Contents

Configuring DRNI

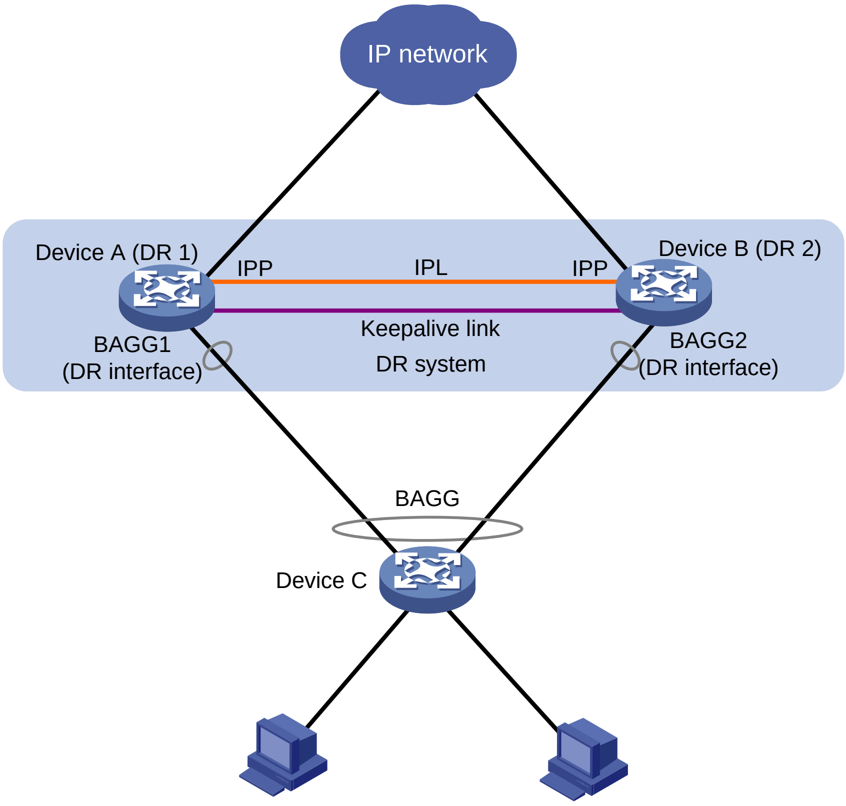
About DRNI

Distributed Resilient Network Interconnect (DRNI) virtualizes two physical devices into one system through multichassis link aggregation.

DRNI network model

As shown in Figure 1, DRNI virtualizes two devices into a distributed-relay (DR) system, which connects to the remote aggregation system through a multichassis aggregate link. To the remote aggregation system, the DR system is one device.

Figure 1 DRNI network model



The DR member devices are DR peers to each other. For features that require centralized traffic processing (for example, spanning tree), a DR member device is assigned the primary or secondary role based on its DR role priority. The secondary DR device passes the traffic of those features to the primary DR device for processing. If the DR member devices in a DR system have the same DR role priority, the device with the lower bridge MAC address is assigned the primary role.

DRNI defines the following interface roles for each DR member device:

- **DR interface**—Layer 2 aggregate interface connected to the remote aggregation system. DR interfaces connected to the same remote aggregation system belong to one DR group. In Figure 1, Bridge-Aggregation 1 on Device A and Bridge-Aggregation 2 on Device B belong to the same DR group. DR interfaces in a DR group form a multichassis aggregate link.
- **Intra-portal port (IPP)**—Interface connected to the DR peer for internal control. Each DR member device has only one IPP. The IPPs of the DR member devices transmit DRNI protocol

packets and data packets through the intra-portal link (IPL) established between them. A DR system has only one IPL.

DR member devices use a keepalive link to monitor each other's state. For more information about the keepalive mechanism, see "Keepalive and failover mechanism."

DRCP

DRNI uses IEEE P802.1AX Distributed Relay Control Protocol (DRCP) for multichassis link aggregation. DRCP runs on the IPL and uses distributed relay control protocol data units (DRCPDUs) to advertise the DRNI configuration out of IPPs and DR interfaces.

DRCP operating mechanism

DRNI-enabled devices use DRCPDUs for the following purposes:

- Exchange DRCPDUs through DR interfaces to determine whether they can form a DR system.
- Exchange DRCPDUs through IPPs to negotiate the IPL state.

DRCP timeout timers

DRCP uses a timeout mechanism to specify the amount of time that an IPP or DR interface must wait to receive DRCPDUs before it determines that the peer interface is down. This timeout mechanism provides the following timer options:

- Short DRCP timeout timer, which is fixed at 3 seconds. If this timer is used, the peer interface sends one DRCPDU every second.
- Long DRCP timeout timer, which is fixed at 90 seconds. If this timer is used, the peer interface sends one DRCPDU every 30 seconds.

Short DRCP timeout timer enables the DR member devices to detect a peer interface down event more quickly than the long DRCP timeout timer. However this benefit is at the expense of bandwidth and system resources.

Keepalive and failover mechanism

For the secondary DR device to monitor the state of the primary device, you must establish a Layer 3 keepalive link between the DR member devices.

The DR member devices periodically send keepalive packets over the keepalive link. If a DR member device has not received keepalive packets from the peer when the keepalive timeout timer expires, it determines that the keepalive link is down. When both the keepalive link and the IPL are down, a DR member device acts depending on its role.

- If its role is primary, the device retains its role as long as it has up DR interfaces. If all its DR interfaces are down, its role becomes None.
- If its role is secondary, the device takes over the primary role and retains the role as long as it has up DR interfaces. If all its DR interfaces are down, its role becomes None.

A device with the None role cannot send or receive keepalive packets. Its keepalive link stays in the down state.

If the keepalive link is down while the IPL is up, the DR member devices prompt you to check for keepalive link issues.

If the keepalive link is up while the IPL is down, the DR member devices elect a primary device based on the information in the keepalive packets.

MAD mechanism

A multi-active collision occurs if the IPL goes down while the keepalive link is up. To avoid network issues, the secondary DR device sets all network interfaces to DRNI MAD DOWN state, except for the following interfaces:

- Interfaces excluded from the MAD shutdown action by IRF.
- Interfaces excluded from the MAD shutdown action by DRNI.

The interfaces excluded from the MAD shutdown action by DRNI include system-configured interfaces and user-configured interfaces. System-configured interfaces include the following:

- IPP.
- Aggregation member interfaces if a Layer 2 aggregate interface is used as the IPP.
- DR interfaces.
- Management interfaces.

When the IPL comes up, the secondary DR device starts a delay timer and begins to restore table entries (including MAC address entries and ARP entries) from the primary DR device. When the delay timer expires, the secondary DR device brings up all network interfaces.

