第15章　网络地址转换

本章主题

- NAT细节概述
- NAT术语
- 静态内部源地址转换
- 动态内部源地址转换
- 复用内部全局地址
- 转换重叠地址
- 目的地址轮流转换
- 改变转换超时时间长度
- 详细故障查找示例

15.1　引言

网络地址转换(NAT)是路由器提供的将一个IP地址转换为另一IP地址的功能，那些拥有私有（或没注册的）地址并想访问一个公共服务（用的是注册过的公用地址）的用户将需要地址的转换。本章讨论Cisco IOS提供的NAT功能。

15.1.1　NAT技术概述

Internet今天面临的最大的问题之一就是地址不够用的问题。而 NAT可以通过一定的方式缓解这方面的压力，即：允许一个组织重用全局的、唯一的、注册过的 IP地址（在其网络的另外一部分中）。

NAT使一个组织在多个域内重用注册过的 IP地址，只要离开该域以前将那些重用地址转换为全局的唯一注册IP地址即可。图15-1显示了基本的NAT工作原理。

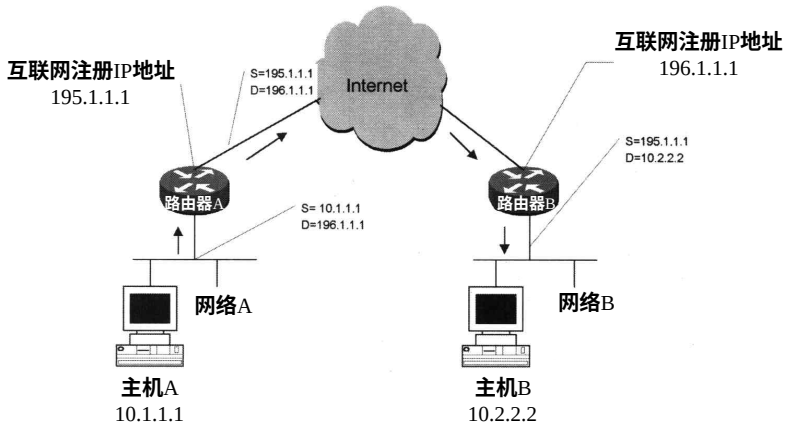

图15-1　网络地址转换(NAT)

两根网都用A类地址10.0.0.0作为它们的内部地址。每一组织都分配到一个 Internet注册过的唯一的C类地址，以在通信量想从专用内部网到外部公用网时用。

图15-1中，主机A（10.1.1.1）想向B（10.2.2.2）发送数据时，主机A用主机B的全局唯一地址196.1.1.1作为报文的目的地址。当报文到达路由器 A时，源地址10.1.1.1转换为全局唯一地址195.1.1.1。当报文到达路由器 B时，目的地址转为没注册的 IP地址10.2.2.2。相同道理，返回的报文也作相似的转换。

这些转换不需要对内部网络的主机进行附加配置。对主机 A来说，196.1.1.1是网络B上主机B（10.2.2.2）的IP地址。对B来说，195.1.1.1是网络A上的主机A（10.1.1.1）的IP地址。

15.1.2 NAT术语

当在Cisco路由器上应用NAT时，应理解下面的术语（见图15-2）。

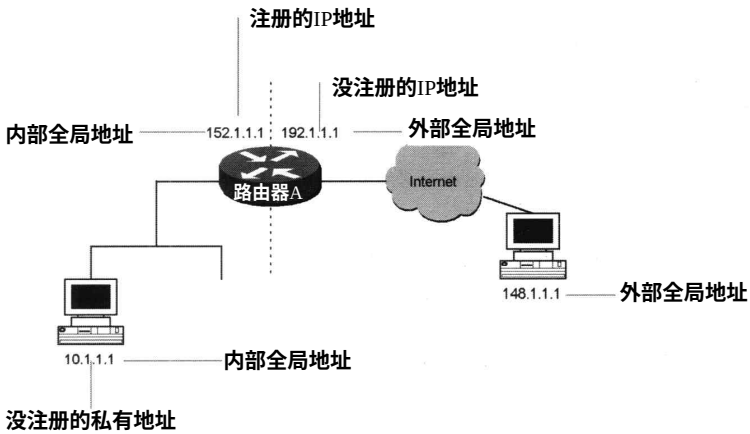

图15-2 NAT术语

- Inside local address：指在一个网络内部分配给一台主机的 IP地址。这个地址可能不是网络信息中心（NIC）或服务提供商分配的IP地址。
- Inside global address：用来代替一个或者多个本地 IP地址的、对外的、 NIC注册过的IP地址。
- Outside local address: 一个外部主机相对于内部网所用的 IP地址。不一定是合法的地址，但是，是从内部网可以进行路由的地址空间中进行分配的。
- outside global address：主机拥有者分配给在外部网络的一个 IP地址。它是从一个全局可路由地址或网络空间中分配的。

15.2 本章所讨论的命令

- **clear ip nat translations**
- **debug ip nat**
- **ip nat** {inside | outside}
- **ip nat inside destination list** {access-list-number | name} pool name
- **ip nat inside source** {list {access-list-number | name} pool name [overload] | static local-ip global-ip}

- **ip nat outside source** {list {access-list-number | name} pool name | static global-ip local-ip}
- **ip nat pool name** start-ip end-ip {netmask | prefix-length prefix-length} [type rotary]
- **ip nat translation** {timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout} seconds
- **show ip nat statistics**
- **show ip nat translations**

命令的定义

- clear ip nat：用来清除所有（或指定的）活动的 NAT转换。
- ip nat ：用来为发送报文（从内部）或接收（到外部）的接口应用 NAT。
- ip nat inside destination list：这条全局命令为内部目的地址应用 NAT。可以配置为动态的或静态的。
- ip nat inside source：这条全局命令为内部源地址应用NAT。可以配置为动态的或静态的。
- ip nat outside source：这条全局命令为外部源地址应用NAT。也可以配置为动态或静态的。
- ip nat pool name：这条全局命令定义一个IP地址池用来为网络转换，可以定义为内部全局池、外部本地池或旋转池。
- ip nat translation：NAT超时后，这个全局命令用来改变时间长。
- show ip nat statistics：用来显示关于NAT的统计数据。
- show ip nat translations：显示所有激活的NAT转换。

