VRF-Aware Dynamic NAT Mapping with HSRP

The VRF-Aware Dynamic NAT Mapping with HSRP feature supports stateless redundancy using HSRP with dynamic Network Address Translation (NAT), Port Address Translation (PAT), and interface overload configuration. Dynamic NAT, PAT and interface overload support HSRP with and without virtual routing and forwarding (VRF) instances. All these configurations are supported in the Carrier Grade NAT (CGN) mode.

This module describes the feature and explains how to configure it.

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.

Prerequisites for VRF-Aware Dynamic NAT Mapping with HSRP

- Both the active and standby devices must be configured with the same Network Address Translation (NAT) rules.
- Hot Standby Router Protocol (HSRP) must be configured between the active and standby devices.

Restrictions for VRF-Aware Dynamic NAT Mapping with HSRP

- During failovers, NAT translated IP addresses on devices may be different from the IP address before the failover, because no state information is exchanged between active and standby devices.
- During a failover, all existing NAT sessions are destroyed and new sessions are established in the active device.
- HSRP Virtual IP Address (VIP) cannot be used by NAT pools.
- Active/active configuration is not supported; only active/standby configuration is supported.
- IPv6 is not supported; only IPv4 is supported.

Information About VRF-Aware Dynamic NAT Mapping with HSRP

VRF-Aware Dynamic NAT Mapping with HSRP Overview

The VRF-Aware Dynamic NAT Mapping with HSRP feature supports stateless redundancy using HSRP with dynamic Network Address Translation (NAT), Port Address Translation (PAT), and interface overload configuration. Dynamic NAT, PAT and interface overload support HSRP with and without virtual routing and forwarding (VRF) instances. All these configurations are supported in the Carrier Grade NAT (CGN) mode.

Hot Standby Router Protocol (HSRP) provides high network availability by providing first-hop routing redundancy for IP hosts on networks configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active device and a standby device. HSRP provides redundancy for routing IP traffic without being dependent on the availability of a single router. In a group of device interfaces, the active device is the device of choice for routing packets; the standby device is the device that takes over when the active device fails or when preset conditions are met.

Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby devices. Selection of active and standby devices is based on the assigned priority. The device with the highest priority is selected as the active device. After failover, a new active device sends a gratuitous Address Resolution Protocol (ARP) request to LAN users to notify about the change in MAC address for the virtual IP address (VIP).

To enable this feature, both the active and standby devices must be configured with the same NAT rules and HSRP must be configured on both the devices. Based on the configured priority one of the devices will be active and the other standby. This feature supports VRF-aware NAT translation and Carrier Grade NAT (CGN) mode.

This feature supports the LAN-LAN topology as well as the LAN-WAN topology. In the LAN-WAN topology, only symmetric routing is supported.

When an Address Resolution Protocol (ARP) query is triggered for an address that is configured with dynamic NAT mapping and owned by the device, NAT responds with the burned-in MAC (BIA MAC) address on the interface to which the ARP is pointing. You must enable and configure the NAT inside interfaces of the active and standby devices to belong to a group.

In Cisco IOS XE Denali 16.3 release, the Allow same ACL/router-map on multiple NAT statements feature was introduced to support usage of same ACL for configuring both dynamic mapping and static mapping in NAT. Dynamic mapping is given the precedence over static mapping regardless of the configuration order. The precedence of dynamic mapping over static mapping using the sequence number of the class ensures class order consistency in NAT.

Address Resolution with ARP

A device in IP can have both a local address (which uniquely identifies the device on its local segment or LAN) and a network address (which identifies the network to which the device belongs). The local address is known as a data link address because it is contained in the data link layer (Layer 2 of the OSI model) part of the packet header and is read by data-link devices such as bridges, all device interfaces and so on. The local address is referred to as the MAC address, because the MAC sublayer within the data-link layer processes addresses for the layer.

To communicate with a device on Ethernet, for example, the Cisco IOS software must first determine the 48-bit MAC or local data-link address of that device. The process of determining the local data-link address from an IP address is called address resolution. The process of determining the IP address from a local data-link address is called reverse address resolution.