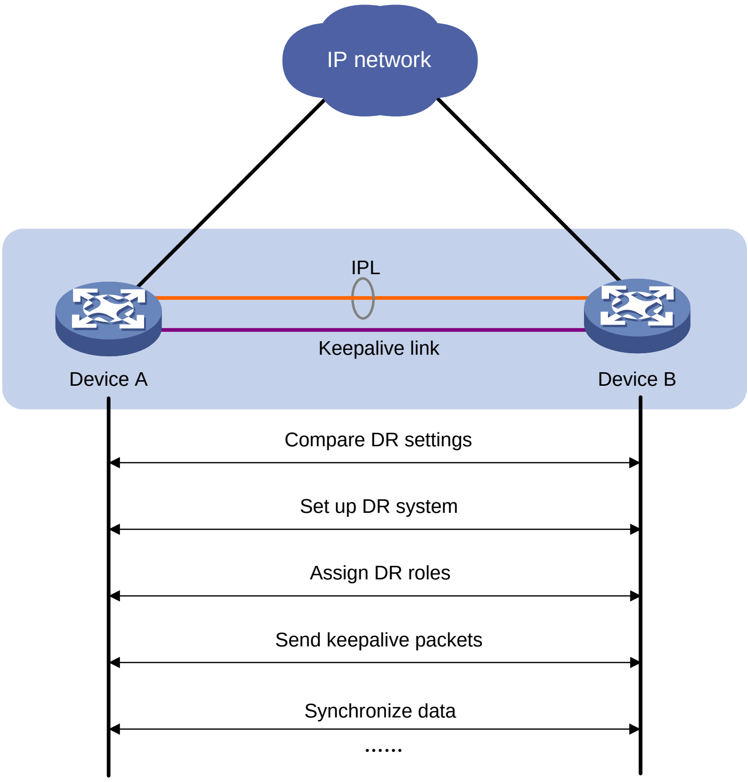
You can use the **`display drni mad verbose`** command to view detailed information about DRNI MAD.

DR system setup process

As shown in Figure 2, two devices perform the following operations to form a DR system:

1. Send DRCPDUs over the IPL to each other and compare the DRCPDUs to determine the DR system stackability and device roles:
   a. Compare the DR system settings. The devices can form a DR system if they have the same DR system MAC address and system priority and different DR system numbers.
   b. Determine the device roles based on the DR role priority and the bridge MAC address.
   c. Perform configuration consistency check. For more information, see "Configuration consistency check."
2. Send keepalive packets over the keepalive link after primary DR member election to verify that the peer system is operating correctly.
3. Synchronize configuration data by sending DRCPDUs over the IPL. The configuration data includes MAC address entries and ARP entries.

Figure 2 DR system setup process



Configuration consistency check

During DR system setup, DR member devices exchange the configuration and perform configuration consistency check to verify their consistency in the following configurations:

- **Type 1 configuration**—Settings that affect traffic forwarding of the DR system. If an inconsistency in type 1 configuration is detected, the secondary DR device shuts down its DR interfaces.
- **Type 2 configuration**—Settings that affect only service features. If an inconsistency in type 2 configuration is detected, the secondary DR device disables the affected service features, but it does not shut down its DR interfaces.

To prevent interface flapping, the DR system performs configuration consistency check when half the data restoration internal elapses.

NOTE:

The data restoration interval specifies the maximum amount of time for the secondary DR device to synchronize data with the primary DR device during DR system setup. For more information, see "Setting the data restoration interval."

Type 1 configuration

Type 1 configuration consistency check is performed both globally and on DR interfaces. Table 1 and Table 2 show settings that type 1 configuration contains.

Table 1 Global type 1 configuration

Setting	Details
IPP link type	IPP link type, including access, hybrid, and trunk.

Setting	Details
PVID on the IPP	PVID on the IPP.
Spanning tree state	• Global spanning tree state. • VLAN-specific spanning tree state.
Spanning tree mode	Spanning tree mode, including STP, RSTP, PVST, and MSTP.
MST region settings	• MST region name. • MST region revision level. • VLAN-to-MSTI mappings.

Table 2 DR interface type 1 configuration

Setting	Details
Aggregation mode	Aggregation mode, including static and dynamic.
Spanning tree state	Interface-specific spanning tree state.
Link type	Interface link type, including access, hybrid, and trunk.
PVID	Interface PVID.

Type 2 configuration

Type 2 configuration consistency check is performed both globally and on DR interfaces. Table 3 and Table 4 show settings that type 2 configuration contains.

Table 3 Global type 2 configuration

Setting	Details
VLAN interfaces	Up VLAN interfaces of which the VLANs contain the IPP.
Passing tagged VLANs or passing PVID	VLANs of which the IPP forwards tagged traffic or PVID of which the IPP forwards traffic.

Table 4 DR interface type 2 configuration

Setting	Details
Passing tagged VLANs	VLANs of which a DR interface forwards tagged traffic.
Passing untagged VLANs	VLANs of which a DR interface forwards untagged traffic.

DRNI failure handling mechanisms

DR interface failure handling mechanism

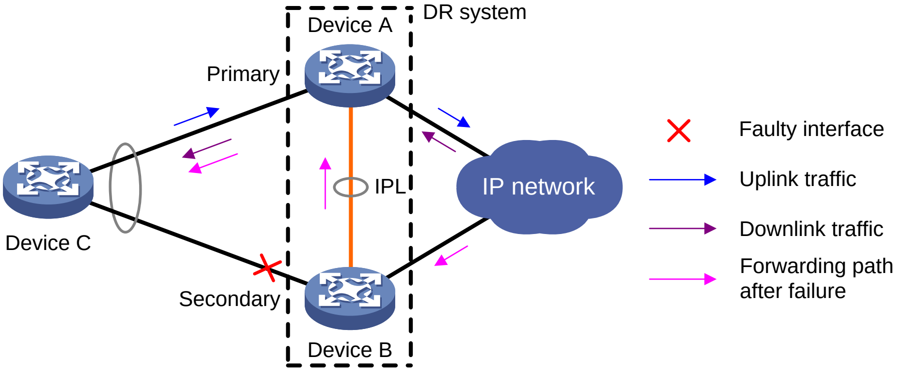
When the DR interface of one DR member device fails, the DR system forwards traffic through the other DR member device.

As shown in Figure 3, Device A and Device B form a DR system, to which Device C is attached through a multichassis aggregation. If traffic to Device C arrives at Device B after the DR interface connected Device B to Device C has failed, the DR system forwards the traffic as follows:

1. Device B sends the traffic to Device A over the IPL.
2. Device A forwards the downlink traffic received from the IPL to Device C.

After the faulty DR interface comes up, Device B forwards traffic to Device C through the DR interface.

