cisco.



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

Application Visibility and Control 2NBAR Supported Feature 2AVC-FNF Feature Summary on IOS XE 16.10C9800 AVC-FNF Deployment ModesFlexible Netflow SupportC9800 AVC-FNF Supported PlatformsSAireOS vs C9800 Config ModelC9800 -CL Basic AAA Configuration-Day1C9800 -CL AVC WLAN configuration-Day1NBAR2 Protocol Pack UpgradeC9800 -CL AVC CLI CommandsC9800 -CL AVC CLI COMC9800 -CL AVC CLI COMC0800 -CL AVC CLI COMC9800 -CL AVC CLI COM<

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 :	Not applicable	Not applicable
	AVC Supported		
	FNF Supported		
	Ipv6 Traffic		
	AVC Supported		
	FNF Supported		
Flex mode (Central switching)	Ipv4 Traffic :	Not applicable	Not applicable
	AVC Supported		
	FNF Supported		
	Ipv6 Traffic :		
	AVC Supported		
	FNF Supported		
Flex mode (Local switching)	Not applicable	Ipv4 Traffic	Ipv4 Traffic
		AVC Supported	AVC Supported
		FNF Supported	FNF Supported
		Ipv6 Traffic :	Ipv6 Traffic :
		AVC Supported	AVC supported
		FNF Supported	FNF not supported
Local mode (Fabric Mode)		Ipv4 Traffic	Ipv4 Traffic
		AVC Supported	AVC supported
		FNF Supported	FNF supported
		Ipv6 Traffic :	Ipv6 Traffic :
		AVC Supported	AVC supported
		FNF Supported	FNF not supported



AVC-FNF vs. AVC-QoS



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



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

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.

e altalta cisco	Cisco Catalyst 9800-CL Wirele	ess Controller	Welcome admin
Q. Search Menu Iter	Add Wizard		
			Basic
Dashboard	Ø	•	
(Monitoring	SERVER	SERVER GROUP ASSOCIATION	MAP AAA
	RADIUS		
ැ ිරි Administrati	Name*	ISE-Server-Group	
Y Troubleshoo	Group Type	RADIUS	
6.6	MAC-Delimiter	none	
	MAC-Filtering	none 🔻	
	Dead-Time (mins)	1-1440	
	Available Servers	Assigned Servers	
	*	> ISE-MA109 ISE-MA106	

Step 2To 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:

e altalia cisco	Cisco Catalyst 9800-CL Wireless	Controller	Welcome admin 🛛 🌴 😵 🖺 🔅
Q Search Menu Iter	Add Wizard		×
			Basic Advanced
Dashboard	Ø		•
	SERVER	SERVER GROUP ASSOCIATION	MAP AAA
	General 🗹 Authentication 🗹	Authorization Accounting	
	General Authentication		
∑ Administrati∑ Troubleshoo	Method List Name*	ISE-ML-MA	
	Group Type	group	
	Fallback to local		
	Available Server Groups	Assigned Server Groups	
	radius Idap tacacs+ ISE-group-MA ISE-Server-Group	> <	
	Previous		Save & Apply to Device

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

Example is as shown below:

Cisco Cisco	Catal	yst 9800-CL Wireless	s Controller		Welcome admin	*) 🗘
Q Search Menu Items		Authentication Autho	rization and Accounting]				
📰 Dashboard		+ AAA Wizard			2			
Monitoring	>	AAA Method List	Servers / Groups	AAA Advanced				
Configuration	>	+ Add X Del						
O Administration	>	RADIUS	-					
💥 Troubleshooting		TACACS+	Servers	Server Groups				
		LDAP	Name	 Server 1 	Server 2		Serve	r 3
			ISE-group-MA	ISE-MA106	ISE-MA109		N/A	
				10 🔻 items per page				

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**.

Cisco Catalyst 9800-CL Wireless Controller	Welcome a	dmin 🔗 🍖 🖹 🌣	Ø
	Wireless Setup	Basic 🔹	
Q Search Menu Items Basic Wireless Setup		Select Type	
+ Add		Basic	
Dashboard		Advanced	
Monitoring >	able		
Configuration >			
Administration			
X Troubleshooting			

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

Cisco Cisco	Catal	yst 9800-CL W	ireless Controller		Welcome admin	* *
Q Search Menu Items		Basic Wireless	Setup: REQ-TME-Lab			
ashboard		← Back			2	X Delete
Monitoring	>	General	Wireless Networks	AP Provisioning		
	>	Location Name*	REQ-TME-Lab			
O Administration	>	Description	TME Lab			
₩ Troubleshooting		Location Type	Local			
		Client Density	Low Typical	High		

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

Security	Radio Policy Broadcast SSID	Advanced All ENABLED	•
na1	Radio Policy Broadcast SSID	All ENABLED	T
na1	Broadcast SSID	ENABLED	
D			
	D		

Configure security parameters of the selected WLAN.

