

Application Visibility and Control Feature Deployment Guide–Phase 2, Software Release 7.5

Last Updated: August, 2013

Application Visibility and Control–Phase 1

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 is supported on 2500, 5500, 7500, 8500 and WiSM2 controllers on Local and Flex Mode APs (For WLANs configured for central switching only)

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

Application Visibility and Control–Phase 2

In phase two of the AVC support for Protocol Packs has been added. Protocol packs are software packages that allow update of signature support without replacing the image on the Controller. You have an option to load protocol packs dynamically when new protocol support is being added. There will be two kinds of Protocol Packs–Major and Minor:

- Major protocol packs include support for new protocols, updates and bug fixes.
- Minor protocol packs typically do not include support for new protocols.
- Protocol packs are targeted to specific platform types, software versions and releases separately.
 Protocol Packs can be downloaded from CCO using the software type "NBAR2 Protocol Pack".

Protocol packs are released with specific NBAR engine versions. For example, WLC 7.5 has NBAR engine 13, so protocol packs for it are written for engine 13 (pp-unified-wng-152-4.S-13-4.1.1.pack). Loading a protocol pack can be done if the engine version on the platform is same or higher than the version required by the protocol pack (13 in the example above). Therefore for example – PP4.1 for 3.7 (version 13) can be loaded on top of 3.7 (ver 13) and 3.8, but PP4.1 for 3.8 cannot be loaded on top of 3.7. It is strongly recommended to use the protocol pack that is the exact match for the engine.

For AVC phase 2, protocol packs can be downloaded directly from CCO–Protocol Pack 4.1.1 for engine XE 3.7. The protocol pack file "pp-AIR-7.5-13-4.1.1.pack" (Format: pp-AIR-{release}-{engine version}-M.m.r.pack) will be located in the same location with the controller code ver 7.5. This is the only tested and supported protocol pack released with controller software version 7.5.



Note

If you download the protocol pack from the below link where protocol packs for other Cisco devices is posted for download, the protocol packs might work but will not be supported. See http://software.cisco.com/download/release.html?mdfid=282993672&flowid=20841&softwareid=2845 09011&release=4.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest

Download So	ftware	Download Cart (0 tems) [+] Feedback Help
Downloads Home > Produ Cisco 5508 Wireless Contro Cisco 5508 Wireless	ts > Wireless > Wireless LAN Controller > Standalone Controllers > Cis iller > NBAR2 Protocol Packs-4.1.1	co 5500 Series Wireless Controllers. >
0.000 0000 1110.000	Controller	
Search	Release 4.1.1	Release Notes for 4.1.1 🗮 🞄
Seruch.	Release 4.1.1	Release Notes for 4.1.1 📓 🞄 Release Date 🔹 Size

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html



For AVC phase 2 the downloadable NBAR Protocol Packs are supported on 5500, 7500, 8500 and WiSM2 controllers on Local and Flex Mode APs (For WLANs configured for central switching only). The 2500 series controllers do not support Protocol Packs.

NBAR/AVC Facts

- NBAR/AVC phase 2 on WLC can classify and take action on 1054 different applications.
- Two actions, either DROP or MARK is possible on any classified application.
- Maximum 16 AVC profiles can be created on a WLC.
- Each AVC profile can be configured with a maximum 32 rules.
- Same AVC profile can be mapped to multiple WLANs. But one WLAN can have only one AVC profile.
- Only 1 NetFlow exporter and monitor can be configured on WLC.
- NBAR/AVC stats are displayed only for top 10 applications on GUI. CLI can be used to see all applications.
- NBAR/AVC is supported on WLANs configured for central switching only.
- If AVC profile mapped to WLAN has a rule for MARK action, that application will get precedence as per QOS profile configured in AVC rule overriding the QOS profile configured on WLAN.
- Any application, which is not supported/recognized by NBAR engine on WLC, is captured under the bucket of UNCLASSIFIED traffic.
- IPv6 traffic cannot be classified.
- AAA override of AVC profiles is not supported.
- AVC profile can be configured per WLAN and cannot be applied per user basis.
- NBAR/AVC is not supported in vWLC and SRE WLC.

AVC and QoS Interaction on the WLAN

The AVC/NBAR2 engine on the controller interoperates with the QoS settings on the specific WLAN. The NBAR2 functionality is based on the DSCP setting. The following occurs to the packets in Upstream and Downstream directions if AVC and QoS are configured on the same WLAN:

Upstream

- 1. Packet comes with or without inner DSCP from wireless side (wireless client).
- 2. AP will add DSCP in the CAPWAP header that is configured on WLAN (QoS based config).
- **3**. WLC will remove CAPWAP header.
- **4.** AVC module on the controller will overwrite the DSCP to the configured **marked** value in the AVC profile and send it out.

Downstream

- 1. Packet comes from switch with or without inner DSCP wired side value.
- 2. AVC module will overwrite the inner DSCP value.

- **3.** Controller will compare WLAN QoS configuration (as per 802.1p value that is actually 802.11e) with inner DSCP value that NBAR had overwritten. WLC will choose the lesser value and put it into CAPWAP header for DSCP.
- WLC will send out the packet to AP with QoS WLAN setting on the outer CAPWAP and AVC inner DSCP setting.
- 5. AP strips the CAPWAP header and sends the packet on air with AVC DSCP setting; if AVC was not applied to an application then that application will adopt the QoS setting of the WLAN.