Figure 3 DR interface failure handling mechanism



IPL failure handling mechanism

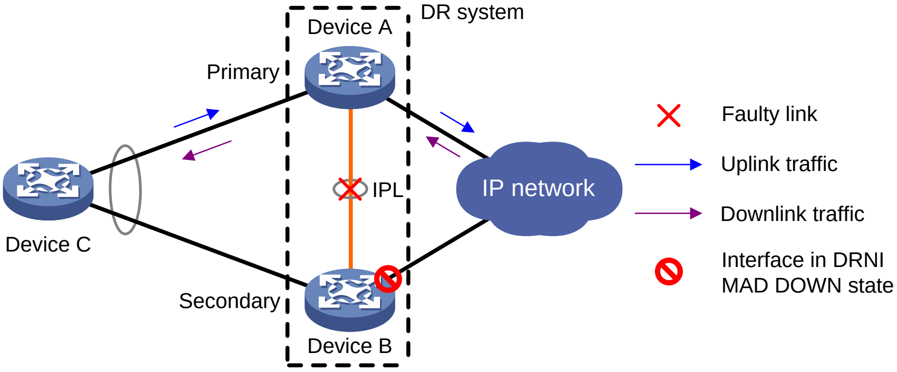
As shown in Figure 4, multi-active collision occurs if the IPL goes down while the keepalive link is up. To avoid network issues, the secondary DR device sets all network interfaces to DRNI MAD DOWN state, except for the following interfaces:

- Interfaces excluded from the MAD shutdown action by IRF.
- Interfaces excluded from the MAD shutdown action by DRNI.

In this situation, the primary DR device forwards all traffic for the DR system.

When the IPP comes up, the secondary DR device does not bring up the network interfaces immediately. Instead, it starts a delay timer and begins to recover data from the primary DR device. When the delay timer expires, the secondary DR device brings up all network interfaces.

Figure 4 IPL failure handling mechanism

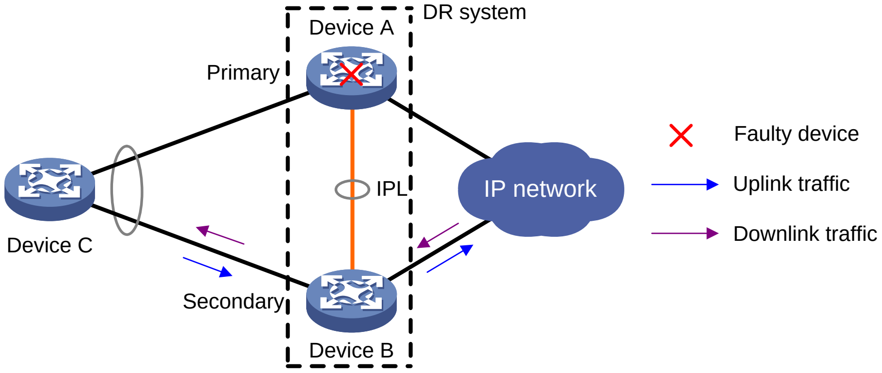


Device failure handling mechanism

As shown in Figure 5, when the primary DR device fails, the secondary DR device takes over the primary role to forward all traffic for the DR system. When the faulty device recovers, it becomes the secondary DR device.

When the secondary DR device fails, the primary DR device forwards all traffic for the DR system.

Figure 5 Device failure handling mechanism

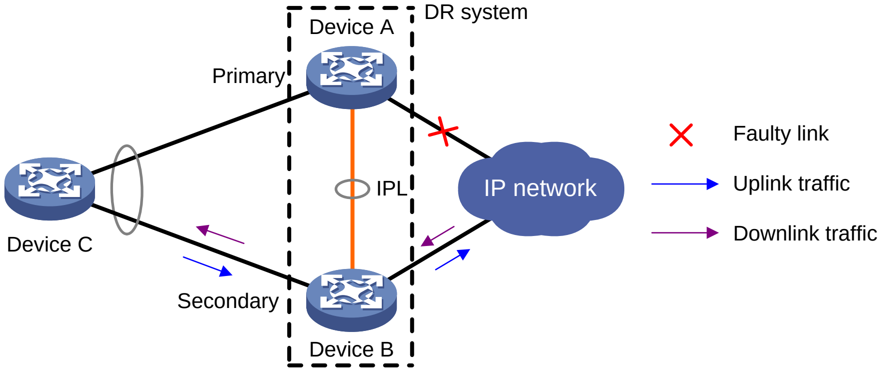


Uplink failure handling mechanism

Uplink failure does not interrupt traffic forwarding of the DR system. As shown in Figure 6, when the uplink of Device A fails, Device A passes traffic destined for the IP network to Device B for forwarding.

To enable faster traffic switchover in response to an uplink failure and minimize traffic losses, configure Monitor Link to associate the DR interfaces with the uplink interfaces. When the uplink interface of a DR member device fails, that device shuts down its DR interface for the other DR member device to forward all traffic of Device C. For more information about Monitor Link, see *High Availability Configuration Guide*.

Figure 6 Uplink failure handling mechanism



Protocols and standards

IEEE P802.1AX-REV™/D4.4c, *Draft Standard for Local and Metropolitan Area Networks*

Restrictions and guidelines: DRNI configuration

For the DR member devices to be identified as one DR system, you must configure the same DR system MAC address and DR system priority on them. You must assign different DR system numbers to the DR member devices.

For correct traffic forwarding, make sure the DR member devices are consistent in service feature settings.

For DRNI to operate correctly, follow these guidelines:

- Do not configure automatic link aggregation on a DR system.

- Do not assign DR interfaces or IPPs to a port isolation group. For more information about port isolation, see "Configuring port isolation."

When you configure a DR interface, follow these restrictions and guidelines:

- The **`link-aggregation selected-port maximum`** and **`link-aggregation selected-port minimum`** commands do not take effect on a DR interface.
- If you execute the **`display link-aggregation verbose`** command for a DR interface, the displayed system ID contains the DR system MAC address and the DR system priority.
- If the reference port is a member port of a DR interface, the **`display link-aggregation verbose`** command displays the reference port on both DR member devices.

If a DR member device has a large number of MAC address entries, increase its MAC aging time by using the **`mac-address timer aging`** command. As a best practice, set the MAC aging time to be longer than 20 minutes. For more information about the MAC aging time, see "Configuring the MAC address table."

DRNI tasks at a glance

To configure DRNI, perform the following tasks:

1. Configuring DR system settings
   - Configuring the DR system MAC address
   - Setting the DR system number
   - Setting the DR system priority
2. Setting the DR role priority of the device
3. Configuring DR keepalive settings
   - Configuring DR keepalive packet parameters
   - Setting the DR keepalive interval and timeout timer
4. Excluding an interface from the shutdown action by DRNI MAD
5. Configuring a DR interface
6. Specifying a Layer 2 aggregate interface or VXLAN tunnel interface as the IPP
7. (Optional.) Disabling configuration consistency check

   Configuration consistency check might fail when you upgrade the DR member devices in a DR system. To prevent the DR system from falsely shutting down DR interfaces, you can temporarily disable configuration consistency check.
8. (Optional.) Enabling the short DRCP timeout timer on the IPP or a DR interface
9. (Optional.) Setting the keepalive hold timer for identifying the cause of IPL down events
10. Configuring DR system auto-recovery
11. (Optional.) Setting the data restoration interval

Configuring DR system settings

Configuring the DR system MAC address

Restrictions and guidelines

Changing the DR system MAC address causes DR system split. When you perform this task on a live network, make sure you are fully aware of its impact.

The DR system MAC address uniquely identifies the DR system on the network. For the DR member devices to be identified as one DR system, you must configure the same DR system MAC address on them. As a best practice, use the bridge MAC address of one DR member device as the DR system MAC address.

