

Understand Application Visibility and Control on 9800 Wireless Controller

Contents

[Introduction](#)

[Prerequisite](#)

[Information about Application Visibility and Control \(AVC\)](#)

[How AVC Works](#)

[Network-Based Application Recognition \(NBAR\)](#)

[Enable NBAR Protocol on Policy Profile](#)

[Upgrading NBAR on 9800 WLC](#)

[NetFlow](#)

[Flexible Netflow](#)

[Flow Monitor](#)

[AVC Supported Access Points](#)

[Support for different 9800 deployment modes](#)

[Restrictions while implementing AVC on 9800](#)

[Network Topology](#)

[AP In Local Mode](#)

[AP In flex Mode](#)

[Configuration of AVC on 9800 WLC](#)

[Local Exporter](#)

[External NetFlow Collector](#)

[Configuration of AVC on 9800 WLC using CiscoDNA](#)

[Verification of AVC](#)

[On 9800](#)

[On Cisco DNA](#)

[On External NetFlow Collector](#)

[Example1: Cisco Prime as Netflow Collector](#)

[Example 2: Third party NetFlow Collector](#)

[Traffic Control](#)

[Troubleshooting](#)

[Log Collection](#)

[WLC logs](#)

[AP Logs](#)

[Related Information](#)

Introduction

This document describes Application Visibility and Control (AVC) on a Cisco Catalyst 9800 WLC.

Prerequisite

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Cisco WLC 9800.
- Basic knowledge of local and flex connect mode AP.
- The access points must be AVC capable. (Not applicable with Local Mode AP)
- For the control part of AVC (QoS) to work, the application visibility feature with FNF has to be configured.

Information about Application Visibility and Control (AVC)

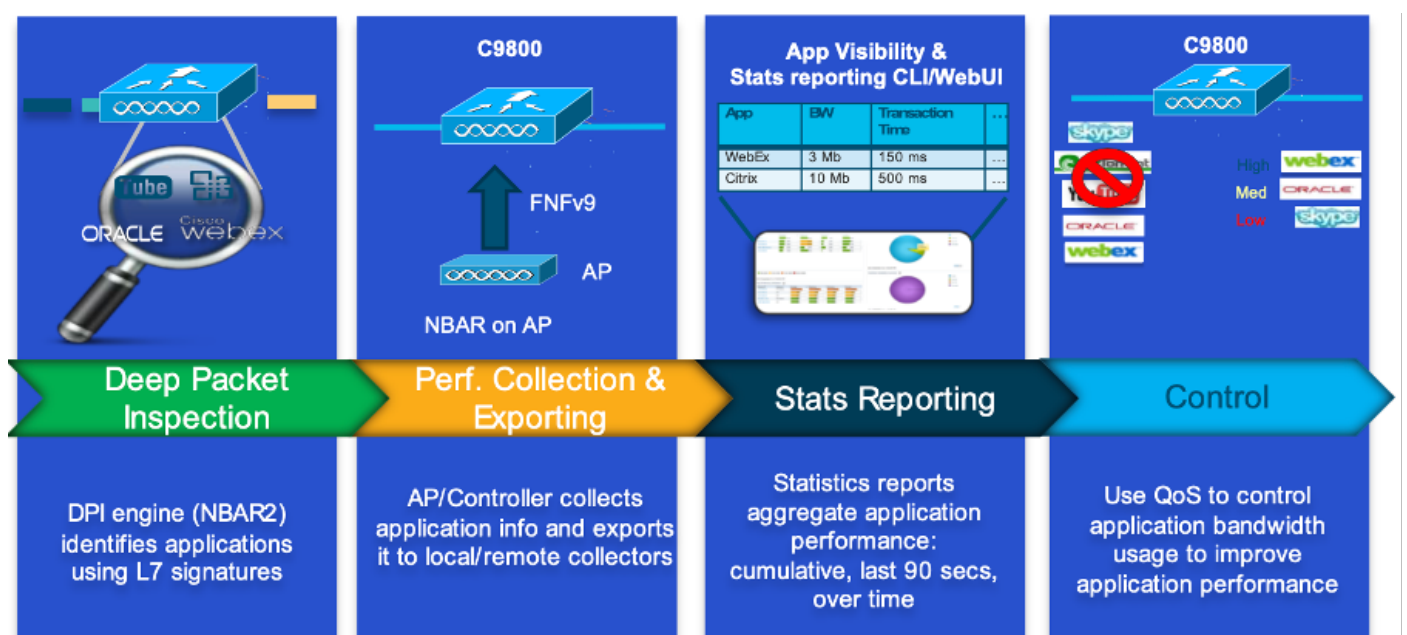
Application Visibility and Control (AVC) is leading approach for deep-packet inspection (DPI) technology in both wireless and wired networks. With AVC, you can perform real-time analysis and create policies to effectively reduce network congestion, minimize costly network link usage, and avoid unnecessary infrastructure upgrades. In short, AVC empowers users to achieve a whole new level of traffic recognition and shaping through Network Based Application Recognition (NBAR). NBAR packages running on the 9800 WLC are used for DPI and the results are reported using Flexible NetFlow (FNF).

In addition to visibility, AVC provides the capability to prioritize, block, or throttle different types of traffic. For instance, administrators can create policies that prioritize voice and video applications to ensure quality of service (QoS) or limit the bandwidth available to non-essential applications during peak business hours. It can also be integrated with other Cisco technologies, such as Cisco Identity Services Engine (ISE) for identity-based application policies and Cisco Catalyst Center for centralized management.

How AVC Works

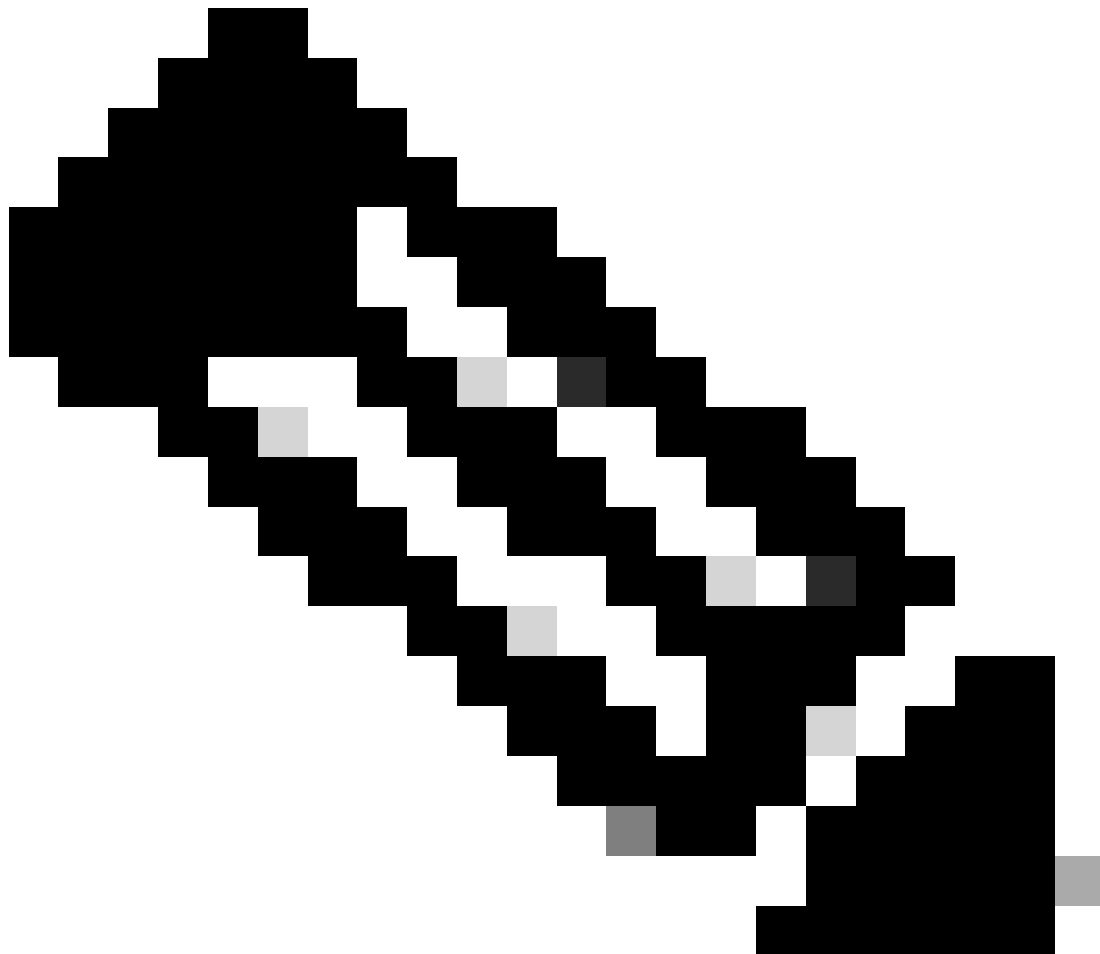
AVC utilizes advanced technologies such as FNF and NBAR2 engine for DPI. By analyzing and identifying traffic flows using the NBAR2 engine, specific flows are marked with the recognized protocol or application. The controller collects all reports and presents them through show commands, Web UI, or additional NetFlow export messages to external NetFlow collectors like Prime.

Once Application Visibility is established, users can create control rules with policing mechanisms for clients by configuring Quality of service (QOS).



Network-Based Application Recognition (NBAR)

NBAR is a mechanism integrated on the 9800 WLC, which is used to perform DPI for identifying and classifying a wide variety of applications running over a network. It can recognize and classify a vast number of applications, including encrypted and dynamically port-mapped applications, which are often invisible to traditional packet inspection technologies.



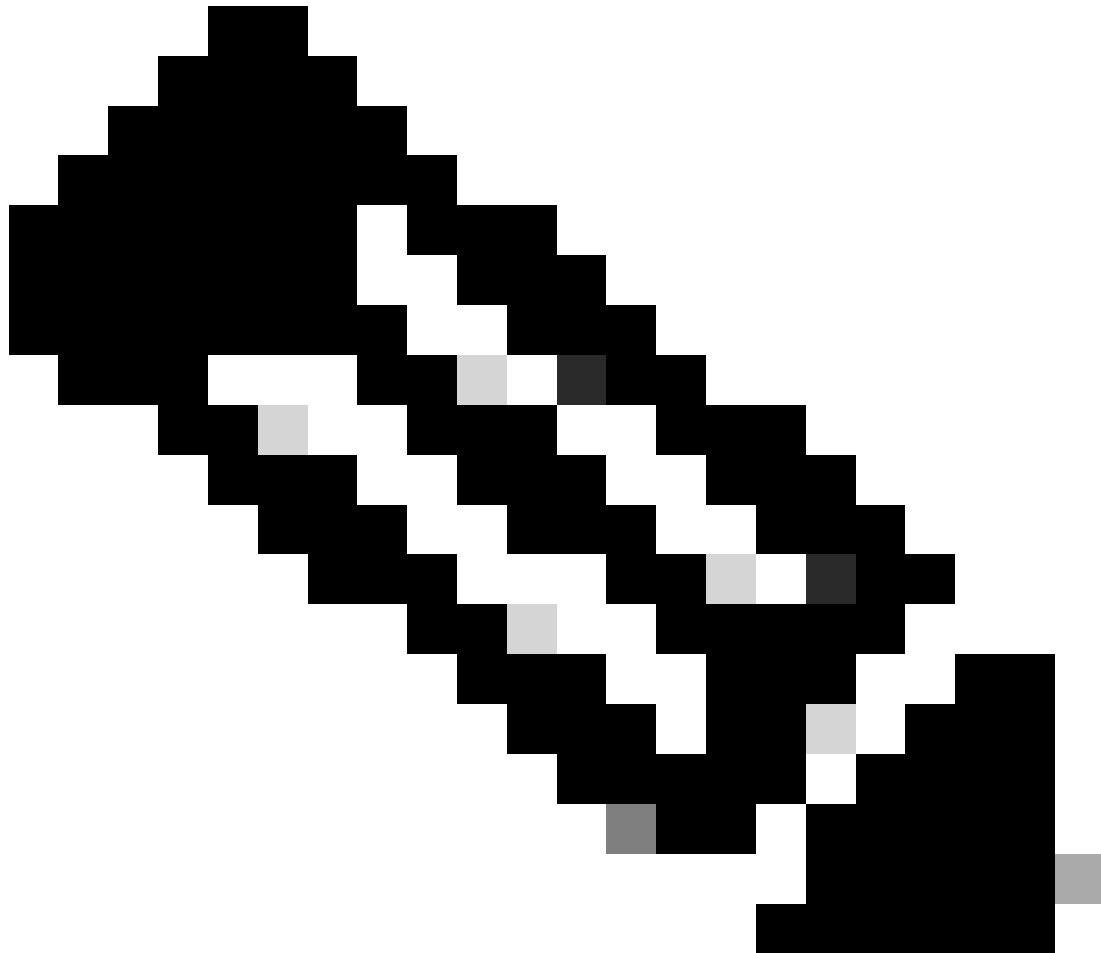
Note: To leverage NBAR on the Catalyst 9800 WLC, it is necessary to enable and configure it correctly, often in conjunction with specific AVC profiles that define the appropriate actions to be taken based on the classification of the traffic.

NBAR continues to be periodically updated, and it is important to keep the WLC software up to date to ensure that the NBAR feature set remains current and effective.

A complete list of the protocols supported in the latest releases can be found at https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Enable NBAR Protocol on Policy Profile

```
9800WLC#configure terminal
9800WLC(config)#wireless profile policy AVC_testing
9800WLC(config-wireless-policy)#ip nbar protocol-discovery
9800WLC(config-wireless-policy)#end
```



Note: % Policy profile needs to be disabled before performing this operation.

