

# AVC auf dem Catalyst 9800 Wireless LAN Controller verstehen

## Inhalt

---

[Einleitung](#)

[Voraussetzung](#)

[Informationen zu Application Visibility and Control \(AVC\)](#)

[Funktionsweise von AVC](#)

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

[NBAR-Protokoll in Richtlinienprofil aktivieren](#)

[Aktualisieren von NBAR auf dem 9800 WLC](#)

[NetFlow](#)

[Flexibles NetFlow](#)

[Datenflussüberwachung](#)

[Von AVC unterstützte Access Points](#)

[Unterstützung verschiedener Bereitstellungsmodi des 9800](#)

[Einschränkungen bei der Implementierung von AVC auf 9800](#)

[Netzwerktopologie](#)

[AP im lokalen Modus](#)

[AP im flexiblen Modus](#)

[Konfiguration von AVC auf dem 9800 WLC](#)

[Lokaler Exporteur](#)

[Externer NetFlow-Collector](#)

[Konfiguration von AVC auf dem 9800 WLC mit Cisco Catalyst Center](#)

[AVC-Prüfung](#)

[Auf 9800](#)

[Bei DNAC](#)

[Auf externem NetFlow-Collector](#)

[Beispiel 1: Cisco Prime als NetFlow Collector](#)

[Beispiel 2: Drittanbieter NetFlow Collector](#)

[Datenverkehrskontrolle](#)

[Fehlerbehebung](#)

[Protokollsammlung](#)

[WLC-Protokolle](#)

[AP-Protokolle](#)

[Zugehörige Informationen](#)

---

## Einleitung

Dieses Dokument beschreibt Application Visibility and Control (AVC) auf einem Cisco Catalyst 9800 WLC, der eine präzise Verwaltung des Anwendungsdatenverkehrs ermöglicht.

## Voraussetzung

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse des Cisco WLC 9800.
- Grundkenntnisse der APs im lokalen und Flex-Connect-Modus
- Die Access Points müssen AVC-fähig sein. (Nicht zutreffend für AP im lokalen Modus)
- Damit der Kontrollteil von AVC (QoS) funktioniert, muss die Funktion für Anwendungstransparenz mit FNF konfiguriert werden.

## Informationen zu Application Visibility and Control (AVC)

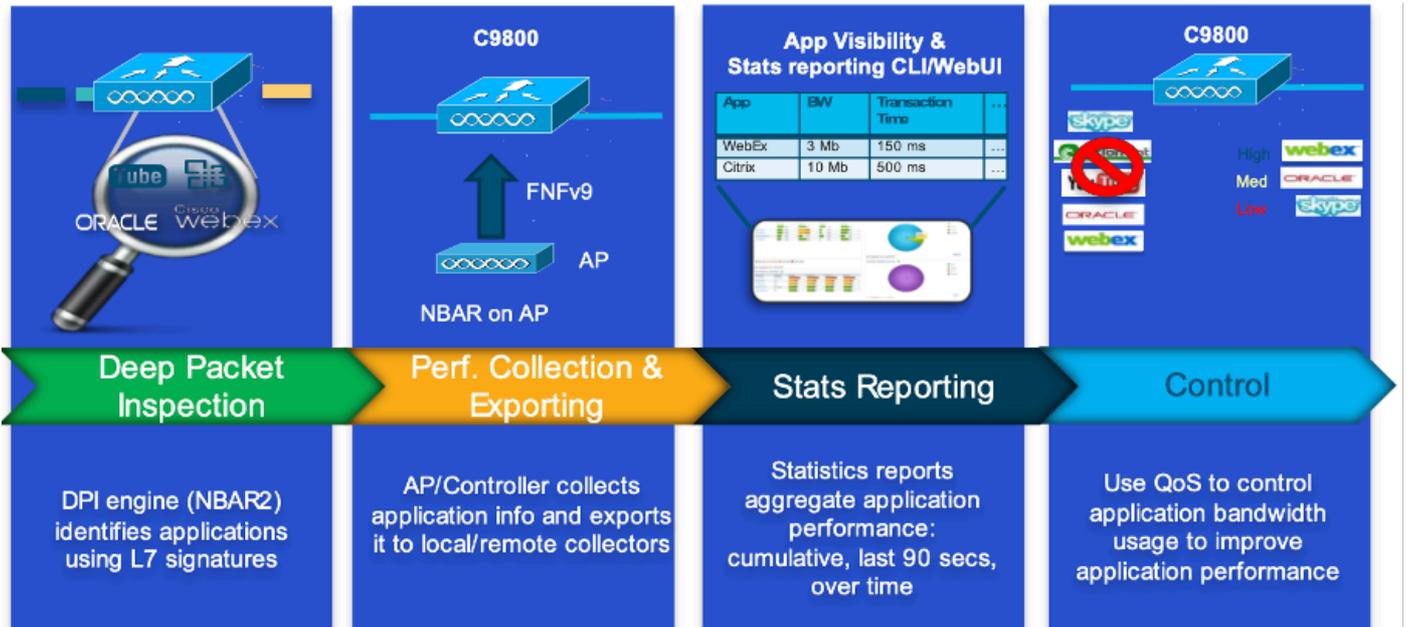
Application Visibility and Control (AVC) ist der führende Ansatz von Cisco für die Deep Packet Inspection (DPI)-Technologie in kabelgebundenen und Wireless-Netzwerken. Mit AVC können Sie Echtzeitanalysen durchführen und Richtlinien erstellen, um Netzwerküberlastungen wirksam zu reduzieren, die kostspielige Nutzung von Netzwerkverbindungen zu minimieren und unnötige Infrastruktur-Upgrades zu vermeiden. Kurz gesagt: Mit AVC können Benutzer mithilfe von Network Based Application Recognition (NBAR) eine völlig neue Ebene der Erkennung und des Shapings von Datenverkehr erreichen. NBAR-Pakete, die auf dem 9800 WLC ausgeführt werden, werden für DPI verwendet, und die Ergebnisse werden mithilfe von Flexible NetFlow (FNF) gemeldet.

AVC bietet nicht nur Transparenz, sondern ermöglicht auch die Priorisierung, Blockierung oder Drosselung verschiedener Arten von Datenverkehr. So können Administratoren beispielsweise Richtlinien zur Priorisierung von Sprach- und Videoanwendungen erstellen, um die Quality of Service (QoS) sicherzustellen oder die verfügbare Bandbreite für nicht wichtige Anwendungen während der Hauptgeschäftszeiten zu begrenzen. Die Lösung kann auch in andere Cisco Technologien integriert werden, z. B. die Cisco Identity Services Engine (ISE) für identitätsbasierte Anwendungsrichtlinien und Cisco Catalyst Center für zentrales Management.

## Funktionsweise von AVC

AVC verwendet erweiterte Technologien wie die FNF- und NBAR2-Engine für DPI. Durch die Analyse und Identifizierung von Datenverkehrsflüssen mithilfe der NBAR2-Engine werden bestimmte Flüsse mit dem erkannten Protokoll oder der erkannten Anwendung markiert. Der Controller erfasst alle Berichte und stellt sie mithilfe von Anzeigebefehlen, der Webbenutzeroberfläche oder zusätzlichen NetFlow-Exportmeldungen an externe NetFlow-Collectors wie Prime dar.

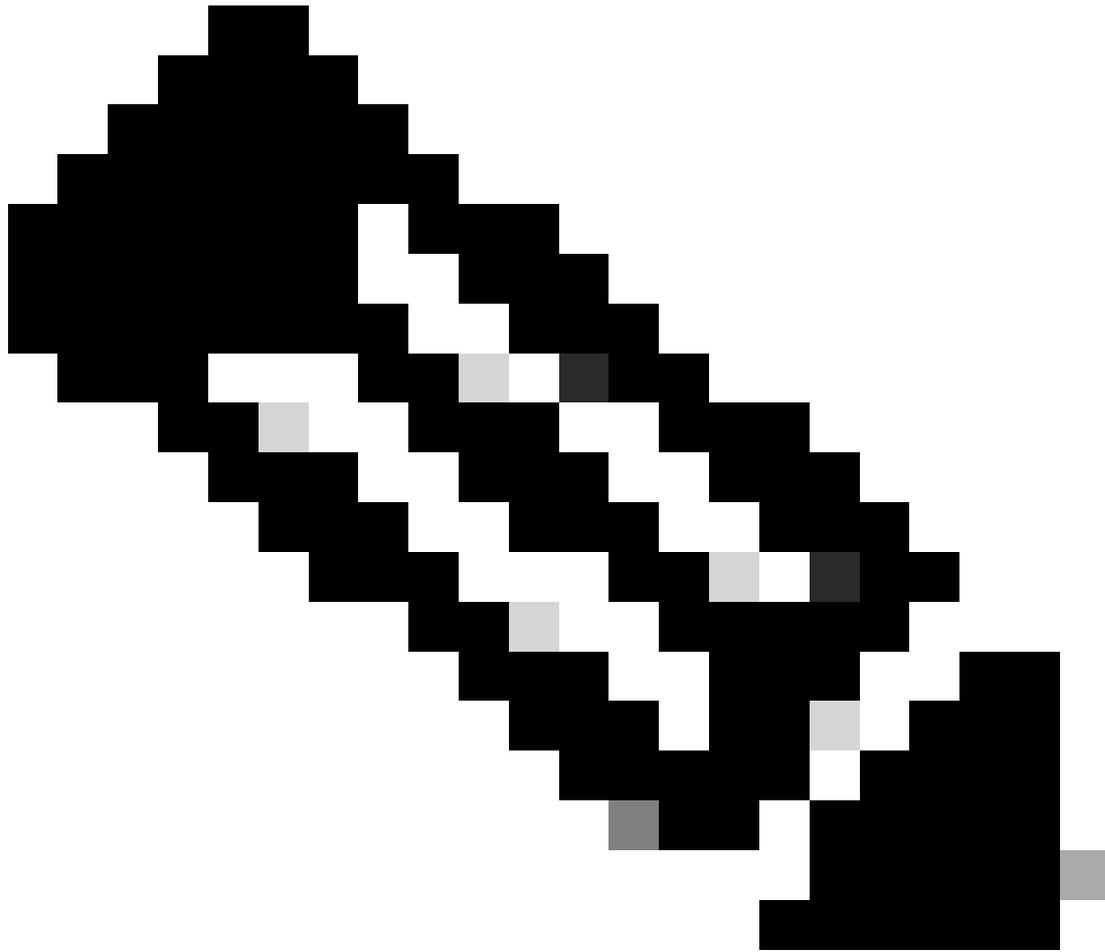
Sobald die Anwendungstransparenz eingerichtet ist, können Benutzer Kontrollregeln mit Richtlinienmechanismen für Clients erstellen, indem sie Quality of Service (QoS) konfigurieren.



Arbeitsmechanismus von AVC

## Network-Based Application Recognition (NBAR)

NBAR ist ein in den 9800 WLC integrierter Mechanismus, mit dem DPI zum Identifizieren und Klassifizieren einer Vielzahl von Anwendungen, die über ein Netzwerk ausgeführt werden, ausgeführt wird. Er kann eine große Anzahl von Anwendungen erkennen und klassifizieren, einschließlich verschlüsselter und dynamisch portseitiger Anwendungen, die für herkömmliche Paketprüfungstechnologien häufig unsichtbar sind.



Hinweis: Um NBAR auf dem Catalyst 9800 WLC zu nutzen, muss es korrekt aktiviert und konfiguriert werden. Dies geschieht häufig in Verbindung mit spezifischen AVC-Profilen, die die geeigneten Aktionen auf Basis der Klassifizierung des Datenverkehrs definieren.

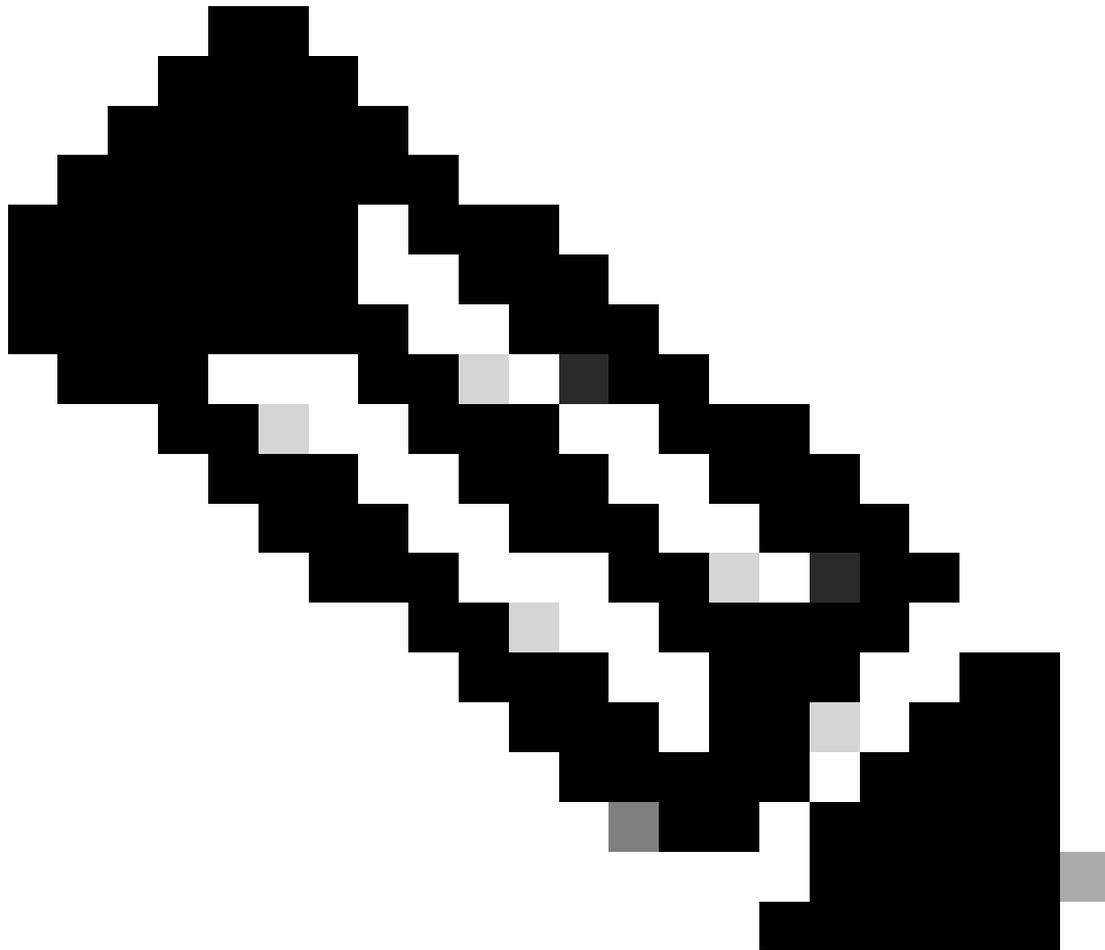
NBAR wird weiterhin regelmäßig aktualisiert. Daher ist es wichtig, die WLC-Software auf dem neuesten Stand zu halten, um sicherzustellen, dass die NBAR-Funktionen aktuell und effektiv bleiben.

