



## Configuring ERSPAN

This chapter describes how to configure an encapsulated remote switched port analyzer (ERSPAN) to transport mirrored traffic in an IP network on Cisco NX-OS devices.

This chapter contains the following sections:

- [Finding Feature Information, on page 1](#)
- [About ERSPAN, on page 1](#)
- [Prerequisites for ERSPAN, on page 6](#)
- [Guidelines and Limitations for ERSPAN, on page 6](#)
- [Default Settings, on page 10](#)
- [Configuring ERSPAN, on page 11](#)
- [Verifying the ERSPAN Configuration, on page 28](#)
- [Configuration Examples for ERSPAN, on page 28](#)
- [Related Documents, on page 32](#)
- [Feature History for ERSPAN, on page 32](#)

## Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter or the Feature History table in this chapter.

## About ERSPAN

ERSPAN transports mirrored traffic over an IP network, which provides remote monitoring of multiple switches across your network. The traffic is encapsulated at the source router and is transferred across the network. The packet is decapsulated at the destination router and then sent to the destination interface.

## ERSPAN Types

Cisco NX-OS Release 6.1 and later releases support ERSPAN Type II and Type III. All previous Cisco NX-OS releases support only ERSPAN Type II.

ERSPAN Type III supports all of the ERSPAN Type II features and functionality and adds these enhancements:

- Provides timestamp information in the ERSPAN Type III header that can be used to calculate packet latency among edge, aggregate, and core switches.
- Identifies possible traffic sources using the ERSPAN Type III header fields.
- Provides the ability to configure timestamp granularity across all VDCs to determine how the clock manager synchronizes the ERSPAN timers.

## ERSPAN Sources

The interfaces from which traffic can be monitored are called ERSPAN sources. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. ERSPAN sources include the following:

- Ethernet ports and port channels.
- The inband interface to the control plane CPU—You can monitor the inband interface only from the default virtual device context (VDC). Inband traffic from all VDCs is monitored.
- VLANs (ingress only)—When a VLAN is specified as an ERSPAN source, all supported interfaces in the VLAN are ERSPAN sources.
- Fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender (FEX).
- Satellite ports and host interface port channels on the Cisco Nexus 2000 Series Fabric Extender— These interfaces are supported in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode.




---

**Note** Layer 3 subinterfaces are not supported.

---




---

**Note** A single ERSPAN session can include mixed sources in any combination of the above.

---

See the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide* for information on the number of supported ERSPAN sessions.

ERSPAN source ports have the following characteristics:

- A port configured as a source port cannot also be configured as a destination port.
- ERSPAN does not monitor any packets that are generated by Supervisor 1, regardless of their source. This limitation does not apply to Supervisor 2.

## ERSPAN Destinations

Destination ports receive the copied traffic from ERSPAN sources.

ERSPAN destination ports have the following characteristics:

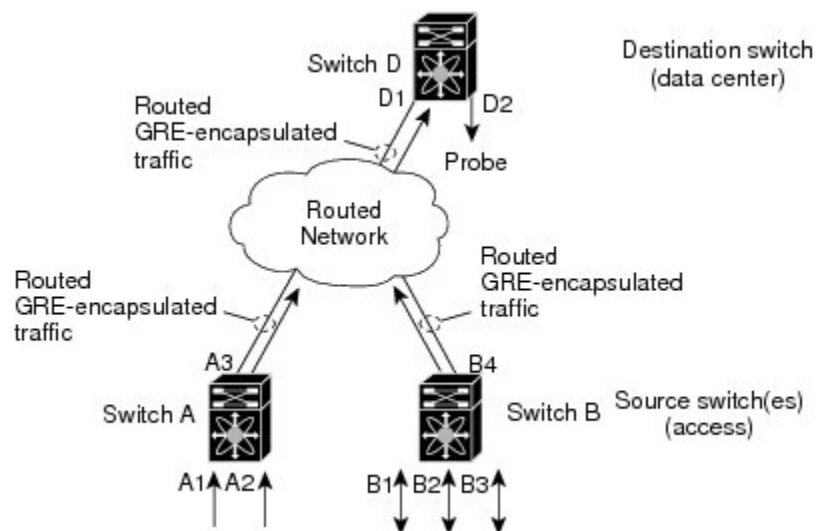
- Destinations for an ERSPAN session include Ethernet ports or port-channel interfaces in either access or trunk mode.
- A port configured as a destination port cannot also be configured as a source port.
- A destination port can be configured in only one ERSPAN session at a time.
- Destination ports do not participate in any spanning tree instance or any Layer 3 protocols.
- Ingress and ingress learning options are not supported on monitor destination ports.
- F Series module core ports, Fabric Extender host interface (HIF) ports, HIF port channels, and fabric port-channel ports are not supported as ERSPAN destination ports.

## ERSPAN Sessions

You can create ERSPAN sessions that designate sources and destinations to monitor.

The figure below shows an ERSPAN configuration.

**Figure 1: ERSPAN Configuration**



## Extended ERSPAN Session

Cisco NX-OS Release 6.2(2) and later releases support extended ERSPAN sessions in addition to the two traditional ERSPAN sessions in prior releases. Extended ERSPAN sessions can be bidirectional or unidirectional. The session direction is specified during session creation. A pool of 12 independent session resources are available. Unidirectional sessions use one resource, and bidirectional use two resources. These 12 resources are shared between local and ERSPAN source sessions across all VDCs.

If you are configuring an extended SPAN session on a Cisco Nexus 70xx or a Cisco Nexus 77xx switch, the following applies:

- You can configure 16 sessions as unidirectional or bidirectional, as required.
- You do not need to maintain two traditional sessions.

- You do not need to use the resource manager to reserve the two traditional sessions.
- ERSPAN ACL-based filtering is not supported.

**Note**

On a Cisco Nexus 77xx switch, all sessions are extended by default and are not classified as Traditional sessions or Extended sessions. The **mode extended** command is not supported on Cisco Nexus 77xx switches.

## 4K VLANs per ERSPAN Session

Cisco NX-OS Release 7.3(0)D1(1) and later releases support 4K VLANs per ERSPAN session. You can use the **source interface all** command to enable the monitor session on the switch to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The 4K VLANs per ERSPAN Session feature also enables monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in the monitor session by using the **filter vlan** command with the **source interface all** command to filter the irrelevant VLANs.

The 4K VLANs per ERSPAN Session feature has the following characteristics:

- You can use the **source interface all** command for multiple sessions in the same VDC.
- Supports all session parameters such as MTU truncation, Sampling and Rate Limiting.
- Simple and Complex Rule-based SPAN is supported with the **source interface all** command. This enables traffic flow-based monitoring using a set of filter rules across the VDC.
- Traffic generated by Supervisors is not spanned.
- Supported only in Ethernet VDCs of Cisco Nexus 7000 Series switches.
- Supported only in extended SPAN sessions.

## Rule-Based ERSPAN

Rule-based ERSPAN filters the ingress or egress ERSPAN traffic based on a set of rules. For Cisco NX-OS releases prior to 6.2(2), you can filter on VLANs, the destination index, and the source index. Beginning with Cisco NX-OS Release 6.2(2), you can filter the ERSPAN traffic based on a combination of fields in the Layer 2, Layer 3, or Layer 4 header packet.

Every ERSPAN session (traditional and extended) has an associated filter. Every ERSPAN session has one filter resource. A simple filter has only one rule, and you can add multiple fields or conditions to this rule. The packets are spanned only if all conditions are met.

