

Verifying NAT Operation and Basic NAT Troubleshooting

Document ID: 8605

This document contains Flash animation.

Interactive: This document offers customized analysis of your Cisco device.

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

How to Rule Out NAT

Flash Animation Case Study: Can Ping Host, but Cannot Telnet

Flash Animation Case Study: Cannot Ping Beyond NAT

Sample Problem: Can Ping One Router But Not Another

Problem Summary

Sample Problem: Outside Network Devices Cannot Communicate with Inside Routers

Problem Summary

Troubleshooting Checklists

- Translation Not Installed in the Translation Table
- Correct Translation Entry Isn't Being Used
- NAT Operating Correctly, But There Are still Connectivity Problems
- NAT Translation for Port 80 Does not Work
- %NAT: System busy. Try later
- Large Translation Table Increases the CPU
- % Public ip-address already mapped (Internal ip-address -> Public ip-address)
- No Entries in the ARP table

Conclusion

Bad token 0, wanted TOK_NUMBER|TOK_PUNCT

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

When you have IP connectivity problems in a NAT environment, it is often difficult to determine the cause of the problem. Many times NAT is mistakenly blamed, when in reality there is an underlying problem. This document demonstrates how to verify NAT operation using tools available on Cisco routers. This document also shows you how to perform basic NAT troubleshooting, and how to avoid common mistakes when troubleshooting NAT.

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 in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

How to Rule Out NAT

When you attempt to determine the cause of an IP connectivity problem, it helps to rule out NAT. Follow these steps to verify that NAT is operating as expected:

1. Based on the configuration, clearly define what NAT is supposed to achieve. At this point you may determine that there is a problem with the configuration. For help with configuring NAT refer to [Configuring Network Address Translation: Getting Started](#).
2. Verify that correct translations exist in the translation table.
3. Use the **show** and **debug** commands to verify that the translation is occurring.
4. Review in detail what is happening to the packet and verify that routers have the correct routing information to move the packet along.

Below are some sample problems in which we use the above steps to help determine the cause of the problem.

Flash Animation Case Study: Can Ping Host, but Cannot Telnet

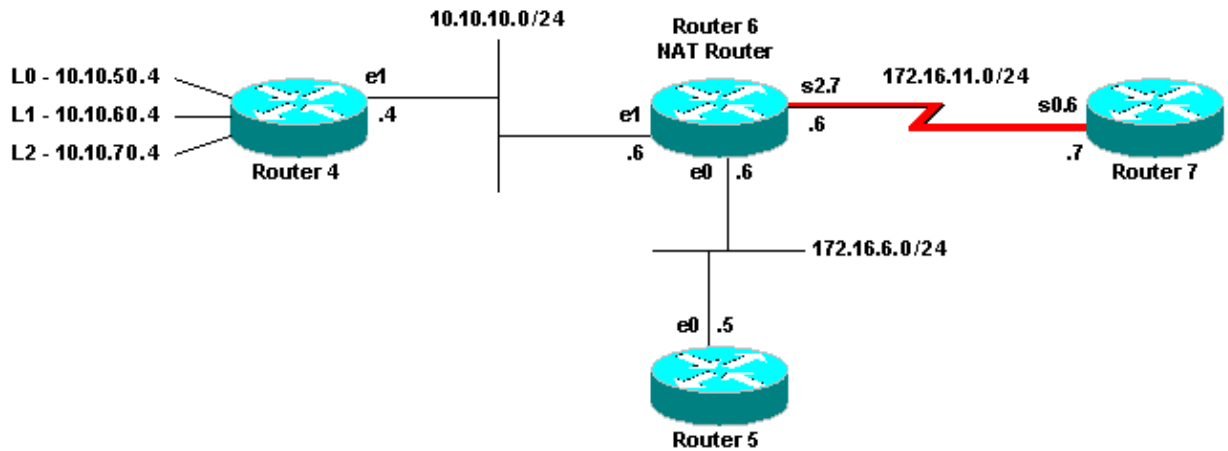
Click here [🔗](#) to watch a 7-minute Flash animation on why a device can ping the host, but cannot telnet.

Flash Animation Case Study: Cannot Ping Beyond NAT

Click here [🔗](#) to watch a 10-minute Flash animation on why a device cannot ping beyond NAT.

Sample Problem: Can Ping One Router But Not Another

In this network diagram, Router 4 can ping Router 5 (172.16.6.5), but not Router 7 (172.16.11.7):



There are no routing protocols running in any of the routers, and Router 4 has Router 6 as its default gateway. Router 6 is configured with NAT in this manner:

```

Router 6
interface Ethernet0
 ip address 172.16.6.6 255.255.255.0
 ip directed-broadcast
 ip nat outside
 media-type 10BaseT
 !
interface Ethernet1
 ip address 10.10.10.6 255.255.255.0
 ip nat inside
 media-type 10BaseT
 !
interface Serial2.7 point-to-point
 ip address 172.16.11.6 255.255.255.0
 ip nat outside
 frame-relay interface-dlci 101
 !
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
 !
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4

```

First, determine that NAT is working correctly. You know from the configuration that the Router 4 IP address (10.10.10.4) is supposed to be statically translated to 172.16.6.14. You can use the **show ip nat translation** command on Router 6 to verify that the translation does exist in the translation table:

```

router-6# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.6.14        10.10.10.4        ---                ---

```

Now, ensure this translation is taking place when Router 4 sources IP traffic. You can do this in two ways from Router 6: by running NAT **debug** or by monitoring NAT statistics with the **show ip nat statistics** command. Because **debug** commands should always be used as a last resort, start with the **show** command.

The intention here is to monitor the hits counter to see if it is increasing as we send traffic from Router 4. The hits counter increments every time a translation in the translation table is used to translate an address. First,

clear the statistics, then display the statistics, try to ping Router 7 from Router 4, and then display the statistics again.

```
router-6# clear ip nat statistics
router-6#
router-6# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Ethernet0, Serial2.7
Inside interfaces:
Ethernet1
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 7 pool test refcount 0
pool test: netmask 255.255.255.0
start 172.16.11.70 end 172.16.11.71
type generic, total addresses 2, allocated 0 (0%), misses 0
router-6#
```

After you use the **ping 172.16.11.7** command on Router 4, the NAT statistics on Router 6 show as:

```
router-6# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Ethernet0, Serial2.7
Inside interfaces:
Ethernet1
Hits: 5 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 7 pool test refcount 0
pool test: netmask 255.255.255.0
start 172.16.11.70 end 172.16.11.71
type generic, total addresses 2, allocated 0 (0%), misses 0
```

You can see from the **show** commands that the number of hits incremented by five. In a successful **ping** from a Cisco router, the number of hits should increase by ten. The five Internet Control Message Protocol (ICMP) echoes sent by the source router (Router 4) should be translated, and the five echo reply packets from the destination router (Router 7) should also be translated, for a total of ten hits. The five missing hits are most likely due to the echo replies not getting translated or not being sent from Router 7.

See if you can find any reason Router 7 would not send echo reply packets to Router 4. First review what NAT is doing to the packet. Router 4 is sending ICMP echo packets with a source address of 10.10.10.4 and a destination address of 172.16.11.7. After NAT takes place the packet received by Router 7 has a source address of 172.16.6.14 and a destination address of 172.16.11.7. Router 7 needs to reply to 172.16.6.14, and since 172.16.6.14 is not directly connected to Router 7, it needs a route for this network in order to respond. Check Router 7's routing table to verify the route exists.

```
router-7# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```

172.16.0.0/24 is subnetted, 4 subnets
C       172.16.12.0 is directly connected, Serial0.8
C       172.16.9.0 is directly connected, Serial0.5
C       172.16.11.0 is directly connected, Serial0.6
C       172.16.5.0 is directly connected, Ethernet0

```

You can see that the Router 7 routing table does not have a route for 172.16.6.14. Once you add this route, ping works fine.

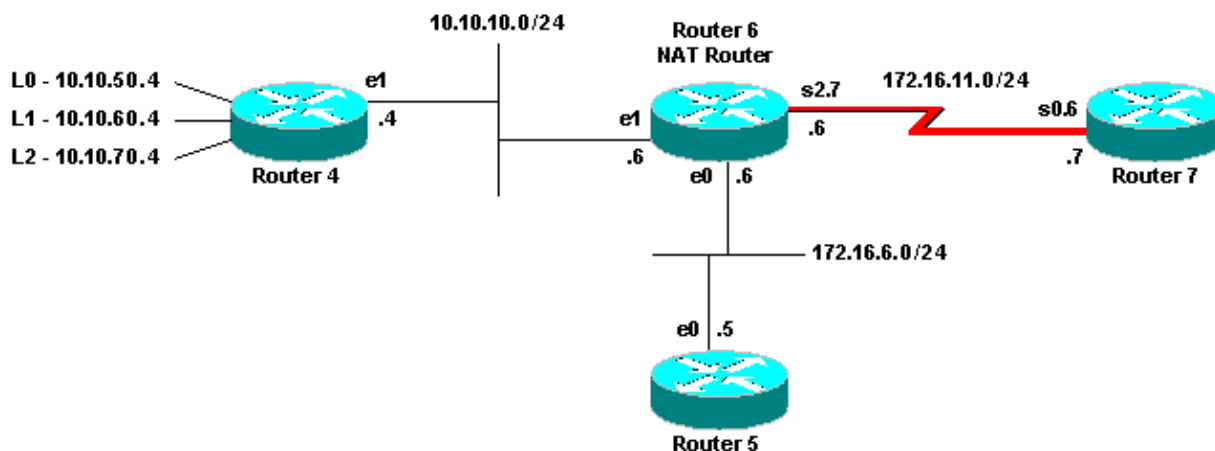
Problem Summary

You first defined what NAT was supposed to accomplish. Next, you verified that the static NAT entry existed in the translation table and that it was accurate. You verified that translation truly was taking place by monitoring the NAT statistics. There you found a problem which led you to check the routing information on Router 7, where you found that Router 7 needed a route to the inside global address of Router 4.

Note that in this simple lab environment, it is useful to monitor NAT statistics with the **show ip nat statistics** command. However, in a more complex NAT environment with several translations taking place, this **show** command is no longer useful. In this case it may be necessary to run **debugs** on the router. The next problem scenario demonstrates the use of **debug** commands.

Sample Problem: Outside Network Devices Cannot Communicate with Inside Routers

In this scenario, Router 4 can **ping** both Router 5 and Router 7, but devices on the 10.10.50.0 network cannot communicate with Router 5 or Router 7 (in the test lab we emulate this by sourcing **pings** from the loopback interface with the IP address 10.10.50.4). Look at the network diagram:



Router 6
<pre> interface Ethernet0 ip address 172.16.6.6 255.255.255.0 ip directed-broadcast ip nat outside media-type 10BaseT ! interface Ethernet1 ip address 10.10.10.6 255.255.255.0 ip nat inside media-type 10BaseT </pre>

```

!
interface Serial2.7 point-to-point
 ip address 172.16.11.6 255.255.255.0
 ip nat outside
 frame-relay interface-dlci 101
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24
ip nat inside source list 7 pool test
ip nat inside source static 10.10.10.4 172.16.6.14
!
access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4
access-list 7 permit 10.10.70.4

```

First, clearly state the expected behavior of NAT. From the configuration of Router 6, you know that NAT is supposed to dynamically translate 10.10.50.4 to the first available address in the NAT pool "test". The pool consists of addresses 172.16.11.70 and 172.16.11.71. From what you learned in the problem above, you can deduce that the packets that Routers 5 and 7 receive either have a source address of 172.16.11.70 or 172.16.11.71. These addresses are on the same subnet as Router 7, so Router 7 should have a directly connected route, however Router 5 needs a route to the subnet if it does not have one already.

You can use the **show ip route** command to see that the Router 5 routing table does list 172.16.11.0:

```

router-5# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 4 subnets
C 172.16.9.0 is directly connected, Serial1
S 172.16.11.0 [1/0] via 172.16.6.6
C 172.16.6.0 is directly connected, Ethernet0
C 172.16.2.0 is directly connected, Serial0

```

You can use the **show ip route** command to see that the Router 7 routing table lists 172.16.11.0 as a directly connected subnet:

```

router-7# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets
C 172.16.12.0 is directly connected, Serial0.8
C 172.16.9.0 is directly connected, Serial0.5
C 172.16.11.0 is directly connected, Serial0.6
C 172.16.5.0 is directly connected, Ethernet0
S 172.16.6.0 [1/0] via 172.16.11.6

