Traffic Capturing for Granular Traffic Analysis

This chapter describes how to significantly increase the granularity of network traffic analysis by combining two key features of the Cisco Catalyst 6500 Series switches: Remote Switched Port Analyzer (RSPAN) and the redirect feature of VLAN access control lists (VACLs). RSPAN and VACLs can be combined for increased granularity in analyzing traffic.

Using RSPAN combined with VACL redirect differs from the use of both the Catalyst 6500 SPAN and the Catalyst 6500 VACL capture.

Note This document is based on Cisco IOS software, but most of the concepts are equally applicable to Cisco Catalyst IOS.

This chapter includes the following sections:

Traffic Capture Requirements

When configuring traffic capture for the purposes of intrusion detection analysis, anomaly detection, or simply for traffic analysis with one or more sniffers, the normal requirements are the following:

- Monitoring a set of ports or VLANs without affecting the forwarding performance of the Layer 3 switch—You can do this by using features implemented in hardware such as SPAN or VACL capture.
- Monitoring switched and routed frames—When traffic is routed from one VLAN to another, the copied traffic can be tagged with either VLAN, so you must design traffic capturing so that the monitoring port can forward either frame.
- Avoiding the generation of duplicate frames—Depending on the reference for the SPAN or capture (port or VLAN incoming or outgoing direction), there are situations in which the switch can generate multiple copies of the same frame, which is undesirable and can be addressed with proper design.

- Filtering out uninteresting packets from the copied traffic—To optimize the performance of the devices that are monitoring the traffic, it is best to drop copies of the frames that are not interesting in hardware. For example, you can combine multiple hardware features to ensure that a sensor or a sniffer sees only HTTP traffic.
- Support for several sessions—Sessions can be conceived as funnels receiving copies of traffic from multiple ports to one or multiple sensor ports. For example, traffic from port A, B, and C copied to port D is one session, and traffic from port E, F, and G copied to port H is another session. You do not want all traffic from A, B, C, E, F, and G to go out to both port D and H, because this is equivalent to having a single session.

Using VACLs

VACLs are a security enforcement tool based on Layer 2, Layer 3, and Layer 4 information. A VACL lookup against a packet can result in a permit, a deny, a permit and capture, or a redirect. When you associate a VACL with a particular VLAN, all traffic must be permitted by the VACL before the traffic is allowed into the VLAN. VACLs are enforced in hardware, so there is no performance penalty for applying VACLs to a VLAN on the Cisco Catalyst 6500 Series switches.

Note In this chapter, the terminology VACL and VLAN access map are used interchangeably.

This section includes the following topics:

VACL Command Syntax

VACLs can be used with the following types of traffic:

- IP
- IPX
- MAC

IP

IP VACLs match IP traffic, using the following syntax:

```
router(config)# ip access-list extended name
router(config-ext-nacl)# {deny | permit} protocol {source-source-wildcard | any}
{destination- destination-wildcard | any} [precedence precedence] [tos tos] [established]
[log | log-input] [time-range time-range-name] [fragments]
```

The protocol field can take the following values:

```
router(config-ext-nacl)#permit ?
  <0-255>  An IP protocol number
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
```

```
  igmp     Internet Gateway Message Protocol
  igrp     Cisco's IGRP routing protocol
  ip       Any Internet Protocol
  ipinip   IP in IP tunneling
  nos      KA9Q NOS compatible IP over IP tunneling
  ospf     OSPF routing protocol
  pcp      Payload Compression Protocol
  pim      Protocol Independent Multicast
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```

For TCP/UDP traffic, you can match Layer 4 ports:

```
router(config-ext-nacl)# {deny | permit} {tcp | udp} {source-source-wildcard | any}
[operator port] {destination-destination-wildcard | any} [operator port] [established]
[precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]
[fragments]
```

IPX

IPX VACLs match IPX traffic using the following syntax:

```
router(config)#ipx access-list extended name
router(config-ipx-ext-nacl)# {deny | permit} protocol [source-network][[[.source-node]
source-node-mask] | [.source-node source-network-mask.source-node-mask]] [source-socket]
[destination.network][[[.destination-node] destination-node-mask] | [.destination-node
destination-network-mask.destination-node-mask]] [destination-socket] [log] [time-range
time-range-name]
```

MAC

MAC VACLs match non-IP, non-IPX traffic using the following syntax:

```
router(config)#mac access-list extended name
router(config-ext-macl)# {permit | deny} {src-mac-mask | any} {dest-mac-mask | any}
[ethertype]
```

The Ethertype field can take the following values:

```
router(config-ext-macl)#permit any any ?
  aarp          EtherType: AppleTalk ARP
  amber         EtherType: DEC-Amber
  appletalk     EtherType: AppleTalk/EtherTalk
  dec-spanning  EtherType: DEC-Spanning-Tree
  decnet-iv     EtherType: DECnet Phase IV
  diagnostic    EtherType: DEC-Diagnostic
  dsm           EtherType: DEC-DSM
  etype-6000    EtherType: 0x6000
  etype-8042    EtherType: 0x8042
  lat           EtherType: DEC-LAT
  lavc-sca      EtherType: DEC-LAVC-SCA
  mop-console   EtherType: DEC-MOP Remote Console
  mop-dump      EtherType: DEC-MOP Dump
  msdos         EtherType: DEC-MSDOS
  mumps         EtherType: DEC-MUMPS
  netbios       EtherType: DEC-NETBIOS
  vines-echo    EtherType: VINES Echo
  vines-ip      EtherType: VINES IP
  xns-idp       EtherType: XNS IDP
```

VACL Capture

The VACL capture feature allows you to mirror traffic to ports configured to forward captured traffic. The capture action sets the capture bit for the forwarded packets so that ports with the capture function enabled can receive the packets. Only forwarded packets can be captured.

CatOS Configuration Examples

The following commands create a security ACL to capture all traffic on VLAN 10 and send the traffic to port 3/5.

```
catOS6500 (enable) set security acl ip CATCHALL permit ip any any capture
catOS6500 (enable) commit security acl CATCHALL
catOS6500 (enable) set security acl map CATCHALL 10
catOS6500 (enable) set security acl capture-ports 8/25
```

To remove the VACL capture, use the **clear security acl CATCHALL** command. To commit the changes, use the **commit security acl CATCHALL** command.

Cisco IOS Configuration Examples

The following commands create a security ACL to capture all traffic on VLAN 10:

```
ip access-list extended IP-catch-all
 permit ip any any
!
vlan access-map CATCHALL 10
 match ip address IP-catch-all
 action forward capture
!
vlan filter CATCHALL vlan-list 10
!
interface FastEthernet8/25
 switchport
 switchport capture
 switchport capture allowed vlan 10
 no shut
!
```

Capturing Locally Switched Traffic

The following configuration demonstrates how VACL capture works. You first define the *interesting traffic* that you want to monitor; for example, HTTP traffic (as defined in the ACL HTTPTRAFFIC). Then you define a VACL (or VLAN access map, which in this example is also called HTTPTRAFFIC).

The VACL provides two functions. It filters the traffic on the VLAN to which you assign it, and it provides a copy of the traffic to the sensing interface (**action forward capture**) for the entries configured to forward and capture; in this example, it is **vlan access-map HTTPTRAFFIC 10**).

In this example, the VACL HTTPTRAFFIC is assigned to VLAN 10 (**vlan filter HTTPTRAFFIC vlan-list 10**).

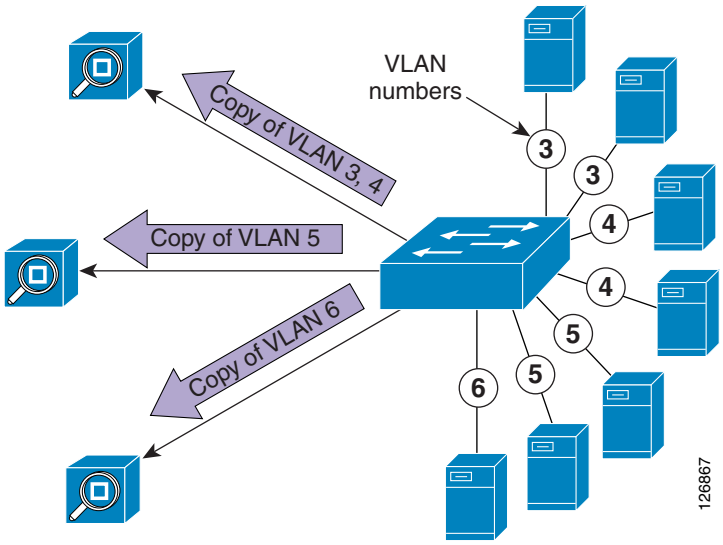
```
ip access-list extended HTTPTRAFFIC
 permit tcp any any eq www
 permit tcp any eq www any
!
ip access-list extended IP-catch-all
 permit ip any any
```

