

# Captura de VACL para análise de tráfego granular com Cisco Catalyst 6000/6500 executando Cisco IOS Software

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Conventions](#)

[Informações de Apoio](#)

[SPAN Baseado em VLAN](#)

[VLAN ACL](#)

[Vantagens do uso de VACL sobre o uso de VSPAN](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração com SPAN baseado em VLAN](#)

[Configuração com VACL](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento apresenta um exemplo de configuração do uso do recurso de Porta de Captura de ACL de VLAN (VACL) para a análise de tráfego de rede de modo mais granular. Este documento também descreve a vantagem do uso da Porta de Captura de VACL em comparação com o SPAN baseado em VLAN (VSPAN).

Para configurar o recurso de Porta de Captura de VACL no Cisco Catalyst 6000/6500 executando o Cisco OS Software, consulte [Captura de VACL para Análise de Tráfego Granular com o Cisco Catalyst 6000/6500 Executando o CatOS Software](#).

## [Prerequisites](#)

## [Requirements](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Listas de acesso IP: consulte [Configurando Listas de Acesso IP](#) para obter mais informações.
- LAN Virtual: consulte [Virtual LANs/VLAN Trunking Protocol \(VLANs/VTP\) - Introdução](#) para obter mais informações.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware: Cisco Catalyst 6506 Series Switch com Cisco IOS<sup>®</sup> Software Release 12.2(18)SXF8.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Produtos Relacionados

Essa configuração pode ser usada também com Cisco Catalyst 6000 / 6500 Series Switches que executam o Cisco IOS Software Release 12.1(13)E ou posterior.

## Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

## Informações de Apoio

### SPAN Baseado em VLAN

O SPAN (Switched Port ANalyzer) copia o tráfego de uma ou mais portas de origem em qualquer VLAN ou de uma ou mais VLANs para uma porta de destino para fins de análise. O SPAN local suporta portas de origem, VLANs de origem e portas de destino no mesmo Switch Catalyst 6500 Series.

Uma VLAN de origem é uma VLAN monitorada para análise de tráfego de rede. O SPAN baseado em VLAN (VSPAN) usa uma VLAN como origem do SPAN. Todas as portas das VLANs de origem se tornam portas de origem. Uma porta de origem é uma porta monitorada para análise de tráfego de rede. As portas do tronco podem ser configuradas como portas de origem e misturadas a portas de origem não pertencentes ao tronco, mas o SPAN não copia o encapsulamento de uma porta de tronco de origem.

Para sessões de VSPAN com entrada e saída configuradas, dois pacotes são encaminhados da porta de destino se os pacotes são comutados na mesma VLAN (uma como tráfego de entrada da porta de entrada e outro como tráfego de saída da porta de saída).

O VSPAN monitora somente o tráfego que sai ou entra nas porta da camada 2 na VLAN.

- Se você configurar uma VLAN como origem de entrada e o tráfego for roteado para a VLAN monitorada, o tráfego roteado não será monitorado porque ele nunca é mostrado como tráfego de entrada em uma porta da camada 2 na VLAN.
- Se você configurar uma VLAN como origem de saída e o tráfego for roteado para a VLAN

monitorada, o tráfego roteado não será monitorado porque ele nunca é mostrado como tráfego de saída de uma porta da camada 2 na VLAN.

Consulte [Características da VLAN de Origem](#) para obter mais informações sobre VLANs de origem.

## VLAN ACL

As VACLs podem fornecer controle de acesso para todos os pacotes interligados em uma VLAN ou que são roteados para dentro ou fora de uma interface de VLAN ou WAN para a captura de VACL. Ao contrário das ACLs padrão ou estendidas normais do Cisco IOS que são configuradas somente em interfaces de roteador e aplicadas apenas a pacotes roteados, as VACLs são adequadas a todos os pacotes e podem ser aplicadas a qualquer interface de VLAN ou WAN. As VACLs são processadas no hardware. As VACLs usam as ACLs do Cisco IOS. As VACLs ignoram quaisquer campos da ACL do Cisco IOS sem suporte no hardware.

É possível configurar VACLs para tráfego IP, IPX e da camada MAC. As VACLs aplicadas a interfaces WAN oferecem suporte somente a tráfego IP para a captura de VACL.

