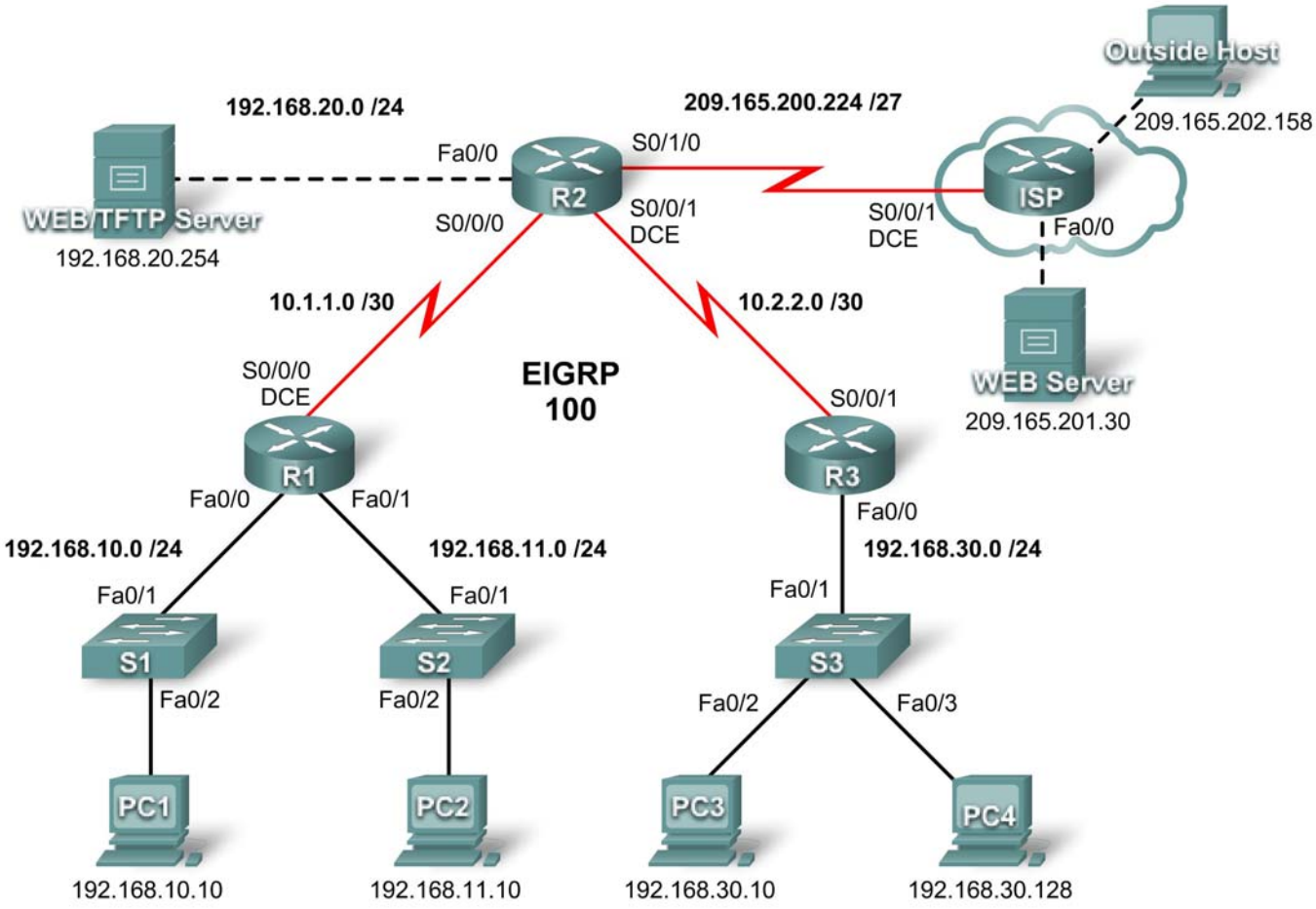
PT Activity 5.3.4: Configuring Extended ACLs

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	10.2.2.2	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	**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 extended ACLs
- Configure named extended ACLs

Introduction

Extended ACLs are router configuration scripts that control whether a router permits or denies packets based on their source or destination address as well as protocols or ports. Extended ACLs provide more flexibility and granularity than standard ACLs. This activity focuses on defining filtering criteria, configuring extended 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. It is assumed 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 fully connectivity. Without testing connectivity in your network prior to applying an ACL, troubleshooting will be very difficult.

