# 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.

**Cisco Systems, Inc.**
www.cisco.com

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=284509011&release=4.0.0&relind=AVAILABLE&rellifecycle=&reltype=latest


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

**Note** 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.
4. 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.

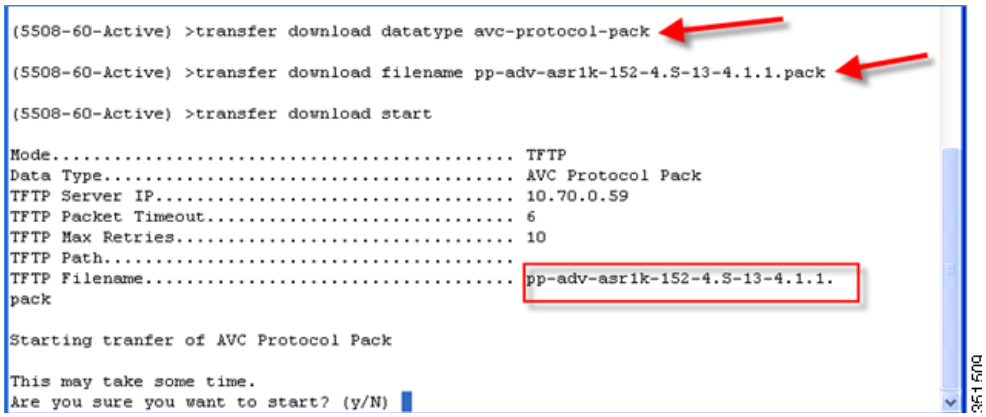
## AVC Operation with Anchor/Foreign Controller's Setup

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:

```
(Cisco Controller) >transfer download datatype avc-protocol-pack
(Cisco Controller) >transfer download start
Mode..............................  FTP
Data Type.........................  AVC Protocol Pack
FTP Server IP.....................  A.B.C.D
FTP Server Port...................  21
FTP Path..........................  /
FTP Filename..................... pp-unified-wng-152-4.S-13-4.1.1.pack
FTP Username......................  cisco
FTP Password......................  *********
Starting transfer of AVC Protocol Pack
This may take some time.
Are you sure you want to start? (y/N)
Y
```



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.
```

351510

### 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:

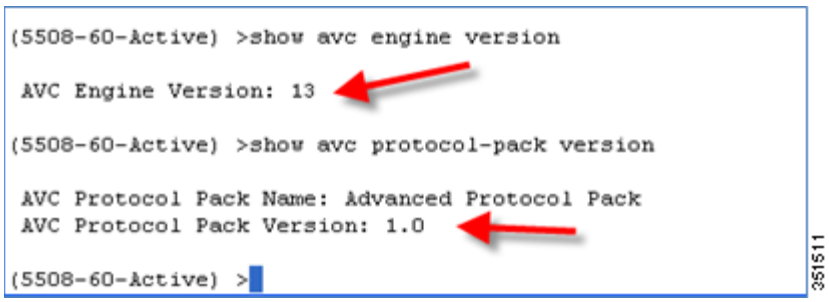
```
(5508-60-Active) >show avc engine version

 AVC Engine Version: 13

(5508-60-Active) >show avc protocol-pack version

 AVC Protocol Pack Name: Advanced Protocol Pack
 AVC Protocol Pack Version: 1.0

(5508-60-Active) >
```



351511

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

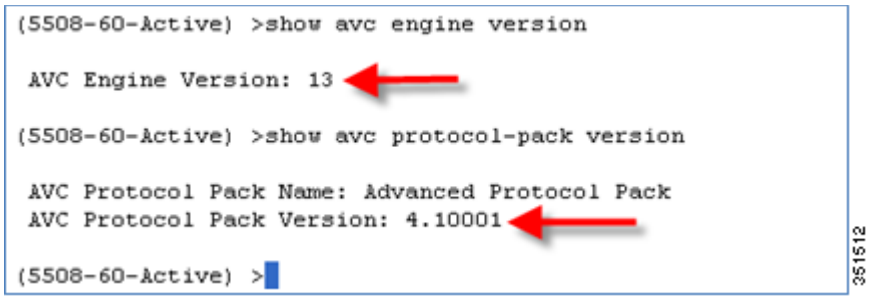
```
(5508-60-Active) >show avc engine version

 AVC Engine Version: 13

(5508-60-Active) >show avc protocol-pack version

 AVC Protocol Pack Name: Advanced Protocol Pack
 AVC Protocol Pack Version: 4.10001