```
!
vlan access-map HTTPTRAFFIC 10
 match ip address HTTPTRAFFIC
 action forward capture
vlan access-map HTTPTRAFFIC 20
 match ip address IP-catch-all
 action forward
!
vlan filter HTTPTRAFFIC vlan-list 10
!
interface FastEthernet8/25
 switchport
 switchport capture
 switchport capture allowed vlan 10
 no shut
!
```

Captured traffic is sent out on port FastEthernet8/25 as indicated by the configuration (**switchport capture allowed vlan 10**).

Using VACL capture for mirroring traffic provides very good scalability for mirroring locally-switched traffic, as shown in Figure 7-1.

Figure 7-1 Using VACL Capture to Mirror Locally Switched Traffic



In this topology, the switch is configured on four VLANs. The traffic from these VLANs is mirrored to three monitoring devices because VACLs are configured on each of the VLANs with entries whose action is “capture” and “forward”.

For sensor 1 to receive traffic from VLAN 3 and 4, the port that connects to sensor 1 must be a trunk forwarding VLAN 3 and 4. Sensor 2 is configured to receive traffic from VLAN 5 and sensor 3 is configured to receive traffic from VLAN 6.

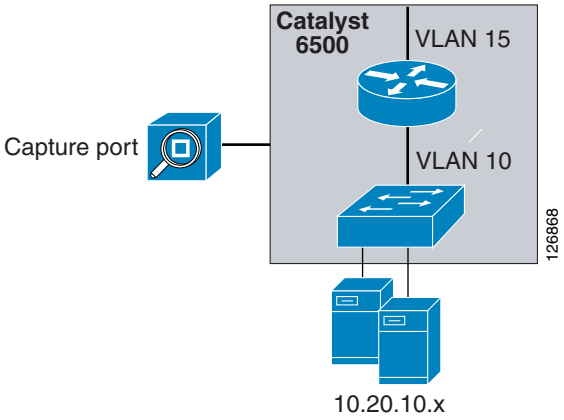
The advantage of VACL capture is that you can assign traffic from each VLAN to a different sensor, which provides granularity to the VLAN level.

Capturing Routed Traffic

For routed traffic, capture ports transmit packets only after they are Layer 3 switched; packets are transmitted out of a port only if the output VLAN of the Layer 3 switched flow is the same as the capture port VLAN.

For example, assume that you have flows from VLAN 10 to VLAN 15, as shown in Figure 7-2.

Figure 7-2 Using VACL Capture to Mirror Routed Traffic



You add a VACL on one of the VLANs permitting these flows, and you specify a capture port. This traffic gets transmitted out of the capture port only if it belongs to VLAN 15 or if the port is a trunk carrying VLAN 15. If the capture port is in VLAN 10, it does not transmit any traffic. Whether a capture port transmits the traffic or not is independent of the VLAN on which you placed the VACL. If you want to capture traffic from one VLAN going to many VLANs, the capture port has to be a trunk carrying all output VLANs.

So in the example of Figure 7-2, for the capture port to show both client-to-server and server-to-client traffic, you need to make sure that the port is forwarding both VLAN 10 and 15.

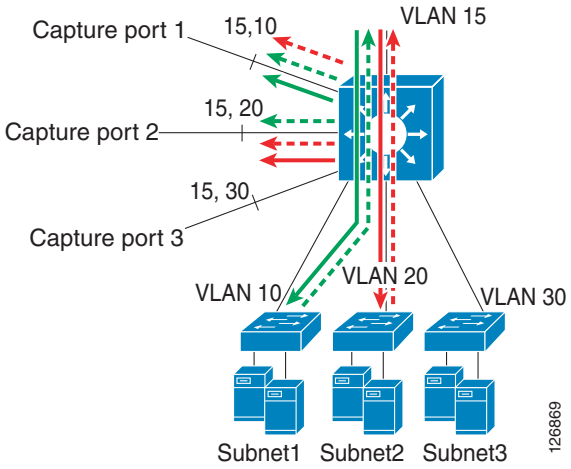
The corrected configuration appears as follows:

```
ip access-list extended HTTPTRAFFIC
 permit tcp any any eq www
 permit tcp any eq www any
!
ip access-list extended IP-catch-all
 permit ip any any
!
vlan access-map HTTPTRAFFIC 10
 match ip address HTTPTRAFFIC
 action forward capture
vlan access-map HTTPTRAFFIC 20
 match ip address IP-catch-all
 action forward
!
vlan filter HTTPTRAFFIC vlan-list 10
!
interface FastEthernet8/25
 switchport
 switchport capture
 switchport capture allowed vlan 10, 15
 no shut
!
```

Now assume that you have multiple capture ports configured on a switch and you want to send traffic exchanged on VLAN 10 to one sensor or sniffer, traffic exchanged on VLAN 20 to a second sensor or sniffer, and traffic exchanged on VLAN 30 to a third sensor or sniffer.

Figure 7-3 shows the traffic distribution when a VACL is applied to VLAN 10, 20, and 30.

Figure 7-3 Using VACL Capture to Mirror Routed Traffic on Multiple Subnets



Capture port 1 is to monitor traffic routed between VLAN 15 and VLAN 10, so it is configured to forward VLAN 10 and 15. Capture port 2 is to monitor traffic routed between VLAN 15 and VLAN 20, so it is configured to forward VLAN 15 and 20. Capture port 3 is to monitor traffic routed between VLAN 15 and VLAN 30, so it forwards VLAN 15 and 30.

```
ip access-list extended HTTPTRAFFIC
 permit tcp any any eq www
 permit tcp any eq www any
!
ip access-list extended IP-catch-all
 permit ip any any
!
vlan access-map HTTPTRAFFIC 10
 match ip address HTTPTRAFFIC
 action forward capture
vlan access-map HTTPTRAFFIC 20
 match ip address IP-catch-all
 action forward
!
vlan filter HTTPTRAFFIC vlan-list 10, 20, 30
!
interface FastEthernet8/25
 switchport
 switchport capture
 switchport capture allowed vlan 10, 15
 no shut
!
interface FastEthernet8/26
 switchport
 switchport capture
 switchport capture allowed vlan 20, 15
 no shut
!
interface FastEthernet8/27
```

```
 switchport
 switchport capture
 switchport capture allowed vlan 30, 15
 no shut
!
```

With this configuration, some traffic from VLAN 10 also goes to capture ports 2 and 3 and some traffic from VLAN 20 also goes to capture ports 1 and 3, because all the capture ports trunk VLAN 15 to forward captured traffic routed to VLAN 15.

VACL Capture Granularity

The previous section describes how to monitor routed traffic with VACL capture, and also shows that with the VACL capture, differentiating traffic on multiple ports for routed traffic can generate some spurious traffic.

Another drawback of VACL capture is that it does not allow you to send one type of traffic, such as HTTP, to one sensor and another type of traffic, such as DNS, to another sensor. With VACL capture, you can configure a VACL that matches HTTP frames and sets the capture bit on them. Capture port 1 is then set as a "switchport capture" port and sends a replica frame. The problem is that there exists only a single capture bit. So if you create another VACL to match the SMTP traffic and you set the capture bit for SMTP frames, capture port 1 picks up both HTTP and SMTP frames.

All these restrictions can be addressed by using the technique of RSPAN with VACLs described in this guide.

Using SPAN

This section describes the use of SPAN, and includes the following topics:

- SPAN Fundamentals
- Designing with SPAN

SPAN Fundamentals

SPAN copies packets from multiple sources, VLANs (VSPAN) or ports (PSPAN), to a single destination port. SPAN captures all traffic from the designated sources and identifies it as received (Rx), transmitted (Tx), or Both. Ingress traffic is the traffic entering the switch (Rx), and egress traffic is the traffic leaving the switch (Tx). A source SPAN port is considered to be a port that is monitored using the SPAN feature, and a destination SPAN port is considered to be a port where the sniffer or a sensor device is connected.

CatOS Configuration Examples

The following command creates a SPAN session with a source port of 2/2 and a destination port of 3/5, and filters VLANs 10 and 20 from the source:

```
catOS6500 (enable) set span 2/2 3/5 filter 10, 20
```

The following command creates a SPAN session with a source VLAN of 10 and a destination port of 3/5:

```
catOS6500 (enable) set span 10 3/5
```

The following command creates a SPAN session with a source VLAN of 10 and a destination port of 3/5 with learning disabled:

```
catOS6500 (enable) set span 10 3/5 inpkts enable learning disable
```

To disable the SPAN command session, enter the following command:

```
set span disable source port
```

Cisco IOS Configuration Examples

The following commands create a SPAN session with a source port of 2/2 and a destination port of 3/5, and filter VLAN 10 from the source:

```
catIOS(config)# monitor session 1 source interface GigabitEthernet 2/2
catIOS(config)# monitor session 1 filter vlan 10
catIOS(config)# monitor session 1 destination interface GigabitEthernet 3/5
```

The following commands create a SPAN session with a source VLAN of 10 and a destination port of 3/5:

```
catIOS(config)# monitor session 1 source vlan 10 both
catIOS(config)# monitor session 1 destination interface GigabitEthernet 3/5
```

To disable the SPAN session, enter the following command:

```
no monitor session id
```

RSPAN

Unlike SPAN, which allows you to mirror traffic from one or more ports on a Cisco Catalyst switch (the SPAN source) only to another port on the same switch (the SPAN destination), RSPAN allows you to capture traffic on one switch, mirror it to a designated VLAN, and forward it to one or more ports on one or more other switches for analysis.

The following is an example of how to configure RSPAN source VLANs:

```
monitor session 1 source vlan 5 , 10 , 20 rx
monitor session 1 destination remote vlan 300
```

This RSPAN source session mirrors traffic from VLAN 5, 10, and 20 onto the RSPAN VLAN 300.

The following is an example of how to configure RSPAN destination ports:

```
monitor session 2 destination interface Fa8/1 - 40
monitor session 2 source remote vlan 300
```

This RSPAN destination session collects traffic from RSPAN VLAN 300 and forwards it to the interfaces Fa8/1–40. A single destination session can forward traffic to a maximum of 64 different ports with Cisco IOS.

Note When using RSPAN, mirrored traffic loses the VLAN tag.

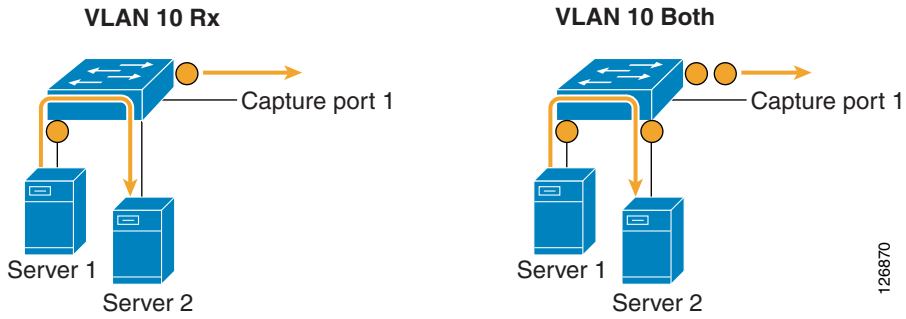
Designing with SPAN

This section discusses design considerations when using SPAN.

Avoid Generating Duplicate Frames

A key requirement of the design with SPAN is to avoid duplicates, as shown in Figure 7-4.

Figure 7-4 VSPAN Rx versus Both



Suppose the switch has been configured for VSPAN on VLAN 10 in the Rx direction. When Server 1 talks to Server 2, the frame (represented by the circle) enters the switch (Rx), so the switch generates a copy of the traffic and sends it out to the capture port.

```
monitor session 1 source vlan 10 rx
monitor session 1 destination interface Fa8/25
```

If the same switch is configured for VSPAN Both, the switch generates a copy when the traffic enters (Rx) and when the traffic exits the switch going to Server 2. Thus, the capture port sees the same frame twice, which is undesirable.

Cisco recommends using SPAN in the Tx or in the Rx direction to avoid generating duplicate frames.

SPAN Sessions

A SPAN session is defined as the aggregation of a number of sources (from where the traffic is captured) and a number of destination ports (to where the traffic is copied). Traffic is not differentiated within a session, as for example in the following configuration:

```
monitor session 2 source vlan 300
monitor session 2 destination interface Fa8/25 , Fa8/26
```

This is a single session with two destination ports: Fa8/25 and Fa8/26. Both ports Fa8/25 and Fa8/26 receive all frames copied from VLAN 300. Both ports receive the exact same frames. This configuration consumes one hardware resource; that is, one session.

Note Some documentation uses the terminology “sessions” to indicate the number of “destination ports”.

The number of available SPAN sessions varies according to the switch hardware platform, the supervisor, and the OS (Cisco IOS or Catalyst IOS). In the case of the Catalyst 6500, the number of supported SPAN session is as follows:

- Catalyst 6500 sup2 – CatOS—Two Rx sessions, two Both sessions, or four Tx sessions; one RSPAN session, and 24 RSPAN destination ports
- Catalyst 6500 sup2 – Cisco IOS—Two sessions or one RSPAN session, and 64 RSPAN destination ports

- Catalyst 6500 sup720 – CatOS—Two Rx sessions, two Both sessions, four Tx sessions, or two RSPAN sessions; and 24 RSPAN destination ports
- Catalyst 6500 sup720 – Cisco IOS—Two sessions or two RSPAN sessions, and 64 RSPAN destination ports

VSPAN and PSPAN

VLAN-based SPAN (VSPAN) indicates a SPAN session used to monitor all the ports belonging to a particular VLAN in a single command. The following is an example of a VSPAN session:

```
monitor session 1 source vlan 13 , 14 , 10 , 20 , 30 , 40 tx
```

Port-based SPAN (PSPAN) indicates a SPAN session used to monitor one or several ports on the switch:

```
monitor session 1 source int ten1/1, ten1/2, giga8/1, giga8/2, giga8/3, giga8/4 rx
```

It is not possible to mix PSPAN and VSPAN by specifying ports and VLANs within the same **monitor** command:

```
agg (config)# monitor session 1 source vlan 13, 14, 10, 20, 30, 40 tx
agg (config)# monitor session 1 source int Te7/1 rx
% Cannot add interfaces as sources for SPAN session 1
```

It is possible instead to run two sessions; one VSPAN and one PSPAN, and to use the same RSPAN destination, as follows:

```
monitor session 1 source vlan 13, 14, 10, 20, 30, 40 tx
monitor session 1 destination remote vlan 300
monitor session 2 source int ten1/1, ten1/2, giga8/1, giga8/2, giga8/3, giga8/4 rx
monitor session 2 destination remote vlan 300
monitor session 3 source remote vlan 300
monitor session 3 destination interface Fa8/25
```

Note In the above configuration, it is clear that port Fa8/25 cannot handle all the traffic that is captured. To address this problem, see Capturing and Differentiating Traffic on Multiple Ports, page 7-12.

Note The above configuration assumes that you have removed the “service module” session. For more information, see Service Module Session, page 7-11.

Service Module Session

A SPAN session is used by default when using Sup720 with a Cisco Firewall Services Module (FWSM) in the chassis. If you check for unused sessions (**show monitor**), you see that “session 1” is in use:

```
agg#show monitor
Session 1
---------
Type                   : Service Module Session
```

This session is automatically installed for the support of hardware multicast replication when a firewall blade is in the Catalyst 6500 chassis.

For data center designs, to understand whether you need to keep this automatically configured session or not, verify whether there is a multicast source on one inside VLAN of the FWSM. If there is, you need to keep the “monitor session servicemodule”; if not, you can remove this session.

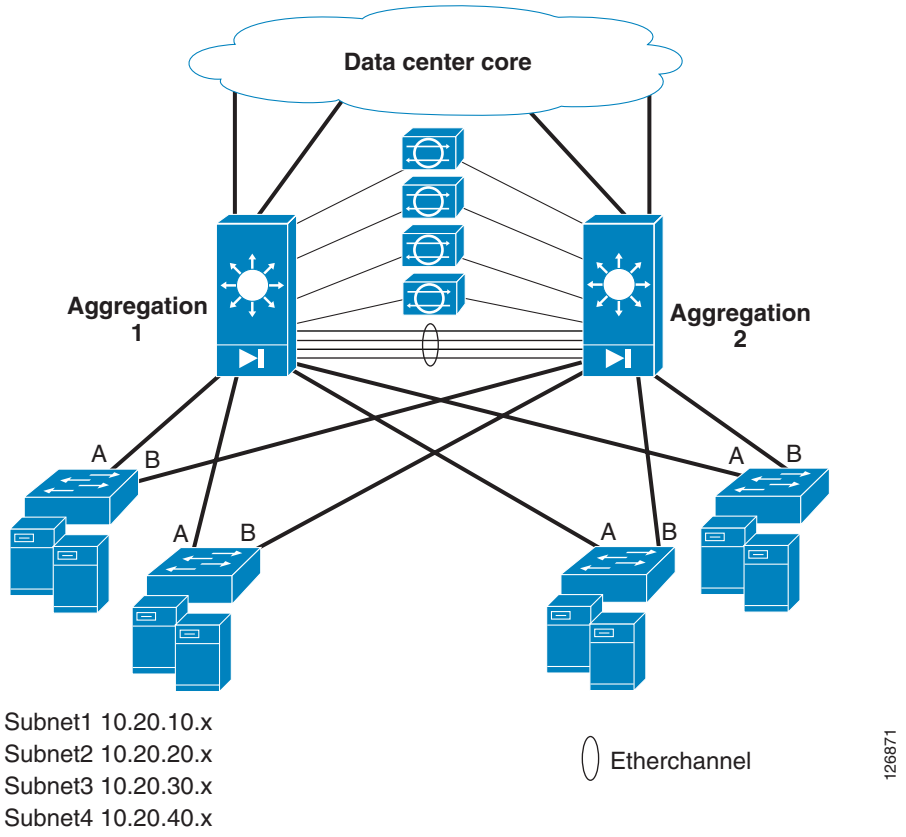
Capturing and Differentiating Traffic on Multiple Ports

This section describes the methods of capturing and differentiating traffic on multiple ports. It includes the following topics:

Data Center Topology

Figure 7-5 shows the reference data center topology.

Figure 7-5 Data Center Design and Placement of Sniffers, Sensors, and Analysis Tools



The aggregation switches are Catalyst 6500 switches with a firewall blade. The servers connect to the access layer. Subnet1, Subnet2, Subnet3, and Subnet4 can be on any of the four access switches; the monitoring design does not make assumptions about on which of the access devices each VLAN exists.

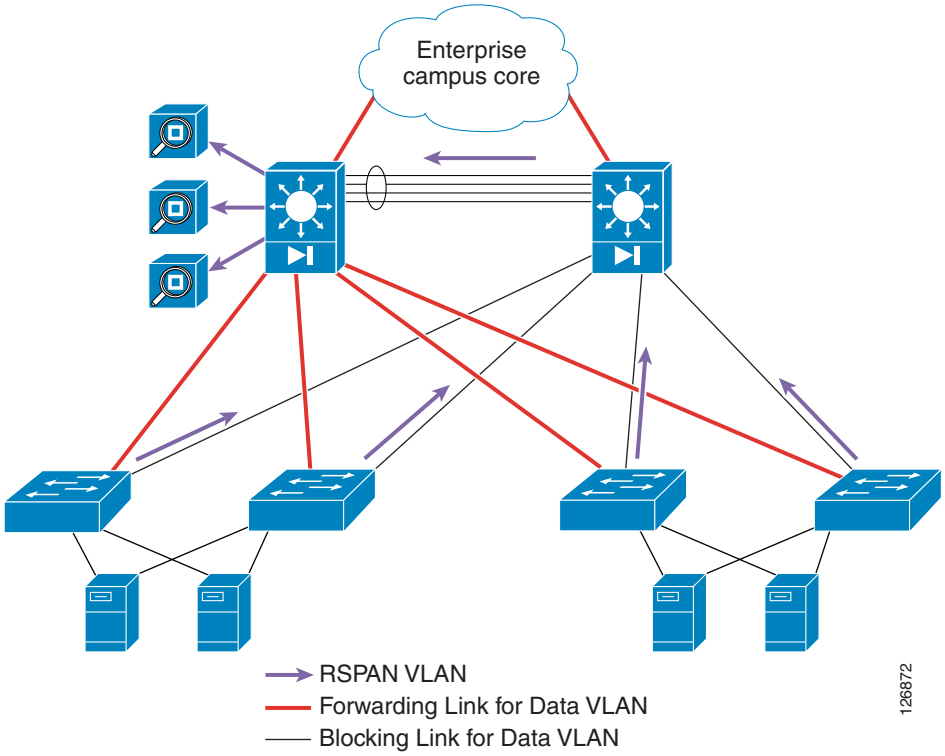
Sniffers and analyzing devices can connect to the access layer and the aggregation layer. It is often impractical to place a sniffer on every network device, so the logical placement point for network monitoring is the aggregation layer.

The root switch is Aggregation 1 and the secondary root is Aggregation 2. Depending on the topology, all traffic leaving the server farm might either traverse Aggregation 1 or be load balanced to both Aggregation 1 and Aggregation 2. Similarly, incoming traffic from the core can take either Aggregation 1 or Aggregation 2, so the design should be capable of capturing traffic regardless of which incoming and outgoing path is chosen. For this reason, depending on the analyzing/monitoring device, these can have one or multiple interfaces and connect to either Aggregation 1 or both aggregation switches.

By using the design shown in Figure 7-5, the visibility into the locally switched traffic on individual access switches is lost. This means that if two servers communicate at Layer 2 on an access switch, by default the monitoring device at the access layer cannot see this communication. Depending on the requirements of the monitoring implementation, you can extend the visibility of the monitoring device into the locally switched traffic by using Remote SPAN on the access switch and by aggregating the monitored traffic on the aggregation switches.

Figure 7-6 shows an example of how to use RSPAN to monitor the access layer devices with the instrumentation placed at the aggregation layer.

Figure 7-6 RSPAN Design used to Monitor the Locally Switched Traffic on the Access Layer Devices



The links from the access switches to the aggregation switches are the trunk and the link to Aggregation 2 is the blocking for the data traffic. You can design the network such that the links to Aggregation 2 also trunk the RSPAN VLAN, so that the forwarding topology of the RSPAN VLAN matches the blocking links of the data VLANs. By doing this, the RSPAN traffic does not take the bandwidth that is used for transactions. The RSPAN traffic is collected on Aggregation 2 and differentiated on the sensors.

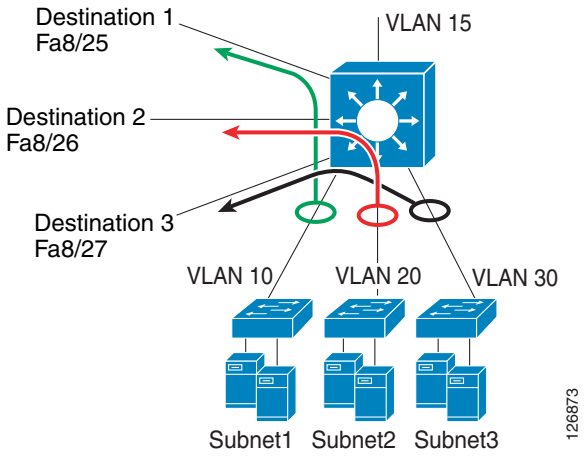
Using Virtual SPAN Sessions

With the Catalyst 6500 starting from Cisco IOS 12.2(18)SXD and 12.1(24)E, you can configure a single SPAN session to differentiate traffic on multiple ports. When defining the following SPAN session, Fa8/25, Fa8/26, and Fa8/27 see all traffic from VLAN 10, 20, and 30:

```
monitor session 2 source vlan 10 , 20 , 30
monitor session 2 destination interface Fa8/25 , Fa8/26 , Fa8/27
```

For most deployments, you need to separate the traffic and, for example, send traffic from VLAN 10 to Fa8/25, traffic from VLAN 20 to Fa8/26, and traffic from VLAN 30 to Fa8/27, as shown in Figure 7-7.

Figure 7-7 Using Virtual SPAN to Differentiate Multiple Source VLANs



With the introduction of virtual SPAN, you can define the following additional configurations to differentiate the traffic:

- Configure the intended SPAN destination interfaces as trunk ports.
- Configure the different allowed VLAN lists on the SPAN destination interfaces so that each interface allows only one or a few VLANs. In the case of Figure 7-7, you configure interface Fa8/25 to forward only VLAN 10, Fa8/26 to forward only VLAN 20, and Fa8/27 to forward only VLAN 30.

```
interface FastEthernet8/25
  description SPAN destination interface for VLAN 10
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10
  switchport mode trunk
  switchport nonegotiate
!
interface FastEthernet8/26
  description SPAN destination interface for VLAN 20
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 20
  switchport mode trunk
  switchport nonegotiate
!
interface FastEthernet8/27
```