```

Now that you have clearly stated what NAT is supposed to do, you need to verify that it is operating correctly. Start by checking the NAT translation table and verifying that the expected translation exists. Since the translation you are interested in is created dynamically, you must first send IP traffic sourced from the appropriate address. After a sent **ping**, sourced from 10.10.50.4 and destined to 172.16.11.7, the translation table in Router 6 shows this:

```
router-6# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
--- 172.16.6.14         10.10.10.4        ---                ---
--- 172.16.11.70       10.10.50.4        ---                ---
```

Since the expected translation is in the translation table, you know that the ICMP echo packets are getting translated appropriately, but what about the echo reply packets? As mentioned above, you could monitor the NAT statistics, but this is not very useful in a complex environment. Another option is to run NAT debugging on the NAT router (Router 6). In this case, you should turn on **debug ip nat** on Router 6 while you send a **ping** sourced from 10.10.50.4 destined to 172.16.11.7. The **debug** results are below.

Note: When you use any **debug** command on a router, you could overload the router which causes it to become inoperable. Always use extreme caution, and if possible never run a **debug** on a critical production router without the supervision of a Cisco Technical Support engineer.

```
router-6# show log
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 39 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 39 messages logged
  Trap logging: level informational, 33 message lines logged

Log Buffer (4096 bytes):

05:32:23: NAT: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [70]
05:32:23: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [70]
05:32:25: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [71]
05:32:25: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [71]
05:32:27: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [72]
05:32:27: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [72]
05:32:29: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [73]
05:32:29: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [73]
05:32:31: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [74]
05:32:31: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [74]
```

As you can see from the above **debug** output, the first line shows the source address of 10.10.50.4 being translated to 172.16.11.70. The second line shows the destination address of 172.16.11.70 being translated back to 10.10.50.4. This pattern repeats throughout the rest of the **debug**. This tells you that Router 6 is translating the packets in both directions.

Now review in more detail exactly what should be happening. Router 4 sends a packet sourced from 10.10.50.4 destined for 172.16.11.7. Router 6 performs NAT on the packet and forwards a packet with a source of 172.16.11.70 and a destination of 172.16.11.7. Router 7 sends a response with a source of 172.16.11.7 and a destination of 172.16.11.70. Router 6 performs NAT on the packet, which results in a packet with source address 172.16.11.7 and destination address 10.10.50.4. At this point Router 6 should route the packet to 10.10.50.4 based on information it has in its routing table. You need to use the **show ip route** command to confirm that Router 6 has the necessary route in its routing table.

```
router-6# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/24 is subnetted, 5 subnets
C 172.16.8.0 is directly connected, Serial1
C 172.16.10.0 is directly connected, Serial2.8
C 172.16.11.0 is directly connected, Serial2.7
C 172.16.6.0 is directly connected, Ethernet0
C 172.16.7.0 is directly connected, Serial0
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Ethernet1
```

Problem Summary

First you clearly defined what NAT was supposed to accomplish. Second, you verified that the necessary translations existed in the translation table. Third, you used the **debug** or **show** commands to verify that the translation was actually taking place. Finally, you reviewed in more detail what was happening to the packet and what the routers need in order to forward or respond to the packet.

Troubleshooting Checklists

Now that you have a basic procedure for finding the cause of connectivity problems, here are some checklists for troubleshooting common issues.

Translation Not Installed in the Translation Table

If you find that the appropriate translation does not get installed in the translation table, verify that:

- The configuration is correct. Getting NAT to accomplish what you want can sometimes be tricky. For some configuration help, refer to *Configuring Network Address Translation: Getting Started*.
- There are not any inbound access lists that deny the packets from entering the NAT router.
- The NAT router has the appropriate route in the routing table if the packet is going from inside to outside. Refer to *NAT Order of Operation* for more information.
- The access list referenced by the NAT command permits all necessary networks.
- There are enough addresses in the NAT pool. This should only be a problem if NAT is not configured for overloading.
- That the router interfaces are appropriately defined as NAT inside or NAT outside.
- In the case of translating the payload of Domain Name System (DNS) packets, make sure that translation takes place on the address in the IP header of the packet. If this does not happen, then NAT does not look into the payload of the packet.

Correct Translation Entry Isn't Being Used

If the correct translation entry is installed in the translation table, but is not used, check these:

- Verify there are not any inbound access lists that deny the packets from entering the NAT router.
- For packets going from inside to outside, verify there is a route to the destination as this is checked before translation. Refer to *NAT Order of Operation* for more information.

