Configuring NAT for High Availability

Last Updated: December 18, 2011

This module contains procedures for configuring Network Address Translation (NAT) to support the increasing need for highly resilient IP networks. This network resiliency is required where application connectivity needs to continue unaffected by failures to links and routers at the NAT border.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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 Configuring NAT for High Availability

- Before performing the tasks in this module, you should be familiar with the concepts described in the “Configuring NAT for IP Address Conservation” module.
- All access lists required for use with the tasks in this module should be configured prior to beginning the configuration tasks. For information about how to configure an access list, see the “IP Access List Sequence Numbering" document.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Note If you specify an access list to use with a NAT command, NAT does not support the commonly used **permit ip any any** command in the access list.

Restrictions for Configuring NAT for High Availability

- Cisco has announced the End-of-Sale and End-of-Life for the Cisco IOS SNAT. For more information, see the End-of-Sale and End-of-Life Announcement for the Cisco IOS Stateful Failover of Network Address Translation (SNAT) document.
- The Address Resolution Protocol (ARP) queries are always replied to by the Hot Standby Routing Protocol (HSRP) active router. If the active HSRP router fails upstream devices will point to the new HSRP active router and will not have an ARP entry pointing to the original active router, which may no longer be available.

Information About Configuring NAT for High Availability

Stateful NAT

Stateful NAT (SNAT) enables continuous service for dynamically mapped NAT sessions. Sessions that are statically defined receive the benefit of redundancy without the need for SNAT. In the absence of SNAT, sessions that use dynamic NAT mappings would be severed in the event of a critical failure and would have to be reestablished.

SNAT can be used with protocols that do not need payload translation.

NAT Stateful Failover for Asymmetric Outside-to-Inside ALG Support

NAT stateful failover for asymmetric outside-to-inside and Application Layer Gateway (ALG) support improves the ability to handle asymmetric paths by allowing multiple routing paths from outside-to-inside, and per-packet load balancing. This feature also provides seamless failover translated IP sessions with traffic that includes embedded IP addressing such as Voice over IP, FTP, and Domain Name System (DNS) applications.

Interaction with HSRP

SNAT can be configured to operate with the Hot Standby Routing Protocol (HSRP) to provide redundancy. Active and Standby state changes are managed by HSRP.

SNAT applies a more global context to the task of forwarding a particular datagram. Consideration is given to understanding the application state along with forwarding. Devices can take action to avoid potential failures that will have less impact on the flow and to the application that is transmitting data. Multiple NAT routers that share stateful context can work cooperatively and thereby increase service availability.

Translation Group

Two or more network address translators function as a translation group. One member of the group handles traffic requiring translation of IP address information. It also informs the backup translator of active flows as they occur. The backup translator can then use information from the active translator to prepare duplicate translation table entries, and in the event that the active translator is hindered by a critical failure, the traffic can rapidly be switched to the backup. The traffic flow continues since the same network address translations are used, and the state of those translations has been previously defined.

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 more properly 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 (bridges and all device interfaces, for example). The local address is referred to as the MAC address, because the MAC sub-layer within the data link layer processes addresses for the layer.

To communicate with a device on Ethernet, for example, the Cisco IOS software first must 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).