To ensure network-wide connectivity, use the **ping** and **tracert** commands between various network devices to verify connections.

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

Step 1. Evaluate the policy for the R1 LANs.

- For the 192.168.10.0/24 network, block Telnet access to all locations and TFTP access to the corporate Web/TFTP server at 192.168.20.254. All other access is allowed.
- For the192.168.11.0/24 network, allow TFTP access and web access to the corporate Web/TFTP server at 192.168.20.254. Block all other traffic from the 192.168.11.0/24 network to the 192.168.20.0/24 network. All other access is allowed.

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

- Two ACLs fully implement the security policy for the R1 LANs.
- The first ACL supports the first part of the policy and is configured on R1 and applied inbound to the Fast Ethernet 0/0 interface.
- The second ACL supports the second part of the policy and is configured on R1 and applied inbound to the Fast Ethernet 0/1 interface.

Step 3. Evaluate the policy for the R3 LAN.

- All IP addresses of the 192.168.30.0/24 network are blocked from accessing all IP addresses of the 192.168.20.0/24 network.
- The first half of 192.168.30.0/24 is allowed access to all other destinations.
- The second half of 192.168.30.0/24 network is allowed access to the 192.168.10.0/24 and 192.168.11.0/24 networks.
- The second half of 192.168.30.0/24 is allowed web and ICMP access to all remaining destinations.
- All other access is implicitly denied.

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

This step requires one ACL configured on R3 and applied inbound to the Fast Ethernet 0/0 interface.

Step 5. Evaluate the policy for traffic coming from the Internet via the ISP.

- Outside hosts are allowed to establish a web session with the internal web server on port 80 only.
- Only established TCP sessions are allowed in.

- Only ping replies are allowed through R2.

Step 6. Plan the ACL implementations for traffic coming from the Internet via the ISP.

This step requires one ACL configured on R2 and applied inbound to the Serial 0/1/0 interface.

Task 3: Configure Numbered Extended ACLs

Step 1. Determine the wildcard masks.

Two ACLs are needed to enforce the access control policy on R1. Both ACLs will be designed to deny an entire Class C network. You will configure a wildcard mask that matches all hosts on each of these Class C networks.

For example, for the entire subnet of 192.168.10.0/24 to be matched, the wildcard mask is 0.0.0.255. This can be thought of as “check, check, check, ignore” and, in essence, matches the entire 192.168.10.0/24 network.

Step 2. Configure the first extended ACL for R1.

From global configuration mode, configure the first ACL with number 110. First, you want to block Telnet to any location for all IP addresses on the 192.168.10.0/24 network.

When writing the statement, make sure that you are currently in global configuration mode.

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

Next, block all IP addresses on the 192.168.10.0/24 network from TFTP access to the host at 192.168.20.254.

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

Finally, permit all other traffic.

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

Step 3. Configure the second extended ACL for R1.

Configure the second ACL with number 111. Permit WWW to the host at 192.168.20.254 for any IP addresses on the 192.168.11.0/24 network.

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

Next, permit TFTP to the host at 192.168.20.254 for any IP addresses on the 192.168.11.0/24 network.

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

Block all other traffic from 192.168.11.0/24 network to the 192.168.20.0/24 network.

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

Finally, permit any other traffic. This statement ensures that traffic from other networks is not blocked.

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


Step 4. Verify the ACL configurations.

Confirm your configurations on R1 by issuing the **show access-lists** command. Your output should look like this:

```
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
```

Step 5. Apply the statements to the interfaces.

To apply an ACL to an interface, enter interface configuration mode for that interface. Configure the command **ip access-group** *access-list-number* {**in** | **out**} to apply the ACL to the interface.

Each ACL filters inbound traffic. Apply ACL 110 to Fast Ethernet 0/0 and ACL 111 to Fast Ethernet 0/1.

```
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
```

Confirm that the ACLs appear in the running configuration of R1 and that they have been applied to the correct interfaces.

Step 6. Test the ACLs configured on R1.

Now that ACLs have been configured and applied, it is very important to test that traffic is blocked or permitted as expected.

- From PC1, attempt to gain Telnet access to any device. This should be blocked.
- From PC1, attempt to access the corporate Web/TFTP server via HTTP. This should be allowed.
- From PC2, attempt to access the Web/TFTP server via HTTP. This should be allowed.
- From PC2, attempt to access the external Web server via HTTP. This should be allowed.

