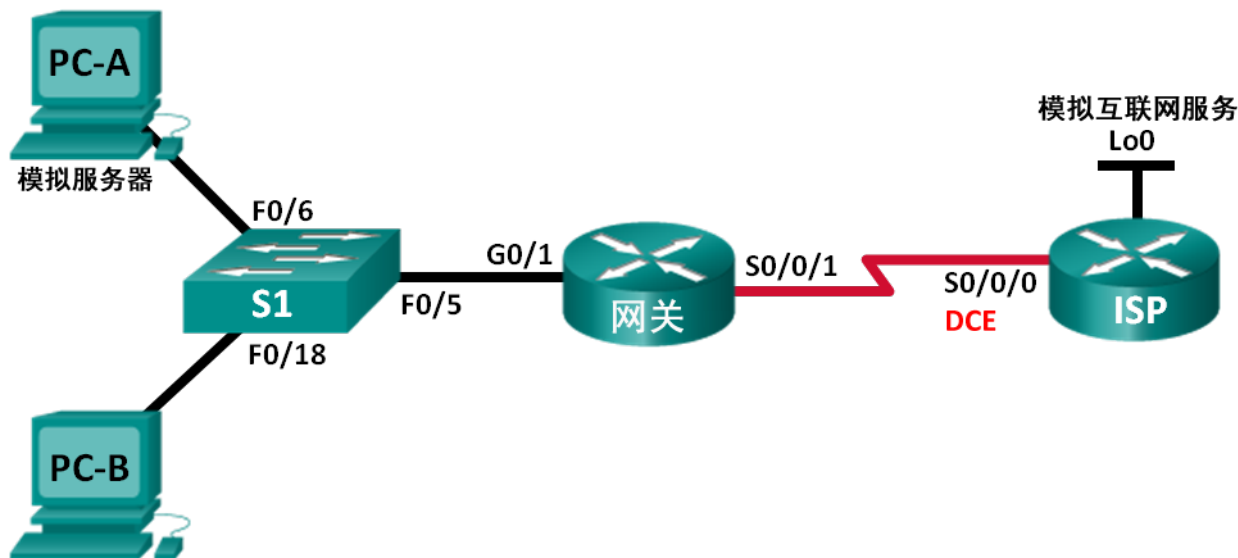


实验 - 配置动态和静态 NAT

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
网关	G0/1	192.168.1.1	255.255.255.0	不适用
	S0/0/1	209.165.201.18	255.255.255.252	不适用
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	不适用
	Lo0	192.31.7.1	255.255.255.255	不适用
PC-A (模拟服务器)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

目标

第 1 部分：构建网络和验证连接

第 2 部分：配置和验证静态 NAT

第 3 部分：配置和验证动态 NAT

背景/场景

网络地址转换 (NAT) 属于一种进程，在该进程中，思科路由器等网络设备将公共地址分配给专用网络内的主机设备。使用 NAT 的主要原因是减少组织所使用的公共 IP 地址数量，因为可用的 IPv4 公共地址数量有限。

在该实验中，ISP 已将 209.165.200.224/27 的公共 IP 地址空间分配给公司。这为公司提供 30 个公共 IP 地址。地址 209.165.200.225 至 209.165.200.241 用于静态分配，209.165.200.242 至 209.165.200.254 用于动态分配。从 ISP 至网关路由器使用静态路由，而从网关至 ISP 路由器使用默认路由。ISP 路由器上的环回地址模拟 ISP 互联网连接。

注：CCNA 动手实验所用的路由器是采用思科 IOS 15.2(4)M3 版（universalk9 映像）的思科 1941 集成多业务路由器 (ISR)。所用的交换机是采用思科 IOS 15.0(2) 版（lanbasek9 映像）的思科 Catalyst 2960 系列。也可使用其他路由器、交换机以及思科 IOS 版本。根据型号以及思科 IOS 版本的不同，可用命令和产生的输出可能与实验显示的不一样。请参考本实验末尾的“路由器接口汇总表”以了解正确的接口标识符。

注：确保路由器和交换机的启动配置已经清除。如果不确定，请联系教师。

所需资源

- 2 台路由器（采用思科 IOS 15.2(4)M3 版通用映像的思科 1941 或同类路由器）
- 1 台交换机（采用思科 IOS 15.0(2) lanbasek9 版映像的思科 2960 或同类交换机）
- 2 台 PC（采用 Windows 7、Vista 或 XP 且支持终端模拟程序，比如 Tera Term）
- 用于通过控制台端口配置思科 IOS 设备的控制台电缆
- 拓扑所示的以太网和串行电缆

第 1 部分：建立网络并验证连接

在第 1 部分中，您将建立网络拓扑结构和配置接口 IP 地址、静态路由、设备访问和密码等基本设置。

步骤 1：建立如拓扑图所示的网络。

按照拓扑图所示连接设备和电缆。

步骤 2：配置 PC 主机。

步骤 3：根据需要初始化路由器和交换机并重新加载。

步骤 4：为每台路由器配置基本设置。

- 通过控制台连接到路由器，然后进入全局配置模式。
- 复制以下基本配置并将其粘贴到路由器上的运行配置中。

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited.#
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. 根据拓扑指示配置主机名。
- d. 将运行配置复制到启动配置中。

步骤 5：在 ISP 上创建模拟 Web 服务器。

- a 创建名为 **webuser** 的本地用户，加密密码为 **webpass**。

```
ISP(config)# username webuser privilege 15 secret webpass
```
- b 启用 ISP 上的 HTTP 服务器服务。

```
ISP(config)# ip http server
```
- c 配置 HTTP 服务，以便使用本地用户数据库。

```
ISP(config)# ip http authentication local
```

步骤 6：配置静态路由。

- a 使用分配的公共网络地址范围 209.165.200.224/27 创建从 ISP 路由器到网关路由器的静态路由。

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```
- b 创建从网关路由器到 ISP 路由器的默认路由。

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

步骤 7：将运行配置保存到启动配置。

步骤 8：检验网络连接。

- a 从 PC 主机，ping 网关路由器上的 G0/1 接口。若 ping 未成功，则进行故障排除。
- b 显示两个路由器上的路由表，验证静态路由是否在路由表中且在两个路由器上是否配置正确。

第 2 部分：配置和验证静态 NAT

静态 NAT 使用本地地址与全局地址的一对一映射，这些映射保持不变。对于必须具有可从互联网进行访问的静态地址的 Web 服务器或设备而言，静态 NAT 尤为有用。

步骤 1：配置静态映射。

配置静态映射告知路由器在专用内部服务器地址 192.168.1.20 和公共地址 209.165.200.225 间转换。这让互联网用户能够访问 PC-A。PC-A 为模拟服务器或设备，含可从互联网进行访问的不变地址。

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

步骤 2：指定接口。

向接口发出 **ip nat inside** 和 **ip nat outside** 命令。

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

步骤 3：测试配置。

- a 通过发出
- show ip nat translations**
- 命令显示静态 NAT 表。

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---

内部本地主机地址的转换是什么？

192.168.1.20 = _____

内部全局地址的分配方是什么？

内部本地地址的分配方是什么？

- b 从 PC-A ping ISP 上的 Lo0 接口 (192.31.7.1)。若 ping 不成功，则进行故障排除并更正问题。在网关路由器上，显示 NAT 表。

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:1	192.168.1.20:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.225	192.168.1.20	---	---

PC-A 将 ICMP 请求 (ping) 发送至 ISP 上的 192.31.7.1 时，NAT 条目已添加至将 ICMP 列为协议的表中。

该 ICMP 交换中使用的端口号是多少？ _____

注：可能有必要禁用 PC 防火墙，才能 ping 成功。

- c 从 PC-A，通过 Telnet 远程登录 ISP Lo0 接口，并显示 NAT 表。

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:1	192.168.1.20:1	192.31.7.1:1	192.31.7.1:1
tcp	209.165.200.225:1034	192.168.1.20:1034	192.31.7.1:23	192.31.7.1:23
---	209.165.200.225	192.168.1.20	---	---

注：ICMP 请求 NAT 可能超时，并已从 NAT 表中删除。

在该转换中所使用的协议是什么？ _____

所使用的端口号是多少？

内部全局/本地： _____

外部全局/本地： _____

- d 由于静态 NAT 配置用于 PC-A，请验证静态 NAT 公共地址 (209.165.200.225) 上从 ISP 到 PC-A 的 ping 是否成功。

- e 在网关路由器上，显示 NAT 表以验证转换。

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.200.225:12	192.168.1.20:12	209.165.201.17:12	209.165.201.17:12
---	209.165.200.225	192.168.1.20	---	---

