Cisco IOS Network Address Translation

Overview

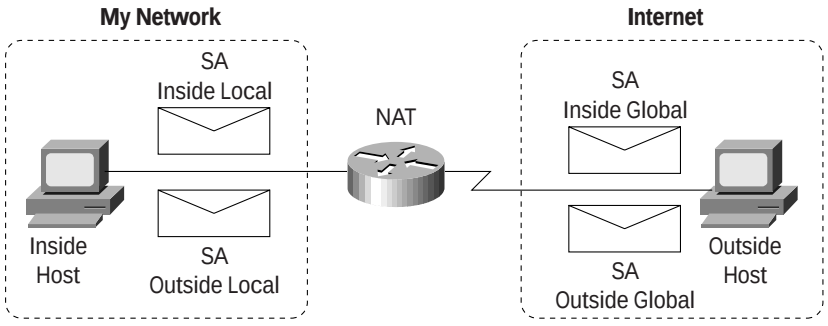
In its simplest configuration, the Network Address Translator (NAT) operates on a router connecting two networks together; one of these networks (designated as inside) is addressed with either private or obsolete addresses that need to be converted into legal addresses before packets are forwarded onto the other network (designated as outside). The translation operates in conjunction with routing, so that NAT can simply be enabled on a customer-side Internet access router when translation is desired.

Use of a NAT device provides RFC 1631-style network address translation on the router platform. The goal of NAT is to provide functionality as if the private network had globally unique addresses and the NAT device was not present. RFC 1631 represents a subset of Cisco IOS NAT functionality.

Cisco IOS NAT supports "bi-directional translation" through the simultaneous use of "inside source" and "outside source" translations.

Terminology

Figure 1
NAT Concepts



- An IP address is either local or global
- Local IP addresses are seen in the inside network
- Global IP addresses are seen in the Outside network

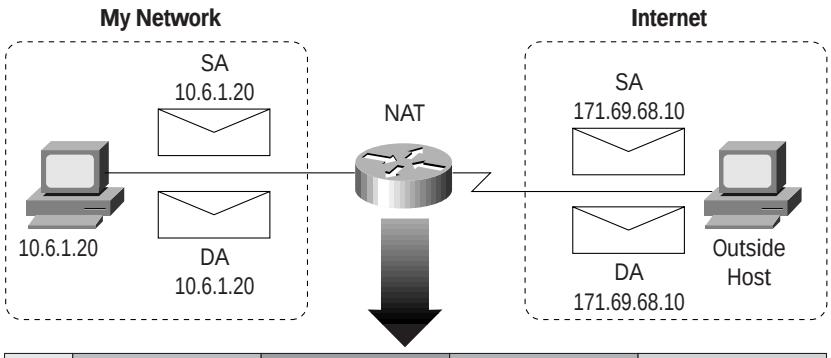
Inside

Set of networks subject to translation

Outside

All other addresses. Usually these are valid addresses located on the Internet.

Figure 2
NAT Terminology « Inside Addressing»

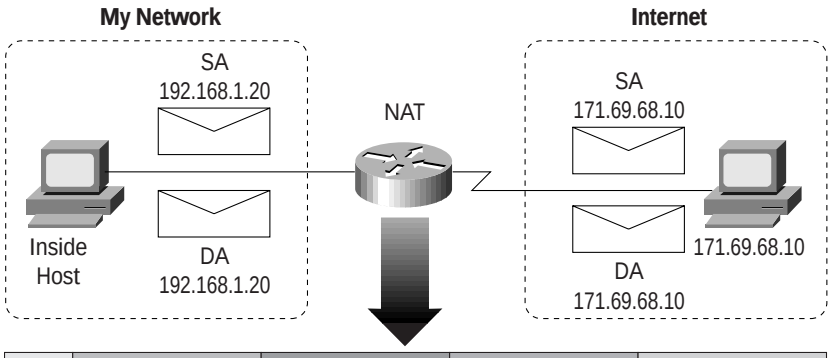


Pro	Inside Global	Inside Local	Outside Local	Outside Global
--	171.69.68.10	10.6.1.20	--	--

10.6.1.20 is inside local address
171.69.68.10 is inside global address

- Inside local: configured IP address assigned to a host on the inside network. Address may be globally unique, allocated out of the private address space defined in RFC 1918, or might be officially allocated to another organization
- Inside global: the IP address of an inside host as it appears to the outside network, “Translated IP Address”. Addresses can be allocated from a globally unique address space, typically provided by the ISP (if the enterprise is connected to the global Internet)

Figure 3
NAT Terminology “Outside Addressing”



Pro	Inside Global	Inside Local	Outside Local	Outside Global
--	--	--	192.168.1.20	171.69.68.10