(5508-60-Active) >
```



351512

### Debug Commands

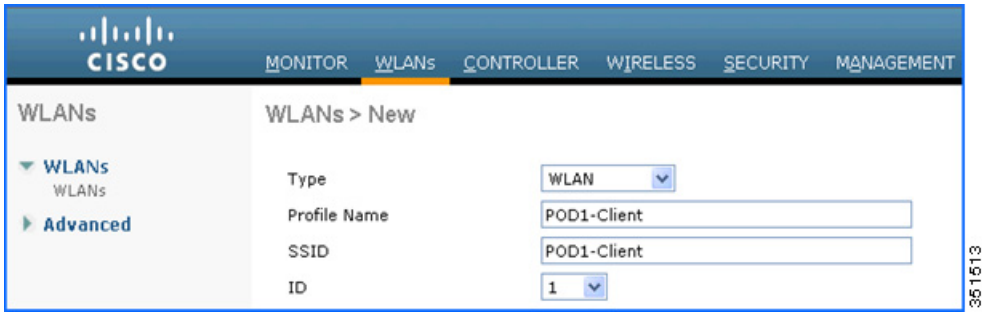
```
(Cisco Controller) >debug avc events enable
(Cisco Controller) >debug avc error enable
```

# 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**.



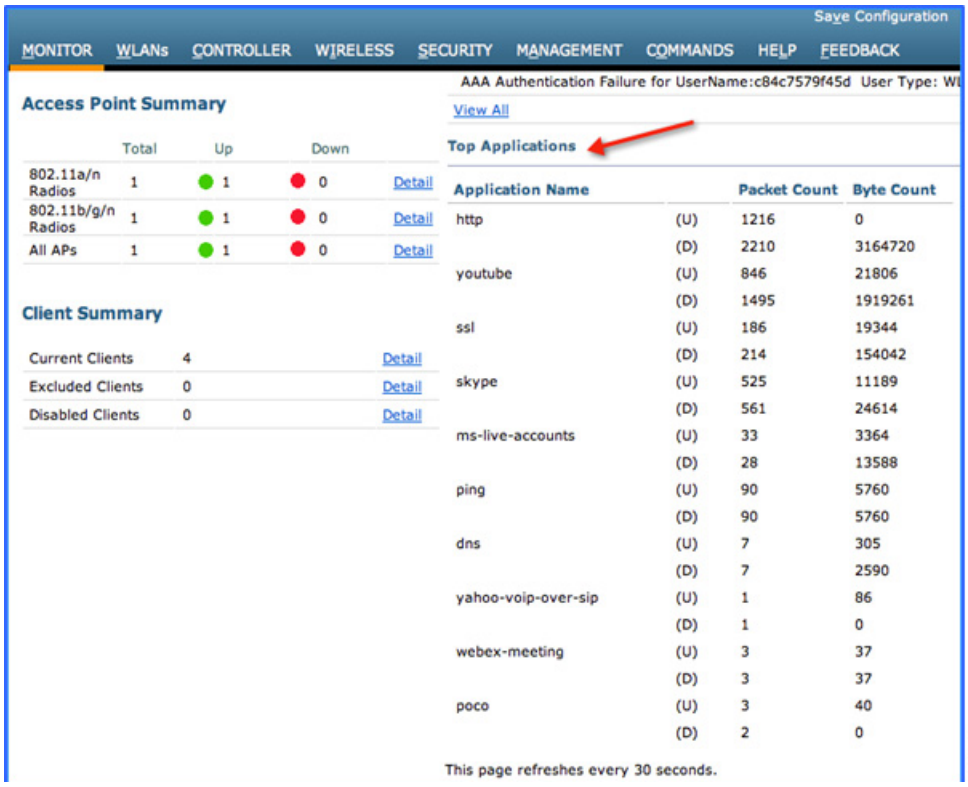


3. Once Application Visibility is enabled on the specific WLAN, from the associated wireless client start different types of traffic using the applications (already installed) like Cisco Jabber/WebEx Connect, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, Microsoft Messenger, YouTube, Ping, Trace route, etc. 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:

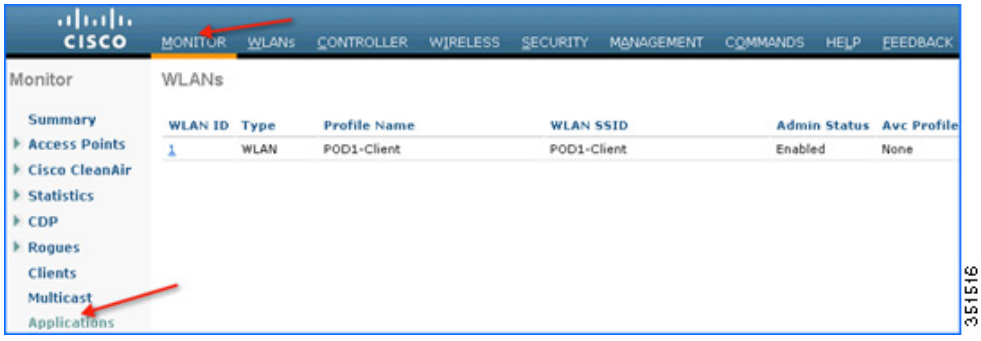
- Globally for all WLANs
- Individual WLAN
- Individual Client

4. To check the visibility globally for all WLANs on WLC, click and scroll down.

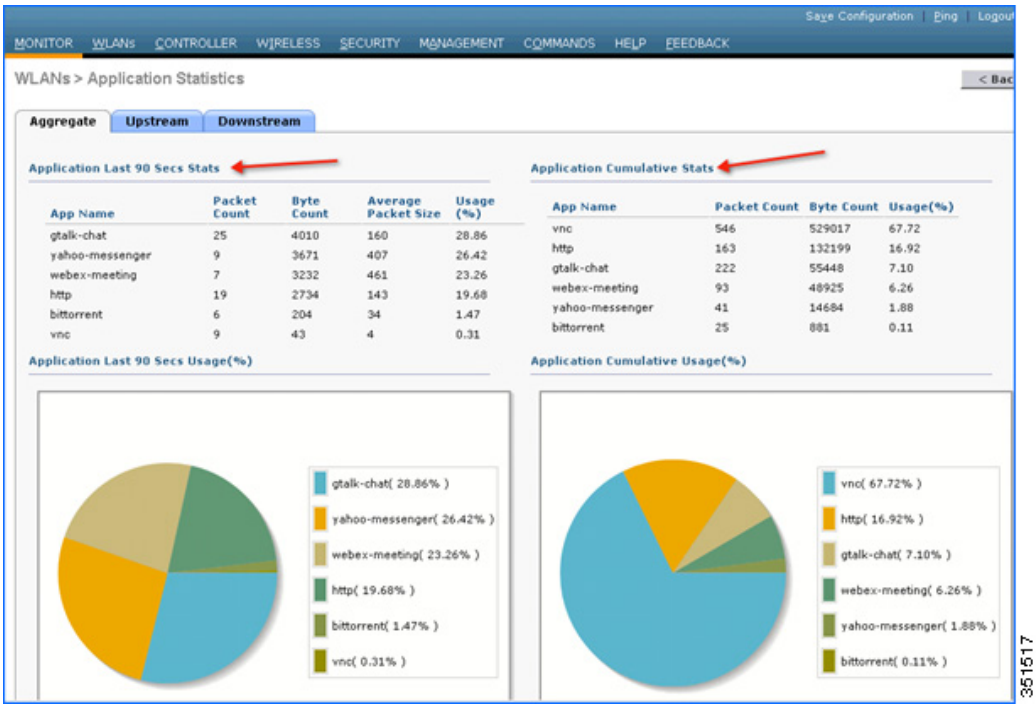



**Note** The monitor screen list the applications classified by NBAR engine running on WLC for all the WLANs. The top ten applications in the last 90 seconds in both Upstream (U) and Downstream (D) directions will be listed on this page.

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.



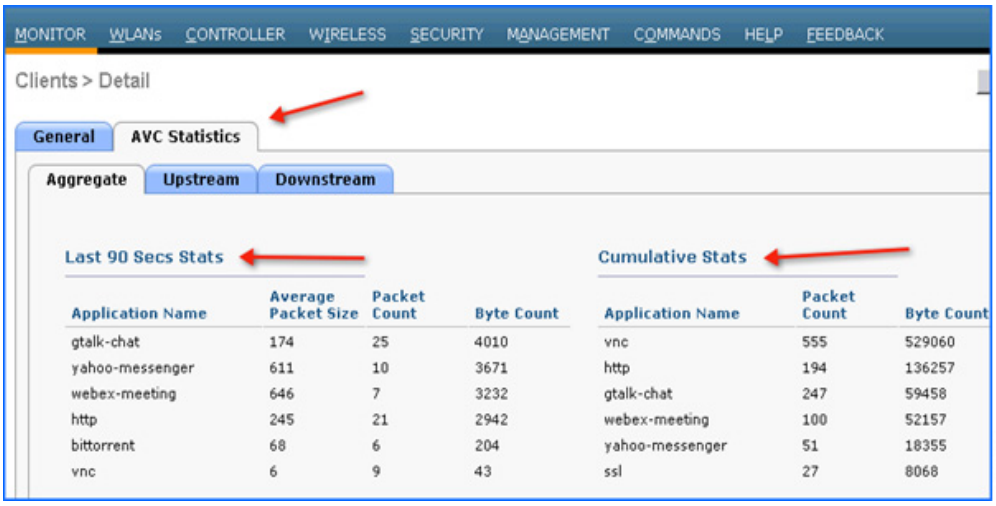

Now click the individual WLAN ID and the below screen will be visible which will list aggregate data for the top ten applications running on that particular WLAN.




