Configuring SPAN

This chapter contains the following sections:

Information About SPAN

SPAN Sources

SPAN sources refer to the interfaces from which traffic can be monitored. The Cisco Nexus device supports Ethernet, Fibre Channel, virtual Fibre Channel, port channels, SAN port channels, VSANs and VLANs as SPAN sources. With VLANs or VSANs, all supported interfaces in the specified VLAN or VSAN are included as SPAN sources. You can choose the SPAN traffic in the ingress direction, the egress direction, or both directions for Ethernet, Fibre Channel, and virtual Fibre Channel source interfaces:

- Ingress source (Rx)—Traffic entering the device through this source port is copied to the SPAN destination port.

- Egress source (Tx)—Traffic exiting the device through this source port is copied to the SPAN destination port.

Note VSAN ports cannot be configured as ingress source ports in a SPAN session.

Characteristics of Source Ports

A source port, also called a monitored port, is a switched interface that you monitor for network traffic analysis. The switch supports any number of ingress source ports (up to the maximum number of available ports on the switch) and any number of source VLANs or VSANs.

A source port has these characteristics:

- Cannot be monitored in multiple SPAN sessions.

- Cannot be a destination port.

- Can be configured with a direction (ingress, egress, or both) to monitor. For VLAN and VSAN sources, the monitored direction can only be ingress and applies to all physical ports in the group. The RX/TX option is not available for VLAN or VSAN SPAN sessions.

- Can be in the same or different VLANs or VSANs.

- For VLAN or VSAN SPAN sources, all active ports in the source VLAN or VSAN are included as source ports.

SPAN Destinations

SPAN destinations refer to the interfaces that monitors source ports. The Cisco Nexus Series device supports Ethernet interfaces as SPAN destinations.

Source SPAN	Dest SPAN
Ethernet	Ethernet
Virtual Fibre Channel	Ethernet (FCoE)

Characteristics of Destination Ports

Each local SPAN session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports, VSANs, or VLANs. A destination port has these characteristics:

• Cannot be a source port.

• Cannot be a port channel or SAN port channel group.

• Does not participate in spanning tree while the SPAN session is active.

• Is excluded from the source list and is not monitored if it belongs to a source VLAN of any SPAN session.

• Receives copies of sent and received traffic for all monitored source ports.

Multiple SPAN Destinations

Local SPAN and SPAN-on-Drop sessions can support multiple destination ports. This allows traffic in a single local SPAN session or a SPAN-on-Drop session also to be monitored and send to multiple destinations.

Note Multiple destinations are not supported on ERSPAN, or SPAN-on-Latency sessions.

SPAN with ACL

The SPAN with ACL filtering feature allows you to filter SPAN traffic so that you can reduce bandwidth congestion. To configure SPAN with ACL filtering, you use ACL's for the session to filter out traffic that you do not want to span. An ACL is a list of permissions associated to any entity in the system; in the context of a monitoring session, an ACL is a list of rules which results in spanning only the traffic that matches the ACL criteria, saving bandwidth for more meaningful data. The filter can apply to all sources in the session.

SPAN on Drop

The SPAN-on-drop feature enables the spanning of packets which would normally be dropped due to unavailable buffer or queue space on ingress. Instead of dropping a packet when congestion occurs, the system stores the packet in a separate SPAN-on-drop buffer and then sends the packet to the specified SPAN-on-drop destination port.

SPAN-on-Latency Sessions

The SPAN-on-Latency feature allows the system to SPAN packets that exceed a pre-configured latency threshold.

For high-latency flows the system can be configured to send a copy to any pre-configured SPAN destination. This creates a data set for analytics that can be used to check which applications are impacted by increased latency in the network. This feature can also be used to identify traffic flows that experience congestion.

> **Note**   SPAN copies can be transported to a local analyzer port, or remote analyzer using IPFIX/ERSPAN encapsulation. The SPAN copies can be truncated to save bandwidth.

Guidelines and Limitations for SPAN

SPAN traffic is rate-limited as follows on Cisco Nexus devices to prevent a negative impact to production traffic:

- SPAN supports 16 active bi-directional SPAN sessions.

The following guidelines and limitations apply to SPAN session where multiple destinations are configured:

- Multiple destinations are supported for Local SPAN or SPAN-on-Drop sessions only. Multiple destinations are not supported on ERSPAN or SPAN-on-Latency sessions.