Ethernet	IPv4	IPv6	ARP/RARP	FCoE
Frame Type	Frame Type	Frame Type	Frame Type	Frame Type
VLAN	VLAN	VLAN	VLAN	VLAN
TR	TR	TR	TR	TR
BPDU	BPDU	BPDU	BPDU	BPDU
Port Channel	Port Channel	Port Channel	Port Channel	Port Channel
Lane	Lane	Lane	Lane	Lane
Flow Hash	Flow Hash	Flow Hash	Flow Hash	Flow Hash
L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA
L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA
EtherType	EtherType	EtherType	EtherType	EtherType
CoS/VL	CoS/VL	CoS/VL	CoS/VL	CoS/VL
	ToS	ToS	ARP	FCD_ID
	L4 Protocol	L4 Protocol	Request	FCS_ID
	IPv4 SA	IPv6 SA	Sender IP	SOF
	IPv4 DA	IPv6 DA	Target IP	R_CTL
				TYPE
				Cmd_Code
				Sec_Hdr Exists

## Exception ERSPAN

Exception ERSPAN enables you to span exception packets. Packets that have failed an intrusion detection system (IDS), Layer 3 IP verification, and FabricPath are treated as exception packets.

The exception ERSPAN session is supported in either one of the two traditional ERSPAN sessions or in one of the extended ERSPAN sessions. Rate limiters, MTU truncation, and sampling are supported in the exception ERSPAN session. Only the exception packets sent to the drop destination interface are supported as an ERSPAN source. Exception packets that are pushed to the supervisor, the ACLQoS, or Layer 2 are not spanned. Each VDC supports one exception ERSPAN session.

Exception ERSPAN is supported in the egress direction only. In the case of an extended ERSPAN Rx session, the exception source configuration will be rejected.

## Network Analysis Module

You can also use the Cisco Network Analysis Module (NAM) to monitor ERSPAN data sources for application performance, traffic analysis, and packet header analysis.

To use NAM for monitoring the Cisco Nexus 7000 ERSPAN data sources, see the *Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1) Quick Start Guide*.

## High Availability

The ERSPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied.

For more information on high availability, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*.

## Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. ERSPAN applies only to the VDC where the commands are entered.

**Note**

You can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored.

For information about configuring VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

## Prerequisites for ERSPAN

ERSPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired ERSPAN configuration. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

## Guidelines and Limitations for ERSPAN

ERSPAN has the following configuration guidelines and limitations:

- For ERSPAN session limits, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.
- All ERSPAN replication is performed in the hardware. The supervisor CPU is not involved.
- Control plane traffic generated by Supervisor 2 can be ERSPAN encapsulated but cannot be filtered by an ERSPAN ACL.
- Control plane packets generated by Supervisor 1 cannot be ERSPAN encapsulated or filtered by an ERSPAN ACL.
- When you configure ERSPAN source on a Cisco Nexus 7000 Series switch that acts as a MPLS PE and the destination of the ERSPAN session is remote across the MPLS network, the ERSPAN packet will be transmitted as a regular IP packet and does not include the MPLS label. It causes the packet being dropped at the remote PE.
- ERSPAN and ERSPAN ACLs are not supported on F1 Series modules. For the VDCs that have F1 Series modules only, you can configure ERSPAN source and destination sessions and ERSPAN ACL source sessions but never come up.

- ERSPAN source sessions are supported on F2 Series and F2e (enhanced) Series modules. Beginning with Cisco NX-OS Release 6.2(2), ERSPAN destination sessions are also supported on these modules. However, ERSPAN ACL sessions are not supported on F2 Series and F2e Series modules.
- ERSPAN source, destination, and ACL sessions are supported on M Series modules.
- The decapsulation of generic routing encapsulation (GRE) or ERSPAN packets received on an F1 Series module is not supported.
- ERSPAN and ERSPAN ACL sessions are terminated identically at the destination router.
- ERSPAN is not supported for management ports.
- ERSPAN does not support packet fragmentation. The "do not fragment" bit is set in the IP header of ERSPAN packets.
- A destination port can be configured in only one ERSPAN session at a time.
- You cannot configure a port as both a source and destination port.
- A single ERSPAN session can include mixed sources in any combination of the following:
  - Ethernet ports or port channels but not subinterfaces
  - VLANs (ingress only)
  - The inband interface or port channels to the control plane CPU



---

**Note** ERSPAN does not monitor any packets that are generated by the supervisor, regardless of their source.

---

- Destination ports do not participate in any spanning tree instance or Layer 3 protocols.
- When an ERSPAN session contains source ports or VLAN sources that are monitored in the transmit or transmit and receive direction, packets that these ports receive might be replicated to the ERSPAN destination port even though the packets are not actually transmitted on the source ports. Some examples of this behavior on source ports are as follows:
  - Traffic that results from flooding
  - Broadcast and multicast traffic
- You can enable ERSPAN for a source port before it becomes operationally active. For Layer 2 ports, traffic flooded to the VLANs that contain these ports are captured even when the link is not connected for the ports.
- For VLAN ERSPAN sessions with both ingress and egress configured, two packets (one from ingress and one from egress) are forwarded from the destination port if the packets get switched on the same VLAN.
- You can monitor the inband interface only from the default VDC. Inband traffic from all VDCs is monitored.

- A FabricPath core port is not supported as an ERSPAN destination when an F2 Series or F2e Series module is present in a VDC. However, a FabricPath core port can be configured as an ERSPAN source interface.
- When using ERSPAN sessions on F2 Series or F2e Series modules, ensure that the total amount of source traffic in a given session is less than or equal to the capacity of the ERSPAN destination interface or port channel for that session. If the ERSPAN source traffic exceeds the capacity of the ERSPAN destination, packet drops might occur on the ERSPAN source interfaces.
- Beginning with Cisco NX-OS Release 5.2, you can configure the Cisco Nexus 2000 Series Fabric Extender (FEX) interfaces and the fabric port channels connected to the Cisco Nexus 2000 Series Fabric Extender as ERSPAN sources. However, you cannot configure them as ERSPAN destinations.




---

**Note** ERSPAN on Fabric Extender interfaces and fabric port channels is supported on the M1 Series and M2 Series modules. ERSPAN runs on the Cisco Nexus 7000 Series device, not on the Fabric Extender. F2 Series and F2e Series modules support FEX, but they do not support FEX ERSPAN. Therefore, the FEX interfaces that are connected through the F2 Series and F2e Series modules cannot be made ERSPAN sources.

---

- You can span Fabric port channels on F2 Series and F2e Series modules.
- VLANs that contain FEX interfaces can be an ERSPAN source, but the ingress traffic through the F2 Series or F2e Series module-based FEX ports cannot be captured.
- Layer 3 multicast egress packets cannot be spanned on F2 Series or F2e Series modules.
- ERSPAN is supported on Fabric Extender interfaces in Layer 2 access mode, Layer 2 trunk mode, and Layer 3 mode. Layer 3 subinterfaces are not supported.
- For ERSPAN sessions, the recommended MTU size is 144 bytes or greater because MTU truncation occurs after the packets are encapsulated.
- The rate limit percentage of an ERSPAN session is based on 10G, 40G, and 100G for the respective modules (that is, 1 percent corresponds to 0.1G, 0.4G, or 1G respectively), and the value is applied per every forwarding engine instance.
- MTU truncation and the ERSPAN source rate limit are supported only on F2 Series, F2e Series, and M2 Series modules and Supervisor 2. They are not supported on M1 Series modules.
- For F2 Series and F2e Series modules, spanned FabricPath (core) packets have a 16-byte core header at the ERSPAN destination, and ingress FEX packets spanned through the fabric port channel have a 6-byte Vntag header at the ERSPAN destination. In addition, when trunk ports are used as the ERSPAN destination, the spanned packets have a 4-byte VLAN tag.
- For F2 Series and F2e Series modules, egress ERSPAN packets of all traffic that ingresses on Layer 2 ports (including edge-to-edge traffic) have a 16-byte MAC-in-MAC header at the ERSPAN destination.
- While setting IP TTL in the ERSPAN header,
  - In M-series LC, after ERSPAN encapsulation / de-capsulation, the packets are sent to EARL for recirculating and hence, the TTL is decremented by EARL.



- In F2/F2e, there are no overheads of recirculating and hence, there is digression from the actual behavior of TTL decrements.
- F1 series does not support ERSPAN.
- For MTU truncation on M2 Series modules, the truncated length of ERSPAN packets is rounded down to the nearest multiplier of 16 bytes. For example, with an MTU configuration value of 65 to 79, packets are truncated to 64 bytes.
- For certain rate limit and packet size values on F2 Series modules, F2e Series modules, M2 Series modules, and Supervisor 2, the ERSPAN packet rate is less than the configured value because of the internal accounting of packet sizes and internal headers.
- ERSPAN sampling is supported only on F2 Series and F2e Series modules. It is not supported on M Series modules.
- Multicast best effort mode applies only to M1 Series modules.
- Beginning with Cisco NX-OS Release 6.1, ERSPAN source sessions are supported on Supervisor 2, but ERSPAN ACL sessions are not.
- ERSPAN Type III source is supported only on F2 Series, F2e Series, and M2 Series modules.
- ERSPAN Type III termination is supported only on M2 Series modules. That is, Type III ERSPAN packets are decapsulated only when they reach their destination through M2 Series modules.
- Beginning with Cisco NX-OS Release 6.2(2), ERSPAN packets ingressing the destination switch on F2 Series or F2e Series modules can be terminated. IPv4 termination is supported but not IPv6 termination. F2 Series module termination on VDC virtual routing and forwarding (VRF) instances is not supported.
- Supervisor 2 supports ERSPAN Type II and ERSPAN Type III for inband ports, but timestamps are not synchronized with the Precision Time Protocol (PTP) master timers.
- 1588 granularity mode is not supported in Cisco NX-OS Release 6.1 and is rejected if selected.
- M2 Series modules support 100 microseconds (ms), 100 nanoseconds (ns), and ns granularity. F2 Series and F2e Series modules support only 100 ms and 100 ns granularity.
- When ERSPAN traffic is terminated on M2 Series modules, drops can occur at higher rates because all ERSPAN traffic for one session converges into one forwarding instance.
- If the global granularity configuration is not supported for a particular module, that module reverts to 100-ms granularity. For example, if granularity is set to ns, all M2 Series modules will enable ns granularities, and all F2 Series and F2e Series modules will internally enable and send packets with the 100-ms timestamp. Use the **show monitor session** command to display the supported and unsupported granularities for each module.
- F2 Series and F2e Series modules do not use the access control list (ACL) complex for ERSPAN Type III ACLs, so an ACL filter cannot be applied to F2 Series and F2e Series module traffic. However, for M2 Series modules, it is possible to encapsulate the packets using the Type III header after applying an ACL.
- F2 Series and F2e Series modules support a 32-bit timestamp in the ERSPAN Type III header while M2 Series modules support a 64-bit timestamp.
- If you enable ERSPAN on a vPC and ERSPAN packets need to be routed to the destination through the vPC, packets that come through the vPC peer-link cannot be captured.

- Extended ERSPAN sessions cannot source incoming traffic on M1 Series modules in either the ingress or egress direction.
- Traditional SPAN sessions support traffic from F Series and M Series modules. Extended SPAN sessions support traffic only from F Series and M2 Series modules.
- Hardware session 15 is used by NetFlow on F2 and F2e Series modules. Any extended session using this hardware ID will not span incoming traffic on the F2 and the F2e ports.
- Only eight sessions can support rate limiting on M2 Series modules. Any additional hardware sessions will not apply the configured rate limiter on M2 Series modules.
- M1 Series modules and Supervisor 1 do not support rule-based ERSPAN. They support only VLAN filtering.
- M1 and M2 Series modules support exception ERSPAN only in the nonadministration VDC, and at least one interface of the module must be present for the VDC.
- F1 Series modules have limited support for rule-based ERSPAN. They do not support the IPv6 source IP filter and the IPv6 destination IP filter. They support only IPv4 and IPv6 ToS filters with values from 0 to 3. Port-channel member lane, FCoE source ID, and FCoE destination ID are not supported.
- F2 and F2e Series modules have limited support for rule-based ERSPAN. They do not support wildcards in the IPv6 source IP filter and IPv6 destination IP filter, and they do not support egress ERSPAN filtering for destination MAC addresses and source MAC addresses.
- ERSPAN ACLs are not supported for use with OTV.
- ERSPAN source sessions are supported on F3 Series modules. Beginning with Cisco NX-OS Release 7.2, ERSPAN destination sessions are also supported on these modules. However, ERSPAN ACL sessions are not supported on F3 Series modules.
- The ERSPAN termination takes place at the ingress point of entry of the destination switch (and not the final destination), so the ingress module at the destination switch must support ERSPAN termination. Beginning with Cisco NX-OS release 7.2(0)D1(1), ERSPAN Termination is supported on F3 linecards.
- Beginning with Cisco NX-OS Release 7.3(0)DX(1), ERSPAN source and destination sessions are supported on M3 Series modules.

## Default Settings

The following table lists the default settings for ERSPAN parameters.

**Table 1: Default ERSPAN Parameters**

Parameters	Default
ERSPAN sampling	Disabled
ERSPAN sessions	Created in the shut state
ERSPAN source rate limit for traditional ERSPAN sessions	Disabled

Parameters	Default
ERSPAN source rate limit for extended ERSPAN sessions	Enabled
Global granularity of ERSPAN Type III sessions	100 microseconds
MTU truncation	Disabled
Multicast best effort mode	Disabled

## Configuring ERSPAN



**Note** Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.

### Configuring an ERSPAN Source Session

You can configure an ERSPAN session on the local device only. By default, ERSPAN sessions are created in the shut state.

For sources, you can specify Ethernet ports, port channels, the supervisor inband interface, and VLANs (ingress only). A single ERSPAN session can include mixed sources in any combination of Ethernet ports, VLANs, or the inband interface to the control plane CPU.

For traditional sessions, you can configure the sessions without specifying the direction of the traffic.



**Note** ERSPAN does not monitor any packets that are generated by the supervisor, regardless of their source.

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor erspan origin ip-address ip-address global</b>	Configures the ERSPAN global origin IP address.
<b>Step 3</b>	switch(config)# <b>no monitor session {session-number   all}</b>	Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.
<b>Step 4</b>	switch(config)# <b>monitor session {session-number   all} type erspan-source [shut]</b>	Configures an ERSPAN Type II source session. By default the session is bidirectional.

	Command or Action	Purpose
		The optional keyword <b>shut</b> specifies a shut state for the selected session.
<b>Step 5</b>	switch(config-erspan-src)# <b>description</b> <i>description</i>	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.
<b>Step 6</b>	switch(config-erspan-src)# <b>source</b> {[ <b>interface</b> [ <b>all</b> ] [ <i>type slot/port[-port]</i> ], [ <i>type slot/port[-port]</i> ]} [ <b>port-channel</b> <i>channel-number</i> ] [ <b>vlan</b> { <i>number</i>   <i>range</i> }] [ <b>rx</b>   <b>tx</b>   <b>both</b> ]	<p>Configures the sources and traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, or a range of VLANs.</p> <p>You can configure one or more sources, as either a series of comma-separated entries or a range of numbers.</p> <p>You can specify the traffic direction to copy as ingress, egress, or both. The default direction is both.</p> <p><b>Note</b> Source VLANs are supported only in the ingress (rx) direction.</p> <p>For a unidirectional session, the direction of the source must match the direction specified in the session.</p> <p>Beginning with Cisco NX-OS Release 7.3(0)D1(1), you can use the <b>all</b> keyword to enable the monitor session to monitor all VLANs and ports in the VDC such as physical ports, Port Channels, FEX ports and FEX Port Channels. The <b>all</b> keyword is supported only in extended ERSPAN sessions.</p>
<b>Step 7</b>	(Optional) Repeat Step 6 to configure all ERSPAN sources.	—
<b>Step 8</b>	(Optional) switch(config-erspan-src)# <b>filter vlan</b> { <i>number</i>   <i>range</i> }	<p>Configures which VLANs to select from the configured sources. You can configure one or more VLANs, as either a series of comma-separated entries or a range of numbers. For information on the VLAN range, see the <i>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide</i>.</p> <p>You can enable monitoring of a higher number of specific VLAN sources than the VLAN source limits currently supported in extended ERSPAN monitor session by using the <b>filter vlan</b> command with the <b>source interface all</b> command to filter the irrelevant VLANs.</p>

	Command or Action	Purpose
<b>Step 9</b>	(Optional) Repeat Step 8 to configure all source VLANs to filter.	—
<b>Step 10</b>	(Optional) switch(config-erspan-src)# <b>filter access-group</b> <i>acl-filter</i>	Associates an ACL with the ERSPAN session.  <b>Note</b> You can create an ACL using the standard ACL configuration process. For more information, see the <i>Cisco Nexus 7000 Series NX-OS Security Configuration Guide</i> .
<b>Step 11</b>	switch(config-erspan-src)# <b>destination ip</b> <i>ip-address</i>	Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session.
<b>Step 12</b>	switch(config-erspan-src)# <b>erspan-id</b> <i>erspan-id</i>	Configures the ERSPAN ID for the ERSPAN source session. The ERSPAN range is from 1 to 1023.
<b>Step 13</b>	switch(config-erspan-src)# <b>vrf</b> <i>vrf-name</i>	Configures the virtual routing and forwarding (VRF) instance that the ERSPAN source session uses for traffic forwarding. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>Step 14</b>	(Optional) switch(config-erspan-src)# <b>ip ttl</b> <i>ttl-number</i>	Configures the IP time-to-live (TTL) value for the ERSPAN traffic. The range is from 1 to 255.
<b>Step 15</b>	(Optional) switch(config-erspan-src)# <b>ip dscp</b> <i>dscp-number</i>	Configures the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic. The range is from 0 to 63.
<b>Step 16</b>	switch(config-erspan-src)# <b>no shut</b>	Enables the ERSPAN source session. By default, the session is created in the shut state.
<b>Step 17</b>	switch(config-erspan-src)# <b>exit</b>	Exits the monitor configuration mode.
<b>Step 18</b>	(Optional) switch(config)# <b>show monitor session</b> {all   <i>session-number</i>   <b>range</b> <i>session-range</i> } [ <b>brief</b> ]	Displays the ERSPAN session configuration.
<b>Step 19</b>	(Optional) switch(config)# <b>show running-config monitor</b>	Displays the running ERSPAN configuration.
<b>Step 20</b>	(Optional) switch(config)# <b>show startup-config monitor</b>	Displays the ERSPAN startup configuration.
<b>Step 21</b>	(Optional) switch(config)# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

## Configuring an ERSPAN Destination Session

You can configure an ERSPAN destination session to copy packets from a source IP address to destination ports on the local device. By default, ERSPAN destination sessions are created in the shut state.

### Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you have already configured the destination ports in monitor mode. For more information, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>interface ethernet</b> <i>slot/port[-port]</i>	Enters interface configuration mode on the selected slot and port or range of ports.
<b>Step 3</b>	switch(config-if)# <b>switchport</b>	Configures switchport parameters for the selected slot and port or range of ports.
<b>Step 4</b>	switch(config-if)# <b>switchport mode</b> [access   <b>trunk</b> ]	Configures the following switchport modes for the selected slot and port or range of ports: <ul style="list-style-type: none"> <li>• access</li> <li>• trunk</li> </ul>
<b>Step 5</b>	switch(config-if)# <b>switchport monitor</b>	Configures the switchport interface as an ERSPAN destination.
<b>Step 6</b>	(Optional) Repeat Steps 2 to 5 to configure monitoring on additional ERSPAN destinations.	—
<b>Step 7</b>	switch(config-if)# <b>no monitor session</b> { <i>session-number</i>   <b>all</b> }	Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.
<b>Step 8</b>	switch(config-if)# <b>monitor session</b> { <i>session-number</i>   <b>all</b> } <b>type</b> <b>erspan-destination</b>	Configures an ERSPAN destination session.
<b>Step 9</b>	switch(config-erspan-dst)# <b>description</b> <i>description</i>	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.
<b>Step 10</b>	switch(config-erspan-dst)# <b>source ip</b> <i>ip-address</i>	Configures the source IP address in the ERSPAN session. Only one source IP address is supported per ERSPAN destination session.

	Command or Action	Purpose
		<b>Note</b> The source IP address must be the IP address on the local device that is configured as the destination IP address on the ERSPAN source. This is the interface on the local device where the Cisco Nexus 7000 device expects to receive packets for decapsulation.
<b>Step 11</b>	switch(config-erspan-dst)# <b>destination</b> {[ <b>interface</b> <i>[type slot/port[-port]][, type slot/port[-port]]</i> ]   [ <b>port-channel</b> <i>channel-number</i> ]}	<p>Configures a destination for copied source packets. You can configure one or more interfaces as a series of comma-separated entries.</p> <p><b>Note</b> You can configure destination ports as trunk ports. For more information, see the <i>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide</i>.</p>
<b>Step 12</b>	(Optional) Repeat Step 11 to configure all ERSPAN destination ports.	—
<b>Step 13</b>	switch(config-erspan-dst)# <b>erspan-id</b> <i>erspan-id</i>	Configures the ERSPAN ID for the ERSPAN session. The range is from 1 to 1023.
<b>Step 14</b>	switch(config-erspan-dst)# <b>vrf</b> <i>vrf-name</i>	Configures the VRF that the ERSPAN destination session uses for traffic forwarding.
<b>Step 15</b>	switch(config-erspan-dst)# <b>no shut</b>	Enables the ERSPAN destination session. By default, the session is created in the shut state.
<b>Step 16</b>	switch(config-erspan-dst)# <b>exit</b>	Exits monitor configuration mode.
<b>Step 17</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 18</b>	(Optional) switch# <b>show monitor session</b> { <b>all</b>   <i>session-number</i>   <b>range</b> <i>session-range</i> } [ <b>brief</b> ]	Displays the ERSPAN session configuration.
<b>Step 19</b>	(Optional) switch# <b>show running-config monitor</b>	Displays the running ERSPAN configuration.
<b>Step 20</b>	(Optional) switch# <b>show startup-config monitor</b>	Displays the ERSPAN startup configuration.
<b>Step 21</b>	(Optional) switch# <b>copy running-config startup-config</b> [ <b>vdc-all</b> ]	Copies the running configuration to the startup configuration.

## Shutting Down or Activating an ERSPAN Session

You can shut down ERSPAN sessions to discontinue the copying of packets from sources to destinations. You can shut down one session in order to free hardware resources to enable another session. By default, ERSPAN sessions are created in the shut state.