**Note** 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.


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.

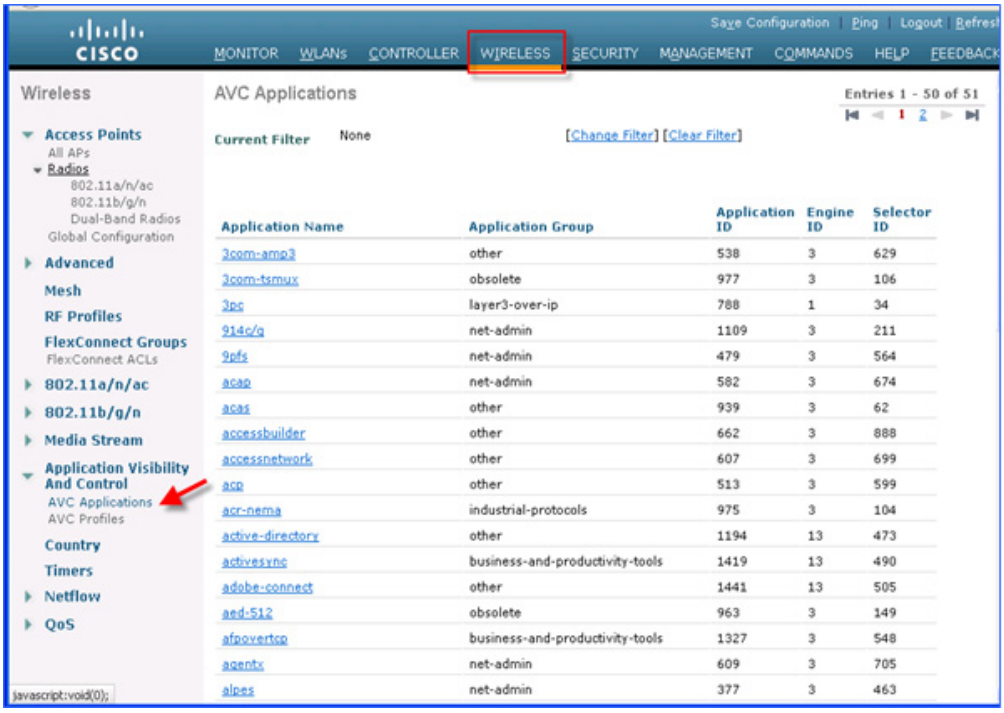



**Note** This page will provide further granular stats per client associated on WLAN on which Application Visibility is enabled and will list the top ten applications in last 90 seconds as well as cumulative stats for top ten applications. The above screen lists the aggregate traffic per client, which 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

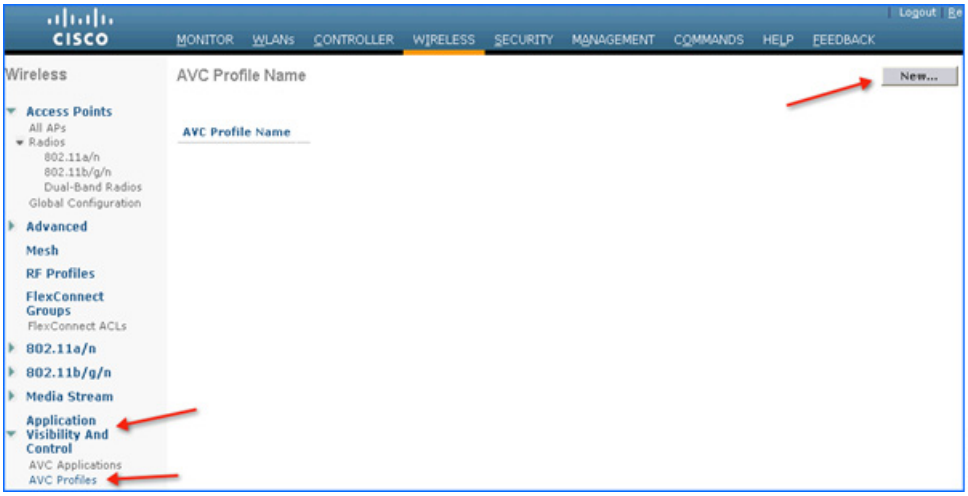
Complete these steps:

1. 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)
2. 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.

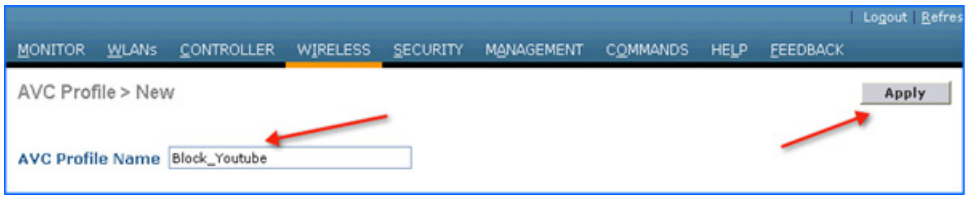



**Note** While creating the drop/mark action for any application under AVC profile, application group need to be selected first. This page list down all the applications with application group they belong and with simple lookup for application using browser "FIND" option, an administrator can find applications 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.

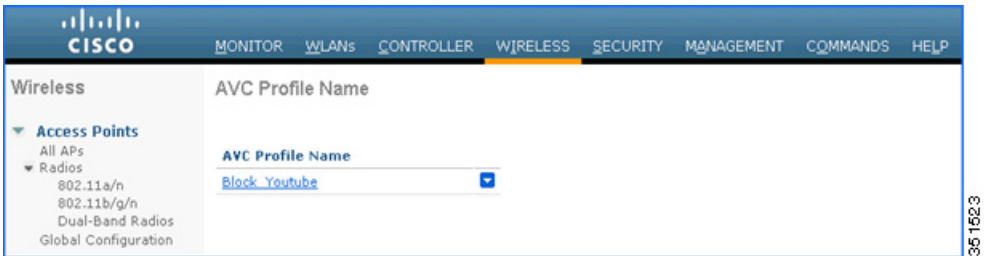
3. To configure any action (drop/mark), the AVC profile should be created first. To configure the AVC profile, navigate to **Wireless > Application Visibility And Control > AVC Profiles** and then click **New** to create the AVC profile.