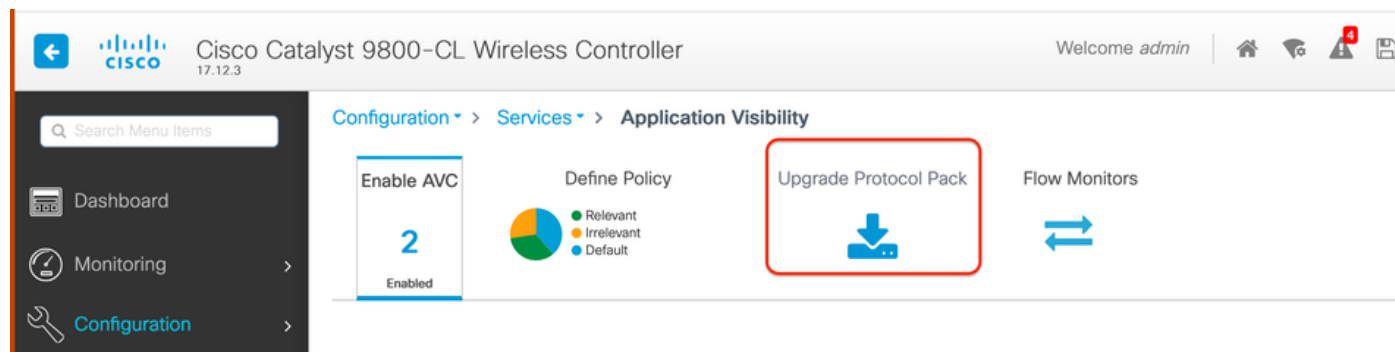
```
9800WLC#show wireless profile policy detailed AVC_testing | in NBAR
NBAR Protocol Discovery : Enabled
```

Upgrading NBAR on 9800 WLC

9800 WLC already has ~1500 recognizable applications. In the case where a new application is released, the protocol for the same can be updated in the latest NBAR which would be needed to be downloaded from the Software Download page for the specific 9800 model.

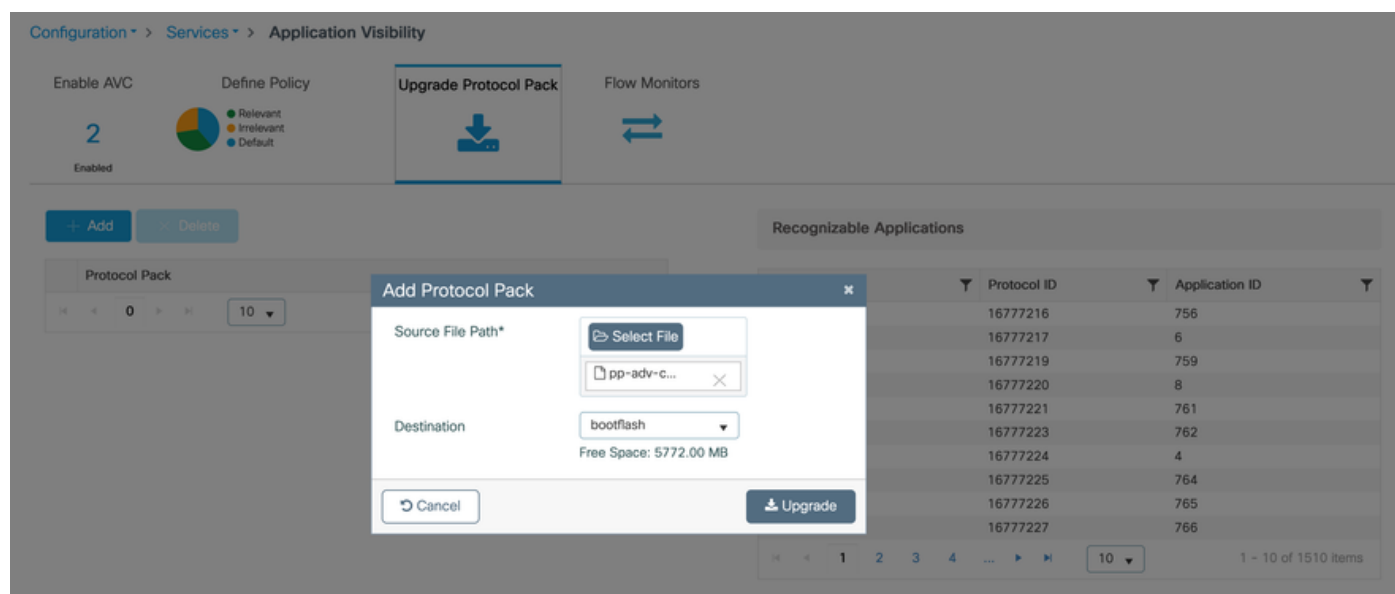
Via GUI

Navigate to **Configuration > Services > Application Visibility**. Click **Upgrade Protocol Pack**.



Upload Protocol Section in 9800 WLC

Click **Add**, then choose the protocol pack to be downloaded and click **Upgrade**.



Adding NBAR Protocol

Once Upgrade is done, you can see the protocol pack added.

Enable AVC

2

Enabled

Define Policy

Relevant

Irrelevant

Default

Upgrade Protocol Pack

Flow Monitors

+ Add

× Delete

1

10

1 - 1 of 1 items

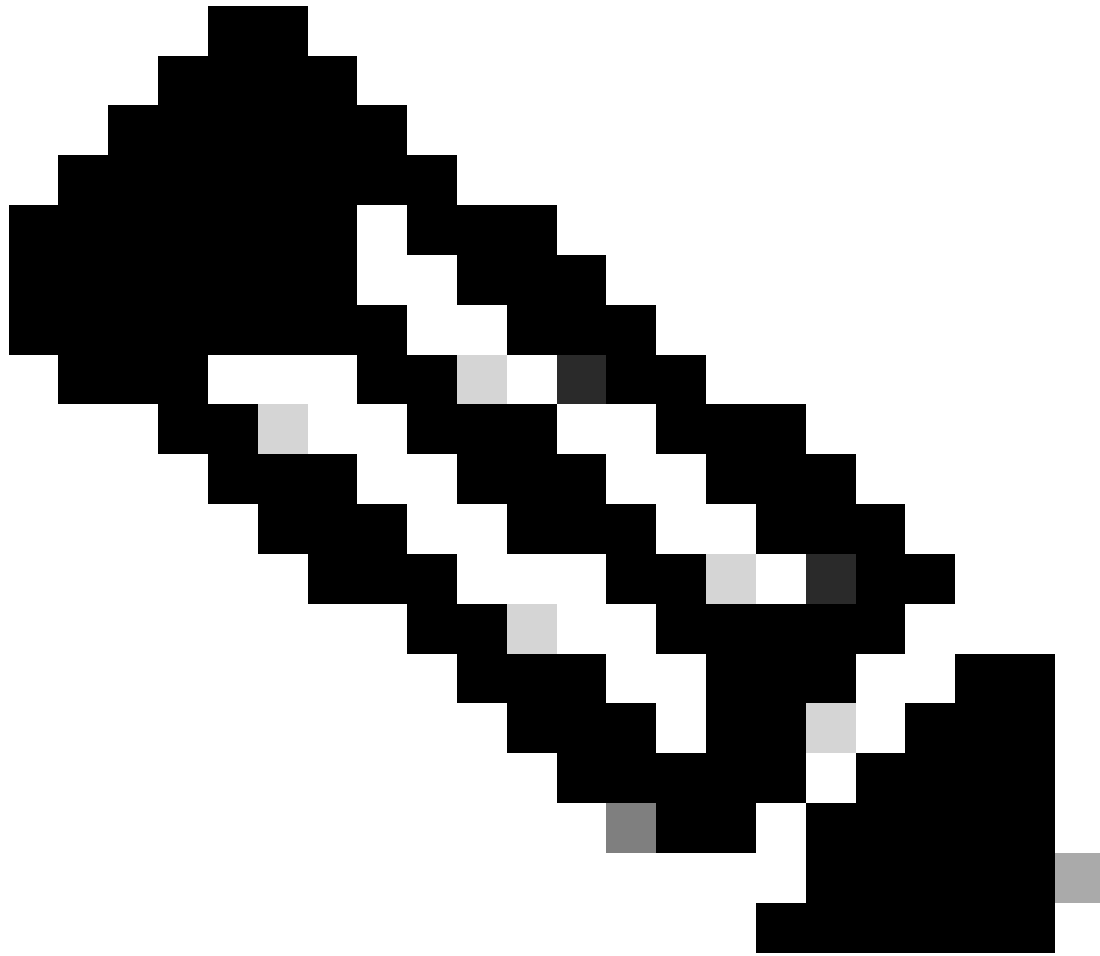
Verification of Protocol Pack

Via CLI

```
9800WLC#copy tftp://10.10.10.1/pp-adv-c9800-1712.1-49-70.0.0.pack bootflash:
9800WLC#configure terminal
9800WLC(config)#ip nbar protocol-pack bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack
```

To verify NBAR protocol pack version

```
9800WLC#show ip nbar protocol-pack active
Active Protocol Pack:
Name: Advanced Protocol Pack
Version: 70.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 49
Creation time: Tue Jun 4 10:18:09 UTC 2024
File: bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack
State: Active
```



Note: There is no service disruption during the upgrade of NBAR protocol pack.

NetFlow

NetFlow is a network protocol used for collecting IP traffic information and monitoring network flow data. It is used primarily for network traffic analysis and bandwidth monitoring. Here is an overview of how NetFlow works on the Cisco Catalyst 9800 series controllers:

- **Data Collection:** 9800 WLC collect data about IP traffic flowing through them. This data includes information such as source and destination IP addresses, source and destination ports, protocols used, class of service, and the cause of flow termination.
- **Flow Records:** The collected data is organized into flow records. A flow is defined as a unidirectional sequence of packets sharing a set of common attributes, such as the same source/destination IP, source/destination ports, and protocol type.
- **Exporting Data:** The flow records are periodically exported from the NetFlow-enabled device to a NetFlow collector. The collector can be local WLC or a dedicated server or software application that receives, stores, and processes the flow data.
- **Analysis:** You can use NetFlow collectors and analysis tools to visualize traffic patterns, identify

bandwidth, detect unusual traffic flows indicative of security breaches, optimize network performance, and plan for network expansion.

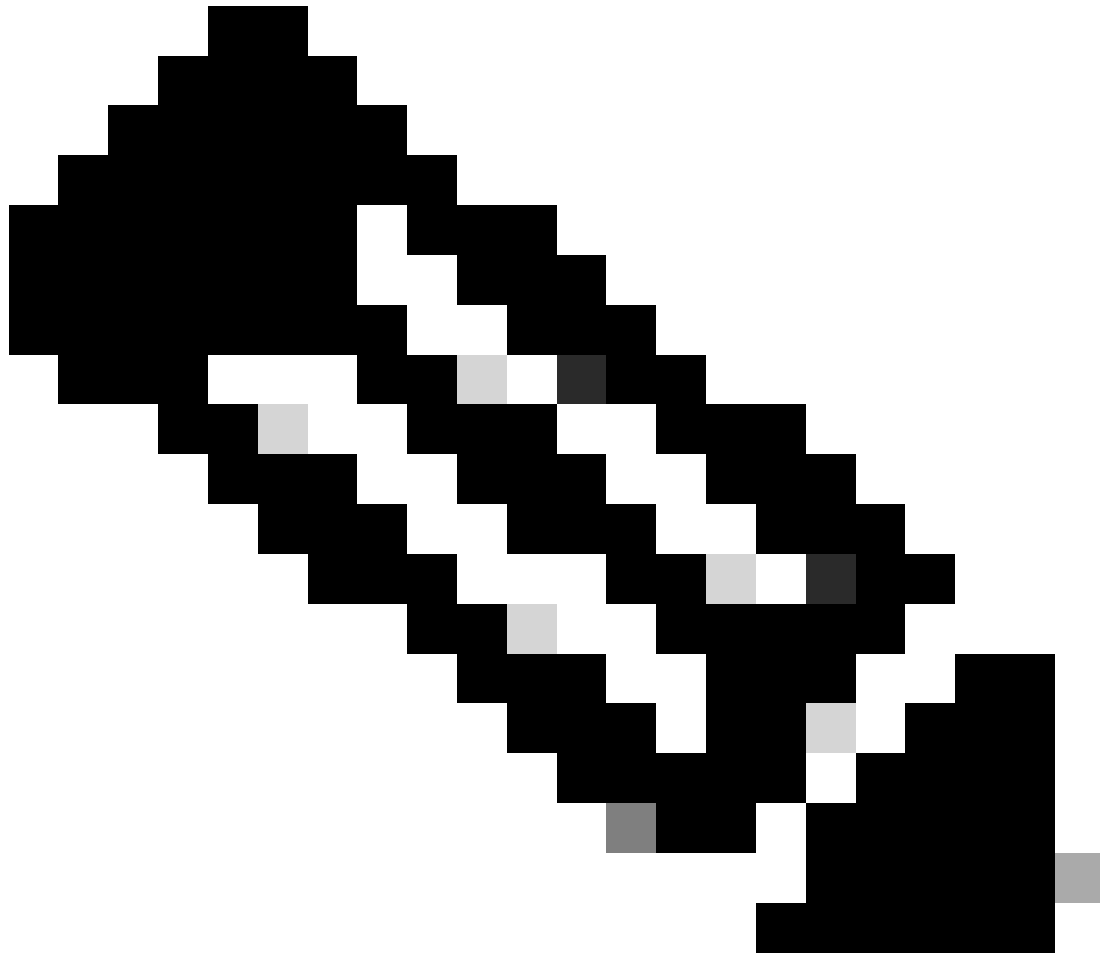
- **Wireless-Specific Information:** In the context of wireless controllers, NetFlow can include additional information specific to wireless networking, such as the SSID, AP names, client MAC addresses, and other details relevant to Wi-Fi traffic.

Flexible Netflow

Flexible NetFlow (FNF) is an advanced version of traditional NetFlow, and it is supported by the Cisco Catalyst 9800 Series Wireless LAN Controllers (WLCs). It provides more customization options for tracking, monitoring, and analyzing network traffic patterns. Key features of Flexible NetFlow on the Catalyst 9800 WLC include:

- **Customization:** FNF allows users to define what information they want to collect from the network traffic. This includes a wide range of traffic attributes like IP addresses, port numbers, timestamps, packet and byte counts, application types, and more.
- **Enhanced Visibility:** By leveraging FNF, administrators gain detailed visibility into the types of traffic flowing through the network, which is essential for capacity planning, usage-based network billing, network analysis, and security monitoring.
- **Protocol Independence:** FNF is flexible enough to support various protocols beyond IP, making it adaptable to different types of network environments.

