利用 eNSP 仿真软件实现 ACL 配置实训的教学设计

蒋振根

（福建省邮电学校，福建福州 350008）

【摘要】文章介绍了 eNSP 网络仿真工具平台和 ACL 工作原理，基于 eNSP 仿真软件进行计算机网络技术实训教学设计，模拟分析了企业网络环境，提出了实训设计构想，并加以模拟组网实现。通过采用 ACL 配置，该实训设计可以满足企业的网络安全需求。

【关键词】eNSP；访问控制列表；实训

【doi:10.3969/j.issn.2095-7661.2020.01.008】

【中图分类号】TP393.01　　【文献标识码】A　　【文章编号】2095-7661(2020)01-0025-04

Practical Teaching Design of ACL Configuration with the Simulation Software of eNSP

JIANG Zhen-gen

(Fujian Posts and Telecommunications School, Fuzhou, Fujian, China 350008)

Abstract: This paper introduces the eNSP network simulation tool platform and ACL working principle. Based on the eNSP simulation software, the computer network technology training teaching design is carried out. The enterprise network environment is simulated and analyzed, the training design concept is proposed, and the simulation networking is realized. By using ACL configuration, the training design can meet the network security needs of enterprises.

Keywords: eNSP; access control list; practical training

计算机网络技术是职业院校计算机专业和通信专业的核心专业课程之一，该课程的教学分为理论教学和实训教学两个部分。[1]理论部分的教学目前已有较成熟的教学方式，而实训部分的教学，在以往的实训教学设计中，受到交换机、路由器等物理数据设备数量的限制，使学生需要分组才能进行实训教学。这样的设计方式，既难以保证每位学生的实训时间，也难以很好的帮助学生理解相关协议的工作原理和工作方式。[2]为解决上述问题，本文对借由 eNSP 仿真软件实现计算机网络技术课程中的“访问控制列表配置”实训进行了教学设计的尝试。

eNSP 软件是一款由华为公司提供的免费的、可扩展的、图形化操作的网络仿真工具平台，[3]主要对企业网络路由器、交换机等数据设备进行软件仿真，较完美呈现真实设备实景，并支持大型网络组网的模拟，让广大学习者有机会在没有真实物理设备的情况下模拟演练，学习网络技术。

1 实训原理

访问控制列表 ACL(Access Control List)是路由器和交换机接口的指令列表，用来控制端口进出的数据包，是一种应用非常广泛的网络技术，它的基本原理极为简单：配置了 ACL 的网络设备根据事先设定好的报文匹配规则对经过该设备的报文进行匹配，然后对匹配上的报文执行事先设定好的处理动作。[4]这些匹配规则及相应的处理动作是根据具体的网络需求而设定的。处理动作的不同以及匹配规则的多样性，使得 ACL 可以发挥出各种各样的功效。

ACL 通常是由 permit 或 deny 语句组成的一系列

[收稿日期] 2019-10-29

[作者简介] 蒋振根(1974-)，男，福建尤溪人，福建省邮电学校(福州)高级讲师、高级工程师，工学学士，研究方向：有线通信网络的规划与设计。

[基金项目] 福建省教育厅中青年教师教育科研项目(科技类)2018 年度课题“现代学徒制下 ICT 定向班人才培养模式的研究”(课题编号：JZ181091)。

有顺序的规则集合，每条语句就是该 ACL 的一条规则，每条语句中的 permit 或 deny 就是与这条规则相对应的处理动作。处理动作 permit 的含义是“允许”，处理动作 deny 的含义是“拒绝”。ACL 规则可以根据数据包的源地址、目的地址、源端口、目的端口等信息来描述。ACL 规则通过匹配报文中的信息对数据包进行分类，路由设备根据这些规则判断哪些数据包可以通过，哪些数据包需要拒绝。

按照 ACL 的用途，可以分为基本的访问控制列表和高级的访问控制列表。基本 ACL 可使用报文的源 IP 地址、时间段信息来定义规则，编号范围为 2000~2999。高级的访问控制列表在匹配项上做了扩展，编号范围为 3000~3999，既可使用报文的源 IP 地址，也可使用目的地址、IP 优先级、IP 协议类型、ICMP 类型、TCP 源端口 / 目的端口、UDP 源端口 / 目的端口号等信息来定义规则。高级访问控制列表可以定义比基本访问控制列表更准确、更丰富、更灵活的规则，因此得到更加广泛的应用。

