ترجمة عنوان الشبكة على عصا

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
مثال 1 شبكة رسم بياني وتكوين
الرسم التخطيطي للشبكة
المتطلبات
تكوين موجه NAT
مثال 1 عرض و debug أمر إنتاج
الاختبار الأول
رائزين
مثال 2 شبكة رسم بياني وتكوين
الرسم التخطيطي للشبكة
المتطلبات
تكوين موجه NAT
مثال 2 عرض و debug أمر إنتاج
الاختبار الأول
ملخص
معلومات ذات صلة

المقدمة

ماذا نعني بترجمة عنوان الشبكة (NAT) على عصا؟ عادة ما يعني مصطلح "على عصا" إستخدام واجهة مادية واحدة للموجه لمهمة. مثلما يمكننا إستخدام الواجهات الفرعية من نفس الواجهة المادية لإجراء توصيل الارتباط بين المحولات (ISL)، يمكننا إستخدام واجهة مادية واحدة على موجه من أجل تحقيق NAT.

ملاحظة: يجب أن يعالج الموجه المحول كل حزمة بسبب واجهة الاسترجاع. يؤدي ذلك إلى تدهور أداء الموجه.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تتطلب هذه الميزة إستخدام إصدار من برنامج Cisco IOS®الذي يدعم NAT. أستخدم متصفح الميزات II من Cisco (العملاء المسجلون فقط) لتحديد إصدارات IOS التي يمكنك إستخدامها مع هذه الميزة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

