

Información sobre AVC en el controlador de LAN inalámbrica Catalyst 9800

Contenido

[Introducción](#)

[Requisito previo](#)

[Información sobre Application Visibility and Control \(AVC\)](#)

[Cómo funciona AVC](#)

[Reconocimiento de aplicaciones basadas en red \(NBAR\)](#)

[Habilitar el protocolo NBAR en el perfil de política](#)

[Actualización de NBAR en 9800 WLC](#)

[Netflow](#)

[Flexible NetFlow](#)

[Monitor de Flujo](#)

[Puntos de acceso compatibles con AVC](#)

[Compatibilidad con diferentes modos de implementación de 9800](#)

[Restricciones al implementar AVC en 9800](#)

[Topología de red](#)

[AP en modo local](#)

[AP en modo flexible](#)

[Configuración de AVC en 9800 WLC](#)

[Exportador local](#)

[Recopilador de NetFlow externo](#)

[Configuración de AVC en 9800 WLC mediante Cisco Catalyst Center](#)

[Verificación de AVC](#)

[En 9800](#)

[En DNAC](#)

[En colector de NetFlow externo](#)

[Ejemplo 1: Cisco Prime como NetFlow Collector](#)

[Ejemplo 2: Recopilador de NetFlow de terceros](#)

[Control de tráfico](#)

[Resolución de problemas](#)

[Recopilación de registros](#)

[Registros WLC](#)

[Registros de AP](#)

[Información Relacionada](#)

Introducción

Este documento describe la Visibilidad y control de la aplicación (AVC) en un WLC Cisco Catalyst 9800 que permite una administración precisa del tráfico de la aplicación.

Requisito previo

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Cisco WLC 9800.
- Conocimiento básico de AP de modo de conexión flexible y local.
- Los puntos de acceso deben ser compatibles con AVC. (No se aplica con el AP de modo local)
- Para que funcione la parte de control de AVC (QoS), debe configurarse la función de visibilidad de aplicaciones con FNF.

Información sobre Application Visibility and Control (AVC)

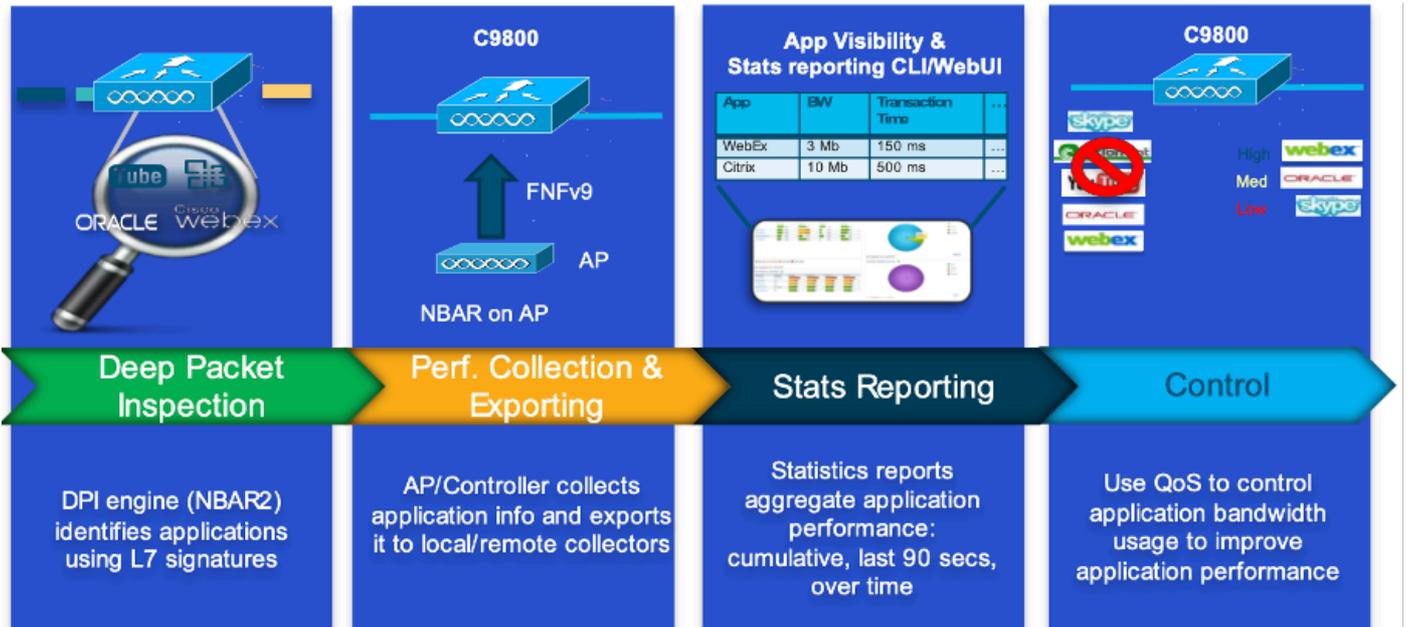
Visibilidad y control de aplicaciones (AVC) es el enfoque líder de Cisco para la tecnología de inspección profunda de paquetes (DPI) tanto en redes inalámbricas como por cable. Con AVC, puede realizar análisis en tiempo real y crear políticas para reducir eficazmente la congestión de la red, minimizar el costoso uso de enlaces de red y evitar actualizaciones de infraestructura innecesarias. En resumen, AVC permite a los usuarios alcanzar un nivel completamente nuevo de reconocimiento y modelado del tráfico a través de Network Based Application Recognition (NBAR). Los paquetes NBAR que se ejecutan en el WLC 9800 se utilizan para DPI y los resultados se notifican mediante Flexible NetFlow (FNF).

Además de la visibilidad, AVC proporciona la capacidad de priorizar, bloquear o regular los diferentes tipos de tráfico. Por ejemplo, los administradores pueden crear políticas que den prioridad a las aplicaciones de voz y vídeo para garantizar la calidad del servicio (QoS) o limitar el ancho de banda disponible para las aplicaciones no esenciales durante las horas punta de la empresa. También se puede integrar con otras tecnologías de Cisco, como Cisco Identity Services Engine (ISE) para políticas de aplicaciones basadas en identidad y Cisco Catalyst Center para una gestión centralizada.

Cómo funciona AVC

AVC utiliza tecnologías avanzadas como FNF y el motor NBAR2 para DPI. Al analizar e identificar los flujos de tráfico mediante el motor NBAR2, los flujos específicos se marcan con el protocolo o la aplicación reconocidos. El controlador recopila todos los informes y los presenta a través de los comandos show, la interfaz de usuario web o los mensajes de exportación de NetFlow adicionales a los recopiladores de NetFlow externos como Prime.

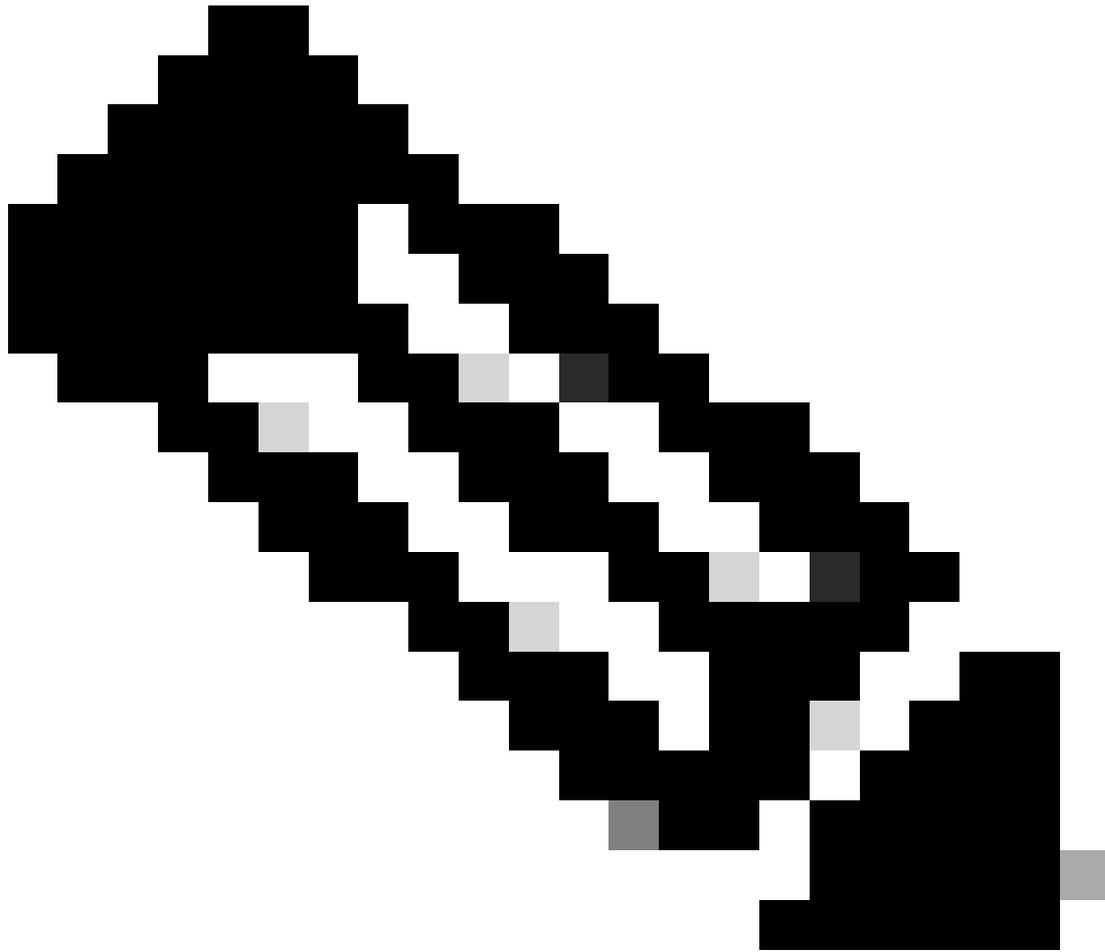
Una vez establecida la visibilidad de la aplicación, los usuarios pueden crear reglas de control con mecanismos de regulación para los clientes mediante la configuración de la calidad del servicio (QoS).



Mecanismo de trabajo de AVC

Reconocimiento de aplicaciones basadas en red (NBAR)

NBAR es un mecanismo integrado en el WLC 9800, que se utiliza para realizar DPI para identificar y clasificar una amplia variedad de aplicaciones que se ejecutan en una red. Puede reconocer y clasificar un gran número de aplicaciones, incluidas las aplicaciones cifradas y asignadas dinámicamente a los puertos, que a menudo son invisibles para las tecnologías de inspección de paquetes tradicionales.



Nota: Para aprovechar NBAR en el WLC Catalyst 9800, es necesario habilitarlo y configurarlo correctamente, a menudo junto con perfiles AVC específicos que definen las acciones adecuadas que se deben tomar en función de la clasificación del tráfico.

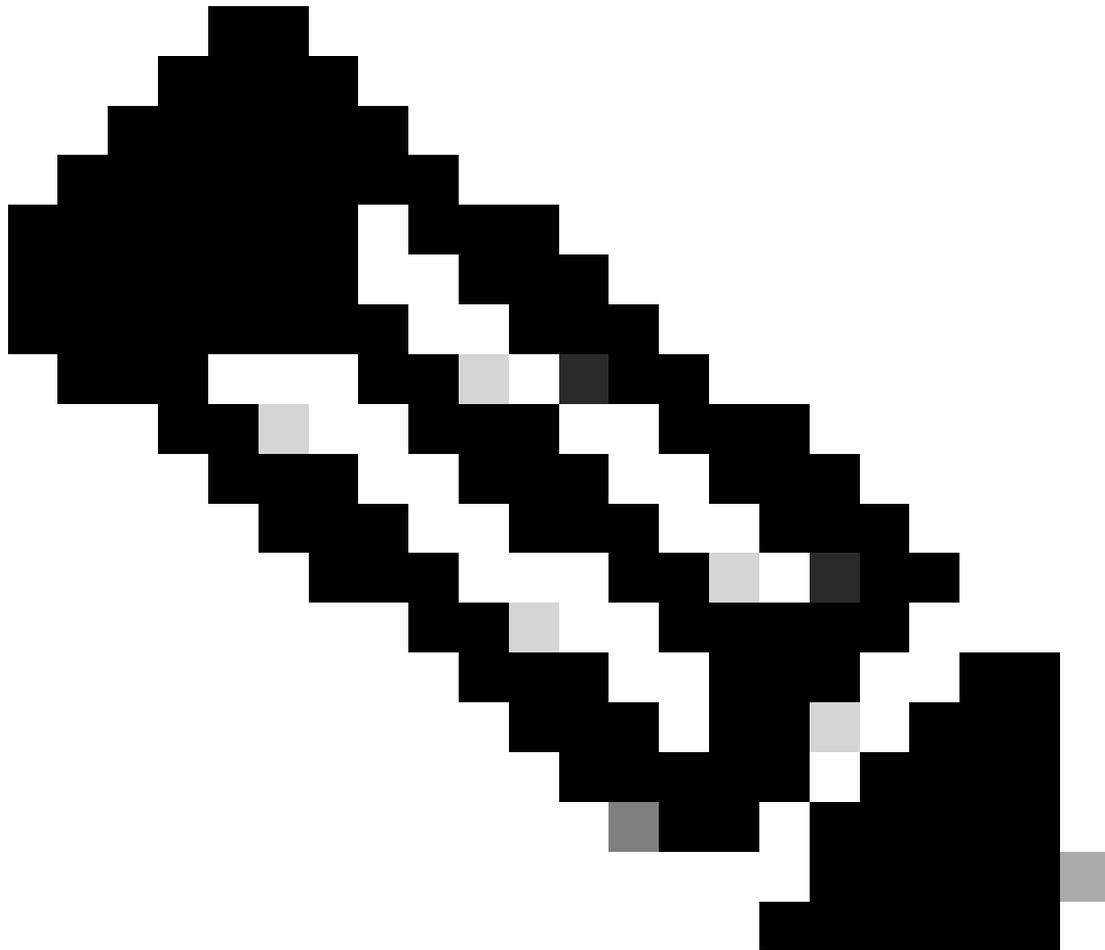
NBAR continúa siendo actualizado periódicamente, y es importante mantener el software del WLC actualizado para asegurarse de que el conjunto de funciones de NBAR se mantenga actualizado y efectivo.

