Contents

DRNI commands

display drni consistency

Use **display drni consistency** to display information about configuration consistency check done by DRNI.

Syntax

display drni consistency { **type1** | **type2** } { **global** | **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

type1: Specifies type 1 configuration consistency check.

type2: Specifies type 1 configuration consistency check.

global: Specifies global information.

interface *interface-type interface-number*: Specifies a DR interface by its type and number.

Examples

Display global information about type 1 configuration consistency check.

```
<Sysname> display drni consistency type1 global
VLAN consistency check: Success
Local IPP interface link type: Access
Peer IPP interface link type: Access
Local IPP interface PVID: 1
Peer IPP interface PVID: 1

STP consistency check: Success
Local global STP protocol state: Enabled
Peer global STP protocol state: Enabled
Local STP mode: MSTP
Peer STP mode: MSTP
Local MST region name: text
Peer MST region name: text
Local MSTP revision level: 0
Peer MSTP revision level: 0
MSTP VLAN-to-instance mappings: Consistent
STP-enabled VLANs: Consistent
```

Display global information about type 2 configuration consistency check.

```
<Sysname> display drni consistency type2 global
VLAN consistency check: Success
Local VLAN interfaces:
  2-10, 15, 20-30, 40, 50
```

```
Peer VLAN interfaces:
  2-10, 15, 20-30, 40, 50
The passing VLANs-tagged or PVID on Local IPP:
  1
The passing VLANs-tagged or PVID on Peer IPP:
  1
Invalid VLANs on Local IPP interface:
  None
```

Display information about type 1 configuration consistency check on DR interface Bridge-Aggregation 1.

```
<Sysname> display drni consistency type1 interface bridge-aggregation 1
LAGG consistency check: Success
Local aggregation mode: Dynamic
Peer aggregation mode: Dynamic

STP consistency check: Success
Local STP protocol state: Enabled
Peer STP protocol state: Enabled

VLAN consistency check :Success
Local link type: Trunk
Peer link type: Trunk
Local PVID: 10
Peer PVID: 10
```

Display information about type 2 configuration consistency check on DR interface Bridge-Aggregation 1.

```
<Sysname> display drni consistency type2 interface bridge-aggregation 1
VLAN consistency check :Success
The passing VLANs-tagged on Local DR interface:
  None
The passing VLANs-tagged on Peer DR interface:
  None
The passing VLANs-untagged on Local DR interface:
  1
The passing VLANs-untagged on Peer DR interface:
  1
Invalid VLANs on Local DR interface:
  None
```

Table 1 Command output

Field	Description
Feature consistency check	Result of configuration consistency check for a feature: • **Success**. • **Failure**.
Local VLAN interfaces Peer VLAN interfaces	VLAN interfaces on the local or peer device. These fields display VLAN interfaces that meet the following conditions: • The interface is up. • The IPP has been assigned to the corresponding VLANs.

Field	Description
	If no VLAN interfaces are present, this field displays **NULL**.
The passing VLANs-tagged or PVID on Local IPP	VLANs of which the local IPP forwards tagged traffic or PVID of which the IPP forwards traffic. This field does not include VLANs that are permitted on the IPP but have not been created yet.
The passing VLANs-tagged or PVID on Peer IPP	VLANs of which the peer IPP forwards tagged traffic or PVID of which the IPP forwards traffic. This field does not include VLANs that are permitted on the IPP but have not been created yet.
Invalid VLANs on Local IPP interface	VLANs of which the local IPP cannot forward traffic because of incomplete or inconsistent VLAN settings: • VLANs to which the IPP is assigned as an untagged member (PVID not included). • VLANs that contain the local IPP but do not contain the peer IPP. If no invalid VLANs exist, this field displays **None**.
The passing VLANs-tagged on Local DR interface The passing VLANs-tagged on Peer DR interface	VLANs of which the local or peer DR interface forwards tagged traffic. These fields do not include VLANs that are permitted on the DR interfaces but have not been created yet.
The passing VLANs-untagged on Local DR interface The passing VLANs-untagged on Peer DR interface	VLANs of which the local or peer DR interface forwards untagged traffic. These fields do not include VLANs that are permitted on the DR interfaces but have not been created yet.
Invalid VLANs on Local DR interface	VLANs of which the local DR interface cannot forward traffic because of incomplete or inconsistent VLAN settings. A VLAN is in this list if it meets one of the following conditions: • The VLAN is permitted on the local DR interface, but it is not in the **passing VLANs-tagged or PVID** list on the local or peer IPP. • The VLAN is in the passing VLANs-tagged or PVID list on the local or peer IPP, but it is not permitted on the local DR interface. • The VLAN has been created on the local DR member device and is permitted on both local and DR interfaces, but it has not been created on the DR peer yet. If no invalid VLANs exist, this field displays **None**.

