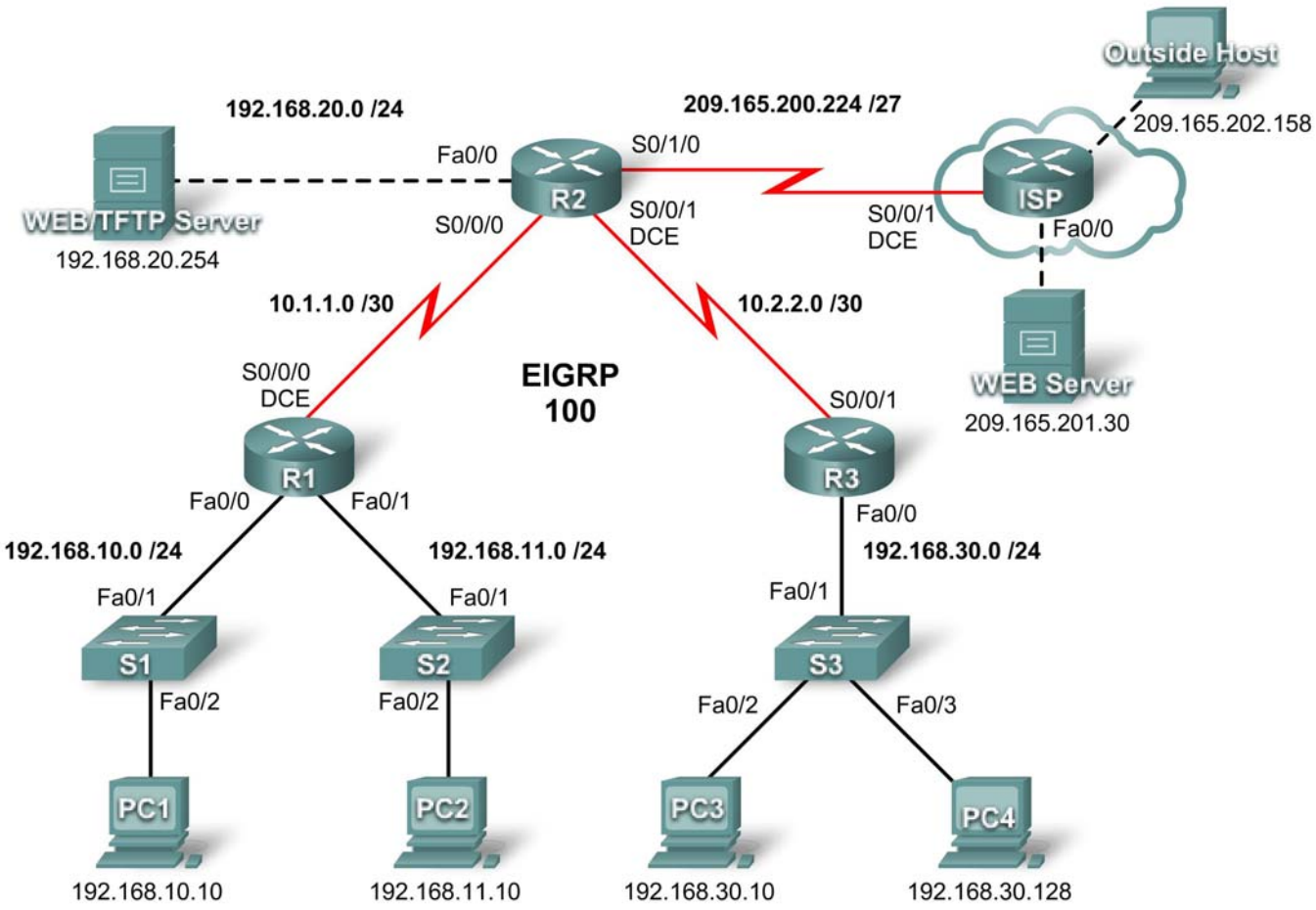
PT 练习 5.3.4：配置扩展 ACL

拓扑图



地址表

设备	接口	IP 地址	子网掩码
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.2	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.1	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	网卡	192.168.10.10	255.255.255.0
PC2	网卡	192.168.11.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0
PC4	网卡	192.168.30.128	255.255.255.0
WEB/TFTP Server	网卡	192.168.20.254	255.255.255.0
WEB Server	网卡	209.165.201.30	255.255.255.224
Outside Host	网卡	209.165.202.158	255.255.255.224