On the Catalyst 9800 WLC, FNF can be configured to export flow records to an external NetFlow collector or analysis application. This data can then be used for troubleshooting, network planning, and security analysis. The FNF configuration involves defining a flow record (what to collect), a flow exporter (where to send the data), and attaching the flow monitor (which binds the record and exporter) to the appropriate interfaces.



Note: FNF can send 17 different data records (as defined in RFC 3954) to the External 3rd Party Netflow collector such as Stealthwatch, Solarwinds and others which are: Application Tag, Client Mac Address, AP Mac address, WlanID, Source IP, Destination IP, Source Port, Destination Port, Protocol, Flow Start Time, Flow End Time, Direction, Packet out, Byte count, VLAN ID (Local mode) – Mgmt/Client and TOS - DSCP Value

Flow Monitor

A flow monitor is a component used in conjunction with Flexible NetFlow (FNF) to capture and analyse network traffic data. It plays a crucial role in monitoring and understanding traffic patterns for network management, security, and troubleshooting. The flow monitor is essentially an applied instance of FNF that collects and tracks flow data based on defined criteria. It is associated with three main elements:

- **Flow Record:** This defines the data that the flow monitor must collect from the network traffic. It specifies the keys (such as source and destination IP addresses, ports, protocol types) and non-key fields (like packet and byte counters, timestamps) that is included in the flow data.
- **Flow Exporter:** This specifies the destination where the collected flow data must be sent. It includes details like the IP address of the NetFlow collector, the transport protocol (usually UDP), and the destination port number where the collector is listening.

- **Flow Monitor:** The flow monitor itself binds the flow record and flow exporter together and applies them to an interface or WLAN to actually start the monitoring process. It determines how the flow data must be collected and exported based on the criteria set in the flow record and the destination set in the flow exporter.

AVC Supported Access Points

AVC is supported only on these access points:

- Cisco Catalyst 9100 Series Access Points
- Cisco Aironet 2800 Series Access Point
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points

Support for different 9800 deployment modes

Deployment Mode	9800 WLC	Wave 1 Access Point	Wave 2 Access Point	Wifi 6 Access Point
Local Mode (Central Switching)	IPV4 Traffic: AVC Supported FNF Supported IPV6 Traffic: AVC Supported FNF Supported	Processing at WLC Level	Processing at WLC Level	Processing at WLC Level
Flex Mode (Central Switching)	IPV4 Traffic: AVC Supported FNF Supported IPV6 Traffic: AVC Supported FNF Supported	Processing at WLC Level	Processing at WLC Level	Processing at WLC Level
Flex Mode (Local Switching)	Processing at AP Level	IPV4 Traffic: AVC Supported FNF Supported IPV6 Traffic: AVC Supported FNF Not Supported	IPV4 Traffic: AVC Supported FNF Supported IPV6 Traffic: AVC Supported FNF Supported	IPV4 Traffic: AVC Supported FNF Supported IPV6 Traffic: AVC Supported FNF Supported
Local Mode (Fabric)	Processing at AP Level	IPV4 Traffic: AVC Not Supported FNF Not Supported	IPV4 Traffic: AVC Supported FNF Supported	IPV4 Traffic: AVC Supported FNF Supported

		IPV6 Traffic: AVC Not Supported FNF Not Supported	IPV6 Traffic: AVC Supported FNF Supported	IPV6 Traffic: AVC Supported FNF Supported
--	--	---	---	---

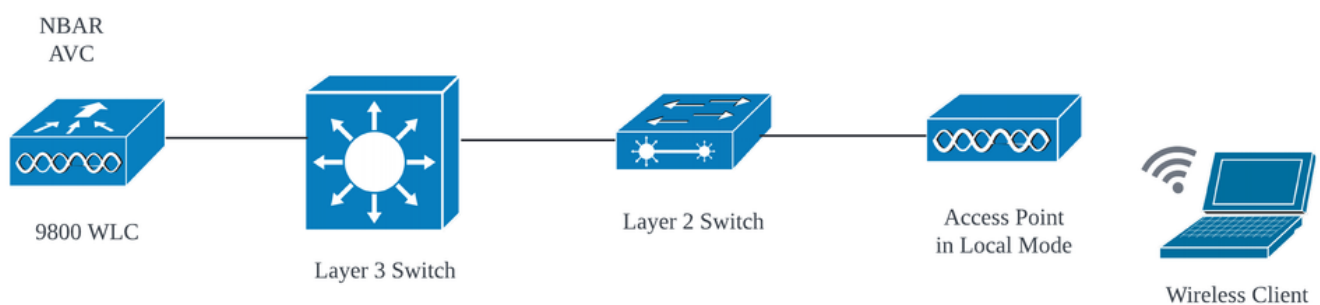
Restrictions while implementing AVC on 9800

Both Application Visibility and Control (AVC) and Flexible NetFlow (FNF) are powerful features on Cisco Catalyst 9800 Series Wireless LAN Controllers that enhance network visibility and control. However, there are some limitations and considerations to keep in mind when using these features:

- Layer 2 roaming is not supported across controllers.
- Multicast traffic is not supported.
- Only the applications that are recognized with App visibility can be used for applying QoS control.
- Data link is not supported for NetFlow fields in AVC.
- You cannot map the same WLAN profile to both the AVC-not-enabled policy profile and the AVC-enabled policy profile.
- You cannot use the policy profile with different switching mechanism to same WLAN to implement AVC.
- AVC is not supported on the management port (Gig 0/0).
- NBAR-based QoS policy configuration is allowed only on wired physical ports. Policy configuration is not supported on virtual interfaces, for example, VLAN, port channel and other logical interfaces.
- When AVC is enabled, the AVC profile supports only up to 23 rules, which includes the default DSCP rule. The AVC policy can not be pushed down to the AP, if rules are more than 23.

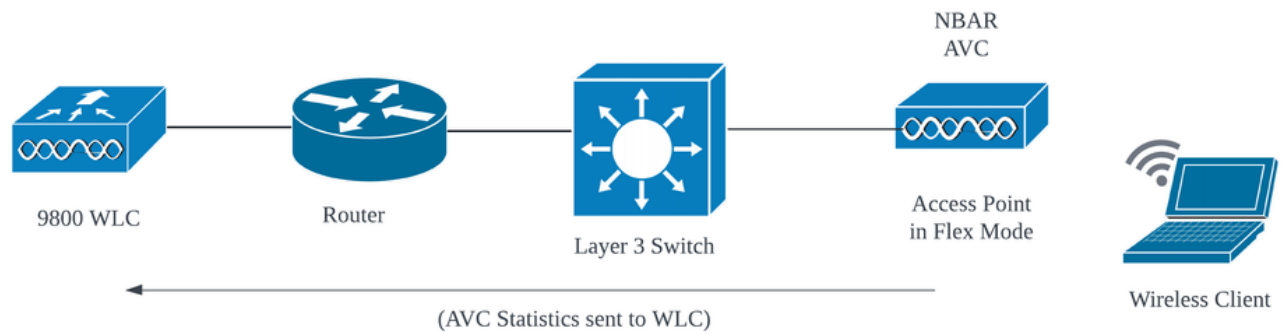
Network Topology

AP In Local Mode



AVC in Local Mode AP (Central Switching)

AP In flex Mode



AVC in Flex Mode AP

Configuration of AVC on 9800 WLC

While Configuring AVC on 9800 WLC, you can use either it as NetFlow Collector or can export the NetFlow data to External NetFlow Collector.

Local Exporter

On a Cisco Catalyst 9800 Wireless LAN Controller (WLC), a local NetFlow collector refers to the embedded feature within the WLC that allows it to collect and locally store NetFlow data. This capability enables the WLC to perform basic NetFlow data analysis without the need to export the flow records to an external NetFlow collector.

Via GUI

Step 1: To enable AVC on Specific SSID Navigate to **Configuration > Services > Application Visibility**. Choose the particular Policy Profile for which you wish to activate AVC.

Configuration > Services > Application Visibility

Enable AVC: 1 Enabled

Define Policy: Relevant, Irrelevant, Default

Upgrade Protocol Pack

Flow Monitors

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

Available (2)	Enabled (0)
Profiles	Profiles Visibility Collector Address
AVC_testing	
default-policy-profile	

Enabling AVC on Policy Profile

Step 2: Select **Local** as Netflow Collector and Click **Apply**.

Configuration > Services > Application Visibility

Enable AVC 1 Enabled

Define Policy

Upgrade Protocol Pack

Flow Monitors

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

Available (1)

Profiles

default-policy-profile

Enabled (1)

Profiles	Visibility	Collector Address
AVC_testing	☒	Local ☒ External ☐

Apply

Selecting Local NetFlow Collector

Observe that the NetFlow Exporter and NetFlow settings have been automatically configured according to the specified preferences once you apply the AVC configuration.

You can Validate the same by navigating to **Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor**.

Configuration > Services > Application Visibility

Enable AVC 1 Enabled

Define Policy

Upgrade Protocol Pack

Flow Monitors

Exporter

Monitor

Name	Description	Type	Source IP	Destination IP
☐ wireless-local-exporter	User defined	Local	0.0.0.0	0.0.0.0

Local Flow Collector Configuration on 9800 WLC

Configuration > Services > Application Visibility

Enable AVC 1 Enabled

Define Policy

Upgrade Protocol Pack

Flow Monitors

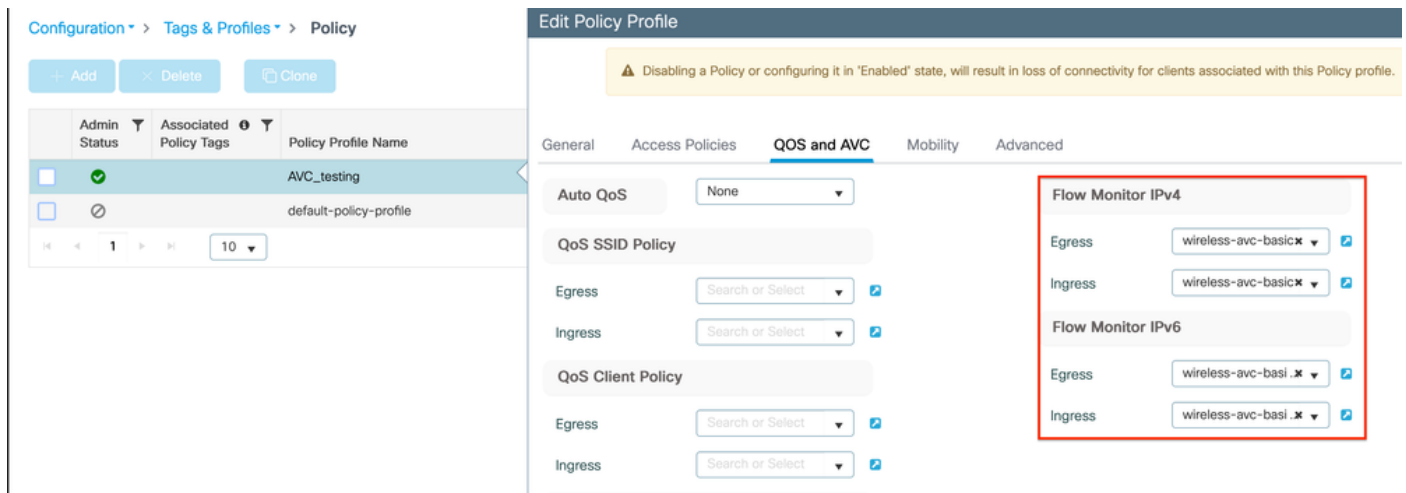
Exporter

Monitor

Name	Description	Flow Exporters
☐ wireless-avc-basic	User defined	wireless-local-exporter
☐ wireless-avc-basic-ipv6	User defined	wireless-local-exporter

Flow Monitor Configuration with Local NetFlow Collector

The IPv4 and IPv6 AVC Flow Monitors are automatically linked with the Policy Profile. Navigate to **Configuration > Tags & Profile > Policy**. Click **Policy Profile > AVC and QOS**.



Flow Monitor Configuration In Policy Profile

Via CLI

Step1: Configure 9800 WLC as Local Exporter.

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter wireless-local-exporter
9800-C1-VM(config-flow-exporter)#destination local wlc
9800-C1-VM(config-flow-exporter)#exit
```

Step2: Configure IPv4 and IPv6 Network Flow Monitor to use Local(WLC) as Netflow Exporter.

```
9800-C1-VM(config)#flow monitor wireless-avc-basic
9800-C1-VM(config-flow-monitor)#exporter wireless-local-exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor wireless-avc-basic-ipv6
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exit
```

Step 3: Map the IPv4 and IPv6 Flow Minitor in Policy Profile for both ingress and egress traffic.

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 output
```

```
9800-CL-VM(config-wireless-policy)#no shutdown
9800-CL-VM(config-wireless-policy)#exit
```

External NetFlow Collector

An external NetFlow collector, when used in the context of Application Visibility and Control (AVC) on a Cisco Catalyst 9800 Wireless LAN Controller (WLC), is a dedicated system or service that receives, aggregates, and analyzes NetFlow data exported from the WLC. You can Either Configure only external NetFlow Collector to Monitor the Application Visibility or can use it along with Local Collector as well.

Via GUI

Step 1: To enable AVC on Specific SSID Navigate to **Configuration > Services > Application Visibility**. Choose the particular Policy Profile for which you wish to activate AVC. Select Collector as External and configure the IP address of NetFlow Collector like Cisco Prime, SolarWind, StealthWatch and click **Apply**.

