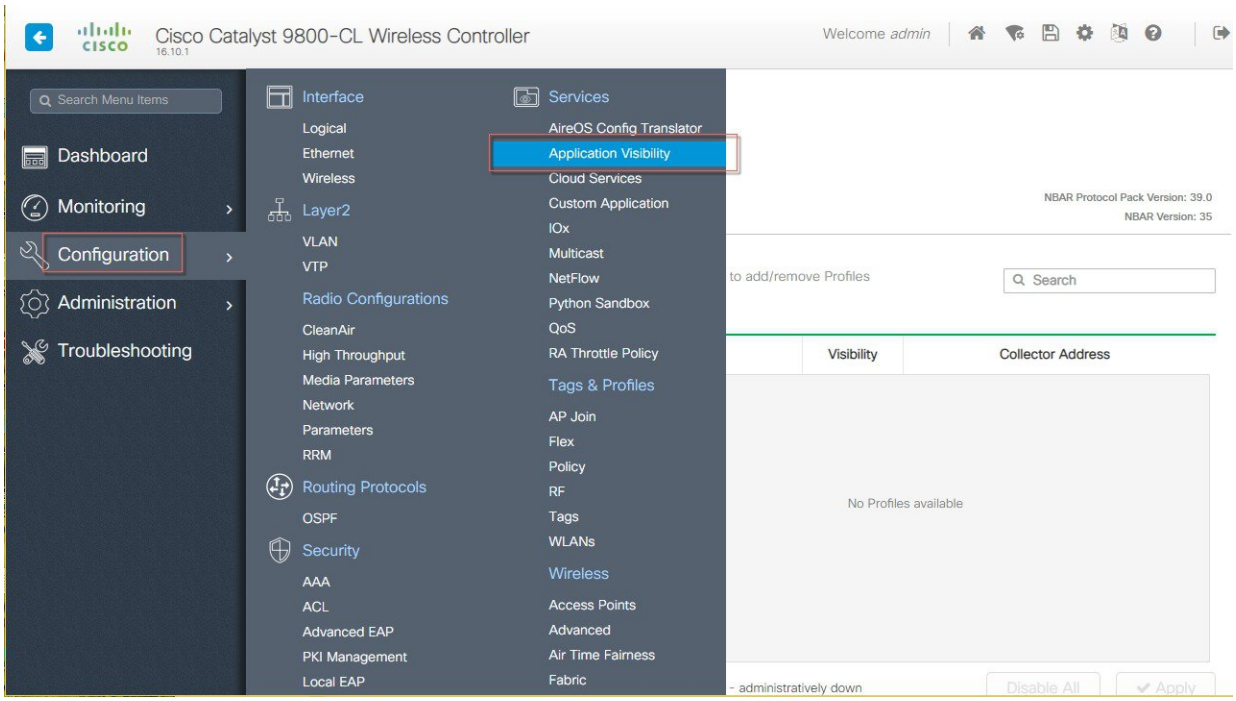


C9800 -CL AVC WLAN configuration-Day1

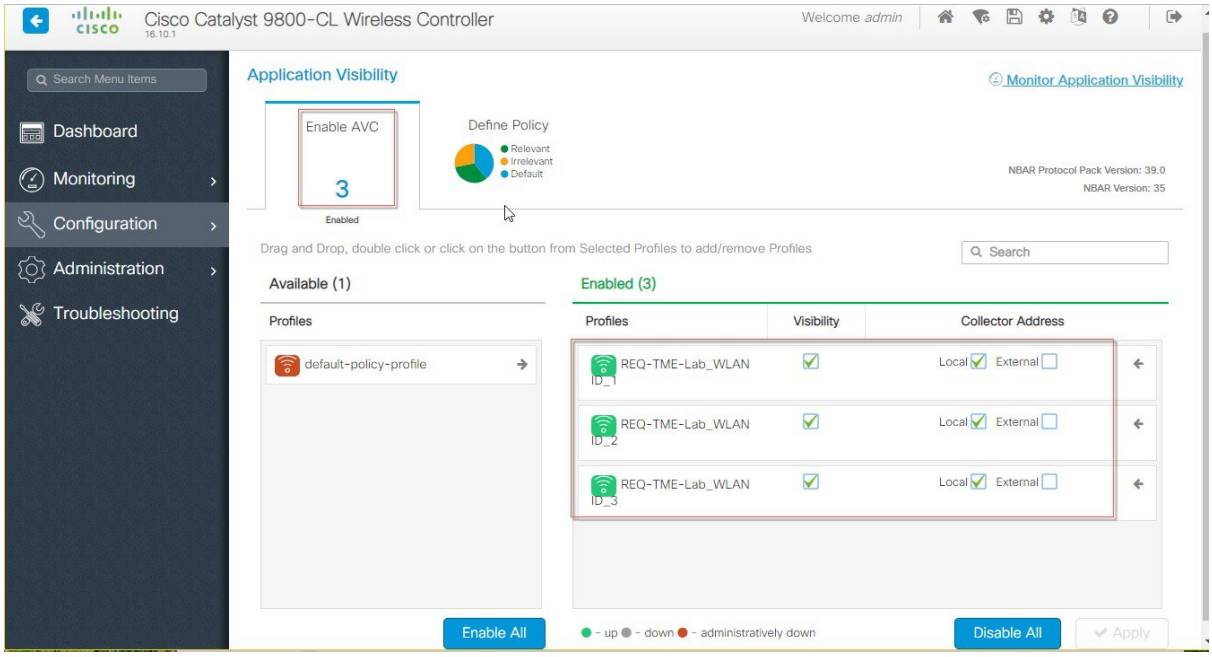
To perform C9800-CL AVC WLAN configuration for Day 1, perform the following steps:

Procedure

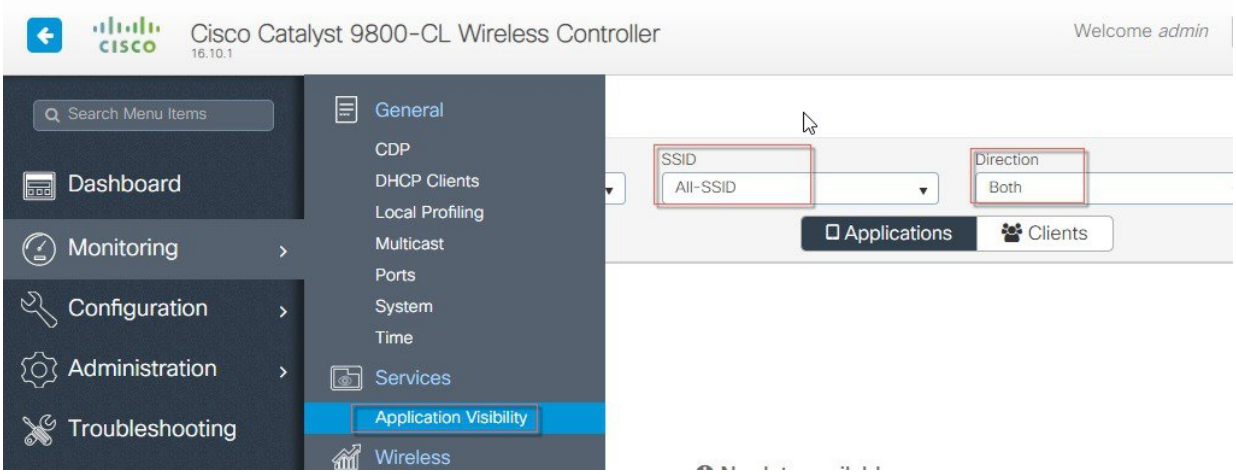
Step 1 Login to C9800 and from the controller main menu go to **Configuration** > **Services** > **Application Visibility**.