Eine vollständige Liste der in den neuesten Versionen unterstützten Protokolle finden Sie unter [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_nbar/prot\\_lib/config\\_library/nbar-prot-pack-library.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html)

NBAR-Protokoll in Richtlinienprofil aktivieren

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

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



Hinweis: Das %-Richtlinienprofil muss deaktiviert werden, bevor dieser Vorgang ausgeführt werden kann.

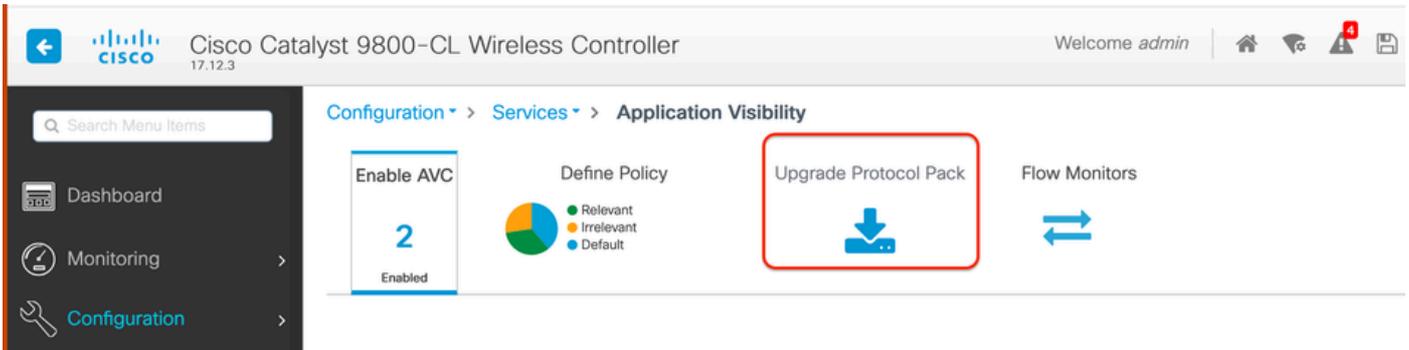
```
9800WLC#show wireless profile policy detailed AVC_testing | in NBAR  
NBAR Protocol Discovery : Enabled
```

Aktualisieren von NBAR auf dem 9800 WLC

9800 WLC hat bereits ~1500 erkennbare Anwendungen. Wenn eine neue Anwendung veröffentlicht wird, wird das Protokoll für dieselbe in der neuesten NBAR aktualisiert, die von der Software-Download-Seite für das spezielle 9800-Modell heruntergeladen werden muss.

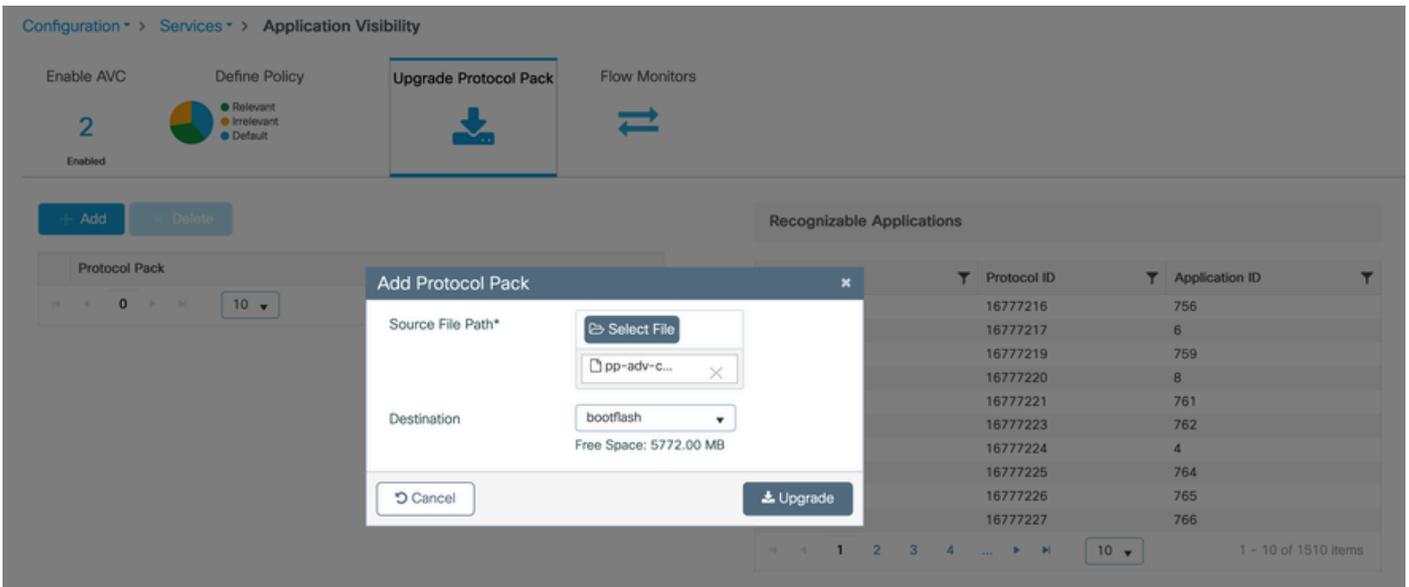
## Über GUI

Navigieren Sie zu Konfiguration > Dienste > Anwendungstransparenz. Klicken Sie auf Upgrade Protocol Pack .



Protokollabschnitt in 9800 WLC hochladen

Klicken Sie auf Hinzufügen, wählen Sie das herunterzuladende Protokollpaket aus, und klicken Sie auf Upgrade .



NBAR-Protokoll hinzufügen

Nach Abschluss des Upgrades wird das Protokollpaket hinzugefügt.