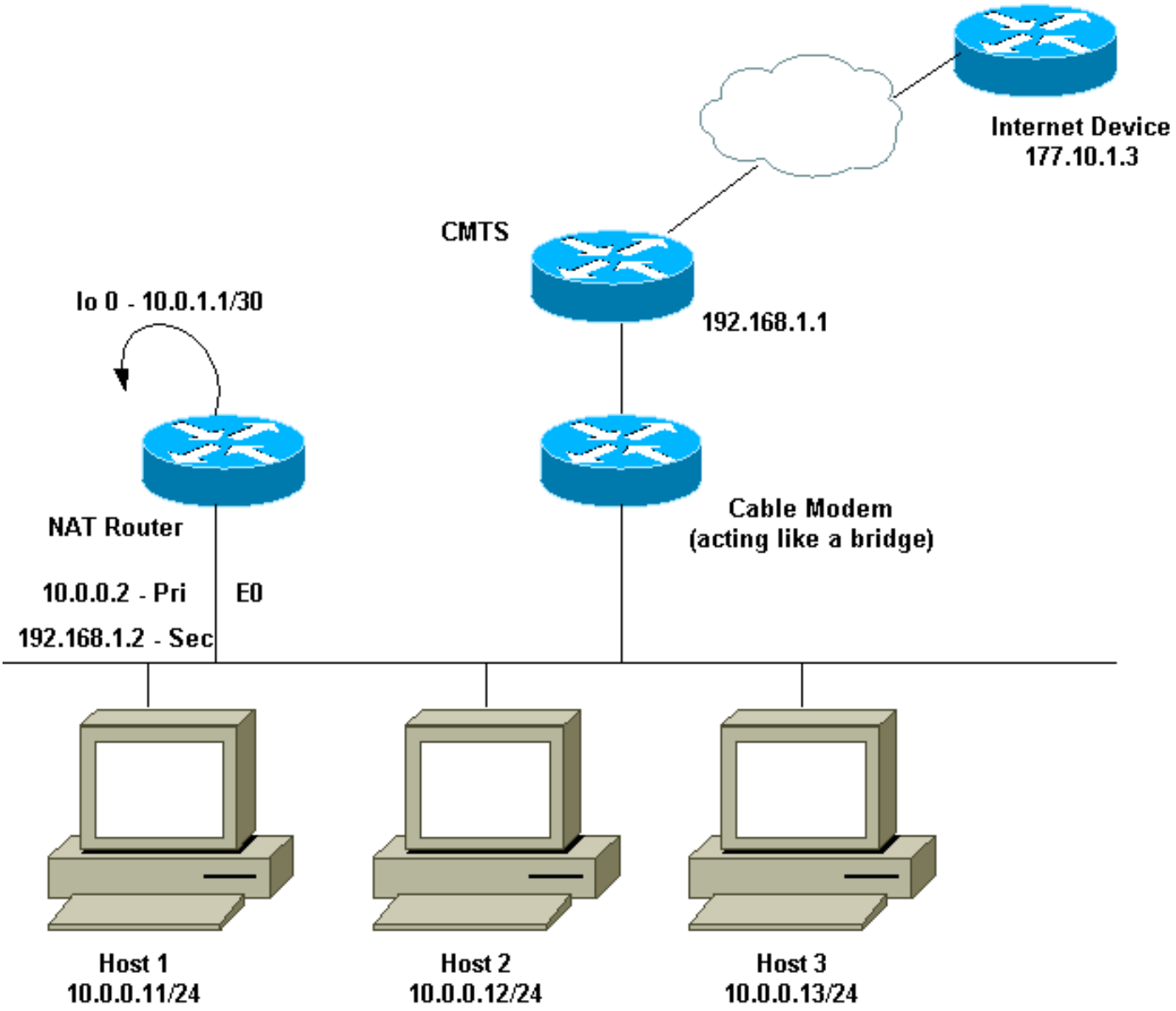
معلومات أساسية

in order for NAT أن يحدث، ربط ينبغي كنت حولت من nat "inside" يعين قارن إلى nat "خارجي" يعين قارن أو العكس. لم يتغير هذا متطلب ل NAT، غير أن هذا وثيقة يوضح كيف أنت يستطيع استعملت قارن ظاهري، خلاف ذلك يعرف باسم قارن الاسترجاع، وتحشد baser سياسة أن يجعل NAT يعمل على مسحاج تخديد مع قارن طبيعي وحيد.

وحاجة ال NAT على عصا نادرة. في الواقع، قد تكون الأمثلة الواردة في هذا المستند هي الحالات الوحيدة التي يلزم فيها هذا التكوين. على الرغم من ظهور مناسبات أخرى حيث يستخدم المستخدمون توجيه السياسة بالاقتران مع NAT، فإننا لا نعتبر هذا الأمر NAT على عصا لأن هذه الأمثلة لا تزال تستخدم أكثر من واجهة مادية واحدة.

مثال 1 شبكة رسم بياني وتكوين

الرسم التخطيطي للشبكة



الرسم التخطيطي للشبكة أعلاه شائع جدا في إعداد مودم الكبل. نظام توصيل المودم الكابلي (CMTS) هو موجه ومودم الكبل (CM) هو جهاز يعمل كجسر. المشكلة التي نواجهها هي أن موفر خدمة الإنترنت (ISP) لم يقدم لنا عناوين صحيحة كافية لعدد البيئات المضيفة التي تحتاج إلى الوصول إلى الإنترنت. أعطانا مزود خدمة الإنترنت (ISP) العنوان 192.168.1.2، والذي كان يجب إستخدامه لجهاز. بناء على طلب إضافي، إستلمنا ثلاثة مصادر أخرى — من 192.168.2.1 إلى 192.168.2.3 — يترجم إليها NAT البيئات المضيفة في النطاق 24/10.0.0.0.

المتطلبات

متطلباتنا هي:

- يجب أن تكون كافة الأجهزة المضيفة على الشبكة قادرة على الوصول إلى الإنترنت.
- يجب أن يكون المضيف 2 قادرا على الوصول إليه من الإنترنت بعنوان IP 192.168.2.1.
- نظرا لأنه يمكن أن يكون لدينا مضيفون أكثر من العناوين القانونية، فإننا نستخدم الشبكة الفرعية 24/10.0.0.0 للعنونة الداخلية الخاصة بنا.

لأغراض هذا المستند، نقوم فقط بإظهار تكوين موجه NAT. ومع ذلك، فنحن نذكر بعض ملاحظات التكوين المهمة فيما يتعلق بالأجهزة المضيفة.

تكوين موجه NAT

تکوین موجه NAT

```
                                                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
```

ملاحظة: تم تعيين البوابة الافتراضية لجميع الأجهزة المضيفة على 10.0.0.2، وهو موجه NAT. يجب أن يكون ل ISP بالإضافة إلى CMTS مسار إلى 29/192.168.2.0 يشير إلى موجه NAT لحركة المرور العائدة إلى العمل، لأن حركة المرور من البيئات المضيفة الداخلية تبدو وكأنها قادمة من هذه الشبكة الفرعية. في هذا المثال، سيقوم CMTS بتوجيه حركة مرور البيانات من 29/192.168.2.0 إلى 192.168.1.2 وهو عنوان IP الثانوي الذي تم تكوينه على موجه NAT.

مثال 1 عرض و debug أمر إنتاج

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

in order to شرحت أن التشكيل يعمل، نحن ركضت a few **عملية** أزيز إختبار بينما **ال debug** إنتاج على ال nat مسحاج تخديد monitore. يمكنك أن ترى أن أوامر **ping** ناجحة وأن يعرض إخراج **تصحيح الأخطاء** ما يحدث بالضبط.