The software uses three forms of address resolution: Address Resolution Protocol (ARP), proxy ARP, and Probe (similar to ARP). The software also uses the Reverse Address Resolution Protocol (RARP). ARP, proxy ARP, and RARP are defined in RFCs 826, 1027, and 903, respectively. Probe is a protocol developed by the Hewlett-Packard Company (HP) for use on IEEE-802.3 networks.

ARP is used to associate IP addresses with media or MAC addresses. Taking an IP address as input, ARP determines the associated media address. Once a media or MAC address is determined, the IP address or media address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP).

Gratuitous ARP

When a host sends an ARP request to resolve its own IP address, it is called gratuitous ARP. In the ARP request packet, the source and destination IP addresses are filled with the same source IP address itself. The destination MAC address is the Ethernet broadcast address.

When a router becomes active, it broadcasts a gratuitous ARP packet with the Hot Standby Router Protocol (HSRP) virtual MAC address to the affected LAN segment. If the segment uses an Ethernet switch, this allows the switch to change the location of the virtual MAC address so that packets flow to the new router instead of the one that is no longer active. End devices do not actually need gratuitous ARP if routers use the default HSRP MAC address.

How to Configure VRF-Aware Dynamic NAT Mapping with HSRP

Enabling HSRP for VRF-Aware Dynamic NAT

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**ip** | **ipv6** | **line-protocol**}
4. **exit**
5. **interface** *type number*
6. **ip nat inside**
7. **ip address** *ip-address mask*
8. **standby** *group-number* **ip** [*ip-address*]
9. **standby use-bia**
10. **standby** *group-number* **priority** *priority*
11. **standby** *group-number* **preempt** [*delay*]
12. **standby** *group-number* **track** *object-number* [**decrement** *priority-decrement*]
13. **exit**
14. **ip nat pool** *pool-name start-ip* **end-ip** **netmask** *netmask*
15. **access-list** *standard-access-list* **permit** *ip-address mask*
16. **ip nat inside source list** *list-name* **pool** *pool-name* [**overload**]
17. **end**

DETAILED STEPS

|	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**track** *object-number* **interface** *type number* {**ip**	**ipv6**	**line-protocol**} **Example:** `Device(config)# track 10 interface gigabitethernet 0/0/0 line-protocol`	Configures an interface to be tracked where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the state of the interface
Step 4	**exit** **Example:** `Device(config-track)# exit`	Exits tracking configuration mode and returns to global configuration mode.
Step 5	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 1/2/1`	Configures an interface and enters interface configuration mode.
Step 6	**ip nat inside** **Example:** `Device(config-f)# ip nat inside`	Connects the interface to the inside network, which is subject to Network Address Translation (NAT).

	Command or Action	**Purpose**
Step 7	**ip address** *ip-address mask* **Example:** Device(config-if)# ip address 192.0.0.2 255.0.0.0	Sets a primary or secondary IP address for an interface.
Step 8	**standby** *group-number* **ip** [*ip-address*] **Example:** Device(config-if)# standby 1 ip 192.0.0.1	Activates the Hot Standby Router Protocol (HSRP).
Step 9	**standby use-bia** **Example:** Device(config-if)# standby use-bia	Configures HSRP to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address or the functional address.
Step 10	**standby** *group-number* **priority** *priority* **Example:** Device(config-if)# standby 1 priority 120	Configures the HSRP priority. • The priority range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The device in the HSRP group with the highest priority value becomes the active device.
Step 11	**standby** *group-number* **preempt** [*delay*] **Example:** Device(config-if)# standby 1 preempt	Configures HSRP preemption and preemption delay. • If you configure this command, when a local device has an HSRP priority higher than the current active device, the local device assumes control as the active device. If preemption is not configured, the local device assumes control as the active device only if it receives information indicating no device is in the active state (acting as the designated device).
Step 12	**standby** *group-number* **track** *object-number* [**decrement** *priority-decrement*] **Example:** Device(config-if)# standby 1 track 10 decrement 15	Configure HSRP to track an object, and change the HSRP priority on the basis of the state of the object. • When a tracked object goes down, the HSRP priority decreases by 10. If an object is not tracked, state changes do not affect the priority.
Step 13	**exit** **Example:** Device(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 14	**ip nat pool** *pool-name start-ipend-ip* **netmask** *netmask* **Example:** Device(config)# ip nat pool pool1 10.1.1.10 10.1.1.52 netmask 255.255.255.0	Defines a pool of IP addresses for Network Address Translation (NAT) translations.
Step 15	**access-list** *standard-access-list* **permit** *ip-address mask* **Example:**	

