第 3 章

网络地址转换

本章任务：根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题。

必备知识：(1) 静态 NAT。

(2) NAPT。

(3) 端口地址重定向。

学习目标：完成模拟公司分支机构网络内外网地址转换配置任务，解决公司内网地址资源不足问题。

3.1 模拟公司分支机构网络地址转换任务分析

由表 2-9 所示的模拟公司 IP 地址分配情况可知，分支机构 B-1 可用的公共 IP 地址仅有 62 个，但随着该分支机构业务发展，网络不断扩大，所分配公共 IP 地址出现不足。为解决 IP 地址紧张问题，模拟公司分支机构 B-1 网络内准备使用私有地址 10.0.0.0/24 替换原网络中的公共 IP 地址。但使用私有地址的分支机构网络不能与分支机构以外的网络通信，为满足分支机构网络以下通信要求，必须使用地址转换技术对进出分支机构网络的报文进行地址转换。

(1) 分支机构 B-1 内部网络中服务器 Ser1 向外网同时提供网站、邮件服务，同时 1 台“独立的”Web 服务器 WebSer1 和 1 台独立的邮件服务器 MailSer1 也同时向外网提供服务。

(2) 分支机构 8 名主管的办公用机需要访问网络上的多媒体服务。

(3) 分支机构 B-1 内部网络中 200 台主机要能访问 Internet 资源。

(4) 分支机构 B-1 在其网络内部模拟公司总部生产网搭建了一套生产系统，该模拟生产系统在分支机构网络内使用了与总部相同的网络地址 200.100.11.0/24，但该生产系统有时需要访问总部生产网下载部分生产数据用于分析研究。

(5) 尽可能节省公共 IP 地址。

表 3-1 显示了分支机构 B-1 内各主机使用 IP 地址情况。

表 3-1 分支机构 B-1 IP 地址分配情况

序号	内网主机	内部本地地址/网络前缀	网关地址
1	模拟生产系统	10.0.0.0/28	10.0.0.14
2	Ser1	10.0.0.17/28	10.0.0.30
3	WebSer1	10.0.0.18/28	10.0.0.30
4	MailSer1	10.0.0.19/28	10.0.0.30
5	普通主机	10.0.2.0/24	10.0.2.254
6	主管用机	10.0.3.0/24	10.0.3.254

3.2 网络地址转换的基本概念

网络地址转换(Network Address Translation,NAT)技术最初是作为缓解 IPv4 地址空间紧张的一种解决方案引入的,其主要作用就是通过将私有 IP 地址转换为合法的公有 IP 地址,使私有网络中的主机可以通过共享少量的公有 IP 地址访问 Internet。随着网络的爆炸性增长,IPv4 的地址空间变得非常紧张,租用公有 IP 地址也变得非常困难和昂贵,因此企业在组建自己的私有网络时,通常会在企业内部网络中使用 RFC1918 定义的私有 IP 地址(10.0.0.0/8、172.16.0.0/12、192.168.0.0/16),而在企业内部网络主机有访问 Internet 需求时,在企业的边界网关路由器上使用 NAT 技术将私有 IP 地址转换到租用的少量公有 IP 地址上,从而使用少量的公有 IP 地址来满足企业连接 Internet 的需求。

除了可以缓解 IPv4 地址空间的紧张外,NAT 技术在客观上屏蔽了企业内部网络的真实 IP 地址,一定程度上保护了内部网络不受到外部网络的主动攻击。例如,在使用动态 NAT 技术进行地址转换时,内部网络主机可以访问外部网络主机,但外部网络主机将无法主动访问内部网络中的主机,因此也提高了企业内部网络的安全性。

3.2.1 网络地址转换的工作过程

网络地址转换一般在网络的边界由网络地址转换设备实现,例如配置了地址转换功能的路由器或防火墙。网络地址转换设备使用地址转换表保存私有 IP 地址和公有 IP 地址的映射关系,并根据保存的映射关系对 IP 地址进行转换。典型的网络地址转换过程如图 3-1 所示。