AVC Operation with Anchor/Foreign Controller's Setup

In the case of Anchor and Foreign controller's configuration, the AVC has to be configured where the application control essentially is required. In most cases in Anchor/Foreign setups the AVC should be enabled on the Anchor controller. AVC profile enforcement will happen on the WLAN on the Anchor controller. If Anchor controller is release 7.4 or higher the above mentioned setup will work.

Loading AVC Protocol Pack–Phase 2

Loading of Protocol Packs is supported only via the command line interface. The command to load a protocol pack is shown in the example below:



The download process might take some time.

```
TFTP AVC Protocol Pack transfer starting.

TFTP receive complete... Loading Protocol Pack.

INFO, deactivation XDR was bypassed as batch config was identified

% INFO NBAR : engine deactivation

AVC Protocol Pack installed.
```

Use the show command to view the currently loaded protocol pack

```
(Cisco Controller) >show avc protocol-pack version
AVC Protocol Pack Name: Advanced Protocol Pack
AVC Protocol Pack Version: 1.0
```

Use the show command to view the current Nbar2 Engine Version

(Cisco Controller) >show avc engine version AVC Engine Version: 13

Before installing the Protocol Pack the default pack will show as follow:



After installing the Protocol Pack the AVC pack will show as ver 4.10001:



Debug Commands

(Cisco Controller) >debug avc events enable (Cisco Controller) >debug avc error enable

Configure Application Visibility

Complete these steps:

- 1. Open a web browser on the Wired Laptop. Enter your WLC IP Address.
- 2. Create an OPEN WLAN with naming convention as for example: "POD1-Client" and enable Application Visibility on that WLAN under QOS TAB. Map this WLAN to management interface.

To enable Application visibility, click **WLAN ID** and then click the QOS tab and check the enable option for **Application Visibility** and click **Apply**.

ဂျက်က င၊sco		<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT
WLANs	WLANs>	New				
WLANS WLANS	Type Profile Na	me	WLAN POD1	-Client		
Advanced	SSID		POD1	-Client		
	ID		1	~		

CISCO MONITOR	Sa <u>v</u> e Configuration <u>P</u> ing Lo <u>WL</u> ANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMA	igout <u>R</u> efresh ANDS HE <u>L</u> P
WLANS	WLANs > Edit 'POD1-Client' < Back	Apply
WLANs Advanced	Quality of Service (QoS) Silver (best effort) V Application Visibility V Enabled AVC Profile none V Netflow Monitor none V	

3. Once Application Visibility is enabled on the specific WLAN, from the associated wireless client start different types of traffic using the applications (already installed) like Cisco Jabber/WebEx Connect, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, Microsoft Messenger, YouTube, Ping, Trace route, etc. Once traffic is initiated from wireless client, visibility of different traffic can be observed globally for all WLANs, Per Client Basis and Per WLAN Basis which provides a good overview to the administrator of the network bandwidth utilization and type of traffic in the network per client, per wlan, and globally.

As mentioned above Visibility of traffic can be monitored:

- Globally for all WLANs
- Individual WLAN
- Individual Client
- 4. To check the visibility globally for all WLANs on WLC, click and scroll down.

MONITOR	WLANS	CONTROLLER	WIRELES	SS SE	CURITY MANAGEMENT	COMMANDS	HELP FE	EDBACK
_		-		-	AAA Authentication Fai	lure for UserNan	ne:c84c7579f45	d User Type: 1
Access Poi	nt Sum	mary			View All			
	Total	Up	Down		Top Applications 👉			
802.11a/n Radios	1	• 1	0	Detail	Application Name		Packet Count	Byte Count
802.11b/g/n	1	• 1	0	Detail	http	(U)	1216	0
All APs	1	• 1	0	Detail		(D)	2210	3164720
					youtube	(U)	846	21806
						(D)	1495	1919261
client Sum	mary				ssl	(U)	186	19344
Current Clier	nts	4		Detail		(D)	214	154042
Excluded Clie	ents	0		Detail	skype	(U)	525	11189
Disabled Clie	nts	0		Detail		(D)	561	24614
					ms-live-accounts	(U)	33	3364
						(D)	28	13588
					ping	(U)	90	5760
						(D)	90	5760
					dns	(U)	7	305
						(D)	7	2590
					yahoo-voip-over-sip	(U)	1	86
						(D)	1	0
					webex-meeting	(U)	3	37
						(D)	3	37
					росо	(U)	3	40
						(D)	2	0

<u>Note</u>

I

The monitor screen list the applications classified by NBAR engine running on WLC for all the WLANs. The top ten applications in the last 90 seconds in both Upstream (U) and Downstream (D) directions will be listed on this page.

5. To have more granular visibility per WLAN, navigate to **Monitor > Applications**. This page will list all the WLANs on which AVC visibility is enabled.

ululu cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Monitor	WLANs								
Summary	WLAN ID	Туре	Profile Name		WLAN	SSID	Admi	n Status	Avc Profile
▶ Access Points	1	WLAN	POD1-Client		POD1-0	lient	Enabl	ed	None
▶ Cisco CleanAir									
▶ Statistics									
▶ CDP									
▶ Rogues									
Clients									5
Multicast									
Applications									Č.

Now click the individual WLAN ID and the below screen will be visible which will list aggregate data for the top ten applications running on that particular WLAN.