```
  description SPAN destination interface for VLAN 30
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 30
  switchport mode trunk
  switchport nonegotiate
!
```

Note The **switchport nonegotiate** command is required only if you want mirrored traffic to include VLAN tags.

Virtual SPAN is very easy to configure for local SPAN that does not require additional traffic differentiation than the VLAN. If you need a design for local SPAN that integrates with remotely collected data and allows you to perform additional processing on the mirrored data such as differentiation based on the protocols, you need to use RSPAN with VACL redirect.

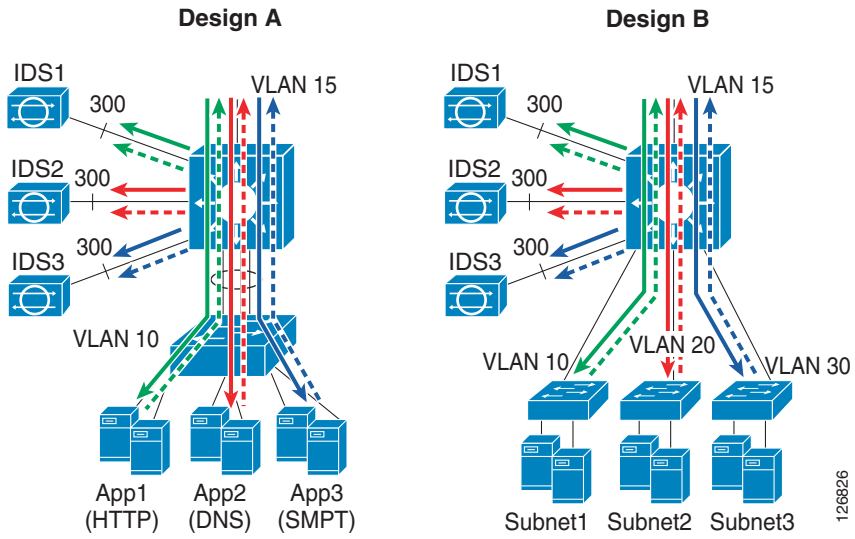
Using RSPAN with VACL Redirect

Using RSPAN with VACL redirect for local traffic monitoring allows you to differentiate network traffic based on the following:

- Protocol—You can send one type of traffic, such as HTTP, to one analyzer, and another type, such as DNS, to another monitoring device.
- Subnet—You can monitor specific subnets with specific analyzers.
- Ethertype for non-IP/non-IPX traffic—You can send non-IP traffic to different probes based on the Ethertype or the MAC address.
- Integration—This solution is easily integrated with remote traffic monitoring.

Figure 7-8 shows the use of RSPAN and VACL redirect to differentiate traffic on multiple sensors.

Figure 7-8 Traffic Differentiation with RSPAN and VACL Redirect



In Design A, traffic is sent to different sensors based on the protocol. The Catalyst 6500 generates a copy of the traffic and sends HTTP traffic to IDS1, DNS traffic to IDS2, and SMTP traffic to IDS3. In Design B, traffic is sent to different sensors based on the subnet. Traffic for Subnet1 is sent to IDS1, traffic for Subnet2 is sent to IDS2, and traffic for Subnet3 is sent to IDS3.

Note In this chapter, the illustrations show intrusion detection system (IDS) devices as the analyzer devices, because this design can be used for the deployment of IDS as well as generic network analysis tools.

Hardware Requirements

The design with RSPAN and VACL redirect works on both the Catalyst 6500 Sup2 and Sup720. On Sup720, if using PFC3A, this functionality is available if the hardware revision is 2.2 or later. You can verify the hardware revision by using the **show module** command:

```
Mod Sub-Module                  Model              Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  6 Policy Feature Card 3       WS-F6K-PFC3A       SAD0812099Y   2.2    Ok
  6 MSFC3 Daughterboard         WS-SUP720          SAD080904AG   2.2    Ok
```

Using RSPAN in conjunction with VACL redirect requires the capability to apply VACLs in hardware on the traffic present on the RSPAN VLAN. This design was tested with Cisco IOS 12.2(17d)SXB3.

VACL Redirect

VACL redirect lets you override MAC address-based forwarding so that you can forward traffic to a specific port in a VLAN. For example, when you specify a VACL redirect on a VLAN, you can send frames to a specified port on that VLAN based on the Layer 3 source and destination address, as well as the Layer 4 protocol and ports.

The following configuration demonstrates the use of the VACL redirect function:

```
ip access-list extended ACL-A
 permit tcp 10.20.5.0 0.0.0.255 10.20.10.0 0.0.0.255 eq 80
 permit tcp 10.20.10.0 0.0.0.255 eq 80 10.20.5.0 0.0.0.255
!
ip access-list extended ACL-B
 permit udp 10.20.5.0 0.0.0.255 10.20.10.0 0.0.0.255
 permit udp 10.20.10.0 0.0.0.255 10.20.5.0 0.0.0.255
!
ip access-list extended ACL-C
 permit tcp host 10.20.5.10 any
 permit tcp any host 10.20.5.10
!
[…]
vlan access-map analyzerfilter 10
 match ip address ACL-A
 action redirect FastEthernet8/1
vlan access-map analyzerfilter20
 match ip address ACL-B
 action redirect FastEthernet8/2
vlan access-map analyzerfilter 30
 match ip address ACL-C
 action redirect FastEthernet8/3
vlan access-map analyzerfilter 40
 match ip address ACL-D
 action redirect FastEthernet8/4
vlan access-map analyzerfilter 50
```

```
 match ip address ACL-E
 action redirect FastEthernet8/5
vlan access-map analyzerfilter 60
 match ip address ACL-F
 action redirect FastEthernet8/6
!
vlan filter analyzerfilter vlan-list 300
```

This configuration filters traffic on VLAN 300 and performs the following actions:

- Redirects HTTP traffic between subnet 10.20.5.x and 10.20.10.x to port Fa8/1
- Redirects UDP traffic between the same two subnets to port Fa8/2
- Redirects TCP traffic exchanged by the host 10.20.5.10 to port fa8/3

You can configure up to 256 redirect ports per VACL and a maximum of five redirect ports per access list clause.

Note Redirect of non-IP traffic with a MAC access list is possible only in Cisco IOS.

Design Details

You can combine RSPAN with VACL redirect to collect traffic from multiple VLANs and ports, separate the traffic, and forward it to different analyzers. The typical topology uses RSPAN to collect traffic from both local and remote switches and send it to the RSPAN VLAN.

You need to use RSPAN on the switch where the analyzers are physically attached, for the purpose of filtering the mirrored traffic with a VACL on the RSPAN VLAN and differentiating it on multiple sensors.

Figure 7-9 shows how the two technologies can be used concurrently to collect and subsequently separate the traffic from a server farm.

Figure 7-9 RSPAN and VACL Redirect Topology Example

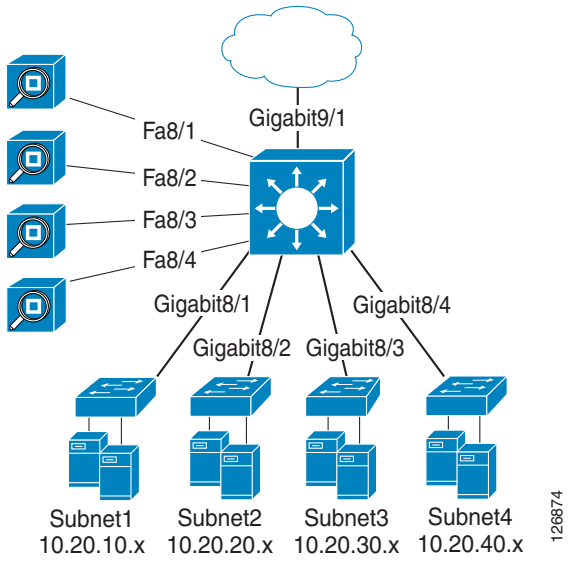


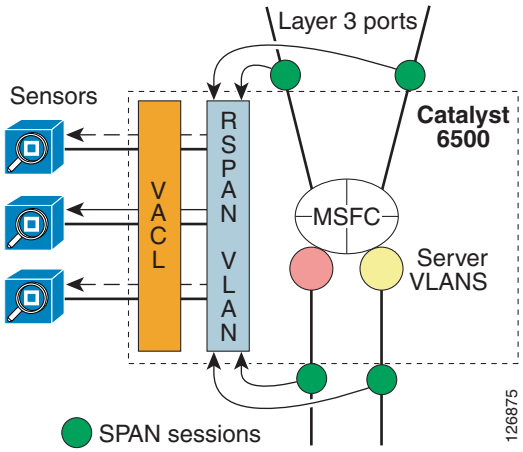
Figure 7-9 shows a server farm connected to four switches. RSPAN is used to collect traffic from all the subnets: 10.20.10.x (VLAN 10), 10.20.20.x (VLAN 20), 10.20.30.x (VLAN 30), and 10.20.40.x (VLAN 40). The RSPAN configuration sends traffic from each respective VLAN into the RSPAN VLAN.

A VACL is applied to the RSPAN VLAN to separate the traffic flows and to distribute them to the four analyzers on ports Fa8/1 to Fa8/4.

Note You can distribute the traffic to as many as 256 analyzers by defining ACLs to match the different traffic types.

Figure 7-10 shows the VLAN topology within the Catalyst 6500.

Figure 7-10 Catalyst 6500 Internal Topology with RSPAN and VACL Redirect



You can see the Layer 3 links that connect the Catalyst 6500 to the core and the links assigned to the server VLANs. The server VLANs are represented with big circles that connect the physical links with the Multilayer Switch Feature Card (MSFC), which is the routing engine. The Layer 3 links connect the core devices directly to the MSFC (the routing engine).

The sniffers and analyzers are connected to a special VLAN, which is the RSPAN VLAN. An RSPAN VLAN is used simply because it allows having a copy of the traffic in a VLAN that can be manipulated with VACLs. All sniffers and sensors connect to the RSPAN VLAN. A VACL filters the traffic that leaves the RSPAN VLAN towards the sensors.

The green circles represent the SPAN configuration that effectively creates a copy of the traffic from each one of the ports and funnels it into the RSPAN VLAN.

Configuration Steps

The following are the key configuration steps for copying traffic with this technique:

- Copy the traffic from all the VLANs or the physical links into the Remote SPAN VLAN. In Figure 7-10, this configuration is applied to the physical port (that is, the point of conjunction of the physical link with the Catalyst 6500). You can apply the mirroring configuration to the VLAN.
- Allow forwarding of the RSPAN traffic to all the sensing ports (the next step controls which sensor gets which traffic, but first, all of the ports that connect to the IDS sensors need to be allowed).
- Configure one access list for each traffic category that you have identified.

- Configure a VLAN access map that associates the access lists with the correct IDS port via an "action redirect" statement and apply the VACL to the Remote SPAN VLAN. In Figure 7-10, all IDS ports belong to the RSPAN VLAN but there is a VACL that controls which traffic is sent to which IDS sensor.

Mirroring All Traffic to the RSPAN VLAN

Unlike SPAN, which allows you to mirror traffic from one or more ports on a Cisco Catalyst switch (the SPAN source) only to another port on the same switch (the SPAN destination), RSPAN allows you to capture traffic on one switch, mirror it to a designated VLAN, and then forward it to one or more ports on one or more other switches for analysis.

In this case, RSPAN is useful because it allows copying the traffic to a VLAN that can be manipulated with VACLs. The goal in this case is not to export the VLAN to another switch; it is just to have a local copy of the traffic on the Catalyst 6500.

VLAN 300 is defined as the RSPAN VLAN on the Catalyst switch.