在 PC_1 访问外部网络主机时,其产生的数据报文的源 IP 地址是 PC_1 在内部网络的私有 IP 地址(内部本地地址)192.168.1.10,当数据报文到达出口路由器的出接口时,路由器将数据报文的源 IP 地址转换为内部全局地址 202.207.120.10,使数据报文可以在公共网络上路由,并将内部本地地址和内部全局地址的映射关系保存在地址转换表中;在返回的数据报文中,目的 IP 地址为内部全局地址 202.207.120.10,在路由器接收到该报文后,根据地址转换表中保存的映射关系将目的 IP 地址转换为内部本地地址 192.168.1.10,并路由给内部网络的目的主机 PC_1,从而实现 PC_1 和外部网络主机之间的通信。

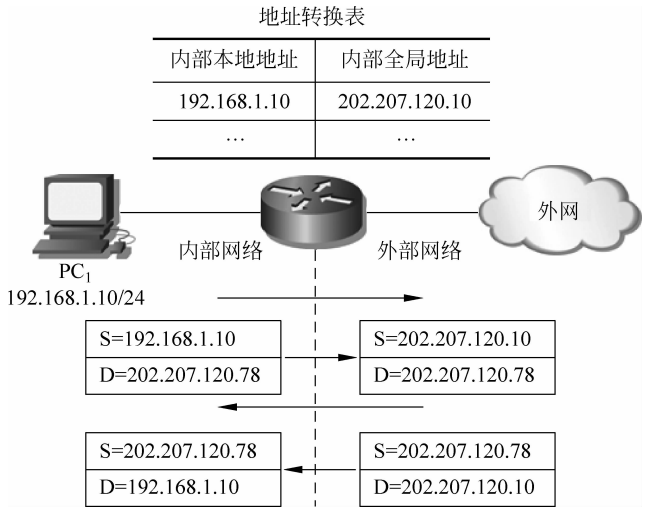

图 3-1　网络地址转换过程

注意：上面给出的只是一个典型的网络地址转换过程，实际上不同类型的网络地址转换在处理上会有所区别。

3.2.2　网络地址转换的类型

按照网络地址转换对象的不同，可以将网络地址转换分为内部网络地址转换和外部网络地址转换两种。其中外部网络地址转换主要用于内外网使用的 IP 地址重叠时，即内部网络随意使用了合法公有 IP 地址时，将外部网络主机与内部网络主机重叠的公有 IP 地址（外部全局地址）在内部网络转换为外部本地地址，由于相对应用比较少，因此在本书中不再进行介绍。

内部网络地址转换按照地址转换的原理、转换方式以及应用场合的不同可以划分为如表 3-2 所示的 5 种。

表 3-2　网络地址转换类型

网络地址转换类型	说　明
静态网络地址转换	手工配置本地地址到全局地址的一对一的映射，适用于需要固定全局 IP 地址的内网服务器
动态网络地址转换	本地地址到全局地址为一对一映射，但映射关系不固定，本地地址共享地址池中的全局地址
网络地址端口转换	本地地址到全局地址使用端口号实现动态的多对一映射，可显著提高全局地址的利用率，又称为地址的过载
基于接口的地址转换	网络地址端口转换的特殊形式，又称为 Easy IP。与网络地址端口转换的区别是本地地址均映射到出口路由器的出接口地址上
端口地址重定向	又称为 NAT Server，手工配置“本地地址＋端口”到“全局地址＋端口”的一对一的映射。适用于多台内网服务器映射到一个全局地址的情况

使用哪一种网络地址转换技术来进行地址的转换需要根据网络的具体需求来确定。很多时候在同一个网络中可能会涉及多种网络地址转换技术。例如,某一企业中大量的内部网络主机都有访问 Internet 的需求,而且企业内部网络还需要提供可以从 Internet 进行访问的 HTTP 服务来进行企业宣传,这时候就会同时用到网络地址端口转换和静态网络地址转换两种网络地址转换技术。

3.3 静态网络地址转换

静态网络地址转换是最简单的一种网络地址转换形式。在静态网络地址转换中,需要手工配置从内部本地地址到内部全局地址的一对一映射关系,配置完成后这些映射关系将一直存在,直到被手工删除。静态网络地址转换一般为需要对外部网络提供服务的内网服务器提供地址转换。