Enable AVC Define Policy Upgrade Protocol Pack Flow Monitors

2

Enabled

+ Add × Delete

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

Navigation: ⏪ ⏩ 1 10 ▼ 1 - 1 of 1 items

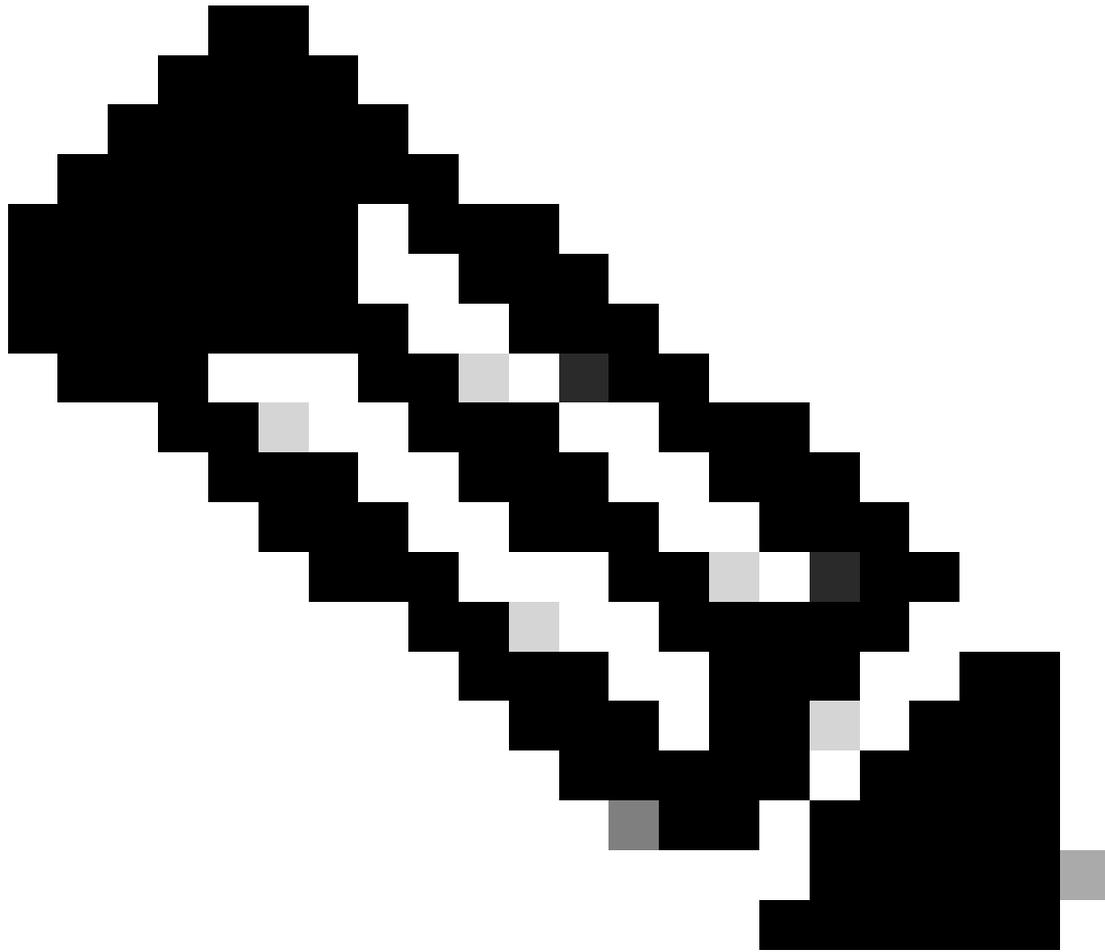
Überprüfung des Protokollpakets

## Über 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
```



Hinweis: Während des Upgrades des NBAR-Protokollpakets kommt es nicht zu einer Unterbrechung des Services.

## NetFlow

NetFlow ist ein Netzwerkprotokoll zum Sammeln von IP-Verkehrsinformationen und zum Überwachen von Netzwerkflussdaten. Es wird hauptsächlich für die Analyse des Netzwerkverkehrs und die Bandbreitenüberwachung verwendet. Nachfolgend finden Sie eine Übersicht über die Funktionsweise von NetFlow auf den Cisco Catalyst Controllern der Serie 9800:

- Datenerfassung: Der 9800 WLC erfasst Daten über den IP-Datenverkehr, der durch den WLC fließt. Zu diesen Daten gehören Informationen wie Quell- und Ziel-IP-Adressen, Quell- und Ziel-Ports, verwendete Protokolle, Serviceklassen und die Ursache für die Beendigung des Datenflusses.
- Flow Records: Die erfassten Daten werden in Flow Records organisiert. Ein Datenfluss wird

als unidirektionale Folge von Paketen definiert, die einen Satz gemeinsamer Attribute gemeinsam nutzen, z. B. dieselbe Quell-/Ziel-IP-Adresse, dieselben Quell-/Ziel-Ports und denselben Protokolltyp.

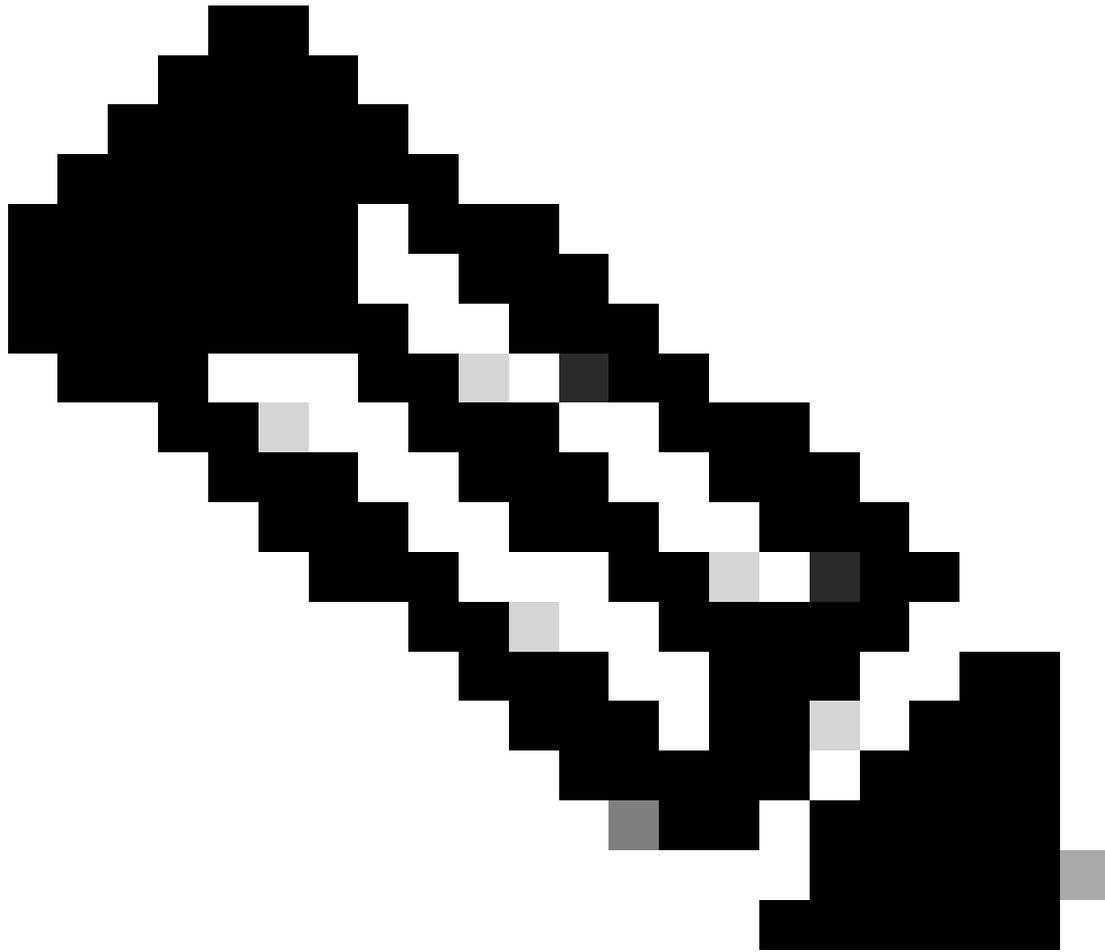
- Exportieren von Daten: Die Datenflussdatensätze werden regelmäßig vom NetFlow-fähigen Gerät in einen NetFlow Collector exportiert. Der Collector kann ein lokaler WLC oder ein dedizierter Server oder eine Softwareanwendung sein, die die Flow-Daten empfängt, speichert und verarbeitet.
- Analyse: Sie können NetFlow-Collectors und Analysetools verwenden, um Datenverkehrsmuster zu visualisieren, Bandbreite zu identifizieren, ungewöhnliche Datenverkehrsflüsse zu erkennen, die auf Sicherheitsverletzungen hinweisen, die Netzwerkleistung zu optimieren und eine Netzwerkerweiterung zu planen.
- Wireless-spezifische Informationen: NetFlow kann im Kontext von Wireless Controllern zusätzliche Informationen speziell für Wireless-Netzwerke wie SSID, AP-Namen, MAC-Adressen von Clients und andere Details für den Wi-Fi-Datenverkehr enthalten.

## Flexibles NetFlow

Flexible NetFlow (FNF) ist eine erweiterte Version des herkömmlichen NetFlow und wird von den Cisco Catalyst Wireless LAN Controllern (WLCs) der Serie 9800 unterstützt. Es bietet weitere Anpassungsoptionen für die Nachverfolgung, Überwachung und Analyse von Netzwerkverkehrsmustern. Wichtigste Funktionen von Flexible NetFlow auf dem Catalyst 9800 WLC:

- Anpassung: Mit FNF können Benutzer definieren, welche Informationen sie aus dem Netzwerkverkehr sammeln möchten. Dazu gehören eine Vielzahl von Datenverkehrsattributen wie IP-Adressen, Portnummern, Zeitstempeln, Paket- und Bytezählern, Anwendungstypen und mehr.
- Verbesserte Transparenz: Durch die Nutzung von FNF erhalten Administratoren einen detaillierten Einblick in die Arten des Datenverkehrs, der durch das Netzwerk fließt. Dies ist für die Kapazitätsplanung, die nutzungsbasierte Netzwerkabrechnung, die Netzwerkanalyse und die Sicherheitsüberwachung unerlässlich.
- Protokollunabhängigkeit: FNF ist flexibel genug, um verschiedene Protokolle über IP hinaus zu unterstützen, sodass es an unterschiedliche Netzwerkumgebungen angepasst werden kann.

Auf dem Catalyst 9800 WLC kann FNF so konfiguriert werden, dass Flow-Datensätze in eine externe NetFlow-Erfassungs- oder -Analyseanwendung exportiert werden. Diese Daten können dann zur Fehlerbehebung, Netzwerkplanung und Sicherheitsanalyse verwendet werden. Die FNF-Konfiguration umfasst die Definition eines Flow-Datensatzes (was erfasst werden soll), eines Flow-Exporteurs (wohin die Daten gesendet werden sollen) und das Anschließen des Flow-Monitors (der den Datensatz und den Exporteur verbindet) an die entsprechenden Schnittstellen.



Hinweis: FNF kann 17 verschiedene Datensätze (gemäß RFC 3954) an den externen NetFlow-Collector eines Drittanbieters senden, z. B. StealthWatch, Solarwinds und andere: Anwendungs-Tag, Client-MAC-Adresse, AP-MAC-Adresse, WlanID, Quell-IP, Ziel-IP, Quell-Port, Ziel-Port, Protokoll, Flow-Startzeit, Richtung, Packet-Out, Byte Anzahl, VLAN-ID (lokaler Modus) - Mgmt/Client und TOS - DSCP-Wert

## Datenflussüberwachung

Ein Flow Monitor ist eine Komponente, die zusammen mit Flexible NetFlow (FNF) zur Erfassung und Analyse von Netzwerkverkehrsdaten verwendet wird. Es spielt eine entscheidende Rolle bei der Überwachung und dem Verständnis von Datenverkehrsmustern für das Netzwerkmanagement, die Sicherheit und die Fehlerbehebung. Bei der Datenflussüberwachung handelt es sich im Wesentlichen um eine angewendete Instanz von FNF, die Datenflussdaten auf der Grundlage definierter Kriterien sammelt und verfolgt. Es umfasst drei Hauptelemente:

- Flow Record: Definiert die Daten, die der Flow Monitor aus dem Netzwerkverkehr sammeln muss. Es gibt die Schlüssel (wie Quell- und Ziel-IP-Adressen, Ports, Protokolltypen) und

Nicht-Schlüsselfelder (wie Paket- und Byte-Zähler, Zeitstempel) an, die in die Flussdaten eingeschlossen werden.

- Flow Exporter: Gibt das Ziel an, an das die erfassten Flow-Daten gesendet werden müssen. Dazu gehören Details wie die IP-Adresse des NetFlow Collectors, das Transportprotokoll (in der Regel UDP) und die Zielportnummer, auf die der Collector wartet.
- Flow Monitor: Der Flow Monitor selbst verbindet den Flow Record mit dem Flow Exporter und wendet sie auf eine Schnittstelle oder ein WLAN an, um den Überwachungsprozess zu starten. Er legt fest, wie die Flow-Daten gesammelt und exportiert werden müssen, basierend auf den Kriterien, die im Flow-Datensatz und dem Ziel-Set im Flow-Exporter festgelegt sind.

## Von AVC unterstützte Access Points

AVC wird nur auf diesen Access Points unterstützt:

- Cisco Catalyst Serie 9100
- Cisco Aironet Access Point der Serie 2800
- Cisco Aironet Access Points der Serie 3800
- Cisco Aironet Access Points der Serie 4800

## Unterstützung verschiedener Bereitstellungsmodi des 9800

Bereitstellungsmodus	9800 WLC	Access Point der Phase 1	Access Point der Phase 2	Wi-Fi 6 Access Point
Lokaler Modus (Zentrales Switching)	IPV4-Datenverkehr: AVC unterstützt Unterstützte FNF  IPV6-Datenverkehr: AVC unterstützt Unterstützte FNF	Verarbeitung auf WLC-Ebene	Verarbeitung auf WLC-Ebene	Verarbeitung auf WLC-Ebene
Flex-Modus (Zentrales Switching)	IPV4-Datenverkehr: AVC unterstützt	Verarbeitung auf WLC-Ebene	Verarbeitung auf WLC-Ebene	Verarbeitung auf WLC-Ebene

	<p>Unterstützte FNF</p> <p>IPV6-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p>			
Flex-Modus (Lokales Switching)	Verarbeitung auf AP-Ebene	<p>IPV4-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p> <p>IPV6-Datenverkehr: AVC unterstützt</p> <p>FNF wird nicht unterstützt</p>	<p>IPV4-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p> <p>IPV6-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p>	<p>IPV4-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p> <p>IPV6-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p>
Lokaler Modus (Fabric)	Verarbeitung auf AP-Ebene	<p>IPV4-Datenverkehr: AVC nicht unterstützt</p> <p>FNF wird nicht unterstützt</p> <p>IPV6-Datenverkehr: AVC nicht unterstützt</p> <p>FNF wird nicht unterstützt</p>	<p>IPV4-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p> <p>IPV6-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p>	<p>IPV4-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p> <p>IPV6-Datenverkehr: AVC unterstützt</p> <p>Unterstützte FNF</p>

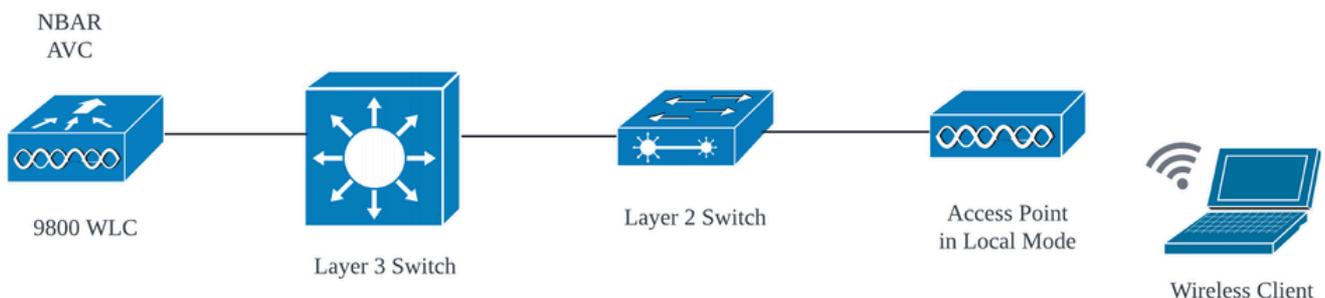
Einschränkungen bei der Implementierung von AVC auf 9800

Application Visibility and Control (AVC) und Flexible NetFlow (FNF) sind leistungsstarke Funktionen für Cisco Catalyst Wireless LAN Controller der Serie 9800, die die Netzwerktransparenz und -kontrolle verbessern. Bei der Verwendung dieser Funktionen sollten jedoch einige Einschränkungen und Überlegungen beachtet werden:

- Controller-übergreifendes Layer-2-Roaming wird nicht unterstützt.
- Multicast-Datenverkehr wird nicht unterstützt.
- Nur Anwendungen, die für Anwendungstransparenz erkannt werden, können für die Anwendung der QoS-Kontrolle verwendet werden.
- Die Datenverbindung wird für NetFlow-Felder in AVC nicht unterstützt.
- Sie können nicht dasselbe WLAN-Profil sowohl dem Richtlinienprofil "AVC nicht aktiviert" als auch dem Richtlinienprofil "AVC aktiviert" zuordnen.
- Sie können das Richtlinienprofil mit unterschiedlichen Switching-Mechanismen für dasselbe WLAN nicht zur Implementierung von AVC verwenden.
- AVC wird auf dem Management-Port (Gig 0/0) nicht unterstützt.
- Eine NBAR-basierte QoS-Richtlinienkonfiguration ist nur für kabelgebundene physische Ports zulässig. Die Richtlinienkonfiguration wird für virtuelle Schnittstellen wie VLAN, Port-Channel und andere logische Schnittstellen nicht unterstützt.
- Wenn AVC aktiviert ist, unterstützt das AVC-Profil nur bis zu 23 Regeln, einschließlich der Standard-DSCP-Regel. Die AVC-Richtlinie wird nicht an den Access Point übertragen, wenn die Regeln mehr als 23 betragen.

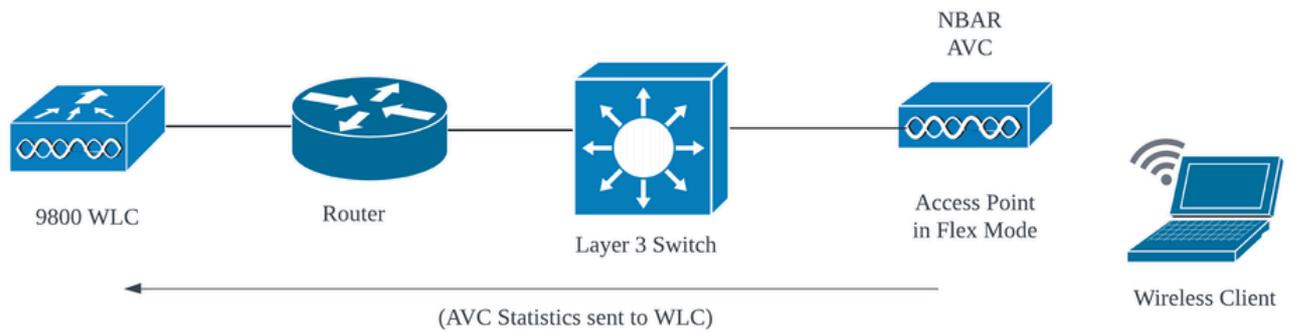
## Netzwerktopologie

### AP im lokalen Modus



AVC im AP im lokalen Modus (zentrales Switching)

### AP im flexiblen Modus



AVC im Flex Mode-AP

## Konfiguration von AVC auf dem 9800 WLC

Bei der Konfiguration von AVC auf dem 9800 WLC können Sie es entweder als NetFlow Collector verwenden oder die NetFlow-Daten in den externen NetFlow Collector exportieren.

### Lokaler Exporteur

Auf einem Cisco Catalyst 9800 Wireless LAN Controller (WLC) bezieht sich ein lokaler NetFlow Collector auf die integrierte Funktion im WLC, mit der NetFlow-Daten gesammelt und lokal gespeichert werden können. Auf diese Weise kann der WLC grundlegende NetFlow-Datenanalysen durchführen, ohne die Flow-Datensätze in einen externen NetFlow Collector exportieren zu müssen.

### Über GUI

Schritt 1: Um AVC für eine bestimmte SSID zu aktivieren, gehen Sie zu Configuration > Services > Application Visibility. Wählen Sie das jeweilige Richtlinienprofil aus, für das Sie AVC aktivieren möchten.

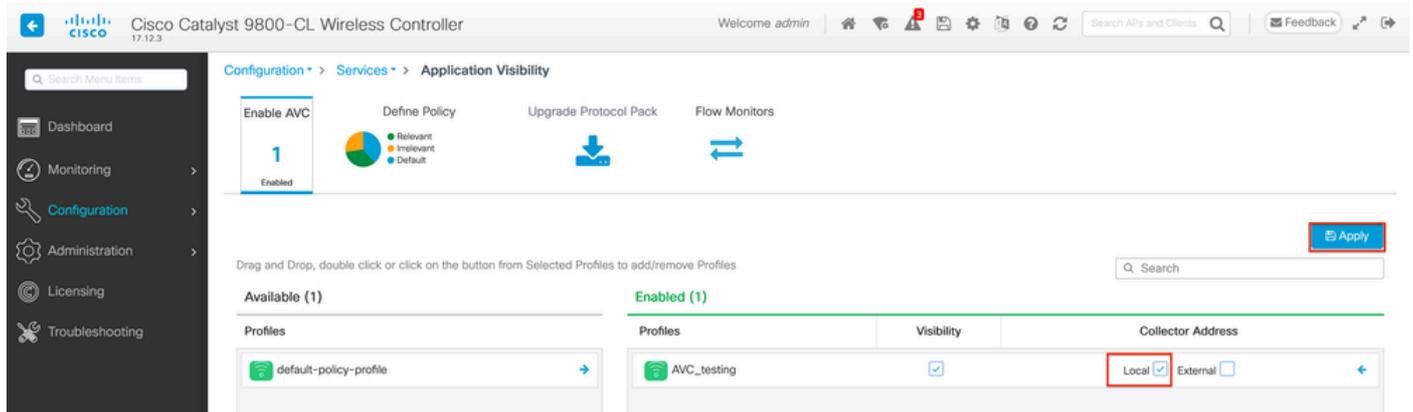
The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is 'Configuration > Services > Application Visibility'. The 'Enable AVC' section is active, showing a '1' and 'Enabled' status. Below this, there are sections for 'Available (2)' and 'Enabled (0)'. The 'Available (2)' section contains a table with two rows:

Profiles	Visibility	Collector Address
AVC_testing		
default-policy-profile		

The 'AVC\_testing' row has a red box around its right-pointing arrow button, indicating it is the profile selected for activation.

Aktivieren von AVC im Richtlinienprofil

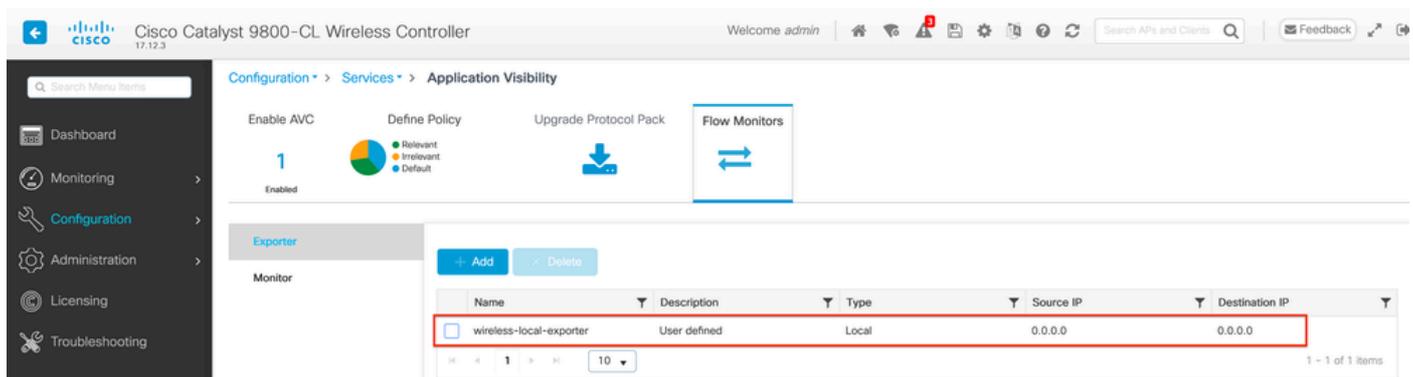
Schritt 2: Wählen Sie als NetFlow Collector Local aus, und klicken Sie auf Apply.



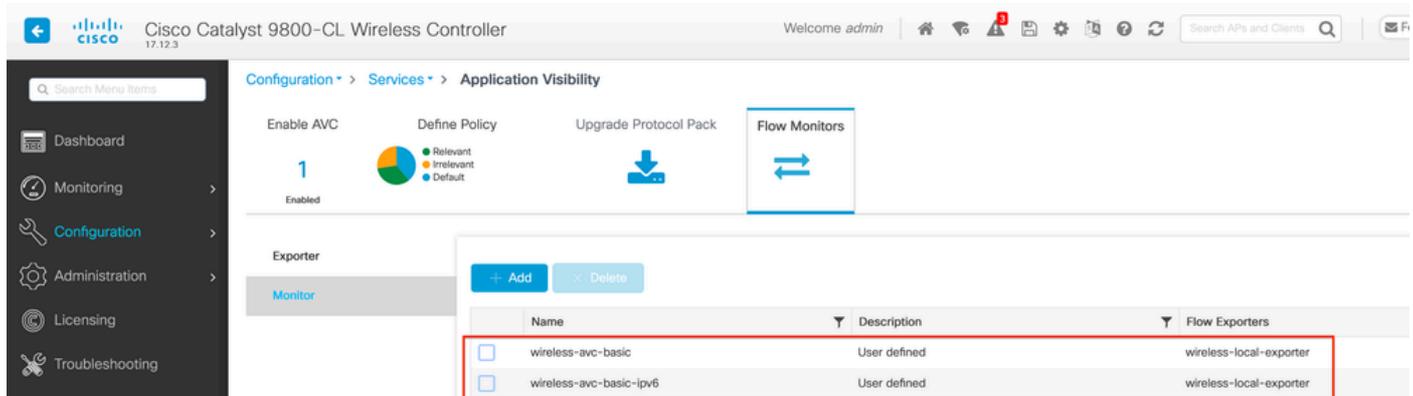
Auswählen des lokalen NetFlow-Collectors

Beachten Sie, dass die NetFlow-Exporter- und NetFlow-Einstellungen automatisch entsprechend der angegebenen Voreinstellungen konfiguriert wurden, nachdem Sie die AVC-Konfiguration angewendet haben.

Sie können dies überprüfen, indem Sie zu Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor navigieren.

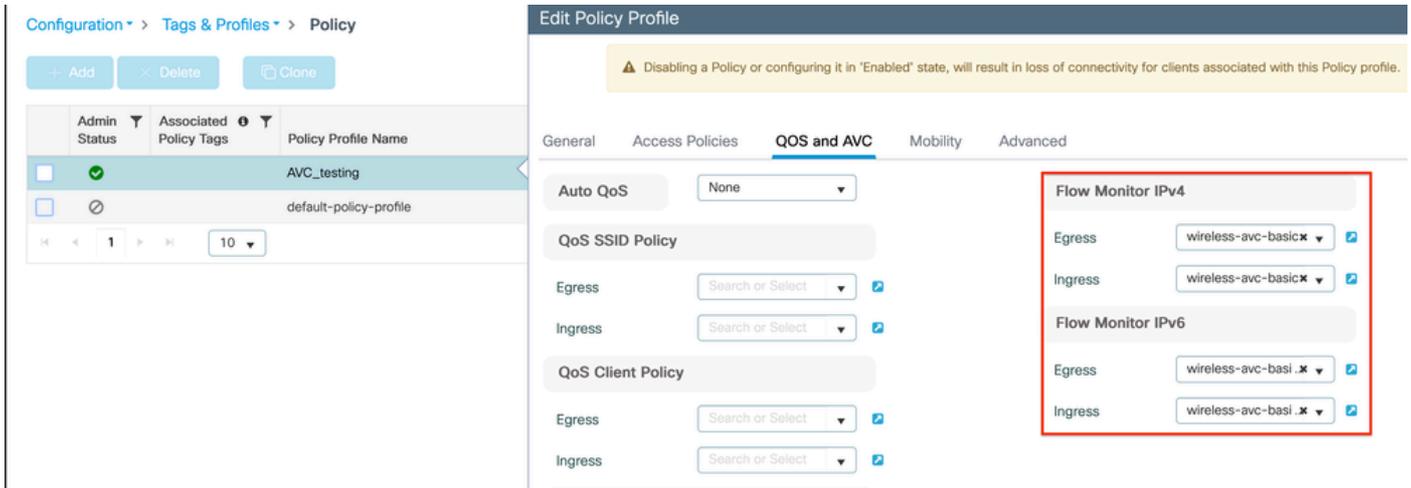


Lokale Flow Collector-Konfiguration auf 9800 WLC



Konfiguration des Datenflussmonitors mit dem lokalen NetFlow Collector

Die IPv4- und IPv6 AVC-Flussmonitore werden automatisch mit dem Richtlinienprofil verknüpft. Navigieren Sie zu Konfiguration > Tags & Profil > Richtlinie. Klicken Sie auf Richtlinienprofil > AVC und QoS.



Konfiguration der Datenflussüberwachung im Richtlinienprofil

## Über CLI

### Schritt 1: Konfigurieren des 9800 WLC als lokaler 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
```

