# Contents

Configuring an IRF fabric

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About IRF</td>
<td>1</td>
</tr>
<tr>
<td>IRF network model</td>
<td>1</td>
</tr>
<tr>
<td>IRF benefits</td>
<td>2</td>
</tr>
<tr>
<td>Basic concepts</td>
<td>3</td>
</tr>
<tr>
<td>Network topology</td>
<td>6</td>
</tr>
<tr>
<td>Master election</td>
<td>6</td>
</tr>
<tr>
<td>Interface naming conventions</td>
<td>7</td>
</tr>
<tr>
<td>File system naming conventions</td>
<td>7</td>
</tr>
<tr>
<td>Configuration synchronization</td>
<td>8</td>
</tr>
<tr>
<td>Multi-active handling procedure</td>
<td>8</td>
</tr>
<tr>
<td>MAD mechanisms</td>
<td>10</td>
</tr>
<tr>
<td>Restrictions: Hardware compatibility with IRF</td>
<td>13</td>
</tr>
<tr>
<td>Restrictions and guidelines: IRF configuration</td>
<td>14</td>
</tr>
<tr>
<td>Hardware compatibility with IRF</td>
<td>14</td>
</tr>
<tr>
<td>Software requirements for IRF</td>
<td>15</td>
</tr>
<tr>
<td>IRF fabric size</td>
<td>15</td>
</tr>
<tr>
<td>IRF topo-domain ID restrictions</td>
<td>15</td>
</tr>
<tr>
<td>IRF network interfaces</td>
<td>15</td>
</tr>
<tr>
<td>Transceiver modules and cables selection for IRF</td>
<td>16</td>
</tr>
<tr>
<td>Configuration backup</td>
<td>16</td>
</tr>
<tr>
<td>IRF merge restrictions</td>
<td>16</td>
</tr>
<tr>
<td>Licensing requirements for IRF</td>
<td>16</td>
</tr>
<tr>
<td>IRF tasks at a glance</td>
<td>16</td>
</tr>
<tr>
<td>Planning the IRF fabric setup</td>
<td>17</td>
</tr>
<tr>
<td>Setting up an IRF fabric</td>
<td>17</td>
</tr>
<tr>
<td>Assigning a member ID to each IRF member device</td>
<td>17</td>
</tr>
<tr>
<td>Specifying a priority for each member device</td>
<td>18</td>
</tr>
<tr>
<td>Assigning the same IRF topo-domain ID to the member devices</td>
<td>18</td>
</tr>
<tr>
<td>Enabling software auto-update for software image synchronization</td>
<td>19</td>
</tr>
<tr>
<td>Enabling IRF auto-merge</td>
<td>19</td>
</tr>
<tr>
<td>Assigning links to an IRF port</td>
<td>20</td>
</tr>
<tr>
<td>Saving configuration to the next-startup configuration file</td>
<td>20</td>
</tr>
<tr>
<td>Connecting IRF network interfaces</td>
<td>20</td>
</tr>
<tr>
<td>Accessing the IRF fabric</td>
<td>21</td>
</tr>
<tr>
<td>Configuring MAD</td>
<td>21</td>
</tr>
<tr>
<td>Restrictions and guidelines for MAD configuration</td>
<td>21</td>
</tr>
<tr>
<td>Configuring LACP MAD</td>
<td>21</td>
</tr>
<tr>
<td>Configuring ARP MAD</td>
<td>22</td>
</tr>
<tr>
<td>Configuring ND MAD</td>
<td>24</td>
</tr>
<tr>
<td>Excluding a network interface from the shutdown action upon detection of multi-active collision</td>
<td>25</td>
</tr>
<tr>
<td>Recovering an IRF fabric</td>
<td>26</td>
</tr>
<tr>
<td>Optimizing IRF settings for an IRF fabric</td>
<td>26</td>
</tr>
<tr>
<td>Configuring a member device description</td>
<td>26</td>
</tr>
<tr>
<td>Configuring IRF bridge MAC persistence</td>
<td>27</td>
</tr>
<tr>
<td>Removing a member device from the IRF fabric</td>
<td>28</td>
</tr>
<tr>
<td>Adding a removed member device back to the IRF fabric</td>
<td>28</td>
</tr>
<tr>
<td>Enabling IRF optimization for WLAN access</td>
<td>28</td>
</tr>
<tr>
<td>Display and maintenance commands for IRF</td>
<td>29</td>
</tr>
</tbody>
</table>
Configuring an IRF fabric

About IRF

The Intelligent Resilient Framework (IRF) technology is a true stacking technology that creates a large virtual stack called IRF fabric from multiple devices to provide data center class availability and scalability. IRF offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

IRF network model

As shown in Figure 1, two IRF fabrics are deployed in a public cloud to provide virtual private cloud services for different tenants. The devices in each IRF fabric appear as a single node to the upper-layer and lower-layer devices.
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.