- The maximum number of unique destinations configured on all active sessions is 16. A single SPAN session can have a maximum of 16 destinations, and a SPAN-on-Drop session can have a maximum of 17 destinations, in which case no further SPAN sessions can be configured.

- You cannot SPAN a single source VLAN to multiple destination ports.

The following guidelines and limitations apply to SPAN-on-Drop sessions:

- Only Ethernet source interfaces are supported (port channels not supported). Sources can be a part of a SPAN-on-Drop session and a local SPAN session simultaneously.

- At most one SPAN-on-Drop or SPAN-on-Drop ERSPAN session may be active at the same time.

- Directions on source interfaces are not supported.

- FEX interfaces are not supported as sources. However, fabric interfaces are supported. Setting a fabric interface as a source allows SPAN-on-Drop sessions to be enabled on all FEX ports associated with that fabric interface.

- Multicast egress drops are not spanned. SPAN-on-Drop applies only to packets dropped in ingress due to a lack of buffer resources or when the Virtual Output Queueing (VOQ) size exceeds the preprogrammed threshold.

- ACL-based SPAN is not supported

- Configuring the maximum transmission unit (MTU) truncation size for packets is not supported for SPAN-on-Drop sessions.

The following guidelines and limitations apply to SPAN-on-Latency sessions:

- Although SPAN-on-Latency detection is performed on a per-port basis, the span pointer configuration is a global value.

- The maximum latency threshold value configuration is per 40 Gigabit port. Therefore, if there the system has 10 Gigabit ports, the latency threshold is shared by four 10 Gigabit ports.

- At most only one SPAN-on-Latency or SPAN-on-Latency ERSPAN session may be active at the same time.

- You must issue the **clear hardware profile latency monitor all** command when the switch is reloaded or when a module is powered on. Until you issue this command no packets are spanned.

The following limitations apply to SPAN (local SPAN) session Access Control Lists (ACL) configurations:

- Due to system limitations, the extent to which an ACL associated to SPAN session can scale depends on the how the SPAN source is configured. The following table shows different scenarios and the corresponding maximum ACL size supported.

  Note   These calculations assume that each ACE in the ACL results in one final TCAM entry.

Scenario	Maximum ACL Size
SPAN has single Switch Port as source with both Tx and Rx.	Current Available TCAM Entries/2
SPAN has multiple Switch Ports as source with both Tx and Rx.	Current Available TCAM Entries/3
SPAN has Port Channel (with one or more member switch ports) as source with both Tx and Rx.	Current Available TCAM Entries/3
SPAN has single HIF Ports as source with both Tx and Rx.	Current Available TCAM Entries/3
SPAN has multiple HIF Ports as source with both Tx and Rx.	Current Available TCAM Entries/4
SPAN has HIF Port Channel (with one or more member HIF ports) as source with both Tx and Rx.	Current Available TCAM Entries/4

- The following scenarios are unaffected by any system limitations for ACL and SPAN session scaling:

- SPAN has single Switch Port as source with Tx only.

- SPAN has multiple Switch Ports as source with Tx only.

- SPAN has a Port Channel (with one or more member switch ports) as source with Tx only.

- SPAN has a single Host Interface (HIF) Port as source with Tx only.

- SPAN has multiple HIF Ports as source with Tx only.

- SPAN has a single Port HIF Channel (with one or more member HIF ports) as source with Tx only.

- SPAN has a single Switch Port as source with Rx only.

- SPAN has multiple Switch Ports as source with Rx only.

- SPAN has a Port Channel (with one or more member switch ports) as source with Rx only.

- SPAN has a single HIF Ports as source with Rx only.

- SPAN has multiple HIF Ports as source with Rx only.

- SPAN has a HIF Port Channel (with one or more member HIF ports) as source with Rx only

- The following guidelines apply when configuring local SPAN sessions with ACLs:

  - When you associate an ACL with a SPAN session, you must ensure that its size is not greater than the calculations given in the table above. Otherwise the SPAN session fails and generate a "TCAM resource unavailable" error. If the ACL has Layer 4 Operations and TCAM resource expansion is enabled, you need to know the expected expanded size and you need to use the expanded size to calculate the maximum ACL size.

  - If you change the ACL that is attached to a SPAN session, the ACL size can exceed the maximum ACL size allowed. In this scenario, the SPAN session continues to work with the modified ACL. However, you should undo the ACEs added to the ACL to limit the size to maximum allowed ACL size.

