VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

In Cisco IOS XE Release 3.14S, Network Address Translation (NAT) supports the VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy feature. VRF-Aware NAT for WAN-to-LAN topology is already supported in NAT.

This module describes this feature.

- Finding Feature Information, on page 1
- Restrictions for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy, on page 2
- Information About VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy, on page 2
- How to Configure VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy, on page 4
- Configuration Examples for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy, on page 5
- Additional References for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy, on page 7
- Feature Information for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy, on page 8

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Restrictions for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

The following features are not supported:

- Asymmetric routing
- Cisco TrustSec
- Edge switching services
- Header Compression
- IPsec
- Lawful intercept (Intercept twice, once at active and once at standby)
- Layer 2 Tunneling Protocol (L2TP)
- Locator-ID Separation Protocol (LISP) inner packet inspection
- Port Bundle
- Stile and Cesar
- Secure Sockets Layer (SSL) VPN
- Session Border Controller (SBC)

If you enable NAT on the primary and backup WAN link, switchover between the primary and backup interface is not supported. NAT backup interface overlord is not supported on the following platforms:

- ASR1000 Series Aggregation Services Routers
- ISR4000 Series Integrated Services Routers
- ISR1000 Series Integrated Services Routers
- CSR1000 Series Cloud Services Routers

Information About VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

VRF-Aware Box-to-Box High Availability Support

In Cisco IOS XE Release 3.14S, Network Address Translation (NAT) supports VRF-aware box-to-box high availability in a WAN-to-WAN topology.

To support VRF-aware box-to-box high availability, NAT ties the NAT mapping with a mandatorily configured mapping ID when a redundancy group (RG) is configured. The standby device retrieves the correct locally significant VRF ID from the mapping ID after synchronization. The VRF ID is set before NAT processes or translates a packet on the active device.

The VRF-aware box-to-box high availability configuration must be the same on both active and standby devices. The VRF configuration must use the same VRF name at active and standby devices. NAT provides a hashed VRF name value in the high availability message, and sends it to active and standby devices, so that...
the corresponding local VRF ID is converted at the peer device by using the VRF name hash value-to-VRF ID mapping.

**Note**

In some cases you might experience FTP disconnection after failover in a NAT B2B scenario. To resolve this issue, quit the existing FTP connection and start a new FTP connection.

**Stateful Interchassis Redundancy Overview**

You can configure the Stateful Interchassis Redundancy feature to determine the active device from a group of devices, based on a number of failover conditions. When a failover occurs, the standby device seamlessly takes over, starts performing traffic forwarding services, and maintains a dynamic routing table.

**Stateful Interchassis Redundancy Operation in NAT**

You can configure pairs of devices to act as hot standbys for each other. Redundancy is configured on an interface basis. Pairs of redundant interfaces are known as redundancy groups (RGs). Redundancy occurs at an application level and does not require a complete physical failure of the interface or device for a switchover of the application to occur. When a switchover occurs, the application activity continues to run seamlessly on the redundant interface.

The figure below depicts an active/standby load-sharing scenario. The figure shows how an RG is configured for a pair of devices that has one outgoing interface. Group A on Router 1 is the active RG and Group A on Router 2 is the standby RG.

**Figure 1: Stateful Interchassis Redundancy Operation in a WAN-WAN Topology**

Redundant devices are joined by a configurable control link and a data synchronization link. The control link is used to communicate the status of devices. The data synchronization link is used to transfer stateful information from Network Address Translation (NAT) and the firewall and synchronize the stateful database. The pairs of redundant interfaces are configured with the same unique ID number known as the redundant interface identifier (RII).
The status of redundancy group members is determined through the use of hello messages sent over the control link. The software considers either device not responding to a hello message within a configurable amount of time to be a failure and initiates a switchover. For the software to detect a failure in milliseconds, control links run the failover protocol that is integrated with the Bidirectional Forwarding Detection (BFD) protocol. You can configure the following parameters for hello messages:

- **Hello time**—Interval at which hello messages are sent.
- **Hold time**—Amount of time before which the active or standby device is declared to be down.

The hello time defaults to 3 seconds to align with the Hot Standby Router Protocol (HSRP), and the hold time defaults to 10 seconds. You can also configure these timers in milliseconds by using the `timers hellotime msec` command.

To determine the pairs of interfaces that are affected by the switchover, you must configure a unique ID for each pair of redundant interfaces. This ID is known as the RII that is associated with the interface.

A switchover to the standby device can occur when the priority setting that is configured on each device changes. The device with the highest priority value acts as the active device. If a fault occurs on either the active or standby device, the priority of the device is decremented by a configurable amount known as the weight. If the priority of the active device falls below the priority of the standby device, a switchover occurs and the standby device becomes the active device. This default behavior can be overridden by disabling the preemption attribute for the RG. You can also configure each interface to decrease the priority when the Layer 1 state of the interface goes down. The priority that is configured overrides the default priority of an RG.

Each failure event that causes a modification of an RG priority generates a syslog entry that contains a timestamp, the RG that was affected, the previous priority, the new priority, and a description of the failure event cause.

A switchover also can occur when the priority of a device or interface falls below a configurable threshold level.

A switchover to the standby device occurs under the following circumstances:

- Power loss or a reload occurs on the active device (including reloads).
- The run-time priority of the active device goes below that of the standby device (with preempt configured).
- The run-time priority of the active device goes below that of the configured threshold.
- The redundancy group on the active device is reloaded manually. Use the `redundancy application reload group rg-number` command for a manual reload.

