VACL-opname voor granulaire verkeersanalyse met Cisco Catalyst 6000/6500 actieve CatOS-software

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Verwante producten](#)
[Conventies](#)
[Achtergrondinformatie](#)
[VLAN-gebaseerde SPAN](#)
[VLAN ACL](#)
[VACL-gebruik via VSPAN-gebruik](#)
[Configureren](#)
[Netwerkdiagram](#)
[Configuratie met VLAN-gebaseerde SPAN](#)
[Configuratie met VACL](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het gebruik van de VACL-poortfunctie (VLAN Access Control List) (VACL) voor netwerkverkeersanalyse op een meer granulaire manier. In dit document wordt ook het voordeel aangegeven van het VACL-opnamepoortgebruik in plaats van het VLAN-gebaseerde Switched Port Analyzer (SPAN)-gebruik.

Om de optie VACL-opnamepoort op Cisco Catalyst 6000/6500 te configureren die Cisco IOS®-software draait, raadpleegt u VACL-opname voor granulaire verkeersanalyse met Cisco Catalyst 6000/6500 die Cisco IOS-software uitvoert.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Virtual LAN-raadpleeg Virtual LANs/VLAN Trunking Protocol (VLAN's/VTP) - Inleiding voor meer informatie.
- Toegangslijsten - raadpleeg de toegangscontrole te configureren voor meer informatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Catalyst 6506 Series Switch die Catalyst OS release 8.1(2) draait.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco Catalyst 6000/6500 Series Switches die Catalyst OS release 6.3 en hoger uitvoeren.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

VLAN-gebaseerde SPAN

SPAN kopieert verkeer van één of meer bronpoorten in om het even welk VLAN of van één of meer VLAN's naar een doelpoort voor analyse. Local SPAN ondersteunt bronpoorten, bron VLAN's en doelpoorten op dezelfde Catalyst 6500 Series Switch.

Een bronpoort is een poort die wordt gecontroleerd voor netwerkverkeersanalyse. Een bron VLAN is een VLAN dat voor de analyse van het netwerkverkeer wordt gecontroleerd. VLAN-gebaseerde SPAN (VSPAN) is analyse van het netwerkverkeer in een of meer VLAN's. U kunt VSPAN configureren als ingress SPAN, SPAN of beide. Alle poorten in de bron-VLAN's worden de operationele bronpoorten voor de VSPAN-sessie. De bestemmingspoorten, als zij tot een van de administratieve bron VLAN's behoren, zijn van de operationele bron uitgesloten. Als u de poorten toevoegt of verwijdert van de administratieve bron VLAN's, worden de operationele bronnen dienovereenkomstig aangepast.

Richtsnoeren voor VSPAN-sessies:

- De boomstampoorten zijn inbegrepen als de bronpoorten voor de VSPAN sessies, maar alleen VLAN's die in de Admin-bronlijst staan, worden gemonitord als deze VLAN's actief zijn voor de stam.
- Voor de VSPAN-sessies met zowel ingress- als progressiegerelateerde SPAN ingesteld werkt het systeem op basis van het type supervisor-machine dat u heeft:WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2, WS-X6K-S2-PFC2, WS-X6K-S1A-MSFC2, WS-

SUP720, WS-SUP32-GE-3B-Twee worden door de pakketten doorgestuurd SPAN de bestemmingspoort als de pakketten op hetzelfde VLAN worden geschakeld.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE—Er wordt slechts één pakket door de SPAN-doelpoort verzonden.

- Een inband poort is niet als operationele bron voor de VSPAN-sessies opgenomen.
- Wanneer een VLAN wordt gewist, wordt het uit de bronlijst voor de VSPAN-sessies verwijderd.
- Een VSPAN-sessie is uitgeschakeld als de lijst Admin-bron VLAN's leeg is.
- De inactieve VLAN's zijn niet toegestaan voor de VSPAN-configuratie.
- Een VSPAN-sessie wordt inactief gemaakt als een van de bronnen VLAN's de RSPAN-VLAN's wordt.

Raadpleeg Kenmerken van Bron VLAN voor meer informatie over bron VLAN's.