2 实训设计构想

本实训模拟一家企业网络环境，R1 为分支机构 A 管理员所在 IT 部门的网关，R2 为分支机构 A 用户部门的网关，R3 为分支机构 A 去往总部出口的网关设备，R4 为总部核心路由器设备。整网运行 OSPF 协议，并在区域 0 内。企业要求通过远程方式管理核心路由器 R4，并要求前期只能由 R1 所连的 PC（本实训使用环回接口 l0 模拟）访问 R4，其他设备均不能访问；后期 R1 所连的 PC（本实训使用环回接口 l0 模拟）只能管理 R4 上的 4.4.4.4 这台服务器（本实训使用环回接口 l0 模拟），另一台同样直连 R4 的服务器 40.40.40.40 不能被管理（本实训使用环回接口 l1 模拟）。模拟企业网络环境的需求，利用 eNSP 仿真软件完成访问控制列表实训拓扑图的搭建，如图 1 所示。

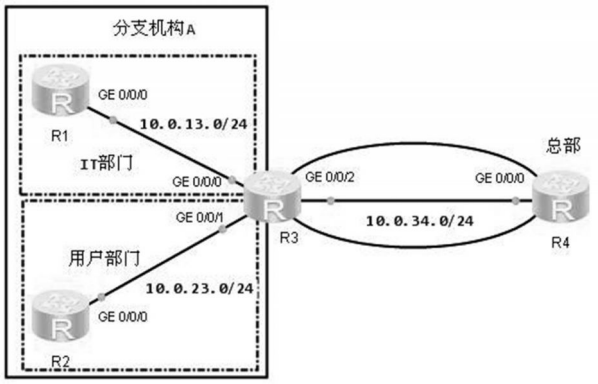

图 1 访问控制列表实训拓扑图

3 数据规划

根据访问控制列表实训拓扑图及模拟企业环境的需求，完成如表 1 所示的 IP 地址规划。

表 1 IP 地址规划表

设备	接口	IP 地址	子网掩码	默认网关
R1（AR2220）	GE0/0/0	10.0.13.1	255.255.255.0	N/A
	Loopback0	1.1.1.1	255.255.255.255	N/A
R2（AR2220）	GE0/0/0	10.0.23.2	255.255.255.0	N/A
R3（AR2220）	GE0/0/0	10.0.13.3	255.255.255.0	N/A
	GE0/0/1	10.0.23.3	255.255.255.0	N/A
	GE0/0/2	10.0.34.3	255.255.255.0	N/A
	Loopback0	3.3.3.3	255.255.255.255	N/A
R4（AR2220）	GE0/0/0	10.0.34.4	255.255.255.0	N/A
	Loopback0	4.4.4.4	255.255.255.255	N/A
	Loopback1	40.40.40.40	255.255.255.255	N/A

4 实训实施过程

4.1 基本配置

根据表 1IP 地址数据规划表完成各路由器设备的基本配置，并使用 ping 命令检测各直连链路的连通性。各路由器设备的基本配置命令如下：

```
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 10.0.13.1 24
[R1-GigabitEthernet0/0/0]int loopback0
[R1-LoopBack0]ip add 1.1.1.1 32
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 10.0.23.2 24
[R3]int g0/0/0
[R3-GigabitEthernet0/0/0]ip add 10.0.13.3 24
[R3-GigabitEthernet0/0/0]int g0/0/1
[R3-GigabitEthernet0/0/1]ip add 10.0.23.3 24
[R3-GigabitEthernet0/0/1]int g0/0/2
[R3-GigabitEthernet0/0/2]ip add 10.0.34.3 24
[R3-GigabitEthernet0/0/2]int loopback0
[R3-LoopBack0]ip add 3.3.3.3 32
[R4]int g0/0/0
[R4-GigabitEthernet0/0/0]ip add 10.0.34.4 24
[R4-GigabitEthernet0/0/0]int loopback0
[R4-LoopBack0]ip add 4.4.4.4 32
[R4-LoopBack0] int loopback1
[R4-LoopBack1]ip add 40.40.40.40 32
```

在 R1 路由器设备上执行 ping -c 1 10.0.13.3 命令，若显示结果如图 2 所示，则表示测试通过，其余直连网段的连通性测试省略。

```
[R1]ping -c 1 10.0.13.3
  PING 10.0.13.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.13.3: bytes=56 Sequence=1 ttl=255 time=650 ms

  --- 10.0.13.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 650/650/650 ms
```

