工业和信息化精品系列教材
网络技术

微课版

网络互联技术

任务驱动式教程

邓启润 钟文基 ◉ 主编
王玲 苏健渊 ◉ 副主编

倾心打磨，专业基础，涵盖主流厂商

任务驱动思维，注重培养分析和解决问题的能力

配套资源丰富，提供教案、课件及自动评分的实验模型

融入课程思政，技术与思政元素有机结合

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

任务2： 实现内网用户访问互联网服务器——端口地址转换（PAT）

任务目标：应用 PAT 技术转换内网地址，实现内网用户访问外网（ping 通 ISP 路由器地址：115.0.0.2/29）。

视频二维码

继续以如图 3.1 所示的网络拓扑进行分析，Laptop3 要 ping 运营商 115.0.0.2/29 的地址，Laptop3 封装了一个 IP 包，其源地址和目的地址如表 3.4 所示。

表3.4 Laptop3 发给 ISP 路由器的数据包地址信息

源 IP 地址	目的 IP 地址	目的网络的网络地址
192.168.20.13/24	115.0.0.2/29	115.0.0.0/29

1. Laptop3 发出 IP 数据包后的分析

Laptop3 发现目的地址 115.0.0.2/29 处于不同网络，因此将 IP 数据包发给其网关（MS0：192.168.20.1/24），请求帮转发。MS0 收到该 IP 数据包后，根据 IP 数据包上的目的 IP 地址查询路由表，如图 3.14 所示。

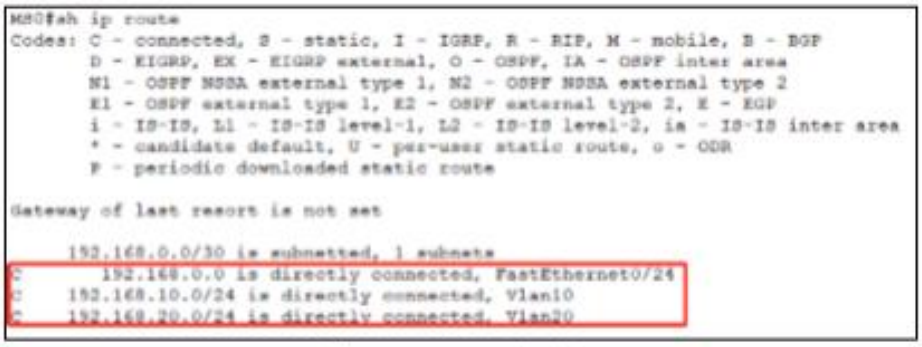

图3.14　MS0 路由表

MS0 发现路由表中没有关于目的网络（115.0.0.0/29）的路由条目，按规则只能丢弃！解决办法之一是按本项目任务 1 的思路，往路由表添加静态路由。

2.　在 MS0 添加静态路由，将发往 ISP 路由器的数据转发给边界路由器 R0

在 MS0 添加 115.0.0.0/29 的路由条目，命令如下：

```
MS0(config)#ip route 115.0.0.0 255.255.255.248 192.168.0.2
```

