スティック上のネットワーク アドレス変換

内容

概要

Network Address Translation（NAT）on a stick とは何を意味していますか。「on a stick」という用語からは一般に、ルータの 1 つの物理インターフェイスを使用してタスクを処理することが推測されます。同じ物理インターフェイスのサブインターフェイスを使用して Inter-Switch Link（ISL）トランキングを実行できるように、ルータで 1 つの物理インターフェイスを使用して NAT を実現できます。

注：ルータは、ループバックインターフェイスが原因で、すべてのパケットのスイッチを処理する必要があります。このため、ルータのパフォーマンスが低下します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

この機能を使用するには、NAT をサポートする Cisco IOS® ソフトウェア バージョンを使用する必要があります。この機能と共に使用できる IOS バージョンを確認するには、Cisco Feature Navigator II（登録ユーザ専用）を使用してください。

表記法

ドキュメントの表記法の詳細は、「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。

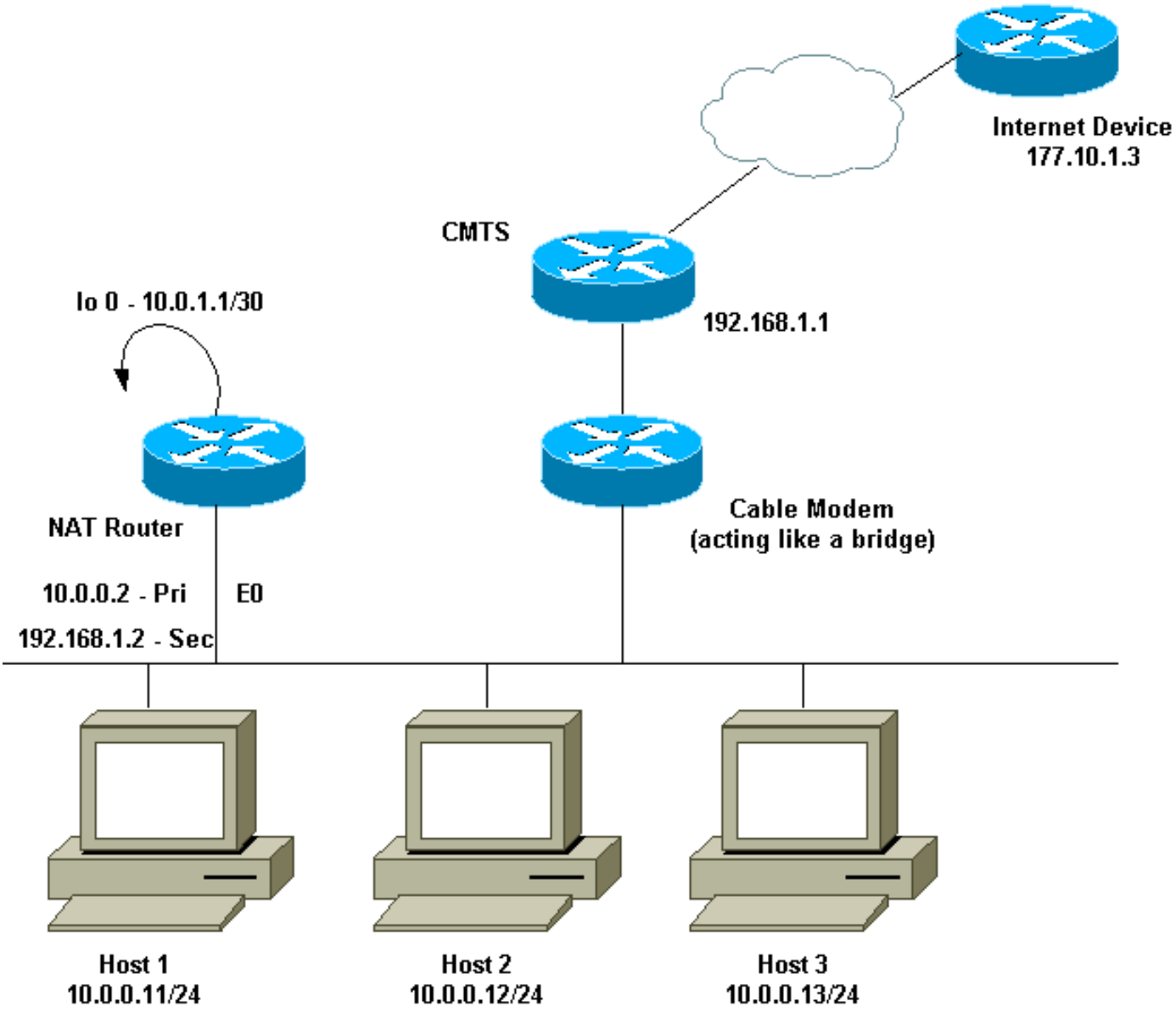
背景説明

NAT を実行するためには、NAT「内部」で定義されたインターフェイスから NAT「外部」で定義されたインターフェイスに、またはその逆に、パケットが交換される必要があります。このドキュメントでは、単一の物理インターフェイスを使用してルータで NAT を動作させるために、仮想インターフェイス（ループバック インターフェイスとも呼ばれます）とポリシーベース ルーティングを使用する方法について示します。

「NAT の役割」の必要性はほとんどありません。実際にこの設定が必要になる状況は、このドキュメントで紹介している例のみであると考えられます。それ以外に、ユーザがポリシー ルーティングを NAT と組み合せて利用する状況もありますが、そのような状況でも複数の物理インターフェイスが使用されることから、これは NAT の役割とは見なしません。

例 1 ネットワーク ダイアグラムと設定

ネットワーク図



上のネットワーク ダイアグラムはケーブル モデムの設定におけるごく一般的なものです。Cable Modem Termination System (CMTS; ケーブルモデム終端システム) はルータであり、Cable Modem (CM; ケーブル モデム) はブリッジと同様に機能する装置です。ここで問題になるのは、インターネットにアクセスする必要のあるホスト数に十分見合った有効なアドレスが Internet Service Provider (ISP; インターネット サービス プロバイダー) から与えられていないことです。ISP からはアドレス 192.168.1.2 が与えられていましたが、これは装置用として使用する必要がありました。さらに要求があると、192.168.2.1 ~ 192.168.2.3の3つのアドレスが受信され、NATは10.0.0.0/24の範囲のホストを変換します。

要件

要件は次のとおりです。

- ネットワーク上のすべてのホストからインターネットにアクセスできること。
- インターネットから IP アドレス 192.168.2.1 を使用してホスト 2 にアクセスできること。
- 正規のアドレス数よりも多くのホストを配置できるため、内部アドレッシング用に 10.0.0.0/24 サブネットを使用していること。

この文書の目的に従い、ここでは NAT ルータの設定のみを示しています。ただし、ホストに関する設定上の重要な注意事項についてはいくつか言及しています。

NAT ルータの設定

NAT ルータの設定

```
interface Loopback0
 ip address 10.0.1.1 255.255.255.252
 ip nat outside
!--- Creates a virtual interface called Loopback 0 and
assigns an !--- IP address of 10.0.1.1 to it. Defines
interface Loopback 0 as !--- NAT outside. ! ! interface
Ethernet0 ip address 192.168.1.2 255.255.255.0 secondary
ip address 10.0.0.2 255.255.255.0 ip Nat inside !---