15.3 IOS 需求

在IOS 11.2中最先应用了NAT。

15.4 实验59：静态内部源地址转换

15.4.1 所需设备

下面列出了本实验所需设备：

1) 两台Cisco路由器各带一个以太网端口和一个串行口；
2) Cisco 11.2或更高；
3) 一台运行终端仿真程序的微机；
4) 一台带有以太网NIC的微机或有一以太网接口的路由器；
5) 两根以太网电缆和一个以太网集线器；
6) 一根Cisco DTE/DCE交叉电缆。

15.4.2 配置概述

本配置将演示NAT将一没注册的、内部IP地址转换为全局的、唯一的外部地址。如图 15-3所示，路由器A将把内部源地址10.1.1.1转换为全局唯一的地址195.1.1.1。

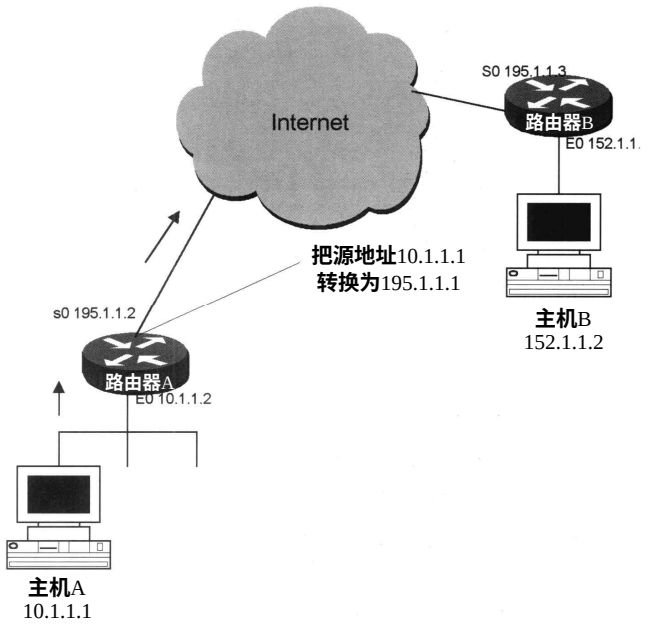

图15-3 内部源地址转换

路由器A和B通过交叉电缆串行连接，A作为DCE为B提供时钟，地址的分配如图15-4中所示。

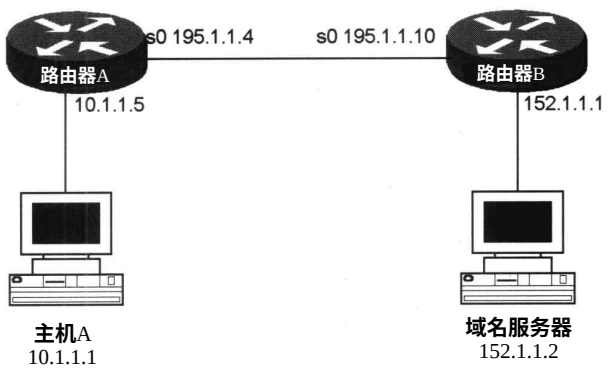

图15-4 内部源地址转换

一台带有一个以太网NIC的微机（或一台路由器）连到与路由器A相连的以太网上。路由器A配置了NAT，并将源IP地址10.1.1.1转换为195.1.1.1。

15.4.3 路由器配置

本例中两台路由器的配置如下所示：

1. 路由器A

```
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname routerA
```

```
!
ip nat inside source static 10.1.1.1 195.1.1.1←Translates the inside source
                                                address 10.1.1.1 to 195.1.1.1
!
interface Ethernet0
  ip address 10.1.1.2 255.255.255.0
 ip nat inside←Marks the interface as connected to the inside.
 !
interface Serial0
  ip address 195.1.1.2 255.255.255.0
 ip nat outside←Marks the interface as connected to the outside.
Clock rate 500000
 !
no ip classless
ip route 152.1.1.1 255.255.255.255 Serial0
!
line con 0
line vty 0 4
 login
!
end
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable password cisco
!
interface Ethernet0/0
  ip address 152.1.1.1 255.255.255.0
!
interface Serial0/0
 ip address 195.1.1.3 255.255.255.0
 !
line con 0
line aux 0
line vty 0 4
 password cisco
 login
```

15.4.4 监测配置

从主机A ping主机B（152.1.1.2）。用debug ip packet命令分析到达路由器B的报文。命令执行结果如下，注意ICMP ping报文的源地址是195.1.1.1。

```
IP: s=195.1.1.1 (Serial0/0), d=152.1.1.1, len 104, rcvd 4←ICMP ECHO
IP: s=152.1.1.1 (local), d=195.1.1.1 (Serial0/0), len 104←ICMP ECHO REPLY
```

在路由器A上执行debug ip nat命令可以看出源IP地址10.1.1.1已转换为195.1.1.1，这是个两部过程。而返回报文的到195.1.1.1的目标地址也转回到10.1.1.1了。

```
NAT: s=10.1.1.1->195.1.1.1, d=152.1.1.1 [2542]
NAT*: s=152.1.1.1, d=195.1.1.1->10.1.1.1 [2542]
```