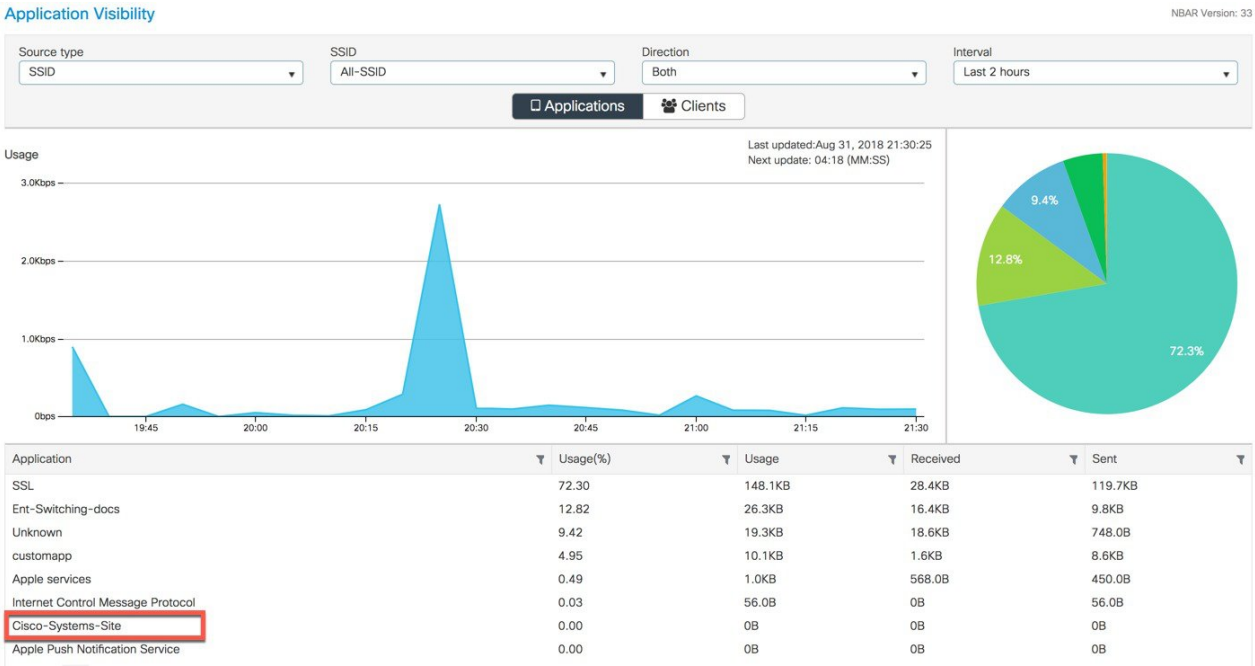
Step 2 Select Configured WLANs and apply AV on them as shown below, also select the local or external Netflow Collector.



Step 3 Connect a client(s) to the one of the AVC enabled WLANs and pass traffic by browsing to different sites. Wait for few seconds and navigate to C9800 main menu **Monitor** > **Application Visibility**.

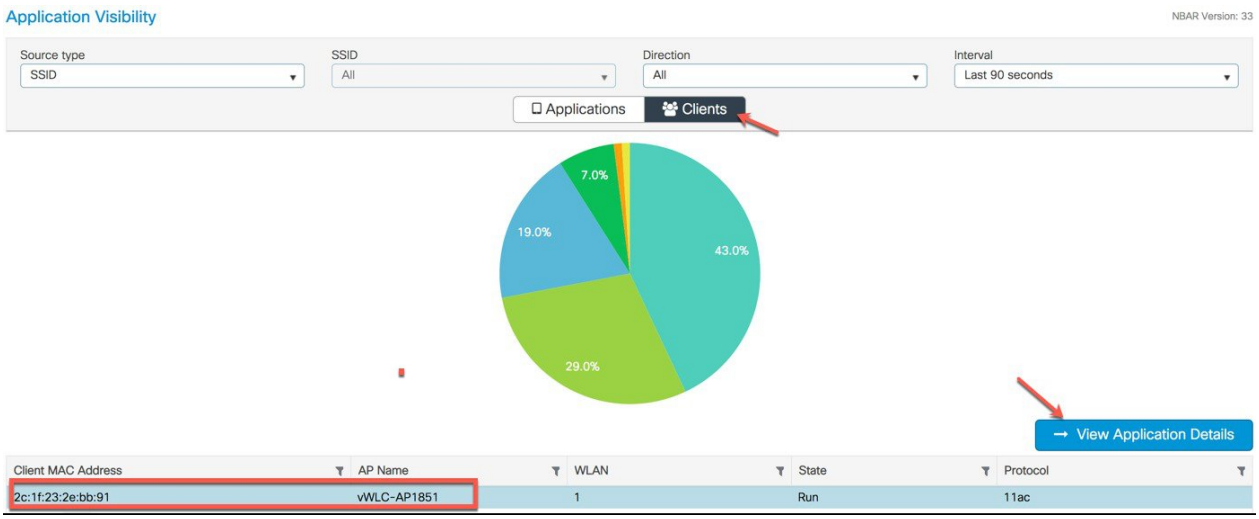


The page will show a graphical view of the all apps running on the network and monitored by the NBAR.