Cisco Catalyst 9800-CL Wireless Controller

Configuration > Services > Application Visibility

Enable AVC 1 Enabled

Define Policy

Upgrade Protocol Pack

Flow Monitors

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

Available (1)

Enabled (1)

Profiles

Profiles Visibility Collector Address

default-policy-profile

AVC_testing

Local External 10.106.36.22

Apply

AVC Configuration for External NetFlow Collector

Observe that, once you apply the AVC configuration, the NetFlow Exporter and NetFlow settings have been automatically configured with the NetFlow Collector IP address as exporter and Exporter address as 9800 WLC with default timeout settings and UDP port 9995. You can Validate the same by navigating to **Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor**.

Cisco Catalyst 9800-CL Wireless Controller

Configuration > Services > Application Visibility

Enable AVC 1 Enabled

Define Policy

Upgrade Protocol Pack

Flow Monitors

Exporter

Monitor

Name	Description	Type	Source IP	Destination IP
export_-1638039067	User defined	External	10.197.234.75	10.106.36.22

External NetFlow Collector Configuration on 9800 WLC

Cisco Catalyst 9800-CL Wireless Controller 17.12.3

Welcome admin

Search Menu Items

Configuration > Services > Application Visibility

Enable AVC 1 Enabled

Define Policy

Upgrade Protocol Pack

Flow Monitors

Exporter

Monitor

+ Add - Delete

Name	Description	Flow Exporters
☐ dwavc_-1638039067	User defined	export_-1638039067
☐ dwavc_ipv6_-1638039067	User defined	export_-1638039067

Flow Monitor Configuration with External NetFlow Collector

You can check the Port Configuration of automatically generated NetFlow Monitor by navigating to **Configuration > Services > NetFlow**.

Cisco Catalyst 9800-CL Wireless Controller 17.12.3

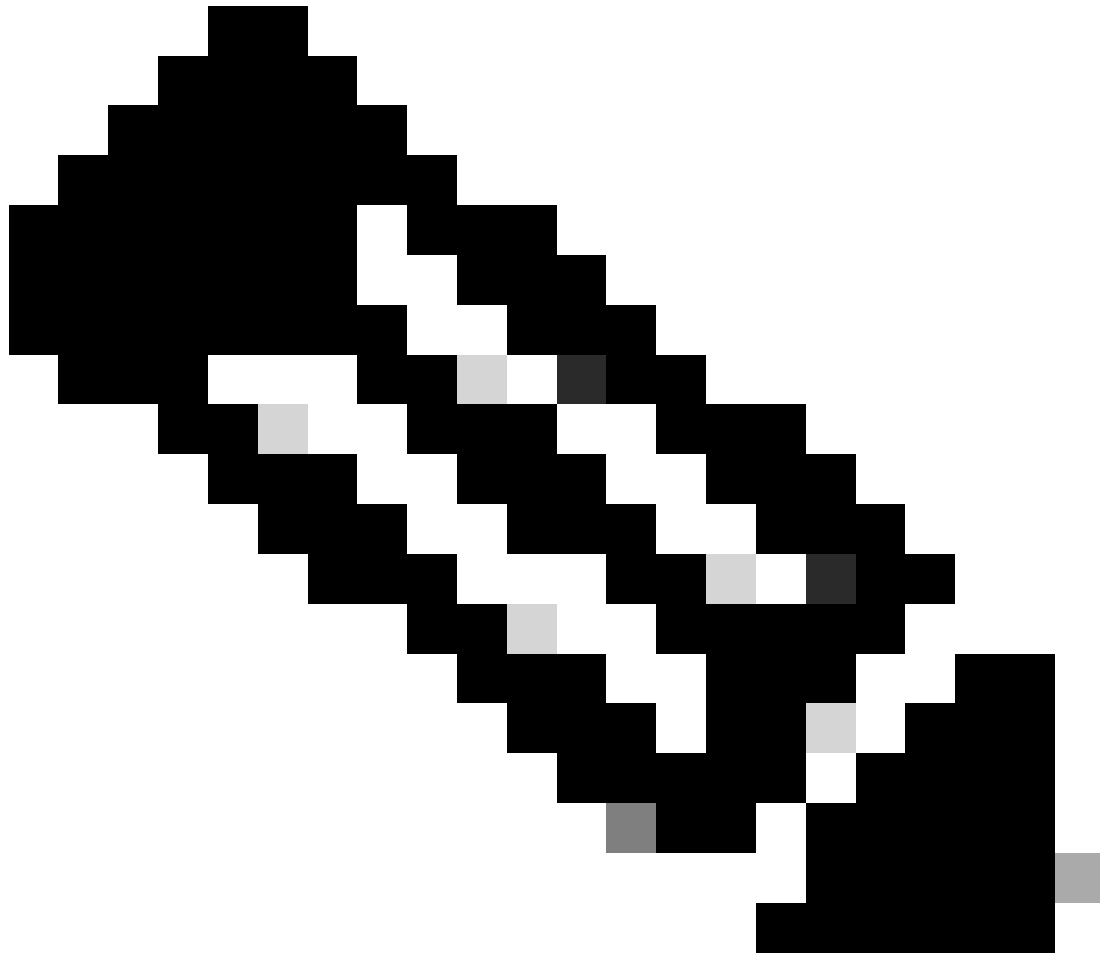
Welcome admin

Search Menu Items

Configuration > Services > NetFlow

+ Add - Delete

Netflow Template	Interfaces/Profiles	Collector	Export Interface IP	Sampling Method	Sampling Range/ACL Name	Exporter Port
☐ Wireless avc basic	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995
☐ Wireless avc basic IPv6	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995



Note: If you Configure AVC via GUI, The automatically generated NetFlow Exporter is set to use UDP 9995 port. Please make sure to validate the port number which is being used by your NetFlow collector.

For Example: If you are using Cisco Prime as your NetFlow Collector, it is essential to set the Exporter port to 9991, as this is the port on which Cisco Prime listens for NetFlow traffic. You can manually change the Exporter Port in NetFlow Configuration.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The main menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area displays the 'Configuration > Services > NetFlow' section. A table lists NetFlow templates:

Netflow Template	Interfaces/Profiles	Collector	Export Int
Wireless avc basic	Not Assigned	10.106.36.22	10.197.234
Wireless avc basic IPv6	Not Assigned	10.106.36.22	10.197.234
Wireless avc basic	AVC_testing		10.197.234
Wireless avc basic IPv6	AVC_testing		10.197.234

The 'Edit NetFlow' dialog is open, showing the 'Wireless avc basic' template. The 'Local Exporter' checkbox is unchecked, and the 'External Exporter' checkbox is checked. The 'Collector Address*' is 10.106.36.22, and the 'Exporter Port*' is 9991. The 'Available (1)' section shows the 'default-policy-profile' and the 'AVC_testing' profile is selected for Ingress and Egress.

Changing Exporter Port Number in NetFlow Configuration

Via CLI

Step1: Configure the IP address of External NetFlow Collector with the source interface.

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter External_Exporter
9800-C1-VM(config-flow-exporter)#destination <IP>
9800-C1-VM(config-flow-exporter)#source $Source_Interface
9800-C1-VM(config-flow-exporter)#transport udp $Port_Numbet
9800-C1-VM(config-flow-exporter)#exit
```

Step2: Configure IPv4 and IPv6 Network Flow Monitor to use Local(WLC) as Netflow Exporter.

```
9800-C1-VM(config)#flow monitor wireless-avc-basic
9800-C1-VM(config-flow-monitor)#exporter External_Exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-C1-VM(config-flow-monitor)#exit

9800-C1-VM(config)#flow monitor wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exporter External_Exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exit
```

Step 3: Map the IPv4 and IPv6 Flow Minitor in Policy Profile for both ingress and egress traffic.

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic output
9800-C1-VM(config-wireless-policy)#no shutdown
9800-C1-VM(config-wireless-policy)#exit
```

Configuration of AVC on 9800 WLC using Cisco DNA

Before proceeding with the configuration of Application Visibility and Control (AVC) on a Cisco Catalyst 9800 Wireless LAN Controller (WLC) through Cisco Catalyst Center, it is important to verify that telemetry communication between the WLC and Cisco Catalyst Center has been successfully established. Ensure that the WLC appears in a managed state within the Cisco Catalyst Center interface and that its health status is being actively updated. Additionally, for effective monitoring of the health status, it is important to properly assign both the WLC and the Access Points (APs) to their respective sites within Cisco Catalyst Center.

9800WLC#show telemetry connection all

Telemetry connections

Index	Peer Address	Port	VRF	Source Address	State	State Description
170	Cisco DNA IP	25103	0	WLC_IP	Active	UP

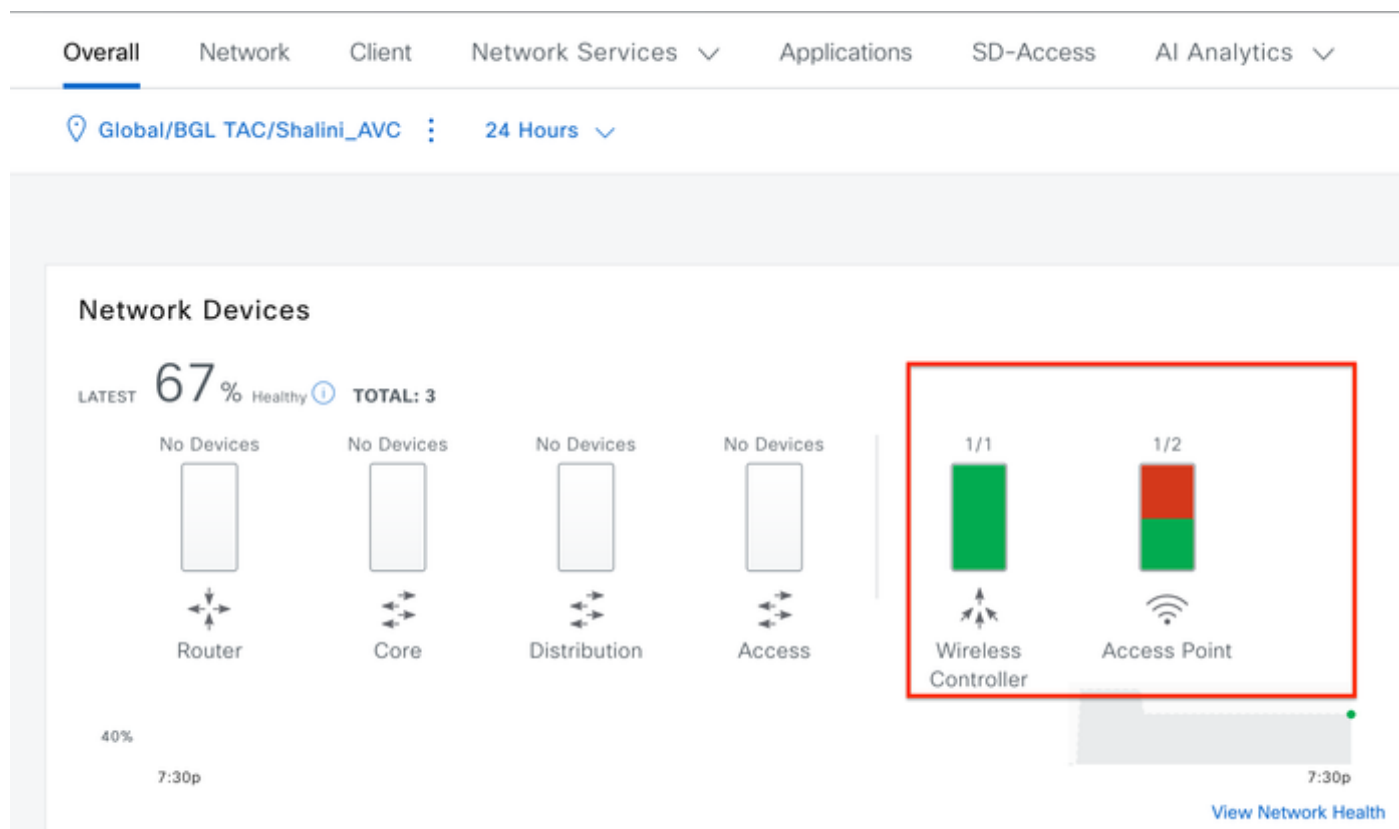
Devices (5) Focus: [Inventory](#) ▾

🔍 Click here to apply basic or advanced filters or view recently applied filters

0 Selected [Tag](#) [+ Add Device](#) [Edit Device](#) [Delete Device](#) [Actions](#) ▾ ⓘ

☐	Tags	Device Name ▴	IP Address	Vendor	Reachability ⓘ	EoX Status ⓘ	Manageability ⓘ
☐		9800WLC.cisco.com 🔗	10.105.193.156	Cisco	🟢 Reachable	⚠ Not Scanned	🟢 Managed
☐		CW9164I-ROW1	10.105.193.152	NA	🟢 Reachable	⚠ Not Scanned	🟢 Managed
☐		CW9164I-ROW2	10.105.60.35	NA	🟢 Reachable	⚠ Not Scanned	🟢 Managed

WLC and AP are in Managed State



Health Status of WLC and AP on Cisco Catalyst Center

Step 1: Configure Cisco Catalyst Center as NetFlow collector and enable Wireless Telemetry in Global setting. Navigate to **Design > Network Setting > Telemetry** and enable the desired configuration as demonstrated.

Catalyst Center Design / Network Settings

Servers Device Credentials IP Address Pools Wireless **Telemetry** Security and Trust

Find Hierarchy [Search Help](#)

- Global
 - BGL TAC

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

Catalyst Center is your default SNMP collector. It polls network devices to gather telemetry data. [View details](#) on the metrics gathered and the frequency with which they are collected.

▼ Application Visibility

Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment ⓘ

☒ **Enable by default on supported wired access devices**

Choose the destination collector for Netflow records sent from network devices.

☒ **Use Catalyst Center as the Netflow Collector**

☐ Use Cisco Telemetry Broker (CTB) or UDP director

▼ Wired Endpoint Data Collection

The primary function of this feature is to track the presence, location, and movement of wired endpoints in the network. Traffic received from endpoints is used to extract and store their identity information (MAC address and IP address). Other features, such as IEEE 802.1X, web authentication, Cisco Security Groups (formerly TrustSec), SD-Access, and Assurance, depend on this identity information to operate properly.

