Contents

1 Configuring SPAN

1.1 Overview

Switch port analyzer (SPAN) is a function that copies packets of a specified port to another port that is connected to a network monitoring device, so as to achieve network monitoring and troubleshooting.

1.1.1 Basic Concepts

1. Session

A session must contain a source port and an output port.

2. Source Port

A source port is also called a monitored port. In a SPAN session, data streams of the source port are monitored for network analysis and troubleshooting.

3. Destination Port

A destination port is also called a monitoring port, and used to receive packets from the source port in a SPAN session.

4. Source Device

A source device is a role in remote SPAN (RSPAN) where the source port resides. It copies packets of the source port and outputs them through the output port of the source device to an intermediate device or the destination device.

5. Reflector Port

A reflector port can be used for "one-to-many RSPAN" (mirroring packets from one port to multiple destination ports). Packets entering a device from the SPAN source port are output from the output port through "reflection" of the reflector port.

6. Destination Device

A destination device is a role in RSPAN where the destination port resides. It forwards the mirrored packets received from the intermediate or source device to the monitoring device through the SPAN destination port.

7. Output Port

An output port on the source device is used to send mirrored packets to a port on an intermediate device or a destination device.

8. SPAN Data Streams

A SPAN session covers data streams in three directions:

- Input data streams

All packets received by a source port are copied to the destination port. Users can monitor input packets of one or more source ports in a SPAN session.

- Output data streams

All packets transmitted by a source port are copied to the destination port. Users can monitor output packets of one or more source ports in a SPAN session.

- Bidirectional data streams

Bidirectional data streams include input data streams and output data streams. In a SPAN session, users can monitor data streams of one or more source ports in the input and output directions.
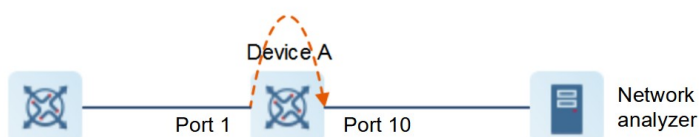
1.1.2 Working Process

SPAN is divided into SPAN, RSPAN, and encapsulated remote switch port analyzer (ERSPAN), depending on whether the source port and destination port of a SPAN session reside on the same device.

1. SPAN Working Process

SPAN is also called local SPAN. In SPAN, the source port and destination port of the same SPAN session must reside on the same device. SPAN can be used to monitor data streams that pass through a device. It copies frames from a port to another port that is connected to a network analyzer to analyze the communication of the port. As shown in Figure 1-1, all packets on port 1 are copied to port 10, and the network analyzer connected to port 10 receives all packets that pass through port 1. The specific process is as follows:

(1) The device identifies and marks the incoming and outgoing packets of the source port.

(2) The device searches for the SPAN session to which the monitored port belongs.

(3) The device searches for the destination port corresponding to the SPAN session.

(4) The device copies packets and sends them to the destination port.

(5) The destination port sends the copied packets to the analyzer.

Figure 1-1   SPAN Principles

2. RSPAN Working Process

RSPAN is an extension of SPAN. It breaks the limitation that the source port and destination port of the same SPAN session must reside on the same device, and allows the source port and the destination port to span multiple network devices. A remote VLAN is created for the source device, intermediate device, and destination device, and all ports involved in an RSPAN session must be added to the remote VLAN. Mirrored packets are broadcast in the remote VLAN so that they are transmitted from the source port of the source device to the destination port of the destination device. Figure 1-1 shows the specific working process.

Figure 1-1   RSPAN Principles
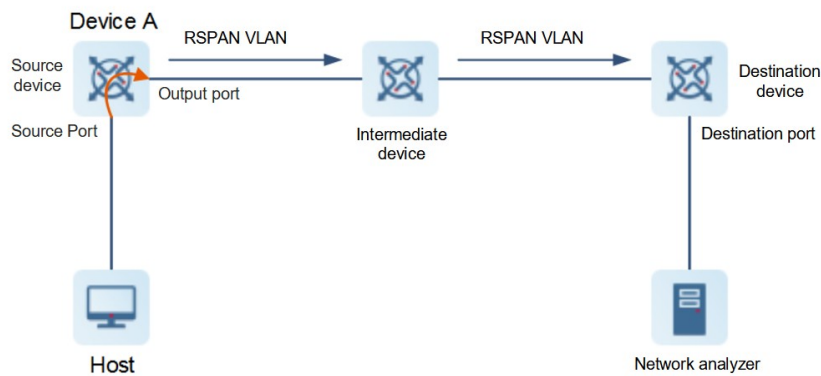
(1) Source device

A source device is where the RSPAN source port resides. It copies packets of the source port, and outputs them through the output port of the source device. These packets are forwarded through the remote VLAN to an intermediate device or the destination device.