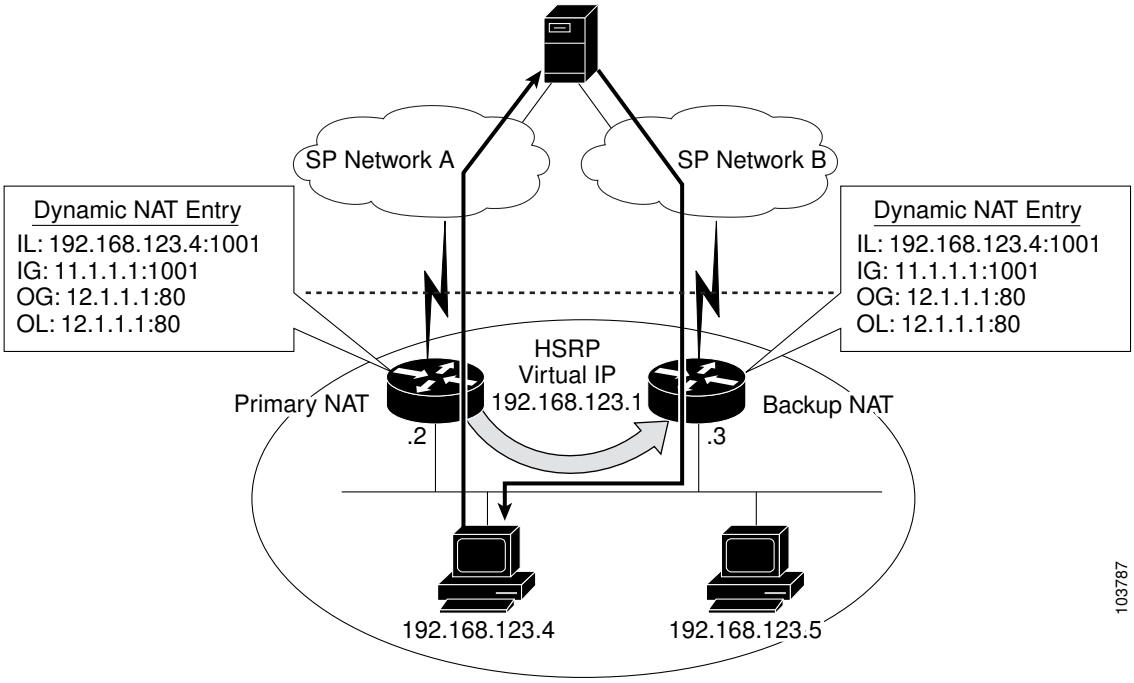
Stateful Failover for Asymmetric Outside-to-Inside Support

Stateful failover for asymmetric outside-to-inside support enables two NAT routers to participate in a primary/backup design. One of the routers is elected as the primary NAT router and a second router acts as the backup router. As traffic is actively translated by the primary NAT router it updates the backup NAT router with the NAT translation state from NAT translation table entries. If the primary NAT router fails or is out of service, the backup NAT router will automatically take over. When the primary comes back into service it will take over and request an update from the backup NAT router. Return traffic is handled by either the primary or the backup NAT translator and NAT translation integrity is preserved.

When the backup NAT router receives asymmetric IP traffic and performs NAT of the packets, it will update the primary NAT router to ensure both the primary and backup NAT translation tables remain synchronized.

The figure below shows a typical configuration that uses the NAT Stateful Failover for Asymmetric Outside-to-Inside and ALG Support feature.

Figure 1 Stateful NAT Asymmetric Outside-to-Inside Support



Stateful Failover for ALGs

The stateful failover embedded addressing enhancement allows the secondary or backup NAT router to properly handle NAT and delivery of IP traffic. NAT inspects all IP traffic entering interfaces that have been configured with the NAT feature. The inspection consists of matching the incoming traffic against a set of translations rules and performs an address translation if a match occurs. The following are examples:

- Matching a source address range
- Matching a specific destination address range
- Matching a list of applications known to NAT that might require a specific source port for control plane negotiation, or embedded source IP addresses within the application protocol

Some of the applications and protocols that embed source port or IP address information include:

- H.323 Registration, Admission, and Status (RAS) Protocol
- DNS queries
- NetMeeting Internet Locator Server (ILS)
- Internet Control Message Protocol (ICMP)
- Simple Mail Transfer Protocol (SMTP)
- Point-to-Point Tunneling Protocol (PPTP)
- Network File System (NFS)

A complete list of current ALG protocols supported by Cisco IOS NAT can be found at

http://www.cisco.com/en/US/tech/tk648/tk361/tech_brief09186a00801af2b9.html

How to Configure NAT for High Availability

Configuring the Stateful Failover of NAT

The NAT Stateful Failover of Network Address Translation feature represents Phase 1 of the stateful failover capability. It introduces support for two or more network address translators to function as a translation group. A backup router running NAT provides translation services in the event the active translator fails. Protocols that do not need payload translations, such as HTTP and telnet, are supported by stateful NAT (SNAT).

This section contains the following procedures:

Restrictions for Configuring Stateful Failover of NAT

The following applications and protocols are not supported in Phase I:

- Application Level Gateway (ALG)
- FTP
- NetMeeting Directory (ILS)
- RAS
- SIP
- Skinny
- TFTP
- Asymmetrical routing

SNAT features are not backward compatible. See "Feature Information for Configuring NAT for High Availability" and “Scalability for Stateful NAT” for information on SNAT features and the releases in which they were introduced.