NOTE:

A VLAN is permitted on an interface if you have assigned the interface to the VLAN as a tagged or untagged member port.

display drni drcp statistics

Use **display drni drcp statistics** to display DRCPDU statistics.

Syntax

display drni drcp statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a Layer 2 aggregate interface or VXLAN tunnel interface by its type and number. If you do not specify this option, the command displays the DRCPDU statistics about the IPP and all DR interfaces.

Examples

Display DRCPDU statistics.

```
<Sysname> display drni drcp statistics
 * indicates the port is the IPP.
Interface type:
BAGG -- Bridge-Aggregation, Tun  -- Tunnel
Interface     State     Sent     Received     Error      Unknown
*BAGG1        UP        6758     5576         50         121
 BAGG5        UP        3324     3300         68         36
 BAGG6        UP        256      124          23         19
 BAGG7        UP        45       41           8          6
```

Table 2 Command output

Field	Description
Interface	Abbreviated interface name. The name of the IPP is prefixed with an asterisk (*).
State	Physical state of the interface: • **UP**. • **DOWN**.
Sent	Number of sent DRCPDUs.
Received	Number of received DRCPDUs.
Error	Number of error DRCPDUs.
Unknown	Number of unrecognized DRCPDUs.

display drni keepalive

Use **display drni keepalive** to display DR keepalive packet statistics.

Syntax

display drni keepalive

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display DR keepalive packet statistics.

```
<Sysname> display drni keepalive
Neighbor keepalive link status: Up
Neighbor is alive for: 135642 sec 501 ms
Last keepalive packet sending status: Successful
Last keepalive packet sending time: 2013.03.18 18:23:53 986 ms
Last keepalive packet receiving status: Successful
Last keepalive packet receiving time: 2013.03.18 18:23:54 99 ms

Distributed relay keepalive parameters:
Destination IP address: 10.0.0.2
Source IP address: 10.0.0.1
Keepalive UDP port : 6400
Keepalive vpn-instance : vpn1
Keepalive interval : 1000 ms
Keepalive timeout  : 5 sec
Keepalive hold time: 3 sec
```

Table 3 Command output

Field	Description
Neighbor keepalive link status	State of the DR peer: • **Unknown**—No DR peer is detected because the destination IP address of keepalive packets is not specified. • **Up**—The DR peer is up. • **Down**—The DR peer is down.
Neighbor is alive for	Time period for which the DR peer has been up.
Last keepalive packet sending status	Result of the most recent keepalive packet transmission: • **Successful**. • **Failed**.
Last keepalive packet sending time	Most recent time when a keepalive packet was sent. If the device has not sent any keepalive packets, this field displays **N/A**.
Last keepalive packet receiving status	Result of the most recent keepalive packet receiving attempt: • **Successful**. • **Failed**.
Last keepalive packet receiving time	Most recent time when a keepalive packet was received. If the device has not received any keepalive packets, this field displays **N/A**.
Destination IP address	Destination IP address of keepalive packets sent by the device.
Source IP address	Source IP address of keepalive packets sent by the device.
Keepalive UDP port	Destination UDP port of keepalive packets.
Keepalive vpn-instance	VPN instance for keepalive packets.
Keepalive interval	Interval at which the device sends keepalive packets.
Keepalive timeout	Keepalive timeout timer.
Keepalive hold time	Keepalive hold timer setting. The keepalive hold timer specifies the amount of time that the device uses to identify the cause of an IPL down event.

