H3C S5560X-EI & S5500V2-EI Switch Series & MS4520V2-30F Switch

Virtual Technologies Configuration Guide

This configuration guide is applicable to the following switches and software versions:
H3C S5560X-EI switch series (Release 6308 and later)
H3C S5500V2-EI switch series (Release 6308 and later)
H3C MS4520V2-30F switch (Release 6308 and later)

New H3C Technologies Co., Ltd.
http://www.h3c.com

Software version: Release 63xx
Document version: 6W101-20201015

Preface

This configuration guide describes the fundamentals and configuration procedures for IRF and IRF 3.1 features.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.
- Documentation feedback.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Configuring an IRF fabric

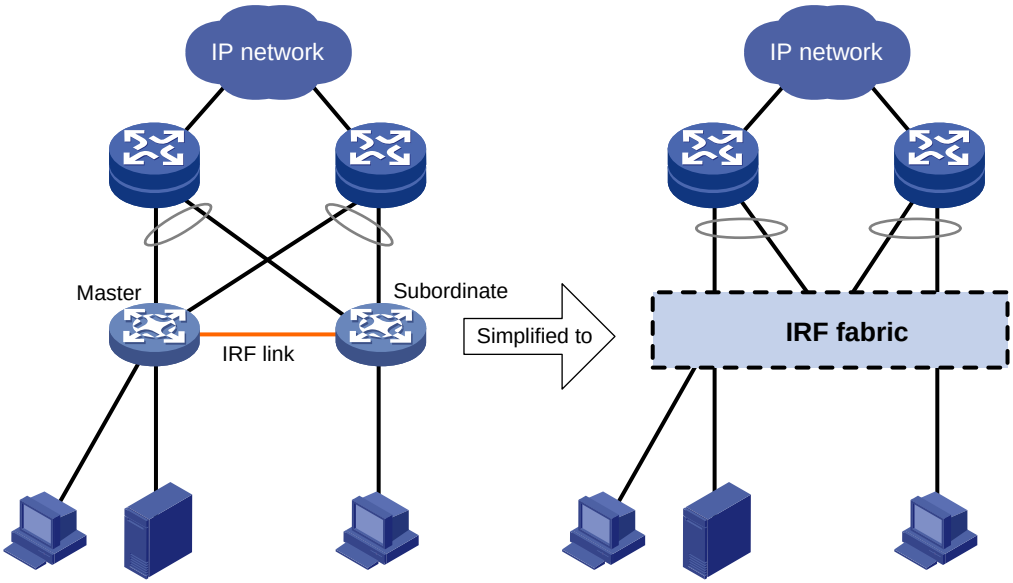
About IRF

The Intelligent Resilient Framework (IRF) technology virtualizes multiple physical devices at the same layer into one virtual fabric to provide data center class availability and scalability. IRF virtualization technology offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

IRF network model

Figure 1 shows an IRF fabric that has two devices, which appear as a single node to the upper-layer and lower-layer devices.

Figure 1 IRF application scenario



IRF benefits

IRF provides the following benefits:

- **Simplified topology and easy management**—An IRF fabric appears as one node and is accessible at a single IP address on the network. You can use this IP address to log in at any member device to manage all the members of the IRF fabric. In addition, you do not need to run the spanning tree feature among the IRF members.
- **1:N redundancy**—In an IRF fabric, one member acts as the master to manage and control the entire IRF fabric. All the other members process services while backing up the master. When the master fails, all the other member devices elect a new master from among them to take over without interrupting services.
- **IRF link aggregation**—You can assign several physical links between neighboring members to their IRF ports to create a load-balanced aggregate IRF connection with redundancy.
- **Multichassis link aggregation**—You can use the Ethernet link aggregation feature to aggregate the physical links between the IRF fabric and its upstream or downstream devices across the IRF members.

- **Network scalability and resiliency**—Processing capacity of an IRF fabric equals the total processing capacities of all the members. You can increase ports, network bandwidth, and processing capacity of an IRF fabric simply by adding member devices without changing the network topology.

Basic concepts

IRF member roles

IRF uses two member roles: master and standby (called subordinate throughout the documentation).

When devices form an IRF fabric, they elect a master to manage and control the IRF fabric, and all the other devices back up the master. When the master device fails, the other devices automatically elect a new master. For more information about master election, see "Master election."

IRF member ID

An IRF fabric uses member IDs to uniquely identify and manage its members. This member ID information is included as the first part of interface numbers and file paths to uniquely identify interfaces and files in an IRF fabric. Two devices cannot form an IRF fabric if they use the same member ID. A device cannot join an IRF fabric if its member ID has been used in the fabric.

Member priority

Member priority determines the possibility of a member device to be elected the master. A member with higher priority is more likely to be elected the master.

IRF port

An IRF port is a logical interface that connects IRF member devices. Every IRF-capable device has two IRF ports.

The IRF ports are named IRF-port *n*/1 and IRF-port *n*/2, where *n* is the member ID of the device. The two IRF ports are referred to as IRF-port 1 and IRF-port 2.

To use an IRF port, you must bind a minimum of one physical interface to it. The physical interfaces assigned to an IRF port automatically form an aggregate IRF link. An IRF port goes down when all its IRF physical interfaces are down.

IRF physical interface

IRF physical interfaces connect IRF member devices and must be bound to an IRF port. They forward traffic between member devices, including IRF protocol packets and data packets that must travel across IRF member devices.

IRF split

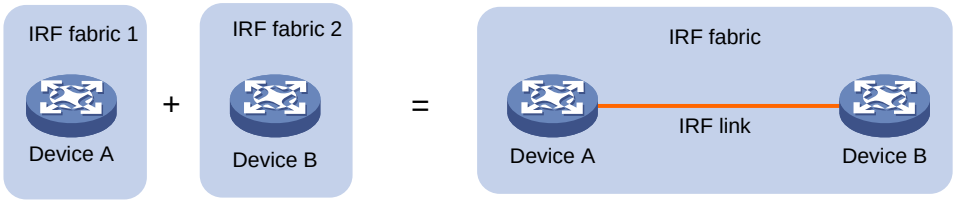
IRF split occurs when an IRF fabric breaks up into multiple IRF fabrics because of IRF link failures, as shown in Figure 2. The split IRF fabrics operate with the same IP address. IRF split causes routing and forwarding problems on the network. To quickly detect a multi-active collision, configure a minimum of one MAD mechanism (see "Configuring MAD").

Figure 2 IRF split

IRF merge

IRF merge occurs when two split IRF fabrics reunite or when two independent IRF fabrics are united, as shown in Figure 3.

Figure 3 IRF merge



MAD

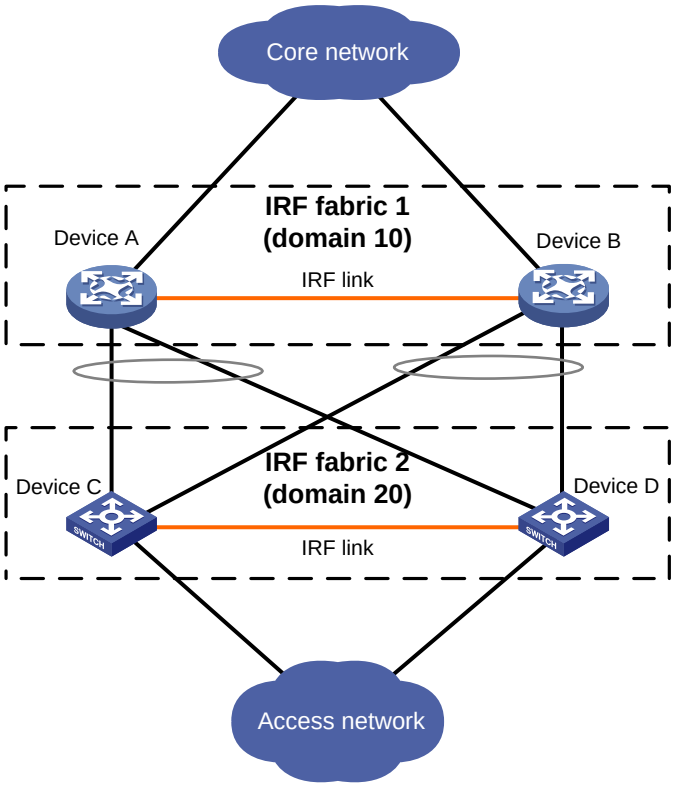
An IRF link failure causes an IRF fabric to split in two IRF fabrics operating with the same Layer 3 settings, including the same IP address. To avoid IP address collision and network problems, IRF uses multi-active detection (MAD) mechanisms to detect the presence of multiple identical IRF fabrics, handle collisions, and recover from faults.

IRF domain ID

One IRF fabric forms one IRF domain. IRF uses IRF domain IDs to uniquely identify IRF fabrics and prevent IRF fabrics from interfering with one another.

As shown in Figure 4, IRF fabric 1 contains Device A and Device B, and IRF fabric 2 contains Device C and Device D. Both fabrics use the LACP aggregate links between them for MAD. When a member device receives an extended LACPDU for MAD, it checks the domain ID to determine whether the packet is from the local IRF fabric. Then, the member device can handle the packet correctly.

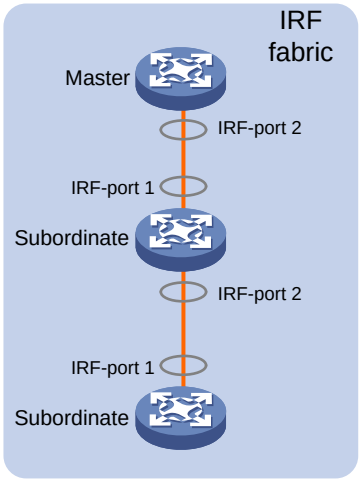
Figure 4 A network that contains two IRF domains



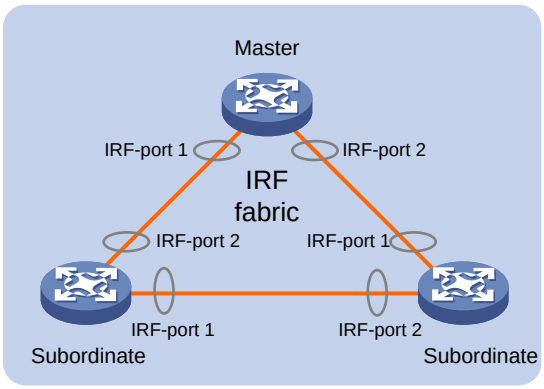
IRF network topology

An IRF fabric can use a daisy-chain or ring topology. As shown in Figure 5, a ring topology is more reliable. In ring topology, the failure of one IRF link does not cause the IRF fabric to split as in daisy-chain topology. Rather, the IRF fabric changes to a daisy-chain topology without interrupting network services.

Figure 5 Daisy-chain topology vs. ring topology



Daisy-chain topology



Ring topology

Master election

Master election occurs each time the IRF fabric topology changes in the following situations:

- The IRF fabric is established.
- The master device fails or is removed.
- The IRF fabric splits.
- Independent IRF fabrics merge.

NOTE:

Master election does not occur when split IRF fabrics merge. For information about the master device of the merged IRF fabric, see "Failure recovery."

Master election selects a master in descending order:

1. Current master, even if a new member has higher priority.

   When an IRF fabric is being formed, all members consider themselves as the master. This rule is skipped.
2. Member with higher priority.
3. Member with the longest system uptime.

   Two members are considered to start up at the same time if the difference between their startup times is equal to or less than 10 minutes. For these members, the next tiebreaker applies.
4. Member with the lowest CPU MAC address.

For the setup of a new IRF fabric, the subordinate devices must reboot to complete the setup after the master election.

For an IRF merge, devices must reboot if they are in the IRF fabric that fails the master election.

Interface naming conventions

A physical interface is numbered in the *chassis-number/slot-number/interface-index* format.

- ***chassis-number***—Member ID of the device. The default value for this argument is 1. Any change to the member ID takes effect after a reboot.
- ***slot-number***—Slot number of the interface.
  - The slot number is 0 if the interface is on the front panel.
  - The slot number is 1 if the interface is on an interface module.
- ***interface-index***—Interface index on the device. Interface index depends on the number of physical interfaces available on the device. To identify the index of a physical interface, examine its index mark on the chassis.

For example, GigabitEthernet 3/0/1 represents the first fixed physical interface on member device 3. Set its link type to trunk, as follows:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] port link-type trunk
```

File system naming conventions

On a single-chassis fabric, you can use its storage device name to access its file system.

On a multichassis IRF fabric, you can use the storage device name to access the file system of the master. To access the file system of any other member device, use the name in the **slot***member-ID#storage-device-name* format.

For more information about storage device naming conventions, see *Fundamentals Configuration Guide*.

For example:

- To create and access the **test** folder under the root directory of the flash memory on the master switch:

  ```
  <Master> mkdir test
  Creating directory flash:/test... Done.
  <Master> cd test
  <Master> dir
  Directory of flash:/test
  The directory is empty.

  514048 KB total (48140 KB free)
  ```

- To create and access the **test** folder under the root directory of the flash memory on member device 3:

  ```
  <Master> mkdir slot3#flash:/test
  Creating directory slot3#flash:/test... Done.
  <Master> cd slot3#flash:/test
  <Master> dir
  Directory of slot3#flash:/test
  The directory is empty.