3.3.1 H3C 设备静态 NAT 配置

H3C 设备静态网络地址转换涉及的配置命令如下:

```
[H3C]nat static local-ip global-ip
[H3C]interface interface-type interface-number
[H3C-Ethernet0/0]nat outbound static
```

首先指定内部本地地址和内部全局地址之间的映射关系,然后在路由器相应的接口上应用静态网络地址转换。

假设存在如图 3-2 所示的网络,要求将内网服务器的 IP 地址静态转换到 202.207.120.100,使其可以为外部网络提供 HTTP 服务。

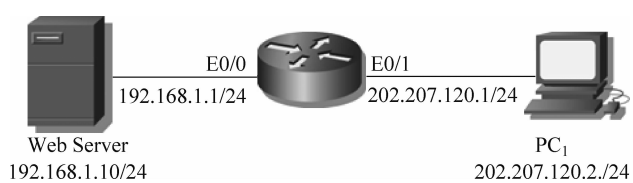

图 3-2 静态网络地址转换

具体的配置命令如下:

```
[H3C]nat static 192.168.1.10 202.207.120.100
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound static
```

配置完成后,在路由器上执行 display nat static 命令,显示结果如下:

```
[H3C]display nat static
NAT static information:
  There are currently 1 NAT static configuration(s)
  single static:
    Local-IP          : 192.168.1.10
```

```
    Global-IP          : 202.207.120.100
    Local-VPN          : ---

NAT static enabled information:
  Interface                                    Direction
  Ethernet0/1                                  out-static
```

从显示的结果可以看出，在路由器上配置了内部本地地址 192.168.1.10 到内部全局地址 202.207.120.100 的静态网络地址转换，该静态地址转换应用到了接口 Ethernet0/1 的 out bound 方向上。

需要注意的是，所有的内部网络地址转换都需要应用在出站接口的 outbound 方向上。

此时，在 PC_1 上使用内部全局地址 202.207.120.100 可以访问到内网服务器的 Web 服务。进行 Web 访问的同时在路由器的用户视图下可以使用 debugging nat packet 命令查看网络地址转换的过程，显示结果如下：

```
<H3C>terminal monitor
<H3C>terminal debugging
<H3C>debugging nat packet
Info: NAT packet debugging is enabled!
<H3C>
*Nov 15 07:26:47:904 2011 H3C NAT/7/debug:
(Ethernet0/1-in:)Pro : TCP
(202.207.120.2: 4981 - 202.207.120.100: 80) ------>
(202.207.120.2: 4981 -192.168.1.10: 80)
*Nov 15 07:26:47:906 2011 H3C NAT/7/debug:
(Ethernet0/1-out:)Pro : TCP
(192.168.1.10: 80-202.207.120.2: 4981) ------>
(202.207.120.100: 80 -202.207.120.2: 4981)
```

从显示的结果可以看出，在 PC_1 访问 Web 服务器的数据报文进入路由器接口 Ethernet0/1 时，会将数据报文的目的 IP 地址 202.207.120.100 转换为内部本地地址 192.168.1.10；而在 Web 服务器返回给 PC_1 的数据报文从路由器的接口 Ethernet0/1 出站之前，会将数据报文的源 IP 地址 192.168.1.10 转换为内部全局地址 202.207.120.100。

需要注意的是，在 H3C 的设备上所有的 debug 类的命令都只能在用户视图下执行，而且在使用 debug 类命令进行系统调试之前，需要先执行 terminal monitor 和 terminal debugging 命令。其中，terminal monitor 命令用来开启控制台对系统信息的监视功能（该功能默认开启，因此可以不执行这条命令）；terminal debugging 命令用来开启调试信息的屏幕输出开关，使调试信息可以在终端上进行显示。

