Name: Miftahul Huq

Course: Network Security

Course Prefix: CSEC 744

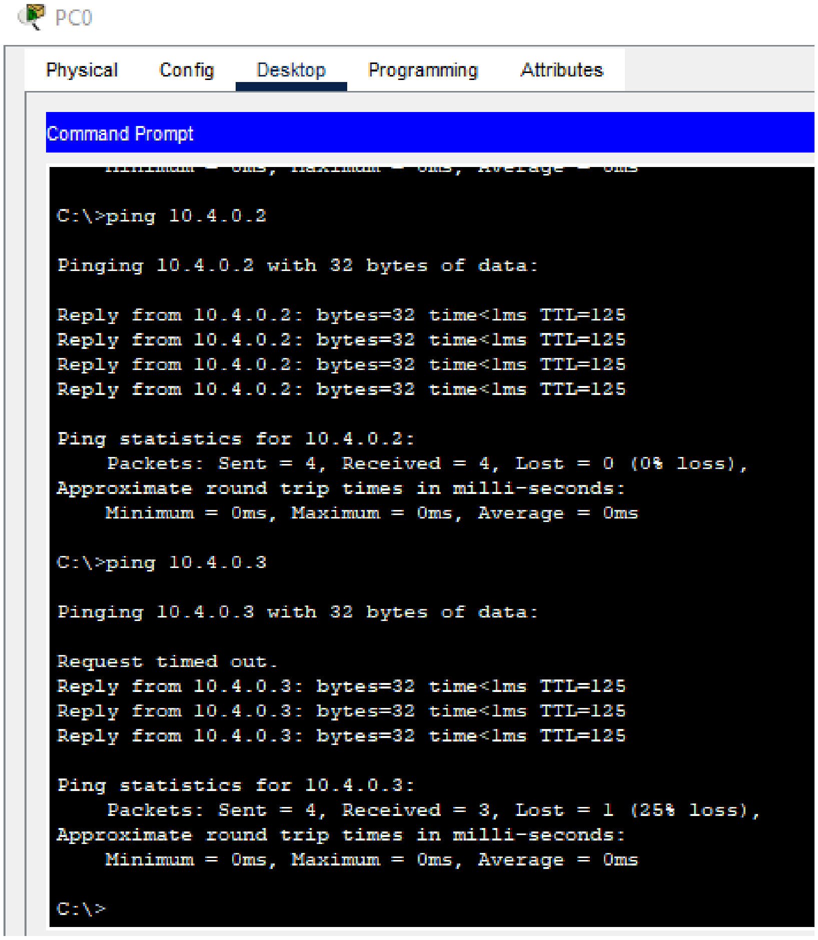
Section: 01

Chapter 10: Infrastructure Security

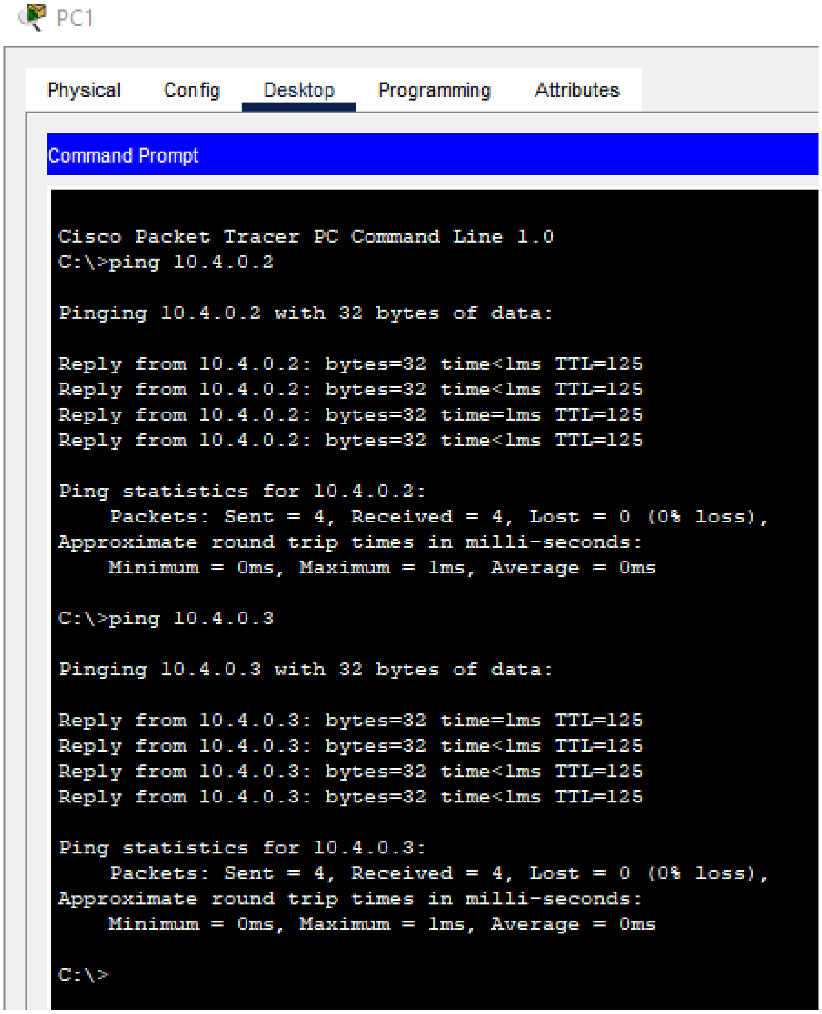
Date: 03/08/2024

Lab Exercise 10.02: Standard ACLs on Routers

Step 1a:

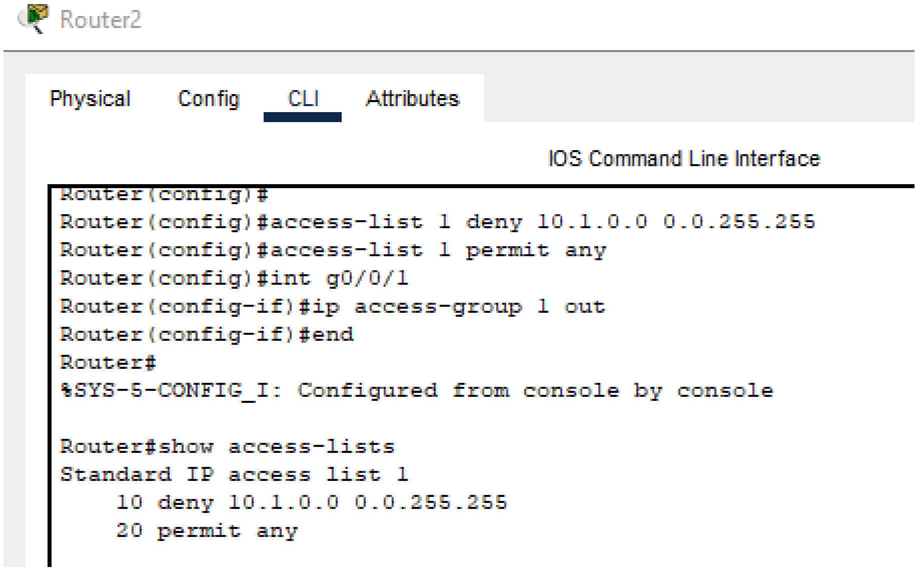


```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Request timed out.
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



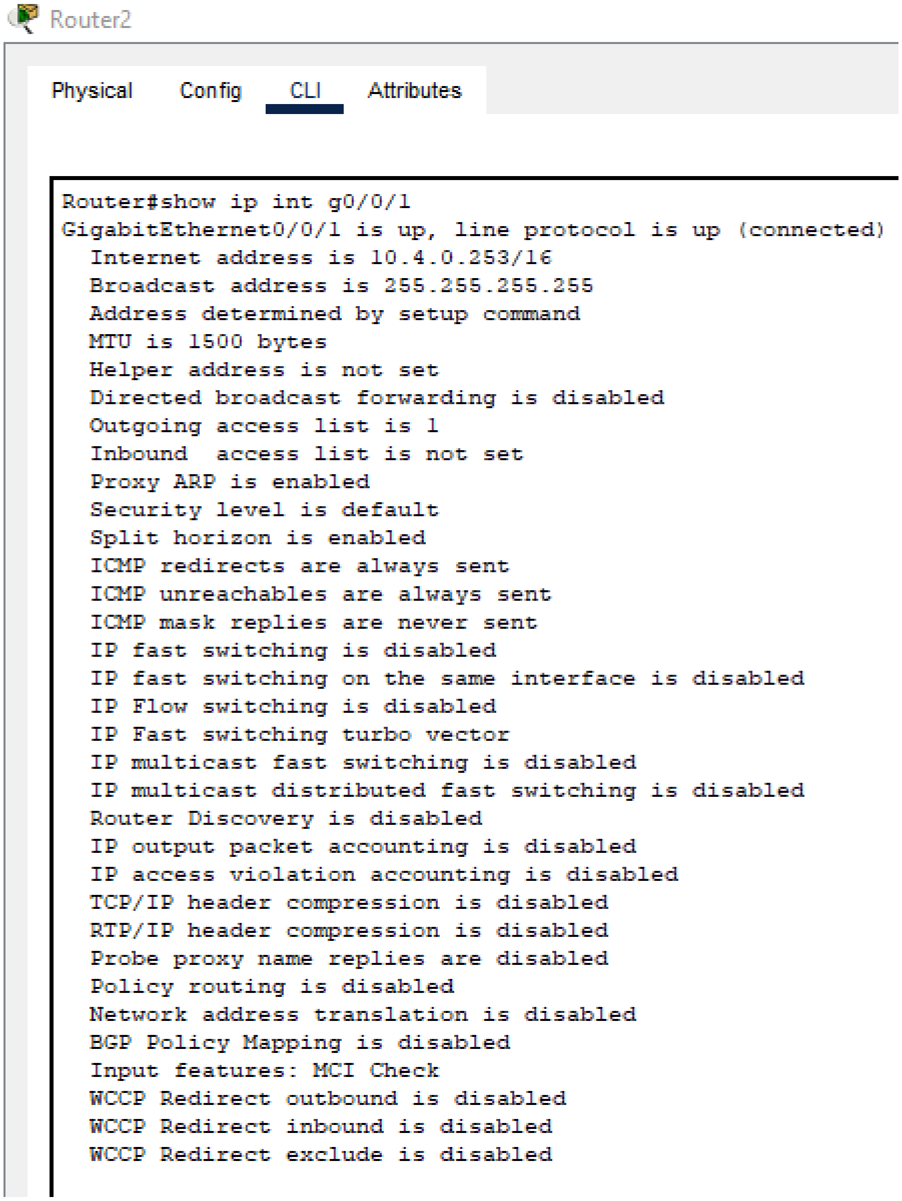
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time=1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.4.0.3: bytes=32 time=1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Step 1b - h (Note: port g0/0/1, on router 2, is the closest port to the destination):



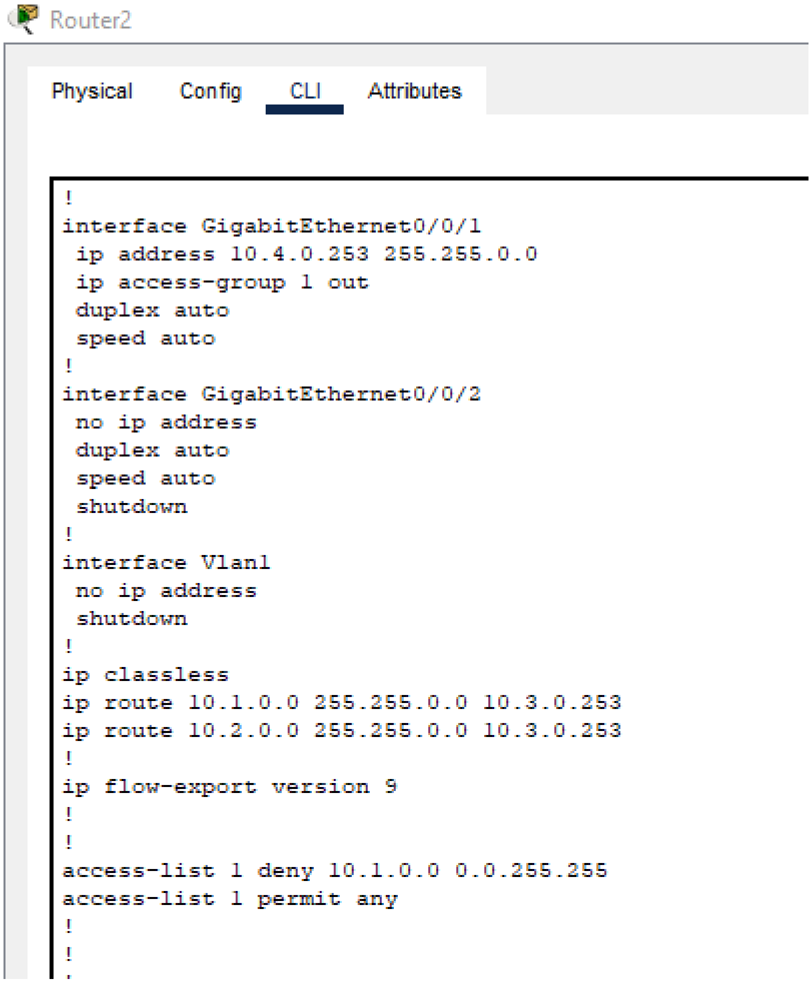
