

实验九：园区网 NAT 接入互联网

一、实验简介

园区网内部通常使用私有 IP 地址，在访问互联网时需要经过 NAT 转换。

本实验在实验八的基础上，将防火墙作为园区网的边界设备，通过在防火墙上配置 NAT，使得园区网内部主机（配置私有 IP 地址）可以访问互联网。

二、实验目的

- 1、理解 NAT 的工作原理；
- 2、掌握华为防火墙配置 NAT 的方法；

三、实验学时

2 学时

四、实验类型

综合型

五、实验需求

- 1、硬件

每人一台计算机。

- 2、软件

计算机安装 Windows 10 操作系统、eNSP 网络仿真软件、VirtualBox 虚拟化软件

- 3、网络

实验本身内容不需要访问互联网。

- 4、工具

无

六、实验拓扑

本实验的网络拓扑如图 9-1 所示。其中“Internet”代表互联网。



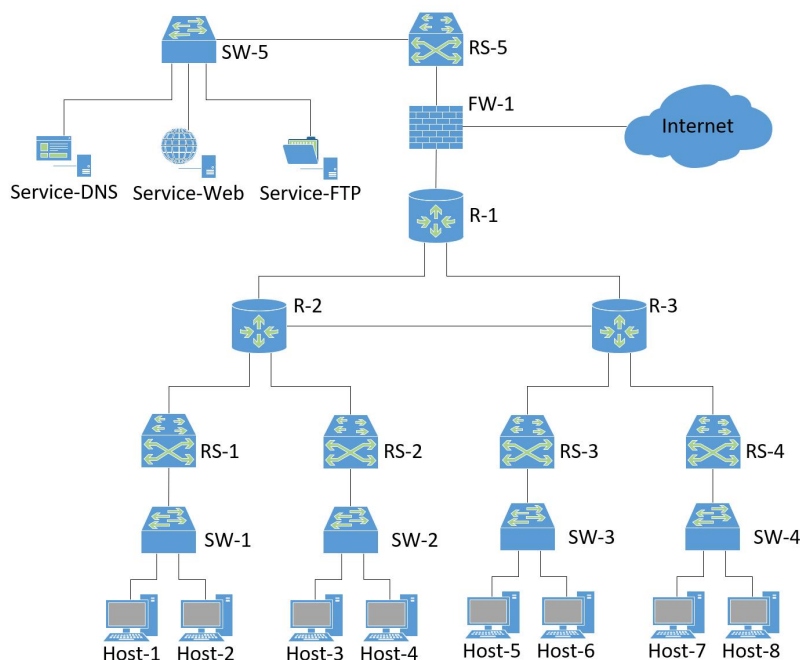


图 9-1 网络拓扑

七、实验要求

学生根据实验要求，自行完成相关实验。

1、园区网设计要求

园区网内部采用 OSPF 路由协议，其他配置参见实验八。

【提醒思考】本实验中，园区网内部主机若要访问互联网，则主机发出的报文，必须能够被转发至防火墙 FW-1，然后以 NAT 方式转发至互联网。此处的路由该如何实现？

2、互联网设计要求

2.1 拓扑要求

此处要求学生自主在 eNSP 中设计一个网络，作为互联网。用来验证 NAT 访问的效果。该“互联网”与园区网 FW-1 直接连接的是一台路由器 R1，此外，该“互联网”中必须至少包含路由器、三层交换机、二层交换机、主机，具体由学生自主设计。

2.2 地址要求

互联网采用公有 IP 地址，静态 IP 地址模式，具体由学生自定。但是，互联网主机的 IP 地址格式为 *.A.*，其中 A 是学生学号的后 3 位。

2.3 路由要求

互联网配置 OSPF 路由。

3、NAT 设计要求

本实验要求在园区网边界防火墙 FW-1 上设置 NAT，采用 NAPT（网络地址端口转换）模式，即园区网内部各主机，共用一个公有 IP（即 FW-1 连接互联网接口 IP 地址）访问互联网。

【提醒】如何在华为防火墙上配置 NAT，由学生自行查询相关资料，或见本课程参考书《网络运维管理从基础到实战》项目八一任务四—步骤 8。

4、通信要求

- 1) 园区网中的服务器网段，**可以** NAT 方式访问互联网主机；
- 2) 园区网中的 Host5-Host-8，**可以** NAT 方式访问互联网主机；
- 3) 园区网中的 Host1-Host-4，**不可以**访问互联网主机；
- 4) 互联网主机**不能**访问园区网内部主机。

八、思考与讨论

1. 本实验中，你采用的 NAT 方式是什么？这种方式有什么特点？
2. 假设执行 Host5 PING 互联网主机，描述一下 ICMP 请求报文从 Host5 到达互联网主机的过程中，报文首部中 IP 地址和 MAC 地址的变化。
3. 假设园区网内部用户主机访问互联网主机，则从内网主机发出的报文，是如何被路由到防火墙 FW-1 的？在所经过的路由设备的路由表中，找出匹配的路由记录。
4. 园区网主机访问互联网时，报文达到防火墙 FW-1 后，为什么能被转发到下一跳（即互联网的路由器 R1）？
5. 园区网内部路由设备是否知道到达互联网上各网络的具体路由？互联网上的路由设备是否知道到达园区网内部各网络的具体路由？
6. 互联网主机能 PING 通 FW-1 的 WAN 口（连接互联网的接口）吗？互联网主机为什么不能访问园区网内部主机？假设执行 互联网主机 PING Host5，互联网主机发出的 ICMP 报文到达哪里被丢弃？为什么？
7. 本实验中，园区网采用 OSPF，互联网也采用 OSPF，为什么相互之间没有交换路由信息？
8. 本实验中，园区网内部能否全网使用静态路由？谈谈你的理由。



九、实验考核（即形成性考核中的“实验实训”考核项目）

1. 学生在老师指定的时间内完成实验，并且当面提交老师检查，回答教师提出的问题。
2. 教师根据学生完成实验情况以及回答问题情况，给本次实验打分。

河南中医药大学信息技术学院