Based on your understanding of ACLs, try some other connectivity tests from PC1 and PC2.

Step 7. Check results.

Packet Tracer does not support testing TFTP access, so you will not be able to verify that policy. However, your completion percentage should be 50%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure a Numbered Extended ACL for R3

Step 1. Determine the wildcard mask.

The access policy for the lower half of the IP addresses on the 192.168.30.0/24 network requires:

- Deny access to the 192.168.20.0/24 network
- Allow access to all other destinations

The top half of the IP addresses in the 192.168.30.0/24 network has the following restrictions:

- Allow access to 192.168.10.0 and 192.168.11.0

- Deny access to 192.168.20.0
- Allow web and ICMP to all other locations

To determine the wildcard mask, consider which bits need to be checked for the ACL to match IP addresses 0–127 (lower half) or 128–255 (upper half).

Recall that one way to determine the wildcard mask is to subtract the normal network mask from 255.255.255.255. The normal mask for IP addresses 0–127 and 128–255 for a Class C address is 255.255.255.128. Using the subtraction method, here is the correct wildcard mask:

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

Step 2. Configure the extended ACL on R3.

On R3, enter global configuration mode and configure the ACL using 130 as the access list number.

The first statement blocks the 192.168.30.0/24 from accessing all addresses in the 192.168.30.0/24 network.

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

The second statement allows the lower half of the 192.168.30.0/24 network access to any other destinations.

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

The remaining statements explicitly permit the upper half of the 192.168.30.0/24 network access to those networks and services that the network policy allows.

```
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
```

Step 3. Apply the statement to the interface.

To apply an ACL to an interface, enter interface configuration mode for that interface. Configure the command **ip access-group** *access-list-number* {**in** | **out**} to apply the ACL to the interface.

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

Step 4. Verify and test ACLs.

Now that the ACL has been configured and applied, it is very important to test that traffic is blocked or permitted as expected.

- From PC3, ping the Web/TFTP server. This should be blocked.
- From PC3, ping any other device. This should be allowed.
- From PC4, ping the Web/TFTP server. This should be blocked.
- From PC4, telnet to R1 at 192.168.10.1 or 192.168.11.1. This should be allowed.
- From PC4, ping PC1 and PC2. This should be allowed.
- From PC4, telnet to R2 at 10.2.2.2. This should be blocked.

After your tests have been conducted and yield the correct results, use the **show access-lists** privileged EXEC command on R3 to verify that the ACL statements have matches.

Based on your understanding of ACLs, conduct other tests to verify that each statement is matching the correct traffic.

Step 5. Check results.

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure a Named Extended ACL

Step 1. Configure a named extended ACL on R2.

Recall that the policy on R2 will be designed to filter Internet traffic. Since R2 has the connection to the ISP, this is the best placement for the ACL.

Configure a named ACL called FIREWALL on R2 using the **ip access-list extended** *name* command. This command puts the router into extended named ACL configuration mode. Note the changed router prompt.

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

In ACL configuration mode, add the statements to filter traffic as outlined in the policy:

- Outside hosts are allowed to establish a web session with the internal web server on port 80 only.
- Only established TCP sessions are allowed in.
- Ping replies are allowed through 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
```

After configuring the ACL on R2, use the **show access-lists** command to confirm that the ACL has the correct statements.

Step 2. Apply the statement to the interface.

Use the **ip access-group** *name* {**in** | **out**} command to apply the ACL inbound on the ISP facing interface of R2.

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

Step 3. Verify and test ACLs.

Conduct the following tests to ensure that the ACL is functioning as expected:

- From Outside Host, open a web page on the internal Web/TFTP server. This should be allowed.
- From Outside Host, ping the internal Web/TFTP server. This should be blocked.
- From Outside Host, ping PC1. This should be blocked.
- From PC1, ping the external Web Server at 209.165.201.30. This should be allowed.
- From PC1, open a web page on the external Web Server. This should be allowed.

After your tests have been conducted and yield the correct results, use the **show access-lists** privileged EXEC command on R2 to verify that the ACL statements have matches.

Based on your understanding of ACLs, conduct other tests to verify that each statement is matching the correct traffic.

Step 4. Check results.

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