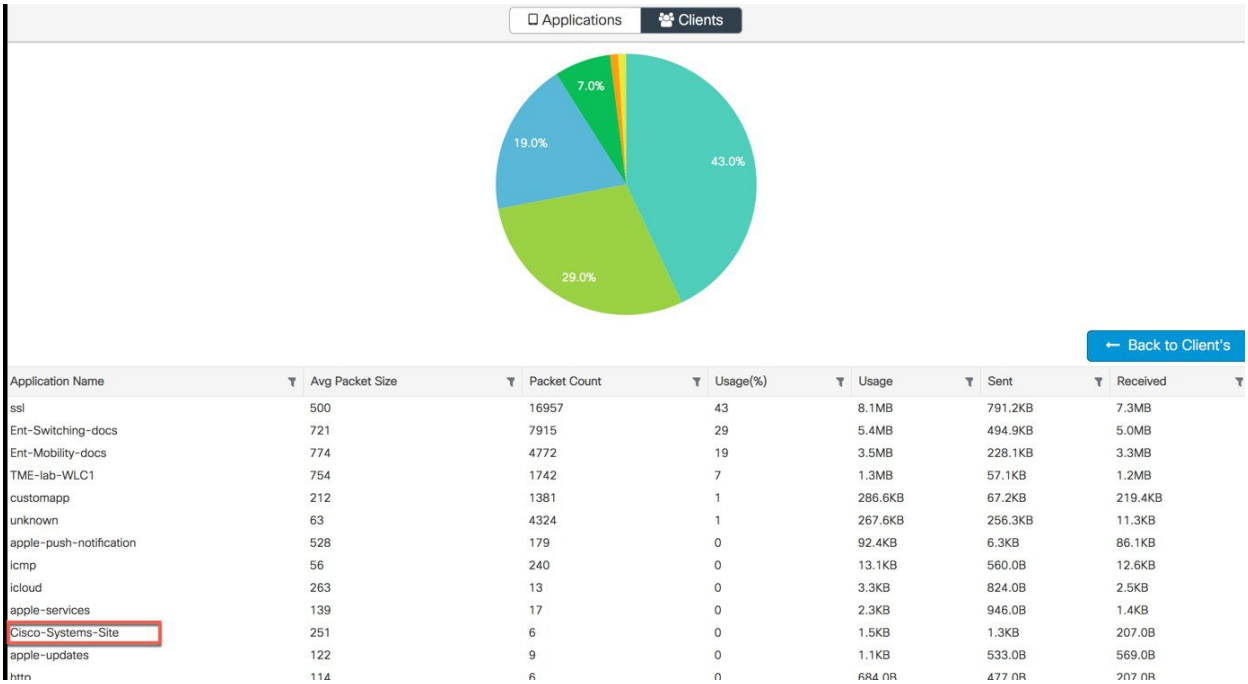


User can filter it through per SSID, direction and time (up to 48 hrs). User can see the apps which clients try to access.

Similarly, to view per client AV status, click Clients tab and select the client and click on **View Application Details**.



