Cisco Network Address Translation (NAT)

Introduction

This document provides answers to some of the more frequently asked questions with regard to Cisco IOS® Network Address Translation (NAT).

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Q. What is NAT?

A. Network Address Translation (NAT) is designed for IP address simplification and conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network. As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation, and is typically implemented in remote-access environments.

Q. What are the main differences between the Cisco IOS® Software and Cisco® PIX® Security Appliance implementations of NAT?

A. Cisco IOS Software-based NAT is not fundamentally different from the NAT function in the Cisco PIX Security Appliance. The main differences involve the different traffic types supported in the implementations. Refer to Cisco PIX 500 Series Security Appliances and NAT Configuration Examples for more information on the configuration of NAT on Cisco PIX devices (includes the traffic types supported).

Q. On which Cisco routing hardware is Cisco IOS NAT available? How can the hardware be ordered?

A. The Cisco Feature Navigator tool allows customers to identify which release and hardware any Cisco IOS Software feature is available on. To use this tool, please refer to http://www.cisco.com/go/fn/.

Originally introduced in Cisco IOS Software Release 11.2, NAT was only available in the "Plus" images. With introduction of Cisco IOS Software Release 11.3, Port Address Translation (PAT) became available in all IP images, while full NAT (1-1 and PAT) was still available only in "Plus" images. With Cisco IOS Software Release 12.0, all IP images provide full NAT capability.

Table 1 shows how the Feature Navigator can be used to find all the hardware and feature sets that support the NAT capability in Cisco IOS Software Release 12.4(11)T:

<table>
<thead>
<tr>
<th>Your Selections</th>
<th>NAT (Network Address Translation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td></td>
</tr>
<tr>
<td>Major Release</td>
<td>Cisco IOS Software Release 12.4T</td>
</tr>
<tr>
<td>Release</td>
<td>Cisco IOS Software Release 12.4(11)T</td>
</tr>
<tr>
<td>Platform</td>
<td>All platforms</td>
</tr>
</tbody>
</table>
Q. Does NAT occur before or after routing?
A. The order in which the transactions are processed using NAT is based on whether a packet is going from the inside network to the outside network, or from the outside network to the inside network. Inside to outside translation occurs after routing, and outside to inside translation occurs before routing. For more information, visit http://www.cisco.com/warp/public/556/5.html.

Q. How is routing awareness learned for IP addresses that are created using NAT?
A. Routing for IP addresses created by NAT is learned if:
   - The inside global address pool is derived from the subnet of a next-hop router
   - Static route entry is configured in the next-hop router and redistributed within the routing network

Q. How many concurrent NAT sessions are supported in Cisco IOS NAT?
A. The NAT session limit is bounded by the amount of available DRAM in the router. Each NAT translation consumes about 312 bytes in DRAM. As a result, 10,000 translations (more than would generally be handled on a single router) would consume about 3 MB. Therefore, typical routing hardware has more than enough memory to support thousands of NAT translations.

Q. What kind of routing performance can be expected when using Cisco IOS NAT?
A. Cisco IOS NAT supports Cisco Express Forwarding switching, fast switching, and process switching. Performance depends on several factors:
   - The type of application and its type of traffic
   - Whether IP addresses are embedded
   - Exchange and inspection of multiple messages
   - Source port required
   - The number of translations
   - Other applications running at the time
   - The type of hardware and processor

For most applications, degradation of performance due to NAT should be negligible.

Q. Can Cisco IOS NAT be applied to subinterfaces?
A. Yes. Source and/or destination NAT translations can be applied to any interface or subinterfaces having an IP address (including dialer interfaces).

Q. Can Cisco IOS NAT be used with Hot Standby Router Protocol (HSRP) to provide redundant links to an ISP?
A. No. In this scenario, the standby router would not have the translation table of the active router; when the cutover happens, connections will time out and fail.

Q. Does Cisco IOS NAT support inbound translations on a serial trunk running Frame Relay? Does it support outbound translations on the Ethernet side?
A. Yes.

Q. Can a single NAT-enabled router allow some users to use NAT and other users on the same Ethernet interface to continue with their own IP addresses?
A. Yes. This can be accomplished through the use of an access list describing the set of hosts or networks that require NAT. All sessions on the same host will either be translated or will pass through the router and not be translated.