4. Enter AVC profile name and click **Apply**.

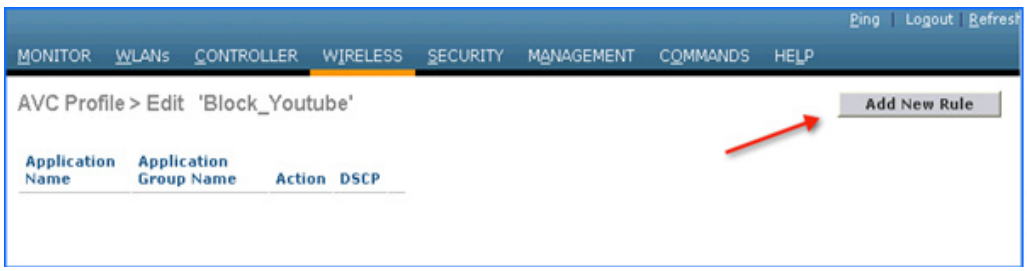



5. After Apply is clicked, the AVC profile will be created and you can see the above-created profile, which can be clicked further to create rules to take drop/mark action. Maximum of 16 AVC profiles can be created on a WLC.

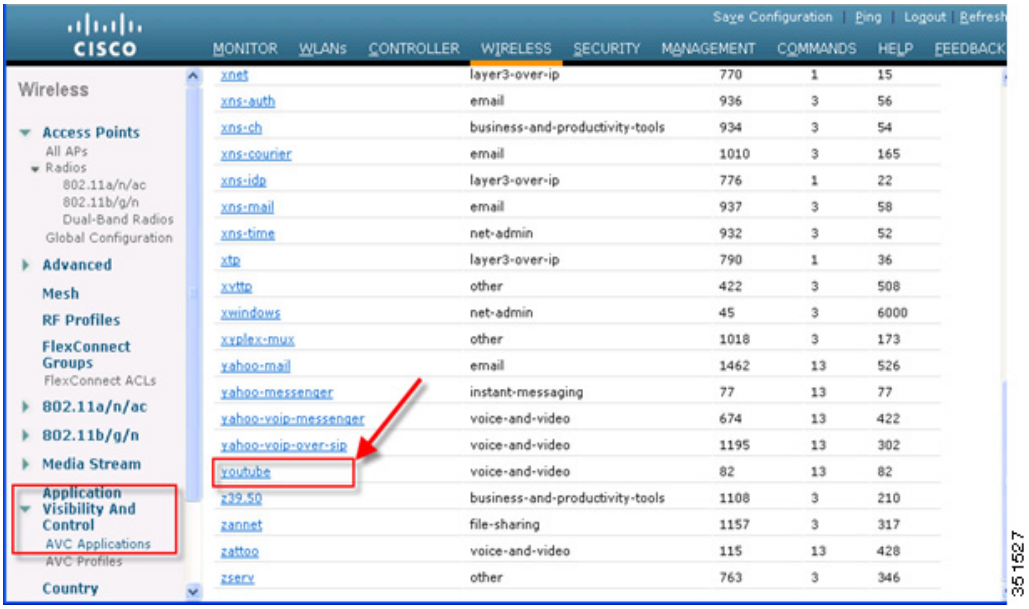



6. After creating the AVC profiles, you can click on any profile name and create rules for individual profiles. Maximum of 32 rules can be configured in each profile. Rules can be configured to take any of the two actions i.e. DROP or MARK. If no rule is configured for any application the default action 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.

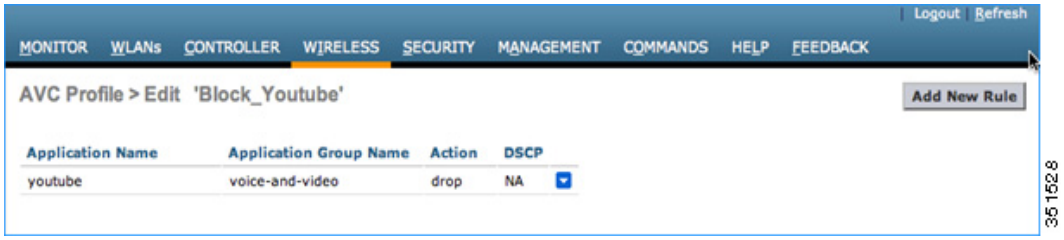

7. Now click **Add New Rule** and the below page (2nd screenshot) is displayed where the administrator can select the application group from the first drop-down which filters the applications that belong to that group only. Then, from the second drop-down application can be selected. Once the application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




**Note** 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.

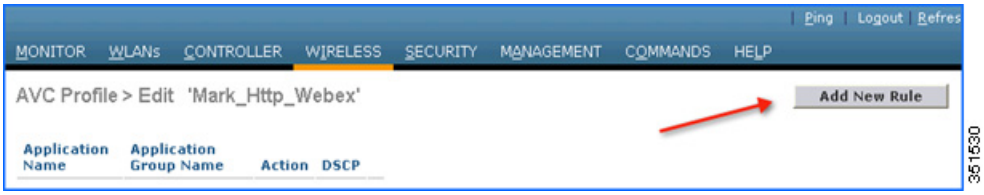



