



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:

- [About ERSPAN, on page 1](#)
- [Licensing Requirements for ERSPAN, on page 3](#)
- [Prerequisites for ERSPAN, on page 3](#)
- [Guidelines and Limitations for ERSPAN, on page 4](#)
- [Default Settings, on page 7](#)
- [Configuring ERSPAN, on page 7](#)
- [Verifying the ERSPAN Configuration, on page 17](#)
- [Configuration Examples for ERSPAN, on page 17](#)
- [Additional References, on page 20](#)

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 Nexus 9300 Series switches support ERSPAN Type II and Type III, and Cisco Nexus 9500 Series switches support only ERSPAN.

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

- Provides Precision Time Protocol (PTP) timestamp information (defined in IEEE 1588) 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.



Note For more information on PTP, see [Configuring PTP](#).

ERSPAN Marker Packet

The ERSPAN Type III header carries a hardware-generated 32-bit timestamp. This timestamp field wraps periodically. When the switch is set to 1 ns granularity, this field wraps every 4.29 seconds. Such a wrap time makes it difficult to interpret the real value of the timestamp.

To recover the real value of the ERSPAN timestamp, you can configure a periodical marker packet to carry the original UTC timestamp information and provide a reference for the ERSPAN timestamp. The marker packet is sent out in 1-second intervals. Therefore, the destination site can detect the 32-bit wrap by checking the difference between the timestamp of the reference packet and the packet order.

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 (but not subinterfaces)
- Port channels
- The inband interface to the control plane CPU
- VLANs



Note When a VLAN is specified as an ERSPAN source, all supported interfaces in the VLAN are ERSPAN sources.



Note VLANs can be ERSPAN sources only in the ingress direction.

- Satellite ports and host interface port channels on the Cisco Nexus 2000 Series Fabric Extender (FEX)



Note These interfaces are supported in Layer 2 access mode and Layer 2 trunk mode. They are not supported in Layer 3 mode, and Layer 3 subinterfaces are not supported.



Note FEX ports are supported as ERSPAN sources in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.



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

ERSPAN Sessions

You can create ERSPAN sessions that designate sources to monitor.

Localized ERSPAN Sessions

An ERSPAN session is localized when all of the source interfaces are on the same line card.



Note An ERSPAN session with a VLAN source is not localized.

ERSPAN Truncation

Beginning with Cisco NX-OS Release 7.0(3)I7(1), you can configure the truncation of source packets for each ERSPAN session based on the size of the MTU. Truncation helps to decrease ERSPAN bandwidth by reducing the size of monitored packets. Any ERSPAN packet that is larger than the configured MTU size is truncated to the given size. For ERSPAN, an additional ERSPAN header is added to the truncated packet from 54 to 166 bytes depending on the ERSPAN header type. For example, if you configure the MTU as 300 bytes, the packets are replicated with an ERSPAN header size from 354 to 466 bytes depending on the ERSPAN header type configuration.

ERSPAN truncation is disabled by default. To use truncation, you must enable it for each ERSPAN session.

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 9000 Series NX-OS High Availability and Redundancy Guide](#).