Access lists, extended access lists, and route maps can be used to define "rules" by which IP devices get translated. The network address and appropriate subnet mask should always be specified. The keyword "any" should not be used in place of the network address or subnet mask.
Table 2. Sample NAT Configuration Rules

<table>
<thead>
<tr>
<th>NAT Translation Configuration</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip nat inside source static 10.1.1.10 140.16.1.254</td>
<td>Static translation for ns.bar.com DNS server</td>
</tr>
<tr>
<td>ip nat outside source static 10.1.1.10 192.168.1.254</td>
<td>Static translation for ns.foo.com DNS server</td>
</tr>
<tr>
<td>ip nat pool iga 140.16.1.1 140.16.1.253 netmask 255.255.255.0</td>
<td>Dynamic IL-&gt;IG address translations</td>
</tr>
<tr>
<td>ip nat pool ola 192.168.1.1 192.168.1.253 netmask 255.255.255.0</td>
<td>Dynamic OG-&gt;OL address translations</td>
</tr>
<tr>
<td>ip nat inside source list 1 pool iga</td>
<td>NAT Translation rule for inside traffic to be NAT'd, for which inside addresses and to what will they be NAT'd</td>
</tr>
<tr>
<td>ip nat outside source list 2 pool ola</td>
<td>NAT Translation rule for outside traffic to be NAT'd, for which inside addresses and to what will they be NAT'd</td>
</tr>
<tr>
<td>access-list 1 permit 10.2.17.0 .255.255.255.0</td>
<td>Translate all traffic from 10.2.17 internal hosts</td>
</tr>
<tr>
<td>access-list 2 permit 10.0.0.0 255.0.0.0</td>
<td>Translate all externally originated traffic</td>
</tr>
</tbody>
</table>

Q. What is PAT, or overloading?
A. PAT, or overloading, is a feature of Cisco IOS NAT and can be used to translate "internal" (inside local) private addresses to one or more "outside" (inside global, usually registered) IP addresses. Unique source port numbers on each translation are used to distinguish between the conversations. With NAT overload, a translation table entry containing full address and source port information is created.

Q. When configuring for PAT (overloading), what is the maximum number of translations that can be made per inside global IP address?
A. PAT (overloading) divides the available ports per global IP address into three ranges: 0-511, 512-1023, and 1024-65535. PAT assigns a unique source port for each UDP or TCP session. It will attempt to assign the same port value of the original request, but if the original source port has already been used, it will start scanning from the beginning of the particular port range to find the first available port and will assign it to the conversation.

Q. How does PAT work?
A. PAT works with either one IP address or multiple addresses.

   a) PAT with one IP address:
   1. NAT/PAT inspects traffic and matches it to a translation rule.
   2. Rule matches to a PAT configuration.
   3. If PAT knows about the traffic type, and that traffic type has "a set of specific ports or ports it negotiates" that it will use, PAT sets them aside and does not allocate them as unique identifiers.
   4. If a session with no special port requirements attempts to connect out, PAT translates the IP source address and checks availability of the originated source port (433, for example).

   Note: For Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), the ranges are: 1-511, 512-1023, 1024-65535. For Internet Control Message Protocol (ICMP), the first group starts at 0.

   5. If the requested source port is available, PAT assigns the source port, and the session continues.
   6. If the requested source port is not available, NAT starts searching from the beginning of the relevant group (starting at 1 for TCP or UDP applications, and from 0 for ICMP).
7. If a port is available it is assigned, and the session continues.
8. If no ports are available, the packet is dropped.

b) PAT with multiple IP addresses:
1–7. The first seven conditions are the same as with a single IP address.
8. If no ports are available in the relevant group on the first IP address, NAT flips to the next IP address in the pool and tries to allocate the original source port requested.
9. If the requested source port is available, NAT assigns the source port and the session continues.
10. If the requested source port is not available, NAT starts searching from the beginning of the relevant group (starting at 1 for TCP or UDP applications, and from 0 for ICMP).
11. If a port is available, it is assigned and the session continues.
12. If no ports are available, the packet is dropped, unless another IP address is available in the pool.

