White Paper

High-Performance Switched Port Analyzer with Cisco Nexus 3000 Series Switches

What You Will Learn

In this guide, you will learn about the Cisco® Switched Port Analyzer (SPAN) feature for Cisco Nexus® 3000 Series Switches. The document explains what SPAN is and why it is needed and defines relevant terminology. It then describes the specific Cisco Nexus 3000 Series architecture for SPAN and provides configuration guidance for high-performance results. The document also provide guidance for configuration validation as well as troubleshooting tips.

On many platforms in actual high-performance environments in which ultra-low latency is essential to provide near-real-time information, SPAN creates additional latency since the network device needs to duplicate the packets. The Cisco Nexus 3000 Series is equipped with a high-performance implementation of SPAN that enables traffic replication without additional latency for the destination SPAN port.

SPAN Overview

What Is SPAN and Why Is It Needed?

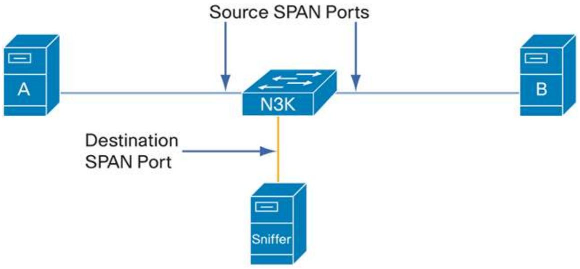
The SPAN feature was introduced on switches because of a fundamental difference between switches and hubs. When a hub receives a packet on one port, the hub sends a copy of that packet from all ports except the one on which the hub received the packet. After a switch boots, it starts to build a Layer 2 forwarding table on the basis of the source MAC addresses of the various packets that the switch receives. After this forwarding table is built, the switch forwards traffic destined for a MAC address directly to the corresponding port. To be able to monitor traffic on the switches, SPAN is needed.

SPAN Terminology

Main terms used to discuss are defined here and illustrated in Figure 1.

- Ingress traffic: Traffic that enters the switch
- Egress traffic: Traffic that leaves the switch
- Source (SPAN) port: A port that is monitored with the SPAN feature
- Source (SPAN) VLAN: A VLAN whose traffic is monitored with the SPAN feature
- Destination (SPAN) port: A port that monitors source ports, usually ports with a sniffer connected

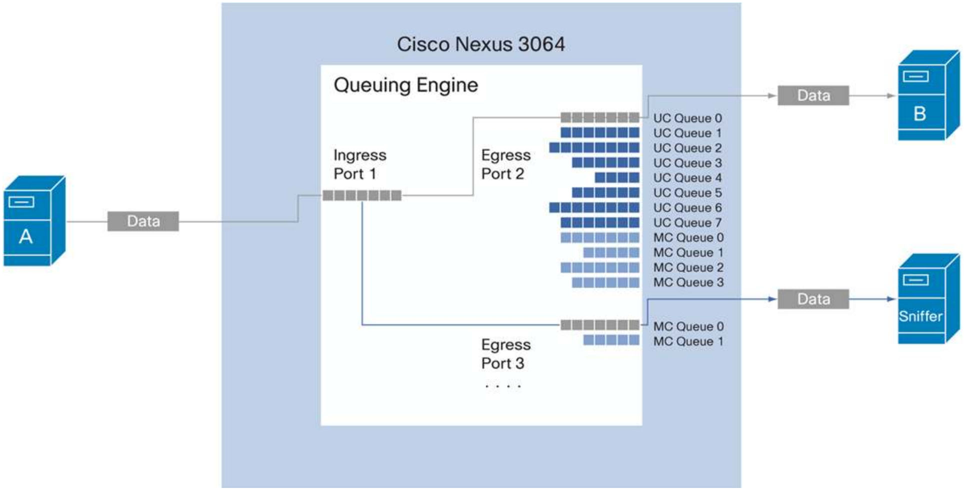
Figure 1. SPAN Terminology



Architecture

The SPAN feature allows traffic to be mirrored from within a switch from a specified source to a specified destination. As explained in the Cisco Nexus 3000 Series architecture white paper, the Cisco Nexus 3064PQ Switch queuing engine has unicast and multicast queues for each port. The replication mechanism works as follows: The source SPAN port packets are marked for SPAN replication in the ingress flow. The packet is then replicated in the queuing engine: When the packet is sent to egress port 2 for destination traffic, simultaneously it is replicated in the multicast queue of egress port 3, which is configured as the destination SPAN port. The replication happens while the packet is transiting the queuing engine, as shown in Figure 2. Therefore, no additional delay occurs during the replication process.

Figure 2. Cisco Nexus 3064PQ SPAN Mechanism



When the source SPAN port is configured for egress (transmit [TX]), then replication occurs after the packet has been rewritten. It therefore includes an IEEE 802.1q VLAN tag header. The ingress SPAN (receive [RX]) does not include the header since the replication is performed before the packet is rewritten. Note that the receive direction for a SPAN source port is processed using cut-through switching, whereas the transmit direction for a SPAN source port is processed using store-and-forward switching. Refer to "Configuring SPAN for High Performance" later in this guide for configuration details.