检查路由表，确认已经添加成功，如图 3.15 所示。

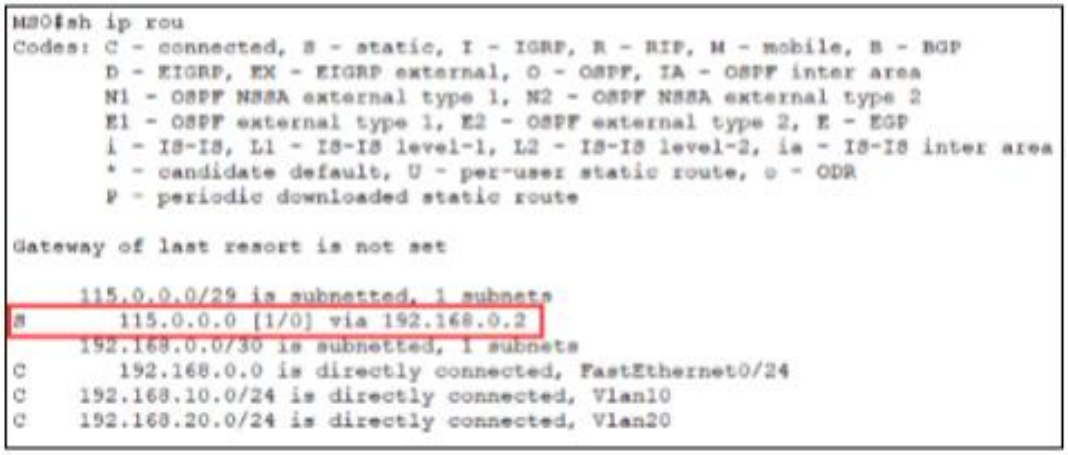

图3.15　核心交换机 MS0 的路由表

MS0 根据新添加的路由条目，将数据转发给 192.168.0.2（边界路由器 R0）。R0 同样也要去查路由表，如图 3.16 所示。

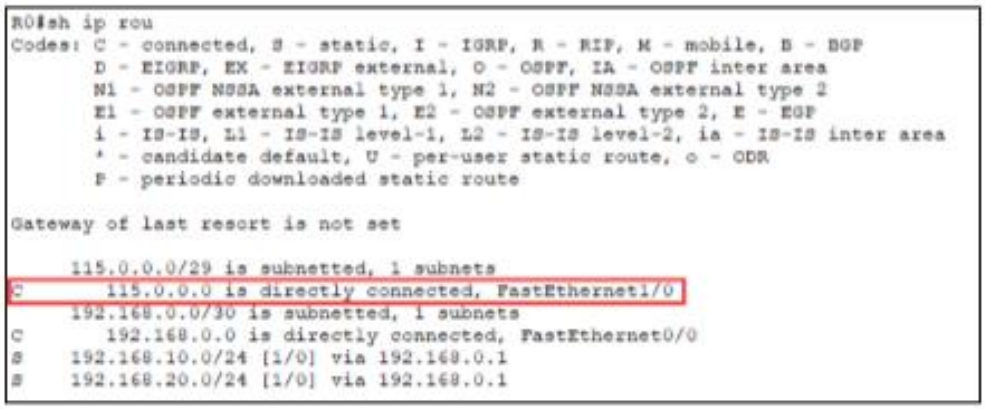

图3.16　边界路由器 R0 的路由表

路由表会告诉 R0，发往 115.0.0.0/29 的网络，通过 FastEthernet1/0 接口发出。最终数据就到达对端——ISP 的路由器。

3.　再分析 ISP 路由器应答包返回的过程

ISP 的路由器接收到数据包以后，会生成一个应答包发回 3 给 Laptop3，地址信息如表 3.5 所示。

表3.5　ISP 路由器发给 Laptop3 的数据包地址信息

源 IP 地址	目的 IP 地址	目的网络的网络地址
115.0.0.2/29	192.168.20.13/24	192.168.20.0/24

为了把这个数据包发回给 Laptop3，ISP 路由器会去查自己的路由表，以便确定该从哪个接口发出该数据包。ISP 的路由表如图 3.17 所示。

```
ISP#sh ip rou
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     115.0.0.0/29 is subnetted, 1 subnets
C       115.0.0.0 is directly connected, FastEthernet1/0
```

图3.17　ISP 路由器的路由表

但是，从输出的路由信息来看，ISP 路由器的路由表并没有关于 192.168.20.0/24 网络的路由条目。按规则，ISP 会将应答包丢弃，导致数据通信无法继续。

很多人在掌握了静态路由技术以后，很容易会想到要按照本项目任务 1 的思路，在 ISP 路由器添加一条静态路由，让 ISP 将数据发回给 R0 就可以了。

但是这样做会产生两个问题：

①私有 IP 地址在互联网是不可以被路由的，因为公网设备的路由表不允许存在私有 IP 地址的记录；

②私有网络的地址是组织内部自己规划，可以任意使用的。运营商的多个客户如果用的是相同的私有网络地址，如果允许私有网络地址出现在公网的路由器，运营商必须配置到达用户网络的路由条目，而对于某个被重复使用的网络，下一跳地址是不唯一的，最终会导致数据丢失。比如 A 公司和 B 公司都接入了同一个运营商，而且这两个公司都使用同一个私有 IP 地址段，那么运营商在写路由条目的时候，下一跳节点应该指向 A 公司还是 B 公司呢？显然都不行。

解决问题的办法是应用网络地址转换（Network Address Translation，NAT）技术。边界路由器负责将 Laptop3 发过来的数据包上的源 IP 地址（私有地址）转换成公有 IP 地址。因为 ISP 路由器生成应答包的时候，目的地址是根据它接收到的数据包的源地址确定的（类似于我们收到一封信，回信的时候，目的地址写的是收到信件的源地址）。就这样，当 ISP 的路由器返回应答包的时候，目的地址也是公有地址，避免了私有地址在公网上的非法存在。

PAT（Port Address Translation，端口地址转换）是 NAT（Network Address Translation，网络地址转换）技术最常用的一种方式。下面在边界路由器应用 PAT 技术将数据包的源地址进行转换（私有 IP 地址转换成公有 IP 地址）。

