

NAT の動作確認と NAT の基本的なトラブルシューティング

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[NAT を対象から外す方法](#)

[問題の例： あるルータには PING できるが、別のルータにはできない](#)

[問題の要約](#)

[問題の例： Outside のネットワーク デバイスが Inside のルータと通信できない](#)

[問題の要約](#)

[トラブルシューティング チェックリスト](#)

[変換が変換テーブルに組み込まれていない](#)

[正しい変換エントリが使用されていない](#)

[NAT は正常に動作しているが、それでも接続に問題がある](#)

[ポート 80 の NAT 変換が機能しない](#)

[%%NAT: System busy. Try later](#)

[変換テーブルが大きいために、CPU 使用率が高い](#)

[% Public ip-address already mapped \(Internal ip-address -> Public ip-address\)](#)

[ARP テーブルにエントリがない](#)

[結論](#)

[悪いトークン 0、望まれた TOK NUMBER| TOK PUNCT](#)

[関連情報](#)

概要

NAT 環境で IP 接続に問題がある場合、たいていは問題の原因を探ることが困難です。NAT が原因であると誤解されることが多くありますが、実際には根本的な問題が潜んでいます。このドキュメントでは、Cisco ルータで使用可能なツールを使用して NAT オペレーションを検証する方法を説明しています。ここでは NAT の基本的なトラブルシューティングの方法と、NAT のトラブルシューティングによくある失敗を防ぐ方法について示します。

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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[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。

NAT を対象から外す方法

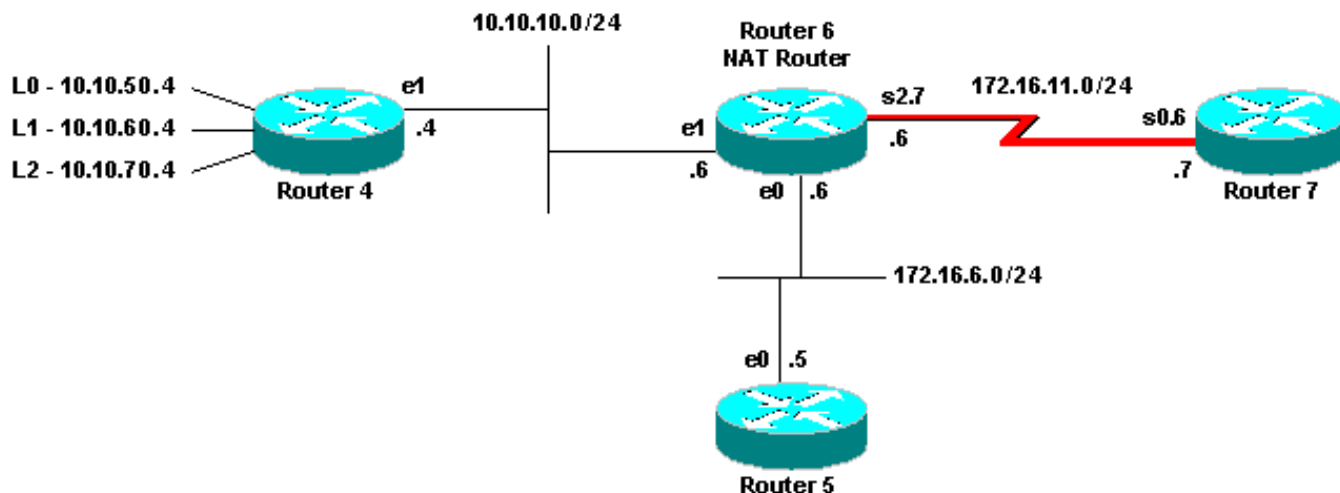
IP 接続問題の原因を探る場合、NAT を対象から外すことが役に立ちます。次の手順にしたがって、NAT が予想通りに動作していることを検証します。

1. 設定に基づき、本来 NAT が実行すべきことを明確に定義します。この時点で、設定に問題があることがわかる場合があります。NAT の設定を用いるヘルプに関しては[ネットワークアドレス変換 \(NAT \) 設定](#)を参照して下さい: 『[内部デバイスのアクセスにインターネットを許可](#)』を参照してください。
2. 変換テーブルに正しい変換が存在することを確認します。
3. `show` コマンドと `debug` コマンドを使用して、変換が行われていることを確認します。
4. パケットに何が生じているかを詳細に確認して、パケットを運ぶための正しいルーティング情報がルータにあることを確認します。