Ns > Application \$	Statistics							
lication Last 90 Secs	n Downstr	eam			Application Cumulative	Stats	-	
App Name	Packet	Byte Count	Average Packet Size	Usage (%)	App Name	Packet Count	Byte Count	Usage(%)
stalk-chat	25	4010	160	28.86	VNC	546	529017	67.72
aboo-messenger	9	3671	407	26.42	http	163	132199	16.92
webex-meeting	7	3232	461	23.26	gtalk-chat	222	55448	7.10
ttp	19	2734	143	19.68	webex-meeting	93	48925	6.26
ittorrent	6	204	34	1.47	yahoo-messenger	41	14684	1.88
une.	9	43	4	0.31	bittoment	25	881	0.11
		gt/	sik-chat(28.86%))			vnc(67	.72%)
		ya we	bex-meeting(23.)	26.42%) 26%)			gtalk-cf	5.92%) hat(7.10%) meeting(6.26%)

This page will provide more granular visibility per WLAN and will list the top ten applications in last the 90 seconds, as well as cumulative stats for the top ten applications. The above screen lists the aggregate traffic on a particular WLAN, which includes upstream as well as downstream data. You can view UPSTREAM and DOWNSTREAM stats individually per WLAN from same page by clicking the **Upstream** and **Downstream** tab.

6. To have further granular visibility of the top ten applications per client on a particular WLAN on which AVC visibility is enabled, navigate to **Monitor > Clients** and click any individual client MAC entry listed on that page.

ululu cisco		ROLLER WIRELESS	SECURITY MA	NAGEMENT COMMANDS	ration Ping	Logou	t <u>B</u> efr
Monitor	Clients				Entr	ies 1 - 1	1 of 1
Summary Access Points Cisco CleanAir	Current Filter M	ione (Change)	ilter) (Clear Filter) WLAN Prof	ile WLAN SSID	Status	Auth	Port
 Statistics CDP Rogues 	00:40:96:b9:25:60 POD1-AP	2	POD1-Clien	t POD1-Client	Associated	Yes	1
Clients							

After clicking on an individual client MAC entry listed on the above page, the client details page will open which will have two tabs; one for general information and another tab with the name **AVC Statistics**. Click the **AVC Statistics** tab to see the NBAR statistics for the top ten applications for that particular client.

	-					
eneral AVC Statistic	5					
Aggregate Upstream	Downstrea	m				
Lact 00 Poor Ptate				Cumulating State	-	_
Last 90 Secs Stats	•			Cumulative Stats	•	
Last 90 Secs Stats	Average Packet Size	Packet Count	Byte Count	Cumulative Stats	Packet Count	Byte Cour
Last 90 Secs Stats Application Name gtalk-chat	Average Packet Size 174	Packet Count 25	Byte Count 4010	Cumulative Stats Application Name vnc	Packet Count 555	Byte Cour 529060
Last 90 Secs Stats Application Name gtalk-chat yahoo-messenger	Average Packet Size 174 611	Packet Count 25 10	Byte Count 4010 3671	Application Name	Packet Count 555 194	Byte Cou 529060 136257
Last 90 Secs Stats Application Name gtalk-chat yahoo-messenger webex-meeting	Average Packet Size 174 611 646	Packet Count 25 10 7	Byte Count 4010 3671 3232	Cumulative Stats Application Name vnc http gtalk-chat	Packet Count 555 194 247	Byte Cou 529060 136257 59458
Last 90 Secs Stats Application Name gtalk-chat yahoo-messenger webex-meeting http	Average Packet Size 174 611 646 245	Packet Count 25 10 7 21	Byte Count 4010 3671 3232 2942	Cumulative Stats Application Name vnc http gtalk-chat webex-meeting	Packet Count 555 194 247 100	Byte Cou 529060 136257 59458 52157
Last 90 Secs Stats Application Name gtalk-chat yahoo-messenger webex-meeting http bittorrent	Average Packet Size 174 611 646 245 68	Packet Count 25 10 7 21 6	Byte Count 4010 3671 3232 2942 204	Cumulative Stats Application Name vnc http gtalk-chat webex-meeting yahoo-messenger	Packet Count 555 194 247 100 51	Byte Court 529060 136257 59458 52157 18355

This page will provide further granular stats per client associated on WLAN on which Application Visibility is enabled and will list the top ten applications in last 90 seconds as well as cumulative stats for top ten applications. The above screen lists the aggregate traffic per client, which includes upstream as well as downstream stats. You can view UPSTREAM and DOWNSTREAM stats individually per client from same page by clicking the **Upstream** and **Downstream** tab.

Configure AVC Profile

Complete these steps:

- The NBAR feature on a WLC not only gives a visibility of applications running in the network, but also gives the administrator an option to control the applications running in the network by creating an AVC profile. AVC profiles can be configured to take the following actions on the recognized applications:
 - a. Action DROP (Traffic for that application will be dropped)
 - **b.** Action MARK (Particular applications can be marked with different QOS profiles available on WLC, or the administrator can custom define the DSCP value for that application)
- To see all the applications supported by NBAR engine for stats, visibility and control action (DROP/MARK), navigate to Wireless > Application Visibility And Control > AVC Applications. This page will list down all the applications in sorted order with the application group they belong.