Configuring SPAN

Creating and Deleting a SPAN Session

You create a SPAN session by assigning a session number using the **monitor** command. If the session already exists, any additional configuration settings are added to that session.

To create a SPAN session, perform the task shown here.

	Command	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **monitor session** *session-number*	Enters monitor configuration mode. New session configuration information is added to the existing session configuration.

The following example creates a SPAN session:

```
switch# configure terminal
```

```
switch(config)# monitor session 2
```

To help ensure that you are working with a completely new session, you can delete the desired session number or all SPAN sessions.

To delete SPAN sessions, perform the task shown here.

Command	Purpose
`switch(config)# no monitor session {all | session-number}`	Deletes the configuration of the specified SPAN session or all sessions.

Configuring the Destination Ports

The SPAN destination port can be only a physical port on the switch, not a PortChannel.

To configure an Ethernet interface as a SPAN destination port, perform the task shown here.

	Command	Purpose
Step 1	`switch# configure terminal`	Enters global configuration mode.
Step 2	`switch(config)# interface ethernet slot/port`	Enters interface configuration mode for the specified Ethernet interface selected by the *slot* and *port* values.
Step 3	`switch(config-if)# switchport monitor`	Sets the interface to monitor mode. Priority flow control (PFC) is disabled when the port is configured as a SPAN destination.
Step 4	`switch(config-if)# exit`	Reverts to global configuration mode.
Step 5	`switch(config)# monitor session session-number`	Enters monitor configuration mode.
Step 6	`switch(config-monitor)# destination interface ethernet slot/port`	Configures the Ethernet destination port.

The following example configures an Ethernet SPAN destination port:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface ethernet 1/3
```

Configuring the Source Port

You can configure the source ports for a SPAN session. The source port type is e Ethernet

To configure the source ports for a SPAN session, perform the task shown here.

Command	Purpose
`switch(config-monitor)# source interface type slot/port [rx | tx | both]`	Configures the source ports and the traffic direction in which to duplicate packets. You can enter a range of Ethernet ports. You can specify the traffic direction in which to duplicate traffic as ingress (**rx**), egress (**tx**), or **both**. By default, the direction is **both**.

The following example configures an Ethernet SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface ethernet 1/16
```

Configuring Source PortChannels or VLANs

You can configure the source channels for a SPAN session. These ports can be PortChannels or VLANs. The monitored direction can only be ingress and applies to all physical ports in the group.

To configure the source channels for a SPAN session, perform the task shown here.

Command	Purpose
switch(config-monitor)# source {**interface** {**port-channel**} *channel-number* **rx** | **vlan** *vlan-range*}	Configures PortChannel, SAN PortChannel, or VLAN sources. The monitored direction can only be ingress and applies to all physical ports in the group. For VLAN sources, the monitored direction is implicit.

The following example configures a PortChannel SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 1 rx
```

The following example configures a VLAN SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source vlan 1
```

Configuring the Description of a SPAN Session

To provide a descriptive name of the SPAN session for ease of reference, perform the task shown here.

Command	Purpose
switch(config-monitor)# **description** *description*	Applies a descriptive name to the SPAN session.

The following example configures a description of a SPAN session:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# description monitoring ethernet ports
```

Activating or Suspending a SPAN Session

By default, the session state is shut. To open a session that duplicates packets from sources to destinations, perform the task shown here.

Command	Purpose
switch(config)# **no monitor session** {**all** | *session-number*} **shut**	Opens the specified SPAN session or all sessions.

To suspend a SPAN session, perform the task shown here.

Command	Purpose
switch(config)# **monitor session** {**all** | *session-number*} **shut**	Suspends the specified SPAN session or all sessions.

The following example suspends a SPAN session:

```
...
switch(config)# monitor session 3 shut
```

Configuring SPAN for High Performance

The Cisco Nexus 3064PQ can handle:

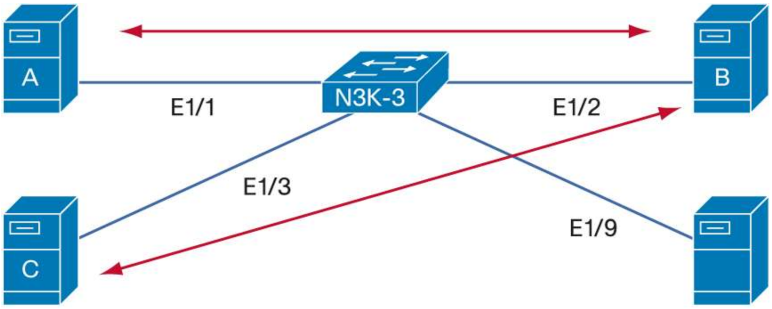
- A maximum of four active sessions simultaneously:
  - Two sessions with source interfaces monitoring in both directions
  - Four sessions when monitored traffic is in only one direction (RX or TX)
- Up to 18 configured sessions, allowing easier configuration changes

For better performance, the best practice is to use only RX source traffic for SPAN. RX traffic uses cut-through switching, whereas TX uses store-and-forward switching. Hence, when SPAN monitors traffic in both directions (RX and TX), performance is not as good as when SPAN monitors only RX traffic. If you need to monitor both directions of traffic, you can monitor RX traffic on more physical ports to capture both sides of the traffic.

Example: Monitor Bidirectional Traffic To and From Server B

The goal in this example (Figure 3) is to monitor traffic to server B in both directions. The other devices communicating with server B are servers A and C. The SPAN destination client to receive the traffic is also connected to the Cisco Nexus 3064PQ. To achieve better performance, the configuration needs to monitor RX traffic on three ports - Ethernet 1/1, 1/2, and 1/3 - instead of just Ethernet 1/2 (both directions).

Figure 3. SPAN Configuration Example



The configuration on the Cisco Nexus 3064PQ (N3K-3) is as follows:

```
interface ethernet1/9
 switchport monitor

monitor session 1
 source interface ethernet 1/1,ethernet 1/2,ethernet 1/3 rx
 destination interface ethernet 1/9
 no shutdown
```

Verification is as follows:

```
n3k-3# show monitor session 2
   session 1
```

```
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/1       Eth1/2       Eth1/3
    tx            :
    both          :
source VLANs      :
    rx            :
destination ports : Eth1/9
```

Note: If more than the four SPAN resources are used (two bidirectional or four unidirectional SPAN sessions), the following error message will be displayed when you attempt to bring up the monitor session with the **no shutdown** command:

ERROR: Destination resource unavailable. All destination resources used up.

You can also monitor a VLAN as a source traffic or a PortChannel.

Verifying SPAN and Monitoring for Problems

After SPAN is configured, two aspects need to be verified: Was configuration performed correctly, and if SPAN is operational, where are the traffic counters?

Verifying the SPAN Configuration

To display the SPAN configuration, perform the task shown here.

Command	Purpose

`switch#` **`show monitor`** `[`**`session`** `{`**`all`** `|`
`session-number |` **`range`** *`session-range`*`}`
`[`**`brief`**`]]`
	Displays the SPAN configuration.

This example displays SPAN session information:

```
switch# show monitor   SESSION  STATE        REASON                 DESCRIPTION
-------  -----------  ----------------------  --------------------------------
2        up           The session is up
3        down         Session suspended
```

This example displays SPAN session details:

```
switch# show monitor session 2
   session 2
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/10
    tx            :
    both          :
source VLANs      :
    rx            : 1
destination ports : Eth1/12
```

Legend: f = forwarding enabled, l = learning enabled

Checking SPAN Traffic Counters

The command used for the traffic counters is:

show queuing interface ethernet

To help understand how to read the traffic counters, in this section server A is sending only unicast unidirectional traffic to server B. Server A sent a burst of 1000 packets with a size of 64 bytes.

The **show queuing interface ethernet 1/1** command shows that 1000 unicast packets were received by the port. Since the packets are unicast, the counters for unicast packets sent over the port increment.

```
switch#show queuing interface ethernet 1/1
Ethernet1/1 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR            100

  RX Queuing
    qos-group 0
    HW MTU: 1500 (1500 configured)
    drop-type: drop, xon: 0, xoff: 0
    Statistics:
        Ucast pkts sent over the port           : 1000
        Ucast bytes sent over the port          : 64000
        Mcast pkts sent over the port           : 0
        Mcast bytes sent over the port          : 0
        Ucast pkts dropped                      : 0
        Ucast bytes dropped                     : 0
        Mcast pkts dropped                      : 0
        Mcast bytes dropped                     : 0
```

The **show queuing interface ethernet 1/9** command shows that 1000 multicast packets were received by the port. Since packet replication in the queuing engine occurs in the multicast queue, the multicast packet counters increment in this output; this behavior is expected by design.

```
switch# show queuing interface ethernet 1/9
Ethernet1/9 queuing information:
  TX Queuing
    qos-group  sched-type  oper-bandwidth
        0       WRR            100

  RX Queuing
```

```
        qos-group 0
        HW MTU: 1500 (1500 configured)
        drop-type: drop, xon: 0, xoff: 0
        Statistics:
            Ucast pkts sent over the port           : 0
            Ucast bytes sent over the port          : 0
            Mcast pkts sent over the port           : 1000
            Mcast bytes sent over the port          : 64000
            Ucast pkts dropped                      : 0
            Ucast bytes dropped                     : 0
            Mcast pkts dropped                      : 0
            Mcast bytes dropped                     : 0
```

If multicast drop counters increment on the SPAN destination port, most likely there is oversubscription in the traffic. Review the bandwidth of the actual traffic sent as source traffic with the respective **show queuing interface** counters to help understand why the SPAN destination port may be dropping SPAN data.

When investigating SPAN problems with received traffic, be sure to check for the proper configuration and packet counters as described in this section.

For More Information

http://www.cisco.com/go/nexus3000

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-670244-00 06/11