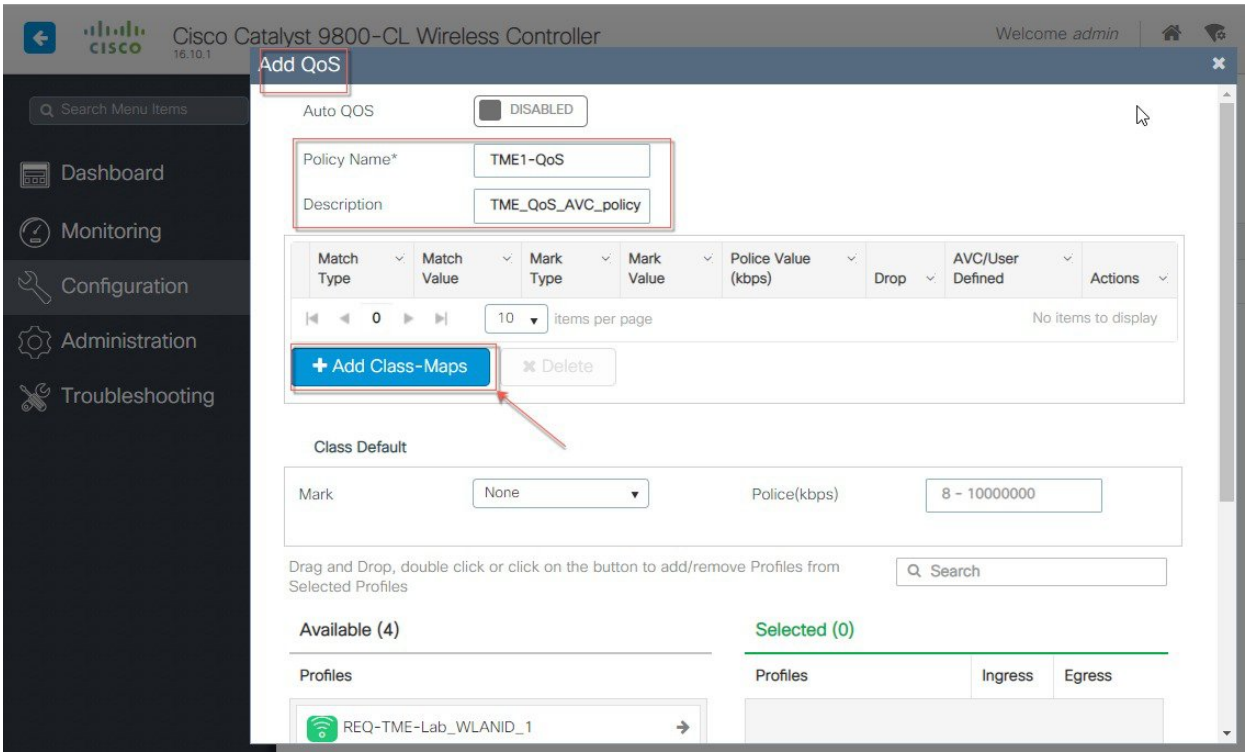
It displays all the apps usage in % graph and in tabular format which client has tried to access.



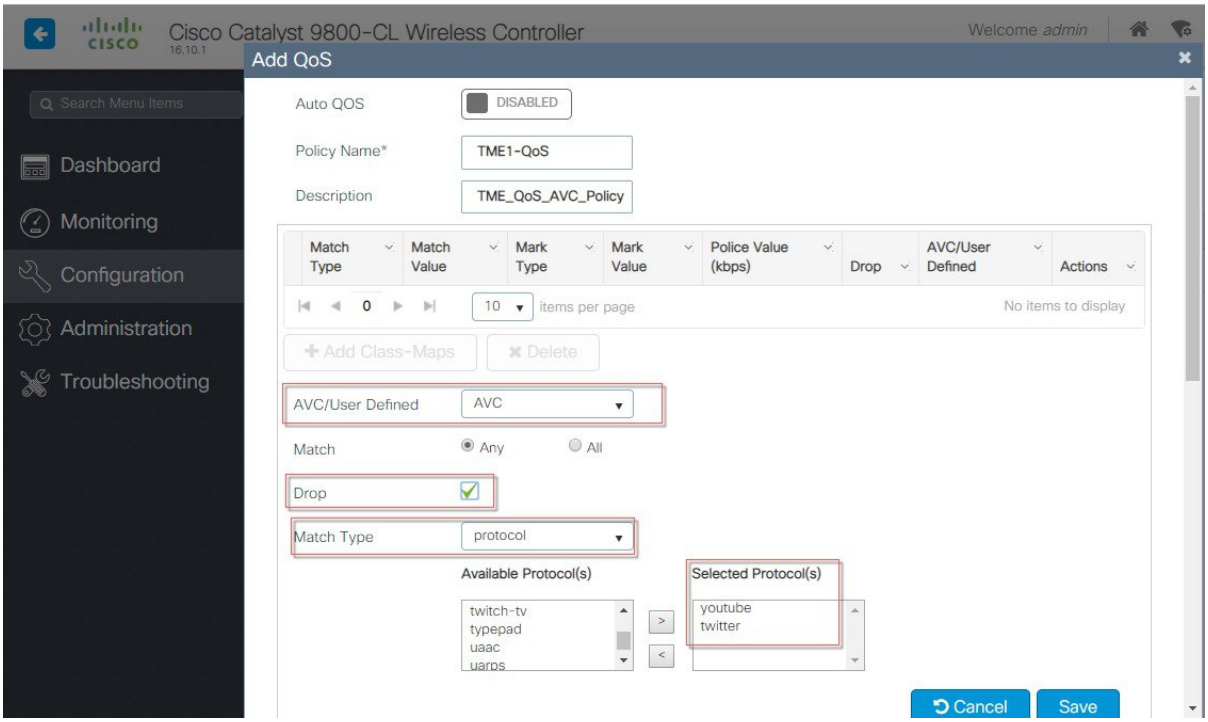
Application Name	Avg Packet Size	Packet Count	Usage(%)	Usage	Sent	Received
ssl	500	16957	43	8.1MB	791.2KB	7.3MB
Ent-Switching-docs	721	7915	29	5.4MB	494.9KB	5.0MB
Ent-Mobility-docs	774	4772	19	3.5MB	228.1KB	3.3MB
TME-lab-WLC1	754	1742	7	1.3MB	57.1KB	1.2MB
customapp	212	1381	1	286.6KB	67.2KB	219.4KB
unknown	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 4 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.