aludo				ation P	ing Logout <u>R</u> efr
CISCO	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MA	NAGEMENT C <u>O</u> I	MMANDS	HELP FEEDBA
Wireless	AVC Applications			En	tries 1 - 50 of 51
Access Points All APs Redios 802.11a/p/ac	Current Filter None	[Change Filter] [Cl	ear Filter]	H	⊲ 1 <u>2</u> ⊳ ₩
802.11b/g/n Dual-Band Radios Global Configuration	Application Name	Application Group	Application ID	Engine ID	Selector ID
Advanced	3com-amp3	other	538	3	629
Mach	3com-tsmux	obsolete	977	3	106
Piesii RE Deofilos	300	layer3-over-ip	788	1	34
ElexConnect Crouns	<u>914c/q</u>	net-admin	1109	3	211
FlexConnect ACLs	9pfs	net-admin	479	3	564
▶ 802.11a/n/ac	acap	net-admin	582	3	674
▶ 802.11b/g/n	acas	other	939	3	62
Media Stream	accessbuilder	other	662	3	888
Application Visibility	accessnetwork	other	607	3	699
And Control	aco	other	513	3	599
AVC Applications	acr-nema	industrial-protocols	975	3	104
Country	active-directory	other	1194	13	473
Timers	activesync	business-and-productivity-tools	1419	13	490
 Netflow 	adobe-connect	other	1441	13	505
E Oas	aed-512	obsolete	963	3	149
F Q05	afpovertop	business-and-productivity-tools	1327	3	548
	agentx	net-admin	609	3	705
waterint wold(0):	alpes	net-admin	377	3	463

While creating the drop/mark action for any application under AVC profile, application group need to be selected first. This page list down all the applications with application group they belong and with simple lookup for application using browser "FIND" option, an administrator can find applications and its group and use this group in AVC profile to configure drop/mark action which is discussed further in this guide. NBAR on WLC supports visibility of 1054 different applications.

To configure any action (drop/mark), the AVC profile should be created first. To configure the AVC profile, navigate to Wireless > Application Visibility And Control > AVC Profiles and then click New to create the AVC profile.

1

	ာါကျက cisco	MONITOR	<u>₩</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	Logout <u>R</u> e
w	ireless	AVC Pro	file Name	•						1	New
•	Access Points All APs Radios 802.11a/n 802.11b/g/n Dual-Band Radios Global Configuration	AVC Profi	le Name						-		
Þ	Advanced										
	Mesh										
	RF Profiles										
	FlexConnect Groups FlexConnect ACLs										
Þ	802.11a/n										
Þ	802.11b/g/n										
E	Media Stream										
*	Application Visibility And Control AVC Applications AVC Profiles										

4. Enter AVC profile name and click Apply.

								L	.ogout <u>R</u> efres
MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
AVC Prof	file > Nev	v						-	Apply
AVC Profi	le Name	Block_Youtube							36 1600

5. After Apply is clicked, the AVC profile will be created and you can see the above-created profile, which can be clicked further to create rules to take drop/mark action. Maximum of 16 AVC profiles can be created on a WLC.

،،ا،،،ا،، cısco	MONITOR WLANS	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Wireless	AVC Profile Name					
Access Points	AVC Profile Name					
* Kadlos 802.11a/n	Block Youtube	-				
802.11b/g/n Dual-Band Radios Global Configuration						

6. After creating the AVC profiles, you can click on any profile name and create rules for individual profiles. Maximum of 32 rules can be configured in each profile. Rules can be configured to take any of the two actions i.e. DROP or MARK. If no rule is configured for any application the default action will be "Allow" with QOS policy configured on a WLAN. To create rules under profile, navigate to **Wireless > Application Visibility And Control > AVC Profiles** and then click any of the above created profile.

									Ping Logout Refrest
MONITOR	<u>W</u> LANs		LLER V	NIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
AVC Profil	e > Edit	Block	_Youtul	be'					Add New Rule
Application Name	Applio	cation Name	Action	DSCP					
									4
									ų

7. Now click **Add New Rule** and the below page (2nd screenshot) is displayed where the administrator can select the application group from the first drop-down which filters the applications that belong to that group only. Then, from the second drop-down application can be selected. Once the application is selected from second drop down, the administrator can select what action should be taken on that application from third the drop-down. Once the action is selected click **Apply**.

									Ping Logout <u>R</u> efrest
MONITOR	<u>W</u> LANs		LLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
AVC Prof	ile>Edit	t 'Block	_Youtu	be'			/	~	Add New Rule
Name	Grou	o Name	Action	DSCP					94 19 19

	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	Logout <u>R</u> efrest
AVC Prof	file > Rule	e > 'Block_You	utube'					Apply
Application	Group	voice-and-vid	eo	× 🔶			/	
Application I	Name	youtube	× -	<u> </u>				
Action		Drop ⊻ 🔶	_					



In 7.5 release, WLC is capable of classifying 1054 applications and provide an option to take any action. To take an action on any application, the administrator has to select application group first to which that application belongs which will filter the list of applications for that application group only. The reason for this implementation is all 1054 applications cannot be displayed in a single drop-down. Also in release 7.5, the Application Names are now selectable and by hovering over and clicking the application name in the list the above profile rule can be created.