```
vlan 300
 name rspan
 remote-span
!
```

The following configuration captures traffic from all interfaces of interest and sends the mirrored traffic to VLAN 300:

```
monitor session 1 source int giga9/1 , giga8/1 , giga8/2 , giga8/3 , giga8/4 rx
monitor session 1 destination remote vlan 300
```

Ensuring that All Monitoring Devices Can Receive the Mirrored Frames

The four IDS sensors connect the Catalyst 6500 to the following ports: int fa8/1, fa8/2, fa8/3, and fa8/4. These ports must be capable of forwarding traffic present on the RSPAN VLAN. The VACL eventually decides which sensor gets which traffic, but first all sensors must be capable of receiving the mirrored traffic.

This is achieved with the following configuration, which creates an RSPAN destination session that forwards the traffic to all the sensors (interfaces fa8/1–4).

```
monitor session 2 destination interface Fa8/1 - 4
monitor session 2 source remote vlan 300
```

Defining the Categories for Separating the Mirrored Traffic

With four instruments, you normally want to define four traffic categories.

Assume that you want to assign the traffic to the sniffers/sensors as follows:

- Sensor1 to monitor HTTP traffic exchanged between the Internet and subnet1 (10.20.10.x)
- Sensor2 to monitor HTTP traffic exchanged between the Internet and subnet2 (10.20.20.x)
- Sensor3 to monitor HTTP traffic exchanged between the Internet and subnet3 (10.20.30.x)
- Sensor4 to monitor HTTP traffic exchanged between the Internet and subnet4 (10.20.40.x)

The access lists for each sensor are configured to deny all traffic sourced by the subnets that are not of interest (for sensor1, this means denying subnets 2, 3, and 4), to deny the locally switched traffic (for sensor1, this means denying subnet1 to subnet1 traffic).

```
ip access-list extended toSensor1
 deny ip 10.20.20.0 0.0.0.255 any
 deny ip 10.20.30.0 0.0.0.255 any
```

```
 deny ip 10.20.40.0 0.0.0.255 any
 deny ip 10.20.10.0 0.0.0.255 10.20.10.0 0.0.0.255
 permit tcp any 10.20.10.0 0.0.0.255 eq 80
 permit tcp 10.20.10.0 0.0.0.255 eq 80 any
 deny ip any any
!
ip access-list extended toSensor2
 deny ip 10.20.10.0 0.0.0.255 any
 deny ip 10.20.30.0 0.0.0.255 any
 deny ip 10.20.40.0 0.0.0.255 any
 deny ip 10.20.20.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit tcp any 10.20.20.0 0.0.0.255 eq 80
 permit tcp 10.20.20.0 0.0.0.255 eq 80 any
 deny ip any any
!
[…]
```

You might want to define a catch-all to collect all the remaining traffic for analysis on a dedicated sensor or for sniffing it, as follows:

```
ip access-list extended IP-catch-all
 permit ip any any
!
ipx access-list extended IPX-catch-all
 permit any any
!
mac access-list extended non-IP-catch-all
 permit any any
!
```

Note Notice that the VACLs that you define here do not affect traffic forwarding on any of the server VLANs nor do they affect routing. These VACLs are applied on the RSPAN VLAN, which only carries mirrored frames of the data center traffic. This is another advantage of using RSPAN and VACL redirect: its use does not interfere with regular traffic filtering.

Redirecting the Traffic to the Appropriate Sensors

Next, you create a VLAN access map and assign each traffic category to the port to which the associated sensor is connected. For example, the traffic category that is defined by the access list to Sensor1 is redirected to the port Fa8/1 where Sensor1 is connected.

The VLAN access map is then applied to VLAN 300. Remember that traffic that matches a deny entry in an access list in the VLAN access-map rule 10 is subject to the processing in the VLAN access-map rule 20, and if it matches a deny, it is in turn processed by the VLAN access-map rule 30, and so on.

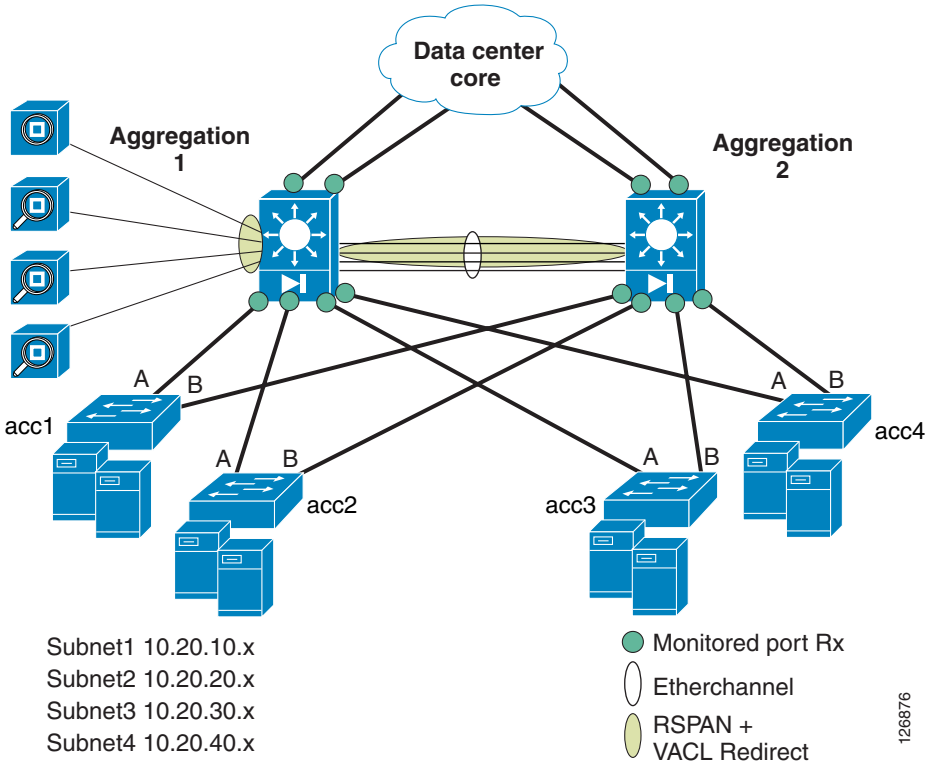
```
vlan access-map analyzerfilter 10
 match ip address toSensor1
 action redirect FastEthernet8/1
vlan access-map analyzerfilter 20
 match ip address toSensor2
 action redirect FastEthernet8/2
vlan access-map analyzerfilter 30
 match ip address toSensor3
 action redirect FastEthernet8/3
vlan access-map analyzerfilter 40
 match ip address toSensor4
 action redirect FastEthernet8/4
!
! catch all entries
!
```