192.168.1.20 is outside local address
171.69.68.10 is outside :global address

- Outside local: the IP address of an outside host as it appears to the inside network. These addresses can be allocated from the RFC 1918 space if desired
- Outside global: the configured IP address assigned to a host in the outside network

Simple Translation Entry

Translation entry that maps one IP address to another

Extended Translation Entry

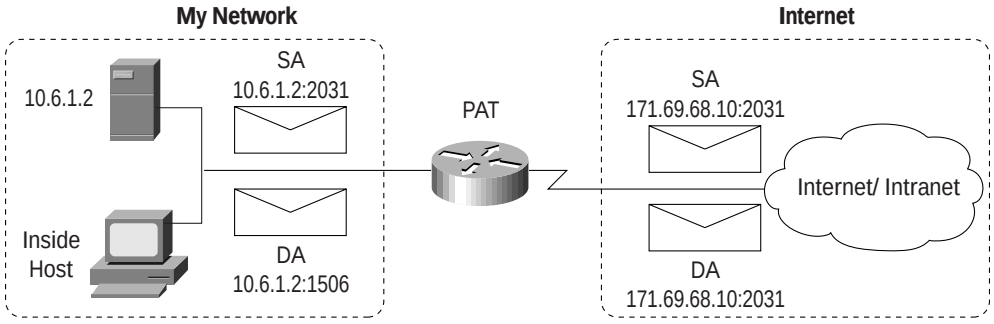
Translation entry that maps one IP address and port pair to another

Main Features

- Static Address Translation—Telnet 207.33.94.1
  The user can establish a one-to-one mapping between local and global addresses

  Users can also configure Static address translations to the port level, and use the remainder of the IP address for other translations. Typically where you are performing Port Address Translation (PAT)
- Dynamic Address Translation
  The user can establish dynamic mapping between the local and global addresses. This is done by describing the local addresses to be translated and the pool of addresses from which to allocate global addresses, and associating the two.
- Match Host
  The ability to configure NAT to assign the same Host portion of an IP Address and only translate the Network prefix portion of the IP Address. Useful where you are using the host portion as a means to identify or number users uniquely
- Port Address Translation (PAT)

Figure 4
Basic Concepts of PAT



Port Address Translations (PAT) extends NAT form "1 to 1"
to "many-to-1"by associating the source port with each flow

Figure 5
Unique Source Port per Translation Entry

Pro	Inside Global	Inside Local	Outside Local	Outside Global
tcp	171.69.68.5:1405	10.6.15.2:1405	204.71.200.69:80	204.71.200.69:80

PAT (Port Address Translation) includes ports in addition to IP address
Many-to-one translation
Maps multiple IP addresses to 1 or a few IP addresses
Unique source port number identifies each session
Conserves registered IP addresses
Also called NAPT in IEFTF documents

Several internal addresses can be NATed to only one or a few external addresses by using a feature called Port Address Translation (PAT) which is also referred to as "overload", a subset of NAT functionality.

PAT uses unique source port numbers on the Inside Global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number could theoretically be as high as 65,536 per IP address. PAT will attempt to preserve the original source port, if this source port is already allocated PAT will attempt to find the first available port number starting from the beginning of the appropriate port group 0-511[1], 512-1023 or 1024-65535. If there is still no port available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and IP addresses.

- Destination Address Rotary Translation
  A dynamic form of destination translation can be configured for some outside-to-inside traffic. Once a mapping is set up, a destination address matching one of those on an access list will be replaced with an address from a rotary pool. Allocation is done in a round-robin basis, performed only when a new connection is opened from the outside to the inside. All non-TCP traffic is passed untranslated (unless other translations are in effect).

This feature was designed to provide protocol translation load distribution. It is not designed nor intended to be used as a substitute technology for Cisco's LocalDirector product. Destination address rotary translation should not be used to provide web service load balancing because, like vanilla DNS, it knows nothing about service availability. As a result, if a web server were to become offline, the destination address rotary translation feature would continue to send requests to the downed server.

For additional information, please visit:

http://www.cisco.com/warp/public/732/Tech/ipservices/docs/algs.pdf

Configuration Commands

Interface Configuration Commands

```
ip nat { inside | outside }
```

Interfaces need to be marked whether they are on the inside or the outside. Only packets arriving on a marked interface will be subject to translation.

1. Group starts at 0 for ICMP, but 1 for all other applications. As of DDTS CSCdm05636 the number of Port groups changed from 4 to the 3 outlined above.

Global Configuration Commands

- Defining a pool

  ```
  ip nat pool <name> <start-ip> <end-ip> { netmask <netmask>
   | prefix-length <prefix-length> } [ type { rotary } ]
  ```

  Defines a pool of addresses using start address, end address, and netmask. These addresses will be allocated as needed.