次に示すいくつかの問題例の中で、問題の原因を探る上で役立つ上記の手順を使用します。

問題の例：あるルータには PING できるが、別のルータにはできない

次のネットワークダイアグラムでは、ルータ 4 はルータ 5 (172.16.6.5) には PING できるものの、ルータ 7 (172.16.11.7) にはできません。



ルーティング プロトコルはいずれのルータでも実行されておらず、ルータ 4 はルータ 6 をデフォルト ゲートウェイとしています。ルータ 6 は、次のように NAT で設定されています。

```

ルータ 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

```

まず、NAT が正常に機能していることを確認します。設定から、ルータ 4 の IP アドレス (10.10.10.4) は 172.16.6.14 に静的に変換されるようになっていることがわかります。この変換が変換テーブルに存在していることを確認するには、ルータ 6 で **show ip nat translation** コマンドを使用します。

```

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

```

次に、ルータ 4 が IP トラフィックを発信するときに、この変換が行われていることを確認します。このことは、ルータ 6 から次の 2 つの方法で確認できます。NAT の **debug** を実行する方法と、**show ip nat statistics** コマンドで NAT の統計情報を監視する方法です。debug コマンドは常に最後の手段として使用するものであるため、まずは **show** コマンドから始めます。

ここでの目的は、ヒットカウンタを監視して、ルータ 4 からトラフィックを送信するとその数が

増加するかどうかを確認することです。ヒットカウンタは、変換テーブル内の変換を使用してアドレスを変換するごとに増加します。まず、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 してから再度統計情報を表示します。

```
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#
```

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

```
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
```

`show` コマンドから、ヒットの数は 5 増加したことがわかります。シスコルータからの ping が正常に行われれば、ヒットの数は 10 増加するはずですが、発信元ルータ (ルータ 4) から送信された 5 つの Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) エコーが変換され、宛先ルータ (ルータ 7) からの 5 つのエコー応答パケットも変換され、合計 10 のヒットになるはずですが、不足している 5 つのヒットは、多くの場合エコー応答が変換されていないかルータ 7 から送信されていないことによるものです。

ルータ 7 がエコー応答パケットをルータ 4 に送信しない理由があるかどうかを確認します。まず、NAT がパケットに何を行っているかを調べます。ルータ 4 は、ICMP エコーパケットを 10.10.10.4 の送信元アドレスと 172.16.11.7 の送信先アドレスで送信しています。NAT が行われると、ルータ 7 が受信したパケットは送信元アドレスが 172.16.6.14、送信先アドレスが 172.16.11.7 になります。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、応答するためにはこのネットワークのルートが必要になります。ルータ 7 のルーティングテーブルを調べて経路が存在するか検証します。

```
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
```