Procedure

1. Enter system view.

   `system-view`

2. Configure the DR system MAC address.

   `drni system-mac` *`mac-address`*

   By default, the DR system MAC address is not configured.

Setting the DR system number

Restrictions and guidelines

Changing the DR system number causes DR system split. When you perform this task on a live network, make sure you are fully aware of its impact.

You must assign different DR system numbers to the DR member devices in a DR system.

Procedure

1. Enter system view.

   `system-view`

2. Set the DR system number.

   `drni system-number` *`system-number`*

   By default, the DR system number is not set.

Setting the DR system priority

About the DR system priority

A DR system uses its DR system priority as the system LACP priority to communicate with the remote aggregation system.

Restrictions and guidelines

Changing the DR system priority causes DR system split. When you perform this task on a live network, make sure you are fully aware of its impact.

You must configure the same DR system priority for the DR member devices in a DR system.

Procedure

1. Enter system view.

   `system-view`

2. Set the DR system priority.

   `drni system-priority` *`system-priority`*

   By default, the DR system priority is 32768.

Setting the DR role priority of the device

About the DR role priority

DRNI assigns the primary or secondary role to a DR member device based on its DR role priority. The smaller the priority value, the higher the priority. If the DR member devices in a DR system use the same DR role priority, the device with the lower bridge MAC address is assigned the primary role.

Restrictions and guidelines

To prevent a primary/secondary role switchover from causing network flapping, avoid changing the DR priority assignment after the DR system is established.

Procedure

1. Enter system view.

   system-view

2. Set the DR role priority of the device.

   drni role priority *priority-value*

   By default, the DR role priority of the device is 32768.

Configuring DR keepalive settings

Restrictions and guidelines for configuring DR keepalive settings

Use Layer 3 Ethernet interfaces or management Ethernet interfaces to set up the keepalive link.

Make sure the two ends use the same keepalive settings. DR member devices check the peer keepalive settings for consistency. If an inconsistency is found, the device will prompt for configuration revision.

Configuring DR keepalive packet parameters

About DR keepalive packet parameters

Perform this task to specify the parameters for sending DR keepalive packets, such as its source and destination IP addresses.

The device accepts only keepalive packets that are sourced from the specified destination IP address. The keepalive link goes down if the device receives keepalive packets sourced from any other IP address.

Restrictions and guidelines

Make sure the DR member devices in a DR system use the same keepalive destination UDP port.

Procedure

1. Enter system view.

   system-view

2. Configure DR keepalive packet parameters.

   drni keepalive { **ip** | **ipv6** } **destination** { *ipv4-address* | *ipv6-address* } [**source** { *ipv4-address* | *ipv6-address* } | **udp-port** *udp-number* | **vpn-instance** *vpn-instance-name*] *

   By default, the DR keepalive packet parameters are not configured. If you do not specify a source IP address or destination UDP port when you execute this command, the IP address of the outgoing interface and UDP port 6400 are used, respectively.

Setting the DR keepalive interval and timeout timer

About the DR keepalive interval and timeout timer

The device sends keepalive packets at the specified interval to its DR peer. If the device has not received a keepalive packet from the DR peer before the keepalive timeout timer expires, the device determines that the keepalive link is down.

Restrictions and guidelines

The local DR keepalive timeout timer must be two times the DR keepalive interval of the peer at minimum.

Configure the same DR keepalive interval on the DR member devices in the DR system.

Procedure

1. Enter system view.

   `system-view`

2. Set the DR keepalive interval and timeout timer.

   `drni keepalive interval` *`interval`* [**`timeout`** *`timeout`*]

   By default, the DR keepalive interval is 1000 milliseconds, and the DR keepalive timeout timer is 5 seconds.

Excluding an interface from the shutdown action by DRNI MAD

Restrictions and guidelines

Follow these restrictions and guidelines when you exclude interfaces from the MAD shutdown action by DRNI:

- For correct keepalive detection, you must exclude the interfaces used for keepalive detection from the shutdown action by DRNI MAD.
- If the IPP is a tunnel interface, you must exclude the traffic outgoing interface for the tunnel from the shutdown action by DRNI MAD.
- For DR member devices to synchronize ARP entries, you must exclude the VLAN interfaces of the VLANs to which the DR interfaces and IPPs belong from the shutdown action.

To view interfaces excluded from the MAD shutdown action, see the **Excluded ports (user-configured)** field in the output from the **`display drni mad verbose`** command.

If you exclude an interface that is already in DRNI MAD DOWN state from the MAD shutdown action, the interface stays in that state. It will not come up automatically.

Procedure

1. Enter system view.

   `system-view`

2. Exclude an interface from the MAD shutdown action by DRNI.

   `drni mad exclude interface` *`interface-type interface-number`*

   By default, DRNI MAD shuts down all network interfaces when detecting a multi-active collision, except for the network interfaces set by the system to not shut down.

Configuring a DR interface

Restrictions and guidelines

The device can have multiple DR interfaces. However, you can assign a Layer 2 aggregate interface to only one DR group.

A Layer 2 aggregate interface cannot operate as both IPP and DR interface.

To improve forwarding efficiency, exclude the DR interface on the secondary DR device from the shutdown action by DRNI MAD. This action enables the DR interface to forward traffic immediately after a multi-active collision is removed without having to wait for the secondary DR device to complete entry restoration.

Procedure

1. Enter system view.

   `system-view`

2. Enter Layer 2 aggregate interface view.

   `interface bridge-aggregation` *`interface-number`*

3. Assign the aggregate interface to a DR group.

   `port drni group` *`group-id`*

Specifying a Layer 2 aggregate interface or VXLAN tunnel interface as the IPP

Restrictions and guidelines

A DR member device can have only one IPP. A Layer 2 aggregate interface or VXLAN tunnel interface cannot operate as both IPP and DR interface.

Do not associate a VXLAN tunnel interface with a VXLAN if you use it as the IPP. You can use a VXLAN tunnel interface as an IPP only in an EVPN network. For more information about EVPN, see *EVPN Configuration Guide*.

As a best practice to reduce the impact of interface flapping on upper-layer services, execute the **`link-delay`** command on the IPP. For more information about this command, see Ethernet link aggregation commands in *Layer 2—LAN Switching Command Reference*.

By default, MAC address learning is enabled on the IPP. This feature is not configurable on the IPP. For more information about the MAC address learning feature, see "Configuring the MAC address table."

To prevent data synchronization failure, you must set the same maximum jumbo frame length on the IPPs of the DR member devices. For more information about jumbo frames, see "Configuring Ethernet link aggregation."

Do not use the MAC address of a remote MEP for CFD tests on IPPs. These tests cannot work on IPPs. For more information about CFD, see *High Availability Configuration Guide*.

Procedure

1. Enter system view.

   `system-view`

2. Enter interface view.
   - Enter Layer 2 aggregate interface view.

     `interface bridge-aggregation` *`interface-number`*

- Enter VXLAN tunnel interface view.
  interface tunnel *number*

3. Specify the interface as the IPP.
   port drni intra-portal-port *port-id*

Disabling configuration consistency check

About disabling configuration consistency check

To ensure that the DR system can operate correctly, DRNI by default performs configuration consistency check when the DR system is set up.