ملاحظة: قبل إستخدام أوامر **debug**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

الاختبار الأول

في أول إختبار لنا، **نختبر** من جهاز في شبكة الإنترنت المعرفة في المختبر لدينا إلى المضيف 2. تذكر أن أحد المتطلبات كانت أن الأجهزة الموجودة في الإنترنت يجب أن تكون قادرة على الاتصال بالمضيف 2 بعنوان IP 192.168.2.1. فيما يلي إخراج **تصحيح الأخطاء** كما هو موضح على موجه NAT. كانت أوامر تصحيح الأخطاء التي كانت تعمل على موجه NAT هي **debug ip packet 177 detail** التي تستخدم **access-list 177**، و**debug ip nat**، و**debug ip policy** التي تعرض الحزم الموجهة نحو السياسة.

هذا هو المخرج من **العرض ip nat ترجمة** أمر تنفيذ على ال nat مسحاج تخديد:

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

من جهاز على الإنترنت، وفي هذه الحالة يكون أحد الموجهات، نقوم **بإختبار اتصال** 192.168.2.1 الذي يكون ناجحا كما هو موضح هنا:

```
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
```

لترى ما يحدث في الموجه NAT، ارجع إلى إخراج **تصحيح الأخطاء** هذا والتعليقات:

```
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

[رائزين]

أحد متطلباتنا الأخرى هو السماح للمضيفين بالتواصل مع الإنترنت. لهذا الاختبار، **نختبر** جهاز الإنترنت من المضيف 1. تكون أوامر **العرض** و**تصحيح الأخطاء** التالية.

مبدئيا ال nat ترجمة طاولة في ال nat مسحاج تخديد كما يلي:

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

بمجرد إصدار **إختبار الاتصال** من المضيف 1، نرى:

```
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#
```

نرى أعلاه أن **إختبار الاتصال** كان ناجحا. جدول NAT في موجه NAT يبدو الآن:

```
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
---                    ---                10.0.0.12          192.168.2.1 ---
                                                                #NAT-router
```

ال nat ترجمة يبدي طاولة أعلاه الآن ترجمة إضافي أي هو نتيجة ال حركي nat تشكيل (as opposed ال ساكن إستاتيكي nat تشكيل).

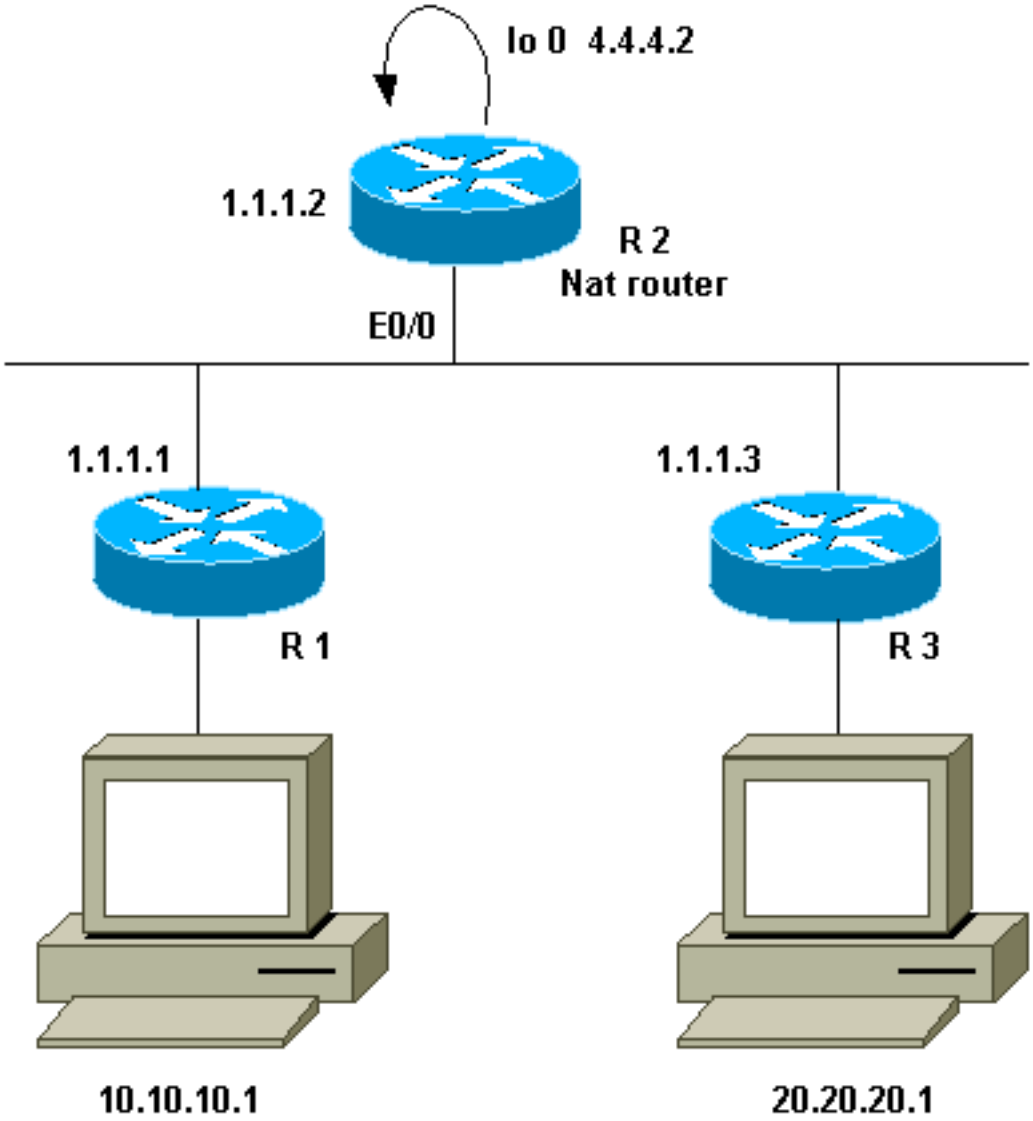
يعرض إخراج **تصحيح الأخطاء** أدناه ما يحدث على موجه NAT.