ルータ 7 のルーティングテーブルには 172.16.6.14 へのルートがないことがわかります。このルートを追加すると、PING は正常に動作します。

問題の要約

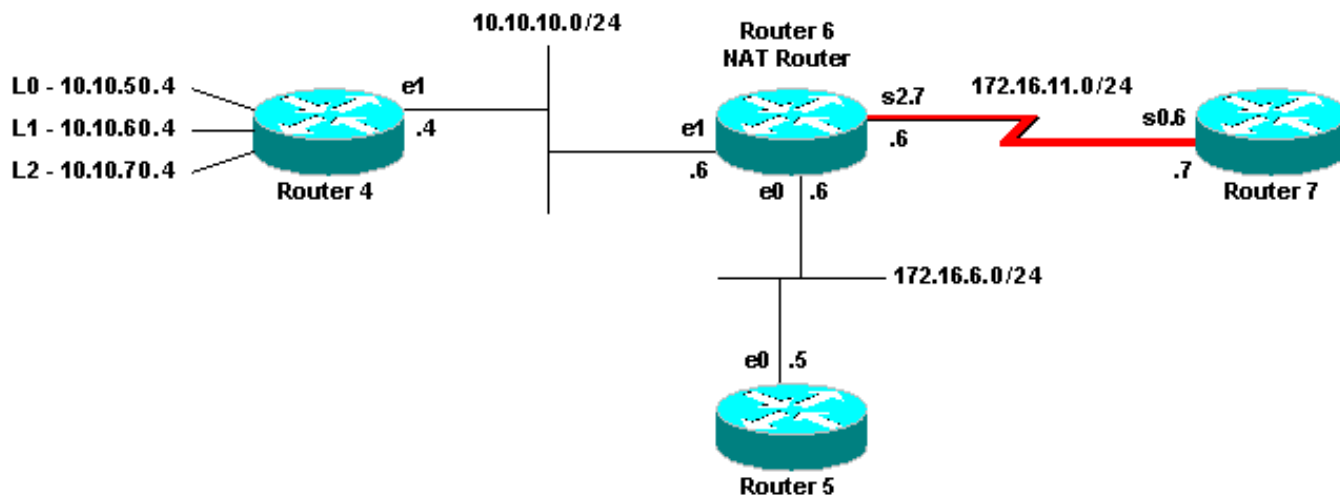
まず、NAT が実行すべきものを定義しました。次に、静的 NAT エントリが変換テーブルに存在し、正確であることを検証しました。NAT 統計情報をモニタリングして、変換が実際に行われていることを確認しました。そこである問題を発見することによりルータ 7 のルーティング情報の確認を行い、ルータ 7 はルータ 4 のグローバルアドレスの内側への経路が必要なことがわかりました。

このように単純な実験環境では、`show ip nat statistics` コマンドで NAT 統計情報を監視すると効果的です。しかし、複数の変換が行われるさらに複雑な NAT 環境では、この `show` コマンドでは役に立ちません。この場合は、`debugs` をルータ上で実行する必要があります。次の問題シナ

リオでは、debug コマンドの使用について説明しています。

問題の例： Outside のネットワーク デバイスが Inside のルータと通信できない

このシナリオでは、ルータ 4 はルータ 5 とルータ 7 に PING できますが、10.10.50.0 ネットワーク上のデバイスはルータ 5 やルータ 7 と通信できません (実験テストでこれをエミュレートするには、PING を IP アドレス 10.10.50.4 のループバック インターフェイスから発信します)。次のネットワーク ダイアグラムを見てください。



ルータ 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
```

まず、NAT の予測動作を明確にします。ルータ 6 の設定から、NAT は 10.10.50.4 を NAT プール「test」内の最初の空いているアドレスに動的に変換すると想定されていることがわかります。プールは、アドレス 172.16.11.70 と 172.16.11.71 で構成されます。前述の問題で学

習したことから、ルータ 5 と 7 が受信するパケットの送信元アドレスは 172.16.11.70 か 172.16.11.71 のどちらかであることが推測できます。これらのアドレスはルータ 7 と同じサブネットに存在するため、ルータ 7 には直接接続されたルートがあるはずですが、ない場合は、ルータ 5 からサブネットへのルートがある必要があります。

show ip route コマンドを使用して、ルータ 5 のルーティング テーブルに 172.16.11.0 が記載されていることを確認します。

```
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
```

show ip route コマンドを使用して、ルータ 7 のルーティング テーブルに 172.16.11.0 が直接接続されたサブネットとして記載されていることを確認します。

```
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
```

NAT が実行すべきことを明確に定義したので、ここで NAT が正常に動作していることを確認する必要があります。まず NAT 変換テーブルをチェックして、予測された変換が存在するのを検証します。ここで対象にしている変換はダイナミックに作成されるため、まず適切なアドレスを発信元にして IP トラフィックを送信する必要があります。10.10.50.4 を送信元、172.16.11.7 を宛先にして PING を送信すると、ルータ 6 の変換テーブルは次のようになります。

```
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 --- ---
```

想定通りの変換が変換テーブル内にあることから ICMP エコー パケットは適切に変換されていることがわかりますが、エコー 応答パケットについてはどうでしょうか。前述のように、NAT 統計情報は監視できませんが、これは複雑な環境ではあまり役に立ちません。別の選択肢は、NAT デバッグを NAT ルータ (ルータ 6) で実行することです。この場合、ルータ 6 で **debug ip nat** をオンにしつつ、10.10.50.4 を送信元、172.16.11.7 を宛先にして PING を送信します。debug の結果は次のようになります。

注: ルータで **debug** コマンドを使用すると、ルータが過負荷状態になって動作不能になることがあります。常に最大の注意を払い、できれば Cisco テクニカルサポートのエンジニアの指導がない場合は **debug** を重要な実稼働用ルータでは実行しないでください。

