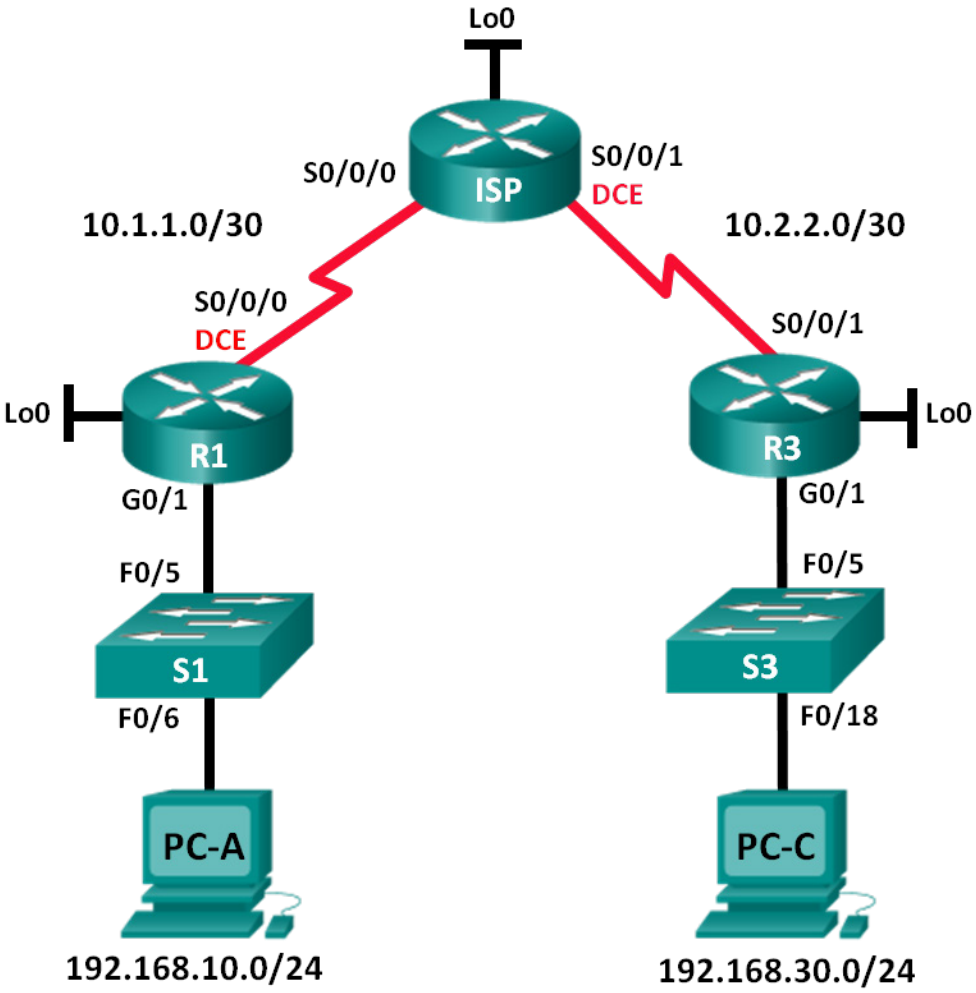
实验 - 配置和验证标准 IPv4 ACL

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	G0/1	192.168.10.1	255.255.255.0	不适用
	Lo0	192.168.20.1	255.255.255.0	不适用
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	不适用
ISP	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	不适用
	Lo0	209.165.200.225	255.255.255.224	不适用
R3	G0/1	192.168.30.1	255.255.255.0	不适用
	Lo0	192.168.40.1	255.255.255.0	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

目标

第 1 部分：设置拓扑并初始化设备

- 根据网络拓扑要求设置设备。
- 初始化并重新加载路由器和交换机。

第 2 部分：配置设备并验证连接

- 为 PC 分配静态 IP 地址。
- 配置路由器的基本设置。
- 配置交换机的基本设置。
- 配置 R1、ISP 和 R3 上的 OSPF 路由。
- 验证设备之间的连接。