步骤 1：定义 NAT 内网接口和外网接口

对照项目拓扑，边界路由器 R0 的 Fa0/0 接口连接的是企业内网，如图 3.18 所示。

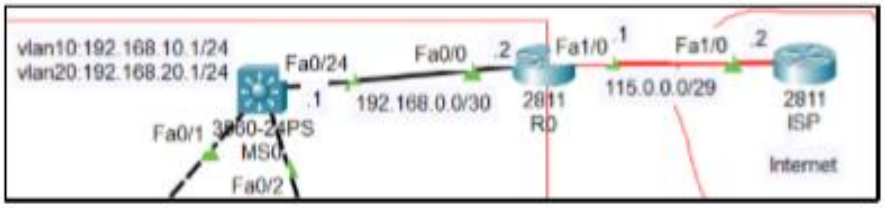

图3.18　任务拓扑

所以在这里需要将这个接口定义为 NAT 的内网接口。命令如下：

```
R0>
R0>en
R0#conf t
R0(config)#int fa 0/0
R0(config-if)#ip nat inside          //将 Fa0/0 接口定义为 NAT 内部接口
R0(config-if)#exit
R0(config)#
```

路由器 R0 的 Fa1/0 接口连接的是企业内网，所以在这里需要将这个接口定义为 NAT 的外网接口。命令如下：

```
R0(config)#int fa 1/0
R0(config-if)#ip nat outside      //将 Fa1/0 接口定义为 NAT 外部接口
R0(config-if)#exit
```

步骤 2：用访问控制列表（Access Control Lists，ACL）捕获需要转换的流量。这里捕获 Laptop3 所在网络发出的数据包，命令如下：

```
R0(config)#access-list 1 permit 192.168.20.0 0.0.0.255
```

这里创建了一个列表，编号是“1”，这个列表可以捕获网络 192.168.20.0/24 发出的数据包。（编号可以根据情况自己定义，但是要遵守规则，具体的 ACL 规则在项目八展开讨论）

小贴士：这里用到了通配符掩码（Wildcard bits）而不是以前习惯使用的掩码的格式。一种通配符掩码的计算方法，就是简单地将 255. 255. 255. 255 减掉子网掩码。在这个例子，255. 255. 255. 255 减去 255. 255. 255. 0，就得到 0. 0. 0. 255。

步骤 3：将捕获的流量映射到外网接口。命令如下：

```
R0(config)#ip nat inside source list 1 interface fastEthernet 1/0
```

参数解读：

① “ip nat”指令是要求路由器执行地址转换；

② “inside source”参数表示当数据包由内网发往外网的时候，需要转换其源地址；

③ “list 1”表示编号为“1”的访问控制列表。这里要注意的是：列表的编号要和步骤 2 中定义的列表编号一致；

④ “fastEthernet 1/0”指的是边界路由器 R0 的外网接口，连接运营商的网络接口；

⑤ “overload”表示允许过载，边界路由器会通过端口映射的方式，允许内网多个用户同时实现地址转换，理论上的数量可以达到 64511 个（65535 - 1024）。

步骤 4：测试从内网主机访问外网的情况

从 Laptop3 ping 外网 ISP 路由器（115.0.0.2/29），结果如图 3.19 所示。

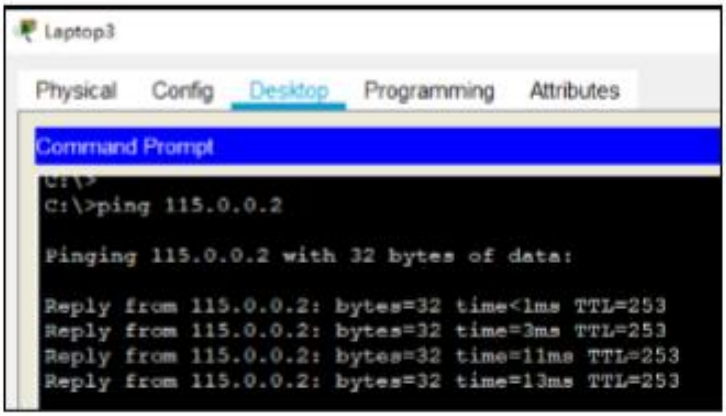

图3.19　Laptop3 ping 外网 ISP 路由器（115.0.0.2/29）结果

结果显示通信是正常的，我们通过应用 PAT 技术成功实现了内网用户访问外网。在边界路由器 R0 我们可以查看到地址转换的详细信息。如图 3.20 所示。

```
R0#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 115.0.0.1:17      192.168.20.13:17   115.0.0.2:17       115.0.0.2:17
icmp 115.0.0.1:18      192.168.20.13:18   115.0.0.2:18       115.0.0.2:18
icmp 115.0.0.1:19      192.168.20.13:19   115.0.0.2:19       115.0.0.2:19
icmp 115.0.0.1:20      192.168.20.13:20   115.0.0.2:20       115.0.0.2:20
```

图3.20　边界路由器的地址转换信息

Show ip nat translations 命令显示的每个包转换的的信息，转换了 4 个 icmp 数据包的地址。包括数据包从内网出去的时候，将源地址（192.168.20.13）转换为内部全局地址（Inside global：115.0.0.1）；数据包从外网进入内网的时候，将目的地址（115.0.0.1）转换为内部本地地址（192.168.20.13）。往返的数据包进行地址转换的时候，是一个相反的过程。

通过 ACL 也可以查看到捕获的数据包统计信息，一共 8 个数据包被捕获。如图 3.21 示：

```
R0#
R0#sh ip access-lists 1
Standard IP access list 1
    permit 192.168.20.0 0.0.0.255 (8 match(es))

R0#
```

图3.21　检查边界路由器 R0 上捕获的数据包

边界路由器访问控制列表捕获的数据报统计数据“8 match（es）”：一共有 8 个数据包被匹配到。我们用 ping 命令不是只发出了 4 个包吗？show ip translations 命令显示的信息也只有 4 条记录而已啊。但是，这个捕获的统计数据包括了出去的 4 个数据包和返回的 4 个数据包。（注意：数据包出去和返回都需要转换，只是数据包出去的时候源地址是私有地址，需要转换成公有地址；数据包回来的时候转换的是目的地址：目的地址是公有地址，要转换成原来的私有地址。）

这个时候，销售部 vlan10 的用户还是不能访问外网。因为边界路由器 R0 没有去捕获他们网络发出来的流量，也就没有去转换那些数据包的地址。按本任务开始时候的分析，这导致了数据包到达目的地以后，因为应答包的目的地址是一个私有 IP 地址而无法被路由回来最终被丢弃。

解决的办法很简单，在边界路由器的访问控制列表添加一条规则，让路由器捕获 vlan10 发出的数据即可。

步骤 5：在边界路由器 R0 的访问控制列表添加规则，让路由器捕获 VLAN 10 网络发出的数据。命令如下：

```
R0(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

测试销售部用户 Laptop0 访问外网，结果如图 3.22 所示。

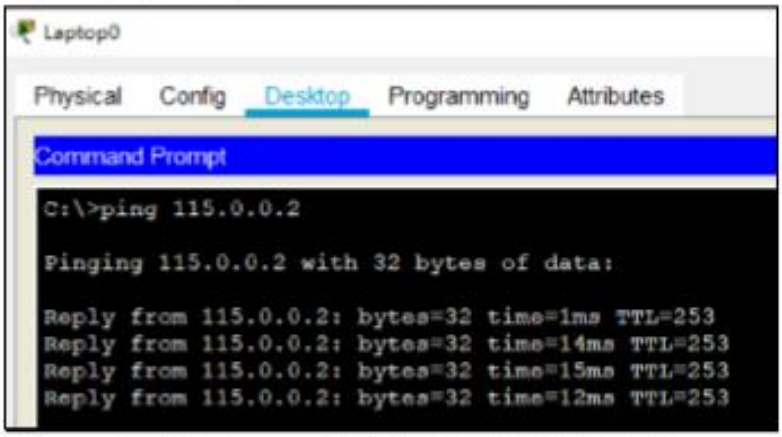

图3.22　Laptop0 访问 ISP 路由器应答信息

结果显示，销售部用户的计算机也能正常访问外网。

课堂练习：参照本任务，在边界路路由器配置 PAT，让企业内网所有用户都能访问到 ISP 的路由器。注：ISP 路由器上不能有任何内网的路由。

小贴士：运营商为用户提供互联网的接入服务。人们可以通过网络获取信息的方式更加方便、多样，大部分人特别是年轻人越来越主要地依靠网络获取信息。与此同时，网上也充斥着越来越多的虚假、低俗甚至反动、淫秽和暴力等信息内容，特别是一些有组织的网上恶意攻击和思想渗透行为，更是严重地影响了网络生活秩序。大学生应当正确使用网络，提高信息的获取能力，加强信息的辨识能力，增进信息的应用能力，使网络成为开阔视野、提高能力的重要工具。

网络互联技术

任务驱动式教程

扫此二维码下载
本书配套资源

人邮教育
www.ryjiaoyu.com

教材服务热线：010-81055256
反馈／投稿／推荐信箱：315@ptpress.com.cn
人邮教育服务与资源下载社区：www.ryjiaoyu.com

ISBN 978-7-115-56732-1

封面设计：董志桢