以前，我们曾讨论了在一内部本地地址和一内部全局地址之间的一对一的映射。这个方

法是低效的且不能推广。因为一个 IP地址只能让一个端主机使用。静态转换经常在一个固定的外部的IP地址访问一内部主机的情况下使用。

图15-5给出了一个需要静态地址映射的示例。

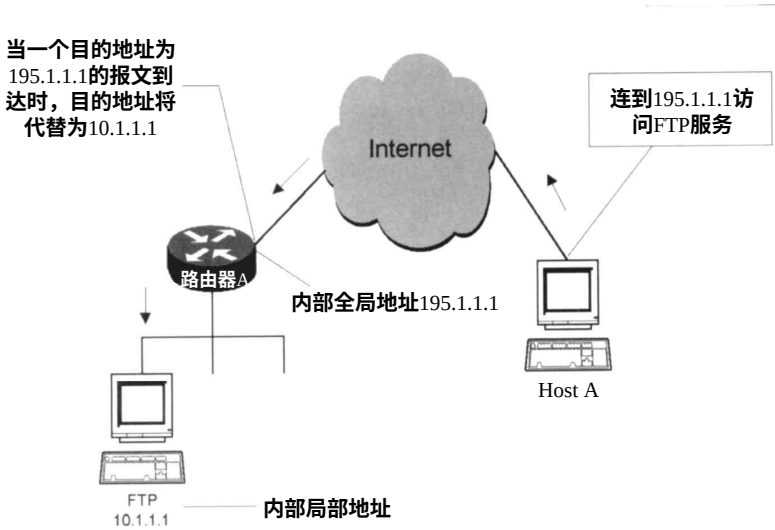

图15-5 静态路由映射

主机A想访问FTP服务器上的文件，然而 FTP服务器属于内部网络，没有一个唯一的全局IP地址，这时就需要定义一个全局地址 195.1.1.1到本地地址 10.1.1.1的静态映射。

15.5 实验60：动态内部源地址转换

15.5.1 所需设备

下面列出了本实验所需设备：

1) 两台Cisco路由器，各带一个以太网端口和一串行口；
2) Cisco IOS 11.2或更高的；
3) 一台运行终端仿真程序的微机；
4) 一根Cisco DTE/DCE交叉电缆。

15.5.2 概述

另外一种内部地址转换是动态转换，这种方法在一组内部本地地址与一个全局地址池之间建立一种映射关系。这种转换在有很多没有注册的主机想访问离线服务时非常有用。

动态内部地址转换用一个预定义地址池动态地将没注册的 IP地址转换为注册过的IP地址。这种关系是一对一的。当有一外部连接请求时，从池中取出一个 IP地址用。而一旦连接断开，取出的全局IP地址将重新放入池中，以供其他的连接使用。动态转换效率是非常高的，因为一个注册过的IP地址可以让多个不同的端站点使用多次。相反前面定义的静态转换，只能让一个特定的端站点使用。

图15-6表明局域网上的三台工作站都想访问外部网络。当报文到达路由器 A时，用前面定

义的地址池将报文源地址转换为 Internet注册过的地址。这个过程仍含有一对一的映射。需要为每一台想与外面网络通信的工作站分配一注册过的 IP地址。然而，并不是所有主机都要同时通信。例如，根据通信量模式， 10个注册过的IP地址可以为40台PC用。

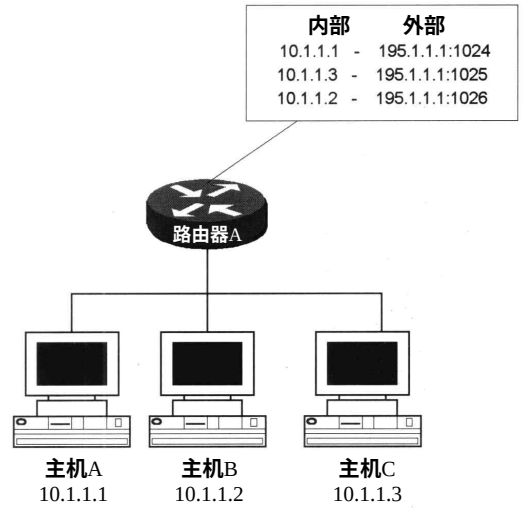

图15-6 动态地址转换

注意 虽然动态地址转换是高效的并易于管理，但外部用户并不能访问内部地址，因为它们之间没有静态映射，当每一个会话结束时，注册过的IP地址仍放入到池中以供其他会话用。当一端主机每次建立一个新连接时，都很可能分配到不同于上次的全局地址，因此，不可能用一个全局地址访问一内部特定的地址。

15.5.3 配置概述

本配置将演示内部源地址到外部全局地址之间的动态转换。路由器 A将把在10.1.1.1与10.1.1.3之间的任一源地址转换为在地址池中的三个全局地址之一。

两台Cisco路由器串行连接。路由器 A通过交叉电缆连接到路由器 B。路由器 B作为DCE为A提供时钟。一台运行终端仿真程序的微机连到路由A上的控制台端口上。IP地址的分配如图15-7所示。

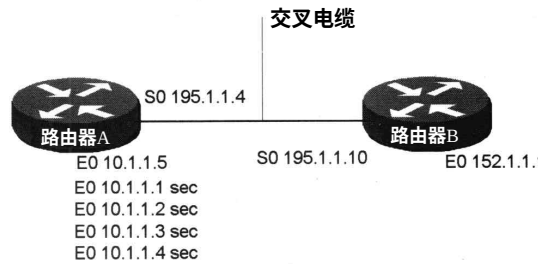

图15-7 动态地址转换

路由器A配置给NAT，将动态转换访问表1指定的范围内的任何内部源地址到一个 Internet注册过的唯一的全局地址。

15.5.4 路由器配置

下面列出本例中两台路由器配置：

1. 路由器A

```
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname routerA
!
                    ↓Name of the pool
ip nat pool globalpool 195.1.1.1 195.1.1.3 netmask 255.255.255.0←Defines the pool
                                                                  of address
                              List 1 reference access-list 1 and defines which
                         ↓addresses will be translated
ip nat inside source list 1 pool globalpool←Globalpool references the pool of
                                            addresses defined in the previous line.
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0 secondary
```

```
 ip address 10.1.1.2 255.255.255.0 secondary
 ip address 10.1.1.3 255.255.255.0 secondary→Secondary IP addresses are used
                                              as test points
 ip address 10.1.1.4 255.255.255.0 secondary
 ip address 10.1.1.5 255.255.255.0
 ip nat inside→Defines the inside interface
!
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip nat outside→Defines the outside interface
!
no ip classless
ip route 152.1.1.1 255.255.255.255 Serial0
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.3
access-list 1 permit 10.1.1.1→Access list 1 defines which inside source
                              addresses will be translated
access-list 1 permit 10.1.1.4
!
line con 0
line vty 0 4
 login
!
end
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable password cisco
!
interface Ethernet0/0
  ip address 152.1.1.1 255.255.255.0
!
interface Serial0/0
 ip address 195.1.1.10 255.255.255.0
 clock rate 500000←Defines the clock rate for the DCE interface

 !
line con 0
line aux 0
line vty 0 4
 password cisco
 login
```

