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

Document ID: 97411

Contents

Introduction

This document provides a sample configuration for the use of the VLAN Access Control List (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 Switched Port Analyzer (SPAN) (VSPAN) usage.

In order to configure the VACL Capture Port feature on Cisco Catalyst 6000/6500 that runs Cisco IOS® software, refer to VACL Capture for Granular Traffic Analysis with Cisco Catalyst 6000/6500 Running Cisco IOS Software.

Prerequisites

Requirements

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

- Virtual LAN Refer to Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) − Introduction for more information.
- Access Lists Refer to Configuring Access Control for more information.

Components Used

The information in this document is based on the Cisco Catalyst 6506 Series Switch that runs Catalyst OS release 8.1(2).

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 Catalyst OS release 6.3 and later.

Conventions

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

Background Information

VLAN–based SPAN

SPAN 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 port is a port monitored for network traffic analysis. A source VLAN is a VLAN monitored for network traffic analysis. VLAN–based SPAN (VSPAN) is analysis of the network traffic in one or more VLANs. You can configure VSPAN as ingress SPAN, egress SPAN, or both. All the ports in the source VLANs become the operational source ports for the VSPAN session. The destination ports, if they belong to any of the administrative source VLANs, are excluded from the operational source. If you add or remove the ports from the administrative source VLANs, the operational sources are modified accordingly.

Guidelines for VSPAN sessions:

- The trunk ports are included as the source ports for the VSPAN sessions, but only the VLANs that are in the Admin source list are monitored if these VLANs are active for the trunk.
- For the VSPAN sessions with both ingress and egress SPAN configured, the system operates based on the type of supervisor engine that you have:

    ♦ 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 Two packets are forwarded by the SPAN destination port if the packets get switched on the same VLAN.
    ♦ WS–X6K–SUP1–2GE, WS–X6K–SUP1A–2GE Only one packet is forwarded by the SPAN destination port.
- An inband port is not included as Operational source for the VSPAN sessions.
- When a VLAN is cleared, it is removed from the source list for the VSPAN sessions.
- A VSPAN session is disabled if the Admin source VLANs list is empty.
- The inactive VLANs are not allowed for the VSPAN configuration.
- A VSPAN session is made inactive if any of the source VLANs become the RSPAN VLANs.

Refer to Characteristics of Source VLAN for more information on source VLANs.

VLAN ACL

The VACLs can access control all traffic. You can configure the VACLs on the switch to apply to all packets

that are routed into or out of a VLAN or are bridged within a VLAN. The VACLs are strictly for security packet filtering and redirecting traffic to specific physical switch ports. Unlike the Cisco IOS ACLs, the VACLs are not defined by direction (input or output).

You can configure the VACLs on the Layer 3 addresses for IP and IPX. All other protocols are access controlled through the MAC addresses and EtherType using the MAC VACLs. The IP traffic and IPX traffic are not access controlled by the MAC VACLs. All other traffic types (AppleTalk, DECnet, and so on) are classified as MAC traffic. The MAC VACLs are used to access control this traffic.

ACEs Supported in VACLs

VACL contains an ordered list of access control entries (ACEs). Each VACL can contain ACEs of only one type. Each ACE contains a number of fields that are matched against the contents of a packet. Each field can have an associated bit mask to indicate which bits are relevant. An action is associated with each ACE that describes what the system should do with the packet when a match occurs. The action is feature dependent. Catalyst 6500 Series Switches support three types of ACEs in the hardware:

- IP ACEs
- IPX ACEs
- Ethernet ACEs

This table lists the parameters that are associated with each ACE type:

ACE Type	TCP or UDP	ICMP	Other IP	IPX	Ethernet
Layer 4 Parameters	Source Port	—	—	—	—
	Source Port Operator			—	
	Destination Port	—	—	—	—
	Destination Port Operator	ICMP Code	—	—	—
	N/A	ICMP Type	N/A	—	—
Layer 3 Parameters	IP ToS Byte	IP ToS Byte	IP ToS Byte	—	—
	IP Source Address	IP Source Address	IP Source Address	IPX Source Network	—
	IP Destination Address	IP Destination Address	IP Destination Address	IP Destination Network Node	—
	—	Address —	Address —	Network Destination Node	—
	TCP or UDP	ICMP	Other Protocol	IPX Packet Type	—
	—	—	—	—	EtherType
Layer 2 Parameters	—	—	—	—	Ethernet Source