Related commands

drni keepalive destination

drni keepalive hold-time

drni keepalive interval

display drni mad verbose

Use **display drni mad verbose** to display detailed DRNI MAD information.

Syntax

display drni mad verbose

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display detailed DRNI MAD information.

```
<Sysname> display drni mad verbose
DRNI MAD DOWN state    : No
Restore delay          : 30 s
Keepalive status       : Faulty
System number  Keepalive Destination IP                   UDP port
1              1.1.1.1                                    1000
Excluded ports(user-configured):
  Ten-GigabitEthernet1/0/5
Excluded ports(system-configured):
  Management interfaces:
    M-GigabitEthernet0/0/0
  DR interfaces:
    Bridge-Aggregation4
  IPP:
    Bridge-Aggregation3
  Member interfaces of IPP Bridge-Aggregation3:
    Ten-GigabitEthernet1/0/1
    Ten-GigabitEthernet1/0/2
```

Table 4 Command output

Field	Description
DRNI MAD DOWN state	Whether the network interfaces on the device are in MAD DOWN state: • **Yes**—All network interfaces are in MAD DOWN state, except for the interfaces excluded manually or automatically from the shutdown action by DRNI. • **No**—No network interfaces are in DRNI MAD DOWN state. If this field displays **Yes**, check the IPL for the link down issue to remove multi-active collision.
Restore delay	Data restoration interval, in seconds.

Field	Description
Keepalive status	Keepalive link status: • **Normal**—The keepalive link is operating correctly. The device can receive keepalive packets from the peer. **Faulty**—The keepalive link is not operating correctly. The device cannot receive keepalive packets from the peer.
System number	DR system number.
Keepalive Destination IP	Destination IP address of keepalive packets.
UDP port	Destination UDP port of keepalive packets.
Excluded ports(user-configured)	Network interfaces manually configured to not shut down by DRNI MAD.
Excluded ports(system-configured)	Network interfaces set by the system to not shut down by DRNI MAD, including: • Management interfaces. • DR interfaces. • IPP. • Aggregation member interfaces of the IPP if the IPP is a Layer 2 aggregate interface.

display drni role

Use **display drni role** to display DR role information.

Syntax

display drni role

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display DR role information.

```
<Sysname> display drni role
DR      Role priority    Bridge MAC          Configured role    Effective role
Local   32667            0000-0001-002e      Primary            Primary
Peer    32667            00e0-fc00-512d      Secondary          Secondary
```

Table 5 Command output

Field	Description
DR	Device location: • **Local**—The local device. • **Peer**—The DR peer.
Configured role	The DR role you have configured for the device: • **Primary**. • **Secondary**. If the device role is unknown, this field displays **None**.

Field	Description
Effective role	Current role of the device: • **Primary**. • **Secondary**. If the device role is unknown, this field displays **None**.

Related commands

drni role priority

display drni summary

Use **display drni summary** to display summary information about the IPP and DR interfaces.

Syntax

display drni summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display summary information about the IPP and DR interfaces. In this example, global configuration consistency check was successful.

```
<Sysname> display drni summary
Global consistency check           : SUCCESS
Inconsistent type 1 global settings: -

IPP             IPP ID        State
BAGG2           1             UP

DR interface    DR group ID   State   Check result   Type 1 inconsistency
BAGG1           1             UP      SUCCESS        -
BAGG11          2             DOWN    FAILURE        STP/VLAN/LAGG
BAGG15          5             UP      SUCCESS        -
```