Quando você configura uma VACL e a aplica a uma VLAN, todos os pacotes que entram na VLAN são verificados em relação a essa VACL. Se você aplicar uma VACL à VLAN e uma ACL a uma interface roteada na VLAN, um pacote recebido na VLAN será primeiro verificado em relação à VACL e, se permitido, verificado novamente em comparação com a ACL de entrada antes de ser manipulado pela interface roteada. Quando o pacote é roteado para outra VLAN, ele é primeiro verificado em relação à ACL de saída que é aplicada à interface roteada e, se permitido, a VACL configurada para a VLAN de destino é aplicada. Se uma VACL for configurada para um tipo de pacote e um pacote desse tipo não corresponder à VACL, a ação padrão será negar. Estas são as diretrizes para a opção de captura na VACL.

- A porta de captura não pode ser uma porta ATM.
- A porta de captura precisa estar no estado de encaminhamento de spanning tree para a VLAN.
- O switch não tem nenhuma restrição no número de portas de captura.
- A porta de captura captura somente pacotes permitidos pela ACL configurada.
- Capture as portas somente transmitem o tráfego que pertence à porta de captura VLAN. Configure a porta de captura como um tronco que transporta as VLANs necessárias para capturar o tráfego que vai para muitas VLANs.

**Cuidado:** uma combinação incorreta de ACLs pode interromper o fluxo de tráfego. Tenha muito cuidado ao configurar as ACLs em seu dispositivo.

**Observação:** a VACL não é suportada com IPv6 em um switch da série Catalyst 6000. Em outras palavras, o redirecionamento da ACL da VLAN e o IPv6 não são compatíveis, portanto, a ACL não pode ser usada para corresponder ao tráfego IPv6.

## Vantagens do uso de VACL sobre o uso de VSPAN

Há várias limitações do uso de VSPAN para análise de tráfego:

- Todo o tráfego da camada 2 transmitido em uma VLAN é capturado. Isso aumenta a quantidade de dados a serem analisados.
- O número de sessões de SPAN que podem ser configuradas nos Catalyst 6500 Series

Switches é limitado. Consulte [Limitações de Sessões de SPAN Local e RSPAN](#) para obter mais informações.

- Uma porta de destino recebe cópias do tráfego enviado e recebido para todas as portas de origem monitoradas. Se uma porta de destino receber um excesso de assinaturas, ela poderá ficar congestionada. Esse congestionamento poderá afetar o encaminhamento de tráfego em uma ou mais portas de origem.

O recurso Porta de Captura de VACL pode ajudar a superar algumas dessas limitações. O objetivo principal das VACLs não é monitorar tráfego, mas, com uma grande variedade de recursos de classificação de tráfego, o recurso de Porta de Captura foi introduzido para que a análise do tráfego de rede se torne muito mais simples. Estas são as vantagens do uso da Porta de Captura de VACL sobre VSPAN:

- Análise de tráfego granularAs VACLs podem corresponder com base no endereço IP origem, endereço IP destino, tipo de protocolo da Camada 4, portas da Camada 4 origem e destino e outras informações. Esse recurso torna as VACLs muito úteis para a identificação e filtragem de tráfego granular.
- Número de sessõesAs VACLs são aplicadas no hardware; o número de entradas de controle de acesso (ACE) que podem ser criadas depende do TCAM disponível nos switches.
- Excesso de assinatura da porta de destinoA identificação de tráfego granular reduz o número de quadros a serem encaminhados para a porta de destino e, assim, minimiza a probabilidade de sua sobreassinatura.
- DesempenhoAs VACLs são aplicadas no hardware; não há penalidade de desempenho para a aplicação de VACLs a uma VLAN nos switches Cisco Catalyst 6500 Series