How to Configure VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

The configuration for VRF-aware box-to-box redundancy is same as the configuration for stateful interchassis redundancy. For more information, see the "Configuring Stateful Interchassis Redundancy" module in the IP Addressing: NAT Configuration Guide.
Configuration Examples for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

Example: Configuring VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

The following is a sample WAN-to-WAN symmetric routing configuration:

```conf
vrf definition Mgmt-intf
  address-family ipv4
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
!
vrf definition VRFA
  rd 100:1
  route-target export 100:1
  route-target import 100:1
    address-family ipv4
      exit-address-family
    !
  !
  no logging console
  no aaa new-model
  !
  multilink bundle-name authenticated
  !
  redundancy
  mode sso
  application redundancy
    group 1
      preempt
      priority 120
      control GigabitEthernet 0/0/1 protocol 1
      data GigabitEthernet 0/0/2
    !
    !
    !
    !
    !
    !
    !
  ip tftp source-interface GigabitEthernet0
  ip tftp blocksize 8192
  !
  track 1 interface GigabitEthernet 0/0/4 line-protocol
  !
  interface Loopback 0
  ip address 209.165.201.1 255.255.255.224
  !
  interface GigabitEthernet 0/0/0
  vrf forwarding VRFA
  ip address 192.168.0.1 255.255.255.248
  ip nat inside
  negotiation auto
```
bfd interval 50 min_rx 50 multiplier 3
redundancy ril 2
!
interface GigabitEthernet 0/0/1
  ip address 209.165.202.129 255.255.255.224
  negotiation auto
!
interface GigabitEthernet 0/0/2
  ip address 192.0.2.1 255.255.255.224
  negotiation auto
!
interface GigabitEthernet 0/0/3
  ip address 198.51.100.1 255.255.255.240
  negotiation auto
!
interface GigabitEthernet 0/0/4
  ip address 203.0.113.1 255.255.255.240
  negotiated auto
!
interface GigabitEthernet 0
  vrf forwarding Mgmt-intf
  ip address 172.16.0.1 255.255.0.0
  negotiation auto
!
interface vasileft 1
  vrf forwarding VRFA
  ip address 10.4.4.1 255.255.0.0
  ip nat outside
  no keepalive
!
interface vassiright 1
  ip address 10.4.4.2 255.255.0.0
  no keepalive
!
router mobile
!
router bgp 577
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 203.0.113.1 remote-as 223
  neighbor 203.0.113.1 description PEERING to PTNR neighbor 10.4.4.1 remote-as 577 neighbor 10.4.4.1 description PEERING to VASI interface
!
address-family ipv4
  network 203.0.113.1 mask 255.255.255.240
  network 10.4.0.0 mask 255.255.0.0
  network 209.165.200.224 mask 255.255.255.224
  neighbor 203.0.113.1 activate
  neighbor 10.4.4.1 activate
  neighbor 10.4.4.1 next-hop-self
  exit-address-family
!
address-family ipv4 vrf VRFA
  bgp router-id 4.4.4.4
  network 192.168.0.0 mask 255.255.255.248
  network 10.4.0.0 mask 255.255.0.0
  redistribute connected
  redistribute static
  neighbor 192.168.0.2 remote-as 65004
  neighbor 192.168.0.2 fall-over bfd
  neighbor 192.168.0.2 activate
  neighbor 10.4.4.2 remote-as 577
  neighbor 10.4.4.2 description PEERING to VASI Global intf
  neighbor 10.4.4.2 activate
exit-address-family
!
ip nat switchover replication http
ip nat pool att_pool 209.165.200.225 209.165.200.225 prefix-length 16
ip nat inside source list 4 pool att_pool redundancy 1 mapping-id 100 vrf VRFA overload
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 203.0.113.1 255.255.255.224 10.4.4.1
ip route 192.168.0.0 255.255.0.0 10.4.4.1
ip route 209.165.200.224 255.255.255.224 10.4.4.1
ip route vrf Mgmt-intf 209.165.200.1 255.255.255.224 172.16.0.0
!
ip prefix-list VRF_Pool seq 5 permit 209.165.200.0/27
ip prefix-list p1-adv-1 seq 5 permit 209.165.200.0/27
ip prefix-list p1-exist-1 seq 5 permit 203.0.113.193/27
logging esm config
access-list 4 permit 203.0.113.193 255.255.255.224
!
control-plane
line console 0
  stopbits 1
!
line vty 0 3
  login
!
line vty 4
  password lab
  login
!
end

Additional References for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>NAT commands</td>
<td>Cisco IOS IP Addressing Services Command Reference</td>
</tr>
<tr>
<td>NAT stateful interchassis redundancy</td>
<td>Configuring Stateful Interchassis Redundancy</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy</td>
<td>Cisco IOS XE Release 3.14S</td>
<td>In Cisco IOS XE Release 3.14S, Network Address Translation (NAT) supports the VRF-Aware NAT for WAN-WAN Topology with Symmetric Routing Box-to-Box Redundancy feature. This feature contains the following two features: VRF-aware stateful interchassis redundancy and VRF-aware interchassis symmetric routing. No commands were introduced or modified by this feature.</td>
</tr>
</tbody>
</table>