|  |  |  |  |
| --- | --- | --- | --- |
| **实训日志** | | | |
| 实训时间 | 2019年9月11日 | 实训地点 | 逸夫教学楼418教室 |
| 实训内容 | 1. 配置telnet安全防护，在设备上设定ACL，并在line 0 4 中应用，使用PC2 和PC3进行测试； 2. 在SW1和SW2上部署ACL，实现不允许宿舍访问服务器，使用PC2和PC3进行测试； 3. 在总校区R1，和分校区A R2上部署NAT，分校区B通过总校区访问外网。 | | |
| 收获感想 | 1. 访问控制列表简称为ACL，它使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL 分很多种，不同场合应用不同种类的ACL，如标准ACL、扩展ACL和命名ACL； 2. NAT（网络地址转换）将私有（保留）地址的"内部"网络通过路由器发送数据包时，私有地址被转换成合法的IP地址，一个局域网只需使用少量IP地址（甚至是1个）即可实现私有地址网络内所有计算机与Internet的通信需求。 3. NAT将自动修改IP报文的源IP地址和目的IP地址，Ip地址校验则在NAT处理过程中自动完成。有些应用程序将源IP地址嵌入到IP报文的数据部分中，所以还需要同时对报文的数据部分进行修改，以匹配IP头中已经修改过的源IP地址。否则，在报文数据部分嵌入IP地址的应用程序就不能正常工作。 | | |