Puede encontrar una lista completa de los protocolos admitidos en las últimas versiones en https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Habilitar el protocolo NBAR en el perfil de política

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

```
9800WLC(config-wireless-policy)#end
```



Nota: el perfil de política % debe desactivarse antes de realizar esta operación.

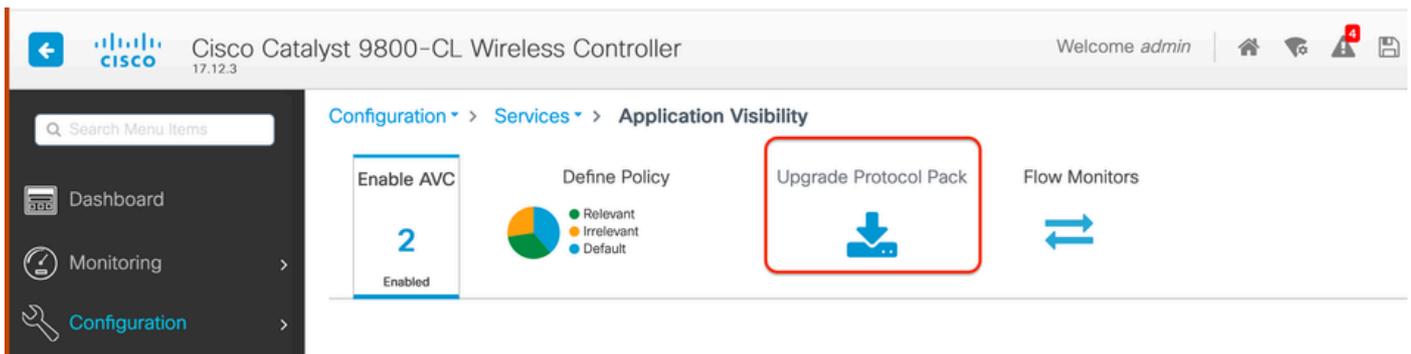
```
9800WLC#show wireless profile policy detailed AVC_testing | in NBAR  
NBAR Protocol Discovery : Enabled
```

Actualización de NBAR en 9800 WLC

El WLC 9800 ya tiene ~1500 aplicaciones reconocibles. En el caso de que se lance una nueva aplicación, el protocolo para la misma se actualizará en la última versión de NBAR, que deberá descargarse de la página de descarga de software para el modelo 9800 específico.

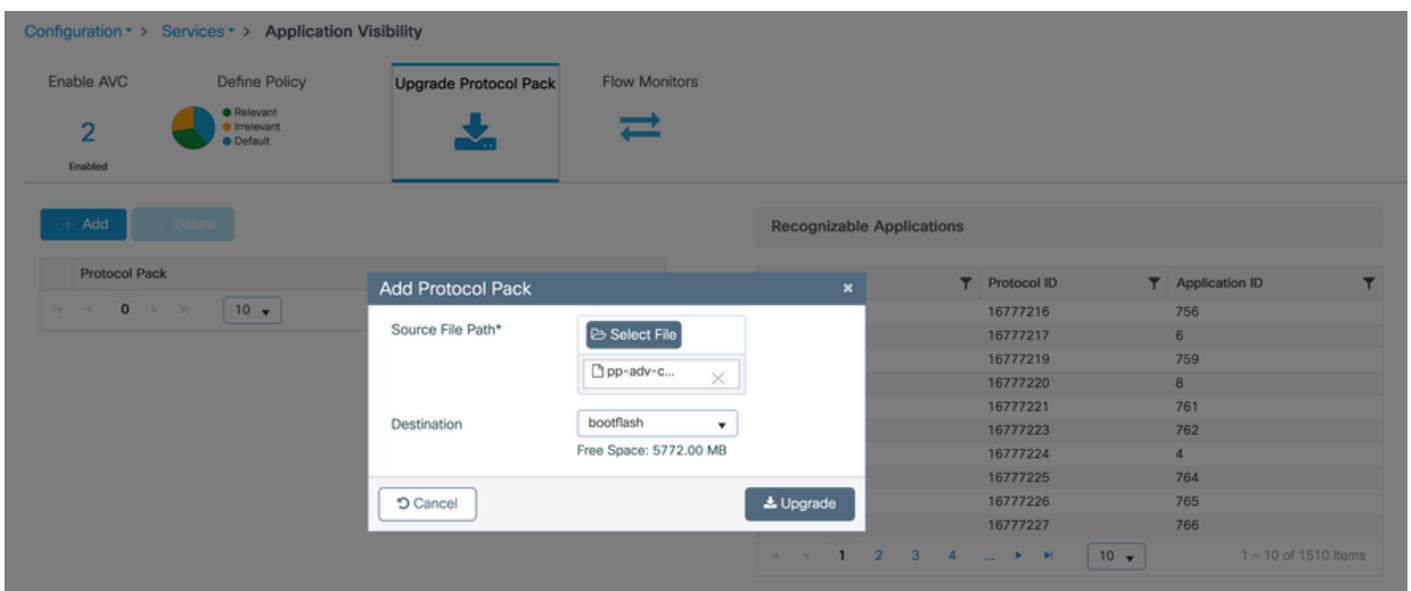
Mediante GUI

Vaya a Configuration > Services > Application Visibility. Haga clic en Upgrade Protocol Pack .



Sección de carga de protocolo en 9800 WLC

Haga clic en Agregar, luego elija el paquete de protocolo que se descargará y haga clic en Actualizar .



Agregar protocolo NBAR

Una vez que se haya realizado la actualización, verá que se ha agregado el paquete de protocolo.

Enable AVC 2 Enabled

Define Policy

- Relevant
- Irrelevant
- Default

Upgrade Protocol Pack

Flow Monitors

+ Add × Delete

Protocol Pack
<input type="checkbox"/> bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack

1 10 1 - 1 of 1 items

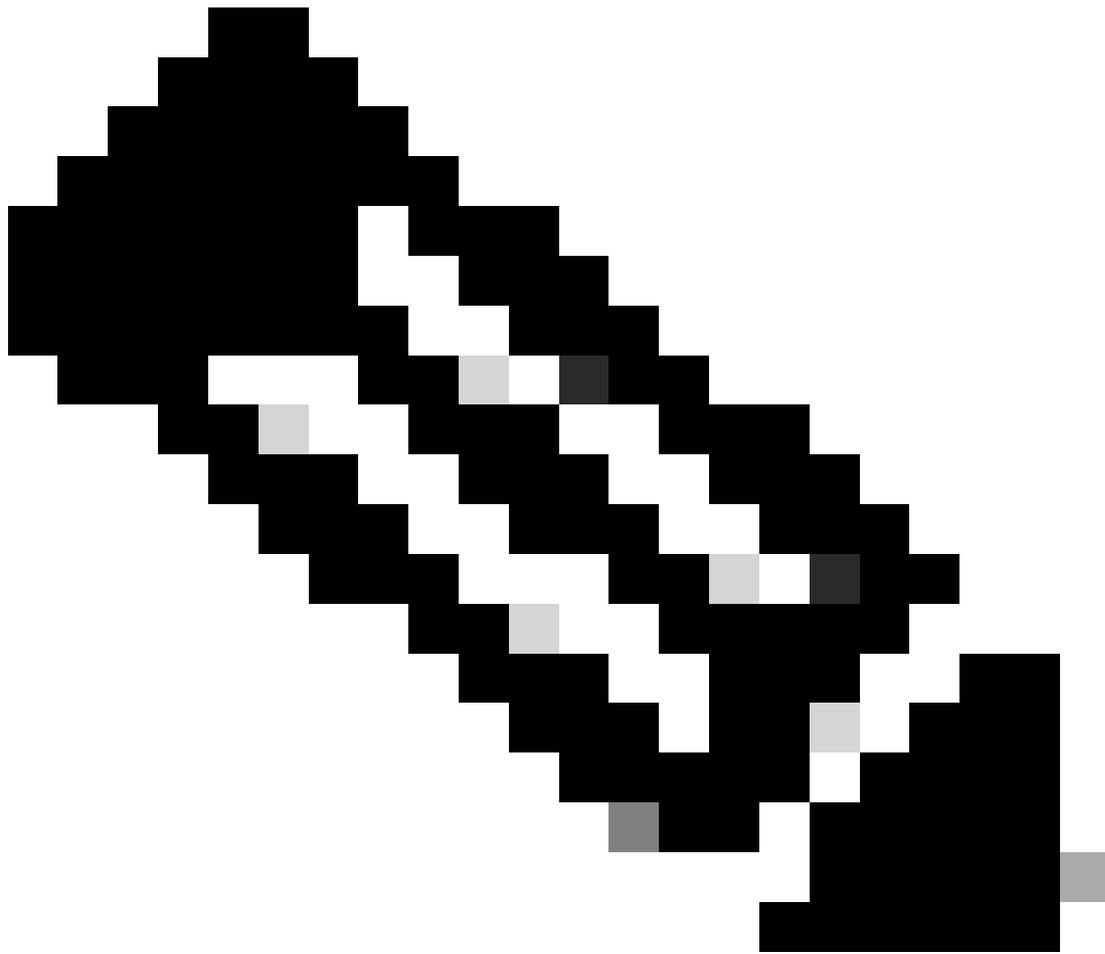
Verificación del paquete de protocolos

Mediante 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
```



Nota: no habrá ninguna interrupción del servicio durante la actualización del paquete de protocolo NBAR.

Netflow

NetFlow es un protocolo de red utilizado para recopilar información de tráfico IP y supervisar los datos de flujo de la red. Se utiliza principalmente para el análisis del tráfico de red y la supervisión del ancho de banda. A continuación se presenta una descripción general de cómo funciona NetFlow en los controladores Cisco Catalyst 9800 Series:

- Recopilación de datos: el WLC 9800 recopila datos sobre el tráfico IP que fluye a través de ellos. Estos datos incluyen información como las direcciones IP de origen y destino, los puertos de origen y destino, los protocolos utilizados, la clase de servicio y la causa de la terminación del flujo.
- Registros de Flujo: Los datos recopilados se organizan en registros de flujo. Un flujo se define como una secuencia unidireccional de paquetes que comparten un conjunto de

atributos comunes, como la misma IP de origen/destino, puertos de origen/destino y tipo de protocolo.

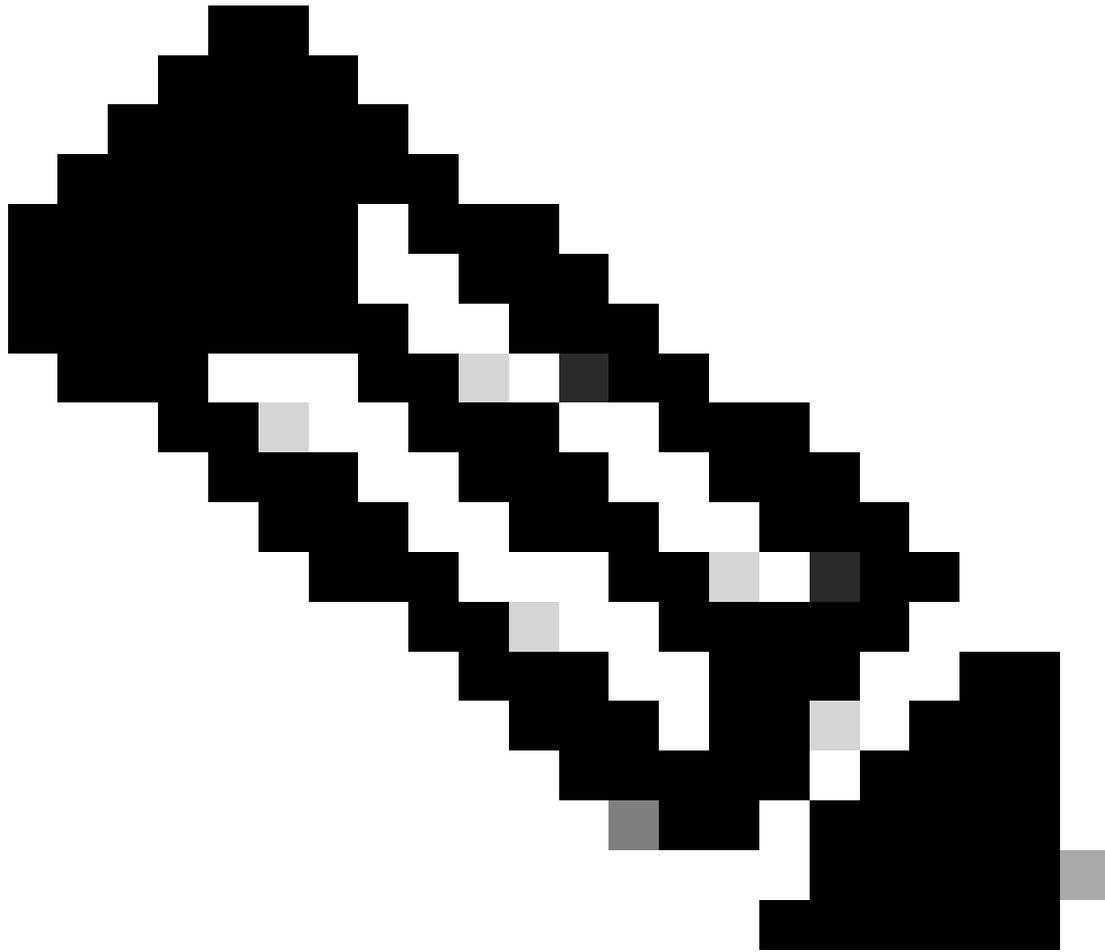
- **Exportación de Datos:** Los registros de flujo se exportan periódicamente desde el dispositivo con NetFlow activado a un recopilador de NetFlow. El colector puede ser un WLC local o un servidor dedicado o una aplicación de software que recibe, almacena y procesa los datos de flujo.
- **Análisis:** puede utilizar los recopiladores y las herramientas de análisis de NetFlow para visualizar los patrones de tráfico, identificar el ancho de banda, detectar flujos de tráfico inusuales indicativos de infracciones de seguridad, optimizar el rendimiento de la red y planificar la expansión de la red.
- **Información específica de conexión inalámbrica:** en el contexto de los controladores inalámbricos, NetFlow puede incluir información adicional específica de las redes inalámbricas, como el SSID, los nombres de AP, las direcciones MAC del cliente y otros detalles relevantes para el tráfico Wi-Fi.

Flexible NetFlow

Flexible NetFlow (FNF) es una versión avanzada de NetFlow tradicional y es compatible con los controladores de LAN inalámbrica (WLC) de Cisco Catalyst serie 9800. Proporciona más opciones de personalización para realizar el seguimiento, la supervisión y el análisis de los patrones de tráfico de red. Las características clave de Flexible NetFlow en el WLC Catalyst 9800 incluyen:

- **Personalización:** FNF permite a los usuarios definir qué información desean recopilar del tráfico de red. Esto incluye una amplia gama de atributos de tráfico, como direcciones IP, números de puerto, marcas de tiempo, recuentos de paquetes y bytes, tipos de aplicaciones, etc.
- **Visibilidad mejorada:** al aprovechar FNF, los administradores obtienen una visibilidad detallada de los tipos de tráfico que fluyen por la red, lo que resulta esencial para la planificación de la capacidad, la facturación de red basada en el uso, el análisis de la red y la supervisión de la seguridad.
- **Independencia de protocolo:** FNF es lo suficientemente flexible como para admitir varios protocolos más allá de IP, lo que lo hace adaptable a diferentes tipos de entornos de red.

En el WLC Catalyst 9800, FNF se puede configurar para exportar registros de flujo a un colector NetFlow externo o a una aplicación de análisis. Estos datos se pueden utilizar para la resolución de problemas, la planificación de la red y el análisis de seguridad. La configuración de FNF implica definir un registro de flujo (qué recopilar), un exportador de flujo (dónde enviar los datos) y conectar el monitor de flujo (que une el registro y el exportador) a las interfaces adecuadas.



Nota: FNF puede enviar 17 registros de datos diferentes (tal y como se definen en RFC 3954) al recopilador externo de Netflow de terceros, como Stealthwatch, Solarwinds y otros, que son: etiqueta de aplicación, dirección MAC del cliente, dirección MAC del AP, ID de WLAN, IP de origen, IP de destino, puerto de origen, puerto de destino, protocolo, tiempo de inicio del flujo, tiempo de fin del flujo, dirección, salida de paquetes, recuento de bytes, ID de VLAN (modo local): gestión/cliente y TOS: valor DSCP

Monitor de Flujo

Un monitor de flujo es un componente que se utiliza junto con Flexible NetFlow (FNF) para capturar y analizar datos de tráfico de red. Desempeña un papel fundamental en la supervisión y la comprensión de los patrones de tráfico para la gestión de la red, la seguridad y la resolución de problemas. El monitor de flujo es esencialmente una instancia aplicada de FNF que recopila y realiza un seguimiento de los datos de flujo en función de criterios definidos. Se asocia a tres elementos principales:

- Registro de flujo: define los datos que el monitor de flujo debe recopilar del tráfico de red.

Especifica las claves (como las direcciones IP de origen y destino, los puertos y los tipos de protocolo) y los campos que no son claves (como los contadores de paquetes y bytes, las marcas de tiempo) que se incluirán en los datos de flujo.

- Exportador de flujo: especifica el destino al que se deben enviar los datos de flujo recopilados. Incluye detalles como la dirección IP del colector de NetFlow, el protocolo de transporte (generalmente UDP) y el número de puerto de destino donde escucha el colector.
- Monitor de flujo: el propio monitor de flujo une el registro de flujo y el exportador de flujo y los aplica a una interfaz o WLAN para iniciar realmente el proceso de supervisión. Determina cómo se deben recopilar y exportar los datos de flujo en función de los criterios establecidos en el registro de flujo y el destino establecido en el exportador de flujo.

Puntos de acceso compatibles con AVC

AVC sólo es compatible con los siguientes puntos de acceso:

- Puntos de acceso Cisco Catalyst serie 9100
- Punto de acceso Cisco Aironet serie 2800
- Puntos de acceso Cisco Aironet serie 3800
- Puntos de acceso Cisco Aironet serie 4800

Compatibilidad con diferentes modos de implementación de 9800

Modo de implementación	WLC 9800	Punto de acceso de onda 1	Punto de acceso de onda 2	Punto de acceso Wi-Fi 6
Modo local (Switching central)	Tráfico de IPv4: Compatible con AVC Compatibilidad con FNF Tráfico IPv6: Compatible con AVC Compatibilidad con FNF	Procesamiento a nivel WLC	Procesamiento a nivel WLC	Procesamiento a nivel WLC
Modo flexible (Switching central)	Tráfico de IPv4: Compatible con AVC Compatibilidad con FNF	Procesamiento a nivel WLC	Procesamiento a nivel WLC	Procesamiento a nivel WLC

	Tráfico IPv6: Compatible con AVC Compatibilidad con FNF			
Modo flexible (Conmutación local)	Procesamiento a nivel de PA	Tráfico de IPv4: Compatible con AVC Compatibilidad con FNF Tráfico IPv6: Compatible con AVC FNF no compatible	Tráfico de IPv4: Compatible con AVC Compatibilidad con FNF Tráfico IPv6: Compatible con AVC Compatibilidad con FNF	Tráfico de IPv4: Compatible con AVC Compatibilidad con FNF Tráfico IPv6: Compatible con AVC Compatibilidad con FNF
Modo local (Fabric)	Procesamiento a nivel de PA	Tráfico de IPv4: AVC no compatible FNF no compatible Tráfico IPv6: AVC no compatible FNF no compatible	Tráfico de IPv4: Compatible con AVC Compatibilidad con FNF Tráfico IPv6: Compatible con AVC Compatibilidad con FNF	Tráfico de IPv4: Compatible con AVC Compatibilidad con FNF Tráfico IPv6: Compatible con AVC Compatibilidad con FNF

Restricciones al implementar AVC en 9800

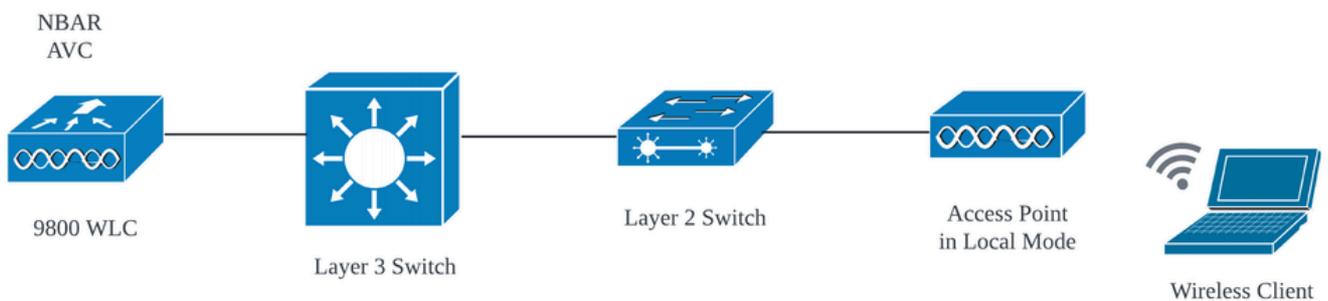
Tanto Application Visibility and Control (AVC) como Flexible NetFlow (FNF) son potentes funciones de los controladores de LAN inalámbrica de Cisco Catalyst serie 9800 que mejoran la visibilidad y el control de la red. Sin embargo, hay algunas limitaciones y consideraciones que se deben tener en cuenta al utilizar estas funciones:

- La itinerancia de capa 2 no se admite en todos los controladores.
- No se admite el tráfico multidifusión.
- Solo las aplicaciones reconocidas con visibilidad de aplicaciones se pueden utilizar para aplicar el control de QoS.
- El enlace de datos no es compatible con los campos de NetFlow en AVC.
- No puede asignar el mismo perfil WLAN al perfil de política no habilitada para AVC y al perfil de política habilitada para AVC.

- No puede utilizar el perfil de política con un mecanismo de conmutación diferente a la misma WLAN para implementar AVC.
- El puerto de administración no admite AVC (Gig 0/0).
- La configuración de políticas de QoS basada en NBAR solo se permite en puertos físicos con cables. La configuración de políticas no se soporta en interfaces virtuales, por ejemplo, VLAN, canal de puerto y otras interfaces lógicas.
- Cuando AVC está habilitado, el perfil AVC admite solo hasta 23 reglas, lo que incluye la regla DSCP predeterminada. La política AVC no se enviará al AP, si las reglas son más de 23.

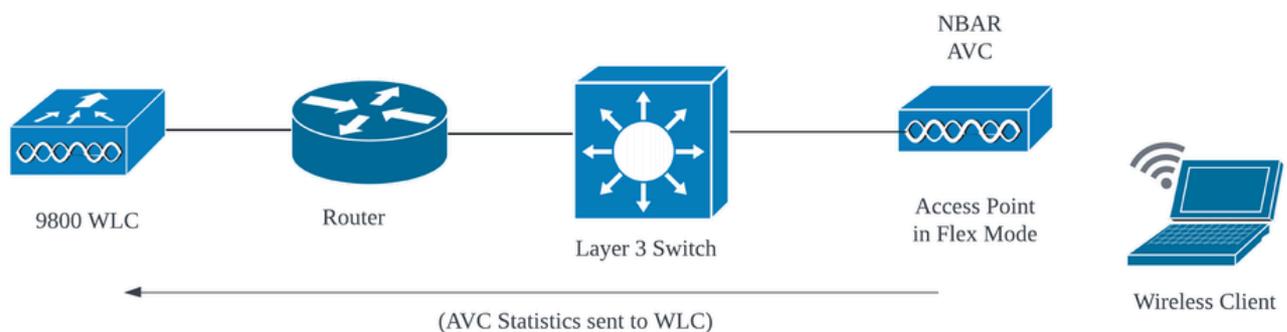
Topología de red

AP en modo local



AVC en modo local AP (conmutación central)

AP en modo flexible



AVC en AP de modo flexible

Configuración de AVC en 9800 WLC

Al configurar AVC en 9800 WLC, puede utilizarlo como NetFlow Collector o puede exportar los

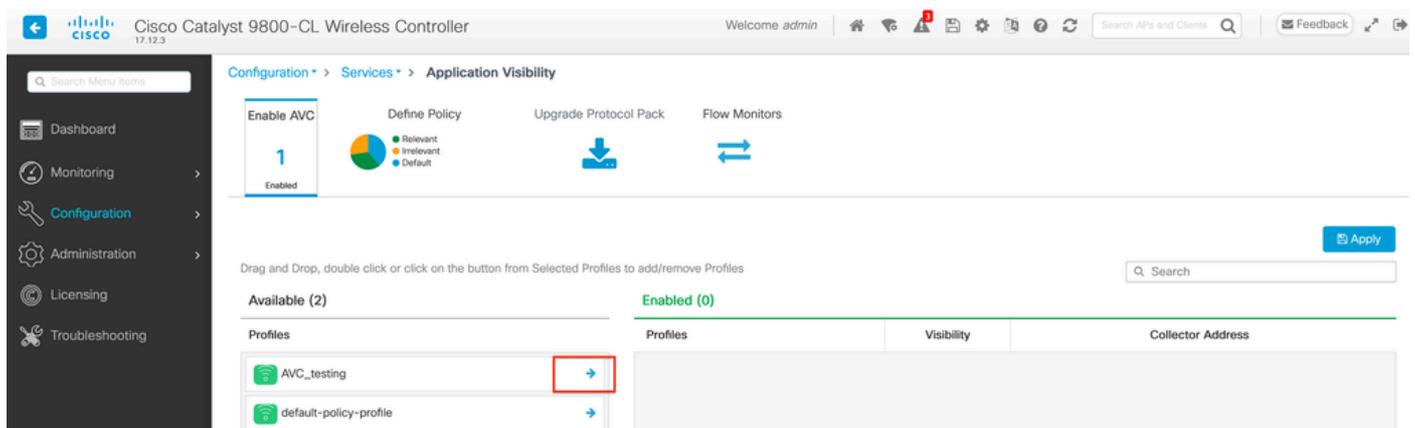
datos de NetFlow a External NetFlow Collector.

Exportador local

En un Cisco Catalyst 9800 Wireless LAN Controller (WLC), un colector de NetFlow local hace referencia a la función incorporada en el WLC que le permite recopilar y almacenar localmente los datos de NetFlow. Esta capacidad permite que el WLC realice el análisis básico de los datos de NetFlow sin la necesidad de exportar los registros de flujo a un colector de NetFlow externo.

Mediante GUI

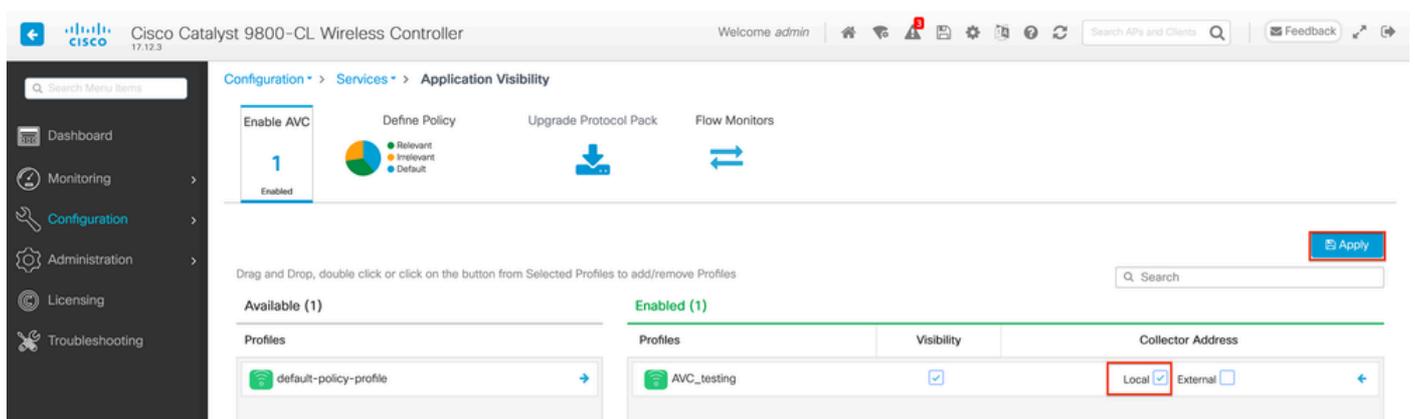
Paso 1: para habilitar AVC en un SSID específico, vaya a Configuration > Services > Application Visibility. Elija el perfil de política concreto para el que desea activar AVC.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Services > Application Visibility. The 'Enable AVC' step is highlighted with a red box and the number '1'. Below this, there are four main sections: 'Define Policy', 'Upgrade Protocol Pack', and 'Flow Monitors'. A table below shows the 'Available (2)' profiles and the 'Enabled (0)' profiles. The 'Available (2)' section lists two profiles: 'AVC_testing' and 'default-policy-profile'. The 'AVC_testing' profile has a red box around its right arrow button, indicating it is being selected for activation.

Habilitación de AVC en el Perfil de Política

Paso 2: Seleccione Local como Netflow Collector y haga clic en Apply.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Services > Application Visibility. The 'Apply' button is highlighted with a red box. Below this, there are four main sections: 'Define Policy', 'Upgrade Protocol Pack', and 'Flow Monitors'. A table below shows the 'Available (1)' profiles and the 'Enabled (1)' profiles. The 'Available (1)' section lists one profile: 'default-policy-profile'. The 'Enabled (1)' section lists one profile: 'AVC_testing'. The 'Collector Address' column for 'AVC_testing' has 'Local' selected with a red box around the 'Local' radio button, and 'External' is unselected.

Selección del Recopilador de NetFlow Local

Observe que los valores de Exportador de NetFlow y NetFlow se han configurado automáticamente de acuerdo con las preferencias especificadas una vez que aplica la configuración AVC.

Puede validar lo mismo si navega hasta Configuration > Services > Application Visibility > Flow

Monitor > Exporter/Monitor .

Configuration > Services > Application Visibility

Enable AVC: 1 Enabled

Define Policy: Relevant, Irrelevant, Default

Upgrade Protocol Pack

Flow Monitors

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

Configuración del Flow Collector Local en 9800 WLC

Configuration > Services > Application Visibility

Enable AVC: 1 Enabled

Define Policy: Relevant, Irrelevant, Default

Upgrade Protocol Pack

Flow Monitors

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

Configuración del Monitor de Flujo con el Recopilador de NetFlow Local

Los monitores de flujo AVC IPv4 e IPv6 se asociarán automáticamente al perfil de política. Vaya a Configuration > Tags & Profile > Policy . Haga clic en Perfil de política > AVC y QOS .

Configuration > Tags & Profiles > Policy

Edit Policy Profile

Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QoS and AVC Mobility Advanced

Auto QoS: None

QoS SSID Policy

Egress: Search or Select

Ingress: Search or Select

QoS Client Policy

Egress: Search or Select

Ingress: Search or Select

Flow Monitor IPv4

Egress: wireless-avc-basic

Ingress: wireless-avc-basic

Flow Monitor IPv6

Egress: wireless-avc-basi

Ingress: wireless-avc-basi

Configuración Del Monitor De Flujo En El Perfil De Política

Mediante CLI

Paso 1: Configure el WLC 9800 como Exportador Local.