图 2 R1 与 R3 路由器连通性的测试图

4.2 搭建 OSPF 网络

在所有路由器上运行 OSPF 协议，通告相应网段至区域 0 中，各路由器配置命令如下：

[R1]ospf 1

[R1-ospf-1]area 0

[R1-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255

[R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0

[R2]ospf 1

[R2-ospf-1]area 0

[R2-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255

[R3]ospf 1

[R3-ospf-1]area 0

[R3-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255

[R3-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255

[R3-ospf-1-area-0.0.0.0]network 10.0.34.0 0.0.0.255

[R3-ospf-1-area-0.0.0.0]network 3.3.3.3 0.0.0.0

[R4]ospf 1

[R4-ospf-1]area 0

[R4-ospf-1-area-0.0.0.0]network 10.0.34.0 0.0.0.255

[R4-ospf-1-area-0.0.0.0]network 4.4.4.4 0.0.0.0

[R4-ospf-1-area-0.0.0.0]network 40.40.40.40 0.0.0.0

配置完成之后，在 R1 的路由器上查看 OSPF 路由信息，如图 3 所示。

```
[R1]dis ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Public routing table : OSPF
         Destinations : 5        Routes : 5

OSPF routing table status : <Active>
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        3.3.3.3/32  OSPF    10   1           D   10.0.13.3       GigabitEthernet
0/0/0
        4.4.4.4/32  OSPF    10   2           D   10.0.13.3       GigabitEthernet
0/0/0
      10.0.23.0/24  OSPF    10   2           D   10.0.13.3       GigabitEthernet
0/0/0
      10.0.34.0/24  OSPF    10   2           D   10.0.13.3       GigabitEthernet
0/0/0
    40.40.40.40/32  OSPF    10   2           D   10.0.13.3       GigabitEthernet
0/0/0

OSPF routing table status : <Inactive>
         Destinations : 0        Routes : 0
```

图 3　R1 路由器的 OSPF 路由信息图

由图 3 可以看出，路由器 R1 已经学习到了相关网段的路由条目，用 ping 命令测试 R1 环回口 l0 与 R4 环回口 l0 间的连通性，如图 4 所示。

```
[R1]ping -c 1 -a 1.1.1.1 4.4.4.4
  PING 4.4.4.4: 56  data bytes, press CTRL_C to break
    Reply from 4.4.4.4: bytes=56 Sequence=1 ttl=254 time=760 ms

  --- 4.4.4.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 760/760/760 ms
```

图 4　R1 环回口 l0 与 R4 环回口 l0 间的连通性测试图

由图 4 可以看出，R1 环回口 l0 与 R4 环回口 l0 间的通信正常，其他路由器之间测试省略。

4.3 采用基本 ACL 配置完成企业前期的网络需求

在总部核心路由器 R4 上完成 telnet 功能的相关配置，配置用户密码，配置命令如下：

[R4]user-interface vty 0 4

[R4-ui-vty0-4]authentication-mode password

Please configure the login password (maximum length 16):huawei

配置完成后，尝试在 IT 部门网关设备 R1 上与 R4 路由器设备建立 telnet 连接，如图 5 所示。

```
<R1>
<R1>telnet 4.4.4.4
  Press CTRL_] to quit telnet mode
  Trying 4.4.4.4 ...
  Connected to 4.4.4.4 ...

Login authentication


Password:
<R4>
```

图 5　配置 ACL 前 R1 与 R4 的 telnet 连接图

由图 5 可以观察到，R1 可以成功登录 R4。再尝试在普通员工部门网关设备 R2 上与 R4 路由器设备建立 telnet 连接，如图 6 所示。

```
<R2>telnet 4.4.4.4
  Press CTRL_] to quit telnet mode
  Trying 4.4.4.4 ...
  Connected to 4.4.4.4 ...

Login authentication


Password:
<R4>
```

图 6　配置 ACL 前 R2 与 R4 的 telnet 连接图

综合图 5、图 6 可以发现，只要与核心路由器 R4 之间的路由是可达的，并且拥有 telnet 的密码，都可以成功访问核心设备 R4。这显然是极为不安全的。网络管理员可以通过配置标准 ACL 来实现访问过滤，禁止普通员工设备登录核心路由器 R4。基本的 ACL 可以针对数据包的源 IP 地址进行过滤，在 R4 上使用 acl 命令创建一个编号型 ACL，基本 ACL 的编号范围是 2000-2999。

[R4]acl 2000

接下来在 ACL 视图中，使用 rule 命令配置 ACL 规则，指定规则 ID 为 5，允许数据包源地址为 1.1.1.1 的报文通过，反掩码为全 0，即精确匹配。