ahaha							Sa <u>v</u> e Co	nfiguration P	ing Log	out <u>R</u> efresh
CISCO		MONITOR			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Minelana	^	xnet			layer3-over-ip		770	1	15	_
wireless		xns-auth			email		936	3	56	
▼ Access Points		xns-ch			business-and-p	productivity-to	ols 934	3	54	
All APs		xns-courier	5		email		1010	3	165	
 Kadios 802.11a/n/ac 		xns-idp			layer3-over-ip		776	1	22	
802.11b/g/n		xns-mail			email		937	3	58	
Global Configuration		xns-time			net-admin		932	3	52	
Advanced		xtp			layer3-over-ip		790	1	36	
Mesh		xvttp			other		422	3	508	
RF Profiles		xwindows			net-admin		45	3	6000	
FlexConnect		xyplex-mu	x		other		1018	3	173	
Groups		yahoo-mail	1		email		1462	13	526	
FlexConnect ACLs		yahoo-mes	senger	11	instant-messa	ging	77	13	77	
▶ 802.11a/n/ac		yahoo-voip	messenge	a //	voice-and-vide	:0	674	13	422	
▶ 802.11b/g/n		yahoo-voip	-over-sip		voice-and-vide	:0	1195	13	302	
Media Stream		youtube			voice-and-vide	:0	82	13	82	
Application	μ	z39.50		9	business-and-p	productivity-to	ols 1108	3	210	
Control		zannet			file-sharing		1157	3	317	
AVC Applications		zattoo			voice-and-vide	10	115	13	428	
Country	~	zserv			other		763	3	346	

8. After Apply is clicked, the action rule will be created and displayed as captured in the below screen. You can add more rules under the AVC profile on the same page. Maximum of 32 rules can be configured in a single AVC profile.

										Logout Refresh	
MONITOR	WLANs		WIRELESS	SECURITY	MANAC	SEMENT	COMMANDS	HELP	FEEDBACK		
AVC Pro	file > Edi	t 'Block_Yo	utube'							Add New Rule	
Applicatio	n Name	Applicat	ion Group Nam	e Action	DSCP						
youtube		voice-an	d-video	drop	NA						25
											361

9. Another rule can be configured under the same AVC profile to MARK traffic with a different QOS profile or custom DSCP value. In this example, another AVC profile was created following step 3, 4 and 5 with the name "Mark_Http_Webex". In this example this AVC profile is used to create a rule to mark "Http" with low priority and give "Webex" more precedence.

<u>M</u> ONITOR	<u>W</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
AVC Prof	īle Name	1						
AVC Profil	e Name							
Block Yout	ube		2					
<u>Mark Http</u>	Webex	6	•					

As discussed in previous steps 6, 7 and 8, click the AVC profile name to create rules for the profile. Click **Add New Rule.**



Select Application group from the first drop-down and Application name as **Webex** from second drop-down. Then, configure Action as **MARK** and select QOS profile as **Platinum** and the click **Apply**.

								Logout <u>R</u> efre
MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
AVC Prof	file > Rul	e > 'Mark_Http	_Webex'				_	Apply
Application	Group	voice-and-vide	eo	v 🔶				
Application I	Name	webex-meetin	g 🗸					-
Action		Mark 💌 ┥	_					54
Dscp (0 to 6	53)	Platinum(voice) 🗸					55.1

After **Apply** is clicked, the action rule will be created and displayed as captured in below screen. Click **Add New Rule** on same page to create another rule to MARK another application "Http".

						-	<u> </u>		<u>P</u> ing Logout <u>R</u> efre
MONITOR	<u>W</u> LANs		WIRELESS	SECUR	UTY .	MANAGEMENT	C <u>O</u> MMANDS	HELP	
AVC Prof	īle > Edit	'Mark_Http_	Webex'				_	-	Add New Rule
Applicatio Name	'n	Application Group Nam	n ne	Action	DSCP				
webex-me	eting	voice-and-v	ideo	mark	46				

Create another rule in the same profile by just clicking **Add New Rule** on the same page. Select Application group from the first drop-down and Application name as **http** from second drop-down. Then, configure Action as **Mark** with QOS profile as Bronze. Then click **Apply**.

						10. p	1	Logout <u>R</u> efre
MONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
AVC Prof	īle > Rul	e > 'Mark_Http	_Webex'				-	Apply
Application (Group	browsing		~				
Application M	Name	http	× (_				
Action		Mark 💌 👉						
Dscp (0 to 6	3)	Bronze(backgr	round) 💌					

After **Apply** is clicked, the action rule will be created and displayed as captured in below screen.



For the same AVC profile two rules are created. The Administrator can configure up to 32 rules in the same AVC profile. Individual rules can be configured for action MARK or DROP in the same profile. A single rule can only be configured with a single action i.e. either MARK or DROP.

The administrator is also flexible while configuring Action as MARK to choose the Differentiated Services Code Point (DSCP) value as Custom instead of selecting "Platinum/Gold/Silver/Bronze". Once Custom is selected as DSCP value, a text filed will be visible where admin can enter a custom DSCP value in range of 0 - 63.

