

VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running Cisco IOS Software

Document ID: 89962

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

- VLAN based SPAN
- VLAN ACL
- Advantages of VACL Usage over VSPAN Usage

Configure

- Network Diagram
- Configuration with VLAN-based SPAN
- Configuration with VACL

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for the use of the VLAN ACL (VACL) Capture Port feature for network traffic analysis in a more granular manner. This document also states the advantage of VACL capture-port usage as opposed to VLAN-based SPAN (VSPAN) usage.

In order to configure the VACL capture-port feature on Cisco Catalyst 6000/6500 that runs Catalyst OS software, refer to VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running CatOS Software.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- IP Access Lists: refer to Configuring IP Access Lists for more information.
- Virtual LAN: refer to Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) – Introduction for more information.

Components Used

The information in this document is based on these software and hardware versions: Cisco Catalyst 6506 Series Switch that runs Cisco IOS[®] 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.

Related Products

This configuration can also be used with Cisco Catalyst 6000 / 6500 Series Switches that run Cisco IOS Software Release 12.1(13)E and later.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

VLAN based SPAN

SPAN (Switched Port ANalyzer) copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis. Local SPAN supports source ports, source VLANs, and destination ports on the same Catalyst 6500 Series Switch.

A source VLAN is a VLAN monitored for network traffic analysis. VLAN-based SPAN (VSPAN) uses a VLAN as the SPAN source. All the ports in the source VLANs become source ports. A source port is a port monitored for network traffic analysis. Trunk ports can be configured as source ports and mixed with nontrunk source ports, but SPAN does not copy the encapsulation from a source trunk port.

For VSPAN sessions with both ingress and egress configured, two packets are forwarded from the destination port if the packets get switched on the same VLAN (one as ingress traffic from the ingress port and one as egress traffic from the egress port).

VSPAN only monitors traffic that leaves or enters Layer 2 ports in the VLAN.

- If you configure a VLAN as an ingress source and traffic gets routed into the monitored VLAN, the routed traffic is not monitored because it never appears as ingress traffic that enters a Layer 2 port in the VLAN.
- If you configure a VLAN as an egress source and traffic gets routed out of the monitored VLAN, the routed traffic is not monitored because it never appears as egress traffic that leaves a Layer 2 port in the VLAN.

For more information on source VLANs, refer to Characteristics of Source VLAN.

VLAN ACL

VACLs can provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN or a WAN interface for VACL capture. Unlike regular Cisco IOS standard or extended ACLs that are configured on router interfaces only and are applied on routed packets only, VACLs apply to all packets and can be applied to any VLAN or WAN interface. VACLs are processed in hardware. VACLs use Cisco IOS ACLs. VACLs ignore any Cisco IOS ACL fields that are not supported in hardware.

You can configure VACLs for IP, IPX, and MAC-Layer traffic. VACLs applied to WAN interfaces support only IP traffic for VACL capture.

When you configure a VACL and apply it to a VLAN, all packets that enter the VLAN are checked against this VACL. If you apply a VACL to the VLAN and an ACL to a routed interface in the VLAN, a packet that comes into the VLAN is first checked against the VACL and, if permitted, is then checked against the input ACL before it is handled by the routed interface. When the packet is routed to another VLAN, it is first checked against the output ACL that is applied to the routed interface, and, if permitted, the VACL configured for the destination VLAN is applied. If a VACL is configured for a packet type and a packet of that type does not match the VACL, the default action is deny. These are the guidelines for the capture option in VACL.

- The capture port cannot be an ATM port.
- The capture port needs to be in the spanning-tree forwarding state for the VLAN.
- The switch has no restriction on the number of capture ports.
- The capture port captures only packets permitted by the configured ACL.
- Capture ports only transmit traffic that belongs to the capture port VLAN. Configure the capture port as a trunk that carries the required VLANs in order to capture traffic that goes to many VLANs.



Caution: Incorrect combination of ACLs can disrupt the traffic flow. Exercise extra caution while you configure the ACLs in your device.

Note: VACL is not supported with IPv6 on a Catalyst 6000 series switch. In other words, VLAN ACL redirect and IPv6 are not compatible so ACL cannot be used to match IPv6 traffic.

