

NAT の基本的な動作の確認とトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[問題](#)

[1つのルータに ping を実行するが、別のルータには ping を実行しない](#)

[トラブルシューティング](#)

[外部のネットワーク デバイスが内部のルータと通信できない](#)

[トラブルシューティング](#)

[一般的な問題のチェックリスト](#)

[変換テーブルに変換がインストールされていない](#)

[正しい変換エントリが使用されていない](#)

[NAT は正しく動作しているが、まだ接続の問題がある](#)

[ポート 80 の NAT 変換が機能しない](#)

[%NAT システムがビジー状態である - 後でやり直す](#)

[変換テーブルが大きいため CPU 使用率が高い](#)

[% のパブリック Ip-address はすでにマッピングがされている \(内部 Ip-address からパブリック Ip-address へ \)](#)

[ARP テーブルにエントリがない](#)

[不正なトークン 0 が TOK NUMBER|TOK PUNCT を要求した](#)

[関連情報](#)

はじめに

このドキュメントでは、NAT 環境での IP 接続の問題をトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるもの

ではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

問題

このドキュメントでは、次の 2 つの例を確認して、NAT 環境での IP 接続の問題をトラブルシューティングする方法について説明します。

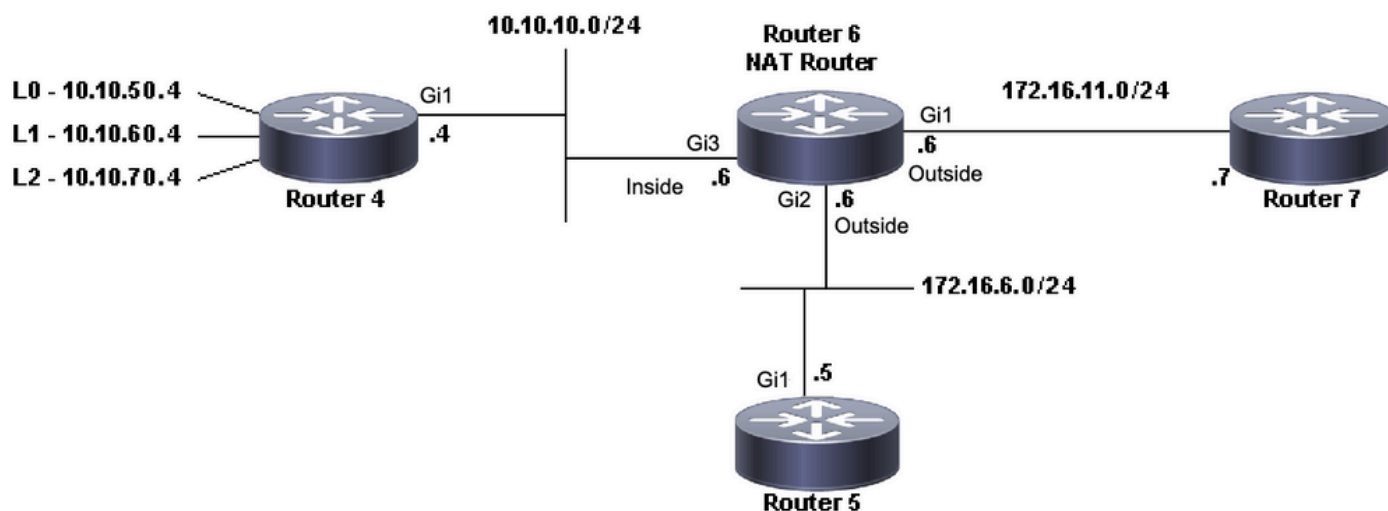
- 1 つのルータに ping を実行するが、別のルータには ping を実行しない
- 外部のネットワーク デバイスが内部のルータと通信できない

次の基本的な手順は、NAT 動作に問題があるかどうかを判断するのに役立ちます。

1. 設定を確認し、NAT による達成が想定されることを明確に定義します。レビューに基づいて、設定に問題があるかどうかを判断できます。NAT の設定については、「[ネットワーク アドレス変換の設定](#)」を参照してください。
2. 正しい変換が変換テーブルに存在することを検証します。
3. show および debug コマンドを使用して、変換が発生していることを検証します。
4. パケットに何が起きているかを詳細にレビューして、パケットを移動するための正しいルーティング情報がルータにあることを検証します。