You can enable ERSPAN sessions to activate the copying of packets from sources to destinations. To enable an ERSPAN session that is already enabled but operationally down, you must first shut it down and then enable it. You can shut down and enable the ERSPAN session states with either a global or monitor configuration mode command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor session</b> { <i>session-range</i>   <b>all</b> } <b>shut</b>	Shuts down the specified ERSPAN sessions. By default, sessions are created in the shut state.
<b>Step 3</b>	switch(config)# <b>no monitor session</b> { <i>session-range</i>   <b>all</b> } <b>shut</b>	Resumes (enables) the specified ERSPAN sessions. By default, sessions are created in the shut state.  If a monitor session is enabled but its operational status is down, then to enable the session, you must first specify the <b>monitor session shut</b> command followed by the <b>no monitor session shut</b> command.
<b>Step 4</b>	switch(config)# <b>monitor session</b> <i>session-number</i> <b>type erspan-source</b>	Enters the monitor configuration mode for the ERSPAN source type. The new session configuration is added to the existing session configuration.
<b>Step 5</b>	switch(config-erspan-src)# <b>monitor session</b> <i>session-number</i> <b>type erspan-destination</b>	Enters the monitor configuration mode for the ERSPAN destination type.
<b>Step 6</b>	switch(config-erspan-src)# <b>shut</b>	Shuts down the ERSPAN session. By default, the session is created in the shut state.
<b>Step 7</b>	switch(config-erspan-src)# <b>no shut</b>	Enables the ERSPAN session. By default, the session is created in the shut state.
<b>Step 8</b>	switch(config-erspan-src)# <b>exit</b>	Exits the monitor configuration mode.
<b>Step 9</b>	(Optional) switch(config)# <b>show monitor session all</b>	Displays the status of ERSPAN sessions.
<b>Step 10</b>	(Optional) switch(config)# <b>show running-config monitor</b>	Displays the ERSPAN running configuration.
<b>Step 11</b>	(Optional) switch(config)# <b>show startup-config monitor</b>	Displays the ERSPAN startup configuration.



	Command or Action	Purpose
<b>Step 12</b>	(Optional) switch(config)# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

## Configuring MTU Truncation for Each ERSPAN Session

Beginning with Cisco NX-OS Release 6.1, in order to reduce the ERSPAN traffic bandwidth, you can configure the maximum bytes allowed for each replicated packet in an ERSPAN session. This value is called the maximum transmission unit (MTU) truncation size. Any ERSPAN packet larger than the configured size is truncated to the configured size.



**Note** MTU truncation and ERSPAN sampling can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (size versus packet count).



**Note** Do not enable MTU truncation if the destination ERSPAN router is a Cisco Catalyst 6000 Series switch because the Cisco Catalyst 6000 Series switch drops these truncated packets.

### Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor session session-number type erspan-source</b>	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which the MTU truncation size is to be configured.
<b>Step 3</b>	(Optional) switch(config-erspan-src)# <b>header-type version</b>	Changes the ERSPAN source session from Type II to Type III.
<b>Step 4</b>	switch(config-erspan-src)# <b>[no] mtu mtu</b>	Configures the MTU truncation size for packets in the specified ERSPAN session. The range is from 176 to 1500 bytes.
<b>Step 5</b>	switch(config-erspan-src)# <b>exit</b>	Exits monitor configuration mode.
<b>Step 6</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 7</b>	(Optional) switch# <b>show monitor session session-number</b>	Displays the status of ERSPAN sessions, including the configuration status of MTU truncation, the maximum bytes allowed for each

	Command or Action	Purpose
		packet per session, and the modules on which MTU truncation is and is not supported.
<b>Step 8</b>	(Optional) switch# <b>copy running-config startup-config</b> [vdc-all]	Copies the running configuration to the startup configuration.

## Configuring a Source Rate Limit for Each ERSPAN Session

When an ERSPAN session is configured with multiple interfaces as the sources in a high-traffic environment, the destination port can be overloaded, causing the normal data traffic to be disrupted at the source port. Beginning with Cisco NX-OS Release 6.1, you can alleviate this problem as well as traffic overload on the source forwarding instance by configuring a source rate limit for each ERSPAN session.



**Note** ERSPAN sampling takes precedence over ERSPAN source rate limiting. Rate limiting takes effect after sampling is completed on ERSPAN source packets.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor session</b> <i>session-number</i> <b>type erspan-source</b>	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which the source rate limit is to be configured.
<b>Step 3</b>	(Optional) switch(config-erspan-src)# <b>header-type</b> <i>version</i>	Changes the ERSPAN source session from Type II to Type III.
<b>Step 4</b>	switch(config-erspan-src)# <b>[no] rate-limit</b> { <b>auto</b>   <i>rate-limit</i> }	Configures the source rate limit for ERSPAN packets in the specified ERSPAN session in automatic or manual mode: <ul style="list-style-type: none"> <li>• Auto mode—Automatically calculates the rate limit on a per-gigabyte basis as follows: destination bandwidth / aggregate source bandwidth. For example, if the rate limit per gigabyte is 0.5, for every 1G of source traffic, only 0.5G of packets are spanned.</li> </ul> <p>For ingress traffic, the per-gigabyte limit is applied to each forwarding engine of the F2 Series or F2e Series module based on how many ports are used as the ERSPAN source so that the source can be spanned at the maximum available bandwidth. For</p>

	Command or Action	Purpose
		<p>egress traffic, the per-gigabyte limit is applied to each forwarding engine of the F2 Series or F2e Series module without considering how many ports are used as the ERSPAN source.</p> <ul style="list-style-type: none"> <li>Manual mode—Specifies the percentage of the maximum rate of ERSPAN packets that can be sent out from each forwarding engine on a module. The range is from 1 to 100. For example, if the rate limit is 10 percent, the maximum rate of ERSPAN packets that can be sent out from each of the forwarding engines on an F2 Series or F2e Series module is 1G (or 10 percent of the 10G line rate).</li> </ul>
<b>Step 5</b>	switch(config-erspan-src)# <b>exit</b>	Exits monitor configuration mode.
<b>Step 6</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 7</b>	(Optional) switch# <b>show monitor session</b> <i>session-number</i>	Displays the status of ERSPAN sessions, including the configuration status of the rate limit, the percentage of the maximum ERSPAN rate allowed per session, and the modules on which the rate limit is and is not supported.
<b>Step 8</b>	(Optional) switch# <b>copy running-config startup-config [vdc-all]</b>	Copies the running configuration to the startup configuration.

## Configuring Sampling for Each ERSPAN Session

Beginning with Cisco NX-OS Release 6.1, you can configure a sampling range for spanned traffic in order to reduce the ERSPAN traffic bandwidth and to monitor peer-to-peer traffic. Packet range-based sampling is used to provide an accurate count of the ERSPAN source packets.



### Note

Sampling and MTU truncation can be enabled at the same time and have no precedence over each other because they are applied to different aspects of the source packet (packet count versus size). However, sampling takes precedence over ERSPAN source rate limiting. Rate limiting takes effect after sampling is completed on ERSPAN source packets.

### Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor session</b> <i>session-number</i> <b>type erspan-source</b>	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which ERSPAN sampling is to be configured.
<b>Step 3</b>	(Optional) switch(config-erspan-src)# <b>header-type version</b>	Changes the ERSPAN source session from Type II to Type III.
<b>Step 4</b>	switch(config-erspan-src)# [ <b>no</b> ] <b>sampling range</b>	Configures the sampling range for ERSPAN source packets. The sampling value is the range in which one packet out of x packets will be spanned, where x is from 2 to 1023. In this example, 1 out of every 100 packets will be spanned.
<b>Step 5</b>	switch(config-erspan-src)# <b>exit</b>	Exits monitor configuration mode.
<b>Step 6</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 7</b>	(Optional) switch# <b>show monitor session</b> <i>session-number</i>	Displays the status of ERSPAN sessions, including the configuration status of ERSPAN sampling, the sampling value, and the modules on which sampling is and is not supported.
<b>Step 8</b>	(Optional) switch# <b>copy running-config</b> <b>startup-config</b> [ <b>vdc-all</b> ]	Copies the running configuration to the startup configuration.