Display summary information about the IPP and DR interfaces. In this example, global configuration consistency check failed.

```
<Sysname> display drni summary
Global consistency check           : FAILURE
Inconsistent type 1 global settings: STP

IPP             IPP ID        State
BAGG2           1             UP

DR interface    DR group ID   State   Check result   Type 1 inconsistency
BAGG1           1             UP      SUCCESS        -
BAGG11          2             DOWN    FAILURE        STP/VLAN/LAGG
```

```
BAGG15              5                   UP        SUCCESS          -
```

Table 6 Command output

Field	Description
Global consistency check	Result of global configuration consistency check: • **SUCCESS**. • **FAILURE**.
IPP	Abbreviated name of the IPP.
DR interface	Abbreviated name of the DR interface.
State	State of the interface: • **UP**. • **DOWN**.
Check result	Result of interface-specific configuration consistency check: • **SUCCESS**. • **FAILURE**.

Related commands

port drni group

display drni system

Use **display drni system** to display the DR system settings.

Syntax

display drni system

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the DR system settings.

```
<Sysname> display drni system
IPP: Bridge-Aggregation10
State: UP

DR          System number System MAC         System priority
Local       1             0000-fc00-6504     32768
Peer        2             0000-fc00-6504     32768
```

Table 7 Command output

Field	Description
IPP	Full name of the IPP.
State	State of the IPP: • **UP**.

Field	Description
	• **DOWN**.
Local	Information about the local device: • **System number**—This field displays **N/A** if the system number is not configured. • **System MAC**—This field displays **N/A** if the system MAC address is not configured. • **System priority**—The DR system priority, which is used as the system LACP priority.
Peer	Information about the DR peer: • **System number**—This field displays **N/A** if the system number is not configured or no DR peer exists. • **System MAC**—This field displays **N/A** if the system MAC address is not configured or no DR peer exists. • **System priority**—This field displays **N/A** if no DR peer exists.

Related commands

drni system-mac

drni system-number

drni system-priority

port drni intra-portal port

display drni verbose

Use **display drni verbose** to display detailed information about the IPP and DR interfaces.

Syntax

display drni verbose [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a DR interface or the IPP by its number. The interface number must already exist. If you do not specify an interface, the command displays detailed information about the IPP and all DR interfaces.

Usage guidelines

If the specified interface is not the IPP or a DR interface, no information is displayed.

Examples

Display detailed information about DR interface Bridge-Aggregation 1.

```
<Sysname> display drni verbose bridge-aggregation 1
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired
```

```
DR interface/DR group ID: BAGG1/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports Index: 16385, 16386
Peer Selected ports Index: 32769, 32770
```

Display detailed information about IPP Bridge-Aggregation 2.

```
<Sysname> display drni verbose bridge-aggregation 2
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: BAGG2/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports Index: 16385, 16386
Peer Selected ports Index: 32769, 32770
```

Table 8 Command output

Field	Description
Flags	DRCP state flags. The flag field is one byte long, represented by ABCDEFGH from the lowest bit to the highest bit. A letter is displayed when its bit is 1 and is not displayed when its bit is 0. • **A**—Indicates whether DRCP is enabled on the local device. 1 indicates enabled. 0 indicates disabled. • **B**—Indicates whether DRCP is enabled on the DR peer. 1 indicates enabled. 0 indicates disabled. • **C**—Indicates whether DRCP is enabled on a third DR member device. 1 indicates enabled. 0 indicates disabled. • **D**—Indicates whether the local IPP has determined that DRCP is enabled on the DR peer. 1 indicates yes. 0 indicates no. • **E**—Indicates the DRCP timeout timer. 1 indicates the short timeout timer. 0 indicates the long timeout timer. • **F**—Indicates whether the local IPP permits the packets that contain the negotiated gateway conversation IDs. 1 indicates yes. 0 indicates no. • **G**—Indicates whether the local IPP permits the packets that contain the negotiated port conversation IDs. 1 indicates yes. 0 indicates no. • **H**—Indicates whether the local DRCPDU receive machine is in default or expired state. 1 indicates yes. 0 indicates no.
IPP	Abbreviated name of the IPP.
DR interface	Abbreviated name of the DR interface.
State	State of the interface: • **UP**. • **DOWN**.
Local state	Local DRCP state flags. If all bits are set to 0, this field displays **Unknown**.
Peer state	Peer DRCP state flags. If all bits are set to 0 or no peer exists, this field displays **Unknown**.