[R4-acl-basic-2000]rule 5 permit source 1.1.1.1 0

使用 rule 命令配置第二条规则，指定规则 ID 为 10，拒绝任意源地址的数据包通过。

[R4-acl-basic-2000]rule 10 deny source any

ACL 配置完成后，在 VTY 中调用。使用 inbound 参数，即在 R4 的数据入方向上调用。

[R4]user-interface vty 0 4

[R4-ui-vty0-4]acl 2000 inbound

配置完成后，使用 R1 的环回口地址 1.1.1.1 测试访问 4.4.4.4 的连通性，如图 7 所示。

```
<R1>telnet -a 1.1.1.1 4.4.4.4
  Press CTRL_] to quit telnet mode
  Trying 4.4.4.4 ...
  Connected to 4.4.4.4 ...

Login authentication


Password:
<R4>
```

图 7 配置 ACL 后 R1 与 R4 的 telnet 连接图

发现没有问题，然后尝试在 R2 上访问 R4，如图 8 所示。

```
<R2>telnet 4.4.4.4
  Press CTRL_] to quit telnet mode
  Trying 4.4.4.4 ...
  Error: Can't connect to the remote host
<R2>
```

图 8 配置 ACL 后 R2 与 R4 的 telnet 连接图

可以观察到，此时 R2 已经无法访问 4.4.4.4，即上述 ACL 配置已经生效。

4.4 采用高级 ACL 配置完成企业后期的网络需求

根据企业后期网络设计的要求，R1 的环回接口只能通过 R4 上的 4.4.4.4 进行 telnet 访问，但是不能通过 40.40.40.40 进行 telnet 访问。如果要 R1 只能通过访问 R4 的 l0 环回口地址登录设备，即同时要匹配数据包的源地址和目的地址实现过滤，此时通过基本 ACL 是无法实现的，因为 ACL 只能通过匹配源地址实现过滤，所以需要使用到高级 ACL。在 R4 上使用 acl 命令创建一个高级 ACL3000。

[R4]acl 3000

在高级 ACL 视图中，使用 rule 命令配置 ACL 规则，ip 为协议类型，允许源地址为 1.1.1.1、目的地址为 4.4.4.4 的数据包通过。

[R4-acl-adv-3000]rule permit ip source 1.1.1.1 0 destination 4.4.4.4 0

配置完成后，查看 ACL 配置信息，如图 9 所示。

```
[R4-acl-adv-3000]dis acl all
 Total quantity of nonempty ACL number is 2

Basic ACL 2000, 2 rules
Acl's step is 5
 rule 5 permit source 1.1.1.1 0 (1 matches)
 rule 10 deny (1 matches)

Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit ip source 1.1.1.1 0 destination 4.4.4.4 0
```

图 9 查看 ACL 配置信息图

可以观察到，在不指定规则 ID 的情况下，默认步长为 5，第一条规则的规则 ID 即为 5。将 ACL3000 调用在 VTY 下，使用 inbound 参数，即在 R4 的数据入方向上调用。

[R4]user-interface vty 0 4

[R4-ui-vty0-4]acl 3000 inbound

配置完成后，在 R1 上使用环回口地址 1.1.1.1 尝试访问 40.40.40.40，如图 10 所示。

```
<R1>telnet -a 1.1.1.1 40.40.40.40
  Press CTRL_] to quit telnet mode
  Trying 40.40.40.40 ...
  Error: Can't connect to the remote host
<R1>
```

图 10 配置高级 ACL 后 R1 与 R4 的 telnet 连接图

可以观察到，此时过滤已经实现，R1 不能使用环回口地址访问 40.40.40.40。

5 结束语

利用 eNSP 仿真软件可以完美模拟路由器访问控制列表的实训。利用 eNSP 仿真软件可以解决计算机网络技术课程实训部分教学中存在的问题：在交换机、路由器设备不足的情况下，学生可以在自己的电脑上安装该免费仿真软件，随时随地自主学习，极大提高学生的学习积极性。[5]eNSP 仿真软件应用于计算机网络技术实训教学，对提高学生的职业技能、创新能力和就业能力具有极大的帮助。

【参考文献】

[1]于鉴桐.信息化环境下的课堂教学设计研究与实践[J].湖南邮电职业技术学院学报,2019(4):38-40.

[2]李妍.信息化整合背景下《计算机网络》课程教学设计研究[J].计算机产品与流通,2019(9):266.

[3]孟祥成.基于 eNSP 的二层 VLAN 虚拟仿真实验[J].实验室研究与探索,2017(9):102-106.

[4]华为技术有限公司.HCNA 网络技术学习指南[M].北京：人民邮电出版社,2015.

[5]林金山，林金慧.基于面向创新人才培养的《计算机网络》课程教学探讨[J].当代教育实践与教学研究,2019(19):43-44.