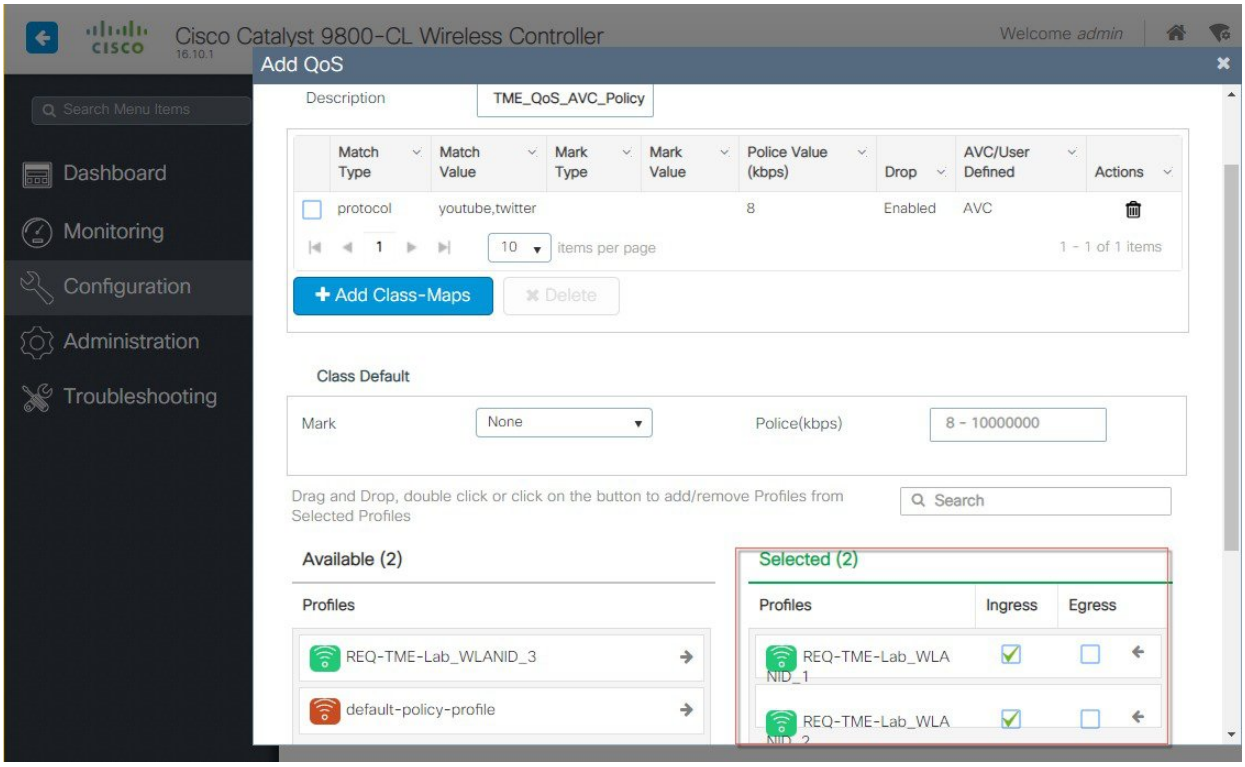
Go to **Configuration** >**Services** > **QoS** and Click on Add button and it will take you to QoS policy page.