```
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]
```

上記の debug 出力でわかるように、最初の行は 10.10.50.4 の送信元アドレスが 172.16.11.70 に変換されていることを示しています。2 行目は、172.16.11.70 の送信先アドレスが元の 10.10.50.4 に再度変換されていることを示します。このパターンは、debug の最後まで繰り返されます。これにより、ルータ 6 はパケットを両方向に変換していることがわかります。

ここでは、何が行われているかをさらに詳しく検討します。ルータ 4 はパケットを 10.10.50.4 の発信元から 172.16.11.7 の送信先に送信します。ルータ 6 は NAT をパケット上で実行して、発信元が 172.16.11.70 で送信先が 172.16.11.7 のパケットを転送します。ルータ 7 は、発信元が 172.16.11.7 で送信先が 172.16.11.70 の応答を送信します。ルータ 6 はパケットで NAT を実行し、その結果パケットの送信元アドレスは 172.16.11.7、宛先アドレスは 10.10.50.4 になります。この時点で、ルータ 6 はルーティング テーブル内の情報に基づいて、パケットを 10.10.50.4 に転送します。show ip route コマンドを使用して、ルータ 6 に必要なルートがルーティング テーブル内にあることを確認する必要があります。

```
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
```

問題の要約

まず、NAT が実行すべきものを明確に定義しました。次に、必要な変換が変換テーブルに存在していることを確認しました。さらに、debug コマンドまたは show コマンドを使用して、変換が実際に行われていることを確認しました。最後に、パケットに行われたこと、パケットを転送したり応答したりするためにルータに必要なことを詳細に検討しました。

トラブルシューティング チェックリスト

接続問題の原因を探る基本的な手順がわかったところで、次によくある問題をトラブルシューティングするためのチェックリストをいくつか示します。

変換が変換テーブルに組み込まれていない

適切な変換が変換テーブルに組み込まれていないことがわかった場合は、次の点を確認してください。

- 設定が正しい。NAT を使用して目的の処理を行うときは、注意を要する場合があります。設定ヘルプに関しては、[ネットワークアドレス変換 \(NAT\) 設定を参照](#)して下さい: 『[内部デバイスのアクセスにインターネットを許可](#)』を参照してください。
- パケットが NAT ルータに入ることを拒否する着信アクセス リストがない。
- パケットがルータの内側から外側へ移動する場合、NAT ルータのルーティング テーブルに適切な経路がある。詳細は、『[NAT の処理順序](#)』を参照してください。
- NAT コマンドが参照するアクセス リストが、必要なネットワークをすべて許可している。
- 十分なアドレスが NAT プール内にある。これは、NAT が過負荷に設定されていない場合のみ問題になります。
- ルータ 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。
- Domain Name System (DNS; ドメイン ネーム システム) パケットのペイロードを変換する

場合、パケットの IP ヘッダー内のアドレス上で変換が行われることを確認する。変換が行われない場合、NAT はパケットのペイロードを調べません。

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組み込まれているものの、使用されていない場合は、次の点を確認してください。

- パケットが NAT ルータに入ることを拒否する着信アクセスリストがないこと。
- ルータの内側から外側へ送られるパケットでは、宛先への経路は変換前に確認されるため、これが存在することを確認します。詳細は、『[NAT の処理順序](#)』を参照してください。

NAT は正常に動作しているが、それでも接続に問題がある

NAT が正常に動作している場合は、接続問題のトラブルシューティングを次のように行います。

- レイヤ 2 の接続を検証する。
- レイヤ 3 のルーティング情報を検証する。
- 問題の原因であることが考えられるパケット フィルタを探す。

ポート 80 の NAT 変換が機能しない

NAT 変換は、ポート 80 に対しては機能しませんが、それ以外のポートに対しては正常に機能します。

この問題を解決するには、次の手順を実行します。

1. `debug ip nat translations` コマンドと `debug ip packet` コマンドを実行して、変換が正しく、正しい変換エントリが変換テーブルに組み込まれていることを確認します。
2. サーバが応答することを確認します。
3. HTTP サーバをディセーブルにします。
4. NAT テーブルおよび ARP テーブルをクリアします。

%%NAT: System busy. Try later

`%NAT: System busy.` 表示コマンドが NAT に関連しているか、または `show running-config` が `write memory` コマンドが実行されるときにエラーメッセージが現れます。この問題は、NAT テーブルのサイズが増えたために発生します。NAT テーブルのサイズが増えると、ルータはメモリを使い果たします。

この問題を解決するには、ルータをリロードします。HSRP SNAT が設定されている場合にこのエラーメッセージが表示された場合、問題を解決するには、次のコマンドを設定します。