- **Star topology**—The IRF member devices are connected in star topology through a Layer 2 network. Service traffic and IRF protocol packets are delivered between member devices over
existing physical links. You do not need to use dedicated physical links to connect IRF member devices.

- **IRF link redundancy**—You can assign several links to an IRF port for redundancy. You do not need to aggregate the links. The IRF technology removes the loop automatically.

- **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 add and remove IRF member devices as needed without causing network topology change.

### Basic concepts

**IRF member roles**

IRF uses two member roles: master and standby.

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.

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 IRF 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 forwards data and IRF control packets between IRF member devices.

Every IRF-capable device has one IRF port. The IRF port is named `irf-port n`, where `n` is the IRF member ID of the device.

An IRF port must contain a minimum of one channel to send data and control packets.

An IRF port goes down when all its physical links are down.

**IRF links**

Links of the network interfaces bound to IRF ports are called IRF links.

You can configure an IRF link as one of the following channels:

- **Control channel**—The link forwards only IRF control packets between member devices.

- **Data channel**—The link forwards only data packets between member devices.

- **Hybrid channel**—The link forwards both control and data packets.

For more information about network interfaces that can be used for IRF links, see "IRF network interfaces."

**IRF topo-domain ID**

An IRF topo-domain ID uniquely identifies an IRF fabric. Devices must have the same IRF topo-domain ID to form one IRF fabric.

As shown in Figure 2, IRF fabric 1 contains Device A and Device B, and IRF fabric 2 contains Device C and Device D. The IRF fabrics can reach each other at Layer 2. When a member device receives
a packet from an IRF link, it checks the topo-domain ID to determine whether the packet is from the local IRF fabric. Then, the member device can handle the packet correctly.

**Figure 2 A network that contains two IRF topo-domains**

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 MAD domain ID**

An IRF MAD domain ID uniquely identifies an IRF MAD domain.

As shown in **Figure 3**, 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 MAD domain ID to determine whether the packet is from the local IRF fabric. Then, the member device can handle the packet correctly.

For easy management, you can assign the same value to the IRF topo-domain ID and MAD domain ID for an IRF fabric. For more information about IRF MAD domain ID configuration, see “Configuring MAD.”
**IRF merge**

IRF merge occurs when two split IRF fabrics reunite or when two independent IRF fabrics are united, as shown in Figure 4.

**Figure 4 IRF merge**

**IRF split**

IRF split occurs when an IRF fabric breaks up into multiple IRF fabrics when Layer 2 connectivity is lost, as shown in Figure 5. The split IRF fabrics operate with the same IP address. IRF split causes routing and forwarding problems on the network.
Network topology

The IRF implementation of the device supports star topology. As shown in Figure 6, member devices are connected through a Layer 2 network. The member devices can communicate with one another as long as they have Layer 2 connectivity.

An IRF link can transmit IRF protocol packets, data packets, or both. For high availability, set up redundant IRF links between IRF member devices.

As a best practice to reduce data traffic across member devices, make sure the incoming and outgoing interfaces of packets for a session are on the same IRF member device.

Master election

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

- The IRF fabric is established.
- The master device fails or is removed.
- The IRF fabric splits.
• Merge of independent IRF fabrics.

NOTE:
Master election does not occur when split IRF fabrics merge. In this situation, the master device in the active IRF fabric maintains its role. For more information about IRF fabric split and merge, see "Multi-active handling procedure."

Master election selects a master in the following order:
1. Current master, even if a new member has higher priority.
   This rule is skipped in the following situations:
   o Devices are forming an IRF fabric. In this situation, all devices consider themselves as the master.
   o Independent IRF fabrics merge. In this situation, the master in each IRF fabric consider itself as the master.
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 a new IRF fabric to be established, all devices placed in standby state must reboot after the master election.

For independent IRF fabrics to be merged, all devices must reboot after master election except those in the IRF fabric that won the master election.

Interface naming conventions

A network 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.
• interface-index—Interface index on the device. Interface index depends on the number of interfaces available on the device. To identify the index of an interface, examine its interface index mark on the chassis.

For example:

```
# Configure the description of the first interface GigabitEthernet 1/0/1 on member device 1 as for LAN1.
<Sysname> system-view
<Sysname-GigabitEthernet1/0/1] description for LAN1
```

```
# Configure the description of the first interface GigabitEthernet 2/0/1 on member device 2 as for LAN2.
<Sysname> system-view
<Sysname-GigabitEthernet2/0/1] description for LAN2
```

File system naming conventions

On a single-member fabric, you can use its storage device name to access its file system.
On a multimember 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 `slotmember-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 device:
  ```
  <Master> mkdir test
  Creating directory flash:/test... Done.
  <Master> cd test
  <Master> dir
  Directory of flash:/test
  The directory is empty.
  ```

  524288 KB total (29832 KB free)

- To create and access the `test` folder under the root directory of the flash memory on member device 2:
  ```
  <Master> mkdir slot2#flash:/test
  Creating directory slot2#flash:/test... Done.
  <Master> cd slot2#flash:/test
  <Master> dir
  Directory of slot2#flash:/test
  The directory is empty.
  ```

  524288 KB total (128812 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.

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, 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 ARP, see *Layer 3—IP Services Configuration Guide*. For information about ND, see IPv6 basics in *Layer 3—IP Services Configuration Guide*.  