  514048 KB total (48140 KB free)
  ```

Configuration synchronization

IRF uses a strict running-configuration synchronization mechanism. In an IRF fabric, all devices obtain and run the running configuration of the master. Configuration changes are automatically propagated from the master to the remaining devices. The configuration files of these devices are retained, but the files do not take effect. The devices use their own startup configuration files only after they are removed from the IRF fabric.

As a best practice, back up the next-startup configuration file on a device before adding the device to an IRF fabric as a subordinate.

A subordinate device's next-startup configuration file might be overwritten if the master and the subordinate use the same file name for their next-startup configuration files. You can use the backup file to restore the original configuration after removing the subordinate from the IRF fabric.

For more information about configuration management, see *Fundamentals Configuration Guide*.

Multi-active handling procedure

The multi-active handling procedure includes detection, collision handling, and failure recovery.

Detection

IRF provides MAD mechanisms by extending LACP, BFD, ARP, and IPv6 ND to detect multi-active collisions. As a best practice, configure a minimum of one MAD mechanism on an IRF fabric. For more information about the MAD mechanisms and their application scenarios, see "MAD mechanisms."

For information about LACP, see Ethernet link aggregation in *Layer 2—LAN Switching Configuration Guide*. For information about BFD, see *High Availability Configuration Guide*. For information about ARP, see *Layer 3—IP Services Configuration Guide*. For information about ND, see IPv6 basics in *Layer 3—IP Services Configuration Guide*.

Collision handling

When detecting a multi-active collision, MAD disables all IRF fabrics except one from forwarding data traffic by placing them in Recovery state. The IRF fabrics placed in Recovery state are called inactive IRF fabrics. The IRF fabric that continues to forward traffic is called the active IRF fabric.

LACP MAD and BFD MAD use the following process to handle a multi-active collision:

1. Compare the number of members in each fabric.
2. Set all fabrics to the Recovery state except the one that has the most members.
3. Compare the member IDs of the masters if all IRF fabrics have the same number of members.
4. Set all fabrics to the Recovery state except the one that has the lowest numbered master.
5. Shut down all common network interfaces in the Recovery-state fabrics except for the following interfaces:
   - Interfaces automatically excluded from being shut down by the system.
   - Interfaces specified by using the **`mad exclude interface`** command.

ARP MAD and ND MAD use the following process to handle a multi-active collision:

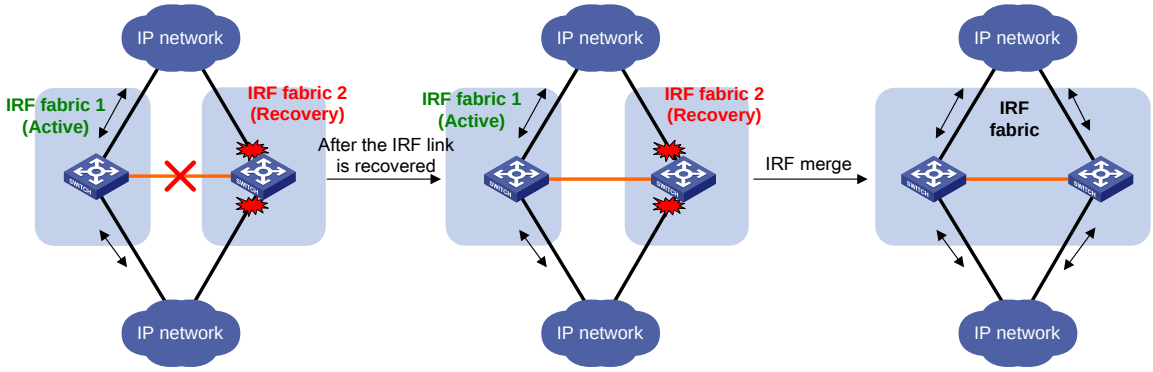
1. Compare the member IDs of the masters in the IRF fabrics.
2. Set all fabrics to the Recovery state except the one that has the lowest numbered master.
3. Take the same action as LACP MAD and BFD MAD on the network interfaces in Recovery-state fabrics.

Failure recovery

To merge two split IRF fabrics, first repair the failed IRF link and remove the IRF link failure.

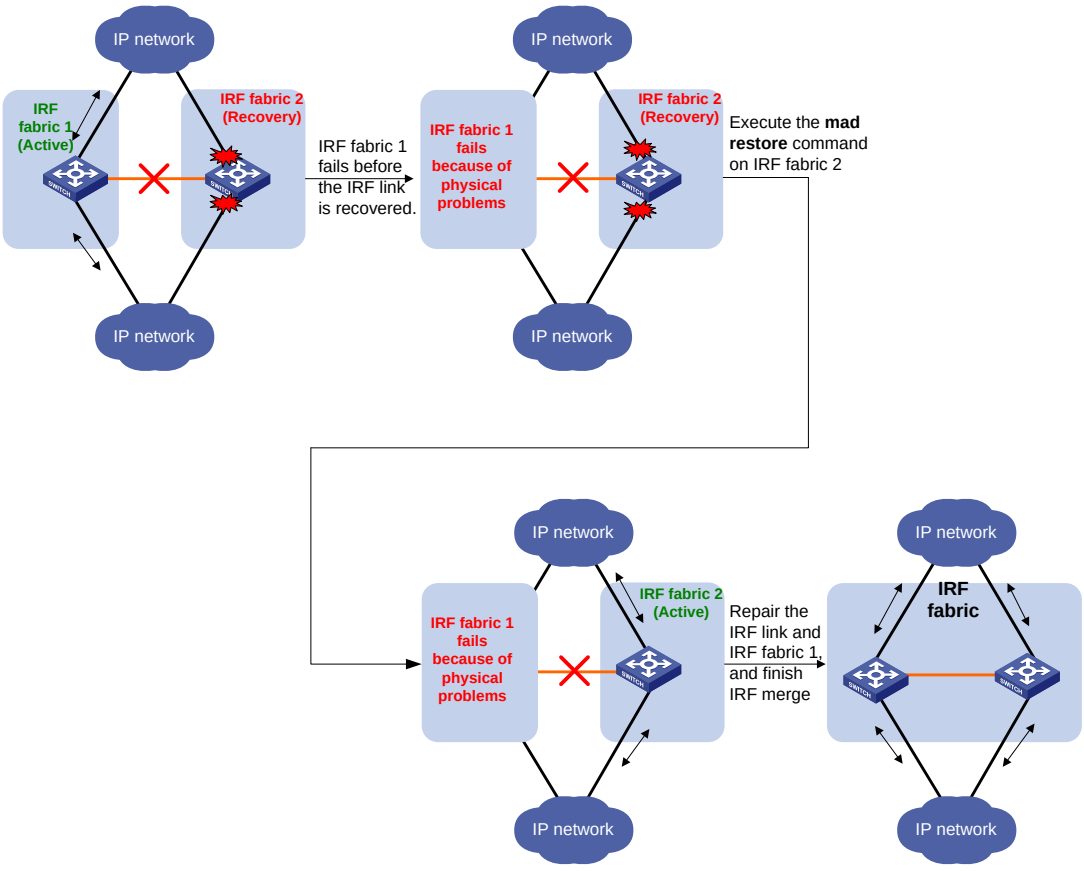
When the failed IRF link between two split IRF fabrics is recovered, all member devices in the inactive IRF fabric automatically reboot to join the active IRF fabric as subordinate members. The network interfaces that have been shut down by MAD automatically restore their original state, as shown in Figure 6.

Figure 6 Recovering the IRF fabric



If the active IRF fabric fails before the IRF link is recovered (see Figure 7), use the **`mad restore`** command on the inactive IRF fabric to recover the inactive IRF fabric. This command brings up all network interfaces that were shut down by MAD. After the IRF link is repaired, merge the two parts into a unified IRF fabric.

Figure 7 Active IRF fabric fails before the IRF link is recovered



MAD mechanisms

IRF provides MAD mechanisms by extending LACP, BFD, ARP, and IPv6 ND.

Table 1 compares the MAD mechanisms and their application scenarios.

Table 1 Comparison of MAD mechanisms

MAD mechanism	Advantages	Disadvantages	Application scenarios
LACP MAD	• Detection speed is fast. • Runs on existing aggregate links without requiring MAD-dedicated physical links or Layer 3 interfaces.	Requires an intermediate device that supports extended LACP for MAD.	Link aggregation is used between the IRF fabric and its upstream or downstream device.
BFD MAD	• Detection speed is fast. • Intermediate device, if used, can come from any vendor.	Requires MAD dedicated physical links and Layer 3 interfaces, which cannot be used for transmitting user traffic.	• No special requirements for network scenarios. • If no intermediate device is used, this mechanism is only suitable for IRF fabrics that have only two members that are geographically close to one another.
ARP MAD	• No intermediate device is required. • Intermediate device, if used, can come from any vendor. • Does not require MAD dedicated ports.	• Detection speed is slower than BFD MAD and LACP MAD. • The spanning tree feature must be enabled if common Ethernet ports are used for ARP MAD links.	Non-link aggregation IPv4 network scenarios. Spanning tree-enabled non-link aggregation IPv4 network scenarios if common Ethernet ports are used.
ND MAD	• No intermediate device is required. • Intermediate device, if used, can come from any vendor. • Does not require MAD dedicated ports.	• Detection speed is slower than BFD MAD and LACP MAD. • The spanning tree feature must be enabled if common Ethernet ports are used for ND MAD links.	Non-link aggregation IPv6 network scenarios. Spanning tree-enabled non-link aggregation IPv6 network scenarios if common Ethernet ports are used.

LACP MAD

As shown in Figure 8, LACP MAD has the following requirements:

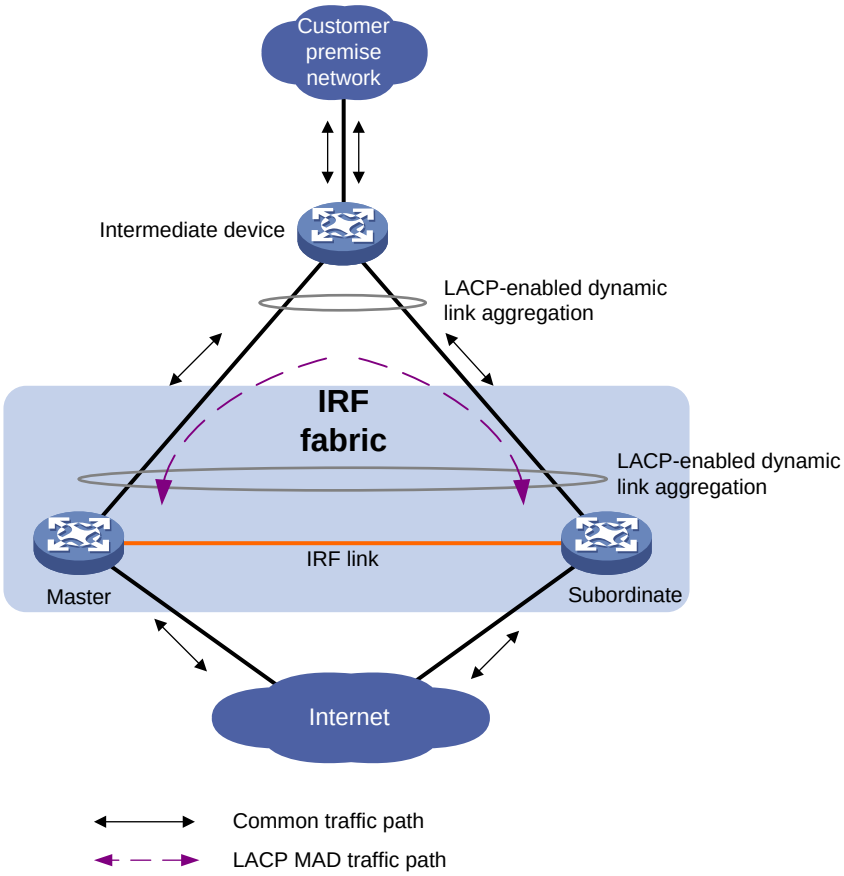
- Every IRF member must have a link with an intermediate device.
- All the links form a dynamic link aggregation group.
- The intermediate device must be a device that supports extended LACP for MAD.

The IRF member devices send extended LACPDUs that convey a domain ID and an active ID (the member ID of the master). The intermediate device transparently forwards the extended LACPDUs received from one member device to all the other member devices.

- If the domain IDs and active IDs sent by all the member devices are the same, the IRF fabric is integrated.

- If the extended LACPDUs convey the same domain ID but different active IDs, a split has occurred. LACP MAD handles this situation as described in "Collision handling."

Figure 8 LACP MAD scenario



BFD MAD

BFD MAD detects multi-active collisions by using BFD.

You can use common or management Ethernet ports for BFD MAD.

If management Ethernet ports are used, BFD MAD has the following requirements:

- An intermediate device is required and each IRF member device must have a BFD MAD link to the intermediate device.
- Each member device is assigned a MAD IP address on the master's management Ethernet port.

If common Ethernet ports are used, BFD MAD has the following requirements:

- If an intermediate device is used, each member device must have a BFD MAD link to the intermediate device. If no intermediate device is used, all member devices must have a BFD MAD link to each other. As a best practice, use an intermediate device to connect IRF member devices if the IRF fabric has more than two member devices. A full mesh of IRF members might cause broadcast loops.
- Ports on BFD MAD links are assigned to the same VLAN or Layer 3 aggregate interface. Each member device is assigned a MAD IP address on the VLAN interface or Layer 3 aggregate interface.

The BFD MAD links and BFD MAD VLAN (or Layer 3 aggregate interface) must be dedicated. Do not use the BFD MAD links or BFD MAD VLAN (or Layer 3 aggregate interface) for any other purposes.

When you use a Layer 3 aggregate interface for BFD MAD, make sure its member ports do not exceed the maximum number of Selected ports allowed for an aggregation group. If the number of member ports exceeds the maximum number of Selected ports, some member ports cannot become Selected. BFD MAD will be unable to work correctly and its state will change to Faulty. For more information about setting the maximum number of Selected ports for an aggregation group, see Ethernet link aggregation in *Layer 2—LAN Switching Configuration Guide*.

NOTE:

- The MAD addresses identify the member devices and must belong to the same subnet.
- Of all management Ethernet ports on an IRF fabric, only the master's management Ethernet port is accessible.

Figure 9 shows a typical BFD MAD scenario that uses an intermediate device. On the intermediate device, assign the ports on the BFD MAD links to the same VLAN.

Figure 10 shows a typical BFD MAD scenario that does not use an intermediate device.

With BFD MAD, the master attempts to establish BFD sessions with other member devices by using its MAD IP address as the source IP address.

- If the IRF fabric is integrated, only the MAD IP address of the master takes effect. The master cannot establish a BFD session with any other member. If you execute the **`display bfd session`** command, the state of the BFD sessions is **Down**.
- When the IRF fabric splits, the IP addresses of the masters in the split IRF fabrics take effect. The masters can establish a BFD session. If you execute the **`display bfd session`** command, the state of the BFD session between the two devices is **Up**.

Figure 9 BFD MAD scenario with an intermediate device

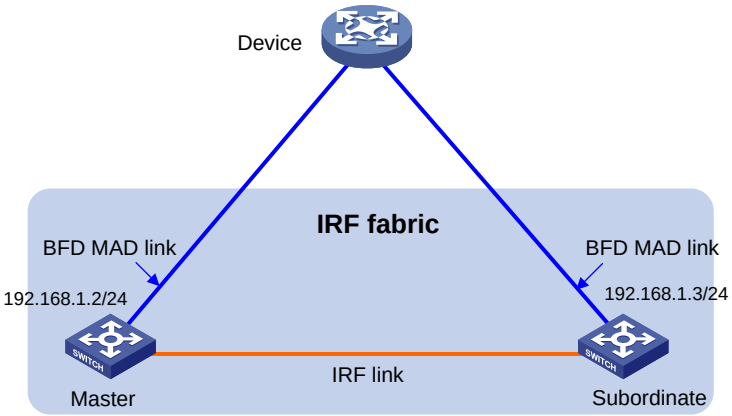
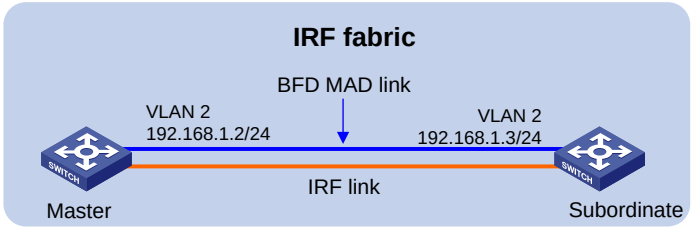


Figure 10 BFD MAD scenario without an intermediate device



ARP MAD

ARP MAD detects multi-active collisions by using extended ARP packets that convey the IRF domain ID and the active ID.

You can use common or management Ethernet ports for ARP MAD.

If management Ethernet ports are used, ARP MAD must work with an intermediate device. Make sure the following requirements are met:

- Connect a management Ethernet port on each member device to the intermediate device.
- On the intermediate device, you must assign the ports used for ARP MAD to the same VLAN.

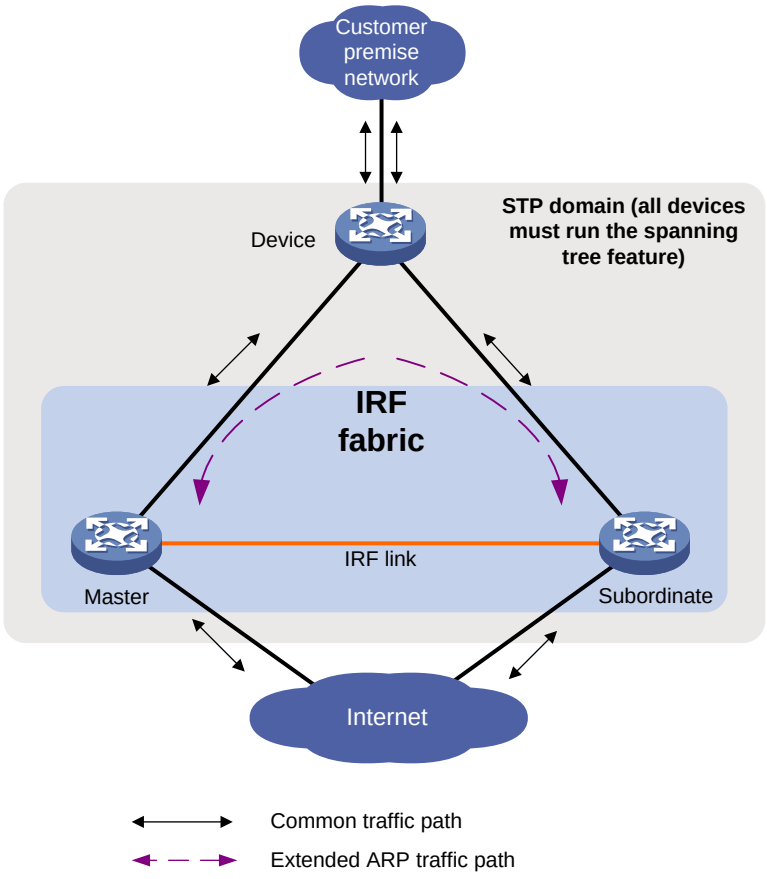
If common Ethernet ports are used, ARP MAD can work with or without an intermediate device. Make sure the following requirements are met:

- If an intermediate device is used, connect each IRF member device to the intermediate device, as shown in Figure 11. Run the spanning tree feature between the IRF fabric and the intermediate device. In this situation, data links can be used.
- If no intermediate device is used, connect each IRF member device to all other member devices. In this situation, IRF links cannot be used for ARP MAD.

Each IRF member compares the domain ID and the active ID (the member ID of the master) in incoming extended ARP packets with its domain ID and active ID.

- If the domain IDs are different, the extended ARP packet is from a different IRF fabric. The device does not continue to process the packet with the MAD mechanism.
- If the domain IDs are the same, the device compares the active IDs.
  - If the active IDs are different, the IRF fabric has split.
  - If the active IDs are the same, the IRF fabric is integrated.

Figure 11 ARP MAD scenario (common Ethernet ports)



ND MAD

ND MAD detects multi-active collisions by using NS packets to transmit the IRF domain ID and the active ID.

You can use common or management Ethernet ports for ND MAD.

If management Ethernet ports are used, ND MAD must work with an intermediate device. Make sure the following requirements are met:

- Connect a management Ethernet port on each member device to the intermediate device.
- On the intermediate device, you must assign the ports used for ND MAD to the same VLAN.

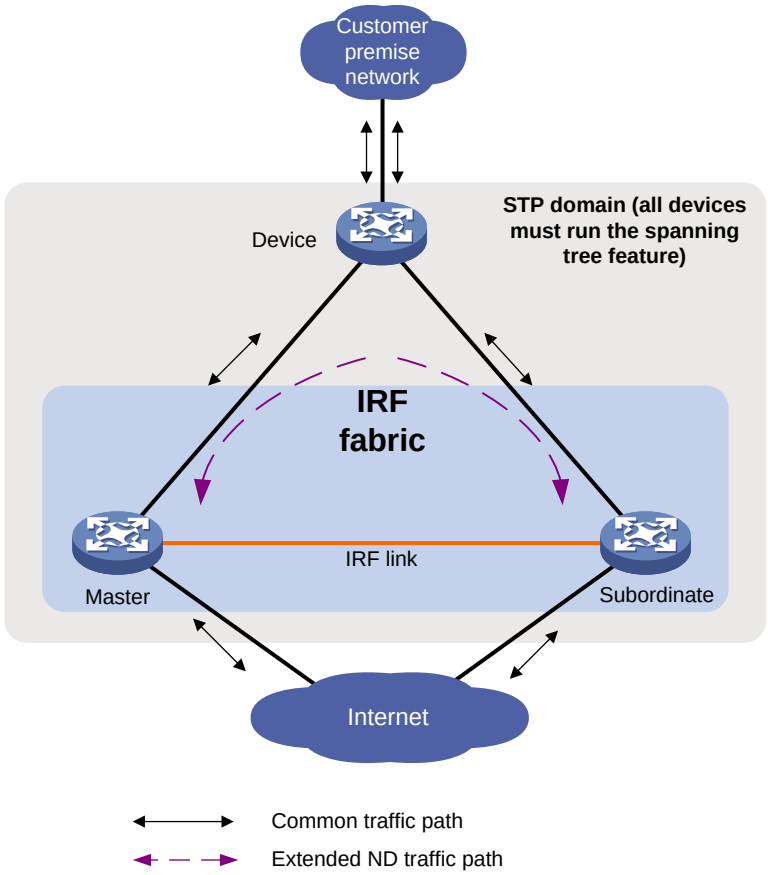
If common Ethernet ports are used, ND MAD can work with or without an intermediate device. Make sure the following requirements are met:

- If an intermediate device is used, connect each IRF member device to the intermediate device, as shown in Figure 12. Run the spanning tree feature between the IRF fabric and the intermediate device. In this situation, data links can be used.
- If no intermediate device is used, connect each IRF member device to all other member devices. In this situation, IRF links cannot be used for ND MAD.

Each IRF member device compares the domain ID and the active ID (the member ID of the master) in incoming NS packets with its domain ID and active ID.

- If the domain IDs are different, the NS packet is from a different IRF fabric. The device does not continue to process the packet with the MAD mechanism.
- If the domain IDs are the same, the device compares the active IDs.
  - If the active IDs are different, the IRF fabric has split.
  - If the active IDs are the same, the IRF fabric is integrated.

Figure 12 ND MAD scenario (common Ethernet ports)



Restrictions and guidelines: IRF configuration

Hardware compatibility with IRF

A switch from the following switch series can form an IRF fabric only with switches in the same series:

- S5560X-EI.
- S5500V2-EI.

An MS4520V2-30F switch can form an IRF fabric only with switches of the same model.

Software requirements for IRF

All IRF member devices must run the same software image version. Make sure the software auto-update feature is enabled on all member devices.

Candidate IRF physical interfaces

Use the following ports on the front panel or on the interface module of the rear panel for IRF links:

- 5G/2.5G/1GBASE-T autosensing Ethernet ports.
- 10G/1GBASE-T autosensing Ethernet ports.
- 10G/5G/2.5G/1GBASE-T autosensing Ethernet ports.
- SFP+ ports.
- SFP28 ports.
- QSFP+ ports.

Make sure these ports operate at their highest rate when they act as IRF physical interfaces.

You cannot use the four SFP+ breakout interfaces of a QSFP+ port as IRF physical interfaces.

Transceiver modules and cables selection for IRF

When you select transceiver modules and cables, follow these restrictions and guidelines:

- Use twisted-pair cables to connect 5G/2.5G/1GBASE-T, 10G/1GBASE-T, or 10G/5G/2.5G/1GBASE-T Ethernet ports. Twisted-pair cables are suitable for short-distance connection. The category and connection distance of applicable cables vary by port rate. For more information, see the installation guide for the device.
- To connect SFP+ ports in a long distance, use SFP+ transceiver modules and fibers. To connect SFP+ ports in a short distance, use SFP+ DAC cables.
- To connect SFP28 ports in a long distance, use SFP28 transceiver modules and fibers. To connect SFP28 ports in a short distance, use SFP28 DAC cables.
- To connect QSFP+ ports in a long distance, use QSFP+ transceiver modules and fibers. To connect QSFP+ ports in a short distance, use QSFP+ DAC cables.
- The transceiver modules at the two ends of an IRF link must be the same type.

For more information about the transceiver modules and cables, see the switch installation guide and *H3C Transceiver Modules User Guide*.

NOTE:

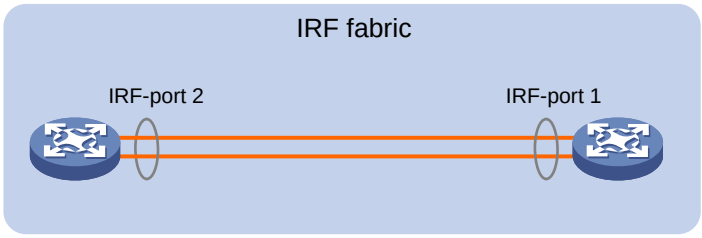
The transceiver modules and cables available for the switch are subject to change over time. For the most up-to-date list of transceiver modules and cables, contact your H3C sales representative.

IRF port connection

When you connect two neighboring IRF members, follow these restrictions and guidelines:

- You must connect the physical interfaces of IRF-port 1 on one member to the physical interfaces of IRF-port 2 on the other.
- For high availability, bind multiple physical interfaces to an IRF port. You can bind a maximum of four physical interfaces to an IRF port.

Figure 13 Connecting IRF physical interfaces



IRF physical interface configuration restrictions and guidelines

Command configuration restrictions

On a physical interface bound to an IRF port, you can execute only the following commands:

- Basic interface commands, including **shutdown** and **description**. For more information about these commands, see Ethernet interface commands in *Layer 2—LAN Switching Command Reference*.
- The **flow-interval** command, which sets the statistics polling interval on an interface. For more information about this command, see Ethernet interface commands in *Layer 2—LAN Switching Command Reference*.
- The **port link-flap protect enable** command, which enables link flapping protection on an interface. To prevent IRF link flapping from affecting system performance, link flapping protection acts differently on IRF physical interfaces than on common network interfaces, as follows:
  - Link flapping protection is enabled by default on IRF physical interfaces. This feature takes effect on an IRF physical interface as long as it is enabled on that interface, regardless of whether link flapping protection has been enabled globally.
  - If the number of link flappings on an IRF physical interface crosses the link flapping threshold during a flapping detection interval, the system displays event messages. However, the system does not shut down that IRF physical interface as it would do with a common network interface.

  For more information about this command, see Ethernet interface commands in *Layer 2—LAN Switching Command Reference*.
- MAC address table configuration commands, including the **mac-address static source-check enable** command. In a VXLAN or EVPN network, to ensure successful forwarding of Layer 3 traffic across member devices, use the **undo mac-address static**

source-check enable command on each IRF physical interface. For information about this command, see *Layer 2—LAN Switching Command Reference*.

- LLDP commands, including:
  - **lldp admin-status**.
  - **lldp check-change-interval**.
  - **lldp enable**.
  - **lldp encapsulation snap**.
  - **lldp notification remote-change enable**.
  - **lldp tlv-enable**.

  For more information about these commands, see *Layer 2—LAN Switching Command Reference*.
- The **mirroring-group reflector-port** command, which specifies the physical interface as a reflector port for remote mirroring. For more information about this command, see port mirroring in *Network Management and Monitoring Command Reference*.

IMPORTANT:

Do not execute the **mirroring-group reflector-port** command on an IRF physical interface if that interface is the only member interface of an IRF port. Doing so will split the IRF fabric, because this command also removes the binding of the physical interface and IRF port.

Suppressing SNMP notifications of packet drops on IRF physical interfaces

Before an IRF member device forwards a packet, it examines its forwarding path in the IRF fabric for a loop. If a loop exists, the device discards the packet on the source interface of the looped path. This loop elimination mechanism will drop a large number of broadcast packets on the IRF physical interfaces.

To suppress SNMP notifications of packet drops that do not require attention, do not monitor packet forwarding on the IRF physical interfaces.

Feature compatibility and configuration restrictions with IRF

System operating mode

To form an IRF fabric, all member devices must work in the same system operating mode. To set the system operating mode, use the **switch-mode** command. For more information about the system operating mode, see device management in *Fundamentals Configuration Guide*.

Routing settings

To form an IRF fabric, all member devices must use the same settings for the following routing features:

- Maximum number of ECMP routes (set by using the **max-ecmp-num** command).
- ECMP mode (set by using the **ecmp mode** command).

For more information about the routing features, see basic IP routing configuration in *Layer 3—IP Routing Configuration Guide*.

Licensing requirements for IRF

For a license-based feature to run correctly on an IRF fabric, make sure the licenses installed for the feature on all member devices are the same. For more information about feature licensing, see *Fundamentals Configuration Guide*.

Configuration rollback restrictions

The configuration rollback feature cannot roll back the following IRF settings:

- Member device description (set by using the **`irf member description`** command).
- Member device priority (set by using the **`irf member priority`** command).
- IRF physical interface and IRF port bindings (set by using the **`port group interface`** command).

For more information about the configuration rollback feature, see configuration file management in *Fundamentals Configuration Guide*.

IRF tasks at a glance

To configure IRF, perform the following tasks:

1. Setting up an IRF fabric
2. Configuring MAD

   Configure a minimum of one MAD mechanism on an IRF fabric. For the MAD compatibility, see "MAD mechanism compatibility."

   - Configuring LACP MAD
   - Configuring BFD MAD
   - Configuring ARP MAD
   - Configuring ND MAD
   - Excluding interfaces from the shutdown action upon detection of multi-active collision

     This feature excludes an interface from the shutdown action for management or other special purposes when an IRF fabric transits to the Recovery state.
   - Recovering an IRF fabric
3. (Optional.) Optimizing IRF settings for an IRF fabric
   - Configuring a member device description
   - Configuring IRF bridge MAC address settings
   - Enabling software auto-update for software image synchronization

     This feature automatically synchronizes the current software images of the master to devices that are attempting to join the IRF fabric.
   - Setting the IRF link down report delay
   - Removing an expansion interface card that has IRF physical interfaces
   - Replacing an expansion interface card that has IRF physical interfaces

Planning the IRF fabric setup

Consider the following items when you plan an IRF fabric:

- Hardware compatibility and restrictions.
- IRF fabric size.
- Master device.
- Member ID and priority assignment scheme.
- Fabric topology and cabling scheme.
- IRF physical interfaces.

Setting up an IRF fabric

IRF setup tasks at a glance

To set up an IRF fabric, perform the following tasks:

4. Configure member IDs, priorities, and IRF physical interfaces separately.
   a. Assigning a member ID to each IRF member device
   b. (Optional.) Specifying a priority for each member device
   c. Binding physical interfaces to IRF ports

   Skip these tasks if you configure member IDs, priorities, domain ID, and IRF physical interfaces in bulk.
5. Bulk-configuring basic IRF settings for a member device

   Skip this task if you configure member IDs, priorities, domain ID, and IRF physical interfaces separately.
6. Connecting IRF physical interfaces
7. Accessing the IRF fabric

Assigning a member ID to each IRF member device

Restrictions and guidelines

To create an IRF fabric, you must assign a unique IRF member ID to each member device.

The new member ID of a device takes effect at a reboot. After the device reboots, the settings on all member ID-related physical resources (including common physical network interfaces) are removed, regardless of whether you have saved the configuration.

In an IRF fabric, changing IRF member IDs might cause undesirable configuration changes and data loss. Before you do that, back up the configuration, and make sure you fully understand the impact on your network.

Procedure

1. Enter system view.

   system-view
2. Assign a member ID to a member device.

   irf member *member-id* **renumber** *new-member-id*

   The default IRF member ID is 1.
3. (Optional.) Save the configuration.

   save

   If you have bound physical interfaces to IRF ports or assigned member priority, you must perform this step for these settings to take effect after the reboot.
4. Return to user view.

   quit
5. Reboot the device.

   reboot [**slot** *slot-number*] [**force**]

Specifying a priority for each member device

About specifying an IRF member priority

IRF member priority represents the possibility for a device to be elected the master in an IRF fabric. A larger priority value indicates a higher priority.

A change to member priority affects the election result at the next master election, but it does not cause an immediate master re-election.

Procedure

1. Enter system view.

   system-view
2. Specify a priority for the device.

   irf member *member-id* **priority** *priority*

   The default IRF member priority is 1.

Binding physical interfaces to IRF ports

Restrictions and guidelines

Select qualified physical interfaces as IRF physical interfaces as described in "Candidate IRF physical interfaces."

After binding physical interfaces to IRF ports for the first time, you must use the **irf-port-configuration active** command to activate the settings on the IRF ports.

The system activates the IRF port settings automatically only in the following situations:

- The configuration file that the device starts with contains IRF port bindings.
- You are adding physical interfaces to an IRF port (in UP state) after an IRF fabric is formed.

Procedure

1. Enter system view.

   system-view
2. Enter interface view or interface range view.
   - Enter interface view.

     interface *interface-type interface-number*
   - Enter interface range view. Choose one of the following commands:

     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>

     interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]

   To shut down a range of IRF physical interfaces, enter interface range view.

   To shut down one IRF physical interface, enter its interface view.
3. Shut down the physical interfaces.

   shutdown

   By default, a physical interface is up.
4. Return to system view.

   quit
5. Enter IRF port view.

   irf-port *member-id/irf-port-number*

6. Bind each physical interface to the IRF port.

   port group interface *interface-type interface-number*

   By default, no physical interfaces are bound to an IRF port.

   Repeat this step to assign multiple physical interfaces to the IRF port.

7. Return to system view.

   quit

8. Enter interface view or interface range view.
   - Enter interface view.

     interface *interface-type interface-number*
   - Enter interface range view. Choose one of the following commands:

     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>

     interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]

9. Bring up the physical interfaces.

   undo shutdown

10. Return to system view.

    quit

11. Save the configuration.

    save

    Activating IRF port configurations causes IRF merge and reboot. To avoid data loss, save the running configuration to the startup configuration file before you perform the operation.

12. Activate the IRF port settings.

    irf-port-configuration active

Bulk-configuring basic IRF settings for a member device

About easy IRF

Use the easy IRF feature to bulk-configure basic IRF settings for a member device, including the member ID, domain ID, priority, and IRF port bindings.

The easy IRF feature provides the following configuration methods:

- **Interactive method**—Enter the **easy-irf** command without parameters. The system will guide you to set the parameters step by step.
- **Non-interactive method**—Enter the **easy-irf** command with parameters.

As a best practice, use the interactive method if you are new to IRF.

Restrictions and guidelines

The member device reboots immediately after you specify a new member ID for it. Make sure you are aware of the impact on the network.

If you execute the **easy-irf** command multiple times, the following settings take effect:

- The most recent settings for the member ID, domain ID, and priority.
- IRF port bindings added through repeated executions of the command. To remove an IRF physical interface from an IRF port, you must use the **undo port group interface** command in IRF port view.

If you specify IRF physical interfaces by using the interactive method, you must also follow these restrictions and guidelines:

- Do not enter spaces between the interface type and interface number.
- Use a comma (,) to separate two physical interfaces. No spaces are allowed between interfaces.

Procedure

1. Enter system view.

   system-view

2. Bulk-configure basic IRF settings for the device.

   easy-irf [**member** *member-id* [**renumber** *new-member-id*] **domain** *domain-id* [**priority** *priority*] [**irf-port1** *interface-list1*] [**irf-port2** *interface-list2*]]

   Make sure the new member ID is unique in the IRF fabric to which the device will be added.

Connecting IRF physical interfaces

Follow the restrictions in "IRF port connection" to connect IRF physical interfaces as well as based on the topology and cabling scheme. The devices perform master election. The member devices that fail the master election automatically reboot to form an IRF fabric with the master device.

Accessing the IRF fabric

The IRF fabric appears as one device after it is formed. You configure and manage all IRF members at the CLI of the master. All settings you have made are automatically propagated to the IRF members.

The following methods are available for accessing an IRF fabric:

- **Local login**—Log in through the console port of any member device.
- **Remote login**—Log in at a Layer 3 interface on any member device by using methods including Telnet and SNMP.

When you log in to an IRF fabric, you are placed at the CLI of the master, regardless of at which member device you are logged in.

For more information, see login configuration in *Fundamentals Configuration Guide*.

Configuring MAD

Restrictions and guidelines for MAD configuration

MAD mechanism compatibility

As a best practice, configure a minimum of one MAD mechanism on an IRF fabric for prompt IRF split detection. Because MAD mechanisms use different collision handling processes, follow these restrictions and guidelines when you configure multiple MAD mechanisms on an IRF fabric:

- Do not configure LACP MAD together with ARP MAD or ND MAD.
- Do not configure BFD MAD together with ARP MAD or ND MAD.

Assigning IRF domain IDs

An IRF fabric has only one IRF domain ID. You can change the IRF domain ID by using the following commands: **irf domain**, **mad enable**, **mad arp enable**, or **mad nd enable**. The IRF domain IDs configured by using these commands overwrite each other.

If LACP MAD, ARP MAD, or ND MAD runs between two IRF fabrics, assign each fabric a unique IRF domain ID. (For BFD MAD, this task is optional.)

Actions on interfaces shut down by MAD

To prevent a multi-active collision from causing network issues, avoid using the **undo shutdown** command to bring up the interfaces shut down by a MAD mechanism on a Recovery-state IRF fabric.

Configuring LACP MAD

1. Enter system view.
   system-view
2. Assign a domain ID to the IRF fabric.
   irf domain *domain-id*
   The default IRF domain ID is 0.
3. Create an aggregate interface and enter aggregate interface view.
   - Enter Layer 2 aggregate interface view.
     interface bridge-aggregation *interface-number*
   - Enter Layer 3 aggregate interface view.
     interface route-aggregation *interface-number*

   Perform this step also on the intermediate device.
4. Configure the aggregation group to operate in dynamic aggregation mode.
   link-aggregation mode dynamic
   By default, an aggregation group operates in static aggregation mode.
   LACP MAD takes effect only on dynamic aggregate interfaces.
   Perform this step also on the intermediate device.
5. Enable LACP MAD.
   mad enable
   By default, LACP MAD is disabled.
6. Return to system view.
   quit
7. Enter Ethernet interface view or interface range view.
   - Enter Ethernet interface view.
     interface *interface-type interface-number*
   - Enter interface range view. Choose one of the following commands:
     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>
     interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]

   To assign a range of ports to the aggregation group, enter interface range view.
   To assign one port to the aggregation group, enter Ethernet interface view.
8. Assign the Ethernet port or the range of Ethernet ports to the specified aggregation group.
   port link-aggregation group *group-id*
   Multichassis link aggregation is allowed.
   Perform this step also on the intermediate device.

Configuring BFD MAD

Restrictions and guidelines for configuring BFD MAD

As a best practice, use the following procedure to set up BFD MAD:

1. Choose a BFD MAD link scheme as described in "BFD MAD."
2. Configure BFD MAD.
3. Connect the BFD MAD links.

When you configure BFD MAD on a VLAN interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines

BFD MAD VLAN	• Do not enable BFD MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On the IRF fabric and the intermediate device, create a VLAN for BFD MAD.
	  ○ On the IRF fabric and the intermediate device, assign the ports of BFD MAD links to the BFD MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the BFD MAD VLAN.
	• Make sure the IRF fabrics on the network use different BFD MAD VLANs.
	• Make sure the BFD MAD VLAN contains only ports on the BFD MAD links. Exclude a port from the BFD MAD VLAN if that port is not on a BFD MAD link. If you have assigned that port to all VLANs by using the **`port trunk permit vlan all`** command, use the **`undo port trunk permit`** command to exclude that port from the BFD MAD VLAN.

BFD MAD VLAN and feature compatibility	Do not use the BFD MAD VLAN and its member ports for any purpose other than configuring BFD MAD. • Use only the **`mad bfd enable`** and **`mad ip address`** commands on the BFD MAD-enabled VLAN interface. If you configure other features, both BFD MAD and other features on the interface might run incorrectly. • Disable the spanning tree feature on any Layer 2 Ethernet ports in the BFD MAD VLAN. The MAD feature is mutually exclusive with the spanning tree feature.
MAD IP address	• To avoid network issues, only use the **`mad ip address`** command to configure IP addresses on the BFD MAD-enabled VLAN interface. Do not configure an IP address by using the **`ip address`** command or configure a VRRP virtual address on the BFD MAD-enabled VLAN interface. • Make sure all the MAD IP addresses are on the same subnet.

When you configure BFD MAD on a Layer 3 aggregate interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines
BFD MAD-enabled Layer 3 aggregate interface	• Make sure the Layer 3 aggregate interface operates in static aggregation mode. • Make sure the member ports in the aggregation group do not exceed the maximum number of Selected ports allowed for an aggregation group. If the number of member ports exceeds the maximum number of Selected ports, some member ports cannot become Selected. BFD MAD will be unable to work correctly and its state will change to Faulty.
BFD MAD VLAN	• On the intermediate device (if any), assign the ports on the BFD MAD

Category	Restrictions and guidelines
	links to the same VLAN. Do not assign the ports to an aggregate interface. If the ports are hybrid ports, make sure these ports are untagged members of their PVIDs. • If the intermediate device acts as a BFD MAD intermediate device for multiple IRF fabrics, assign different BFD MAD VLANs to the IRF fabrics. • Do not use the BFD MAD VLAN on the intermediate device for any purposes other than BFD MAD. • Make sure the BFD MAD VLAN on the intermediate device contains only ports on the BFD MAD links. Exclude a port from the BFD MAD VLAN if that port is not on a BFD MAD link. If you have assigned that port to all VLANs by using the **port trunk permit vlan all** command, use the **undo port trunk permit** command to exclude that port from the BFD MAD VLAN.
BFD MAD-enabled Layer 3 aggregate interface and feature compatibility	Use only the **mad bfd enable** and **mad ip address** commands on the BFD MAD-enabled interface. If you configure other features, both BFD MAD and other features on the interface might run incorrectly.
MAD IP address	• To avoid network issues, only use the **mad ip address** command to configure IP addresses on the BFD MAD-enabled interface. Do not configure an IP address by using the **ip address** command or configure a VRRP virtual address on the BFD MAD-enabled interface. • Make sure all the MAD IP addresses are on the same subnet.

When you configure BFD MAD on a management Ethernet port, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for BFD MAD	Connect a management Ethernet port on each IRF member device to the common Ethernet ports on the intermediate device.
BFD MAD VLAN	• On the intermediate device, create a VLAN for BFD MAD, and assign the ports used for BFD MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN. • Make sure the IRF fabrics on the network use different BFD MAD VLANs. • Make sure the BFD MAD VLAN on the intermediate device contains only ports on the BFD MAD links.
MAD IP address	• Use the **mad ip address** command instead of the **ip address** command to configure MAD IP addresses on the BFD MAD-enabled management Ethernet ports. • Make sure all the MAD IP addresses are on the same subnet.

Configuring BFD MAD on a VLAN interface

1. Enter system view.
   system-view
2. (Optional.) Assign a domain ID to the IRF fabric.
   irf domain *domain-id*
   By default, the domain ID of an IRF fabric is 0.
3. Create a VLAN dedicated to BFD MAD.
   vlan *vlan-id*
   By default, only VLAN 1 exists.
   Do not enable BFD MAD on VLAN-interface 1.
   Perform this step also on the intermediate device (if any).

4. Return to system view.
   quit
5. Enter Ethernet interface view or interface range view.
   - Enter Ethernet interface view.
     interface *interface-type interface-number*
   - Enter interface range view. Choose one of the following commands:
     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>
     interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]

   To assign a range of ports to the BFD MAD VLAN, enter interface range view.

   To assign one port to the BFD MAD VLAN, enter Ethernet interface view.
6. Assign the port or the range of ports to the BFD MAD VLAN.
   - Assign the ports to the VLAN as access ports.
     port access vlan *vlan-id*
   - Assign the ports to the VLAN as trunk ports.
     port trunk permit vlan *vlan-id*
   - Assign the ports to the VLAN as hybrid ports.
     port hybrid vlan *vlan-id* { **tagged** | **untagged** }

   The link type of BFD MAD ports can be access, trunk, or hybrid.

   The default link type of a port is access.

   Perform this step also on the intermediate device (if any).
7. Return to system view.
   quit
8. Enter VLAN interface view.
   interface vlan-interface *vlan-interface-id*
9. Enable BFD MAD.
   mad bfd enable

   By default, BFD MAD is disabled.
10. Assign a MAD IP address to a member device on the VLAN interface.
    mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

    By default, no MAD IP addresses are configured on any VLAN interfaces.

    Repeat this step to assign a MAD IP address to each member device on the VLAN interface.

Configuring BFD MAD on a Layer 3 aggregate interface

1. Enter system view.
   system-view
2. (Optional.) Assign a domain ID to the IRF fabric.
   irf domain *domain-id*

   By default, the domain ID of an IRF fabric is 0.
3. Create a Layer 3 aggregate interface for BFD MAD.
   interface route-aggregation *interface-number*
4. Return to system view.
   quit
5. Enter interface view or interface range view.

- Enter Ethernet interface view.

  interface *interface-type interface-number*

- Enter interface range view. Choose one of the following commands:

  interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>

  interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]

To assign a range of ports to the aggregation group for the aggregate interface, enter interface range view.

To assign one port to the aggregation group for the aggregate interface, enter Ethernet interface view.

6. Assign the port or the range of ports to the aggregation group for the aggregate interface.

   port link-aggregation group *number*

7. Return to system view.

   quit

8. Enter Layer 3 aggregate interface view.

   interface route-aggregation *interface-number*

9. Enable BFD MAD.

   mad bfd enable

   By default, BFD MAD is disabled.

10. Assign a MAD IP address to a member device on the Layer 3 aggregate interface.

    mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

    By default, no MAD IP addresses are configured on aggregate interfaces.

    Repeat this step to assign a MAD IP address to each member device on the aggregate interface.

Configuring BFD MAD on a management Ethernet port

1. Enter system view.

   system-view

2. (Optional.) Assign a domain ID to the IRF fabric.

   irf domain *domain-id*

   By default, the domain ID of an IRF fabric is 0.

3. Enter management Ethernet interface view.

   interface m-gigabitethernet *interface-number*

   Of all management Ethernet ports on an IRF fabric, only the master's management Ethernet port is accessible.

4. Enable BFD MAD.

   mad bfd enable

   By default, BFD MAD is disabled.

5. Assign a MAD IP address to each member device.

   mad ip address *ip-address* { *mask* | *mask-length* } **member** *member-id*

   By default, no MAD IP addresses are configured.

Configuring ARP MAD

Restrictions and guidelines for configuring ARP MAD

As a best practice, use the following procedure to set up ARP MAD:

1. Choose an ARP MAD link scheme as described in "ARP MAD."
2. Configure ARP MAD.
3. Connect the ARP MAD links if you are not using existing data links as ARP MAD links.

When you configure ARP MAD on a VLAN interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines

ARP MAD VLAN	• Do not enable ARP MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On the IRF fabric and the intermediate device, create a VLAN for ARP MAD.
	  ○ On the IRF fabric and the intermediate device, assign the ports of ARP MAD links to the ARP MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the ARP MAD VLAN.
	• Do not use the ARP MAD VLAN for any other purposes.

ARP MAD and feature configuration	If an intermediate device is used, make sure the following requirements are met: • Run the spanning tree feature between the IRF fabric and the intermediate device to ensure that there is only one ARP MAD link in forwarding state. For more information about the spanning tree feature and its configuration, see *Layer 2—LAN Switching Configuration Guide*. • Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you configure ARP MAD on a management Ethernet port, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for ARP MAD	Connect a management Ethernet port on each member device to the common Ethernet ports on the intermediate device.
ARP MAD VLAN	On the intermediate device, create a VLAN for ARP MAD, and assign the ports used for ARP MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN.
ARP MAD and feature configuration	• Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

Configuring ARP MAD on a VLAN interface

1. Enter system view.
   `system-view`
2. Assign a domain ID to the IRF fabric.
   `irf domain` *`domain-id`*
   The default IRF domain ID is 0.

3. Configure the IRF bridge MAC address to change as soon as the address owner leaves.

   undo irf mac-address persistent

   By default, the IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves.

4. Create a VLAN dedicated to ARP MAD.

   vlan *vlan-id*

   By default, only VLAN 1 exists.

   Do not configure ARP MAD on VLAN-interface 1.

   Perform this task also on the intermediate device (if any).

5. Return to system view.

   quit

6. Enter Ethernet interface view or interface range view.

   - Enter Ethernet interface view.

     interface *interface-type interface-number*

   - Enter interface range view. Choose one of the following commands:

     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>

     interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]

   To assign a range of ports to the ARP MAD VLAN, enter interface range view.

   To assign one port to the ARP MAD VLAN, enter Ethernet interface view.

7. Assign the port or the range of ports to the ARP MAD VLAN.

   - Assign the ports to the VLAN as access ports.

     port access vlan *vlan-id*

   - Assign the ports to the VLAN as trunk ports.

     port trunk permit vlan *vlan-id*

   - Assign the ports to the VLAN as hybrid ports.

     port hybrid vlan *vlan-id* { **tagged** | **untagged** }

   The link type of ARP MAD ports can be access, trunk, or hybrid.

   The default link type of a port is access.

   Perform this task also on the intermediate device (if any).

8. Return to system view.

   quit

9. Enter VLAN interface view.

   interface vlan-interface *vlan-interface-id*

10. Assign the interface an IP address.

    ip address *ip-address* { *mask* | *mask-length* }

    By default, no IP addresses are assigned to any VLAN interfaces.

11. Enable ARP MAD.

    mad arp enable

    By default, ARP MAD is disabled.

Configuring ARP MAD on a management Ethernet port

1. Enter system view.

   system-view

2. Assign a domain ID to the IRF fabric.

   irf domain *domain-id*

   The default IRF domain ID is 0.

3. Configure the IRF bridge MAC address to change as soon as the address owner leaves.

   undo irf mac-address persistent

   By default, the IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves.

4. Enter management Ethernet interface view.

   interface m-gigabitethernet *interface-number*

   Of all management Ethernet ports on an IRF fabric, only the master's management Ethernet port is accessible.

5. Assign an IP address to the management Ethernet port.

   ip address ip-address { *mask* | *mask-length* }

   By default, no IP addresses are configured.

6. Enable ARP MAD.

   mad arp enable

   By default, ARP MAD is disabled.

Configuring ND MAD

Restrictions and guidelines for configuring ND MAD

As a best practice, use the following procedure to set up ND MAD:

1. Choose an ND MAD link scheme as described in "ND MAD."
2. Configure ND MAD.
3. Connect the ND MAD links if you are not using existing data links as ND MAD links.

When you configure ND MAD on a VLAN interface, follow these restrictions and guidelines:

Category	Restrictions and guidelines

ND MAD VLAN	• Do not enable ND MAD on VLAN-interface 1.
	• If you are using an intermediate device, perform the following tasks:
	  ○ On the IRF fabric and the intermediate device, create a VLAN for ND MAD.
	  ○ On the IRF fabric and the intermediate device, assign the ports of ND MAD links to the ND MAD VLAN.
	  ○ On the IRF fabric, create a VLAN interface for the ND MAD VLAN.
	• Do not use the ND MAD VLAN for any other purposes.

ND MAD and feature configuration	If an intermediate device is used, make sure the following requirements are met: • Run the spanning tree feature between the IRF fabric and the intermediate device to ensure that there is only one ND MAD link in forwarding state. For more information about the spanning tree feature and its configuration, see *Layer 2—LAN Switching Configuration Guide*. • Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

When you configure ND MAD on a management Ethernet port, follow these restrictions and guidelines:

Category	Restrictions and guidelines
Management Ethernet ports for ND MAD	Connect a management Ethernet port on each member device to the common Ethernet ports on the intermediate device.
ND MAD VLAN	On the intermediate device, create a VLAN for ND MAD, and assign the ports used for ND MAD to the VLAN. On the IRF fabric, you do not need to assign the management Ethernet ports to the VLAN.
ND MAD and feature configuration	• Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves. • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection.

Configuring ND MAD on a VLAN interface

1. Enter system view.

   system-view
2. Assign a domain ID to the IRF fabric.

   irf domain *domain-id*

   The default IRF domain ID is 0.
3. Configure the IRF bridge MAC address to change as soon as the address owner leaves.

   undo irf mac-address persistent

   By default, the IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves the fabric.
4. Create a VLAN dedicated to ND MAD.

   vlan *vlan-id*

   By default, only VLAN 1 exists.

   Do not configure ND MAD on VLAN-interface 1.

   Perform this task also on the intermediate device (if any).
5. Return to system view.

   quit
6. Enter Ethernet interface view or interface range view.
   - Enter Ethernet interface view.

     interface *interface-type interface-number*
   - Enter interface range view. Choose one of the following commands:

     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>

     interface range name *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>]

   To assign a range of ports to the ND MAD VLAN, enter interface range view.

   To assign one port to the ND MAD VLAN, enter Ethernet interface view.
7. Assign the port or the range of ports to the ND MAD VLAN.
   - Assign the ports to the VLAN as access ports.

     port access vlan *vlan-id*
   - Assign the ports to the VLAN as trunk ports.

     port trunk permit vlan *vlan-id*
   - Assign the ports to the VLAN as hybrid ports.

     port hybrid vlan *vlan-id* { **tagged** | **untagged** }

The link type of ND MAD ports can be access, trunk, or hybrid.

The default link type of a port is access.

Perform this task also on the intermediate device (if any).

8. Return to system view.

   quit

9. Enter VLAN interface view.

   interface vlan-interface *interface-number*

10. Assign the interface an IPv6 address.

    ipv6 address { *ipv6-address/prefix-length* | *ipv6-address prefix-length* }

    By default, no IPv6 addresses are assigned to a VLAN interface.

11. Enable ND MAD.

    mad nd enable

    By default, ND MAD is disabled.

Configuring ND MAD on a management Ethernet port

1. Enter system view.

   system-view

2. Assign a domain ID to the IRF fabric.

   irf domain *domain-id*

   The default IRF domain ID is 0.

3. Configure the IRF bridge MAC address to change as soon as the address owner leaves.

   undo irf mac-address persistent

   By default, the IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves the fabric.

4. Enter management Ethernet interface view.

   interface m-gigabitethernet *interface-number*

   Of all management Ethernet ports on an IRF fabric, only the master's management Ethernet port is accessible.

5. Assign an IPv6 address to the management Ethernet port.

   ipv6 address { *ipv6-address/pre-length* | *ipv6 address pre-length* }

   By default, no IPv6 addresses are assigned to a management Ethernet port.

6. Enable ND MAD.

   mad nd enable

   By default, ND MAD is disabled.

Excluding interfaces from the shutdown action upon detection of multi-active collision

About excluding interfaces from being shut down

When an IRF fabric transits to the Recovery state, the system automatically excludes the following network interfaces from being shut down:

- IRF physical interfaces.
- Interfaces used for BFD MAD.

- Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.

You can exclude an interface from the shutdown action for management or other special purposes. For example:

- Exclude a port from the shutdown action so you can Telnet to the port for managing the device.
- Exclude a VLAN interface and its Layer 2 ports from the shutdown action so you can log in through the VLAN interface.

Restrictions and guidelines

If the Layer 2 ports of a VLAN interface are distributed on multiple member devices, the exclusion operation might introduce IP collision risks. The VLAN interface might be up on both active and inactive IRF fabrics.

Procedure

1. Enter system view.
   system-view
2. Configure an interface to not shut down when the IRF fabric transits to the Recovery state.
   mad exclude interface *interface-type interface-number*
   By default, all network interfaces on a Recovery-state IRF fabric are shut down, except for the network interfaces automatically excluded by the system.

Recovering an IRF fabric

About recovering an IRF fabric

If the active IRF fabric fails before the IRF link is recovered, perform this task on the inactive IRF fabric to recover the inactive IRF fabric for traffic forwarding. The manual recovery operation brings up all interfaces that were shut down by MAD on the inactive IRF fabric.

Procedure

1. Enter system view.
   system-view
2. Recover the inactive IRF fabric.
   mad restore

Optimizing IRF settings for an IRF fabric

Configuring a member device description

1. Enter system view.
   system-view
2. Configure a description for a member device.
   irf member *member-id* **description** *text*
   By default, no member device description is configured.

Configuring IRF bridge MAC address settings

About IRF bridge MAC address configuration

The bridge MAC address of a system must be unique on a switched LAN. IRF bridge MAC address identifies an IRF fabric by Layer 2 protocols (for example, LACP) on a switched LAN.

By default, an IRF fabric uses the bridge MAC address of the master as the IRF bridge MAC address. After the master leaves, the IRF bridge MAC address persists for a period of time or permanently depending on the IRF bridge MAC persistence setting. When the IRF bridge MAC persistence timer expires, the IRF fabric uses the bridge MAC address of the current master as the IRF bridge MAC address.

In special occasions that require a fixed special IRF bridge MAC address, you can specify that MAC address as the IRF bridge MAC address. For example, when you replace an IRF fabric as a whole, you can configure the new IRF fabric with the IRF bridge MAC address of the existing IRF fabric before the replacement to minimize service interruption.

The IRF bridge MAC persistence setting does not take effect on the manually specified IRF bridge MAC address.

If IRF fabric merge occurs, IRF determines the IRF bridge MAC address of the merged IRF fabric as follows:

1. When IRF fabrics merge, IRF ignores the IRF bridge MAC addresses and checks the bridge MAC address of each member device in the IRF fabrics. IRF merge fails if any two member devices have the same bridge MAC address.
2. After IRF fabrics merge, the merged IRF fabric uses the bridge MAC address of the merging IRF fabric that won the master election as the IRF bridge MAC address.

Restrictions and guidelines for IRF bridge MAC address configuration

CAUTION:
Bridge MAC address change will cause transient traffic disruption.

When you configure IRF bridge MAC persistence, follow these restrictions and guidelines:

- If ARP MAD or ND MAD is used with the spanning tree feature, you must disable IRF bridge MAC persistence by using the **undo irf mac-address persistent** command. In addition, do not specify a MAC address as the IRF bridge MAC address.
- If the IRF fabric has multichassis aggregate links, do not use the **undo irf mac-address persistent** command. Use of this command might cause traffic disruption.

When you specify a MAC address as the IRF bridge MAC address, follow these restrictions and guidelines:

- Do not specify any of the following MAC addresses as the IRF bridge MAC address:
  - Static MAC addresses.
  - Dynamic MAC addresses.
  - Blackhole MAC addresses.
  - Multiport unicast MAC addresses.
- IRF reserves the IRF bridge MAC address and its subsequent higher 103 MAC addresses. These MAC addresses cannot be configured as any types of MAC addresses listed above.

Configuring IRF bridge MAC persistence

1. Enter system view.

   system-view
2. Configure IRF bridge MAC persistence.

- Retain the bridge MAC address permanently even if the address owner has left the fabric.

  irf mac-address persistent always
- Retain the bridge MAC address for 6 minutes after the address owner leaves the fabric.

  irf mac-address persistent timer
- Change the bridge MAC address as soon as the address owner leaves the fabric.

  undo irf mac-address persistent

By default, the IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves the fabric.

The **irf mac-address persistent timer** command avoids unnecessary bridge MAC address changes caused by device reboot, transient link failure, or purposeful link disconnection.

Specifying a MAC address as the IRF bridge MAC address

1. Enter system view.

   system-view
2. Specify a MAC address as the IRF bridge MAC address.

   irf mac-address *mac-address*

   By default, an IRF fabric uses the bridge MAC address of the master as the IRF bridge MAC address.

   If an IRF fabric splits after you configure the IRF bridge MAC address, both the split IRF fabrics use the configured bridge MAC address as the IRF bridge MAC address.

Enabling software auto-update for software image synchronization

About IRF software auto-update

The software auto-update feature automatically synchronizes the current software images of the master to devices that are attempting to join the IRF fabric.

To join an IRF fabric, a device must use the same software images as the master in the fabric.

When you add a device to the IRF fabric, software auto-update compares the startup software images of the device with the current software images of the IRF master. If the two sets of images are different, the device automatically performs the following operations:

1. Downloads the current software images of the master.
2. Sets the downloaded images as its main startup software images.
3. Reboots with the new software images to rejoin the IRF fabric.

You must manually update the new device with the software images running on the IRF fabric if software auto-update is disabled.

Restrictions and guidelines

To ensure a successful software auto-update in a multi-user environment, prevent anyone from rebooting member devices during the auto-update process. To inform administrators of the auto-update status, configure the information center to output the status messages to configuration terminals (see *Network Management and Monitoring Configuration Guide*).

Make sure the device you are adding to the IRF fabric has sufficient storage space for the new software images.

If sufficient storage space is not available, the device automatically deletes the current software images. If the reclaimed space is still insufficient, the device cannot complete the auto-update. You must reboot the device, and then access the Boot menu to delete files.

Procedure

1. Enter system view.
   system-view
2. Enable software auto-update.
   irf auto-update enable
   By default, software auto-update is enabled.

Setting the IRF link down report delay

About IRF link down report delay

To prevent frequent IRF splits and merges during link flapping, configure the IRF ports to delay reporting link down events.

An IRF port does not report a link down event to the IRF fabric immediately after its link changes from up to down. If the IRF link state is still down when the delay is reached, the port reports the change to the IRF fabric.

IRF ports do not delay link up events. They report the link up event immediately after the IRF link comes up.

Restrictions and guidelines

Make sure the IRF link down report delay is shorter than the heartbeat or hello timeout settings of upper-layer protocols (for example, CFD and OSPF). If the report delay is longer than the timeout setting of a protocol, unnecessary recalculations might occur.

Set the delay to 0 seconds in the following situations:

- The IRF fabric requires a fast master/subordinate or IRF link switchover.
- The RRPP, BFD, or GR feature is used.
- You want to shut down an IRF physical interface or reboot an IRF member device. (After you complete the operation, reconfigure the delay depending on the network condition.)

Procedure

1. Enter system view.
   system-view
2. Set the IRF link down report delay.
   irf link-delay *interval*
   The default IRF link down report delay is 4 seconds.

Removing an expansion interface card that has IRF physical interfaces

To remove an expansion interface card that provides IRF physical interfaces:

1. Perform one of the following tasks to eliminate temporary packet loss:
   - Remove cables from the IRF physical interfaces on the card.
   - Shut down the IRF physical interfaces on the card by using the **shutdown** command.
2. Remove the card.

Replacing an expansion interface card that has IRF physical interfaces

Replacing the old card with a different model replacement card

1. Shut down the IRF physical interfaces on the old card by using the **shutdown** command.
2. Remove the IRF port bindings that contain the physical interfaces.
3. Remove the old card, and then install the replacement card.
4. Verify that the replacement card has been correctly installed by using the **display device** command.
5. Reconfigure the IRF port bindings, as described in "Binding physical interfaces to IRF ports."
6. Activate the IRF port settings by using the **irf-port-configuration active** command.

   You can skip this step if the IRF port is in UP state when you add bindings.

Replacing the old card with the same model replacement card

1. Shut down the IRF physical interfaces on the old card by using the **shutdown** command.
2. Remove the old card, and then install the replacement card.
3. Verify that the replacement card has been correctly installed by using the **display device** command.

   Bring up the physical interfaces by using the **undo shutdown** command after the interface card completes startup.

Display and maintenance commands for IRF

Execute **display** commands in any view.

Task	Command
Display information about all IRF members.	**display irf**
Display the IRF fabric topology.	**display irf topology**
Display IRF link information.	**display irf link**
Display IRF configuration.	**display irf configuration**
Display MAD configuration.	**display mad** [**verbose**]

IRF configuration examples

The IRF configuration examples show how to set up IRF fabrics that use different MAD mechanisms.

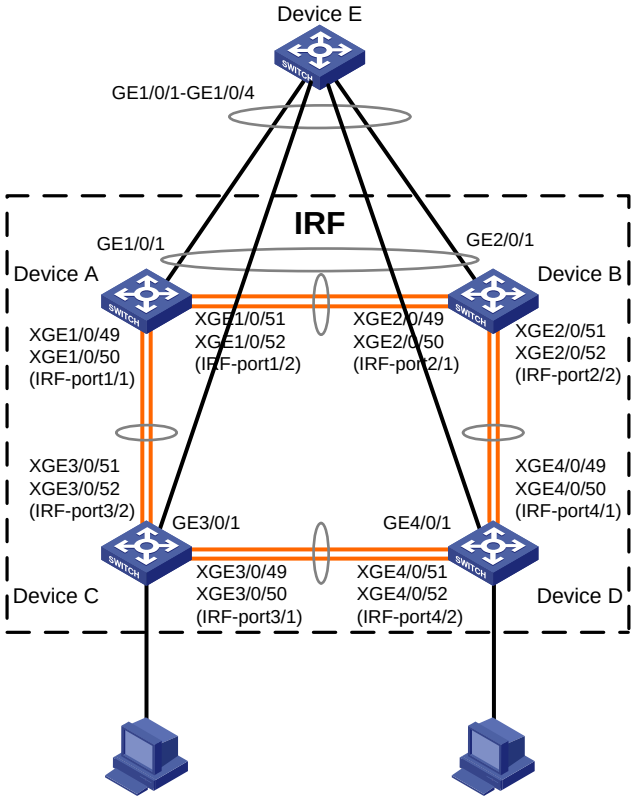
Example: Configuring an LACP MAD-enabled IRF fabric

Network configuration

As shown in Figure 14, set up a four-chassis IRF fabric at the access layer of the enterprise network.

Configure LACP MAD on the multichassis aggregation to Device E, which supports extended LACP.

Figure 14 Network diagram



Procedure

1. Configure Device A:

   # Shut down the physical interfaces used for IRF links. In this example, the physical interfaces are shut down in batch. For more information, see *Layer 2—LAN Switching Configuration Guide*.

   ```
   <Sysname> system-view
   [Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
   [Sysname-if-range] shutdown
   [Sysname-if-range] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/49 and Ten-GigabitEthernet 1/0/50 to IRF-port 1/1.

   ```
   [Sysname] irf-port 1/1
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/49
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/50
   [Sysname-irf-port1/1] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/51 and Ten-GigabitEthernet 1/0/52 to IRF-port 1/2.

   ```
   [Sysname] irf-port 1/2
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/51
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/52
   [Sysname-irf-port1/2] quit
   ```

   # Bring up the physical interfaces and save the configuration.

   ```
   [Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
   [Sysname-if-range] undo shutdown
   [Sysname-if-range] quit
   [Sysname] save
   ```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

2. Configure Device B:

Change the member ID of Device B to 2 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device B to Device A as shown in Figure 14, and log in to Device B. (Details not shown.)

Shut down the physical interfaces for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 2/0/49 and Ten-GigabitEthernet 2/0/50 to IRF-port 2/1.

```
[Sysname] irf-port 2/1
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/49
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/50
[Sysname-irf-port2/1] quit
```

Bind Ten-GigabitEthernet 2/0/51 and Ten-GigabitEthernet 2/0/52 to IRF-port 2/2.

```
[Sysname] irf-port 2/2
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/51
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/52
[Sysname-irf-port2/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

The two devices perform master election, and the one that has lost the election reboots to form an IRF fabric with the master.

3. Configure Device C:

Change the member ID of Device C to 3 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device C to Device A as shown in Figure 14, and log in to Device C. (Details not shown.)

Shut down the physical interfaces for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] shutdown
```

```
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 3/0/49 and Ten-GigabitEthernet 3/0/50 to IRF-port 3/1.

```
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/49
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/50
[Sysname-irf-port3/1] quit
```

Bind Ten-GigabitEthernet 3/0/51 and Ten-GigabitEthernet 3/0/52 to IRF-port 3/2.

```
[Sysname] irf-port 3/2
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/51
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/52
[Sysname-irf-port3/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device C reboots to join the IRF fabric.

4. Configure Device D:

Change the member ID of Device D to 4 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 4
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device D to Device B and Device C as shown in Figure 14, and log in to Device D. (Details not shown.)

Shut down the physical interfaces.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 4/0/49 and Ten-GigabitEthernet 4/0/50 to IRF-port 4/1.

```
[Sysname] irf-port 4/1
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/49
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/50
[Sysname-irf-port4/1] quit
```

Bind Ten-GigabitEthernet 4/0/51 and Ten-GigabitEthernet 4/0/52 to IRF-port 4/2.

```
[Sysname] irf-port 4/2
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/51
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/52
[Sysname-irf-port4/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
```

```
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

5. Configure LACP MAD on the IRF fabric:

Set the domain ID of the IRF fabric to 1.

```
<Sysname> system-view
[Sysname] irf domain 1
```

Create a dynamic aggregate interface and enable LACP MAD.

```
[Sysname] interface bridge-aggregation 2
[Sysname-Bridge-Aggregation2] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation2] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain ID is: 1]:
The assigned domain ID is: 1
[Sysname-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 3/0/1, and GigabitEthernet 4/0/1 to the aggregate interface.

```
[Sysname] interface range gigabitethernet 1/0/1  gigabitethernet 2/0/1
gigabitethernet 3/0/1 gigabitethernet 4/0/1
[Sysname-if-range] port link-aggregation group 2
[Sysname-if-range] quit
```

6. Configure Device E as the intermediate device:

CAUTION:

If the intermediate device is also an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

Create a dynamic aggregate interface.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 2
[Sysname-Bridge-Aggregation2] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to the aggregate interface.

```
[Sysname] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[Sysname-if-range] port link-aggregation group 2
[Sysname-if-range] quit
```

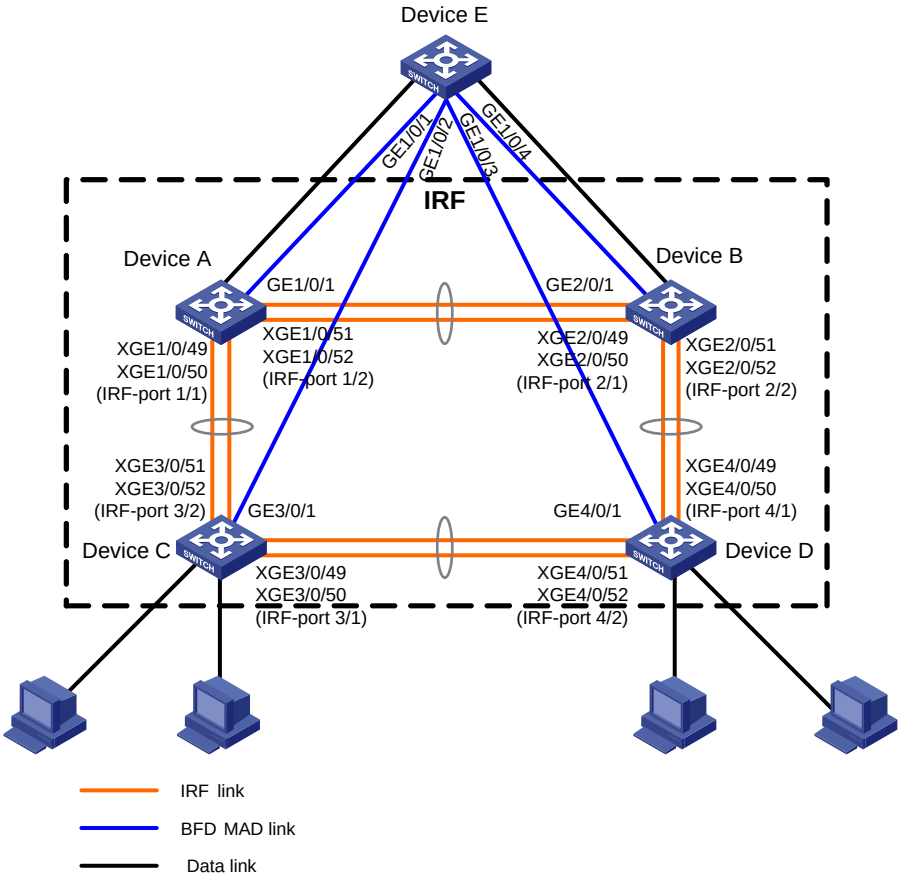
Example: Configuring a BFD MAD-enabled IRF fabric

Network configuration

As shown in Figure 15, set up a four-chassis IRF fabric at the distribution layer of the enterprise network.

- Configure BFD MAD on the IRF fabric and set up BFD MAD links between each member device and the intermediate device.
- Disable the spanning tree feature on the ports used for BFD MAD, because the two features conflict with each other.

Figure 15 Network diagram



Procedure

1. Configure Device A:

   # Shut down the physical interfaces used for IRF links.

   ```
   <Sysname> system-view
   [Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
   [Sysname-if-range] shutdown
   [Sysname-if-range] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/49 and Ten-GigabitEthernet 1/0/50 to IRF-port 1/1.

   ```
   [Sysname] irf-port 1/1
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/49
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/50
   [Sysname-irf-port1/1] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/51 and Ten-GigabitEthernet 1/0/52 to IRF-port 1/2.

   ```
   [Sysname] irf-port 1/2
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/51
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/52
   [Sysname-irf-port1/2] quit
   ```

   # Bring up the physical interfaces and save the configuration.

   ```
   [Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
   [Sysname-if-range] undo shutdown
   [Sysname-if-range] quit
   ```

```
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

2. Configure Device B:

Change the member ID of Device B to 2 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device B to Device A as shown in Figure 15, and log in to Device B. (Details not shown.)

Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 2/0/49 and Ten-GigabitEthernet 2/0/50 to IRF-port 2/1.

```
[Sysname] irf-port 2/1
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/49
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/50
[Sysname-irf-port2/1] quit
```

Bind Ten-GigabitEthernet 2/0/51 and Ten-GigabitEthernet 2/0/52 to IRF-port 2/2.

```
[Sysname] irf-port 2/2
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/51
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/52
[Sysname-irf-port2/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

The two devices perform master election, and the one that has lost the election reboots to form an IRF fabric with the master.

3. Configure Device C:

Change the member ID of Device C to 3 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device C to Device A as shown in Figure 15, and log in to Device C. (Details not shown.)

Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
```

```
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 3/0/49 and Ten-GigabitEthernet 3/0/50 to IRF-port 3/1.

```
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/49
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/50
[Sysname-irf-port3/1] quit
```

Bind Ten-GigabitEthernet 3/0/51 and Ten-GigabitEthernet 3/0/52 to IRF-port 3/2.

```
[Sysname] irf-port 3/2
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/51
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/52
[Sysname-irf-port3/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device C reboots to join the IRF fabric.

4. Configure Device D:

Change the member ID of Device D to 4 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 4
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device D to Device B and Device C as shown in Figure 15, and log in to Device D. (Details not shown.)

Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 4/0/49 and Ten-GigabitEthernet 4/0/50 to IRF-port 4/1.

```
[Sysname] irf-port 4/1
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/49
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/50
[Sysname-irf-port4/1] quit
```

Bind Ten-GigabitEthernet 4/0/51 and Ten-GigabitEthernet 4/0/52 to IRF-port 4/2.

```
[Sysname] irf-port 4/2
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/51
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/52
[Sysname-irf-port4/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
```

```
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

5. Configure BFD MAD on the IRF fabric:

   # Create VLAN 3, and add GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 3/0/1, and GigabitEthernet 4/0/1 to VLAN 3.

```
[Sysname] vlan 3
[Sysname-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1 gigabitethernet
3/0/1 gigabitethernet 4/0/1
[Sysname-vlan3] quit
```

   # Create VLAN-interface 3, and configure a MAD IP address for each member device on the VLAN interface.

```
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad bfd enable
[Sysname-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[Sysname-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
[Sysname-Vlan-interface3] mad ip address 192.168.2.3 24 member 3
[Sysname-Vlan-interface3] mad ip address 192.168.2.4 24 member 4
[Sysname-Vlan-interface3] quit
```

   # Disable the spanning tree feature on GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 3/0/1, and GigabitEthernet 4/0/1.

```
[Sysname] interface range gigabitethernet 1/0/1 gigabitethernet 2/0/1
gigabitethernet 3/0/1 gigabitethernet 4/0/1
[Sysname-if-range] undo stp enable
[Sysname-if-range] quit
```

6. Configure Device E as the intermediate device:

   # Create VLAN 3, and assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to VLAN 3 for forwarding BFD MAD packets.

```
<DeviceE> system-view
[DeviceE] vlan 3
[DeviceE-vlan3] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceE-vlan3] quit
```

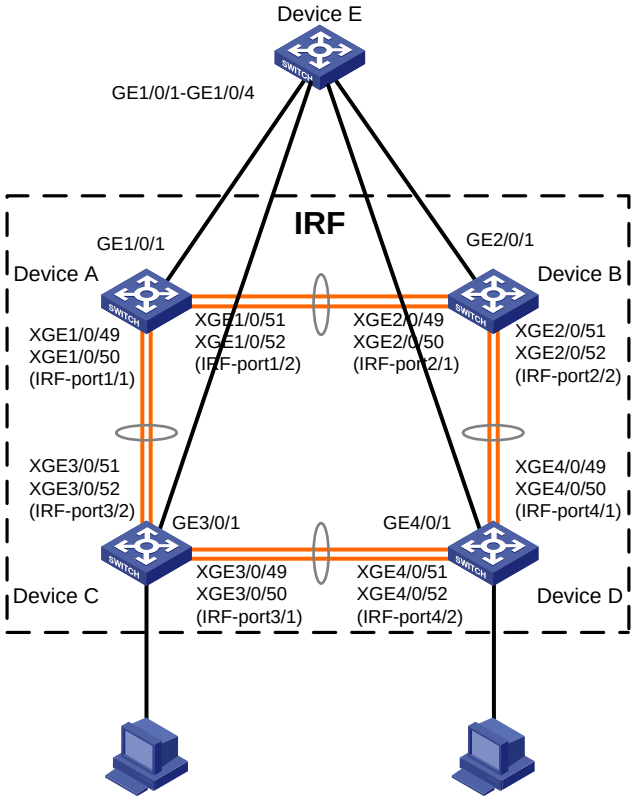
Example: Configuring an ARP MAD-enabled IRF fabric

Network configuration

As shown in Figure 16, set up a four-chassis IRF fabric in the enterprise network.

- Configure ARP MAD on the IRF fabric and use the links connected to Device E for transmitting ARP MAD packets.
- To prevent loops, run the spanning tree feature between Device E and the IRF fabric.

Figure 16 Network diagram



Procedure

1. Configure Device A:

   # Shut down the physical interfaces used for IRF links.

   ```
   <Sysname> system-view
   [Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
   [Sysname-if-range] shutdown
   [Sysname-if-range] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/49 and Ten-GigabitEthernet 1/0/50 to IRF-port 1/1.

   ```
   [Sysname] irf-port 1/1
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/49
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/50
   [Sysname-irf-port1/1] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/51 and Ten-GigabitEthernet 1/0/52 to IRF-port 1/2.

   ```
   [Sysname] irf-port 1/2
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/51
   [Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/52
   [Sysname-irf-port1/2] quit
   ```

   # Bring up the physical interfaces and save the configuration.

   ```
   [Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
   [Sysname-if-range] undo shutdown
   [Sysname-if-range] quit
   [Sysname] save
   ```

   # Activate the IRF port configuration.

   ```
   [Sysname] irf-port-configuration active
   ```

2. Configure Device B:

   # Change the member ID of Device B to 2 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

   # Connect Device B to Device A as shown in Figure 16, and log in to Device B. (Details not shown.)

   # Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

   # Bind Ten-GigabitEthernet 2/0/49 and Ten-GigabitEthernet 2/0/50 to IRF-port 2/1.

```
[Sysname] irf-port 2/1
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/49
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/50
[Sysname-irf-port2/1] quit
```

   # Bind Ten-GigabitEthernet 2/0/51 and Ten-GigabitEthernet 2/0/52 to IRF-port 2/2.

```
[Sysname] irf-port 2/2
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/51
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/52
[Sysname-irf-port2/2] quit
```

   # Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

   # Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

   The two devices perform master election, and the one that has lost the election reboots to form an IRF fabric with the master.

3. Configure Device C:

   # Change the member ID of Device C to 3 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

   # Connect Device C to Device A as shown in Figure 16, and log in to Device C. (Details not shown.)

   # Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

   # Bind Ten-GigabitEthernet 3/0/49 and Ten-GigabitEthernet 3/0/50 to IRF-port 3/1.

```
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/49
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/50
[Sysname-irf-port3/1] quit
```

Bind Ten-GigabitEthernet 3/0/51 and Ten-GigabitEthernet 3/0/52 to IRF-port 3/2.

```
[Sysname] irf-port 3/2
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/51
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/52
[Sysname-irf-port3/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device C reboots to join the IRF fabric.

4. Configure Device D:

Change the member ID of Device D to 4 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 4
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device D to Device B and Device C as shown in Figure 16, and log in to Device D. (Details not shown.)

Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 4/0/49 and Ten-GigabitEthernet 4/0/50 to IRF-port 4/1.

```
[Sysname] irf-port 4/1
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/49
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/50
[Sysname-irf-port4/1] quit
```

Bind Ten-GigabitEthernet 4/0/51 and Ten-GigabitEthernet 4/0/52 to IRF-port 4/2.

```
[Sysname] irf-port 4/2
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/51
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/52
[Sysname-irf-port4/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

5. Configure ARP MAD on the IRF fabric:

Enable the spanning tree feature globally. Map the ARP MAD VLAN to MSTI 1 in the MST region.

```
<Sysname> system-view
[Sysname] stp global enable
[Sysname] stp region-configuration
[Sysname-mst-region] region-name arpmad
[Sysname-mst-region] instance 1 vlan 3
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
```

Configure the IRF fabric to change its bridge MAC address as soon as the address owner leaves.

```
[Sysname] undo irf mac-address persistent
```

Set the domain ID of the IRF fabric to 1.

```
[Sysname] irf domain 1
```

Create VLAN 3, and assign GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 3/0/1, and GigabitEthernet 4/0/1 to VLAN 3.

```
[Sysname] vlan 3
[Sysname-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1 gigabitethernet
3/0/1 gigabitethernet 4/0/1
[Sysname-vlan3] quit
```

Create VLAN-interface 3, assign it an IP address, and enable ARP MAD on the interface.

```
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] ip address 192.168.2.1 24
[Sysname-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 1]:
The assigned domain ID is: 1
```

6. Configure Device E as the intermediate device:

CAUTION:

If the intermediate device is also in an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

Enable the spanning tree feature globally. Map the ARP MAD VLAN to MSTI 1 in the MST region.

```
<DeviceE> system-view
[DeviceE] stp global enable
[DeviceE] stp region-configuration
[DeviceE-mst-region] region-name arpmad
[DeviceE-mst-region] instance 1 vlan 3
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

Create VLAN 3, and assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to VLAN 3 for forwarding ARP MAD packets.

```
[DeviceE] vlan 3
[DeviceE-vlan3] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

```
[DeviceE-vlan3] quit
```

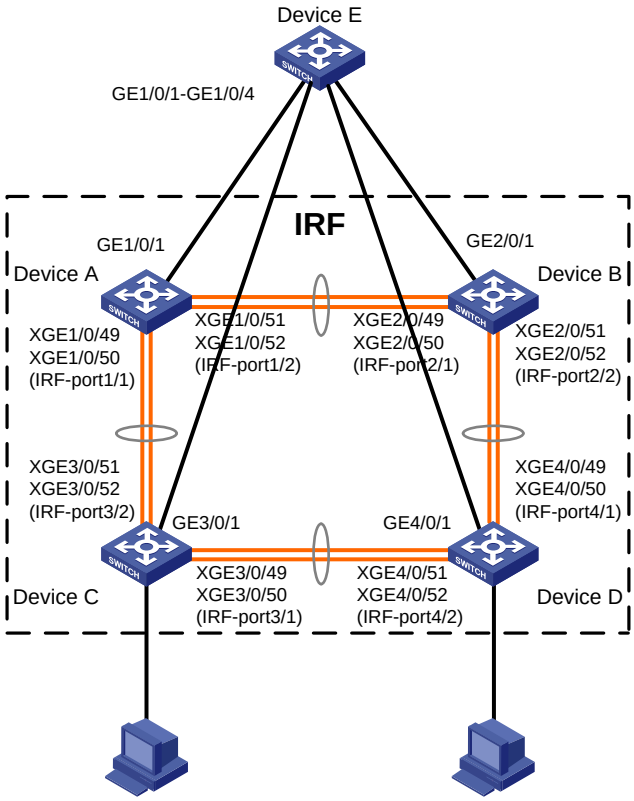
Example: Configuring an ND MAD-enabled IRF fabric

Network configuration

As shown in Figure 17, set up a four-chassis IRF fabric in the IPv6 enterprise network.

- Configure ND MAD on the IRF fabric and use the links connected to Device E for transmitting ND MAD packets.
- To prevent loops, run the spanning tree feature between Device E and the IRF fabric.

Figure 17 Network diagram



Procedure

1. Configure Device A:

   # Shut down the physical interfaces used for IRF links.

   ```
   <Sysname> system-view
   [Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
   [Sysname-if-range] shutdown
   [Sysname-if-range] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/49 and Ten-GigabitEthernet 1/0/50 to IRF-port 1/1.

   ```
   [Sysname] irf-port 1/1
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/49
   [Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/50
   [Sysname-irf-port1/1] quit
   ```

   # Bind Ten-GigabitEthernet 1/0/51 and Ten-GigabitEthernet 1/0/52 to IRF-port 1/2.

   ```
   [Sysname] irf-port 1/2
   ```

```
[Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/51
[Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/52
[Sysname-irf-port1/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 1/0/49 to ten-gigabitethernet 1/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

2. Configure Device B:

Change the member ID of Device B to 2 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device B to Device A as shown in Figure 17, and log in to Device B. (Details not shown.)

Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 2/0/49 and Ten-GigabitEthernet 2/0/50 to IRF-port 2/1.

```
[Sysname] irf-port 2/1
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/49
[Sysname-irf-port2/1] port group interface ten-gigabitethernet 2/0/50
[Sysname-irf-port2/1] quit
```

Bind Ten-GigabitEthernet 2/0/51 and Ten-GigabitEthernet 2/0/52 to IRF-port 2/2.

```
[Sysname] irf-port 2/2
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/51
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/52
[Sysname-irf-port2/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 2/0/49 to ten-gigabitethernet 2/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

The two devices perform master election, and the one that has lost the election reboots to form an IRF fabric with the master.

3. Configure Device C:

Change the member ID of Device C to 3 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
```

```
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device C to Device A as shown in Figure 17, and log in to Device C. (Details not shown.)

Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 3/0/49 and Ten-GigabitEthernet 3/0/50 to IRF-port 3/1.

```
[Sysname] irf-port 3/1
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/49
[Sysname-irf-port3/1] port group interface ten-gigabitethernet 3/0/50
[Sysname-irf-port3/1] quit
```

Bind Ten-GigabitEthernet 3/0/51 and Ten-GigabitEthernet 3/0/52 to IRF-port 3/2.

```
[Sysname] irf-port 3/2
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/51
[Sysname-irf-port3/2] port group interface ten-gigabitethernet 3/0/52
[Sysname-irf-port3/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 3/0/49 to ten-gigabitethernet 3/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device C reboots to join the IRF fabric.

4. Configure Device D:

Change the member ID of Device D to 4 and reboot the device to have the change take effect.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 4
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Connect Device D to Device B and Device C as shown in Figure 17, and log in to Device D. (Details not shown.)

Shut down the physical interfaces used for IRF links.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 4/0/49 and Ten-GigabitEthernet 4/0/50 to IRF-port 4/1.

```
[Sysname] irf-port 4/1
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/49
[Sysname-irf-port4/1] port group interface ten-gigabitethernet 4/0/50
[Sysname-irf-port4/1] quit
```

Bind Ten-GigabitEthernet 4/0/51 and Ten-GigabitEthernet 4/0/52 to IRF-port 4/2.

```
[Sysname] irf-port 4/2
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/51
[Sysname-irf-port4/2] port group interface ten-gigabitethernet 4/0/52
[Sysname-irf-port4/2] quit
```

Bring up the physical interfaces and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 4/0/49 to ten-gigabitethernet 4/0/52
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

Device D reboots to join the IRF fabric. A four-chassis IRF fabric is formed.

5. Configure ND MAD on the IRF fabric:

Enable the spanning tree feature globally. Map the ND MAD VLAN to MSTI 1 in the MST region.

```
<Sysname> system-view
[Sysname] stp global enable
[Sysname] stp region-configuration
[Sysname-mst-region] region-name ndmad
[Sysname-mst-region] instance 1 vlan 3
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
```

Configure the IRF fabric to change its bridge MAC address as soon as the address owner leaves.

```
[Sysname] undo irf mac-address persistent
```

Set the domain ID of the IRF fabric to 1.

```
[Sysname] irf domain 1
```

Create VLAN 3, and add GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 3/0/1, and GigabitEthernet 4/0/1 to VLAN 3.

```
[Sysname] vlan 3
[Sysname-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1 gigabitethernet
3/0/1 gigabitethernet 4/0/1
[Sysname-vlan3] quit
```

Create VLAN-interface 3, assign it an IPv6 address, and enable ND MAD on the interface.

```
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] ipv6 address 2001::1 64
[Sysname-Vlan-interface3] mad nd enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 1]:
The assigned domain ID is: 1
```

6. Configure Device E as the intermediate device:

CAUTION:

If the intermediate device is also in an IRF fabric, assign the two IRF fabrics different domain IDs for correct split detection. False detection causes IRF split.

Enable the spanning tree feature globally. Map the ND MAD VLAN to MSTI 1 in the MST region.

```
<DeviceE> system-view
[DeviceE] stp global enable
[DeviceE] stp region-configuration
[DeviceE-mst-region] region-name ndmad
[DeviceE-mst-region] instance 1 vlan 3
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

Create VLAN 3, and add GigabitEthernet 1/0/1, GigabitEthernet1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to VLAN 3 for forwarding ND MAD packets.

```
[DeviceE] vlan 3
[DeviceE-vlan3] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceE-vlan3] quit
```

Configuring an IRF 3.1 system

About IRF 3.1

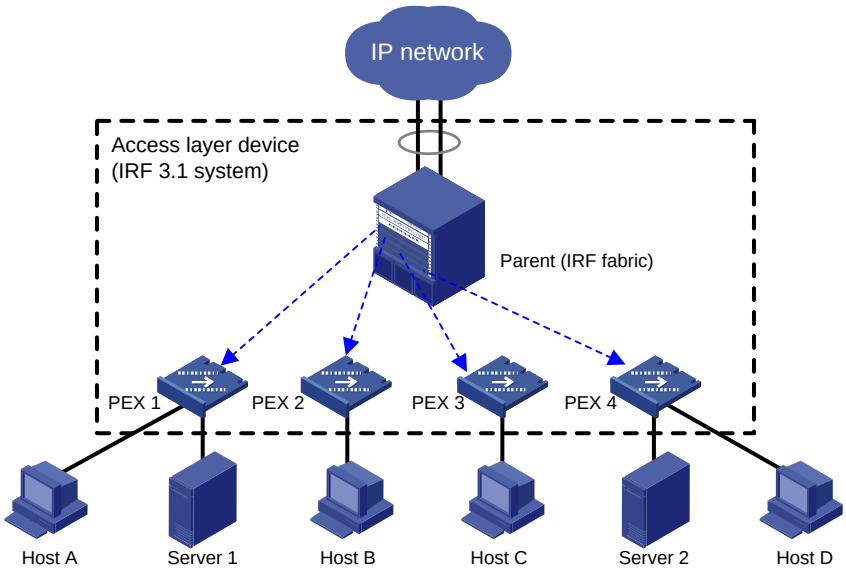
IRF 3.1 integrates multiple lower-layer devices with a higher-layer IRF fabric to provide high-density, low-cost connectivity at the access layer. IRF 3.1 is implemented based on IEEE 802.1BR.

In an IRF 3.1 system, the higher-layer IRF fabric is called the parent fabric and the lower-layer devices are called bridge port extenders (PEXs). You manage and configure the PEXs from the parent fabric as if they were interface modules on the parent fabric.

IRF 3.1 network model

Typically, IRF 3.1 works at the access layer of data centers and large-scale enterprise networks. As shown in Figure 18, the access layer of a network is virtualized into an IRF 3.1 system. The system contains one parent fabric (a two-chassis IRF fabric) and multiple PEXs to provide connectivity for servers and hosts.

Figure 18 IRF 3.1 application scenario



IRF 3.1 benefits

IRF 3.1 provides the following benefits:

- **Simplified topology**—Devices in an IRF 3.1 system appear as one node. For redundancy and load balancing, a downstream or upstream device can connect to the IRF 3.1 system through multichassis link aggregation. Together with link aggregation, IRF 3.1 creates a loop-free Layer 2 network. The spanning tree feature is not needed among devices in the IRF 3.1 system or on the link aggregations. IRF 3.1 also simplifies the Layer 3 network topology because it reduces the number of routing peers. The network topology does not change when a device is added to or removed from the IRF 3.1 system.
- **Single point of management**—An IRF 3.1 system is accessible at a single IP address on the network. You can use this IP address to log in through any network port to manage all the devices in the system. For an SNMP NMS, an IRF 3.1 system is one managed network node.

- **Network scalability and resiliency**—You can increase the number of ports in an IRF 3.1 system by adding PEXs without changing network topology.
- **High availability**—Each PEX has multiple high-speed physical ports for uplink connectivity to the parent fabric. The links on these ports are aggregated and load balanced automatically.
- **Decreased TCO**—IRF 3.1 decreases hardware investments and management costs. In an IRF 3.1 system, the parent fabric performs all the management and routing functions, and the PEXs only forward traffic. You can add low-performance devices as PEXs to an IRF 3.1 system for network scalability.
- **High software compatibility**—The software versions of the parent fabric and PEXs are highly compatible. You can independently upgrade software for the parent and PEXs.

Network topology

You can set up an IRF 3.1 system that contains one tier of PEXs. Each PEX is connected to the parent fabric through a Layer 2 aggregate interface in dynamic aggregation mode.

(Modular parent devices.) A PEX can be a single device or an IRF fabric as shown in Figure 19 and Figure 20. Single-device PEXs and IRF-fabric PEXs can coexist.

IMPORTANT:

To avoid loops, do not connect one PEX to another PEX.

Figure 19 IRF 3.1 network topology (PEXs are single devices)

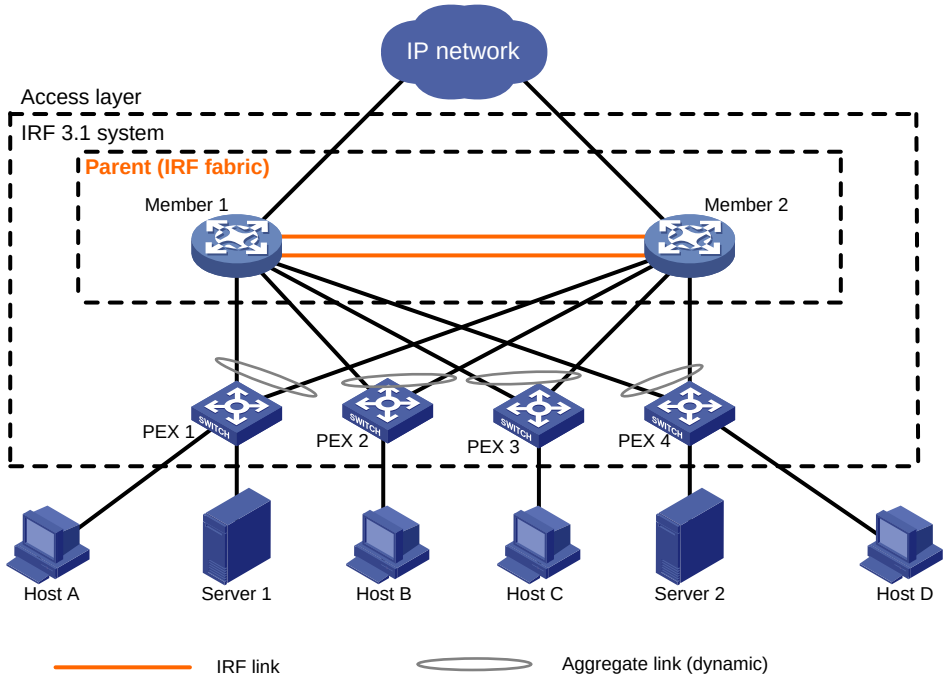
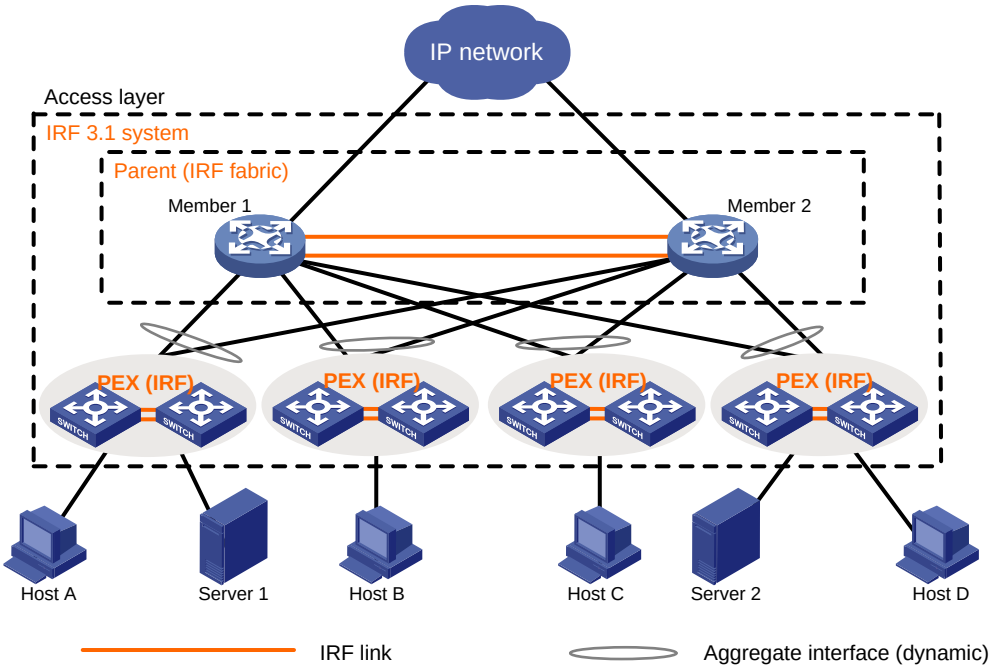


Figure 20 IRF 3.1 network topology (PEXs are IRF fabrics)



Basic concepts

IRF 3.1 includes IRF concepts and adds the concepts in this section.

IRF 3.1 roles

The devices in an IRF 3.1 system have the following roles:

- **Parent fabric**—Higher-layer single-chassis or multichassis IRF fabric that controls the entire IRF 3.1 system, including PEXs. Each IRF 3.1 system has one parent fabric.
- **Parent devices**—Member devices in the parent fabric.
- **Master device**—The device that controls and manages the entire IRF 3.1 system, including all parent devices and PEXs. The master device in the parent fabric is also the master device for the IRF 3.1 system. You configure all devices (including PEXs and parent devices) from the master device.
- **PEXs**—Operate as I/O modules of the parent fabric to receive and transmit traffic. All forwarding decisions are made on the parent fabric. PEXs can be configured only on the parent fabric. Table 2 shows the operating states of PEXs.

Table 2 PEX operating states

State	Description
Offline	The PEX is offline. The PEX and the parent fabric have not established a PE CSP connection. The PEX cannot be managed by the parent fabric.
Online	The PEX is online. An online PEX has been discovered by the parent fabric through LLDP and has finished Port Extender Control and Status Protocol (PE CSP) negotiation with the parent fabric.

Operating modes

The device supports auto, PEX, and switch modes as described in Table 3.

Table 3 IRF 3.1 operating modes

Mode	Application scenario	Description
auto	The device is planned to join an IRF 3.1 system and operates as a PEX.	When the device detects LLDP packets from the parent fabric, it automatically reboots, starts up with factory defaults, and operates as a PEX. Before changing to a PEX, the device operates as an independent node.
PEX	The device is planned to join an IRF 3.1 system and operates as a PEX.	The device operates as a PEX and acts as an interface card on the parent fabric.
switch	The device is planned to be an independent device or a parent device in an IRF 3.1 system.	The device operates as an independent node or a parent device in an IRF 3.1 system. The device does not change to a PEX even if it receives protocol packets from a parent device.

PEX categories

The following PEX categories are available:

- **Standard PEX**—A device that can act as an independent device or a PEX. To use a standard PEX in an IRF 3.1 system, you must convert its operating mode to PEX or auto.
- **Fit PEX**—A device that can act only as a PEX in an IRF 3.1 system. The operating mode of a fit PEX is not convertible.

You configure standard and fit PEXs from the parent fabric in the same way.

Cascade port

A cascade port is a Layer 2 dynamic aggregate interface with PEX connection capability enabled, and it connects the parent fabric to a PEX. The physical interfaces assigned to a cascade port are cascade member interfaces.

Upstream port

An upstream port is a Layer 2 dynamic aggregate interface automatically created on a PEX for parent fabric connection. The aggregate interface automatically aggregates physical interfaces that connect the PEX to the cascade member interfaces of the parent fabric.

PEX group

A PEX group contains a group of PEXs that are connected to cascade ports assigned to the same PEX group.

Extended port

In an IRF 3.1 system, the physical interfaces on PEXs are called extended ports, except for the physical interfaces aggregated in the upstream ports.

Layer 2 extended-link aggregate interface

A Layer 2 extended-link aggregate interface aggregates a group of extended ports. The aggregation group of a Layer 2 extended-link aggregate interface is a Layer 2 extended-link aggregation group.

Layer 2 extended-link aggregate interfaces can act as interfaces that forward service traffic.

For more information about extended-link aggregate interfaces, see Ethernet link aggregation configuration in *Layer 2—LAN Switching Configuration Guide*.

PEX fabric (modular parent devices)

A PEX fabric is a multichasiss IRF fabric that acts as a PEX. Unless otherwise stated, the term "PEX" in this documentation refers to not only single-device PEXs but also PEX fabrics.

Virtual chassis number and virtual slot number (modular parent devices)

For management purposes, each PEX is assigned to a unique virtual chassis on the parent fabric. A single-device PEX or a PEX fabric member is managed as an interface module on its virtual chassis. The slot numbers for single-device PEXs or PEX fabric members are identical to their IRF member IDs.

Virtual slot number (fixed-port or expandable fixed-port parent devices)

Each PEX is identified by a unique virtual slot number in an IRF 3.1 system.

IRF 3.1 system setup process

Neighbor discovery

After you finish configuration on the parent fabric and a PEX and the PEX link is up, the parent fabric and the PEX send LLDP packets to each other for neighbor discovery.

PE CSP connection establishment

After the parent fabric and the PEX finish neighbor discovery, they send PE CSP Open requests to each other. If the parent fabric and the PEX can receive PE CSP Open responses from each other within 60 seconds, the connection between them is established.

PEX registration

After the connection is established between the parent and PEX, the PEX uses the following process to join the IRF 3.1 system:

1. The PEX requests to register with the parent fabric. The parent fabric assigns the configured virtual slot number to the PEX.
2. The PEX requests to create its extended ports on the parent fabric. After receiving the request, the parent fabric creates the extended ports of the PEX on the parent fabric and assigns an E-channel Identifier (ECID) to each port. The ECID must be unique in the PEX group. At the same time, the interface attributes such as link state, duplex state, and rate are synchronized from the PEX to the parent fabric.

PEX link maintenance

The parent fabric and the PEX use Layer 2 aggregate interfaces in dynamic aggregation mode to connect each other. The Layer 2 aggregate interface uses LACP and PE CSP to detect and maintain link status. The PEX is offline when the aggregate interface is down or when the parent fabric and PEX do not receive PE CSP responses from each other within 60 seconds. For the PEX to come online again, the parent fabric and PEX must send PE CSP Open requests to each other and can receive Open responses from each other.

Interface naming conventions

(Modular parent devices.) After a PEX joins an IRF 3.1 system, the virtual chassis number and slot number are included as the first two segments of the interface numbers on the PEX. For example, a single-device PEX with an IRF member ID of 1 has an interface numbered 1/0/1 before it is added to an IRF 3.1 system. After it is added to chassis 100 on an IRF 3.1 system, the interface number changes to 100/1/0/1.

(Fixed-port or expandable fixed-port parent devices.) After a PEX joins an IRF 3.1 system, the first segment in its interface numbers changes to the virtual slot number assigned to the PEX. For example, a PEX has an interface numbered 1/0/1 before it is added to an IRF 3.1 system. After it is added to an IRF 3.1 system as slot 100, the interface number changes to 100/0/1.

Configuration management

An IRF 3.1 system manages all its settings (including settings for PEXs) on the master device. You can configure and manage PEXs from the master device. The running configuration on the master device typically has all settings in the IRF 3.1 system, including settings for PEXs. When a PEX reboots or is added, the master device issues the running configuration of the virtual chassis or slot to the PEX.

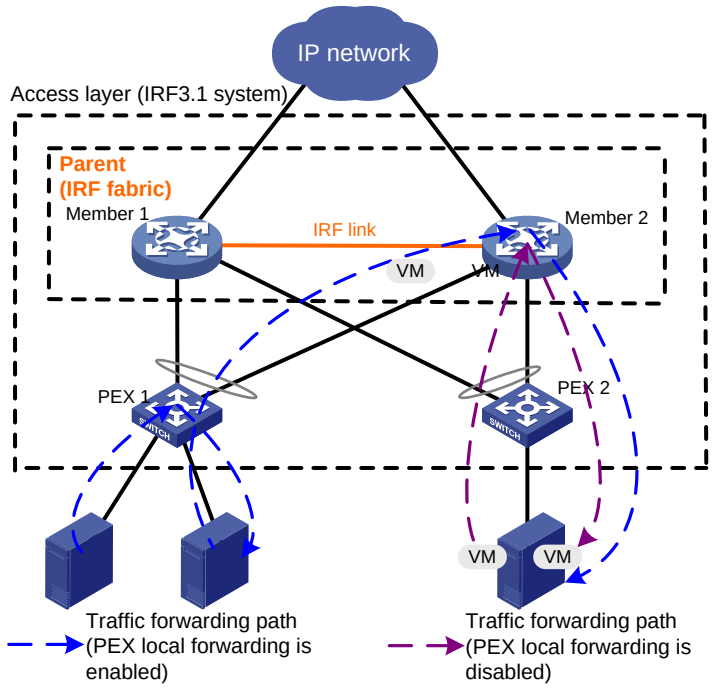
Data forwarding

When PEX local forwarding is enabled for a PEX, the PEX performs local forwarding for Layer 2 unicast packets with known MAC addresses. For other packets, the PEX forwards them to the parent fabric for processing.

When PEX local forwarding is disabled for a PEX, the PEX sends any incoming traffic to the parent fabric. The parent fabric makes forwarding decisions and sends the traffic to the outgoing interfaces (see Figure 21).

When the PEX receives a packet, it tags the packet with an E-tag. The E-tag carries the ECID of the interface that receives the packet. IRF 3.1 forwards the packet based on the ECID within the IRF 3.1 system. When the packet leaves the IRF 3.1 system, the E-tag is removed.

Figure 21 Data forwarding model



Protocols and standards

IEEE 802.1BR, *Virtual Bridged Local Area Networks—Bridge Port Extension*

Restrictions: Hardware compatibility with IRF 3.1

The S5500V2-EI switch series and the MS4520V2-30F switch do not support IRF 3.1.

Restrictions and guidelines: IRF 3.1 configuration

Hardware compatibility with IRF 3.1

An S5560X-EI switch can act as a parent device or PEX. When an S5560X-EI switch acts as a PEX, it cannot connect lower-tier PEXs.

The following switch series can be attached as PEXs to an S5560X-EI parent fabric:

- H3C S5560X-EI, which are standard PEXs.
- H3C FS4100, which are fit PEXs.

System operating mode restrictions

Before you configure IRF 3.1 settings, you must use the **`switch-mode 2`** command to set the system operating mode to 802.1BR. For more information about setting the system operating mode, see device management in *Fundamentals Configuration Guide*.

PEX upstream member interface requirements

You can use only some high-speed physical interfaces on a PEX as upstream member interfaces. To identify candidate upstream member interfaces, use one of the following methods:

- Obtain information from the configuration guide for the device to be used as a PEX. On the S5560X-EI switch series, the two highest numbered ports on the front panel can be used as upstream member interfaces.
- Execute the **`display system internal pex upstreamport`** command in probe view on the device to be used as a PEX when the device operates in PEX mode.

Loop elimination

By default, the spanning tree feature is disabled on the ports of PEXs to prevent unnecessary topology calculations and conserve system resources. When you set up an IRF 3.1 system, you must make sure it is physically or logically loop free.

To conserve system resources, set up a physically loop-free IRF 3.1 system as shown in "Network topology." Make sure no connections exist between PEXs or between PEXs and parent devices except the cascade links.

If a port on a PEX is in a loop because of physical redundancy design, you must enable the spanning tree feature on that port.

PEX fabric restrictions (applicable only to modular parent devices)

Support for PEX fabrics of this switch series depends on the parent device model. To identify the support of the parent fabric for PEX fabrics of this switch series, see IRF configuration in the configuration guides of the parent fabric.

To use an S5560X-EI IRF fabric as a PEX fabric, make sure the IRF fabric meets the following requirements:

- The IRF fabric contains only four or fewer member devices.
- The IRF fabric uses a daisy-chain topology.

- The IRF member ID is in the range of 1 to 5 for each member device.

After you change the member ID of a member device in the PEX fabric, you must reboot the master device in addition to that member device for the change to take effect.

Link aggregation restrictions and guidelines

To assign extended ports to a Layer 2 extended-link aggregation group, make sure the PEXs that contain the ports meet the following requirements:

- The PEXs belong to the same switch series.
- The PEXs are in the same PEX group.

When FS4100 fit switches act as PEXs, Layer 2 extended-link aggregation groups are not supported.

PEX configuration management restrictions and guidelines

You must configure a PEX from the parent fabric.

To display PEX running information, use the method in "Logging in to a PEX from the parent fabric."

IRF split detection requirements

For the PEXs to quickly identify parent fabric split events, perform the following tasks on the parent fabric:

- Use the **lacp system-priority** command to set the system LACP priority to a value lower than 32768.
- Use the **undo irf mac-address persistent** command to disable IRF bridge MAC persistence. In addition, do not specify an IRF bridge MAC address by using the **irf mac-address** *mac-address* command.

Ports on a PEX cannot be used for IRF MAD of the parent fabric.

The IRF 3.1 system automatically issues the LACP MAD configuration to the upstream port of each PEX fabric to detect multi-active collisions. If a PEX fabric splits into two fabrics, the MAD mechanism automatically shuts down all network interfaces on the Recovery-state fabric.

Configuration rollback restrictions

As a best practice, do not roll back the configuration if the replacement configuration file contains IRF 3.1 settings different than the running configuration. If you roll back the configuration, the system might fail to reconfigure IRF 3.1 settings as expected. For more information about the configuration rollback feature, see configuration file management in *Fundamentals Configuration Guide*.

IRF 3.1 tasks at a glance

An IRF 3.1 system can be set up with automatically configured PEXs or manually configured PEXs.

For PEXs to come online or operate correctly, do not manually configure PEXs when the PEX autoconfiguration feature is enabled on the IRF 3.1 system.

Configuring an IRF 3.1 system with manually configured PEXs

To configure an IRF 3.1 system with manually configured PEXs, perform the following tasks:

1. Configuring the operating mode
   - Configuring a device as an independent device
   - Configuring a device as a PEX
2. Setting up the parent fabric
3. Configuring PEXs on the parent fabric
   a. Creating a PEX group
   b. Configuring cascade ports for PEXs
   c. Assigning virtual slot numbers to PEXs
   d. Connecting the PEXs to the parent fabric
4. (Optional.) Maintaining an IRF 3.1 system
   - Enabling PEX local forwarding
   - Enabling PEX persistent forwarding
   - Logging in to a PEX from the parent fabric
   - Deleting idle cascade ports
5. Removing PEXs from an IRF 3.1 system

Configuring an IRF 3.1 system with automatically configured PEXs

To configure an IRF 3.1 system with automatically configured PEXs, perform the following tasks:

1. Configuring the operating mode
   - Configuring a device as an independent device
   - Configuring a device as a PEX
2. Setting up the parent fabric
3. Enabling PEX autoconfiguration
4. Connecting the PEXs to the parent fabric
5. (Optional.) Maintaining an IRF 3.1 system
   - Enabling PEX local forwarding
   - Enabling PEX persistent forwarding
   - Logging in to a PEX from the parent fabric
   - Deleting idle cascade ports
6. Removing PEXs from an IRF 3.1 system

Planning the IRF 3.1 system setup

Consider the following items when you plan an IRF 3.1 system:

- Hardware compatibility and restrictions.
- IRF 3.1 system size.
- Parent devices and PEXs.

- Cascade ports, cascade member interfaces, upstream member interfaces, and cabling scheme.
- Virtual chassis or slot assignment for PEXs.

The plan must meet the requirements described in "Restrictions and guidelines: IRF 3.1 configuration."

For more information about hardware and cabling, see the installation guide for the device.

Configuring the operating mode

Configuring a device as an independent device

About configuring a device as an independent device

As a best practice, change the operating mode to switch and save the configuration to avoid the operating mode changing from auto to PEX due to connection errors or attacks.

Mode change from auto to switch takes effect immediately, and mode change from PEX to switch takes effect after a reboot.

Restrictions and guidelines

Perform this task on each parent device before you set up the parent fabric.

Procedure

1. Enter system view.

   `system-view`
2. Change the operating mode to switch.

   `pex system-working-mode switch`

   By default, the device operates in auto mode. The device automatically changes to the PEX mode to join an IRF 3.1 system when it detects any LLDP packets from a parent device.
3. Save the running configuration.

   `save`

   For the switch mode to take effect after a reboot, save the running configuration.

Configuring a device as a PEX

About configuring a device as a PEX

For the device to operate as a PEX, set the device operating mode to auto or PEX.

If you set the operating mode to auto, the device automatically reboots with factory defaults when it detects LLDP packets from a parent device. After the reboot, the device operates as a PEX.

For the PEX mode to take effect, you must save the running configuration and manually reboot the device. The device starts up with the factory defaults. After the reboot, the device operates as a PEX.

Restrictions and guidelines for mode configuration

This task is not applicable to fit PEXs. A fit PEX can act only as a PEX in an IRF 3.1 system. The operating mode of a fit PEX is not convertible. For a fit PEX to join an IRF 3.1 system, you only need to connect the upstream member interfaces of that PEX to the parent fabric.

When the device operates in PEX mode, you cannot set the operating mode to auto.

To use an IRF fabric as a PEX, perform the following tasks:

1. Set the operating mode of all member devices to auto or PEX. All member devices in a PEX fabric must operate in the same mode.
2. Set up the PEX fabric. For information about setting up a PEX fabric, see "Configuring an IRF fabric."
3. Add the PEX fabric to the IRF 3.1 system.

To avoid system exceptions, do not change (add, delete, or modify) IRF port bindings on the PEX fabric after it is added to the IRF 3.1 system. If a change is required, remove the PEX fabric from the IRF 3.1 system, change its IRF port bindings, and then add the PEX fabric back to the IRF 3.1 system.

Setting the operating mode to auto

1. Enter system view.

   `system-view`
2. Set the operating mode to auto.

   `pex system-working-mode auto`

   By default, the device operates in auto mode. The device can automatically change to a PEX upon receiving LLDP packets from a parent device.

   For the device to automatically change to a PEX, make sure the device does not have interfaces enabled with PEX connection capability.
3. (Optional.) Save the running configuration.

   `save`

   Save the running configuration to the next-startup configuration file for the auto mode to take effect after another reboot.

Setting the operating mode to PEX

1. Enter system view.

   `system-view`
2. Set the operating mode to PEX.

   `pex system-working-mode pex`

   By default, the device operates in auto mode. The device can automatically change to a PEX upon receiving LLDP packets from a parent device.
3. Save the running configuration.

   `save`
4. Return to user view.

   `quit`
5. Reboot the device.

   `reboot`

Setting up the parent fabric

You can use a single-member or multimember IRF fabric as the parent fabric. Before you set up the parent fabric, change the operating mode of its member devices to switch. To set up the parent fabric, use the procedure described in "Configuring an IRF fabric."

Creating a PEX group

Restrictions and guidelines

After a PEX group is created, the device automatically enables the NTP service and specifies the local clock as the reference source at stratum 2.

If you delete a PEX group, all PEXs in that group will go offline with all settings issued from the parent device removed.

Procedure

1. Enter system view.
   system-view
2. Create a PEX group.
   pex group *group-id*
3. (Optional.) Configure a description for the PEX group.
   description *text*
   By default, the description for a PEX group uses the **PEX group** *group-id* format.

Configuring cascade ports for PEXs

About cascade ports for PEXs

The cascade ports for PEXs are Layer 2 aggregate interfaces in dynamic aggregation mode. The member interfaces in each cascade port are physical interfaces that connect the parent fabric to a PEX.

The system automatically places a Layer 2 aggregate interface in dynamic aggregation mode after you enable its PEX connection capability. In addition, the system automatically configures the aggregate interface as an edge port of the spanning tree feature for the PEX to quickly come online.

Restrictions and guidelines

Make sure all physical interfaces assigned to a cascade port connect to the same PEX.

For PEXs to come online successfully, do not execute any other commands on cascade ports except for the IRF 3.1 commands, the **shutdown** command, and the **description** command. In addition, do not execute any other commands on the cascade member interfaces except for the **lldp enable** command.

Disabling PEX connection capability on a cascade port causes the attached PEX to go offline. When you assign a cascade port to a new PEX group, its attached PEX goes offline and then comes online again. When the PEX goes offline in either situation, all settings issued from the parent fabric are automatically removed from the PEX.

Procedure

1. Enter system view.
   system-view
2. Enable LLDP globally.
   lldp global enable
   The default setting varies by the startup configuration.
   - If the device starts up with the empty configuration, LLDP is disabled globally.
   - If the device starts up with the factory defaults, LLDP is enabled globally.
3. Create a Layer 2 aggregate interface and enter Layer 2 aggregate interface view.

interface bridge-aggregation *interface-number*

When you create a Layer 2 aggregate interface, the system automatically creates a Layer 2 aggregation group with the same number as the aggregate interface. The aggregation group operates in static aggregation mode by default.

4. Enable PEX connection capability on the Layer 2 aggregate interface and assign it to a PEX group.

   pex-capability enable group *group-id*

   By default, an aggregate interface cannot connect PEXs.

5. Return to system view.

   quit

6. Enter Layer 2 Ethernet interface view or Layer 2 Ethernet interface range view.
   - Enter interface view.

     interface *interface-type interface-number*
   - Enter interface range view.

     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>

   To assign one port to the aggregation group, enter Ethernet interface view.

   To assign a range of ports to the aggregation group, enter interface range view.

7. Assign Layer 2 Ethernet ports to the aggregation group.

   port link-aggregation group *group-id*

   All physical interfaces assigned to the aggregate interface must connect to the same PEX

8. Enable LLDP on the ports.

   lldp enable

   By default, LLDP is enabled on a port.

Assigning virtual slot numbers to PEXs

Restrictions and guidelines

When you remove or change the virtual PEX slot number of an online PEX, make sure you understand its impact on that PEX:

- If you remove the virtual slot number, the PEX goes offline. All settings issued from the parent fabric are cleared on the PEX.
- If you change the virtual slot number, the PEX goes offline and then comes online with the new virtual slot.

Procedure

1. Enter system view.

   system-view

2. Enter Layer 2 aggregate interface view.

   interface bridge-aggregation *interface-number*

3. Assign a virtual slot number to the PEX.

   pex associate slot *slot-number*

   By default, no virtual slot number is assigned to a PEX.

Enabling PEX autoconfiguration

About PEX autoconfiguration

After PEX autoconfiguration is enabled, the parent fabric identifies a device as a PEX once it receives LLDP packets carrying the Port Extension TLV from the device. The parent fabric automatically establishes a connection with the device and issues PEX settings to the device.

A PEX is automatically configured in the following process:

1. The parent fabric automatically creates PEX group 1 for PEXs to come online through autoconfiguration.
2. After receiving LLDP packets from the PEX, the parent fabric creates a Layer 2 aggregate interface and assigns the physical interfaces connecting to the PEX to the aggregation group. The number of the Layer 2 aggregate interface is randomly selected from the unused interface numbers in the system.
3. The parent fabric enables PEX connection capability on the Layer 2 aggregate interface and assigns the interface to PEX group 1.
4. The parent fabric assigns an unused virtual slot number to the PEX.

After the process, the PEX comes online.

You can view log messages or execute the **display current-configuration** command to obtain the detailed PEX settings issued by the PEX autoconfiguration feature.

Restrictions and guidelines

For an IRF 3.1 system enabled with PEX autoconfiguration to operate correctly, follow these restrictions and guidelines:

- Do not execute any other commands on the cascade ports except for the automatically configured IRF 3.1 commands.
- Do not execute any other commands on the cascade member interfaces except for the **lldp enable** command.

Disabling PEX autoconfiguration does not affect the PEX configuration already issued.

Procedure

1. Enter system view.

   system-view
2. Enable LLDP globally.

   lldp global enable

   The default setting varies by startup configuration.
   - If the device starts up with the initial configuration, LLDP is disabled globally.
   - If the device starts up with factory defaults, LLDP is enabled globally.
3. Enter Layer 2 Ethernet interface view or Layer 2 Ethernet interface range view.
   - Enter interface view.

     interface *interface-type interface-number*
   - Enter interface range view.

     interface range { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-24>

   To enable LLDP on one port, enter Ethernet interface view.

   To enable LLDP on a range of ports, enter interface range view.
4. Enable LLDP on the ports.

   lldp enable

By default, LLDP is enabled on a port.

5. Return to system view.
   quit
6. Enable PEX autoconfiguration.
   pex auto-config enable
   By default, PEX autoconfiguration is disabled.

Connecting the PEXs to the parent fabric

Connect the upstream member interfaces on a PEX to the cascade member interfaces of the cascade port on the parent fabric.

To identify candidate upstream member interfaces, see "PEX upstream member interface requirements."

For information about connection restrictions and guidelines, see "Network topology."

Enabling PEX local forwarding

About PEX local forwarding

This feature enables a PEX to perform local forwarding for Layer 2 unicast packets with known MAC addresses. The PEX delivers a packet to the parent fabric for processing only if that packet is not a Layer 2 unicast packet with a known MAC address.

If PEX local forwarding is disabled for a PEX, the PEX sends any incoming traffic to the parent fabric. The parent fabric makes forwarding decisions and sends the traffic to the outgoing interfaces.

When you enable or disable PEX local forwarding on a cascade port, the PEX will go offline and then come online again.

Restrictions and guidelines

With PEX local forwarding enabled, an S5560X-EI or FS4100 PEX delivers all packets except for Layer 2 known unicast packets to the parent fabric through the CPU. The delivery rate is limited by the CPU forwarding rate.

Procedure

1. Enter system view.
   system-view
2. Enter Layer 2 aggregate interface view of a cascade port.
   interface bridge-aggregation *interface-number*
3. Enable PEX local forwarding.
   pex local-forwarding
   By default, PEX local forwarding is disabled.

Enabling PEX persistent forwarding

About PEX persistent forwarding

If PEX persistent forwarding is enabled for a PEX, the system will not clear the running data or shut down the network interfaces on the PEX after the PEX goes offline. The PEX can still perform local forwarding.

If PEX persistent forwarding is disabled for a PEX, the system clears the running data and shuts down all network interfaces on the PEX after the PEX goes offline. However, the system does not shut down the upstream member interfaces on the PEX. The PEX will attempt to recover the connection with the parent fabric by sending protocol control packets out of the upstream member interfaces.

Prerequisites

For PEX persistent forwarding to take effect on a PEX, you must enable PEX local forwarding for that PEX.

Procedure

1. Enter system view.
   `system-view`
2. Enter Layer 2 aggregate interface view of a cascade port.
   `interface bridge-aggregation` *`interface-number`*
3. Enable PEX persistent forwarding.
   `pex persistent-forwarding`
   By default, PEX persistent forwarding is disabled.

Logging in to a PEX from the parent fabric

About logging in to a PEX from the parent fabric

After you log in to a PEX, you can execute the following commands:

- The **`display`** commands.
- File system management commands. To obtain information about the access permissions to the commands, use the **`display role feature name filesystem`** command in RBAC. For more information about the file system management and RBAC commands, see *Fundamentals Command Reference*.

Procedure

1. Enter system view.
   `system-view`
2. Log in to a PEX.
   `switchto pex slot` *`slot-number`*

Deleting idle cascade ports

About deleting idle cascade ports

Perform this task to delete all the cascade ports of which the connected PEXs are offline to release resources.

Restrictions and guidelines

For the connected PEX of a deleted cascade port to come online again, you must reconfigure a cascade port for connecting the PEX. Do not delete a cascade port if the connected PEX goes offline temporarily.

Procedure

1. Enter system view.
   `system-view`

2. Delete idle cascade ports.
   pex idle-cascade delete

Removing PEXs from an IRF 3.1 system

About removing PEXs from an IRF 3.1 system

To temporarily remove a PEX from an IRF 3.1 system, disconnect the PEX links between the PEX and the parent fabric or power off the PEX.

To remove a PEX from an IRF 3.1 system and use it as an independent device, log in to the PEX through the console port and change the operating mode to switch.

Procedure

1. Enter system view.
   system-view
2. Change the PEX to switch mode.
   pex system-working-mode switch
   By default, the device operates in auto mode.
3. Save the running configuration.
   save
   The device will operate in the mode set in the startup configuration after a reboot if you do not save the running configuration.
4. Return to user view.
   quit
5. Reboot the PEX for the mode change to take effect.
   reboot

Display and maintenance commands for IRF 3.1

Execute **display** commands in any view.

Task	Command
Display device information.	**display device**
Display electronic label information for the device.	**display device manuinfo**
Display information about PEX state and PE CSP statistics for a cascade port or for all cascade ports.	**display pex interface** [*interface-name*] [**brief**]
Display system operating mode information in an IRF 3.1 system.	**display pex system-working-mode**
Display PEX topology information.	**display pex topology**
Display system version information.	**display version**

NOTE:

For information about the **display device**, **display device manuinfo**, and **display version** commands, see *Fundamentals Command Reference*.

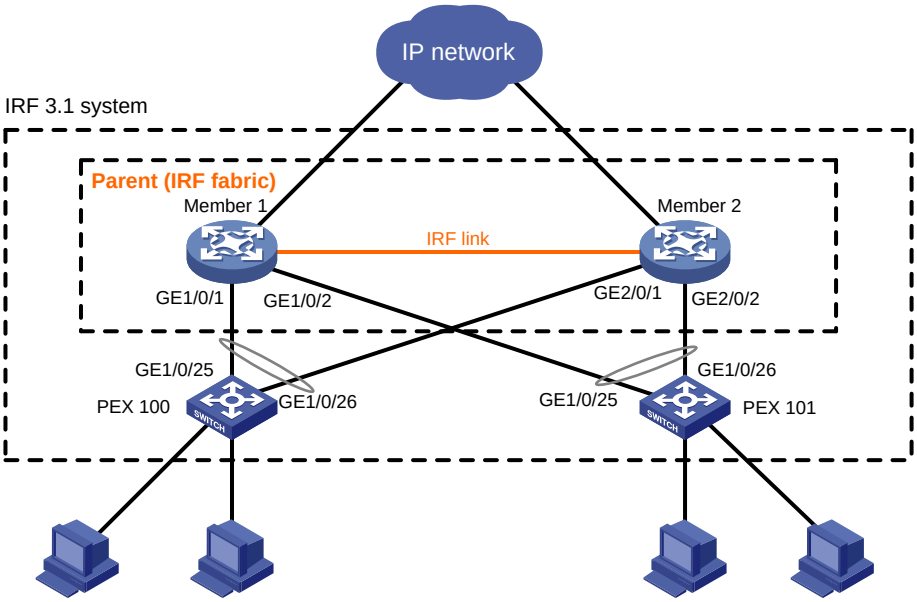
IRF 3.1 configuration examples

Example: Configuring an IRF 3.1 system

Network configuration

As shown in Figure 22, set up an IRF 3.1 system. The parent fabric contains two devices of this series. The PEXs are two FS4100-26P switches.

Figure 22 Network diagram



Setting up the parent fabric

Log in to Member 1 and Member 2, and change the operating mode of Member 1 and Member 2 to switch, respectively.

```
<Sysname> system-view
[Sysname] pex system-working-mode switch
```

Set up a two-chassis IRF fabric with Member 1 and Member 2, as described in "Configuring an IRF fabric." (Details not shown.)

Configuring cascade ports for PEXs on the parent fabric

Enter the system view.

```
<Sysname> system-view
```

Enable LLDP globally.

```
[Sysname] lldp global enable
```

Create PEX group 1.

```
[Sysname] pex group 1
[Sysname-pex-group-1] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 100. The aggregate interface will act as the cascade port to the PEX in slot 100.

```
[Sysname] interface bridge-aggregation 100
```

Enable PEX connection capability on Bridge-Aggregation 100 and assign Bridge-Aggregation 100 to PEX group 1.

```
[Sysname-Bridge-Aggregation100] pex-capability enable group 1
The aggregate interface was automatically set to dynamic aggregation mode and configured
as an STP edge port.
```

Assign virtual slot number 100 to the PEX.

```
[Sysname-Bridge-Aggregation100] pex associate slot 100
[Sysname-Bridge-Aggregation100] quit
```

Enable LLDP on GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1 in interface range view, and assign the ports to aggregation group 100. The ports will act as the cascade member interfaces.

```
[Sysname] interface range gigabitethernet 1/0/1 gigabitethernet 2/0/1
[Sysname-if-range] lldp enable
[Sysname-if-range] port link-aggregation group 100
[Sysname-if-range] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 101. The aggregate interface will act as the cascade port to the PEX in slot 101.

```
[Sysname] interface bridge-aggregation 101
```

Enable PEX connection capability on Bridge-Aggregation 101 and assign the interface to PEX group 1.

```
[Sysname] interface bridge-aggregation 101
[Sysname-Bridge-Aggregation101] pex-capability enable group 1
The aggregate interface was automatically set to dynamic aggregation mode and configured
as an STP edge port.
```

Assign virtual slot number 101 to the PEX.

```
[Sysname-Bridge-Aggregation101] pex associate slot 101
[Sysname-Bridge-Aggregation101] quit
```

Enable LLDP on GigabitEthernet 1/0/2 and GigabitEthernet 2/0/2 in interface range view, and assign the ports to aggregation group 101. The ports will act as the cascade member interfaces.

```
[Sysname] interface range gigabitethernet 1/0/2 gigabitethernet 2/0/2
[Sysname-if-range] lldp enable
[Sysname-if-range] port link-aggregation group 101
[Sysname-if-range] quit
```

Configuring PEXs

Connect the highest numbered two ports on the PEX device panel to the cascade member interfaces of the parent fabric. Because the FS4100 switches are fit PEXs, no additional configuration is required.

Verifying the configuration

Display device information on the parent fabric. Verify that the output contains information about both the parent fabric and the PEXs.

```
<Sysname> display device
...
```

Display PEX topology information.

```
<Sysname> display pex topology
Group  1
  Tier 1
    PEX 100 -----> Parent
    PEX 101 -----> Parent
```