Configuring SNAT with HSRP

Perform this task to configure Stateful NAT using HSRP to provide router backup facilities.

Note This task must be performed on both the **active** and the **standby** routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby** [*group-name*] **ip**[*ip-address*[**secondary**]]
5. **exit**
6. **ip nat stateful id** *id-number* {**redundancy** *name* **mapping-id** *map-number*}
7. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
8. **ip nat inside source** {**route-map** *name* **pool** *pool-name* **mapping-id** *map-number*} [**overload**]
9. **exit**
10. **show ip snat distributed verbose**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**standby** [*group-name*] **ip**[*ip-address*[**secondary**]] **Example:** `Router(config-if)# standby SNATHSRP ip 10.1.1.1`	Enables the HSRP protocol.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 6	**ip nat stateful id** *id-number* {**redundancy** *name* **mapping-id** *map-number*} **Example:** `Router(config)# ip nat stateful id 1 redundancy snathsrp mapping-id 10`	Specifies SNAT on routers configured for HSRP.
Step 7	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* **Example:** `Router(config)# ip nat pool snatpool1 10.1.1.1 10.1.1.9 prefix-length 24`	Defines a pool of IP addresses.
Step 8	**ip nat inside source** {**route-map** *name* **pool** *pool-name* **mapping-id** *map-number*} [**overload**] **Example:** `Router(config)# ip nat inside source route-map rm-101 pool snatpool1 mapping-id 10 overload`	Enables stateful NAT for the HSRP translation group.
Step 9	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 10	**show ip snat distributed verbose** **Example:** `Router# show ip snat distributed verbose`	(Optional) Displays active stateful NAT translations.

Configuring SNAT on the Primary (Active) Router

Perform this task to manually configure your primary SNAT router. When you have completed this task, perform the steps in "Configuring SNAT on the Backup (Standby) Router".

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-number*
4. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
5. **ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**]
6. **exit**
7. **show ip snat distributed verbose**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-number* **Example:** `Router(config)# ip nat stateful id 1 primary 10.10.10.10 peer 10.22.22.22 mapping-id 10`	Specifies stateful NAT on the primary router.
Step 4	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* **Example:** `Router(config)# ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24`	Defines a pool of IP addresses.
Step 5	**ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**] **Example:** `Router(config)# ip nat inside source route-map rm-101 pool snatpool1 mapping-id 10 overload`	Enables stateful NAT for the HSRP translation group.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 7	**show ip snat distributed verbose** **Example:** `Router# show ip snat distributed verbose`	(Optional) Displays active stateful NAT translations.

Configuring SNAT on the Backup (Standby) Router

Perform this task to manually configure your backup (standby) SNAT router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat stateful id** *id-number* **backup** *ip-address* **peer** *ip-address* **mapping-id** *map-number*
4. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
5. **ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**]
6. **exit**
7. **show ip snat distributed verbose**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip nat stateful id** *id-number* **backup** *ip-address* **peer** *ip-address* **mapping-id** *map-number* **Example:** `Router(config)# ip nat stateful id 1 backup 10.2.2.2 peer 10.10.10.10 mapping-id 10`	Specifies stateful NAT on the backup router.
Step 4	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* **Example:** `Router(config)# ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24`	Defines a pool of IP addresses.
Step 5	**ip nat inside source route-map** *name* **pool** *pool-name* **mapping-id** *map-number* [**overload**] **Example:** `Router(config)# ip nat inside source route-map rm-101 pool snatpool1 mapping-id 10 overload`	Enables stateful NAT for the HSRP translation group.
Step 6	**exit** **Example:** `Router(config)# exit`	Returns to privileged EXEC mode.
Step 7	**show ip snat distributed verbose** **Example:** `Router# show ip snat distributed verbose`	(Optional) Displays active stateful NAT translations.

Configuring NAT Stateful Failover for Asymmetric Outside-to-Inside and ALG Support

Stateful NAT Phase I required all sessions to pass through the primary NAT router that controlled the NAT translation entries unless the primary NAT router was unavailable. This requirement assured integrity of the translation information by guarding against the possibility of some packets relevant to NAT session control from traversing the backup without the primary being aware of it. Without synchronized IP sessions NAT eventually times out the IP session entries and the result is IP session states that are out of sequence.