- Enabling translation of inside source addresses

  ```
  ip nat inside source { list <acl> pool <name> [overload] |
   static <local-ip><global-ip> }
  ```

  The first form enables dynamic translation. Packets from addresses that match those on the simple access list are translated using global addresses allocated from the named pool. The optional keyword overload enables port translation for UDP and TCP. The term overload is equivalent to Port Address Translation (PAT), as used on the Combinet C7x0 product.

  The second form of the command sets up a single static translation.

- Enabling translation of inside destination addresses

  ```
  ip nat inside destination { list <acl> pool <name> |
   static <global-ip> <local-ip> }
  ```

  This command is similar to the source translation command. For dynamic destination translation to make any sense, the pool should be a rotary-type pool.

- Enabling translation of outside source addresses

  ```
  ip nat outside source { list <acl> pool <name> | static <global-ip> <local-ip> }
  ```

  The first form (list..pool..) enables dynamic translation. Packets from addresses that match those on the simple access list are translated using local addresses allocated from the named pool.

  The second form (static) of the command sets up a single static translation.

- Configuring translation timeouts

  ```
  ip nat translation timeout <seconds>
  ```

  Dynamic translations time out after a period of non-use. When port translation is not configured, translation entries time out after 24 hours. This time can be adjusted with the above command or the following variations:

  ```
  ip nat translation udp-timeout <seconds>
  ip nat translation dns-timeout <seconds>
  ip nat translation tcp-timeout <seconds>
  ip nat translation finrst-timeout <seconds>
  ```

  When port translation is configured, there is finer control over translation entry timeouts, because each entry contains more context about the traffic using it. Non-DNS UDP translations time out after 5 minutes; DNS times out in 1 minute. TCP translations time out after 24 hours, unless a RST or FIN is seen on the stream, in which case it times out in 1 minute.

Exec Commands

- Showing active translations

  ```
  show ip nat translations [ verbose ]
  ```

- Showing translation statistics

  ```
  show ip nat statistics
  ```

- Clearing dynamic translations

  ```
  clear ip nat translation *
  ```

  Clears all dynamic translations.

  ```
  clear ip nat translation <global-ip>
  ```

  Clears a simple translation.

  ```
  clear ip nat translation <global-ip> &ltlocal-ip> <proto> <global-port> <local-port>
  ```

  Clears a particular dynamic translation.

- Debugging

  ```
  debug ip nat [ <list> ] [ detailed ]
  ```

Configuration Examples

The following sample configuration translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 nets to the globally-unique 171.69.233.208/28 network.

```
ip nat pool net-20 171.69.233.208 171.69.233.223 netmask <netmask> 255.255.255.240
ip nat inside source list 1 pool net-20
!
interface Ethernet0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface Ethernet1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The next sample configuration translates between inside hosts addressed from the 9.114.11.0 net to the globally unique 171.69.233.208/28 network. Packets from outside hosts addressed from 9.114.11.0 net (the “true” 9.114.11.0 net) are translated to appear to be from net 10.0.1.0/24.

```
ip nat pool net-20 171.69.233.208 171.69.233.223 netmask <netmask> 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 netmask <netmask> 255.255.255.0
ip nat inside source list 1 pool net-20
ip nat outside source list 1 pool net-10
!
interface Ethernet0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface Ethernet1
ip address 9.114.11.39 255.255.255.0
ip nat inside
!
access-list 1 permit 9.114.11.0 0.0.0.255
```

Feature Enhancements

- More flexible pool configuration:

  The pool configuration syntax has been extended to allow discontiguous ranges of addresses. The following syntax is now allowed:

  ```
  ip nat pool <name> { netmask <mask> | prefix-length <length> } [ type { rotary } ]
  ```

  This command will put the user into IP NAT Pool configuration mode, where a sequence of address ranges can be configured. There is only one command in this mode:

  ```
  address <start> <end>
  ```

  Example:

  ```
  Router(config)#ip nat pool fred prefix-length 24
  Router(config-ipnat-pool)#address 171.69.233.225 171.69.233.226
  Router(config-ipnat-pool)#address 171.69.233.228 171.69.233.238
  ```

  This configuration creates a pool containing addresses 171.69.233.225-226 and 171.69.233.228-238 (171.69.233.227 has been omitted).

- Translating to interface's address:

  As a convenience for users wishing to translate all inside addresses to the address assigned to an interface on the router, the NAT code allows one to simply name the interface when configuring the dynamic translation rule:

  ```
  ip nat inside source list <number> interface <interface> overload
  ```

  If there is no address on the interface, or it the interface is not up, no translation will occur.

  Example:

  ```
  ip nat inside source list 1 interface Serial0 overload
  ```

- Static translations with ports:

  When translating addresses to an interface's address, outside-initiated connections to services on the inside network (like mail) will require additional configuration to send the connection to the correct inside host. This command allows the user to map certain services to certain inside hosts.