15.5.5 监测配置

在路由器A上，用扩展ping命令测试配置。这条命令可以从路由器中任何现存的 IP地址中为ping报文找其源地址。只需在特权级状态下键入 ping即可。

```
routerA#ping
Protocol [ip]:
Target IP address: 152.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]:
```

```
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
```

下面的例子都是在路由器A上用扩展ping命令从在配置中定义的二级IP地址为报文源路。用这个方法代替路由器A的局域网上的多个微机。

1) 从路由器A，用源地址10.1.1.2 ping 152.1.1.1。

2) 从路由器A，用源地址10.1.1.1 ping 152.1.1.1。

3) 从路由器A，用源地址10.1.1.3 ping 152.1.1.1。

从在路由器A上执行debug ip nat 命令的结果，得知源地址10.1.1.2转换为195.1.1.1（池中的第一个地址）。池中的全局IP地址按请求的顺序分配。

```
NAT: s=10.1.1.2->195.1.1.1, d=152.1.1.1 [20]
NAT: s=10.1.1.1->195.1.1.2, d=152.1.1.1 [25]
NAT: s=10.1.1.3->195.1.1.3, d=152.1.1.1 [35]
```

在路由器A上执行debug ip nat translation命令显示了当第4台端站点想访问外面的网络时，所发生的情况，但是池中的所有地址都用完了。

```
NAT: translation failed (L), dropping packet s=10.1.1.4 d=152.1.1.1
```

从上面的各例中得知，虽然动态地址转换比静态转换效率更高，但每一转换仍需要自己的地址。因此，网络管理者必须正确地掌握离线访问的通信量并相应地定义地址池的大小。

15.6 实验61：复用内部全局地址

15.6.1 所需设备

下面列出了本实验所需设备：

1) 两台Cisco路由器，各带一个以太网端口和一个串行口；

2) Cisco IOS 11.2或更高的；

3) 一台运行终端仿真程序的微机；

4) 一根Cisco DTE/DCE交叉电缆。

15.6.2 概述

Cisco IOS可以复用全局地址，因此就避免了在本地地址与全局地址之间的一对一映射需求。IOS的这个特性大大地减少了所需注册IP地址的数目。

当地址复用被应用时，路由器在高层协议（如TCP或UDP端口号）维持足够的信息，以将全局地址转换为正确的本地地址。当多个本地地址映射到同一个全局地址时，TCP或UDP端口号将用来区别不同的本地地址。

图15-8中，所有局域网上的本地地址都被转换为全局地址195.1.1.1。路由器为每一个转换复用一个内部全局地址，而用TCP或UDP端口号区别各个不同的端主机。

当复用地址时，路由器A将采取下列步骤：

1) 在Internet上，主机A（10.1.1.1）与主机152.1.1.1建立一个连接。

2) 路由器收到的第一个从主机A来的报文使路由器检查它的NAT表。

3) 如果不存在转换，则路由器A用全局195.1.1.1代替报文源地址。

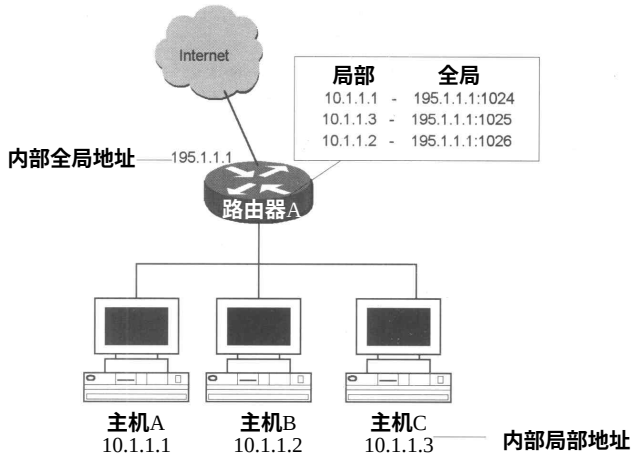

图15-8 复用一个内部全局地址

4) 当路由器收到一从主机152.1.1.1到195.1.1.1的报文后，路由器用协议建立一个NAT表、内部全局地址和端口号、外部地址和端口号作为关键字，根据这些关键字，路由器A能够把目的地址195.1.1.1转换为内部本地地址10.1.1.1，并把报文转发到主机10.1.1.1。

在路由器A上执行show ip nat translations命令，注意地址后的端口号，内部局域地址后的端口号1029是主机A选择的暂时端口。而外部地址后跟的端口号23是众所周知的Telnet端口。

```
routerA# show ip nat translations

Pro I    inside global     Inside local       Outside local      Outside global
icmp     195.1.1.1:256      10.1.1.1:256       152.1.1.1:256      152.1.1.1:256
tcp      195.1.1.1:1029     10.1.1.1:1029      152.1.1.1:23       152.1.1.1:23
```

15.6.3 配置概述

本配置将演示复用一个外部全局地址，路由器A将把在10.1.1.1到10.1.1.3之间的任何源地址转换为全局地址195.1.1.1。

两台路由器串行连接。路由器A用交叉电缆连到路由器B上，B作为DCE为路由器A提供时钟。一台远程终端仿真程序的微机连到路由器A的控制台端口。所有IP地址的分配如图15-9中所示。