Licensing Requirements for ERSPAN

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	ERSPAN requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco NX-OS Licensing 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 9000 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 9000 Series NX-OS Verified Scalability Guide*.
- The number of ERSPAN sessions per line card reduces to two if the same interface is configured as a bidirectional source in more than one session.
- Only ERSPAN source sessions are supported. Destination sessions are not supported.
- Configuring two SPAN or ERSPAN sessions on the same source interface, with only one filter is not supported.
- Statistics are not supported for the filter access group.
- An access-group filter in an ERSPAN session must be configured as `vlan-accessmap`.
- All ERSPAN replication is performed in the hardware. The supervisor CPU is not involved.
- Control plane packets that are generated by the supervisor cannot be ERSPAN encapsulated or filtered by an ERSPAN access control list (ACL).
- ERSPAN is not supported for management ports.
- ERSPAN does not support destinations on Layer 3 port-channel subinterfaces.
- ERSPAN and ERSPAN ACL sessions are terminated identically at the destination router only when the ERSPAN destination IP address is resolved through Cisco Nexus 9300 Series switch uplink ports.
- ERSPAN does not support destinations on N9K-X9408PC-CFP2 line card ports.
- Cisco Nexus 9500 Series switches with a X9732C-EX line card support ERSPANv2 or ERSPANv3 headers in spanned copy. Cisco Nexus 9300 Series switches support ERSPANv2 or ERSPANv3 headers but only for sessions with 40G uplink SPAN destinations.
- Supervisor-generated stream of bytes module header (SOBMH) packets have all the information to go out on an interface and can bypass all forwarding lookups in the hardware, including SPAN and ERSPAN. CPU-generated frames for Layer 3 interfaces and the Bridge Protocol Data Unit (BPDU) class of packets are sent using SOBMH. This guideline does not apply for Cisco Nexus 9508 switches with N9K-X9636C-R and N9K-X9636Q-R line cards. The Cisco Nexus N9K-X9636C-R and N9K-X9636Q-R both support inband SPAN and local SPAN.
- A VLAN can be part of only one session when it is used as an ERSPAN source or filter.
- VLAN ERSPAN monitors only the traffic that leaves or enters Layer 2 ports in the VLAN.
- If you enable ERSPAN on a vPC and ERSPAN packets must be routed to the destination through the vPC, packets that come through the vPC peer link cannot be captured.
- ERSPAN is not supported over a VXLAN overlay.
- ERSPAN copies for multicast packets are made before rewrite. Therefore, the TTL, VLAN ID, any remarking due to egress policy, and so on, are not captured in the ERSPAN copy.

- The timestamp granularity of ERSPAN Type III sessions is not configurable through the CLI. It is 100 picoseconds and driven through PTP.
- ERSPAN works on default and nondefault VRFs, but ERSPAN marker packets work only on the default VRF.
- Marker packet for ERSPAN is not supported on Cisco Nexus 9508 switches with an N9K-X9732C-EX line card.
- Cisco Nexus 9300 and 9500 Series switches support multiple ACL filters on the same source.
- The same source can be part of multiple sessions.

The following guidelines and limitations apply to egress (Tx) ERSPAN:

- Cisco Nexus 9300 Series switches do not support Tx ERSPAN on 40G uplink ports.
- The flows for post-routed unknown unicast flooded packets are in the ERSPAN session, even if the ERSPAN session is configured to not monitor the ports on which this flow is forwarded. This limitation applies to Network Forwarding Engine (NFE) and NFE2-enabled EOR switches and ERSPAN sessions that have TX port sources.
- For Tx interface ERSPAN with Layer 2 switch port and port-channel sources on Cisco Nexus 9300-EX Series switches, only one copy is made per receiver unit regardless of how many Layer 2 members are receiving the stream in the same VLAN. For example, if e1/1-8 are all Tx direction ERSPAN sources and all are joined to the same group, the ERSPAN destination port sees one pre-rewrite copy of the stream, not eight copies. In addition, if for any reason one or more of those ports drops the packets on egress (for example, due to congestion), the packets may still reach the ERSPAN destination port. For the N9K-X9732C-EX line card, one copy is made per unit that has members. For port-channel sources, the Layer 2 member that will SPAN is the first port-channel member.
- ERSPAN Tx broadcast and ERSPAN Tx multicast are supported for Layer 2 port and port-channel sources across slices on Cisco Nexus 9300-EX Series switches and the Cisco Nexus N9K-X9732C-EX line card but only when IGMP snooping is disabled. (Otherwise, the slice limitation still applies.) These features are not supported for Layer 3 port sources, FEX ports (with unicast or multicast traffic), and VLAN sources.

The following guidelines and limitations apply to ingress (Rx) ERSPAN:

- VLAN sources are spanned only in the Rx direction.
- Session filtering functionality (VLAN or ACL filters) is supported only for Rx sources.
- A single forwarding engine instance supports four ERSPAN sessions. For Cisco Nexus 9300 Series switches, if the first three sessions have bidirectional sources, the fourth session has hardware resources only for Rx sources. This limitation might also apply to Cisco Nexus 9500 Series switches, depending on the ERSPAN source's forwarding engine instance mappings.
- An ERSPAN copy of Cisco Nexus 9300 Series switch 40G uplink interfaces will miss the dot1q information when spanned in the Rx direction.
- VLANs are supported as ERSPAN sources only in the ingress direction.