AVC Profile > Rule > 'Mark_Http_Webex'									
Application Group	browsing	~							
Application Name	flash-video 💌								
Action	Mark 💌								
Dscp (0 to 63)	Custom	v 0							
		99							

10. The Next step will be to apply these AVC profiles on the WLAN. Only one AVC profile can be mapped to a single WLAN. A single AVC profile can be mapped to multiple WLANs. Once an AVC profile is mapped to a WLAN and if it has a rule for MARK action, that application will get precedence as per QoS profile configured in AVC rule interacting with the QOS profile configured on the WLAN. All the AVC profiles created will be visible under AVC Profile drop-down in WLAN under QOS TAB. To see the AVC profile in the drop-down on WLAN, navigate to WLANs > WLAN ID and then click QOS tab. All the AVC profiles created are visible under the AVC Profile drop-down. The administrator can select the AVC profile on the WLAN as per network requirement.

uluilu cisco		<u>W</u> LANs		WIRELESS	SECURITY	Saye Co MANAGEMENT	nfiguration <u>P</u> in C <u>O</u> MMANDS	g Logout <u>R</u> efresh HELP <u>F</u> EEDBACK
WLANs		WLANs >	Edit 'POD1	-Client'			< Back	Apply
WLANS	is	General	Security	QoS I	Policy-Mapping	Advanced		
▶ Advan	iced	Quality	of Service (QoS) Silver	(best effort)	~		<u>^</u>
		Applica	ation Visibility	🗹 Enal	bled		-	
		AVC Pr	rofile • Monitor	none	~			
		Override	e Per-User Ba	ndwic Mark	Youtube) 16		
				DownStre	eam UpStrea	m		
		Average	e Data Rate	0	0			

11. For example, select the AVC profile **Block_Youtube** from the drop-down and click **Apply.**

ahaha				nfiguration <u>P</u> ing	Logout <u>R</u> efresh
	ITOR <u>W</u> LANS <u>C</u> ONTROLLER V	NIRELESS SECURITY	MANAGEMENT	COMMANDS HE	P EEEDBACK
WLANs	WLANs > Edit 'POD1-CI	ient'		< Back	Apply
 ₩LANs WLANs Advanced 	General Security Quality of Service (QoS) Application Visibility	QoS Policy-Mapping Silver (best effort)	Advanced		^
	AVC Profile Netflow Monitor	Block_Youtube	1 20		

Note

If Application visibility is not enabled on the WLAN, and users selects an AVC profile and Apply is clicked, this automatically enables Application visibility. But to disable Application visibility from WLAN, AVC profile, which is mapped to WLAN, should be removed first by selecting **None** from drop-down.

12. Once AVC profiles are applied on WLAN it is also visible under **Monitor > Applications**. All the WLANs which has Application Visibility enabled will be displayed

ဂျက်၊ cisco	MONITOR	WLANs		WIRELESS	SECURITY	M@NAGEMENT	COMMANDS HELP	EEEDBACK
Monitor Summary	WLANS	Туре	Profile Name		WLAN	SSID	Admin Status	Avc Profile
Access Points	1	WLAN	POD1-Client		POD1-C	lient	Enabled	Block_Youtube
Cisco CleanAir								
Statistics								
▶ CDP								
Rogues								
Clients								
Multicast								
Applications								

13. Now try to open www.youtube.com from wireless clients. Make sure that the client cannot play any videos on YouTube. Also try to open your Facebook account (in case you have one) and try to open any YouTube video from your Facebook account. You will observe YouTube videos cannot be played.

Because YouTube is blocked in the AVC profile and AVC profile is been mapped to WLAN, clients will not be able to access YouTube videos via browser or even via YouTube application or from any other website.

<u>)</u> Note

If your browser was already open and running Youtube.com, refresh the browser for the AVC profile to take effect.

Now change the AVC profile on the WLAN to test the MARK operation of the NBAR feature. Select AVC profile Mark_Http_Webex from the drop-down under QOS tab on the WLAN and click Apply.

 cısco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	Sa <u>v</u> e Cor MANAGEMENT	nfiguration <u>P</u> i C <u>O</u> MMANDS	ng Logout <u>R</u> efre HELP <u>F</u> EEDBA	esh ICK
WLANS	İs	WLANs >	Edit 'POD1	-Client'	Policy-Mapping	Advanced	_ < Back	Apply	^
wLANs ▶ Advan	iced	Quality Applica AVC Pr Netflov	v of Service (QoS ation Visibility rofile v Monitor) Silver Enal Mark_ none	(best effort) bled HTTP_Webex 💙	•		^	

 Once the AVC profiles are applied on the WLAN, it is also visible under Monitor > Applications. All the WLANs which has Application Visibility enabled will be displayed.



16. Once the AVC profile Mark_Http_Webex is applied on the WLAN, initiate or login to your individual WebEx account (if you have one) and also initiate some HTTP connections and observe the marking for these two applications under client details. Once the AVC profile is mapped to a WLAN and if it has a rule for the MARK action, that application will get precedence as per QoS profile configured in AVC rule overriding the QoS profile configured on the WLAN.

Although the WLAN in this example is mapped to the default QOS profile **SILVER**, the AVC profile has been created and mapped to this WLAN to MARK application WebEx and HTTP with a different QOS profile. Traffic for application WebEx will be marked with **PLATINUM** profile and traffic for all HTTP application will be marked with **BRONZE** profile. Rest of the applications that do not match any rules in the AVC profile; will be marked with QOS profile configured on WLAN i.e. SILVER in this example.

17. To see the markings stats for client traffic, navigate to **Monitor > Clients** and then click any individual client MAC entry listed on that page.