Related commands

port drni group

drni auto-recovery reload-delay

Use **drni auto-recovery reload-delay** to enable DR system auto-recovery and set the reload delay timer.

Use **undo drni auto-recovery reload-delay** to restore the default.

Syntax

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

undo drni auto-recovery reload-delay

Default

DR system auto-recovery is disabled and the reload delay timer is not set.

Views

System view

Predefined user roles

network-admin

Parameters

delay-value: Specifies a reload delay in the range of 240 to 3600 seconds.

Usage guidelines

If only one DR member device recovers after the entire DR system reboots, auto-recovery enables that member device to take over the primary role when the reload delay timer expires. Then, the member device can forward traffic through its DR interfaces.

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

If both DR member devices recover 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.

Examples

Enable DR system auto-recovery and set the reload delay timer to 245 seconds.

```
<Sysname> system-view
[Sysname] drni auto-recovery reload-delay 245
```

Related commands

display drni role

drni consistency-check disable

Use **drni consistency-check disable** to disable DRNI from performing configuration consistency check.

Use **undo drni consistency-check disable** to enable DRNI to perform configuration consistency check.

Syntax

drni consistency-check disable

undo drni consistency-check disable

Default

DRNI performs configuration consistency check.

Views

System view

Predefined user roles

network-admin

Usage guidelines

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.

You must make sure the DR member devices use the same setting for configuration consistency check.

Examples

Disable DRNI from performing configuration consistency check.

```
<Sysname> system-view
[Sysname] drni consistency-check disable
```

drni drcp period short

Use **drni drcp period short** to enable the short DRCP timeout timer (3 seconds) on the IPP or a DR interface.

Use **undo drni drcp period** to restore the default.

Syntax

drni drcp period short

undo drni drcp period

Default

An aggregate interface uses the long DRCP timeout timer (90 seconds).

Views

Layer 2 aggregate interface view

VXLAN tunnel interface view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on the IPP or a DR interface.

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.

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*.

Examples

Enable the short DRCP timeout timer on Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] drni drcp period short
```

drni keepalive { ip | ipv6 }

Use **drni keepalive** { **ip** | **ipv6** } to configure DR keepalive packet parameters.

Use **undo drni keepalive** { **ip** | **ipv6** } to restore the default.

Syntax

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

undo drni keepalive { **ip** | **ipv6** }

Default

The destination and source IP addresses and VPN instance are not specified for DR keepalive packets, and the keepalive destination UDP port is 6400.

Views

System view

Predefined user roles

network-admin

Parameters

ip: Specifies IPv4 addresses.

ipv6: Specifies IPv6 addresses.

destination: Specifies an IP address of the DR peer as the destination IP address of keepalive packets.

source: Specifies a local IP address as the source IP address of keepalive packets. If you do not specify a source IP address, the IP address of the outgoing interface is used.

ipv4-address: Specifies an IPv4 address.

ipv6-address: Specifies an IPv6 address.

udp-port *udp-number*: Specifies the destination UDP port of keepalive packets. The value range for the *udp-number* argument is 1 to 65535, and the default value is 6400.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the addresses of keepalive packets belong to the public network, do not specify a VPN instance.

Usage guidelines

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 addresses.

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

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the destination and source IP addresses of keepalive packets as 192.168.68.125 and 192.168.68.100, respectively.

```
<Sysname> system-view
[Sysname] drni keepalive ip destination 192.168.68.125 source 192.168.68.100
```

Related commands

display drni keepalive

drni keepalive hold-time

Use **drni keepalive hold-time** to set the keepalive hold timer.

Use **undo drni keepalive hold-time** to restore the default.

Syntax

drni keepalive hold-time *value*

undo drni keepalive hold-time

Default

The keepalive hold timer is 3 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies a timer value in the range of 3 to 10 seconds.

Usage guidelines

IMPORTANT:

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.

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.

Examples

Set the keepalive hold timer to 5 seconds.