The following guidelines and limitations apply to FEX ports:

- If the sources used in bidirectional ERSPAN sessions are from the same FEX, the hardware resources are limited to two ERSPAN sessions.

- FEX ports are supported as ERSPAN sources in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.
- The Cisco Nexus 9300 Series does not support ERSPAN destination being connected on a FEX interface. The ERSPAN destination must be connected to a front panel port.
- VLAN and ACL filters are not supported for FEX ports.

Priority flow control (PFC) ERSPAN has the following guidelines and limitations:

- PFC (Priority Flow Control) and LLFC (Link-Level Flow Control) are supported for all Cisco Nexus 9300 and 9500 platform switches except for the 100 Gb 9408PC line card and the 100 Gb M4PC generic expansion module (GEM).
- It is not supported on Cisco Nexus 9300 Series uplink ports.
- It cannot co-exist with filters.
- It is supported only in the Rx direction on physical or port-channel interfaces. It is not supported in the Rx direction on VLAN interfaces or in the Tx direction.

The following guidelines and limitations apply to Cisco Nexus 9200 Series switches:

- The **set-erspan-gre-proto** and **set-erspan-dscp** actions for ERSPAN ACLs are supported.
- UDF-based ERSPAN is supported.
- ERSPAN supports forward drops.
- Rx ERSPAN is not supported for multicast if the ERSPAN source and destination are on the same slice and no forwarding interface is on the slice. It is supported if a forwarding interface is on the slice or if the ERSPAN source and destination are on different slices.
- When multiple egress ports on the same slice are congested by egressing ERSPAN traffic, those egress ports will not get the line rate.
- The CPU ERSPAN source can be added only for the Rx direction (ERSPAN packets coming from the CPU).
- Using the ACL filter to span subinterface traffic on the parent interface is not supported.
- Multiple ACL filters are not supported on the same source.

The following guidelines and limitations apply to ERSPAN truncation:

- Truncation is supported only for Cisco Nexus 9300-EX and 9300-FX platform switches.
- Truncation is supported only for local and ERSPAN source sessions. It is not supported for ERSPAN destination sessions.
- For ERSPAN sessions, the configured MTU value excludes the ERSPAN header. The egress packet for ERSPAN will have the MTU value + the number of bytes for the ERSPAN header.
- The bytes specified are retained starting from the header of the packets. The rest are truncated if the packet is longer than the MTU.
- The cyclic redundancy check (CRC) is recalculated for the truncated packet.

Default Settings

The following table lists the default settings for ERSPAN parameters.

Table 1: Default ERSPAN Parameters

Parameters	Default
ERSPAN sessions	Created in the shut state

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.



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

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	monitor erspan origin ip-address <i>ip-address</i> global Example: switch(config)# monitor erspan origin ip-address 10.0.0.1 global	Configures the ERSPAN global origin IP address.
Step 3	no monitor session {<i>session-number</i> all} Example: switch(config)# no monitor session 3	Clears the configuration of the specified ERSPAN session. The new session configuration is added to the existing session configuration.

	Command or Action	Purpose
Step 4	<p>monitor session {<i>session-number</i> all} type erspan-source [shut]</p> <p>Example:</p> <pre>switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#</pre>	Configures an ERSPAN Type II source session. By default the session is bidirectional. The optional keyword shut specifies a shut state for the selected session.
Step 5	<p>description <i>description</i></p> <p>Example:</p> <pre>switch(config-erspan-src)# description erspan_src_session_3</pre>	Configures a description for the session. By default, no description is defined. The description can be up to 32 alphanumeric characters.
Step 6	<p>source {interface <i>type</i> [rx tx both] vlan {<i>number</i> <i>range</i>} [rx]} [</p> <p>Example:</p> <pre>switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx</pre> <p>Example:</p> <pre>switch(config-erspan-src)# source interface port-channel 2</pre> <p>Example:</p> <pre>switch(config-erspan-src)# source interface sup-eth 0 both</pre> <p>Example:</p> <pre>switch(config-erspan-src)# source vlan 3, 6-8 rx</pre> <p>Example:</p> <pre>switch(config-erspan-src)# source interface ethernet 101/1/1-3</pre>	<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, a range of VLANs, or a satellite port or host interface port channel on the Cisco Nexus 2000 Series Fabric Extender (FEX).</p> <p>You can configure one or more sources, as either a series of comma-separated entries or a range of numbers. You can specify the traffic direction to copy as ingress, egress, or both.</p> <p>For a unidirectional session, the direction of the source must match the direction specified in the session.</p> <p>Note Source VLANs are supported only in the ingress direction. Source FEX ports are supported in the ingress direction for all traffic and in the egress direction only for known Layer 2 unicast traffic.</p>
Step 7	(Optional) Repeat Step 7 to configure all ERSPAN sources.	—
Step 8	<p>(Optional) filter vlan {<i>number</i> <i>range</i>}</p> <p>Example:</p> <pre>switch(config-erspan-src)# filter vlan 3-5, 7</pre>	<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 9000 Series NX-OS Layer 2 Switching Configuration Guide</i>.</p> <p>Note A FEX port that is configured as an ERSPAN source does not support VLAN filters.</p>
Step 9	(Optional) Repeat Step 9 to configure all source VLANs to filter.	—

	Command or Action	Purpose
Step 10	(Optional) filter access-group <i>acl-filter</i> Example: switch(config-erspan-src) # filter access-group ACL1	Associates an ACL with the ERSPAN session. (You can create an ACL using the standard ACL configuration process. For more information, see the <i>Cisco Nexus 9000 Series NX-OS Security Configuration Guide</i> .)
Step 11	destination ip <i>ip-address</i> Example: switch(config-erspan-src) # destination ip 10.1.1.1	Configures the destination IP address in the ERSPAN session. Only one destination IP address is supported per ERSPAN source session.
Step 12	erspan-id <i>erspan-id</i> Example: switch(config-erspan-src) # erspan-id 5	Configures the ERSPAN ID for the ERSPAN source session. The ERSPAN range is from 1 to 1023.
Step 13	vrf <i>vrf-name</i> Example: switch(config-erspan-src) # vrf default	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.
Step 14	(Optional) ip ttl <i>tll-number</i> Example: switch(config-erspan-src) # ip ttl 25	Configures the IP time-to-live (TTL) value for the ERSPAN traffic. The range is from 1 to 255.
Step 15	(Optional) ip dscp <i>dscp-number</i> Example: switch(config-erspan-src) # ip dscp 42	Configures the differentiated services code point (DSCP) value of the packets in the ERSPAN traffic. The range is from 0 to 63.
Step 16	no shut Example: switch(config-erspan-src) # no shut	Enables the ERSPAN source session. By default, the session is created in the shut state.
Step 17	exit Example: switch(config-erspan-src) # exit switch(config) #	Exits the monitor configuration mode.
Step 18	(Optional) show monitor session {all <i>session-number</i> range <i>session-range</i> } [brief] Example: switch(config) # show monitor session 3	Displays the ERSPAN session configuration.
Step 19	(Optional) show running-config monitor Example: switch(config) # show running-config monitor	Displays the running ERSPAN configuration.

	Command or Action	Purpose
Step 20	(Optional) show startup-config monitor Example: <pre>switch(config)# show startup-config monitor</pre>	Displays the ERSPAN startup configuration.
Step 21	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	monitor session {session-range all} shut Example: <pre>switch(config)# monitor session 3 shut</pre>	Shuts down the specified ERSPAN sessions. By default, sessions are created in the shut state.
Step 3	no monitor session {session-range all} shut Example: <pre>switch(config)# no monitor session 3 shut</pre>	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 monitor session shut command followed by the no monitor session shut command.
Step 4	monitor session session-number type erspan-source Example:	Enters the monitor configuration mode for the ERSPAN source type. The new session configuration is added to the existing session configuration.

	Command or Action	Purpose
	<pre>switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#</pre>	
Step 5	shut Example: <pre>switch(config-erspan-src)# shut</pre>	Shuts down the ERSPAN session. By default, the session is created in the shut state.
Step 6	no shut Example: <pre>switch(config-erspan-src)# no shut</pre>	Enables the ERSPAN session. By default, the session is created in the shut state.
Step 7	exit Example: <pre>switch(config-erspan-src)# exit switch(config)#</pre>	Exits the monitor configuration mode.
Step 8	(Optional) show monitor session all Example: <pre>switch(config)# show monitor session all</pre>	Displays the status of ERSPAN sessions.
Step 9	(Optional) show running-config monitor Example: <pre>switch(config)# show running-config monitor</pre>	Displays the ERSPAN running configuration.
Step 10	(Optional) show startup-config monitor Example: <pre>switch(config)# show startup-config monitor</pre>	Displays the ERSPAN startup configuration.
Step 11	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Configuring an ERSPAN ACL

You can create an IPv4 ERSPAN ACL on the device and add rules to it.

Before you begin

To modify the DSCP value or the GRE protocol, you need to allocate a new destination monitor session. A maximum of four destination monitor sessions are supported.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	ip access-list <i>acl-name</i> Example: <pre>switch(config)# ip access-list erspan-acl switch(config-acl)#</pre>	Creates the ERSPAN ACL and enters IP ACL configuration mode. The <i>acl-name</i> argument can be up to 64 characters.
Step 3	<p>[<i>sequence-number</i>] {permit deny} <i>protocol source destination</i> [set-erspan-dscp dscp-value] [set-erspan-gre-proto protocol-value]</p> <p>Example:</p> <pre>switch(config-acl)# permit ip 192.168.2.0/24 any set-erspan-dscp 40 set-erspan-gre-proto 5555</pre>	<p>Creates a rule in the ERSPAN ACL. You can create many rules. The <i>sequence-number</i> argument can be a whole number between 1 and 4294967295.</p> <p>The permit and deny commands support many ways of identifying traffic.</p> <p>The set-erspan-dscp option sets the DSCP value in the ERSPAN outer IP header. The range for the DSCP value is from 0 to 63. The DSCP value configured in the ERSPAN ACL overrides the value configured in the monitor session. If you do not include this option in the ERSPAN ACL, 0 or the DSCP value configured in the monitor session will be set.</p> <p>The set-erspan-gre-proto option sets the protocol value in the ERSPAN GRE header. The range for the protocol value is from 0 to 65535. If you do not include this option in the ERSPAN ACL, the default value of 0x88be will be set as the protocol in the GRE header for ERSPAN-encapsulated packets.</p> <p>Each access control entry (ACE) with the set-erspan-gre-proto or set-erspan-dscp action consumes one destination monitor session. A maximum of three ACEs with one of these actions is supported per ERSPAN ACL. For example, you can configure one of the following:</p> <ul style="list-style-type: none"> • One ERSPAN session with an ACL having a maximum of three ACEs with the set-erspan-gre-proto or set-erspan-dscp action • One ERSPAN session with an ACL having two ACEs with the set-erspan-gre-proto

	Command or Action	Purpose
		or set-erspan-dscp action and one additional local or ERSPAN session <ul style="list-style-type: none"> • A maximum of two ERSPAN sessions with an ACL having one ACE with the set-erspan-gre-proto or set-erspan-dscp action
Step 4	(Optional) show ip access-lists <i>name</i> Example: <pre>switch(config-acl)# show ip access-lists erspan-acl</pre>	Displays the ERSPAN ACL configuration.
Step 5	(Optional) show monitor session { all <i>session-number</i> range <i>session-range</i> } [brief] Example: <pre>switch(config-acl)# show monitor session 1</pre>	Displays the ERSPAN session configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch(config-acl)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Configuring UDF-Based ERSPAN

You can configure the device to match on user-defined fields (UDFs) of the outer or inner packet fields (header or payload) and to send the matching packets to the ERSPAN destination. Doing so can help you to analyze and isolate packet drops in the network.

Before you begin

Make sure that the appropriate TCAM region (racl, ifacl, or vacl) has been configured using the **hardware access-list tcam region** command to provide enough free space to enable UDF-based ERSPAN. For information, see the "Configuring ACL TCAM Region Sizes" section in the [Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#).

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	udf <i>udf-name</i> <i>offset-base</i> <i>offset</i> <i>length</i> Example:	Defines the UDF as follows:

	Command or Action	Purpose
	<pre>switch(config)# udf udf-x packet-start 12 1 switch(config)# udf udf-y header outer 13 20 2</pre>	<ul style="list-style-type: none"> • <i>udf-name</i>—Specifies the name of the UDF. You can enter up to 16 alphanumeric characters for the name. • <i>offset-base</i>—Specifies the UDF offset base as follows, where header is the packet header to consider for the offset: packet-start header {outer inner {13 14}}. • <i>offset</i>—Specifies the number of bytes offset from the offset base. To match the first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0. • <i>length</i>—Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs. <p>You can define multiple UDFs, but Cisco recommends defining only required UDFs.</p>
Step 3	<p>hardware access-list tcam region {racl ifacl vACL} qualify udf <i>udf-names</i></p> <p>Example:</p> <pre>switch(config)# hardware access-list tcam region racl qualify udf udf-x udf-y</pre>	<p>Attaches the UDFs to one of the following TCAM regions:</p> <ul style="list-style-type: none"> • racl—Applies to Layer 3 ports. • ifacl—Applies to Layer 2 ports. • vACL—Applies to source VLANs. <p>You can attach up to 8 UDFs to a TCAM region.</p> <p>Note When the UDF qualifier is added, the TCAM region goes from single wide to double wide. Make sure enough free space is available; otherwise, this command will be rejected. If necessary, you can reduce the TCAM space from unused regions and then re-enter this command. For more information, see the "Configuring ACL TCAM Region Sizes" section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.</p>

	Command or Action	Purpose
		<p>Note The no form of this command detaches the UDFs from the TCAM region and returns the region to single wide.</p>
Step 4	<p>Required: copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.
Step 5	<p>Required: reload</p> <p>Example:</p> <pre>switch(config)# reload</pre>	<p>Reloads the device.</p> <p>Note Your UDF configuration is effective only after you enter copy running-config startup-config + reload.</p>
Step 6	<p>ip access-list erspan-acl</p> <p>Example:</p> <pre>switch(config)# ip access-list erspan-acl-udf-only switch(config-acl)#</pre>	Creates an IPv4 access control list (ACL) and enters IP access list configuration mode.
Step 7	<p>Enter one of the following commands:</p> <ul style="list-style-type: none"> • permit udf udf-name value mask • permit ip source destination udf udf-name value mask <p>Example:</p> <pre>switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F</pre> <p>Example:</p> <pre>switch(config-acl)# permit ip 10.0.0./24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F</pre>	<p>Configures the ACL to match only on UDFs (example 1) or to match on UDFs along with the current access control entries (ACEs) for the outer packet fields (example 2).</p> <p>A single ACL can have ACEs with and without UDFs together. Each ACE can have different UDF fields to match, or all ACEs can match for the same list of UDFs.</p>
Step 8	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Configuring ERSPAN Truncation

You can configure truncation for local and ERSPAN source sessions only.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	monitor session <i>session-number</i> Example: switch(config)# monitor session 5 switch(config-monitor)#	Enters monitor configuration mode for the specified ERSPAN session.
Step 3	source interface <i>type slot/port [rx tx both]</i> Example: switch(config-monitor)# source interface ethernet 1/5 both	Configures the source interface.
Step 4	mtu <i>size</i> Example: switch(config-monitor)# mtu 512	Configures the MTU size for truncation. Any ERSPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU size range is 512 to 1518 bytes for Cisco Nexus 9300-EX platform switches and 64 to 1518 bytes for Cisco Nexus 9300-FX platform switches.
Step 5	destination interface <i>type slot/port</i> Example: switch(config-monitor)# destination interface Ethernet 1/39	Configures the Ethernet ERSPAN destination port.
Step 6	no shut Example: switch(config-monitor)# no shut	Enables the ERSPAN session. By default, the session is created in the shut state.
Step 7	(Optional) show monitor session <i>session</i> Example: switch(config-monitor)# show monitor session 5	Displays the ERSPAN configuration.
Step 8	copy running-config startup-config Example: switch(config-monitor)# copy running-config startup-config	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
show monitor session {all <i>session-number</i> range <i>session-range</i> } [brief]	Displays the ERSPAN session configuration.
show running-config monitor	Displays the running ERSPAN configuration.
show startup-config monitor	Displays the ERSPAN startup configuration.

