Configuring Span

This chapter describes port and EFP span. This chapter also describes procedures to configure port and EFP span.

Understanding Span

Span

Span is a technique of replicating the ingress or egress frames in a specific port to a specified list of destination ports. It is a monitoring feature used to monitor the traffic that is coming in and out of a port, channel group, or an Ethernet Flow Point (EFP). The monitored traffic can be used to debug the network and can also be used by law enforcement agencies.

The span can be configured to monitor ingress traffic, egress traffic, or both. The span source can be a physical port, channel group, or an EFP. The span destination can be a physical port or a channel group.

CPT supports two span modes:

- Port Span—In this configuration, the ingress or egress traffic on all the Ethernet Virtual Circuits (EVCs) in the source port or channel group is captured on the destination port or channel group. The pseudowire or tunnel port is not supported as a span destination.
- EFP Span—In this configuration, the ingress or egress traffic on the specified EFPs on a particular port or channel group is captured on the destination port or channel group. All types of services such as Multiprotocol Label Switching (MPLS), Virtual Private LAN Service (VPLS), Virtual Private Wire Service (VPWS), xconnect can be monitored. The pseudowire or tunnel port is not supported as a span destination.

Span Session

A span session is a collection of span source and destination ports, where traffic from each source port (based on their span direction) is replicated to the destination ports. Both the egress and ingress spans can be configured in a single session. A span destination port must not be a source of another span session. A span destination port cannot be shared among different sessions. CPT supports up to 50 span sessions.

Limitations and Restrictions of Port and EFP Span in CPT

- CPT supports only local span and not remote span. Therefore, the destination port or channel group can be any port or channel group on the same card or on different card on the same node.
- A port on the CPT 50 fanned out from a fabric card can be a destination span port only if the source span port is also on the same CPT 50.
- A span source port on a CPT 50 fanned out from a line card and a span destination port on another CPT 50 fanned out from another line card is not supported. If traffic is affected due to this issue, remove the span and reload the line card that has the fanout of the destination CPT 50 span.
- For egress span of the line card, only Ethernet Virtual Private LAN (EVPLAN) traffic is supported. The operations, administration, and maintenance (OAM) control traffic is not replicated.
- The span destination can only be a port or a channel group and not an EFP. The span source can be a port, channel group, or an EFP.
- If a channel group is selected as a destination port, the member ports of the channel group cannot be selected as destination ports.
- The egress span for the line card is supported only for point-to-multipoint traffic.
- The EFP, Resilient Ethernet Protocol (REP), Ethernet in the first mile (EFM) loopback, Link Aggregation Control Protocol (LACP), and Quality of Service (QoS) cannot be configured on the span destination port.
- For port span, two egress span destinations and three ingress span destinations for each card is supported.
- For EFP span, one egress span destination for each card is supported.
- For EFP span, three ingress span destinations for each card is supported. When you add the fourth destination port to the span, the traffic is not received on the three destination ports.
- The maximum egress span bandwidth traffic is 10 Gbps for each card; the maximum egress span bandwidth traffic for the line card is 16 Gbps for the CPT system.
- CPT can monitor up to 256 EFPs for each fabric card, line card (ingress), and CPT 50 panel.
- CPT can monitor up to 150 EFPs in the entire CPT system for line card egress span.
- If there are multiple source ports, the traffic sent by each source port is not equally shared on the destination port.
- If other services are available on a port, a service with default encap cannot be created on that port and vice-versa
- On MPLS-TP port, no service can be created.
- If QoS policy is attached to a port, span destination port cannot be configured on that.
- If the service is tagged, MVR cannot be enabled on that.

- If a port is MPLS-TP core port, span destination port cannot be configured on that.
- If a port is FOG port, span destination port cannot be configured on that.
- A port that has egress policy in the port-channel as a member-link cannot be associated.

NTP-J119 Configure a Span Using Cisco IOS Commands

Purpose	This procedure configures a span using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J359 Configure a Port Span Using Cisco IOS Commands, on page 3
- DLP-J360 Configure an EFP Span Using Cisco IOS Commands, on page 5
- DLP-J362 Restrict the Destination Ports for a Span Using Cisco IOS Commands, on page 7
- DLP-J361 Verify the Span Configuration Using Cisco IOS Commands, on page 8

Stop. You have completed this procedure.