路由器A上应用了NAT，将动态地把任一指定的内部源地址转换为唯一的、注册的全局地址195.1.1.1。

图15-9 复用一内部全局地址

15.6.4 路由器配置

本例中的两台路由器的配置如下所示：

1. 路由器A

```
version 11.2
no service udp-small-servers
no service tcp-small-servers
```

```
!
hostname routerA
!
                        ↓Name of the pool
ip nat pool globalpool 195.1.1.1 195.1.1.1 netmask 255.255.255.0←Defines range of
                                                                  pool; in this
                                                                  case, there is
                                                                  only one address
                                                                  in the pool
                              List 1 references access list 1 and defines which
                        ↓address will be translated.
ip nat inside source list 1 pool globalpool overload←Allows multiple inside
!                                    ↑Defines what     local addresses to be
                                      global address   translated to one
                                      to use           outside global address.
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.1.1.2 255.255.255.0 secondary
 ip address 10.1.1.3 255.255.255.0 secondary→Secondary IP addresses are used
                                              as test points.
 ip address 10.1.1.4 255.255.255.0 secondary
 ip address 10.1.1.5 255.255.255.0
 ip nat inside→Defines the inside interface
!
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip nat outside←Defines the outside interface
 !
no ip classless
ip route 152.1.1.1 255.255.255.255 Serial0
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.3
access-list 1 permit 10.1.1.1→Access list 1 defines which inside source
                               addresses that will be translated
access-list 1 permit 10.1.1.4
!
line con 0
line vty 0 4
 login
!
end
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable password cisco
!
interface Ethernet0/0
  ip address 152.1.1.1 255.255.255.0
!
interface Serial0/0
 ip address 195.1.1.10 255.255.255.0
clock rate 500000
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
```

15.6.5 监测配置

在路由器A上用扩展ping命令ping主机B（195.1.1.3）。从10.1.1.1和10.1.1.2为报文源路。用debug ip nat 监视转换。

下面给出命令的输出，注意内部源地址 10.1.1.1和10.1.1.2都已转换为 195.1.1.1。

```
NAT: s=10.1.1.1->195.1.1.1, d=195.1.1.3 [5]
NAT: s=10.1.1.2->195.1.1.1, d=195.1.1.3 [10]
```

现在，用show ip nat translations命令显示NAT表。其执行结果如下：注意每一地址后所带的端口号，这些端口号及地址将作为关键字把返回的报文映射到正确的内部本地 IP地址。

```
RouterA#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 195.1.1.1:9       10.1.1.2:4         195.1.1.3:4        195.1.1.3:9
icmp 195.1.1.1:8       10.1.1.2:3         195.1.1.3:3        195.1.1.3:8
icmp 195.1.1.1:7       10.1.1.2:2         195.1.1.3:2        195.1.1.3:7
icmp 195.1.1.1:6       10.1.1.2:1         195.1.1.3:1        195.1.1.3:6
icmp 195.1.1.1:5       10.1.1.2:0         195.1.1.3:0        195.1.1.3:5
```

15.7 实验62：重叠地址转换

15.7.1 所需设备

下面列出了本实验所需设备：

1) 两台Cisco路由器，各带一个以太网端口和一串行端口；
2) Cisco IOS 11.2或更高的；
3) 一台运行终端仿真程序的微机；
4) 两台带有以太网卡的微机，其中一台微机应运行服务器 DNS守护进程；
5) 四根以太网电缆和两个以太网集线器及一个 Cisco DTE/DCE交叉电缆。

15.7.2 概述

当一个内部本地地址与所想连接的外部地址相同时，就发生了地址重叠。如图 15-10所示，

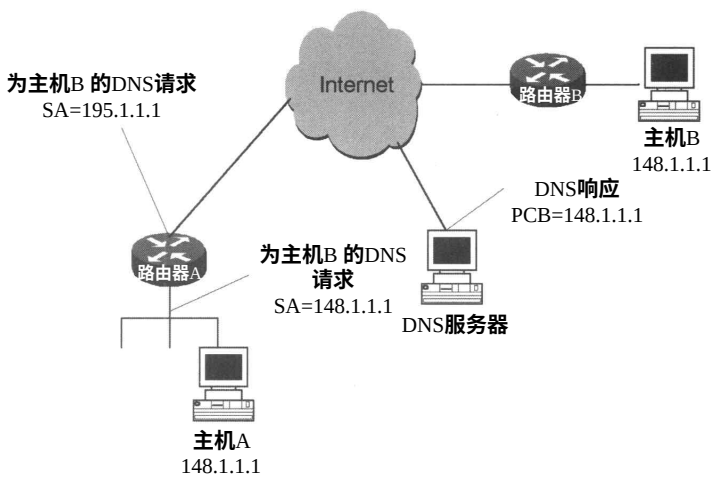

图15-10 IP地址重叠

主机A（148.1.1.1）用主机B的主机名同B建立一连接，这需要查询DNS服务器进行主机名到主机地址的转换。而DNS服务器就给出了主机B的地址148.1.1.1，则内部本地地址与外部地址发生了重叠。

Cisco IOS解决这一问题的方法是将外部全局地址转换为外部本地地址。

路由器A将采取以下步骤：

1) 主机A用主机B的主机名请求与B建立一个连接，这时一个主机名到地址的转换请求送往DNS服务器。

2) DNS服务器有回应，把主机B的地址148.1.1.1返回。

3) 路由器A截取报文并从外部本地地址池中选择一个外部本地地址代替源地址。

4) 路由器A同时维持一张全局地址到外部本地地址的一张映射表。

5) 当主机A向主机B发送报文时，目的IP地址就是外部本地地址。

6) 而当路由器A收到目的为外部本地地址的报文时，就把本地地址转换为全局地址。

在路由器A上执行show ip nat translations命令，结果如下。外部全局地址148.1.1.1映射到外部本地地址2.2.2.2。

```
routerA#show ip nat translations

Pro   Inside global      Inside local       Outside local      Outside global
--- ---                  --                 2.2.2.2            148.1.1.1
tcp   195.1.1.1:1071     10.1.1.1:1071      148.1.1.1:23       148.1.1.1:23
```

15.7.3 配置概述

本配置将演示外部全局地址转换，路由器A监视所有的DNS回应，如果发生了与内部本地地址重叠的话（10.1.1.1），路由器A就把DNS查询的地址转换为2.2.2.2。

两台路由器串行连接。路由器 A通过转接电缆连到B上。B作为DCE为A提供时钟，一台运行终端仿真程序的微机连到了B的控制台端口。所有IP地址的分配如图15-11所示。