请注意，外部本地地址和外部局部地址相同。该地址为 ISP 远程网络源地址。若要从 ISP 成功执行 ping 操作，则将内部全局静态 NAT 地址 209.165.200.225 转换成 PC-A 内部本地地址 (192.168.1.20)。

- f 通过使用网关路由器上的 **show ip nat statistics** 命令验证 NAT 统计数据。

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39 Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

注：这仅是一个输出示例。您的输出可能与此示例不完全一致。

第 3 部分：配置和验证动态 NAT

动态 NAT 使用公有地址池，并以先到先得的原则分配这些地址。内部设备请求访问外部网络时，动态 NAT 分配该池中的可用公共 IPv4 地址。动态 NAT 结果导致本地和全局地址间的多对多地址映射。

步骤 1：清除 NAT。

继续添加动态 NAT 前，请清除第 2 部分中的 NAT 和统计数据。

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

步骤 2：定义匹配局域网专用 IP 地址范围的访问控制列表 (ACL)。

ACL 1 用于实现 192.168.1.0/24 网络的转换。

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

步骤 3：验证 NAT 接口配置是否仍然有效。

在网关路由器上发出 **show ip nat statistics** 命令验证 NAT 配置。

步骤 4：定义可使用的公共 IP 地址池。

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

步骤 5：定义从内部源列表到外部池的 NAT。

注：请记住，NAT 池名称区分大小写，且在此输入的池名称必须与上一步中所用的相匹配。

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

步骤 6：测试配置。

- a 从 PC-B ping ISP 上的 Lo0 接口 (192.31.7.1)。若 ping 不成功，则进行故障排除并更正问题。在网关路由器上，显示 NAT 表。

```
Gateway# show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
icmp	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	209.165.200.242	192.168.1.21	---	---

PC-B 内部本地主机地址的转换是什么？

192.168.1.21 = _____

PC-B 将 ICMP 消息发送至 ISP 上的 192.31.7.1 时，已将动态 NAT 条目添加至以 ICMP 作为协议的表中。

该 ICMP 交换中使用的端口号是多少？ _____

- b 从 PC-B，打开浏览器并输入 ISP 模拟 Web 服务器（Lo0 接口）的 IP 地址。提示时，以 **webuser** 的身份登录，密码为 **webpass**。
- c 显示 NAT 表。

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1041	192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042	192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043	192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044	192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1045	192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046	192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047	192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048	192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049	192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050	192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1051	192.168.1.21:1051	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1052	192.168.1.21:1052	192.31.7.1:80	192.31.7.1:80
---	209.165.200.242	192.168.1.22	---	---

在该转换中所使用的协议是什么？ _____

所使用的端口号是多少？

内侧: _____

外侧: _____

所使用的熟悉端口号和服务是什么？ _____

- d 通过使用网关路由器上的 **show ip nat statistics** 命令验证 NAT 统计数据。

```
Gateway# show ip nat statistics
```

```
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 0:06:40 ago
```

```
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345 Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

注：这仅是一个输出示例。您的输出可能与此示例不完全一致。

步骤 7： 删除静态 NAT 条目。

在步骤 7 中，静态 NAT 条目被删除，您可查看该 NAT 条目。

- a 从第 2 部分中删除静态 NAT。提示删除子条目时，请输入 **yes**。

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225
```

```
Static entry in use, do you want to delete child entries? [no]: yes
```

- b 清除 NAT 和统计数据。
- c 从两台主机 ping ISP (192.31.7.1)
- d 显示 NAT 表和统计数据。

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 0:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
```

实验 – 配置动态和静态 NAT

```
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Gateway# **show ip nat translation**

```
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512    192.31.7.1:512
--- 209.165.200.243     192.168.1.20     ---               ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512    192.31.7.1:512
--- 209.165.200.242     192.168.1.21     ---               ---
```

注：这仅是一个输出示例。您的输出可能与此示例不完全一致。

思考

1. 为什么要在网络中使用 NAT?

2. NAT 的限制有哪些?

路由器接口汇总表

路由器接口汇总				
路由器型号	以太网接口 1	以太网接口 2	串行接口 1	串行接口 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

注：若要了解如何配置路由器，请查看接口来确定路由器类型以及路由器拥有的接口数量。我们无法为每类路由器列出所有的配置组合。下表列出了设备中以太网和串行接口组合的标识符。此表中未包含任何其他类型的接口，但实际的路由器可能会含有其他接口。例如 ISDN BRI 接口。括号中的字符串是约定缩写，可在思科 IOS 命令中用来代表接口。