学习目标

- 检查当前的网络配置
- 评估网络策略并规划 ACL 实施
- 配置采用数字编号的扩展 ACL
- 配置命名扩展 ACL

简介

扩展 ACL 是一种路由器配置脚本，根据源地址、目的地址，以及协议或端口来控制路由器应该允许还是应该拒绝数据包。扩展 ACL 比标准 ACL 更加灵活而且精度更高。本练习的主要内容是定义过滤标准、配置扩展 ACL、将 ACL 应用于路由器接口并检验和测试 ACL 实施。路由器已经过配置，包括 IP 地址和 EIGRP 路由。用户执行口令是 **cisco**，特权执行口令是 **class**。

任务 1：检查当前的网络配置

步骤 1. 查看路由器的运行配置。

逐一在三台路由器的特权执行模式下使用 **show running-config** 命令查看运行配置。请注意，接口和路由已配置完整。将 IP 地址配置与上面的地址表相比较。此时，路由器上应该尚未配置任何 ACL。

本练习不需要配置 ISP 路由器。假设 ISP 路由器不属于您的管理范畴，而是由 ISP 管理员配置和维护。

步骤 2. 确认所有设备均可访问所有其它位置。

将任何 ACL 应用于网络中之前，都必须确认网络完全连通。如果应用 ACL 之前不测试网络连通性，排查故障会非常困难。

要确保整个网络连通，请在不同的网络设备之间使用 **ping** 命令和 **tracert** 命令检验连接。

任务 2：评估网络策略并规划 ACL 实施

步骤 1. 评估 R1 LAN 的策略。

- 对于 192.168.10.0/24 网络，阻止 telnet 访问所有位置，并且阻止通过 TFTP 访问地址为 192.168.20.254 的企业 Web/TFTP Server。允许所有其它访问。
- 对于 192.168.11.0/24 网络，允许通过 TFTP 和 Web 访问地址为 192.168.20.254 的企业 Web/TFTP Server。阻止从 192.168.11.0/24 网络发往 192.168.20.0/24 网络的所有其它流量。允许所有其它访问。

步骤 2. 为 R1 LAN 规划 ACL 实施。

- 用两个 ACL 可完全实施 R1 LAN 的安全策略。
- 第一个 ACL 支持策略的第一部分，配置在 R1 上并应用于 Fast Ethernet 0/0 接口的入站流量。
- 第二个 ACL 支持策略的第二部分，配置在 R1 上并应用于 Fast Ethernet 0/1 接口的入站流量。

步骤 3. 评估 R3 LAN 的策略。

- 阻止 192.168.30.0/24 网络的所有 IP 地址访问 192.168.20.0/24 网络的所有 IP 地址。
- 允许 192.168.30.0/24 的前一半地址访问所有其它目的地址。
- 允许 192.168.30.0/24 的后一半地址访问 192.168.10.0/24 网络和 192.168.11.0/24 网络。
- 允许 192.168.30.0/24 的后一半地址通过 Web 访问和 ICMP 访问所有其余目的地址。
- 明确拒绝所有其它访问。

步骤 4. 为 R3 LAN 规划 ACL 实施。

本步骤需要在 R3 上配置一个 ACL 并应用于 FastEthernet 0/0 接口的入站流量。

步骤 5. 评估通过 ISP 进入的 Internet 流量的策略。

- 仅允许 Outside Host 通过端口 80 与内部 Web Server 建立 Web 会话。
- 仅允许已建立 TCP 会话进入。
- 仅允许 ping 应答通过 R2。

步骤 6. 为通过 ISP 进入的 Internet 流量规划 ACL 实施。

本步骤需要在 R2 上配置一个 ACL 并应用于 Serial 0/1/0 接口的入站流量。

任务 3：配置采用数字编号的扩展 ACL

步骤 1. 确定通配符掩码。

在 R1 上实施访问控制策略需要两个 ACL。这两个 ACL 将用于拒绝整个 C 类网络。您需要配置一个通配符掩码，匹配这些 C 类网络中每个网络的所有主机。

例如，要匹配整个 192.168.10.0/24 子网，通配符掩码就应为 0.0.0.255。此掩码可以理解为“检查、检查、检查、忽略”，实质上能匹配整个 192.168.10.0/24 网络。