VLAN ACL

De VACL's kunnen al het verkeer benaderen. U kunt de VACL's op de switch configureren om van toepassing te zijn op alle pakketten die in of uit een VLAN worden verzonden of in een VLAN worden overbrugd. De VACL's zijn streng voor security pakketfiltering en het doorsturen van verkeer naar specifieke fysieke switch poorten. In tegenstelling tot Cisco IOS ACL's worden VACL's niet gedefinieerd door richting (invoer of uitvoer).

U kunt de VACL's op Layer 3-adressen voor IP en IPX configureren. Alle andere protocollen zijn toegang gecontroleerd door de MAC-adressen en EtherType met behulp van de MAC VACL's. Het IP-verkeer en het IPX-verkeer zijn niet toegankelijk via de MAC-VACL's. Alle andere verkeerstypen (AppleTalk, DECnet, enz.) worden geclassificeerd als MAC-verkeer. De MAC VACL's worden gebruikt om dit verkeer te beheersen.

ACE's ondersteund in VACL's

VACL's bevat een geordende lijst met toegangscontrolelijsten (ACE's). Elke VACL kan ACE's van slechts één type bevatten. Elke ACE bevat een aantal velden die aangepast worden aan de inhoud van een pakje. Elk veld kan een gekoppeld bitmasker hebben om aan te geven welke bits relevant zijn. Een actie wordt geassocieerd met elk ACE dat beschrijft wat het systeem met het pakket zou moeten doen wanneer een overeenkomst plaatsvindt. Deze actie is afhankelijk van de functie. Catalyst 6500 Series Switches ondersteunen drie typen ACE's in de hardware:

- IP-ACE's
- IPX-ACE's
- Ethernet ACE's

Deze tabel toont de parameters die bij elk ACE-type zijn gekoppeld:

ACE type	TCP of UDP	ICMP	Overige IP	IPX	Ethernet
Layer 4 parameters	Bronpoort	-	-	-	-
	Bron-poortoperator	-	-	-	-
	Doelpoort	-	-	-	-
	Doelpoort	ICMP-	-	-	-

	operator	code			
	N.v.t.	ICMP-type	N.v.t.	-	-
Layer 3 parameters	IP naar S-bytes	IP naar S-bytes	IP naar S-bytes	-	-
	IP-bronadres	IP-bronadres	IP-bronadres	IPX-bronnetwerk	-
	IP-doeladres	IP-doeladres	IP-doeladres	IP-doelnetwerk	-
	-	-	-	IP-doelknooppunt	-
	TCP of UDP	ICMP	Ander protocol	IPX-pakkettype	-
Layer 2 parameters	-	-	-	-	EtherType
	-	-	-	-	Ethernet-bronadres
	-	-	-	-	Ethernet-doeladres

VACL-gebruik via VSPAN-gebruik

Er zijn verschillende beperkingen voor het gebruik van VSPAN voor verkeersanalyse:

- Alle Layer 2-verkeer dat in een VLAN stroomt, wordt opgenomen. Dit verhoogt de te analyseren hoeveelheid gegevens.
- Het aantal SPAN-sessies dat op Catalyst 6500 Series Switches kan worden ingesteld, is beperkt. Raadpleeg de functieoverzicht en de beperkingen voor meer informatie.
- Een doelhaven ontvangt exemplaren van verzonden en ontvangen verkeer voor alle gecontroleerde bronhavens. Als een doelpoort wordt oversubscript, kan deze verstopt raken. Deze congestie kan het doorsturen van verkeer op een of meer bronpoorten beïnvloeden.