Q. What are NAT IP pools?
A. NAT IP pools are a range of IP addresses that are allocated for NAT translation as needed. To define a pool, the configuration command is used:

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

Q. What is the maximum number of configurable NAT IP pools (ip nat pool “name”)?
A. In practical use, the maximum number of configurable IP pools is limited by the amount of available DRAM being used in the particular router. It is highly recommended that a pool of size 255 is configured.

Q. How does NAT support multiple pools using route maps?

Q. What is IP address “overlapping” within the context of NAT?
A. IP address overlapping refers to a situation where two locations that want to interconnect are both using the same IP address scheme. This is not an unusual occurrence; it often happens when companies merge or are acquired. Without special support, the two locations will not be able to connect and establish sessions. The overlapped IP address can be a public address assigned to another company, a private address assigned to another company, or can come from the range of private addresses as defined in RFC 1918. Private IP addresses are unroutable and require NAT translations to allow connections to the outside world. The solution involves intercepting Domain Name System (DNS) name-query responses from the outside to the inside, setting up a translation for the outside address, and fixing up the DNS response before forwarding it to the inside host. A DNS server is required to be involved on both sides of the NAT device to resolve users wanting to have connection between both networks.

NAT is able to inspect and perform address translation on the contents of DNS “A” and “PTR” records, as shown in http://www.cisco.com/warp/public/556/3.html.

Q. What are static NAT translations?
A. Static NAT translations have 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. This typically occurs where you are performing Port Address Translation (PAT).

Q. What are dynamic NAT translations?
A. In dynamic NAT translations, the users can establish dynamic mapping between 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.

Q. Is it possible to build a configuration with both static and dynamic NAT translations?
A. Yes. However, the global addresses used in static translations are not automatically excluded with dynamic pools containing those global addresses. Dynamic pools have to be created to exclude addresses assigned by static entries. For more information, visit http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093f31.shtml.

Q. How do I change the dynamic NAT configuration?

Q. Can routing loops be avoided when using dynamic NAT?

Q. Can IP sessions be translated based on the destination network a session is trying to reach?
A. Yes. IP sessions can be translated by NAT based on the destination network the sessions and user are trying to reach. This capability is commonly referred to as `destination based NATing'.

Destination-based NATing uses route maps to determine which IP address each IP session is translated to based on routing reachability of the destination IP host. 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.


Q. Why does a subnet mask need to be specified when configuring a NAT address pool?
A. The subnet mask is used to double-check the addresses allocated from the pool. For example, the subnet broadcast address does not get allocated. The subnet mask must match the size of the subnet into which it is translated.

Q. Can IP addresses be allocated from the NAT router’s outside interface subnet to a dynamic NAT pool?
A. Yes. The NAT router will answer Address Resolution Protocol (ARP) requests for these IP addresses in the dynamic pool.

Q. Will a NAT router properly handle ICMP redirects?
A. Yes.

Q. How does NAT handle ICMP fragments?
A. Whether NAT drops or forwards an ICMP fragment depends on several factors, such as the order in which the NAT router receives the fragments, and the state of the translation table at that time. Under certain conditions, NAT translates the fragments differently, which makes it impossible for the destination device to reassemble the packet. The handling of ICMP fragments depends on the state of the NAT translation table, and the order in which the NAT router receives the ICMP fragments. For more information, visit http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093f96.shtml.

Q. Does Cisco NAT support all application traffic?
A. Application traffic is transparent to Cisco IOS NAT unless:

1. There are embedded IP addresses in the data portion.
2. An application requires preset or negotiated source/destination port values.

Cisco IOS NAT performs "stateful inspection" and needs to have previous knowledge of all applications that embed or require specific source ports. For instance, Cisco supports the translation of embedded IP addresses in DNS "A and PTR" records, FTP, and NetMeeting v2.11 (4.3.2519) and 3.01 (4.4.3385) by setting aside the source port values they require. Cisco will not assign those source port values when using the PAT feature of Cisco IOS NAT.

With embedded IP addresses, Cisco IOS NAT needs to know the messages that will be containing embedded addresses and the offset within these messages. If the embedded addresses match the configured rules, they will be translated according to the configuration. An application that embeds IP addresses that Cisco IOS NAT does not know about will not work properly in a Cisco IOS NAT configuration.

