Avoiding Routing Loops When Using Dynamic NAT

Document ID: 13775

Contents

Introduction

This document describes a scenario in which packets loop between the NAT router and the neighboring router on the outside interface when using dynamic Network Address Translation (NAT) due to traffic destined for an unused ip address in a NAT pool and the presence of a default route on the NAT router routing these packets back to the outside.

Prerequisites

Requirements

There are no specific requirements for this document.

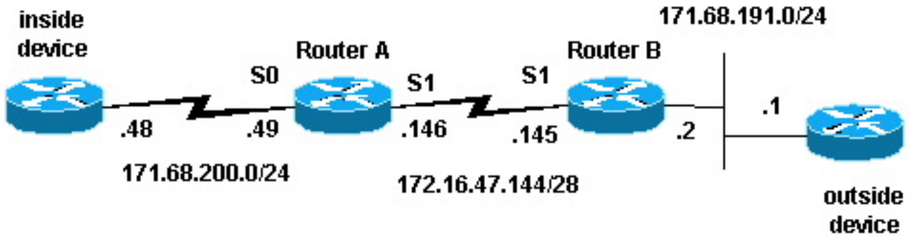
Components Used

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

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Network Diagram

The following topology was used to create the example scenario.



Conventions

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

Example Scenario

In the above topology, Router−A is configured with NAT so that it translates packets sourced from network 171.68.200.0/24 to a range of addresses defined by the NAT pool "test−loop". Router−A's configuration is as follows (all other routers are configured with static routes in order to obtain connectivity):

```
hostname Router−A
!
!
ip nat pool test−loop 172.16.47.161 172.16.47.165 prefix−length 28
ip nat inside source list 7 pool test−loop
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 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
 no ip mroute−cache
 no ip route−cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access−list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec−timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Using NAT translation debugging and IP packet debugging commands, we generated a ping from the router on the inside device. The ping worked, and a translation table entry was generated. In the output below, we see that IP packet debugging and IP NAT debugging are on, and that there are no entries in the translation table at this time.

Note: The **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.

```
Router−A# show debug
Generic IP:
  IP packet debugging is on (detailed)
  IP NAT debugging is on
```

```
Router−A# show ip nat translations
Router−A#
```

The inside router (inside device) originates an ICMP packet with a source address of 171.68.200.48 and a destination address of 171.68.191.1 (the address of the outside device). The following **debug** output shows an IP packet with a source IP address of 171.68.200.48 being translated to 172.16.47.161. The packet comes in the Serial0 interface and is destined out the Serial1 interface.

```
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [401]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

The following **debug** output shows the return IP packet with a destination IP address of 172.16.47.161 being translated back to 171.68.200.48. The packet comes in the Serial1 interface and is destined out the serial0 interface.

```
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [401]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

The **debug** output shows the successful ping exchange between the inside device and outside device:

```
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [402]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [402]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [403]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [403]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [404]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [404]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [405]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [405]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

Using the **show ip nat translations** command, we see an entry in the translation table for the inside device.

```
Router−A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.161      171.68.200.48      ---                ---
```

Now that a translation for the inside device exists in the translation table, we can successfully ping from the outside device to the inside device's global address, as shown in the debug output generated by Router−A below.

Note: The packet originated by the outside device has a source address of 171.68.191.1 and a destination address of 172.16.47.161 (the inside global address in the translation table).

```
Router−A#
```

```
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [108]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [108]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [109]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [109]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [110]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [110]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [111]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [111]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161−>171.68.200.48 [112]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48−>172.16.47.161, d=171.68.191.1 [112]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
```

The following debug output demonstrates what can happen when an outside device tries to initiate communication with a destination address that's an unused IP address in the test−loop pool. The **clear ip nat translation** command was used to clear the translation table and a ping was sent to an unused IP address within the test−loop pool.

The outside device sends an ICMP packet destined for the inside global address of 172.16.47.161. However, the output interface is the same as the input interface for this packet.

```
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
```

```
        ICMP type=8, code=0
```

NAT translates packets going from outside to inside before routing the packet. In this case, there is no entry in the translation table, so Router−A can only route the packet. Router−A relies on its default route to route the packets, sending the packets back out the Serial1 interface, which causes a loop that could eventually bring the serial line down.

To avoid this kind of routing loop, never originate packets from the outside devices to the inside global addresses. However, since this is difficult to enforce, you can add a static route for the inside global addresses with a next hop of null0 in Router−A. This way, when an outside device sends packets destined for an inside global address, and there is no entry in the translation table, Router−A routes the packet to null0, avoiding the loop. Using the example above, the static route looks like the following:

```
    ip route 172.16.47.160 255.255.255.252 null0.
```

Related Information

- **NAT Support Page**
- **IP Routed Protocols Support Page**
- **IP Routing Support Page**
- **Technical Support − Cisco Systems**

Updated: Aug 10, 2005 Document ID: 13775