```
Router(config)#
Router(config)#access-list 1 deny 10.1.0.0 0.0.255.255
Router(config)#access-list 1 permit any
Router(config)#int g0/0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-lists
Standard IP access list 1
    10 deny 10.1.0.0 0.0.255.255
    20 permit any
```

Step 1i:



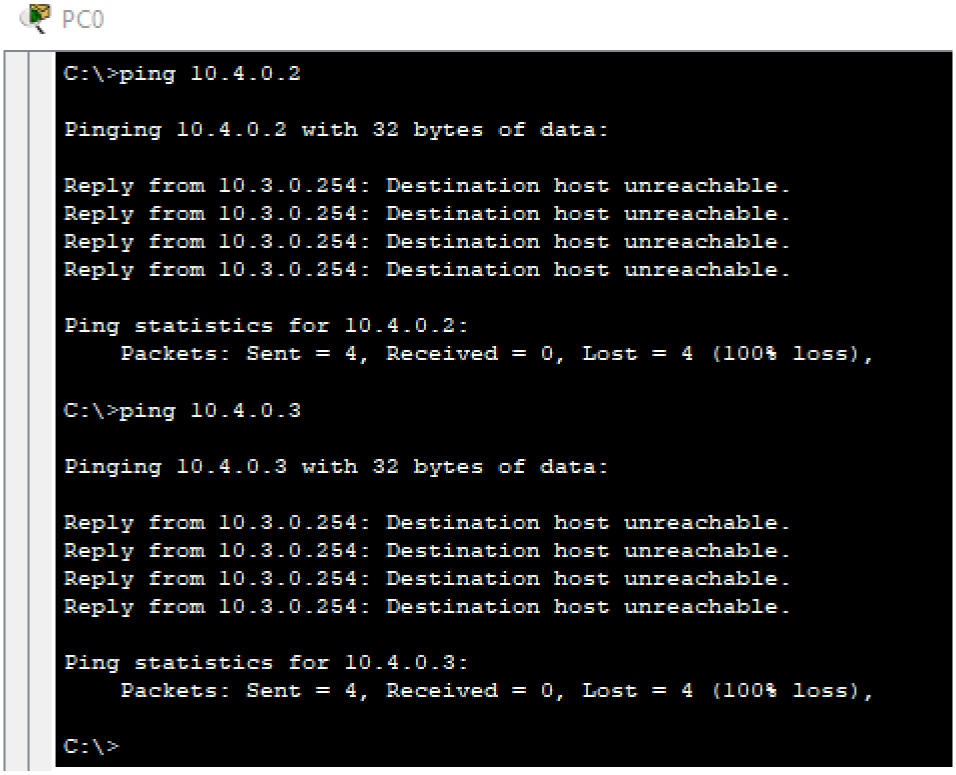
```
Router#show ip int g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up (connected)
  Internet address is 10.4.0.253/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