```
vlan access-map analyzerfilter 50
 match ip address IP-catch-all
 action redirect FastEthernet8/46
vlan access-map analyzerfilter 60
 match ipx address IPX-catch-all
 action redirect FastEthernet8/47
vlan access-map analyzerfilter 70
 match mac address non-IP-catch-all
 action redirect FastEthernet8/48
!
vlan filter analyzerfilter vlan-list 300
```

Monitoring Best Practices in a Fully Redundant Topology

Figure 7-11 shows a fully redundant topology.

Figure 7-11 Fully Redundant Traffic Monitoring Architecture



The key design challenges that need to be addressed in a fully redundant topology include the following issues:

- Avoiding sending duplicate traffic to the sensors
- Ensuring that the sensors can see both directions of the traffic regardless of the redundant Layer 2 and Layer 3 paths

Avoiding Duplicate Frames

As an example of the first concern, assume that in the topology shown in Figure 7-11 you configured a **monitor session** *1* **source interface** *giga8/1, giga8/2* **both**. Assume that a server from 10.20.10.x sends traffic to a server in 10.20.20.x. The traffic from switch acc1 arrives to Aggregation 1 and the SPAN

configuration generates a copy of the traffic (Rx). Then the MSFC routes to 10.20.20.x and the frame goes out to giga8/2 (Tx), and another copy of the same frame is generated and sent to the sensors. This means that for the same frame, this configuration is generating two copies. This problem can be fixed by making sure that the SPAN session is configured on all the physical interfaces for the Rx direction only.

Now assume that in the fully redundant topology you configured a **monitor session** *1* **source interface** *giga8/1, giga8/2, Po10* **rx** where the port channel 10 connects the two aggregation switches. Assume that traffic is routed from 10.20.10.x to 10.20.20.x, and that the path to 10.20.20.x takes the port channel. In this case, there is no generation of duplicate frames on Aggregation 1. But with the overall topology, considering that you want to monitor what gets switched on Aggregation 2, it is very likely that on Aggregation 2 you also have a session **monitor session** *1* **source interface** *giga8/1 , giga8/2 , Po10* **rx**. This means that both Aggregation 1 and Aggregation 2 generate one copy of the same frame.

Whether this is a problem or not depends on the design, but if you have a single set of instruments that monitor the overall traffic going into the server farm, it is advisable not to monitor the port channel, and to aggregate the traffic captured on both aggregation switches on the same RSPAN VLAN, as you can see in Figure 7-11.

In Figure 7-11, there is no SPAN session on the port channel; SPAN sessions are configured on the physical links.

Monitoring Traffic Flows across both Aggregation Switches

The second concern refers to ensuring that the instruments can see both directions of the traffic regardless of whether the traffic enters from the core to Aggregation 1 or to Aggregation 2 and regardless of whether the forwarding port on the access switches is port A or port B.

Sniffers connect to only one of the switches; for example, Aggregation 1 as it is shown in Figure 7-11. Traffic from Aggregation 2 is copied on the RSPAN VLAN, which is carried across the EtherChannel trunk that connects Aggregation 1 and Aggregation 2.

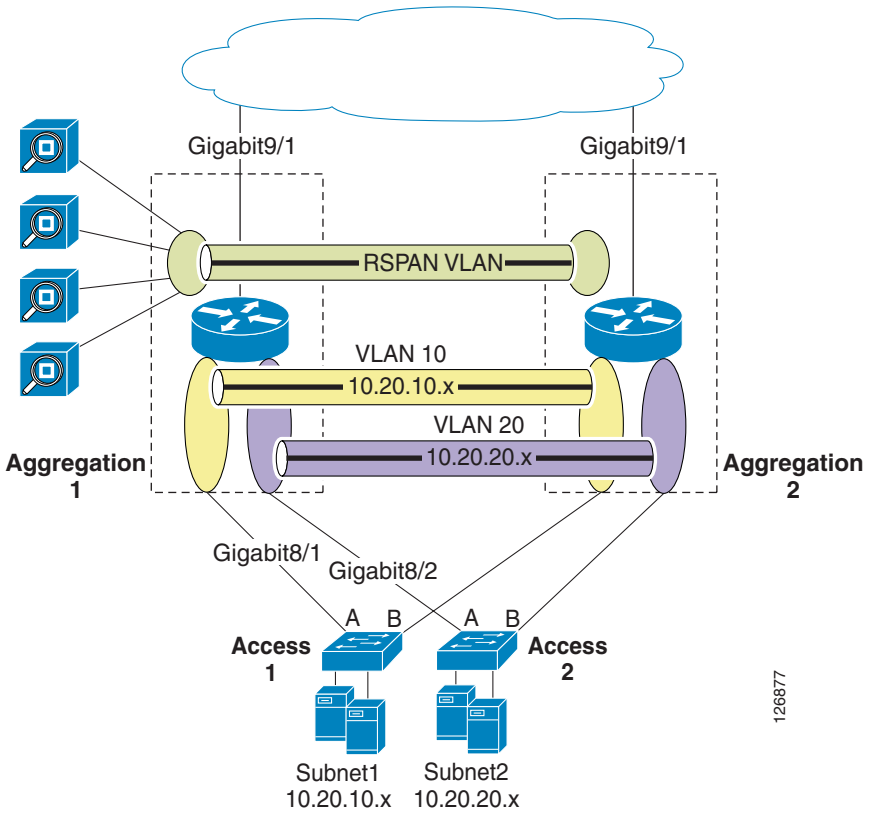
Note With IDS, you can implement a different design. IDS sensors can be dual-homed to both aggregation switches. The configuration of Aggregation 1 and Aggregation 2 are identical from the point of view of traffic capturing. This means that the IDS port connected to Aggregation 2 is configured on the RSPAN VLAN and a VACL redirect configured on Aggregation 2. From the IDS point of view, both interfaces belong to the virtual sensor, and traffic for the same stream can come in from either interface.

VSPAN versus PSPAN

Traffic can be captured on the VLAN with a SPAN Rx or from the physical port with a SPAN Rx configuration. This second design better reduces duplicate traffic in fully redundant topologies.

Figure 7-12 shows the logical topology inside the Catalyst 6500.

Figure 7-12 VLAN Topology



The MSFC is represented as a router, VLAN 10 (Subnet1) is represented as an oval in yellow, and VLAN 20 (Subnet2) is represented as an oval in purple. These two VLANs are obviously trunked between the two aggregation switches for reasons of Layer 2 redundancy.

Assume that you want to configure the SPAN on the VLANs. On Aggregation 1 and Aggregation 2, you configure the following:

```
monitor session 1 source vlan 10 , 20 , 30 , 40 rx
monitor session 1 destination remote vlan 300
```

Under normal conditions, traffic from 10.20.10.x directed to 10.20.20.x is copied once to VLAN 300, when it enters VLAN 10 from Giga8/1. The MSFC then routes to VLAN 20 and the traffic goes out to Giga8/2 to reach the destination host. The reverse traffic comes from Access 2 and the frame is copied when it enters VLAN 20 from Giga8/2. Then the MSFC routes to VLAN 10 and the traffic is sent out to Giga8/1.

This scenario considers the topology where on Access 2, port A is forwarding and port B is blocking. Now consider the case where on Access 2, port A is blocking and port B is forwarding. In this case, everything works the same until the traffic from 10.20.10.x is routed to 10.20.20.x. The first copy of the 10.20.10.x-to-10.20.20.x traffic is generated when the frame enters VLAN 10 from Gigabit8/1. The MSFC then routes to VLAN 20.

Differently from the first scenario described, the frame now must go to Aggregation 2 to arrive at Access 2. The frame then takes the EtherChannel trunk and the second copy of the same frame is generated when it enters Aggregation 2.

This is because, as previously stated, for reasons of redundancy both aggregation switches must be configured the same to replicate traffic to the IDSs regardless of which path the traffic takes.

This example demonstrates that configuring SPAN on a VLAN is not optimal when the traffic takes asymmetric paths.

Assume configuring SPAN as follows:

```
monitor session 1 source int giga9/1 , giga8/1 , giga8/2 , giga8/3 , giga8/4 rx
monitor session 1 destination remote vlan 300
```

In the basic scenario where port A is forwarding and port B blocking on all access switches, the mirroring does not produce any duplicate frames. In the scenario where Access 2 has port A blocking and port B forwarding, there are no duplicate frames either. In fact, the problem of SPAN on the VLAN is that Aggregation 2 generates a second copy when the traffic enters the VLAN from the EtherChannel trunk.

When SPAN is configured on physical interfaces (and it should not be configured on the EtherChannel trunk), the traffic forwarded from one aggregation switch to the other does not generate any duplicate traffic.

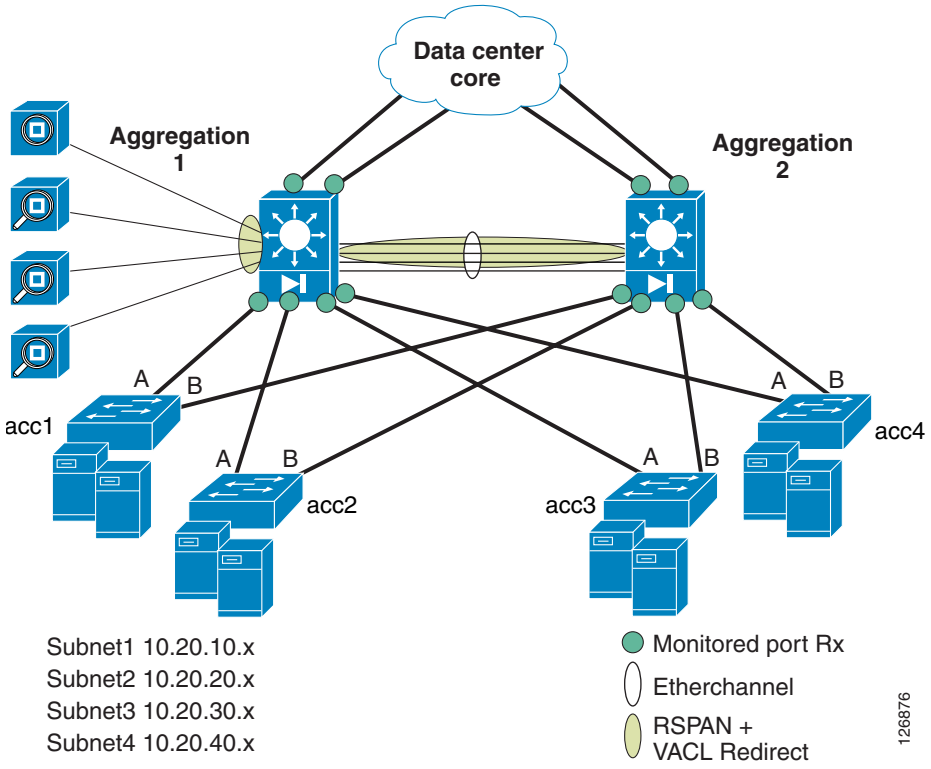
The return traffic from 10.20.20.x goes to Aggregation 2, which generates a copy of the traffic for the 10.20.20.x-to-10.20.10.x direction. The traffic is sent back to Aggregation 1 to be routed to 10.20.10.x. No other copies of the traffic are generated.

For these reasons, Cisco recommends configuring SPAN on the physical interfaces that require monitoring, but only in the Rx direction to avoid generating duplicate copies of the traffic.

Complete Architecture

Figure 7-13 shows the complete architecture that defines how to capture traffic.

Figure 7-13 Traffic Monitoring Architecture



This is a fully redundant data center topology with access and aggregation layers. The aggregation layer consists of Catalyst 6500s with sniffers or sensors attached to Aggregation 1 with a Cisco FWSM (optional component) in each aggregation switch.

This topology has four subnets: 10.20.10.x, 10.20.20.x, 10.20.30.x, and 10.20.40.x. No assumption is made on where these subnets reside in the access switches. RSPAN and VACL redirect allow these subnets to be monitored respectively by Sensor1, Sensor2, Sensor3, and Sensor4 regardless of where these subnets reside in the data center. What traffic Sensor1, Sensor2, Sensor3, and Sensor4 need to monitor is determined by the user, and this is defined by creating access lists to be applied to the VLAN that carries the copy of the traffic (the RSPAN VLAN). You can modify this policy without impacting traffic forwarding on the network.

The green circles indicate to which port the SPAN configuration is applied. This ensures that all traffic that flows in and out of the data center is copied on the RSPAN VLAN for processing and analysis. The RSPAN VLAN exists on both Aggregation 1 and Aggregation 2. On Aggregation 1, the sensors/sniffers are connected to the RSPAN VLAN. Traffic captured on Aggregation 2 is copied to the RSPAN VLAN and trunked between Aggregation 1 and Aggregation 2 on the port channel.

The Rx option is used to avoid duplicate traffic. SPAN is not applied to the ports in the EtherChannel connecting the two aggregation switches. Monitoring the physical interfaces instead of the VLANs ensures that even in the presence of asymmetric traffic forwarding there is no duplicate traffic.

The same configuration present on Aggregation 1 is also present on Aggregation 2 so that a given flow can take one aggregation switch in its inbound direction and Aggregation 2 in the outbound direction. The sensors receive both directions of the flows because both Aggregation 1 and Aggregation 2 copy the traffic on the RSPAN VLAN.

When capturing traffic in the presence of load balancers or firewalls, you must consider the implications on the TCP sequence number of the frames. Client-to-server traffic captured between the client and the firewall or the load balancer might show an acknowledgement number that does not match the sequence number from the server-to-client traffic captured between servers and the firewall or load balancer. This is because firewalls and load balancers are TCP proxy devices, thus the sequence numbers on either side are different. This is typically a problem with intrusion detection sensors. Most sniffer tools can still correlate TCP streams.

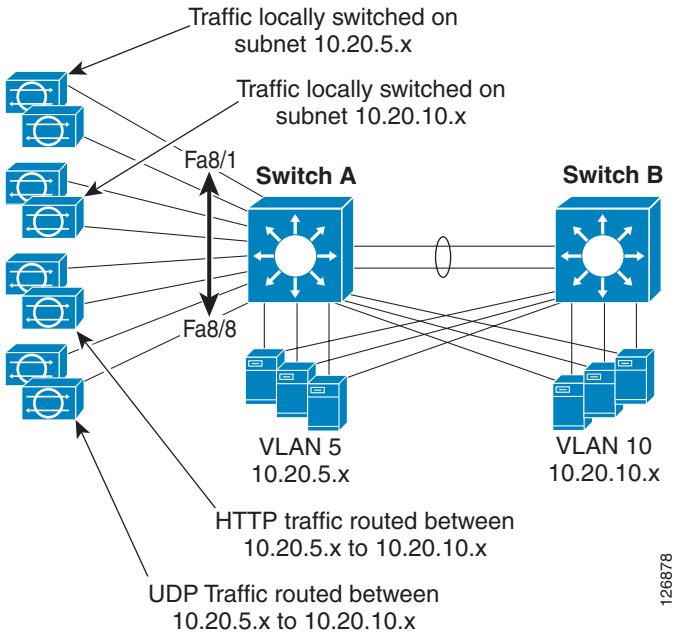
Note If NAT identifies multiple servers as a single IP address, modify the design to include, for example, the load balancer ports among the SPAN ports or to use SPAN for the VLANs that the load balancer uses.

Using Redundant Analyzers

In the design described in the previous sections, if one analyzer fails, there is no way to reassign the traffic to the remaining analyzer devices. You can solve this problem by using redundant analyzers, generating a copy of the frame and sending both frames to both devices.

Figure 7-14 demonstrates how to configure a network to include redundancy.

Figure 7-14 Analyzer Redundancy



In Figure 7-14, each analyzer (in this case an IDS sensor) is duplicated, and each traffic category is sent to two sensors. If one analyzer fails, the peer device can still receive the traffic. This can be done both with virtual SPAN and with RSPAN.

In the case of RSPAN, if the two analyzers assigned to subnet 10.20.5.x are connected to ports FastEthernet8/1 and FastEthernet8/2, and the two analyzers assigned to subnet 10.20.10.x are connected to ports FastEthernet8/3 and FastEthernet8/4, the VACLs are configured as follows:

```
vlan access-map analyzerfilter 10
 match ip address ACL-A
 action redirect FastEthernet8/1 FastEthernet8/2
vlan access-map analyzerfilter 20
 match ip address ACL-B
 action redirect FastEthernet8/3 FastEthernet8/4
vlan access-map analyzerfilter 30
 match ip address ACL-C
 action redirect FastEthernet8/5 FastEthernet8/6
vlan access-map analyzerfilter 40
 match ip address ACL-D
 action redirect FastEthernet8/7 FastEthernet8/8
!
vlan filter analyzerfilter vlan-list 300
```

Conclusion

Various technologies can perform traffic monitoring and analysis for an end-to-end Cisco data center network.

VACL capture requires changing security VACLs to include a special action (forward capture). VACL capture scales well and does not generate duplicate frames, but it is difficult to differentiate routed traffic to multiple sensors.

SPAN does not require changes to security VACLs, and can be defined on physical interfaces or VLANs. SPAN can generate duplicates by using the Rx or Tx options, and offers a limited number of sessions. More recently, the virtual SPAN option is available. Virtual SPAN allows differentiating traffic on multiple ports based on the VLAN information of the source traffic. Virtual SPAN has great scalability, does not allow differentiating the traffic based on the Layer 4 information, and does not work on RSPAN traffic; that is, you cannot differentiate traffic collected from remote devices based on the source information of the VLANs.

You can use RSPAN for local SPAN purposes to create a copy of the traffic and do further processing on it with VACLs. RSPAN combined with VACL redirect does not require any modification in the security VACLs, and allows differentiating the traffic based on the subnet information, the Layer 4 protocols, and Layer 4 port. It can be easily integrated with an RSPAN design to aggregate traffic from multiple switches to the device where the instrumentation is connected and to differentiate this traffic based on subnets, Layer 4 protocols, and Layer 4 ports. RSPAN combined with VACL redirect allow differentiating the traffic to up to 64 sniffers/analyzers.

In a fully redundant topology, you must monitor all traffic entering and leaving the data center (client-to-server and server-to-client) and routed within the data center (server-to-server) without generating duplicates, and it is important to make sure that the instrumentation sees both directions of the traffic even in the presence of asymmetric paths. One solution consists in configuring SPAN Rx or Tx on the physical ports of the aggregation switches with the exception of the port channel connecting the two aggregation switches. If the sniffers/sensors are connected to one aggregation switch only (the root switch), RSPAN carries the traffic captured from the secondary root switch to the primary root.

Additional References

For more information, see the following documents:

- “Using RSPAN with VACLs for Granular Traffic Analysis,” Tim Stevenson
  http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/rspan_wp.pdf
- Information about SPAN on the Catalyst 6500:
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml
- Information about VACLs:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.pdf