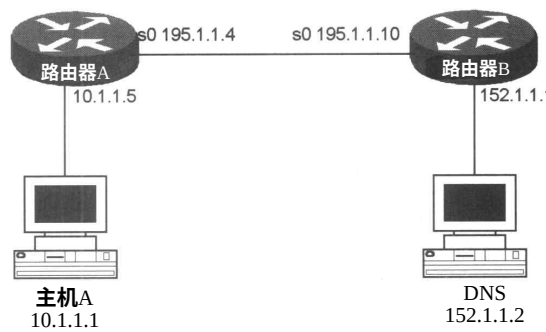

图15-11 IP 地址重叠

主机A配置为一缺省的到10.1.1.5和DNS的入口项：152.1.1.2。路由器A上应用NAT并将监视所有的DNS回应，如果DNS转换的地址与10.1.1.1发生重叠，将静态地把它转换为2.2.2.2。

第二个工作站配置为DNS，它将完成主机名到地址的转换。

15.7.4 路由器配置

下面的配置在外部全局地址10.1.1.1和外部本地地址2.2.2.2之间定义一个静态映射。

1. 路由器A

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname routerA
!
```

```
!
ip nat pool globalpool 195.1.1.1 195.1.1.3 netmask 255.255.255.0
ip nat inside source list 1 pool globalpool overload
ip nat outside source static 10.1.1.1 2.2.2.2←Defines translation from the outside
                                               global address 10.1.1.1 to the outside
                                               local address of 2.2.2.2
!
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0 secondary
 ip address 10.1.1.3 255.255.255.0 secondary
 ip address 10.1.1.4 255.255.255.0 secondary
 ip address 10.1.1.5 255.255.255.0
 ip nat inside←Defines the inside interface
 !
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip nat outside←Defines the outside interface
 !
no ip classless
ip route 152.1.1.1 255.255.255.255 Serial0
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.3
access-list 1 permit 10.1.1.1
access-list 1 permit 10.1.1.4
!
line con 0
line vty 0 4
 login
!
end
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable password cisco
!
interface Ethernet0/0
   ip address 152.1.1.1 255.255.255.0
!
interface Serial0/0
 ip address 195.1.1.10 255.255.255.0
clock rate 500000
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
```

下面的配置在一个外部本地地址池与访问表定义的一组外部全局地址之间定义动态的映射关系。

1. 路由器A

```
Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname routerA
```

```
!
!ip nat pool globalpool 195.1.1.1 195.1.1.3 netmask 255.255.255.0
                    ↓Pool Name
ip nat pool outsidelocal 2.2.2.1 2.2.2.4 netmask 255.255.255.0
                          ↑Pool Range
ip nat inside source list 1 pool globalpool overload

                                  ↓References the outside local pool
ip nat outside source list 2 pool outsidelocal←(If the outside global source
                          ↑Specifies what       address matches access list 1
                           addresses should     change to one of the addresses
                           be changed           defined in pool outsidelocal)
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.1.1.2 255.255.255.0 secondary
 ip address 10.1.1.3 255.255.255.0 secondary
 ip address 10.1.1.4 255.255.255.0 secondary
 ip address 10.1.1.5 255.255.255.0
 ip nat inside←Defines the inside interface
 !
interface Serial0
 ip address 195.1.1.4 255.255.255.0
 ip nat outside←Defines the outside interface
 !
no ip classless
ip route 152.1.1.1 255.255.255.255 Serial0
access-list 2 permit 10.1.1.1
access-list 2 permit 10.1.1.2←If the outside global source address matches one
                              of these changes
access-list 2 permit 10.1.1.3
access-list 2 permit 10.1.1.4
no cdp run
!
line con 0
line vty 0 4
 login
!
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable password cisco
!
interface Ethernet0/0
  ip address 152.1.1.1 255.255.255.0
!
interface Serial0/0
 ip address 195.1.1.10 255.255.255.0
clock rate 500000
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
```

15.7.5 监测配置

用域名从主机A ping**主机**B，**用**debug ip nat **和**show ip nat translations**命令验证转换是否正常。**

Debug ip nat命令的输出如下。注意DNS回应已转换为2.2.2.2。

```
r3#deb ip nat
01:04:23: NAT: i: udp (10.1.1.1, 1082) -> (10.10.3.111, 53) [62735]
01:04:23: NAT: s=10.1.1.1->195.1.1.1, d=10.10.3.111 [62735]
01:04:23: NAT: o: udp (10.10.3.111, 53) -> (195.1.1.1, 1082) [9227]
01:04:23: NAT: DNS resource record 10.1.1.1 -> 2.2.2.2
01:04:23: NAT: s=10.10.3.111, d=195.1.1.1->10.1.1.1 [9227]
01:04:23: NAT: o: icmp (10.1.1.100, 256) -> (10.1.1.1, 256) [21]
01:04:24: NAT: o: icmp (10.1.1.100, 256) -> (10.1.1.1, 256) [22]
01:04:25: NAT: o: icmp (10.1.1.100, 256) -> (10.1.1.1, 256) [23]
01:04:26: NAT: o: icmp (10.1.1.100, 256) -> (10.1.1.1, 256) [24]
```

路由器A上的show ip translation命令的输出如下。注意重叠的外部全局地址 10.1.1.1已转换为2.2.2.2。

