

NAT Order of Operation

Document ID: 6209

- Introduction
- Prerequisites
 - Requirements
 - Components Used
 - Conventions
- NAT Overview
- NAT Configuration and Output
- Related Information

Introduction

This document illustrates that the order in which transactions are processed using Network Address Translation (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.

Prerequisites

Requirements

Readers of this document should have knowledge of the following topic:

- Network Address Translation (NAT). For more information on NAT, see How NAT Works.

Components Used

This document is not restricted to specific software and hardware versions.

Note: The information in this document is based on the Software Version, Cisco IOS® Software Release 12.2(27)

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

NAT Overview

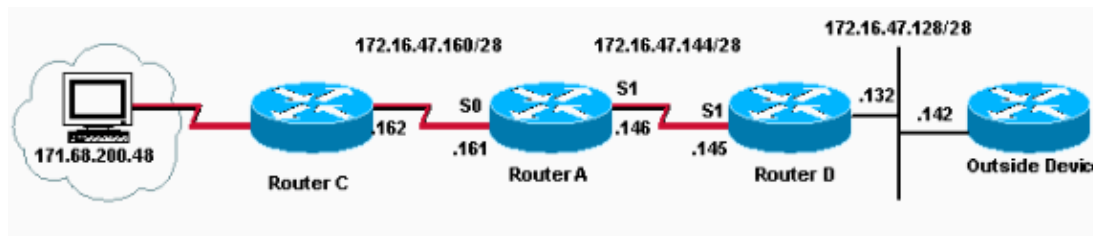
In the table below, when NAT performs the global to local, or local to global, translation is different in each flow.

Inside-to-Outside	Outside-to-Inside
<ul style="list-style-type: none">• If IPSec then check input access list• decryption – for CET (Cisco Encryption)	<ul style="list-style-type: none">• If IPSec then check input access list• decryption – for CET or IPSec

<ul style="list-style-type: none"> Technology) or IPSec • check input access list • check input rate limits • input accounting • policy routing • routing • redirect to web cache • NAT inside to outside (local to global translation) • crypto (check map and mark for encryption) • check output access list • inspect (Context-based Access Control (CBAC)) • TCP intercept • encryption • Queueing 	<ul style="list-style-type: none"> • check input access list • check input rate limits • input accounting • NAT outside to inside (global to local translation) • policy routing • routing • redirect to web cache • crypto (check map and mark for encryption) • check output access list • inspect CBAC • TCP intercept • encryption • Queueing
--	---

NAT Configuration and Output

The following example demonstrates how the order of operations can effect NAT. In this case, only NAT and routing are shown.



In the above example, Router-A is configured to translate the inside local address 171.68.200.48 to 172.16.47.150, as shown in the configuration below.

```

!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
enable password ww
!
ip nat inside source static 171.68.200.48 172.16.47.150

!--- This command creates a static NAT translation
!--- between 171.68.200.48 and 172.16.47.150

ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Ethernet0
no ip address
shutdown

```

```

!
interface Serial0
 ip address 172.16.47.161 255.255.255.240
 ip nat inside

!--- Configures Serial0 as the NAT inside interface

no ip mroute-cache
no ip route-cache
no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside

!--- Configures Serial1 as the NAT outside interface

no ip mroute-cache
no ip route-cache
!
no ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145

!--- Configures a default route to 172.16.47.145

ip route 171.68.200.0 255.255.255.0 172.16.47.162
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password ww
 login
!
end

```

The translation table indicates that the intended translation exists.

```

Router-A#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.47.150      171.68.200.48    ---                ---

```

The following output is taken from Router-A with **debug ip packet detail** and **debug ip nat** enabled, and a ping issued from device 171.68.200.48 destined for 172.16.47.142.

Note: Debug commands generate a significant amount of output. Use them only when traffic on the IP network is low, so other activity on the system is not adversely affected. Before issuing **debug** commands, please see Important Information on Debug Commands.

```

IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
 ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
 ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
 ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
 ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
 ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
 ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable

```

```
ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
ICMP type=3, code=1
```

Since there are no NAT debug messages in the output above, you know that the existing static translation is not being used and that the router does not have a route for the destination address (172.16.47.142) in its routing table. The result of the non-routable packet is an ICMP Unreachable message, which is sent to the inside device.

However, Router-A has a default route of 172.16.47.145, so why is the route considered non-routable?

Router-A has **no ip classless** configured, which means if a packet destined for a "major" network address (in this case, 172.16.0.0) for which subnets exist in the routing table, the router does not rely on the default route. In other words, issuing the **no ip classless** command turns off the router's ability to look for the route with the longest bit match. To change this behavior, you have to configure **ip classless** on Router-A. The **ip classless** command is enabled by default on Cisco routers with IOS Version 11.3 and above.

```
Router-A#configure terminal
Enter configuration commands, one per line. End with CTRL/Z.
Router-A(config)#ip classless
Router-A(config)#end

Router-A#show ip nat translation
%SYS-5-CONFIG_I: Configured from console by console nat tr
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.47.150      171.68.200.48      ---                ---
```

Repeating the same ping test as before, we see that the packet gets translated and the ping is successful.

Ping Response on device 171.68.200.48

```
D:\>ping 172.16.47.142
Pinging 172.16.47.142 with 32 bytes of data:
```

```
Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
```

```
Ping statistics for 172.16.47.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Debug messages on Router A indicating that the packets generated by device 171.68.200.48 are getting translated by NAT.

```
Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=171.68.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [161]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [161]
```

```
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [162]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [163]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [164]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
```

```
Router-A#undebug all
```

```
All possible debugging has been turned off
```

The above example shows that when a packet is traversing inside to outside, a NAT router checks its routing table for a route to the outside address before it continues to translate the packet. Therefore, it is important that the NAT router has a valid route for the outside network. The route to the destination network must be known through an interface that is defined as NAT outside in the router configuration.

It is important to note that the return packets are translated before they are routed. Therefore, the NAT router must also have a valid route for the Inside local address in its routing table.

Related Information

- [Configuring Network Address Translation: Getting Started](#)
- [Verifying NAT Operation and Basic NAT Troubleshooting](#)
- [NAT: Local and Global Definitions](#)
- [How Does Multicast NAT Work on Cisco Routers?](#)
- [NAT Support Page](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 30, 2008

Document ID: 6209