There is an exception. When a tunneling protocol such as Point-to-Point Tunneling Protocol (PPTP) is used, the embedded IP addresses of the tunneled packets will not be translated, but it is assumed that users who are connecting back to their corporate networks using PPTP would be using the IP addressing scheme of the corporate network, so NAT would not need to be applied to any embedded messages. If those users then want to access the outside world through their corporate networks, they might choose to apply NAT at that point.
Embedded IP addresses are an issue regardless of the types of translation that have been configured with Cisco IOS NAT (simple or extended overload, for example). Pre-set or negotiated source port values are an issue only when the PAT feature of Cisco IOS NAT is used. PAT multiplexes multiple IP conversations over one or more IP addresses and uses the source port to uniquely identify conversations on each IP address. The PAT feature needs to set aside all specific port values that Cisco has awareness for, in case it gets a conversation for those application types (FTP or NetMeeting, for example).

Q. Why doesn’t Cisco IOS NAT support Simple Network Management Protocol (SNMP) traffic?
A. The SNMP packet format depends on the particular MIB being used and is not self-describing. There is no single format for SNMP requests and responses that can be processed in a general fashion.

Q. Does Cisco IOS NAT support Domain Name System (DNS) queries?
A. Yes. Cisco IOS NAT will translate the addresses that appear in DNS responses to name lookups (A queries) and inverse lookups (PTR queries). Thus, if an outside host sends a name lookup to a DNS server on the inside, and that server responds with a local address, the NAT code will translate that local address to a global address. The opposite is also true. This is how Cisco supports IP addresses overlapping: an inside host queries an outside DNS server; the response contains an address that matches the access list specified on the “outside source” command, so the code translates the outside global address to an outside local address.

Time-to-live (TTL) values on all DNS resource records, which receive address translations in resource records payloads, are automatically set to zero.

Cisco IOS NAT does not translate IP addresses embedded in DNS zone transfers.

Q. How does multicast NAT work on Cisco routers?
A. When you configure NAT on a Cisco IOS router, multicast sources and receivers or Protocol Independent Multicast (PIM) entities, such as rendezvous points (RPs) or RP mapping agents, work on either side of the NAT router without additional configuration commands. You must enable multicast on all the routers (inside, outside, and the NAT router itself). For more information, visit http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a008009474d.shtml.

Q. What is “NAT on a stick”? 
A. The term “on a stick” usually implies the use of a single physical interface of a router for a task. Just as we can use subinterfaces of the same physical interface to perform Inter-Switch Link (ISL) trunking, we can use a single physical interface on a router in order to accomplish NAT. For more information, visit http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094430.shtml.

Q. Why does active FTP work with static and extended port forwarding, but not with PAT?
A. The reason is that when you open up the FTP connection you connect to port 21 at the remote FTP server. But when you do a "ls", "put", "get", or anything that needs to use a data port, the server opens up another connection back to the client. When you open your original FTP connection from the inside and the router pretends that you are a specific outside IP, and picks a random port number to use, the FTP server thinks it is talking to that IP address and that port number. Therefore, when it needs to open up the data connection back, due to the
"get" or "ls", it attempts to open a TCP connection from port 20 to a random port that the server decides. While on the outside IP it thinks it is talking to, the router hears traffic directed at its outside IP, but does not have any PAT mapping for that random port number that the server picked. Therefore, it does not know that this traffic is supposed to go back to the client.

The port 20 never gets established. The fix is to use "passive FTP" mode. Passive FTP has the client open both port 21 and port 20 connections from the start. The router knows about both of them rather than just port 21, and allows the server to open port 20.

Refer to Analysis of the File Transfer Protocol (FTP) for more information on FTP.

You need extended translations for port 20 and 21 with static mappings (example address)

```
ip nat inside source static tcp 192.168.0.4 20 66.46.64.82 20 extendable
```

```
ip nat inside source static tcp 192.168.0.4 21 66.46.64.82 21 extendable
```

The way that active FTP works does not allow for the use of dynamic NAT. Only static NAT can be used in this case. This is a limitation of FTP.