Step 1j:

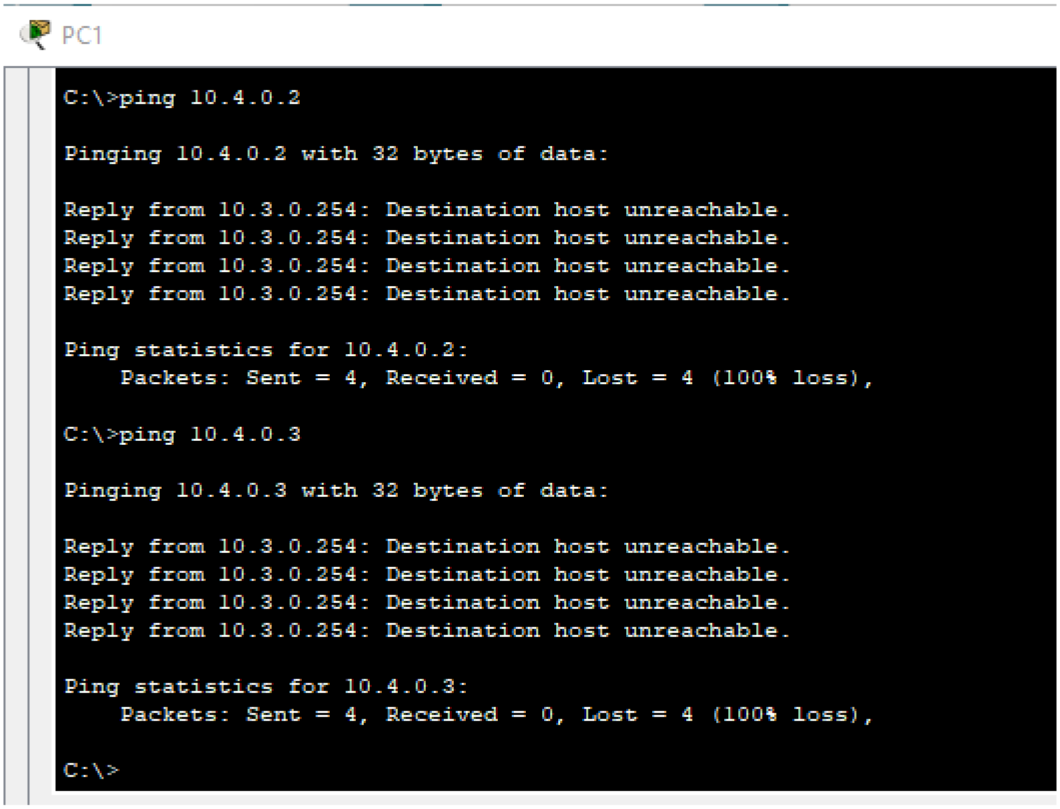


```
!
interface GigabitEthernet0/0/1
 ip address 10.4.0.253 255.255.0.0
 ip access-group 1 out
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 10.1.0.0 255.255.0.0 10.3.0.253
ip route 10.2.0.0 255.255.0.0 10.3.0.253
!
ip flow-export version 9
!
!
access-list 1 deny 10.1.0.0 0.0.255.255
access-list 1 permit any
!
!
```

Step 1k:

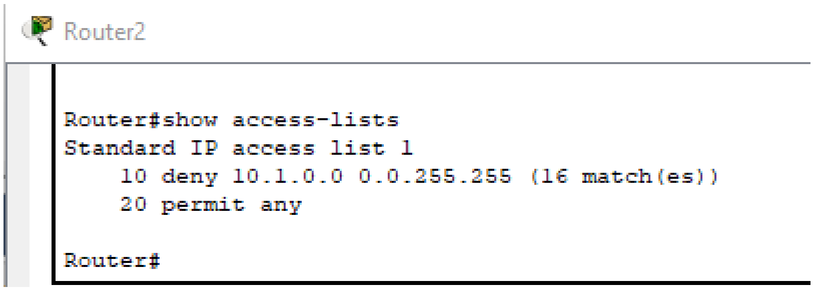


```
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



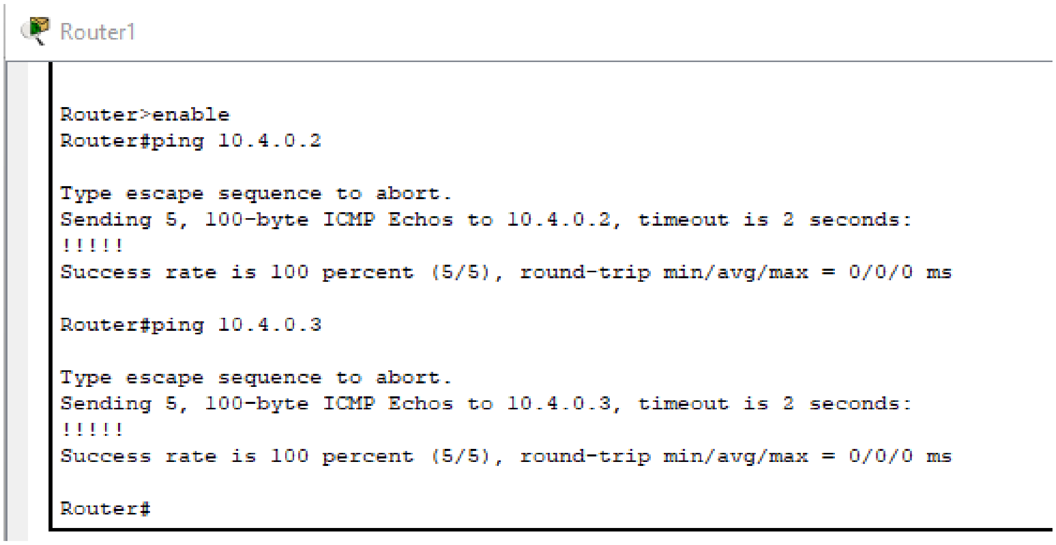
```
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Step 1l:



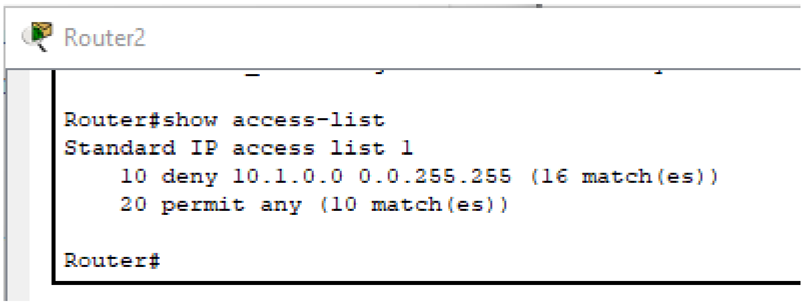
```
Router#show access-lists
Standard IP access list 1
    10 deny 10.1.0.0 0.0.255.255 (16 match(es))
    20 permit any

Router#
```

Step 1m:



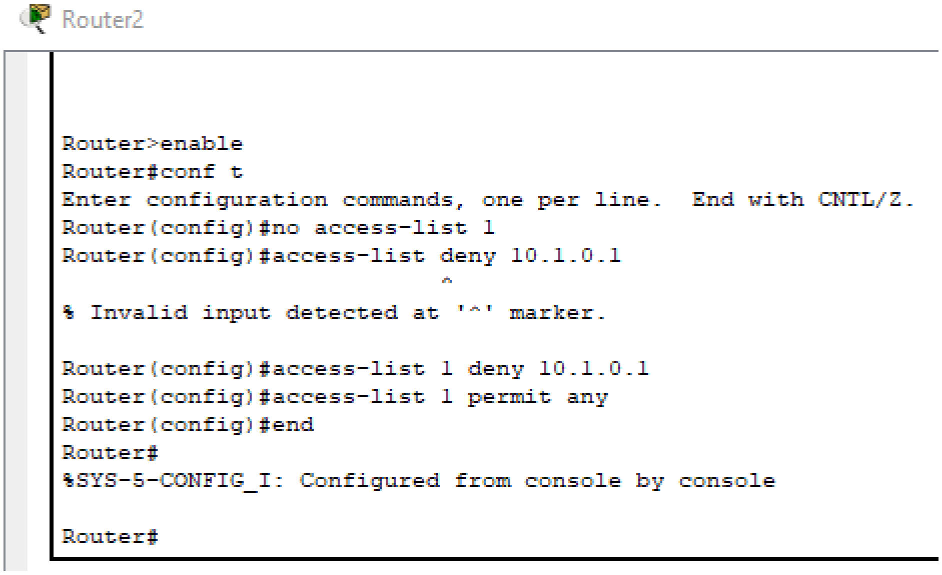
```
Router>enable
Router#ping 10.4.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Router#ping 10.4.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Router#
```

Step 1n:



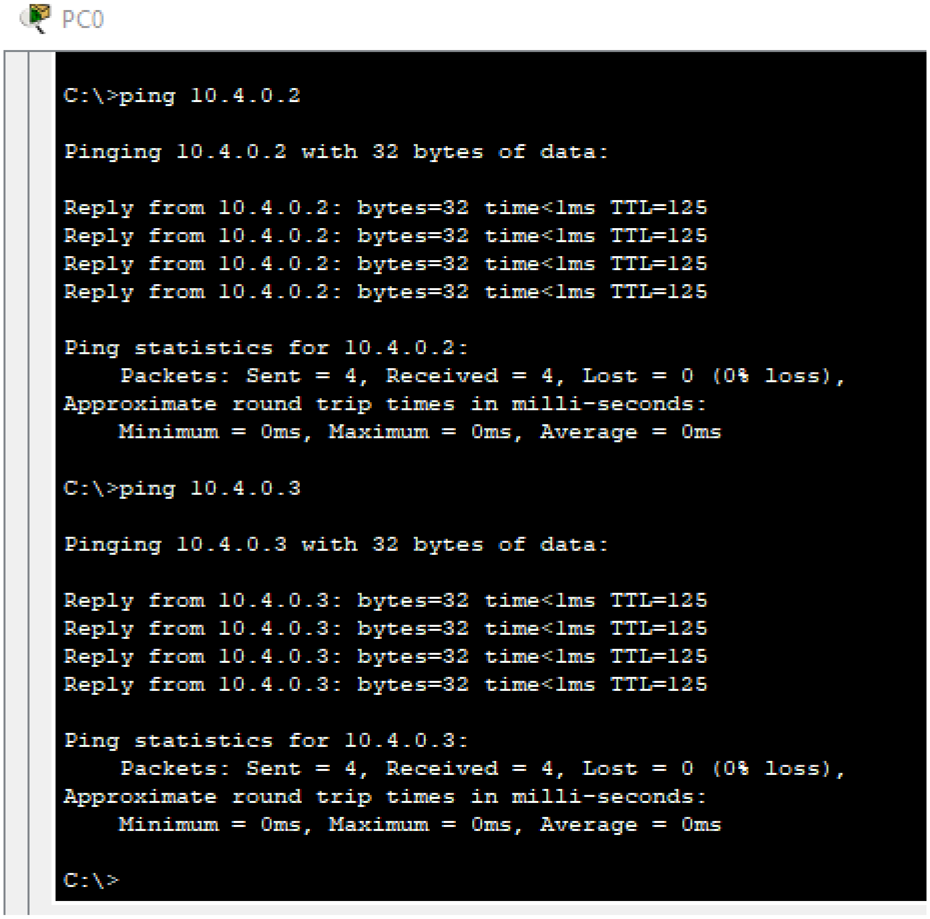
```
Router#show access-list
Standard IP access list 1
    10 deny 10.1.0.0 0.0.255.255 (16 match(es))
    20 permit any (10 match(es))

Router#
```

Step 2a - d:



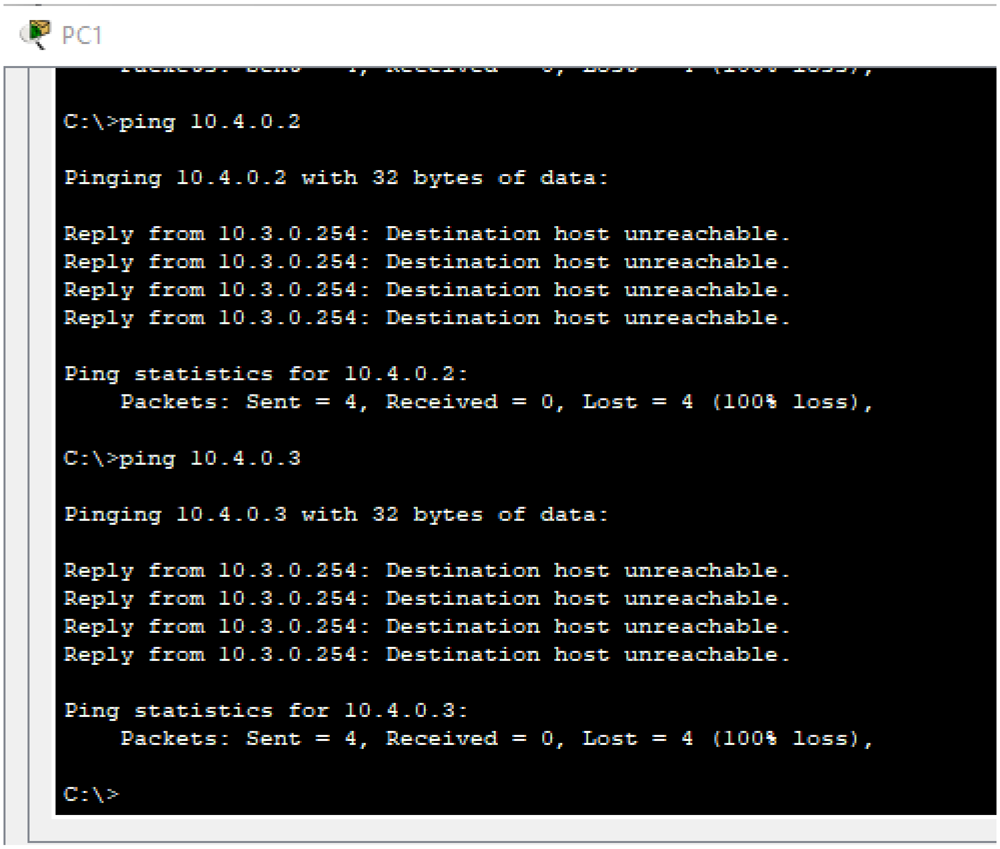
```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no access-list 1
Router(config)#access-list deny 10.1.0.1
                           ^
% Invalid input detected at '^' marker.

Router(config)#access-list 1 deny 10.1.0.1
Router(config)#access-list 1 permit any
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Step 2e:



```
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

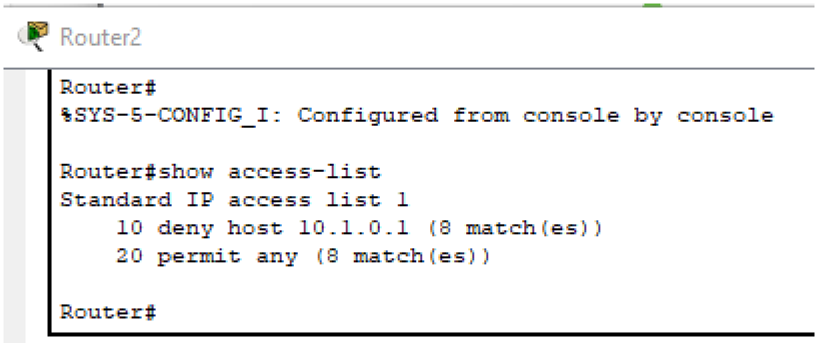
Step 2f:



PC1

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.
Reply from 10.3.0.254: Destination host unreachable.