  - If you add a SPAN session when one already exists, then to modify the first span session there should be free TCAM entries of size equal to number of ACEs in the associated ACL (Assuming that each ACE requires one TCAM entry. If it gets expanded, the expanded size should be considered). Therefore, TCAM entries consumed by the second SPAN session should be released.

  - To replace a large ACL with another large ACL (which could cause the SPAN session to enter a generic error state), you must first remove the existing filter access group (using the **no filter access-group** *current acl name* command), and then configure the new filter access group (using the **filter access-group** *new acl name* command).

- Local SPAN/SPAN on Drop/SPAN on Latency is not aware of VPC.

- The following is the limitation for HIF and Virtual Ethernet (Veth) as SPAN destination:

  - Multi-destination SPAN is not supported. If HIF/VETH port is a destination, the monitor session must have single destination.

Creating or Deleting a SPAN Session

You create a SPAN session by assigning a session number using the **monitor session** command. If the session already exists, any additional configuration information is added to the existing session.

Procedure

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

The following example shows how to configure a SPAN monitor session:

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

Configuring an Ethernet Destination Port

You can configure an Ethernet interface as a SPAN destination port.

✎ **Note** The SPAN destination port can only be a physical port on the switch.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface ethernet** *slot/port*	Enters interface configuration mode for the Ethernet interface with the specified slot and port. **Note** To enable the **switchport monitor** command on virtual ethernet ports, you can use the **interface vethernet** *slot/port* command.
Step 3	switch(config-if)# **switchport monitor**	Enters monitor mode for the specified Ethernet interface. Priority flow control is disabled when the port is configured as a SPAN destination.
Step 4	switch(config-if)# **exit**	Reverts to global configuration mode.

	Command or Action	Purpose
Step 5	switch(config)# **monitor session** *session-number*	Enters monitor configuration mode for the specified SPAN session.
Step 6	switch(config-monitor)# **destination interface ethernet** *slot*/*port*	Configures the Ethernet SPAN destination port. **Note** To enable the virtual ethernet port as destination interface in the monitor configuration, you can use the **destination interface vethernet** *slot*/*port* command.

The following example shows how to configure an Ethernet SPAN destination port (HIF):

```
switch# configure terminal
switch(config)# interface ethernet100/1/24
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# destination interface ethernet100/1/24
switch(config-monitor)#
```

The following example shows how to configure a virtual ethernet (VETH) SPAN destination port:

```
switch# configure terminal
switch(config)# interface vethernet10
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface vethernet10
switch(config-monitor)#
```

Configuring MTU Truncation for Each SPAN Session

To reduce the SPAN traffic bandwidth, you can configure the maximum bytes allowed for each replicated packet in a SPAN session. This value is called the maximum transmission unit (MTU) truncation size. Any SPAN packet larger than the configured size is truncated to the configured size.

Note   MTU Truncation is not supported for SPAN-on-Drop sessions.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode and specifies the SPAN session for which the MTU truncation size is to be configured.

	Command or Action	**Purpose**
Step 3	switch(config-monitor) # [**no**] **mtu**	Configures the MTU truncation size for packets in the specified SPAN session. The range is from 64 to 1518 bytes.
Step 4	switch(config-monitor) # **show monitor session** *session-number*	(Optional) Displays the status of SPAN sessions, including the configuration status of MTU truncation, the maximum bytes allowed for each packet per session, and the modules on which MTU truncation is and is not supported.
Step 5	switch(config-monitor) # **copy running-config** startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure MTU truncation for a SPAN session:

```
switch# configure terminal
switch(config) # monitor session 3
switch(config-monitor) # mtu
switch(config-monitor) # copy running-config startup-config
switch(config-monitor) #
```

Configuring the Rate Limit for SPAN Traffic

By configuring a rate limit for SPAN traffic to 1Gbps across the entire monitor session, you can avoid impacting the monitored production traffic.

Procedure

	Command or Action	**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 rate-limit 1G**	Specifies that the rate limit is 1 Gbps.
Step 4	switch(config-if)# **exit**	Reverts to global configuration mode.

This example shows how to limit the bandwidth on Ethernet interface 1/2 to 1 Gbps:

```
switch(config)# interface ethernet 1/2
switch(config-if)# switchport monitor rate-limit 1G
switch(config-if)#
```

Configuring Source Ports

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode for the specified monitoring session.
Step 3	switch(config-monitor) # **source interface** *type slot*/*port* [**rx** | **tx** | **both**]	Adds an Ethernet SPAN source port and specifies the traffic direction in which to duplicate packets. You can enter a range of Ethernet, Fibre Channel, or virtual Fibre Channel ports. You can specify the traffic direction to duplicate as ingress (Rx), egress (Tx), or both. By default, the direction is both.