```
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
```

Paso 2: Configure el monitor de flujo de red IPv4 e IPv6 para utilizar Local(WLC) como Exportador de NetFlow.

```
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
```

Paso 3: asigne el monitor de flujo IPv4 e IPv6 en el perfil de política para el tráfico de entrada y de salida.

```
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-C1-VM(config-wireless-policy)#no shutdown
9800-C1-VM(config-wireless-policy)#exit
```

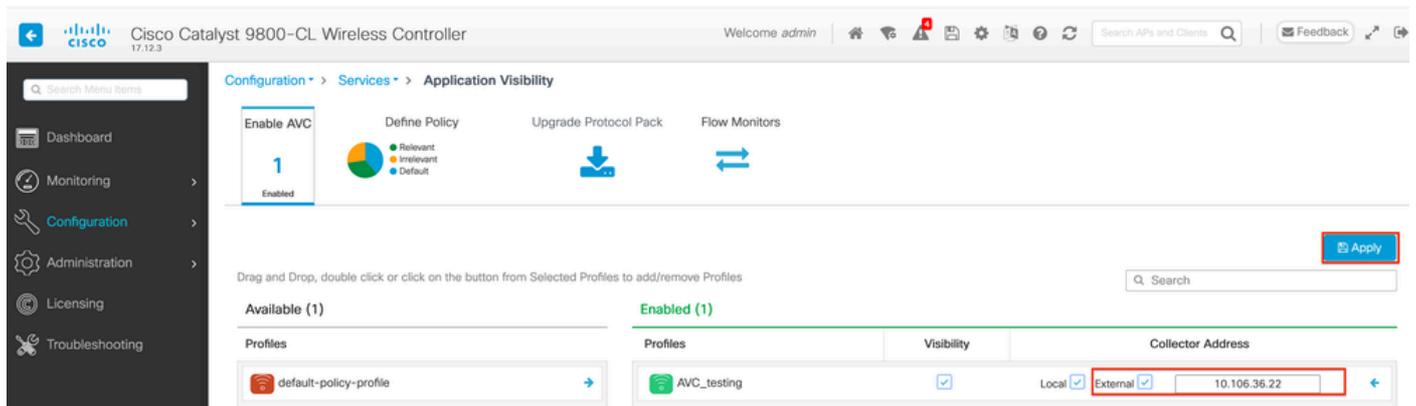
Recopilador de NetFlow externo

Un recopilador NetFlow externo, cuando se utiliza en el contexto de Application Visibility and Control (AVC) en un Cisco Catalyst 9800 Wireless LAN Controller (WLC), es un sistema o servicio dedicado que recibe, agrega y analiza los datos de NetFlow exportados desde el WLC. Puede configurar sólo el colector de NetFlow externo para supervisar la visibilidad de la aplicación o puede utilizarlo junto con el colector local.

Mediante GUI

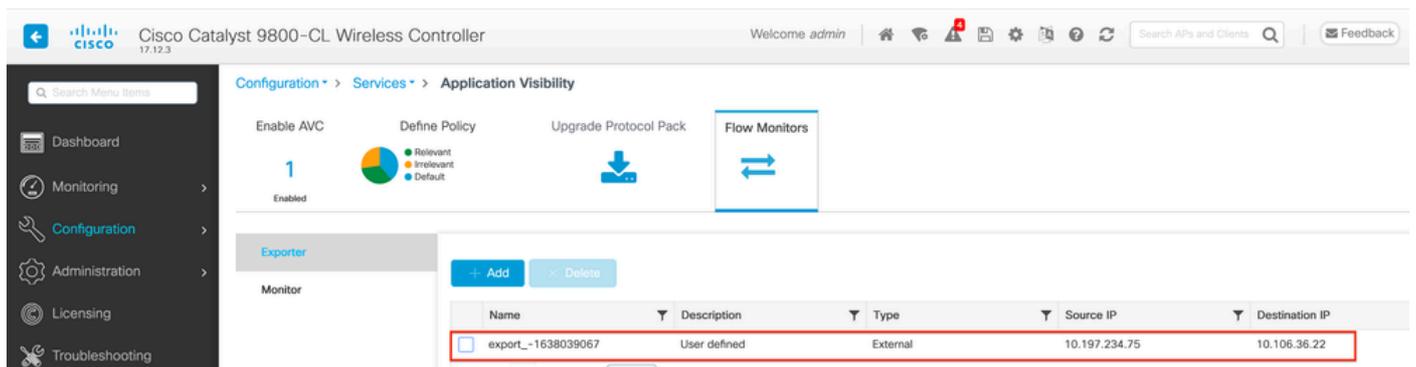
Paso 1: para habilitar AVC en un SSID específico, vaya a Configuración > Servicios > Visibilidad de la aplicación. Elija el perfil de política concreto para el que desea activar AVC. Seleccione

Collector as External (Recopilador externo) y configure la dirección IP de NetFlow Collector como Cisco Prime, SolarWind, StealthWatch y haga clic en Apply (Aplicar).

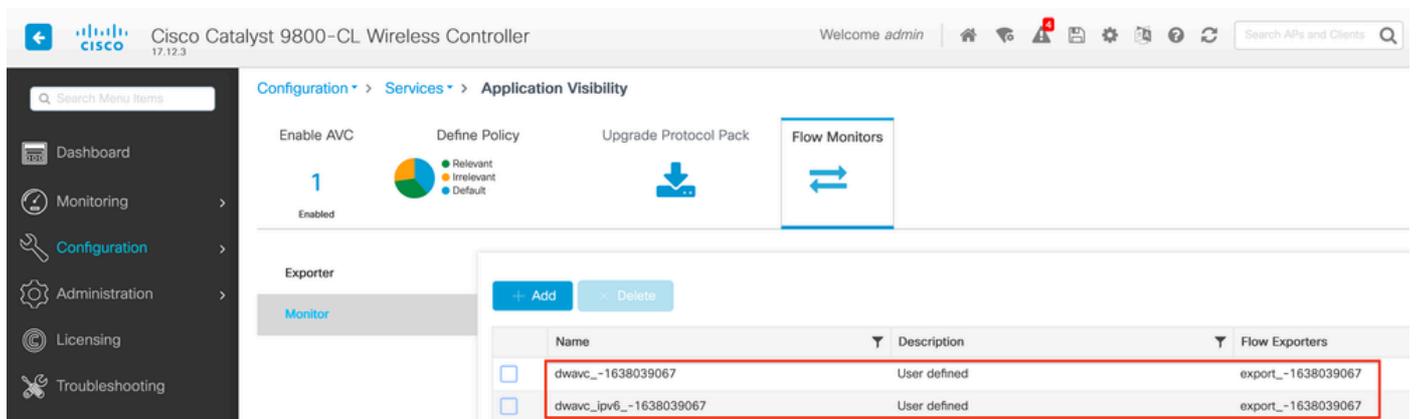


Configuración de AVC para el colector de NetFlow externo

Observe que, una vez que aplica la configuración de AVC, los valores de Exportador de NetFlow y NetFlow se han configurado automáticamente con la dirección IP del Recopilador de NetFlow como exportador y la dirección del Exportador como WLC 9800 con los valores de tiempo de espera predeterminados y el puerto UDP 9995. Puede validar lo mismo si navega hasta Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor .



Configuración del colector de NetFlow externo en el WLC 9800



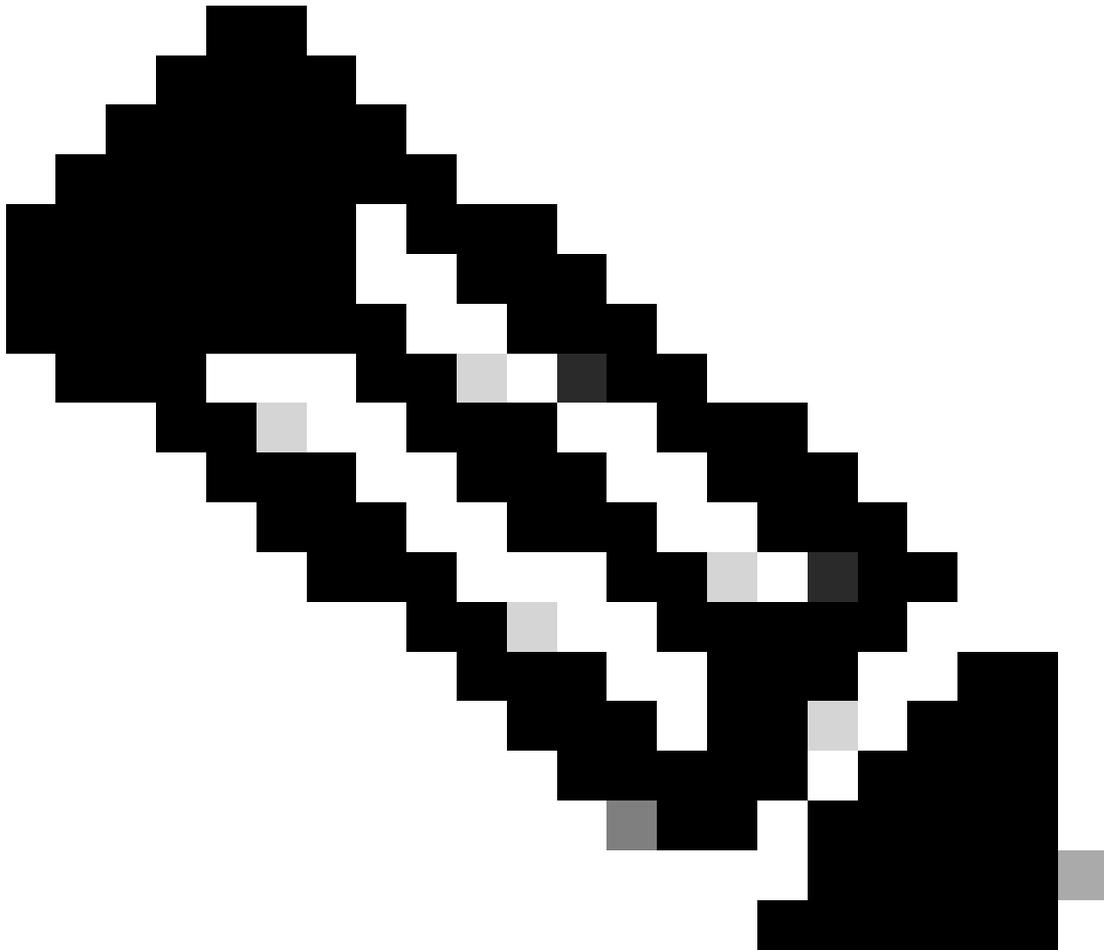
Configuración del Monitor de Flujo con el Recopilador de NetFlow Externo

Puede verificar la Configuración de Puerto del NetFlow Monitor generado automáticamente navegando hasta Configuration > Services > NetFlow .

Cisco Catalyst 9800-CL Wireless Controller
Welcome admin

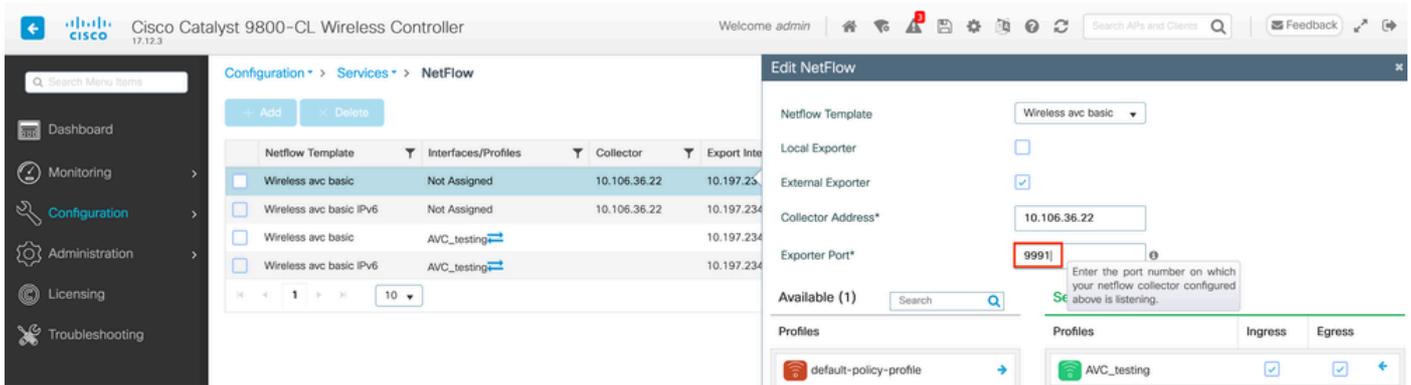
Configuration > Services > NetFlow

Netflow Template	Interfaces/Profiles	Collector	Export Interface IP	Sampling Method	Sampling Range/ACL Name	Exporter Port
<input type="checkbox"/> Wireless avc basic	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995
<input type="checkbox"/> Wireless avc basic IPv6	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995



Nota: Si configura AVC a través de la GUI, el Exportador de NetFlow generado automáticamente se configurará para utilizar el puerto UDP 9995. Asegúrese de validar el número de puerto que está utilizando el recopilador de NetFlow.

Por ejemplo, si utiliza Cisco Prime como recopilador de NetFlow, es fundamental establecer el puerto del exportador en 9991, ya que es el puerto en el que Cisco Prime escucha el tráfico de NetFlow. Puede cambiar manualmente el puerto del exportador en la configuración de NetFlow.



Cambio del Número de Puerto del Exportador en la Configuración de NetFlow

Mediante CLI

Paso 1: Configure la dirección IP del colector de NetFlow externo con la interfaz de origen.

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter External_Exporter
9800-C1-VM(config-flow-exporter)#destination 10.106.36.22
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
```

