Using RSPAN with VACLs for Granular Traffic Analysis

This application note demonstrates how to combine two powerful features, Remote Switch Port Analyzer (RSPAN) and virtual LAN (VLAN) access control lists (VACLs) to create an effective, highly granular tool for traffic analysis on the Cisco® Catalyst® 6500 Series switches.

Overview of RSPAN

SPAN is a well-understood and widely used technology for mirroring traffic from one or more ports on a Cisco Catalyst switch (the SPAN source) to another port on the same switch (the SPAN destination). This is frequently called "local SPAN." Local SPAN has many important uses, including enabling users to capture and analyze traffic passing through a single switch.

RSPAN is another traffic-mirroring technology that allows users to extend the scope of their analysis to encompass multiple switches that are interconnected in the same Layer 2 domain. Pioneered on the Cisco Catalyst 6500 Series switches, RSPAN increases the flexibility afforded by the switch for port mirroring by allowing users 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.

RSPAN software support is available in the following software releases for the Cisco Catalyst 6500 series switches:

- Cisco Catalyst Operating System Software Release 5.3 and later
- Cisco IOS® Software Release 12.1(13)E and later

There are specific limits on the number of local and remote SPAN sessions permitted on a given Cisco Catalyst 6500 Series system. These limits are documented in the *Software Configuration Guides* for the Cisco IOS Software and the Cisco Catalyst OS Software. For details, visit:

- "Configuring Local SPAN and RSPAN" in the *Cisco IOS Software Configuration Guide* for Release 12.1E

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/span.htm#1036881
- "Configuring SPAN and RSPAN" in the *Catalyst OS Software Configuration Guide* for Release 7.5

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_5/confg_gd/span.htm#1019903

Overview of VACLs

Another very powerful tool, also pioneered on the Cisco Catalyst 6500 Series switches, is network-security enforcement based on Layer 2, Layer 3, and Layer 4 information for all traffic in a VLAN, using VLAN access control lists, or VACLs. When a VACL is associated with a particular VLAN, all traffic, whether bridged within the VLAN or Layer 3-switched into the VLAN, is subjected to the configured VACL policy. VACLs are enforced in hardware; there is no performance penalty for applying VACLs to a VLAN on the Cisco Catalyst 6500 Series switches.

VACLs can enforce VLAN security based on a variety of information. For IP packets, 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.

VACL software support is available in the following releases for the Cisco Catalyst 6500 Series switches:

- Cisco Catalyst OS Software Release 5.3 and later
- Cisco IOS Software Release 12.1(8a)EX and later

While local SPAN has its uses, in some cases it is simply not flexible or granular enough for the user's purposes. Local SPAN always captures all the traffic from the SPAN source to the SPAN destination, including control traffic, broadcasts, and other frequently irrelevant traffic.

RSPAN provides several additional functions that are not available with local SPAN. The examples in the next section, "Using RSPAN and VACLs Together," illustrate the flexibility and power of combining RSPAN with VACLs in the Cisco Catalyst 6500 Series switches.

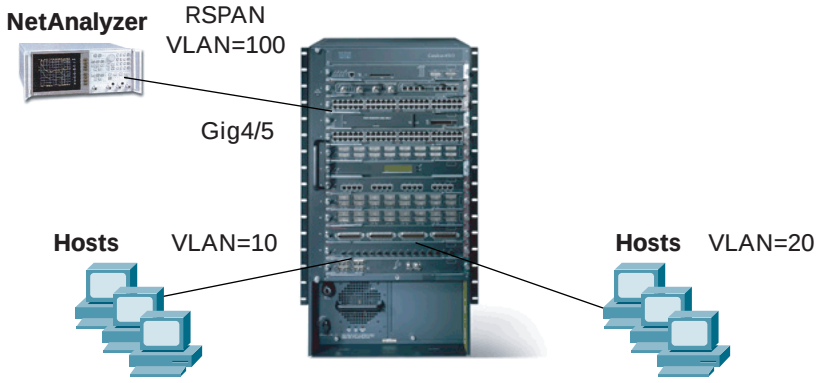
Using RSPAN and VACLs Together

Now we will examine several example network scenarios where RSPAN and VACLs together can be used to achieve flexible, highly granular traffic analysis.

Example 1—Using RSPAN and VACLs on a Single Switch

Combining RSPAN and VACLs on a single switch (Figure 1) offers a great deal of flexibility in terms of the type and amount of traffic captured for analysis, while keeping the mirrored traffic local to a single switch.

Figure 1
Using RSPAN and VACLs on a Single Switch



In this example, there are hosts in two different VLANs, VLAN 10 and VLAN 20. The network administrator wants to capture bidirectional traffic passing through these VLANs to a network analyzer on interface GigabitEthernet4/5. However, the only traffic the administrator is interested in is Transmission Control Protocol (TCP) traffic destined to a specific range of ports, 5000–6000.

With traditional local SPAN, the administrator configures a bidirectional SPAN session with VLANs 10 and 20 as the SPAN source and the port connected to the analyzer as the SPAN destination. However, all traffic in VLANs 10 and 20 is forwarded to the SPAN destination port, which may overrun the analyzer or oversubscribe the destination port, resulting in some packets not being captured.

By itself, RSPAN does not add much to this equation. Rather than specifying the SPAN destination as the analyzer port, the administrator defines an RSPAN VLAN and specifies that VLAN as the SPAN destination. Because the RSPAN destination is also on the same switch, there does not appear to be any advantage to using RSPAN instead of local SPAN.

However, using an RSPAN session instead of local SPAN allows the administrator to define a security VACL that identifies the exact traffic that needs to be captured. When this VACL is applied to the RSPAN VLAN, only traffic matching the access-control entries specified in the VACL are permitted to pass into the RSPAN VLAN and, by extension, to the RSPAN destination port.

Configuration Example 1 Using Cisco IOS Software

The following configuration was used to achieve the results described in this example on a Supervisor Engine 2 with MSFC2 using Cisco IOS Software Release 12.1(13)E4 on the supervisor engine.

```
!
hostname Switch_A
! Defines L2 VLANs 10 and 20
vlan 10,20
!
! Defines VLAN 100 as the RSPAN VLAN
vlan 100
 remote-span
!
! The monitor port requires no special configuration
interface GigabitEthernet4/5
 description Monitor Port
 no ip address
!
! Defines L3 VLANs 10 and 20
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
 ip address 10.20.20.1 255.255.255.0
!
! VACLs require that a corresponding SVI (L3 interface) exists
! It can remain unconfigured and administratively shutdown
interface Vlan100
 description RSPAN VLAN - Must exist for VACL on RSPAN VLAN
 no ip address
 shutdown
!
! The IP extended ACL that matches TCP traffic destined to ports 5000 – 6000
ip access-list extended TCP-TRAFFIC
 permit tcp any any range 5000 6000
!
! Defines the VLAN access-map (VACL)
vlan access-map RSPAN-VACL 10
 match ip address TCP-TRAFFIC
```

```
 action forward
!
! Maps the VACL to the RSPAN VLAN
vlan filter RSPAN-VACL vlan-list 100
!
! Monitor session 1 captures bidirectional traffic from
! VLANs 10 and 20 to RSPAN VLAN 100
monitor session 1 source vlan 10 , 20
monitor session 1 destination remote vlan 100
!
! Monitor session 2 captures bidirectional traffic from
! RSPAN VLAN 100 to interface gig4/5
monitor session 2 source remote vlan 100
monitor session 2 destination interface Gi4/5
```

