

《网络运维管理》—— 实验指导书

实验一：园区网 NAT 接入互联网

一、实验简介

如果园区网只有一条出口链路，一旦该链路出现问题，则会造成全网无法访问互联网。因此，园区网通常建设多条出口链路，并分别接入不同的电信运营商，从而更好保障园区网对互联网的访问。

本实验在 eNSP 中的园区网出口构建双链路出口，并在园区网出口路由器上配置 NAT，使得园区网可以通过 NAT 访问互联网。

二、实验目的

- 1、掌握在路由器上配置 NAT 服务的方法；
- 2、实现双链路 NAT 接入互联网。

三、实验理论

- 1、网络地址转换（NAT）
- 2、接入互联网

四、实验规划

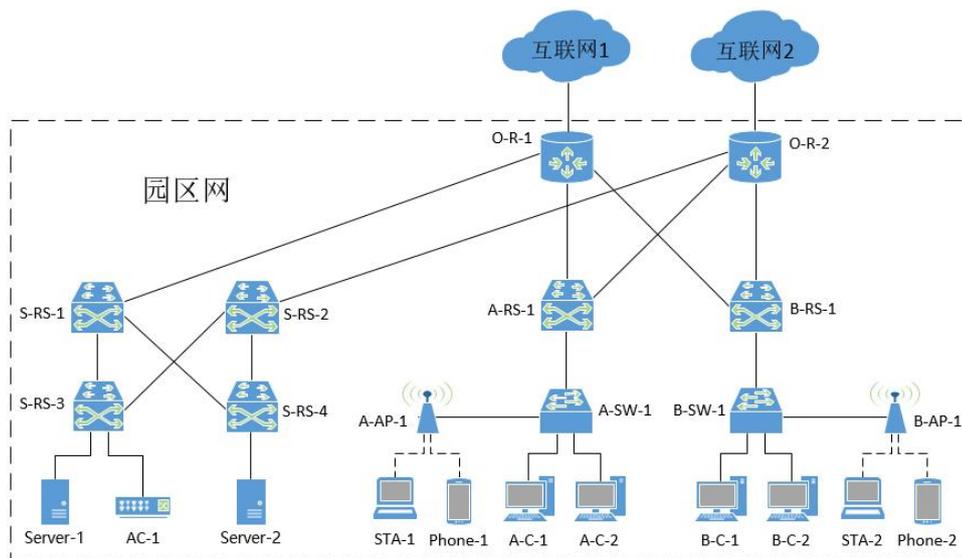


图 1 实验二网络拓扑规划

1、网络拓扑规划

表 1 网络设备说明

序号	设备线路	设备类型	规格型号	备注
1	A-C-1、A-C-2	用户主机	PC	A 区用户
2	B-C-1、B-C-2	用户主机	PC	B 区用户
3	STA-1、STA-2	移动终端	STA	移动用户
4	Phone-1、Phone-2	移动终端	Cellphone	移动用户
5	A-SW-1、B-SW-1	二层交换机	S3700	用户区域接入交换机
6	A-RS-1、B-RS-1	三层交换机	S5700	用户区域汇聚交换机
7	O-R-1、O-R-2	核心路由器	AR2220	核心区域路由器
8	S-RS-1、S-RS-2	三层交换机	S5700	数据中心汇聚交换机
9	S-RS-3、S-RS-4	三层交换机	S5700	数据中心接入交换机
10	A-AP-1、B-AP-1	无线接入点 (AP)	AP3030	接入移动终端
11	AC-1	无线控制器	AC6605	用于 AP 的管理和配置
12	Server-1	服务器 1	PC	用 PC 替代
13	Server-2	服务器 2	PC	用 PC 替代

【提醒】

- (1) 本任务中，必须保证实验用的计算机（即实体主机）能够正常访问互联网；
- (2) 本任务中，通过 eNSP 的云设备（Cloud）绑定本地实体主机的网卡时，要绑定有线网卡，若绑定无线网卡无法访问互联网；
- (3) 若实验用的计算机没有配置有线网卡，则学生可自行设计创建两个仿真网络，分别替代拓扑图中的“互联网 1”和“互联网 2”，只要能体现 NAT 的效果即可。

2、交换机 VLAN 设计**设计要求：**

- (1) 本实验采用基于端口划分 VLAN。
- (2) 用户主机（有线）VLAN 设计：第一个 VLAN ID 用自己的学号后两位+1 来定义。例如 2022181001，其第 1 个 VLAN 的 ID 是 2，后面的 VLAN 依次加 1，即 VLAN3、VLAN 4……
- (3) 移动终端（无线）VLAN 设计：第一个 VLAN ID 用自己的学号后两位+200 来定义。例如 2022181001，其第 1 个 VLAN 的 ID 是 201，后面的 VLAN 依次加 1，即 VLAN 202、VLAN203……
- (4) 无线用户终端采用 2.4GHz 和 5GHz 两个频段接入网络，分别属于不同 VLAN；
- (5) 其他 VLAN 设计：三层虚拟接口的 VLAN，AP 所属的 VLAN 等，由学生自行设计。

3、IP 地址设计**设计要求：**

- (1) 用户主机（含无线终端）IP 地址设计：格式是 192.A.B.*，其中，A 等于学号的最后两位，B 必须大于等于学号的后两位且小于等于学号后两位+5，*表示该位数值由考生自定。例如张三（2021181002）可以使用的 IP 地址范围是：192.2.2.0~192.2.7.255。**设计用户主机 IP 地址时要考虑路由聚合。**

注意：各网段的默认网关地址，使用本网段最后一个单播地址。

- (2) 服务器 IP 地址设计：格式是 172.16.A.*，其中，A 等于学号的最后两位，*表示该位数值由考生自定。

- (3) 路由接口 IP 地址设计：路由接口 IP 地址格式是 10.0.A.*。其中，A 等于学号的最后两位，

*表示该位数值由考生自定。

(4) 其他 IP 地址设计由学生自定。

【提醒】

本实验中的外网 IP 地址，与操作者的计算机（实体计算机）所接入的实际网络环境有关。

4、路由表规划

本实验采用 OSPF 协议。

五、实验任务及要求

本实验共包含 5 个任务，由学生独立完成。。

【提示】各任务的具体操作，可参考教材或课程网站

1、任务一：在 eNSP 中部署园区网（10 分）

根据实验规划，在 eNSP 中部署硬件设备。

2、任务二：实现园区网内部的通信（20 分）

根据前面规划设计的有关要求，完成园区网（不包含接入互联网）的通信配置，要求：

(1) 有线网络可以正常通信；

(2) 无线网络可以正常通信；

(3) 测试：关闭 S-RS-1 或 S-RS-2（保持其他设备正常工作），仍然可以实现用户区域和数据中心区域之间的通信；

(4) 测试：关闭 O-R-1 或 O-R-2（保持其他设备正常工作），仍然可以实现用户区域和数据中心区域之间的通信；

3、任务三：实现园区网接入互联网（20 分）

根据前面规划设计的有关要求，在园区网的边界路由器上配置 NAT，使得园区网内部用户可以访问互联网。

【再次提醒】

若实验用的计算机没有配置有线网卡，则学生可自行设计创建两个仿真网络，分别替代拓扑图中的“互联网 1”和“互联网 2”，只要能体现 NAT 的效果即可。

4、任务四：抓包验证 NAT 结果的报文（20 分）

在园区网边界路由器处抓取报文，验证 NAT 的结果，即报文在经过 NAT 设备时，源 IP 地址的变化。

5、扩展任务：互联网主机透过 NAT 访问内部服务器（不记分）

从互联网上的主机，反向透过 NAT，访问（ping）园区网内部的服务器 Server1。

注意：此任务为扩展任务，不做考核。学生自行查询相关资料，完成任务要求。



六、实验考核

实验考核从【完成维度】和【时间维度】两个维度进行评分。

1、【完成维度】考核

本维度主要考核学生完成实验的程度以及对实验内容的理解程度，包括【任务完成度】和【回答问题】两个部分。具体如下：

(1) 任务完成度 (70 分)

学生在完成实验后，要当面提交教师检查实验结果。教师检查每个实验任务的完成情况，并根据实验指导书中每个任务的分值，给出任务完成度的分数。本项目满分 70 分。

(2) 回答问题 (30 分)

学生在完成实验后，要当面提交教师检查实验结果，并回答教师提问。教师根据学生回答情况评分。本项目满分 30 分。

【注意】：教师提问时，可参考“七、思考与讨论”中的问题，从中随机选取 2-3 个问题进行提问。

2、【时间维度】考核

本维度主要考核学生完成实验的时间，具体如下：

(1) 当堂提交 (100 分起评)

本实验的实验课当堂提交并通过【完成维度】考核的，从 100 分起评。

(2) 一周内提交 (90 分起评)

本实验的实验课结束一周内提交并通过【完成维度】考核的，从 90 分起评，即本次实验考核最高 90 分。

(3) 一周后提交 (80 分起评)

本实验的实验课结束一周后提交并通过【完成维度】考核的，从 80 分起评，即本次实验考核最高 80 分。

(4) 未提交 (0 分)

本学期教学工作结束时，仍未提交的，本次实验考核 0 分。

七、思考与讨论

学生在做实验时，要结合实验内容和过程，讨论分析以下问题，以备教师提问

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. 从园区网内部的主机访问互联网主机的过程中，描述一下 ICMP 报文首部中，IP 地址和 MAC 地址的变化。
3. 在配置边界路由器 O-R-1 和 O-R-2 时，如果不使用 `default-route-advertise always` 命令，则用户主机 A-C-1 能够正常访问互联网主机吗？举例说明原因。
4. 如果在配置边界路由器 O-R-1 和 O-R-2 时，不使用 `default-route-advertise always` 命令，但在用户区域的三层交换机上配置一条默认路由（例如 `ip route-static 0.0.0.0 0.0.0.0 下一跳地址`），能否实现“当一台边界路由器故障时，内部网用户仍然可以通过另一条出口链路访问互联网”？



请学生自行实验验证，并分析原因。

5. 本实验中，园区网边界路由器 O-R-1 和 O-R-2 的出接口 IP 地址是配置成相同网段的地址，还是不同网段的地址？谈谈你的理由。
6. 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。
7. 本实验中，`default-route-advertise` 命令起到了什么作用？

河南中医药大学互联网技术教学团队

