ダイナミック NAT の使用時にルーティング ループを回避する方法

目次

概要

このドキュメントでは、トラフィックが NAT プールの未使用 IP アドレス宛で、外部にパケットをルーティングしている NAT ルータにデフォルトのルートが存在するために、ダイナミック ネットワーク アドレス変換（NAT）を使用する場合に、外部インターフェイスの NAT ルータと隣接ルータ間でパケットがループするシナリオ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。

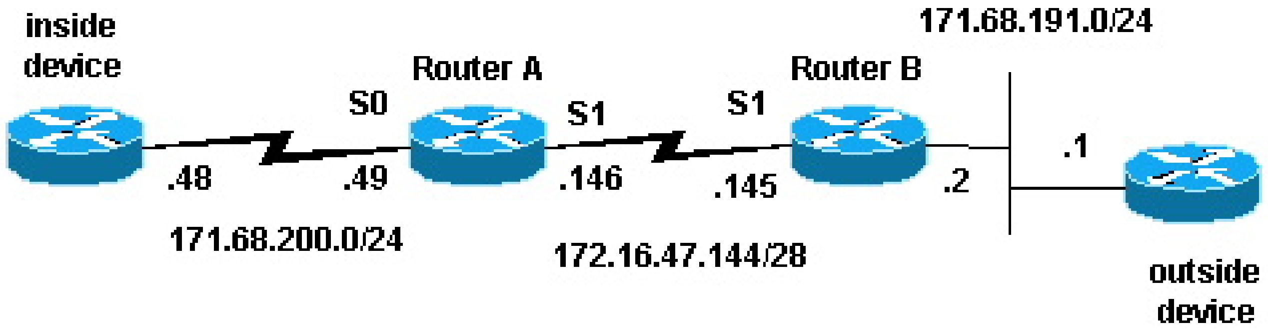
使用するコンポーネント

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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

次のトポロジーがシナリオ例を作成するのに使用されました。



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。

シナリオ例

上記の構成図では、ルータ A に NAT が設定されているため、ルータ A はネットワーク 171.68.200.0/24 を送信元として持つパケットを、NAT プール "test-loop" によって定義されているアドレス範囲に変換します。 ルータ A の設定は、次のとおりです（他のすべてのルータには、接続性を得るためにスタティック ルートが設定されています）。

```
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
```

NAT 変換デバッグ コマンドと IP パケット デバッグ コマンドを使って、内部デバイス上のルータからの ping を生成しました。 ping は動作し、変換テーブル エントリが作成されました。 次の出力では、IP パケット デバッグと IP NAT デバッグがオンになっており、この時点では変換テーブル内にエントリが存在していないことがわかります。

注: 注：**デバッグ コマンド**は、大量の出力を生成します。 システムの他の動作に悪影響が及ばないように、IP ネットワーク上のトラフィック負荷が低い場合にだけ使用してください。

```
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#
```

内部ルータ（内部デバイス）は、送信元アドレス 171.68.200.48 と宛先アドレス 171.68.191.1（外部デバイスのアドレス）を持つ ICMP パケットを発信します。 次のデバッグ出力は、送信元 IP アドレス 171.68.200.48 を持つ IP パケットが 172.16.47.161 に変換される様子を示しています。 パケットはシリアル 0 インターフェイスに到着し、シリアル 1 インターフェイス宛てに送られます。

```
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
```

次のデバッグ出力は、宛先 IP アドレス 172.16.47.161 を持つリターン IP パケットが 171.68.200.48 に変換し直される様子を示しています。 パケットはシリアル 1 インターフェイスに到着し、シリアル 0 インターフェイス宛てに送られます。

```
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
```

デバッグ出力は、内部デバイスと外部デバイスの間で ping が正常に交換されたことを示しています。

```
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
```

show ip nat translations コマンドを使って、内部デバイスの変換テーブル内のエントリを確認します。

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

この時点で、内部デバイスの変換エントリが変換テーブル内に存在しています。次のルータ A によって生成されたデバッグ出力に示されているとおり、外部デバイスから内部デバイスのグローバル アドレス宛てに ping を正常に実行できます。

注: 外部デバイスによって発信されたパケットは、送信元アドレスとして 171.68.191.1、宛先アドレスとして 172.16.47.161（変換テーブル内の内部グローバル アドレス）を持っています。

```
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
```

次のデバッグ出力は、外部デバイスが、test-loop プール内の未使用の IP アドレスである宛先アドレスと通信を開始しようとした場合に何が起こるかを示しています。 clear ip nat translation コマンドを使って変換テーブルをクリアし、ping を test-loop プール内の未使用の IP アドレスへ送信しました。

外部デバイスは、内部グローバル アドレス 172.16.47.161 宛てに ICMP パケットを送信しました。 ただし、出力インターフェイスは、このパケットの入力インターフェイスと同一です。

```
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 は、外部から内部宛てのパケットを変換してから、そのパケットをルーティングします。 この場合、変換テーブルに No エントリがあります、従ってルータA はパケットしかルーティングなできます。 ルータA はデフォルト ルートにパケットを Serial1 インターフェイス 送信 するパケットをルーティングするためにキャンセルします結局シリアルラインをダウンさせる可能性があるループを引き起こす頼ります。

この種のルーティング ループを回避するために、外部デバイスから内部グローバル アドレス宛てには、決してパケットを発信しないでください。 ただし、これを適用するのは困難なため、ルータ A で、ネクストホップとしてヌル 0 を持つ、内部グローバル アドレスのスタティック ルートを追加することができます。 この方法を使えば、外部デバイスが内部グローバル アドレスにパケットを送信し、変換テーブル内にエントリがない場合に、ルータ A はパケットをヌル 0 へルーティングするため、ループは回避できます。 上記の例を使うと、スタティック ルートは次のようになります。

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

関連情報

- NAT に関するサポートページ
- IP ルーティング プロトコルに関するサポート ページ
- IP ルーティングに関するサポート ページ
- テクニカルサポート - Cisco Systems