8. After Apply is clicked, the action rule will be created and displayed as captured in the below screen. You can add more rules under the AVC profile on the same page. Maximum of 32 rules can be configured in a single AVC profile.



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.


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**.

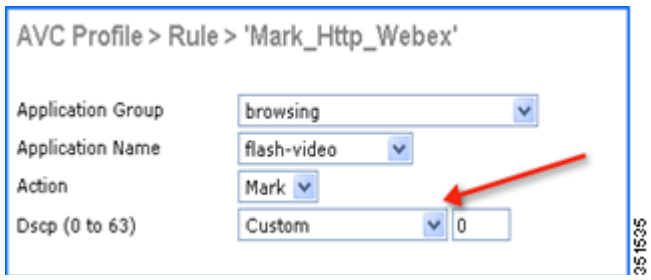

After **Apply** is clicked, the action rule will be created and displayed as captured in below screen. Click **Add New Rule** on same page to create another rule to MARK another application “Http”.


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**.

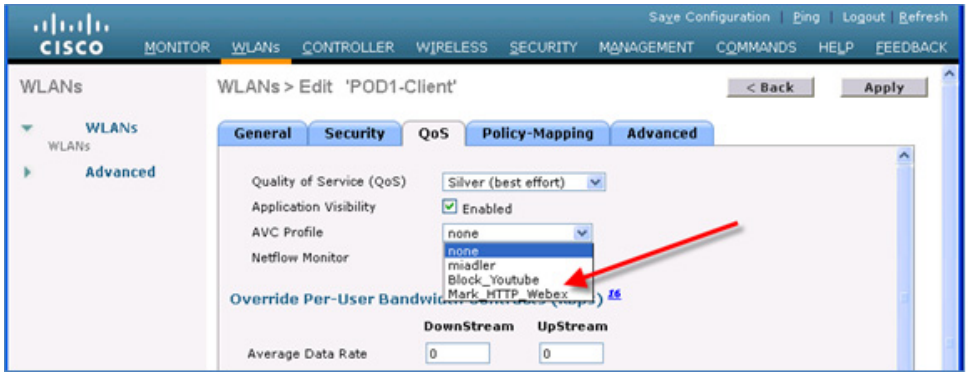

After **Apply** is clicked, the action rule will be created and displayed as captured in below screen.


**Note** 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.

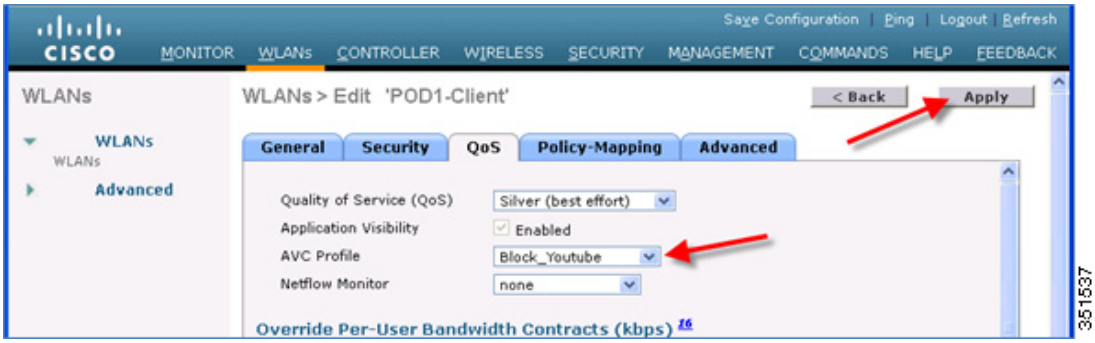
The administrator is also flexible while configuring Action as MARK to choose the Differentiated Services Code Point (DSCP) value as Custom instead of selecting “Platinum/Gold/Silver/Bronze”. Once Custom is selected as DSCP value, a text filed will be visible where admin can enter a custom DSCP value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




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.




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




**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

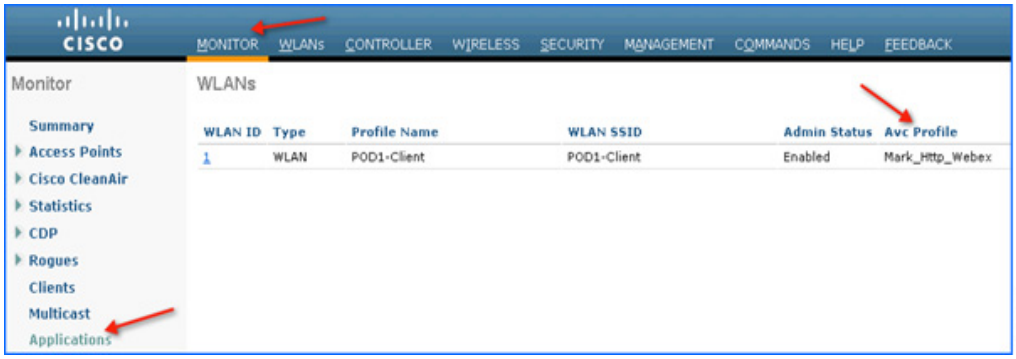

