LAB 8: Firewall Implementation, Router Access Control List (ACL)

Objective(s):

- To Understand the Router Firewall: Access Control Lists (ACLs).

Background:

Packet filtering at the network level can be achieved by applying the Access Control Lists (ACLs) at the router called router firewall. ACLs at the router filter the inbound traffic while it permits or deny packets based on source IP/network and destination IP/network, IP, TCP, UDP protocol information. Generally, we use the ACLs to provide a basic level of security for accessing our network. Access lists can allow one host to access a part of network and prevent another host from accessing the same area.

A standard ACL can be used for several purpose. In this lab we will see how it can be used in controlling the unwanted network traffic. With standard ACL, we can define certain conditions for the network traffic passing through the router.

By default, router does not filter any traffic unless we manually configure an ACL.

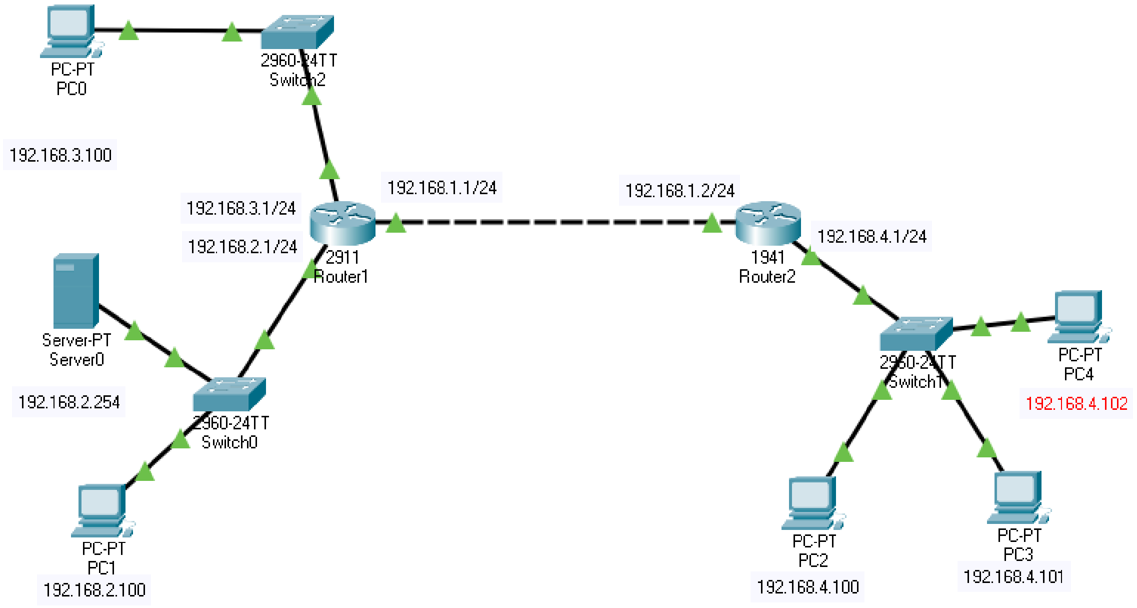
There are two types of ACLs:

1. **Standard ACL:** permits or denies packets based on source IP address.
    - Valid ACL ID range is: 1 - 99.
    - Applied closest to the destination.
    - Denies or permits
        - **Source IP Address**
2. **Extended ACL:** it permits or denies packets based on source and destination IP address and also based on IP protocol information.
    - Valid Extended ACL ID range is: 100 - 199
    - Applied closest to the Source.
    - Denies or permits
        - **Source IP Address**
        - **Destination IP Address**
        - **Port or Service**

Access lists of some protocols must be identified by a name, and access lists of other protocols must be identified by a number. Some protocols can be identified by either a name or a number. When a number is used to identify an access list, the number must be within the specific range of numbers that is valid for the protocol. Cisco Access Control Lists are the set of conditions grouped together by name or number. These conditions are used in filtering the traffic passing from router. Through these conditions we can filter the traffic; either when it enters in router or when it exits from router.

When creating an access list, we define criteria that are applied to each packet that is processed by the router; the router decides whether to forward or block each packet on the basis of whether or not the packet matches the criteria.