Wired Endpoint Data Collection enables Device Tracking policies on devices assigned to the Access role in Inventory.

☐ Enable Catalyst Center Wired Endpoint Data Collection At This Site

☒ **Disable Catalyst Center Wired Endpoint Data Collection At This Site** ⓘ

▼ Wireless Controller, Access Point and Wireless Clients Health

Enables Streaming Telemetry on your wireless controllers in order to determine the health of your wireless controller, access points and wireless clients.

☒ **Enable Wireless Telemetry**

Wireless Telemetry and AVC Configuration

Step 2: Enable Application Telemetry on the desired 9800 WLC to push the AVC configuration on 9800 WLC. For this navigate to **Provision > Network Device > Inventory**. Choose the 9800 WLC on which you wish to activate Application Telemetry, and then navigate to **Action > Telemetry > Enable Application Telemetry**.

Catalyst Center Provision / Inventory

Global ✓ All Routers Switches Wireless Controllers Access Points Sensors

DEVICE WORK ITEMS

- ☐ Unreachable
- ☐ Unassigned
- ☐ Untagged
- ☐ Failed Provision
- ☐ Non Compliant
- ☐ Outdated Software Image
- ☐ No Golden Image
- ☐ Failed Image Prechecks
- ☐ Under Maintenance
- ☐ Security Advisories

Devices (5) Focus: **Inventory** ▼

Click here to apply basic or advanced filters or view recently applied filters

1 Selected Tag Add Device Edit Device Delete Device Actions ⓘ

Tags	Device Name	IP Address	Inventory	EoX Status ⓘ	Manageability ⓘ
☒	9800WLC.cisco.com	10.105.193.156	Inventory >	Not Scanned	Managed
☐	CW9164I-ROW1	10.105.193.152	Software Image >		
☐	CW9164I-ROW2	10.105.60.35	Provision >		
☐	SDA_WLC.cisco.com	10.106.38.185	Telemetry >		
			Device Replacement >		
			Compliance >		
			More >		

Enable Application Telemetry

Disable Application Telemetry

Update Telemetry Settings

Enabling Application Telemetry on 9800 WLC

Step 3: Choose the Deployment Mode as per the requirement.

Local: To enable AVC in local Policy profile (Central Switching)

Flex/Fabric: To enable AVC in Flex Policy Profile (Local Switching) or Fabric based SSID.

Enable Application Telemetry

You have chosen to enable Netflow with application telemetry on 1 wireless controllers.

By default, all non-guest WLANs on Wireless Controllers will be provisioned to send Netflow with Application telemetry. To override this default behavior, tag specific WLAN profile names with keyword "lan". Once specific WLANs are tagged, only those WLANs will be monitored.

For each wireless controller, select the AP modes where you would like to enable application telemetry.

- For Catalyst 9800 Series Wireless Controllers, the application telemetry source is always Netflow.
- For AireOS wireless controllers, the application telemetry source may be either Netflow or WSA (Wireless Service Assurance).

 Enabling or disabling application telemetry on the selected SSID types will cause a disruption in network services.

 Note: In order to update application telemetry configuration on the WLC, disable application telemetry first and then re-enable it. To do so, please use the Disable/Enable Application Telemetry buttons in the Actions menu.

9800WLC.cisco.com

☒ Local ☐ Flex/Fabric

☐ Include Guest SSIDs



Telemetry Source: **NetFlow**

Note: Devices require Catalyst Center Advantage license for this feature to be enabled.

Deployment Mode Selection on Cisco Catalyst Center

Step 4: It initiates a task to activate the AVC settings, and the corresponding configuration is applied to the 9800 WLC. You can view the status by navigating to **Activities > Audit Log**.

Jul 18, 2024 09:22 PM 

3:37p

8/19/1112/11/12/13/14/15/1

 Filter

Time	Description
Today	
Jul 18, 2024 20:52 PM (IST)	Compliance run completed for device 10.105.193.156[9800WLC.cisco.com] and compliance status is NON_COMPLIANT
Jul 18, 2024 20:36 PM (IST)	Executing command config t wireless profile policy default-policy-profile no shutdown exit wireless profile policy testpsk no shutdown exit wireless profile policy BGL14-4_WLANID_12 no shutdown exit wireless profile po...
Jul 18, 2024 20:36 PM (IST)	Executing command config t flow exporter avc_exporter destination 10.78.8.84 source Vlan1 transport udp 6007 export-protocol ipfix option vrf-table timeout 300 option ssid-table timeout 300 option application-table tim...
Jul 18, 2024 20:36 PM (IST)	Request received to enable telemetry on device(s) : [10.105.193.156]

Audit Logs after Enabling Telemetry on 9800 WLC

Cisco Catalyst Center deploys the Flow Exporter and Flow Monitor configurations, including the specified port and other settings, and activate them within the chosen mode policy profile as shown below:

Configure Cisco Catalyst Center as Flow Exporter:

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter avc_exporter
9800-C1-VM(config-flow-exporter)#destination <IP>
9800-C1-VM(config-flow-exporter)#source Vlan10
9800-C1-VM(config-flow-exporter)#transport udp 6007
9800-C1-VM(config-flow-exporter)#export-protocol ipfix
9800-C1-VM(config-flow-exporter)#option vrf-table timeout 300
9800-C1-VM(config-flow-exporter)#option ssid-table timeout 300
9800-C1-VM(config-flow-exporter)#option application-table timeout 300
9800-C1-VM(config-flow-exporter)#option application-attributes timeout 300
9800-C1-VM(config-flow-exporter)#exit
```

Configure 9800 WLC as Local Exporter

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter avc_local_exporter
9800-C1-VM(config-flow-exporter)#destination local wlc
9800-C1-VM(config-flow-exporter)#exit
```

Configure Network Flow Monitor to use both Local(WLC) and Cisco Catalyst Center as Netflow Exporter:

```
9800-C1-VM(config)#flow monitor avc_ipv4_assurance
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 assurance
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv6_assurance
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 assurance
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv4_assurance_rtp
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 assurance-rtp
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv6_assurance_rtp
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 assurance-rtp
9800-C1-VM(config-flow-monitor)#exit
```

Mapping the IPv4 and IPv6 Flow Monitor in Policy Profile

```
9800-Cl-VM(config)#wireless profile policy AVC_Testing
9800-Cl-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

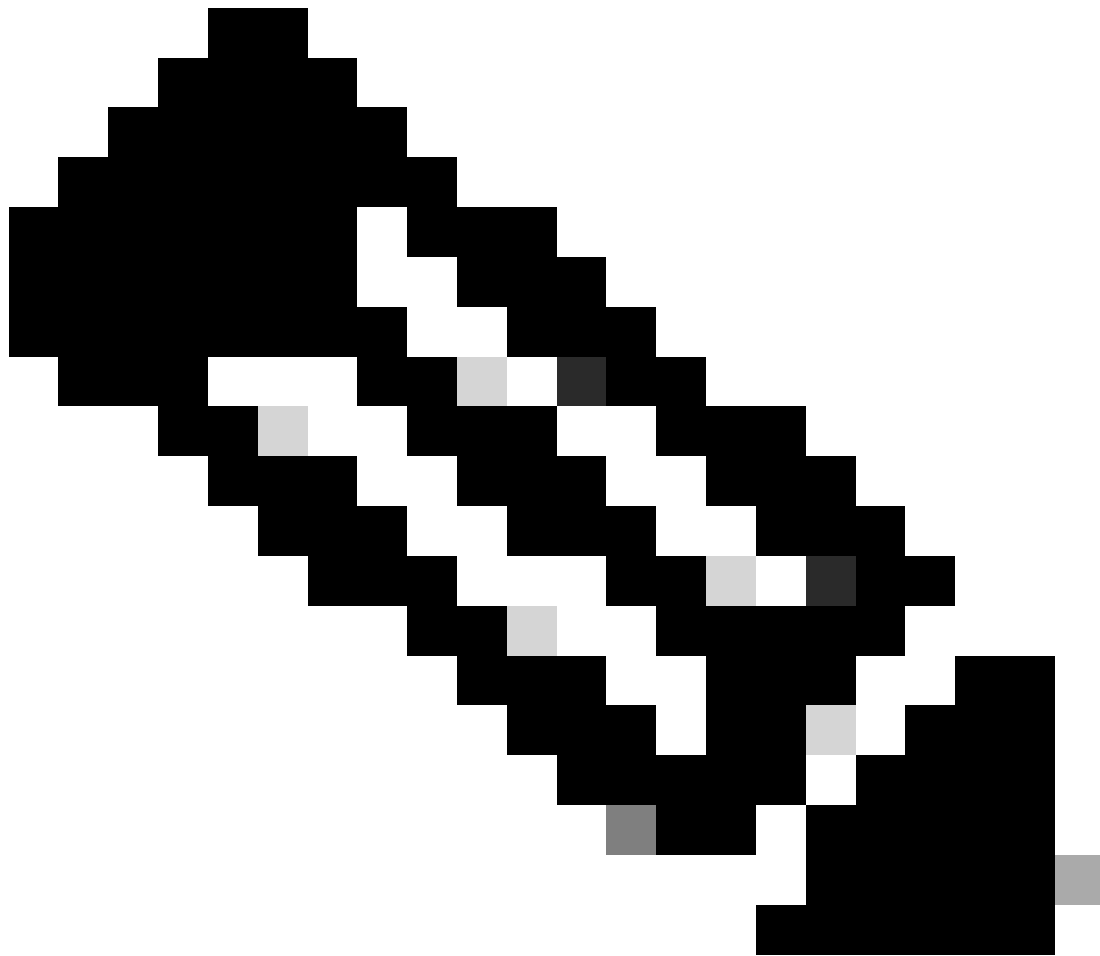
```
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp output
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance input
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance output
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp input
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp output
9800-Cl-VM(config-wireless-policy)#no shutdown
9800-Cl-VM(config-wireless-policy)#exit
```

Verification of AVC

On 9800

When the 9800 WLC is utilized as a Flow exporter, these AVC statistics can be observed:

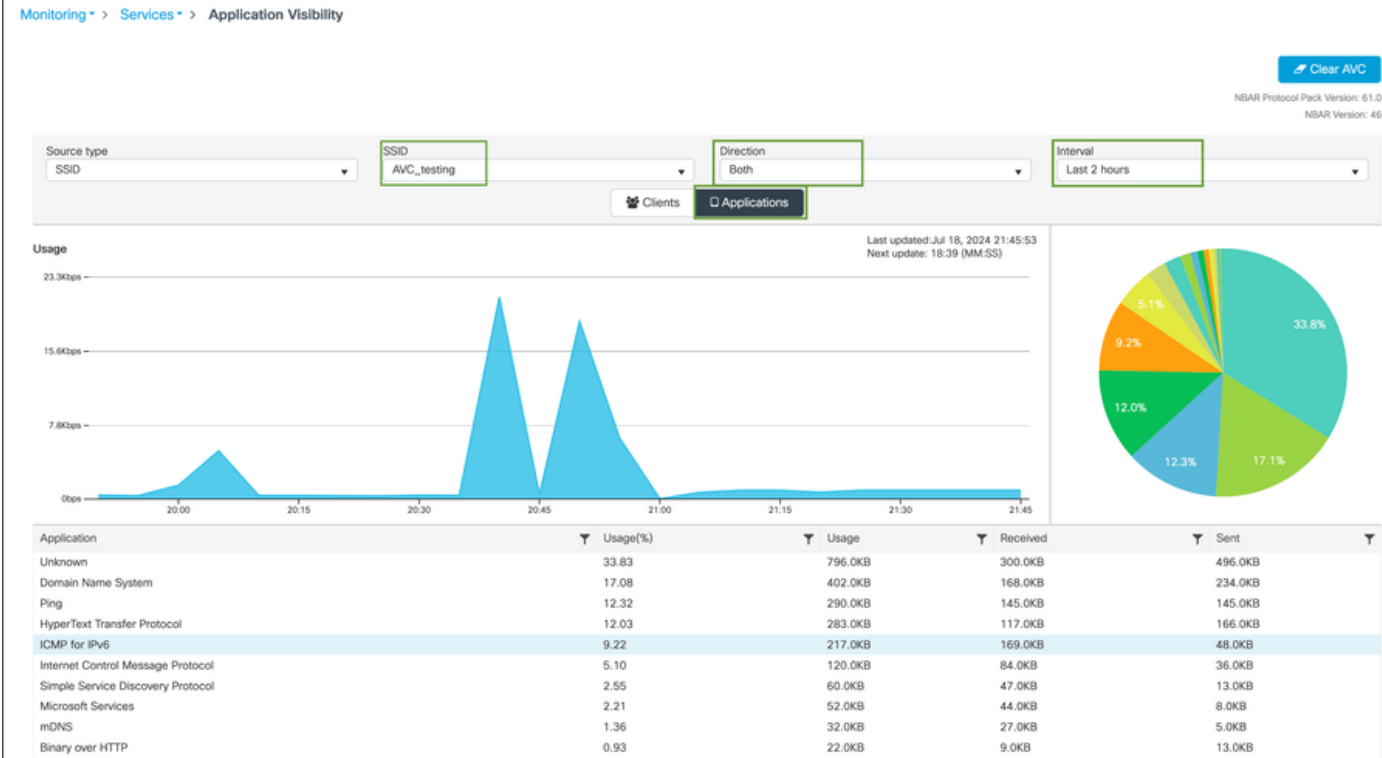
- Application Visibility for clients connected across all SSIDs.
- Individual Application usage for each client.
- Specific Application usage on each SSID separately.



Note: You have the option to filter the data by direction, covering both incoming (ingress) and outgoing (egress) traffic, as well as by time interval, with the ability to select a range of up to 48 hours.

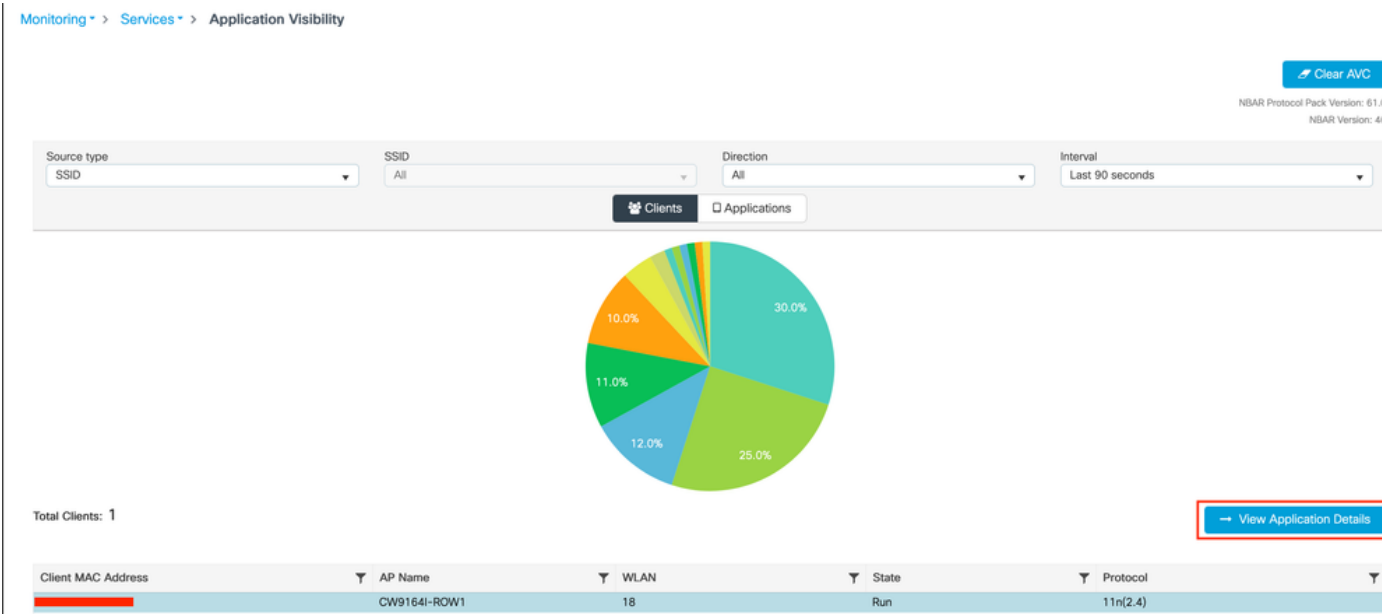
Via GUI

Navigate to **Monitoring > Services > Application Visibility** .



Application Visibility of users connected to AVC_testing SSID for both Ingress and Egress Traffic

To view Application Visibility statistics for each client, you can click on the Clients tab, choose a specific client, and then click **View Application Details**.



Application Visibility for Specific Client - 1

Back to Client's

Application Name	Avg Packet Size	Packet Count	Usage(%)	Usage	Sent	Received
ping	60	6662	29	390.4KB	195.2KB	195.2KB
unknown	693	572	29	387.2KB	122.4KB	264.8KB
dns	108	1511	12	160.4KB	23.3KB	137.1KB
ipv6-icmp	111	1313	10	142.6KB	115.4KB	27.2KB
http	300	427	9	125.4KB	52.1KB	73.3KB
icmp	147	333	4	47.8KB	44.1KB	3.7KB
ssdp	168	123	1	20.3KB	16.0KB	4.3KB
mdns	80	204	1	16.0KB	14.8KB	1.2KB
ms-services	64	231	1	14.6KB	10.9KB	3.7KB
llmnr	81	159	1	12.6KB	6.9KB	5.7KB

1 - 10 of 17 items

Via CLI

Verify AVC status