13. Now try to open www.youtube.com from wireless clients. Make sure that the client cannot play any videos on YouTube. Also try to open your Facebook account (in case you have one ) and try to open any YouTube video from your Facebook account. You will observe YouTube videos cannot be played.

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.

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

14. 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.**


15. 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.

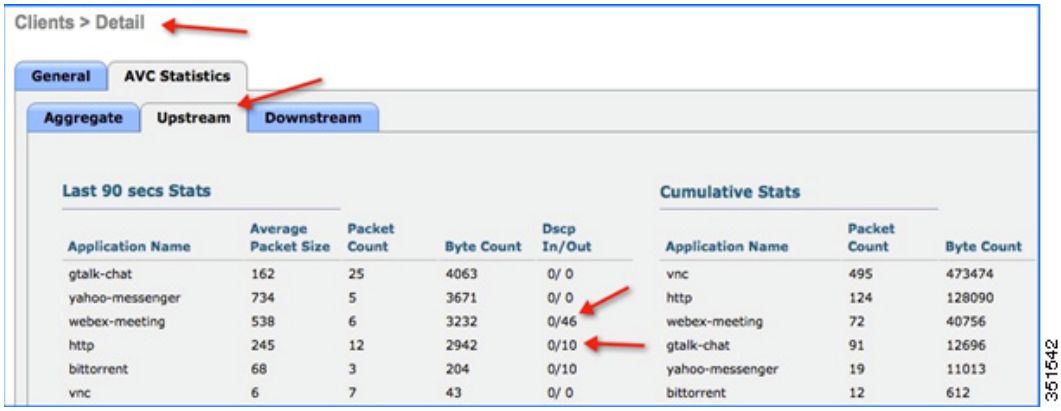



16. Once the AVC profile **Mark_Http_Webex** is applied on the WLAN, initiate or login to your individual WebEx account (if you have one) and also initiate some HTTP connections and observe the marking for these two applications under client details. Once the AVC profile is mapped to a WLAN and if it 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.


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.

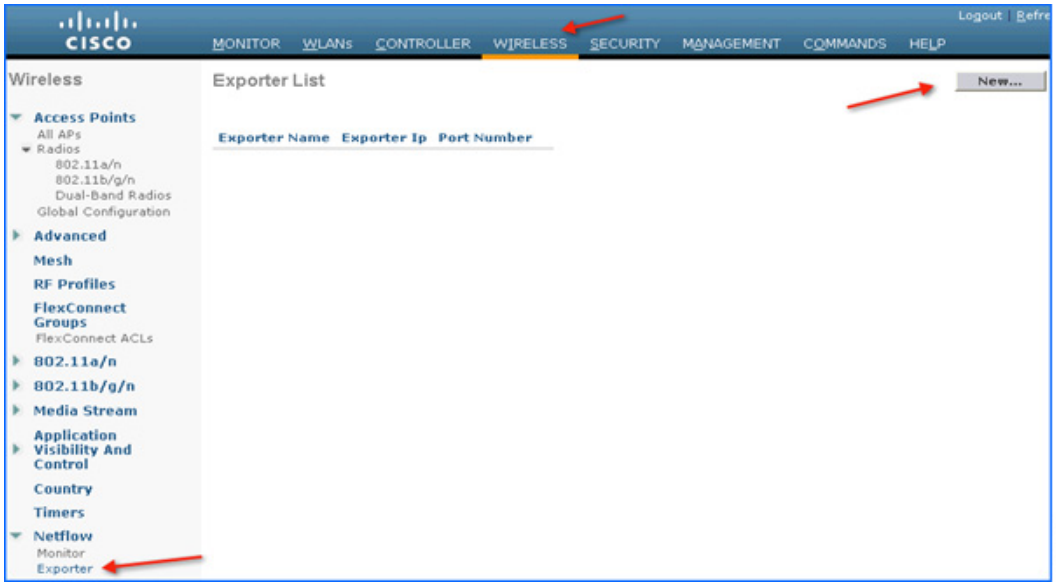



Notice the above output and make sure the WebEx application is getting OUT DSCP value as 46 because the WebEx application is been configured with Platinum QOS profile and HTTP application is getting OUT DSCP value as 10 because the HTTP application is been configured with Bronze profile.