Paso 2: Configure el monitor de flujo de red IPv4 e IPv6 para utilizar Local(WLC) como Exportador de NetFlow.

```
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
```

Paso 3: asigne el monitor de flujo IPv4 e IPv6 en el perfil de política para el tráfico de entrada y de salida.

```
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

```

Configuración de AVC en 9800 WLC mediante Cisco Catalyst Center

Antes de continuar con la configuración de Application Visibility and Control (AVC) en un Cisco Catalyst 9800 Wireless LAN Controller (WLC) a través de Cisco Catalyst Center, es importante verificar que la comunicación de telemetría entre el WLC y Cisco Catalyst Center se haya establecido correctamente. Asegúrese de que el WLC aparezca en un estado administrado dentro de la interfaz de Cisco Catalyst Center y de que su estado se esté actualizando activamente. Además, para una supervisión eficaz del estado, es importante asignar correctamente tanto el WLC como los puntos de acceso (AP) a sus sitios respectivos dentro de Cisco Catalyst Center.

```

9800WLC#show telemetry connection all
Telemetry connections

```

Index	Peer Address	Port	VRF	Source Address	State	State Description
170	10.78.8.84	25103	0	10.105.193.156	Active	Connection up

Verificación de conexión de telemetría en el WLC 9800

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 **ℹ**

<input type="checkbox"/>	Tags	Device Name ▲	IP Address	Vendor	Reachability ℹ	EoX Status ℹ	Manageability ℹ
<input type="checkbox"/>	🔗	9800WLC.cisco.com 🔗	10.105.193.156	Cisco	🟢 Reachable	⚠ Not Scanned	🟢 Managed
<input type="checkbox"/>	🔗	CW9164I-ROW1	10.105.193.152	NA	🟢 Reachable	⚠ Not Scanned	🟢 Managed
<input type="checkbox"/>	🔗	CW9164I-ROW2	10.105.60.35	NA	🟢 Reachable	⚠ Not Scanned	🟢 Managed

El WLC y el AP están en estado administrado

Network Devices

LATEST **67%** Healthy TOTAL: 3

No Devices



Router

No Devices



Core

No Devices

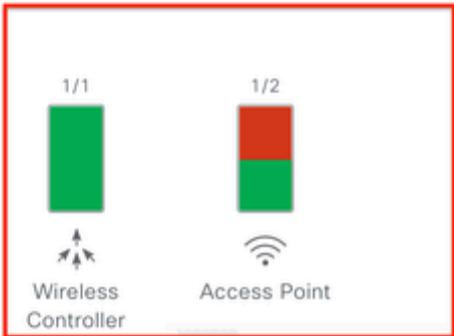


Distribution

No Devices



Access



Wireless Controller

Access Point

40%

7:30p

7:30p

[View Network Health](#)

Estado de estado del WLC y el AP en Cisco Catalyst Center

Paso 1: Configuración de Cisco Catalyst Center como recopilador de NetFlow y activación de la telemetría inalámbrica en configuración global. Navegue hasta Diseño > Configuración de red > Telemetría y habilite la configuración deseada como se muestra.

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

Telemetría inalámbrica y configuración AVC

Paso 2: Habilite la telemetría de la aplicación en el WLC 9800 deseado para presionar la configuración del AVC en el WLC 9800. Para esto, navegue hasta Aprovisionamiento > Dispositivo de red > Inventario. Elija el WLC 9800 en el que desea activar la telemetría de la aplicación, y luego navegue hasta Acción > Telemetría > Habilitar telemetría de la aplicación .

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
<input checked="" type="checkbox"/>	9800WLC.cisco.com	10.105.193.156	Inventory >	Not Scanned	Managed
<input type="checkbox"/>	CW9164I-ROW1	10.105.193.152	Software Image >		
<input type="checkbox"/>	CW9164I-ROW2	10.105.60.35	Provision >		
<input type="checkbox"/>	SDA_WLC.cisco.com	10.106.38.185	Telemetry >		
			Device Replacement >		
			Compliance >		
			More >		

Enable Application Telemetry

Disable Application Telemetry

Update Telemetry Settings

Habilitación de la Telemetría de Aplicación en 9800 WLC

Paso 3: Elija el modo de implementación según los requisitos.

Local: para activar AVC en el perfil de política local (switching central)

Flex/Fabric: para habilitar AVC en el perfil de política Flex (switching local) o SSID basado en fabric.

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.

Selección del modo de implementación en Cisco Catalyst Center

Paso 4: Inicia una tarea para activar los ajustes de AVC, y la configuración correspondiente se aplicará al WLC 9800. Puede ver el estado en Actividades > Registro de auditoría .

Jul 18, 2024 09:22 PM

3:37p

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]

Registros de auditoría después de habilitar la telemetría en el WLC 9800

Cisco Catalyst Center implementará las configuraciones de Flow Exporter y Flow Monitor, incluidos el puerto especificado y otros ajustes, y las activará dentro del perfil de política de modo seleccionado, como se muestra a continuación:

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 10.104.222.201
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-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

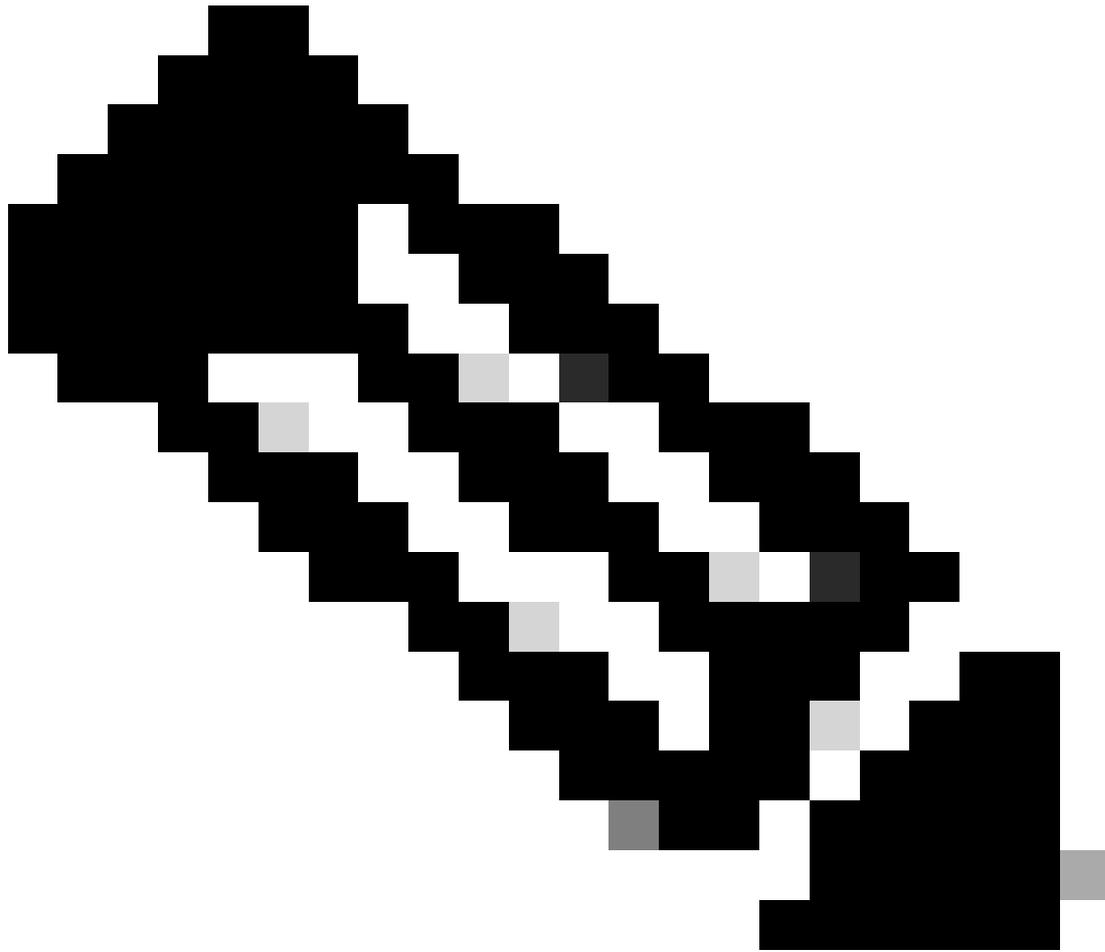
```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp output
9800-C1-VM(config-wireless-policy)#no shutdown
9800-C1-VM(config-wireless-policy)#exit
```

Verificación de AVC

En 9800

Cuando el 9800 WLC se utiliza como un exportador de flujo, estas estadísticas de AVC se pueden observar:

- Visibilidad de la aplicación para clientes conectados a través de todos los SSID.
- Uso de aplicaciones individuales para cada cliente.
- Uso de aplicaciones específicas en cada SSID por separado.



Nota: Tiene la opción de filtrar los datos por dirección, lo que abarca el tráfico entrante (entrada) y saliente (salida), así como por intervalo de tiempo, con la capacidad de seleccionar un intervalo de hasta 48 horas.

Mediante GUI

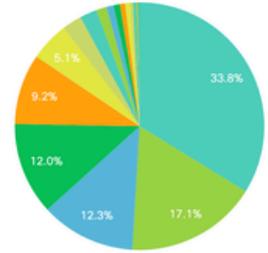
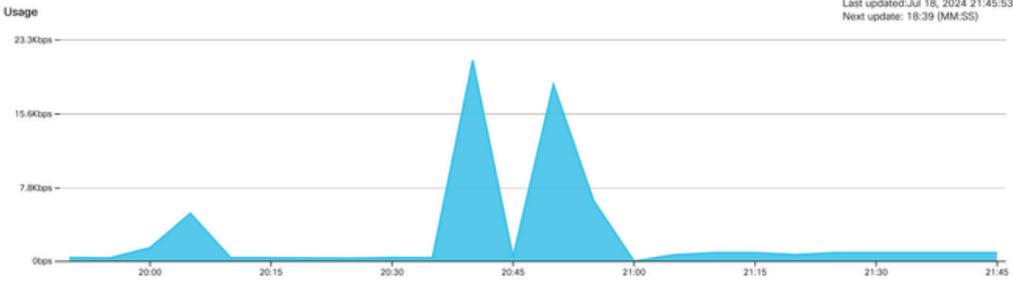
Vaya a [Monitoring > Services > Application Visibility](#) .

Clear AVC

NBAR Protocol Pack Version: 61.0
NBAR Version: 46

Source type: SSID | SSID: AVC_testing | Direction: Both | Interval: Last 2 hours

Clients
 Applications



Application	Usage(%)	Usage	Received	Sent
Unknown	33.83	796.0KB	300.0KB	496.0KB
Domain Name System	17.08	402.0KB	168.0KB	234.0KB
Ping	12.32	290.0KB	145.0KB	145.0KB
HyperText Transfer Protocol	12.03	283.0KB	117.0KB	166.0KB
ICMP for IPv6	9.22	217.0KB	169.0KB	48.0KB
Internet Control Message Protocol	5.10	120.0KB	84.0KB	36.0KB
Simple Service Discovery Protocol	2.55	60.0KB	47.0KB	13.0KB
Microsoft Services	2.21	52.0KB	44.0KB	8.0KB
mDNS	1.36	32.0KB	27.0KB	5.0KB
Binary over HTTP	0.93	22.0KB	9.0KB	13.0KB

Visibilidad de la aplicación de los usuarios conectados a AVC_testing SSID para el tráfico de entrada y de salida

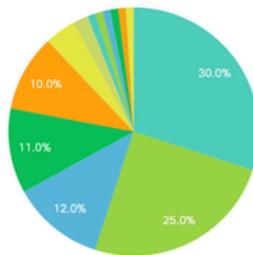
Para ver las estadísticas de Visibilidad de la aplicación para cada cliente, puede hacer clic en la ficha Clientes, elegir un cliente específico y, a continuación, hacer clic en Ver detalles de la aplicación.

Clear AVC

NBAR Protocol Pack Version: 61.0
NBAR Version: 46

Source type: SSID | SSID: All | Direction: All | Interval: Last 90 seconds

Clients
 Applications



Total Clients: 1

View Application Details

Client MAC Address	AP Name	WLAN	State	Protocol
[Redacted]	CW9164I-ROW1	18	Run	11n(2,4)

Visibilidad de la aplicación para un cliente específico - 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

Visibilidad de la aplicación para un cliente específico - 2

Mediante CLI

Verificar estado AVC

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

AVC configuration complete: YES

Estadísticas de NetFlow (FNF Cache)

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

```
9800WLC#show flow monitor wireless-avc-basic cache format table
Cache type: Normal (Platform cache)
Cache size: 200000
Current entries: 102
High Watermark: 102

Flows added: 102
Flows aged: 0
```

IPV4 SRC ADDR	IPV4 DST ADDR	TRNS SRC PORT	TRNS DST PORT	FLOW DIRN	WIRELESS SSID	IP PROT	APP NAME	bytes long
wireless client mac addr	mac addr							
10.105.193.170	10.105.193.195	5355	61746	Output	AVC_testing	17	layer7 llmnr	120
10.105.193.129	10.105.193.195	5355	61746	Output	AVC_testing	17	port dns	120
10.105.193.195	10.105.193.2	0	771	Input	AVC_testing	1	prot icmp	148
10.105.193.195	10.105.193.114	0	771	Input	AVC_testing	1	prot icmp	120
10.105.193.4	10.105.193.195	5355	64147	Output	AVC_testing	17	layer7 llmnr	120
10.105.193.169	10.105.193.195	5355	64147	Output	AVC_testing	17	port dns	120
10.105.193.195	10.105.193.52	0	771	Input	AVC_testing	1	prot icmp	148
10.105.193.59	10.105.193.195	5355	64147	Output	AVC_testing	17	port dns	120

Verificación de AVC en CLI 9800

Para examinar individualmente el uso principal de aplicaciones para cada WLAN y sus clientes conectados:

```
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
```

Verifique los recuentos de paquetes FNFv9 y descodifique el estado en el plano de control (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

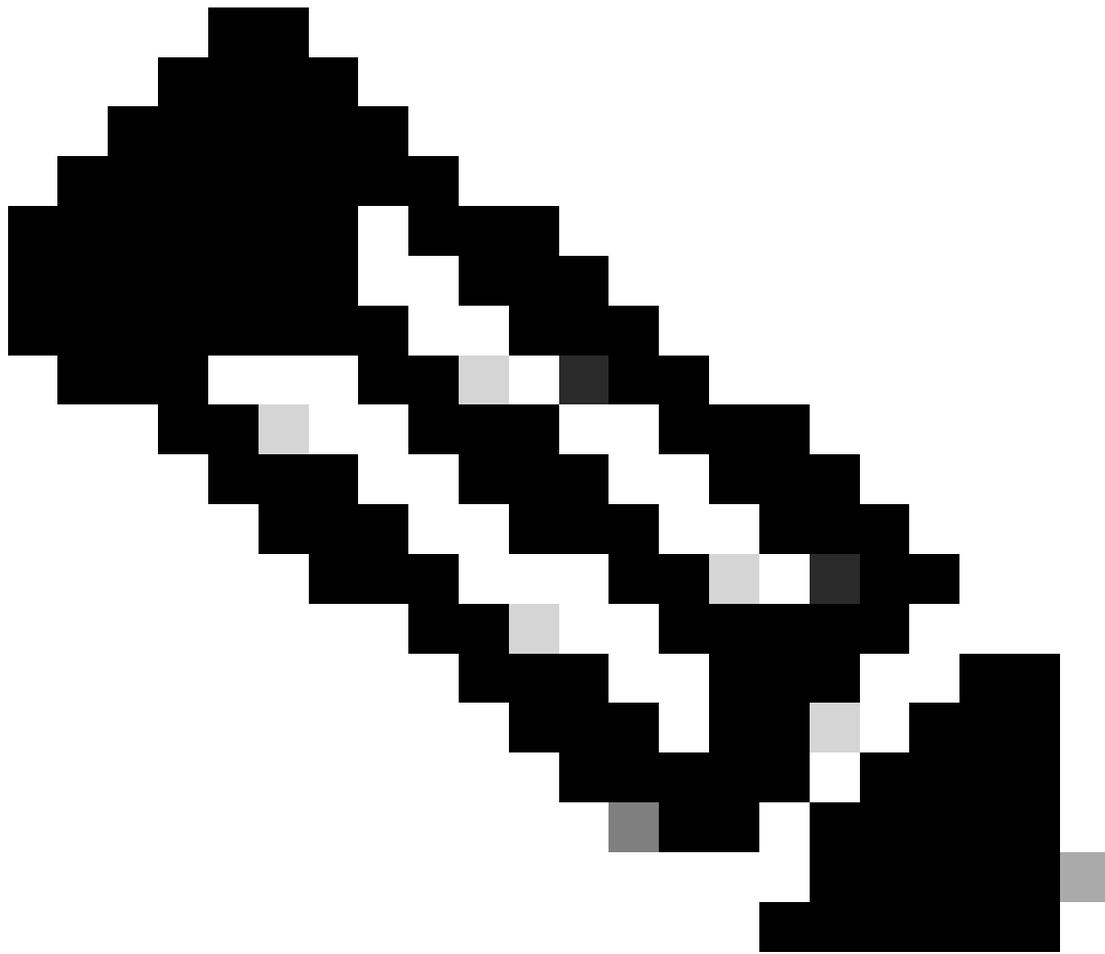
Registro de paquetes FNFv9

También puede comprobar las estadísticas de nbar directamente.

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

En los modos Fabric y Flex, puede obtener las estadísticas de NBAR desde el punto de acceso mediante:

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



Nota: En una configuración de anclaje externo, el WLC de anclaje sirve como presencia de Capa 3 para el cliente, mientras que el WLC externo funciona en la Capa 2. Dado que Application Visibility and Control (AVC) funciona en la capa 3, los datos relevantes solo se pueden observar en el WLC de anclaje.

En DNAC

A partir de la captura de paquetes realizada en el WLC 9800, podemos confirmar que está enviando datos relacionados con las aplicaciones y el tráfico de red a Cisco Catalyst Center de forma continua.

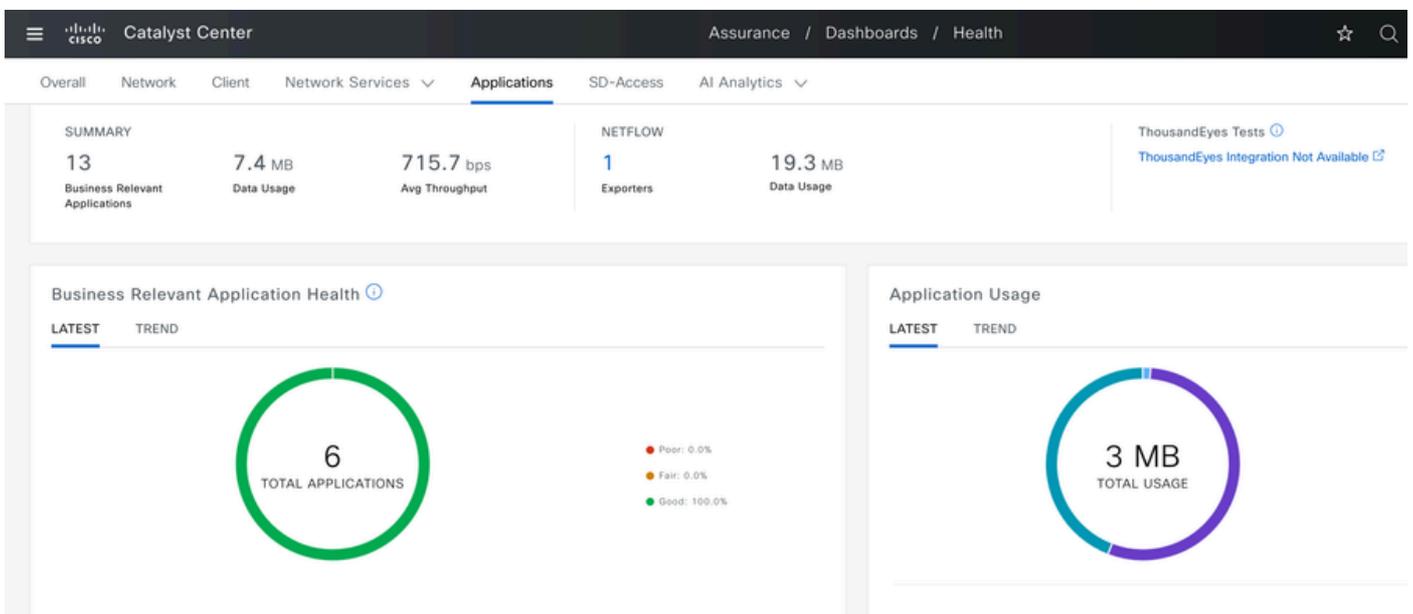
ip.addr == 10.78.8.84 and udp.port == 6007

No.	Time	Source	Destination	Protocol	Length	Info
74227	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]: 000a00886698e17a00001fa700000100011800780a69c150080808080411003501242fd0daa7da00000002000000120d000309005
 [Length: 136]