在 PC_1 上访问 Web 服务器后，在路由器上执行 display nat session 命令，显示结果如下：

```
[H3C]display nat session
There are currently 1 NAT session:
Protocol      GlobalAddr        Port     InsideAddr       Port    DestAddr   Port
  ---         202.207.120.100   0        192.168.1.10     0       ---        ---
```

```
status:800      TTL:00:05:00    Left:00:04:56    VPN:---
```

从显示的结果可以看出,当前存在一个 NAT 会话,为内部本地地址 192.168.1.10 到内部全局地址 202.207.120.100 的映射。

3.3.2 Cisco 设备静态 NAT 配置

Cisco 设备静态网络地址转换涉及的配置命令如下:

```
Router(config)#ip nat inside source static local-ip global-ip
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat outside
```

需要注意的是,H3C 设备上只需要在连接外部网络的接口上配置 nat outbound 命令来应用 NAT,与 H3C 不同,在 Cisco 设备上需要在连接内部网络的接口上配置 ip nat inside,在连接外部网络的接口上配置 ip nat outside。

在此依然使用图 3-2 所示的网络进行 Cisco 设备静态 NAT 的配置,具体的配置命令如下:

```
Router(config)#ip nat inside source static 192.168.1.10 202.207.120.100
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat outside
```

配置完成后,在路由器上执行 show ip nat translations 命令,显示结果如下:

```
Router#show ip nat translations
Pro     Inside global       Inside local        Outside local       Outside global
---     202.207.120.100     192.168.1.10          ---                 ---
```

从显示的结果可以看出,在路由器上存在一条内部本地地址 192.168.1.10 到内部全局地址 202.207.120.100 的静态网络地址转换。

此时,在 PC_1 上使用内部全局地址 202.207.120.100 可以访问到内网服务器的 Web 服务。进行 Web 访问的同时,在路由器的用户视图下可以使用 debug ip nat 命令查看网络地址转换的过程,显示结果如下:

```
Router#debug ip nat
IP NAT debugging is on
Router#
*Mar  1 01:48:40.963: NAT: s=202.207.120.2, d=202.207.120.100->192.168.1.10
[6358]
*Mar  1 01:48:40.967: NAT: s=192.168.1.10->202.207.120.100, d=202.207.120.2
[6609]
```

在路由器上执行 show ip nat statistics 命令查看 NAT 的统计信息,显示结果如下:

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet0/1
Inside interfaces:
  FastEthernet0/0
Hits: 18   Misses: 0
Expired translations: 0
Dynamic mappings:
```

注意：静态网络地址转换由于需要静态地指定从内部本地地址到内部全局地址的一对一的映射，因此无法实现 IP 地址的节约。

3.4　动态网络地址转换

动态网络地址转换又称为 Basic NAT，动态网络地址转换也是一种一对一的映射关系，但是与静态网络地址转换不同的是，动态网络地址转换的映射关系不是一直存在的，而是只有在出口路由器的出站接口上出现符合地址转换条件的内网流量时才会触发路由器进行网络地址的转换。而且映射关系不会一直存在，到达老化时间以后就会被删除，以便于将回收的内部全局地址映射给其他需要的内部本地地址。

3.4.1　H3C 设备动态 NAT 配置

H3C 设备动态网络地址转换涉及的配置命令如下：

(1) 创建一个 ACL 用于匹配需要进行动态网络地址转换的内部本地地址。

```
[H3C]acl number acl-number
[H3C-acl-basic-2000]rule [rule-id] {deny|permit} [source {sour-addr sour-wildcard|any}]
```

在 NAT 中使用 ACL 匹配内部本地地址时需要注意以下 3 点。

① 不必使用 firewall enable 命令启用防火墙。

② ACL 中只有被显式规则 permit 的源 IP 地址才会进行地址转换，默认允许所有的规则不生效。

③ 如果内网中有些特殊的 IP 地址不需要做动态网络地址转换，例如，内部服务器要做静态网络地址转换，则应将其在定义 ACL 时首先 deny 掉。

(2) 创建一个存放有内部全局地址的地址池。

```
[H3C]nat address-group group-number start-addr end-addr
```

(3) 在出口路由器的出站接口上配置 ACL 与地址池的关联。