1 つのルータに ping を実行するが、別のルータには ping を実行しない

この最初のシナリオでは、ルータ 4 はルータ 5 (172.16.6.5) に ping できますが、ルータ 7 (172.16.11.7) には ping できません。



NAT トポロジ

<#root>

Router4#

ping 172.16.6.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms

Router4#

ping 172.16.11.7

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Router4#

このシナリオに関する重要な考慮事項 :

- ルータではダイナミック ルーティング プロトコルが設定されておらず、スタティックルー
トのみが使用されます。
- ルータ 4 のデフォルトゲートウェイはルータ 6 です。
- ルータ 6 は NAT で設定されています。

<#root>

```
interface GigabitEthernet1
```

```
ip address 172.16.11.6 255.255.255.0
```

```
ip nat outside
```

```
negotiation auto
```

```
no mop enabled
```

```

no mop sysid
!
interface GigabitEthernet2
ip address 172.16.6.6 255.255.255.0

ip nat outside

negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet3
ip address 10.10.10.6 255.255.255.0

ip nat inside

negotiation auto
no mop enabled
no mop sysid
!
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source static 10.10.10.4 172.16.11.70
!
ip access-list standard 7
10 permit 10.10.50.4
20 permit 10.10.60.4
30 permit 10.10.70.4

```

トラブルシューティング

1. まず、NAT が正しく機能していることを確認する必要があります。前の設定から、ルータ 4 の IP アドレス 10.10.10.4 が 172.16.6.14 に静的に変換されていることがわかります。ルータ 6 で show ip nat translation コマンドを使用して、変換が変換テーブルに存在することを検証できます。

<#root>

NAT-Router#

show ip nat translations

```

Pro  Inside global      Inside local      Outside local      Outside global
---  172.16.6.14         10.10.10.4       ---                ---
Total number of translations: 1

```

NAT-Router#

2. ルータ 4 が IP トラフィックを送信するときに、この変換が行われるようにします。これは、ルータ 6 から 2 つの方法で実行できます。show ip nat statistics コマンドを使用して、NAT デバッグを実行するか、NAT 統計情報をモニターします。debug コマンドは最後の手段であるため、

show コマンドから始めます。

3. カウンタをモニターして、ルータ 4 からトラフィックを受信するにつれてカウンタが増加することを確認します。カウンタは、変換テーブルを使用してアドレスを変換するたびに増加します。

4. 統計情報をクリアしてから統計情報を表示し、ルータ 4 からルータ 7 に ping を実行してから、統計情報を再度表示します。

```
<#root>
```

```
NAT-Router#
```

```
clear ip nat statistics
```

```
NAT-Router#
```

```
NAT-Router#
```

```
show ip nat statistics
```

```
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
```

```
Outside interfaces:
```

```
  GigabitEthernet1, GigabitEthernet2
```

```
Inside interfaces:
```

```
  GigabitEthernet3
```

```
Hits: 0 Misses: 0
```

```
Expired translations: 0
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 1] access-list 7 pool test refcount 0
```

```
  pool test: id 1, 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
```

```
nat-limit statistics:
```

```
  max entry: max allowed 0, used 0, missed 0
```

```
In-to-out drops: 0 Out-to-in drops: 0
```

```
Pool stats drop: 0 Mapping stats drop: 0
```

```
Port block alloc fail: 0
```

```
IP alias add fail: 0
```

```
Limit entry add fail: 0
```

```
NAT-Router#
```

ルータ 4 で ping 172.16.11.7 コマンドを使用すると、ルータ 6 の NAT 統計情報は次のようになります。

```
<#root>
```

```
Router4#
```

```
ping 172.16.11.7
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