8
Collision handling

When MAD detects a multi-active collision, it sets all IRF fabrics except one to the Recovery state. The fabric that is not placed in Recovery state can continue to forward traffic. The Recovery-state IRF fabrics are inactive and cannot forward traffic.

LACP MAD uses the following process to handle a multi-active collision:
1. Compares the number of members in each fabric.
2. Sets all fabrics to the Recovery state except the one that has the most members.
3. Compares the member IDs of the masters if all IRF fabrics have the same number of members.
4. Sets all fabrics to the Recovery state except the one that has the lowest numbered master.
5. Shuts down all network interfaces in the Recovery-state fabrics except for the following interfaces:
   - IRF network interfaces.
   - Interfaces specified by using the `mad exclude interface` command.

In contrast, ARP MAD and ND MAD do not compare the number of members in fabrics. These MAD mechanisms 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 on the network interfaces in Recovery-state fabrics as LACP MAD and BFD MAD.

Failure recovery

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

After the failed IRF link between two split IRF fabrics is recovered, log in to the inactive IRF fabric to reboot its member devices if the system requires you to do so. After these member devices join the active IRF fabric as subordinate devices, the IRF merge is complete, as shown in Figure 8. The network interfaces that have been shut down by MAD automatically restore their original state.

⚠️ CAUTION:

If you inadvertently reboot the active IRF fabric after the failed IRF link recovers, its member devices will join the inactive IRF fabric with their network interfaces shut down by MAD. To restore the original states of the network interfaces in the merged IRF fabric, use the `mad restore` command.

NOTE:

If the IRF auto-merge feature is enabled, the inactive IRF member devices will automatically reboot after the failed IRF link recovers and a manual reboot is typically not required.

Figure 8 Recovering the IRF fabric
If the active IRF fabric fails before the IRF link is recovered (see Figure 9), 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 9 Active IRF fabric fails before the IRF link is recovered

MAD mechanisms

IRF provides MAD mechanisms by extending LACP, ARP, and IPv6 ND. Table 1 compares the MAD mechanisms and their application scenarios.

Table 1 Comparison of MAD mechanisms

<table>
<thead>
<tr>
<th>MAD mechanism</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Application scenario</th>
</tr>
</thead>
</table>
| 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. |
| ARP MAD       | • Intermediate device, if used, can come from any vendor.  
                 • Does not require MAD | • Detection speed is slower than LACP MAD.  
                 • The spanning tree | Non-link aggregation IPv4 network scenario. |
<table>
<thead>
<tr>
<th>MAD mechanism</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Application scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dedicated interfaces.</td>
<td>feature must be enabled if Ethernet ports are used.</td>
<td></td>
</tr>
</tbody>
</table>
| ND MAD | • Intermediate device, if used, can come from any vendor.  
• Does not require MAD dedicated interfaces. | • Detection speed is slower than LACP MAD.  
• The spanning tree feature must be enabled if Ethernet ports are used. | Non-link aggregation IPv6 network scenario. |

**LACP MAD**

As shown in Figure 10, 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 MAD 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 MAD 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 MAD domain ID but different active IDs, a split has occurred. LACP MAD handles this situation as described in "Collision handling."
ARP MAD

ARP MAD detects multi-active collisions by using extended ARP packets that convey the IRF MAD domain ID and the active ID (the member ID of the master). Each IRF member compares the MAD domain ID and the active ID in incoming extended ARP packets with its MAD domain ID and active ID.

- If the MAD 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 MAD 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.

You can configure ARP MAD on a VLAN interface.

If a VLAN interface is 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.

If the IRF fabric is integrated, only one ARP MAD port on the IRF fabric can forward ARP packets and the other ARP MAD ports on the IRF fabric are blocked. If the IRF fabric splits, each split IRF fabric has an ARP MAD port that can forward ARP packets. As a result, one split IRF fabric receives
ARP packets from another split IRF fabric. Because these ARP packets have the same MAD domain ID but different active IDs, ARP MAD determines that a multi-active collision has occurred.

Figure 11 ARP MAD scenario

ND MAD

ND MAD detects multi-active collisions by using NS packets to transmit the IRF MAD domain ID and the active ID (the member ID of the master).

ND MAD is applicable to IPv6 network scenarios. It uses the same multi-active detection mechanism and topology as ARP MAD.

Restrictions: Hardware compatibility with IRF

<table>
<thead>
<tr>
<th>Hardware series</th>
<th>Model</th>
<th>Product code</th>
<th>IRF compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>WX1800H series</td>
<td>WX1804H</td>
<td>EWP-WX1804H-PWR-CN</td>
<td>No</td>
</tr>
<tr>
<td>WX2500H series</td>
<td>WX2508H-PWR-LTE</td>
<td>EWP-WX2508H-PWR-LTE</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>WX2510H</td>
<td>EWP-WX2510H-PWR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WX2510H-F</td>
<td>EWP-WX2510H-F-PWR-LTE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WX2540H</td>
<td>EWP-WX2540H-PWR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WX2540H-F</td>
<td>EWP-WX2540H-F-PWR-LTE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WX2560H</td>
<td>EWP-WX2560H-PWR</td>
<td></td>
</tr>
<tr>
<td>WX3000H series</td>
<td>WX3010H</td>
<td>EWP-WX3010H-PWR-X-PWR</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>WX3010H-X</td>
<td>EWP-WX3010H-X-PWR</td>
<td></td>
</tr>
<tr>
<td>Hardware series</td>
<td>Model</td>
<td>Product code</td>
<td>IRF compatibility</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>-----------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>WX3010H-L</td>
<td>EWP-WX3010H-L-PWR</td>
<td>EWP-WX3010H-L-PWR</td>
<td>EWP-WX3024H-F</td>
</tr>
<tr>
<td>WX3024H</td>
<td>EWP-WX3024H</td>
<td>EWP-WX3024H-L-PWR</td>
<td>EWP-WX3024H-F</td>
</tr>
<tr>
<td>WX3024H-L</td>
<td>EWP-WX3024H-L-PWR</td>
<td>EWP-WX3024H-F</td>
<td>Yes</td>
</tr>
<tr>
<td>WX3024H-F</td>
<td>EWP-WX3024H-F</td>
<td>EWP-WX3024H-L-PWR</td>
<td>EWP-WX3024H-F</td>
</tr>
<tr>
<td>WX3508H</td>
<td>EWP-WX3508H</td>
<td>EWP-WX3510H</td>
<td>EWP-WX3520H</td>
</tr>
<tr>
<td>WX3510H</td>
<td>EWP-WX3510H</td>
<td>EWP-WX3520H</td>
<td>EWP-WX3520H-F</td>
</tr>
<tr>
<td>WX3520H</td>
<td>EWP-WX3520H</td>
<td>EWP-WX3540H</td>
<td>EWP-WX3540H</td>
</tr>
<tr>
<td>WX3520H-F</td>
<td>EWP-WX3520H-F</td>
<td>EWP-WX3540H</td>
<td>Yes</td>
</tr>
<tr>
<td>WX3540H</td>
<td>EWP-WX3540H</td>
<td>EWP-WX3540H</td>
<td>Yes</td>
</tr>
<tr>
<td>WX5510E</td>
<td>EWP-WX5510E</td>
<td>EWP-WX5540E</td>
<td>Yes</td>
</tr>
<tr>
<td>WX5540E</td>
<td>EWP-WX5540E</td>
<td>EWP-WX5540H</td>
<td>Yes</td>
</tr>
<tr>
<td>WX5560H</td>
<td>EWP-WX5560H</td>
<td>EWP-WX5560H</td>
<td>Yes</td>
</tr>
<tr>
<td>WX5580H</td>
<td>EWP-WX5580H</td>
<td>EWP-WX5580H</td>
<td>Yes</td>
</tr>
<tr>
<td>Access controller modules</td>
<td>LSUM1WCME0</td>
<td>LSUM1WCME0</td>
<td>EWPX1WCME0</td>
</tr>
<tr>
<td></td>
<td>EWPX1WCME0</td>
<td>EWPX1WCME0</td>
<td>EWPX1WCME0</td>
</tr>
<tr>
<td></td>
<td>LSUM1WCNX20</td>
<td>LSUM1WCNX20</td>
<td>LSUM1WCNX20</td>
</tr>
<tr>
<td></td>
<td>LSUM1WCNX20RT</td>
<td>LSUM1WCNX20RT</td>
<td>LSUM1WCNX20RT</td>
</tr>
<tr>
<td></td>
<td>LSUM1WCNX40</td>
<td>LSUM1WCNX40</td>
<td>LSUM1WCNX40</td>
</tr>
<tr>
<td></td>
<td>LSUM1WCNX40RT</td>
<td>LSUM1WCNX40RT</td>
<td>LSUM1WCNX40RT</td>
</tr>
<tr>
<td></td>
<td>EWPX1MCMD0F</td>
<td>EWPX1MCMD0F</td>
<td>EWPX1MCMD0F</td>
</tr>
<tr>
<td></td>
<td>EWPX1MAC0F</td>
<td>EWPX1MAC0F</td>
<td>EWPX1MAC0F</td>
</tr>
<tr>
<td>Hardware series</td>
<td>Model</td>
<td>Product code</td>
<td>IRF compatibility</td>
</tr>
<tr>
<td>WX1800H series</td>
<td>WX1804H</td>
<td>EWP-WX1804H-PWR</td>
<td>EWP-WX1810H-PWR</td>
</tr>
<tr>
<td></td>
<td>WX1810H</td>
<td>EWP-WX1804H-PWR</td>
<td>EWP-WX1810H-PWR</td>
</tr>
<tr>
<td></td>
<td>WX1820H</td>
<td>EWP-WX1804H-PWR</td>
<td>EWP-WX1810H-PWR</td>
</tr>
<tr>
<td></td>
<td>WX1840H</td>
<td>EWP-WX1804H-PWR</td>
<td>EWP-WX1810H-PWR</td>
</tr>
<tr>
<td>WX3800H series</td>
<td>WX3820H</td>
<td>EWP-WX3820H-GL</td>
<td>EWP-WX3820H-GL</td>
</tr>
<tr>
<td></td>
<td>WX3840H</td>
<td>EWP-WX3820H-GL</td>
<td>EWP-WX3840H-GL</td>
</tr>
<tr>
<td>WX5800H series</td>
<td>WX5860H</td>
<td>EWP-WX5860H-GL</td>
<td>EWP-WX5860H-GL</td>
</tr>
</tbody>
</table>

Restrictions and guidelines: IRF configuration

For a successful IRF setup, follow the restrictions and guidelines in this section and the setup procedure in "IRF tasks at a glance" or "Planning the IRF fabric setup."

Hardware compatibility with IRF

The device can form an IRF fabric only with devices of the same model.

When setting up an IRF fabric of access controller modules, use the following restrictions and guidelines if WLAN hardware fast forwarding is enabled on them:
• On the EWPXM2WCM0F, LSQM1WCMX20, or LSUM1WCMX20RT module, use only one Ten-GigabitEthernet interface for IRF connection. The other Ten-GigabitEthernet interface must be used as a normal service interface.

• On the EWPXM1MAC0, LSQM1WCMX40, LSUM1WCME0, or LSUM1WCMX40RT module, Ten-GigabitEthernet interfaces are in two port groups. Use interfaces in one group for IRF connection and use interfaces in another group to provide normal forwarding services. The following are port groups on the modules:
  - Ten-GigabitEthernet n/0/1 and Ten-GigabitEthernet n/0/3.
  - Ten-GigabitEthernet n/0/2 and Ten-GigabitEthernet n/0/4.
Letter n in the port numbers represents the IRF member ID.

Software requirements for IRF

All IRF member devices must run the same software image version as the master. For software synchronization, make sure the software auto-update feature is enabled. The feature can automatically synchronize the device with the software running on the master if the software versions are different.

You must manually synchronize the software if software auto-update fails to update software. This situation might occur if the IRF fabric cannot identify the software version used on the new device. For more information, see "Enabling software auto-update for software image synchronization."

IRF fabric size

An IRF fabric can contain a maximum of two member devices.

IRF topo-domain ID restrictions

To form an IRF fabric, devices must have the same IRF topo-domain ID.

IRF network interfaces

Typically, use high-speed interfaces as IRF network interfaces. The following interfaces can be used as IRF network interfaces:

• GE interfaces.
• 10-GE interfaces except MGE interfaces.
• SFP interfaces.

You must manually assign network interfaces to the IRF port.

An IRF port must have a minimum of one hybrid (control&data) channel, or a minimum of one data channel and one control channel.

An IRF port can have a maximum of four IRF network interfaces. Hybrid channels can coexist with dedicated data or control channels.

To avoid IRF split, do not use the shutdown command on an IRF network interface if the interface is the only control channel available on the IRF standby device.

The same type of IRF network interfaces must operate at the same rate.
Transceiver modules and cables selection for IRF

When you select transceiver modules for IRF network interfaces, follow these restrictions and guidelines:

- Do not use 100-Mbps optical transceiver modules for 100Base-FX SFP ports or 1000Base-X SFP ports.
- Do not use 1-Gbps optical transceiver modules for 10GBase-R SFP+ ports.

Support for transceiver modules and cables varies by device model.

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

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

Configuration backup

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

A standby device's next-startup configuration file might be overwritten if the master and the standby devices 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 standby device from the IRF fabric.

IRF merge restrictions

If two IRF fabrics have the same IRF bridge MAC address, they cannot merge. You must change one of the bridge MAC addresses for the IRF fabrics to merge.

If an IRF fabric splits, do not change the IRF settings on any IRF member devices before they reunite.

Spanning tree feature

Do not enable the spanning tree feature on any IRF network interfaces.