Advantages of VACL Usage over VSPAN Usage

There are several limitations of VSPAN usage for traffic analysis:

- All layer 2 traffic that flows in a VLAN is captured. This increases the amount of data to be analyzed.
- The number of SPAN sessions that can be configured on the Catalyst 6500 Series Switches is limited. Refer to Local SPAN and RSPAN Session Limits for more information.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it can become congested. This congestion can affect traffic forwarding on one or more of the source ports.

The VACL Capture Port feature can help to overcome some of these limitations. VACLs are primarily not designed to monitor traffic, but, with a wide range of capability to classify the traffic, the Capture Port feature was introduced so that network traffic analysis can become much simpler. These are the advantages of VACL Capture Port usage over VSPAN:

- Granular Traffic Analysis

VACLs can match based on source IP address, destination IP address, Layer 4 protocol type, source and destination Layer 4 ports, and other information. This capability makes VACLs very useful for granular traffic identification and filtering.

- Number of Sessions

VACLs are enforced in hardware; the number of Access Control Entries (ACE) that can be created depends upon the TCAM available in the switches.

- Destination Port Oversubscription

Granular traffic identification reduces the number of frames to be forwarded to the destination port and thereby minimizes the probability of their oversubscription.

- Performance

VACLs are enforced in hardware; there is no performance penalty for the application of VACLs to a VLAN on the Cisco Catalyst 6500 Series Switches

Configure

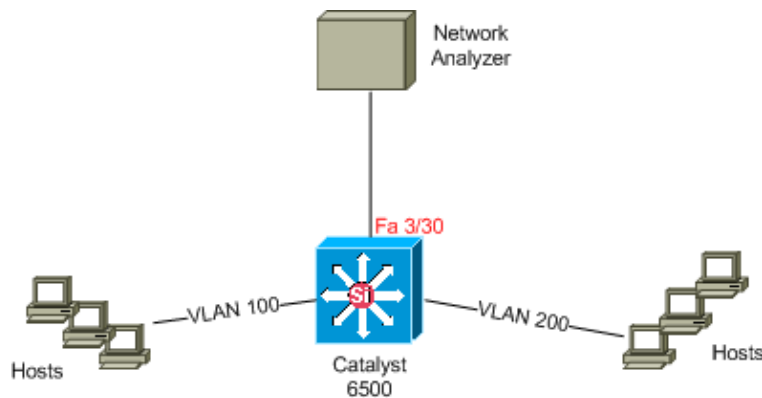
In this section, you are presented with the information to configure the features described in this document.

- Configuring with VLAN based SPAN
- Configuring with VACL

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configuration with VLAN-based SPAN

This configuration example lists the steps required to capture all Layer 2 traffic that flows in VLAN 100 and VLAN 200 and send them to the Network Analyzer device.

1. Specify the interesting traffic. In our example, it is traffic that flows in VLAN 100 and 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. Specify the destination port for the captured traffic.

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

```
Cat6K-IOS(config)#
```

With this, all the layer 2 traffic that belongs to VLAN 100 and VLAN 200 is copied and sent to port Fa3/30. If the destination port is part of the same VLAN whose traffic is monitored, the traffic that goes out of the destination port is not captured.

Verify your SPAN configuration with the **show monitor** command.

```
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
```

Configuration with VACL

In this configuration example, there are multiple requirements from the network administrator:

- HTTP Traffic from a range of hosts (10.20.20.128/25) in VLAN 200 to a specific server (10.10.10.101) in VLAN 100 needs to be captured.
- Multicast User Datagram Protocol (UDP) traffic in the transmit direction destined for group address 239.0.0.100 needs to be captured from VLAN 100.

1. Define the interesting traffic to be captured and sent to analysis.

```
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 v
```

```
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
```

```
Cat6K-IOS(config-ext-nacl)#exit
```

2. Define an umbrella ACL to map all other traffic.

```
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. Define the VLAN access map.

```
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. Apply the VLAN access map to the appropriate VLANs.

```
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 the Capture Port.

```
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
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show vlan access-map** Displays the contents of the VLAN Access Maps.

```
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** Displays information about the VLAN Filters.

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

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running CatOS Software](#)
 - [Cisco Catalyst 6500 Series Switches Support](#)
 - [LAN Product Support](#)
 - [LAN Switching Technology Support](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 22, 2007

Document ID: 89962