Configuration Example 1 Using Cisco Catalyst OS Software

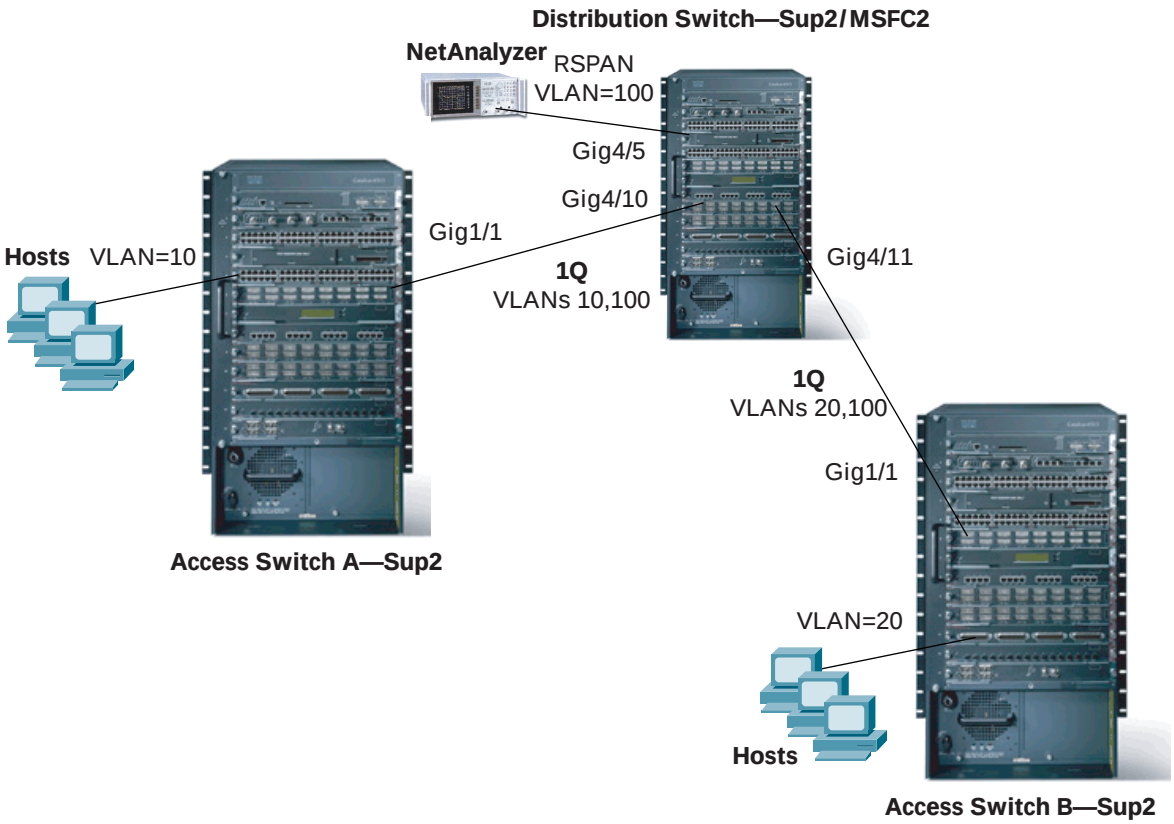
The following configuration was used on a Supervisor Engine 2 with MSFC2 to achieve the results described in this example using Cisco Catalyst OS Software Release 7.5(1) on the supervisor engine and Cisco IOS Software Release 12.1(13)E4 on the MSFC2.

```
#CatOS Configuration on Supervisor Engine:
set system name Switch_A
!
#Defines L2 VLANs 10 and 20
set vlan 10,20
!
#Defines RSPAN VLAN 100
set vlan 100 rspan name VLAN0100 state active
!
#Defines VACL TCP-TRAFFIC that matches TCP traffic
#destined to ports 5000 – 6000
set security acl ip TCP-TRAFFIC permit tcp any any range 5000 6000
!
#Commits the VACL to the hardware
commit security acl TCP-TRAFFIC
!
#Maps the VACL to the RSPAN VLAN
set security acl map TCP-TRAFFIC 100
!
#Defines the RSPAN source as bidirectional traffic on VLANs 10 and 20
set rspan source 10,20 100 both multicast enable create
!
#Defines the RSPAN destination as port 4/5
set rspan destination  4/5  100  inpkts disable learning enable create

************************

! Cisco IOS Configuration on MSFC2:
!
hostname Switch_A_MSFC2
!
! Defines L3 VLANs (SVIs) 10 and 20
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
 ip address 10.20.20.1 255.255.255.0
```

Example 2—Using RSPAN and VACLs on Multiple Switches

Consider the scenario shown in Figure 2.

Figure 2
Using RSPAN and VACLs on Multiple Switches



In this example, there are hosts in two different VLANs, VLAN 10 and VLAN 20, but this time they are on different access-layer switches. The network administrator wants to capture bidirectional traffic from these VLANs to a network analyzer located on interface GigabitEthernet4/5 on a third distribution-layer switch located in another building. In addition, the only traffic the administrator is interested in is TCP traffic destined to a specific range of ports, 5000–6000.

With traditional local SPAN, this is not possible. The administrator must visit each particular switch where traffic collection is required and use local SPAN and a local traffic analyzer to capture the necessary traffic.

RSPAN removes the requirement that the SPAN source and the SPAN destination be on the same switch. The administrator defines an RSPAN VLAN and then configures RSPAN source sessions on one or both of the access-layer switches. The RSPAN destination is configured on the distribution switch, where the network analyzer is attached.

One downside of RSPAN is that any traffic that needs to be captured from the access-layer switch to the distribution-layer switch must be carried across the trunk port and therefore consumes bandwidth. As such, it is generally unwise to mirror huge amounts of traffic using RSPAN if bandwidth is a consideration.

VACLs combined with RSPAN are extremely useful in this case. RSPAN traffic can be filtered at the access-layer switches or at the distribution-layer switch or both, reducing the number of packets transported over the wiring closet uplinks.

Configuration Example 2 Using Cisco IOS Software and Cisco Catalyst OS Software

The following configuration was used to achieve the results described in this example:

- *Distribution switch*—Supervisor Engine 2 with MSFC2 using Cisco IOS Software Release 12.1(13)E4 on the supervisor engine
- *Access switches*—Supervisor Engine 2 using Cisco Catalyst OS Software Release 7.5(1) on the supervisor engine

Distribution Switch Configuration

```
#Cisco IOS Configuration on Distribution Switch:
!
hostname Distribution
!
! Defines L2 VLANs 10 and 20
vlan 10,20
!
! Defines VLAN 100 as the RSPAN VLAN
vlan 100
 remote-span
!
! The monitor port requires no special configuration
interface GigabitEthernet4/5
 description Monitor Port
 no ip address
!
! Configures a Layer 2 802.1Q trunk that carries VLANs 10 and 100
interface GigabitEthernet4/10
 description Trunk to Access Switch A
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,100
!
! Configures a Layer 2 802.1Q trunk that carries VLANs 20 and 100
interface GigabitEthernet4/11
 description Trunk to Access Switch B
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,100
!
! Defines L3 VLANs 10 and 20
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
 ip address 10.20.20.1 255.255.255.0

! VACLs require that a corresponding SVI (L3 interface) exist
! It can remain unconfigured and administratively shutdown
interface Vlan100
 description RSPAN VLAN - Must exist for VACL on RSPAN VLAN
```

```
 no ip address
 shutdown
!
! The IP extended ACL that matches TCP traffic destined to ports 5000 – 6000
ip access-list extended TCP-TRAFFIC
 permit tcp any any range 5000 6000
!
! Defines the VLAN access-map (VACL)
vlan access-map RSPAN-VACL 10
 match ip address TCP-TRAFFIC
 action forward
!
! Maps the VACL to the RSPAN VLAN
vlan filter RSPAN-VACL vlan-list 100
!
! Monitor session 1 captures bidirectional traffic from
! VLANs 10 and 20 to RSPAN VLAN 100
monitor session 1 source vlan 10 , 20
monitor session 1 destination remote vlan 100
!
! Monitor session 2 captures bidirectional traffic from
! RSPAN VLAN 100 to interface gig4/5
monitor session 2 source remote vlan 100
monitor session 2 destination interface Gi4/5
```

Access Switch A Configuration

```
#Catalyst OS Configuration:
!
set system name Access_A
!
#Defines L2 VLAN 10
set vlan 10
!
#Defines RSPAN VLAN 100
set vlan 100 rspan name VLAN0100 state active
!
#Creates an 802.1Q trunk on 1/1 with only VLAN 10 and
#VLAN 100 in the allowed list
clear trunk 1/1  1-9,11-99,101-1005,1025-4094
set trunk 1/1  desirable dot1q 10,100
!
#Defines VACL TCP-TRAFFIC that matches TCP traffic
#destined to ports 5000 – 6000
set security acl ip TCP-TRAFFIC permit tcp any any range 5000 6000
!
#Commits the VACL to the hardware
commit security acl TCP-TRAFFIC
!
#Maps the VACL to the RSPAN VLAN
set security acl map TCP-TRAFFIC 100
!
#Defines the RSPAN source as bidirectional traffic on VLAN 10
set rspan source 10 100 both multicast enable create
```

Access Switch B Configuration

```
#Catalyst OS Configuration:
!
set system name Access_B
!
#Defines L2 VLAN 20
set vlan 20
!
#Defines RSPAN VLAN 100
set vlan 100 rspan name VLAN0100 state active
!
#Creates an 802.1Q trunk on 1/1 with only VLAN 20 and
#VLAN 100 in the allowed list
clear trunk 4/11 1-19,21-99,101-1005,1025-4094
set trunk 4/11 desirable dot1q 20,100
!
#Defines VACL TCP-TRAFFIC that matches TCP traffic
#destined to ports 5000 – 6000
set security acl ip TCP-TRAFFIC permit tcp any any range 5000 6000
!
#Commits the VACL to the hardware
commit security acl TCP-TRAFFIC
!
#Maps the VACL to the RSPAN VLAN
set security acl map TCP-TRAFFIC 100
!
#Defines the RSPAN source as bidirectional traffic on VLAN 20
set rspan source 20 100 both multicast enable create
```