				Address
–	–	–	–	Ethernet Destination Address

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 Feature Summary and Limitations 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. However, 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 ACEs 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.
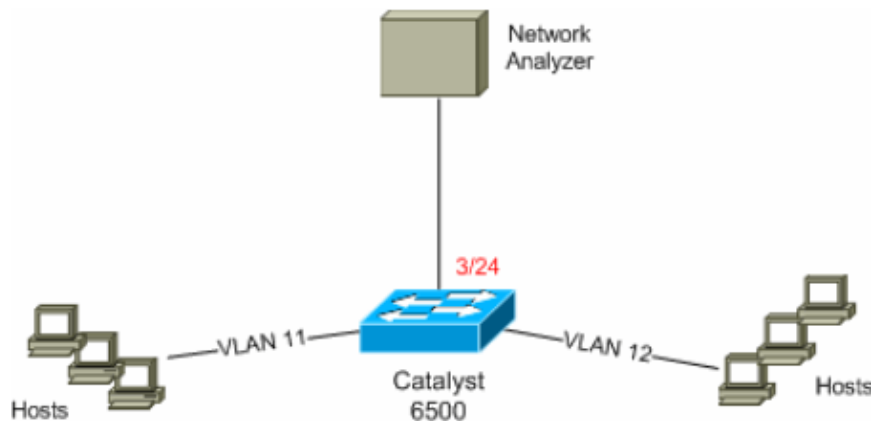
This document uses these configurations:

- Configuration with VLAN−based SPAN
- Configuration with VACL

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

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 11 and VLAN 12 and send them to the Network Analyzer device.

1. Specify the interesting traffic.

   In this example, it is traffic that flows in VLAN 100 and VLAN 200.

   ```
   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
   ```

   With this, all the Layer 2 traffic that belongs to VLAN 11 and VLAN 12 are copied and sent to port 3/24.

2. Verify your SPAN configuration with the **show span all** command.

   ```
   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)
```

Configuration with VACL

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

- HTTP traffic from a range of hosts (10.12.12.128/25) in VLAN 12 to a specific server (10.11.11.100) in VLAN 11 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 11.

1. Define the interesting traffic using the Security ACLs. Remember to mention the keyword **capture** for all the ACEs defined.

   ```
   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. Verify if the ACE configuration is correct and in proper order.

   ```
   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. Commit the ACL to the hardware.

   ```
   6K-CatOS> (enable) commit security acl HttpUdp_Acl

   ACL commit in progress.

   ACL 'HttpUdp_Acl' successfully committed.
   6K-CatOS> (enable)
   ```
4. Verify the status of the 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. Apply the VLAN access map to the appropriate VLANs.

```
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. Verify the ACL to VLAN mapping.

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl

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

7. Configure the capture port.

```
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)
```

Note: If an ACL is mapped to multiple VLANs, then the capture port must be configured to all those
VLANs. In order to make the capture port allow multiple VLANs, configure the port as trunk and
allow only the VLANs mapped to the ACL. For example, if the ACL is mapped to VLANs 11 and 12,
then complete the configuration.

```
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. Verify the capture port configuration.

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

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 security acl info** Displays the contents of the VACL that are currently configured or last
  committed to NVRAM and 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)
```

- **show security acl map** Displays the ACL–to–VLAN or ACL–to–port mapping for a specific ACL, port, or VLAN.

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

- **show security acl capture–ports** Displays the list of capture ports.

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

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 Cisco IOS Software**
- **Configuring Access Control – Catalyst 6500 Series Software Configuration Guide, 8.6**
- **LAN Product Support Pages**
- **LAN Switching Support Page**
- **Technical Support & Documentation – Cisco Systems**