```
Router4#
```

```
NAT-Router#
```

```
show ip nat statistics
```

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
```

```
Outside interfaces:
```

```
GigabitEthernet1, GigabitEthernet2
```

```
Inside interfaces:
```

```
GigabitEthernet3
```

```
Hits: 4
```

```
Misses: 1
```

```
Expired translations: 0
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 1] access-list 7 pool test refcount 0
```

```
pool test: id 1, 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
```

```
nat-limit statistics:
```

```
max entry: max allowed 0, used 0, missed 0
```

```
In-to-out drops: 0 Out-to-in drops: 0
```

```
Pool stats drop: 0 Mapping stats drop: 0
```

```
Port block alloc fail: 0
```

```
IP alias add fail: 0
```

```
Limit entry add fail: 0
```

```
NAT-Router#
```

show コマンドでヒット数が増加したことを確認できます。Cisco ルータからの ping が成功すると、ヒット数が 10 増加します。送信元ルータ (ルータ 4) から送信された Internet Control Message Protocol (ICMP) エコーが変換されます。また、宛先ルータ (ルータ 7) からのエコー応答パッケージも変換される必要があり、ヒット数は合計 10 回になります。5 ヒットの損失があるのは、エコー応答が変換されないか、ルータ 7 から送信されないためです。

次に、ルータ 7 がルータ 4 にエコー応答パッケージを送信しない理由があるかどうかを確認します。この時点で、次の手順が実行されています。

- ルータ 4 は、送信元アドレスが 10.10.10.4、宛先アドレスが 172.16.11.7 の ICMP エコーパッケージを送信します。
- NAT の実行後、ルータ 7 が受信したパッケージの送信元アドレスは 172.16.6.14、宛先アドレスは 172.16.11.7 です。
- ルータ 7 は 172.16.6.14 に応答する必要があり、172.16.6.14 はルータ 7 に直接接続されていないため、応答するにはこのネットワークのルータが必要です。

注：パケットが宛先ルータに到達しているかどうかを確認するもう 1 つの方法は、組み込みパケットキャプチャ (EPC) を使用するか、アクセスリスト (ACL) とともに debug ip icmp/debug ip packet を使用することです。

次に、ルータ 7 のルーティングテーブルを調べて、172.16.6.14 へのルートが存在するかどうかを確認する必要があります。

```
<#root>
```

```
Router7#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, 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, m - OMP  
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR
& - replicated local route overrides by connected

Gateway of last resort is not set

```
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.16.11.0/24 is directly connected, GigabitEthernet1
L      172.16.11.7/32 is directly connected, GigabitEthernet1
Router7#
```

前の出力から、ルータ 7 のルーティングテーブルに 172.16.6.14 サブネットのルートがないことがわかります。これが修正され、ルートが設定に追加されると、ping が機能します。show ip nat statistics コマンドを使用した NAT 統計情報をモニターすることが効果的です。ただし、より複雑な NAT 環境で複数の変換が行われる場合は、この show コマンドは役に立たないため、ルータでデバッグを使用する必要があります。

<#root>

Router7#

configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Router7(config)#ip route 172.16.6.0 255.255.255.0 172.16.11.6
Router7(config)#end
Router7#
```

Router4#

ping 172.16.11.7

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
Router4#
```

NAT-Router#

show ip nat statistics

```
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  GigabitEthernet1, GigabitEthernet2
Inside interfaces:
  GigabitEthernet3

Hits: 9
```

```
Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 7 pool test refcount 0
pool test: id 1, 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
nat-limit statistics:
max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0 Out-to-in drops: 0
Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
NAT-Router#
```

外部のネットワーク デバイスが内部のルータと通信できない

この問題では、ルータ 4 はルータ 5 とルータ 7 の両方を ping できますが、10.10.50.0 のネットワーク上のデバイスはルータ 5 またはルータ 7 と通信できません。

<#root>

Router4#

```
ping 172.16.11.7 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:

Packet sent with a source address of 10.10.50.4

.....