## [Configurar](#)

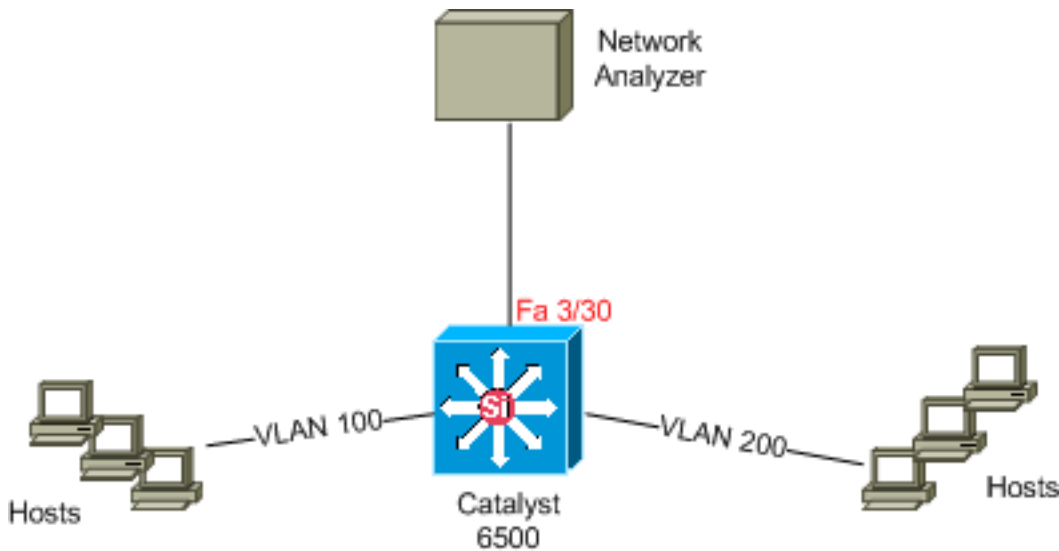
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

- [Configuração com SPAN Baseado em VLAN](#)
- [Configuração com VACL](#)

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

## [Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:



## Configuração com SPAN baseado em VLAN

Este exemplo de configuração relaciona as etapas obrigatórias para capturar todo o tráfego da camada 2 transmitido em VLAN 100 e VLAN 200 e enviá-lo para o dispositivo analisador de redes.

1. Especifique o tráfego interessante. Em nosso exemplo, trata-se do tráfego transmitido na VLAN 100 e na VLAN 200.

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
,      Specify another range of VLANs
-      Specify a range of VLANs
both  Monitor received and transmitted traffic
rx    Monitor received traffic only
tx    Monitor transmitted traffic only
<cr>

!--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. Especifique a porta de destino para o tráfego capturado.

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

Com isso, todo o tráfego da camada 2 que pertence à VLAN 100 e à VLAN 200 é copiado e enviado à porta Fa3/30. Se a porta de destino fizer parte da mesma VLAN cujo tráfego é monitorado, o tráfego que sai da porta de destino não será capturado.

Use o comando **show monitor** para verificar a configuração do SPAN.

```
Cat6K-IOS#show monitor detail
Session 50
-----
Type           : Local Session
Source Ports   :
  RX Only      : None
  TX Only      : None
  Both         : None
Source VLANs   :
  RX Only      : None
```

```
TX Only      : None
Both         : 100,200
Source RSPAN VLAN : None
Destination Ports : Fa3/30
Filter VLANs  : None
Dest RSPAN VLAN  : None
```

## Configuração com VACL

Neste exemplo de configuração, há vários requisitos do administrador de rede:

- O tráfego HTTP de uma faixa de hosts (10.20.20.128/25) na VLAN 200 para um servidor específico (10.10.10.101) na VLAN 100 precisa ser capturado.
- O tráfego de Multicast User Datagram Protocol (UDP) na direção de transmissão destinado ao endereço de grupo 239.0.0.100 precisa ser capturado da VLAN 100.

### 1. Defina o tráfego de interesse a ser capturado e enviado para análise.

```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```

### 2. Defina uma ACL guarda-chuva para mapear todos os demais tipos de tráfego.

```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```

### 3. Defina o mapa de acesso da VLAN.

```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```

### 4. Aplique o mapa de acesso à VLAN às VLANs apropriadas.

```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```

### 5. Configure a porta de captura.

```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
WORD      VLAN IDs of the allowed VLANs when this po
add       add VLANs to the current list
all       all VLANs
except    all VLANs except the following
remove    remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(somente clientes registrados\) \(OIT\)](#) oferece suporte a determinados [comandos show](#). Use a OIT para exibir uma análise da saída do comando show.

- **show vlan access-map** — Exibe o conteúdo dos mapas de acesso da VLAN.

```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP" 10
    match: ip address HTTP_UDP_TRAFFIC
    action: forward capture
Vlan access-map "HTTP_UDP_MAP" 20
    match: ip address ALL_TRAFFIC
    action: forward
```

- **show vlan filter** — Exibe informações sobre os filtros da VLAN.

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
    Configured on VLANs: 100
    Active on VLANs: 100
```

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [Captura de VACL para análise de tráfego granular com Cisco Catalyst 6000/6500 executando CatOS Software](#)
- [Suporte aos switches Cisco Catalyst 6500 Series](#)
- [Suporte a Produtos de LAN](#)
- [Suporte de tecnologia de switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)