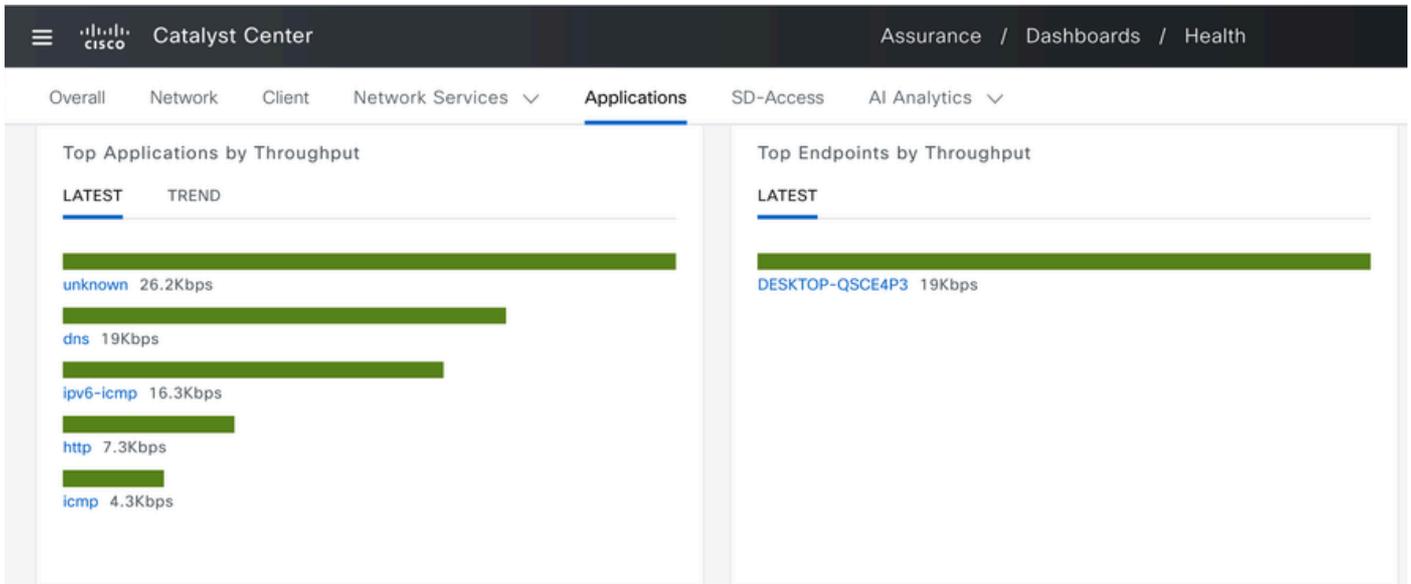
Captura de paquetes en 9800 WLC

Para ver los datos de la aplicación para los clientes conectados a un WLC específico en Cisco Catalyst Center, navegue hasta Assurance > Dashboards > Health > Application .



Supervisión de AVC en Cisco Catalyst Center

Podemos realizar un seguimiento de las aplicaciones utilizadas con más frecuencia por los clientes e identificar los consumidores de datos más altos, como se muestra aquí.



Principales estadísticas de usuarios de aplicaciones y ancho de banda superior

Puede establecer un filtro para un SSID determinado, lo que le permitirá supervisar el rendimiento general y el uso de aplicaciones de los clientes asociados con ese SSID.

Esta funcionalidad le permite identificar las principales aplicaciones y los usuarios que consumen más ancho de banda de su red.

Además, puede utilizar la función Time Filter (Filtro de tiempo) para examinar estos datos durante períodos de tiempo anteriores, lo que ofrece información histórica sobre el uso de la red.

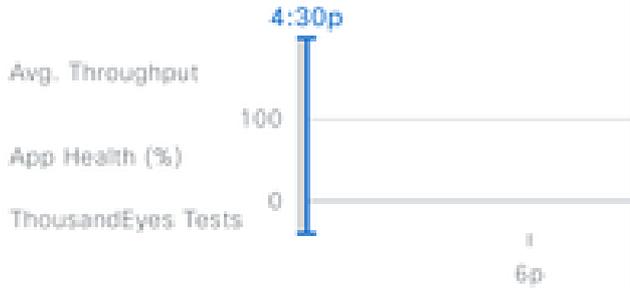
Global/BGL TAC/Shalini_AVC

24 Hours

Filter (1)



By default, hourly data is shown



Time Range

3 Hours 24 Hours 7 Days

Start Date

7 / 17 / 2024

4:23 PM

End Date

7 / 18 / 2024

4:23 PM

SSID: AVC_testing

SUMMARY

13

Business Relevant Applications

7.4 M

Data Usage

Cancel

Apply

Filtro de tiempo para mostrar las estadísticas de AVC

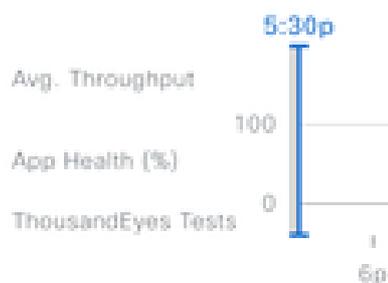


By default, hourly data is show

SSID (1/14)

Clear Filter

- CWA-test-321
- Session_timeout
- LM-INTERNAL
- AVC_testing
- testvritti
- CWA-test-2
- renjith
- Start-Stop
- testm...



SSID: AVC_testing

Cancel

Apply

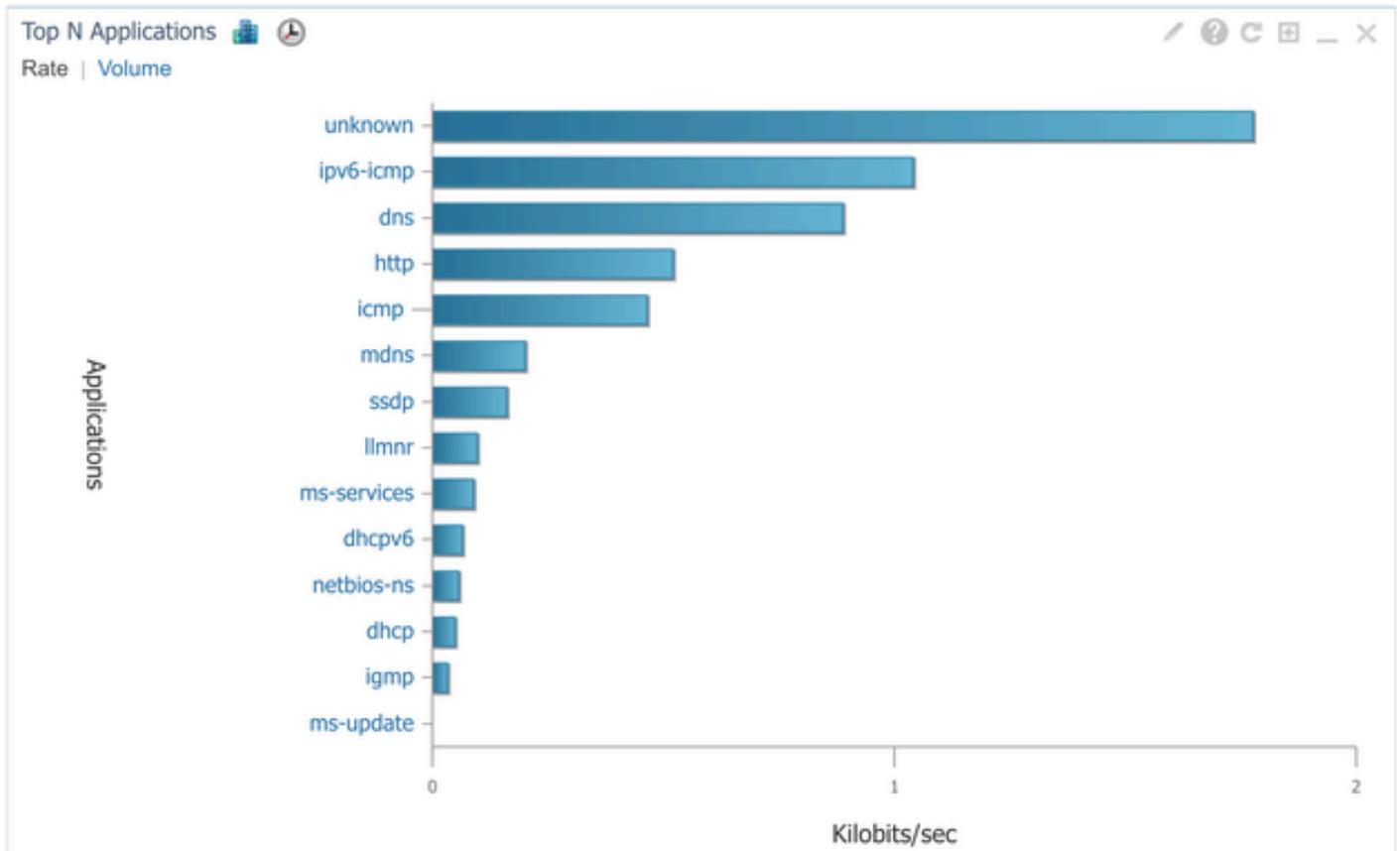
Filtro SSID para mostrar las estadísticas de AVC

En colector de NetFlow externo

Ejemplo 1: Cisco Prime como NetFlow Collector

Cuando utiliza Cisco Prime como recopilador de Netflow, el WLC recopilado puede ver el 9800 como origen de datos que envía datos de Netflow y la plantilla de NetFlow se creará automáticamente según los datos que envía el WLC 9800.

A partir de la captura de paquetes realizada en el WLC 9800, podemos comprobar que está enviando datos relativos a las aplicaciones y al tráfico de red a Cisco Prime de forma continua.

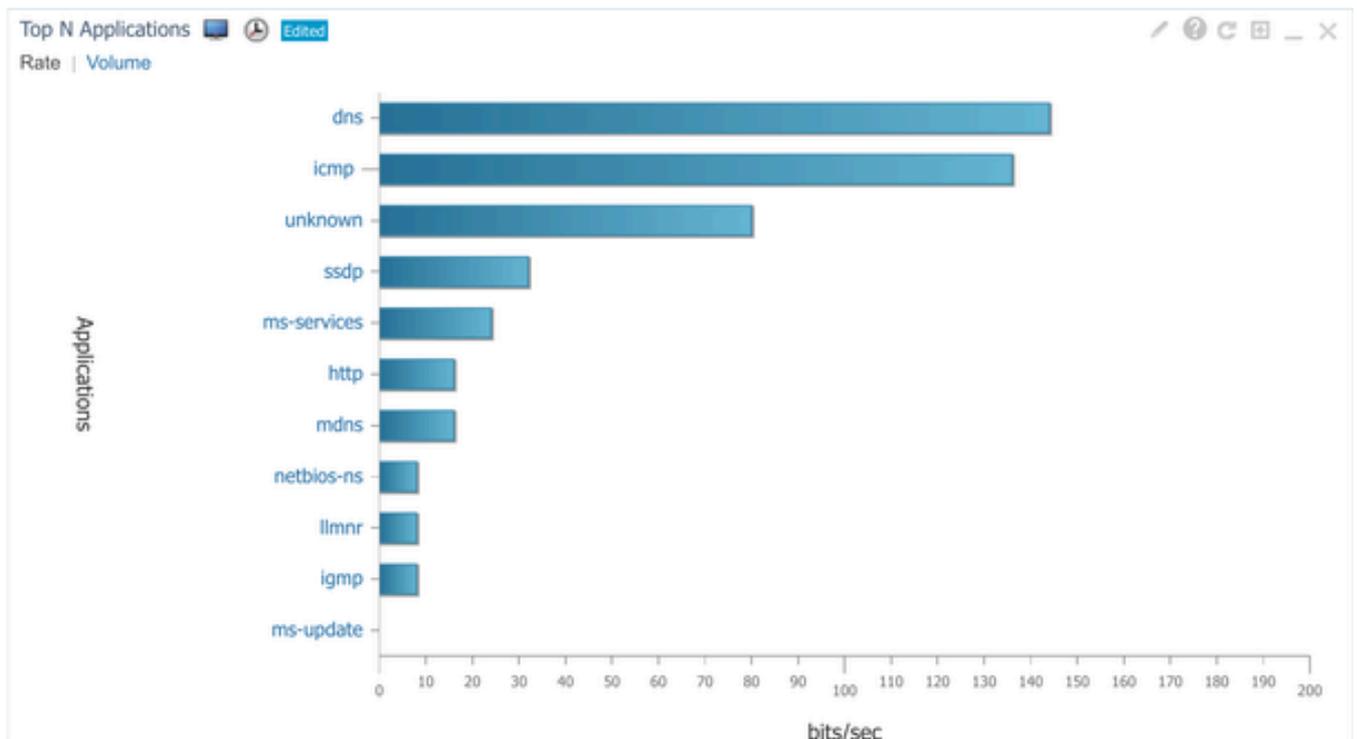


Visibilidad de la aplicación para todos los clientes

Dashboard / Performance

[Site](#) |
 [Device](#) |
 [Access Point](#) |
 [Interface](#) |
 [Application](#) |
 [Voice/Video](#) |
 [End User Experience](#)

