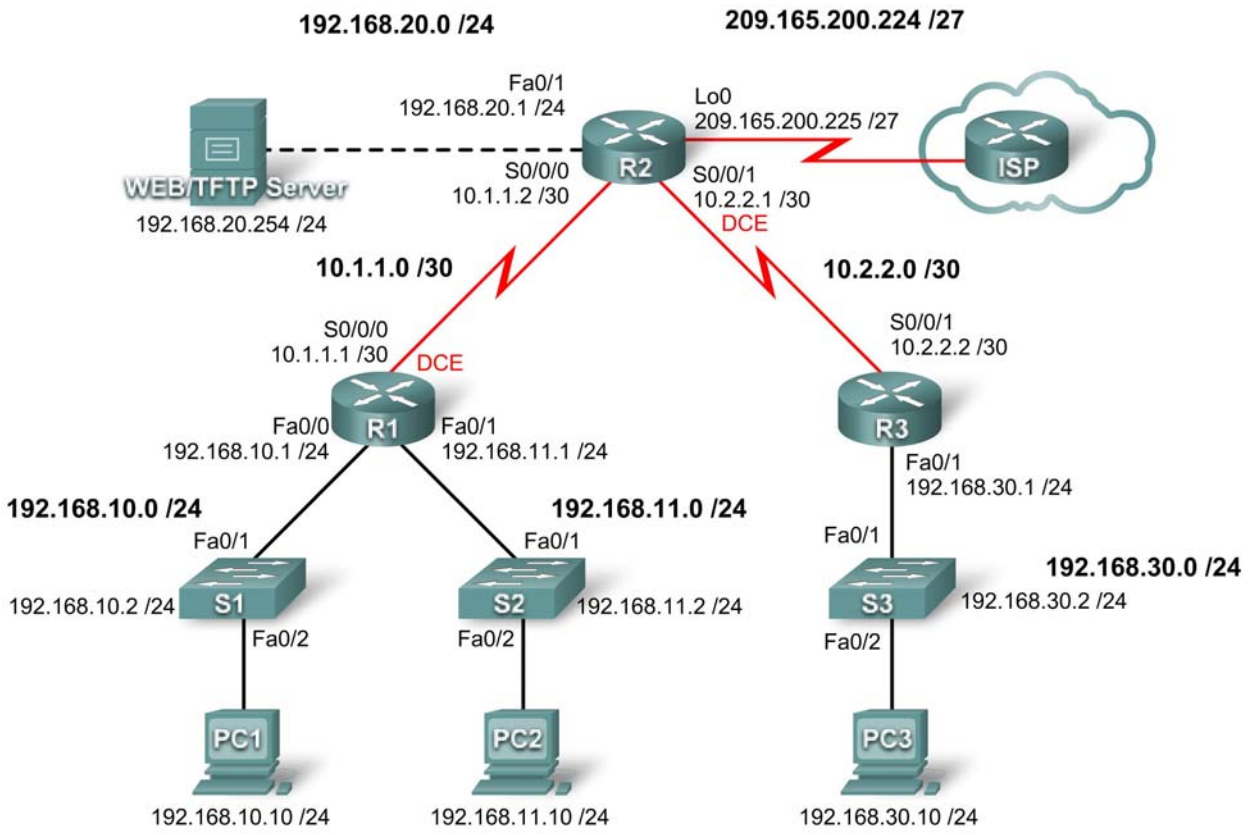
Lab 5.5.1: Basic Access Control Lists

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	**Fa0/1**	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	**Fa0/1**	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	**Vlan1**	192.168.10.2	255.255.255.0	192.168.10.1

S2	**Vlan1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**Vlan1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Web Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Design named standard and named extended ACLs.
- Apply named standard and named extended ACLs.
- Test named standard and named extended ACLs.
- Troubleshoot named standard and named extended ACLs.

Scenario

In this lab, you will learn how to configure basic network security using Access Control Lists. You will apply both standard and extended ACLs.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: This lab was developed and tested using 1841 routers. If you use 1700, 2500, or 2600 series routers, the router outputs and interface descriptions might be different. On older routers, or versions of the IOS before 12.4, some commands may be different or non-existent.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, R3, S1, S2, and S3 routers and switches according to the following guidelines:

- Configure the router hostname to match the topology diagram.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a message-of-the-day banner.
- Configure a password of cisco for console connections.
- Configure a password for VTY connections.
- Configure IP addresses and masks on all devices.
- Enable OSPF area 0 with a process ID of 1 on all routers for all networks.
- Configure a loopback interface on R2 to simulate the ISP.

- Configure IP addresses for the VLAN 1 interface on each switch.
- Configure each switch with the appropriate default gateway.
- Verify full IP connectivity using the **ping** command.