Add WLAN			
General	Security	Advanced	
Layer2	Layer3	ААА	
Layer 2 Security Mode	WPA + WPA2	Fast Transition Adaptive Enable	ed 🖌
MAC Filtering		Over the DS	
Protected Management Fram	ne	Reassociation Timeout 20	
PMF	Disabled 🗸		
WPA Parameters			
WPA Policy			
Cancel		🖺 Save & Apply to	Device

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

id WLAN			
General	Security	Advanced	
Layer2	Layer3	AAA	
Authentication List	USE-ML-MA		
Local EAP Authentication	Select a value		
9 Cancel		Save	& Apply to Device

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

Cisco Cisco C 16.10.1	Catalyst 9800-CL Wireless Controller Basic Wireless Setup: REQ-TME-Lab	Welcome admin 🛛 🎓 🌾 🖺 🌣 🔯 🕢 🕩
Dashboard	Back General Wireless Networks AP Provisioning	* Delete Location
	Add/Select APs	APs on this Location
	> AP MAC Address	Associated AP list
X Troubleshooting	Available AP list Q Search Number of selected APs : 2	Number of selected APs : 0 AP MAC
	AP MAC AP Name ✓ 58ac.78dc.bc40 AP58AC.78DC.BC40 ✓ 4001.7ab2.c916 AP4800_4001.7AB2.C916 ✓ 1 ► 1 ► 1 ► 1 ► 1 ► 1 ► 1 ► 1 ► ► 1 ► 1 ► 1 ► 1 ► 1 ► 1 ► 1 ► 1 ► ► ► ► ► ► ► ► ► ► ► ► ► ► <	No items to display



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

Cisco Catal	lyst 9800-CL Wireless Controller		Welcome admin	*	T a	¢
Q Search Menu Items	Policy Profile	3				
📷 Dashboard	+ Add × Delete					
Monitoring	Policy Profile Name	 Description 	~	Status		
	REQ-TME-Lab_WLANID_1	REQ-TME-Lab_tme-ma1		Enable		
🔾 Configuration 🛛 🔸	REQ-TME-Lab_WLANID_2	REQ-TME-Lab_tmelab1		Enable		
	REQ-TME-Lab_WLANID_3	REQ-TME-Lab_9800tmeopen		Enable		
Administration >	default-policy-profile	default policy profile		Disable		
✗ Troubleshooting	◀ ◀ 1 ► ► 10 ▼ items per pag	e				

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

Step 7 Configure security parameters of the selected WLAN.

Q Search Menu Items	Manage Tags	Edit Site Tag	
Dashboard	Policy	Name*	REQ-TME-Lab
		Description	REQ TME Lab
Monitoring >	+ Add ×	AP Join Profile	REQ-TME-Lab
Configuration >	Site Tag Name	Control Plane Name	default-control-plaxe 🗸
	REQ-TME-Lab	Epoble Legal Site	

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**.

Cisco Cisco C	Cata	lyst 9800-CL Wireless Cont	troller	Welcome admin	• • • • •
Q Search Menu Items)	Interface Logical Ethernet Wireless ⊡ Layer2	Services AireOS Config Translator Application Visibility Cloud Services Custom Application IOx		NBAR Protocol Pack Version: 39.0 NBAR Version: 35
Configuration	> >	VLAN VTP Radio Configurations	Multicast NetFlow Python Sandbox	to add/remove Profiles	Q Search
X Troubleshooting		CleanAir High Throughput Media Parameters Network Parameters RRM Routing Protocols OSPF Security AAA ACL Advanced EAP PKI Management	QoS RA Throttie Policy Tags & Profiles AP Join Flex Policy RF Tags WLANs Wireless Access Points Advanced Air Time Faimess	Visibility No Profiles available	Collector Address
		Local EAP	Fabric	- administratively down	Disable All

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

Cisco Ca	talyst 9800-CL Wireless Controller		Welcome adm	in 🖌 🏶 🛱 🏟	0
Q Search Menu Items	Application Visibility			(2) Monitor Applic	ation Visibility
Dashboard	Enable AVC Define Policy Relevant 3			NBAR Protocol Paci NBJ	k Version: 39.0 AR Version: 35
Configuration >	Enabled	om Salacted Profiles to add/romava	Profiles		
(○) Administration >	Available (1)	Enabled (3)	Fromes	Q Search	
X Troubleshooting	Profiles	Profiles	Visibility	Collector Address	
	efault-policy-profile	REQ-TME-Lab_WLAN		Local 🖌 External 🗌	÷
		REQ-TME-Lab_WLAN		Local 🗹 External 🗌	*
		REQ-TME-Lab_WLAN		Local 🖌 External 🗌	÷
	Enable All	🔵 - up 🖲 - down 🔴 - administrativ	ely down	Disable All	Apply

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**.

Cisco Cisco	Catalyst 9800-CL Wireless Controller	Welcome admin
Q Search Menu Items	General	
B Dashboard	DHCP Clients Local Profiling	
Monitoring	> Multicast Applications Clien	ts
Configuration	> System Time	
() Administration	> Services	
💥 Troubleshooting	Application Visibility Wireless	

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.



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.

Cisco Catal	/st 9800-CL Wireles	ss Controller		Welcome a	admin 🛛 🎓 🕵 🗙
Q Search Menu Items	Auto QOS	DISABLED			↓ }
📻 Dashboard	Policy Name*	TME1-QoS			
	Description	TME_QoS_AVC_policy			
	Match × Match Type Value	✓ Mark ✓ Mark ✓ Type Value	Police Value ~ (kbps) Drop	AVC/User ~ ~ Defined	Actions ~
िते Administration	⊲ ⊲ 0 ⊳ ⊳	10 v items per page		No iter	ns to display
C Troubleshooting	+ Add Class-Maps	* Delete			
	Mark [None 🔻	Police(kbps)	8 - 10000000	
	Drag and Drop, double click Selected Profiles	k or click on the button to add/remo	ve Profiles from	Search	
	Available (4)		Selected (0)		
	Profiles		Profiles	Ingress E	gress
	REQ-TME-Lab_WL	ANID_1		in di	-

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.

Cisco Cat	alyst 9800-CL Wirel dd QoS	less Controller			Welcome a	dmin 🛛 🐔
Search Menu Items	Auto QOS	DISABLED				
Dashboard	Policy Name*	TME1-QoS				
Monitoring	Description	TME_QoS_AVC_Policy				
Configuration	Match v Match Type Value	 Mark Yalue Mark Value 	 Police Value (kbps) 	Drop ~	AVC/User v Defined	Actions ~
Administration		10 V items per page			No item	ns to display
lanimilou autori	+ Add Class-Maps	Belete				
Troubleshooting	AVC/User Defined	AVC •				
	Match	● Any ● All				
	Drop					
	Match Type	protocol 🗸				
	4	Available Protocol(s)	Selected Protocol(s)	1		
		twitch-tv typepad uaac uarps	youtube twitter	*		
					Cancel	Save

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.

cisco Cisco Ca	talyst 9800-CL Wireless Controller Add QoS	Welcome admin
Search Menu Items	Description TME_QoS_AVC_Policy	
Dashboard	Match × Match × Mark × Mark Type Value Type Value	Police Value × AVC/User × AVC/User × Attons ×
Monitoring	protocol youtube,twitter	8 Enabled AVC 💼
Configuration	+ Add Class-Maps * Delete	
Administration	Class Default	
Iroubleshooting	Mark None •	Police(kbps) 8 - 10000000
	Drag and Drop, double click or click on the button to add/ren Selected Profiles Available (2)	ove Profiles from Q Search Selected (2)
	Profiles	Profiles Ingress Egress
	REQ-TME-Lab_WLANID_3	REQ-TME-Lab_WLA
	default-policy-profile	

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.

Cisco Catal	lyst 9800-CL Wireless Co	ontroller		Welcome admir	n 🔺 🐔 🖪	* • •
Q Search Menu Items	QoS - Policy	IIT QOS	TME1_OoS	1	N	×
戻 Dashboard	+ Add X Del	Description	TME_QoS_AVC_Policy	ſ	13	
Monitoring >	Policy Name	Match ~ Match Type Value	n ~ Mark ~ Type	Mark v Police Value v Value (kbps)	AVC/User Drop ~ Defined	× Actions ×
Configuration		protocol youtul	be,twitter None	8	Enabled AVC	ŵ
() Administration >	12 3 1 2 21		10 🔹 items per pag	ge		1 - 1 of 1 items
X Troubleshooting		Class Default	Deco	Police/(these)	1000	
		Mark	V V	Police(kbps)	1000	
		Value	6 •			
		Drag and Drop, double clic Selected Profiles	k or click on the button	to add/remove Profiles from	Q Search	
		Available (2)		Selected (2)		-
		Cancel			🗍 🗍 Upd	ate & Apply to Device

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:

Cisco Cata	lyst 9800-CL Wire	less Controller	
Q Search Menu Items	Software Upgrade	5	
📻 Dashboard	Device Mode	INSTALL	
Monitoring >	Transport Type	Desktop (HTTPS)]
Configuration >	File System	bootflash 🔻	Free Space: 5059.30 MB
Administration	Source File Path*	Select File Proto	ocol Pack file
💥 Troubleshooting		📥 Download & Inst	tall
		Save Configura	ation & Reload

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:

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

uluilu cisco.

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.