Configuration Example 2 Using Cisco Catalyst OS Software

The following configuration was used to achieve the results described in this example:

- *Distribution switch*—Supervisor Engine 2 with MSFC2 using Cisco Catalyst OS Software Release 7.5(1) on the supervisor engine and Cisco IOS Software Release 12.1(13)E4 on the MSFC2
- *Access switches*—Supervisor Engine 2 using Cisco Catalyst OS Software Release 7.5(1) on the supervisor engine

In this case, security ACLs are defined for the RSPAN VLAN on each access switch to prevent unwanted traffic from traversing the wiring closet uplinks. Therefore, no VACL is configured on the distribution switch because no additional filtering is desired.

Note: The Cisco Catalyst OS configurations on Access Switch A and Access Switch B are the same as in the previous section, “Configuration Example 2 Using Cisco IOS Software and Cisco Catalyst OS Software.”

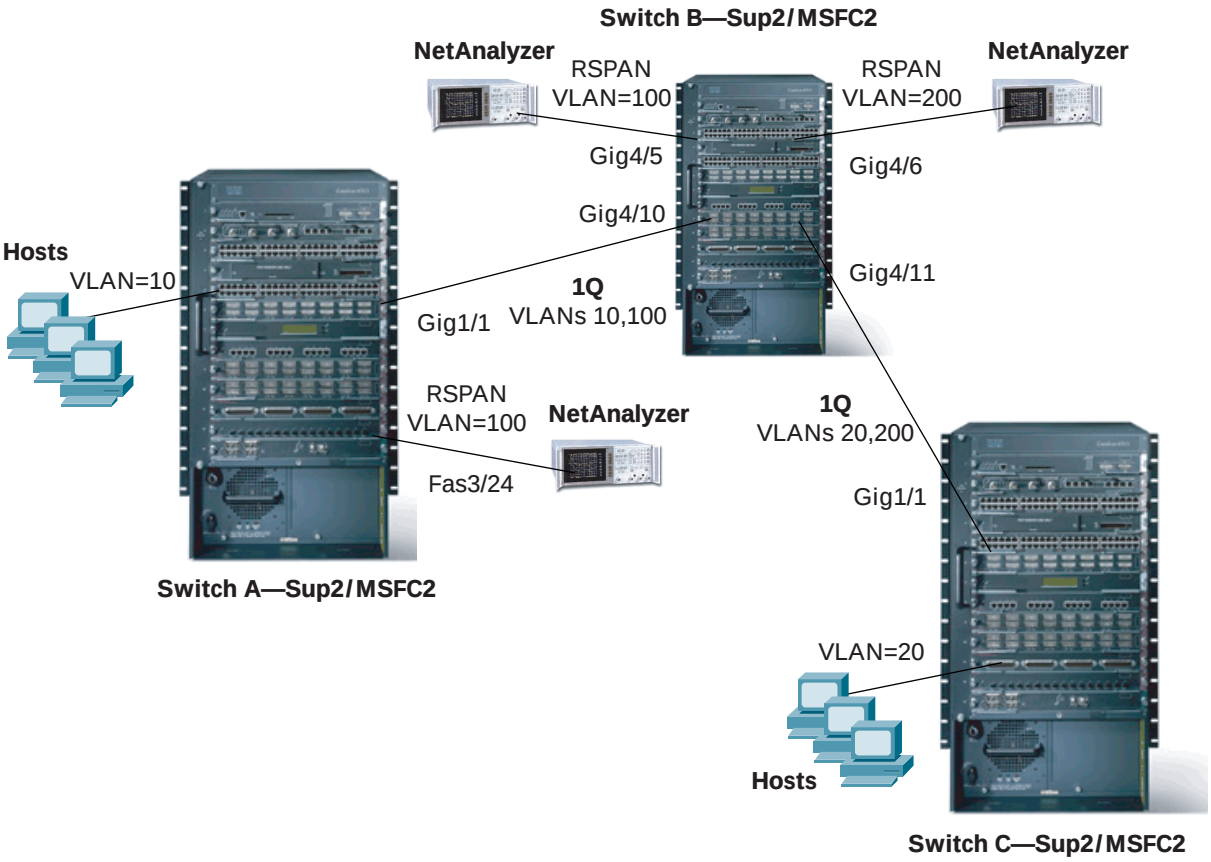
Distribution Switch Configuration

```
#Catalyst OS Configuration on Distribution Switch:
!
set system name Distribution
!
#Defines L2 VLANs 10 and 20
set vlan 10,20
!
#Defines RSPAN VLAN 100
set vlan 100 rspan name VLAN0100 state active
!
#Creates an 802.1Q trunk on 4/10 with only VLAN 10 and
#VLAN 100 in the allowed list
clear trunk 4/10 1-9,11-99,101-1005,1025-4094
set trunk 4/10 desirable dot1q 10,100
!
#Creates an 802.1Q trunk on 4/11 with only VLAN 20 and
#VLAN 100 in the allowed list
clear trunk 4/11 1-19,21-99,101-1005,1025-4094
set trunk 4/11 desirable dot1q 20,100
!
# Defines the RSPAN destination as port 4/5
set rspan destination  4/5  100  inpkts disable learning enable create

************************

! Cisco IOS Configuration on Distribution Switch MSFC2:
!
hostname Dist_MSFC2
!
! Defines L3 VLANs (SVIs) 10 and 20
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
 ip address 10.20.20.1 255.255.255.0
```