### Schritt 2: Konfigurieren von IPv4 und IPv6 Network Flow Monitor zur Verwendung von Local (WLC) als 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
```

### Schritt 3: Zuordnen des IPv4- und IPv6 Flow Monitor im Richtlinienprofil für eingehenden und ausgehenden Datenverkehr

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

```

## Externer NetFlow-Collector

Ein externer NetFlow Collector ist ein dediziertes System oder ein Service, das bzw. der im Kontext von Application Visibility and Control (AVC) auf einem Cisco Catalyst 9800 Wireless LAN Controller (WLC) verwendet wird und die vom WLC exportierten NetFlow-Daten empfängt, aggregiert und analysiert. Sie können entweder nur den externen NetFlow Collector konfigurieren, um die Anwendungstransparenz zu überwachen, oder Sie können ihn zusammen mit dem lokalen Collector verwenden.

### Über GUI

Schritt 1: Um AVC für eine bestimmte SSID zu aktivieren, navigieren Sie zu Configuration > Services > Application Visibility. Wählen Sie das jeweilige Richtlinienprofil aus, für das Sie AVC aktivieren möchten. Wählen Sie Collector als External aus, konfigurieren Sie die IP-Adresse von NetFlow Collector wie Cisco Prime, SolarWind, StealthWatch, und klicken Sie auf Apply.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The navigation path is Configuration > Services > Application Visibility. The 'Enable AVC' section is active, showing a '1' and 'Enabled' status. Below this, there are sections for 'Available (1)' and 'Enabled (1)'. The 'Enabled (1)' section contains a table with the following data:

Profiles	Visibility	Local	External	Collector Address
AVC_testing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.106.36.22

AVC-Konfiguration für externen NetFlow Collector

Beachten Sie, dass nach Anwendung der AVC-Konfiguration die NetFlow Exporter- und NetFlow-Einstellungen automatisch mit der IP-Adresse von NetFlow Collector als Exporter- und Exporter-Adresse als 9800 WLC mit Standard-Timeout-Einstellungen und UDP-Port 9995 konfiguriert wurden. Sie können dies überprüfen, indem Sie zu Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor navigieren.