第 3 部分：配置和验证编号和命名的标准 ACL

- 配置、应用和验证编号的标准 ACL。
- 配置、应用和验证命名的 ACL。

第 4 部分：修改标准 ACL

- 修改和验证命名的标准 ACL。
- 测试 ACL。

背景/场景

在设计和管理 IP 网络时，网络安全是一个重要问题。能够配置正确规则以根据建立的安全策略来过滤数据包是一个重要技能。

在本实验中，您将为 R1 和 R3 代表的两个办公室设置过滤规则。管理人员已经创建了 R1 和 R3 的 LAN 之间的一些访问策略，您必须实施这些策略。ISP 路由器位于 R1 和 R3 之间，上面不会放置任何 ACL。您不能对 ISP 路由器进行管理访问，因为您只能控制和管理您自己的设备。

注：CCNA 动手实验所用的路由器是采用思科 IOS 15.2(4)M3 版（universalk9 映像）的思科 1941 集成多业务路由器 (ISR)。所用的交换机是采用思科 IOS 15.0(2) 版（lanbasek9 映像）的思科 Catalyst 2960 系列。也可使用其他路由器、交换机以及其他思科 IOS 版本。根据型号以及思科 IOS 版本的不同，可用命令和产生的输出可能与实验显示的不一样。请参阅本实验末尾的“路由器接口汇总表”了解正确的接口标识符。

注：确保路由器和交换机的启动配置已经清除。如果不确定，请联系教师。

所需资源

- 3 台路由器（采用思科 IOS 版本 15.2(4)M3 通用映像的思科 1941 或同类路由器）
- 2 台交换机（采用思科 IOS 版本 15.0(2) lanbasek9 映像的思科 2960 或同类交换机）
- 2 台 PC（采用 Windows 7、Vista 或 XP 且支持终端模拟程序，比如 Tera Term）
- 用于通过控制台端口配置思科 IOS 设备的控制台电缆
- 拓扑所示的以太网和串行电缆

第 1 部分：设置拓扑并初始化设备

在第 1 部分，您将设置网络拓扑，必要时可清除任何配置。

步骤 1： 建立如拓扑图所示的网络。

步骤 2： 初始化并重新加载路由器和交换机。

第 2 部分：配置设备并验证连接

在第 2 部分，您配置路由器、交换机和 PC 上的基本设置。有关设备名称和地址信息，请参阅拓扑和地址分配表。

步骤 1： 配置 PC-A 和 PC-C 上的 IP 地址。

步骤 2： 配置路由器的基本设置。

a. 通过控制台连接到路由器，然后进入全局配置模式。

b. 复制以下基本配置并将其粘贴到路由器上的运行配置中。

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited.#
```

```
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. 如拓扑所示配置设备名称。

d. 在每个路由器上创建环回接口，如地址分配表中所示。

e. 创建接口 IP 地址，如拓扑和地址分配表中所示。

f. 为 DCE 串行接口指定 **128000** 的时钟速率。

g. 启用 Telnet 访问。

h. 将运行配置复制到启动配置中。

步骤 3： （可选）配置交换机的基本设置。

a 通过控制台连接到交换机，然后进入全局配置模式。

b 复制以下基本配置并将其粘贴到交换机上的运行配置中。

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited.#
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

c 如拓扑所示配置设备名称。

d 配置管理接口 IP 地址，如拓扑和地址分配表中所示。

e 配置默认网关。

f 启用 Telnet 访问。

g 将运行配置复制到启动配置中。

步骤 4： 在 R1、ISP 和 R3 上配置 Rip 路由。

a 在 R1、ISP 和 R3 上配置 RIP 版本 2 并通告所有网络。在此包括了 R1 和 ISP 的配置以供您参考。

```
R1(config)# router rip
R1(config-router)# version 2
```

```
R1(config-router)# network 192.168.10.0
R1(config-router)# network 192.168.20.0
R1(config-router)# network 10.1.1.0

ISP(config)# router rip
ISP(config-router)# version 2
ISP(config-router)# network 209.165.200.224
ISP(config-router)# network 10.1.1.0
ISP(config-router)# network 10.2.2.0
```