```
[H3C-Ethernet0/0]nat outbound acl-number address-group group-number no-pat
```

注意：no-pat 参数表示是一个 Basic NAT 的转换，不做地址的过载。

假设存在如图 3-3 所示的网络，要求将内部网络 IP 地址段 192.168.1.0/24 动态转换到 202.207.120.10～202.207.120.50。

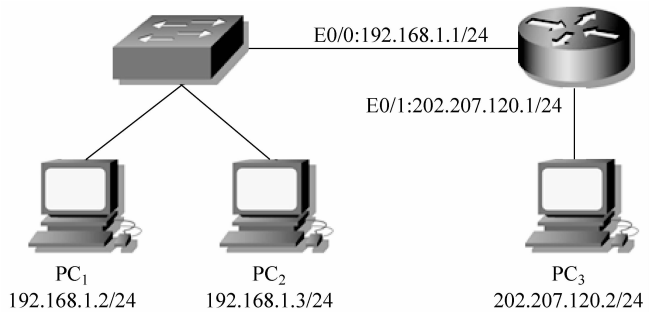

图 3-3 动态网络地址转换

具体的配置命令如下:

```
[H3C]acl number 2000
[H3C-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[H3C-acl-basic-2000]quit
[H3C]nat address-group 1 202.207.120.10 202.207.120.50
[H3C]interface Ethernet 0/1
[H3C-Ethernet0/1]nat outbound 2000 address-group 1 no-pat
```

配置完成后,从 PC_1 去 ping PC_3,同时在路由器上执行 debugging nat packet 命令,显示结果如下:

```
<H3C>debugging nat packet
Info: NAT packet debugging is enabled!
<H3C>
*Nov 15 08:48:17:170 2011 H3C NAT/7/debug:
(Ethernet0/1-out :)Pro : ICMP
(192.168.1.2: 512 -202.207.120.2:512) ------>
(202.207.120.10: 512 -202.207.120.2:512)
*Nov 15 08:48:17:171 2011 H3C NAT/7/debug:
(Ethernet0/1-in:)Pro : ICMP
(202.207.120.2:512 -202.207.120.10:512) ------>
(202.207.120.2:512 -192.168.1.2:512)
```

从显示的结果可以看出数据报文在路由器上进行双向地址转换的过程。

在路由器上执行 display nat session 命令,显示结果如下:

```
[H3C]display nat session
There are currently 2 NAT sessions:
Protocol        GlobalAddr          Port      InsideAddr      Port        DestAddr      Port
  ---           202.207.120.10      ---       192.168.1.2     ---           ---         ---
    status:NOPAT    TTL:00:04:00    Left:00:03:54    VPN:---

   ICMP  202.207.120.10   512      192.168.1.2     512      202.207.120.2  512
    status:NOPAT    TTL:00:00:10    Left:00:00:04    VPN:---
```

从显示的结果可以看出,当前存在两个 NAT 会话,其中一个是内部本地地址

192.168.1.2到内部全局地址 202.207.120.10 的映射，生存时间为 4min；另一个为基于 ICMP 协议的映射关系，是内部本地地址 192.168.1.2 和端口号 512 到内部全局地址 202.207.120.10 和端口号 512 的映射，生存时间为 10s。在从 PC_1 去 ping PC_3 时，这两条会话会同时出现。关于不同协议的 NAT 会话生存时间可以通过 display nat aging-time 命令来查看。

其实在看到上面 display nat session 显示的结果时，还会有一个疑问：ICMP 协议处于网络层，ICMP 协议的数据报文根本不会有传输层的封装，因此也就不可能会有端口号的存在，那端口号 512 又是从哪里来的呢？实际上 512 并不是端口号，而是 ICMP 报头封装中的 Identifier 字段（即标识字段）的值。在定义 ICMP 协议的请求注解文档 RFC792 中，描述 Identifier 字段可以像 TCP 或 UDP 协议的端口号一样来区分不同的 ICMP 进程，但实际上在特定的操作系统中，ICMP 协议的 Identifier 字段是一个定值。例如，在 Windows XP 系统中，ICMP 协议封装中的 Identifier 字段的值为 0x0200，即十进制的 512，这一点可以在 Wireshark 软件捕获的 ICMP 请求/应答报文的报头中看到。因此 Identifier 字段实际上并不具备区分进程的功能，ICMP 进程的区分实际上使用的是 Sequence number 字段。而 Identifier 字段的一个重要功能就是在 NAT 中作为地址映射的依据，因此在 display nat session 命令的显示结果中会看到 ICMP 协议的端口号为 512。Identifier 字段会在 NAT 对 ICMP 分片报文的处理中发挥非常重要的作用，在此不再进行介绍，感兴趣的学生可以自行查阅相关资料。

在进行动态网络地址转换时，路由器总是会从地址池中拿第一个可用地址来进行映射，此时如果 PC_2 去 ping PC_3，则会为 PC_2 分配内部全局地址 202.207.120.11。

可以在用户视图下使用 reset nat session 命令清除掉未到老化时间的地址映射关系。

3.4.2　Cisco 设备动态 NAT 配置

在 Cisco 设备上动态 NAT 的配置同样需要创建匹配内部本地地址的 ACL 和存放内部全局地址的地址池，涉及的命令如下：