Assigns a primary IP address of 10.0.0.2 and a secondary
IP !--- address of 192.168.1.2 to Ethernet 0. Defines
interface Ethernet 0 !--- as NAT inside. The 192.168.1.2
address will be used to communicate !--- through the CM
to the CMTS and the Internet. The 10.0.0.2 address !---
will be used to communicate with the local hosts. ip
policy route-map Nat-loop !--- Assigns route-map "Nat-
loop" to Ethernet 0 for policy routing. ! ip Nat pool
external 192.168.2.2 192.168.2.3 prefix-length 29 ip Nat
inside source list 10 pool external overload ip Nat
inside source static 10.0.0.12 192.168.2.1 !--- NAT is
defined: packets that match access-list 10 will be !---
translated to an address from the pool called
"external". !--- A static NAT translation is defined for
10.0.0.12 to be !--- translated to 192.168.2.1 (this is
for host 2 which needs !--- to be accessed from the
Internet).


ip classless
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 192.168.2.0 255.255.255.0 Ethernet0
 !--- Static default route set as 192.168.1.1, also a
static !--- route for network 192.168.2.0/24 directly
attached to !--- Ethernet 0 ! ! access-list 10 permit
10.0.0.0 0.0.0.255 !--- Access-list 10 defined for use
by NAT statement above.


access-list 102 permit ip any 192.168.2.0 0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!--- Access-list 102 defined and used by route-map "Nat-
loop" !--- which is used for policy routing.

!
Access-list 177 permit icmp any any
 !--- Access-list 177 used for debug.

!
route-map Nat-loop permit 10
 match ip address 102
 set ip next-hop 10.0.1.2
!--- Creates route-map "Nat-loop" used for policy
routing. !--- Route map states that any packets that
match access-list 102 will !--- have the next hop set to
10.0.1.2 and be routed "out" the !--- loopback
interface. All other packets will be routed normally. !-
-- We use 10.0.1.2 because this next-hop is seen as
```

```
located !--- on the loopback interface which would
result in policy routing to !--- loopback0.
Alternatively, we could have used "set interface !---
loopback0" which would have done the same thing. ! end
NAT-router#
```

注：すべてのホストのデフォルトゲートウェイは、NATルータである10.0.0.2に設定されています。戻りトラフィックが機能するには、ISP と CMTS には、NAT ルータを指し示す 192.168.2.0/29 へのルートが必要です。これは、ホスト内部からのトラフィックはこのサブネットから着信するように見えるためです。この例では、CMTS は 192.168.1.2 のトラフィックを 192.168.2.0/29 (NAT ルータで設定されているセカンダリ IP アドレス) にルーティングします。

例 1 show および debug コマンドの出力

この項では、設定が正常に動作しているかどうかを確認する際に役立つ情報を紹介しています。

上の設定が動作することを実証するために、NAT ルータの **debug 出力の監視中に ping test をいくつか実行しました。**ping コマンドが成功し、debug 出力によってどんな処理が行われているのかが正確に示されることがわかります。

注：debugコマンドを使用する前**に**、『debugコマンド[の重要な情報』を参照してください](#)。

テスト 1

最初のテストでは、ラボで定義したインターネット上のデバイスからホスト2にpingを実行します。インターネット上のデバイスは、IPアドレス192.168.2.1を使用してホスト2と通信できる必要があります。次に**debugの出力を示します。**NAT ルータで実行していた debug コマンドは、定義済みの access-list 177 を使用する debug ip packet 177 detail、debug ip Nat、およびポリシー ルーティングされたパケットを表示する debug ip policy です。

NAT ルータで実行した **show ip Nat translation コマンドの出力を次に示します。**

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

インターネット上の装置 (この場合はルータ) から 192.168.2.1 に対して **ping を発行します。これは次のように成功します。**

```
Internet-device# ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/92 ms
Internet-device#
```

次の **debug 出力とコメントを確認して、NAT ルータでどんな処理が行われているのかを理解してください。**

```
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1, len 100, policy match
    ICMP type=8, code=0
```

```
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), Len 100, policy routed
    ICMP type=8, code=0
!--- The above debug output shows the packet with source 177.10.1.3 destined !--- to
192.168.2.1. The packet matches the statements in the "Nat-loop" !--- policy route map and is
permitted and policy-routed. The Internet !--- Control Message Protocol (ICMP) type 8, code 0
indicates that this !--- packet is an ICMP echo request packet.


IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), g=10.0.1.2, Len 100,
forward
    ICMP type=8, code=0
 !--- The packet now is routed to the new next hop address of 10.0.1.2 !--- as shown above. IP:
NAT enab = 1 trans = 0 flags = 0 NAT: s=177.10.1.3, d=192.168.2.1->10.0.0.12 [52] IP:
s=177.10.1.3 (Loopback0), d=10.0.0.12 (Ethernet0), g=10.0.0.12, Len 100, forward ICMP type=8,
code=0 IP: NAT enab = 1 trans = 0 flags = 0 !--- Now that the routing decision has been made,
NAT takes place. We can !--- see above that the address 192.168.2.1 is translated to 10.0.0.12
and !--- this packet is forwarded out Ethernet 0 to the local host. !--- Note: When a packet is
going from inside to outside, it is routed and !--- then translated (NAT). In the opposite
direction (outside to inside), !--- NAT takes place first.


IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3, Len 100, policy match
    ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
    ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
!--- Host 2 now sends an ICMP echo response, seen as ICMP type 0, code 0. !--- This packet also
matches the policy routing statements and is !--- permitted for policy routing. NAT:
s=10.0.0.12->192.168.2.1, d=177.10.1.3 [52] IP: s=192.168.2.1 (Ethernet0), d=177.10.1.3
(Loopback0), g=10.0.1.2, Len 100, forward ICMP type=0, code=0 IP: s=192.168.2.1 (Loopback0),
d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100, forward ICMP type=0, code=0 IP: NAT enab = 1
trans = 0 flags = 0 !--- The above output shows the Host 2 IP address is translated to !---
192.168.2.1 and the packet that results packet is sent out loopback 0, !--- because of the
policy based routing, and finally forwarded !--- out Ethernet 0 to the Internet device. !--- The
remainder of the debug output shown is a repeat of the previous !--- for each of the additional
four ICMP packet exchanges (by default, !--- five ICMP packets are sent when pinging from Cisco
routers). We have !--- omitted most of the output since it is redundant.

IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1, Len 100, policy match
    ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), Len 100, policy routed
    ICMP type=8, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), g=10.0.1.2, Len 100,
forward
    ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
NAT: s=177.10.1.3, d=192.168.2.1->10.0.0.12 [53]
IP: s=177.10.1.3 (Loopback0), d=10.0.0.12 (Ethernet0), g=10.0.0.12, Len 100,
forward
    ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3, Len 100, policy match
    ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
    ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
NAT: s=10.0.0.12->192.168.2.1, d=177.10.1.3 [53]
IP: s=192.168.2.1 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100,
```

```
forward
    ICMP type=0, code=0
IP: s=192.168.2.1 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100,
forward
    ICMP type=0, code=0
IP: NAT enab = 1 trans = 0 flags = 0
```

テスト 2

もう 1 つの要件として、各ホストがインターネットと通信できるようにすることがあります。このテストでは、ホスト1から**インター**ネットデバイスにpingを実行します。結果として得られる**showコマンドとdebugコマンドは**次のとおりです。

初期状態では、NAT ルータの NAT 変換テーブルは次のようになっています。

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

ホスト 1 から **ping を発行すると、次の結果が得られます。**

```
Host-1# ping 177.10.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 177.10.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/96 ms
Host-1#
```

上の結果から ping が成功したことがわかります。NAT ルータの NAT テーブルは次のようになります。

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.2.2:434   10.0.0.11:434      177.10.1.3:434     177.10.1.3:434
icmp 192.168.2.2:435   10.0.0.11:435      177.10.1.3:435     177.10.1.3:435
icmp 192.168.2.2:436   10.0.0.11:436      177.10.1.3:436     177.10.1.3:436
icmp 192.168.2.2:437   10.0.0.11:437      177.10.1.3:437     177.10.1.3:437
icmp 192.168.2.2:438   10.0.0.11:438      177.10.1.3:438     177.10.1.3:438
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

上の NAT 変換テーブルが示す追加のトランスレーションは (スタティックな NAT コンフィギュレーションではなく) ダイナミックな NAT コンフィギュレーションの結果です。