This section contains the following procedures:

- Prerequisites for Configuring the NAT Stateful Failover for Asymmetric Outside-to-Inside and ALG Support Feature, page 11

Prerequisites for Configuring the NAT Stateful Failover for Asymmetric Outside-to-Inside and ALG Support Feature

Each router must have the same Network Address Translation (NAT) configurations.

The stateful failover asymmetric outside-to-inside enhancement provides the following benefits:

- Ability to support multiple routing paths from outside-to-inside
- Ability to handle per-packet load balancing of asymmetric routing from outside-to-inside

Configuring SNAT with HSRP

To configure your Hot Standby Router Protocol (HSRP) router with Stateful Network Address Translation (SNAT), use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby** [*group-name]* **ip**[*ip-address*[**secondary**]]
5. **exit**
6. **ip nat stateful id** *ip-address* **redundancy** *group-name* **mapping-id** *map-id*
7. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
8. **ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**]
9. **ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id*
10. **ip nat outside source static** *global-ip local-ip* **extendable mapping-id** *map-id*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**standby** [*group-name]* **ip**[*ip-address*[**secondary**]] **Example:** `Router(config-if)# standby SNATHSRP ip 11.1.1.1 secondary`	Enables the HSRP protocol.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 6	**ip nat stateful id** *ip-address* **redundancy** *group-name* **mapping-id** *map-id* **Example:** `Router(config)# ip nat stateful id 1 redundancy snathsrp mapping-id 10`	Specifies SNAT on routers configured for HSRP.
Step 7	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* **Example:** `Router(config)# ip nat pool snatpool1 11.1.1.1 11.1.1.9 prefix-length 24`	Defines a pool of IP addresses.
Step 8	**ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**] **Example:** `Router(config)# ip nat inside source static route-map rm-101 pool snatpool2 mapping-id 10 overload`	Enables stateful NAT for the HSRP translation group.
Step 9	**ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id* **Example:** `Router(config)# ip nat inside destination list 1 pool snatpool2 mapping-id 10`	Enables the local SNAT router to distribute a particular set of locally created entries to a peer SNAT router.

	Command or Action	Purpose
Step 10	**ip nat outside source static** *global-ip local-ip* **extendable mapping-id** *map-id* **Example:** `Router(config)# ip nat outside source static 1.1.1.1 2.2.2.2 extendable mapping-id 10`	Enables stateful NAT for the HSRP translation group.
Step 11	**end** **Example:** `Router(config)# end`	Exits global configuration mode. • Use the **end** command to save your configuration and leave configuration mode.

Configuring SNAT Primary Backup

Use the following commands to enable the NAT Stateful Failover for Asymmetric Outside-to-Inside and ALG Support feature:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-id*
4. **ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length*
5. **ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**]
6. **ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id*
7. **ip nat outside source Static** *global-ip local-ip* **extendable mapping-id** *map-id*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip nat stateful id** *id-number* **primary** *ip-address* **peer** *ip-address* **mapping-id** *map-id* **Example:** `Router(config)# ip nat stateful id 1 primary 1.1.1.1 peer 2.2.2.2 mapping-id 10`	Specifies stateful NAT on the primary router.
Step 4	**ip nat pool** *name start-ip end-ip* **prefix-length** *prefix-length* **Example:** `Router(config)# parser config cache interface`	Defines a pool of IP addresses.
Step 5	**ip nat inside source static route-map** *name* **pool** *pool-name* **mapping-id** *map-id* [**overload**] **Example:** `Router(config)# ip nat inside source static route-map rm-101 pool snatpool2 mapping-id 10 overload`	Enables stateful NAT of the inside source address to distribute a particular set of locally created entries to a peer SNAT router.
Step 6	**ip nat inside destination list** *number* **pool** *name* **mapping-id** *map-id* **Example:** `Router(config)# ip nat inside destination list 1 pool snatpool2 mapping-id 10 overload`	Defines the inside destination address that enables the local SNAT router to distribute locally created entries to a peer SNAT router.
Step 7	**ip nat outside source Static** *global-ip local-ip* **extendable mapping-id** *map-id* **Example:** `Router(config)# ip nat outside source static 1.1.1.1 2.2.2.2 extendable mapping-id 10`	Enables stateful NAT of the outside source address to distribute a particular set of locally created entries to a peer SNAT router.
Step 8	**end** **Example:** `Router(config)# end`	Exits global configuration mode. • Use the **end** command to save your configuration and leave configuration mode.