Configuration consistency check might fail when you upgrade the DR member devices in a DR system. To prevent the DR system from falsely shutting down DR interfaces, you can temporarily disable configuration consistency check.

Restrictions and guidelines

Make sure the DR member devices use the same setting for configuration consistency check.

Procedure

1. Enter system view.
   system-view
2. Disable configuration consistency check.
   drni consistency-check disable
   By default, configuration consistency check is enabled.

Enabling the short DRCP timeout timer on the IPP or a DR interface

About the DRCP timeout timer

By default, the IPP or a DR interface uses the 90-second long DRCP timeout timer. To detect peer interface down events more quickly, enable the 3-second short DRCP timeout timer on the interface.

Restrictions and guidelines

To avoid traffic interruption during an ISSU or DRNI process restart, disable the short DRCP timeout timer before you perform an ISSU or DRNI process restart. For more information about ISSU, see *Fundamentals Configuration Guide*.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   - Enter Layer 2 aggregate interface view.
     interface bridge-aggregation *interface-number*
   - Enter VXLAN tunnel interface view.
     interface tunnel *number*
3. Enable the short DRCP timeout timer.
   drni drcp period short
   By default, an interface uses the long DRCP timeout timer (90 seconds).

Setting the keepalive hold timer for identifying the cause of IPL down events

About the keepalive hold timer

The keepalive hold timer starts when the IPL goes down. The keepalive hold timer specifies the amount of time that the device uses to identify the cause of an IPL down event.

- If the device receives keepalive packets from the DR peer before the timer expires, the IPL is down because the IPL fails.
- If the device does not receive keepalive packets from the DR peer before the timer expires, the IPL is down because the peer DR device fails.

Restrictions and guidelines

For the DR member device to correctly determine the cause of an IPL down event, make sure the keepalive hold timer is longer than the keepalive interval and is shorter than the keepalive timeout timer.

If you use DRNI and VRRP together, make sure the keepalive hold timer is shorter than the interval at which the VRRP master sends VRRP advertisements. Violation of this restriction might cause a VRRP master/backup switchover to occur before IPL failure is confirmed. To set the interval at which the VRRP master sends VRRP advertisements, use the **`vrrp vrid timer advertise`** command. For more information about this command, see *High Availability Command Reference*.

Procedure

1. Enter system view.

   ```
   system-view
   ```

2. Set the keepalive hold timer.

   ```
   drni keepalive hold-time value
   ```

   By default, the keepalive hold timer is 3 seconds.

Configuring DR system auto-recovery

About DR system auto-recovery

If only one DR member device recovers after the entire DR system reboots, auto-recovery enables that member device to remove its DR interfaces from the DRNI DOWN interface list.

- If that member device has up DR interfaces, it takes over the primary role when the reload delay timer expires and forwards traffic.
- If that member device does not have up DR interfaces, it is stuck in the None role and does not forward traffic.

If auto-recovery is disabled, that DR member device will be stuck in the None role with all its DR interfaces being DRNI DOWN after it recovers.

Restrictions and guidelines

If both DR member devices recover and have up DR interfaces after the entire DR system reboots, active-active situation might occur if both IPL and keepalive links were down when the reload delay timer expires. If this rare situation occurs, examine the IPL and keepalive links and restore them.

To avoid incorrect role preemption, make sure the reload delay timer is longer than the amount of time required for the device to restart.

Procedure

1. Enter system view.

system-view

2. Configure DR system auto-recovery.

   drni auto-recovery reload-delay *delay-value*

   By default, DR system auto-recovery is not configured. The reload delay timer is not set.

Setting the data restoration interval

About the data restoration interval

The data restoration interval specifies the maximum amount of time for the secondary DR device to synchronize data with the primary DR device during DR system setup. Within the data restoration interval, the secondary DR device sets all network interfaces to DRNI MAD DOWN state, except for the following interfaces:

- Interfaces excluded from the MAD shutdown action by IRF.
- Interfaces excluded from the MAD shutdown action by DRNI.

When the data restoration interval expires, the secondary DR device brings up all network interfaces.

Restrictions and guidelines

Increase the data restoration interval as needed for the following purposes:

- Avoid packet loss and forwarding failure that might occur when the amount of data is large or when you perform an ISSU between the DR member devices.
- Avoid DR interface flapping that might occur if type 1 configuration consistency check fails after the DR interfaces come up upon expiration of the data restoration interval.

Procedure

1. Enter system view.

   system-view

2. Set the data restoration interval.

   drni restore-delay *value*

   By default, the data restoration interval is 30 seconds.

Displaying and maintaining DRNI

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display information about the configuration consistency check done by DRNI.	**display drni consistency** { **type1** | **type2** } { **global** | **interface** *interface-type interface-number* }
Display DRCPDU statistics.	**display drni drcp statistics** [**interface** *interface-type interface-number*]
Display DR keepalive packet statistics.	**display drni keepalive**
Display detailed DRNI MAD information.	**display drni mad verbose**
Display DR role information.	**display drni role**
Display brief information about the IPP and DR interfaces.	**display drni summary**

Task	Command
Display the DR system settings.	**display drni system**
Display detailed information about the IPP and DR interfaces.	**display drni verbose** [**interface bridge-aggregation** *interface-number*]
Clear DRCPDU statistics.	**reset drni drcp statistics** [**interface** *interface-list*]

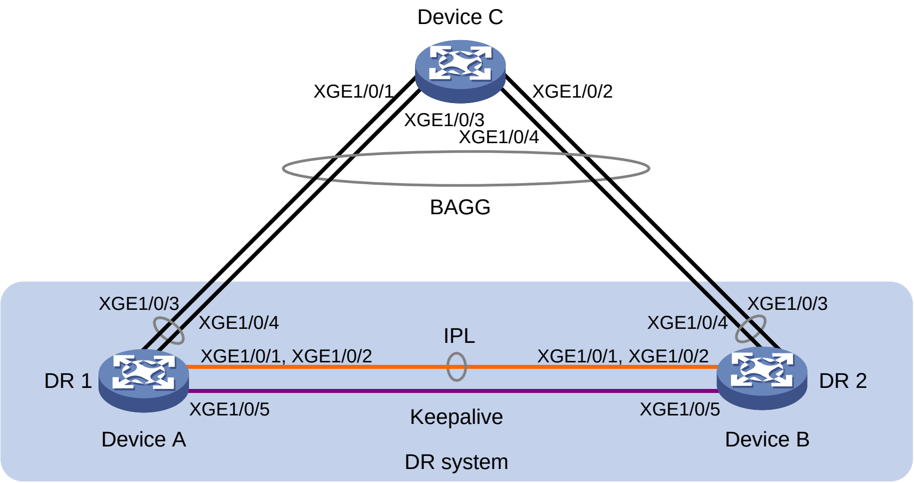
DRNI configuration examples

Example: Configuring basic DRNI functions

Network configuration

As shown in Figure 7, configure DRNI on Device A and Device B to establish a multichassis aggregate link with Device C.