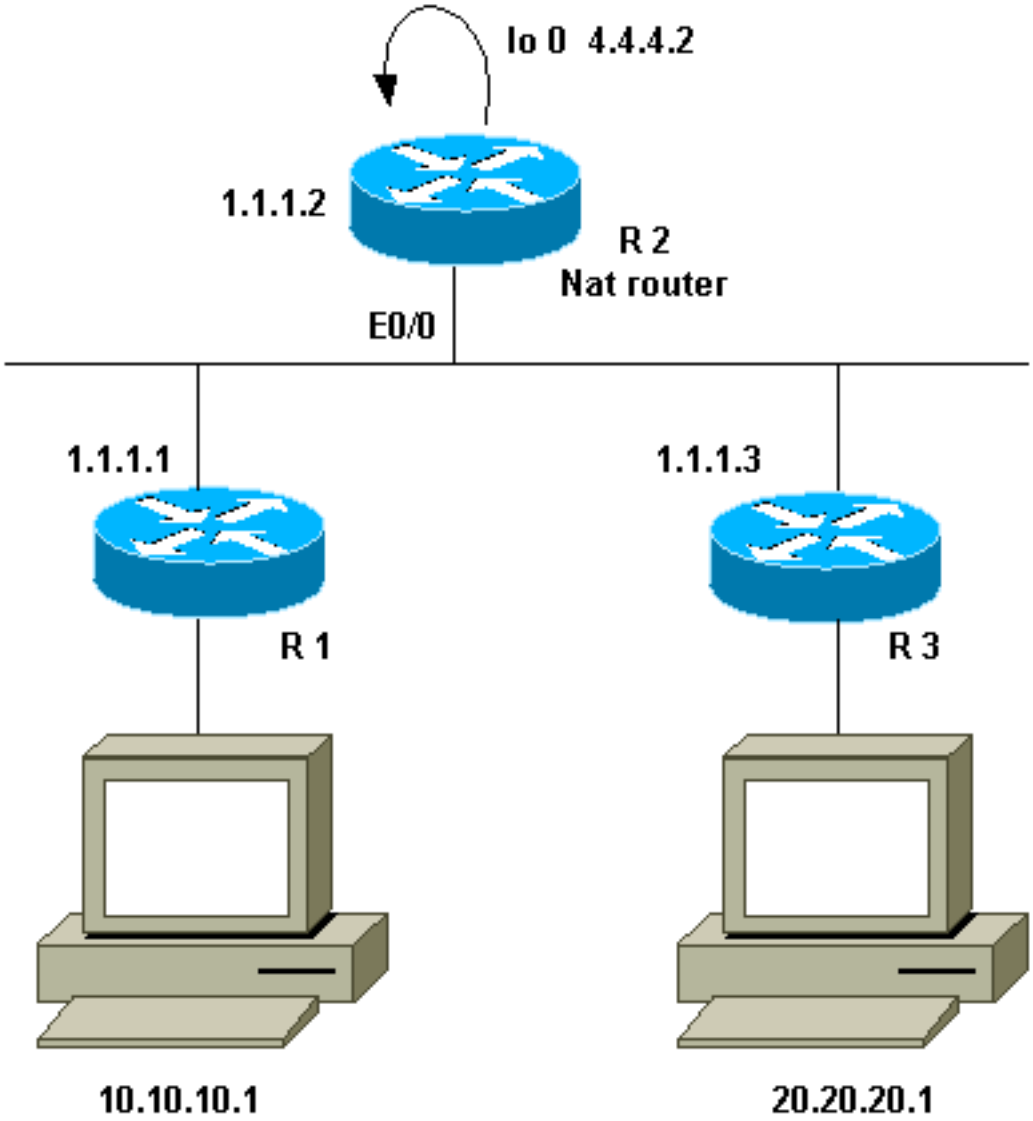
次の **debug 出力は、NAT ルータでどのような処理が行われているのかを示しています。**

```
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3, Len 100, policy match
    ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
```

```
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
    ICMP type=8, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
!--- The above output shows the ICMP echo request packet originated by !--- Host 1 which is
policy-routed out the loopback interface. NAT: s=10.0.0.11->192.168.2.2, d=177.10.1.3 [8] IP:
s=192.168.2.2 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100, forward ICMP type=8,
code=0 IP: s=192.168.2.2 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100, forward
ICMP type=8, code=0 IP: NAT enab = 1 trans = 0 flags = 0 !--- After the routing decision has
been made by the policy routing, !--- translation takes place, which translates the Host 1 IP
address of 10.0.0.11 !--- to an address from the "external" pool 192.168.2.2 as shown above. !--
- The packet is then forwarded out loopback 0 and finally out Ethernet 0 !--- to the Internet
device. IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2, Len 100, policy match ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0),
Len 100, policy routed ICMP type=0, code=0 IP: Ethernet0 to Loopback0 10.0.1.2 IP: s=177.10.1.3
(Ethernet0), d=192.168.2.2 (Loopback0), g=10.0.1.2, Len 100, forward ICMP type=0, code=0 !---
The Internet device sends an ICMP echo response which matches our !--- policy, is policy-routed,
and forward out the Loopback 0 interface. IP: NAT enab = 1 trans = 0 flags = 0 NAT:
s=177.10.1.3, d=192.168.2.2->10.0.0.11 [8] IP: s=177.10.1.3 (Loopback0), d=10.0.0.11
(Ethernet0), g=10.0.0.11, Len 100, forward ICMP type=0, code=0 !--- The packet is looped back
into the loopback interface at which point !--- the destination portion of the address is
translated from 192.168.2.2 !--- to 10.0.0.11 and forwarded out the Ethernet 0 interface to the
local host. !--- The ICMP exchange is repeated for the rest of the ICMP packets, some of !---
which are shown below. IP: NAT enab = 1 trans = 0 flags = 0 IP: s=10.0.0.11 (Ethernet0),
d=177.10.1.3, Len 100, policy match ICMP type=8, code=0 IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed ICMP type=8,
code=0 IP: Ethernet0 to Loopback0 10.0.1.2 NAT: s=10.0.0.11->192.168.2.2, d=177.10.1.3 [9] IP:
s=192.168.2.2 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100, forward ICMP type=8,
code=0 IP: s=192.168.2.2 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100, forward
ICMP type=8, code=0 IP: NAT enab = 1 trans = 0 flags = 0 IP: s=177.10.1.3 (Ethernet0),
d=192.168.2.2, Len 100, policy match ICMP type=0, code=0 IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0), Len 100, policy routed ICMP type=0,
code=0 IP: Ethernet0 to Loopback0 10.0.1.2 IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2
(Loopback0), g=10.0.1.2, Len 100, forward ICMP type=0, code=0 IP: NAT enab = 1 trans = 0 flags =
0 NAT: s=177.10.1.3, d=192.168.2.2->10.0.0.11 [9] IP: s=177.10.1.3 (Loopback0), d=10.0.0.11
(Ethernet0), g=10.0.0.11, Len 100, forward ICMP type=0, code=0
```