In the IRF member devices are connected across a Layer 2 network, disable the spanning tree feature on the switch ports to which the IRF member devices are connected.

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.

IRF tasks at a glance

To configure IRF, perform the following tasks:

1. **Setting up an IRF fabric**
   a. Assigning a member ID to each IRF member device
   b. (Optional.) Specifying a priority for each member device
c. Assigning the same IRF topo-domain ID to the member devices
d. Enabling software auto-update for software image synchronization
e. (Optional.) Enabling IRF auto-merge
f. Assigning links to an IRF port
g. Saving configuration to the next-startup configuration file
h. Connecting IRF network interfaces
i. Accessing the 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 ARP MAD
   - Configuring ND MAD
   - Excluding a network interface from the shutdown action upon detection of multi-active collision
     This feature excludes a network 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 persistence
   - Removing a member device from the IRF fabric
   - Adding a removed member device back to the IRF fabric
   - Enabling IRF optimization for WLAN access
   You can also change the member IDs, priorities, IRF port bindings, and domain ID after the IRF fabric is formed. The commands for configuring these parameters on an IRF fabric are the same as the commands for configuring these parameters on a standalone device.

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.
- IRF topology and cabling scheme.
- IRF network interfaces.

Setting up an IRF fabric

Assigning a member ID to each IRF member device

Restrictions and guidelines
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. For example, all member switches in an IRF fabric are the same model. If you
swapped the IDs of any two members, their interface settings would also be swapped.

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

To prevent any undesirable configuration change or data loss, avoid changing member IDs after the
IRF fabric is formed.

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

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 network interfaces to IRF ports or assigned member priority, you must
   perform this step for these settings to take effect after the reboot.

4. Reboot the device.
   
   reboot

Specifying a priority for each member device

About this task

IRF member priority represents the possibility for a device to be elected the master in an IRF fabric.
The higher the priority, the higher the possibility.

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.

Assigning the same IRF topo-domain ID to the member
devices

About this task

To form an IRF fabric, devices must have the same IRF topo-domain ID. IRF topo-domain IDs
prevent IRF fabrics from interfering with one another.

Restrictions and guidelines

For a new topo-domain ID to take effect, you must reboot the device.

Procedure

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

Enabling software auto-update for software image synchronization

About this task

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 IRF 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 tasks:

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 BootWare 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.

Enabling IRF auto-merge

About this task

When two IRF fabrics merge, a member device must reboot to complete the merge if it is in the IRF fabric that fails in master election.

- If the auto-merge feature is enabled, the reboot is automatically performed.
- If the auto-merge feature is disabled, you must reboot the member devices manually.

Procedure

1. Enter system view.
Assigning links to an IRF port

1. Enter system view.
   system-view

2. Enter IRF port view.
   irf-port member-id
   A device has only one IRF port. The port index is the IRF member ID of the device.

3. Bind a network interface to the IRF port.
   port group interface interface-type interface-number [ type { data | control } ]
   By default, no network interfaces are bound to an IRF port.
   Repeat this step to bind multiple network interfaces to the IRF port.
   The channel type of the link is hybrid if you do not specify a channel type.
   To change the channel type of an IRF link, you must first remove the binding, and then rebind its network interface to the IRF port.

4. Return to system view.
   quit

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

6. Activate the IRF port settings.
   irf-port-configuration active
   After this step is performed, the state of the IRF port changes to UP. The member devices elect a master, and the standby devices automatically reboot to complete the IRF establishment.
   After the IRF fabric is formed, you can add additional links to the IRF port (in UP state) without repeating this step.
   This step is optional for the devices that require a reboot for the port group interface to take effect.

Saving configuration to the next-startup configuration file

To save the running configuration to the next-startup configuration file, execute the following command in any view:

   save [ safely ] [ backup | main ] [ force ]

For more information about the save command, see configuration file management commands in Fundamentals Command Reference.

Connecting IRF network interfaces

Connect IRF network interfaces based on the cabling scheme and the requirements in "Network topology."
Accessing the IRF fabric

The IRF fabric appears as one device after it is formed. You configure and manage all IRF members from 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, Web, and SNMP.

Whichever device you connect, you are placed at the CLI or Web-based interface of the master when you log in to the IRF fabric.

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. 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.

**Assigning IRF domain IDs**

If LACP MAD, ARP MAD, or ND MAD runs between two IRF fabrics, assign each fabric a unique IRF MAD domain ID.

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

**Bringing up network interfaces shut down by MAD**

To prevent an interface from being shut down when the IRF fabric transits to the Recovery state, use the `mad exclude interface` command.

To bring up the interfaces shut down by a MAD mechanism in a Recovery-state IRF fabric, use the `mad restore` command instead of the `undo shutdown` command. The `mad restore` command activates the Recovery-state IRF fabric.