	Command or Action	Purpose
	`Device(config)# acces-list 1 permit 190.0.0.0 0.255.255.255`	
Step 16	**ip nat inside source list** *list-name* **pool** *pool-name* [**overload**] **Example:** `Device(config)# ip nat inside source list list1 pool pool1 overload`	Enables NAT of the inside source address. • When overloading is configured, it enables the device to use one global address for many local addresses. The TCP or UDP port number of each inside host distinguishes between the multiple conversations using the same local IP address.
Step 17	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for VRF-Aware Dynamic NAT Mapping with HSRP

Example: Enabling HSRP for VRF-Aware Dynamic NAT

Figure 1: HSRP NAT LAN-WAN Topology
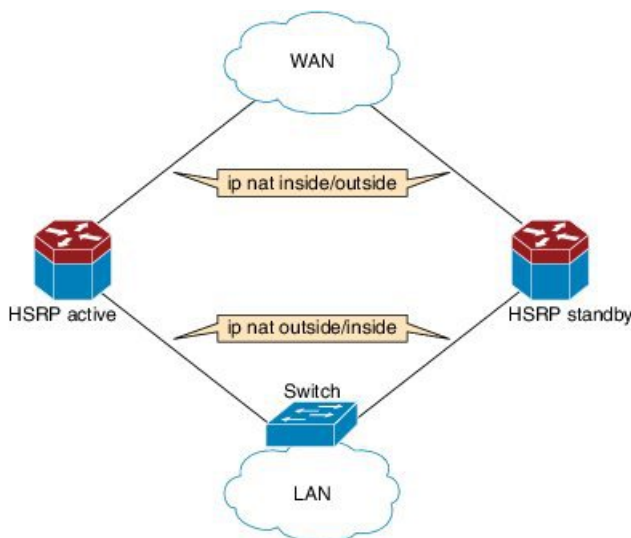
The following example shows a LAN-WAN configuration for dynamic Network Address Translation (NAT) overload mapping with Hot Standby Router Protocol (HSRP). A virtual routing and forwarding (VRF) instance is enabled for this configuration. Devices that are configured with NAT do not have any route configurations related to HSRP Virtual IP Address (VIP). LAN users using static routes have to set the default route or next-hop to the HSRP VIP; for example configure the **ip route 0.0.0.0 0.0.0.0 192.0.2.1** command.

```
! Active device configuration:
Device# configure terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# exit
Device(config)# track 10 interface fastethernet 1/1/1 line-protocol
Device(config-track)# exit
Device(config)# interface fastethernet 1/1/0
Device(config-if)# vrf forwarding vrf1
Device(config-if)# ip nat inside
Device(config-if)# ip address 192.0.2.2 255.255.255.240
Device(config-if)# standby 1 ip 192.0.2.1
Device(config-if)# standby use-bia
Device(config-if)# standby 1 priority 120
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 track 10 decrement 15
Device(config-if)# exit
Device(config)# interface fastethernet 1/1/1
Device(config-if)# ip address 198.51.100.1 255.255.255.240
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# ip nat pool pool1 10.1.1.1 10.1.1.255 netmask 255.255.255.0
Device(config)# access-list 1 permit 203.0.113.0 255.255.255.240
Device(config)# ip nat inside source list1 pool pool1 vrf vrf1 overload
Device(config)# end


! Standby device configuration:
Device# configure terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# exit
Device#(config)# interface fastethernet 1/2/0
Device(config-if)# vrf forwarding vrf1
Device(config-if)# ip nat inside
Device(config-if)# ip address 192.0.2.3 255.255.255.240
Device(config-if)# standby 1 ip 192.0.2.1
Device(config-if)# standby use-bia
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# exit
Device(config)# interface fastethernet 1/2/1
Device(config-if)# ip address 172.16.0.1 255.255.224.0
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# ip nat pool pool1 10.1.1.1 10.1.1.255 netmask 255.255.255.0
Device(config)# access-list 1 permit 2013.0.113.0 255.255.255.240
Device(config)# ip nat inside source list1 pool pool1 vrf vrf1 overload
Device(config)# end
```

Verifying HSRP for VRF-Aware Dynamic NAT

Before you begin

  •

SUMMARY STEPS

1. enable

    2. **show arp**

    3. **show ip alias**

    4. **show ip nat translations**

    5. **show standby brief**

DETAILED STEPS

Step 1   **enable**

Example:

```
Device> enable
```

enables privileged EXEC mode.