NAT Operating Correctly, But There Are still Connectivity Problems

If NAT is operating correctly, begin troubleshooting the connectivity problem as follows:

- Verify layer 2 connectivity.
- Verify layer 3 routing information.
- Search for packet filters that could be causing the problem.

NAT Translation for Port 80 Does not Work

NAT translation for port 80 does not work, but the translation for other ports works normally.

In order to resolve this issue, complete these steps:

1. Run the **debug ip nat translations** and **debug ip packet** commands in order to see if the translations are correct and the correct translation entry is installed in the translation table.
2. Verify that the server responds.
3. Disable the HTTP server.
4. Clear the NAT and ARP tables.

%NAT: System busy. Try later

The `%NAT: System busy. Try later` error message appears when a **show** command related to NAT or a **show running-config** or **write memory** command is executed. This issue is due to the increase in the size of the NAT table. When the size of the NAT table increases, the router runs out of memory.

Reload the router in order to solve this issue. If the error message appears when HSRP SNAT is configured, configure these commands in order to resolve the issue:

```
Router(config)#standby delay minimum 20 reload 20
Router(config)#standby 2 preempt delay minimum 20 reload 20 sync 10
```

Large Translation Table Increases the CPU

A host can send hundreds of translations, which in turn leads to high CPU usage. In other words, it can make the table so large that it causes the CPU to run at 100 percent. The **ip nat translation max-entries 300** command makes the 300 per host limit or an aggregate limit of the amount of translations on the router. The workaround is to use the **ip nat translation max-entries all-hosts 300** command.

% Public ip-address already mapped (Internal ip-address -> Public ip-address)

This message appears when you try to configure two internal IP addresses to one public IP address listening on the same ports.

```
% X.X.X.X already mapped (172.30.62.101 -> X.X.X.X)
```

In order to NAT the public IP address to two internal IP addresses, use two public IP addresses in the DNS.

No Entries in the ARP table

This is a result of the *no-alias* option that is used on the NAT entries. The *no-alias* option means that the router does not respond for the addresses and does not install an ARP entry. If another router uses a NAT pool

as an inside global pool that consists of addresses on an attached subnet, an alias is generated for that address so that the router can answer Address Resolution Protocol (ARP) requests for those addresses. This causes the router to have ARP entries for the fake addresses.

Conclusion

The problems above demonstrated that NAT is not always the cause of IP connectivity issues. In many cases, the cause is something other than NAT and requires further investigation. This document explains basic steps to take when troubleshooting and verifying NAT operation. These steps include:

- Clearly define what NAT is supposed to achieve.
- Verify correct translations exist in the translation table.
- Use the **show** and **debug** commands to verify the translation is occurring.
- Review in detail what is happening to the packet and verify that routers have the correct routing information to move the packet along.

Bad token 0, wanted TOK_NUMBER|TOK_PUNCT

This error message is just an informational message and does not have any impact on the normal behavior of the device.

```
Bad token 0, wanted TOK_NUMBER|TOK_PUNCT
```

The error means that NAT attempts to do a layer 4 fix on the address in an FTP open, and can not find the IP addresses it needs to translate in the packet.

The reason why the message includes tokens is that IP addresses in the packet are found by looking for a token, or a set of symbols, in the IP packet, in order to find the details needed to translate.

When an FTP session is initiated, it negotiates two channels, a command channel and a data channel. These are both IP addresses with different port numbers. The FTP client and server negotiate a second data channel to transfer files. The packet exchanged through control channel has the format "PORT,i,i,i,i,p,p", where i,i,i,i are the four bytes of an IP address and p,p specify the port. NAT tries to match this pattern and translate address/port if necessary. NAT must translate both channels' addressing schemes. NAT scans for numbers in the command stream until it thinks it has found a port command that requires translation. It tries to parse out the translation, which it calculates with the pattern as described earlier.

If the packet is corrupt or the FTP server or client has malforming commands, NAT cannot properly calculate the translation and it generates that error. A suggestion is to set the FTP client to "passive" so that it initiates both channels. This sometimes helps with FTP through NAT.

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.

NetPro Discussion Forums – Featured Conversations for RP
Service Providers: MPLS
Virtual Private Networks: Services
Virtual Private Networks: Security

Related Information

- [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 25, 2008

Document ID: 8605