## Configuring the Multicast Best Effort Mode for an ERSPAN Session

You can configure the multicast best effort mode for any ERSPAN session. By default, ERSPAN replication occurs on both the ingress and egress modules. When you enable the multicast best effort mode, ERSPAN replication occurs only on the ingress module for multicast traffic or on the egress module for packets that egress out of Layer 3 interfaces (that is, on the egress module, packets that egress out of Layer 2 interfaces are not replicated for ERSPAN).

**Note**

For Layer 3 multicast traffic, ERSPAN replication occurs on the egress module. If traffic is multicasted to multiple egress modules, you could capture multiple ERSPAN copies for each packet (that is, one copy from each egress module).

**Before you begin**

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor session</b> <i>session-number type erspan-source</i>	Enters the monitor configuration mode for the ERSPAN source type and specifies the ERSPAN session for which the multicast best effort mode is to be configured.
<b>Step 3</b>	(Optional) switch(config-erspan-src)# <b>header-type version</b>	Changes the ERSPAN source session from Type II to Type III.
<b>Step 4</b>	switch(config-erspan-src)# <b>[no] multicast</b> <b>best-effort</b>	Configures the multicast best effort mode for the specified ERSPAN session.

## Configuring Rule-Based ERSPAN

You can configure filters for ingress or egress ERSPAN traffic based on a set of rules. A simple filter has only one rule, and multiple fields or conditions can be added to this rule. The packets are spanned only if all conditions are met.

**Before you begin**

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor erspan origin</b> <b>ip-address ip-address global</b>	Configures the ERSPAN global origin IP address.  The global origin IP address can be configured in either the default VDC or the admin VDC. The value that is configured in this VDC is valid across all VDCs. Any change made in the default or admin VDC is applied across all nondefault VDCs.
<b>Step 3</b>	(Optional) switch(config)# <b>monitor erspan</b> <b>granularity {100_ms   100_ns   1588   ns}</b>	Specifies the granularity of all ERSPAN Type III sessions across all VDCs. The granularity options are 100 microseconds (ms), 100 nanoseconds (ns), IEEE 1588 (in seconds or nanoseconds), and nanoseconds.

	Command or Action	Purpose
		<p><b>Note</b> The clock manager adjusts the ERSPAN timers based on the granularity setting. If you configure IEEE 1588, the clock manager synchronizes the ERSPAN timers across switches. Otherwise, the clock manager synchronizes the ERSPAN timer with the master timer in the switch.</p> <p><b>Note</b> 1588 granularity mode is not supported in Cisco NX-OS Release 6.1 and is rejected if selected.</p> <p><b>Note</b> M2 Series modules support 100 ms, 100 ns, and ns granularity. F2 series and F2e Series modules support only 100 ms and 100 ns granularity.</p> <p><b>Note</b> This command can be applied only in the default VDC.</p>
<b>Step 4</b>	switch(config)# <b>no monitor session</b> { <i>session-number</i>   <b>all</b> }	Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.
<b>Step 5</b>	switch(config)# <b>monitor session</b> { <i>session-number</i>   <b>all</b> } <b>type erspan-source</b> [ <b>rx</b>   <b>tx</b> ] [ <b>shut</b> ]	<p>Configures an ERSPAN Type II source session. By default the session is bidirectional. The optional keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>rx</b>—Specifies an ingress extended ERSPAN source session.</li> <li>• <b>tx</b>—Specifies an egress extended ERSPAN source session.</li> <li>• <b>shut</b>—Specifies a shut state for the selected session.</li> </ul>
<b>Step 6</b>	(Optional) switch(config-erspan-src)# <b>mode extended</b>	<p>Configures the ERSPAN source session as an extended bidirectional session.</p> <p><b>Note</b> You cannot use this command on a unidirectional ERSPAN source session.</p>
<b>Step 7</b>	(Optional) switch(config-erspan-src)# <b>header-type version</b>	Changes the ERSPAN source session from Type II to Type III.

	Command or Action	Purpose
		<b>Note</b> You can use the <b>no</b> form of this command to change an ERSPAN source session from Type III to Type II.
<b>Step 8</b>	(Optional) switch(config-erspan-src)# <b>description</b> <i>description</i>	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.
<b>Step 9</b>	switch(config-erspan-src)# [ <b>no</b> ] <b>filter</b> [ <b>access-group</b> <i>acl-filter</i> ] [ <b>vlan</b> <i>vlan-range</i> ] [ <b>bpdu</b> [ <b>true</b>   <b>false</b> ]] [ <b>cos</b> <i>cos-value</i> ] [ <b>dest-mac</b> <i>dest-mac</i> ] [ <b>eth-type</b> <i>eth-value</i> ] [ <b>flow-hash</b> <i>flow-value</i> ] [ <b>frame-type</b> [ <b>eth</b>   <b>arp</b>   <b>fcoe</b>   <b>ipv4</b>   <b>ipv6</b> ]] [ <b>pc-lane</b> <i>port-number</i> ] [ <b>src_mac</b> <i>mac-address</i> ] [ <b>trace-route</b> [ <b>true</b>   <b>false</b> ]]	Configures the filter for the ERSPAN session. To remove the filter from the session, enter the <b>no</b> form of the command. The optional keywords are as follows: <ul style="list-style-type: none"> <li>• <b>access-group</b>—Specifies a filter based on an access control group.</li> <li>• <b>vlan</b>—Specifies a filter based on a VLAN range.</li> <li>• <b>bpdu</b>—Specifies a filter based on the bridge protocol data unit (BPDU) class of packets.</li> <li>• <b>cos</b>—Specifies a filter based on the class of service (CoS) in the dot1q header.</li> <li>• <b>dest-mac</b>—Specifies a filter based on a destination MAC address.</li> <li>• <b>eth-type</b>—Specifies a filter based on the Ethernet type.</li> <li>• <b>flow-hash</b>—Specifies a filter based on the result bundle hash (RBH) value.</li> <li>• <b>frame-type</b>—Specifies a filter based on a frame type.</li> <li>• <b>pc-lane</b>—Specifies a filter based on a member of the port channel.</li> <li>• <b>src-mac</b>—Specifies a filter based on a source MAC address.</li> <li>• <b>trace-route</b>—Specifies a filter based on the route bit in the header.</li> </ul>
<b>Step 10</b>	(Optional) switch(config-erspan-src)# [ <b>no</b> ] <b>filter frame-type eth</b>	Configures the Ethernet frame type filter for the ERSPAN session. To remove the filter from the session, enter the <b>no</b> form of the command.