# 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.

1. 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.**

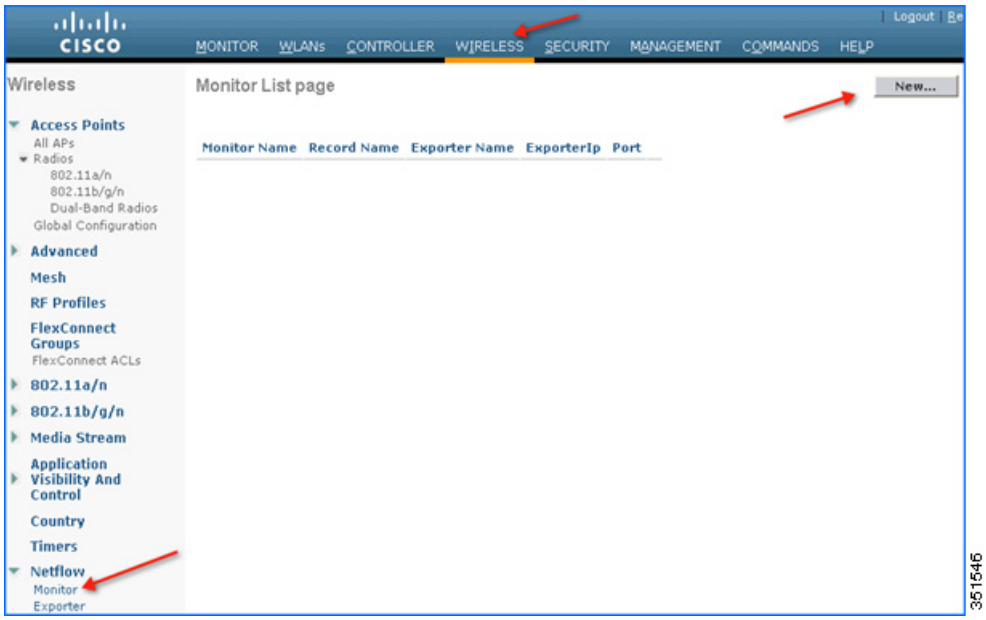



2. Enter the details of PAM, Exporter IP, as an example below 10.10.105.3 and Port Number as 9991 which will collect all the NetFlow stats generated by the WLC and then click **Apply.**

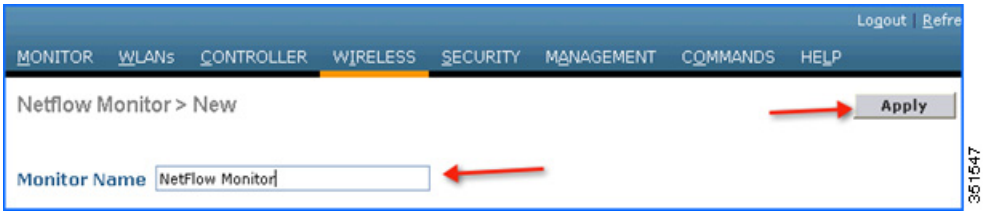


**Note** Only one exporter can be added in the WLC.

3. 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.**



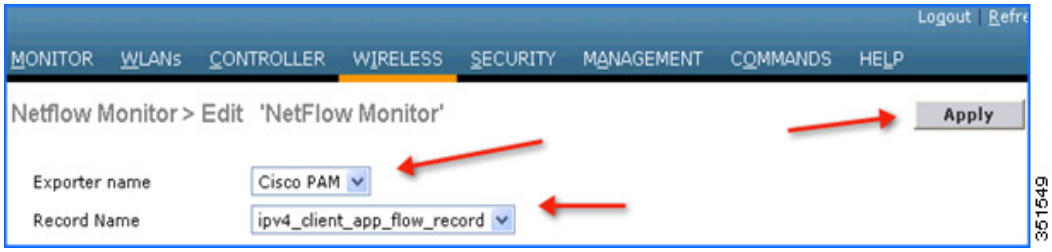

4. Enter any name to create the Monitor entry on WLC and click **Apply**.




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

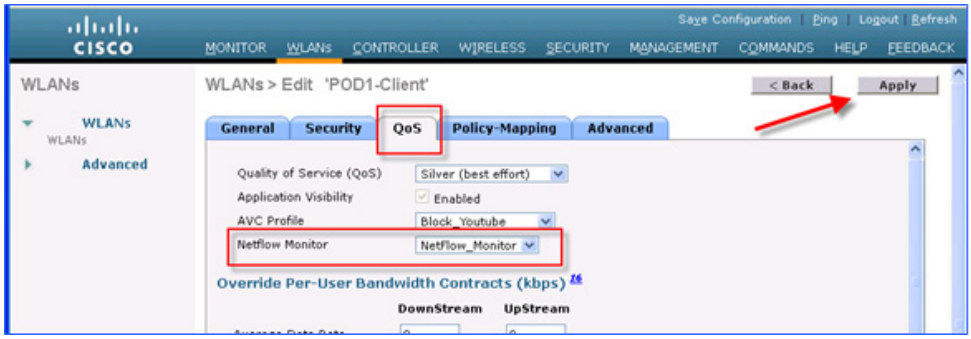

**Note** Only one Monitor entry can be added in the WLC.

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**.





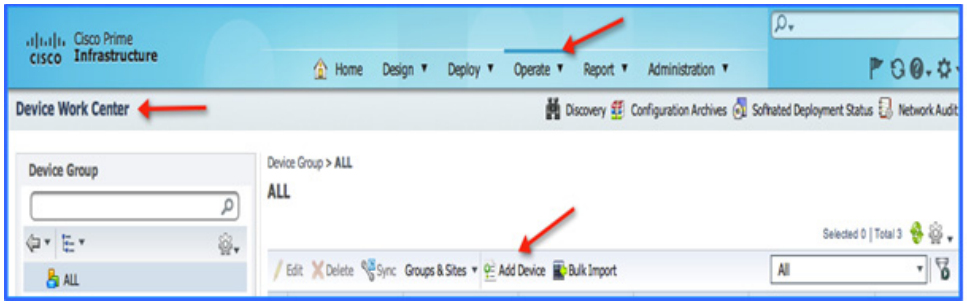
7. Once the Monitor entry is created and the Exporter entry is mapped to the same, it should be mapped to the WLAN. To map the exporter entry to WLAN, click **WLANs** and then click the specific **WLAN ID**. Click the **QOS** tab and choose the Monitor entry created above from the **NetFlow Monitor**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



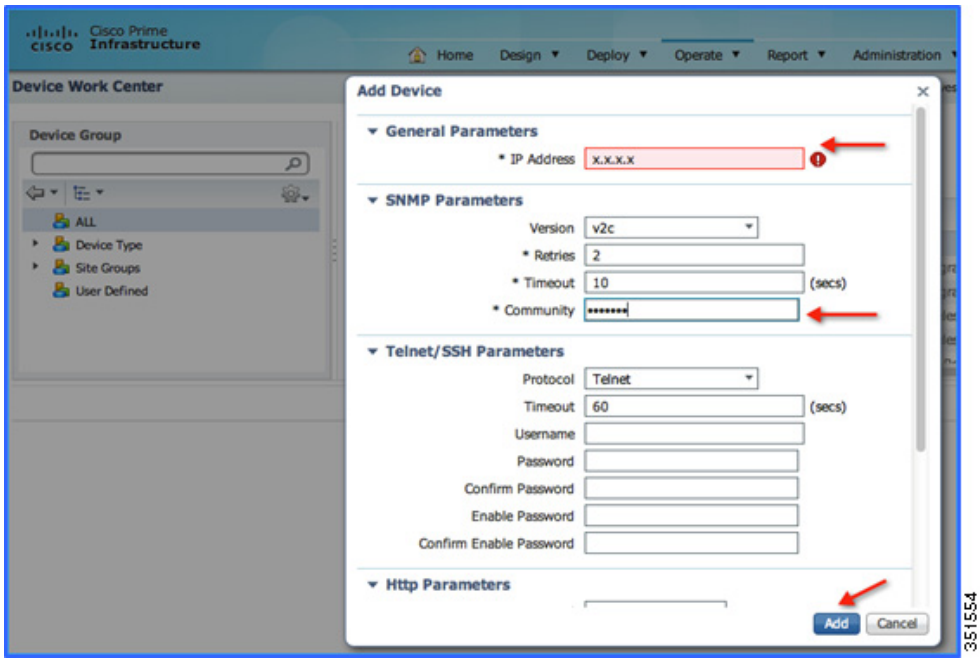

8. Now open a new tab on the browser and login to the Cisco Prime Infrastructure Server to add individual WLCs to PAM.