Example 3—Using Multiple RSPAN Sessions with VACLs on Multiple Switches

Consider the scenario illustrated in Figure 3.

Figure 3
Using Multiple RSPAN Sessions with VACLs on Multiple Switches



In this example, there are multiple network administrator requirements:

- HTTP traffic sourced from a range of hosts in VLAN 20 to a specific server in VLAN 10 needs to be captured from Switch A (in the “transmit” direction) to an analyzer on interface GigabitEthernet4/5 on Switch B
- Multicast User Datagram Protocol (UDP) traffic in the transmit direction destined for group address 239.0.0.100 needs to be captured from VLAN 10 on Switch A to an analyzer on interface FastEthernet3/24 on the same switch
- Bidirectional TCP traffic sourced from hosts in VLAN 20 with destination ports in the range of 5000–6000 needs to be captured from Switch C to an analyzer on interface GigabitEthernet4/6 on Switch B

Given the complexity of the requirements, the corresponding configurations are more involved. To satisfy items 1 and 2, a single RSPAN source is configured on Switch A to send traffic to RSPAN VLAN 100. The VACL for RSPAN VLAN 100 on Switch A must permit both the required HTTP traffic and the required multicast UDP traffic. A local RSPAN destination is configured on Switch A, and another RSPAN destination is configured on Switch B for RSPAN VLAN 100. Note that the network analyzer on Switch A will receive both the HTTP and the multicast UDP packets.

An additional VACL configured on Switch B can be used to prevent the analyzer on interface GigabitEthernet4/5 from receiving the UDP traffic, but realize that the UDP traffic *will* pass over the trunk from Switch A to Switch B before being dropped at Switch B.

Item 3 requires a second RSPAN VLAN, VLAN 200. An RSPAN source is configured on Switch C along with a VACL for VLAN 200 to drop all but the required TCP traffic. An RSPAN destination session for VLAN 200 is required on Switch B, but no additional filtering is required because of the VACL applied on Switch C.

Configuration Example 3 Using Cisco IOS Software

The following configurations were used to achieve the results described in this example with all switches using Supervisor Engine 2 with MSFC2, using Cisco IOS Software Release 12.1(13)E4 on the supervisor engine.

Switch A Configuration

```
#Cisco IOS Configuration on Switch A:
!
hostname Switch_A
!
! Defines L2 VLAN 10
vlan 10
!
! Defines VLAN 100 as the RSPAN VLAN
vlan 100
 remote-span
!
! Configures a Layer 2 802.1Q trunk that carries VLANs 10 and 100
interface GigabitEthernet1/1
 description Trunk to Switch B
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,100
!
! The monitor port requires no special configuration
interface FastEthernet3/24
 description Monitor Port
 no ip address
 switchport
!
! VACLs require that a corresponding SVI (L3 interface) exist
! It can remain unconfigured and administratively shutdown
interface Vlan100
 description RSPAN VLAN - Must exist for VACL on RSPAN VLAN
 no ip address
 shutdown
!
! The IP extended ACL that matches HTTP traffic from a group of hosts
! to a specific server AND multicast UDP traffic to group 239.0.0.100
ip access-list extended HTTP_&_UDP
 permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
 permit udp any host 239.0.0.100
!
! Defines the VLAN access-map (VACL)
vlan access-map RSPAN-FILTER 10
 match ip address HTTP_&_UDP
```

```
 action forward
!
! Maps the VACL to RSPAN VLAN 100
vlan filter RSPAN-FILTER vlan-list 100
!
! Monitor session 1 captures transmit direction traffic from
! VLAN 10 to RSPAN VLAN 100
monitor session 1 source vlan 10 tx
monitor session 1 destination remote vlan 100
!
! Monitor session 2 captures traffic from RSPAN VLAN 100
! to interface fast3/24
monitor session 2 source remote vlan 100
monitor session 2 destination interface Fa3/24
```

Switch B Configuration

```
#Cisco IOS Configuration on Switch B:
!
hostname Switch_B
!
! Defines L2 VLANs 10 and 20
vlan 10,20
!
! Defines VLAN 100 as an RSPAN VLAN
vlan 100
 remote-span
!
! Defines VLAN 200 as an RSPAN VLAN
vlan 200
 remote-span
!
! Enables IP multicast routing
ip multicast-routing
!
! Defines the PIM sparse mode Rendezvous Point
ip pim rp-address 10.10.10.1
!
! The monitor port requires no special configuration
interface GigabitEthernet4/5
 description Monitor Port RSPAN VLAN 100
 no ip address
!
! The monitor port requires no special configuration
interface GigabitEthernet4/6
 description Monitor Port RSPAN VLAN 200
 no ip address
!
! Configures a Layer 2 802.1Q trunk that carries VLANs 10 and 100
interface GigabitEthernet4/10
 description Trunk to Switch A
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,100
!
! Configures a Layer 2 802.1Q trunk that carries VLANs 20 and 200
interface GigabitEthernet4/11
```

```
 description Trunk to Switch C
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,200
!
! Defines L3 VLANs (SVIs) 10 and 20 and enables PIM on each
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface Vlan20
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-dense-mode
!
! VACLs require that a corresponding SVI (L3 interface) exist
! It can remain unconfigured and administratively shutdown
interface Vlan100
 description RSPAN VLAN - Must exist for VACL on RSPAN VLAN
 no ip address
 shutdown
!
! The IP extended ACL that matches any TCP traffic (to further
! filter the RSPAN traffic in VLAN 100)
ip access-list extended JUST-TCP
 permit tcp any any
!
! Defines the VLAN access-map (VACL)
vlan access-map RSPAN-100-FILTER 10
 match ip address JUST-TCP
 action forward
!
! Maps the VACL to RSPAN VLAN 100
vlan filter RSPAN-100-FILTER vlan-list 100
!
! Monitor session 1 captures traffic from RSPAN VLAN 100
! to interface gig4/5
monitor session 1 source remote vlan 100
monitor session 1 destination interface Gi4/5
!
! Monitor session 2 captures traffic from RSPAN VLAN 200
! to interface gig4/6
monitor session 2 source remote vlan 200
monitor session 2 destination interface Gi4/6
```

Switch C Configuration

```
#Cisco IOS Configuration on Switch C:
!
hostname Switch_C
!
! Defines L2 VLAN 20
vlan 20
!
! Defines VLAN 200 as the RSPAN VLAN
vlan 200
 remote-span
!
```

```
! Configures a Layer 2 802.1Q trunk that carries VLANs 20 and 200
interface GigabitEthernet1/1
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,200
!
! VACLs require that a corresponding SVI (L3 interface) exist
! It can remain unconfigured and administratively shutdown
interface Vlan200
 description RSPAN VLAN - Must exist for VACL on RSPAN VLAN
 no ip address
 shutdown
!
! The IP extended ACL that matches any TCP traffic destined
! to ports from 5000 – 6000
ip access-list extended TCP-TRAFFIC
 permit tcp any any range 5000 6000
!
! Defines the VLAN access-map (VACL)
vlan access-map RSPAN-VACL 10
 match ip address TCP-TRAFFIC
 action forward
!
! Maps the VACL to RSPAN VLAN 200
vlan filter RSPAN-VACL vlan-list 200
!
! Monitor session 1 captures bidirectional traffic from VLAN 20
! to RSPAN VLAN 200
monitor session 1 source vlan 20
monitor session 1 destination remote vlan 200
```

Configuration Example 3 Using Cisco Catalyst OS Software

The following configurations were used to achieve the results described in this example with all switches using Supervisor Engine 2 with MSFC2 using Cisco Catalyst OS Software Release 7.5(1) on the supervisor engine and Cisco IOS Software Release 12.1(13)E4 on the MSFC2. Only the MSFC2 on Switch B is used in this example.