- Enter your password if prompted.

Step 2   **show arp**

Displays the entries in the Address Resolution Protocol (ARP) table.

Example:

```
Device# show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.0.0.1               -   0023.eb85.7650  ARPA   GigabitEthernet1/1/0
Internet  192.0.0.2               -   0023.eb85.7650  ARPA   GigabitEthernet1/1/0
```

Step 3   **show ip alias**

Displays the IP addresses that are mapped to TCP ports (aliases) and Serial Line Internet Protocol (SLIP) addresses, which are treated similar to aliases.

Example:

```
Device# show ip alias

Address Type         IP Address      Port
Interface            10.39.21.3
Dynamic              192.0.0.1
Interface            192.0.0.2
```

Step 4   **show ip nat translations**

Displays active Network Address Translation (NAT) translations.

Example:

```
Device# show ip nat translations

Pro  Inside global          Inside local         Outside local        Outside global
udp  10.1.1.4:512           190.0.0.1:435        193.0.0.1:80         193.0.0.1:80
udp  10.1.1.4:515           190.0.0.5:435        193.0.0.1:80         193.0.0.1:80
udp  10.1.1.4:514           190.0.0.4:435        193.0.0.1:80         193.0.0.1:80
udp  10.1.1.4:518           190.0.0.3:435        193.0.0.1:80         193.0.0.1:80
```

Step 5   **show standby brief**

Displays Hot Standby Router Protocol (HSRP) information in a single line of output for each standby group.

Example:

```
Device# show standby brief

                   P indicates configured to preempt.
                   |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Ga1/1/0     1    120 P Active  local           192.0.0.3       192.0.0.1
```

Additional References VRF-Aware Dynamic NAT Mapping with HSRP

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
NAT commands	Cisco IOS IP Addressing Services Command Reference
Static NAT with HSRP	"Static NAT Mapping with HSRP" module of the *IP Addressing: NAT Configuration Guide*

Standards & RFCs

Standard/RFC	Title
RFC 826	*An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses*
RFC 903	*A Reverse Address Resolution Protocol*
RFC 1027	*Using ARP to Implement Transparent Subnet Gateways*

Technical Assistance

Description	Link
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.	http://www.cisco.com/support

Feature Information for VRF-Aware Dynamic NAT Mapping with HSRP

Table 1: Feature Information for VRF-Aware Dynamic NAT Mapping with HSRP

Feature Name	Releases	Feature Information
VRF-Aware Dynamic NAT Mapping with HSRP	Cisco IOS XE Release 3.15S	The VRF-Aware Dynamic NAT Mapping with HSRP feature supports stateless redundancy using HSRP with dynamic Network Address Translation (NAT), Port Address Translation (PAT), and interface overload configuration. Dynamic NAT, PAT and interface overload support HSRP with and without virtual routing and forwarding (VRF) instances. All these configurations are supported in the Carrier Grade NAT (CGN) mode. In Cisco IOS XE Release 3.15S, this feature was supported on Cisco ASR 1000 Series Aggregation Services Routers, Cisco Cloud Services Router 1000V Series, and Cisco ISR 4000 Series Integrated Services Routers. The following commands were updated for this release:**show arp**, **show ip alias**, **show ip nat translations**, and **show standby brief**.
Allow same ACL/router-map on multiple NAT statements	Cisco IOS XE Denali 16.3.1	The Allow use of same ACL/router-map on multiple NAT statements feature supports usage of same ACL for configuring both dynamic mapping and static mapping in NAT. Dynamic mapping is given the precedence over static mapping regardless of the configuration order. The precedence of dynamic mapping over static mapping using the sequence number of the class ensures class order consistency in NAT. This feature uses no new or modified commands.