```
Router(config)#access-list access-list-number {permit|deny} source [source-wildcard]
Router(config)#ip nat pool pool-name start-addr end-addr netmask netmask
Router(config)#ip nat inside source list access-list-number pool pool-name
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface interface-type interface-number
Router(config-if)#ip nat outside
```

在此依然使用图 3-3 所示的网络进行 Cisco 设备动态 NAT 的配置，具体的配置命令如下：

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool dyn-nat 202.207.120.10 202.207.120.50 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool dyn-nat
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip nat inside
```

```
Router(config-if)#exit
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat outside
```

配置完成后,从 PC_1 去 ping PC_3,同时在路由器上执行 debugging nat packet 命令,显示结果如下:

```
Router#debug ip nat
IP NAT debugging is on
Router#
*Mar  1 00:08:43.359: NAT: s=192.168.1.2->202.207.120.10, d=202.207.120.2 [7745]
*Mar  1 00:08:43.359: NAT*: s=202.207.120.2, d=202.207.120.10->192.168.1.2 [7037]
```

在路由器上执行 show ip nat translations 命令,显示结果如下:

```
Router#show ip nat translations
Pro     Inside global       Inside local       Outside local      Outside global
---     202.207.120.10      192.168.1.2        ---                ---
```

3.5 网络地址端口转换

网络地址端口转换(Network Address Port Translation,NAPT)又称为端口地址转换(Port Address Translation,PAT)或者地址过载。动态网络地址转换是一对一的映射关系,它只是解决了内外网通信的问题,但并没有真正意义上解决公有 IP 地址不足的问题。而 NAPT 技术通过使用同一个内部全局地址的不同端口号来标识不同的内部本地地址,实现多对一的地址转换,从而实现公有 IP 地址的节约。

在 NAPT 的转换过程中,路由器维护着如表 3-3 所示的动态地址转换表,通过端口的映射关系使多个内部本地地址转换到一个内部全局地址上。在进行地址转换时,一般会尽量使用与本地地址端口相同的全局地址端口,但如果该端口已经被使用,则会选择最小的可用端口作为全局地址端口。

表 3-3 NAPT 地址转换表

内部本地地址	内部本地地址端口	内部全局地址	内部全局地址端口
192.168.1.2	2000	202.207.120.10	2000
192.168.1.3	1024		1024
192.168.1.20	1024		1025

3.5.1 H3C 设备 NAPT 配置

在 H3C 设备上 NAPT 的配置方法与 Basic NAT 基本相同,唯一的区别是 NAPT 在出口路由器的出站接口上配置 ACL 与地址池的关联时不使用 no-pat 参数,表明是基于端口的多对一的地址转换。

在此依然使用图 3-3 所示的网络,要求将内部网络 192.168.1.0/24 使用 NAPT 技术过载到唯一的内部全局地址 202.207.120.10 上。具体的配置命令如下: