Preface

The H3C S5500-HI documentation set includes 11 configuration guides, which describe the software features for the H3C S5500-HI Switch Series Release 5101, and guide you through the software configuration procedures. These configuration guides also provide configuration examples to help you apply software features to different network scenarios.

The IRF Configuration Guide describes how to use multiple S5500-HI switches to create an IRF virtual device based on the IRF technology. It covers planning the switch roles in the IRF virtual device, connecting the IRF link, and detecting and maintaining the IRF virtual device.

This preface includes:
• Audience
• Conventions
• About the S5500-HI documentation set
• Obtaining documentation
• Technical support
• Documentation feedback

Audience

This documentation is intended for:
• Network planners
• Field technical support and servicing engineers
• Network administrators working with the S5500-HI Switch Series

Conventions

This section describes the conventions used in this documentation set.

Command conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boldface</td>
<td>Bold text represents commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td>Italic</td>
<td>Italic text represents arguments that you replace with actual values.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
</tbody>
</table>
### Convention Description

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{ x</td>
<td>y</td>
</tr>
<tr>
<td><code>&amp;&lt;1-n&gt;</code></td>
<td>The argument or keyword and argument combination before the ampersand (&amp;) sign can be entered 1 to n times.</td>
</tr>
<tr>
<td><code>#</code></td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

### GUI conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Window names, button names, field names, and menu items are in Boldface. For example, the <em>New User</em> window appears; click <strong>OK</strong>.</td>
</tr>
<tr>
<td><code>&gt;</code></td>
<td>Multi-level menus are separated by angle brackets. For example, <em>File &gt; Create &gt; Folder</em>.</td>
</tr>
</tbody>
</table>

### Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴 <strong>WARNING</strong></td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td>🔴 <strong>CAUTION</strong></td>
<td>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.</td>
</tr>
<tr>
<td>🚨 <strong>IMPORTANT</strong></td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td>📌 <strong>NOTE</strong></td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td>💡 <strong>TIP</strong></td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>

### Network topology icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="Generic Network Device" /></td>
<td>Represents a generic network device, such as a router, switch, or firewall.</td>
</tr>
<tr>
<td><img src="icon" alt="Routing-Capable Device" /></td>
<td>Represents a routing-capable device, such as a router or Layer 3 switch.</td>
</tr>
<tr>
<td><img src="icon" alt="Generic Switch" /></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

### About the S5500-HI documentation set

The H3C S5500-HI documentation set includes:

<table>
<thead>
<tr>
<th>Documents</th>
<th>Purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product description and specifications</td>
<td>Describe product specifications and benefits.</td>
</tr>
</tbody>
</table>

**Marketing brochure**
<table>
<thead>
<tr>
<th>Documents</th>
<th>Purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology white papers</td>
<td>Provide an in-depth description of software features and technologies.</td>
</tr>
<tr>
<td><strong>Hardware specifications and installation</strong></td>
<td></td>
</tr>
<tr>
<td>Compliance and safety manual</td>
<td>Provide regulatory information and the safety instructions that must be</td>
</tr>
<tr>
<td>CE DOCs</td>
<td>followed during installation.</td>
</tr>
<tr>
<td>Installation quick start</td>
<td>Guides you through initial installation and setup procedures to help</td>
</tr>
<tr>
<td></td>
<td>you quickly set up your device.</td>
</tr>
<tr>
<td>Installation guide</td>
<td>Provides a complete guide to switch installation and specifications.</td>
</tr>
<tr>
<td></td>
<td>swappable 150W power modules.</td>
</tr>
<tr>
<td>RPS Ordering Information for H3C Low-End Ethernet Switches</td>
<td>Helps you order RPSs for switches that can work with an RPS.</td>
</tr>
<tr>
<td>User manuals for RPSs</td>
<td>Describe the specifications, installation, and replacement of RPSs.</td>
</tr>
<tr>
<td>User manuals for interface cards</td>
<td>Describe the specifications, installation, and replacement of</td>
</tr>
<tr>
<td></td>
<td>expansion interface cards.</td>
</tr>
<tr>
<td>H3C Low End Series Ethernet Switches Pluggable Modules Manual</td>
<td>Describes the specifications of pluggable transceiver modules.</td>
</tr>
<tr>
<td>Pluggable SFP[SFP+]XFP Transceiver Modules Installation Guide</td>
<td>Describe the installation, and replacement of SFP/SFP+/XFP</td>
</tr>
<tr>
<td></td>
<td>transceiver modules.</td>
</tr>
<tr>
<td><strong>Software configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration guides</td>
<td>Describe software features and configuration procedures.</td>
</tr>
<tr>
<td>Command references</td>
<td>Provide a quick reference to all available commands.</td>
</tr>
<tr>
<td><strong>Operations and maintenance</strong></td>
<td></td>
</tr>
<tr>
<td>H3C Series Ethernet Switches Login</td>
<td>Helps you deal with switch login password loss.</td>
</tr>
<tr>
<td>Password Recovery Manual</td>
<td></td>
</tr>
<tr>
<td>Release notes</td>
<td>Provide information about the product release, including the version</td>
</tr>
<tr>
<td></td>
<td>history, hardware and software compatibility matrix, version</td>
</tr>
<tr>
<td></td>
<td>upgrade information, technical support information, and software</td>
</tr>
<tr>
<td></td>
<td>upgrading.</td>
</tr>
</tbody>
</table>

**Obtaining documentation**

You can access the most up-to-date H3C product documentation on the World Wide Web at [http://www.h3c.com](http://www.h3c.com).

Click the links on the top navigation bar to obtain different categories of product documentation:

- [Products & Solutions] – Provides information about products and technologies, as well as solutions.
- [Technical Support & Documents > Software Download] – Provides the documentation released with the software version.
Technical support

customer_service@h3c.com
http://www.h3c.com

Documentation feedback

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

IRF configuration

IRF overview ................................................................. 1
Benefits .................................................................................. 1
Application scenario .............................................................. 1
Basic concepts ......................................................................... 2
Establishment, operation, and maintenance of an IRF fabric .................................................. 3
  Connecting the IRF member switches ........................................... 3
  Topology collection .................................................................. 5
  Master election ......................................................................... 5
IRF fabric management and maintenance .......................................................... 6
IRF multi-active detection ............................................................ 8
IRF fabric configuration task list .................................................. 10
Configuring an IRF fabric .......................................................... 11
  Specifying a domain ID for an IRF fabric ...................................... 11
  Setting a member ID for a switch .............................................. 12
  Configuring IRF ports .............................................................. 13
  Specifying a priority for a member switch .................................... 14
  Configuring a description for a member switch ............................. 15
  Configuring load sharing criteria for IRF links ............................. 15
  Specifying the preservation time of the bridge MAC address ........... 16
  Enabling automatic system software updating ............................. 17
  Setting the IRF link down report delay ....................................... 18
  Configuring MAD detection ...................................................... 18
Accessing an IRF fabric ............................................................ 25
  Accessing the master ............................................................... 25
  Accessing a slave ..................................................................... 25
Displaying and maintaining an IRF fabric .......................................... 26
IRF fabric configuration examples ................................................. 26
  LACP MAD detection-enabled IRF configuration example ............. 26
  BFD MAD detection-enabled IRF configuration example .............. 29
  ARP MAD detection-enabled IRF configuration example .............. 31
Index ......................................................................................... 35
IRF configuration

NOTE:

• The Layer 3 Ethernet port in this chapter refers to an Ethernet port that can perform IP routing and inter-VLAN routing. You can set an Ethernet port as a Layer 3 Ethernet interface by using the `port link-mode route` command (see Layer 2—LAN Switching Configuration Guide).

• S5500-HI switches can form an IRF fabric only with S5500-HI switches.

IRF overview

The H3C Intelligent Resilient Framework (IRF) technology creates a large IRF fabric from multiple switches to provide data center class availability and scalability. IRF virtualization technology offers processing power, interaction, unified management and uninterrupted maintenance of multiple switches.

Benefits

IRF delivers the following benefits:

• Simplified topology and streamlined management. An IRF fabric appears as one node on the network. You can log in at any member switch to manage all members of the IRF fabric.

• High availability and reliability. The member switches in an IRF fabric work in 1:N redundancy. One member switch works as the master to manage and maintain the entire IRF fabric, and all other member switches process services and provide backup. If the master fails, all other member switches elect a new master among them to prevent service interruption. You can perform link aggregation not only for IRF links but also for physical links between the IRF fabric and its upper or lower layer devices for link redundancy.

• Network scalability and resiliency. You can increase ports, network bandwidth, and processing capability of an IRF fabric simply by adding member switches.

Application scenario

Figure 1 shows an IRF fabric that comprises two switches, which appear as a single node to the upper and lower layer devices.
Basic concepts

IRF member switch roles

IRF uses two member switch roles: master and slave.

When switches form an IRF fabric, they elect a master to manage the IRF fabric, and all other switches back up the master. When the master switch fails, the other switches automatically elect a new master from among them to avoid service interruption. For more information about master election, see “Master election.”

IRF port

An IRF port is a logical interface for the internal connection between IRF member switches. Each IRF member switch has two IRF ports: IRF-port 1 and IRF-port 2. An IRF port is activated when you bind a physical port to it.

Physical IRF port

Physical IRF ports are physical ports bound to an IRF port. They connect IRF member switches and forward IRF protocol packets and data packets between IRF member switches.

You can configure an SFP+ port on the front panel or a 10 GE port on the interface card as a physical IRF port.

IRF partition

IRF partition occurs when an IRF fabric splits into two or more IRF fabrics because of IRF link failures, as shown in Figure 2. The partitioned IRF fabrics operate with the same IP address and cause routing and forwarding problems on the network.
IRF merge

IRF merge occurs when two partitioned IRF fabrics re-unite or when you configure and connect two independent IRF fabrics to be one IRF fabric, as shown in Figure 3.

Member priority

Member priority determines the role that a member switch during the master election process. A member with a higher priority is more likely to be a master.

The priority of a switch defaults to 1. You can modify the priority at the command line interface (CLI).

Establishment, operation, and maintenance of an IRF fabric

IRF fabric management involves these stages: Connecting the IRF member switches, Topology collection, Master election, and IRF fabric management and maintenance.

Connecting the IRF member switches

Connection medium

To establish an IRF fabric, physically connect the physical IRF ports of member switches. The S5500-HI switches can provide 10-GE IRF connections through the SFP+ ports on the front panel and the XFP or SFP+ interface card at the rear of the chassis. The following are the interface cards that can provide physical IRF ports:

- Short-haul 2-port 10 GE CX4 interface card (LSPM1CX2P)
- 2-port 10 GE SFP+ interface card (LSPM2SP2P)
- 2-port 10 GE XFP interface card (LSPM1XP2P)
- 1-port 10 GE XFP interface card (LSPM1XP1P)

Use CX4/SFP+ cables or SFP+/XFP transceiver modules and fibers to connect the IRF member switches. If the IRF member switches are far away from one another, choose the SFP+ or XFP transceiver modules.
with optical fibers. If the IRF member switches are all in one equipment room, choose CX4 or SFP+ cables.

**NOTE:**
- For more information about SFP+ and XFP transceivers and CX4/SFP+ cables available for IRF connections supported by the S5500-HI switches, see *H3C S5500-HI Switch Series Installation Guide*.
- For more information about transceivers, see the *H3C Low End Series Ethernet Switches Pluggable Modules Manual*.
- The SFP+ modules and SFP+ cables available for this switch series are subject to change over time. For the most up-to-date list of SFP+ modules and cables, consult your H3C sales representative or technical support engineer.

**Connection requirements**

Bind one physical port, or for link redundancy and bandwidth expansion, multiple physical ports, to an IRF port (see “Configuring IRF ports”).

Table 1 shows the physical ports that can be used as IRF ports and the port use restrictions.

**Table 1 Physical IRF port requirements**

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Candidate physical IRF ports</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>S5500-34C-HI</td>
<td>• The two fixed SFP+ ports on the front panel</td>
<td>The physical ports of an IRF port must be located on the same interface card.</td>
</tr>
<tr>
<td></td>
<td>• Ports on the XFP or SFP+ interface cards on the rear panel</td>
<td>• The SFP+ port numbered 53 on the front panel and the physical ports on interface card 2 must be bound to the same IRF port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The SFP+ port numbered 54 on the front panel and the ports on interface card 1 must be bound to the same IRF port.</td>
</tr>
</tbody>
</table>

You can bind up to three physical IRF ports to an IRF port for link redundancy and load sharing.

As shown in Figure 4, IRF-Port1 on one switch can only be connected to the physical port bound with IRF-Port2 of a neighbor switch; otherwise, an IRF fabric cannot be formed.

**Figure 4 IRF fabric physical connection**

![IRF Fabric Physical Connection Diagram]
IRF topology

An IRF fabric typically adopts daisy chain connection or ring connection, as shown in Figure 5.

- A daisy chain connection is mainly used in a network where member switches are distributedly located.
- A ring connection is more reliable than the daisy chain connection. In a daisy chained IRF fabric, the failure of one link can cause the IRF fabric to partition into two independent IRF fabrics; where the failure of a link in a ring connection result in a daisy chain connection, not affecting IRF services.

Figure 5 IRF connections

Topology collection

Each member exchanges IRF hello packets with neighbors to collect the topology of the IRF fabric. The IRF hello packets carry the topology information, including IRF port connection states, member IDs, priorities, and bridge MAC addresses.

Each member records its known topology information locally. At the startup of a member switch, the member switch records topology information of the local device. When an IRF port of a member is up, the member switch performs the following operations:

1. Periodically sends its known topology information from this port.
2. When receiving the topology information from the directly connected neighbor, the member switch updates the local topology information.

After all member switches have obtained topology information (known as topology convergence), and the IRF fabric enters the master election stage.

Master election

Master election is held each time the topology changes, for example, when the IRF fabric is established, a new member switch is plugged in, the master switch fails or is removed, or the partitioned IRF fabrics merge.

The master is elected based on the following rules in descending order:
• The current master, even if a new member has a higher priority. (When an IRF fabric is being formed, and all member switches consider themselves as the master, and this rule is skipped)
• The switch with higher priority.
• The switch with the longest system up-time. (The member switches exchange system up-time in the IRF hello packets.)
• The switch with the lowest bridge MAC address.

The IRF fabric is formed on election of the master.

---

**NOTE:**

• During an IRF merge, the switches of the IRF fabric that fails the master election must reboot to re-join the IRF fabric that wins the election. The reboot can be automatically performed.
• After a master election, all slave member switches initialize and reboot with the configuration on the master, and their original configuration, even if has been saved, will be lost.

---

**IRF fabric management and maintenance**

After the IRF fabric is established, you can access the master from any member switch to manage all the resources of the member switches.

**Member ID**

An IRF fabric uses member IDs to uniquely identify its members. Member IDs are also included in interface names and file system names for interface and file system identification. To guarantee the operation of the IRF fabric, you must assign each member switch a unique member ID.

**Interface naming conventions**

The interfaces are named in the format of *member ID/subslot number/interface serial number*, where

• The member ID identifies the IRF member switch on which the interface resides. If the switch is standalone, the member ID defaults to 1. If the standalone switch was once an IRF member switch, it uses the same member ID as it was in the IRF fabric.
• The subslot number is the number of the subslot in which the interface card resides. For the S5500-HI series, subslot number of the fixed port on the front panel is 0, and the subslot numbers of the interface card slots 1 and 2 are 1 and 2 respectively.
• The interface serial number depends on the number of interfaces provided by the switch. Look at the number on the silkscreen on the interface card for the number of supported interfaces.

For example, on the standalone switch **Sysname**, GigabitEthernet 1/0/1 represents the first fixed port on the front panel. Set its link type to trunk:

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

For another example, on the IRF fabric **Master**, GigabitEthernet 3/0/1 represents the first fixed port on the front panel of member switch 3. Set its link type to trunk:

```
<Master> system-view
[Master] interface gigabitethernet 3/0/1
[Master-GigabitEthernet3/0/1] port link-type trunk
```
File system naming conventions

On a standalone switch, you can use the name of storage device to access its file system. For more information about storage device naming conventions, see Fundamentals Configuration Guide.

On an IRF fabric, you can also use the name of storage device to access the file system of the master. To access the file system of any other member switch, use the name in the following format: Member-ID#Storage-device-name. For example:

1. To access the test folder under the root directory of the Flash on the master switch, perform the following steps:
   <Master> mkdir test
   ...
   %Created dir flash:/test.
   <Master> dir
   Directory of flash:/
   0   -rw-  19701664  Apr 26 2000 13:44:57   test.bin
   1   -rw-      2445  Apr 26 2000 15:18:19   config.cfg
   2   drw-         -  Jul 14 2008 15:20:35   test
   515712 KB total (513742 KB free)

2. To create and access the test folder under the root directory of the Flash on member switch 3, perform the following steps:
   <Master> mkdir slot3#flash:/test
   %Created dir slot3#flash:/test.
   <Master> cd slot3#flash:/test
   <Master> pwd
   slot3#flash:/test
   Or:
   <Master> cd slot3#flash:
   <Master> mkdir test
   %Created dir slot3#flash:/test.

3. To copy the test.app file on the master to the root directory of the Flash on member switch 3, perform the following steps:
   <Master> pwd
   slot3#flash:

   //The current working path is the root directory of the Flash on slave 3.
   <Master> cd flash:
   <Master> pwd
   flash:

   //The current working path is the root directory of the Flash on the master.
   <Master> copy test.app slot3#flash:/
   Copy flash:/test.app to slot3#flash:/test.app?[Y/N]:y
   %Copy file flash:/test.app to slot3#flash:/test.app...Done.

Configuration file synchronization

IRF uses a strict configuration file synchronization mechanism to make sure that all switches in an IRF fabric can work as a single node on the network, and to make sure that after the master fails, the other switches can operate normally.
• When a slave switch starts up, it automatically gets and runs the master’s configuration file. If all switches in an IRF fabric start up simultaneously, the slave switches get and run the master’s startup configuration file.

• Any configuration you made on the IRF fabric is stored on the master and synchronized in real time to each member switch. When you save the current configuration to the startup configuration file of the master by using the `save` command, all slave switches execute the same saving operation.

This real-time configuration synchronization ensures that all the IRF member switches keep the same configuration file. If the master fails, all the other switches can still operate with the same configuration file.

**IRF fabric topology maintenance**

As soon as a member switch is down or an IRF link is down, its neighbor switches broadcast the leaving of the switch to other members. When a member switch receives the leave message, it looks up its IRF topology database to determine whether the leaving switch is the master. If yes, the member switch starts a master election and updates its IRF topology database. If the leaving switch is not a master, the member switch directly updates its IRF topology database.

**NOTE:**

An IRF port goes down only when all its physical IRF ports are down.

**IRF multi-active detection**

An IRF link failure causes an IRF fabric to split in two IRF fabrics operating with the same Layer 3 configurations, such as the same IP address. To avoid IP address collision and network problems, IRF uses multi-active detection (MAD) mechanism to detect the presence of multiple identical IRF fabrics and handle collisions. MAD provides the following functions:

**Detection**

MAD detects identical active IRF fabrics with the same global configuration by extending the Link Aggregation Control Protocol (LACP), the Bidirectional Forwarding Detection (BFD) protocol, or the Gratuitous Address Resolution (ARP) protocol. For more information, see “Configuring MAD detection.”

**NOTE:**

For more information about LACP, see *Layer 2 — LAN Switching Configuration Guide*; for more information about BFD, see *High Availability Configuration Guide*; for more information about gratuitous ARP, see *Layer 3 — IP Services Configuration Guide*.

**Collision handling**

If multiple identical active IRF fabrics are detected, only the IRF fabric that has the lowest master ID can operate in active state and forward traffic. MAD sets all other IRF fabrics in recovery state (disabled) and shuts down all physical ports but the IRF ports and other ports you have specified with the `mad exclude interface` command. See Figure 6.

**Failure recovery**

An IRF link failure causes an IRF fabric to divide into two fabrics and multi-active collision occurs. When the system detects the collision, it holds a master election between the two collided IRF fabrics. The IRF fabric whose master’s member ID is smaller prevails and operates normally. The state of the other IRF fabric transits to the recovery state and temporarily cannot forward data packets. In this case, recover the
IRF fabric by repairing the IRF link first (The switch tries to automatically repair the failed IRF links. If the reparation fails, manually repair the failed links.)

When the link is recovered, the IRF fabric in recovery state automatically reboots, and then the IRF fabrics both in active state and in recovery state automatically merge into one. Service ports that were shut down and belonged to the IRF fabric in recovery state automatically restore their original physical state, and the whole IRF fabric recovers, as shown in Figure 6.

**Figure 6 Recover the IRF fabric when IRF link failure occurs**

<table>
<thead>
<tr>
<th>IP network</th>
<th>IRF 1 (Active)</th>
<th>IRF 2 (Recovery)</th>
<th>After the IRF link is recovered</th>
<th>IRF 1 (Active)</th>
<th>IRF 2 (Recovery)</th>
<th>IRF merge</th>
</tr>
</thead>
</table>

If the IRF fabric in active state fails due to exceptions (a member fails or link failure occurs, for example) before the IRF link is recovered, as shown in Figure 7, enable IRF fabric 2 (in recovery state) at the CLI by executing the `mad restore` command. Then, the state of IRF fabric 2 changes from recovery to active without the need of rebooting and takes over IRF fabric 1. Repair the IRF links. When the IRF link failure is recovered, the two IRF fabrics merge. The priorities of two masters from the two IRF fabrics are compared, and the IRF fabric whose master’s priority is higher can operate normally. Members (only one in this example) of the IRF fabric whose master’s priority is lower reboot themselves, and the join the other IRF fabric to complete the IRF fabric merge. After that, the original IRF fabric recovers.
Figure 7 Recover the IRF fabric when the IRF link failure occurs and the IRF fabric in active state fails

IRF fabric configuration task list

Before configuring an IRF fabric, plan the roles and functions of all member switches. H3C recommends the configuration procedure in Figure 8.

Figure 8 IRF configuration flow chart

You can connect physical IRF ports after activating IRF port configurations. After the device detects that the IRF ports are connected normally, master election is started immediately, and then the elected slave switches reboot automatically.

After an IRF fabric is formed, you can configure and manage the IRF fabric by logging in to any device in the IRF.

Complete the following tasks to configure an IRF fabric:
<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying a domain ID for an IRF fabric</td>
<td>Optional</td>
</tr>
<tr>
<td>Setting a member ID for a switch</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring IRF ports</td>
<td>Required</td>
</tr>
<tr>
<td>Specifying a priority for a member switch</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring a description for a member switch</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring load sharing criteria for IRF links</td>
<td>Optional</td>
</tr>
<tr>
<td>Specifying the preservation time of the bridge MAC address</td>
<td>Optional</td>
</tr>
<tr>
<td>Enabling automatic system software updating</td>
<td>Optional</td>
</tr>
<tr>
<td>Setting the IRF link down report delay</td>
<td>Optional</td>
</tr>
<tr>
<td>Connecting the physical IRF ports of switches and making sure that</td>
<td></td>
</tr>
<tr>
<td>the physical IRF ports are interconnected (a ring connection is</td>
<td></td>
</tr>
<tr>
<td>recommended).</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring MAD detection**

| Configuring LACP MAD                                               | Use one or more approaches |
| Configuring BFD MAD                                                | H3C recommends that you configure the MAD detection after establishing the IRF fabric. |
| Configuring ARP MAD                                                |                           |
| Excluding a port from the shut down action upon detection of multi-active collision | Optional |
| Manually changing the state of an IRF fabric from recovery to active | Optional |

**Accessing an IRF fabric**

| Accessing the master                                               | Required    |
| Accessing a slave                                                  | Optional    |

**Configuring an IRF fabric**

**Specifying a domain ID for an IRF fabric**

**Introduction to IRF domains**

IRF uses IRF domain IDs for uniquely identifying IRF fabrics. IRF domain IDs prevent IRF fabrics from interfering with one another.

As shown in Figure 9, Switch A and Switch B form IRF fabric 1, and Switch C and Switch D form IRF fabric 2. The fabrics have LACP MAD detection links between them. When a member switch in one IRF fabric receives an extended LACP packet for MAD detection, it looks at the domain ID in the packet to see whether the packet is from the local IRF fabric or from a different IRF fabric. Then, the switch can handle the packet correctly.
Assigning a domain ID to an IRF fabric

Follow these steps to assign a domain ID to an IRF fabric:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Assign a domain ID to the IRF fabric</td>
<td>irf domain domain-id</td>
<td>Required if LACP MAD or ARP MAD is adopted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional if BFD MAD is adopted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the domain ID of an IRF fabric is 0.</td>
</tr>
</tbody>
</table>

**NOTE:**
- You must assign a domain ID for an IRF fabric before enabling LACP MAD or ARP MAD detection.
- H3C recommends that you assign the same domain ID to the members of the same IRF fabric; otherwise, the LACP MAD or ARP MAD detection function cannot function properly.
- To display the domain IDs and verify your configuration, execute the `display irf` command in any view.

Setting a member ID for a switch

An IRF fabric uses member IDs to uniquely identify its members. A lot of information and configurations relate to member IDs, such as port (physical or logical) numbers, configurations on ports, and member priorities.

After you change the member ID of a switch,
If you do not reboot the switch, the original member ID still takes effect and all physical resources are identified by the original member ID. In the configuration file, only the IRF port numbers, configurations on IRF ports, and priority of the switch change with the member ID, other configurations do not change.

If you save the current configuration and reboot the switch, the new member ID takes effect and all physical resources are identified by the new member ID. In the configuration file, only the IRF port numbers, configurations on IRF ports, and priority of the switch still take effect, other configurations (such as configuration for physical IRF ports) no longer take effect and you need to configure them again.

Follow these steps to set a member ID for a switch:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Set a member ID for a switch</td>
<td>irf member member-id renumber new-member-id</td>
<td>Optional The member ID of a switch defaults to 1</td>
</tr>
</tbody>
</table>

⚠️ CAUTION:
- Member ID changes take effect at the reboot of the switch.
- Change member IDs for the switches in an IRF fabric with caution. The change might cause configuration change and even data loss. For example, three members (of the same switch model) with the member IDs of 1, 2 and 3 are connected to an IRF port. Suppose that each member has several ports: change the member ID of switch 2 to 3, change that of switch 3 to 2, reboot both switches, and add them into the IRF fabric again. Then switch 2 will use the original port configurations of device 3, and switch 3 will use those of switch 2.

Configuring IRF ports

IRF ports are logical ports. To use the IRF function on a switch, you must bind its IRF ports with physical IRF ports and activate the IRF configuration on the switch.

Follow these steps to configure IRF ports:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Enter physical IRF port view</td>
<td>interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>Shut down the port</td>
<td>shutdown</td>
<td>Required</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td></td>
</tr>
<tr>
<td>Create an IRF port and enter IRF port view</td>
<td>irf-port member-id/port-number</td>
<td></td>
</tr>
<tr>
<td>Bind the physical IRF port to the IRF port</td>
<td>port group interface interface-type interface-number [ mode { enhanced</td>
<td>normal } ]</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td></td>
</tr>
</tbody>
</table>
To do… | Use the command… | Remarks
---|---|---
Enter physical IRF port view | `interface interface-type interface-number` | —
Bring up the port | `undo shutdown` | Required
Return to system view | `quit` | —
Save the current configuration | `save` | Required
Activate configurations on all IRF ports on the switch | `irf-port-configuration active` | Optional

**NOTE:**
- To realize IRF link redundancy and load sharing and increase the bandwidth and reliability of IRF links, bind one IRF port to multiple physical IRF ports by repeatedly executing the `port group interface` command. You can bind up to three physical IRF ports to an IRF port.

- Before binding a physical IRF port to an IRF port or canceling such a binding, you must manually disable the physical IRF port (that is, execute the `shutdown` command on the port). After finishing your operation, you should manually bring up the physical IRF port (that is, execute the `undo shutdown` command on the port). The system may prevent you to shut down a port to avoid anomalies. Then, follow the system instructions to disable its peer port.

- If you need to shut down two physical IRF ports of an IRF link, execute the `shutdown` command first on the port that is on the master switch or close to the master switch, and then on the other port that is comparatively far from the master switch.

- If you set the IRF operating mode of the physical IRF port by providing the `mode` keyword when you bind the physical port to the IRF port, you must configure its directly connected physical IRF port to work in the same mode.

- If you need to unplug the interface card on which an physical IRF port reside after an IRF fabric is established, unplug cables for IRF connection, or execute the `shutdown` command on the physical IRF port to disable the port, and then unplug the interface card.

- If a common Ethernet interface functions as a physical IRF port and is bound to an IRF port, you can only execute the `cfd`, `default`, `shutdown`, `description`, and `flow-interval` commands on the physical IRF port. For more information about these commands, see *Layer 2—LAN Switching Command Reference*.

### Specifying a priority for a member switch

The greater the priority value, the higher the priority. A member with a higher priority is more likely to be a master.

Follow these steps to specify a priority for a member switch:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
</table>
Enter system view | `system-view` | — |
### Configuring a priority for a member of an IRF fabric

**To do...**  
Specify a priority for a member of an IRF fabric  

**Use the command...**  
`irf member member-id priority priority`  

**Remarks**  
Optional  
The priority of a member defaults to 1

---

**NOTE:**  
The setting of priority takes effect right after your configuration without the need of rebooting the switch.

### Configuring a description for a member switch

You can configure a description for a member switch to identify its physical location, or for any other management purpose.

*Follow these steps to configure a description for a member switch:*

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
</tbody>
</table>
| Configure the description of a member | `irf member member-id description text` | Optional  
Not configured by default. |

### Configuring load sharing criteria for IRF links

When an IRF port is bound with two or more physical IRF ports, there are multiple IRF links among IRF fabrics.

Determine how traffic is load-shared among members by configuring load sharing criteria for IRF links. The criteria can be information carried in packets, such as IP addresses, MAC addresses, and any combination of them. The criteria can also be packet types, such as Layer 2 and Layer 3.

Configure global (in system view) or port-specific (in IRF port view) load sharing criteria for IRF links:

- If you configure the load sharing criteria in system view, the configuration is effective for IRF links on all IRF ports.
- If you configure load sharing criteria in IRF port view, the configuration is effective for IRF links on this IRF port.
- An IRF port preferentially uses the port-specific load sharing criteria. If no port-specific load sharing criteria is available, it uses the global load sharing criteria.

**NOTE:**
- The load sharing criterion or criteria you configured in the same view overwrite the old ones, if any.
- If you configure a load sharing criterion not supported by the switch, you will be prompted that the switch does not support the criterion.
- Before configuring the load sharing criteria, bind IRF ports to corresponding physical IRF ports. Otherwise, load sharing criterion configuration fails.

### Configuring global load sharing criteria

Follow these steps to configure the global IRF link load sharing criteria:
To do… | Use the command… | Remarks
--- | --- | ---
Enter system view | system-view | —

Configure the global IRF link load sharing criteria | irf-port load-sharing mode (destination-ip | destination-mac | source-ip | source-mac) * | Optional
Optional
By default, the global IRF link load sharing criteria are packet types.

### Configuring port-specific load sharing criteria

Follow these steps to configure the port-specific load sharing criteria:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
</table>
Enter system view | system-view | — |
Enter IRF port view | irf-port member-id/port-number | — |

Configure the port-specific load sharing criteria | irf-port load-sharing mode (destination-ip | destination-mac | source-ip | source-mac) * | Optional
Optional
By default, the port-specific load sharing criteria are packet types.

### Specifying the preservation time of the bridge MAC address

A switch uses the bridge MAC address when it communicates with the external networks as a bridge. Some Layer 2 protocols (like LACP) use bridge MAC addresses to identify different switches. Therefore, a bridge device on your network must have a unique bridge MAC address. If two switches on your network have the same bridge MAC addresses, bridge MAC address collision occurs and the communication fails.

An IRF fabric communicates with external networks as a single device; therefore, it also has a bridge MAC address. Typically, an IRF fabric uses the bridge MAC address of the master as its bridge MAC address.

Bridge MAC address collision causes communication failure, and bridge MAC address switching causes traffic interruption. Therefore, configure the preservation time of the bridge MAC address of the IRF fabric:

- **Preserve for 6 minutes:** When the master leaves, the bridge MAC address does not change within six minutes. If the master does not come back when the preserve time is expiring, the IRF fabric uses the bridge MAC address of the newly elected master as its bridge MAC address. If the master leaves the IRF for a short time due to device reboot or link failure, this configuration can reduce unnecessary switch of bridge MAC address and thus avoid traffic interruption.
- **Preserve permanently:** No matter whether the master leaves the IRF fabric or not, the bridge MAC address of the IRF fabric remains unchanged.
- **Not preserved:** As soon as the master leaves, the IRF fabric uses the bridge MAC address of the newly elected master as its bridge MAC address.

Follow these steps to specify the preservation time of the bridge MAC address of an IRF fabric:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
</table>
Enter system view | system-view | — |
<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the bridge MAC address of the IRF fabric to be preserved permanently when the master leaves</td>
<td><code>irf mac-address persistent always</code></td>
<td>Optional</td>
</tr>
<tr>
<td>Specify the preservation time of the bridge MAC address of the IRF fabric as 6 minutes when the master leaves</td>
<td><code>irf mac-address persistent timer</code></td>
<td>By default, the IRF fabric preserves its bridge MAC address for 6 minutes after the master leaves.</td>
</tr>
<tr>
<td>Configure that the bridge MAC address of the IRF fabric changes as soon as the master leaves</td>
<td><code>undo irf mac-address persistent</code></td>
<td></td>
</tr>
</tbody>
</table>

⚠️ **CAUTION:**
- Bridge MAC address change may cause a temporary traffic interruption.
- If two IRF fabrics have the same bridge MAC address, they cannot be merged into one IRF fabric.
- If you use ARP MAD together with the spanning tree feature for an IRF fabric, enable the IRF fabric to change its bridge MAC address as soon as the master leaves by using the `undo irf mac-address persistent` command.

### Enabling automatic system software updating
- When you add a switch to the IRF fabric, the automatic system software updating function compares the software versions of the switch and the IRF master. If the versions are different, the switch automatically downloads the system software image from the master, sets the downloaded file as the system software image for the next reboot, and automatically reboots with the new system software to re-join the IRF fabric.
- If this function is disabled, you must manually make sure that the joining switch uses the same system software as the master switch. If not, the switch cannot join the IRF fabric.

Follow these steps to enable an IRF fabric to automatically synchronize the system software of the master to the switch you are adding to the IRF fabric:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
<tr>
<td>Enable an IRF fabric to automatically synchronize the system software image of the master to the switch you are adding to the IRF fabric</td>
<td><code>irf auto-update enable</code></td>
<td>Optional Enabled by default.</td>
</tr>
</tbody>
</table>

⚠️ **CAUTION:**
- Check that the switch has efficient space for the new system software.
- Changing the operating mode from IRF to standalone can cause the loss of the `irf auto-update enable` command configuration, even if you have saved the configuration.
Setting the IRF link down report delay

You can avoid link flapping causing frequent IRF splits and merges during a short time by configuring the IRF ports to delay reporting link down events. An IRF port thus works as follows:

- When the IRF link changes from up to down, the port does not immediately report the change to the IRF fabric. If the IRF link state is still down when the delay time is reached, the port reports the change to the IRF fabric.
- When the IRF link changes from down to up, the link layer immediately reports the event to the IRF fabric.

Follow these steps to set the IRF link down report delay:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
</tbody>
</table>
| Set the IRF link down report delay | irf link-delay interval | Optional

The function is disabled by default.

The recommended value range (in milliseconds) is 200 to 500. The greater the interval, the slower the service recovery.

Configuring MAD detection

You have the following MAD mechanisms for detecting multi-active collisions in different network scenarios:

- LACP MAD
- BFD MAD
- ARP MAD.

These MAD detection mechanisms operate independently, and you can configure all of them for an IRF fabric.

Configuring LACP MAD

1. LACP MAD detection mechanism

With LACP MAD, an IRF member switch sends extended LACP data units (LACPDUs) with a type length value (TLV) that conveys the domain ID and active ID of the IRF fabric for detecting an IRF split. The domain ID uniquely identifies an IRF device in the network, and the active ID is identical to the member ID of the master switch in the IRF fabric.

An IRF member switch compares the domain ID and the active ID in each received extended LACPDU with its domain ID and active ID:

- If the domain IDs are different, the extended LACPDU is from a different IRF fabric, and the switch does not continue to process the extended LACPDU with the MAD mechanism.
- If the domain IDs are the same, the switch 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 operating normally.

2. Network requirements
Every IRF member switch has a link with an intermediate switch, and all these links form a dynamic link aggregation group, as shown in Figure 10.

The intermediate switch must be an H3C switch capable of handling extended LACPDUs that carry the Active ID field. For more information about LACP and the support of the switch for extended LACPDUs, see Layer 2 — LAN Switching Configuration Guide.

⚠️ CAUTION: ⚠️

If the intermediate switch is in an IRF fabric, you must assign this fabric a different domain ID than the LACP MAD-enabled IRF fabric to avoid false detection of IRF partition.

3. Configuring LACP MAD detection

Configure LACP MAD detection by following these steps:

- Create an Layer 2 aggregate interface or an Layer 3 aggregate interface (also required on the intermediate switch);
- Configure the aggregation group to work in dynamic aggregation mode; (also required on the intermediate switch)
- Enable LACP MAD detection on the dynamic aggregate interface;
- Add member ports to the aggregation group.(also required on the intermediate switch)

Follow these steps to configure LACP MAD detection:
<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Assign a domain ID to the IRF fabric</td>
<td>irf domain domain-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the domain ID of an IRF fabric is 0.</td>
</tr>
<tr>
<td>Create an aggregate interface and enter aggregate interface view</td>
<td>interface bridge-aggregation interface-number</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Enter Layer 2 aggregate interface view</td>
<td>Use either command.</td>
</tr>
<tr>
<td></td>
<td>interface route-aggregation interface-number</td>
<td></td>
</tr>
<tr>
<td>Configure the aggregation group to work in dynamic aggregation mode</td>
<td>link-aggregation mode dynamic</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the aggregation group works in static aggregation mode.</td>
</tr>
<tr>
<td>Enable LACP MAD detection</td>
<td>mad enable</td>
<td>—</td>
</tr>
<tr>
<td>Return to system view</td>
<td>quit</td>
<td>—</td>
</tr>
<tr>
<td>Enter Layer 2 Ethernet port view or Layer 3 Ethernet port view</td>
<td>interface interface-type interface-number</td>
<td>—</td>
</tr>
<tr>
<td>Assign the current Ethernet interface to the specified aggregation group</td>
<td>port link-aggregation group number</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Configuring BFD MAD**

1. **BFD MAD detection mechanism**

   BFD MAD is implemented with the BFD protocol. To configure BFD MAD detection, configure a MAD IP address on a BFD-enabled Layer 3 interface for each member switch. This MAD address identifies the member during BFD MAD detection. The MAD IP addresses assigned to the member switches must belong to the same network segment.

   - When the IRF fabric operates normally, only the MAD IP address of the master is effective and the BFD session is down.
   - When the IRF fabric partitions, the MAD IP addresses of the masters in different IRF fabrics become effective to activate the BFD sessions to detect for multi-active IRF fabric collision.

2. **Network requirements**

   BFD MAD detection can be achieved with or without intermediate switches. The commonly used networking diagram is as shown in Figure 11: there must be a BFD MAD detection link among all members, and the interfaces connected by this link must belong to the same VLAN. In VLAN interface view, assign different IP addresses on the same network segment for different member switches.
**CAUTION:**

A Layer 3 interface used for BFD MAD must be dedicated. Do not configure any other services on a Layer 3 interface with BFD MAD enabled. Otherwise, both the configured services and the BFD MAD detection function may be affected.

**Figure 11 Network diagram**

3. **Configuring BFD MAD detection**

Configure BFD MAD detection by following these steps:

- Create a VLAN dedicated to BFD MAD detection. This is also required on the intermediate switch, if it exists.
- Select the physical IRF ports to be used for BFD MAD detection (at least one on each member switch) and add them into the detection-dedicated VLAN. This is also required on the intermediate switch if it exists.
- Create VLAN interfaces for the detection-dedicated VLAN, enable BFD MAD detection on these interfaces, and then assign MAD IP addresses for them.

Follow these steps to configure BFD MAD:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td></td>
</tr>
<tr>
<td>Create a new VLAN dedicated to BFD MAD detection</td>
<td><code>vlan vlan-id</code></td>
<td>Required The default VLAN on the switch is VLAN 1.</td>
</tr>
<tr>
<td>Return to system view</td>
<td><code>quit</code></td>
<td></td>
</tr>
<tr>
<td>To do…</td>
<td>Use the command…</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Enter Ethernet interface view</td>
<td><code>interface interface-type interface-number</code></td>
<td>—</td>
</tr>
<tr>
<td>Access port</td>
<td><code>port access vlan vlan-id</code></td>
<td>Required</td>
</tr>
<tr>
<td>Trunk port</td>
<td><code>port trunk permit vlan vlan-id</code></td>
<td>You can select one approach according to the port type. BFD MAD detection has no requirement on the link type of the detection port, and you do not need to modify the current link type. By default, the port is an access port.</td>
</tr>
<tr>
<td>Hybrid port</td>
<td>`port hybrid vlan vlan-id { tagged</td>
<td>untagged }`</td>
</tr>
<tr>
<td>Return to system view</td>
<td><code>quit</code></td>
<td>—</td>
</tr>
<tr>
<td>Enter VLAN interface view</td>
<td><code>interface vlan-interface interface-number</code></td>
<td>—</td>
</tr>
<tr>
<td>Enable BFD MAD</td>
<td><code>mad bfd enable</code></td>
<td>Required. Disabled by default.</td>
</tr>
<tr>
<td>Configure a MAD IP address for the VLAN interface on the specified member</td>
<td>`mad ip address ip-address { mask</td>
<td>mask-length } member member-id`</td>
</tr>
</tbody>
</table>

**NOTE:**

- A VLAN interface enabled with BFD MAD detection and the interfaces of this VLAN do not support any Layer 2 and Layer 3 protocol applications, including ARP and LACP.
- You cannot enable BFD MAD detection on VLAN-interface 1.
- The MAD function is mutually exclusive with VPN. Layer 3 interfaces with BFD MAD enabled cannot be bound with VPN.
- The MAD function is mutually exclusive with the spanning tree function. Layer 3 interfaces with BFD MAD enabled cannot be enabled with the spanning tree function.
- You can assign the MAD IP address for an interface used for BFD MAD detection only with the `mad ip address` command. Do not configure other IP addresses—including common IP address or VRRP virtual IP address configured with the `ip address` command—for the interface.
- The MAD IP addresses to be assigned to the member switches and the IP addresses of the member switches cannot belong to the same network segment.

**Configuring ARP MAD**

1. **ARP MAD detection mechanism**

   With ARP MAD, an IRF member switch sends extended gratuitous ARP packets that convey the domain ID and active ID of the IRF fabric for detecting an IRF split. The domain ID uniquely identifies an IRF fabric in the network, and the active ID is identical to the member ID of the master switch in the IRF fabric.

   An IRF member switch compares the domain ID and the active ID in each received extended gratuitous ARP packet with its domain ID and active ID:
   - If the domain IDs are different, the extended gratuitous ARP packet is from a different IRF fabric, and the switch does not continue to process the packet with the MAD mechanism.
If the domain IDs are the same, the switch 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 operating normally.

2. Network requirements

Set up ARP MAD links between neighbor IRF member switches, or more commonly, between each IRF member switch and an intermediate switch (see Figure 12). If an intermediate switch is used, you must enable MSTP on the intermediate switch and the IRF fabric.

⚠️ **CAUTION:**

If the intermediate switch is in an IRF fabric, you must assign this fabric a different domain ID than the ARP MAD-enabled IRF fabric to avoid false detection of IRF partition.

**Figure 12 Network diagram**

3. Configuring ARP MAD detection

Follow these steps to configure ARP MAD:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Assign a domain ID to the IRF fabric</td>
<td>irf domain domain-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the domain ID of an IRF fabric is 0.</td>
</tr>
<tr>
<td>Create a new VLAN dedicated to ARP MAD detection</td>
<td>vlan vlan-id</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default VLAN on the switch is VLAN 1.</td>
</tr>
</tbody>
</table>

23
To do… | Use the command… | Remarks
--- | --- | ---
Return to system view | quit | —
Enter Ethernet interface view | interface interface-type interface-number | —
Assign the port to the VLAN dedicated for ARP MAD detection
Access port | port access vlan vlan-id | Required
Trunk port | port trunk permit vlan vlan-id | You can select one approach according to the port type.
Hybrid port | port hybrid vlan vlan-id { tagged | untagged } | ARP MAD detection has no requirement on the link type of the detection port, and you do not need to modify the current link type. By default, the port is an access port.
Return to system view | quit | —
Enter VLAN interface view | interface vlan-interface interface-number | —
Assign the interface an IP address | ip address ip-address { mask | mask-length } | Required
No IP address is assigned to any VLAN interface by default.
Enable ARP MAD | mad arp enable | Required
By default, ARP MAD is disabled.

Excluding a port from the shut down action upon detection of multi-active collision

By default all service ports of an IRF fabric except the IRF ports are shut down when the IRF fabric transits to recovery state upon detection of a multi-active collision. If a port must be kept in up state for special purposes such as telnet connection, exclude it from the shut down action.

Follow these steps to configure a port not to shut down when the IRF fabric transits to recovery state:

To do… | Use the command… | Remarks
--- | --- | ---
Enter system view | system-view | —
Configure a service port not to shut down when the IRF fabric transits to recovery state | mad exclude interface interface-type interface-number | Required
When an IRF fabric transits to recovery state, all its service ports are shut down by default.

**NOTE:**
- Physical IRF ports are not shut down when the IRF fabric transits to recovery state.
- If a certain VLAN interface is required to go on receiving and sending packets (for example, the VLAN interface is used for remote login) after the IRF fabric transits to recovery state, you need to configure this VLAN interface and its corresponding Layer 2 Ethernet interface not to shut down when the IRF fabric transits to recovery state. However, if the VLAN interface is up in the IRF fabric in active state, IP collision will occur in your network.
Manually changing the state of an IRF fabric from recovery to active

Follow these steps to manually change the state of an IRF fabric from recovery to active:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>Change the state of an IRF fabric</td>
<td>mad restore</td>
<td>Required</td>
</tr>
<tr>
<td>from recovery to active</td>
<td></td>
<td>IMPORTANT: See “Failure recovery” for the application scenario of this command.</td>
</tr>
</tbody>
</table>

Accessing an IRF fabric

Accessing the master

Access an IRF fabric in either of the following two ways:

- Local login—Log in through the AUX or console port of a member switch.
- Remote login—Remotely log in at a Layer 3 Ethernet interface on any member switch through Telnet, Web, or SNMP.

When you log in to an IRF fabric, you are placed at the CLI of its master, regardless of through which member switch you are logged in. The master switch is the configuration and control center of the IRF fabric. You make configuration for the IRF fabric on the master, and the IRF fabric synchronizes the configurations to all slaves.

Accessing a slave

You can log in to the CLI of a member switch to display its configurations and debug the switch. When you switch from the master’s CLI to the slave’s CLI, you are placed in the user view of the slave switch and the command prompt changes to <Sysname-Slave#X>, where X represents the member ID of the slave switch, for example, <Sysname-Slave#2>. You can perform the following commands at the CLI of a slave switch:

- display
- quit
- return
- system-view
- debugging
- terminal debugging
- terminal trapping
- terminal logging

To return to the CLI of the master switch, use the quit command.

Follow these steps to log in to a slave switch:

<table>
<thead>
<tr>
<th>To do…</th>
<th>Use the command…</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td></td>
</tr>
</tbody>
</table>
To do... | Use the command... | Remarks
--- | --- | ---
Log in to a slave switch | `irf switch-to member-id` | Required

By default, you are placed at the CLI of the master when you log in to the IRF fabric.

**NOTE:**
An IRF fabric allows 16 concurrent VTY log-in users at most. And the maximum number of allowed console log-in users is equal to the number of IRF members.

### Displaying and maintaining an IRF fabric

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display related information about the IRF fabric</td>
<td>`display irf [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display topology information about the IRF fabric</td>
<td>`display irf topology [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display configuration information of all IRF member switches</td>
<td>`display irf configuration [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display the load sharing criteria for IRF links</td>
<td>`display irf-port load-sharing mode [ irf-port [ member-id/port-number</td>
<td>begin</td>
</tr>
<tr>
<td>Display the master/slave switchover states of IRF members</td>
<td>`display switchover state [ slot member-id</td>
<td>begin</td>
</tr>
<tr>
<td>Display MAD configuration</td>
<td>`display mad [ verbose</td>
<td>begin</td>
</tr>
</tbody>
</table>

### IRF fabric configuration examples

#### LACP MAD detection-enabled IRF configuration example

**Network requirements**

The number of PCs on the enterprise network (see Figure 13) is outgrowing the number of ports available on the access switches. To address business growth, the number of ports at the access layer must be increased while protecting the current investments of the customer, and maintaining the ease of management and maintenance.
Configuration considerations

- To increase the number of access ports, additional devices are needed. In this example, Device B is added.
- To address the requirements for high availability, ease of management and maintenance, use IRF2 technology to create an IRF fabric with Device A and Device B at the access layer.
- To offset the risk of IRF fabric partition, configure MAD to detect multi-active collisions. In this example, LACP MAD is adopted because there are many access switches. For LACP MAD, use an intermediate switch that supports extended LACPDUs.

Configuration procedure

**NOTE:**
This example assumes that the system names of Device A, Device B and Device C are DeviceA, DeviceB, and DeviceC respectively before the IRF fabric is formed.

1. Set member IDs
   # Keep the default member ID of Device A unchanged.
   # Set the member ID of Device B to 2.
   <DeviceB> system-view
   [DeviceB] irf member 1 renumber 2
   Warning: Renumbering the switch number may result in configuration change or loss. Continue? [Y/N]:y
   [DeviceB]

2. Power off the two devices and connect IRF links and LACP MAD detection links according to Figure 13. Then power on the two devices.
   # Create IRF port 2 on Device A, and bind it to the physical IRF port Ten-GigabitEthernet 1/1/2. Then save the configuration.
   <DeviceA> system-view
   [DeviceA] interface ten-gigabitethernet 1/1/2
   [DeviceA-Ten-GigabitEthernet1/1/2] shutdown
[DeviceA] irf-port 1/2
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet 1/1/2
[DeviceA] interface ten-gigabitethernet 1/1/2
undo shutdown
save

# Create IRF port 1 on Device B, and bind it to the physical IRF port Ten-GigabitEthernet 2/1/1. Then save the configuration.
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/1/1
shutdown
irf-port 2/1
port group interface ten-gigabitethernet 2/1/1
quit
interface ten-gigabitethernet 2/1/1
undo shutdown
save

# Activate IRF port configuration on Device A.
[DeviceA-Ten-GigabitEthernet1/1/2] quit
irf-port-configuration active

# Activate IRF port configuration on Device B.
[DeviceB-Ten-GigabitEthernet2/1/1] quit
irf-port-configuration active

3. Master election is held between the two devices. Master election rules are followed. Device B reboots automatically and joins the Device A as a slave switch, and the IRF fabric is formed. The system name on both devices is DeviceA.

4. Configure LACP MAD detection

# Create a dynamic aggregation interface and enable LACP MAD detection. Because the LACP MAD detection is not configured between two IRF domains, when the system prompts you to enter the domain ID for the IRF fabric, you can keep the default value 0.
<DeviceA> system-view
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation2] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]:
The assigned domain ID is: 0
Info: MAD LACP only enable on dynamic aggregation interface.

# Add ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1 to the aggregation interface and they are dedicated to the LACP MAD detection for Device A and Device B.
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 2
quit
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-aggregation group 2

5. Configure Device C as the intermediate device
Acting as the intermediate device, Device C needs to support LACP to forward and process LACP protocol packets, and help Device A and Device B implement MAD detection. An LACP-supported switch is used here to save the cost.

```
# Create a dynamic aggregation interface.
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 2
[DeviceC-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation2] quit
# Add ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the aggregation interface and they are used for the LACP MAD detection.
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-aggregation group 2
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-aggregation group 2
```

BFD MAD detection-enabled IRF configuration example

**Network requirements**

The network as shown in Figure 14 is outgrowing the forwarding capability of the existing core switch, namely, Device A. To address business growth, the network must be scaled up to extend its forwarding capability while the present investments of the customer are protected. Ease of management and maintenance must also be ensured.

**Figure 14 Network diagram**
Configuration considerations

- Device A is located at the distribution layer of the network. To improve the forwarding capability at this layer, additional devices are needed. In this example, Device B is added.
- To address the requirements for high availability, ease of management and maintenance, use IRF2 technology to create an IRF fabric with Device A and Device B at the distribution layer. The access devices are each connected to the distribution layer with dual links.
- To offset the risk of IRF fabric partition, configure MAD to detect multi-active collisions. In this example, BFD MAD is adopted because the number of member switches is small.

Configuration procedure

NOTE:
This example assumes that the system names of Device A and Device B are DeviceA and DeviceB respectively before the IRF fabric is formed.

1. Set member IDs
   # Keep the default member ID of Device A unchanged.
   # Set the member ID of Device B to 2.
   <DeviceB> system-view
   [DeviceB] irf member 1 renumber 2
   Warning: Renumbering the switch number may result in configuration change or loss. Continue? [Y/N]:y
   [DeviceB]

2. Power off the two devices and connect IRF links and BFD MAD detection links according to Figure 14. Then power on the two devices.
   # Create IRF port 2 on Device A, and bind it to the physical IRF port Ten-GigabitEthernet 1/1/2. Then save the configuration.
   <DeviceA> system-view
   [DeviceA] interface ten-gigabitethernet 1/1/2
   [DeviceA-Ten-GigabitEthernet1/1/2] shutdown
   [DeviceA] irf-port 1/2
   [DeviceA-irf-port1/2] port group interface ten-gigabitethernet 1/1/2
   [DeviceA-irf-port1/2] quit
   [DeviceA] interface ten-gigabitethernet 1/1/2
   [DeviceA-Ten-GigabitEthernet1/1/2] undo shutdown
   [DeviceA-Ten-GigabitEthernet1/1/2] save

   # Create IRF port 1 on Device B, and bind it to the physical IRF port Ten-GigabitEthernet 2/1/1. Then save the configuration.
   <DeviceB> system-view
   [DeviceB] interface ten-gigabitethernet 2/1/1
   [DeviceB-Ten-GigabitEthernet2/1/1] shutdown
   [DeviceB] irf-port 2/1
   [DeviceB-irf-port2/1] port group interface ten-gigabitethernet 2/1/1
   [DeviceB-irf-port2/1] quit
   [DeviceB] interface ten-gigabitethernet 2/1/1
   [DeviceB-Ten-GigabitEthernet2/1/1] undo shutdown
   [DeviceB-Ten-GigabitEthernet2/1/1] save
# Activate IRF port configuration on Device A.
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] irf-port-configuration active

# Activate IRF port configuration on Device B.
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] irf-port-configuration active

3. Master election is held between the two devices. As a result of the master election, Device B automatically reboots to join the IRF fabric as a slave switch. The system name on both devices is DeviceA.

4. Configure BFD MAD detection

# Create VLAN 3, and add port GigabitEthernet 1/0/1 on Device A (with the member ID of 1) and port GigabitEthernet 2/0/1 on Device B (with the member ID of 2) to VLAN 3.

<DeviceA> system-view
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1
[DeviceA-vlan3] quit

# Create VLAN-interface 3 and configure the MAD IP address for the interface.

[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] mad bfd enable
[DeviceA-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[DeviceA-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
[DeviceA-Vlan-interface3] quit

# Connect the BFD MAD detection links according to Figure 14.

# Disable the spanning tree function on port GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.

[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-Gigabitethernet1/0/1] undo stp enable
[DeviceA-Gigabitethernet1/0/1] quit
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-Gigabitethernet2/0/1] undo stp enable

ARP MAD detection-enabled IRF configuration example

Network requirements

The network (see Figure 15) is outgrowing the forwarding capability of the existing core switch, namely, Device A. To address business growth, the network must be scaled up to extend its forwarding capability while the present investments of the customer are protected. Ease of management and maintenance must also be ensured.
Configuration considerations

- Device A is located at the distribution layer of the network. To improve the forwarding capability at this layer, additional devices are needed. In this example, Device B is added.
- To address the requirements for high availability, ease of management and maintenance, use IRF2 technology to create an IRF fabric with Device A and Device B at the access layer. The IRF fabric is connected to Device C with dual links.
- To offset the risk of IRF fabric partition, configure MAD to detect multi-active collisions. In this example, ARP MAD is adopted because the number of members in the IRF fabric is small, and the ARP MAD packets are transmitted over dual links connected to Device C. Enable the spanning tree function on the IRF fabric and Device to prevent loops.

Configuration procedure

NOTE:
This example assumes that the system names of Device A, Device B and Device C are DeviceA, DeviceB, and DeviceC respectively before the IRF fabric is formed.

1. **Set member IDs**
   - # Keep the default member ID of Device A unchanged.
   - # Set the member ID of Device B to 2.

   ```
   <DeviceB> system-view
   [DeviceB] irf member 1 renumber 2
   Warning: Renumbering the switch number may result in configuration change or loss. Continue? [Y/N]:y
   [DeviceB]
   ```

2. **Power off the two devices and connect IRF links and ARP MAD detection links according to Figure 15. Then power on the two devices.**

   - # Create IRF port 2 on Device A, and bind it to the physical IRF port Ten-GigabitEthernet 1/1/2. Then save the configuration.

   ```
   <DeviceA> system-view
   ```
# Create IRF port 1 on Device A, and bind it to the physical IRF port Ten-GigabitEthernet 1/1/2. Then save the configuration.

# Create IRF port 1 on Device B, and bind it to the physical IRF port Ten-GigabitEthernet 2/1/1. Then save the configuration.

3. Master election is held between the two devices. As a result of the master election, Device B automatically reboots to join the IRF fabric as a slave switch. The system name on both devices is DeviceA.

4. Configure ARP MAD

# Enable MSTP globally on the IRF fabric to prevent loops.

# Connect the ARP MAD detection links according to Figure 15.

# Configure that the bridge MAC address of the IRF fabric changes as soon as the master leaves.

# Create VLAN 3, and add port GigabitEthernet 1/0/1 (located on Device A) and port GigabitEthernet 2/0/1 (located on Device B) to VLAN 3.

# Create VLAN-interface 3, assign it an IP address, and enable ARP MAD on the interface. Because the ARP MAD detection is not configured between two IRF domains, when the system prompts you to enter the domain ID for the IRF fabric, you can keep the default value 0.
[DeviceA-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]:
The assigned domain ID is: 0

5. Configure Device C

# Enable MSTP globally on Device C to prevent loops.
<DeviceC> system-view
[DeviceC] stp enable
# Create VLAN 3, and add port GigabitEthernet 1/0/1 and port GigabitEthernet 1/0/2 to VLAN 3 to forward ARP MAD packets.
[DeviceC] vlan 3
[DeviceC-vlan3] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceC-vlan3] quit
Index

A B C D E I

A
Accessing an IRF fabric, 25

B
Basic concepts, 2

C
Configuring an IRF fabric, 11

D

Displaying and maintaining an IRF fabric, 26

E
Establishment, operation, and maintenance of an IRF fabric, 3

I
IRF fabric configuration examples, 26
IRF fabric configuration task list, 10
IRF overview, 1