Success rate is 0 percent (0/5)

Router4#

```
ping 172.16.6.5 source 10.10.50.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:

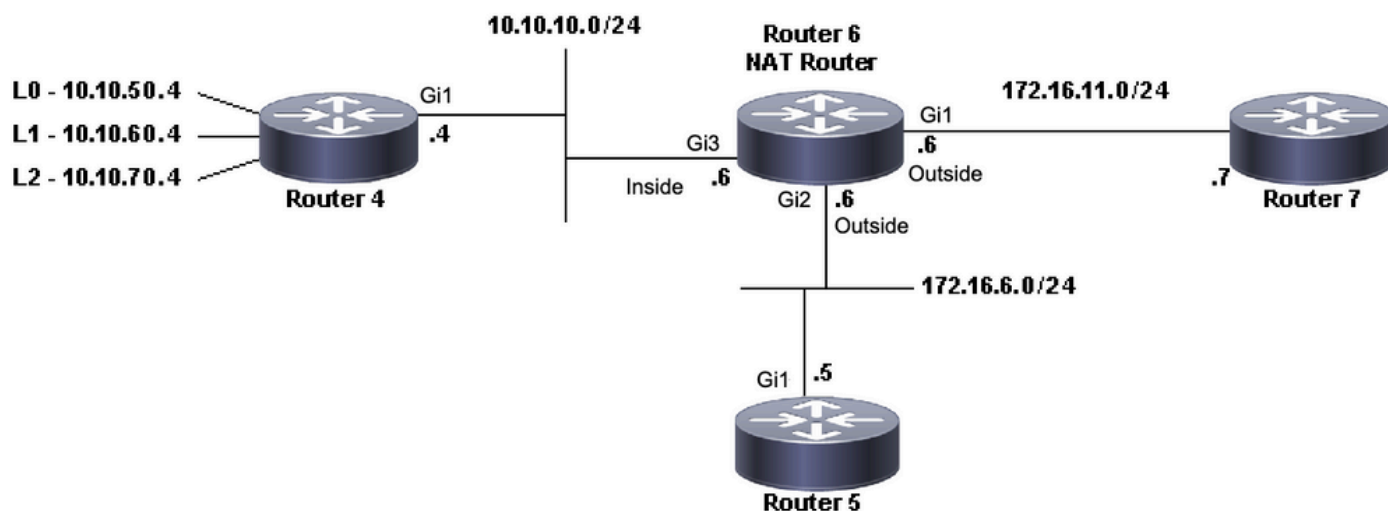
Packet sent with a source address of 10.10.50.4

.....

Success rate is 0 percent (0/5)

Router4#

この問題のネットワーク構成図は同じです。



NAT トポロジ

```

interface GigabitEthernet1
ip address 172.16.11.6 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 172.16.6.6 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet3
ip address 10.10.10.6 255.255.255.0
ip nat inside
negotiation auto
no mop enabled
no mop sysid
!
!
ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24
ip nat inside source static 10.10.10.4 172.16.6.14
ip nat inside source list 7 pool test
!
ip access-list standard 7
10 permit 10.10.50.4
20 permit 10.10.60.4
30 permit 10.10.70.4

```

トラブルシューティング

ルータ 6 の設定から、NAT が NAT プール「テスト」の使用可能な最初のアドレスに、

10.10.50.4 を動的に変換するものと想定されていることがわかります。プールは、172.16.11.70 と 172.16.11.71 のアドレスで構成されています。この問題から、ルータ 5 とルータ 7 が受信するパケットは 172.16.11.70 または 172.16.11.71 の発信元アドレスを持つことがわかります。これらのアドレスはルータ 7 と同じサブネット上にあるため、ルータ 7 にはこのサブネットに直接接続されたルートがあるはずですが、ルータ 5 にサブネットへのルートがまだない場合は必要です。

ルータ 5 のルーティング テーブルに 172.16.11.0 が記載されているを確認するためには、show ip route コマンドを使用できます。

```
<#root>
```

```
Router5#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, 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, m - OMP
        n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        H - NHRP, G - NHRP registered, g - NHRP registration summary
        o - ODR, P - periodic downloaded static route, l - LISP
        a - application route
        + - replicated route, % - next hop override, p - overrides from PfR
        & - replicated local route overrides by connected
```

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