Figure 7 Network diagram



Procedure

1. Configure Device A:

# Configure DR system settings.

```
<DeviceA> system-view
[DeviceA] drni system-mac 1-1-1
[DeviceA] drni system-number 1
[DeviceA] drni system-priority 123
```

# Configure DR keepalive packet parameters.

```
[DeviceA] drni keepalive ip destination 1.1.1.1 source 1.1.1.2
```

# Set the link mode of Ten-GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceA] interface ten-gigabitethernet 1/0/5
[DeviceA-Ten-GigabitEthernet1/0/5] port link-mode route
[DeviceA-Ten-GigabitEthernet1/0/5] ip address 1.1.1.2 24
[DeviceA-Ten-GigabitEthernet1/0/5] quit
```

# Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface ten-gigabitethernet 1/0/5
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] quit
```

# Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 3.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

# Specify Bridge-Aggregation 3 as the IPP.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation3] quit
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[DeviceA] interface bridge-aggregation 4
[DeviceA-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation4] quit
```

# Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 4.

```
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 4
[DeviceA-Ten-GigabitEthernet1/0/3] quit
[DeviceA] interface ten-gigabitethernet 1/0/4
[DeviceA-Ten-GigabitEthernet1/0/4] port link-aggregation group 4
[DeviceA-Ten-GigabitEthernet1/0/4] quit
```

# Assign Bridge-Aggregation 4 to DR group 4.

```
[DeviceA] interface bridge-aggregation 4
[DeviceA-Bridge-Aggregation4] port drni group 4
[DeviceA-Bridge-Aggregation4] quit
```

2. Configure Device B:

# Configure DR system settings.

```
<DeviceB> system-view
[DeviceB] drni system-mac 1-1-1
[DeviceB] drni system-number 2
[DeviceB] drni system-priority 123
```

# Configure DR keepalive packet parameters.

```
[DeviceB] drni keepalive ip destination 1.1.1.2 source 1.1.1.1
```

# Set the link mode of Ten-GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface ten-gigabitethernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] port link-mode route
[DeviceB-Ten-GigabitEthernet1/0/5] ip address 1.1.1.1 24
[DeviceB-Ten-GigabitEthernet1/0/5] quit
```

# Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface ten-gigabitethernet 1/0/5
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] quit
```

# Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 3.

```
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceB-Ten-GigabitEthernet1/0/1] quit
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

# Specify Bridge-Aggregation 3 as the IPP.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port drni intra-portal-port 1
[DeviceB-Bridge-Aggregation3] quit
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[DeviceB] interface bridge-aggregation 4
[DeviceB-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation4] quit
```

# Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 4.

```
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port link-aggregation group 4
[DeviceB-Ten-GigabitEthernet1/0/3] quit
[DeviceB] interface ten-gigabitethernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] port link-aggregation group 4
[DeviceB-Ten-GigabitEthernet1/0/4] quit
```

# Assign Bridge-Aggregation 4 to DR group 4.

```
[DeviceB] interface bridge-aggregation 4
[DeviceB-Bridge-Aggregation4] port drni group 4
[DeviceB-Bridge-Aggregation4] quit
```

3. Configure Device C:

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 4
[DeviceC-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation4] quit
```

# Assign Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4 to aggregation group 4.

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

Verifying the configuration

# Verify that the keepalive link is working correctly on Device A.

```
[DeviceA] display drni keepalive
Neighbor keepalive link status: Up
Neighbor is alive for: 104 s, 16 ms
Last keepalive packet sending status: Successful
Last keepalive packet sending time: 2017/03/09 10:12:09 620 ms
Last keepalive packet receiving status: Successful
Last keepalive packet receiving time: 2017/03/09 10:12:09 707 ms

Distributed relay keepalive parameters:
Destination IP address: 1.1.1.1
Source IP address: 1.1.1.2
Keepalive UDP port : 6400
Keepalive VPN name : N/A
Keepalive interval : 1000 ms
Keepalive timeout  : 5 sec
Keepalive hold time: 3 sec
```

# Verify that the IPP and the DR interface are working correctly on Device A.

```
[DeviceA] display drni summary
Global consistency check           : SUCCESS
Inconsistent type 1 global settings: -
IPP             IPP ID        State
BAGG3           1             UP
DR interface    DR group ID   State   Check result   Type 1 inconsistency
BAGG4           4             UP      SUCCESS        -
[DeviceA] display drni verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired
IPP/IPP ID: BAGG3/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports (index): XGE1/0/1 (1), XGE1/0/2 (2)
Peer Selected ports indexes: 1, 2

DR interface/DR group ID: BAGG4/4
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports (index): XGE1/0/3 (16387), XGE1/0/4 (16388)
Peer Selected ports indexes: 32771, 32772
```

# Verify that all member ports of aggregation group 4 are in Selected state on Device C, which indicates a successful link aggregation between the DR system and Device C.

```
[DeviceC] display link-aggregation verbose bridge-aggregation 4
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Aggregate Interface: Bridge-Aggregation4
Creation Mode: Manual
```

```
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 2e56-cbae-0600
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  XGE1/0/1(R)          S         32768    1        1                     {ACDEF}
  XGE1/0/2             S         32768    2        1                     {ACDEF}
  XGE1/0/3             S         32768    3        1                     {ACDEF}
  XGE1/0/4             S         32768    4        1                     {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  XGE1/0/1             32768    16387    40004    0x7b  , 0001-0001-0001 {ACDEF}
  XGE1/0/2             32768    16388    40004    0x7b  , 0001-0001-0001 {ACDEF}
  XGE1/0/3             32768    32771    40004    0x7b  , 0001-0001-0001 {ACDEF}
  XGE1/0/4             32768    32772    40004    0x7b  , 0001-0001-0001 {ACDEF}
```

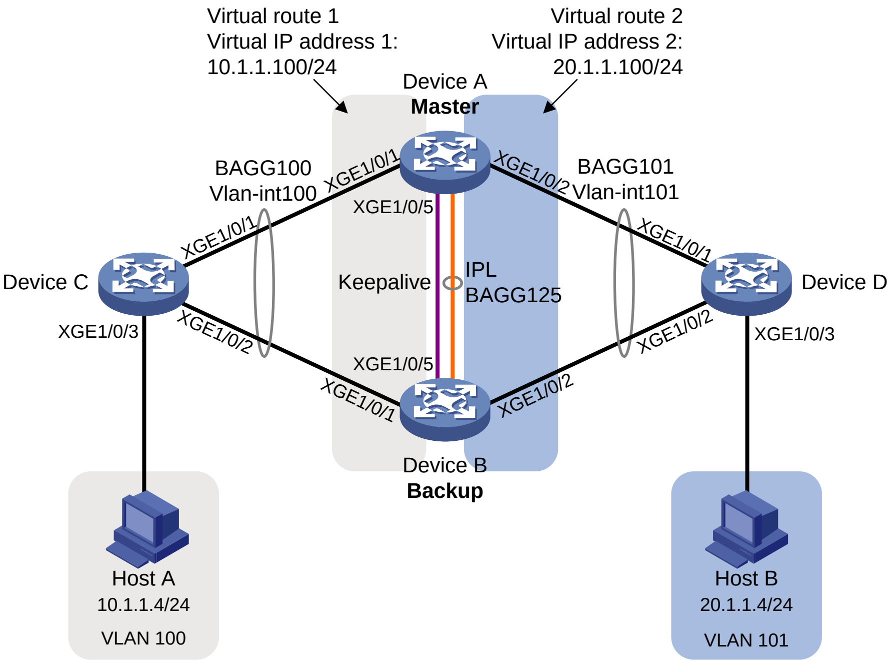
Example: Configuring Layer 3 gateways on a DR system