(2) Intermediate device

An intermediate device resides between the source device and the destination device. It forwards the mirrored packets through the remote VLAN to a next intermediate device or the destination device.

> 🛈 **Note**
>
> If the source device is directly connected to the destination device, there is no intermediate device.

(3) Destination device

A destination device is where the RSPAN destination port resides. It forwards the mirrored packets received from the remote VLAN to the monitoring device through the RSPAN destination port.

3. **ERSPAN Working Process**

ERSPAN is an extension of RSPAN. RSPAN packets can be transmitted only at Layer 2 and cannot pass through routing networks. However, ERSPAN can encapsulate the mirrored packets to IP packets through the GRE tunnel and route them to the destination port of the RSPAN device, thus transmitting mirrored packets between routing networks.

Figure 1-1 shows how to forward ERSPAN packets.

(1) The source device copies and encapsulates the incoming packets of the source port.

  ○ Encapsulate the source and destination IP addresses of the GRE packet.

  ○ Set the TTL and DSCP of the GRE packet.

  Figure 1-2 shows the header format of a packet encapsulated in ERSPAN.

(2) The source port forwards mirrored packets to the destination device through the GRE tunnel.

(3) The destination device decapsulates GRE packets to remove the header encapsulated by ERSPAN, and forwards the packets to the destination port.

(4) The destination port forwards the mirrored packets to the data analyzer.

> ⚠ **Caution**

The IP packets after GRE encapsulation can be normally routed to the destination device in the network. Therefore, the destination IP address is generally the next-hop IP address of the route. That is, the output port of the source device is the next-hop egress of the L3 path where the destination IP address to be encapsulated is located. The output port must be reachable, and can be an SVI, an L3AP, or a routed port.

Figure 1-1   ERSPAN Principles
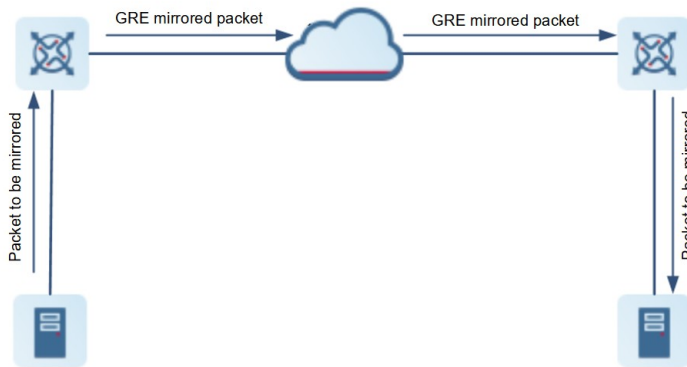
Figure 1-2   Format of an Encapsulated Packet in ERSPAN

MAC_HEADER(14/18B)	IP_HEADER(20B)	GRE_HEADER(48B)	L2_Mirrored_Packet(untagged)

4. **Stream Mirroring Principles**

Stream mirroring is to associate the source port with an ACL on the basis of SPAN, and filter packets based on the ACL rules, so as to mirror only specified packets. Only the packets matching the permit ACE in the ACL on the source port can be mirrored to the destination port. A source port can be associated with only one ACL. Currently, the standard ACL, extended ACL, MAC ACL, and custom ACL can be associated.

ACL-based SPAN is supported only in the receive (RX) direction, but not in the transmit (TX) direction.

1.2 Restrictions and Guidelines

- A source port has the following features:
  - The source port can be an L2 port, L3 port, or aggregation port.
  - Data streams on multiple source ports on the source device can be mirrored to a specified output port.
  - The source port and the output port cannot be the same one.
  - When the source port is an L3 port, L2 and L3 packets can be monitored.
  - Upon bidirectional monitoring of multiple ports, a packet is received from one port and output from another port, and monitoring is effective as long as one packet is monitored among these ports.
  - When a port is STP enabled and in the block state, the incoming and outgoing packets of the port can

also be monitored.

- o The source port and the destination port can belong to the same VLAN or different VLANs.

● A destination port has the following features:

- o The destination port can be a switched port, a routed port, or an aggregation port.

- o A destination port cannot be used as a source port simultaneously.

- o The SPAN destination port is used for the Spanning Tree Protocol (STP) calculation.

● A configured session ID cannot be used as the ID of another SPAN session.

● If a source port is added to an aggregation port, the source port exits the SPAN session.

By default, the switch function is disabled on the SPAN destination port, and the destination port only receives mirrored packets and does not forward data. If the destination port needs to forward data, the switch function must be enabled; otherwise, packets passing through this port will be discarded.

● Due to other reasons (such as port security), incoming packets of a source port may be discarded, but it does not affect the SPAN function, and these packets are still mirrored to the destination port. Due to other reasons, packets sent from other ports to a source port may be discarded, and these packets are not sent to the destination port.

● If the format of a packet output from the source port is changed, for example, the source MAC, destination MAC, VLAN ID, and TTL of the packet change, the format of the packet mirrored to the destination port will change as well.

● You can configure the following types of ACL on the source port to filter mirrored packets: standard ACL, extended ACL, MAC ACL, and custom ACL.

1.3 Configuration Task Summary

SPAN configuration includes the following tasks:

● Configuring SPAN

● Configuring RSPAN

● Configuring ERSPAN

- a Configuring Basic Functions of ERPSAN

- b (Optional) Configuring Stream-based ERSPAN

- c   (Optional) Configuring ERSPAN Attributes

1.4 Configuring SPAN

1.4.1 Overview

SPAN copies packets of the designated port or designated VLAN to the port connected to the data monitoring device, so that you can use the data monitoring device to analyze these copied packets for network monitoring and troubleshooting.

1.4.2 Restrictions and Guidelines

● When configuring the SPAN source port, you can specify the following items as the data source simultaneously: some VLANs, an interface, and specified streams on the specified port.

- When configuring the SPAN source port, if you specify a VLAN as the data source, you cannot specify an interface or streams on the specified port as the data source.

- When configuring the SPAN source port, if you specify some VLANs as the data source, you must also specify the source port.

- If you change the VLAN configuration on the source port, the configuration takes effect immediately.

- If you change the VLAN configuration on the destination port, the configuration takes effect immediately.

- If you disable the source or destination port, the SPAN function does not take effect.

- If you configure a VLAN or a VLAN list as the SPAN source, ensure that the destination port has sufficient bandwidth for receiving mirrored data of the entire VLAN (or VLAN list).

- If you add or delete a VLAN source port to or from an effective SPAN session, you need to re-apply the entire SPAN session. Therefore, a few existing mirrored packets may be lost.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a SPAN source port. Configure at least one of the following tasks.

○ Specify an interface as the data source of SPAN.

monitor session *session-number* **source interface** *interface-type interface-number* [**both** | **rx** | **tx**]

○ Specify some streams of an interface as the data source of SPAN.

monitor session *session-number* **source interface** *interface-type interface-number* **rx acl** { *acl-name* | *acl-number* }

○ Exclude one or more VLANs as the data source of SPAN.

monitor session *session-num* **filter vlan** *vlan-id-list* **rx**

This command must be configured together with monitor session source **interface** or monitor session source **interface acl**

○ Specify one or more VLANs as the data source of SPAN.

monitor session *session-num* **source vlan** *vlan-id-list* **rx**

This configuration is mutually exclusive with the preceding three configurations.

By default, no source port is configured for a SPAN session.

(4) Configure a SPAN destination port.

monitor session *session-num* **destination interface** *interface-type interface-number* [**switch**]

By default, no SPAN destination port is configured.

1.5 Configuring RSPAN

1.5.1 Overview

- Configure a source port and destination port on the source device of an RSPAN session and configure the destination port on the destination device.

- Configure the destination port on the RSPAN destination device to monitor any packets that are transmitted or received by the source port.

1.5.2 Restrictions and Guidelines

- All ports involved in RSPAN must be added to a remote VLAN.

- A remote VLAN must be configured on each device, their VLAN IDs must be consistent, and all ports that participate in a session must be added to the VLAN. It is not recommended that common ports be added to a remote VLAN.

- Do not configure a port that is connected to an intermediate device or a destination device as an RSPAN source port. Otherwise, traffic on the network may be in chaos.

- The reflector port cannot serve as a normal port to forward packets. You are advised to configure a port in Down state as the reflector port, and not to add other configurations for this port.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN configuration mode.

vlan *vlan-id*

(4) Configure a remote VLAN.

remote-span

By default, no remote VLAN is configured.

(5) Exit the VLAN configuration mode.

exit

(6) Configure an RSPAN source device.

monitor session *session-num* **remote-source**

By default, no source device is configured for an RSPAN session.

(7) (Optional) Configure the MAC loopback function on the source device.

a   Enter the interface configuration mode.

interface *interface-type interface-number*

b   Enable the MAC loopback function of the interface.

mac-loopback

By default, MAC loopback is disabled for an interface.

(8) Configure a source port on the source device. Configure at least one of the following tasks.

○ Specify an interface as the data source of ERSPAN.

monitor session *session-number* **source interface** *interface-type interface-number* [**both** | **rx** | **tx**]

○ Specify streams of an interface as the data source of RSPAN.

monitor session *session-number* **source interface** *interface-type interface-number* **rx acl** { *acl-name* | *acl-number* }

By default, no source port on the source device is configured for an RSPAN session.

(9) Configure an RSPAN destination device.

monitor session *session-num* **remote-destination**

By default, no destination device is configured for an RSPAN session.

(10) Configure an output port on the source device or a destination port on the destination device.

monitor session *session-number* **destination remote vlan** *remote-vlan-id* **interface** *interface-type interface-number* [**switch**]

By default, no output port on the RSPAN source device or no destination port on the RSPAN destination device is configured.

1.6 Configuring ERSPAN

1.6.1 Configuration Tasks

ERSPAN configuration includes the following tasks:

(1) Configuring Basic Functions of ERPSAN

(2) (Optional) Configuring Stream-based ERSPAN

(3) (Optional) Configuring ERSPAN Attributes

1.6.2 Configuring Basic Functions of ERPSAN

1.   Overview

After ERSPAN is configured, a network analyzer can be used to monitor users. Devices can normally exchange data with each other.

2.   Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ERSPAN session.

monitor session *session-number* **erspan**-**source**

No ERSPAN session is configured by default.

(4) Specify an interface as the data source of ERSPAN.

source interface *interface-type interface-number* { [**rx** | **tx** | **both**] }

By default, no source port is configured. If a source port is configured, the mirroring direction is **both** by default.

When a sub-interface is configured as the source port, mirroring is supported only in the inbound direction.

(5) Configure the source IP address for encapsulation.

original ip address *ipv4-address*

By default, no source IP address is configured for GRE encapsulation.

(6) Configure the destination IP address for encapsulation.

destination ip address *ipv4-address*

By default, no encapsulation type or destination IP address is configured.

1.6.3 Configuring Stream-based ERSPAN

1.   Overview

After stream-based ERSPAN is configured, a network analyzer can be used to monitor specified packets. Devices can normally exchange data with each other

2.   Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ERSPAN session.

monitor session *session-number* **erspan**-**source**

(4) (Optional) Specify data streams of an interface as the data source of ERSPAN.

source interface *interface-type interface-number* **rx acl** { *acl-name* | *acl-number* }

By default, no source port is configured. If a source port is configured, the mirroring direction is **both** by default.

(5) Configure the source IP address for encapsulation.

original ip address *ip-address*

(6) Configure the destination IP address for encapsulation.

destination ip address *ip-address*

1.6.4 Configuring ERSPAN Attributes

1.   Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an ERSPAN session.

monitor session *session-number* **erspan**-**source**

(4) Configure attributes of an ERSPAN session. The following configurations are optional. Select at least one of the configurations as actually needed.

(5) (Optional) Configure the TTL of the encapsulated IP packet.

ip ttl *ttl-value*

The default TTL of the encapsulated IP packet is **64**.

(6) (Optional) Configure the DSCP of the encapsulated IP packet.

ip dscp *dscp-value*

The default DSCP of the encapsulated IP packet is **0**.

(7) (Optional) Associate ERSPAN with a VRF.

vrf *vrf-name*

By default, no VRF is associated with ERSPAN.

When this function is configured, the VRF must be already configured.

(8) (Optional) Shut down the ERSPAN session.

shutdown

The session is enabled by default.

1.7 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Table 1-1   Monitoring

| Command	Purpose
show monitor [**session** *session-number*]	Displays the SPAN session information.
debug span	Debugs the SPAN.

1.8 Configuration Examples

1.8.1 Configuring SPAN

1.   Requirements

As shown in Figure 1-1, after appropriate configuration, the network analyzer can monitor all data streams forwarded by device A to device B and specified data streams of device B (for example, data streams from PC 1 and PC 2).

2. Topology

Figure 1-1   SPAN Topology
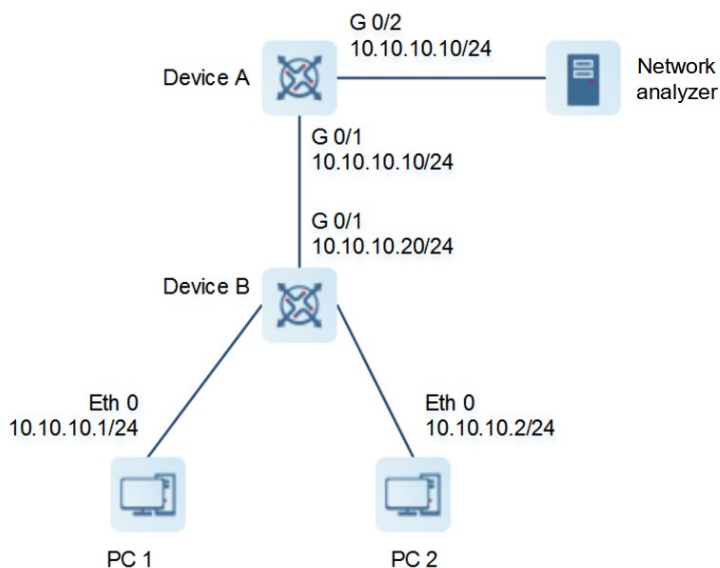
3. Notes

- Add GigabitEthernet 0/1 and GigabitEthernet 0/2 of device A to VLAN 1. Create SVI 1 and set the address of SVI 1 to 10.10.10.10/24.

- Add GigabitEthernet 0/1 of device B to VLAN 1. Create SVI 1 and set the address of SVI 1 to 10.10.10.20/24.

- Set the IP addresses of PC 1 and PC 2 to 10.10.10.1/24 and 10.10.10.2/24, respectively.

- Configure SPAN for Device A and configure ports GigabitEthernet 0/1 and GigabitEthernet 0/2 as the source port and destination port of SPAN respectively. Monitor all data streams forwarded by device A to device B and specified data streams of device B.

4. Procedure

Add GigabitEthernet 0/1 and GigabitEthernet 0/2 of device A to VLAN 1.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# vlan 1
DeviceA(config-vlan)# exit
```

On device A, create SVI 1 and set the address of SVI 1 to 10.10.10.10/24.

```
DeviceA(config)# interface VLAN 1
DeviceA(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0
DeviceA(config-if-VLAN 1)# exit
```

Add GigabitEthernet 0/1 of device B to VLAN 1.

```
DeviceB# configure
DeviceB(config)# vlan 1
DeviceB(config-vlan)# exit
```

On device B, create SVI 1 and set the address of SVI 1 to 10.10.10.20/24.

```
DeviceB (config)# interface VLAN 1
DeviceB(config-if-VLAN 1)# ip address 10.10.10.20 255.255.255.0
DeviceB(config-if-VLAN 1)# exit
```

On device A, configure an ACL to match packets with the source address 10.10.10.20.

```
DeviceA(config)# access-list 100 permit ip host 10.10.10.20 any
```

On device A, configure GigabitEthernet 0/1 as the SPAN source port, and monitor all data streams forwarded by device A to device B and specified data streams of device B.

```
DeviceA(config)# monitor session 1 source interface gigabitEthernet 0/1 tx
DeviceA(config)# monitor session 1 source interface gigabitEthernet 0/1 rx acl
100
```

On device A, configure GigabitEthernet 0/2 on device A as the SPAN destination port.

```
DeviceA(config)# monitor session 1 destination interface gigabitEthernet 0/2
```

5. **Verification**

Run the **show monitor** command to check whether the SPAN configuration is correct.

```
DeviceA# show monitor
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
  GigabitEthernet 0/1        frame-type TX Only
src-intf:
  GigabitEthernet 0/1        frame-type RX Only
rx acl id 100
dest-intf:
  GigabitEthernet 0/2
```

6. **Configuration Files**

● Device A configuration file

```
hostname DeviceA
!
ip access-list extended 100
 10 permit ip host 10.10.10.20 any
!
interface VLAN 1
 ip address 10.10.10.10 255.255.255.0
!
monitor session 1 destination interface GigabitEthernet 0/2
monitor session 1 source interface GigabitEthernet 0/1 tx
monitor session 1 source interface GigabitEthernet 0/1 rx acl 100
!
end
```

● Device B configuration file

```
hostname DeviceB
!
interface VLAN 1
 ip address 10.10.10.20 255.255.255.0
!
end
```

## 1.8.2 Configuring RSPAN to Realize One-to-Many SPAN

⚠️ **Caution**

When deploying One-to-Many SPAN, you must run the **switchport trunk allowed vlan remove** *vlan-list* command to remove the flood VLANs from a trunk interface on each SPAN device. Otherwise, the trunk interface may be fully occupied by the traffic flood, causing service interruption.

1. **Requirements**

As shown in Figure 1-1, the RSPAN function enables the network analyzer to monitor users connected to the source device A from the destination devices B and C. The devices can normally exchange data with each other.

2. **Topology**

Figure 1-1   Topology of RSPAN Used to Realize One-to-Many SPAN
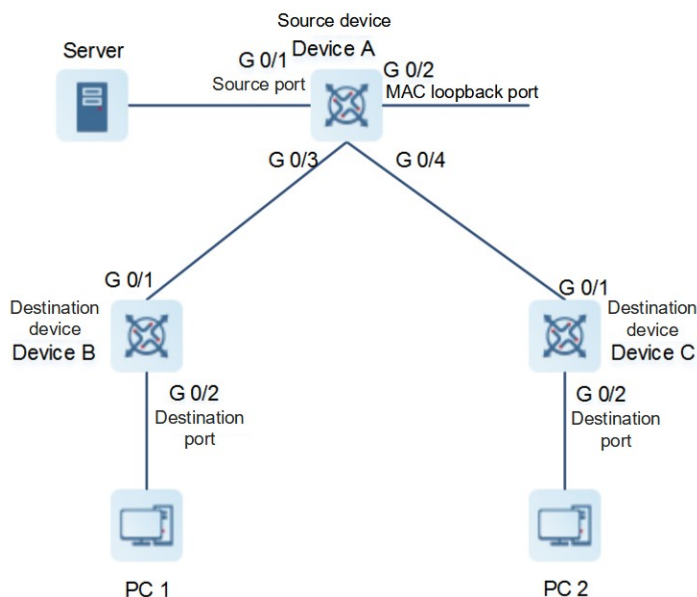
3. **Notes**

- Configure device A as the source device. Configure a remote VLAN. Configure GigabitEthernet 0/1 directly connected to users as the source port, GigabitEthernet 0/3 and GigabitEthernet 0/4 connected to the destination device as the output ports, and GigabitEthernet 0/2 as the MAC loopback port to realize the reflection function of one-to-many SPAN. Configure the switching function of the output port.

● Configure devices B and C as the destination devices. Configure a remote VLAN. Configure GigabitEthernet 0/1 connected to the source device as the source port. Configure a trunk port. Configure GigabitEthernet 0/2 connected to the network analyzer as the SPAN destination port, and configure the switching function for the SPAN destination port.

4. Procedure

(1) Configure device A as the source device.
   a. Configure a remote VLAN.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# vlan 7
DeviceA(config-vlan)# remote-span
DeviceA(config-vlan)# exit
```

   b. Configure a source port.

```
DeviceA(config)# monitor session 1 remote-source
DeviceA(config)# monitor session 1 source interface GigabitEthernet 0/1 both
```

   c. Configure an output port.

```
DeviceA(config)# monitor session 1 destination remote vlan 7 interface
GigabitEthernet 0/2 switch
```

   d. Configure a loopback port.

```
DeviceA(config)# interface GigabitEthernet 0/2
DeviceA(config-if)# mac-loopback
DeviceA(config-if)# switchport access vlan 7
DeviceA(config-if)# exit
DeviceA(config)# interface range GigabitEthernet 0/3-4
DeviceA(config-if-range)# switchport mode trunk
```

(2) Configure device B as the destination device.
   a. Configure a remote VLAN.

```
DeviceB> enable
DeviceB# configure
DeviceB(config)# vlan 7
DeviceB(config-vlan)# remote-span
DeviceB(config-vlan)# exit
```

   b. Configure a destination port.

```
DeviceB(config)# monitor session 1 remote-destination
DeviceB(config)# monitor session 1 destination remote vlan 7 interface
GigabitEthernet 0/2 switch
DeviceB(config)# interface GigabitEthernet 0/1
DeviceB(config-if)# switchport mode trunk
```

(3) Configure device C as the destination device.
   a. Configure a remote VLAN.

```
DeviceC> enable
DeviceC# configure
```

```
DeviceC(config)# vlan 7
DeviceC(config-vlan)# remote-span
DeviceC(config-vlan)# exit
```

b. Configure a destination port.

```
DeviceC(config)# monitor session 1 remote-destination
DeviceC(config)# monitor session 1 destination remote vlan 7 interface
GigabitEthernet 0/2 switch
DeviceC(config)# interface GigabitEthernet 0/1
DeviceC(config-if)# switchport mode trunk
```

5. Verification

Run the **show monitor** command on device A to view the SPAN source device configurations.

```
DeviceA# show monitor
sess-num: 1
span-type: SOURCE_SPAN
src-intf:
GigabitEthernet 0/1      frame-type Both
dest-intf:
GigabitEthernet  0/2
Remote vlan 7
mtp_switch on
```

Run the **show monitor** command on devices B and C to view the SPAN destination device configurations.

Device B is taken as an example below:

```
DeviceB# show monitor
sess-num: 1
span-type: DEST_SPAN
dest-intf:
GigabitEthernet  0/2
Remote vlan 7
mtp_switch on
```

6. Configuration Files

● Device A configuration file of

```
hostname DeviceA
!
vlan 7
!
 remote-span
!
interface GigabitEthernet 0/2
 mac-loopback
 switchport access vlan 7
!
interface GigabitEthernet 0/3
switchport mode trunk
```

```
interface GigabitEthernet 0/4
switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 source interface GigabitEthernet 0/1 both
monitor session 1 destination remote vlan 7 interface GigabitEthernet0/2 switch
!
end
```

● Device B configuration file

```
hostname DeviceB
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet0/2 switch
!
end
```

● Device C configuration file

```
hostname Device
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
 !
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2 switch
!
end
```

7. Common Errors

- A remote VLAN must be configured on the source device, intermediate device, and destination device, and their VLAN IDs must be consistent.

- Packet loss may occur if packets of a port with large bandwidth are mirrored to a port with small bandwidth.

- One MAC loopback port and multiple output ports need to be configured to implement one-to-many RSPAN.
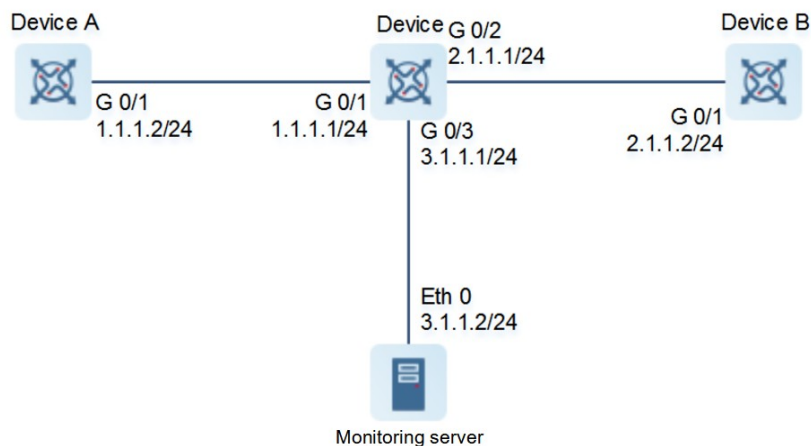
1.8.3 Configuring Basic Functions of ERPSAN

1.   Requirements

As shown in [Figure 1-1](#), the network administrator wants to use the network analyzer to monitor traffic on devices A and B. For device A, packets in both directions are monitored. For device B, only some incoming packets are monitored.