. cısco			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	ration Ping	Logou	t <u>R</u> efr
Monitor	Clients						Entri	ies 1 - 1	l of 1
Summary	Current Filter	None	[Change F	ilter] [Clear Fi	iter]				
Access Points Cisco CleanAir	Client MAC Add	AP Name		WLAN	Profile	WLAN SSID	Status	Auth	Port
Statistics	00:40:96:b9:2b:60	POD1-AP		POD1-	Client	POD1-Client	Associated	Yes	1
Rogues Clients	-								

After clicking on the individual client MAC entry listed on the above page, the client details page will open which will have two tabs; one for general information and another tab with name AVC **Statistics**. Click the **AVC Statistics** tab and further click the **UPSTREAM** tab to notice the MARKING operation of the AVC profile.

AVC Statistic	5						
Aggregate Upstrea	Downstre	am					
Last 90 secs Stats					Cumulative Stats		
Application Name	Average Packet Size	Packet Count	Byte Count	Dscp In/Out	Application Name	Packet Count	Byte Coun
gtalk-chat	162	25	4063	0/ 0	vnc	495	473474
vahoo-messenger	734	5	3671	0/0	http	124	128090
have were and a start		6	3232	0/46	webex-meeting	72	40756
webex-meeting	538						
webex-meeting http	538 245	12	2942	0/10 🔶	gtalk-chat	91	12696
webex-meeting http bittorrent	538 245 68	12 3	2942 204	0/10	gtalk-chat yahoo-messenger	91 19	12696 11013

Notice the above output and make sure the WebEx application is getting OUT DSCP value as 46 because the WebEx application is been configured with Platinum QOS profile and HTTP application is getting OUT DSCP value as 10 because the HTTP application is been configured with Bronze profile.

Configure NBAR NetFlow Monitor

A NetFlow monitor can also be configured on the WLC to collect all the stats generated on a WLC and these can be exported to the NetFlow collector. In the following example, Cisco Performance Application Manager (PAM) is shown as being used as a NetFlow collector. PAM is a licensed application running on Cisco Prime Infrastructure.

 Add NetFlow Exporter first on WLC by configuring Exporter (NetFlow collector). In this example Cisco PAM is an exporter. It collects all the NetFlow stats generated by the WLC. To add an exporter in the WLC, navigate to Wireless > NetFlow > Exporter, then click New.



2. Enter the details of PAM, Exporter IP, as an example below 10.10.105.3 and Port Number as 9991 which will collect all the NetFlow stats generated by the WLC and then click **Apply**.

 cısco	MONITOR WLAN	Is <u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	Logout <u>R</u> ef HELP
Wireless	Exporter Creat	9				/	Apply
 Access Points All APs 	Exporter Name	Cisco PAM		-			
▼ Radios	Exporter Ip	10.10.105.3	-	_			
802.11b/g/n	Port Number	9991 🔸					
Exporter List							New
Exporter Name Expo	orter Ip Port Num	er					9
	0.105.3 9991						154
Cisco PAM 10.10							35

 After adding Exporter details on the WLC i.e. PAM server, a monitor needs to be created which will store the NetFlow stats and export the same to the PAM server. To create a Monitor, navigate to Wireless > NetFlow > Monitor, then click New.

<u>Note</u>

	ဂျက်က cisco	MONITOR	<u>W</u> LANs		ER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	Logout <u>R</u> e
W	ireless	Monitor Li	ist page						<u>, 1</u>	New
*	Access Points All APs Radios 802.11a/n 802.11b/g/n Dual-Band Radios Global Configuration	Monitor Na	me Rec	ord Name E	xporter Name	ExporterIp	Port			
Þ	Advanced									
	Mesh									
	RF Profiles									
	FlexConnect Groups FlexConnect ACLs									
Þ	802.11a/n									
Þ	802.11b/g/n									
Þ	Media Stream									
Þ	Application Visibility And Control									
	Country									
	Timers									
*	Netflow Monitor Exporter									2515df

4. Enter any name to create the Monitor entry on WLC and click Apply.

								Logout <u>R</u> efre
MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Netflow N	/lonitor >	New				-	-	Apply
Monitor N	ame Net	Flow Monitor		-	-			

5. Once applied, the Monitor entry will be created which will need to be further mapped to the Exporter created in step 2.

Monitor List page					New
Monitor Name	Record Name	Exporter Name	ExporterIp	Port	
NetFlow Monitor	none	None	0.0.0.0	0	



ſ

Only one Monitor entry can be added in the WLC.

6. Click the Monitor entry and map it to the Exporter entry, which is Cisco PAM. The exporter name drop-down list the "Exporter" entry that is created above. Record name "ipv4_client_app_flow_record" is auto generated by WLC, which records all the NBAR statistics and exports to the Cisco PAM. Select this record entry in the record name drop-down and click Apply.



											Logout Re	
MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK				
Monitor L	.ist page					-				1	New	
Monitor N	ame	Red	cord Name		Exporter Nan	ne	Ехр	orterIp	Port			20
NetFlow Mo	onitor	ipw	4_client_app_fl	ow_record	Cisco PAM		10.1	0.105.3	9991			3515

Once the Monitor entry is created and the Exporter entry is mapped to the same, it should be mapped to the WLAN. To map the exporter entry to WLAN, click WLANs and then click the specific WLAN ID. Click the QOS tab and choose the Monitor entry created above from the NetFlow Monitor drop-down and then click Apply on the WLAN Edit page.