```
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.6.0/24 is directly connected, GigabitEthernet1
L       172.16.6.5/32 is directly connected, GigabitEthernet1
s 172.16.11.0/24 [1/0] via 172.16.6.6
```

ルータ 7 のルーティング テーブルに、直接接続のサブネットとして 172.16.11.0 が記載されているを確認するためには、次のように show ip route コマンドを使用できます。

```
<#root>
```

```
Router7#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, 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, m - OMP
        n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        H - NHRP, G - NHRP registered, g - NHRP registration summary
        o - ODR, P - periodic downloaded static route, l - LISP
```

```
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected
```

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

```
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S 172.16.6.0/24 [1/0] via 172.16.11.6
C 172.16.11.0/24 is directly connected, GigabitEthernet1
L 172.16.11.7/32 is directly connected, GigabitEthernet1
```

NAT 変換テーブルを確認し、予測される変換が存在することを確認します。目的の変換は動的に作成されるため、まず適切なアドレスから IP トラフィックを送信する必要があります。10.10.50.4 から 172.16.11.7 宛ての ping が送信されると、ルータ 6 (NAT ルータ) の変換テーブルに次の出力が表示されます。

```
<#root>
```

```
NAT-Router#
```


```
show ip nat translations
```

```
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
```

```
---
Total number of translations: 2
```

想定される変換が変換テーブルにあるため、ICMP エコーパケットが適切に変換されていることがわかります。1 つの方法は、NAT 統計情報をモニターすることですが、これは複雑な環境では役に立ちません。次のオプションは、NAT ルータ (ルータ 6) 上で NAT のデバッグを実行することです。10.10.50.4 から 172.16.11.7 宛てに ping を送信している間、debug ip nat を実行できます。デバッグの結果を次のコード例に示します。

 注：ルータで debug コマンドを使用すると、ルータが過負荷になり、動作不能になる可能性があります。常に細心の警戒を払い、可能であれば、シスコテクニカルサポートのエンジニアの監督なしに、重要な製品であるルータで debug を絶対に実行しないでください。

```
<#root>
```

```
NAT-Router#
```

```
show logging
```

```
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]
```

Router7#show monitor capture cap buffer brief

```
-----
#  size  timestamp  source      destination  dscp  protocol
-----
0  114    0.000000    172.16.11.70  -> 172.16.11.7  0 BE  ICMP
1  114    2.000000    172.16.11.70  -> 172.16.11.7  0 BE  ICMP
2  114    4.000000    172.16.11.70  -> 172.16.11.7  0 BE  ICMP
3  114    6.001999    172.16.11.70  -> 172.16.11.7  0 BE  ICMP
4  114    8.001999    172.16.11.70  -> 172.16.11.7  0 BE  ICMP
```

上記の debug の出力から確認できるように、最初の行では 10.10.50.4 の発信元アドレスが 172.16.11.70 に変換されていることを示しています。2 番目の行では、宛先アドレス 172.16.11.70 が 10.10.50.4 に変換し戻されていることを示しています。このパターンは残りの debug を通じて繰り返されます。これは、NAT ルータがパケットを双方向に変換することを意味します。また、パケットキャプチャから、ルータ 7 が送信元 172.16.11.70 および宛先 172.16.11.7 の ICMP パケットを実際に受信していることがわかります。

後続の手順は、この問題の現在のステータスを要約しています。

1. ルータ 4 では 10.10.50.4 から発信し、172.16.11.7 (実行したテストによっては 172.16.6.5) を宛先とするパケットが送信されます。
2. NAT ルータは、パケットに対して NAT 変換を実行し、送信元を 172.16.11.70、宛先を 172.16.11.7 として転送します。
3. ルータ 7 は、送信元が 172.16.11.7、宛先が 172.16.11.70 の応答を送信します。
4. NAT ルータ (ルータ 6) はパケットに対して NAT を実行します。その結果、送信元アドレスが 172.16.11.7、宛先アドレスが 10.10.50.4 のパケットが生成されます。
5. NAT ルータ (ルータ 6) は、ルーティングテーブルの情報に基づいてパケットを 10.10.50.4 にルーティングします。

この時点で、show ip route コマンドと show ip cef コマンドを使用して、NAT ルータ (ルータ 6) のルーティングテーブルに必要なルートがあることを確認する必要があります。

```
<#root>
```

```
NAT-Router#
```

```
show ip route
```

```
Codes: L - local, C - connected, S - static, 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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

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

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.10.10.0/24 is directly connected, GigabitEthernet3
L      10.10.10.6/32 is directly connected, GigabitEthernet3
172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C      172.16.6.0/24 is directly connected, GigabitEthernet2
L      172.16.6.6/32 is directly connected, GigabitEthernet2
L      172.16.6.14/32 is directly connected, GigabitEthernet2
C      172.16.11.0/24 is directly connected, GigabitEthernet1
L      172.16.11.6/32 is directly connected, GigabitEthernet1
L      172.16.11.70/32 is directly connected, GigabitEthernet1
```

```
NAT-Router#
```

```
show ip route 10.10.50.4
```

```
% Subnet not in table
```

```
NAT-Router#
```

```
show ip cef 10.10.50.4
```

```
0.0.0.0/0
```

```
no route
```

```
NAT-Router#
```

喪失しているルートを NAT ルータに追加すると、ping は成功します。

```
<#root>
```

```
NAT-Router#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
NAT-Router(config)#
```

```
ip route 10.10.50.4 255.255.255.255 10.10.10.4
```

```
NAT-Router(config)#end  
NAT-Router#
```

```
Router4#
```

```
ping 172.16.11.7 source 10.10.50.4
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 172.16.11.7, timeout is 2 seconds:  
Packet sent with a source address of 10.10.50.4
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

```
Router4#
```

```
ping 172.16.6.5 source 10.10.50.4
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 172.16.6.5, timeout is 2 seconds:  
Packet sent with a source address of 10.10.50.4
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
Router4#
```

一般的な問題のチェックリスト

次のチェックリストを使用して、一般的な問題をトラブルシューティングしてください。

変換テーブルに変換がインストールされていない

適切な変換が変換テーブルにインストールされていない場合は、次のことを確認します。

1. この設定は正しいです。NAT で必要なものを取得するのが難しい場合があります。設定のヘルプについては、「[ネットワークアドレス変換の設定](#)」を参照してください。
2. NAT ルータからのパケットのエントリを拒否するインバウンドアクセスリストがありません。
3. パケットが内部から外部に向かう場合、NAT ルータはルーティングテーブルに適切なルートを持ちます。詳細については、「NAT の処理順序」を参照してください。
4. NAT コマンドによって参照されるアクセス リストは、すべての必要なネットワークを許可する。
5. NAT プールに十分なアドレスがある。これは、NAT が輻輳用に設定されていない場合にのみ問題になる可能性があります。
6. ルータのインターフェイスが NAT 内部または NAT 外部として適切に定義されていること。
7. ドメインネームシステム (DNS) パケットのペイロードの変換では、パケットの IP ヘッダー内のアドレスで変換が行われるようにします。これが発生していなくても、NAT ではパケットのペイロードは調査されません。

正しい変換エントリが使用されていない

正しい変換エントリが変換テーブルにインストールされているが、使用されていない場合は、次のことを確認します。

1. NAT ルータからのパケットのエントリを拒否するインバウンドアクセスリストがないことを確認します。
2. 内部から外部に向かうパケットの場合は、変換前にチェックされるため、宛先へのルートがあることを確認します。詳細については、「NAT の処理順序」を参照してください。

NAT は正しく動作しているが、まだ接続の問題がある

接続の問題をトラブルシューティングするには、次のようにします。

1. レイヤ 2 の接続を検証する。
2. レイヤ 3 のルーティング情報を検証する。
3. 問題の原因となっているパケットフィルタを検索します。

ポート 80 の NAT 変換が機能しない

これは、ポート 80 の NAT 変換は機能しないが、他のポートの変換は正常に機能することを意味します。

この問題を解決する手順は、次のとおりです。

1. `debug ip nat translations` および `debug ip packet` コマンドを実行して、変換が正しいかどうか、および正しい変換エントリが変換テーブルにインストールされているかどうかを確認します。
2. サーバが応答することを検証します。
3. HTTP サーバを無効にする。
4. NAT および ARP テーブルをクリアします。

%NAT システムがビジー状態である - 後でやり直す

NAT に関連する `show` コマンド、または `show running-config` または `write memory` コマンドが実行されると、後でやり直すというエラーメッセージが表示されます。これは、NAT テーブルのサイズが増加したために発生します。NAT テーブルのサイズが増えると、ルータはメモリ不足になります。

1. この問題を解決するには、ルータをリロードします。
2. HSRP SNAT が設定されるとエラーメッセージが表示される場合は、次のコマンドを設定して問題を解決します。
 - `Router(config)#standby delay minimum 20 reload 20`
 - `Router(config)#standby 2 preempt delay minimum 20 reload 20 sync 10`

変換テーブルが大きいため CPU 使用率が高い

ホストは何百もの変換を送信する可能性があるため、CPU 使用率が高くなります。つまり、作成できるテーブルが大きすぎて、CPU が 100 パーセントで実行される原因となります。 `ip nat translation max-entries 300` コマンドは、ホストあたり 300 の制限またはルータ上の変換量の総計

の制限を作成します。回避策は、`ip nat translation max-entries all-hosts 300` コマンドを使用することです。

% のパブリック Ip-address はすでマッピングがされている (内部 Ip-address からパブリック Ip-address へ)

このメッセージは、2つの内部 IP アドレスを、同じポートをリッスンしている 1つのパブリック IP アドレスに設定しようとするときに表示されます。

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

これを修正するには、2つの内部 IP アドレスを持つようにパブリック IP アドレスを設定し、DNS で2つのパブリック IP アドレスを使用します。

ARP テーブルにエントリがない

これは、NATエントリの `no-alias` オプションの結果です。 `no-alias` オプションは、ルータがアドレスに 응답せず、ARPエントリをインストールしないことを意味します。別のルータで、NATプールが、接続されているサブネット上でアドレスを構成する内部グローバルプールとして使用される場合、これらのアドレスに対する Address Resolution Protocol (ARP) 要求にルータが応答できるように、そのアドレスに対してエイリアスが生成されます。これにより、ルータは偽のアドレスに対して ARP エントリを持つことになります。

不正なトークン 0 が TOK_NUMBER|TOK_PUNCT を要求した

このエラー メッセージは情報メッセージで、デバイスの通常動作への影響はありません。

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

このエラーは、NAT が FTP を開いてアドレスにレイヤ 4 の修正を行おうとしても、パケットには変換が必要な IP アドレスが見つけれないことを意味しています。メッセージにトークンが含まれている理由は、変換に必要な詳細を探すため、IP パケット内でトークンまたは一連のシンボルを探すと、パケットで IP アドレスが見つかるためです。

FTP セッションが始まると、FTP セッションではコマンド チャネルとデータ チャネルの 2つのチャネルがネゴシエートされます。これらはともに、さまざまなポート番号を持つ IP アドレスです。FTP クライアントとサーバーでは、2 番目のデータチャネルがネゴシエートされ、ファイルが転送されます。コントロールチャネルを介して交換されたパケットには、「PORT,i,i,i,p,p」というフォーマットがあります。i,i,i,i は 4 バイトの IP アドレスで、p,p はポートを明示しています。NAT によってこのパターンへの合致が試行され、必要に応じて、アドレスとポートが変換されます。NAT では、両方のチャネル方式が変換される必要があります。NAT では、変換が必要なポートコマンドが見つかったと判断されるまで、コマンドストリームで数値がスキャンされます。次に、変換の解析が試行され、同じフォーマットで計算されます。

パケットに破損があるか、FTP サーバーまたはクライアントに不正な形式のコマンドがある場合、NAT では正しく変換が計算されず、エラーが生成されます。両方のチャネルが開始されるように、FTP クライアントを `passive` に設定します。

関連情報

- [Network Address Translation \(NAT: ネットワーク アドレス変換\) に関する FAQ](#)
- [サポートとダウンロード - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。