Table of Contents

Configuring the Catalyst Switched Port Analyzer (SPAN)

Introduction

The Switched Port Analyzer (SPAN) feature, sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. Previously, SPAN was a relatively basic feature on the Catalyst family of switches, but the latest releases of the CatOS introduced great enhancements and many new possibilities that are now available to the user. This document is not intended to be an alternate configuration guide for the SPAN feature, but rather an introduction to the recent features of SPAN that have been implemented. This document answers the most common questions about SPAN, such as:

- What is SPAN and how do I configure it?
- What are the different features available (especially multiple SPAN sessions at the same time) and what software level is needed to run them?
- Does SPAN impact the performances of a switch?

Before You Begin

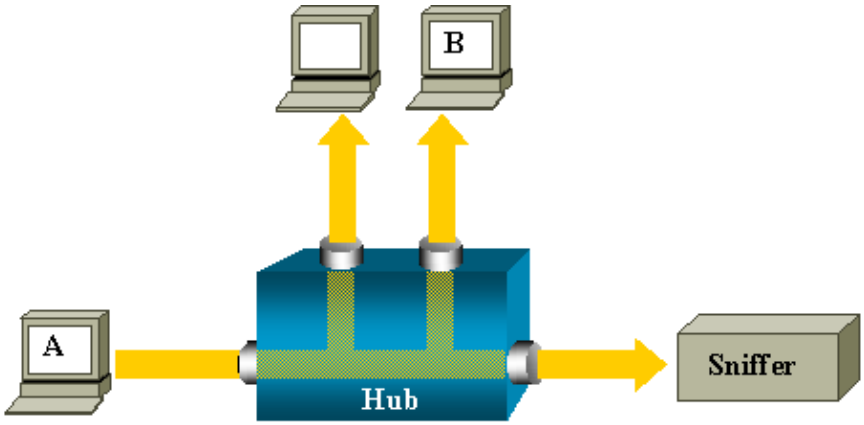
Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

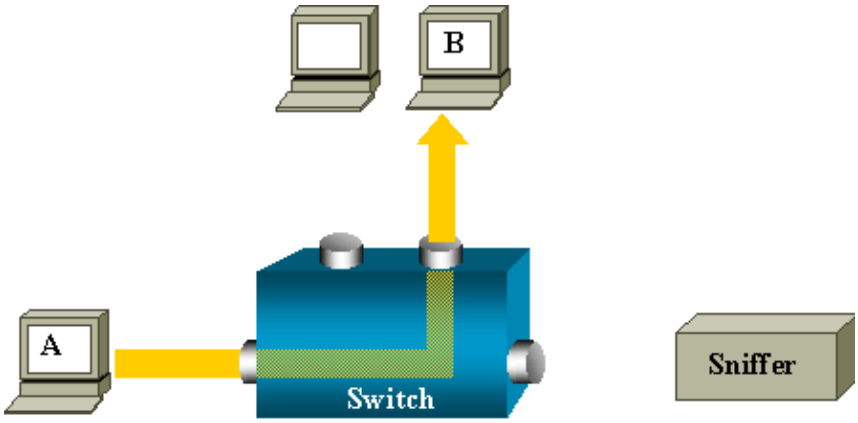
Brief Description of SPAN

What is SPAN and why is it needed? The SPAN feature was introduced on switches because of a fundamental difference they have with hubs. When a hub receives a packet on one port, it will send out a copy of that packet on all ports except on the one where it was received. After a switch boots up, it will start to build up a Layer 2 forwarding table based upon the source MAC address of the different packets received. Once this forwarding table has been built, the switch forwards traffic destined for a MAC address directly to the corresponding port.

For example, if you want to capture Ethernet traffic sent by host A to host B and both are connected to a hub, just attach a sniffer to this hub as all other ports see the traffic between host A and B:

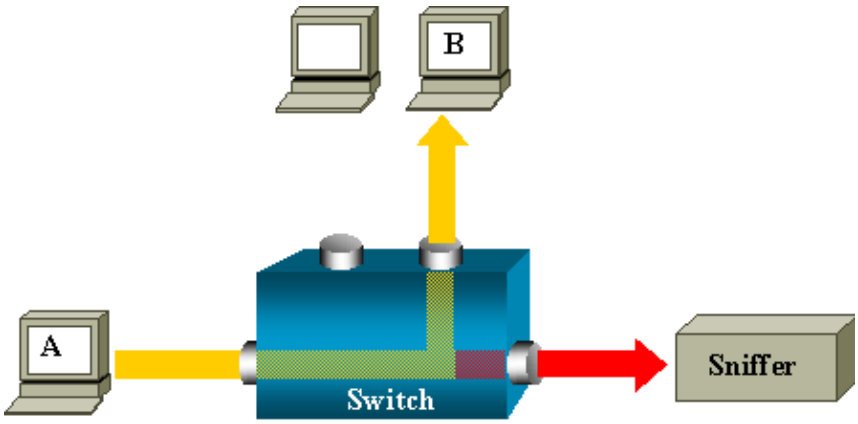


On a switch, after host B's MAC address is learned, unicast traffic from A to B is only forwarded to B's port, and therefore not seen by the sniffer:



In this configuration, the sniffer would only capture traffic flooded to all ports like broadcast traffic, multicast traffic with CGMP or IGMP snooping disabled and unknown unicast traffic. Unicast flooding happens when the switch does not have the destination MAC in its CAM table. It will not know where to send the traffic and it will flood the packets to all the ports in the destination VLAN.

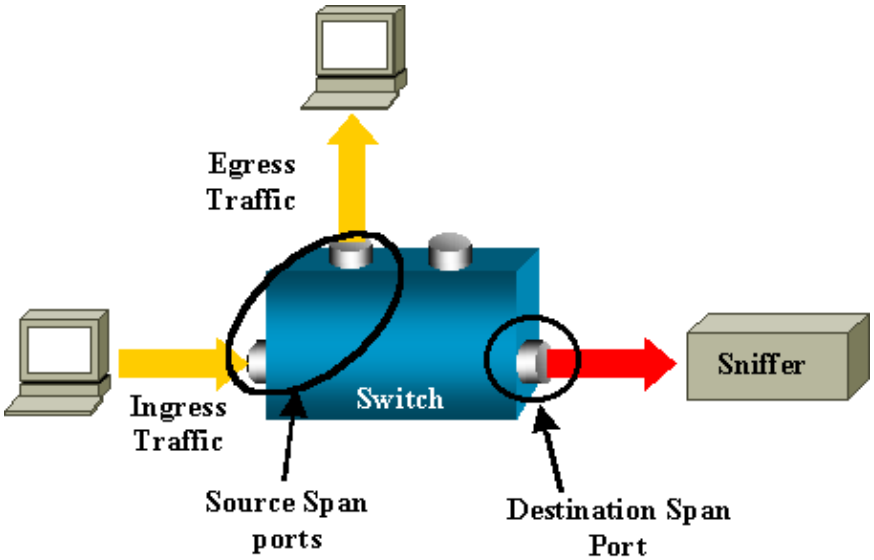
An extra feature is needed that will artificially copy unicast packets sent by host A to the sniffer port:



In this above diagram, the sniffer is attached to a port that is configured to receive a copy of every single packet that is sent by host A. This port is called a SPAN port. The sections below describe how this feature can be tuned very precisely to do more than just monitoring a port.

SPAN Terminology

- **Ingress traffic:** traffic entering the switch
- **Egress traffic:** traffic leaving the switch
- **Source (SPAN) Port:** port that is monitored using the SPAN feature.
- **Destination (SPAN) Port:** a port that is monitoring source ports, usually where a network analyzer is connected.
- **Monitor Port:** a monitor port is also a destination SPAN port in Catalyst 2900XL/3500XL/2950 terminology.



- **Local SPAN:** the SPAN feature is local when the monitored ports are all located on the same switch as the destination port. This is in contrast to Remote SPAN below:
- **Remote SPAN or RSPAN:** some source ports are not located on the same switch as the destination port. This is an advanced feature that requires a special VLAN to carry the traffic being monitored by SPAN between switches. RSPAN is not supported on all switches so please check the respective release notes or configuration guide to see if it can be used on the switch you are deploying.

- **PSPAN:** stands for port−based SPAN. The user specifies one or several source ports on the switch and one destination port.
- **VSPAN:** stands for VLAN−based SPAN. On a given switch, the user can choose to monitor all the ports belonging to a particular VLAN in a single command.
- **ESPAN** means enhanced SPAN version. This term has been used several times during the evolution of the SPAN to name additional features and, therefore, is not very clear. Its use is avoided in this document.
- **Administrative Source:** List of source ports or VLANs that have been configured to be monitored.
- **Operational Source:** List of ports that are effectively monitored. This can be different from the administrative source. For example, a port that is in shutdown mode can appear in the administrative source, while it will not be effectively monitored.

Components Used

This document uses CatOS 5.5 as a reference for the Catalyst 4000, 5000, and 6000 families. On the Catalyst 2900XL/3500XL family, Cisco IOS® Software Release 12.0(5)XU is used. Though this document will be updated to reflect changes to SPAN, see the documentation release notes for the latest developments on the SPAN feature.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

SPAN on the Catalyst 2900XL/3500XL Switches

Features Available and Restrictions

The port monitoring feature is not very extended on the Catalyst 2900XL/3500XL and is therefore relatively easy to understand.

You can create as many local PSPAN sessions as necessary. For example, you can create PSPAN sessions on the configuration port that you have chosen to be a destination SPAN port; just list the source ports you would like to monitor using the **port monitor *interface*** command. A monitor port is actually a destination SPAN port in Catalyst 2900XL/3500XL terminology.

- The main restriction is that all the ports related to a given session (whether source or destination) must belong to the same VLAN.
- If you do not specify any interface in the port monitor command, all other ports belonging to the same VLAN as the interface will be monitored.

Here are some restrictions that are taken from the Catalyst 2900XL/3500XL Command Reference:

ATM ports are the only ports that cannot be monitor ports. However, you can monitor ATM ports. The following restrictions apply for ports that have port−monitoring capability:

- A monitor port cannot be in a Fast EtherChannel or Gigabit EtherChannel port group.
- A monitor port cannot be enabled for port security.
- A monitor port cannot be a multi−VLAN port.
- A monitor port must be a member of the same VLAN as the port monitored. VLAN membership changes are disallowed on monitor ports and ports being monitored.
- A monitor port cannot be a dynamic−access port or a trunk port. However, a static−access port can

monitor a VLAN on a trunk, a multi−VLAN, or a dynamic−access port. The VLAN monitored is the one associated with the static−access port.
- Port monitoring does not work if both the monitor and monitored ports are protected ports.

See the following links for additional information on feature conflicts:

- Managing Switches − Managing Configuration Conflicts − Catalyst 2900XL/3500XL Series

Be careful that a port in the monitor state is not running the Spanning−Tree Protocol (STP), but is still belonging to the VLAN of the ports it is mirroring. If the port monitor is part of a loop (if you connect it to a hub or a bridge, looping to another part of the network for instance), you may end up in a catastrophic bridging loop condition as you are not protected by the STP any more. See the section entitled Why is My SPAN Session Creating a Bridging Loop? for an example on how this can happen.

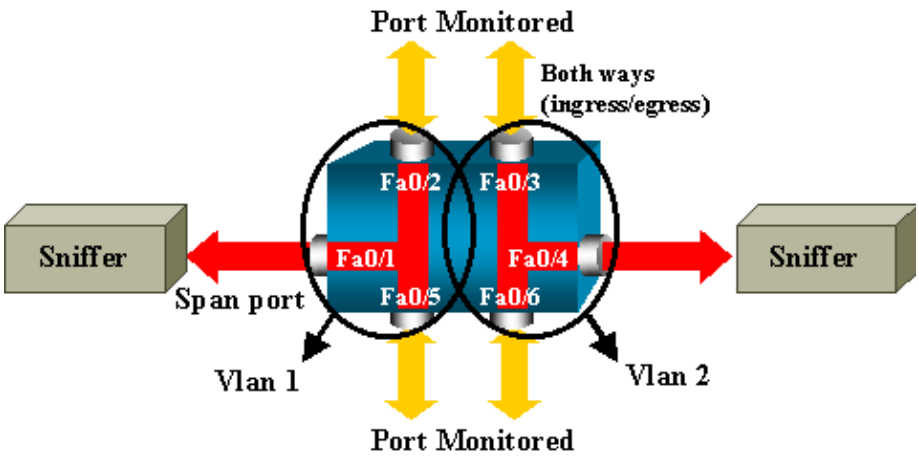
Configuration Example

In this example, two concurrent SPAN sessions are created.

- Port Fa0/1 will be monitoring traffic sent and received by port Fa0/2 and Fa0/5. It will also monitor traffic to and from the management interface VLAN 1.
- Port Fa0/4 will be monitoring ports Fa0/3 and Fa0/6.

Ports Fa0/3, Fa0/4, and Fa0/6 are all configured in VLAN 2; other ports and the management interface are configured in the default VLAN 1.

Network Diagram



Sample Configuration on the Catalyst 2900XL/3500XL

2900XL/3500XL SPAN Sample Configuration

`<snip>`
`!`
`interface FastEthernet0/1`
`port monitor FastEthernet0/2`
`port monitor FastEthernet0/5`
`port monitor VLAN1`
`!`
`interface FastEthernet0/2`
`!`

```
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
 port monitor FastEthernet0/3
 port monitor FastEthernet0/6
 switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 2
!
<snip>
!
interface VLAN1
 ip address 10.200.8.136 255.255.252.0
 no ip directed-broadcast
 no ip route-cache
!
<snip>
```

Configuration Steps Explained

To configure port Fa0/1 as a destination port on the source ports Fa0/2, Fa0/5, and the management interface, select the interface Fa0/1 in the configuration mode:

```
Switch(config)#int fa0/1
```

Enter the list of ports to be monitored:

```
Switch(config-if)#port monitor fastEthernet 0/2
Switch(config-if)#port monitor fastEthernet 0/5
```

With this, every packet received or transmitted by these two ports is also be copied to port Fa0/1. Configure the monitoring for the administrative interface, using a variation on the **port monitor** command:

```
Switch(config-if)#port monitor VLAN 1
```

Note: The command above does not mean that port Fa0/1 will monitor the entire VLAN 1. The VLAN 1 keyword is simply referring to the administrative interface of the switch.

The following command has just been entered to illustrate the impossibility of monitoring a port in a different VLAN:

```
Switch(config-if)#port monitor fastEthernet 0/3
FastEthernet0/1 and FastEthernet0/3 are in different vlan
```

To finish the configuration, configure another session, this time using Fa0/4 as a destination SPAN port:

```
Switch(config-if)#int fa0/4
Switch(config-if)#port monitor fastEthernet 0/3
Switch(config-if)#port monitor fastEthernet 0/6
Switch(config-if)#^Z
```

The best way to check the configuration is to issue a simple **show running**, or to use the **show port monitor** command:

```
Switch#show port monitor
Monitor Port Port Being Monitored
------------------- --------------------
FastEthernet0/1 VLAN1
FastEthernet0/1 FastEthernet0/2
FastEthernet0/1 FastEthernet0/5
FastEthernet0/4 FastEthernet0/3
FastEthernet0/4 FastEthernet0/6
```

Note: The Catalyst 2900XL and 3500XL do not support SPAN in receive direction only (Rx SPAN or ingress SPAN), or in tranmsit direction only (Tx SPAN or egress SPAN). All ports are spanned for both receive (Rx) and transmit (Tx) traffic.

SPAN on the Catalyst 2948G−L3 and 4908G−L3

The Catalyst 2948G−L3 and 4908G−L3 are fixed−configuration switch−routers or Layer 3 switches. The SPAN feature on a Layer 3 switch is called port snooping. However, port snooping is not supported on these switches. Refer to Features Not Supported on the Catalyst 2948G−L3 and the Catalyst 4908G−L3 Switch Routers and the latest release notes for the Catalyst 2948G−L3.

SPAN on the Catalyst 8500

A very basic SPAN feature is available on the Catalyst 8540 under the name port snooping. Check the current Catalyst 8540 documentation for additional information:

- Catalyst 8500 Command Reference
- About Port Snooping (from the Layer 3 Switching Interface Configurations Guide)

Here is an excerpt from the command reference:

Port snooping lets you transparently mirror traffic from one or more source ports to a destination port.

To set up port−based traffic mirroring, or snooping, use the **snoop** command. To disable snooping, use the no form of this command.

snoop interface *source−port*direction *snoop−direction*

no snoop interface *source−port*

Source−port refers to the port being monitored and snoop−direction is the direction of traffic on the source port or ports that is monitored: receive, transmit, or both.

```
8500CSR# configure terminal
8500CSR(config)# interface fastethernet 12/0/15
8500CSR(config−if)# shutdown
8500CSR(config−if)# snoop interface fastethernet 0/0/1 direction both
8500CSR(config−if)# no shutdown
```

The following example shows output from the **show snoop** command.

```
8500CSR# show snoop
Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option:         (configured=enabled)(actual=enabled)
```

```
Snoop direction:      (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```

Note: This command is not supported on Ethernet ports in a Catalyst 8540 if you are running an MSR image, such as 8540m−in−mz. Instead, you must use a CSR image, such as 8540c−in−mz. When running an MSR image, snooping is supported only on ATM interfaces by issuing the following commands:

- **atm snoop**
- **atm snoop−vp**
- **atm snoop−vc**

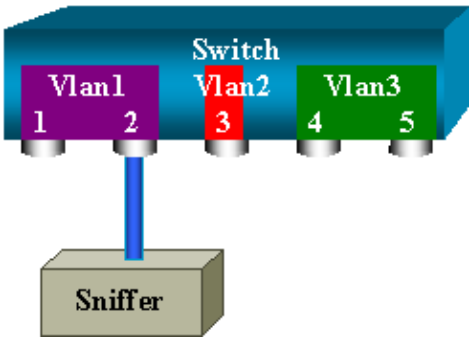
SPAN on the Catalyst 4000, 5000, and 6000 Series Switches Running CatOS

Local SPAN

SPAN features have been added one by one to the CatOS, and a SPAN configuration consists of a single set span command. There is now a wide range of options available for the command:

```
switch (enable) set span
Usage: set span disable [dest_mod/dest_port|all]
       set span <src_mod/src_ports...|src_vlans...|sc0>
              <dest_mod/dest_port> [rx|tx|both]
              [inpkts <enable|disable>]
              [learning <enable|disable>]
              [multicast <enable|disable>]
              [filter <vlans...>]
              [create]
```

The different SPAN possibilities using variations are introduced on the following network diagram:

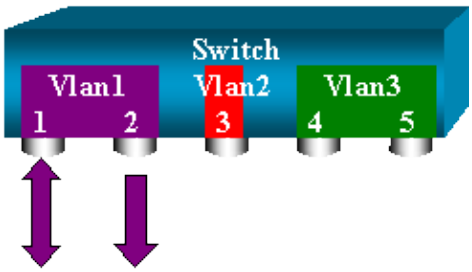


This diagram represents part of a single line card located in slot 6 of a Catalyst 6000 switch. Ports 6/1 and 6/2 belong to VLAN 1, port 6/3 belongs to VLAN 2, and ports 6/4 and 6/5 belong to VLAN 3. Connect a sniffer to port 6/2 and use it as a monitor port in several different cases.

PSPAN, VSPAN: Monitoring Some Ports or an Entire VLAN

The simplest form of the **set span** command is used to monitor a single port. The syntax is: **set span** ***source port destination port***

Monitoring a Single Port with SPAN

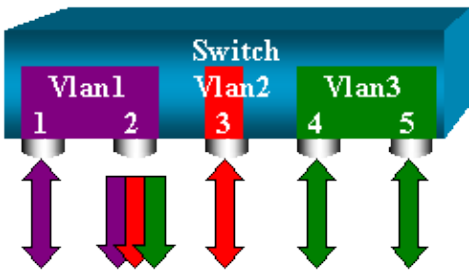



```
switch (enable) set span 6/1 6/2

Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

With this configuration, every packet received or sent by port 6/1 will be copied on port 6/2. This is clearly described when the configuration is entered. To get a summary of the current SPAN configuration, just use the show span command:

```
switch (enable) show span
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active

Total local span sessions: 1
```

Monitoring Several Ports with SPAN



The **set span** ***source ports destination port*** allows the user to specify more than one source port. Just list all the ports on which you want to implement the SPAN, separated by commas. The command line interpreter also allows you to specify a range of ports by using the hyphen. The following example illustrates this ability: SPAN on port 6/1 and a range of three ports starting from 6/3 is used. There can only be one destination port, and it is always specified after the SPAN source.

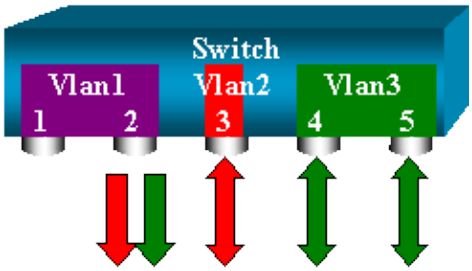
```
switch (enable) set span 6/1,6/3-5 6/2

2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
      for destination port 6/2
      Destination : Port 6/2
      Admin Source : Port 6/1,6/3-5
      Oper Source : Port 6/1,6/3-5
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : -
      Status : active
      switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
      session active for destination port 6/2
```

Note: Unlike the Catalysts 2900XL/3500XL, the Catalyst 4000/5000/6000 can monitor ports belonging to several different VLANs earlier than CatOS 5.1. Here, the mirrored ports are assigned to VLAN 1,2, and 3.

Monitoring VLANs with SPAN

Eventually, the **set span** command allows you to simply configure a port to monitor local traffic for an entire VLAN: **set span** ***source vlan(s) destination port*** .

Instead of a list of port, just use a list of one or more VLANs as a source:




```
switch (enable) set span 2,3 6/2
          2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
          for destination port 6/2
          Destination : Port 6/2
          Admin Source : VLAN 2-3
          Oper Source : Port 6/3-5,15/1
          Direction : transmit/receive
          Incoming Packets: disabled
          Learning : enabled
          Multicast : enabled
          Filter : -
          Status : active
          switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
          session active for destination port 6/2
```

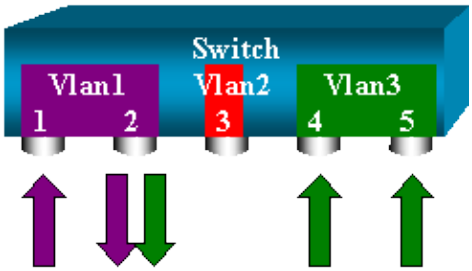
With the above configuration, every single packet entering or leaving VLAN 2 or 3 will be duplicated to port 6/2. Note that the result is exactly the same as if you were implementing SPAN individually on all the ports belonging to the VLANs specified in the command. You can see this by comparing the **Oper Source** and the **Admin Source** fields. The Admin Source basically lists all that you have configured for the SPAN session, whereas the Oper Source field lists what ports are using SPAN.

Ingress/Egress SPAN

In the previous example, traffic entering and leaving the specified ports was monitored. You can see this on the field **Direction: transmit/receive**. The Catalyst 4000/5000/6000 range of switch allows you to collect only egress (outbound) or ingress (inbound) traffic on a given port. You just need to add a keyword **rx** (receive) or **tx** (transmit) in the end, the default value being **both** (transmit and receive).

```
set span source destination port rx/tx/both
```

Example: This session capture all incoming traffic for VLAN 1 and 3 and mirrors it to port 6/2:




```
switch (enable) set span 1,3 6/2 rx
          2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span session
          inactive for destination port 6/2
          Destination : Port 6/2
          Admin Source : VLAN 1,3
          Oper Source : Port 1/1,6/1,6/4-5,15/1
          Direction : receive
          Incoming Packets: disabled
          Learning : enabled
          Multicast : enabled
          Filter : -
          Status : active
          switch (enable) 2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span
          session active for destination port 6/2
```

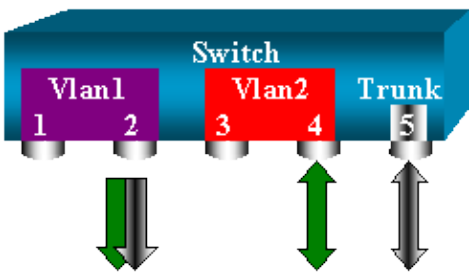
Implementing SPAN on a Trunk

Trunks are a special case in a switch as they are ports carrying several VLANs. If a trunk is selected as a source port, the traffic for all the VLANs on this trunk will be monitored.

Monitoring a Subset of VLANs Belonging to a Trunk

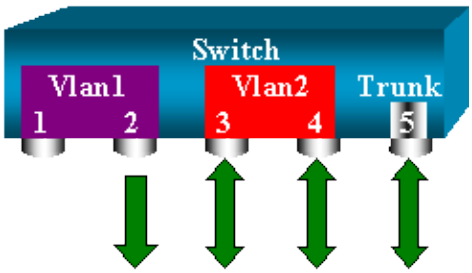
In the following diagram, port 6/5 is now a trunk carrying all VLANs. Imagine you want to SPAN the traffic in VLAN 2 for ports 6/4 and 6/5. Simply use the command:

```
switch (enable) set span 6/4-5 6/2
```



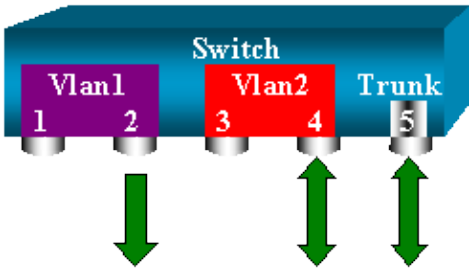
In that case, the traffic received on the SPAN port will be a mix of the traffic you want and all the VLANs carried by trunk 6/5. For instance, there is no way to distinguish on the destination port if a packet is coming from port 6/4 in VLAN 2 or port 6/5 in VLAN 1. Another possibility would be to use SPAN on the entire VLAN 2:

```
switch (enable) set span 2 6/2
```



With this configuration, at least, you will only monitor traffic belonging to VLAN 2 from the trunk. The problem is now you also receive traffic that you did not want from port 6/3. The CatOS includes another keyword allowing you to select some VLAN to monitor from a trunk:

```
switch (enable) set span 6/4-5 6/2 filter 2
      2000 Sep 06 02:31:51 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
      for destination port 6/2
      Destination : Port 6/2
      Admin Source : Port 6/4-5
      Oper Source : Port 6/4-5
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : 2
      Status : active
```



This command will achieve our goal by only selecting VLAN 2 on all the trunks monitored. (Of course, you can specify several VLANs with this filter option).

Note: This filter option is only supported on Catalyst 4000 and Catalyst 6000 Switches. Catalyst 5000 does not support the filter option available with the **set span** command.

Trunking on the Destination Port

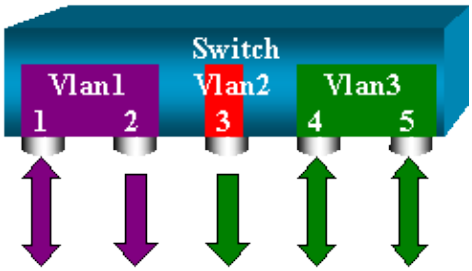
If you have source ports belonging to several different VLANs, or if you are using SPAN on several VLANs on a trunk port, you may want to identify to which VLAN a packet you are receiving on the destination SPAN port belongs. This is possible by enabling trunking on the destination port before configuring it for SPAN. This way, all packets forwarded to the sniffer will also be tagged with their respective VLAN IDs.

Note: Your sniffer needs to recognize the corresponding encapsulation.

```
switch (enable) set span disable 6/2
        This command will disable your span session.
        Do you want to continue (y/n) [n]?y
        Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/4-5
        2000 Sep 06 02:52:22 %SYS-5-SPAN_CFGSTATECHG:local span session
        inactive for destination port 6/2
        switch (enable) set trunk 6/2 nonegotiate isl

        Port(s) 6/2 trunk mode set to nonegotiate.
        Port(s) 6/2 trunk type set to isl.
        switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become isl trun
        switch (enable) set span 6/4-5 6/2
        Destination : Port 6/2
        Admin Source : Port 6/4-5
        Oper Source : Port 6/4-5
        Direction : transmit/receive
        Incoming Packets: disabled
        Learning : enabled
        Multicast : enabled
        Filter : -
        Status : active
        2000 Sep 06 02:53:23 %SYS-5-SPAN_CFGSTATECHG:local span session active for
        destination port 6/2
```

Creating Several Simultaneous Sessions

So far, only a single SPAN session has been created. Each time you enter a new **set span** command, the previous configuration was invalidated. The CatOS now has the ability to run several sessions concurrently, that is, it can have different destination ports at the same time. Use the **set span** ***<source>*** ***<destination>*** **create** command to add an additional SPAN session. In the following session, port 6/1 to 6/2, and at the same time, monitor VLAN 3 to port 6/3 is monitored:




```
switch (enable) set span 6/1 6/2
        2000 Sep 05 08:49:04 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
        for destination port 6/2
        Destination : Port 6/2
        Admin Source : Port 6/1
        Oper Source : Port 6/1
        Direction : transmit/receive
        Incoming Packets: disabled
        Learning : enabled
        Multicast : enabled
        Filter : -
        Status : active
        switch (enable) 2000 Sep 05 08:49:05 %SYS-5-SPAN_CFGSTATECHG:local span
        session active for destination port 6/2
        switch (enable) set span 3 6/3 create
        Destination : Port 6/3
        Admin Source : VLAN 3
```

```
      Oper Source : Port 6/4−5,15/1
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : −
      Status : active
      switch (enable) 2000 Sep 05 08:55:38 %SYS−5−SPAN_CFGSTATECHG:local span
      session active for destination port 6/3
```

Now, check if you have two sessions at the same time by issuing the **show span** command:

```
switch (enable) show span
      Destination : Port 6/2
      Admin Source : Port 6/1
      Oper Source : Port 6/1
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : −
      Status : active
      ------------------------------------------------------------------------
      Destination : Port 6/3
      Admin Source : VLAN 3
      Oper Source : Port 6/4−5,15/1
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : −
      Status : active
      Total local span sessions: 2
```

Now additional sessions have been created. You need a way of deleting some sessions. The command is:

```
set span disable all / destination port
```

A session is identified by its destination port (as there can only be one destination port per session). Delete the first session created, the one that uses port 6/2 as destination:

```
switch (enable) set span disable 6/2
      This command will disable your span session.
      Do you want to continue (y/n) [n]?y
      Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/1
      2000 Sep 05 09:04:33 %SYS−5−SPAN_CFGSTATECHG:local span session inactive
      for destination port 6/2
```

You can now check that you have only one session remaining:

```
switch (enable) show span
      Destination : Port 6/3
      Admin Source : VLAN 3
      Oper Source : Port 6/4−5,15/1
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : −
      Status : active
```

```
    Total local span sessions: 1
```

To disable all the current sessions in a single step, use the command below:

```
switch (enable) set span disable all
      This command will disable all span session(s).
      Do you want to continue (y/n) [n]?y
      Disabled all local span sessions
      2000 Sep 05 09:07:07 %SYS−5−SPAN_CFGSTATECHG:local span session inactive
      for destination port 6/3

    switch (enable) show span
      No span session configured
```

Other SPAN Options

The syntax for the set span command is:

```
switch (enable) set span
Usage: set span disable [dest_mod/dest_port|all]
      set span <src_mod/src_ports...|src_vlans...|sc0>
               <dest_mod/dest_port> [rx|tx|both]
               [inpkts <enable|disable>]
               [learning <enable|disable>]
               [multicast <enable|disable>]
               [filter <vlans...>]
               [create]
```

This section introduces briefly the options that have not yet been discussed in this document:

- **Sc0:** The sc0 keyword is specified in a SPAN configuration when monitoring the traffic to the management interface sc0 is needed. This feature is available on the Catalyst 5000 and 6000 from CatOS 5.1.
- **Inpkts <enable/disable>:** This option is extremely important. As stated earlier, a port you configure as the SPAN destination still belongs to its original VLAN. Packets received on a destination port will then enter the VLAN, as if this port was a normal access port. This behavior may be desired. If you are using a PC as a sniffer, you may want this PC to be fully connected to the VLAN. Nevertheless, it may be dangerous if you connect the destination port to another networking equipment that create a loop in the network. The destination SPAN port does not run the STP and you can end up in a dangerous bridging loop situation. See the section in this document Why is My SPAN Session Creating a Bridging Loop? to understand how this can happen. The default setting for this option is disable, which means that the destination SPAN port discards packet it receives, thus protecting from bridging loops. This option appeared in CatOS 4.2.
- **Learning <enable/disable>:** This option allows disabling learning on the destination port. By default, learning is enabled and the destination port learns MAC addresses from incoming packets it receives. This feature appeared in CatOS 5.2 on the Catalyst 4000 and 5000, and 5.3 on the Catalyst 6000.
- **Multicast <enable/disable>:** As its name suggests, this option allows you to enable or disable the monitoring of multicast packets (default is enable). This feature is available on the Catalyst 5000 and 6000 from CatOS 5.1.
- **Spanning port 15/1:** On the Catalyst 6000, it is also possible to use port 15/1 (or 16/1) as a SPAN source, that will allow it to monitor the traffic forwarded to the Multilayer Switch Feature Card (MSFC) (for software routing or directed to the MSFC).

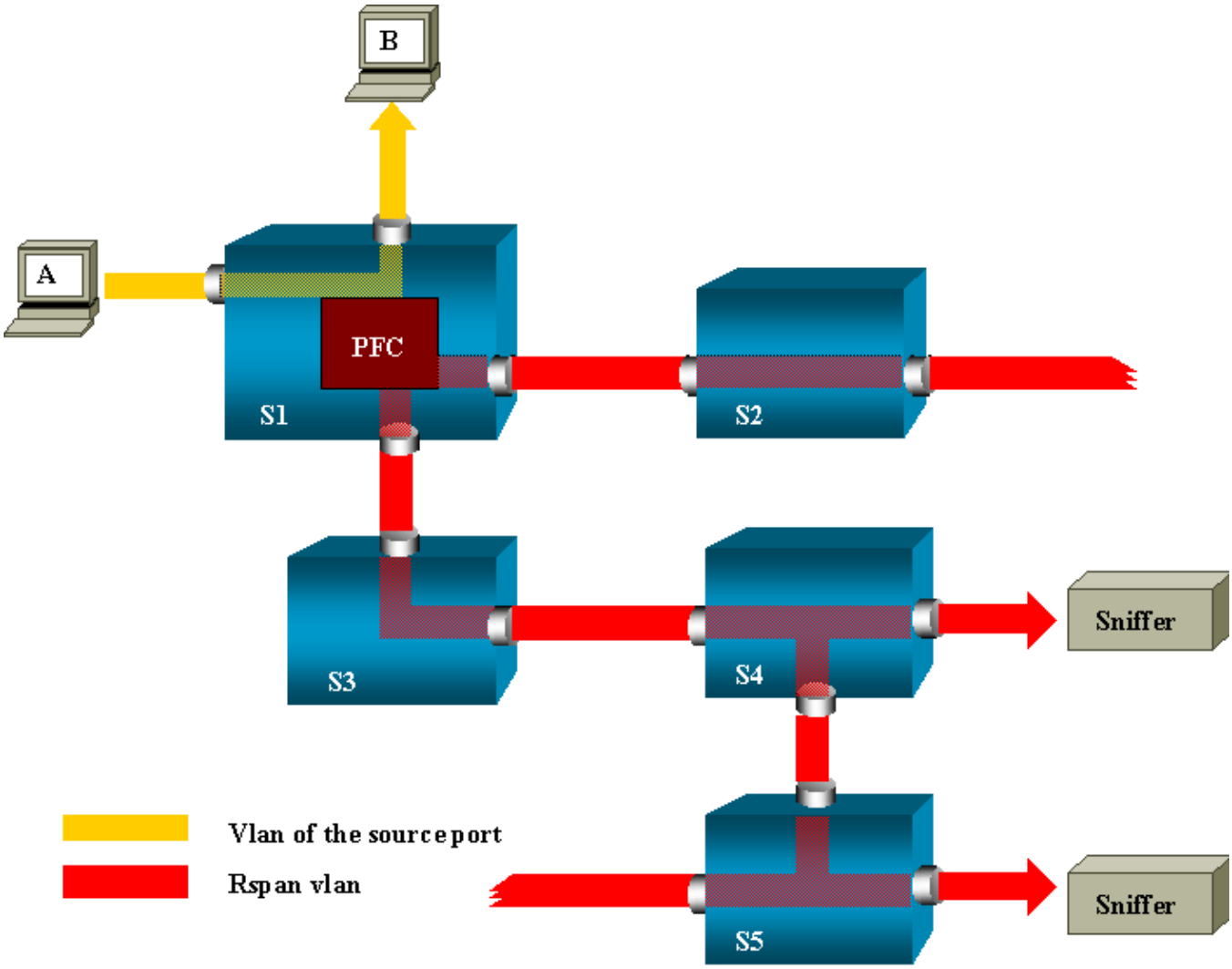
Remote SPAN

RSPAN Overview

Remote SPAN (RSPAN) allows you to monitor source ports spread all over a switched network, not only locally on a switch with SPAN. This feature appeared in CatOS 5.3 in the Catalyst 6000 family and has been added in the Catalyst 4000 family Switches since CatOS 6.3.

The functionality works exactly as a regular SPAN session. The traffic monitored by SPAN, instead of being directly copied to the destination port, is flooded into a special RSPAN VLAN. The destination port can then be located anywhere in this RSPAN VLAN (there can even be several destination ports).

The following diagram illustrates the structure of a RSPAN session.



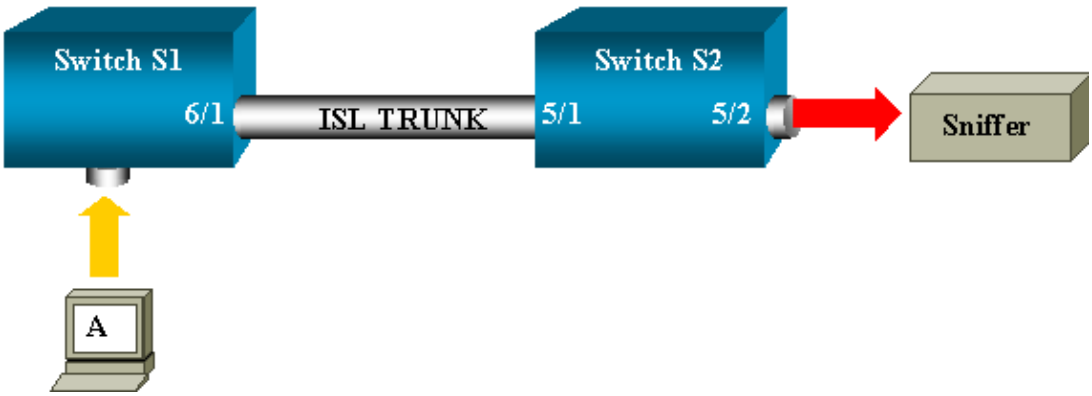
Suppose you configure RSPAN to monitor traffic sent by host A. When A generates a frame destined for B, the packet is copied by an application−specific integrated circuit (ASIC) of the Catalyst 6000 Policy Feature Card into a predefined RSPAN VLAN. From there, the packet is flooded to all other ports belonging to the RSPAN VLAN. All the interswitch links drawn here are trunks; this is a requirement for RSPAN. The only access ports are destination ports, where the sniffers are connected (here on S4 and S5).

A few remarks on this design:

- S1 is called a source switch. Packets only enter the RSPAN VLAN in switches configured as RSPAN source. Currently, a switch can only be source for one RSPAN session (which means that a source switch can only feed one RSPAN VLAN at a time).
- S2 and S3 are intermediate switches. They are not RSPAN sources and do not have destination ports. A switch can be intermediate for any number of RSPAN sessions.
- S4 and S5 are destination switches. Some of their ports are configured to be destination for a RSPAN session. Currently, a Catalyst 6000 can have up to 24 RSPAN destination ports, for one or several different sessions. You can also notice that S4 is both a destination and an intermediate switch.
- You can see that RSPAN packets are flooded into the RSPAN VLAN: even switches like S2, which are not on the path to a destination port, are receiving the traffic for the RSPAN VLAN. It clearly shows that it may be useful to prune this VLAN on such S1−S2 links.
- The flooding is achieved by disabling learning on the RSPAN VLAN.
- In order to prevent loops, the STP has been maintained on the RSPAN VLAN. Because of this, RSPAN cannot monitor Bridge Protocol Data Units (BPDUs).

RSPAN Configuration Example

The following information will illustrate the setup of these different elements with a very simple RSPAN design. S1 and S2 are two Catalyst 6000 switches and you will monitor some S1 ports or VLANs from S2. In order to achieve that, you will see that most of the work consists in setting up a dedicated RSPAN VLAN. The rest of the commands are syntactically very similar to the ones of a usual SPAN session.



Setup of the ISL Trunk Between the Two Switches S1 and S2

Starting from the beginning, you just need to put the same VLAN Trunk Protocol (VTP) domain on each switch, and configure one side as trunking desirable. VTP negotiation will do the rest. On S1:

```
S1> (enable) set vtp domain cisco
      VTP domain cisco modified
```

On S2:

```
S2> (enable) set vtp domain cisco
      VTP domain cisco modified
      S2> (enable) set trunk 5/1 desirable
      Port(s) 5/1 trunk mode set to desirable.
      S2> (enable) 2000 Sep 12 04:32:44 %PAGP−5−PORTFROMSTP:Port 5/1 left bridge
      port 5/1
      2000 Sep 12 04:32:47 %DTP−5−TRUNKPORTON:Port 5/1 has become isl trunk
```

Creation of the RSPAN VLAN

A RSPAN session needs a specific RSPAN VLAN. This VLAN must be created (you cannot convert an existing VLAN into a RSPAN VLAN). In this example, the VLAN 100 is used.

```
S2> (enable) set vlan 100 rspan
      Vlan 100 configuration successful
```

Enter this command on one switch (which is configured as VTP server). The knowledge of RSPAN VLAN 100 is propagated automatically in the whole VTP domain.

Configuration of Port 5/2 of S2 as a RSPAN Destination Port

```
S2> (enable) set rspan destination 5/2 100
      Rspan Type : Destination
      Destination : Port 5/2
      Rspan Vlan : 100
      Admin Source : −
      Oper Source : −
      Direction : −
      Incoming Packets: disabled
      Learning : enabled
      Multicast : −
      Filter : −
      Status : active
      2000 Sep 12 04:34:47 %SYS−5−SPAN_CFGSTATECHG:remote span destination session
      active for destination port 5/2
```

Configuration of a RSPAN Source Port on S1

In this example, monitor incoming traffic entering S1 via port 6/2. Enter the following:

```
S1> (enable) set rspan source 6/2 100 rx
      Rspan Type : Source
      Destination : −
      Rspan Vlan : 100
      Admin Source : Port 6/2
      Oper Source : Port 6/2
      Direction : receive
      Incoming Packets: −
      Learning : −
      Multicast : enabled
      Filter : −
      Status : active
      S1> (enable) 2000 Sep 12 05:40:37 %SYS−5−SPAN_CFGSTATECHG:remote span
      source session active for remote span vlan 100
```

All incoming packets on port 6/2 will now be flooded on the RSPAN VLAN 100, and reach the destination port configured on S1 via the trunk.

Verifying the Configuration

The **show rspan** command gives a summary of the current RSPAN configuration on the switch. Again, there can only be one source RSPAN session at a given time.

```
S1> (enable) show rspan
    Rspan Type : Source
    Destination : −
    Rspan Vlan : 100
```

```
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: −
Learning : −
Multicast : enabled
Filter : −
Status : active
Total remote span sessions: 1
```

Other Configurations Possible with the set rspan Command

See the command reference for a complete list of the **set rspan** command options. You configure the source and the destination using several command lines with RSPAN. This apart, SPAN and RSPAN really behave the same. You can even use RSPAN locally, on a single switch, if you want to have several destination SPAN ports.

See the RSPAN Configuration Guidelines for a list of restrictions that apply to RSPAN configuration.

Feature Summary and Limitations

This table summarizes the different features introduced and provides the minimum CatOS release needed to run the feature on the specified platform:

Feature	Catalyst 4000	Catalyst 5000	Catalyst 6000
Inpkts enable/disable option	4.4	4.2	5.1
Multiple sessions, ports in different VLANs	5.1	5.1	5.1
Sc0 option	X	5.1	5.1
Multicast enable/disable option	X	5.1	5.1
Learning enable/disable option	5.2	5.2	5.3
RSPAN	6.3	X	5.3

Here is a short summary of the current restrictions on the number of possible SPAN sessions:

Feature	Catalyst 4000 Range of Switches	Catalyst 5000 Range of Swtiches	Catalyst 6000 Range of Switches
Rx or Both SPAN sessions	5	1	2
Tx SPAN sessions	5	4	4
Rx, Tx, or both RSPAN source sessions	5	Not Supported	1

RSPAN destination	5	Not Supported	24
Total Sessions	5	5	30

Refer to Cisco documentation for the Catalyst 4000, Catalyst 5000, Catalyst 6000 for additional restrictions and configuration guidelines.

SPAN on the Catalyst 2950/Catalyst 3550 Series Switches

The following are guidelines to configure the SPAN feature on Catalyst 2950 and Catalyst 3550 Switches.

- The Catalyst 2950 Switches can have only one SPAN session active at a time and can monitor only source ports, it can not monitor VLANs.
- The Catalyst 2950 and 3550 Switches can forward traffic on a destination SPAN port in Cisco IOS Software Release 12.1(13)EA1 and later.
- The Catalyst 3550 Switches can support up to two SPAN sessions at a time and can monitor source ports as well as VLANs.

The SPAN feature configuration commands are similar on Catalyst 2950 and Catalyst 3550, except that Catalyst 2950 can not monitor the VLANs. The SPAN can be configured as shown in the following example:

```
C2950#configure terminal
C2950(config)#
C2950(config)#monitor session 1 source interface fastEthernet 0/2

!--- Interface fa0/2 is configured as source port.

C2950(config)#monitor session 1 destination interface fastEthernet 0/3

!--- Interface fa0/3 is configured as destination port.

C2950(config)#

C2950#show monitor session 1
Session 1
---------
Source Ports:
    RX Only:       None
        TX Only:       None
        Both:          Fa0/2
Destination Ports: Fa0/3
C2950#
```

Note: Unlike the 2900XL and 3500XL family Switches, the Catalyst 2950 and 3550 faimly Switches are able SPAN source port traffic in receive direction only, (Rx span or ingress span) or in tranmsit direction only (Tx span or egress span) or both.

Note: The above commands are not supported on Catalyst 2950 with Cisco IOS Software Release 12.0(5.2)WC(1) and with any software earlier than version 12.1(6)EA2. To configure SPAN on a Catalyst 2950 with software earlier than Cisco IOS Software Release 12.1(6)EA2, refer to the Enabling Switch Port Analyzer section of the following document:

- Managing Catalyst 2950 Switches

Note: Catalyst 2950 switches using software release 12.1.(9)EA1d and earlier versions in 12.1 train supported SPAN with the caveat that all packets seen on the SPAN destination port (connected to the sniffing device/PC) had a 802.1Q tag on them, even though the SPAN source port (monitored port) may not be a 802.1Q trunk port. If the sniffing device or PC NIC does not understand 802.1Q tagged packets, they may drop the packets or have difficulty decoding them. Ability to see the 802.1Q tagged frames is important only when the SPAN source port is a trunk port. Starting from 12.1(11)EA1, you can enable/disable tagging of the packets at the SPAN destination port. Issue the **monitor session session_number destination interface interface−id encapsulation dot1q** command to enable encapsulation of the packets at the destination port. If the encapsulation keyword is not specified, the packets are sent untagged, which is the default starting from 12.1(11)EA1.

SPAN on the Catalyst 4000 and Catalyst 6000 Series Switches Running Integrated Cisco IOS

SPAN feature is supported on the Catalyst 4000 and Catalyst 6000 running Integrated Cisco IOS (Native mode). Both of these switch platform are using the identical Command Line Interface (CLI) and configuration similar to 3550 configuration discussed earlier. The related configuration document can be found in the following document:

- Configuring Local SPAN and Remote SPAN on Catalyst 6000
- Configuring SPAN on Catalyst 4000

Feature Summary and Limitations

This table summarizes the different features introduced and provides the minimum Cisco IOS release needed to run the feature on the specified platform:

Feature	Catalyst 2950/3550	Catalyst 4000 (Cisco IOS)	Catalyst 6000 (Cisco IOS)
Ingress (inpkts) enable/disable option	12.1(12c)EA[1]	Not Currently Supported[2]	Not Currently Supported[2]
RSPAN	12.1(12c)EA1	Not Currently Supported[2]	12.1(13)E

[1]Only support for Intrusion Detection Systems (IDSs) to monitor, repel, and report network security violations

[2] Feature currently not available and the availability of these features is typically not published until it is released.

Here is a short summary of the current restrictions on the number of possible SPAN/RSPAN sessions:

Feature	Catalyst 2950/3550	Catalyst 4000 (Cisco IOS)	Catalyst 6000 (Cisco IOS)

Rx or Both SPAN sessions	2	2	2
Tx SPAN sessions	2	4	2
Rx, Tx, or both RSPAN source sessions	2	Not Currently Supported[1]	1 (+ 1 ingress SPAN only)[2]
RSPAN destination	2	Not Currently Supported[1]	64
Total Sessions	2	6	66

[1] Feature currently not available and the availability of these features is typically not published until it is released.

[2]If you have two Rx or Tx or Both SPAN sessions already configured, then you can't have RSPAN source sessions.

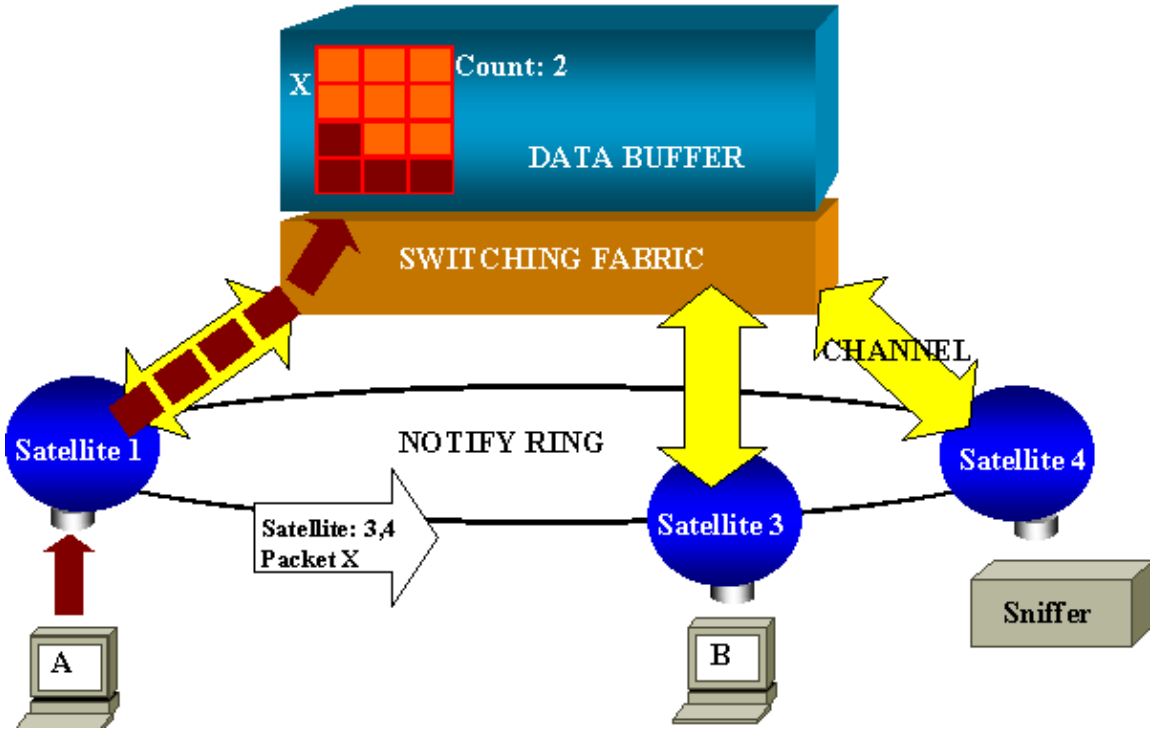
Refer to Cisco documentation for the Catalyst 3550, Catalyst 4000, and Catalyst 6000 for additional restrictions and configuration guidelines.

Performance Impact of SPAN on the Different Catalyst Platforms

Catalyst 2900XL/3500XL Family

Architecture Overview

Here is a very simplistic view of the 2900XL/3500XL Switches internal architecture:



The ports of the switch are attached to satellites that communicate to a switching fabric via radial channels. On the top of that, all the satellites are interconnected via a high−speed notify ring, dedicated to signaling traffic.

When a packet is received by a satellite from a port, it is split into cells and sent to the switching fabric via one or more channels. The packet is then stored in the shared memory. Each satellite has knowledge of the destination ports. In the above diagram, satellite 1 knows that the packet X is to be received by satellite 3 and 4. It sends via the notify ring a message to these satellites, so that they can start retrieving the cells from the shared memory via their radial channels, and eventually forward the packet. As the source satellite knows the destination, it also transmits an index that specifying the number of time this packet will be downloaded by the other satellites. Each time a satellite retrieve the packet from the shared memory, this index is decremented. Once the index reaches zero, the shared memory can be released.

Performance Impact

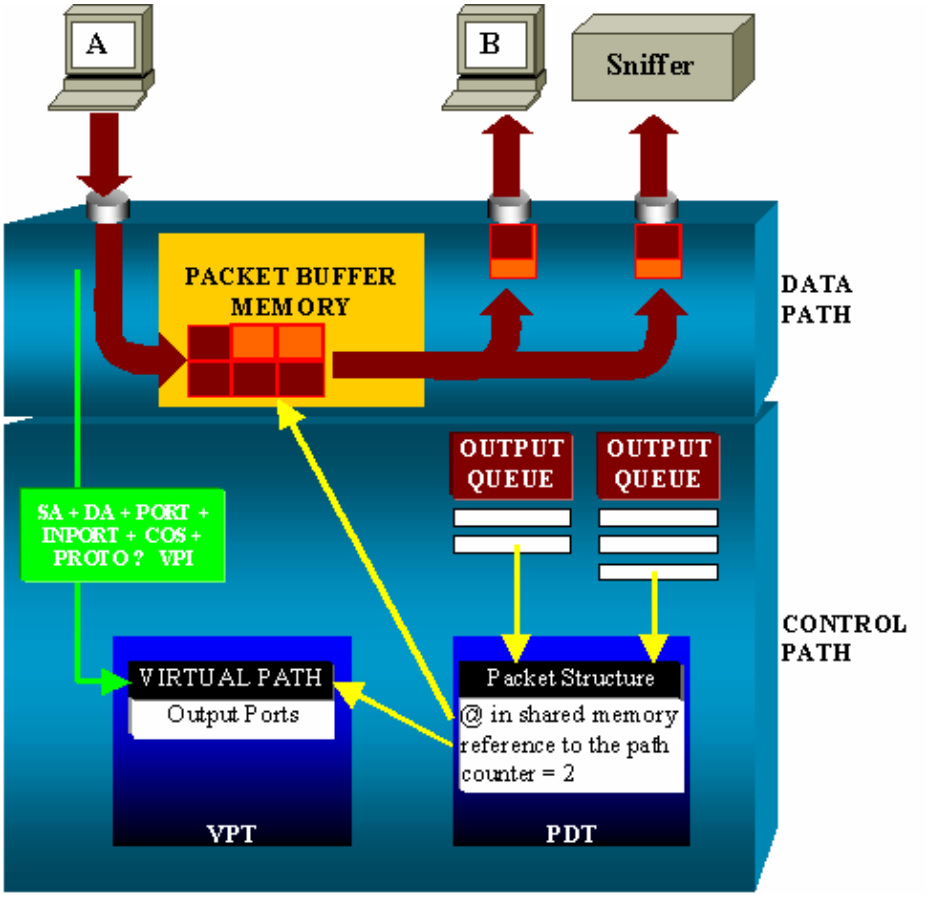
Monitoring some ports with SPAN implies copying an additional time a packet from the data buffer to a satellite. The impact on the high−speed switching fabric is negligible.

The monitoring port receives copies of transmitted and received traffic for all monitored ports. In this architecture, a packet destined for multiple destinations is stored in memory until all copies have been forwarded. If the monitoring port is 50 percent oversubscribed for a sustained period of time, it will probably become congested and hold part of the shared memory. One or more of the ports being monitored might then also experience a slowdown.

Catalyst 4000 Family

Architecture Overview

The Catalyst 4000 is based on a shared memory switching fabric. Here is a high level overview of the path of a packet through the switch. The actual implementation is, in fact, much more complex.



On a Catalyst 4000, you can distinguish the data path, which corresponds to the real transfer of data within the switch, from the control path, where all the decisions are taken.

When a packet enters the switch, a buffer is allocated in the Packet Buffer Memory (a shared memory), and a packet structure pointing to this buffer is initialized in the Packet Descriptor Table (PDT). While the data is copied into shared memory, the control path determines where to switch it: a hash value is computed from the packet source address, destination address, VLAN, protocol type, input port and COS (either 802.1p tag or port default). This value is used to find the Virtual Path Index (VPI) of a path structure in the Virtual Path Table (VPT). This virtual path entry in the VPT holds several fields related to this particular flow, including the destination port(s). The packet structure in the PDT is now updated with a reference to the virtual path, and counter. In the above example, the packet is to be transmitted to two different ports, thus, the counter is initialized to two. At last, the packet structure added to the output queue of the two destination ports. From there, the data is copied from the shared memory into the output buffer of the port and the packet structure counter is decremented. When it reaches zero, the shared memory buffer is released.

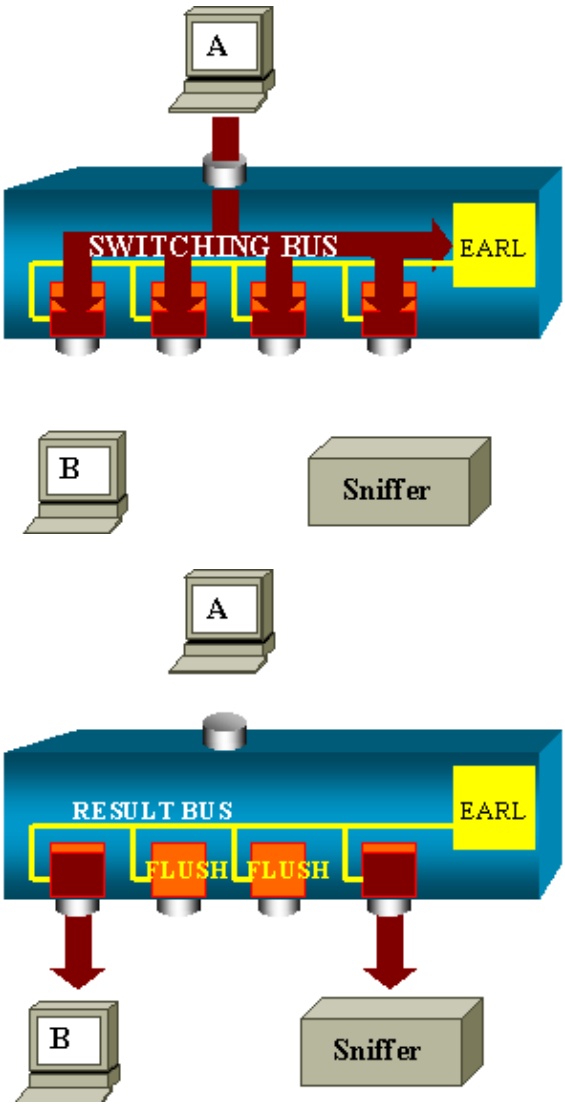
Performance Impact

When using the SPAN feature, a packet has to be sent to two different ports, just like in the above example. This is not an issue as the switching fabric is non−blocking. If the destination SPAN port is congested, packets are dropped in the output queue and thus correctly released from the shared memory. Thus, there is no impact on the switch operation.

Catalyst 5000/6000 Family

Architecture Overview

On the Catalyst 5000 and 6000 family, a packet received on a port is transmitted on the internal switching bus. Every line card in the switch starts storing this packet in its internal buffers. At the same time, the Encoded Address Recognition Logic (EARL) receives the header of the packet and computes a result index that it sends to all the line cards via the result bus. The knowledge of this index allows the line card to decide individually whether they should flush or transmit the packet they are still receiving in their buffers.



Performance Impact

Whether one or several ports will eventually transmit the packet has absolutely no influence on the switch operation. Thus, considering this architecture, the SPAN feature has no impact on the performance.

Frequently Asked Questions and Common Problems

Connectivity Issues Because of SPAN Misconfiguration

This used to occur very frequently before CatOS 5.1. At that time, there use to be only one SPAN session possible and it stayed in the configuration, even when SPAN was disabled. Just entering **set span enable**

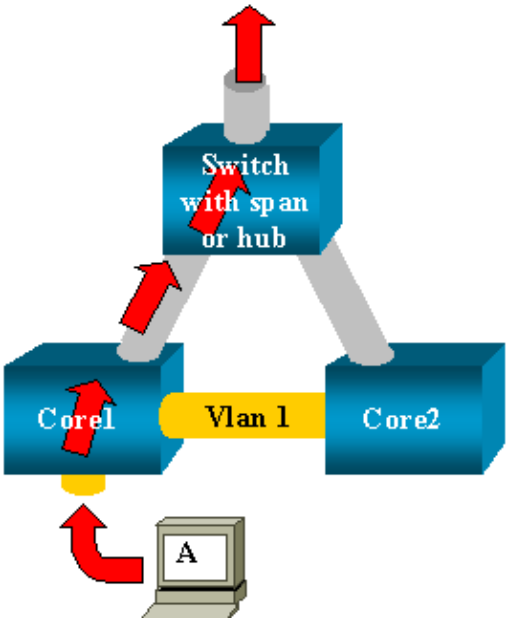
(frequently because of a typo, the user wanting to enable STP for instance) would reactivate the stored SPAN session. This may cause severe connectivity issues if the destination port is used to forward user traffic.

Still in the current implementation of the CatOS, be very careful to the port you choose as a SPAN destination.

Why is My SPAN Session Creating a Bridging Loop?

This typically occurs when the administrator is trying to fake the RSPAN feature, or simply because of a configuration error.

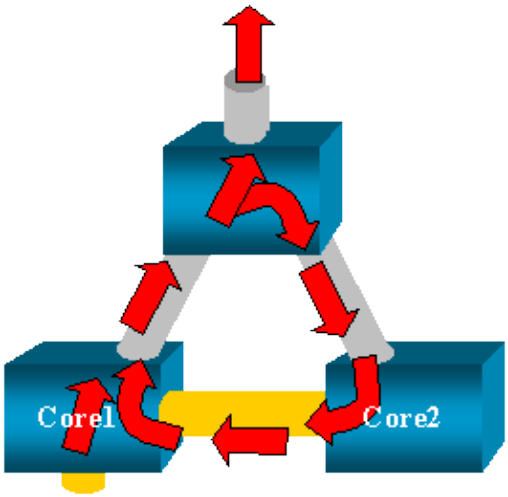
Here is an example of the scenario:



Two core switches, linked by a trunk for instance, each of them having several servers, clients or other bridges connected to them. The administrator wants to monitor VLAN 1 that is appearing on several bridges with SPAN. In order to achieve that, he created a SPAN session monitoring the whole VLAN 1 on each core switch, and, in order to merge these two sessions, the destination port is connected to the same hub (or the same switch, using another SPAN session).

The goal is achieved, each single packet received on VLAN 1 by a core switch is duplicated on its SPAN port and forwarded upward to the hub. The traffic is eventually captured by a sniffer.

The only problem is that the traffic is also re−injected into Core 2 via the destination SPAN port, thus creating a bridging loop in VLAN 1. Remember that a destination SPAN port is not running the STP and is not able to prevent such a loop.



Since the introduction of the inpkts (input packets) option on the CatOS, a SPAN destination port drops by default any incoming packets, thus preventing this failure scenario. But the potential issue is still present on the Catalyst 2900XL/3500XL family. Note also that even with the inpkts option preventing the loop, the above configuration could cause some problem in the network (because of the learning enabled on the destination port at least).

Does SPAN Impact Performances?

The links below describe the performance impact for the specified Catalyst platforms:

- Catalyst 2900XL/3500XL
- Catalyst 4000
- Catalyst 5000/6000

Can I Configure SPAN on an EtherChannel Port?

An EtherChannel will not form if one of the ports in the bundle is a SPAN destination port. If you try to configure this, the switch will tell you the following:

```
Channel port cannot be a Monitor Destination Port
Failed to configure span feature
```

A port in an EtherChannel bundle can be used as a SPAN source port.

Can I Have Several SPAN Sessions Running at the Same Time?

On the Catalyst 2900XL/3500XL family, the number of destination ports available on the switch is the only limit to the number of SPAN sessions.

On the Catalyst 2950 family, you can have only one assigned monitor port at any given time. If you select another port as the monitor port, the previous monitor port is disabled, and the newly selected port becomes the monitor port.

On the Catalyst 4000/5000/6000, since CatOS 5.1, you can have several concurrent SPAN sessions: see the section Creating Several Simultaneous Sessions, and also see the section Configuration Restrictions from this document.

Why Am I Not Able to Capture Corrupted Packets with SPAN?

This is again because of the way switches operate, in general. When a packet is going through a switch, the following occurs:

- The packet reaches the ingress port.
- It is then stored in at least one buffer.
- It is eventually retransmitted on the egress port.

If the switch receives a corrupted packet, the ingress port usually drops it, so you will not see it on the egress port. It is then true that a switch is not completely transparent when it is a matter of capturing traffic. Similarly when you see corrupted packet on you sniffer in the above scenario, the errors where generated at step 3, on the egress segment.

If you think that a device is sending corrupted packets, you might want to put the sending host and the sniffer device on a hub. The hub does not perform any errorchecking so, unlike the switch, the hub will not drop the packets and thsi way the packets can be viewed.

Related Information

- **LAN Product Support**
- **LAN Switching Technology Support**
- **Technical Support − Cisco Systems**