步骤 2. 为 R1 配置第一个扩展 ACL。

在全局配置模式下，使用编号 110 配置第一个 ACL。首先需要阻止 192.168.10.0/24 网络中的所有 IP 地址 telnet 至任何位置。

编写语句时，请确定您目前处于全局配置模式下。

```
R1(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```

接下来要阻止 192.168.10.0/24 网络中的所有 IP 地址通过 TFTP 访问地址为 192.168.20.254 的主机。

```
R1(config)#access-list 110 deny udp 192.168.10.0 0.0.0.255 host
192.168.20.254 eq tftp
```

最后要允许所有其它流量。

```
R1(config)#access-list 110 permit ip any any
```

步骤 3. 为 R1 配置第二个扩展 ACL。

用编号 111 配置第二个 ACL。允许 192.168.11.0/24 网络中的任何 IP 地址通过 WWW 访问地址为 192.168.20.254 的主机。

```
R1(config)#access-list 111 permit tcp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq www
```

然后，允许 192.168.11.0/24 网络中的任何 IP 地址通过 TFTP 访问地址为 192.168.20.254 的主机。

```
R1(config)#access-list 111 permit udp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq tftp
```

阻止从 192.168.11.0/24 网络发往 192.168.20.0/24 网络的所有其它流量。

```
R1(config)#access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0
0.0.0.255
```

最后，允许任何其它流量。此语句用于确保不会阻止来自其它网络的流量。

```
R1(config)#access-list 111 permit ip any any
```

步骤 4. 检验 ACL 配置。

在 R1 上发出 **show access-lists** 命令，确认您的配置。输出应类似下例：

```
R1#show access-lists
Extended IP access list 110
   deny tcp 192.168.10.0 0.0.0.255 any eq telnet
   deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
   permit ip any any
Extended IP access list 111
   permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
   permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
   deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
   permit ip any any
```

步骤 5. 将语句应用到接口。

要将 ACL 应用到某个接口，请进入该接口的接口配置模式。配置 **ip access-group** *access-list-number* {**in** | **out**} 命令，将相应 ACL 应用于该接口。

每个 ACL 都用于过滤入站流量。将 ACL 110 应用于 Fast Ethernet 0/0 接口，ACL 111 应用于 Fast Ethernet 0/1 接口。

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group 110 in
R1(config-if)#interface fa0/1
R1(config-if)#ip access-group 111 in
```

确认这两个 ACL 显示于 R1 的运行配置中而且已应用到正确的接口。

步骤 6. 测试 R1 上配置的 ACL。

配置和应用 ACL 后，必须测试是否能按照预期阻止或允许流量。

- 尝试从 PC1 telnet 访问任何设备。此流量应该阻止。
- 尝试从 PC1 通过 HTTP 访问企业 Web/TFTP Server。此流量应该允许。
- 尝试从 PC2 通过 HTTP 访问 Web/TFTP Server。此流量应该允许。
- 尝试从 PC2 通过 HTTP 访问外部 Web Server。此流量应该允许。

根据您掌握的 ACL 知识，尝试从 PC1 和 PC2 执行一些其它的连通性测试。

步骤 7. 检查结果。

Packet Tracer 不支持测试 TFTP 访问，因此您无法检验该策略。不过，完成比例应为 50%。如果并非如此，请单击 **Check Results（检查结果）**查看尚未完成哪些必要部分。

任务 4：为 R3 配置命名扩展 ACL

步骤 1. 确定通配符掩码。

192.168.30.0/24 网络中前一半 IP 地址的访问策略有如下要求：

- 拒绝其访问 192.168.20.0/24 网络
- 允许其访问所有其它目的地址

对 192.168.30.0/24 网络中的后一半 IP 地址有如下限制：

- 允许其访问 192.168.10.0 和 192.168.11.0
- 拒绝其访问 192.168.20.0
- 允许其对所有其它位置的 Web 访问和 ICMP 访问

要确定通配符掩码，应考虑 ACL 在匹配 IP 地址 0–127（前一半）或 128–255（后一半）时需要检查哪些位。

我们学过，确定通配符掩码的方法之一是从 255.255.255.255 中减去标准网络掩码。对 C 类地址而言，IP 地址 0–127 和 128–255 的标准掩码是 255.255.255.128。用减法可得出正确的通配符掩码：

```
   255.255.255.255
 – 255.255.255.128
------------------
     0.  0.  0.127
```