b 在 R1、ISP 和 R3 上配置 Rip 后，验证所有路由器是否都有完整的路由表，其中列出了所有网络。如果不是这样，请进行故障排除。

步骤 5： 验证设备之间的连接。

注：在配置和应用访问列表**之前**，测试连接是否正常工作非常重要！在开始过滤流量之前，您需要确保网络正常工作。

a 从 PC-A，ping PC-C 以及 R3 上的环回接口。您的 ping 操作是否成功？_____

b 从 R1，ping PC-C 以及 R3 上的环回接口。您的 ping 操作是否成功？_____

c 从 PC-C，ping PC-A 以及 R1 上的环回接口。您的 ping 操作是否成功？_____

d 从 R3，ping PC-A 以及 R1 上的环回接口。您的 ping 操作是否成功？_____

第 3 部分：配置和验证编号和命名的标准 ACL

步骤 1： 配置编号的标准 ACL

标准 ACL 仅基于源 IP 地址过滤流量。通常，标准 ACL 的最佳做法是在尽可能接近目标的位置应用。对于第一个访问列表，创建一个编号的标准 ACL，允许 192.168.10.0/24 网络上所有主机以及 192.168.20.0/24 网络上所有主机的流量访问 192.168.30.0/24 网络上的所有主机。安全策略还指出在所有 ACL 的结尾应该必须有一个 **deny any** 访问控制条目 (ACE)，也称为 ACL 语句。

使用什么通配符掩码来允许 192.168.10.0/24 网络上的所有主机访问 192.168.30.0/24 网络？

_____

按照思科推荐的最佳做法，应该将此 ACL 放置到哪个路由器上？_____

在哪个接口上放置此 ACL？在什么方向上应用？

_____

a 在 R3 上配置 ACL。使用 1 作为访问列表编号。

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b 按正确方向对相应的接口应用 ACL。

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

c 验证编号的 ACL。

使用各种 **show** 命令可帮助您验证 ACL 的语法以及在您的路由器中的放置。

要查看整个访问列表 1 以及所有 ACE，您应该使用哪个命令？

_____

使用什么命令来查看应用访问列表的位置以及方向？

_____

1) 在 R3 上，发出 **show access-lists 1** 命令。

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

2) 在 R3 上，发出 **show ip interface g0/1** 命令。

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  省略输出
```

3) 测试 ACL，查看它是否允许来自 192.168.10.0/24 网络的流量访问 192.168.30.0/24 网络。从 PC-A 命令提示符处，ping PC-C IP 地址。ping 是否成功？_____

4) 测试 ACL，查看它是否允许来自 192.168.20.0/24 网络的流量访问 192.168.30.0/24 网络。您必须执行扩展 ping，使用 R1 上的环回 0 地址作为您的来源。Ping PC-C 的 IP 地址。ping 是否成功？_____

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
```

```
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

d 从 R1 提示符处，再次 ping PC-C 的 IP 地址。

```
R1# ping 192.168.30.3
```

ping 是否成功？原因是什么？

_____

_____

_____

步骤 2： 配置命名的标准 ACL。

创建一个符合以下策略的命名的标准 ACL：允许 192.168.40.0/24 网络上所有主机的流量访问 192.168.10.0/24 网络上的所有主机。此外，只允许主机 PC-C 访问 192.168.10.0/24 网络。此访问列表的名称应称为 BRANCH-OFFICE-POLICY。

按照思科推荐的最佳做法，应该将此 ACL 放置到哪个路由器上？_____

在哪个接口上放置此 ACL？在什么方向上应用？

_____

a 在 R1 上创建名为 ACL BRANCH-OFFICE-POLICY 的标准。

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

查看访问列表中第一个 permit ACE，另一种编写方法是什么？

_____

b 按正确方向对相应的接口应用 ACL。

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c 验证命名的 ACL。

1) 在 R1 上，发出 **show access-lists** 命令。

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3
```

```
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

R1 上的这个 ACL 与 R3 上的 ACL 有区别吗？如果有，那区别是什么？

_____

_____

_____

_____

_____

2) 在 R1 上，发出 **show ip interface g0/1** 命令。

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<省略部分输出>
```