DLP-J359 Configure a Port Span Using Cisco IOS Commands

Purpose	This procedure configures a port span using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**monitor session** *local_span_session_number* type *span-type* **Example:** Router(config)# monitor session 3 type local	Configures a monitor session using a SPAN session number and enters the SPAN session configuration mode. The *local_span_session_number* values range from 1 to 50. Only local span type is supported.
Step 4	**source interface** *type number direction* **Example:** Router(config-mon-local)# source interface TenGigabitEthernet 4/1 rx	Configures a port span for the source port and selects the traffic direction to be monitored. The *direction* accepts the following values: • **both—**Monitors received and transmitted traffic (both ingress and egress). • **rx—**Monitors received traffic (ingress). • **tx—**Monitors transmitted traffic (egress).
Step 5	**destination interface** *type number* **Example:** Router(config-mon-local)# destination interface TenGigabitEthernet 5/1	Configures a port span for the destination port.
Step 6	**exit** **Example:** Router(config-mon-local)# exit	Returns to global configuration mode.
Step 7	Return to your originating procedure (NTP).	—

Example: Configure a Port Span

The following example shows how to configure a port span using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# monitor session 3 type local
```

```
Router(config-mon-local)# source interface TenGigabitEthernet 4/1 rx
Router(config-mon-local)# destination interface TenGigabitEthernet 5/1
Router(config-mon-local)# exit
```

DLP-J360 Configure an EFP Span Using Cisco IOS Commands

Purpose	This procedure configures an EFP span using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface TenGigabitEthernet 4/1	Specifies the interface to configure and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** [*evc-id*] **Example:** Router(config-if)# service instance 101 ethernet	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **second-dot1q** {*any* | *vlan-id* [*vlan-id* [*-vlan-id*]]} **Example:** Router(config-if-srv)# encapsulation dot1q 100 second dot1q 200	Defines the matching criteria that maps the ingress dot1q, QinQ, or untagged frames on an interface to the appropriate service instance.

	Command or Action	Purpose
Step 6	**rewrite ingress tag** {**push** {**dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **pop** {**1** | **2**} | **translate** {**1-to-1** {**dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **2-to-1 dot1q** *vlan-id* | **dot1ad** *vlan-id*}| **1-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*} | **2-to-2** {**dot1q** *vlan-id* **second-dot1q** *vlan-id* | **dot1ad** *vlan-id* **dot1q** *vlan-id*}} {**symmetric**} **Example:** Router(config-if-srv)# rewrite ingress tag push dot1q 20	Specifies the rewrite operation to be applied on the frame ingress to the service instance.
Step 7	exit **Example:** Router(config-if-srv)# exit	Exits to global configuration mode.
Step 8	**monitor session** *local_span_session_number* type *span-type* **Example:** Router(config)# monitor session 3 type local	Configures a monitor session using a SPAN session number and enters the SPAN session configuration mode. The *local_span_session_number* values range from 1 to 50. Only local span type is supported.
Step 9	**source service instance** *EFP_number type number* **direction** **Example:** Router(config-mon-local)# source service instance 1 – 512 TenGigabitEthernet 4/1 rx	Configures an EFP span for the source port and selects the traffic direction to be monitored. The *EFP_number* can be a specific EFP or a range of EFPs. The range is from 1 to 32768. The *direction* values are as follows: • **both—**Monitors received and transmitted traffic (both ingress and egress). • **rx—**Monitors received traffic (ingress). • **tx—**Monitors transmitted traffic (egress).
Step 10	**destination interface** *type number* **Example:** Router(config-mon-local)# destination interface TenGigabitEthernet 5/1	Configures an EFP span for the destination port.

	Command or Action	Purpose
Step 11	**end** **Example:** Router(config-mon-local)# end	Exits configuration mode.
Step 12	Return to your originating procedure (NTP).	—

Example: Configure an EFP Span

The following example shows how to configure an EFP span for a channel group using Cisco IOS commands:

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel 11
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 13
Router(config-if-srv)# rewrite ingress tag push dot1q 20 symmetric
Router(config-if-srv)# exit
Router(config)# monitor session 3 type local
Router(config-mon-local)# source service instance 2 - 200 Port-channel 1 both
Router(config-mon-local)# destination interface TenGigabitEthernet 5/1
Router(config-mon-local)# end
```

DLP-J362 Restrict the Destination Ports for a Span Using Cisco IOS Commands

Purpose	This procedure enables you to restrict the destination ports that can be used for a span session using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**monitor permit-list destination interface** *type number* **Example:** Router(config)# monitor permit-list destination interface TenGigabitEthernet 4/1	Restricts the destination ports that can be used for a span session.
Step 4	**exit** **Example:** Router(config)# exit	Returns to privileged EXEC mode.
Step 5	Return to your originating procedure (NTP).	—

DLP-J361 Verify the Span Configuration Using Cisco IOS Commands

Purpose	This procedure verifies the span configuration using Cisco IOS commands.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

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

Step 2	**show monitor session all**
	
	Example:
		Displays the configuration of all the span sessions.
		
		`Session 1`
		`---------`

	Command or Action	Purpose
	Router# show monitor session all	Type : Local Session Status : Admin Disabled Source Ports : RX Only : Te5/1 Destination Ports : Gi55/26,Gi55/44 Session 5 --------- Type : Local Session Status : Admin Disabled Source EFPs : RX Only : Te5/1: 1 Destination Ports : Te5/4
Step 3	**show monitor permit-list** **Example:** Router# show monitor permit-list	Displays the destination ports that can be used for a span session. SPAN Permit-list :Admin Disabled Permit-list ports :Te3/2
Step 4	Return to your originating procedure (NTP).	—

NTP-J118 Configure a Span Using CTC

Purpose	This procedure configures a span using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Perform any of the following procedures as needed:

- DLP-J357 Configure a Port or EFP Span Using CTC, on page 10
- DLP-J358 Restrict the Destination Ports for a Span Using CTC, on page 11

Stop. You have completed this procedure.

DLP-J357 Configure a Port or EFP Span Using CTC

Purpose	This procedure enables you to configure a port or EFP span using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-J2 Create an EVC Circuit Using CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The span destination can only be a port or a channel group and not an EFP. The span source can be a port, channel group, or an EFP.

Procedure

Step 1 Complete the NTP-J22 Log into CTC procedure at a node where you want to configure a span.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** > **Span** > **Span** tabs.

Step 4 Click **Create**. The Create Span dialog box appears.

Step 5 From the Span type drop-down list, choose **Port** or **EFP**.

Step 6 To set the port span type:

a) In the Source Information area, click **Add** to add the source ports or channel groups.
b) In the Add Source dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
c) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
d) From the Available Ports/Available CHGRPS list, choose the required source ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.
e) Choose **Ingress**, **Egress**, or **Both** for the direction of the span.
f) Click **OK** to close the Add Source dialog box.
The specified details appear in the Source Information area in the Create Span dialog box.
g) In the Destination Information area, click **Add** to add the destination ports or channel groups.
h) In the Add Destination dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
i) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
j) From the Available Ports/Available CHGRPS list, choose the required destination ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.
A port or channel group cannot be specified as a destination port if it carries traffic and has a service ID configured.
k) Click **OK** to close the Add Destination dialog box.

The specified details appear in the Destination Information area in the Create Span dialog box.

Step 7 To set the EFP span type:

a) In the Source Information area, click **Add** to add the source EFPs.
b) In the Add Source dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
c) Enter the Service ID of the EFP in the Service ID field.
If a proper service ID is not specified, the span configuration does not work.
d) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
e) (For Slot/Port interface type) From the Port drop-down list, choose a port.
f) (For CHGRP interface type) From the CHGRP drop-down list, choose a channel group.
g) Choose **Ingress**, **Egress**, or **Both** for the direction of the span.
h) Click **OK** to close the Add Source dialog box.
The specified details appear in the Source Information area in the Create Span dialog box.
i) In the Destination Information area, click **Add** to add the destination ports or channel groups.
j) In the Add Destination dialog box, choose **Slot/Port** or **CHGRP** as an interface type.
k) (For Slot/Port interface type) From the Slot drop-down list, choose a slot.
l) From the Available Ports/Available CHGRPS list, choose the required destination ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.
A port or channel group cannot be specified as a destination port if it carries traffic and has a service ID configured.
m) Click **OK** to close the Add Destination dialog box.
The specified details appear in the Destination Information area in the Create Span dialog box.

Step 8 Click **Add** to create a port or EFP span.
You can also edit or delete a port or EFP span from the Span tab. The span type cannot be changed while editing a span.

Step 9 Return to your originating procedure (NTP).

DLP-J358 Restrict the Destination Ports for a Span Using CTC

Purpose	This procedure enables you to restrict the destination ports that can be used for a span session using CTC.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Only the ports in the Permit List tab can be specified as a destination port while creating a span session. If the Permit List tab is empty, all the ports can be specified as destination ports for the span session except the source span ports.

Procedure

Step 1 Complete the NTP-J22 Log into CTC procedure at a node where you want to restrict the destination ports for a span session.

Step 2 Right-click the fabric or line card and choose **Open Packet Transport System View**. The Packet Transport System View dialog box appears.

Step 3 Click the **Provisioning** > **Span** > **Permit List** tabs.

Step 4 Click **Add**. The Add Source dialog box appears.

Step 5 In the Add Source dialog box, choose **Slot/Port** or **CHGRP** as an interface type.

Step 6 (For Slot/Port interface type) From the Slot drop-down list, choose a slot.

Step 7 From the Available Ports/Available CHGRPS list, choose the required destination ports or channel groups and click the right arrow to move them to the Selected Ports/Selected CHGRPS list.

Step 8 Click **OK** to close the Add Source dialog box.
The ports that can be specified as destination ports appear in the Permit List tab.

Step 9 Return to your originating procedure (NTP).