```
Username: XXXXXX
Password:  XXXXXXX
```

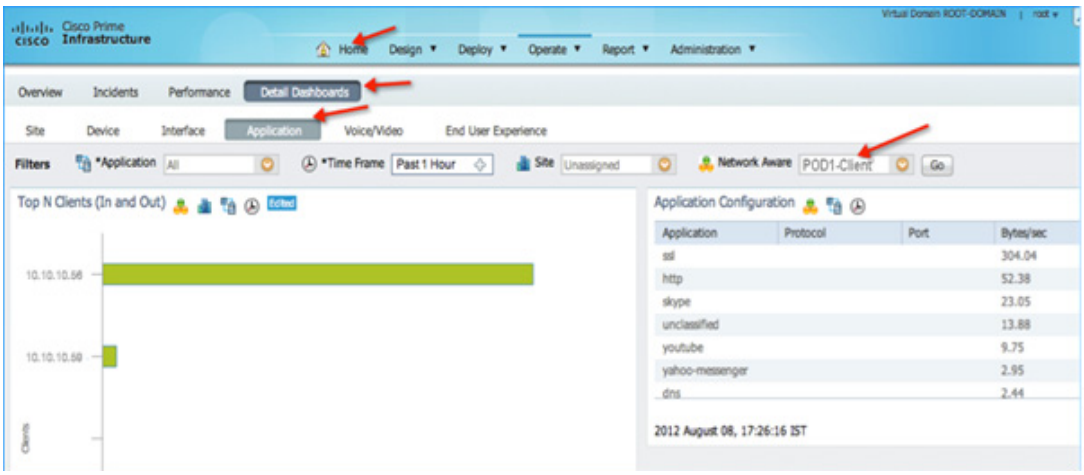

9. Add the WLC in Cisco PAM. To add WLC into Cisco PAM, login to Cisco PAM and navigate to **Operate > Device Work Center**, then click **Add Device** in the Lifecycle Theme.




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**.

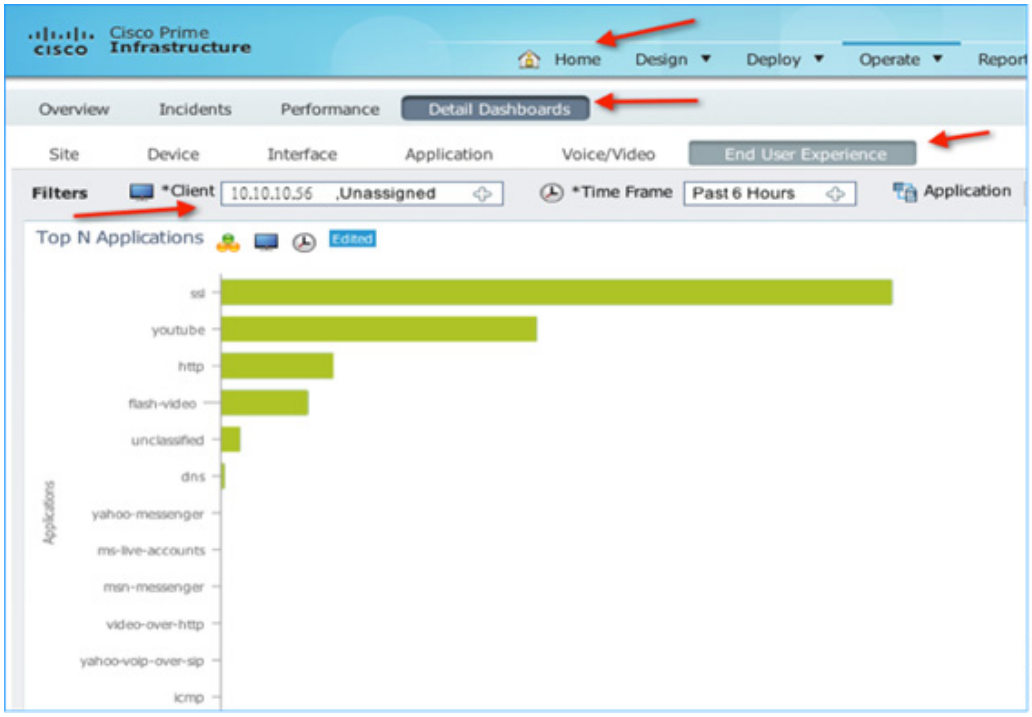



11. Once the WLC is added, start some traffic from wireless clients. You can view the number of clients per WLAN and usage per client. To see the usage by clients, navigate to **Home > Detail Dashboards > Application**. Now filter the Application Box as **All**, Site as **Unassigned**, and Network Aware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

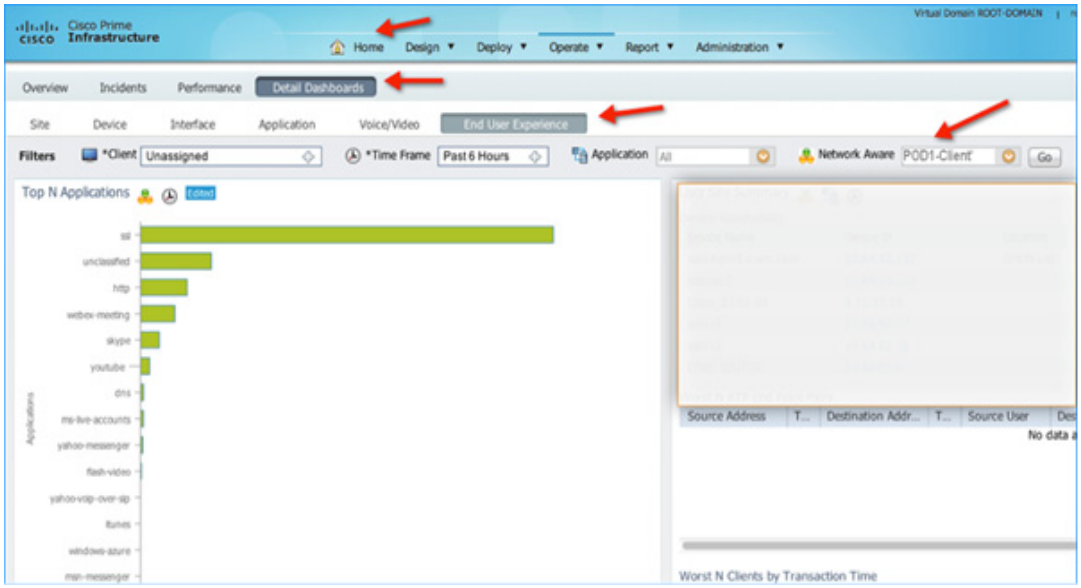



**Note** You can see the number of clients on WLAN "POD1-Client" which is filtered under Network Aware. Also, in same screen, you can see the applications used by both the clients.

12. 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.




13. 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**.




# Web Links and Terminology

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:

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