Task 3: Configuring a Standard ACL

Standard ACLs can filter traffic based on source IP address only. A typical best practice is to configure a standard ACL as close to the destination as possible. In this task, you are configuring a standard ACL. The ACL is designed to block traffic from the 192.168.11.0/24 network located in a student lab from accessing any local networks on R3.

This ACL will be applied inbound on the R3 serial interface. Remember that every ACL has an implicit "deny all" that causes all traffic that has not matched a statement in the ACL to be blocked. For this reason, add the **permit any** statement to the end of the ACL.

Before configuring and applying this ACL, be sure to test connectivity from PC1 (or the Fa0/1 interface on R1) to PC3 (or the Fa0/1 interface on R3). Connectivity tests should be successful before applying the ACL.

Step 1: Create the ACL on router R3.

In global configuration mode, create a standard named ACL called **STND-1**.

```
R3(config)#ip access-list standard STND-1
```

In standard ACL configuration mode, add a statement that denies any packets with a source address of 192.168.11.0/24 and prints a message to the console for each matched packet.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255 log
```

Permit all other traffic.

```
R3(config-std-nacl)#permit any
```

Step 2: Apply the ACL.

Apply the ACL **STND-1** as a filter on packets entering R3 through Serial interface 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
R3#copy run start
```

Step 3: Test the ACL.

Before testing the ACL, make sure that the console of R3 is visible. This will allow you to see the access list log messages when the packet is denied.

Test the ACL by pinging from PC2 to PC3. Since the ACL is designed to block traffic with source addresses from the 192.168.11.0/24 network, PC2 (192.168.11.10) should not be able to ping PC3.

You can also use an extended ping from the Fa0/1 interface on R1 to the Fa0/1 interface on R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
```



```
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 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)
```

You should see the following message on the R3 console:

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0
0.0.0.0 -> 192.168.11.1, 1 packet
```

In privileged EXEC mode on R3, issue the **show access-lists** command. You see output similar to the following. Each line of an ACL has an associated counter showing how many packets have matched the rule.

```
Standard IP access list STND-1
    10 deny   192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
    20 permit any (25 matches)
```

The purpose of this ACL was to block hosts from the 192.168.11.0/24 network. Any other hosts, such as those on the 192.168.10.0/24 network should be allowed access to the networks on R3. Conduct another test from PC1 to PC3 to ensure that this traffic is not blocked.

You can also use an extended ping from the Fa0/0 interface on R1 to the Fa0/1 interface on R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
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 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

Task 4: Configuring an Extended ACL

When greater granularity is required, you should use an extended ACL. Extended ACLs can filter traffic based on more than just source address. Extended ACLs can filter on protocol, source, and destination IP addresses, and source and destination port numbers.

An additional policy for this network states that devices from the 192.168.10.0/24 LAN are only permitted to reach internal networks. Computers on this LAN are not permitted to access the Internet. Therefore, these users must be blocked from reaching the IP address 209.165.200.225. Because this requirement

needs to enforce both source and destination, an extended ACL is needed.

In this task, you are configuring an extended ACL on R1 that blocks traffic originating from any device on the 192.168.10.0/24 network to access the 209.165.200.255 host (the simulated ISP). This ACL will be applied outbound on the R1 Serial 0/0/0 interface. A typical best practice for applying extended ACLs is to place them as close to the source as possible.

Before beginning, verify that you can ping 209.165.200.225 from PC1.

Step 1: Configure a named extended ACL.

In global configuration mode, create a named extended ACL called **EXTEND-1**.

```
R1(config)#ip access-list extended EXTEND-1
```

Notice that the router prompt changes to indicate that you are now in extended ACL configuration mode. From this prompt, add the necessary statements to block traffic from the 192.168.10.0/24 network to the host. Use the **host** keyword when defining the destination.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Recall that the implicit “deny all” blocks all other traffic without the additional **permit** statement. Add the **permit** statement to ensure that other traffic is not blocked.

```
R1(config-ext-nacl)#permit ip any any
```

Step 2: Apply the ACL.

With standard ACLs, the best practice is to place the ACL as close to the destination as possible. Extended ACLs are typically placed close to the source. The **EXTEND-1** ACL will be placed on the Serial interface, and will filter outbound traffic.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group EXTEND-1 out log
R1(config-if)#end
R1#copy run start
```

Step 3: Test the ACL.

From PC1, ping the loopback interface on R2. These pings should fail, because all traffic from the 192.168.10.0/24 network is filtered when the destination is 209.165.200.225. If the destination is any other address, the pings should succeed. Confirm this by pinging R3 from the 192.168.10.0/24 network device.

Note: The extended ping feature on R1 cannot be used to test this ACL, since the traffic will originate within R1 and will never be tested against the ACL applied to the R1 serial interface.

You can further verify this by issuing the **show ip access-list** on R1 after pinging.