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
export_-1638039067	User defined	External	10.197.234.75	10.106.36.22

Externe NetFlow Collector-Konfiguration auf dem 9800 WLC

Configuration > Services > Application Visibility

Enable AVC: 1 Enabled

Define Policy: Relevant, Irrelevant, Default

Upgrade Protocol Pack

Flow Monitors

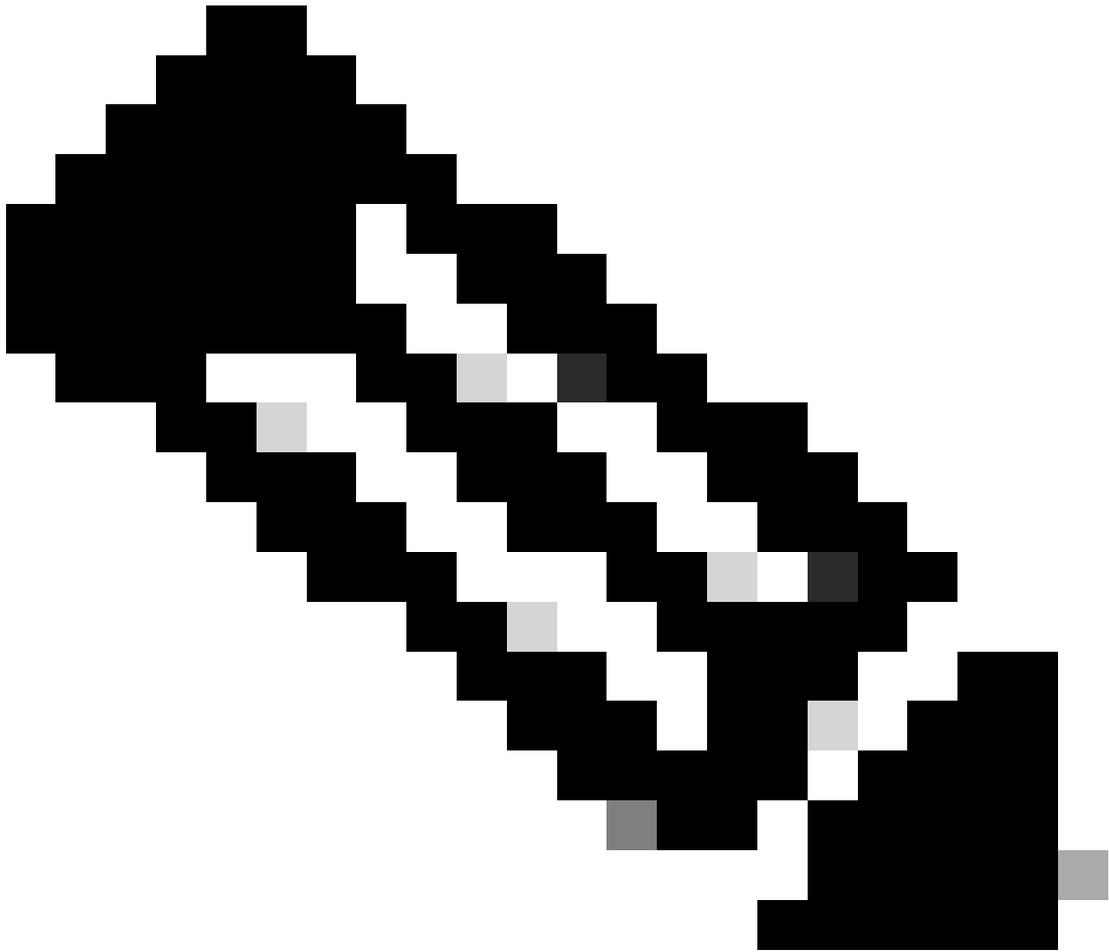
Name	Description	Flow Exporters
dwavc_-1638039067	User defined	export_-1638039067
dwavc_ipv6_-1638039067	User defined	export_-1638039067

Konfiguration des Datenflussmonitors mit externem NetFlow Collector

Sie können die Port-Konfiguration des automatisch generierten NetFlow-Monitors überprüfen, indem Sie zu Configuration > Services > NetFlow navigieren.

Configuration > Services > NetFlow

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



Hinweis: Wenn Sie AVC über die GUI konfigurieren, wird der automatisch generierte NetFlow Exporter für die Verwendung des UDP 9995-Ports konfiguriert. Überprüfen Sie unbedingt die Portnummer, die von Ihrem NetFlow Collector verwendet wird.

Beispiel: Wenn Sie Cisco Prime als NetFlow Collector verwenden, muss der Exporter-Port auf 9991 festgelegt werden, da dies der Port ist, auf dem Cisco Prime auf NetFlow-Datenverkehr wartet. Sie können den Exporter-Port in der NetFlow-Konfiguration manuell ändern.

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

NetFlow Template	Interfaces/Profiles	Collector	Export Inte
<input checked="" type="checkbox"/> Wireless avc basic	Not Assigned	10.106.36.22	10.197.23...
<input type="checkbox"/> Wireless avc basic IPv6	Not Assigned	10.106.36.22	10.197.234
<input type="checkbox"/> Wireless avc basic	AVC_testing		10.197.234
<input type="checkbox"/> Wireless avc basic IPv6	AVC_testing		10.197.234

The 'Edit NetFlow' dialog is open, showing the following configuration:

- Netflow Template: Wireless avc basic
- Local Exporter:
- External Exporter:
- Collector Address\*: 10.106.36.22
- Exporter Port\*: 9991
- Available (1): Search
- Profiles: default-policy-profile
- Profiles: AVC\_testing (Ingress: , Egress: )

A tooltip for the 'Exporter Port\*' field states: 'Enter the port number on which your netflow collector configured above is listening.'

## Über CLI

### Schritt 1: Konfigurieren der IP-Adresse von External NetFlow Collector über die Quellschnittstelle

```
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
```

### Schritt 2: Konfigurieren von IPv4 und IPv6 Network Flow Monitor zur Verwendung von Local (WLC) als 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
```

### Schritt 3: Zuordnen des IPv4- und IPv6 Flow Monitor im Richtlinienprofil für eingehenden und ausgehenden Datenverkehr

```
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
```

## Konfiguration von AVC auf dem 9800 WLC mit Cisco Catalyst

# Center

Bevor Sie mit der Konfiguration von Application Visibility and Control (AVC) auf einem Cisco Catalyst 9800 Wireless LAN Controller (WLC) über Cisco Catalyst Center fortfahren, müssen Sie überprüfen, ob die Telemetrikommunikation zwischen dem WLC und Cisco Catalyst Center erfolgreich eingerichtet wurde. Stellen Sie sicher, dass der WLC in verwaltetem Zustand in der Cisco Catalyst Center-Schnittstelle angezeigt wird und dass sein Zustand aktiv aktualisiert wird. Für eine effektive Überwachung des Diagnosestatus ist es zudem wichtig, den WLC und die Access Points (APs) den entsprechenden Standorten im Cisco Catalyst Center zuzuweisen.

```
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

Telemetrie-Verbindungsprüfung am 9800 WLC

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 und AP befinden sich im verwalteten Zustand

### Network Devices

LATEST **67%** Healthy TOTAL: 3

No Devices



Router

No Devices



Core

No Devices

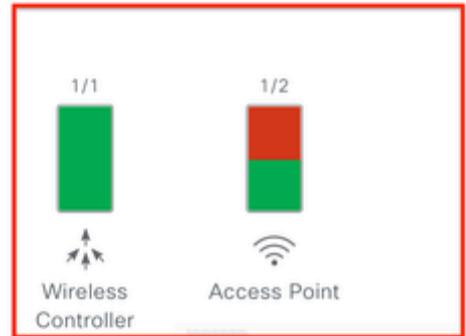


Distribution

No Devices



Access



Wireless Controller

Access Point

40%

7:30p

7:30p

[View Network Health](#)

Zustand von WLC und AP im Cisco Catalyst Center

Schritt 1: Konfigurieren Sie Cisco Catalyst Center als NetFlow Collector, und aktivieren Sie die Wireless-Telemetry in der globalen Einstellung. Navigieren Sie zu Design > Network Setting > Telemetry, und aktivieren Sie die gewünschte Konfiguration wie dargestellt.

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

Konfiguration von Wireless-Telemetrie und AVC

Schritt 2: Aktivieren Sie die Anwendungstelemetrie auf dem gewünschten 9800 WLC, um die AVC-Konfiguration auf dem 9800 WLC zu übertragen. Navigieren Sie dazu zu Provisioning > Network Device > Inventory. Wählen Sie den 9800 WLC aus, auf dem Sie die Anwendungstelemetrie aktivieren möchten, und navigieren Sie dann zu Aktion > Telemetrie > Anwendungstelemetrie aktivieren .

Catalyst Center Provision / Inventory

Global

All Routers Switches Wireless Controllers Access Points Sensors

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 > Software Image > Provision > <b>Telemetry &gt; Enable Application Telemetry</b>	Not Scanned	Managed
<input type="checkbox"/>	CW9164I-ROW1	10.105.193.152	Device Replacement >		
<input type="checkbox"/>	CW9164I-ROW2	10.105.60.35	Compliance >		
<input type="checkbox"/>	SDA_WLC.cisco.com	10.106.38.185	More >		

Enable Application Telemetry

Disable Application Telemetry

Update Telemetry Settings

Aktivieren der Anwendungstelemetrie auf dem 9800 WLC

Schritt 3: Wählen Sie den Bereitstellungsmodus gemäß der Anforderung aus.

Lokal: So aktivieren Sie AVC im lokalen Richtlinienprofil (Central Switching)

Flex/Fabric: Zum Aktivieren von AVC in Flex Policy Profile (Local Switching) oder Fabric-basierten SSIDs.

### 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.

Auswahl des Bereitstellungsmodus in Cisco Catalyst Center

Schritt 4: Es wird eine Aufgabe zur Aktivierung der AVC-Einstellungen initiiert. Die entsprechende Konfiguration wird auf den 9800 WLC angewendet. Sie können den Status anzeigen, indem Sie zu Aktivitäten > Audit Log (Überwachungsprotokoll) navigieren.

Jul 18, 2024 09:22 PM

3:37p

8/1 9/1 10/1 11/1 12/1 1/1 2/1 3/1 4/1 5/1

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]

Prüfprotokolle nach Aktivierung der Telemetrie auf dem 9800 WLC

Cisco Catalyst Center stellt die Flow Exporter- und Flow Monitor-Konfigurationen bereit, einschließlich des angegebenen Ports und anderer Einstellungen, und aktiviert sie im ausgewählten Modus-Richtlinienprofil, wie unten gezeigt:

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

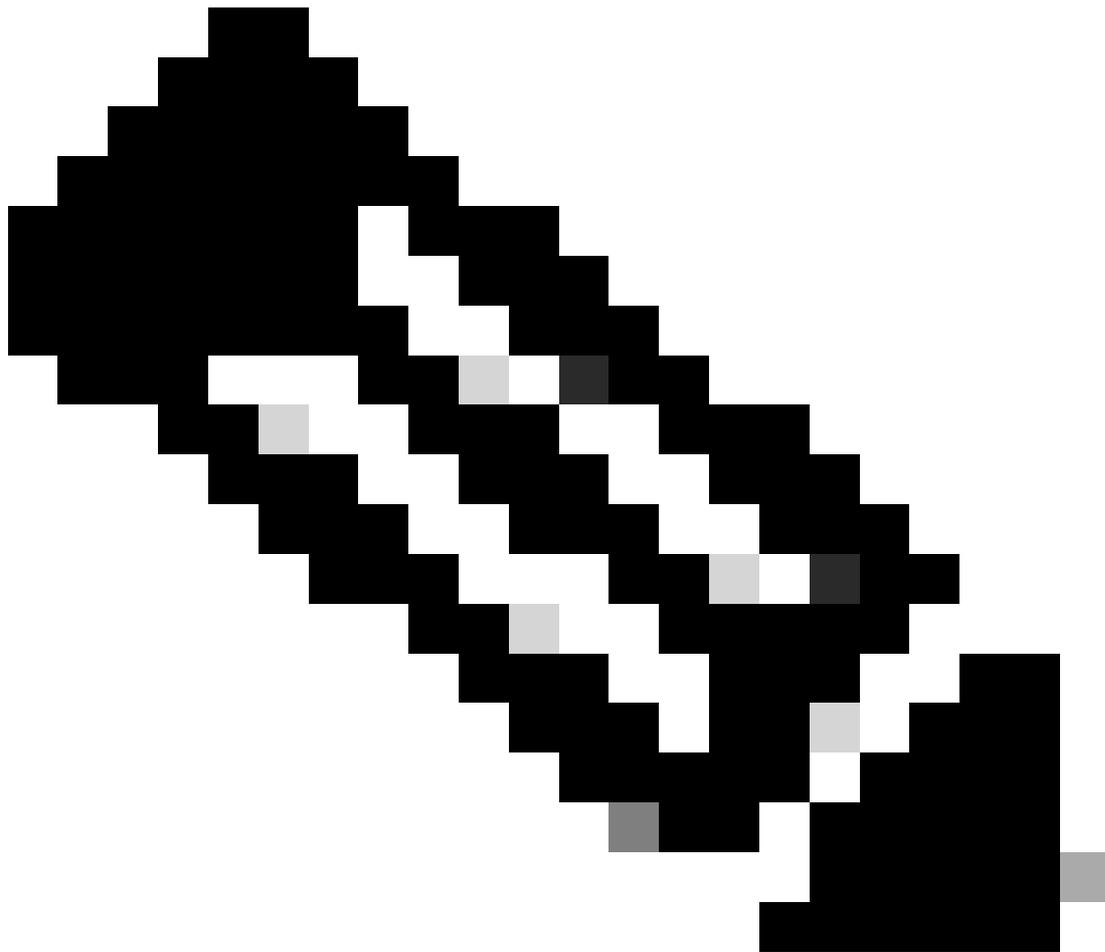
```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp 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
```

## AVC-Prüfung

### Auf 9800

Wenn der 9800 WLC als Flow-Exporter verwendet wird, können die folgenden AVC-Statistiken beobachtet werden:

- Anwendungstransparenz für Clients, die über alle SSIDs verbunden sind
- Individuelle Anwendungsnutzung für jeden Client.
- Spezifische Anwendungsnutzung auf jeder SSID separat.



Hinweis: Sie haben die Möglichkeit, die Daten nach Richtung zu filtern, wobei sowohl ein- als auch ausgehender Datenverkehr (ein- und ausgehender Datenverkehr) sowie nach Zeitintervall gefiltert werden. Dabei können Sie einen Bereich von bis zu 48 Stunden auswählen.