```
r3#show ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
--- 195.1.1.1         10.1.1.1           ---                ---
--- ---               ---                2.2.2.2            10.1.1.1
```

15.8 实验63：目的地址轮流转换

15.8.1 所需设备

下面列出了本实验所需设备：

1) 两台Cisco路由器，各带一个以太网端口和一串行端口；
2) Cisco IOS 11.2或更高的；
3) 一台运行终端仿真程序的微机；
4) 一根Cisco DTE/DCE交叉电缆。

15.8.2 概述

网络地址轮流转换可以作为一种提供在多个、利用率高的主机之间进行分担负载的方法。图15-12说明了这个特征：

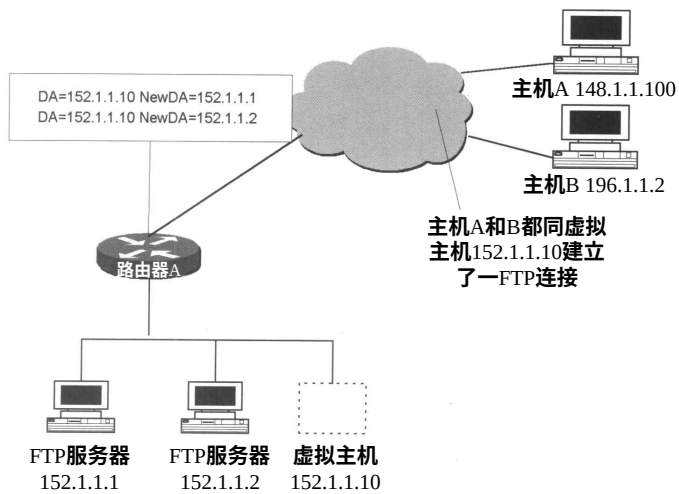

图15-12 用NAT平衡负载

例如：X公司的多个FTP服务会被许多客户访问以下载软件。 NAT转换对用户是透明的。他们只是FTP到虚拟IP地址152.1.1.10。

当路由器A收到目的地址为虚拟IP地址的报文时，它把目的地址转换到第一个FTP服务器。而当又有一到虚拟IP地址的FTP连接建立时，路由器就把目的地址转换到第二个 FTP服务器。假设多个FTP服务器负载平衡的话，那些转换按轮换模式进行。

路由器A进行转换时，采取下列步骤：

1) 主机A（148.1.1.100）与虚拟主机（152.1.1.10）建立一连接。

2) 路由器A收到虚拟主机为152.1.1.10的报文，从池中把目的地址转换为下一个的真实主机（本例中，FTP服务器152.1.1.1）。

3) FTP服务器152.1.1.1收到报文并回应。

4) 路由器A收到从FTP服务器来的回应报文，然后用内部本地地址和端口号进行 NAT表查询（同时也用外部地址和端口号作为关键字）。

5) 路由器然后把源地址转换为虚拟主机地址并转发报文。

6) 主机B（196.1.1.2）与虚拟主机152.1.1.10之间建立连接。

7) 路由器A收到目的地址为虚拟主机152.1.1.10的报文，并把目的地址转换为池中的下一个真实主机地址（本例中，FTP服务器152.1.1.2）。

8) 路由器A收到从FTP服务器来的回应报文然后进行NAT查询，把源地址转换为虚拟地址，转发报文。

15.8.3 配置概述

本配置将演示用目的地址轮流转换的方法进行负载共享。路由器 A将用池中的真实主机地址代替与访问表2匹配的任何报文的目的地址。

池定义真实主机地址，访问表定义虚拟地址。如果还没有存在一个转换，从 serial 0（外部接口）来的、目的地址与访问表2匹配的TCP报文将被转换为池中的一个真实地址。

路由器A和B通过交叉电缆串行连接，路由器B作为DCE，给路由器A提供实钟。IP地址分配如图15-13所示。第二级IP地址只作为测试点用于路由器A。

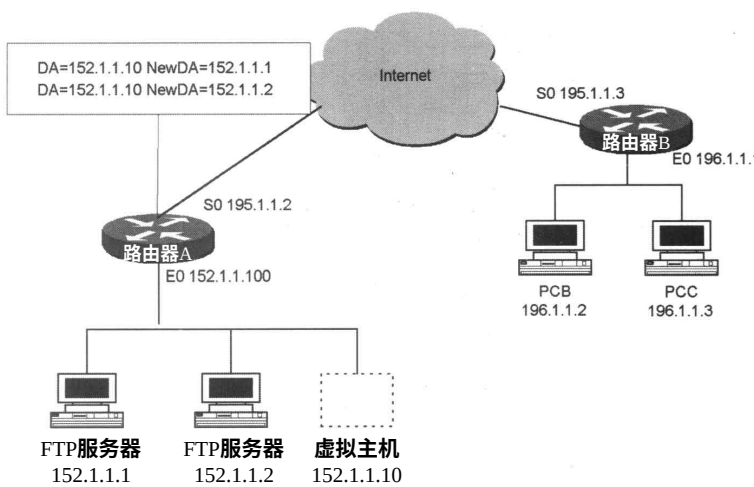

图15-13 目的地址轮流转换

路由器A配置用于目的地址轮流转换。从主机B telnet到虚拟主机152.1.1.10。配置二级IP地址代替多台离线主机。路由器A也将配置VTY会话，从而与其上的二级IP地址建立telnet会话。

15.8.4 路由器配置

下面给出本例中两台路由器的配置（路由器 A的关键配置用黑体标示）。

1. 路由器A

```
Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterA
!
!                                                                    Defines
                                                                     the pool
                    ↓Pool Name      ↓Pool Range                    ↓as rotary
ip nat pool loadsharing 152.1.1.1 152.1.1.2 prefix-length 24 type rotary
ip nat inside destination list 2 pool loadsharing←If the destination address
!                                ↑References access     matches access list 2,
                                  list 2                replace with an IP
                                                        address  from pool
                                                        "loadsharing."
!
interface Ethernet0
 ip address 152.1.1.1 255.255.255.0 secondary←Secondary IP address used for
                                              test point
ip address 152.1.1.2 255.255.255.0 secondary←Secondary IP address used for
                                             test point
ip address 152.1.1.100 255.255.255.0
 ip nat inside←Defines the inside interface
!
interface Serial0
 ip address 195.1.1.2 255.255.255.0
 ip nat outside←Defines the Outside interface
!
no ip classless
access-list 2 permit 152.1.1.10←Defines what destination address will be
                                 translated
!
line con 0
line vty 0 4
 password cisco←Sets the VTY password to cisco
 login←Allows telnet access into the router
!
end
```

2. 路由器B

```
Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable password cisco
!
!
interface Ethernet0/0
  ip address 196.1.1.1 255.255.255.0
 !
```