步骤 2. 在 R3 上配置扩展 ACL。

在 R3 上，进入全局配置模式并以 130 作为访问列表编号配置 ACL。

第一条语句用于阻止 192.168.30.0/24 访问 192.168.30.0/24 网络中的所有地址。

```
R3(config)#access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

第二条语句用于允许 192.168.30.0/24 网络的前一半地址访问任何其它目的地址。

```
R3(config)#access-list 130 permit ip 192.168.30.0 0.0.0.127 any
```

其余的语句则明确允许 192.168.30.0/24 网络的后一半地址访问网络策略允许的网络和服务。

```
R3(config)#access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0
0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0
0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

步骤 3. 将语句应用到接口。

要将 ACL 应用到某个接口，请进入该接口的接口配置模式。配置 **ip access-group** *access-list-number* {**in** | **out**} 命令，将相应 ACL 应用于该接口。

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group 130 in
```

步骤 4. 检验和测试 ACL。

配置和应用 ACL 后，必须测试是否能按照预期阻止或允许流量。

- 从 PC3 ping Web/TFTP Server。此流量应该阻止。
- 从 PC3 ping 任何其它设备。此流量应该允许。
- 从 PC4 ping Web/TFTP Server。此流量应该阻止。
- 从 PC4 通过 192.168.10.1 或 192.168.11.1 接口 telnet 至 R1。此流量应该允许。
- 从 PC4 ping PC1 和 PC2。此流量应该允许。
- 从 PC4 通过 10.2.2.2 接口 telnet 至 R2。此流量应该阻止。

经过测试并得出正确结果后，在 R3 上使用 **show access-lists** 特权执行命令检查 ACL 语句是否存在匹配。

根据您掌握的 ACL 知识执行其它测试，检查每条语句匹配的流量是否正确。

步骤 5. 检查结果。

完成比例应为 75%。如果并非如此，请单击 **Check Results（检查结果）**查看尚未完成哪些必要部分。

任务 5：配置命名扩展 ACL

步骤 1. 在 R2 上配置命名扩展 ACL。

前面讲过，R2 上配置的策略将用于过滤 Internet 流量。由于 R2 连接到 ISP，因此它是配置 ACL 的最佳位置。

在 R2 上使用 **ip access-list extended** *name* 命令配置名为 FIREWALL 的命名 ACL。此命令使路由器进入扩展命名 ACL 配置模式。请留意路由器提示符已更改。

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#
```

在 ACL 配置模式下添加语句，按照策略中所述的要求过滤流量：

- 仅允许 Outside Host 通过端口 80 与内部 Web Server 建立 Web 会话。
- 仅允许已建立 TCP 会话进入。
- 允许 ping 应答通过 R2。

```
R2(config-ext-nacl)#permit tcp any host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#deny ip any any
```

在 R2 上配置了 ACL 后，使用 **show access-lists** 命令确认该 ACL 语句正确。

步骤 2. 将语句应用到接口。

使用 **ip access-group** *name* {**in** | **out**} 命令，将 ACL 应用于 ISP 的入站流量，面向 R2 的接口。

```
R3(config)#interface s0/1/0
R3(config-if)#ip access-group FIREWALL in
```

步骤 3. 检验和测试 ACL。

执行下列测试，确保 ACL 能达到预期效果。

- 从 Outside Host 打开内部 Web/TFTP Server 中的网页。此流量应该允许。
- 从 Outside Host ping 内部 Web/TFTP Server。此流量应该阻止。
- 从 Outside Host ping PC1。此流量应该阻止。
- 从 PC1 ping 地址为 209.165.201.30 的外部 Web Server。此流量应该允许。
- 从 PC1 打开外部 Web Server 中的网页。此流量应该允许。

经过测试并得出正确结果后，在 R2 上使用 **show access-lists** 特权执行命令检查 ACL 语句是否存在匹配。根据您掌握的 ACL 知识执行其它测试，检查每条语句匹配的流量是否正确。

步骤 4. 检查结果。

完成比例应为 100%。如果并非如此，请单击 **Check Results（检查结果）**查看尚未完成哪些必要部分。