Über GUI

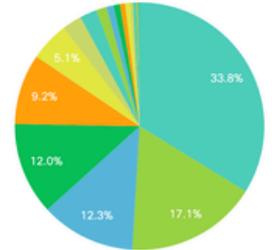
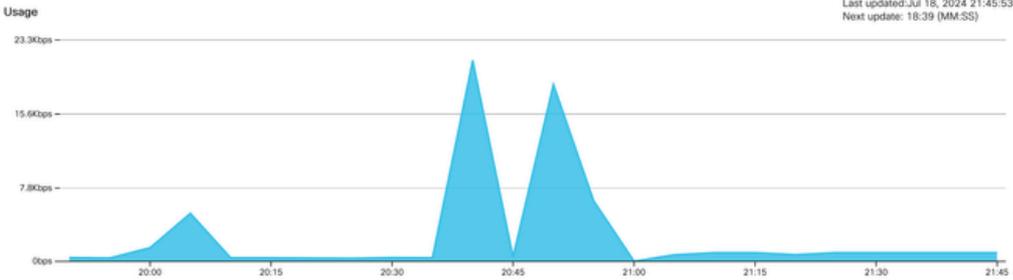
Navigieren Sie zu [Monitoring > Services > Application Visibility](#) .

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

Anwendungstransparenz der mit AVC\_testing verbundenen Benutzer für Eingangs- und Ausgangsverkehr

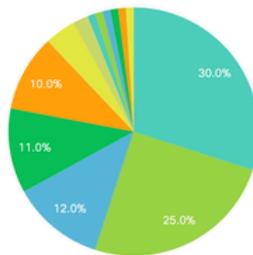
Um Statistiken zur Anwendungstransparenz für jeden Client anzuzeigen, können Sie auf die Registerkarte Clients klicken, einen bestimmten Client auswählen und dann auf Anwendungsdetails anzeigen klicken.

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)

Anwendungstransparenz für bestimmten 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

Anwendungstransparenz für bestimmten Client - 2

## Über CLI

### AVC-Status überprüfen

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

-----

AVC configuration complete: YES

### Statistiken von 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								
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

Überprüfen von AVC auf 9800 CLI

So untersuchen Sie die höchste Anwendungsnutzung für jedes WLAN und die verbundenen Clients einzeln:

```
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
```

## Überprüfung der Anzahl der FNFv9-Pakete und Decodierung des Status auf der Kontrollebene (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

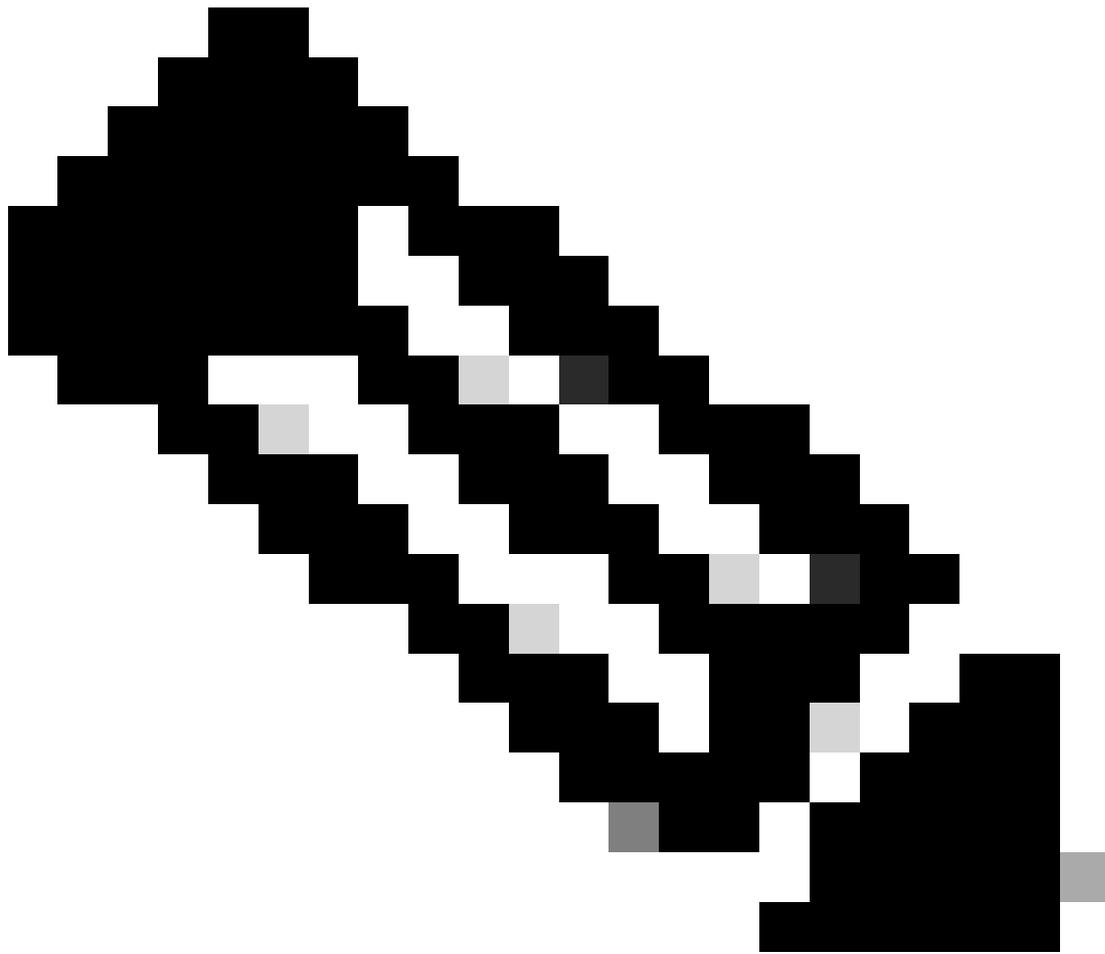
FNFv9-Paketdatensatz

Sie können die nbar-Statistiken auch direkt überprüfen.

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

Im Fabric- und Flex-Modus können Sie die NBAR-Statistiken vom Access Point abrufen über:

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



Hinweis: Bei einer Konfiguration mit einem ausländischen Anker dient der Anker-WLC als Layer-3-Präsenz für den Client, während der ausländische WLC auf Layer 2 betrieben wird. Da Application Visibility and Control (AVC) auf Layer 3 ausgeführt wird, sind die relevanten Daten nur auf dem Anker-WLC sichtbar.

## Bei DNAC

Anhand der Paketerfassung des 9800 WLC können wir überprüfen, ob Daten zu Anwendungen und Netzwerkverkehr kontinuierlich an Cisco Catalyst Center gesendet werden.

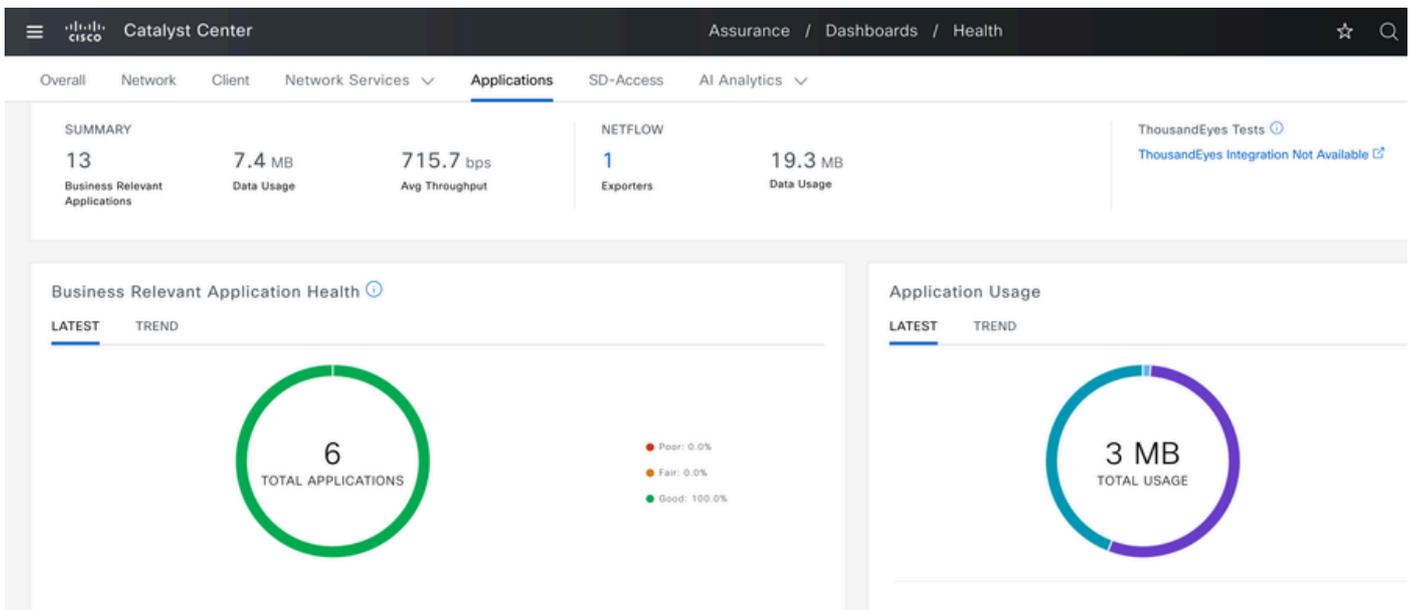
ip.addr == 10.78.8.84 and udp.port == 6007

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]

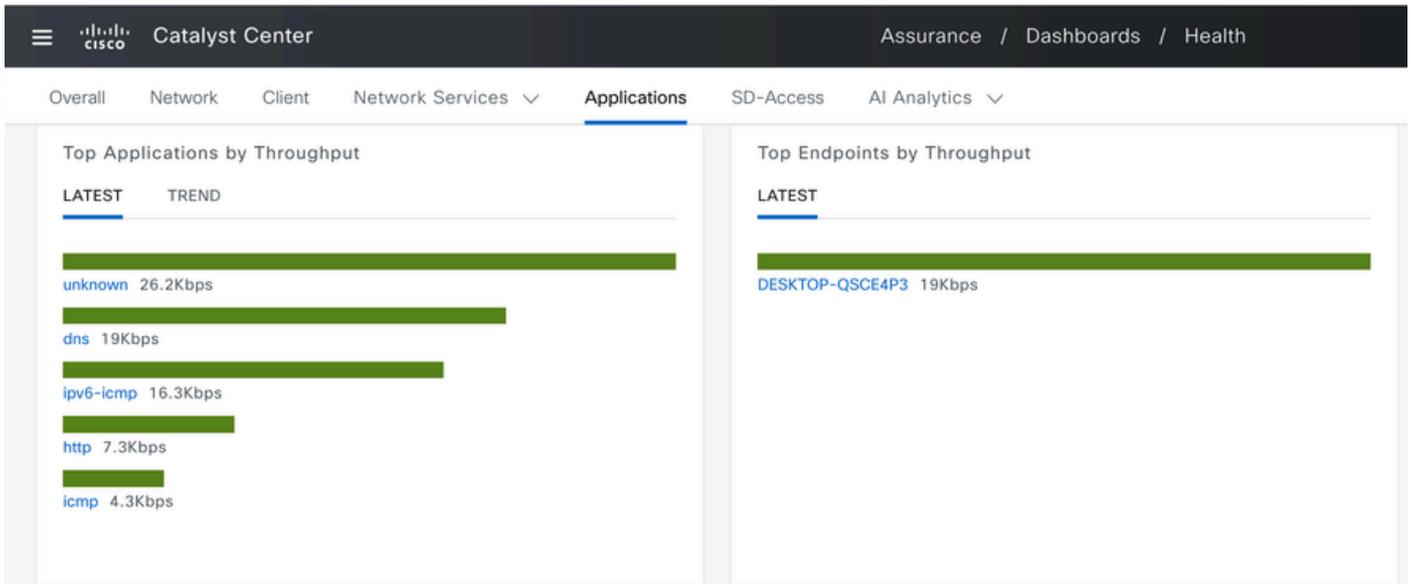
Paketerfassung auf 9800 WLC

Um die Anwendungsdaten für Clients anzuzeigen, die mit einem bestimmten WLC im Cisco Catalyst Center verbunden sind, navigieren Sie zu Assurance > Dashboards > Health > Application .



AVC-Überwachung auf Cisco Catalyst Center

Wir können die von Kunden am häufigsten verwendeten Anwendungen verfolgen und die Daten identifizieren, die am häufigsten von Kunden genutzt werden, wie hier gezeigt.



Benutzerstatistiken für Anwendungen mit höchster und höchster Bandbreite

Sie können einen Filter für eine bestimmte SSID festlegen, mit dem Sie den Gesamtdurchsatz und die Anwendungsnutzung der mit dieser SSID verbundenen Clients überwachen können.

Mit dieser Funktion können Sie die Anwendungen mit dem höchsten Bandbreitenbedarf und die Benutzer mit dem höchsten Bandbreitenbedarf im Netzwerk identifizieren.

Darüber hinaus können Sie die Funktion "Zeitfilter" nutzen, um diese Daten für frühere Zeiträume zu überprüfen und historische Einblicke in die Netzwerknutzung zu erhalten.

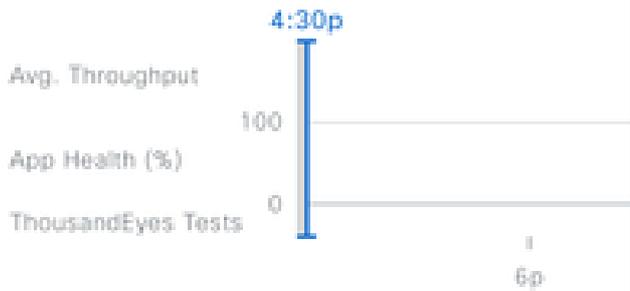
Global/BGL TAC/Shalini\_AVC

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

Zeitfilter zur Anzeige von AVC-Statistiken

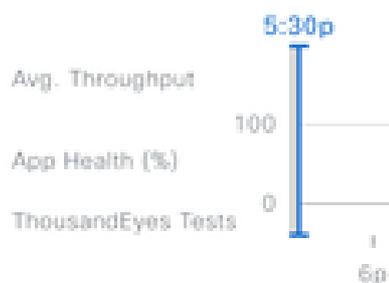


By default, hourly data is show

SSID (1/14)

Clear Filter

- CWA-test-321
- Session\_timeout
- LM-INTERNAL
- AVC\_testing**
- testvritti
- CWA-test-2
- renjith
- Start-Stop
- ...