```
<Sysname> system-view
[Sysname] drni keepalive hold-time 5
```

Related commands

display drni keepalive

drni keepalive interval

Use **drni keepalive interval** to set the DR keepalive interval and timeout timer.

Use **undo drni keepalive interval** to restore the default.

Syntax

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

undo drni keepalive interval

Default

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

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the keepalive interval, in the range of 100 to 10000 milliseconds.

timeout *timeout*: Specifies the keepalive timeout timer, in the range of 3 to 20 seconds. The local keepalive timeout timer must be two times the keepalive interval of the peer at minimum.

Usage guidelines

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.

You must configure the same DR keepalive interval on the DR member devices in a DR system.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the DR keepalive interval and timeout timer to 2000 milliseconds and 6 seconds, respectively.

```
<Sysname> system-view
[Sysname] drni keepalive interval 2000 timeout 6
Changing the keepalive interval might cause system setup failure. Continue? [Y/N]:y
```

Related commands

display drni keepalive

drni restore-delay

Use **drni restore-delay** to set the data restoration interval.

Use **undo drni restore-delay** to restore the default.

Syntax

drni restore-delay *value*

undo drni restore-delay

Default

The data restoration interval is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the data restoration interval, in the range of 1 to 3600 seconds.

Usage guidelines

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 MAD DOWN state, except for the following interfaces:

- IPP.
- Management Ethernet interface.
- Interfaces excluded from the MAD shutdown action.

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

To avoid packet loss and forwarding failure, increase the data restoration interval if the amount of data is large or if an ISSU is to be performed between the DR member devices.

Examples

Set the data restoration interval to 50 seconds.

```
<Sysname> system-view
[Sysname] drni restore-delay 50
```

drni role priority

Use **drni role priority** to set the DR role priority of the device.

Use **undo drni role priority** to restore the default.

Syntax

drni role priority *priority-value*

undo drni role priority

Default

The DR role priority of the device is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority-value: Specifies the DR role priority, in the range of 0 to 65535. The lower the value, the higher the priority.

Usage guidelines

IMPORTANT:

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

For features that require centralized traffic processing, a DR member device is assigned the primary or secondary role based on its DR role priority. The secondary DR device forwards the traffic of those features to the primary DR device for processing. If the DR member devices use the same DR role priority, the member device with a lower bridge MAC address is assigned the primary role.

Examples

Set the DR role priority of the device to 66.

```
<Sysname> system-view
[Sysname] drni role priority 66
```

Related commands

display drni role

drni system-mac

Use **drni system-mac** to configure the DR system MAC address.

Use **undo drni system-mac** to restore the default.

Syntax

drni system-mac *mac-address*

undo drni system-mac

Default

The DR system MAC address is not configured.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the H-H-H format. The MAC address cannot be a multicast MAC address, all-zero MAC address, or all-F MAC address.

Usage guidelines

CAUTION:

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.

Examples

Configure the DR system MAC address as 0001-0001-0001.

```
<Sysname> system-view
[Sysname] drni system-mac 1-1-1
Changing the system MAC address might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
[Sysname]
```

drni system-number

Use **drni system-number** to set the DR system number.

Use **undo drni system-number** to restore the default.

Syntax

drni system-number *system-number*

undo drni system-number

Default

The DR system number is not set.

Views

System view

Predefined user roles

network-admin

Parameters

system-number: Specifies the DR system number. Available values are 1 and 2.

Usage guidelines

CAUTION:

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.

Examples

Set the DR system number to 1.

```
<Sysname> system-view
[Sysname] drni system-number 1
Changing the system number might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
[Sysname]
```

Related commands

display drni system

drni system-priority

Use **drni system-priority** to set the DR system priority.

Use **undo drni system-priority** to restore the default.

Syntax

drni system-priority *priority*

undo drni system-priority

Default

The DR system priority is 32768.

Views

System view

Predefined user roles

network-admin

Parameters

priority: Specifies a priority value in the range of 0 to 65535. The lower the value, the higher the priority.

Usage guidelines

CAUTION:

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.

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

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

Examples

Set the DR system priority to 64.