Network configuration

As shown in Figure 8:

- Configure Device A and Device B as a DR system to establish one multichassis aggregate link with Device C and one with Device D.
- Set up a keepalive link between Ten-GigabitEthernet 1/0/5 of Device A and Ten-GigabitEthernet 1/0/5 of Device B, and exclude the interfaces from the shutdown action by DRNI MAD.
- Configure two VRRP groups on Device A and Device B to provide gateway services for VLAN 100 and VLAN 200. Configure Device A as the master of the VRRP groups.

Figure 8 Network diagram



Procedure

1. Configure Device A:

   # Configure DR system settings.

   ```
   <DeviceA> system-view
   [DeviceA] drni system-mac 1-1-1
   [DeviceA] drni system-number 1
   [DeviceA] drni system-priority 123
   ```

   # Configure DR keepalive parameters.

   ```
   [DeviceA] drni keepalive ip destination 1.1.1.2 source 1.1.1.1
   ```

   # Set the link mode of Ten-GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/5
   [DeviceA-Ten-GigabitEthernet1/0/5] port link-mode route
   [DeviceA-Ten-GigabitEthernet1/0/5] ip address 1.1.1.1 24
   [DeviceA-Ten-GigabitEthernet1/0/5] quit
   ```

   # Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

   ```
   [DeviceA] drni mad exclude interface ten-gigabitethernet 1/0/5
   ```

   # Create Layer 2 dynamic aggregate interface Bridge-Aggregation 125, and specify it as the IPP.

   ```
   [DeviceA] interface bridge-aggregation 125
   [DeviceA-Bridge-Aggregation125] link-aggregation mode dynamic
   [DeviceA-Bridge-Aggregation125] port drni intra-portal-port 1
   [DeviceA-Bridge-Aggregation125] quit
   ```

   # Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 125.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/3
   [DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 125
   [DeviceA-Ten-GigabitEthernet1/0/3] quit
   [DeviceA] interface Ten-GigabitEthernet 1/0/4
   [DeviceA-Ten-GigabitEthernet1/0/4] port link-aggregation group 125
   [DeviceA-Ten-GigabitEthernet1/0/4] quit
   ```

   # Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100, and assign it to DR group 1.

   ```
   [DeviceA] interface bridge-aggregation 100
   [DeviceA-Bridge-Aggregation100] link-aggregation mode dynamic
   [DeviceA-Bridge-Aggregation100] port drni group 1
   [DeviceA-Bridge-Aggregation100] quit
   ```

   # Assign Ten-GigabitEthernet 1/0/1 to aggregation group 100.

   ```
   [DeviceA] interface ten-gigabitethernet 1/0/1
   [DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 100
   [DeviceA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101, and assign it to DR group 2.

   ```
   [DeviceA] interface bridge-aggregation 101
   [DeviceA-Bridge-Aggregation101] link-aggregation mode dynamic
   [DeviceA-Bridge-Aggregation101] port drni group 2
   [DeviceA-Bridge-Aggregation101] quit
   ```

   # Assign Ten-GigabitEthernet 1/0/2 to aggregation group 101.

```
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 101
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

# Create VLAN 100 and VLAN 101.

```
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 101
[DeviceA-vlan101] quit
```

# Set the link type of Bridge-Aggregation 100 to trunk, and assign it to VLAN 100.

```
[DeviceA] interface bridge-aggregation 100
[DeviceA-Bridge-Aggregation100] port link-type trunk
[DeviceA-Bridge-Aggregation100] port trunk permit vlan 100
[DeviceA-Bridge-Aggregation100] quit
```

# Set the link type of Bridge-Aggregation 101 to trunk, and assign it to VLAN 101.

```
[DeviceA] interface bridge-aggregation 101
[DeviceA-Bridge-Aggregation101] port link-type trunk
[DeviceA-Bridge-Aggregation101] port trunk permit vlan 101
[DeviceA-Bridge-Aggregation101] quit
```

# Set the link type of Bridge-Aggregation 125 to trunk, and assign it to VLAN 100 and VLAN 101.

```
[DeviceA] interface bridge-aggregation 125
[DeviceA-Bridge-Aggregation125] port link-type trunk
[DeviceA-Bridge-Aggregation125] port trunk permit vlan 100 101
[DeviceA-Bridge-Aggregation125] quit
```

# Create VLAN-interface 100 and VLAN-interface 101, and assign IP addresses to them.

```
[DeviceA] interface vlan-interface 100
[DeviceA-vlan-interface100] ip address 10.1.1.1 24
[DeviceA-vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-vlan-interface101] ip address 20.1.1.1 24
[DeviceA-vlan-interface101] quit
```

# Exclude VLAN-interface 100 and VLAN-interface 101 from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface vlan-interface 100
[DeviceA] drni mad exclude interface vlan-interface 101
```

# Configure OSPF.

```
[DeviceA] ospf
[DeviceA-ospf-1] import-route direct
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

# Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 10.1.1.100.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 virtual-ip 10.1.1.100
```

# Set the priority of Device A (primary DR device) to 200 for it to become the master in VRRP group 1.

```
[DeviceA-Vlan-interface100] vrrp vrid 1 priority 200
[DeviceA-Vlan-interface100] quit
```

# Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 20.1.1.100.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp vrid 2 virtual-ip 20.1.1.100
```

# Set the priority of Device A (primary DR device) to 200 for it to become the master in VRRP group 2.

```
[DeviceA-Vlan-interface101] vrrp vrid 2 priority 200
[DeviceA-Vlan-interface101] quit
```

2. Configure Device B:

# Configure DR system settings.

```
<DeviceB> system-view
[DeviceB] drni system-mac 1-1-1
[DeviceB] drni system-number 2
[DeviceB] drni system-priority 123
```

# Configure DR keepalive parameters.

```
[DeviceB] drni keepalive ip destination 1.1.1.1 source 1.1.1.2
```

# Set the link mode of Ten-GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface ten-gigabitethernet 1/0/5
[DeviceB-Ten-GigabitEthernet1/0/5] port link-mode route
[DeviceB-Ten-GigabitEthernet1/0/5] ip address 1.1.1.2 24
[DeviceB-Ten-GigabitEthernet1/0/5] quit
```

# Exclude the interface used for DR keepalive detection (Ten-GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface ten-gigabitethernet 1/0/5
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 125, and specify it as the IPP.