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

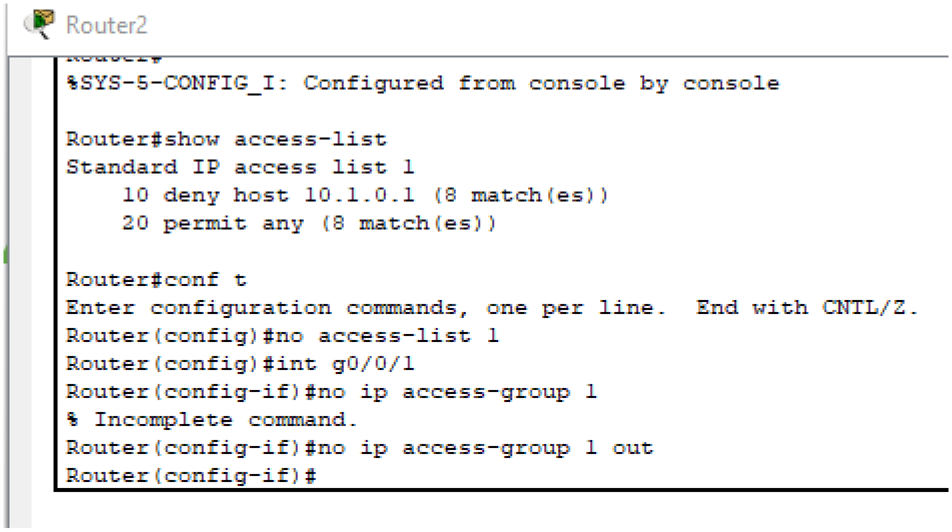
Step 2g:



Router2

```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Standard IP access list 1
    10 deny host 10.1.0.1 (8 match(es))
    20 permit any (8 match(es))

Router#
```

Step 2h - j:

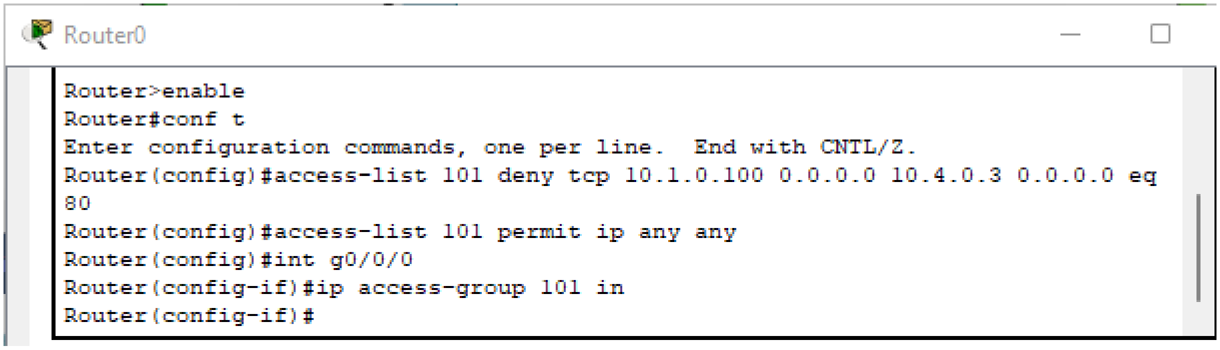


Router2

```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Standard IP access list 1
    10 deny host 10.1.0.1 (8 match(es))
    20 permit any (8 match(es))

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no access-list 1
Router(config)#int g0/0/1
Router(config-if)#no ip access-group 1
% Incomplete command.
Router(config-if)#no ip access-group 1 out
Router(config-if)#
```

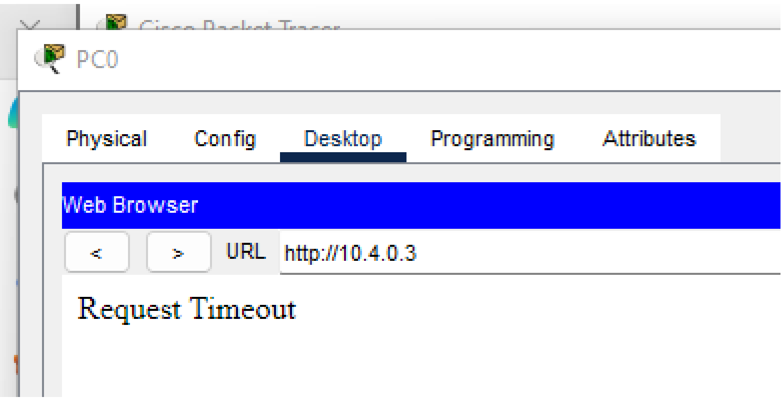
Lab Exercise 10.03: Extended ACLs on Routers

Step 1a - e (Note: interface g0/0/0 is where the PC0 is connected):



```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny tcp 10.1.0.100 0.0.0.0 10.4.0.3 0.0.0.0 eq
80
Router(config)#access-list 101 permit ip any any
Router(config)#int g0/0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#
```