```
interface Serial0/0
 ip address 195.1.1.3 255.255.255.0
 clockrate 500000←Acts as DCE, providing clock
```

15.8.5 监测配置

1) **在路由器A上，执行**debug ip nat**命令。**

2) **在路由器B上，**telnet**到**152.1.1.10**。下面例子给出**debug ip nat**命令的输出。第一行是目的地址**152.1.1.10**到池的第一个地址的转换。下一行是从** 152.1.1.1**返回的报文，注意路由器** A **是在转发报文到**B**之前进行源地址到虚拟**IP**地址**152.1.1.10**的转换的。**

```
NAT: s=195.1.1.3, d=152.1.1.10->152.1.1.1 [0]
NAT: s=152.1.1.1->152.1.1.10, d=195.1.1.3 [0]
```

3) **在路由器B上再次**telnet**到**152.1.1.10**。**

下面是debug ip nat **（在A上执行）的输出。注意，这次目的地址** 152.1.1.10**转换到池中的第二个地址（**152.1.1.2**）。**

```
NAT: s=195.1.1.3, d=152.1.1.10->152.1.1.2 [0]
NAT: s=195.1.1.3, d=152.1.1.10->152.1.1.2 [0]
```

4) **在路由器A，用**show ip nat translations**命令显示**NAT**表。下面给出其输出。注意每一个地址后的端口号。这个端口号将和协议类型一起作为转换返回报文地址的关键词。**

```
Pro Inside global      Inside local       Outside local      Outside global
tcp 152.1.1.10:23      152.1.1.2:23       195.1.1.3:26658    195.1.1.3:26658
tcp 152.1.1.10:23      152.1.1.1:23       195.1.1.3:26146    195.1.1.3:26146
```

15.9 改变转换超时

在一段不用时间之后，动态转换将会超时，缺省设置是：没有配置复用的简单转换将在24**小时之后超时。在全局配置模式下用下面的命令可以改变计时长度。**

```
ip nat translation timeout { seconds}←Command changes the timeout value for
                                      dynamic address translations that do not
                                      use overloading
```

当配置地址复用时，Cisco IOS**有更好的改变超时的方法，每一个入口项都含有用这个入口项的通信量的信息，**UDP、TCP、DNS**和完成计时器可以用下面的全局配置命令改变。**

```
ip nat translation udp-timeout {seconds}←Changes the UDP timeout value. The
                                         default is five minutes.
ip nat translation dns-timeout {seconds}←Changes the DNS timeout value. The
                                         default is one minute.
ip nat translation tcp-timeout (seconds)←Changes the TCP timeout value (the
                                         default is 24 hours)
ip nat translation finrst-timeout (seconds)←Changes the finish and reset
                                            timeouts; the default is one minute
```

15.10 NAT故障查找

Cisco IOS **为**NAT**故障查找提供了许多工具，其中的一些命令及相应的输出采样，在下面给出。**

show ip nat statistics **这个命令显示正在使用的转换的个数，及已经终止的转换的个数。一个已终止的转换是指这个转换已有一段时间没有用，并且已从表中给删掉了。本命令也显**

示内部和外部配置的接口。

```
RouterA#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet0
Hits: 20  Misses: 20
Expired translations: 20
Dynamic mappings:
-- Inside Source
access-list 1 pool pool refcount 0
pool pool: netmask 255.255.255.0
        start 195.1.1.1 end 195.1.1.1
        type generic, total addresses 1, allocated 0 (0%), misses 0
```

show ip nat translations 这条命令显示所有应用的转换：报文的转换协议、内部本地地址、内部全局地址、外部本地地址、外部全局地址。

从下面的输出，不难看出一个带有内部本地地址 10.1.1.1的ping报文（协议ICMP）已被转换为内部全局地址 195.1.1.1。地址之后是端口号，以用来区分不同的转换，因为路由器配置了地址复用。

```
RouterA#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 195.1.1.1:4       10.1.1.1:4         195.1.1.3:4        195.1.1.3:4
icmp 195.1.1.1:3       10.1.1.1:3         195.1.1.3:3        195.1.1.3:3
icmp 195.1.1.1:2       10.1.1.1:2         195.1.1.3:2        195.1.1.3:2
icmp 195.1.1.1:1       10.1.1.1:1         195.1.1.3:1        195.1.1.3:1
icmp 195.1.1.1:0       10.1.1.1:0         195.1.1.3:0        195.1.1.3:0
```

show ip nat translations verbose 这个命令是上一命令的扩展，显示一些更详细的信息，主要是关于这个转换已创建了多长时间，最后一次使用是在什么时候。

从下面的输出可以看出，这个转换是在 1分31秒前创建的，最后一次使用在 31秒前。

```
RouterA#show ip nat translations verbose
Pro  Inside global    Inside local    Outside local     Outside global
icmp 195.1.1.1:4      10.1.1.1:4      195.1.1.3:4       195.1.1.3:4
     create 00:01:31, use 00:00:31, left 00:00:28, flags: extended
icmp 195.1.1.1:3      10.1.1.1:3      195.1.1.3:3       195.1.1.3:3
     create 00:00:31, use 00:00:31, left 00:00:28, flags: extended
```

chear ip nat translation 这个命令清除所有（或指定的）应用的转换，下面列出了这个命令的一些扩展应用：

*	清除所有的动态转换
inside	清除指定的内部地址和端口转换
outside	清除指定的外部地址和端口转换
TCP	根据协议清除指定内部地址
UDP	根据协议清除指定内部地址

clear ip nat statistics 用来清除所有的NAT统计计数器

debug ip nat 这条命令用来通过显示每一个被转换地址的报文的信息来验证 NAT的操作特征。这条命令也显示一些关于出错条件或例外条件的信息，例如：分配全局地址失败。

从下面的输出可以得知源地址 10.1.1.1已被转换为全局地址 195.1.1.1。

```
NAT: s=10.1.1.1->195.1.1.1, d=195.1.1.3 [35]
```

15.11 结论

本章主要讨论了网络地址转换（Network Address Translation (NAT)。NAT使一子网内部的地址可以被任何其他的子网内主机重用。 NAT也使一个组织看起来好像使用不同的地址空间而不是实际使用的情况，因此减少了对唯一的、注册过的 IP地址的需求。 NAT也使私有网络管理者不用再记那些不遵循全局 IP地址分配策略的那些主机和路由器。在 RFC 1631中对NAT进行了定义。