Configuring NAT Static Mapping Support for HSRP

When an Address Resolution Protocol (ARP) query is triggered for an address that is configured with NAT static mapping and owned by the router, NAT responds with the burned in MAC (BIA MAC) address on the interface to which the ARP is pointing. Two routers are acting as HSRP active and standby. Their NAT inside interfaces must be enabled and configured to belong to a group.

Benefits of Configuring Static Mapping Support for HSRP are the following:

- Using static mapping support for HSRP, failover is ensured without having to time out and repopulate upstream ARP caches in a high-availability environment, where HSRP router pairs have identical NAT configuration for redundancy.
- Static mapping support for HSRP allows the option of having only the HSRP active router respond to an incoming ARP for a router configured with a NAT address.

Both of the following tasks are required and must be performed on both the active and standby routers to configure NAT static mapping support for HSRP:

- Restrictions for Configuring Static Mapping Support for HSRP, page 15
- Enabling HSRP on the NAT Interface, page 15
- Enabling Static NAT in an HSRP Environment, page 17

Restrictions for Configuring Static Mapping Support for HSRP

- Configuring static mapping support for HSRP provides NAT support in the presence of HSRP using static mapping configuration only.
- Static NAT mappings must be mirrored on two or more HSRP routers, because NAT state will not be exchanged between the routers running NAT in an HSRP group.
- Behavior will be unpredictable if both HSRP routers have the same static NAT and are not configured with the **hsrp** keyword linking them to the same HSRP group.

Enabling HSRP on the NAT Interface

Perform this task to enable HSRP on the NAT interface of both the active and standby routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **no ip redirects**
6. **ip nat** {**inside** | **outside**}
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **standby** [*group-number*] **name** [*group-name*]
9. **end**
10. **show standby**
11. **show ip nat translations** [**verbose**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 1/1`	Enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 192.168.1.27 255.255.255.0`	Sets the primary IP address on the interface.
Step 5	**no ip redirects** **Example:** `Router(config-if)# no ip redirects`	Disables the sending of redirect messages
Step 6	**ip nat** {**inside** | **outside**} **Example:** `Router(config)# ip nat inside`	Marks the interface as connected to the inside or outside.
Step 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 10 ip 192.168.5.30`	Enables the HSRP protocol.

	Command or Action	Purpose
Step 8	**standby** [*group-number*] **name** [*group-name*] **Example:** `Router(config-if)# standby 10 name HSRP1`	Sets the HSRP group name.
Step 9	**end** **Example:** `Router(config-if)# exit`	Returns to privileged EXEC mode.
Step 10	**show standby** **Example:** `Router# show standby`	(Optional) Displays HSRP information
Step 11	**show ip nat translations** [**verbose**] **Example:** `Router# show ip nat translations verbose`	(Optional) Displays active NAT translations.

- What to Do Next, page 17

What to Do Next

Go to the next section and enable static NAT in the HSRP environment.

Enabling Static NAT in an HSRP Environment

To enable static mapping support with HRSP for high availability, perform this task on both the active and standby routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*}
4. **ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*}
5. **exit**
6. **show ip nat translations** [**verbose**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*} **Example:** `Router(config)# ip nat inside source static 192.168.5.33 10.10.10.5 redundancy HSRP1`	Enables the router to respond to ARP queries using BIA MAC, if HSRP is configured on the NAT inside interface.
Step 4	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name*} [**overload**] | **static** *local-ip global-ip* **redundancy** *group-name*} **Example:** `Router(config)# ip nat outside source static 192.168.5.33 10.10.10.5 redundancy HSRP1`	Enables the router to respond to ARP queries using BIA MAC, if HSRP is configured on the NAT outside interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Returns to privileged EXEC mode.
Step 6	**show ip nat translations** [**verbose**] **Example:** `Router# show ip nat translations verbose`	(Optional) Displays active NAT translations.

