

使用动态NAT时避免路由循环

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[规则](#)

[示例 情景](#)

[相关信息](#)

简介

本文描述在NAT路由器和相邻路由器之间的信息包环路外部接口的，当使用动态网络地址转换的方案(NAT)时由于流量被注定的一个未使用IP地址在NAT池和一个默认路由出现在发送这些数据包的NAT路由器的回到外部。

先决条件

要求

本文档没有任何特定的要求。

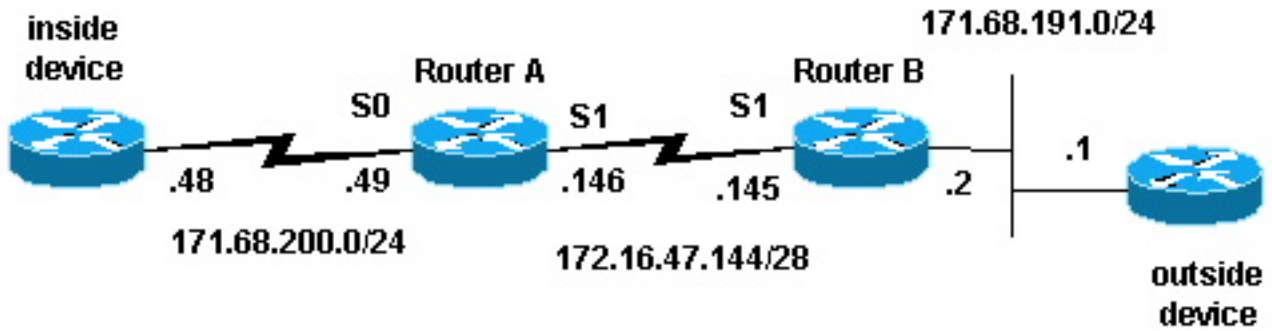
使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

网络图

以下拓扑用于创建示例情形。



规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

示例 情景

在上述拓扑， Router-A配置与NAT，以便转换从网络发出的数据包171.68.200.0/24对NAT池定义的地址范围“测试环路”。Router-A的配置如下(其他路由器配置以静态路由为了获取连接)：

```
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
```

使用NAT转换调试和IP数据包调试命令，我们生成从路由器的一ping在内部设备。ping工作的和转换表条目生成。在下面的输出中，我们看到调试的IP数据包和IP NAT调试打开，并且没有条目在转换表里此时。

注意： debug 命令会产生大量输出。只有 IP 网络上的流量较低时才能使用此类命令，以避免系统上的其他活动受到负面影响。

```
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#
```

内部路由器(内部设备)产生一ICMP数据包和171.68.200.48源地址和171.68.191.1一起(外部设备的地址目的地址)。**debug输出**以下表示与翻译对172.16.47.161的171.68.200.48源IP地址的一IP数据包。数据包在Serial0接口来和被注定Serial1接口。

```
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
```

debug输出以下表示与翻译回到171.68.200.48的172.16.47.161目的IP地址的回归IP数据包。数据包在Serial1接口来和被注定serial0接口。

```
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
```

debug输出显示在内部设备和外部设备之间的ping成功交换：

```
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
```

使用show ip nat translations命令，我们为内部设备在转换表里看到一个条目。

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

即然内部设备的一个转换在转换表里存在，我们能从外部设备顺利ping到内部设备的全局地址，如下面Router-A生成的debug输出所显示。

注意： 外部设备产生的数据包有171.68.191.1源地址和172.16.47.161 (内部全局地址目的地址在转换表里)。


```
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转换去从外向里在路由的数据包数据包前。在这种情况下，没有条目在转换表里，因此Router-A能唯一路由数据包。Router-A依靠其默认路由路由数据包，发送数据包取消Serial1接口，引起一条环路可能最终减少串行线路。

要避免这种路由环路，请勿产生从外部设备的数据包到内部全局地址。然而，因为这是很难强制执行，您能添加内部全局地址的静态路由与null0下一跳在Router-A的。这样，当一个外部设备发送为内部全局地址时注定的数据包，和那里是没有条目在转换表里，Router-A路由数据包对null0，避免环路。使用以上示例，静态路由看起来象以下：

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

[相关信息](#)

- [NAT 支持页](#)
- [IP 路由协议支持页](#)
- [IP 路由支持页](#)
- [技术支持 - Cisco Systems](#)