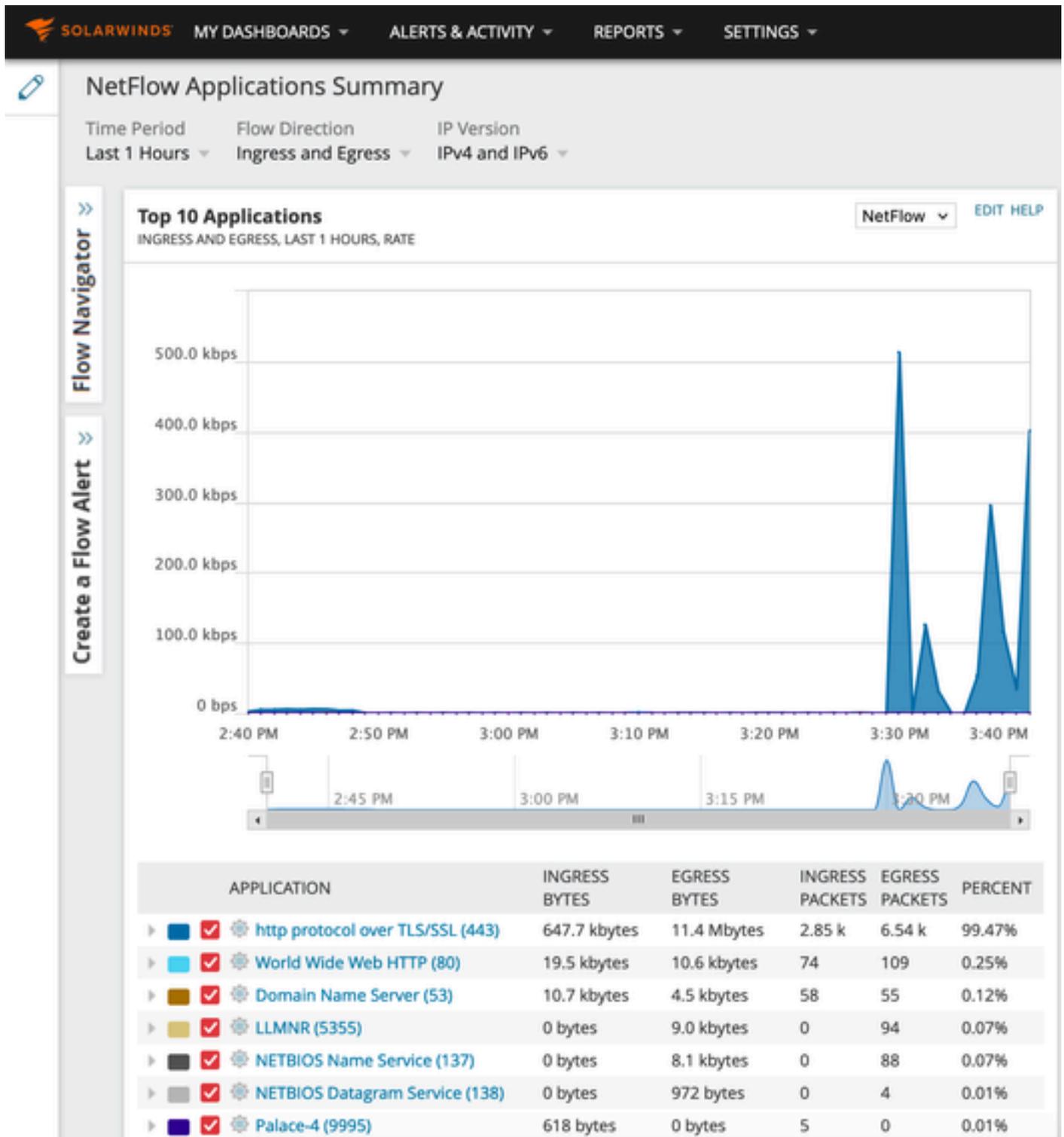
Filters: *Client: 10.105.193.80,Una... |
 *Time Frame: Past 1 Hour |
 Application: All |
 Network Aware



Aplicación de un cliente específico mediante una dirección IP

Ejemplo 2: Recopilador de NetFlow de terceros

En este ejemplo, se utiliza el colector de NetFlow de terceros [SolarWinds] para recopilar estadísticas de la aplicación. El WLC 9800 emplea Flexible NetFlow (FNF) para transmitir datos completos relativos a las aplicaciones y al tráfico de red, que luego recopila SolarWinds.



Estadísticas de aplicaciones de Netflow en SolarWind

Control de tráfico

El control de tráfico hace referencia a un conjunto de funciones y mecanismos que se utilizan para gestionar y regular el flujo del tráfico de red. La regulación del tráfico o la limitación de velocidad son mecanismos utilizados en el controlador inalámbrico para controlar la cantidad de tráfico transmitido desde el cliente. Supervisa la velocidad de datos del tráfico de red y toma medidas inmediatas cuando se supera un límite de velocidad predefinido. Cuando el tráfico supera la velocidad especificada, la limitación de velocidad puede descartar los paquetes en exceso o marcarlos cambiando sus valores de clase de servicio (CoS) o punto de código de servicios diferenciados (DSCP). Esto se puede lograr mediante la configuración de QOS en el WLC 9800. Puede consultar <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html> para obtener la descripción general de cómo funcionan estos componentes y cómo se pueden configurar para lograr diferentes resultados.

Resolución de problemas

La resolución de problemas de AVC implica la identificación y resolución de problemas que posiblemente afecten a la capacidad de AVC para identificar, clasificar y administrar con precisión el tráfico de aplicaciones en su red inalámbrica. Entre los problemas habituales se incluyen la clasificación del tráfico, la aplicación de políticas o la generación de informes. Estos son algunos pasos y consideraciones para la resolución de problemas de AVC en un WLC Catalyst 9800:

- Verifique la configuración de AVC: asegúrese de que AVC esté configurado correctamente en el WLC y asociado con las WLAN y los perfiles correctos.
- Al configurar AVC a través de la GUI, asignará automáticamente el puerto 9995 como predeterminado. Sin embargo, si está utilizando un colector externo, verifique qué puerto está configurado para escuchar el tráfico de NetFlow. Es crucial configurar con precisión este número de puerto para que coincida con la configuración de su colector.
- Verifique el modelo AP y el soporte del modo de implementación.
- Consulte las limitaciones del WLC 9800 mientras implementa AVC en su red inalámbrica.

Recopilación de registros

Registros WLC

1. Active timestamp para tener referencia de tiempo para todos los comandos.

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

2. Para revisar la configuración

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

3. Puede verificar el estado de avc y las estadísticas de netflow.

Compruebe el estado de la configuración de AVC.

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

Verifique los recuentos de paquetes FNFv9 y el estado de decodificación enviado al plano de control (CP).

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

Verifique las estadísticas de NetFlow (FNF Cache).

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

Marque Top n application usage for each wlan, where n = <1-30> Introduzca el número de aplicaciones.

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

Marque n aplicaciones principales para cada cliente, donde n = <1-30> Introduzca el número de aplicaciones.

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

Marque los n clientes principales conectados a una wlan específica mediante la aplicación específica, donde n=<1-10> Introduzca el número de clientes.

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

Compruebe las estadísticas de nbar.

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

4. Establezca el nivel de registro en 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. Active el seguimiento radioactivo (RA) para la dirección MAC del cliente para validar las estadísticas de AVC.

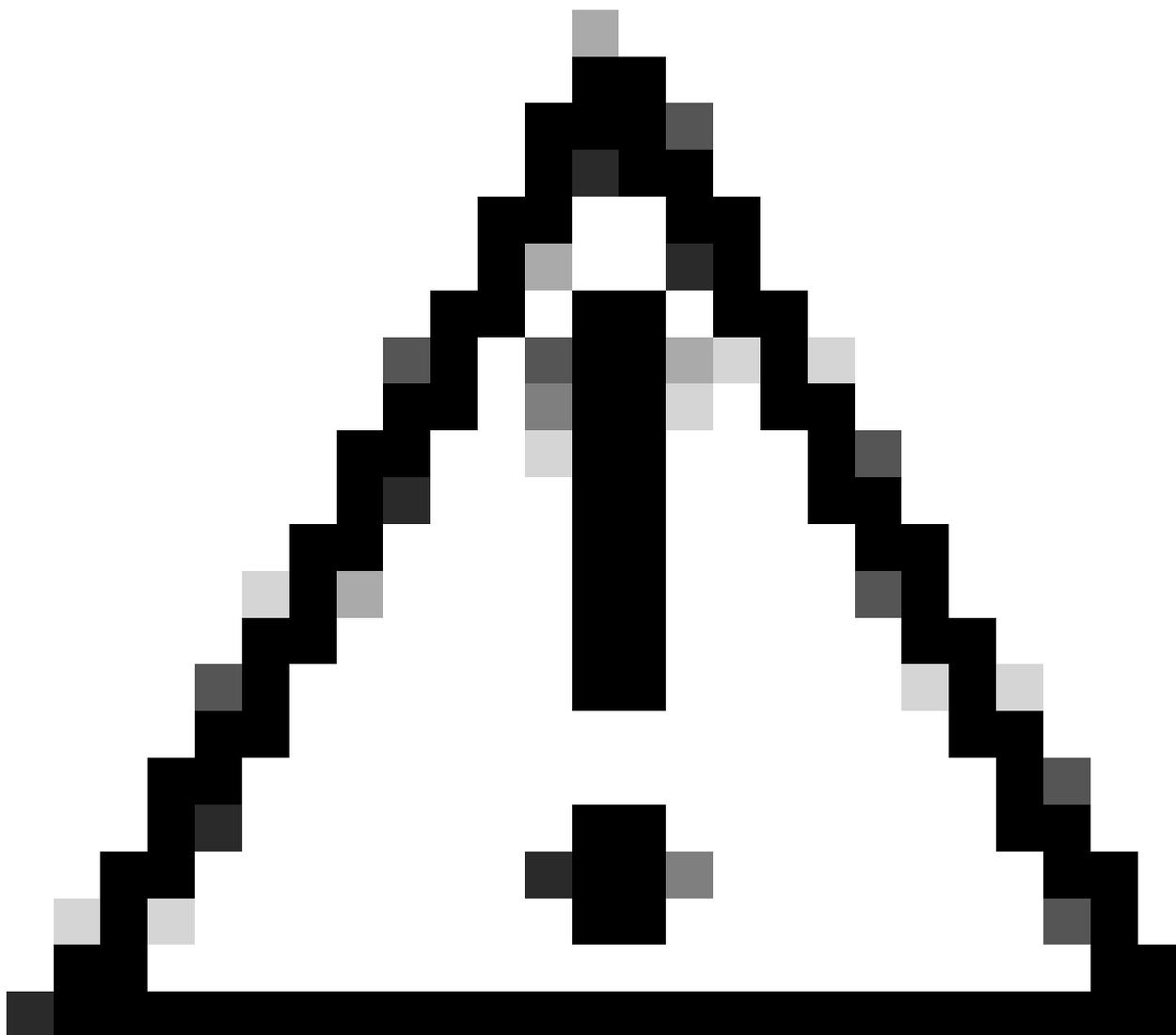
Mediante CLI

```
9800WLC#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
```



Precaución: la depuración condicional habilita el registro de nivel de depuración que, a su vez, aumenta el volumen de los registros generados. Si deja esta opción en ejecución, reducirá la cantidad de tiempo desde el que puede ver los registros. Por lo tanto, se recomienda desactivar siempre la depuración al final de la sesión de solución de problemas.

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

Mediante GUI

Paso 1. Vaya a Troubleshooting > Radioactive Trace .

Paso 2. Haga clic en Agregar e ingrese una dirección MAC del cliente que desee resolver. Puede agregar varias direcciones Mac para realizar un seguimiento.

Paso 3. Cuando esté listo para iniciar el seguimiento radiactivo, haga clic en iniciar. Una vez iniciado, el registro de depuración se escribe en el disco sobre cualquier procesamiento del plano

de control relacionado con las direcciones MAC objeto de seguimiento.

Paso 4. Cuando reproduzca el problema que desea solucionar, haga clic en Detener .

Paso 5. Para cada dirección MAC depurada, puede generar un archivo de registro que recopile todos los registros pertenecientes a esa dirección MAC haciendo clic en Generar .

Paso 6. Elija cuánto tiempo atrás desea que transcurra el archivo de registro intercalado y haga clic en Aplicar al dispositivo.

Paso 7. Ahora puede descargar el archivo haciendo clic en el pequeño icono situado junto al nombre del archivo. Este archivo está presente en la unidad flash de arranque del controlador y también se puede copiar desde el primer momento mediante CLI.

Aquí hay un vistazo de los debugs de AVC en rastros de RA

```
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. Capturas incrustadas filtradas por dirección MAC del cliente en ambas direcciones, filtro MAC interno del cliente disponible después de 17.1.

Es particularmente útil cuando se utiliza un colector externo, ya que ayuda a confirmar si el WLC está transmitiendo los datos de NetFlow al puerto deseado como se espera.

Mediante 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
!! Initiate different application traffic from user
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:../filename.pcap
```

Mediante GUI

Paso 1. Vaya a Troubleshooting > Packet Capture > +Add .

Paso 2. Defina el nombre de la captura de paquetes. Se permite un máximo de 8 caracteres.

Paso 3. Defina los filtros, si los hubiera.

Paso 4. Marque la casilla Monitor Control Traffic (Controlar el tráfico de control) si desea ver el tráfico dirigido a la CPU del sistema e insertado de nuevo en el plano de datos.

Paso 5. Defina el tamaño del búfer. Se permite un máximo de 100 MB.

Paso 6. Defina el límite, ya sea por la duración que permite un rango de 1 - 1000000 segundos o por el número de paquetes que permite un rango de 1 - 100000 paquetes, según lo deseado.

Paso 7. Elija la interfaz de la lista de interfaces de la columna izquierda y seleccione la flecha para moverla a la columna derecha.

Paso 8. Haga clic en Apply to Device.

Paso 9. Para iniciar la captura, seleccione Inicio .

Paso 10. Puede dejar que la captura se ejecute hasta el límite definido. Para detener manualmente la captura, seleccione Stop.

Paso 11. Una vez detenido, un botón Exportar se pone a disposición para hacer clic con la opción de descargar el archivo de captura (.pcap) en el escritorio local a través de HTTP o servidor TFTP o servidor FTP o disco duro del sistema local o flash.

Registros de AP

En los modos Fabric y Flex

1. show tech para tener todos los detalles de configuración y las estadísticas del cliente para el AP.

2. show avc nbar statistics nbar stats from AP

3. Depuraciones de AVC

```
AP#term mon
```

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

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

Información Relacionada

[Guía de configuración de AVC](#)

[Límite de velocidad en 9800 WLC](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).