```
R1#show ip access-list
Extended IP access list EXTEND-1
    10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
    20 permit ip any any
```

Task 5: Control Access to the VTY Lines with a Standard ACL

It is good practice to restrict access to the router VTY lines for remote administration. An ACL can be applied to the VTY lines, allowing you to restrict access to specific hosts or networks. In this task, you will configure a standard ACL to permit hosts from two networks to access the VTY lines. All other hosts are denied.

Verify that you can telnet to R2 from both R1 and R3.

Step 1: Configure the ACL.

Configure a named standard ACL on R2 that permits traffic from 10.2.2.0/30 and 192.168.30.0/24. Deny all other traffic. Call the ACL **TASK-5**.

```
R2(config)#ip access-list standard TASK-5
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Step 2: Apply the ACL.

Enter line configuration mode for VTY lines 0–4.

```
R2(config)#line vty 0 4
```

Use the **access-class** command to apply the ACL to the vty lines in the inbound direction. Note that this differs from the command used to apply ACLs to other interfaces.

```
R2(config-line)#access-class TASK-5 in
R2(config-line)#end
R2#copy run start
```

Step 3: Test the ACL

Telnet to R2 from R1. Note that R1 does not have IP addresses in the address range listed in the ACL TASK-5 permit statements. Connection attempts should fail.

```
R1# telnet 10.1.1.2
Trying 10.1.1.2 …
% Connection refused by remote host
```

From R3, telnet to R2. You will be presented with a prompt for the VTY line password.

```
R3# telnet 10.1.1.2
Trying 10.1.1.2 … Open
CUnauthorized access strictly prohibited, violators will be prosecuted
to the full extent of the law.

User Access Verification

Password:
```

Why do connection attempts from other networks fail even though they are not specifically listed in the ACL?

_____

_____

Task 6: Troubleshooting ACLs

When an ACL is improperly configured or applied to the wrong interface or in the wrong direction, network traffic may be affected in an undesirable manner.

Step 1: Remove ACL STND-1 from S0/0/1 of R3.

In an earlier task, you created and applied a named standard ACL on R3. Use the **show running-config** command to view the ACL and its placement. You should see that an ACL named **STND-1** was configured and applied inbound on Serial 0/0/1. Recall that this ACL was designed to block all network

traffic with a source address from the 192.168.11.0/24 network from accessing the LAN on R3.

To remove the ACL, go to interface configuration mode for Serial 0/0/1 on R3. Use the **no ip access-group STND-1 in** command to remove the ACL from the interface.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 in
```

Use the **show running-config** command to confirm that the ACL has been removed from Serial 0/0/1.

Step 2: Apply ACL STND-1 on S0/0/1 outbound.

To test the importance of ACL filtering direction, reapply the **STND-1** ACL to the Serial 0/0/1 interface. This time the ACL will be filtering outbound traffic, rather than inbound traffic. Remember to use the **out** keyword when applying the ACL.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 out
```

Step 3: Test the ACL.

Test the ACL by pinging from PC2 to PC3. As an alternative, use an extended ping from R1. Notice that this time pings succeed, and the ACL counters are not incremented. Confirm this by issuing the **show ip access-list** command on R3.

Step 4: Restore the ACL to its original configuration.

Remove the ACL from the outbound direction and reapply it to the inbound direction.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 out
R3(config-if)#ip access-group STND-1 in
```

Step 5: Apply TASK-5 to the R2 serial 0/0/0 interface inbound.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group TASK-5 in
```

Step 6: Test the ACL.

Attempt to communicate to any device connected to R2 or R3 from R1 or its attached networks. Notice that all communication is blocked; however, ACL counters are not incremented. This is because of the implicit “deny all” at the end of every ACL. This deny statement will prevent all inbound traffic to serial 0/0/0 from any source other than R3. Essentially, this will cause routes from R1 to be removed from the routing table.

You should see messages similar to the following printed on the consoles of R1 and R2 (It will take some time for the OSPF neighbor relationship to go down, so be patient):

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Once you receive this message, issue the command **show ip route** on both R1 and R2 to see which routes have been removed from the routing table.

Remove ACL TASK-5 from the interface, and save your configurations.

```
R2(config)#interface serial 0/0/0
R2(config-if)#no ip access-group TASK-5 in
R2(config)#exit
R2#copy run start
```


Task 7: Document the Router Configurations

Configurations

Router 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group EXTEND-1 out
 clockrate 64000
 no shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip access-list extended EXTEND-1
 deny   ip 192.168.10.0 0.0.0.255 host 209.165.200.225
 permit ip any any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

Router 2

```
hostname R2
!
enable secret class
!
no ip domain lookup
!
```



```
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clockrate 125000
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5
 permit 10.2.2.0 0.0.0.3
 permit 192.168.30.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class TASK-5 in
 password cisco
 login
!
```

Router 3

```
hostname R3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip access-group STND-1 in
```



```
 no shutdown
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip access-list standard STND-1
 deny   192.168.11.0 0.0.0.255 log
 permit any
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
end
```

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