Q. Does NAT support the use of nonstandard FTP port numbers?
A. Yes. To support the use of non-standard FTP port numbers, you must use the ip nat service command. The following is sample syntax:

```
router-6(config)#ip nat service list 10 ftp tcp port 2021
```


Q. What is Service Provider PAT Port Allocation Enhancement for RTP and RTCP?
A. The Service Provider PAT Port Allocation Enhancement for RTP and RTCP feature ensures that for SIP, H.323, and Skinny voice calls using Cisco IOS Session Border Controller, the port numbers used for RTP streams are even port numbers and the RTCP streams are the next subsequent odd port number. Cisco IOS Session Border Controller gives the administrator the control to ensure that PAT-enabled voice calls will be guaranteed to get the port number translated to a number within the range specified by the RFC, thereby conforming to RFC-1889. A call with a port number within the range will result in a PAT translation to another port number within this range. Likewise, a PAT translation for a port number outside this range will not result in a translation to a number within the given range.


Q. What is Session Initiation Protocol (SIP)?
A. Session Initiation Protocol (SIP) is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints. SIP is an alternative protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. The Cisco SIP implementation enables supported Cisco platforms to signal the setup of voice and multimedia calls over IP networks. For more information, visit http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_chapter09186a008075196f.html.

Q. What is Hosted NAT Traversal support for Session Border Controller?
A. The Cisco IOS Hosted NAT Traversal for Session Border Controller feature enables a Cisco IOS NAT SIP Application-Level Gateway (ALG) router to act as a Session Border Controller
Q. Does Cisco IOS NAT support ACLs that permit any or all packets?
A. When you configure Cisco IOS NAT for dynamic NAT translation, an ACL is used to identify packets that can be translated. The current NAT architecture does not support the use of any or all packets in the ACLs used by NAT. If any or all packets are used, then unexpected behavior can occur.

Q. Does Cisco IOS NAT support ACLs with a “log” keyword?
A. When you configure Cisco IOS NAT for dynamic NAT translation, an ACL is used to identify packets that can be translated. The current NAT architecture does not support ACLs with “log” keyword.

NetPro Discussion Forums—Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

<table>
<thead>
<tr>
<th>NetPro Discussion Forums—Featured Conversations for RP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Providers: MPLS</strong></td>
</tr>
<tr>
<td>• L2VPN/Ethernet over the Internet—May 17, 2007</td>
</tr>
<tr>
<td>• MPLS questions about tunnels—May 16, 2007</td>
</tr>
<tr>
<td>• Xconnect problem—May 16, 2007</td>
</tr>
<tr>
<td>• Tag-switching on Cisco Catalyst 6500 interface VLAN—May 16, 2007</td>
</tr>
<tr>
<td>• RSVP configuration—May 16, 2007</td>
</tr>
<tr>
<td><strong>VPNs: Services</strong></td>
</tr>
<tr>
<td>• Cisco IOS &lt;-&gt; 3000 backup VPN not working—May 17, 2007</td>
</tr>
<tr>
<td>• QoS on VPN (created on Ethernet subinterface)—May 17, 2007</td>
</tr>
<tr>
<td>• VPN question—May 17, 2007</td>
</tr>
<tr>
<td>• Cannot download from intranet sites—May 16, 2007</td>
</tr>
<tr>
<td>• Cisco qdm 2.1—May 10, 2007</td>
</tr>
<tr>
<td><strong>VPNs: Security</strong></td>
</tr>
<tr>
<td>• Flexibility of ASA VPN auth and split tunnel—May 17, 2007</td>
</tr>
<tr>
<td>• Cisco PIX 515e line protocol down on 4FE interfaces—May 17, 2007</td>
</tr>
<tr>
<td>• DMVPN—RIPv2—May 17, 2007</td>
</tr>
<tr>
<td>• When using VPN and unable to get to the Internet—May 17, 2007</td>
</tr>
<tr>
<td>• Forwarding DHCP requests over 802.1q trunk on Cisco ASA 5505—May 17, 2007</td>
</tr>
</tbody>
</table>

Related Information

- NAT Technology Support Pages
- Cisco Technical Support and Documentation