
Contents

1 Configuring Aggregate Port.....	1
1.1 Introduction.....	1
1.1.1 Basic Concepts.....	1
1.1.2 Load Balancing.....	5
1.1.3 Member Port BFD Detection.....	7
1.1.4 Protocols and Standards.....	7
1.2 Configuration Task Summary.....	7
1.3 Configuring Static APs.....	8
1.3.1 Overview.....	8
1.3.2 Restrictions and Guidelines.....	8
1.3.3 Procedure.....	9
1.4 Configuring LACP APs.....	10
1.4.1 Overview.....	10
1.4.2 Restrictions and Guidelines.....	10
1.4.3 Procedure.....	10
1.5 Enabling LinkTrap.....	11
1.5.1 Overview.....	11
1.5.2 Procedure.....	11
1.6 Configuring a Load Balancing Mode.....	12
1.6.1 Overview.....	12
1.6.2 Restrictions and Guidelines.....	12
1.6.3 Procedure.....	12

1.7 Configuring an AP Capacity Mode.....	14
1.7.1 Overview.....	14
1.7.2 Restrictions and Guidelines.....	14
1.7.3 Procedure.....	14
1.8 Enabling BFD for AP Member Ports.....	14
1.8.1 Overview.....	14
1.8.2 Restrictions and Guidelines.....	14
1.8.3 Procedure.....	15
1.9 Configuring a Preferred AP Member Port.....	15
1.9.1 Overview.....	15
1.9.2 Restrictions and Guidelines.....	15
1.9.3 Procedure.....	15
1.10 Configuring the Minimum Number of AP Member Ports.....	16
1.10.1 Overview.....	16
1.10.2 Restrictions and Guidelines.....	16
1.10.3 Procedure.....	16
1.11 Enabling the LACP Independent Port Function.....	17
1.11.1 Overview.....	17
1.11.2 Restrictions and Guidelines.....	17
1.11.3 Procedure.....	17
1.12 Monitoring.....	18
1.13 Configuration Examples.....	19
1.13.1 Configuring Static APs.....	19
1.13.2 Configuring LACP APs.....	20

1.13.3 Enabling LinkTrap.....	22
1.13.4 Configuring a Load Balancing Mode.....	24
1.13.5 Configuring Hash Load Balancing Control.....	26
1.13.6 Configuring an AP Capacity Mode.....	28
1.13.7 Enabling BFD for Member Ports.....	29
1.13.8 Configuring Interworking Between the Access Device and a Server with Two NICs over a Preferred LACP AP.....	32
1.13.9 Configuring Automatic Server Deployment over a Preferred LACP AP.....	34
1.13.10 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Less Than the Minimum Number).....	36
1.13.11 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Not Less Than the Minimum Number).....	38
1.13.12 Enabling the LACP Independent Port Function.....	40

1 Configuring Aggregate Port

1.1 Introduction

An aggregate port (AP) is used to bundle multiple physical links into one logical link to increase the link bandwidth and improve connection reliability.

1.1.1 Basic Concepts

An AP supports load balancing, that is, distributes load evenly among member links. Besides, an AP realizes link backup. When a member link of the AP is disconnected, the load carried by the link is automatically allocated to other functional member links. A member link does not forward broadcast or multicast packets to other member links.

- If the link between two devices supports a maximum bandwidth of 1,000 Mbps (assuming that the devices each have a 1,000 Mbps port), when the service traffic carried by the link exceeds 1,000 Mbps, the traffic in excess will be discarded. Port aggregation can be used to solve the problem. For example, you can connect the two devices with network cables and combine multiple links to form a logical link capable of multiples of 1,000 Mbps.
- If the two devices are connected by one network cable, when the link between the two ports of the devices is disconnected, the services carried by the link will be interrupted. After the connected ports are aggregated, the services will not be affected as long as one link remains connected.

There are two kinds of AP link aggregation. One is the static AP mode, and the other is dynamic aggregation through Link Aggregation Control Protocol (LACP).

1. Static AP

The static AP mode means manually configuring physical ports and adding them to an AP aggregation group. An AP in static AP mode is called a static AP, and its member ports are called static AP member ports. The static AP configuration is simple. You only need to run a command to add the specified physical port to the AP. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

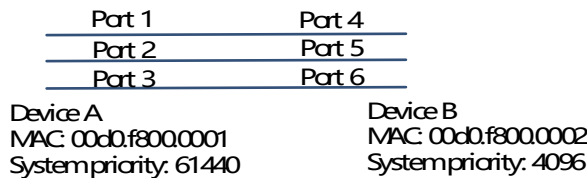
2. Dynamic AP (LACP)

LACP is a protocol about dynamic link aggregation. It exchanges information with the connected device through link aggregation control protocol data units (LACPDU). An AP in LACP mode is called a dynamic AP, and its member ports are called dynamic AP member ports.

An LACP-enabled port sends LACPDUs to advertise its system priority, system MAC address, port priority, port number, and operation key. When receiving the LACPDU from the peer end, the device compares the system priorities of both ends based on the system ID in the packet. The end with a higher system ID priority sets the ports in the aggregation group to **Bundle** state based on the port ID priorities in a descending order, and sends an updated LACPDU. When receiving the LACPDU, the peer end sets corresponding ports to **Bundle** state so that both ends maintain consistency when a port exits or joins the aggregation group. The physical link can forward packets only after the ports at both ends are bundled dynamically.

After link aggregation, the LACP AP member ports periodically exchange LACPDU. When a port does not receive an LACPDU in the specified time, a timeout occurs and the links are unbundled. In this case, the member ports cannot forward packets. There are two timeout modes: long timeout and short timeout. In long timeout mode, a port sends a packet every 30s. If it does not receive a packet from the peer end in 90s, a timeout occurs. In short timeout mode, a port sends a packet every 1s. If it does not receive a packet from the peer end in 3s, a timeout occurs.

Figure 1-1 LACP Negotiation



As shown in [Figure 1-1](#), Device A is connected to Device B through three ports. Set the system priority of Device A to 61440 and that of Device B to 4096. Enables LACP link aggregation on the three directly connected ports of Device A and Device B, set the aggregation mode of the three ports to the active mode, and set the port priority to the default value 32768.

When receiving an LACPDU from Device A, Device B finds that it has a higher system ID priority than Device A (a smaller value indicates a higher priority). Therefore, Device B sets Port 4, Port 5, and Port 6 to **Bundle** state based on the order of port ID priorities (or in an ascending order of port numbers if the port priorities are the same). When receiving an updated LACPDU from Device B, Device A finds that Device B has a higher system ID priority and has set Port 4, Port 5, and Port 6 to **Bundle** state. Then Device A also sets Port 1, Port 2, and Port 3 to **Bundle** state.

3. AP Member Port Mode

There are three aggregation modes available, namely, active, passive, and static.

AP member ports in active mode initiate LACP negotiation. AP member ports in passive mode only respond to received LACPDUs. AP member ports in static mode do not send LACPDUs for negotiation. The following table lists the requirements for peer port mode.

Table 1-1 Requirements for Peer Port Aggregation in Aggregation Mode

Port Mode	Peer Port Mode
Active mode	Active or passive mode
Passive mode	Active mode
Static Mode	Static Mode

4. AP Member Port State

Static AP member ports can be in **Up** or **Down** state.

- When a member port is **Down**, the port cannot forward packets. The **Down** state is displayed.

- When a member port is **Up** and the link protocol is ready, the port can forward packets. The **Up** state is displayed.

LACP AP member ports has the following three states:

- When the link of a port is **Down**, the port cannot forward packets. The **Down** state is displayed.
- When the link of a port is **Up** and the port is added to an aggregation group (as a member of the aggregation group, the port participates in data packet forwarding of the aggregation group) after LACP negotiation, the **bndl** state is displayed.
- When the link of a port is **Up** but the port is suspended because the peer end is not enabled with LACP or the attributes of the ports are inconsistent with those of the master port, the **susp** state is displayed. (The port in **susp** state does not forward packets.)

Note

- Only full-duplex ports are capable of LACP aggregation.
 - LACP aggregation can be implemented only when the rates, flow control approaches, medium types, and L2/L3 attributes of member ports are consistent.
 - If you modify the preceding attributes of a member port in the aggregation group, LACP aggregation will fail.
 - The ports which are prohibited from joining or exiting an AP cannot be added to or removed from a static AP or an LACP AP.
-

5. AP Capacity Mode

The maximum number of member ports is fixed, which is equal to the maximum number of APs multiplied by the maximum number of member ports supported by a single AP. If you want to increase the maximum number of APs, the maximum number of member ports supported by a single AP must be reduced, and vice versa. This concerns the AP capacity mode concept. Some devices support the configuration of the AP capacity mode. For example, if the system supports 16,384 member ports, you can select 1024 x 16, 512 x 32, and other AP capacity modes (Maximum number of APs multiplied by the maximum number of member ports supported by a single AP).

6. LACP System ID

By default, all the LACP ports on a device belong to the same LACP aggregation system.

The system is identified by a system ID and each system has a priority, which is a configurable value. The system ID consists of the LACP system priority and MAC address of the device. A lower system priority indicates a higher priority of the system ID. If the system priorities are the same, a smaller MAC address of the device indicates a higher priority of the system ID. The system with an ID of a higher priority determines the port state. The port state of a system with an ID of a lower priority keeps consistent with that of a higher priority.

The LACP system ID can be configured when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device (for example, LACP ports of two independent ASWs need to negotiate with the LACP port of the NC). You can set the system IDs of the LACP ports of independent devices to the same MAC address and configure different device IDs to implement normal negotiation.

7. LACP Device ID

The LACP device ID can be configured when LACP ports of multiple independent devices need to negotiate with the LACP port of a specific device. It must be configured together with the system ID.

8. LACP Port ID

Each port has an independent LACP port priority, which is a configurable value. The port ID consists of the LACP port priority and port number. A smaller port priority indicates a higher priority of the port ID. If the port priorities are the same, a smaller port number indicates a higher priority of the port ID.

9. LACP Master Port

When dynamic member ports are **Up**, LACP selects one of those ports to be the master port based on the rates and duplex modes, ID priorities of the ports in the aggregation group, and the bundling state of the member ports in the **Up** state. Only the ports that have the same attributes as the master port are in **Bundle** state and participate in data forwarding. When the attributes of ports are changed, LACP reselects a master port.

10. Preferred AP Member Port

The preferred AP member port feature is used when an AP is connected to a server with two systems. An AP member port is selected as the preferred port that forwards specified packets (packets of the management VLAN) to the server. These packets will not be distributed to other member ports by load balancing. This ensures the communication with the server.

Caution

Configure the port connected to the management network interface card (NIC) of the server as the preferred AP member port.

Some Linux servers have two systems. For example, an HP server has a master system and remote management system. The master system is a Linux system. The remote management system with Integrated Lights-Out (iLO) provides remote management at the hardware-level. iLO can manage the server remotely even when the master system is restarted. The master system has two NICs bundled into an AP for service processing. The management system uses one of the two NICs for remote management. Because services are separated by different VLANs, the VLAN used by the management system is called a management VLAN. The port of a device connected to a server with two NICs is an AP. The packets of the management VLAN must be sent by the member port connected to the NICs of the server to ensure the communication with the remote management system. You can configure a preferred AP member port to send the packets of the management VLAN.

Caution

For a server with two NICs bundled through LACP, if LACP is not running when the master system is restarted, LACP negotiation fails and the AP is **Down**. In this case, the preferred AP member port is downgraded into a static member port and it is bound to the AP for communication with the remote management system of the server. The preferred AP member port will be enabled with LACP again for negotiation after the Linux system is restarted and LACP runs normally.

11. Minimum Number of AP Member Ports

An AP can be configured with a minimum number of AP member ports. When a member port exits the AP aggregation group, causing the number of member ports to be smaller than the minimum number, the other member ports in the group are unbundled, and the AP is **Down**. When the member port rejoins the group, causing the number of member ports to be greater than the minimum number, the member ports in the group are automatically bundled, and the AP is **Up** again.

12. LACP Independent Ports

In normal cases, LACP independent ports are used for interworking between access switches and servers with two NICs. If the operating system (OS) is not pre-installed when a server with two NICs starts, the OS needs to be installed via the remote preboot execution environment (PXE) OS installation device. Before the OS is installed, the server with two NICs cannot perform LACP negotiation with the access device, and only one NIC can work. In this case, the port on the access device must be able to automatically change to a common Ethernet physical port to ensure normal communication between the server and the remote PXE OS installation device. After the OS is installed and both NICs can run the LACP, the port on the access device must be able to enable the LACP again for negotiation.

⚠ Caution

- LACP independent ports can work only at layer 2. After an LACP independent port is enabled through configuration, if the LACP independent port does not receive LACP packets, it automatically changes to a common Ethernet port, which automatically copies the rate, duplex mode, flow control, and VLAN configuration from the AP to ensure port forwarding capabilities.
 - An LACP independent port automatically changes to a common Ethernet port only if it does not receive LACP packets within the set timeout period. After the port receives LACP packets, it changes to an LACP AP member port again.
-

1.1.2 Load Balancing

APs segregate packet flows by using load balancing algorithms based on packet features, such as the source and destination MAC addresses, source and destination IP addresses, and L4 source and destination port numbers. The packet flow with the consistent feature is transmitted by one member link, and different packet flows are evenly distributed to member links. For example, in source MAC address-based load balancing, packets are distributed to the member links based on the source MAC addresses of the packets. Packets with different source MAC addresses are evenly distributed to member links. Packets with the identical source MAC address are forwarded by one member link.

Currently, there are several AP load balancing modes as follows:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address
- Source IP address + destination IP address + L4 source port number + L4 destination port number

Note

- Load balancing based on IP addresses or port numbers is applicable only to L3 packets. When a device enabled with this load balancing method receives L2 packets, it automatically switches to the default load balancing method.
 - All the load balancing methods use a load algorithm (hash algorithm) to calculate the member links based on the input parameters of the methods. The input parameters include the source MAC address, destination MAC address, source MAC address + destination MAC address, source IP address, destination IP address, source IP address + destination IP addresses, source IP address + destination IP address + L4 port number and so on. The algorithm ensures that packets with different input parameters are evenly distributed to member links. It does not indicate that these packets are always distributed to different member links. For example, in IP address-based load balancing, two packets with different source and destination IP addresses may be distributed to the same member link through calculation.
-

1. Enhanced Load Balancing

Enhanced load balancing allows the combination of multiple fields in different types of packets. These fields include **src-mac**, **dst-mac**, **I2-protocol**, **vlan**, **src-port**, and **dst-port** in L2 packets, **src-ip**, **dst-ip**, **protocol**, **I4-src-port**, **I4-dst-port**, **vlan**, **src-port**, **dst-port**, **I2-etype**, **src-mac**, and **dst-mac** in IPv4 packets, **src-ip**, **dst-ip**, **protocol**, **I4-src-port**, **I4-dst-port**, **vlan**, **src-port**, **dst-port**, **I2-etype**, **src-mac**, and **dst-mac** in IPv6 packets; **top-label**, **2nd-label**, **3rd-label**, **src-ip**, **dst-ip**, **vlan**, **src-port**, **dst-port**, **src-mac**, **dst-mac**, **protocol**, **I4-src-port**, **I4-dst-port**, and **I2-etype** in MPLS packets; **vlan**, **src-port**, **src-mac**, **src-ip**, **protocol**, **I4-src-port**, **I4-dst-port**, **I2-etype**, **ing-nick**, **egr-nick**, **dst-port**, **dst-mac**, and **dst-ip** in TRILL packets, and **vlan**, **src-port**, **src-id**, **rx-id**, **ox-id**, **fabric-id**, **dst-port**, and **dst-id** in FCoE packets.

A device enabled with enhanced load balancing first determines the types of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

Note

- All the load balancing methods are applicable to L2 and L3 APs. You need to configure proper load distribution methods based on different network environments to fully utilize network bandwidth.
 - Perform enhanced load balancing based on the **src-mac**, **dst-mac**, and **vlan** fields in L2 packets, and the **src-ip** field in IPv4 packets. If the incoming packet is an IPv4 packet with an ever-changing source MAC address, the enhanced balancing algorithm does not take effect, because the device performs load balancing only based on the **src-ip** field in the IPv4 packet after finding that it is an IPv4 packet.
 - In enhanced load balancing, the MPLS balancing algorithm takes effect only for MPLS L3 VPN packets, but does not take effect for MPLS L2 VPN packets.
-

2. Hash Load Balancing Control

Hash load balancing enables users to flexibly control load balancing in different scenarios. Currently, Orion_B26Q adopts the following hash load balancing control functions:

Hash disturbance factor: Traffic over APs is hashed for balancing. For two devices of the same type, the same path is calculated for load balancing for the same stream. When the equal-cost multi-path (ECMP) is deployed, the same stream of the two devices may be balanced to the same destination device, resulting in hash polarization. The hash disturbance factor is used to affect the load balancing algorithm. Different disturbance factors are configured for different devices to ensure that different paths are provided for the same stream.

Hash synchronization: To ensure network security, a firewall cluster is deployed between the internal and external networks for traffic cleaning. This requires that both the uplink and downlink traffic of a session is transmitted to the same device in the firewall cluster for processing. The source and destination IP addresses contained in the uplink and downlink streams of a session are reversed. The uplink and downlink streams will be directed to different firewalls in the firewall cluster based on the traditional hash algorithm. The hash synchronization function ensures that uplink and downlink streams of a session be transmitted over the same path.

Flexible hash: In normal cases, the load balancing cluster interworks with multiple ToRs via the ECMP, and the ToRs are required to balance all packets of a session to the same scheduling server. However, when a server is faulty, all session streams will be ordered and balanced again based on the traditional load balancing mechanism of ToRs. In this case, packets of the same session may be balanced to two servers. The flexible hash function ensures that when one link is faulty, traffic on other links is not affected and only the traffic of the faulty link is balanced to other active links. In this case, traffic of a session is balanced to the same server.

Hash algorithm mode: Apply the most appropriate hash algorithm mode to different traffic models, so that when traffic changes, balance can still be kept. For example, if the source and destination MAC addresses of a stream increase by 1 at the same time, configuring the algorithm based on the source and destination MAC addresses cannot keep stream balance. In this case, a suitable hash algorithm mode needs to be applied.

Hash factor acquisition mode: There are an inner layer and an outer layer in the header in each of VXLAN packets, GRE packets, and other tunnel packets. It can be specified to obtain the hash factor from the inner layer or outer layer, to achieve a better balancing effect. For example, in some scenarios, tunnel packets share the same outer IP address but have different inner IP addresses. In this case, the inner IP address can be specified as the hash factor to achieve an optimal balancing effect.

Note

The performance of hash algorithm mode may vary with different devices.

1.1.3 Member Port BFD Detection

Bidirectional Forwarding Detection (BFD) is a protocol that delivers fast detection of path failures. According to RFC7130, LACP takes 3s to detect link failures even in short timeout mode. All the packets sent to the faulty link during the 3-second period will be dropped. BFD correlation delivers faster failure detection. You can configure BFD on member ports to detect link failure and switch load to other member links in case of a link failure. BFD is classified into IPv4 detection and IPv6 detection, which detect IPv4 and IPv6 paths respectively. When BFD detects that the path on a member port fails, the packets are not distributed to the member port. After BFD is enabled on an AP, BFD sessions are set up on its member ports in forwarding state independently.

1.1.4 Protocols and Standards

- IEEE 802.3ad

1.2 Configuration Task Summary

The AP configuration includes the following tasks:

(1) [Configuring Static APs](#)

- (2) (Optional) [Configuring LACP APs](#)
- (3) (Optional) [Enabling LinkTrap](#)
- (4) (Optional) [Configuring a Load Balancing Mode](#)
- (5) (Optional) [Configuring an AP Capacity Mode](#)
- (6) (Optional) [Enabling BFD for AP Member Ports](#)
- (7) (Optional) [Configuring a Preferred AP Member Port](#)
- (8) (Optional) [Configuring the Minimum Number of AP Member Ports](#)
- (9) (Optional) [Enabling the LACP Independent Port Function](#)

1.3 Configuring Static APs

1.3.1 Overview

- Configure multiple physical ports as AP member ports to realize link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP is disconnected, the load carried by the link is automatically allocated to other functional member links.

1.3.2 Restrictions and Guidelines

- Only physical ports can be added to an AP.
- To prevent a transient loop when a member port exits, you need to set the member port to **shutdown** state before it exits the AP.
- The ports of different medium types or port modes cannot be added to the same AP.
- L2 ports can be added to only a L2 AP, and L3 ports can be added to only a L3 AP. The L2/L3 attributes of an AP that contains member ports cannot be modified.
- After a port is added to an AP, the attributes of the port are replaced by those of the AP.
- After a port is removed from an AP, the attributes of the port before the adding to the AP are restored.
- There is continuous traffic at the AP. If an AP member port changes from **Link Up** to **Link Down**, an error may occur in traffic statistics of the AP.
- When the AP includes a member port that supports **port speed-mode** configuration, the AP does not support speed configuration, and the original speed configuration on the AP is automatically cleared. The configured rate of the AP is switched to that of **port speed-mode** for the member port.
- You can run the **port-group** command to add a physical port to a static AP in the interface configuration mode of the specified Ethernet port. If the AP does not exist, it will be created automatically.
- You can run the **port-group mode** command to add a physical port to an LACP AP in the interface configuration mode of the specified physical port. If the AP does not exist, it will be created automatically.
- The AP feature must be configured on the devices at both ends of a link and the AP mode must be the same (static AP or LACP AP).
- After a member port exits the AP, the default configurations of the member port may be restored. The original configurations of AP members are processed in different ways for different functions. You are advised to check and confirm the port configurations after a member port exits an AP.

- After a member port exits an AP, the port is shut down to avoid loops. After confirming that the topology is normal, you can run **no shutdown** in interface configuration mode to enable the port again.
- If the VLAN resource is in a critical state (the number of configured VLANs and the number of routed ports reach the VLAN capacity values) when a L3 AP member port exits the AP, the port may be switched to a L2 port.
- The AP created on a L3 device that does not support L2 features is a L3 AP; otherwise the AP is a L2 AP.

Warning

- After a port is added to an AP, the attributes of the port are consistent with those of the AP. Therefore, it is generally not allowed to perform configuration on the AP member ports or apply configurations to a specific AP member port. However, some commands or functions (such as the **shutdown** and **no shutdown** commands) can be configured on the AP member ports. When using the AP member ports, you need to check whether the function that you want to configure can take effect on a specific AP member port, and perform the configuration properly.
 - The error detection function is unavailable to static aggregation. Member ports are bound if linked up. Therefore, you need to ensure topology accuracy and negotiated attribute consistency among the member ports.
-

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an Ethernet AP.

interface aggregateport *ap-number*

Perform this configuration on an AP-enabled device. When an Ethernet port needs the aggregation function, create the corresponding Ethernet AP

No AP is configured by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure static AP member ports.

port-group *ap-number*

Perform this configuration on AP-enabled devices. To use the static aggregation function, configure the corresponding static AP member ports.

By default, the Ethernet physical port does not belong to any static AP or LACP AP.

(6) (Optional) Convert L2 APs to L3 APs.

no switchport

The AP is a L2 port by default.

(7) (Optional) Create an Ethernet AP sub-interface.

interface aggregateport *sub-ap-number*

No Ethernet AP sub-interface is configured by default.

1.4 Configuring LACP APs

1.4.1 Overview

- Connected devices perform auto negotiation through LACP to realize dynamic link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP is disconnected, the load carried by the link is automatically allocated to other functional member links.
- It takes 90s for LACP to detect a link failure in long timeout mode and 3s in short timeout mode.

1.4.2 Restrictions and Guidelines

- After a port exits an LACP AP, the default configurations of the port may be restored. The original configurations of LACP AP members are processed in different ways for different functions. You are advised to check and confirm the port configurations after a member port exits an LACP AP.
- To prevent a transient loop when a member port exits, you need to set the member port to **shutdown** state before it exits the AP.
- Changing the LACP system priority may cause LACP AP member ports to be disaggregated and aggregated again.
- Changing the priority of an LACP AP member port may cause the other member ports to be disaggregated and aggregated again.
- There is continuous traffic at the AP. If an AP member port changes from **Link Up** to **Link Down**, an error may occur in traffic statistics of the AP.
- When the AP includes a member port that supports **port speed-mode** configuration, the AP does not support speed configuration, and the original speed configuration on the AP is automatically cleared. The configured rate of the AP is switched to that of **port speed-mode** for the member port.
- The LACP AP member port configurations at both ends of a link must be consistent.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the interface configuration mode.

```
interface interface-type interface-number
```

(4) Configure LACP AP member ports.

```
port-group key-number mode { active | passive }
```

By default, the Ethernet physical port does not belong to any LACP AP.

(5) (Optional) Configure the LACP system ID.

```
lacp system-id system-id
```

Configure the LACP system ID when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device.

The LACP system ID is the system ID (MAC address) of the device by default.

(6) (Optional) Configure the LACP device ID.

lACP device *number*

Configure the LACP device ID when LACP ports of multiple (a maximum of four) independent devices need to negotiate with the LACP port of a specific device.

The device ID is 0 by default.

(7) (Optional) Configure the LACP system priority.

lACP system-priority *system-priority*

Perform this configuration when you need to adjust the system ID priority. A smaller value indicates a higher system ID priority. The device with a higher system ID priority takes precedence in selecting an AP.

The LACP system priority of a port is 32768 by default.

(8) Configure the priority of an LACP AP member port.

lACP port-priority *port-priority*

Perform this configuration when you need to specify the port ID priority. A smaller value indicates a higher port ID priority. The port with the highest port ID priority will be selected as the master port.

The priority of the LACP AP member port is 32768 by default.

(9) Configure the timeout mode of LACP AP member ports.

lACP short-timeout

When you need to implement real-time link failure detection, configure the short timeout mode. A timeout occurs if a port does not receive a packet within 3 seconds in short timeout mode and 90 seconds in long timeout mode.

The timeout mode of an LACP AP member port is long timeout by default.

1.5 Enabling LinkTrap

1.5.1 Overview

Enable the system with LinkTrap to send LinkTrap messages when aggregation links are changed.

1.5.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the AP interface configuration mode.

interface Aggregateport *ap-interface-number*

(4) (Optional) Configure the LinkTrap function of an AP.

snmp trap link-status

The LinkTrap notification function of an AP is enabled by default.

(5) (Optional) Configure the LinkTrap function of AP member ports.

aggregateport member linktrap

The LinkTrap notification function of AP member ports is disabled by default.

1.6 Configuring a Load Balancing Mode

1.6.1 Overview

- The system distributes incoming packets among member links by using the specified load balancing algorithm. The packet flow with the consistent feature is transmitted by one member link, whereas different packet flows are evenly distributed to various links. A device enabled with enhanced load balancing first determines the types of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.
- In enhanced load balancing mode, configure the hash disturbance factor to ensure that same packets from two devices of the same type is balanced to different links.
- In enhanced load balancing mode, enable hash synchronization to ensure that uplink and downlink packets of the same type are transmitted over the same link. For example, in load balancing based on the source and destination IP addresses, enable hash synchronization for IPv4 packets to ensure that the uplink and downlink IPv4 packets are transmitted over the same path.
- Enable flexible hash to balance traffic of a faulty link over an AP member port to other active links without affecting original data streams on these active links.

1.6.2 Restrictions and Guidelines

- Different disturbance factors may lead to the same disturbance effect.
- You can enable or disable the hash synchronization factors **ipv4**, **ipv6**, **fcoe**, and **on** as required.
- The flexible hash function can be configured in global configuration mode or interface configuration mode of a specific AP.
- Different products may support different load balancing algorithms.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) (Optional) Configure the global load balancing algorithm of an AP.

```
aggregateport load-balance { dst-mac | src-mac | src-dst-mac | dst-ip | src-ip | src-dst-ip  
| src-dst-ip-l4port | enhanced profile profile-name }
```

By default, for a device on which an AP is created as a L2 AP by default, load is distributed according to the source MAC addresses and destination MAC addresses of the incoming packets. For a device on which an AP is created as a L3 AP by default, load is distributed according to the source IP addresses and destination IP addresses of the incoming packets.

(4) (Optional) Rename the enhanced load balancing profile.

load-balance-profile *profile-name*

By default, if a device supports enhanced load balancing, the system creates a profile named **default** for enhanced load balancing. You can use this function to rename the profile or restore the default configurations.

- (5) (Optional) Configure the load balancing mode of L2 packets.

l2 field { [**src-mac**] [**dst-mac**] [**src-port**] }

When the enhanced load balancing profile configuration is used as the flow balancing mode of AP, you can perform this configuration according to the traffic feature configuration of the network to implement better load balance.

The load balancing mode of L2 packets is a combination of **src-mac** and **dst-mac**.

- (6) (Optional) Configure the load balancing mode of IPv4 packets.

ipv4 field { [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**src-port**] }

Perform this configuration to specify the load balancing mode of IPv4 packets.

The load balancing mode of IPv4 packets is a combination of **src-ip**, **dst-ip**, **l4-src-port** and **l4-dst-port** by default.

- (7) (Optional) Configure the load balancing mode of IPv6 packets.

ipv6 field { [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**src-port**] }

Perform this configuration to specify the load balancing mode of IPv6 packets.

The load balancing mode of IPv6 packets is a combination of **src-ip**, **dst-ip**, **l4-src-port** and **l4-dst-port** by default.

- (8) (Optional) Configure a hash disturbance factor.

hash-disturb { *factor-string* }

Perform this operation to balance packets of the same type over the AP for devices of the same type. It is not guaranteed that either configuration affects the balancing effect. If there is no expected effect, the other values can be configured.

The load balancing hash disturbance function is disabled by default.

- (9) (Optional) Enable or disable hash synchronization.

hash-symmetrical { **ipv4** | **ipv6** }

Perform this operation to ensure that uplink and downlink streams of the same packet type are transmitted over the same path.

The hash synchronization function is disabled by default.

- (10) (Optional) Configure the global load balance algorithm mode on an AP.

aggregateport algorithm mode *algorithm-number*

Perform this operation when the traffic model changes to keep optimal load balance.

The default algorithm mode is 11.

1.7 Configuring an AP Capacity Mode

1.7.1 Overview

- Change the maximum number of configurable APs and the maximum number of member ports in each AP.

1.7.2 Restrictions and Guidelines

- The system has a default AP capacity mode. You can run **show aggregateport capacity** to display the current capacity mode.
- If the current configuration (maximum number of APs or the number of member ports in each AP) exceeds the capacity to be configured, the capacity mode configuration will fail.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) (Optional) Configure an AP capacity mode.

```
aggregateport capacity mode capacity-mode
```

Perform this configuration to change the AP capacity, so as to meet the requirement imposed by changes in the number of APs in network deployment or the number of member ports that can be bound to each AP.

By default, up to 128 APs can be configured and each AP has up to 8 member ports.

1.8 Enabling BFD for AP Member Ports

1.8.1 Overview

- Enable BFD for all the member ports of a specified AP.
- After BFD is enabled for an AP, each member port performs BFD to determine whether the packets should be distributed to the member port for load balancing. When BFD detects a member port in **Down** state, the packets are not distributed to the port. When BFD detects that the member port is restored to **Up**, the packets are distributed to the port.

1.8.2 Restrictions and Guidelines

- After BFD is enabled for an AP, BFD sessions are set up. To make the sessions take effect, you need to configure BFD parameters. For details, see “Configuring BFD”.
- Enabling or disabling BFD for a single AP member port is not supported. You must enable or disable BFD for the entire AP group.
- Only member ports in forwarding state are enabled with BFD. If a member port is not in forwarding state because the link or LACP is **Down**, the BFD session on the member port is automatically deleted.
- If only one member port is available (that is, in forwarding state), all packets are distributed to this port. In this case, BFD fails. When there are more than one available member port, BFD takes effect again.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) (Optional) Configure BFD for AP member ports.

```
aggregate bfd-detect { ipv4 source-ipv4-address destination-ipv4-address | ipv6 source-ipv6-address destination-ipv6-address }
```

Enable BFD when you need to detect path failure on member ports in milliseconds. The flow on the faulty member port will be switched to other member port in case of link failure.

The BFD function of an AP member port is disabled by default.

1.9 Configuring a Preferred AP Member Port

1.9.1 Overview

- Configure a member port as the preferred AP member port.
- After the preferred member port is configured, the management VLAN packets on the AP are forwarded by this port.

1.9.2 Restrictions and Guidelines

- For details about management VLAN configuration, see “MAC VLAN” in “Configuring Ethernet Switching”.
- Only one preferred member port can be configured for one AP.
- After an LACP AP member port is configured as the preferred AP member port, if the LACP negotiation on all AP member ports fails, the preferred port is automatically downgraded to a static AP member port.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the interface configuration mode.

```
interface interface-type interface-number
```

(4) (Optional) Configure a preferred AP member port.

```
aggregateport primary-port
```

Perform this configuration to specify an AP member port dedicated to forwarding management VLAN packets. The configuration is applicable to dual-system servers. Configure the port connected to the management NIC of the server as the preferred AP member port.

No preferred port is configured by default.

1.10 Configuring the Minimum Number of AP Member Ports

1.10.1 Overview

- After the minimum number of AP member ports is configured, the aggregation group takes effect only when the number of active member ports is greater than the minimum number.
- You can perform this operation to ensure that the link bandwidth provided by an AP aggregation group is greater than or equal to the sum of bandwidth provided by n AP member ports.
- After an action for the minimum number of AP member ports is configured, for example, shutting down the AP, the action is triggered when the number of AP member ports in **Up** state is less than the minimum number of the AP member ports.

1.10.2 Restrictions and Guidelines

- If the number of LACP AP member ports for an LACP aggregation group is less than the minimum number of AP member ports configured, all AP member ports are in the unbinding state, and the peer end is also automatically unbound.
- After the minimum number of static AP member ports is configured, if the number of static AP member ports in **Up** state is less than the minimum number, the static AP member ports in **Up** state cannot forward data and the corresponding AP is **Down**. However, the state of the peer end is not affected. Therefore, the corresponding functions need to be configured on the peer end.
- After an action for the minimum number of AP member port is configured, the action is triggered only when the number of AP member ports in **Up** state decreases to an insufficient number. For example, if the minimum number is set to 3, the action is triggered only when the number of AP member ports decreases from 3 or more to less than 3.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the AP configuration mode.

```
interface aggregateport ap-number
```

(4) (Optional) Configure the minimum number of AP member ports.

```
aggregateport member minimum { port-number | action shutdown }
```

Perform this configuration to specify the minimum number of the member ports of an AP aggregation group.

The minimum number of member ports of an AP is 1 by default.

(5) (Optional) Configure the action triggered when the number of AP member ports is smaller than the minimum value.

```
aggregateport member minimum { port-number | action shutdown }
```

Perform this configuration when some actions need to be triggered when the number of AP member ports in **Up** state is less than the minimum number of AP member ports.

By default, no action is configured for the minimum number of member ports in an AP.

1.11 Enabling the LACP Independent Port Function

1.11.1 Overview

- After the LACP independent port function is enabled, an LACP AP member port automatically changes to a common physical port if the LACP AP member port does not receive LACP packets within the set timeout period. The LACP AP member port state is changed to individual and the LACP AP member port can forward packets properly.
- After the LACP AP member port receives LACP packets, it changes to an LACP independent port again to perform LACP packet negotiation.
- The timeout period of an independent port can be adjusted by configuration.

1.11.2 Restrictions and Guidelines

- After the LACP independent port function is enabled, an LACP AP member port does not immediately change to a common physical port. Instead, the LACP AP member port changes to an independent port (a common physical port) only if it does not receive LACP packets within the set timeout period.
- The timeout period configuration of the LACP independent port only affects LACP AP member ports that have not changed into independent ports. After the timeout period is configured, the period calculation restarts.
- In long timeout mode, the LACP packet is sent every 30s. The timeout period should be longer than 30s so as not to affect the normal LACP negotiation. You are advised to configure the timeout period at least twice the period of LACP packet sending. In short timeout mode, the timeout period is not limited.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the interface configuration mode.

```
interface interface-type interface-number
```

(4) (Optional) Enable the LACP independent port function.

```
lacp individual-port enable
```

Perform this operation so that an LACP AP member port can forward packets normally when the LACP AP member port cannot perform LACP negotiation.

The LACP independent port function is disabled by default.

(5) (Optional) Configure the timeout period of an LACP independent port.

```
lacp individual-timeout period time
```

Run this command to adjust the timeout period of an LACP independent port.

The timeout period of an LACP independent port is 90s by default.

1.12 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

You can run the **clear** commands to clear information.

⚠ Caution

- Running the **clear** command during operation of the device may lose vital information and interrupt services.
- System resources are occupied when debugging information is output. Therefore, disable the debugging function immediately after use.

Table 1-1AP Monitoring

Command	Purpose
clear lacp counters [<i>key-number</i> <i>interface-type interface-number</i>]	Clears the statistics of LACP packets on an LACP AP member port.
show load-balance-profile [<i>profile-name</i>]	Displays the configuration of the enhanced load balancing profile.
show lacp summary [<i>key-number</i>]	Displays the state of an LACP AP. You can view the information of a specified LACP AP by specifying key-number .
show lacp counters [<i>key-number</i>]	Displays the statistics of LACP packets on LACP AP member ports. You can view the information of a specified LACP AP by specifying key-number .
show aggregateport [<i>ap-number</i>] summary	Displays the summary of an AP.
show aggregateport load-balance	Displays the load balancing information of an AP.
show aggregateport capacity	Displays the capacity mode and usage of an AP.
debug lsm ap	Debugs an AP.
debug lacp { cache-database cli ef-packet threadId pkt-agent pkt-statis pkt-thread packet event ha realtime stm timer all }	Debugs LACP.

1.13 Configuration Examples

1.13.1 Configuring Static APs

1. Requirements

Create AP interconnection for two devices on the IPv4 network, and configure static APs.

2. Topology

Figure 1-1 Topology for Configuring Static APs



3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.

4. Procedure

Create AP 3 on Device A.

```

DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
  
```

Create AP 3 on Device B.

```

DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
  
```

5. Verification

Run **show aggregateport summary** to check whether AP 3 contains member ports GigabitEthernet 0/1 and GigabitEthernet 0/2.

```

DeviceA# show aggregateport summary
AggregatePort MaxPorts SwitchPort Mode   Ports
-----
Ag3           8         Enabled  ACCESS Gi0/1,Gi0/2
DeviceB# show aggregateport summary
AggregatePort MaxPorts SwitchPort Mode   Ports
-----
Ag3           8         Enabled  ACCESS Gi0/1,Gi0/2
  
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
  port-group 3
!
interface GigabitEthernet 0/2
  port-group 3
!
interface AggregatePort 3
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
  port-group 3
!
interface GigabitEthernet 0/2
  port-group 3
!
interface AggregatePort 3
!
```

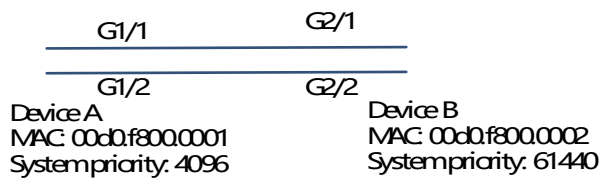
1.13.2 Configuring LACP APs

1. Requirements

Create AP interconnection for two devices on the IPv4 network, and configure dynamic APs.

2. Topology

Figure 1-1 Topology for Configuring LACP APs



3. Notes

- On Device A, set the LACP system priority to 4096.
- Enable dynamic link aggregation on the GigabitEthernet0/1 and GigabitEthernet0/2 ports on Device A and add the ports to LACP AP 3.
- On Device B, set the LACP system priority to 61440.
- Enable dynamic link aggregation on the GigabitEthernet0/1 and GigabitEthernet0/2 ports on Device B and add the ports to LACP AP 3.

4. Procedure

Configure LACP APs on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# lacp system-priority 4096
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# end
```

Configure LACP APs on Device B.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# lacp system-priority 61440
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3 mode active
```

5. Verification

Run **show lacp summary 3** to check whether LACP AP 3 contains member ports GigabitEthernet0/1 and GigabitEthernet0/2.

```
DeviceA# show LACP summary 3
System Id:32768,00d0.f8fb.0001
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs.
A - Device is in active mode.          P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper   Port      Port
Port           Flags  State     Priority   Key      Number    State
-----
Gi0/1          SA     bndl      32768     0x3      0x1       0x3d
Gi0/2          SA     bndl      32768     0x3      0x2       0x3d
Partner information:
Port           Flags  LACP port Priority   Dev ID    Oper   Port      Port
Port           Flags  Priority   Dev ID    Key      Number  State
-----
Gi0/1          SA     32768     00d0.f800.0002 0x3      0x1     0x3d
Gi0/2          SA     32768     00d0.f800.0002 0x3      0x2     0x3d

DeviceB # show LACP summary 3
SystemId:32768,00d0.f8fb.0002
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs.
A - Device is in active mode.          P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper   Port      Port
Port           Flags  State     Priority   Key      Number    State
-----
```


Gi0/1	SA	bndl	32768	0x3	0x1	0x3d
Gi0/2	SA	bndl	32768	0x3	0x2	0x3d
Partner information:						
		LACP port		Oper	Port	Port
Port	Flags	Priority	Dev ID	Key	Number	State
Gi0/1	SA	32768	00d0.f800.0001	0x3	0x1	0x3d
Gi0/2	SA	32768	00d0.f800.0001	0x3	0x2	0x3d

6. Configuration Files

- Device A configuration file

```
!
lacp system-priority 4096
!
interface GigabitEthernet 0/1
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 port-group 3 mode active
!
interface AggregatePort 3
!
```

- Device B configuration file

```
!
lacp system-priority 61440
!
interface GigabitEthernet 0/1
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 port-group 3 mode active
!
interface AggregatePort 3
!
```

1.13.3 Enabling LinkTrap

1. Requirements

On the IPv4 network, create AP interconnection for two devices, configure static APs, and enable LinkTrap.

2. Topology

Figure 1-1 Topology for Enabling LinkTrap



3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, disable LinkTrap for AP 3 and enable LinkTrap for its AP member ports.
- On Device B, disable LinkTrap for AP 3 and enable LinkTrap for its AP member ports.

4. Procedure

Perform the following configuration on Device A.

```

DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# aggregateport member linktrap
DeviceA(config)# interface Aggregateport 3
DeviceA(config-if-AggregatePort 3)# no snmp trap link-status
  
```

Perform the following configuration on Device B:

```

DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
DeviceB(config)# aggregateport member linktrap
DeviceB(config)# interface Aggregateport 3
DeviceB(config-if-AggregatePort 3)# no snmp trap link-status
  
```

5. Verification

Run **show running** to check whether LinkTrap is enabled for AP 3 and its member ports.

```

DeviceA# show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
  no snmp trap link-status
DeviceA# show run | include AggregatePort
aggregateport member linktrap
  
```

```
DeviceB# show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
  no snmp trap link-status
DeviceB# show run | include AggregatePort
aggregateport member linktrap
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
  port-group 3
!
interface GigabitEthernet 0/2
  port-group 3
!
interface AggregatePort 3
  no snmp trap link-status
!
aggregateport member linktrap
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
  port-group 3 mode active
!
interface GigabitEthernet 0/2
  port-group 3 mode active
!
interface AggregatePort 3
  no snmp trap link-status
!
aggregateport member linktrap
!
```

1.13.4 Configuring a Load Balancing Mode

1. Requirements

On the IPv4 network, create AP interconnection for two devices, configure static APs, and enable load balancing.

2. Topology

Figure 1-1 Topology for Configuring a Load Balancing Mode Topology



3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, configure source MAC address-based load balancing for AP 3 in global configuration mode.
- On Device B, configure destination MAC address-based load balancing for AP 3 in global configuration mode.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# aggregateport load-balance src-mac
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
DeviceB(config)# aggregateport load-balance dst-mac
```

5. Verification

Run **show aggregateport load-balance** to check the load balancing algorithm configuration.

```
DeviceA # show aggregatePort load-balance
Load-balance : Source MAC
```

```
DeviceB # show aggregatePort load-balance
Load-balance : Destination MAC
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
port-group 3
```

```

!
interface GigabitEthernet 0/2
  port-group 3
!
interface AggregatePort 3
!
aggregateport load-balance src-mac
!

```

- Device B configuration file

```

!
interface GigabitEthernet 0/1
  port-group 3
!
interface GigabitEthernet 0/2
  port-group 3
!
interface AggregatePort 3
!
aggregateport load-balance dst-mac
!

```

7. Common Errors

A user configures the factors **ipv4**, **ipv6**, **fcoe**, and **on** for enabling hash synchronization. However, no configuration is displayed when the user runs **show running**. This is because hash synchronization is enabled for some products by default. The configuration will be displayed after the user disables the function.

1.13.5 Configuring Hash Load Balancing Control

1. Requirements

Create AP interconnection for two devices on the IPv4 network.

2. Topology

Figure 1-1 Topology for Configuring Static APs



3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, disable hash synchronization for IPv4 packets.
- On Device B, disable hash synchronization for IPv4 packets.

- On Device A, configure the hash disturbance factor A.
- On Device B, configure the hash disturbance factor B.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# load-balance-profile default
DeviceA(config-load-balance-profile)# no hash-symmetrical ipv4
DeviceA(config-load-balance-profile)# hash-disturb A
DeviceA(config-load-balance-profile)# exit
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
DeviceB(config)# load-balance-profile default
DeviceB(config-load-balance-profile)# no hash-symmetrical ipv4
DeviceA(config-load-balance-profile)# hash-disturb B
DeviceB(config-load-balance-profile)# exit
```

5. Verification

Run **show running** to check whether the configuration is correct.

6. Configuration Files

- Device A configuration file

```
!
load-balance-profile default
  no hash-symmetrical ipv4
  hash-disturb A
!
interface GigabitEthernet 0/1
  port-group 3
!
interface GigabitEthernet 0/2
  port-group 3
!
```

- Device B configuration file

```
!
load-balance-profile default
  no hash-symmetrical ipv4
  hash-disturb B
```

```
!
interface GigabitEthernet 0/1
  port-group 3
!
interface GigabitEthernet 0/2
  port-group 3
!
```

7. Common Errors

A user configures the factors **ipv4**, **ipv6** and **on** for enabling hash synchronization. However, no configuration is displayed when the user runs **show running**. This is because hash synchronization is enabled for some products by default. The configuration will be displayed after the user disables the function.

1.13.6 Configuring an AP Capacity Mode

1. Requirements

Create AP interconnection for two devices on the IPv4 network.

2. Topology

Figure 1-1 Configuring an AP Capacity Mode



3. Notes

- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A to static AP 3.
- Add the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B to static AP 3.
- On Device A, configure the 128 x 128 AP capacity mode.
- On Device B, configure the 256 x 64 AP capacity mode.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3
DeviceA(config-if-range)# exit
DeviceA(config)# aggregateport capacity mode 128*8
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# port-group 3
DeviceB(config-if-range)# exit
```

```
DeviceB(config)# aggregateport capacity mode 128*8
```

5. Verification

Run **show aggregateport capacity** to check the AP capacity mode configuration.

```
DeviceA# show aggregatePort capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 128*8.
Effective Capacity Mode      : 128*8.
Available Capacity Mode      : 128*8.
Total Number : 128, Used: 1, Available: 127.
DeviceB DeviceB# show aggregatePort capacity
AggregatePort Capacity Information:
Configuration Capacity Mode: 256*64.
Effective Capacity Mode      : 256*64.
Available Capacity Mode      : 256*64.
Total Number : 256, Used: 1, Available: 255.
```

6. Configuration Files

- Device A configuration file

```
!
aggregateport capacity mode 128*8
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
```

- Device B configuration file

```
!
aggregateport capacity mode 128*8
!
interface GigabitEthernet 0/1
 port-group 3
!
interface GigabitEthernet 0/2
 port-group 3
!
interface AggregatePort 3
!
```

1.13.7 Enabling BFD for Member Ports

1. Requirements

Create AP interconnection for two devices on the IPv4 network.

2. Topology

Figure 1-1 Topology for Enabling BFD for AP Member Ports



3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A and add the ports to LACP AP 3.
- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B and add the ports to LACP AP 3.
- Configure IP address 1.0.0.1 for AP 3 on Device A and enable IPv4 BFD.
- Configure IP address 1.0.0.2 for AP 3 on Device B and enable IPv4 BFD.

4. Procedure

Perform the following configuration on Device A:

```

DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# no switchport
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# ip address 1.0.0.1 255.255.255.0
DeviceA(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
DeviceA(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
  
```

Perform the following configuration on Device B:

```

DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# no switchport
DeviceB(config-if-range)# port-group 3 mode active
DeviceB(config-if-range)# exit
DeviceB(config)# interface aggregateport 3
DeviceB(config-if-Aggregateport 3)# ip address 1.0.0.2 255.255.255.0
DeviceB(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1
DeviceB(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
  
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show interface aggregateport** to view the BFD state of each AP member port.

```

DeviceA# show run | include AggregatePort 3
Building configuration...
  
```

```

Current configuration: 54 bytes
interface AggregatePort 3
  no switchport
  ip address 1.0.0.1 255.255.255.0
  aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
  bfd interval 50 min_rx 50 multiplier 3
DeviceA# show interface aggregateport 3
...
Aggregate Port Informations:
  Aggregate Number: 3
  Name: "AggregatePort 3"
  Members: (count=2)
  GigabitEthernet 0/1      Link Status: Up    LACP Status: bndl  BFD
Status: UP
  GigabitEthernet 0/2      Link Status: Up    LACP Status: bndl  BFD
Status: UP

```

```

DeviceB# show run | include AggregatePort 3
Building configuration...
Current configuration: 54 bytes
interface AggregatePort 3
  no switchport
  ip address 1.0.0.2 255.255.255.0
  aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1
  bfd interval 50 min_rx 50 multiplier 3
DeviceB# show interface aggregateport 3
...
Aggregate Port Informations:
  Aggregate Number: 3
  Name: "AggregatePort 3"
  Members: (count=2)
  GigabitEthernet 0/1      Link Status: Up    LACP Status: bndl  BFD
Status: UP
  GigabitEthernet 0/2      Link Status: Up    LACP Status: bndl  BFD
Status: UP

```

6. Configuration Files

- Device A configuration file

```

!
interface GigabitEthernet 0/1
  no switchport
  port-group 3 mode active
!
interface GigabitEthernet 0/2
  no switchport

```

```
port-group 3 mode active
!
interface AggregatePort 3
no switchport
aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2
ip address 1.0.0.1 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
```

- Device B configuration file

```
!
interface GigabitEthernet 0/1
no switchport
port-group 3 mode active
!
interface GigabitEthernet 0/2
no switchport
port-group 3 mode active
!
interface AggregatePort 3
no switchport
aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1
ip address 1.0.0.2 255.255.255.0
bfd interval 50 min_rx 50 multiplier 3
!
```

7. Common Errors

- If BFD is enabled for an AP without BFD parameters, BFD does not take effect.
- After BFD is enabled for an AP, the BFD neighbor must be a directly connected AP enabled with BFD.

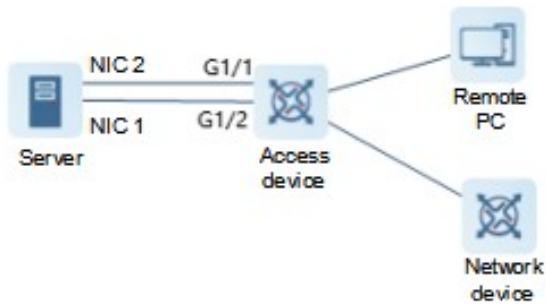
1.13.8 Configuring Interworking Between the Access Device and a Server with Two NICs over a Preferred LACP AP

1. Requirements

The server has two management systems: the remote management OS and server OS. The two OSs are independent of each other. When the server OS restarts, access to the remote management OS is normal. The remote management OS is used to manage the server OS and uses NIC 1 as the communication port to access the access device GigabitEthernet0/1 in Figure 1-1. It is allocated with a specific VLAN, for example, VLAN 10. The server OS is used to handle routine production services and uses NIC 1 and NIC 2 as the communication ports. LACP aggregation is enabled between NIC 1 and NIC 2. The server OS accesses the access device over the aggregate link. A VLAN except the management VLAN is allocated to the server OS. NIC 1 is used as the communication port for both the remote management OS and server OS. Based on the VLAN tag carried in packets, the server determines whether packets received from NIC 1 are sent to the remote management OS or server OS.

2. Topology

Figure 1-1Topology for Configuring Interworking Between the Access Device and a Server with Two NICs over a Preferred LACP AP



3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on the access device and add the ports to LACP AP 3.
- Configure GigabitEthernet 0/1 on the access device as the preferred port.
- Configure VLAN 10 on the access device as the management VLAN.

4. Procedure

Create LACP AP 3 and add AP 3 to the trunk.

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# switchport mode trunk
DeviceA(config-if-Aggregateport 3)# exit
```

Configure VLAN 10 as the management VLAN.

```
DeviceA(config)# aggregateport-admin vlan 10
```

Configure GigabitEthernet 0/1 as the preferred port.

```
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1) aggregateport primary-port
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show interface aggregateport** to query the preferred AP member port.

```
DeviceA# show run | include aggregateport-admin
Building configuration...
Current configuration: 54 bytes
aggregateport-admin vlan 10
DeviceA# show run | include GigabitEthernet 0/1
```

```

Building configuration...
Current configuration: 54 bytes
interface GigabitEthernet 0/1
aggregateport primary-port
  portgroup 3 mode active
DeviceA# show interface aggregateport 3
...
Aggregate Port Informations:
  Aggregate Number: 3
  Name: "AggregatePort 3"
  Members: (count=2)
  Primary Port: GigabitEthernet 0/1
  GigabitEthernet 0/1      Link Status: Up      LACP Status: bndl
  GigabitEthernet 0/2      Link Status: Up      LACP Status: bndl
...

```

6. Configuration Files

- Device A configuration file

```

!
aggregateport-admin vlan 10
!
interface GigabitEthernet 0/1
  port-group 3 mode active
  aggregateport primary-port
!
interface GigabitEthernet 0/2
  port-group 3 mode active
!
interface AggregatePort 3
  switchport mode trunk
!

```

1.13.9 Configuring Automatic Server Deployment over a Preferred LACP AP

1. Requirements

The server has two NICs, and the two NICs connect to Switch A over the LACP AP. The server can be automatically installed over NIC 1. After the server is installed, management data streams are sent over NIC 1 and NIC 2 for mutual backup and load balancing.

2. Topology

Figure 1-1 Topology for Configuring Automatic Server Deployment over a Preferred LACP AP



3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A and add the ports to LACP AP 3.
- Configure GigabitEthernet 0/1 on Device A as the preferred port.

4. Procedure

Create LACP AP 3.

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
```

Configure GigabitEthernet 0/1 as the preferred port.

```
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1) aggregateport primary-port
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show interface aggregateport** to query the preferred AP member port.

```
DeviceA# show run | include GigabitEthernet 0/1
Building configuration...
Current configuration: 54 bytes
interface GigabitEthernet 0/1
aggregateport primary-port
 portgroup 3 mode active
DeviceA# show interface aggregateport 3
...
Aggregate Port Informations:
  Aggregate Number: 3
  Name: "AggregatePort 3"
  Members: (count=2)
  Primary Port: GigabitEthernet 0/1
  GigabitEthernet 0/1      Link Status: Up      LACP Status: bndl
  GigabitEthernet 0/2      Link Status: Up      LACP Status: bndl
...
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3 mode active
 aggregateport primary-port
!
interface GigabitEthernet 0/2
```

```

port-group 3 mode active
!
interface AggregatePort 3
!

```

1.13.10 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Less Than the Minimum Number)

1. Requirements

On the IPv4 network, create AP interconnection for two devices, and configure a number of AP member ports less than the minimum number of AP Member ports.

2. Topology

Figure 1-1 Topology for Configuring the Minimum Number of AP Member Ports



3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device A and add the ports to LACP AP 3.
- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on Device B and add the ports to LACP AP 3.
- On Device A, set the minimum number of the member ports of AP 3 to 3.

4. Procedure

Perform the following configuration on Device A:

```

DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# no switchport
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# aggregateport member minimum 3

```

Perform the following configuration on Device B:

```

DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-2
DeviceB(config-if-range)# no switchport
DeviceB(config-if-range)# port-group 3 mode active
DeviceB(config-if-range)# exit
DeviceB(config)# interface aggregateport 3
DeviceB(config-if-Aggregateport 3)# aggregateport member minimum 3

```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show lacp summary** to view the aggregation state of each AP member port.

```
DeviceA# show LACP summary 3
System Id:32768, 00d0.f8fb.0001
Flags: -S - Device is requesting Slow LACPDUs
-F - Device is requesting Fast LACPDUs.-A - Device is in active mode.      -P -
Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper      Port      Port
Port      Flags      State      Priority      Key      Number      Sta--
Gi0/1      SA          susp       32768        0x3      0x1          0x3d
Gi0/2      SA          susp       32768        0x3      0x2          0x3d
Partner information:
Port      Flags      LACP port      Oper      Port      Port
Port      Flags      Priority      Dev ID      Key      Number      Sta--
Gi0/1      SA          32768        00d0.f800.0002  0x3      0x1          0x3d
Gi0/2      SA          32768        00d0.f800.0002  0x3      0x2          0x3d
```

6. Configuration Files

- Configuration file of device A

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
!
interface AggregatePort 3
 no switchport
 aggregateport member minimum 3
!
```

- Configuration file of Device B

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
```



```
!
interface AggregatePort 3
  no switchport
  aggregateport member minimum 3
!
```

1.13.11 Configuring the Minimum Number of AP Member Ports (When the Number of AP Member Ports Is Not Less Than the Minimum Number)

1. Requirements

On the IPv4 network, create AP interconnection for two devices, and configure the number of AP member ports not less than the minimum number of AP Member ports.

2. Topology

Figure 1-1 Topology for Configuring the Minimum Number of AP Member Ports



3. Notes

- Enable LACP for the GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 ports on Device A and add the ports to LACP AP 3.
- Enable LACP for the GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 ports on Device B and add the ports to LACP AP 3.
- On Device A, set the minimum number of member ports of AP 3 to 2.

4. Procedure

Perform the following configuration on Device A:

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-3
DeviceA(config-if-range)# no switchport
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# aggregateport member minimum 2
```

Perform the following configuration on Device B:

```
DeviceB# configure terminal
DeviceB(config)# interface range GigabitEthernet 0/1-3
DeviceB(config-if-range)# no switchport
DeviceB(config-if-range)# port-group 3 mode active
DeviceB(config-if-range)# exit
DeviceB(config)# interface aggregateport 3
```

```
DeviceB(config-if-Aggregateport 3)# aggregateport member minimum 2
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show lacp summery** to view the aggregation state of each AP member port.

```
DeviceA# show LACP summary 3
System Id:32768,00d0.f8fb.0001
Flags: -S - Device is requesting Slow LACPDUs
-F - Device is requesting Fast LACPDUs.-A - Device is in active mode.      -P -
Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper    Port      Port
Port      Flags    State    Priority    Key      Number    Sta--
Gi0/1     SA      bndl     32768     0x3     0x1     0x3d
Gi0/2     SA      bndl     32768     0x3     0x2     0x3d
Gi0/3     SA      bndl     32768     0x3     0x3     0x3d

Partner information:
Port      Flags    LACP port      Oper    Port      Port
Port      Flags    Priority    Dev ID    Key      Number    Sta--
Gi0/1     SA      32768     00d0.f800.0002  0x3     0x1     0x3d
Gi0/2     SA      32768     00d0.f800.0002  0x3     0x2     0x3d
Gi0/3     SA      32768     00d0.f800.0002  0x3     0x3     0x3d
```

6. Configuration Files

- Configuration file of device A

```
!
interface GigabitEthernet 0/1
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/2
 no switchport
 port-group 3 mode active
!
interface GigabitEthernet 0/3
 no switchport
 port-group 3 mode active
!
interface AggregatePort 3
 no switchport
 aggregateport member minimum 2
!
```

- Configuration file of device A

```
!  
interface GigabitEthernet 0/1  
  no switchport  
  port-group 3 mode active  
!  
interface GigabitEthernet 0/2  
  no switchport  
  port-group 3 mode active  
!  
interface GigabitEthernet 0/3  
  no switchport  
  port-group 3 mode active  
!  
interface AggregatePort 3  
  no switchport  
  aggregateport member minimum 2  
!
```

1.13.12 Enabling the LACP Independent Port Function

1. Requirements

The server uses NIC 1 and NIC 2 as the communication ports to get access to the GigabitEthernet0/1 and GigabitEthernet0/2 of the access device. GigabitEthernet0/1 and GigabitEthernet0/2 are added to the LACP aggregation group, for example, AP 3. A specific VLAN, for example, VLAN 10 is allocated. The LACP independent port function is enabled for GigabitEthernet0/1 and GigabitEthernet0/2. When the OS is not installed on the server, LACP negotiation between the server and the access device fails. In this case, GigabitEthernet0/1 and GigabitEthernet0/2 of the access device change to common physical ports and are allocated to VLAN 10 automatically. The server uses NIC 1 or NIC 2 to communicate with the remote OS installation device. After the OS is installed, the server connects to the access device in LACP mode.

2. Topology

Figure 1-1 Topology for Enabling the LACP Independent Port Function



3. Notes

- Enable LACP for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on the access device and add the ports to LACP AP 3.
- Enable the LACP independent port function for the GigabitEthernet 0/1 and GigabitEthernet 0/2 ports on the access device.
- Allocate AP 3 on the access device to VLAN 10.

4. Procedure

Create an AP on Device A.

```
DeviceA# configure terminal
DeviceA(config)# interface range GigabitEthernet 0/1-2
DeviceA(config-if-range)# port-group 3 mode active
DeviceA(config-if-range)# lacp individual-port enable
DeviceA(config-if-range)# exit
DeviceA(config)# interface aggregateport 3
DeviceA(config-if-Aggregateport 3)# switch access vlan 10
```

5. Verification

Run **show run** to check whether the configuration is correct.

Run **show lacp summary** to view the aggregation state of each AP member port.

```
DeviceA# show LACP summary 3
System Id:32768,00d0.f8fb.0001
Flags: -S - Device is requesting Slow LACPDUs
-F - Device is requesting Fast LACPDUs.-A - Device is in active mode.      -P -
Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper      Port      Port
Port      Flags      State      Priority      Key      Number      Sta--
Gi0/1      SA      individual  32768      0x3      0x1      0x3d
Gi0/2      SA      individual  32768      0x3      0x2      0x3d
Partner information:
LACP port      Oper      Port      Port
Port      Flags      Priority      Dev ID      Key      Number      Sta--
Gi0/1      SA      32768      00d0.f800.0002  0x3      0x1      0x3d
Gi0/2      SA      32768      00d0.f800.0002  0x3      0x2      0x3d
```

6. Configuration Files

- Device A configuration file

```
!
interface GigabitEthernet 0/1
 port-group 3 mode active
 lacp individual-port enable
!
interface GigabitEthernet 0/2
 port-group 3 mode active
 lacp individual-port enable
!
interface AggregatePort 3
 switchport access vlan 10
!
```