  ```
  ip nat inside source static { tcp | udp } <localaddr> <localport> <globaladdr> <globalport>
  ```

  Example:

  ```
  ip nat inside source static tcp 192.168.10.1 25 171.69.232.209 25
  ```

  In this example, outside-initiated connections to the SMTP port (25) will be sent to the inside host 192.168.10.1.

- Support for route maps:

  The dynamic translation command can now specify a route-map to be processed instead of an access-list. A route-map allows the user to match any combination of access-list, next-hop IP address, and output interface to determine which pool to use:

  ```
  ip nat inside source route-map <name> pool <name>
  ```

  Example:

  ```
  ip nat pool provider1-space 171.69.232.1 171.69.232.254 prefix-length 24
  ip nat pool provider2-space 131.108.43.1 131.108.43.254 prefix-length 24
ip nat inside source route-map provider1-map pool provider1-space
```

```
ip nat inside source route-map provider2-map pool provider2-space
!
interface Serial0/0
 ip nat outside
!
interface Serial0/1
 ip nat outside
!
interface Fddi1/0
 ip nat inside
!
route-map provider1-map permit 10
 match ip address 1
 match interface Serial0/0
!
route-map provider2-map permit 10
 match ip address 1
 match interface Serial0/1
```

- "Extendable" static translations:

  The extendable keyword allows the user to configure several ambiguous static translations, where an ambiguous translations are translations with the same local or global address.

  ```
  ip nat inside source static <localaddr> <globaladdr> extendable
  ```

  Some customers want to use more than one service provider and translate into each provider's address space. You can use route-maps to base the selection of global address pool on output interface as well as an access-list match. Following is an example:

  ```
  ip nat pool provider1-space ...
  ip nat pool provider2-space ...
  ip nat inside source route-map provider1-map pool provider1-space
  ip nat inside source route-map provider2-map pool provider2-space
  !
  route-map provider1-map permit 10
   match ip address 1
   match interface Serial0/0
  !
  route-map provider2-map permit 10
   match ip address 1
   match interface Serial0/1
   .
   .
   .
  ```

Once that is working, they might also want to define static mappings for a particular host using each provider's address space. The software does not allow two static translations with the same local address, though, because it is ambiguous from the inside. The router will accept these static translations and resolve the ambiguity by creating full translations (all addresses and ports) if the static translations are marked as "extendable". For a new outside-to-inside flow, the appropriate static entry will act as a template for a full translation. For a new inside-to-outside flow, the dynamic route-map rules will be used to create a full translation.

- Autoaliasing of Pool Addresses:

  Many customers want to configure the NAT software to translate their local addresses to global addresses allocated from unused addresses from an attached subnet. This requires that the router answer ARP requests for those addresses so that packets destined for the global addresses are accepted by the router and translated. (Routing takes care of this packet delivery when the global addresses are allocated from a virtual network which isn't connected to anything.) When a NAT pool used as an inside global or outside local pool consists of addresses on an attached subnet, the software will generate an alias for that address so that the router will answer ARPs for those addresses.

  This automatic aliasing also occurs for inside global or outside local addresses in static entries. It can be disabled for static entries can be disabled by using the "no-alias" keyword:.

  ```
  ip nat inside source static <local-ip-address> <global-ip-address> no-alias
  ```

- Host Number Preservation:

  For ease of network management, some sites wish to translate prefixes, not addresses. That is, they wish the translated address to have the same host number as the original address. Of course, the two prefixes must be of the same length. This feature can be enabled by configuring dynamic translation as usual, but configuring the address pool to be of type "match-host":

  ```
  ip nat pool fred <start> <end> prefix-length <len> type match-host
  ```

- Translation Timeout Improvements:

  The following new timeouts have been implemented for extended translation entries:

  ```
  ip nat translation ?
     icmp-timeout Specify timeout for NAT ICMP flows
     syn-timeout Specify timeout for NAT TCP flows after a SYN and no further data
  ```

- Translation Entry Limit:

  Using the following command, Cisco IOS NAT can be configured to limit the number of translation entries it creates. The default is that there is no limit.

  ```
  ip nat translation max-entries <n>
  ```

For More Information

NAT

Visit the main CCO NAT Page.

Refer to the “Configure Network Address Translation (NAT)” section in the Configuring IP Addressing documentation.

RFCs

For information about the RFCs referenced in this document, see:

- Primary and Secondary RFC Repositories, a Technical Tip that explains where and how to obtain RFCs.
- List of Cisco-Supported RFCs, a list of RFCs supported by Cisco’s system software as of release 10.0(1).
- RFCs, Standards and Technical Publications, an index of requests for comment.

Additional Informaiton

http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:NAT

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

ETMG 202925—SH 08/03