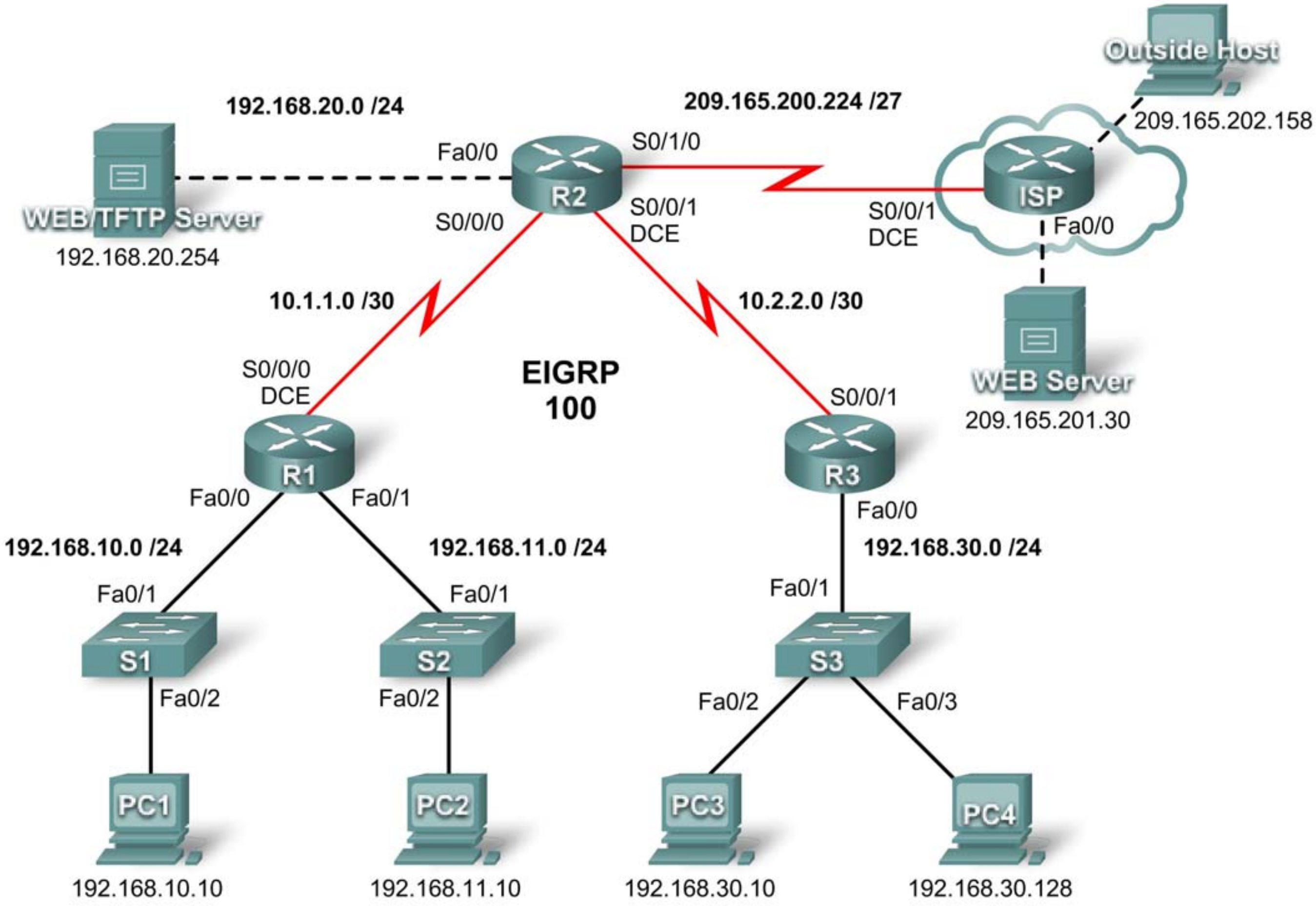
PT Activity 5.2.8: Configuring Standard ACLs

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
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	10.2.2.1	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**	10.2.2.2	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	**NIC**	192.168.10.10	255.255.255.0
PC2	**NIC**	192.168.11.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
PC4	**NIC**	192.168.30.128	255.255.255.0
WEB/TFTP Server	**NIC**	192.168.20.254	255.255.255.0
WEB Server	**NIC**	209.165.201.30	255.255.255.224
Outside Host	**NIC**	209.165.202.158	255.255.255.224

Learning Objectives

- Investigate the current network configuration
- Evaluate a network policy and plan an ACL implementation
- Configure numbered standard ACLs
- Configure named standard ACLs

Introduction

Standard ACLs are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and EIGRP routing. The user EXEC password is **cisco,** and the privileged EXEC password is **class**.

Task 1: Investigate the Current Network Configuration

Step 1. View the running configuration on the routers.

View the running configurations on all three routers using the **show running-config** command while in privileged EXEC mode. Notice that the interfaces and routing are fully configured. Compare the IP address configurations to the Addressing Table above. There should not be any ACLs configured on the routers at this time.

The ISP router does not require any configuration during this exercise. Assume that the ISP router is not under your administration and is configured and maintained by the ISP administrator.

Step 2. Confirm that all devices can access all other locations.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Without testing connectivity in your network prior to applying an ACL, troubleshooting may be more difficult.

One helpful step in testing connectivity is to view the routing tables on each device to ensure that each network is listed. On R1, R2, and R3, issue the **show ip route** command. You should see that each device has connected routes for attached networks, and dynamic routes to all other remote networks. All devices can access all other locations.

Although the routing table can be helpful in assessing the status of the network, you should still test connectivity using **ping**. Complete the following tests:

- From PC1, ping PC2.
- From PC2, ping Outside Host.
- From PC4, ping the Web/TFTP Server.