SSID: AVC\_testing

Cancel

Apply

SSID-Filter zur Anzeige von AVC-Statistiken

## Auf externem NetFlow-Collector

### Beispiel 1: Cisco Prime als NetFlow Collector

Wenn Sie Cisco Prime als NetFlow-Collector verwenden, werden die gesammelten Daten vom 9800 WLC als Datenquelle angezeigt, die NetFlow-Daten senden. Die NetFlow-Vorlage wird entsprechend den vom 9800 WLC gesendeten Daten automatisch erstellt.

Anhand der Paketerfassung des 9800 WLC können wir überprüfen, ob Daten zu Anwendungen und Netzwerkverkehr kontinuierlich an Cisco Prime gesendet werden.

ip.addr == 10.106.36.22 && udp.port == 9991

No.	Time	Source	Destination	Protocol	Length	Info
87	20:50:23.855943	10.105.193.156	10.106.36.22	UDP	170	51154 → 9991 Len=128
1453	20:50:24.775945	10.105.193.156	10.106.36.22	UDP	458	51154 → 9991 Len=416
1465	20:50:24.856950	10.105.193.156	10.106.36.22	UDP	170	51154 → 9991 Len=128
1583	20:50:25.776952	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1584	20:50:25.776952	10.105.193.156	10.106.36.22	UDP	1082	51154 → 9991 Len=1040
1596	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1597	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1598	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	474	51154 → 9991 Len=432
1779	20:50:26.777959	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1780	20:50:26.777959	10.105.193.156	10.106.36.22	UDP	1158	51154 → 9991 Len=1116
1857	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1858	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1859	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1860	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	270	51154 → 9991 Len=228
1861	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1862	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	678	51154 → 9991 Len=636
2086	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
2087	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
2088	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	534	51154 → 9991 Len=492
2113	20:50:27.859940	10.105.193.156	10.106.36.22	UDP	578	51154 → 9991 Len=536
2287	20:50:28.779958	10.105.193.156	10.106.36.22	UDP	378	51154 → 9991 Len=336
2295	20:50:28.859940	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352

> Frame 87: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits)  
 > Ethernet II, Src: [REDACTED]  
 > Internet Protocol Version 4, Src: 10.105.193.156, Dst: 10.106.36.22  
 > User Datagram Protocol, Src Port: 51154, Dst Port: 9991  
 > Data (128 bytes)  
 Data [truncated]: 0009000120eb01e9669932b70000000400000400014f006c000000000000000000000000000000ff0200000000000000000011  
 [Length: 128]

Paketerfassung am 9800 WLC

Prime Infrastructure

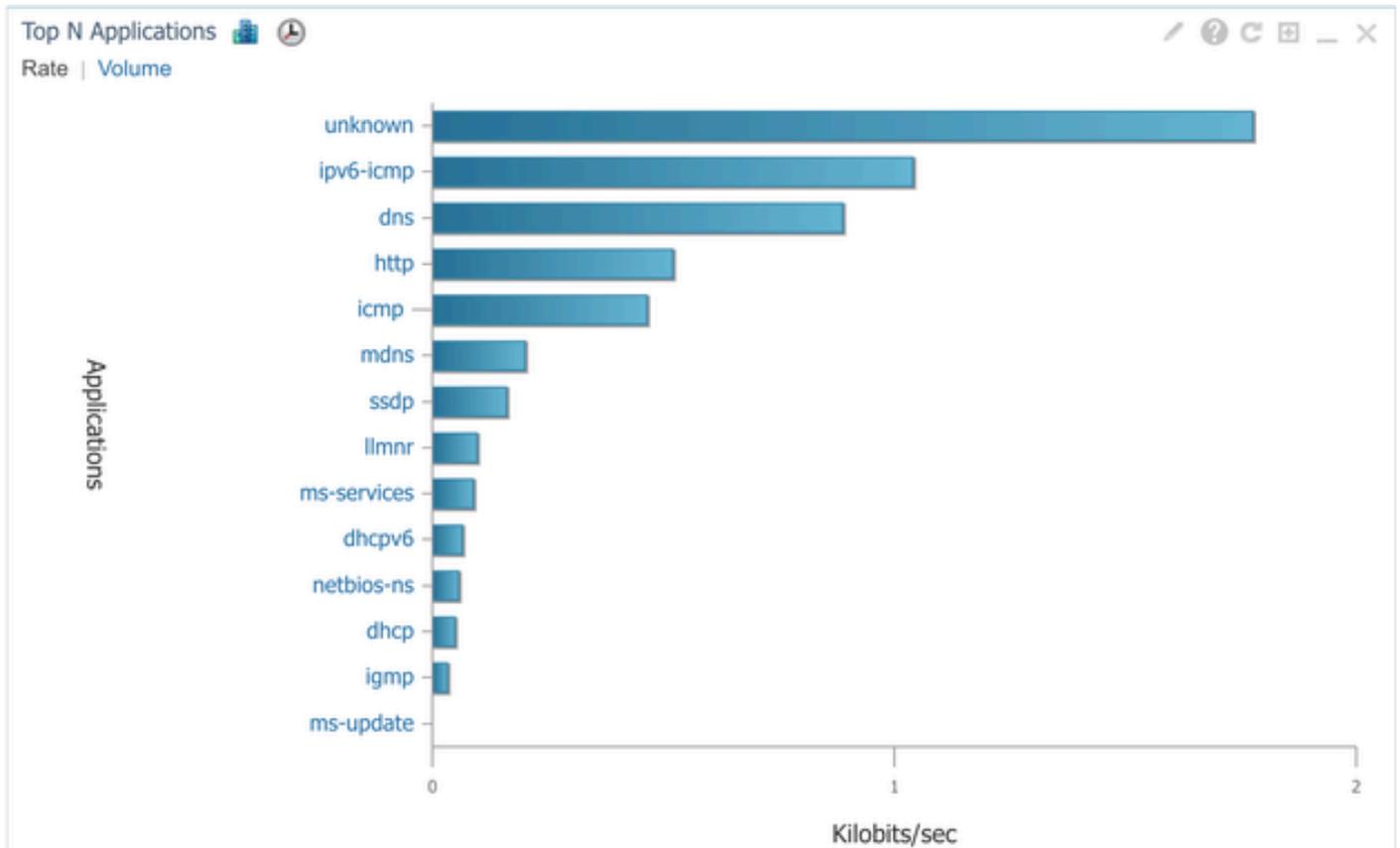
Services / Application Visibility & Control / Data Sources

Device Data Sources

Device Name	Data Source	Type	Exporting Device	Last 5 min Flow Record Rate	Last Active Time
<input type="checkbox"/> 9800WLC.cisco.com	10.105.193.156	NETFLOW	10.105.193.156	2	Friday, July 19 2024 at 04:50:18 AM India Standa...

Cisco Prime Detecting 9800 WLC als NetFlow-Datenquelle

Mithilfe der IP-Adresse können Sie Filter basierend auf Anwendungen, Services und sogar auf dem Client für eine gezieltere Datenanalyse einrichten.

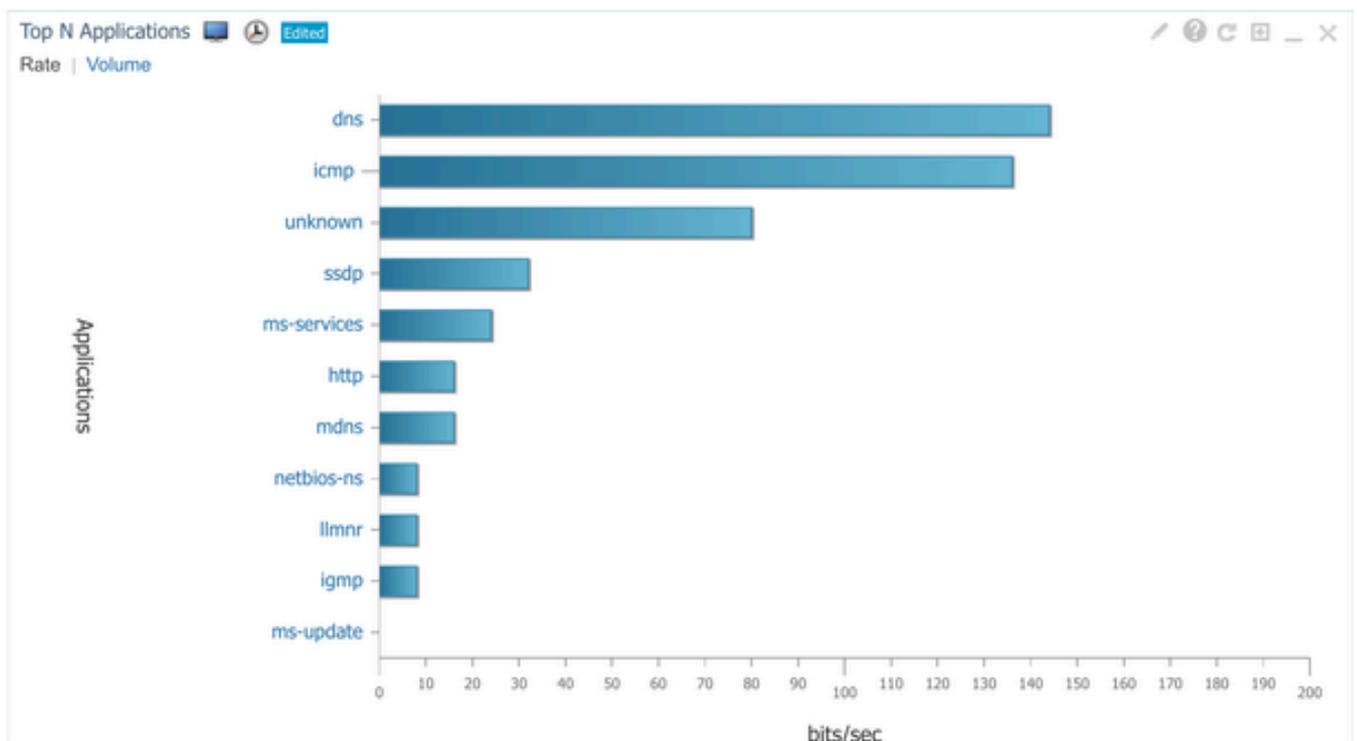


Anwendungstransparenz für alle Clients

 Dashboard / Performance 

Site | 
 Device | 
 Access Point | 
 Interface | 
 Application | 
 Voice/Video | 
 End User Experience

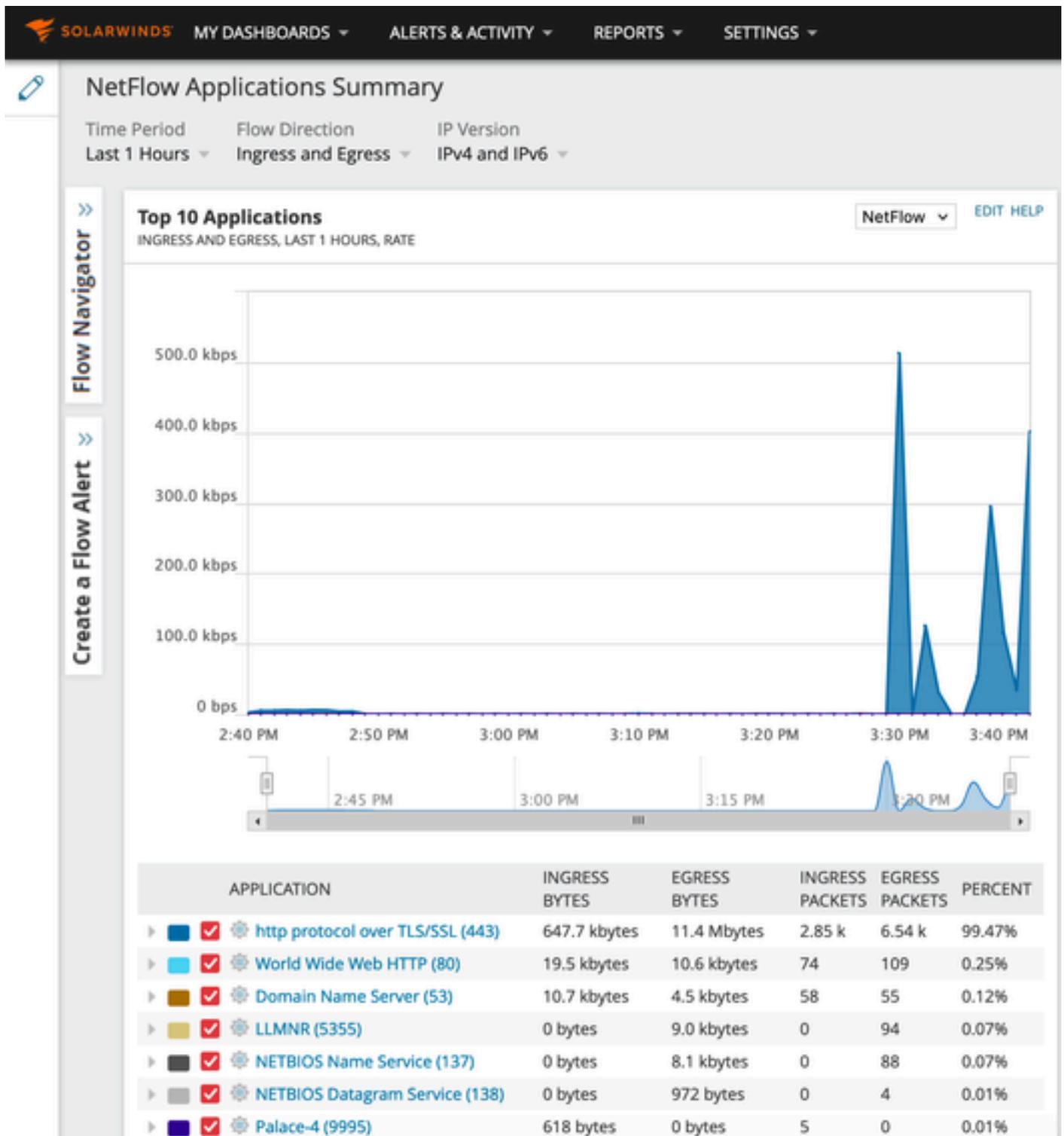
Filters  \*Client  | 
  \*Time Frame  | 
  Application  | 
  Network Aware



Anwendung eines bestimmten Clients mithilfe der IP-Adresse

## Beispiel 2: Drittanbieter NetFlow Collector

In diesem Beispiel wird der NetFlow Collector [SolarWinds] eines Drittanbieters zum Erfassen von Anwendungsstatistiken verwendet. Der 9800 WLC nutzt Flexible NetFlow (FNF), um umfassende Daten zu Anwendungen und Netzwerkverkehr zu übertragen, die dann von SolarWinds erfasst werden.