The following example shows how to configure an Ethernet SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface ethernet 1/16
switch(config-monitor)#
```
The following example shows how to configure a virtual Fibre Channel SPAN source port:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface vfc 129
switch(config-monitor)#
```

Configuring Source Port Channels, VSANs, or VLANs

You can configure the source channels for a SPAN session. These ports can be port channels SAN port channels, VSANs and VLANs. The monitored direction can be ingress, egress, or both and applies to all physical ports in the group.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode for the specified SPAN session.
Step 3	switch(config-monitor) # **source** {**interface** {**port-channel** | **san-port-channel**} *channel-number* [**rx** | **tx** | **both**] | **vlan** *vlan-range* | **vsan** *vsan-range* }	Configures port channel, SAN port channel, VLAN, or VSAN sources. For VLAN or VSAN sources, the monitored direction is implicit.

The following example shows how to configure a port channel SPAN source:

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface port-channel 1 rx
switch(config-monitor)# source interface port-channel 3 tx
switch(config-monitor)# source interface port-channel 5 both
switch(config-monitor)#
```

This example shows how to configure a SAN port channel SPAN source:

```
switch(config-monitor)#switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface san-port-channel 3 rx
switch(config-monitor)#
```

The following example shows how to configure a VLAN SPAN source:

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

switch(config-monitor)#This example shows how to configure a VSAN SPAN source:

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

Configuring the Description of a SPAN Session

For ease of reference, you can provide a descriptive name for a SPAN session.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode for the specified SPAN session.
Step 3	switch(config-monitor) # **description** *description*	Creates a descriptive name for the SPAN session.

The following example shows how to configure a SPAN session description:

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # description monitoring ports eth2/2-eth2/4
switch(config-monitor) #
```

Configuring an ACL Filter for a SPAN Session

To selectively monitor traffic in a SPAN session, you can configure an access-control list (ACL) to filter packets. The SPAN session ignores any permit or deny actions specified in the access-list, and spans only the packets that match the access-list filter criteria.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *session-number*	Enters monitor configuration mode and specifies the SPAN session for which the ACL filter is to be configured.
Step 3	switch(config-monitor) # [**no**] **filter access-group** *acl_filter*	Configures the ACL filter for packets in the specified SPAN session. The ACL filter can be a MAC or an IP access-list.
Step 4	switch(config-monitor) # **show monitor session** *session-number*	(Optional) Displays the status of SPAN sessions, including the configuration status of ACL filter.
Step 5	switch(config-monitor) # **copy running-config** startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure an ACL filter for a SPAN session:

```
switch# configure terminal
switch(config) # monitor session 3
switch(config-monitor) # filter access-group acl_span_ses_3
switch(config) # copy running-config startup-config
switch(config) #
```

Configuring a SPAN-on-Drop Session

Use the monitor session command to configure a SPAN-on-Drop session. Each session is identified by a unique SPAN-on-Drop session number.

Note   There can only be one active SPAN-on-Drop or SPAN-on-Drop ERSPAN session at any time.

Note   You can configure more than one destination for a SPAN-on-Drop sessions.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** *span-on-drop-session-number* **type span-on-drop**	Enters SPAN-on-Drop monitor configuration mode for the specified SPAN-on-drop session.
Step 3	switch(config-span-on-drop) # **description** *description*	Creates descriptive name for the SPAN-on-Drop session.
Step 4	switch(config-span-on-drop) # **source interface ethernet** *slot*/*port* **rx**	Configures session sources. You can enter a range of Ethernet ports. SPAN-on-Drop sessions supports ingress traffic only.
Step 5	switch(config-span-on-drop) # **destination interface ethernet** *slot*/*port*	Configures the Ethernet SPAN-on-Drop destination port.
Step 6	switch(config) # **show monitor session** *session-number*	(Optional) Displays the status of SPAN-on-Drop sessions.
Step 7	switch(config) # **copy running-config** startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure a SPAN-on-Drop session:

```
switch# configure terminal
switch(config) # monitor session 3 type span-on-drop
switch(config-span-on-drop) # description span-on-drop-session_3
switch(config-span-on-drop) # source interface ethernet 1/3
switch(config-span-on-drop) # destination interface ethernet 1/2
switch(config) # copy running-config startup-config
switch(config) #
```

Configuring a SPAN-on-Latency Session

You can configure a maximum transmission unit (MTU) size for the SPAN traffic to reduce the amount of fabric or network bandwidth used in sending SPAN packets.