```
9800WLC#show avc status wlan AVC_testing
WLAN profile name: AVC_testing
```

```
-----
AVC configuration complete: YES
```

Statistics from NetFlow (FNF Cache)

```
9800WLC#show flow monitor $Flow_Monitor_Name cache format table
```

To individually examine the top application usage for each WLAN and its connected clients:

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
where n = <1-30> Enter the number of applications
```

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
where n = <1-10> Enter the number of clients
```

Verify FNFv9 packets counts and decode status punted to Control Plane (CP)

```
9800WLC#show platform software wlavc status decoder
```

```
9800WLC#show platform software wlavc status decoder
AVC FNFv9 Decoder status:
```

Pkt Count	Pkt Decoded	Pkt Errors	Data Records	Last decoded time	Last error time
25703	25703	0	132480	07/20/2024 14:10:46	01/01/1970 05:30:00

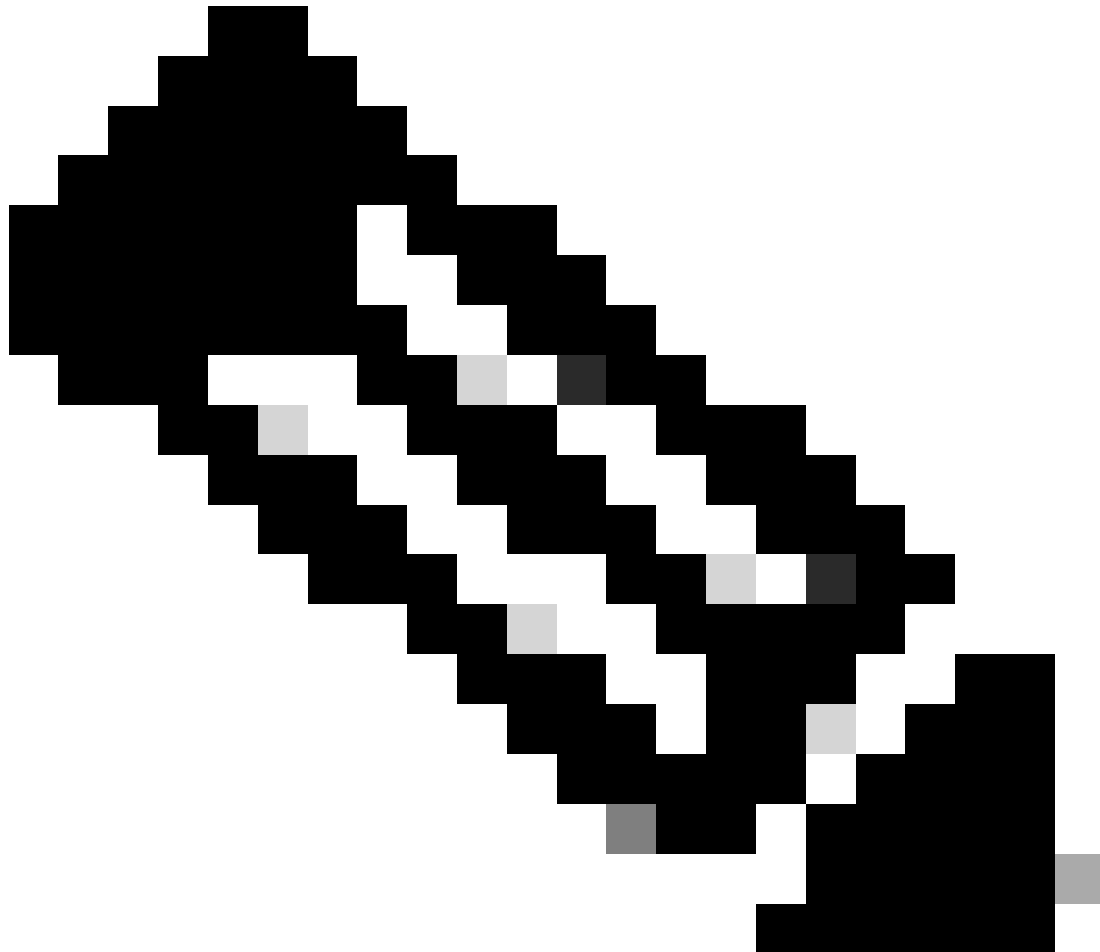
FNFv9 Packet Record

You can also check the nbar statistics directly.