2.   Topology

Figure 1-1   Topology of ERSPAN

Monitoring server

3.   Notes

- Configure reachable L3 routes between devices.
- Configure device C as the source device. Configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as the source ports, mirror packets in both directions on GigabitEthernet 0/1, mirror packets with the destination IP address 2.1.1.1 on GigabitEthernet 0/2, and configure GigabitEthernet 0/3 as the output port.

4.   Procedure

Configure the IP address of Device.

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1
Device(config-if-GigabitEthernet 0/1)# ip address 1.1.1.1 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# interface gigabitEthernet 0/2
Device(config-if-GigabitEthernet 0/1)# ip address 2.1.1.1 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# interface gigabitEthernet 0/3
Device(config-if-GigabitEthernet 0/1)# ip address 13.1.1.1 255.255.255.0
Device(config-if-GigabitEthernet 0/1)# exit
```
Configure the IP address of device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 1.1.1.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure the IP address of device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 2.1.1.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure an ACL on Device.

```
Device(config)#access-list 1 permit host 1.1.1.1
```

Create ERSPAN Session 1, and configure Device as the source device. Configure GigabitEthernet 0/1 as the source port, and mirror packets in both directions. Configure GigabitEthernet 0/2 as the source port, and mirror packets with the destination IP address 1.1.1.1.

```
Device(config)# monitor session 1 erspan-source
Device(config-mon-erspan-src)# source interface gigabitEthernet 0/1 both
Device(config-mon-erspan-src)# source interface gigabitEthernet 0/2 rx acl acl1
Device(config-mon-erspan-src)# origin ip address 10.1.1.2
Device(config-mon-erspan-src)# destination ip address 3.1.1.2
```

5. **Verification**

Check that the L3 route between Device and Device A is reachable.

```
Device# ping 1.1.1.2
Sending 5, 100-byte ICMP Echoes to 1.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms.
```

Check that the L3 route between Device and Device B is reachable.

```
Device# ping 2.1.1.2
Sending 5, 100-byte ICMP Echoes to 2.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms.
```

Check that the L3 route between Device and the network analyzer is reachable.

```
Device# ping 3.1.1.2
Sending 5, 100-byte ICMP Echoes to 3.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/8 ms.
```

Run the **show access-lists** command to check that the ACL configuration takes effect.

```
Device# show access-lists
```

```
ip access-list standard 1
 10 permit host 1.1.1.1
```

Run the **show monitor** command to check that the ERSPAN session is in Active state in the configuration result.

```
Device# show monitor
sess-num: 1
span-type: ERSPAN_SOURCE
src-intf:
  GigabitEthernet 0/1        frame-type: Both        TX status: Active    RX
status: Active
src-intf:
  GigabitEthernet 0/2        frame-type: RX Only     Rx acl id: 1
status: Active
original ip address: 2.1.1.2
destination ip address: 3.1.1.2
ip ttl: 64
ip dscp: 0
vrf: default
```

6. **Configuration Files**

   ● Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 1.1.1.2 255.255.255.0
!
end
```

   ● Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ip address 2.1.1.2 255.255.255.0
!
end
```

   ● Device configuration file

```
hostname Device
!
ip access-list standard 1
 10 permit host 1.1.1.1
!
interface GigabitEthernet 0/1
 ip address 1.1.1.1 255.255.255.0
!
```

```
interface GigabitEthernet 0/2
 ip address 2.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 ip address 3.1.1.1 255.255.255.0
!
monitor session 1 erspan-source
 source interface gigabitEthernet 0/1 both
 source interface gigabitEthernet 0/2 rx acl acl1
 origin ip address 10.1.1.2
 destination ip address 3.1.1.2


!
end
```

7. Common Errors

- The session ID used to configure ERSPAN is already configured with RSPAN or LOCAL SPAN.
- The L3 route between the source device and destination device is unreachable.