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** switch> enable	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose

Step 2	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 3	**interface ethernet** *slot/port*
	
	Example:
	`switch(config)# interface ethernet`
	`1/1`
		Enters interface configuration mode.

Step 4	**packet latency threshold** *threshold*
	
	Example:
	`switch(config-if)# packet latency`
	`threshold 53000000`
		Configures the latency threshold value on an interface. Valid values are from 8 to 536870904 nano seconds.

Step 5	**monitor session** *session_number* **type span-on-latency**
	
	Example:
	`switch(config)# monitor session 1`
	`type span-on-latency`
	`switch(config-span-on-latency)#`
		Defines a SPAN source session using the session ID and the session type, and places the command in SPAN monitor source session configuration mode.
		
		The session_number argument range is from 1 to 1024. The same session number cannot be used more than once.
		
		The session ID (configured by the span_session number argument) and the session type (configured by the span-on-latency keyword) cannot be changed once entered. To change session ID or session type, use the no version of the command to remove the session and then re-create the session through the command with a new session ID or a new session type.

Step 6	**description** *description*
	
	Example:
	`switch(config-span-on-latency)#`
	`description SPAN-on-Latency-session`
		Adds a description to the session configuration.

Step 7	**source interface ethernet** *slot/port*
	
	Example:
	`switch(config-span-on-latency)#`
	`source interface ethernet 1/3`
		Specifies the Ethernet interface to use as the source SPAN port.

Step 8	**destination interface ethernet** *slot/port*
	
	Example:
	`switch(config-span-on-latency)#`
	`destination interface ethernet 1/1`
		Specifies the Ethernet interface to use as the session destination port.

	Command or Action	Purpose
Step 9	**mtu** *mtu-value* **Example:** `switch(config-span-on-latency)# mtu 1500`	Defines the MTU truncation size for SPAN packets. Valid values are from 64 to 1518. The default is no truncation enabled.
Step 10	**exit** **Example:** `switch(config-span-on-latency)# exit`	Updates the configuration and exits SPAN-on-Latency session configuration mode.
Step 11	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Activating a SPAN Session

The default is to keep the session state shut. You can open a session that duplicates packets from sources to destinations.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **no monitor session** {**all** | *session-number*} **shut**	Opens the specified SPAN session or all sessions.

The following example shows how to activate a SPAN session:

```
switch# configure terminal
switch(config) # no monitor session 3 shut
```

Suspending a SPAN Session

By default, the session state is **shut**.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **monitor session** {**all** | *session-number*} **shut**	Suspends the specified SPAN session or all sessions.

The following example shows how to suspend a SPAN session:

```
switch# configure terminal
switch(config) # monitor session 3 shut
switch(config) #
```

Displaying SPAN Information

Procedure

	Command or Action	Purpose
Step 1	switch# **show monitor** [**session** {**all** | *session-number* | **range** *session-range*} [**brief**]]	Displays the SPAN configuration.

The following example shows how to display SPAN session information:

```
switch# show monitor
SESSION  STATE        REASON                 DESCRIPTION
-------  -----------  ---------------------  --------------------------------
2        up           The session is up
3        down         Session suspended
4        down         No hardware resource
```

The following example shows how to display SPAN session details:

```
switch# show monitor session 2
   session 2
--------------
type            : local
state           : up

source intf     :

source VLANs    :
    rx          :
source VSANs    :
    rx          : 1
destination ports : Eth3/1
```

Configuration Example for a SPAN ACL

This example shows how to configure a SPAN ACL:

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# monitor session 1
switch(config-erspan-src)# filter access-group match_11_pkts
```

Configuration Example for SPAN-on-Latency Session

This example shows how to configure an SPAN-on-Latency session:

```
switch# configure terminal
switch(config) # interface ethernet 1/1
switch(config-if) # packet latency threshold 530000000
switch(config) # monitor session 11 type span-on-latency
switch(config-span-on-latency) # description span-on-latency-session_11
switch(config-span-on-latency) # source interface ethernet 1/3
switch(config-span-on-latency) # destination interface ethernet 1/1
switch(config-span-on-latency) # mtu 1500
switch(config) # copy running-config startup-config
switch(config) #
```