Configuration Examples for ERSPAN

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 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)# filter access_group erspan_filter
```

Configuration Example for a Marker Packet

This example shows how to enable the ERSPAN marker packet with an interval of 2 seconds:

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 172.28.15.250 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
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)# source interface ethernet 1/15 both
switch(config-erspan-src)# marker-packet 100
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1
session 1
-----
type           : erspan-source
state          : up
granularity    : nanoseconds
erspan-id      : 1
vrf-name       : default
destination-ip : 9.1.1.2
ip-ttl         : 16
ip-dscp        : 5
header-type    : 3
origin-ip      : 172.28.15.250 (global)
source intf    :
  rx           : Eth1/15
  tx           : Eth1/15
  both         : Eth1/15
source VLANs   :
  rx           :
marker-packet  : enabled
packet interval : 100
packet sent    : 25
packet failed  : 0
egress-intf    :
```

Configuration Examples for UDF-Based ERSPAN

This example shows how to configure UDF-based ERSPAN to match on the inner TCP flags of an encapsulated IP-in-IP packet using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + Outer IP (20) + Inner IP (20) + Inner TCP (20, but TCP flags at 13th byte)
- Offset from packet-start: 14 + 20 + 20 + 13 = 67

- UDF match value: 0x20
- UDF mask: 0xFF

```

udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify udf udf_tcpflags
copy running-config startup-config
reload
ip access-list acl-udf
    permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1 type erspan-source
    source interface Ethernet 1/1
    filter access-group acl-udf

```

This example shows how to configure UDF-based ERSPAN to match regular IP packets with a packet signature (DEADBEEF) at 6 bytes after a Layer 4 header start using the following match criteria:

- Outer source IP address: 10.0.0.2
- Inner TCP flags: Urgent TCP flag is set
- Bytes: Eth Hdr (14) + IP (20) + TCP (20) + Payload: 112233445566DEADBEEF7788
- Offset from Layer 4 header start: 20 + 6 = 26
- UDF match value: 0xDEADBEEF (split into two-byte chunks and two UDFs)
- UDF mask: 0xFFFFFFFF

```

udf udf_pktsig_msb header outer 13 26 2
udf udf_pktsig_lsb header outer 13 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb udf_pktsig_lsb
copy running-config startup-config
reload
ip access-list acl-udf-pktsig
    permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1 type erspan-source
    source interface Ethernet 1/1
    filter access-group acl-udf-pktsig

```

Configuration Example for ERSPAN Truncation

This example shows how to configure ERSPAN truncation for use with MPLS stripping:

```

mpls strip
ip access-list mpls
    statistics per-entry
    20 permit ip any any redirect Ethernet1/5

interface Ethernet1/5
    switchport
    switchport mode trunk
    mtu 9216
    no shutdown

monitor session 1
    source interface Ethernet1/5 tx
    mtu 64
    destination interface Ethernet1/6
    no shut

```

```

monitor session 21 type erspan-source
  description "ERSPAN Session 21"
  header-type 3
  erspan-id 21
  vrf default
  destination ip 19.1.1.2
  source interface Ethernet1/5 tx
  mtu 64
  no shut
monitor session 22 type erspan-source
  description "ERSPAN Session 22"
  erspan-id 22
  vrf default
  destination ip 19.2.1.2
  source interface Ethernet1/5 tx
  mtu 750
  no shut
monitor session 23 type erspan-source
  description "ERSPAN Session 23"
  header-type 3
  marker-packet 1000
  erspan-id 23
  vrf default
  destination ip 19.3.1.2
  source interface Ethernet1/5 tx
  mtu 1000
  no shut

```

Additional References

Related Documents

Related Topic	Document Title
FEX	<i>Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 9000 Series Switches</i>