```
9800WLC#show ip nbar protocol-discovery
```

On Fabric and Flex modes, you can get the NBAR stats from AP via:

AP#show avc nbar statistics
Works on both IOS and ClickOS APs



Note: In a foreign-anchor setup, the anchor WLC serves as the Layer 3 presence for the client, while the foreign WLC operates at Layer 2. Because Application Visibility and Control (AVC) operates at Layer 3, the relevant data is only observable on the anchor WLC.

On Cisco DNA

From the packet capture taken on 9800 WLC we can validate it is sending data regarding the applications and network traffic to Cisco Catalyst Center continuously.

ip.addr == 10.78.8.84 and udp.port == 6007						
No.	Time	Source	Destination	Protocol	Length	Info
74224	15:06:30.002990	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
74228	15:06:30.002990	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
76582	15:06:41.012984	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
76879	15:06:45.016997	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
79686	15:07:01.032987	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
85872	15:07:17.047986	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
93095	15:07:37.066982	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
94989	15:07:43.073986	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
98292	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1434	55148 → 6007 Len=1392
98293	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1434	55148 → 6007 Len=1392
98294	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98295	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98296	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98297	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98298	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98299	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98300	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98301	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98302	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98303	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98304	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98305	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98306	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98307	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310

> Frame 1332: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)

> Ethernet II, Src: [REDACTED]

> Internet Protocol Version 4, Src: 10.105.193.156, Dst: 10.78.8.84

> User Datagram Protocol, Src Port: 55148, Dst Port: 6007

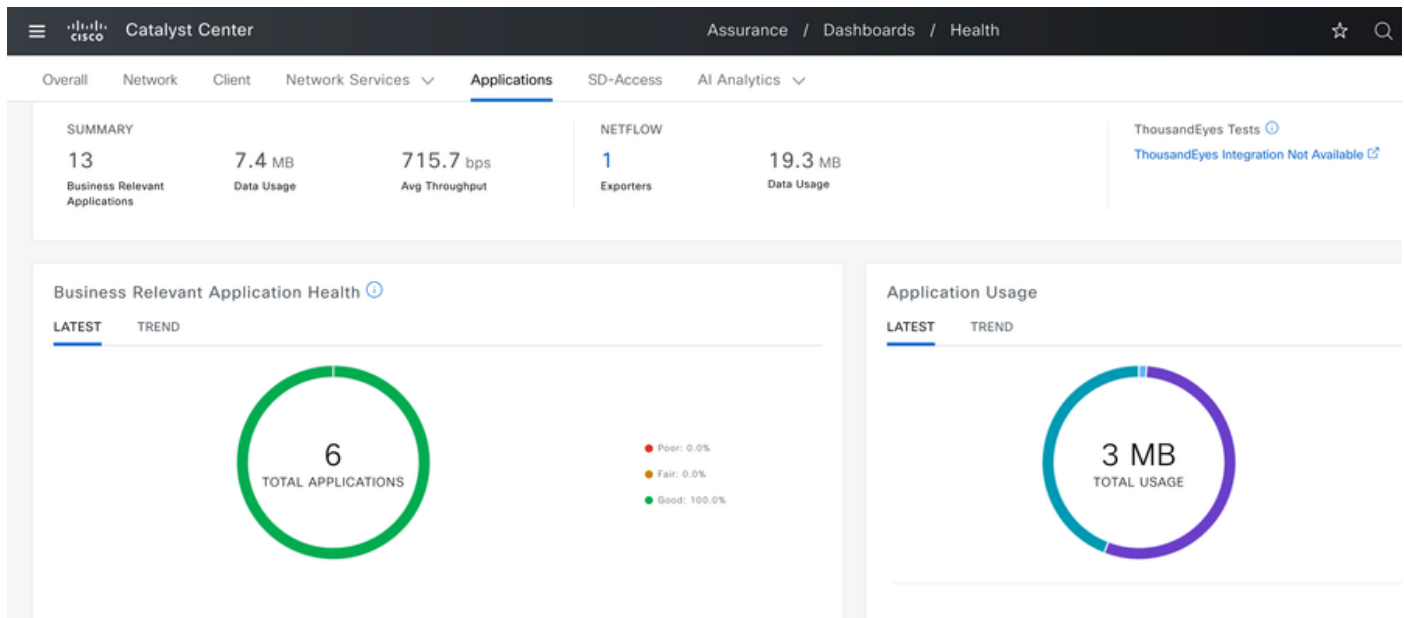
> Data (136 bytes)

 Data [truncated]: 000a00886698e17a00001fa700000100011800780a69c150080808080411003501242fd0daa7da00000002000000120d000309005c

 [Length: 136]

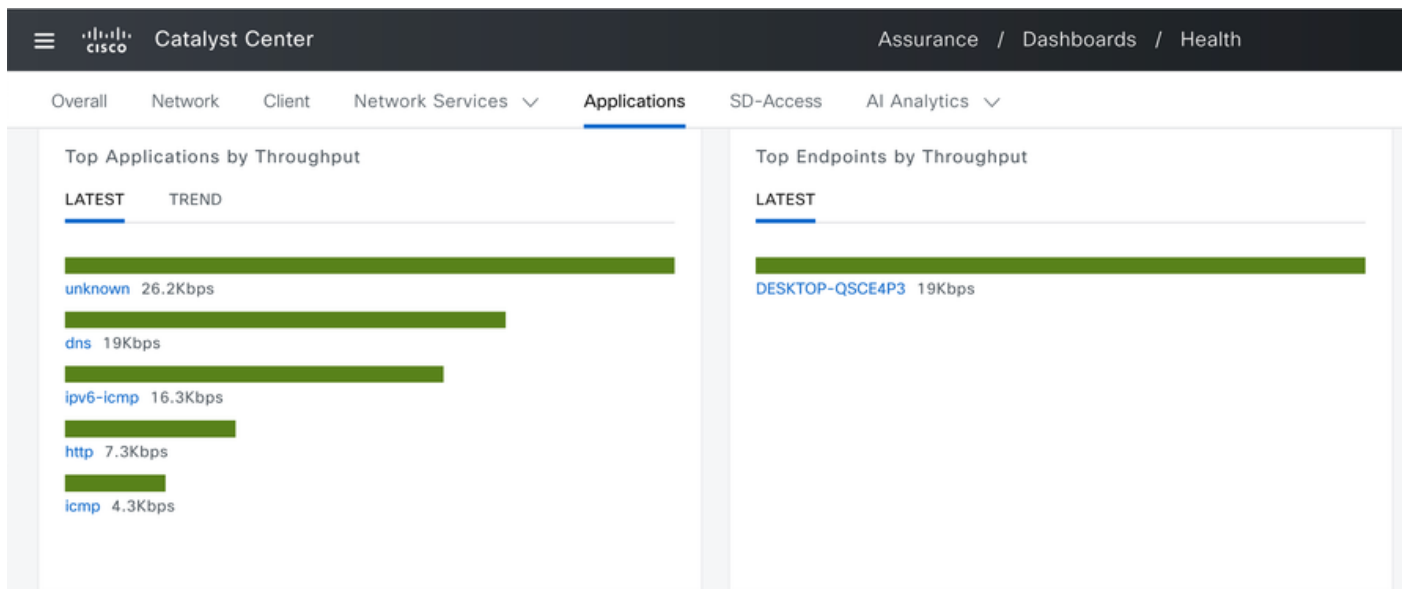
Packet Capture on 9800 WLC

To view the application data for clients connected to a specific WLC on Cisco Catalyst Center, navigate to **Assurance > Dashboards > Health > Application** .



AVC Monitoring on Cisco Catalyst Center

We can track the most frequently used applications by clients and identify the highest data consumers, as demonstrated here.



Top application and Top Bandwidth User Statistics

You have the ability to set a filter for a particular SSID, which allows you to monitor the overall throughput and application usage of clients associated with that SSID.

This functionality enables you to identify the Top applications and the highest bandwidth-consuming users within your network.

Additionally, you can utilize the Time Filter feature to examine this data for previous time periods, offering historical insights into network usage.

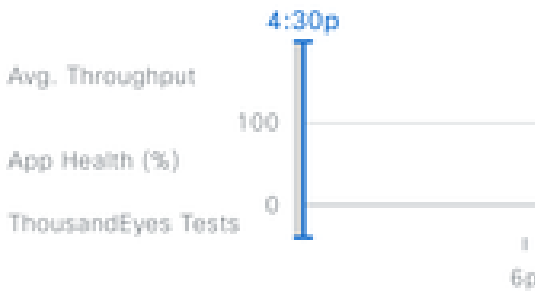
Global/BGL TAC/Shalini_AVC

24 Hours

Filter (1)



By default, hourly data is shown



SSID: AVC_testing

SUMMARY

13

Business Relevant Applications

7.4 M

Data Use

Time Range

☐ 3 Hours ☒ 24 Hours ☐ 7 Days

Start Date

7 / 17 / 2024

4:23 PM

End Date

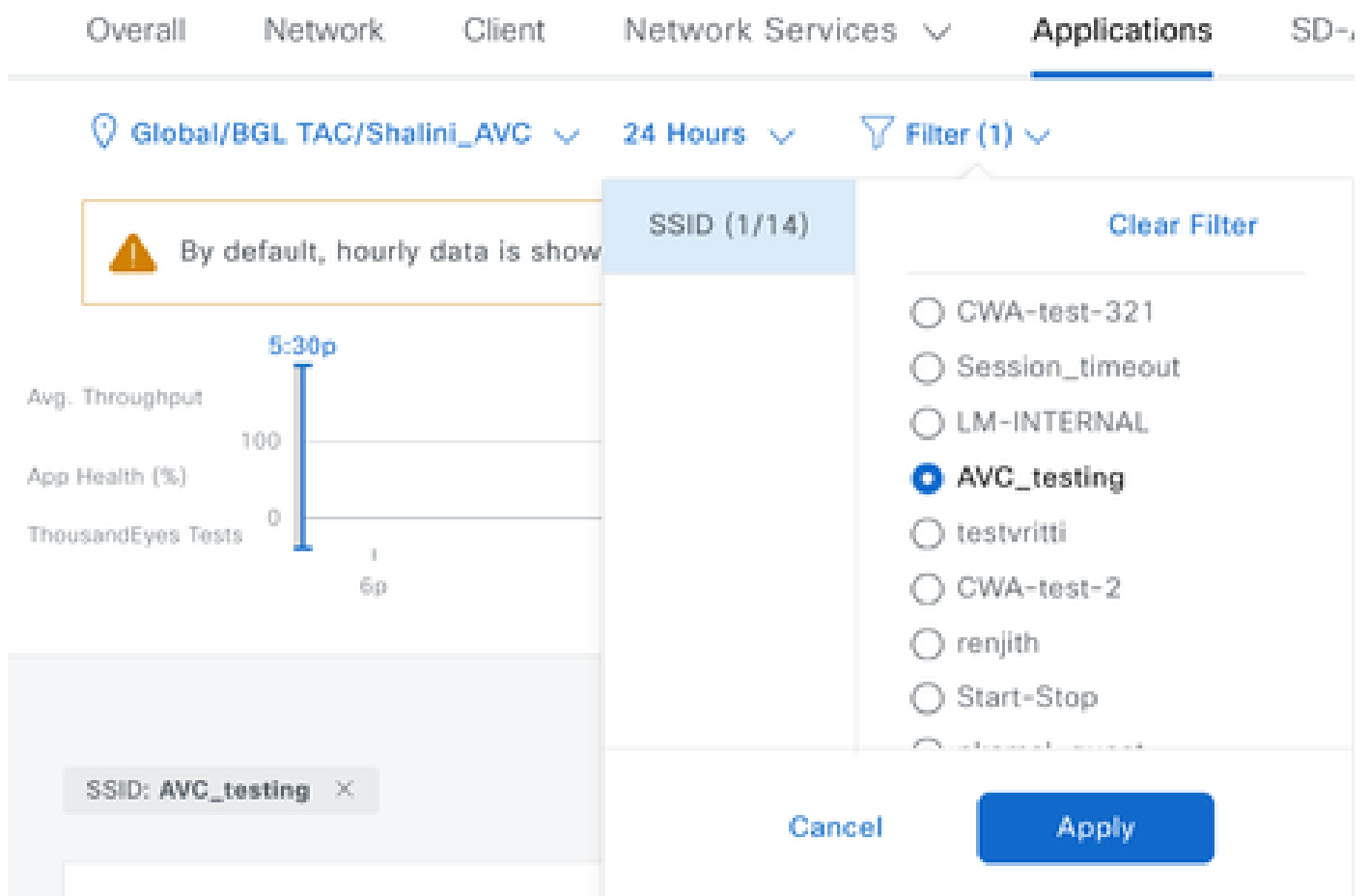
7 / 18 / 2024

4:23 PM

Cancel

Apply

Time Filter to display AVC statistics



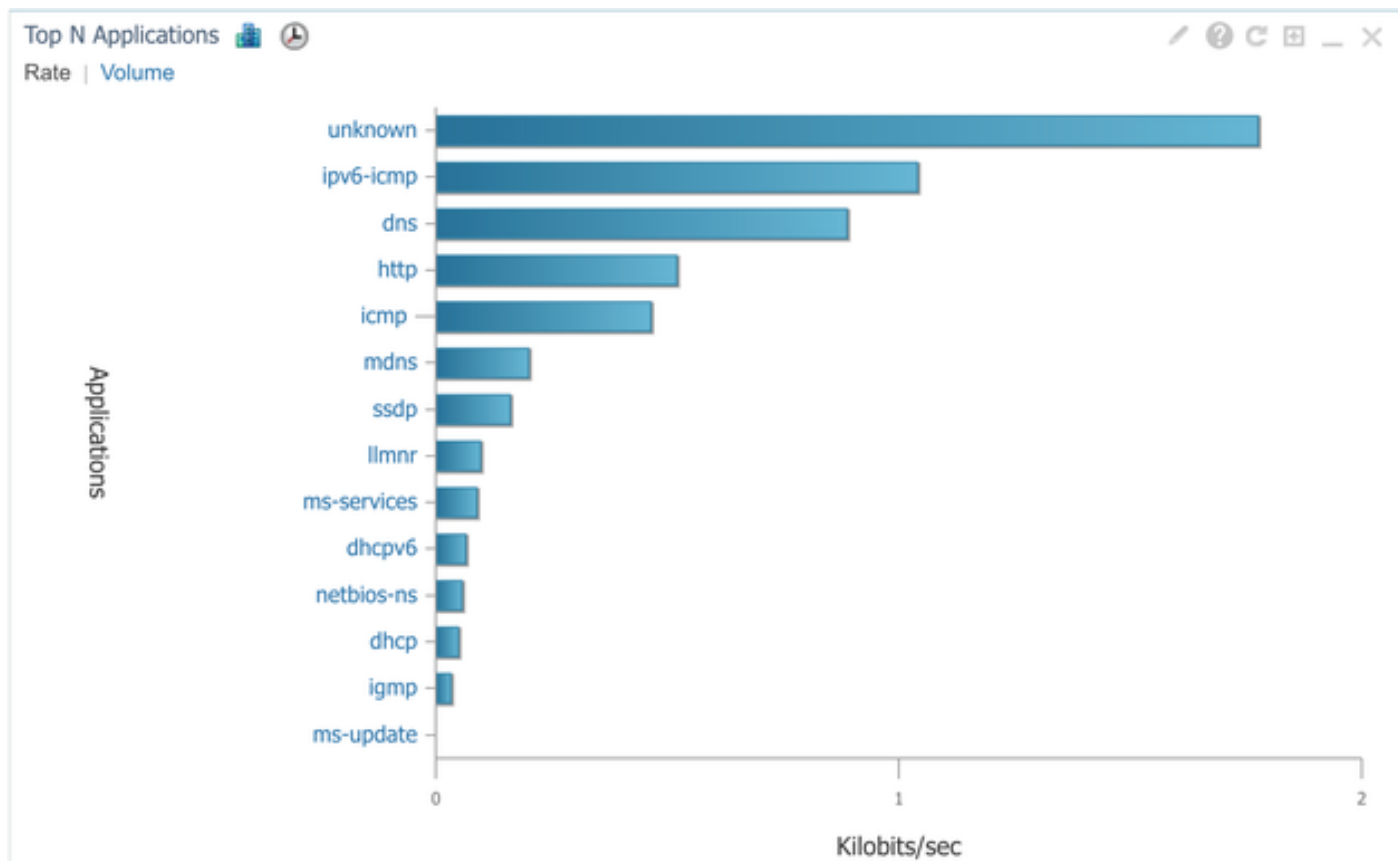
SSID Filter to display AVC Statistics

On External NetFlow Collector

Example1: Cisco Prime as Netflow Collector

When Cisco Prime is used as the NetFlow collector, the 9800 WLC appears as a data source sending NetFlow data, and the NetFlow template is automatically created based on the data transmitted by the 9800 WLC.

From the packet capture taken on 9800 WLC we can validate it is sending data regarding the applications and network traffic to Cisco Prime continuously.

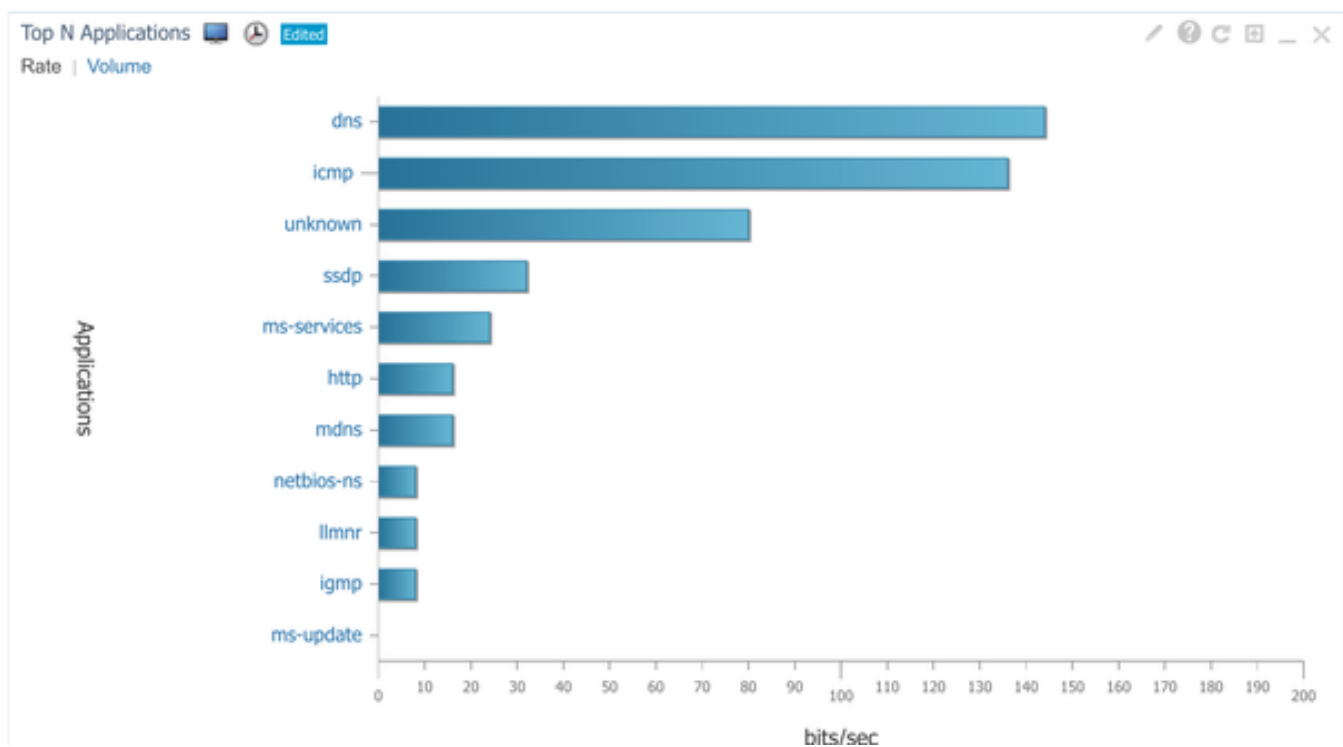


Application Visibility for all Clients

Dashboard / Performance



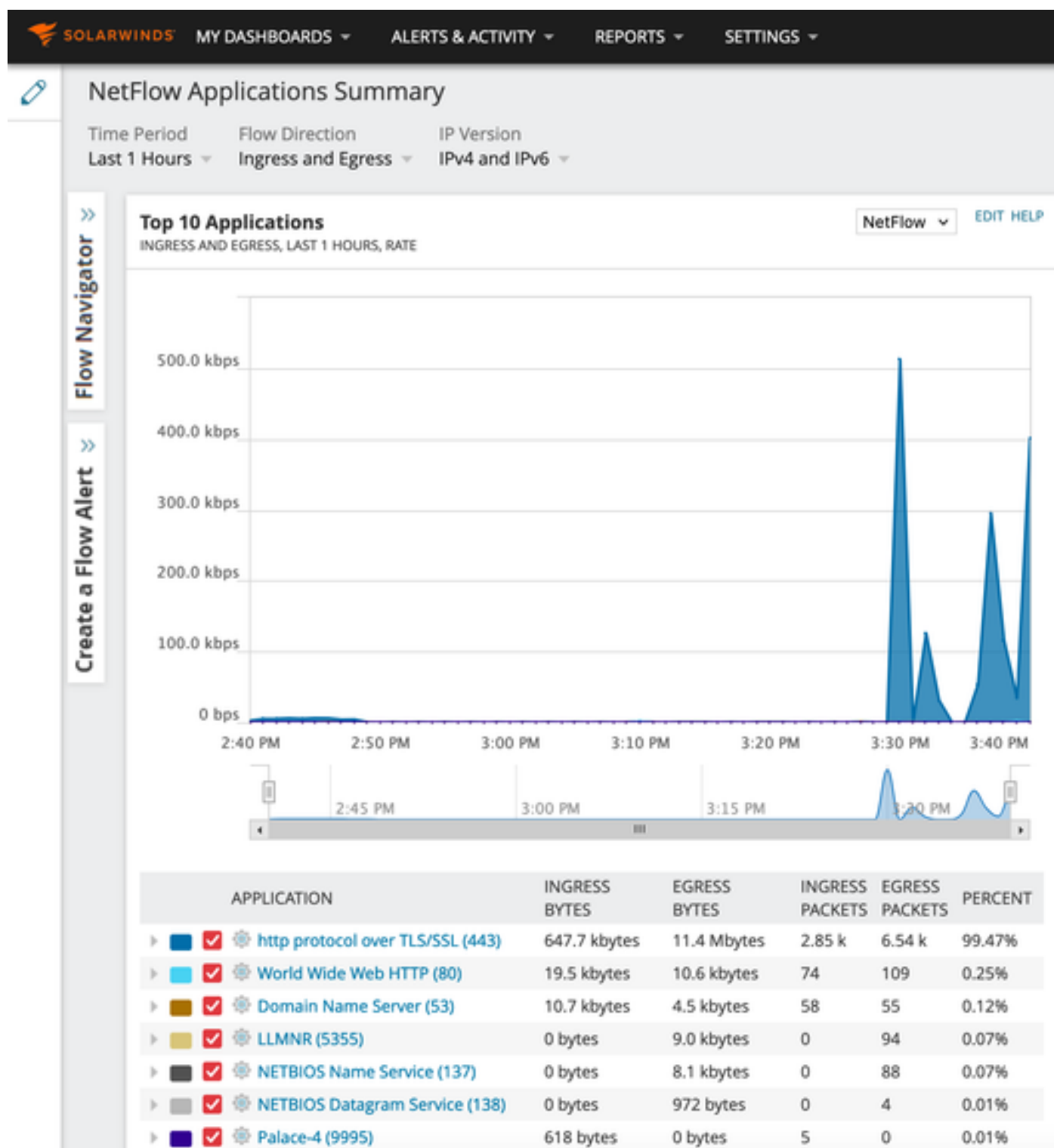
Filters  *Client 10.105.193.80,Una...  *Time Frame Past 1 Hour  Application All  Network Aware



Application of specific Client Using IP address

Example 2: Third party NetFlow Collector

In this example, the third-party NetFlow collector [SolarWinds] is utilized to gather application statistics. The 9800 WLC employs Flexible NetFlow (FNF) to transmit comprehensive data regarding the applications and network traffic, which is then collected by SolarWinds.



Netflow Application Statistics on SolarWind

Traffic Control

Traffic control refers to a set of features and mechanisms used to manage and regulate the flow of network

traffic. Traffic policing or rate limiting are mechanisms used in wireless controller to control the amount of traffic transmitted from client. It monitors the data rate for network traffic and takes immediate action when a predefined rate limit is exceeded. When the traffic exceeds the specified rate, rate limiting can drop the excess packets or mark them down by changing their Class of Service (CoS) or Differentiated Services Code Point (DSCP) values. This can be achieved by configuring QOS in 9800 WLC, You can refer to <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html> to get the overview of how these components work and how can they be configured to achieve different results.

Troubleshooting

Troubleshooting AVC issues involves identifying and resolving problems that possibly affect the AVC ability to accurately identify, classify, and manage application traffic on your wireless network. Common issues can include problems with traffic classification, policy enforcement, or reporting. Here are some steps and considerations when troubleshooting AVC issues on a Catalyst 9800 WLC:

- Verify AVC Configuration: Ensure that AVC is properly configured on the WLC and associated with the correct WLANs and profiles.
- When setting up AVC through the GUI, it automatically assign port 9995 as the default. However, if you are using an External Collector, verify which port it is configured to listen on for NetFlow traffic. It is crucial to accurately configure this port number to match your netflow collector settings.
- Verify the AP Model and deployment mode support.
- Refer to limitations on 9800 WLC while implementing AVC in your wireless network.

Log Collection

WLC logs

1. Enable timestamp to have time reference for all the commands.