```
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に、CPU 使用率が高い

ホストから数百の変換が送信されることがあり、これにより CPU 使用率が高くなります。つまり、CPU が 100 % で動作するほど、テーブルのサイズが大きくなることがあります。ip nat

translation max-entries 300 コマンドを使用すると、ルータでの変換量をホストあたり 300 に制限したり、総量を制限したりできます。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。

[% Public ip-address already mapped \(Internal ip-address -> Public ip-address\)](#)

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

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

NAT でパブリック IP アドレスを 2 つの内部 IP アドレスに変換するには、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 エントリで *no-alias* オプションが使用されるために発生します。no-alias オプションが設定されていると、ルータはアドレスに 응답せず、ARP エントリを組み込みません。Inside グローバルプールとして NAT プールを使用するルータが他にあり、そのプールには接続されたサブネット上のアドレスが構成されている場合、ルータがそのアドレスに対する Address Resolution Protocol (ARP; アドレス解決プロトコル) 要求に 응답できるように、そのアドレスのエイリアスが生成されます。このため、ルータには擬似アドレスの ARP エントリが組み込まれます。

[結論](#)

上記の問題は、NAT が必ずしも IP 接続問題の原因ではないことを示しています。多くの場合、原因は NAT 以外にあり、さらに調査する必要があります。このドキュメントでは、NAT オペレーションをトラブルシューティングおよび検証する場合に行う基本的な手順を説明します。これらの手順は次のとおりです。

- NAT が実行すべきことを明確に定義する。
- 正しい変換が変換テーブルに存在することを確認する。
- show コマンドと debug コマンドを使用して、変換が行われていることを確認する。
- パケットに何が生じているかを詳細に確認して、パケットを運ぶための正しいルーティング情報がルータにあることを確認します。

[悪いトークン 0、望まれた TOK_NUMBER| TOK_PUNCT](#)

このエラーメッセージは単なる情報メッセージであり、デバイスの正常な動作に影響するものではありません。

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

ここでのエラーは、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たものの、パケットには変換を必要とする IP アドレスが見つから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には、IP パケットに含まれるトークン (シンボルのセット) を探して、パケット内の IP アドレスを見つけるためです。

FTP セッションを開始すると、コマンドチャンネルと D チャンネルの 2 つのチャンネルとのネゴシエーションが行われます。どちらも IP アドレスで、それぞれポート番号が異なります。FTP クライアントとサーバは、ファイルを転送するために 2 つ目の D チャンネルをネゴシエートします。

制御チャンネル経由で交換されたパケットは、「PORT,i,i,i,p,p」という形式になります。i,i,i,i は 4 バイトの IP アドレスであり、p,p はポートです。NAT はこのパターンを照合し、必要に応じてアドレスとポートを変換しようとしています。どちらのチャンネルのアドレッシング方式も変換する必要があります。NAT は、変換を必要とするポート コマンドが見つかったと判断するまで、コマンドストリームで数値をスキャンします。続いて、その変換の解析を試み、前述したパターンで計算します。

パケットが破損であるか、または FTP サーバにクライアントは malforming コマンドがあれば、NAT はきちんと変換を計算できないし、そのエラーを生成します。推奨事項は両方のチャンネルを始めるように「受動態」に FTP クライアントを設定 することです。これは、NAT 経由の FTP には有用である場合があります。

[関連情報](#)

- [NAT に関するサポートページ](#)
- [テクニカルサポート - Cisco Systems](#)