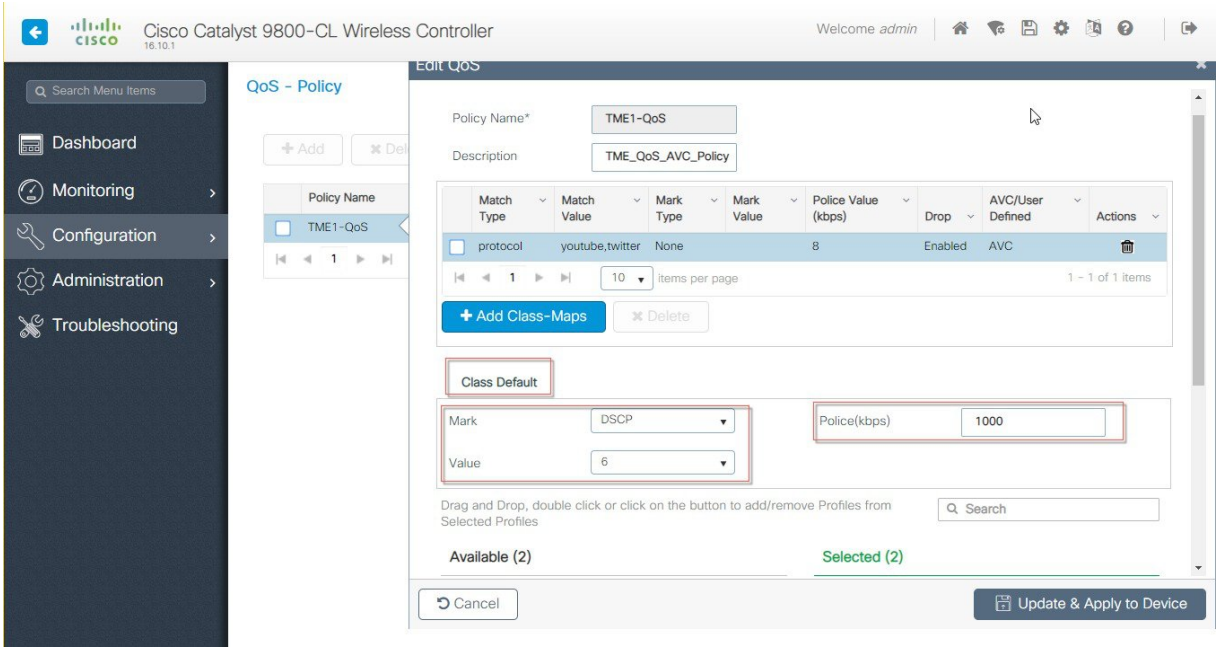
In that Auto QoS page select a button +Add Class_Maps, and in that next page configure desired AVC options such as Mark DSCP value or Drop a specific Protocol as shown in the example below YouTube and Twitter are configured to be Dropped by the AVC policy.



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.



Step 5 Configuring Class Default on the previously selected QoS policy. Class Default is an option where you can manage all other applications outside of the configured AV applications. If the Class Default option is not configured it can clog up the wireless bandwidth. By configuring the DSCP and Police Rate Limiting values it applies to all other applications.



Step 6 (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.

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 16.10
- 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

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:

```
veWLC-37b#show ip nbar protocol-pack active
Active Protocol Pack:
Name:                           Advanced Protocol Pack
Version:                        39.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:    35
State:                            Active
```

Same can be done from the WebUI interface:

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
```

Appendix

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.