```
9800WLC#term exec prompt timestamp
```

2. To review the configuration

```
9800WLC#show tech-support wireless
```

3. You can verify the avc status and netflow statistics.

Check the AVC configuration status.

```
9800WLC#show avc status wlan <wlan_name>
```

Check FNFv9 packets counts and decode status punted to Control Plane (CP).

```
9800WLC#show platform software wlcvc status decoder
```

Check Statistics from NetFlow (FNF Cache).

```
9800WLC#show flow monitor <Flow_Monitor_Name>
```

Check Top n application usage for each wlan, where n = <1-30> Enter the number of applications.

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
```

Check top n application usage for each client, where n = <1-30> Enter the number of applications.

```
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
```

Check top n clients connected to specific wlan using the specific application, where n=<1-10> Enter the number of clients.

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
```

Check the nbar statistics.

```
9800WLC#show ip nbar protocol-discovery
```

4. Set logging level to debug/verbose.

```
9800WLC#set platform software trace all debug/verbose
```

!! To View the collected logs

```
9800WLC#show logging profile wireless internal start last clear to-file bootflash:<File_Name>
```

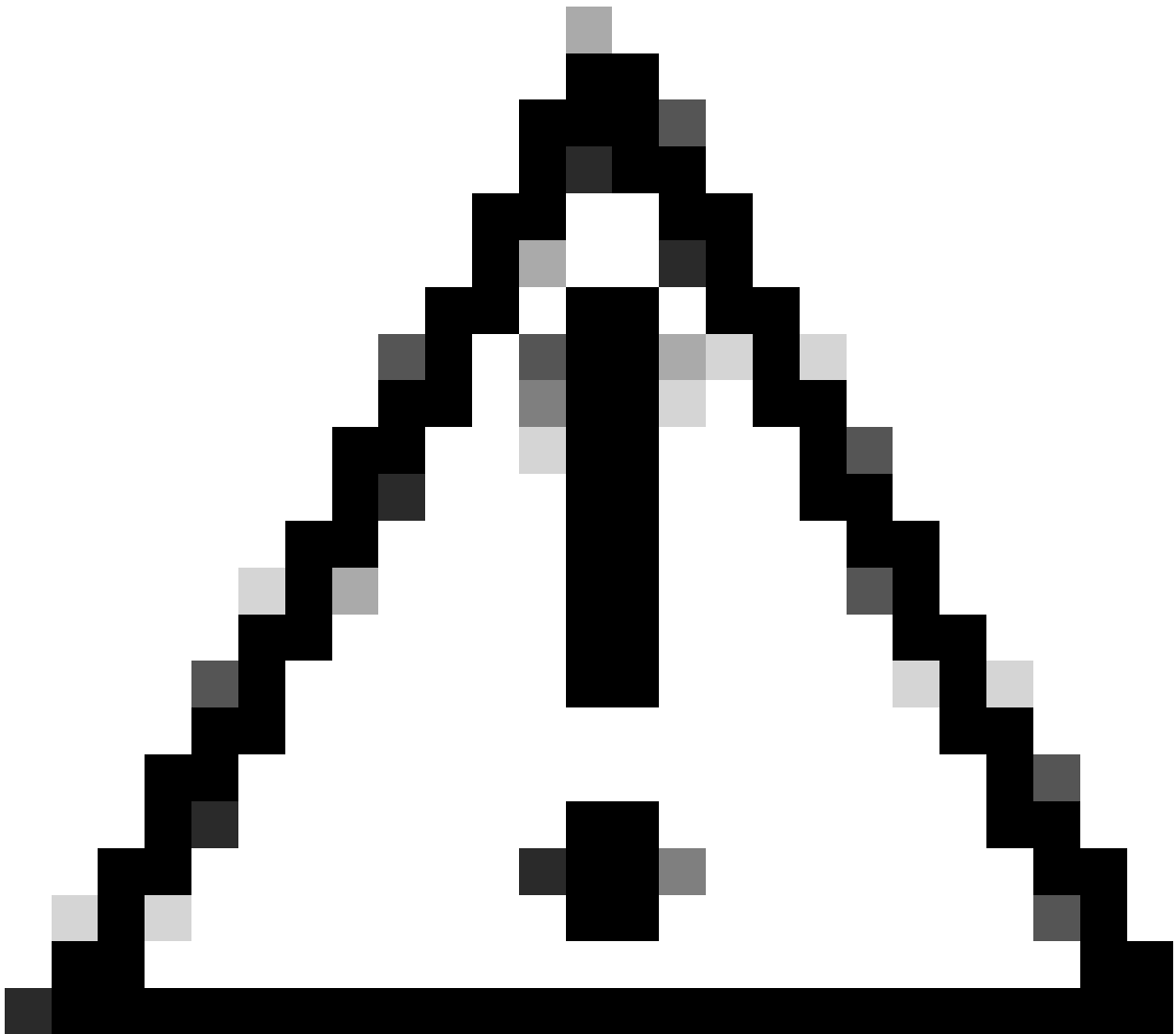
!!Set logging level back to notice post troubleshooting

```
9800WLC#set platform software trace wireless all debug/verbose
```

5. Enable Radioactive (RA) Trace for client MAC address to validate the AVC stats.

Via CLI

```
9800WLLC#debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting ti
9800WLC#no debug wireless mac <Client_MAC>
!!WLC generates a debug trace file with Client_info, command to check for debug trace file generated.
9800WLC#dir bootflash: | i debug
```



Caution: The conditional debugging enables debug-level logging which in turn increases the volume of the logs generated. Leaving this running reduces how far back in time you can view logs from. So, it is recommended to always disable debugging at the end of the troubleshooting session.

```
# clear platform condition all
# undebug all
```

Via GUI

Step 1. Navigate to Troubleshooting > Radioactive Trace .

Step 2. Click **Add** and enter a client Mac address that you want to troubleshoot. You can add several Mac addresses to track.

Step 3. When you are ready to start the radioactive tracing, click start. Once started, debug logging is written to disk about any control plane processing related to the tracked MAC addresses.

Step 4. When you reproduce the issue you want to troubleshoot, click **Stop** .

Step 5. For each mac address debugged, you can generate a log file collating all the logs pertaining to that mac address by clicking **Generate** .

Step 6. Choose how long back you want your collated log file to go and click **Apply to Device**.

Step 7. You can now download the file by clicking the small icon next to the file name. This file is present in the boot flash drive of the controller and can also be copied out of the box through CLI.

Here is a glimpse of AVC debugs in RA traces

```
2024/07/20 20:15:24.514842337 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514865665 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514875837 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:40.530177442 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
```

6. Embedded Captures filtered by client MAC address in both directions, Client inner MAC filter available after 17.1.

It is particularly useful when using an external collector, as it helps confirm whether the WLC is transmitting NetFlow data to the intended port as expected.

Via CLI

```
monitor capture MYCAP clear
monitor capture MYCAP interface <Interface> both
monitor capture MYCAP buffer size 100
monitor capture MYCAP match any
monitor capture MYCAP inner mac CLIENT_MAC@
monitor capture MYCAP start
!! Inititiate different application traffic from user
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap
```

Via GUI

Step 1. Navigate to **Troubleshooting > Packet Capture > +Add** .

Step 2. Define the name of the packet capture. A maximum of 8 characters is allowed.

Step 3. Define filters, if any.

Step 4. Check the box to Monitor Control Traffic if you want to see traffic punted to the system CPU and injected back into the data plane.

Step 5. Define buffer size. A maximum of 100 MB is allowed.

Step 6. Define limit, either by duration which allows a range of 1 - 1000000 seconds or by number of packets which allows a range of 1 - 100000 packets, as desired.

Step 7. Choose the interface from the list of interfaces in the left column and select the arrow to move it to the right column.

Step 8. Click on **Apply to Device**.

Step 9. To start the capture, select **Start** .

Step 10. You can let the capture run to the defined limit. To manually stop the capture, select **Stop**.

Step 11. Once stopped, an **Export** button becomes available to click with the option to download the capture file (.pcap) on the local desktop via HTTP or TFTP server or FTP server or local system hard disk or flash.

AP Logs

On Fabric and Flex modes

1. show tech to have all config details and client stats for the AP.
2. show avc nbar statistics nbar stats from AP
3. AVC debugs

```
AP#term mon
```

```
AP#debug capwap client avc <all/detail/error/event>
```

```
AP#debug capwap client avc netflow <all/detail/error/event/packet>
```

Related Information

[AVC Configuration Guide](#)

[Rate Limiting on 9800 WLC](#)