3) 测试 ACL。从 PC-C 的命令提示符处，ping PC-A 的 IP 地址。ping 是否成功？_____

4) 测试 ACL 以确保只允许 PC-C 主机访问 192.168.10.0/24 网络。您必须执行扩展 ping，使用 R3 上的 G0/1 地址作为您的来源。Ping PC-A 的 IP 地址。ping 是否成功？_____

5) 测试 ACL，查看它是否允许来自 192.168.40.0/24 网络的流量访问 192.168.10.0/24 网络。您必须执行扩展 ping，使用 R3 上的环回 0 地址作为您的来源。Ping PC-A 的 IP 地址。ping 是否成功？_____

第 4 部分：修改标准 ACL

企业常常会更改安全策略。因此，可能需要修改 ACL。在第 4 部分，您将更改此前配置的 ACL 之一，以匹配实施的新管理策略。

管理人员决定允许来自 209.165.200.224/27 网络的用户完全访问 192.168.10.0/24 网络。管理人员还希望所有路由器上的 ACL 遵照一致的规则。在所有 ACL 的结尾应放置 **deny any** ACE。您必须修改 BRANCH-OFFICE-POLICY ACL。

您将为此 ACL 添加另外两行。有两种方法完成此操作：

选项 1：在全局配置模式下发出 **no ip access-list standard BRANCH-OFFICE-POLICY** 命令。这将从路由器中有效去除整个 ACL。根据路由器 IOS，将会出现以下情形之一：将取消数据包的所有过滤，全部数据包都允许通过路由器；或者，由于您没有在 G0/1 接口上去除 **ip access-group** 命令，过滤仍然存在。无论如何，当 ACL 删除后，您都可以重新键入整个 ACL，或者在文本编辑器中进行剪切和粘贴操作。

选项 2：通过在 ACL 本身中添加或删除特定行，您可以修改正在使用的 ACL。这可能非常有用，尤其是当 ACL 有多行代码时。重新键入整个 ACL 或者执行剪切和粘贴操作很容易导致错误。修改 ACL 中的特定行可轻松完成。

注：对于本实验，使用选项 2。

步骤 1： 修改命名的标准 ACL。

a 在 R1 特权执行模式下，发出 **show access-lists** 命令。

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

b 在 ACL 末尾添加另外两行。在全局配置模式下，修改 BRANCH-OFFICE-POLICY ACL。

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c 验证 ACL。

1) 在 R1 上，发出 **show access-lists** 命令。

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits 0.0.0.31
    40 deny   any
```

您是否必须对 R1 上的 G0/1 接口应用 BRANCH-OFFICE-POLICY？

_____

_____

2) 从 ISP 命令提示符处，发出扩展的 ping。测试 ACL，查看它是否允许来自 209.165.200.224/27 网络的流量访问 192.168.10.0/24 网络。您必须执行扩展 ping，使用 ISP 上的环回 0 地址作为您的来源。Ping PC-A 的 IP 地址。ping 是否成功？_____

思考

1. 正如您看到的，标准 ACL 非常强大，效果非常好。为什么曾经会需要使用扩展 ACL？

_____

_____

_____

_____

2. 通常，与使用编号的 ACL 相比，使用命名的 ACL 时要键入更多的内容。您会因为什么原因选择使用命名的 ACL，而不使用编号的 ACL？

_____

_____

_____

_____

路由器接口汇总表

路由器接口汇总				
路由器型号	**以太网接口 1**	**以太网接口 2**	**串行接口 1**	**串行接口 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

注：若要了解如何配置路由器，请查看接口来确定路由器类型以及路由器拥有的接口数量。我们无法为每类路由器列出所有的配置组合。下表列出了设备中以太网和串行接口组合的标识符。此表中未包含任何其他类型的接口，但实际的路由器可能会含有其他接口。例如 ISDN BRI 接口。括号中的字符串是约定缩写，可在思科 IOS 命令中用来代表接口。