```
[DeviceB] interface bridge-aggregation 125
[DeviceB-Bridge-Aggregation125] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation125] port drni intra-portal-port 1
[DeviceB-Bridge-Aggregation125] quit
```

# Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to aggregation group 125.

```
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port link-aggregation group 125
[DeviceB-Ten-GigabitEthernet1/0/3] quit
[DeviceB] interface ten-gigabitethernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] port link-aggregation group 125
[DeviceB-Ten-GigabitEthernet1/0/4] quit
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100, and assign it to DR group 1.

```
[DeviceB] interface bridge-aggregation 100
[DeviceB-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation100] port drni group 1
[DeviceB-Bridge-Aggregation100] quit
```

# Assign Ten-GigabitEthernet 1/0/1 to aggregation group 100.

```
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-aggregation group 100
```

```
[DeviceB-Ten-GigabitEthernet1/0/1] quit
```

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101, and assign it to DR group 2.

```
[DeviceB] interface bridge-aggregation 101
[DeviceB-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation101] port drni group 2
[DeviceB-Bridge-Aggregation101] quit
```

# Assign Ten-GigabitEthernet 1/0/2 to aggregation group 101.

```
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-aggregation group 101
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

# Create VLAN 100 and VLAN 101.

```
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] vlan 101
[DeviceB-vlan101] quit
```

# Set the link type of Bridge-Aggregation 100 to trunk, and assign it to VLAN 100.

```
[DeviceB] interface bridge-aggregation 100
[DeviceB-Bridge-Aggregation100] port link-type trunk
[DeviceB-Bridge-Aggregation100] port trunk permit vlan 100
[DeviceB-Bridge-Aggregation100] quit
```

# Set the link type of Bridge-Aggregation 101 to trunk, and assign it to VLAN 101.

```
[DeviceB] interface bridge-aggregation 101
[DeviceB-Bridge-Aggregation101] port link-type trunk
[DeviceB-Bridge-Aggregation101] port trunk permit vlan 101
[DeviceB-Bridge-Aggregation101] quit
```

# Set the link type of Bridge-Aggregation 125 to trunk, and assign it to VLAN 100 and VLAN 101.

```
[DeviceB] interface bridge-aggregation 125
[DeviceB-Bridge-Aggregation125] port link-type trunk
[DeviceB-Bridge-Aggregation125] port trunk permit vlan 100 101
[DeviceB-Bridge-Aggregation125] quit
```

# Create VLAN-interface 100 and VLAN-interface 101, and assign IP addresses to them.

```
[DeviceB] interface vlan-interface 100
[DeviceB-vlan-interface100] ip address 10.1.1.2 24
[DeviceB-vlan-interface100] quit
[DeviceB] interface vlan-interface 101
[DeviceB-vlan-interface101] ip address 20.1.1.2 24
[DeviceB-vlan-interface101] quit
```

# Exclude VLAN-interface 100 and VLAN-interface 101 from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface vlan-interface 100
[DeviceB] drni mad exclude interface vlan-interface 101
```

# Configure OSPF.

```
[DeviceB] ospf
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

```
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

# Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 10.1.1.100.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] vrrp vrid 1 virtual-ip 10.1.1.100
[DeviceB-Vlan-interface100] quit
```

# Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 20.1.1.100.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] vrrp vrid 2 virtual-ip 20.1.1.100
[DeviceB-Vlan-interface101] quit
```

3. Configure Device C:

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100.

```
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 100
[DeviceC-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation100] quit
```

# Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 100.

```
[DeviceC] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/2
[DeviceC-if-range] port link-aggregation group 100
[DeviceC-if-range] quit
```

# Create VLAN 100.

```
[DeviceC] vlan 100
[DeviceC-vlan100] quit
```

# Set the link type of Bridge-Aggregation 100 to trunk, and assign it to VLAN 100.

```
[DeviceC] interface bridge-aggregation 100
[DeviceC-Bridge-Aggregation100] port link-type trunk
[DeviceC-Bridge-Aggregation100] port trunk permit vlan 100
[DeviceC-Bridge-Aggregation100] quit
```

# Set the link type of Ten-GigabitEthernet 1/0/3 to trunk, and assign it to VLAN 100.

```
[DeviceC] interface ten-gigabitethernet 1/0/3
[DeviceC-Ten-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-Ten-GigabitEthernet1/0/3] port trunk permit vlan 100
[DeviceC-Ten-GigabitEthernet1/0/3] quit
```

# Create VLAN-interface 100, and assign it an IP address.

```
[DeviceC] interface vlan-interface 100
[DeviceC-vlan-interface100] ip address 10.1.1.3 24
[DeviceC-vlan-interface100] quit
```

# Configure OSPF.

```
[DeviceC] ospf
[DeviceC-ospf-1] import-route direct
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

4. Configure Device D:

# Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101.

```
<DeviceD> system-view
[DeviceD] interface bridge-aggregation 101
[DeviceD-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation101] quit
```

# Assign Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to aggregation group 101.

```
[DeviceD] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/2
[DeviceD-if-range] port link-aggregation group 101
[DeviceD-if-range] quit
```

# Create VLAN 101.

```
[DeviceD] vlan 101
[DeviceD-vlan101] quit
```

# Set the link type of Bridge-Aggregation 101 to trunk, and assign it to VLAN 101.

```
[DeviceD] interface bridge-aggregation 101
[DeviceD-Bridge-Aggregation101] port link-type trunk
[DeviceD-Bridge-Aggregation101] port trunk permit vlan 101
[DeviceD-Bridge-Aggregation101] quit
```

# Set the link type of Ten-GigabitEthernet 1/0/3 to trunk, and assign it to VLAN 101.

```
[DeviceD] interface ten-gigabitethernet 1/0/3
[DeviceD-Ten-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-Ten-GigabitEthernet1/0/3] port trunk permit vlan 101
[DeviceD-Ten-GigabitEthernet1/0/3] quit
```

# Create VLAN-interface 101, and assign it an IP address.

```
[DeviceD] interface vlan-interface 101
[DeviceD-vlan-interface101] ip address 20.1.1.3 24
[DeviceD-vlan-interface101] quit
```

# Configure OSPF.

```
[DeviceD] ospf
[DeviceD-ospf-1] import-route direct
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

Verifying the configuration

# Verify that Device C has established OSPF neighbor relationships with Device A and Device B.

```
[DeviceC] display ospf peer

         OSPF Process 1 with Router ID 10.1.1.3
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 20.1.1.1        10.1.1.1        1   37         Full/DR           Vlan100
 20.1.1.2        10.1.1.2        1   32         Full/BDR          Vlan100
```

# Verify that Device D has established OSPF neighbor relationships with Device A and Device B.

```
[DeviceD] display ospf peer

         OSPF Process 1 with Router ID 20.1.1.3
```

```
              Neighbor Brief Information

Area: 0.0.0.0
Router ID       Address         Pri Dead-Time  State            Interface
20.1.1.1        20.1.1.1        1   38         Full/DR          Vlan101
20.1.1.2        20.1.1.2        1   37         Full/BDR         Vlan101
```

# Verify that Host A and Host B can ping each other. (Details not shown.)