```
                                                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

مثال 2 شبكة رسم بياني وتكوين

الرسم التخطيطي للشبكة



المتطلبات

نريد أن تتصل أجهزة معينة خلف الموقعين (R1 و R3). يستخدم الموقعان عناوين IP غير مسجلة، لذلك يجب علينا ترجمة العناوين عند الاتصال ببعضها البعض. في حالتنا، تتم ترجمة المضيف 10.10.10.1 إلى 200.200.200.1 وسيترجم المضيف 20.20.20.1 إلى 100.100.1. لذلك نحتاج إلى ترجمة تحدث في كلا الاتجاهين. لأغراض المحاسبة، يجب أن تمر حركة المرور بين هذين الموقعين عبر R2. وخلاصة القول إن متطلباتنا هي:

- المضيف 10.10.10.1، خلف R1، يحتاج إلى الاتصال بالمضيف 20.20.20.1 خلف R3 باستخدام عناوينهم العالمية.
- يجب إرسال حركة المرور بين هذه الأجهزة المضيفة من خلال R2.
- بالنسبة لحالتنا، نحتاج إلى ترجمات NAT الثابتة كما هو موضح في التكوين أدناه.

تكوين موجه NAT

تكوين موجه NAT
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
```

مثال 2 عرض و debug أمر إنتاج

ملاحظة: يتم دعم بعض أوامر العرض بواسطة أداة مترجم الإخراج، والتي تتيح لك عرض تحليل إخراج أمر العرض. قبل إستخدام أوامر **debug**، ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء.

الاختبار الأول

كما هو موضح في التكوين أعلاه، لدينا ترجمتان ساكنتان ل NAT يمكن رؤيتها على R2 باستخدام الأمر **show ip nat ترجمة**.

هذا هو المخرج من **العرض ip nat ترجمة** أمر تنفيذ على ال nat مسحاج تخديد:

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
    20.20.20.1         100.100.100.1                ---                 --- ---
           ---                  ---         10.10.10.1       200.200.200.1 ---
R2#
```

لهذا الاختبار، تم الحصول على **إختبار اتصال** من جهاز (10.10.10.1) خلف R1 موجه للعنوان العام لجهاز (100.100.100.1) خلف R3. نتج عن تشغيل **debug ip nat** و**debug ip packet** على R2 هذا الإخراج:

```
                                                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
```

هذا هو المخرج كنتيجة لحزمة الاستجابة التي تم الحصول عليها من الجهاز الموجود خلف الموجه 3 الموجهة للجهاز الموجود خلف الموجه 1:

```
                                        [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
```

ملخص

أوضح هذا وثيقة كيف أن يستعمل ال nat و baser تحشد يستطيع كنت استعملت أن يخلق "nat على عصا" سيناريو. من المهم تذكر أن هذا التكوين يمكن أن يقلل الأداء على الموجه الذي يشغل NAT لأنه قد يتم تحويل الحزم من خلال الموجه.

معلومات ذات صلة

- صفحة دعم ترجمة عناوين الشبكة (NAT)

- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).