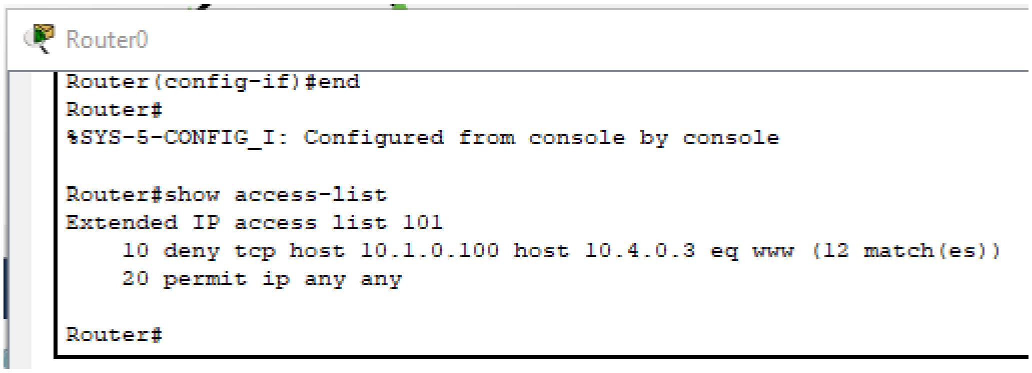
Step 2a - b:



http://10.4.0.3

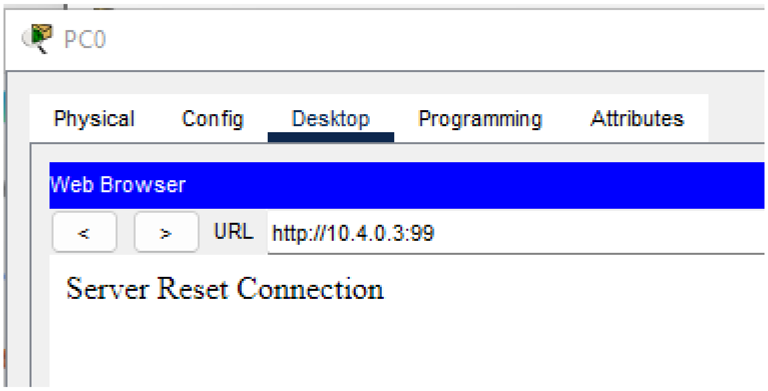
Request Timeout

Step 2c:



```
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Extended IP access list 101
    10 deny tcp host 10.1.0.100 host 10.4.0.3 eq www (12 match(es))
    20 permit ip any any

Router#
```

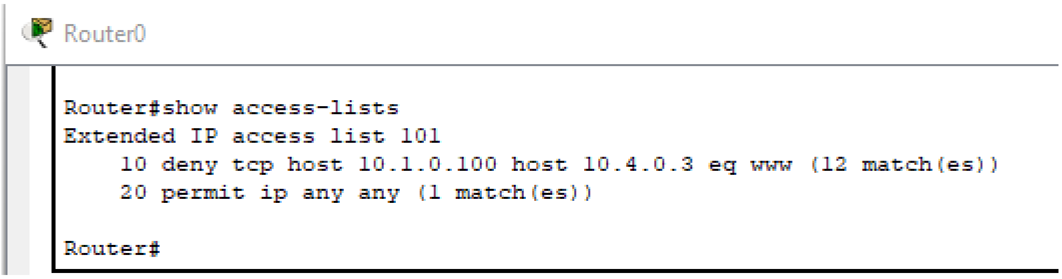
Step 2d - e:



http://10.4.0.3:99

Server Reset Connection

Step 2f:



```
Router#show access-lists
Extended IP access list 101
    10 deny tcp host 10.1.0.100 host 10.4.0.3 eq www (12 match(es))
    20 permit ip any any (1 match(es))

Router#
```

Lab Analysis:

1. The reason for configuring port security is to restrict the switch port to a set number of allowable MAC addresses. Next, to prevent CAM table overflow, which can turn a switch into a hub and allow attackers to eavesdrop on traffic. Finally, to prevent unauthorized access to the network by limiting the devices that can connect to a switch port
2. The actions the port security can take are to shutdown, restrict, or protect the port or interface.
3. Standard ACLs filter by source IP address.
4. Extended ACLs filter by protocol type, source and destination IP addresses, and port number
5. Standard ACLs are typically placed close to the destination of the traffic. Since they only filter on the source IP address, applying them close to the source could deny legitimate traffic from that source to other destinations.
6. Extended ACLs are often placed close to the source of the traffic. Because they are more granular, applying them near the source ensures that only the necessary traffic is allowed and unnecessary traffic is filtered out early.
7. The difference between subnet and wildcard masks is that subnet mask is used in IP addressing to divide networks into subnetworks and to identify the host portion of the IP address. A wildcard mask is used in ACLs to specify which bits of an IP address should be considered for matching; bits set to 0 are checked, bits set to 1 are ignored.
8. Inbound and outbound ACLs from an ACL perspective means that Inbound ACLs are applied to packets as they enter an interface. The ACL checks the packets before they're routed to the outbound interface. Outbound ACLs are applied to packets as they leave an interface. The ACL checks packets after routing has occurred but before they exit the interface. Finally, In normal usage, "inbound" and "outbound" might refer to the general direction of traffic relative to a network. In the ACL context, they're specifically related to the direction of traffic entering or leaving a network interface on a device.

Key Term Quiz:

1. MAC address
2. Source IP address
3. Port
4. Interface