Switch A Configuration

```
#Catalyst OS Configuration on Switch A:
!
set system name  Switch_A
!
#Defines L2 VLAN 10
set vlan 10
!
#Defines RSPAN VLAN 100
set vlan 100 rspan name VLAN0100 state active
!
#Creates an 802.1Q trunk on 1/1 with only VLAN 10 and
#VLAN 100 in the allowed list
clear trunk 1/1  1-9,11-99,101-1005,1025-4094
set trunk 1/1  desirable dot1q 10,100
!
#Defines VACL RSPAN-FILTER that matches HTTP traffic from a group of hosts
#to a specific server AND multicast UDP traffic to group 239.0.0.100
```

```
set security acl ip RSPAN-FILTER permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq 80
set security acl ip RSPAN-FILTER permit udp any host 239.0.0.100
!
#Commits the VACL to the hardware
commit security acl RSPAN-FILTER
!
#Maps the VACL to RSPAN VLAN 100
set security acl map RSPAN-FILTER 100
!
#Defines the RSPAN 100 source as transmit direction traffic on VLAN 10
set rspan source 10 100 tx multicast enable create
!
#Defines the RSPAN 100 destination as port 3/24
set rspan destination  3/24  100  inpkts disable learning enable create
```

Switch B Configuration

```
#Catalyst OS Configuration on Switch B:
!
set system name  Switch_B
!
#Defines L2 VLANs 10 and 20
set vlan 10,20
!
#Defines RSPAN VLANs 100 and 200
set vlan 100 rspan name VLAN0100 state active
set vlan 200 rspan name VLAN0200 state active
!
#Creates an 802.1Q trunk on 4/10 with only VLAN 10 and
#VLAN 100 in the allowed list
clear trunk 4/10 1-9,11-99,101-1005,1025-4094
set trunk 4/10 desirable dot1q 10,100
!
#Creates an 802.1Q trunk on 4/11 with only VLAN 20 and
#VLAN 200 in the allowed list
clear trunk 4/11 1-19,21-199,201-1005,1025-4094
set trunk 4/11 desirable dot1q 20,200
!
#Defines VACL JUST-TCP that matches any TCP traffic (to further
#filter the RSPAN traffic in VLAN 100)
set security acl ip JUST-TCP permit tcp any any
!
#Commits the VACL to the hardware
commit security acl JUST-TCP
!
#Maps the VACL to RSPAN VLAN 100
set security acl map JUST-TCP 100
!
#Defines the RSPAN 200 destination as port 4/6
set rspan destination  4/5  100  inpkts disable learning enable create
!
#Defines the RSPAN 200 destination as port 4/6
set rspan destination  4/6  200  inpkts disable learning enable create

************************

! Cisco IOS Configuration on Switch B MSFC2:
!
```

```
hostname Switch_B_MSFC2
!
! Enables IP multicast routing
ip multicast-routing
!
! Defines the PIM sparse mode Rendezvous Point
ip pim rp-address 10.10.10.1
!
! Defines L3 VLANs (SVIs) 10 and 20 and enables PIM on each
interface Vlan10
 ip address 10.10.10.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface Vlan20
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-dense-mode
```

Switch C Configuration

```
#Catalyst OS Configuration on Switch C:
!
set system name  Switch_C
!
#Defines L2 VLAN 20
set vlan 20
!
#Defines RSPAN VLAN 200
set vlan 200 rspan name VLAN0200 state active
!
#Creates an 802.1Q trunk on 1/1 with only VLAN 20 and
#VLAN 200 in the allowed list
clear trunk 1/1 1-19,21-199,201-1005,1025-4094
set trunk 1/1 desirable dot1q 20,200
!
#Defines VACL TCP-5000-6000 that matches any TCP traffic destined
#to ports from 5000 – 6000
set security acl ip TCP-5000-6000 permit tcp any any range 5000 6000
!
#Commits the VACL to the hardware
commit security acl TCP-5000-6000
!
#Maps the VACL to RSPAN VLAN 200
set security acl map TCP-5000-6000 200
!
#Defines the RSPAN 200 source as VLAN 20
set rspan source 20 200 both multicast enable create
```

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

MH/LW4457 0503