 cisco	Save Co Monitor Wlans Controller Wireless Security Management	onfiguration <u>P</u> ing Logout <u>B</u> efresh C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANS WLANS WLANS Advanced	WLANs > Edit 'POD1-Client' General Security QoS Policy-Mapping Advanced Quality of Service (QoS) Silver (best effort) V Application Visibility Enabled AVC Profile Block Youtube V	< Back Apply
	Override Per-User Bandwidth Contracts (kbps) # DownStream UpStream	a

8. Now open a new tab on the browser and login to the Cisco Prime Infrastructure Server to add individual WLCs to PAM.

Username: XXXXXX Password: XXXXXX

	Cisco Prime Infrastructure Version: 1.4 Username Password Logi	
© 2013 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco S	lystems logo are registered trademarks of Cisco	alialia
Systems,Inc.and/or its affiliates in the U.S and certain other co	suntries	cisco

9. Add the WLC in Cisco PAM. To add WLC into Cisco PAM, login to Cisco PAM and navigate to **Operate > Device Work Center**, then click **Add Device** in the Lifecycle Theme.

uluulu Cisco Prime	ρ.
cisco Infrastructure	🟠 Home Design * Deploy * Operate * Report * Administration * 🛛 🏲 🕄 🚱 - 🌣
Device Work Center	👬 Discovery 🦉 Configuration Archives 👩 Sofhated Deployment Status 😓 Network Aud
Device Group	Device Group > ALL ALL Selected 0 Total 3 😵 🚱 .
S ALL	/ Edit 🗙 Delete 🆓 Sync. Groups & Sites * 😫 Add Device 👔 Bulk Import

10. Enter the details of individual WLC i.e. WLC Management IP Address (Example WLC-POD4 = 10.10.40.2) and **Community String** as public and then click **Add**.

ſ

evice Work Center	Add Device		
Device Group	▼ General Parameters		-
ه	IP Address	x.x.x.x	0
(□• E• · · · · · · · · · · · · · · · · · ·	▼ SNMP Parameters		
🔓 ALL	Version	v2c *	
An Device Type	* Retries	2	
 Site Groups Liser Defined 	* Timeout	10	(secs)
	* Community		
	▼ Telnet/SSH Parameters		
	Protocol	Teinet *	
	Timeout	60	(secs)
	Username		
	Password		
	Confirm Password		
	Enable Password		
	Confirm Enable Password		
	* Http Parameters		-

Once the WLC is added, start some traffic from wireless clients. You can view the number of clients per WLAN and usage per client. To see the usage by clients, navigate to Home > Detail Dashboards > Application. Now filter the Application Box as All, Site as Unassigned, and Network Aware as Wireless > PODX-Client and then click Go.

Issio Prime Isso Infrastructure 😰 Home Design • Deploy • Operate • Rep	Virtual Domen KD	IOT-DOMAIN Heat
Dverview Incidents Performance Detail Deshboards		
Site Device Interface Application Voice/Video End User Experience		
litters 🎨 *Application 📶 📀 🛞 *Time Frame Past 1 Hour 💠 🍙 Site Unassigned	d 💿 🙏 Network Aware POD1-Client 💿 Go	
Fop N Clients (In and Out) 🙏 👔 🐁 🕢 📧	Application Configuration 🤱 🍓 🕢	
	Application Protocol Port	Bytes/sec
	ssi	304.04
10.10.10.56 -	http	52.38
	skype	23.05
	unclassified	13.88
10 10 10 50 -	youtube	9.75
	yahoo-messenger	2.95
	dns	2.44
40	2012 August 08, 17:26:16 15T	

Note

- You can see the number of clients on WLAN "POD1-Client" which is filtered under Network Aware. Also, in same screen, you can see the applications used by both the clients.
- To see the application usage by a particular client, navigate to Home > Detail Dashboards > End User Experience > Under Filter and then select the client IP.



 To see application usage per WLAN, navigate to Home > Detail Dashboards > End User Experience > Under Filter and then select the Network Aware as WLAN i.e. POD1-Client in this example. Click GO.

cisco	Cisco Prime Infrastructure	. 6		Hame Desig	o * Deniny	• 00	arate ¥ Barunt	 Administration 		Virtual	Domain ROOT-	COMAIN
Overview	Incidents	Performance	Detail Dash	boards								
Site	Device	Interface	Application	Voice/Video	End User E	xperience	-				/	
Filters	Client U	nassigned	\$	(*Time Frame	Past 6 Hours	0	Papelication	All C	🔋 🐥 Netw	ork Aware POD1-0	lient (0 60
Top N A	pplications 🚊	(d) [(d) = 1]								0	_	_
	-											
	unclassified -											
	NOD -							1000				
	webex-meeting -											
	skype -											
	youtube							0.000				
1	dns -							Page 144	* 0		for sec.	1000
- n	e-live-accounts -							Source Address	I_ Des	onation Addr 1.	. Source	No da
10	hoo-messenger -											
	Rash-video -											
Jano	ovop-ovo-sp											
	windows abure -											
	non-managements							Worst N Clients	by Transaction	Time		

Web Links and Terminology

ſ

Cisco WLAN Controller Information:

http://www.cisco.com/en/US/products/hw/wireless/products.html http://www.cisco.com/cisco/web/support/index.html Cisco Prime Management Software Information: http://www.cisco.com/en/US/products/ps11686/index.html Cisco MSE Information: http://www.cisco.com/en/US/products/ps9742/index.html Cisco LAP Documentation: 1

http://www.cisco.com/en/US/products/ps10981/index.html