NetFlow-Anwendungsstatistik zu SolarWind

## Datenverkehrskontrolle

Die Datenverkehrskontrolle umfasst eine Reihe von Funktionen und Mechanismen zur Verwaltung und Regulierung des Datenverkehrs im Netzwerk. Traffic Policing oder Durchsatzratenbegrenzung sind Mechanismen, die im Wireless Controller verwendet werden, um die Menge des vom Client übertragenen Datenverkehrs zu steuern. Es überwacht die Datenrate für den Netzwerkverkehr und ergreift sofort Maßnahmen, wenn ein vordefinierter Raten Grenzwert überschritten wird. Wenn der Datenverkehr die angegebene Rate überschreitet, kann die Ratenbeschränkung die überschüssigen Pakete verwerfen oder sie durch Ändern der CoS- (Class of Service) oder DSCP-Werte (Differentiated Services Code Point) nach unten markieren. Dies kann durch die Konfiguration von QoS in 9800 WLC erreicht werden. Eine Übersicht über die Funktionsweise dieser Komponenten und ihre Konfiguration zur Erzielung unterschiedlicher Ergebnisse finden Sie unter <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html>.

## Fehlerbehebung

Zur Fehlerbehebung bei AVC-Problemen müssen Probleme identifiziert und behoben werden, die sich möglicherweise auf die Fähigkeit von AVC auswirken, den Anwendungsdatenverkehr in Ihrem Wireless-Netzwerk genau zu identifizieren, zu klassifizieren und zu verwalten. Häufige Probleme können die Klassifizierung des Datenverkehrs, die Durchsetzung von Richtlinien oder die Berichterstellung betreffen. Im Folgenden sind einige Schritte und Überlegungen zur Fehlerbehebung bei AVC-Problemen mit einem Catalyst 9800 WLC aufgeführt:

- Prüfen der AVC-Konfiguration: Stellen Sie sicher, dass AVC auf dem WLC richtig konfiguriert und den richtigen WLANs und Profilen zugeordnet ist.
- Wenn Sie AVC über die GUI einrichten, weist es automatisch Port 9995 als Standard zu. Wenn Sie jedoch einen externen Collector verwenden, überprüfen Sie, welcher Port für die Überwachung des NetFlow-Datenverkehrs konfiguriert ist. Es ist wichtig, diese Portnummer genau so zu konfigurieren, dass sie mit den Einstellungen Ihres Collectors übereinstimmt.
- Überprüfen der Unterstützung für AP-Modell und Bereitstellungsmodus
- Beachten Sie die Einschränkungen für den 9800 WLC bei der Implementierung von AVC in Ihrem Wireless-Netzwerk.

## Protokollsammlung

### WLC-Protokolle

1. Aktivieren Sie den Zeitstempel, um eine Zeitreferenz für alle Befehle zu erhalten.

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

2. Überprüfen der Konfiguration

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

3. Sie können die AVC-Status- und NetFlow-Statistiken überprüfen.

Prüfen Sie den AVC-Konfigurationsstatus.

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

Überprüfen Sie die Anzahl der FNFv9-Pakete, und decodieren Sie den Status per Zeitlimit für die Kontrollebene (CP).

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

Überprüfen von Statistiken aus NetFlow (FNF-Cache)

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

Aktivieren Sie Top n Anwendungsnutzung für jedes WLAN, wobei n = <1-30> Geben Sie die Anzahl der Anwendungen ein.

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

Prüfen Sie die Top-n-Anwendungsnutzung für jeden Client, wobei n = <1-30> Geben Sie die Anzahl der Anwendungen ein.

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

Aktivieren Sie die oberen n Clients, die über die jeweilige Anwendung mit einem bestimmten WLAN verbunden sind, wobei n=<1-10> Geben Sie die Anzahl der Clients ein.

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

Überprüfen Sie die Nbar-Statistik.

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

4. Legen Sie die Protokollierungsebene auf debug/verbose fest.

```
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. Aktivieren Sie Radioactive (RA) Trace für die MAC-Adresse des Clients, um die AVC-Statistiken zu validieren.

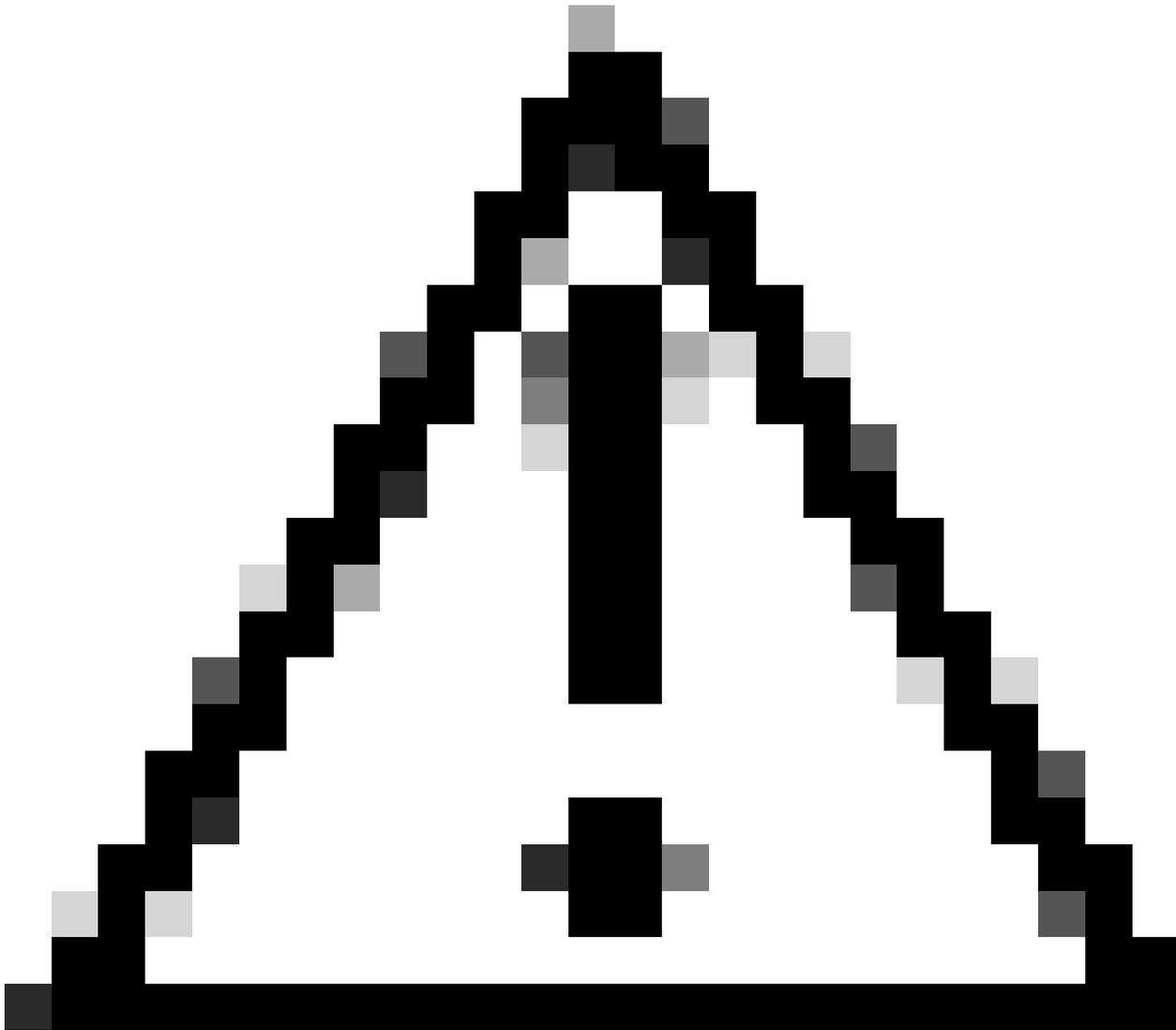
Über CLI

```
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
```



Achtung: Das bedingte Debuggen ermöglicht die Protokollierung auf Debugebene, wodurch sich wiederum die Anzahl der generierten Protokolle erhöht. Wenn Sie diese Option nicht ausführen, wird der Zeitaufwand für das Anzeigen von Protokollen reduziert. Daher wird empfohlen, das Debuggen immer am Ende der Fehlerbehebungssitzung zu deaktivieren.

```
# clear platform condition all  
# undebg all
```

### Über GUI

Schritt 1: Navigieren Sie zu Fehlerbehebung > Radioaktive Spur .

Schritt 2: Klicken Sie auf Hinzufügen, und geben Sie eine Client-MAC-Adresse ein, mit der Sie das Problem beheben möchten. Sie können mehrere Mac-Adressen zum Verfolgen hinzufügen.

Schritt 3: Wenn Sie bereit sind, die radioaktive Verfolgung zu starten, klicken Sie auf Start. Nach dem Start wird die Debug-Protokollierung für jede Verarbeitung auf der Steuerungsebene in

Bezug auf die verfolgten MAC-Adressen auf die Festplatte geschrieben.

Schritt 4: Wenn Sie das Problem reproduzieren, das Sie beheben möchten, klicken Sie auf Beenden .

Schritt 5: Für jede debuggte MAC-Adresse können Sie eine Protokolldatei erstellen, in der alle Protokolle zu dieser MAC-Adresse aufgelistet sind. Klicken Sie dazu auf Generate (Erstellen).

Schritt 6: Wählen Sie aus, wie lange die sortierte Protokolldatei zurückgehen soll, und klicken Sie auf Auf Gerät anwenden.

Schritt 7. Sie können die Datei jetzt herunterladen, indem Sie auf das kleine Symbol neben dem Dateinamen klicken. Diese Datei befindet sich im Boot-Flash-Laufwerk des Controllers und kann auch über die CLI kopiert werden.

Hier ist ein Blick auf AVC-Fehlerbehebungen 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 gefiltert nach Client-MAC-Adresse in beide Richtungen, Client inneren MAC-Filter verfügbar nach 17.1.

Diese Funktion ist besonders bei der Verwendung eines externen Collectors nützlich, da sie dazu beiträgt, zu überprüfen, ob der WLC NetFlow-Daten erwartungsgemäß an den beabsichtigten Port überträgt.

Über 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
```

Über GUI

Schritt 1: Navigieren Sie zu Troubleshooting > Packet Capture > +Add .

Schritt 2: Definieren Sie den Namen der Paketerfassung. Es sind maximal 8 Zeichen zulässig.

Schritt 3: Definieren Sie ggf. Filter.

Schritt 4: Aktivieren Sie das Kontrollkästchen Control Traffic überwachen, wenn der Datenverkehr zur System-CPU geleitet und zurück in die Datenebene eingespeist werden soll.

Schritt 5: Puffergröße definieren. Es sind maximal 100 MB zulässig.

Schritt 6: Definieren Sie einen Grenzwert, entweder nach Dauer, die einen Bereich von 1 bis 1000000 Sekunden zulässt, oder nach Anzahl der Pakete, die einen Bereich von 1 bis 100000 Paketen erlaubt, wie gewünscht.

Schritt 7. Wählen Sie die Schnittstelle aus der Liste der Schnittstellen in der linken Spalte aus, und klicken Sie auf den Pfeil, um sie in die rechte Spalte zu verschieben.

Schritt 8: Klicken Sie auf Auf Gerät anwenden.

Schritt 9. Um die Erfassung zu starten, wählen Sie Start aus.

Schritt 10. Sie können die Erfassung bis zum definierten Limit laufen lassen. Um die Erfassung manuell zu stoppen, wählen Sie Stopp.

Schritt 11. Nach dem Beenden wird eine Export-Schaltfläche verfügbar, auf die Sie klicken können, um die Erfassungsdatei (.pcap) über einen HTTP- oder TFTP-Server oder einen FTP-Server oder eine Festplatte oder einen Flash-Speicher des lokalen Systems auf den lokalen Desktop herunterzuladen.

AP-Protokolle

Im Fabric- und Flex-Modus

1. show tech zeigt alle Konfigurationsdetails und Client-Statistiken für den Access Point.
2. avc nbar Statistiken anzeigen nbar Statistiken von AP
3. AVC-Fehlersuche

```
AP#term mon
```

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

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

## Zugehörige Informationen

[AVC Konfigurationsleitfaden](#)

[Durchsatzbegrenzung für 9800 WLC](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.