例 2 ネットワーク ダイアグラムと設定

ネットワーク図



要件

ここでは、通信相手となる 2 か所のサイト（R1 および R3）のバックに、なんらかの装置が必要になります。2 か所のサイトでは未登録の IP アドレスを使用しているため、互いに通信するときにアドレスを変換する必要があります。この場合、ホスト10.10.10.1は200.200.200.1に変換され、ホスト20.20.20.1は100.100.100.1に変換されます。したがって、両方向で変換を行う必要があります。アカウンティングの目的で、これら2つのサイト間のトラフィックはR2を通過する必要があります。集約するには、次の要件があります。

- R1 の背後にあるホスト 10.10.10.1 と R3 のバックにあるホスト 20.20.20.1 とで、それぞれのグローバル アドレスを使用して通信を行う必要があること。
- これらのホスト間のトラフィックが必ず R2 経由で送信されること。
- この例では、次の設定に示すように「スタティック」な NAT 変換が必要になります。

NAT ルータの設定

NAT ルータの設定
`interface Loopback0`

```
 ip address 4.4.4.2 255.255.255.0
 ip Nat inside
!--- Creates a virtual interface called "loopback 0" and
assigns IP address !--- 4.4.4.2 to it. Also defines for
it a NAT inside interface. ! Interface Ethernet0/0 ip
address 1.1.1.2 255.255.255.0 no ip redirects ip Nat
outside ip policy route-map Nat !--- Assigns IP address
1.1.1.1/24 to e0/0. Disables redirects so that packets
!--- which arrive from R1 destined toward R3 are not
redirected to R3 and !--- visa-versa. Defines the
interface as NAT outside interface. Assigns !--- route-
map "Nat" used for policy-based routing. ! ip Nat inside
source static 10.10.10.1 200.200.200.1 !--- Creates a
static translation so packets received on the inside
interface !--- with a source address of 10.10.10.1 will
have their source address !--- translated to
200.200.200.1. Note: This implies that the packets
received !--- on the outside interface with a
destination address of 200.200.200.1 !--- will have the
destination translated to 10.10.10.1.


ip Nat outside source static 20.20.20.1 100.100.100.1
!--- Creates a static translation so packets received on
the outside interface !--- with a source address of
20.20.20.1 will have their source address !---
translated to 100.100.100.1. Note: This implies that
packets received on !--- the inside interface with a
destination address of 100.100.100.1 will !--- have the
destination translated to 20.20.20.1.


ip route 10.10.10.0 255.255.255.0 1.1.1.1
ip route 20.20.20.0 255.255.255.0 1.1.1.3
ip route 100.100.100.0 255.255.255.0 1.1.1.3
!
access-list 101 permit ip host 10.10.10.1 host
100.100.100.1
route-map Nat permit 10
 match ip address 101
 set ip next-hop 4.4.4.2
```