Each of these connectivity tests should be successful.

Task 2: Evaluate a Network Policy and Plan an ACL Implementation

Step 1. Evaluate the policy for the R1 LANs.

- The 192.168.10.0/24 network is allowed access to all locations, except the 192.168.11.0/24 network.
- The 192.168.11.0/24 network is allowed access to all destinations, except to any networks connected to the ISP.

Step 2. Plan the ACL implementation for the R1 LANs.

- Two ACLs fully implement the security policy for the R1 LANs.
- The first ACL on R1 denies traffic from the 192.168.10.0/24 network to the 192.168.11.0/24 network, but permits all other traffic.
- This first ACL, applied outbound on the Fa0/1 interface, monitors any traffic sent to the 192.168.11.0 network.
- The second ACL on R2 denies the 192.168.11.0/24 network access to the ISP, but permits all other traffic.
- Outbound traffic from the S0/1/0 interface is controlled.
- Place the ACL statements in the order of most specific to least specific. Denying the network traffic from accessing another network comes before permitting all other traffic.

Step 3. Evaluate the policy for the R3 LAN.

- The 192.168.30.0/10 network is allowed access to all destinations.
- Host 192.168.30.128 is not allowed access outside of the LAN.

Step 4. Plan the ACL implementation for the R3 LAN.

- One ACL fully implements the security policy for the R3 LAN.
- The ACL is placed on R3 and denies the 192.168.30.128 host access outside of the LAN, but permits traffic from all other hosts on the LAN.
- Applied inbound on the Fa0/0 interface, this ACL will monitor all traffic attempting to leave the 192.168.30.0/10 network.
- Place the ACL statements in the order of most specific to least specific. Denying the 192.168.30.128 host access comes before permitting all other traffic.

Task 3: Configure Numbered Standard ACLs

Step 1. Determine the wildcard mask.

The wildcard mask in an ACL statement determines how much of an IP source or destination address to check. A 0 bit means to match that value in the address, while a 1 bit ignores that value in the address. Remember that standard ACLs can only check source addresses.

- Since the ACL on R1 denies all 192.168.10.0/24 network traffic, any source IP that begins with 192.168.10 is denied. Since the last octet of the IP address can be ignored, the correct wildcard mask is 0.0.0.255. Each octet in this mask can be thought of as “check, check, check, ignore.”
- The ACL on R2 also denies 192.168.11.0/24 network traffic. The same wildcard mask can be applied, 0.0.0.255.

Step 2. Determine the statements.

- ACLs are configured in global configuration mode.
- For standard ACLs, use a number between 1 and 99. The number **10** is used for this list on R1 to help remember that this ACL is monitoring the 192.168.**10**.0 network.
- On R2, access list **11 will deny** traffic from the 192.168.**11**.0 network to any ISP networks, so the **deny** option is set with the network **192.168.11.0** and wildcard mask **0.0.0.255**.
- All other traffic must be permitted with the **permit** option because of the implicit “deny any” at the end of ACLs. The **any** option specifies any source host.

Configure the following on R1:

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

Note: Packet Tracer will not grade an ACL configuration until all statements are entered in the correct order.

Now create an ACL on R2 to deny the 192.168.11.0 network and permit all other networks. For this ACL, use the number **11**. Configure the following on R2:

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

Step 3. Apply the statements to the interfaces.

On R1, enter configuration mode for the Fa0/1 interface.

Issue the **ip access-group 10 out** command to apply the standard ACL outbound on the interface.

```
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
```

On R2, enter configuration mode for the S0/1/0 interface.

Issue the **ip access-group 11 out** command to apply the standard ACL outbound on the interface.

```
R2(config)#interface s0/1/0
R2(config-if)#ip access-group 11 out
```

Step 4. Verify and test ACLs.

With the ACLs configured and applied, PC1 (192.168.10.10) should not be able to ping PC2 (192.168.11.10), because ACL 10 is applied outbound on Fa0/1 on R1.

PC2 (192.168.11.10) should not be able to ping Web Server (209.165.201.30) or Outside Host (209.165.202.158), but should be able to ping everywhere else, because ACL 11 is applied outbound on S0/1/0 on R2. However, PC2 cannot ping PC1 because ACL 10 on R1 prevents the echo reply from PC1 to PC2.

Step 5. Check results.

Your completion percentage should be 67%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure a Named Standard ACL

Step 1. Determine the wildcard mask.

- The access policy for R3 states that the host at 192.168.30.128 should not be allowed any access outside the local LAN. All other hosts on the 192.168.30.0 network should be allowed access to all other locations.
- To check a single host, the entire IP address needs to be checked, which is accomplished using the **host** keyword.
- All packets that do not match the host statement are permitted.

Step 2. Determine the statements.

- On R3, enter global configuration mode.
- Create a named ACL called NO_ACCESS by issuing the **ip access-list standard NO_ACCESS** command. You will enter ACL configuration mode. All permit and deny statements are configured from this configuration mode.
- Deny traffic from the 192.168.30.128 host with the **host** option.
- Permit all other traffic with **permit any**.

Configure the following named ACL on R3:

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

Step 3. Apply the statements to the correct interface.

On R3, enter configuration mode for the Fa0/0 interface.

Issue the **ip access-group NO_ACCESS in** command to apply the named ACL inbound on the interface. This command causes all traffic entering the Fa0/0 interface from the 192.168.30.0/24 LAN to be checked against the ACL.

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

Step 4. Verify and test ACLs.

Click **Check Results,** and then click **Connectivity Tests**. The following tests should fail:

- PC1 to PC2
- PC2 to Outside Host
- PC2 to Web Server
- All pings from/to PC4 except between PC3 and PC4

Step 5. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.