Configuring LACP MAD

1. Enter system view.
   ```
   system-view
   ```

2. Assign a MAD domain ID to the IRF fabric.
   ```
   irf domain domain-id
   ```
   The default IRF MAD domain ID is 0.

3. Create a Layer 2 aggregate interface and enter Layer 2 aggregate interface view.
   ```
   interface bridge-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.
   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.
   o Enter Ethernet interface view:
     interface interface-type interface-number
   o Enter interface range view. Choose one of the following commands:
     interface range interface-list
     interface range name name [ interface interface-list ]
   For more information about the interface range and interface range name commands, see bulk interface configuration commands in Interface Command Reference.
8. Assign the Ethernet port or the range of Ethernet ports to the specified aggregation group.
   port link-aggregation group group-id
   Multimember link aggregation is allowed.
   Perform this step also on the intermediate device.

Configuring ARP MAD

Restrictions and guidelines for ARP MAD configuration
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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Restrictions and guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP MAD VLAN</td>
<td>• Do not enable ARP MAD on VLAN-interface 1.</td>
</tr>
<tr>
<td></td>
<td>• If you are using an intermediate device, perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>o On the IRF fabric and the intermediate device, create a VLAN for ARP MAD.</td>
</tr>
<tr>
<td></td>
<td>o On the IRF fabric and the intermediate device, assign the ports of ARP MAD links to the ARP MAD VLAN.</td>
</tr>
<tr>
<td></td>
<td>o On the IRF fabric, create a VLAN interface for the ARP MAD VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Do not use the ARP MAD VLAN for any other purposes.</td>
</tr>
<tr>
<td>ARP MAD and feature configuration</td>
<td>If an intermediate device is used, make sure the following requirements are met:</td>
</tr>
<tr>
<td></td>
<td>o 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 Network Connectivity Configuration Guide.</td>
</tr>
<tr>
<td></td>
<td>• Enable the IRF fabric to change its bridge MAC address as soon as the</td>
</tr>
</tbody>
</table>

22
Category | Restrictions and guidelines
---|---
| address owner leaves.
| • If the intermediate device is also an IRF fabric, assign the two IRF fabrics different MAD domain IDs for correct split detection.

Configuring ARP MAD on a VLAN interface

1. Enter system view.
   ```
   system-view
   ```
2. Assign a MAD domain ID to the IRF fabric.
   ```
   irf domain domain-id
   ```
The default IRF MAD 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.
5. Return to system view.
   ```
   quit
   ```
6. Enter Ethernet interface view or interface range view.
   o Enter Ethernet interface view.
     ```
     interface interface-type interface-number
     ```
o Enter interface range view. Choose one of the following commands:
   ```
   interface range interface-list
   ```
   ```
   interface range name name [ interface interface-list ]
   ```
   For more information about the `interface range` and `interface range name` commands, see bulk interface configuration commands in `Interface Command Reference`.
7. Assign the port or the range of ports to the ARP MAD VLAN.
   o Assign the ports to the VLAN as access ports.
     ```
     port access vlan vlan-id
     ```
o Assign the ports to the VLAN as trunk ports.
     ```
     port trunk permit vlan vlan-id
     ```
o 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.
8. Return to system view.
   ```
   quit
   ```
9. Enter VLAN interface view.
   ```
   interface vlan-interface interface-number
   ```
10. Assign the interface an IP address.
    ```
    ip address ip-address { mask | mask-length }
    ```
    By default, no IP addresses are assigned to a VLAN interface.
11. Enable ARP MAD.
    
    `mad arp enable`
    
    By default, ARP MAD is disabled.

## Configuring ND MAD

### Restrictions and guidelines for ND MAD configuration

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

1. Choose an ND MAD link scheme as described in "ARP 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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Restrictions and guidelines</th>
</tr>
</thead>
</table>
| ND MAD VLAN                   | - Do not enable ND MAD on VLAN-interface 1.  
|                               |   - If you are using an intermediate device, perform the following tasks:  
|                               |     o On the IRF fabric and the intermediate device, create a VLAN for ND MAD.  
|                               |     o On the IRF fabric and the intermediate device, assign the ports of ND MAD links to the ND MAD VLAN.  
|                               |     o 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:  
|                               |   o 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 Network Connectivity Configuration Guide.  
|                               |   o Enable the IRF fabric to change its bridge MAC address as soon as the address owner leaves.  
|                               |   o If the intermediate device is also an IRF fabric, assign the two IRF fabrics different MAD domain IDs for correct split detection.  |

### Configuring ND MAD on a VLAN interface

1. Enter system view.
    
    `system-view`

2. Assign a MAD domain ID to the IRF fabric.
    
    `irf domain domain-id`
    
    The default IRF MAD 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 ND MAD.
    
    `vlan vlan-id`
    
    By default, only VLAN 1 exists.

5. Return to system view.
    
    `quit`
6. Enter Ethernet interface view or interface range view.
   o Enter Ethernet interface view.
     `interface interface-type interface-number`
   o Enter interface range view. Choose one of the following commands:
     `interface range interface-list`
     `interface range name name [ interface interface-list ]`
     For more information about the `interface range` and `interface range name`
     commands, see bulk interface configuration commands in `Interface Command Reference`.

7. Assign the port or the range of ports to the ND MAD VLAN.
   o Assign the ports to the VLAN as access ports.
     `port access vlan vlan-id`
   o Assign the ports to the VLAN as trunk ports.
     `port trunk permit vlan vlan-id`
   o 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.

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.

Excluding a network interface from the shutdown action upon detection of multi-active collision

About this task

When an IRF fabric transits to the Recovery state, the system automatically shuts down all network
interfaces except for the interfaces bound to IRF ports.

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

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

Restrictions and guidelines

When you configure this feature, follow these restrictions and guidelines:
• If the Layer 2 Ethernet 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.

• Do not exclude the following interfaces from the shutdown action:
  o Aggregate interfaces used for MAD and their member interfaces.
  o VLAN interfaces used for MAD and its Ethernet ports.

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

Recovering an IRF fabric

About this task
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 network interfaces that were shut down by MAD on the inactive IRF fabric.

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

Optimizing IRF settings for an IRF fabric

Configuring a member device description

About this task
You can configure a description for a member device to easily identify and manage the member device.

Procedure
1. Enter system view.
   ```plaintext
   system-view
   ```
2. Configure a description for a member device.
   ```plaintext
   irf member member-id description text
   ```
   By default, no description is configured for a member device.
Configuring IRF bridge MAC persistence

About this task

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.

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

⚠️ CAUTION:
Bridge MAC address changes 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.
- If the IRF fabric has multimember aggregate links, do not use the `undo irf mac-address persistent` command. Use of this command might cause traffic disruption.

Procedure

1. Enter system view.
   ```
   system-view
   ```
2. Configure IRF bridge MAC persistence.
   ```
   o Retain the bridge MAC address permanently even if the address owner has left the IRF fabric.
     ```
     irf mac-address persistent always
     ```
   o Retain the bridge MAC address for 6 minutes after the address owner leaves the IRF fabric.
     ```
     irf mac-address persistent timer
     ```
     This command avoids unnecessary bridge MAC address changes caused by device reboot, transient link failure, or purposeful link disconnection.
   o Change the bridge MAC address as soon as the address owner leaves the IRF fabric.
     ```
     undo irf mac-address persistent
     ```
   ```
   By default, the IRF bridge MAC address remains unchanged for 6 minutes after the address owner leaves.
Removing a member device from the IRF fabric

About this task
For troubleshooting or maintenance purposes, you can remove a member device from an IRF fabric by disabling the member device’s multimember stacking capability. The device will be removed from the IRF fabric 5 seconds after you disable its multimember stacking capability.

The removed member device still runs the original IRF settings. However, it does not send or receive IRF control packets.

Restrictions and guidelines
The removed IRF member might have the same Layer 2 or Layer 3 settings as the IRF fabric, for example, the IP address and bridge MAC address. To avoid network collisions, change these settings on the removed member or on the IRF fabric.

Procedure
1. Enter system view.
   ```
   system-view
   ```
2. Disable multimember stacking capability for the member device.
   ```
   undo irf member member-id stack enable
   ```
   By default, multimember stacking capability is enabled for an IRF member device.

Adding a removed member device back to the IRF fabric
1. Log in to the removed device.
2. Enter system view.
   ```
   system-view
   ```
3. Enable multimember stacking capability for the device.
   ```
   irf member member-id stack enable
   ```
4. Return to user view.
   ```
   quit
   ```
5. Save the running configuration.
   ```
   save
   ```
6. Reboot the device for the setting to take effect.
   ```
   reboot
   ```
The device will rejoin the IRF fabric after the reboot.

Enabling IRF optimization for WLAN access

About this task
Use this feature to guarantee reliable AP and client access. This feature accelerates IRF master election, new member joining, and IRF member role change to prevent IRF events from causing unstable AP and client access.

Procedure
1. Enter system view.
   ```
   system-view
   ```
2. Enable IRF optimization for WLAN access.
   ```
   irf-optimize wlan reliable-access
   ```
By default, WLAN access optimization is enabled in an IRF fabric.

Display and maintenance commands for IRF

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about all IRF members.</td>
<td><code>display irf</code></td>
</tr>
<tr>
<td>Display information about the IRF hello packets sent and received on a member device.</td>
<td><code>display irf forwarding [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display IRF link information.</td>
<td><code>display irf link</code></td>
</tr>
<tr>
<td>Display the IRF configuration.</td>
<td><code>display irf configuration</code></td>
</tr>
<tr>
<td>Display MAD information.</td>
<td><code>display mad [ verbose ]</code></td>
</tr>
</tbody>
</table>