Configuration Example for NAT for High Availability

Examples Configuring Stateful NAT

The following examples show configuring stateful NAT with HSRP and configuring stateful NAT primary and backup routers.

SNAT with HSRP Example

```
ip nat Stateful id 1
redundancy SNATHSRP
mapping-id 10
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
ip route 10.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

Configuring SNAT Primary/Backup Example

```
ip nat Stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10
!
ip nat Stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

Configuration Examples for NAT Stateful Failover for Asymmetric Outside-to-Inside and ALG Support

This section contains the following examples:

Example Configuring SNAT with HSRP

The following example shows how to configure SNAT with HSRP.

```
ip nat Stateful id 1
redundancy SNATHSRP
mapping-id 10
ip nat pool SNATPOOL1 11.1.1.1 11.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
```

```
ip route 11.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

Example Configuring SNAT Primary Backup

The following example shows how to configure SNAT on the primary/backup router.

```
ip nat Stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10
!
ip nat Stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

Examples Configuring Static NAT in an HSRP Environment

The following example shows support for NAT with a static configuration in an HSRP environment. Two routers are acting as HSRP active and standby, and the NAT inside interfaces are HSRP enabled and configured to belong to the group HSRP1.

Active Router Configuration

```
interface BVI10
 ip address 192.168.5.54 255.255.255.255.0
 no ip redirects
 ip nat inside
 standby 10 priority 105 preempt
 standby 10 name HSRP1
 standby 10 ip 192.168.5.30
 standby 10 track Ethernet2/1
!
!
 ip default-gateway 10.0.18.126
 ip nat inside source static 192.168.5.33 10.10.10.5 redundancy HSRP1
 ip classless
 ip route 10.10.10.0 255.255.255.0 Ethernet2/1
 ip route 172.22.33.0 255.255.255.0 Ethernet2/1
 no ip http server
```

Standby Router Configuration

```
interface BVI10
 ip address 192.168.5.56 255.255.255.255.0
 no ip redirects
 ip nat inside
 standby 10 priority 100 preempt
 standby 10 name HSRP1
 standby 10 ip 192.168.5.30
 standby 10 track Ethernet3/1
!
 ip default-gateway 10.0.18.126
 ip nat inside source static 192.168.5.33 3.3.3.5 redundancy HSRP1
 ip classless
 ip route 10.0.32.231 255.255.255 Ethernet3/1
 ip route 10.10.10.0 255.255.255.0 Ethernet3/1
 no ip http server
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NAT commands: complete command syntax, command mode, command history, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
IP Access List Sequence Numbering	*IP Access List Sequence Numbering* document
NAT configuration tasks	"Configuring NAT for IP Address Conservation" module
NAT maintenance	"Monitoring and Maintaining NAT" module
Using NAT with MPLS VPNs	"Integrating NAT with MPLS VPNs" module

Standards

Standards	Title
None	

MIBs

MIBs	MIBs Link
• None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 903	*Reverse Address Resolution Protocol*
RFC 826	*Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware*
RFC 1027	*Using ARP to implement transparent subnet gateways*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring NAT for High Availability

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 1 Feature Information for Configuring NAT for High Availability

Feature Name	Releases	Feature Configuration Information
NAT Stateful Failover for Asymmetric Outside-to-Inside ALG Support	12.3(7)T	The NAT Stateful Failover for Asymmetric Outside-to-Inside and Application Layer Gateway (ALG) Support feature improves the ability to handle asymmetric paths by allowing multiple routing paths from outside-to-inside, and per-packet load balancing. This feature also provides seamless failover translated IP sessions with traffic that includes embedded IP addressing such as Voice over IP, FTP, and Domain Name System (DNS) applications.

Feature Name	Releases	Feature Configuration Information
NAT Stateful Failover of Network Address Translation	12.2(13)T	The NAT Stateful Failover of Network Address Translation feature represents Phase 1 of the stateful failover capability. It introduces support for two or more network address translators to function as a translation group.
NAT--Static Mapping Support with HSRP for High Availability	12.2(4)T 12.2(4)T2 Cisco IOS XE Release 2.1	Static mapping support for HSRP allows the option of having only the HSRP active router respond to an incoming ARP for a router configured with a NAT address.