```
<Sysname> system-view
[Sysname] drni system-priority 64
Changing the system priority might flap the intra-portal link and cause DR system setup failure. Continue? [Y/N]:y
[Sysname]
```

Related commands

display drni system

drni mad exclude interface

Use **drni mad exclude interface** to exclude an interface from the shutdown action by DRNI MAD.

Use **undo drni mad exclude interface** to enable DRNI MAD to shut down an interface when a multi-active collision is detected.

Syntax

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

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

Default

No interfaces are manually excluded from the DRNI shutdown action.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

When DRNI MAD detects a multi-active collision, DRNI shuts down all network interfaces on the secondary DR device except for the interfaces excluded from the MAD shutdown action by DRNI.

The interfaces excluded from the MAD shutdown action include:

- Interfaces excluded automatically by the system. For example, management interfaces.
- Interfaces excluded manually.

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.

If an interface has been placed in DRNI MAD DOWN state, executing the **drni mad exclude interface** command cannot bring it up.

NOTE:

To identify the outgoing interface of a tunnel, use the **display fib ip-address** command or the **display ip routing-table** *ip-address* command. The *ip-address* argument represents the destination IP address of the tunnel, which you can identify by using the **display interface tunnel** command.

Examples

Exclude Ten-GigabitEthernet 1/0/1 from the shutdown action by DRNI MAD.

```
<Sysname> system-view
[Sysname] drni mad exclude interface ten-gigabitethernet 1/0/1
```

Related commands

display drni mad verbose

display fib (*Layer 3—IP Services Command Reference*)

display interface tunnel (*Layer 3—IP Services Command Reference*)

display ip routing-table (*Layer 3—IP Routing Command Reference*)

port drni group

Use **port drni group** to assign an aggregate interface to a DR group.

Use **undo port drni group** to restore the default.

Syntax

port drni group *group-id*

undo port drni

Default

An aggregate interface does not belong to a DR group.

Views

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a DR group number. The value range is 1 to 1024.

Usage guidelines

To use a Layer 2 aggregate interface as a DR interface, you must assign it to a DR group.

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.

Examples

Assign Bridge-Aggregation 1 to DR group 100.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port drni group 100
```

Related commands

display drni summary

display drni verbose

port drni intra-portal-port

Use **port drni intra-portal-port** to specify a Layer 2 aggregate interface or VXLAN tunnel interface as the IPP.

Use **undo drni intra-portal-port** to restore the default.

Syntax

port drni intra-portal-port *port-id*

undo port drni intra-portal-port

Default

A Layer 2 aggregate interface or VXLAN tunnel interface is not the IPP.

Views

Layer 2 aggregate interface view

VXLAN tunnel interface view

Predefined user roles

network-admin

Parameters

port-id: Specifies the IPP ID, which is fixed at 1.

Usage 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*.

Examples

Specify Bridge-Aggregation 2 as the IPP.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 2
```

```
[Sysname-Bridge-Aggregation2] port drni intra-portal-port 1
```

reset drni drcp statistics

Use **reset drni drcp statistics** to clear DRCPDU statistics.

Syntax

reset drni drcp statistics [**interface** *interface-list*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-list*: Specifies a space-separated list of interface items. Each item specifies an aggregate interface or a range of aggregate interfaces in the form of *interface-type interface-number1* [**to** *interface-type interface-number2*]. The value for *interface-number2* must be greater than or equal to the value for *interface-number1*. The aggregate interfaces must be DR interfaces or the IPP. If you do not specify this option, the command clears the DRCPDU statistics about all DR interfaces and the IPP.

Examples

Clear DRCPDU statistics.

```
<Sysname> reset drni drcp statistics
```

Related commands

display drni drcp statistics