例 2 show および debug コマンドの出力

注：特定のshowコマンドは、アウトプットインタープリタ（登録ユーザ専用）ツールでサポートされています。このツールを使用すると、showコマンドの出力を分析できます。debug コマンドを使用する前に、「debug コマンドの重要な情報」を参照してください。

テスト 1

上の設定に示したように、2 つのスタティック NAT トランスレーションがあり、これらは R2 でコマンド show ip Nat translation を使用して確認できます。

NAT ルータで実行した **show ip Nat translation コマンドの出力を次に示します。**

```
NAT-router# show ip Nat translation
```

```
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                100.100.100.1      20.20.20.1
--- 200.200.200.1      10.10.10.1         ---                ---
R2#
```

このテストでは、R1の背後にあるデバイス(10.10.10.1)から、R3の背後にあるデバイス(100.100.100.1)のグローバルアドレス宛てに**ping**を送信しました。R2で**debug ip Natと debug ip packetを実行すると、次の出力が得られます。**

```
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1, Len 100, policy match
    ICMP type=8, code=0
IP: route map Nat, item 10, permit
IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1 (Loopback0), Len 100, policy
routed
    ICMP type=8, code=0
IP: Ethernet0/0 to Loopback0 4.4.4.2
!--- The above output shows the packet source from 10.10.10.1 destined !--- for 100.100.100.1
arrives on E0/0, which is defined as a NAT !--- outside interface. There is not any NAT that
needs to take place at !--- this point, however the router also has policy routing enabled for
!--- E0/0. The output shows that the packet matches the policy that is !--- defined in the
policy routing statements. IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1 (Loopback0),
g=4.4.4.2, Len 100, forward ICMP type=8, code=0 IP: NAT enab = 1 trans = 0 flags = 0 !--- The
above now shows the packet is policy-routed out the loopback0 !--- interface. Remember the
loopback is defined as a NAT inside interface. NAT: s=10.10.10.1->200.200.200.1, d=100.100.100.1
[26] NAT: s=200.200.200.1, d=100.100.100.1->20.20.20.1 [26] !--- For the above output, the
packet is now arriving on the loopback0 !--- interface. Since this is a NAT inside interface, it
is important to !--- note that before the translation shown above takes place, the router !---
will look for a route in the routing table to the destination, which !--- before the translation
is still 100.100.100.1. Once this route look up !--- is complete, the router will continue with
translation, as shown above. !--- The route lookup is not shown in the debug output.


IP: s=200.200.200.1 (Loopback0), d=20.20.20.1 (Ethernet0/0), g=1.1.1.3, Len 100,
forward
    ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
!--- The above output shows the resulting translated packet that results is !--- forwarded out
E0/0.
```

次の出力は、ルータ 3 のバックにある装置を発信元とし、ルータ 1 のバックにある装置を宛先とする、応答パケットの結果です。

```
NAT: s=20.20.20.1->100.100.100.1, d=200.200.200.1 [26]
NAT: s=100.100.100.1, d=200.200.200.1->10.10.10.1 [26]
 !--- The return packet arrives into the e0/0 interface which is a NAT !--- outside interface.
In this direction (outside to inside), translation !--- occurs before routing. The above output
shows the translation takes place. IP: s=100.100.100.1 (Ethernet0/0), d=10.10.10.1
(Ethernet0/0), Len 100, policy rejected -- normal forwarding ICMP type=0, code=0 IP:
s=100.100.100.1 (Ethernet0/0), d=10.10.10.1 (Ethernet0/0), g=1.1.1.1, Len 100, forward ICMP
type=0, code=0 !--- The E0/0 interface still has policy routing enabled, so the packet is !---
check against the policy, as shown above. The packet does not match the !--- policy and is
forwarded normally.
```

要約

この文書では、「NAT の役割」シナリオの作成に使用できる、NAT とポリシーベース ルーティングの使用方法を説明しました。この設定では、パケットがルータを通じてプロセス交換されることがあるため、NAT を実行しているルータのパフォーマンスが低下する可能性があることに留意してください。

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