De functie VACL-poort kan helpen bij het overwinnen van een aantal van deze beperkingen. VACL's zijn primair niet ontworpen om verkeer te bewaken. Aangezien het verkeer echter over een groot aantal mogelijkheden beschikt om het in te delen, is de optie Capture Port geïntroduceerd zodat de analyse van het netwerkverkeer veel eenvoudiger kan worden. Dit zijn de voordelen van het VACL-opnamepoortgebruik in vergelijking met VSPAN:

- Gedetailleerde verkeersanalyseVACL's kunnen op basis van IP-adres, IP-adres van de bron, Layer 4-protocoltype, bron- en doellaag 4-poorten en andere informatie overeenkomen. Deze mogelijkheid maakt VACL's zeer nuttig voor identificatie en filtering van granulair verkeer.
- Aantal sessiesVACL's worden op hardware toegepast. Het aantal ACE's dat kan worden gemaakt is afhankelijk van de TCAM die in de switches beschikbaar is.
- Overabonnement doelpoortDe identificatie van het granulair verkeer vermindert het aantal

frames dat naar de haven van bestemming moet worden doorgestuurd en minimaliseert aldus de kans op overinschrijving.
- PrestatiesVACL's worden op hardware toegepast. Er is geen prestatiestraf voor de toepassing van VACL's op een VLAN op Cisco Catalyst 6500 Series Switches.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

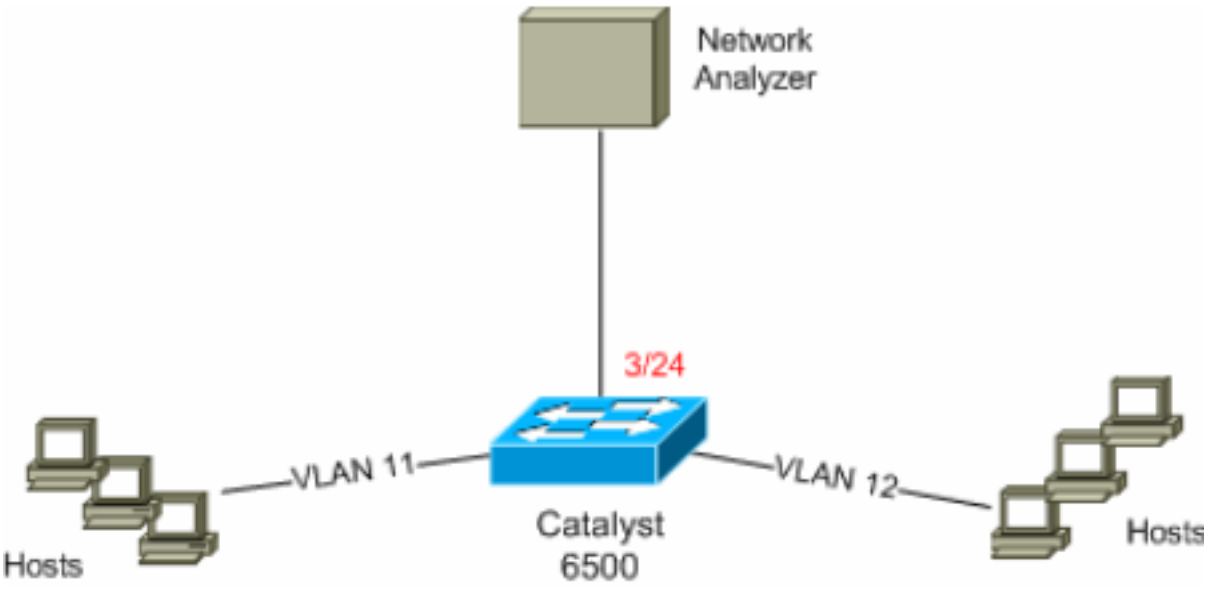
Dit document gebruikt deze configuraties:

- Configuratie met VLAN-gebaseerde SPAN
- Configuratie met VACL

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuratie met VLAN-gebaseerde SPAN

Dit configuratievoorbeeld maakt een lijst van de stappen die vereist zijn om al Layer 2-verkeer dat in VLAN 11 en VLAN 12 stroomt, op te nemen en naar het apparaat voor netwerkanalyse te sturen.

1. Specificeer het interessante verkeer.In dit voorbeeld, is het verkeer dat in VLAN 100 en VLAN 200 stroomt.

```
6K-CatOS> (enable) set span 11-12 3/24
!--- where 11-12 specifies the range of source VLANs and 3/24 specify the destination port.

2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des
tination port 3/24
```

```
Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi
on active for destination port 3/24
```

Hierdoor wordt al Layer 2-verkeer dat tot VLAN 11 en VLAN 12 behoort gekopieerd en naar poort 3/24 verzonden.

2. Controleer de SPAN-configuratie met de **show span all** opdracht.

```
6K-CatOS> (enable) show span all

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active


Total local span sessions:  1

No remote span session configured
6K-CatOS> (enable)
```

Configuratie met VACL

In dit configuratievoorbeeld zijn er meerdere vereisten van de netwerkbeheerder:

- HTTP-verkeer van een reeks hosts (10.12.12.128/25) in VLAN 12 naar een specifieke server (10.11.100) in VLAN 11 moet worden opgenomen.
- Multicast User Datagram Protocol (UDP)-verkeer in de verzendrichting voor groepsadres 239.0.100 moet vanaf VLAN 11 worden opgenomen.

1. Defineert het interessante verkeer met de Security ACL's. Denk eraan om de sleutelwoordenopname te noemen voor alle gedefinieerde ACE's.

```
6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit tcp 10.12.12.128 0.0.0.127 host
10.11.11.100 eq www capture
!--- Command wrapped to the second line. HttpUdp_Acl editbuffer modified. Use 'commit'
command to apply changes. 6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit udp any
host 239.0.0.100 capture
HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.
```

2. Controleer of de ACE-configuratie correct en in de juiste volgorde is.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Not Committed
6K-CatOS> (enable)
```

3. Sluit de ACL aan op de hardware.

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. Controleer de status van de ACL.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Committed
6K-CatOS> (enable)
```

5. Pas de VLAN-toegangskaart op de juiste VLAN's toe.

```
6K-CatOS> (enable) set security acl map HttpUdp_Acl ?
  <vlans>                    Vlan(s) to be mapped to ACL
6K-CatOS> (enable) set security acl map HttpUdp_Acl 11
Mapping in progress.

ACL HttpUdp_Acl successfully mapped to VLAN 11.
6K-CatOS> (enable)
```

6. Controleer de ACL op VLAN-afbeelding.

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. Configuratie van de vangst poort.

```
6K-CatOS> (enable) set vlan 11 3/24
VLAN  Mod/Ports
---- ----------------------
11    3/11,3/24
6K-CatOS> (enable)


6K-CatOS> (enable) set security acl capture-ports 3/24
Successfully set 3/24 to capture ACL traffic.
6K-CatOS> (enable)
```

Opmerking: Als een ACL aan meerdere VLAN's is gekoppeld, moet de opnamepoort op al die VLAN's zijn ingesteld. Om de opnamepoort te maken staat meerdere VLAN's toe, moet u de poort als boomstam configureren en alleen de VLAN's in kaart brengen naar ACL. Als ACL aan VLANs 11 en 12 in kaart wordt gebracht, dan moet u de configuratie voltooien.

```
6K-CatOS> (enable) clear trunk 3/24 1-10,13-1005,1025-4094
6K-CatOS> (enable) set trunk 3/24 on dot1q 11-12
6K-CatOS> (enable) set security acl capture-ports 3/24
```

8. Controleer de configuratie van de poort.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **Laat veiligheidsinformatie zien** - Toont de inhoud van VACL die momenteel ingesteld of laatst geëngageerd is aan NVRAM en hardware.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl
set security acl ip HttpUdp_Acl
---------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
6K-CatOS> (enable)
```

- **Toon kaart** van de **veiligheidscontrole**-Toont ACL-aan-VLAN of ACL-aan-poort mapping voor een specifieke ACL, poort of VLAN.

```
6K-CatOS> (enable) show security acl map all
ACL Name                         Type Vlans
-------------------------------- ---- -----
HttpUdp_Acl                         IP   11
6K-CatOS> (enable)
```

- **Beveiliging tonen** Opname**-poorten**—Hier wordt de lijst met opnamepoorten weergegeven.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- VACL-opname voor granulaire verkeersanalyse met Cisco Catalyst 6000/6500 actieve Cisco IOS-software
- Configuratie van toegangscontrole - Catalyst 6500 Series softwareconfiguratie Guide, 8.6
- Productondersteuningspagina's voor LAN
- Ondersteuningspagina voor LAN-switching
- Technische ondersteuning en documentatie – Cisco Systems