	Command or Action	Purpose
<b>Step 11</b>	(Optional) switch(config-erspan-src)# <b>[no]</b> <b>filter frame-type arp</b> [[ <b>arp-rarp</b> [ <b>arp</b>   <b>rarp</b> ]] [ <b>req-resp</b> [ <b>req</b>   <b>rsp</b> ]] [ <b>sender-ip</b> <i>ip-address</i> ] [ <b>target-ip</b> <i>ip-address</i> ]]	Configures the ARP frame type filter for the ERSPAN session. To remove the filter from the session, enter the <b>no</b> form of the command. <ul style="list-style-type: none"> <li>• <b>arp-rarp</b>—Specifies an ARP or RARP frame type filter.</li> <li>• <b>req-resp</b>—Specifies a filter based on a request or response.</li> <li>• <b>sender-ip</b>—Specifies a filter based on a sender IP address.</li> <li>• <b>target-ip</b>—Specifies a filter based on a target IP address.</li> </ul>
<b>Step 12</b>	(Optional) switch(config-erspan-src)# <b>[no]</b> <b>filter frame-type fcoe</b> [[ <b>fc-sid</b> <i>FC-source-ID</i> ] [ <b>fc-did</b> <i>FC-dest-ID</i> ] [ <b>fcoe-type</b> <i>fcoe-value</i> ] [ <b>r-ctl</b> <i>r-ctl-value</i> ] [ <b>sof</b> <i>sof-value</i> ] [ <b>cmd-code</b> <i>cmd-value</i> ]]	Configures the FCoE frame type filter for the ERSPAN session. To remove the filter from the session, enter the <b>no</b> form of the command. The optional keywords are as follows: <ul style="list-style-type: none"> <li>• <b>fc-sid</b>—Specifies a filter based on an FC source ID.</li> <li>• <b>fc-did</b>—Specifies a filter based on an FC destination ID.</li> <li>• <b>fcoe-type</b>—Specifies a filter based on an FCoE type.</li> <li>• <b>r-ctl</b>—Specifies a filter based on the routing control flags (R CTL) value.</li> <li>• <b>sof</b>—Specifies a filter based on the start of frame (SOF) packets.</li> <li>• <b>cmd-code</b>—Specifies a filter based on a command code.</li> </ul>
<b>Step 13</b>	(Optional) switch(config-erspan-src)# <b>[no]</b> <b>filter frame-type ipv4</b> [[ <b>src-ip</b> <i>src-ip</i> ] [ <b>dest-ip</b> <i>dest-ip</i> ] [ <b>tos</b> <i>tos-value</i> ] [ <b>l4-protocol</b> <i>l4-value</i> ]]	Configures the IPv4 frame type filter for the ERSPAN session. To remove the filter from the session, enter the <b>no</b> form of the command. The optional keywords are as follows: <ul style="list-style-type: none"> <li>• <b>src-ip</b>—Specifies a filter based on an IPv4 source IP address.</li> <li>• <b>dest-ip</b>—Specifies a filter based on an IPv4 destination IP address.</li> <li>• <b>tos</b>—Specifies a filter based on the type of service (ToS) in the IP header.</li> </ul>



	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <b>l4-protocol</b>—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.</li> </ul>
<b>Step 14</b>	(Optional) switch(config-erspan-src)# <b>[no]</b> <b>filter frame-type ipv6</b> <b>[[src-ip src-ip ]</b> <b>[dest-ip dest-ip] [tos tos-value] [l4-protocol</b> <b>l4-value]]</b>	Configures the IPv6 frame type filter for the ERSPAN session. To remove the filter from the session, enter the <b>no</b> form of the command. The optional keywords are as follows: <ul style="list-style-type: none"> <li>• <b>src-ip</b>—Specifies a filter based on an IPv6 source IP address.</li> <li>• <b>dest-ip</b>—Specifies a filter based on an IPv6 destination IP address.</li> <li>• <b>tos</b>—Specifies a filter based on the type of service (ToS) in the IP header.</li> <li>• <b>l4-protocol</b>—Specifies a filter based on a Layer 4 protocol number set in the protocol field of the IP header.</li> </ul>
<b>Step 15</b>	(Optional) Repeat Steps 9 to 14 for all filters for the session.	—
<b>Step 16</b>	switch(config-erspan-src)# <b>source</b> <b>{[interface</b> <b>[type slot/port [-port] [,type slot/port[-port]]</b> <b>[port-channel channel-number]]   [vlan</b> <b>{number   range}]]} [rx   tx   both]</b>	Configures sources and the traffic direction in which to copy packets. You can enter a range of Ethernet ports, a port channel, an inband interface, a range of VLANs, a Cisco Nexus 2000 Series Fabric Extender interface, or a fabric port channel connected to a Cisco Nexus 2000 Series Fabric Extender.  You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify up to 128 interfaces. The VLAN range is from 1 to 3967. The VLAN range of 4048 to 4093 is also supported for Cisco NX-OS releases prior to 6.1.  You can specify the traffic direction to copy as ingress (rx), egress (tx), or both. By default, the direction is both.  For a unidirectional session, the direction of the source must match the direction specified in the session.
<b>Step 17</b>	(Optional) Repeat Step 16 to configure all ERSPAN sources.	—

	Command or Action	Purpose
<b>Step 18</b>	switch(config-erspan-src)# <b>destination ip</b> <i>ip-address</i>	Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session.  <b>Note</b> The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as ERSPAN destinations.
<b>Step 19</b>	switch(config-erspan-src)# <b>erspan-id</b> <i>erspan-id</i>	Configures the ERSPAN ID for the ERSPAN session. The ERSPAN range is from 1 to 1023.
<b>Step 20</b>	switch(config-erspan-src)# <b>vrf</b> <i>vrf-name</i>	Configures the VRF instance that the ERSPAN source session uses for traffic forwarding. The VRF name can be any case-sensitive, alphanumeric string up to 32 characters.
<b>Step 21</b>	(Optional) switch(config-erspan-src)# <b>ip ttl</b> <i>ttl-number</i>	Configures the IP time-to-live (TTL) value for the ERSPAN traffic. The range is from 1 to 255.
<b>Step 22</b>	(Optional) switch(config-erspan-src)# <b>ip dscp</b> <i>dscp-number</i>	Configures the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic. The range is from 0 to 63.
<b>Step 23</b>	switch(config-erspan-src)# <b>no shut</b>	Enables the ERSPAN session. By default, the session is created in the shut state.
<b>Step 24</b>	switch(config-erspan-src)# <b>exit</b>	Exits monitor configuration mode.
<b>Step 25</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 26</b>	(Optional) switch# <b>show monitor session</b> {all   <i>session-number</i>   <b>range</b> <i>session-range</i> } [ <b>brief</b> ]	Displays the status of ERSPAN sessions, including the configuration status of the multicast best effort mode and the modules on which the best effort mode is and is not supported.
<b>Step 27</b>	(Optional) switch# <b>copy running-config</b> <b>startup-config</b>	Copies the running configuration to the startup configuration.

## Configuring Exception ERSPAN

You can configure the device to span exception packets.

### Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>monitor session</b> <i>session-number</i> <b>type erspan-source</b> [ <b>rx</b>   <b>tx</b> ] [ <b>shut</b> ]	Enters the monitor configuration mode and specifies the ERSPAN session. The exception ERSPAN is supported in the egress direction only. In the case of an extended ERSPAN Rx session, the exception source configuration will be rejected. The optional keywords are as follows: <ul style="list-style-type: none"> <li>• <b>rx</b>—Specifies an ingress extended ERSPAN source session.</li> <li>• <b>tx</b>—Specifies an egress extended ERSPAN source session.</li> <li>• <b>shut</b>—Specifies a shut state for the selected session.</li> </ul>
<b>Step 3</b>	(Optional) switch(config-erspan-src)# <b>mode extended</b>	Configures the ERSPAN session as an extended bidirectional session.
<b>Step 4</b>	switch(config-erspan-src)# <b>source exception</b> { <b>layer3</b>   <b>fabricpath</b>   <b>other</b>   <b>all</b> }	Configures the source as an exception ERSPAN session. These exception types are supported: <ul style="list-style-type: none"> <li>• <b>layer3</b>—Specifies the Layer 3 exception type for F2 Series and M Series modules.</li> <li>• <b>fabricpath</b>—Specifies the FabricPath exception type for F Series modules.</li> <li>• <b>other</b>—Specifies exceptions for M Series modules that are dropped through redirect registers programmed with a drop destination interface.</li> <li>• <b>all</b>—Includes all Layer 3, FabricPath, and other exceptions.</li> </ul>
<b>Step 5</b>	switch(config-erspan-src)# <b>destination ip</b> <i>ip-address</i>	Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session. <p><b>Note</b> The Cisco Nexus 2000 Series Fabric Extender interfaces and the fabric port channels connected to the FEX cannot be configured as ERSPAN destinations.</p>

	Command or Action	Purpose
<b>Step 6</b>	switch(config-erspan-src)# <b>no shut</b>	Enables the ERSPAN session. By default, the session is created in the shut state.
<b>Step 7</b>	switch(config-erspan-src)# <b>exit</b>	Exits module configuration mode.
<b>Step 8</b>	switch(config)# <b>exit</b>	Exits global configuration mode.
<b>Step 9</b>	(Optional) switch# <b>show monitor session</b> <i>session-number</i>	Displays the status of ERSPAN sessions, including the configuration status of the multicast best effort mode and the modules on which the best effort mode is and is not supported.
<b>Step 10</b>	(Optional) switch# <b>copy running-config</b> <b>startup-config</b> [vdc-all]	Copies the running configuration to the startup configuration.

## Verifying the ERSPAN Configuration

To display the ERSPAN configuration, perform one of the following tasks:

Command	Purpose
<b>show monitor session</b> {all   <i>session-number</i>   range <i>session-range</i> } [brief]	Displays the ERSPAN session configuration.
<b>show running-config monitor</b>	Displays the running ERSPAN configuration.
<b>show startup-config monitor</b>	Displays the ERSPAN startup configuration.
<b>show resource monitor-session-extended</b>	Displays the resources that are available for the extended session.
<b>show resource monitor-session-mx-exception-src</b>	Displays the resources that are available for the exception session.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*.

## Configuration Examples for ERSPAN

### Configuration Example for an ERSPAN Type III Source Session

This example shows how to configure an ERSPAN Type III source session:

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
```

```
switch(config-if)# exit
switch(config)# monitor erspan origin ip-address 3.3.3.3 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# source interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

## Configuration Example to Monitor All VLANs and Ports in an Extended ERSPAN Monitor Session

This example shows how to monitor all VLANs and ports in an extended ERSPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# destination interface ethernet 14/29
switch(config-monitor)# vrf default
switch(config-monitor)# erspan-id 200
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 1
switch(config)# copy running-config startup-config
```

This example shows how to monitor a higher number of specific VLAN sources than the VLAN source limits currently supported in an extended ERSPAN monitor session:

```
switch# configure terminal
switch(config)# monitor session 2 type erspan-source
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all tx
switch(config-monitor)# destination ip 192.0.2.1
switch(config-monitor)# vrf default
switch(config-monitor)# erspan-id 200
switch(config-monitor)# filter vlan 1-1000
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 2
switch(config)# copy running-config startup-config
```

## Configuration Example for a Unidirectional ERSPAN Session

This example shows how to configure a unidirectional ERSPAN session:

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
```

```

switch(config-erspan-src)# source interface ethernet 2/1-3 rx
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1

```

## Configuration Example for an ERSPAN Destination Session

This example shows how to configure an ERSPAN destination session:

```

switch# configure terminal
switch(config)# interface e14/29
switch(config-if)# no shut
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2 type erspan-destination
switch(config-erspan-dst)# source ip 9.1.1.2
switch(config-erspan-dst)# destination interface e14/29
switch(config-erspan-dst)# erspan-id 1
switch(config-erspan-dst)# vrf default
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
switch(config)# show monitor session 2

```

## Configuration Example for an ERSPAN ACL

This example shows how to configure an ERSPAN 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)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# vlan access-map erspan_filter 5
switch(config-access-map)# match ip address match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map erspan_filter 10
switch(config-access-map)# match ip address match_12_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# filter access_group erspan_filter

```

## Configuration Example for ERSPAN with MTU Truncation and ERSPAN Sampling

This example shows how to configure MTU truncation and ERSPAN sampling for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mtu 100
switch(config-erspan-src)# sampling 10
switch(config-erspan-src)# show monitor session 1
```

## Configuration Example for ERSPAN Using the Multicast Best Effort Mode

This example shows how to configure the multicast best effort mode for an ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# multicast best-effort
switch(config-erspan-src)# show monitor session 1
```

## Configuration Example for Rule-Based ERSPAN

This example shows how to configure a rule-based ERSPAN session:

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 10.0.0.1 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# no monitor session 3
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# description erspan_src_session_3
switch(config-erspan-src)# filter frame-type ipv4 src-ip 10.1.1.1/24
switch(config-erspan-src)# filter vlan 10,20
switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-erspan-src)# destination ip 10.1.1.1
switch(config-erspan-src)# erspan-id 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# ip ttl 25
switch(config-erspan-src)# ip dscp 42
switch(config-erspan-src)# no shut
switch# show monitor session 3
```

## Configuration Example for Exception ERSPAN

This example shows how to configure an exception ERSPAN session:

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# source exception all
switch(config-erspan-src)# destination ip 10.1.1.1
```

```
switch(config-erspan-src)# no shut
switch# show monitor session 3
```

## Related Documents

Related Topic	Document Title
ERSPAN commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco Nexus 7000 Series NX-OS System Management Command Reference</i>
VDCs	<i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide</i>
Cisco Network Analysis Module (NAM)	<i>Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide</i>
Fabric Extender	<i>Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide</i>

## Feature History for ERSPAN

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release.

**Table 2: Feature History for ERSPAN**

Feature Name	Releases	Feature Information
ERSPAN	7.3(0)DX(1)	Added support for ERSPAN source and destination sessions on M3 Series modules.
ERSPAN	7.3(0)D1(1)	Added support for 4K VLANs per ERSPAN Session.
ERSPAN	6.2(2)	Added support for ERSPAN destination sessions on F2 and F2e Series modules.
ERSPAN	6.2(2)	Added NAM support for ERSPAN data sources.
ERSPAN	6.2(2)	Added support for extended ERSPAN.
ERSPAN	6.2(2)	Added support for rule-based ERSPAN.



ERSPAN	6.2(2)	Added support for exception ERSPAN.
ERSPAN	6.2(2)	Added support for ERSPAN termination on F2 or F2e Series modules.
ERSPAN	6.1(2)	Added support for F2e Series modules.
ERSPAN	6.1(1)	Added support for ERSPAN Type III.
ERSPAN	6.1(1)	Added support for Supervisor 2.
ERSPAN	6.1(1)	Added support for F2 and M2 Series modules.
ERSPAN	6.1(1)	Added support for ERSPAN sampling.
ERSPAN	6.1(1)	Added the ability to configure MTU truncation and the source rate limit for each ERSPAN session.
ERSPAN	6.0(1)	ERSPAN and ERSPAN ACLs are not supported on F2 Series modules.
ERSPAN	5.2(1)	Added ERSPAN source support for Cisco Nexus 2000 Series Fabric Extender interfaces.
ERSPAN	5.2(1)	Added the ability to configure the multicast best effort mode for an ERSPAN session.
ERSPAN and ERSPAN ACLs	5.1(1)	This feature was introduced.
ERSPAN	7.2	ERSPAN source sessions are supported on F3 Series modules. However, ERSPAN ACL sessions are not supported on F3 Series modules.