Configurations



Router 1 Configuration

```
Router>enable
Router#configure terminal
Enter configiation commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

Router(config-if)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up

Router(config-if)#interface gigabitEthernet 0/2
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed
state to up

Router(config-if)#exit
Router(config)#
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.1.2
Router(config)#
Router#
```

Router 2 Configuration

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shut down

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up

Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.1.1
Router(config)#
```

1. Standard ACL Implementation

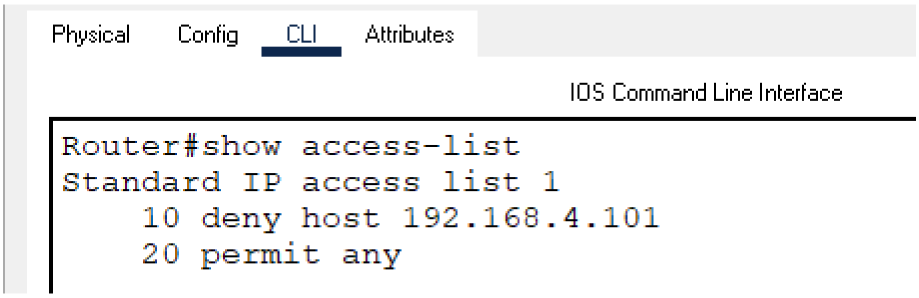
a. Blocking a host (192.168.4.101) in the network 192.168.2.0

1. Create the access list (standard: 1-99)
   a. Specify more specific statements on the top
   b. Specify more general statements at the bottom
   c. Note that at the end of every access-list there is an implicit deny (eg. Access-list 1 deny any)
2. Apply the access list to an interface (outbound)

Router 1 Configuration

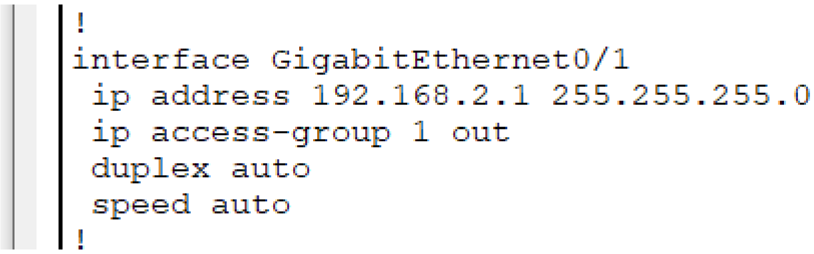
- Deny (source ip address)
- Permit (any ipaddress)
- There is implicit deny (any address) at the end as the default which is not seen.

```
Router(config)#access-list 1 deny 192.168.4.100 0.0.0.0
Router(config)#access-list 1 permit any
Router(config)#exit
Router#show access-list
```



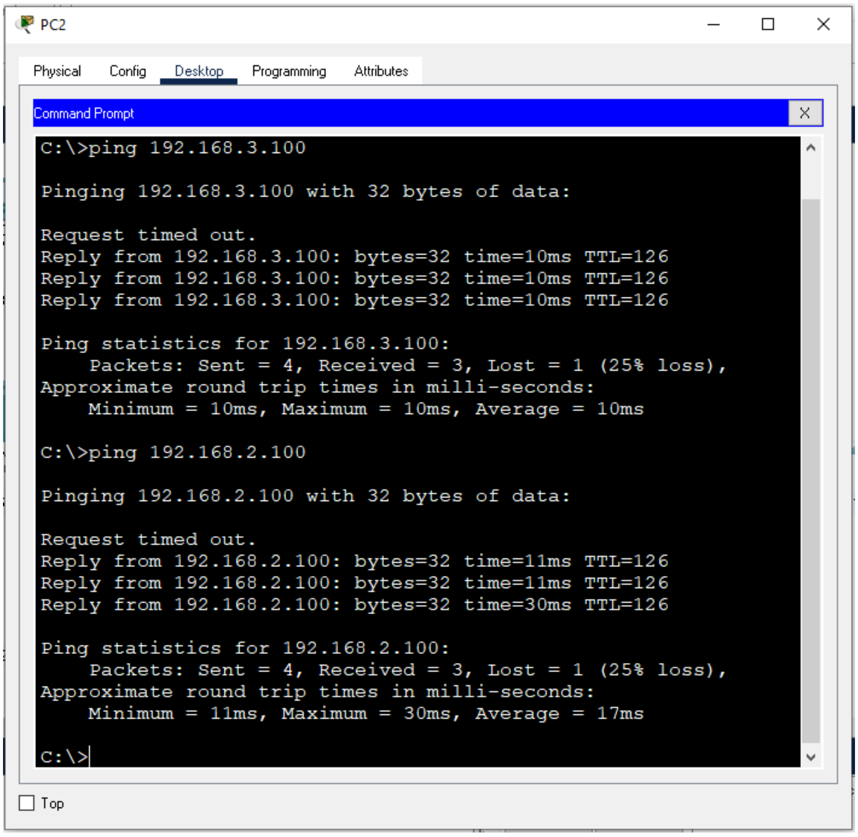
```
Router#show access-list
Standard IP access list 1
    10 deny host 192.168.4.101
    20 permit any
```

```
Router(config)#interface gigabitethernet 0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show run
```

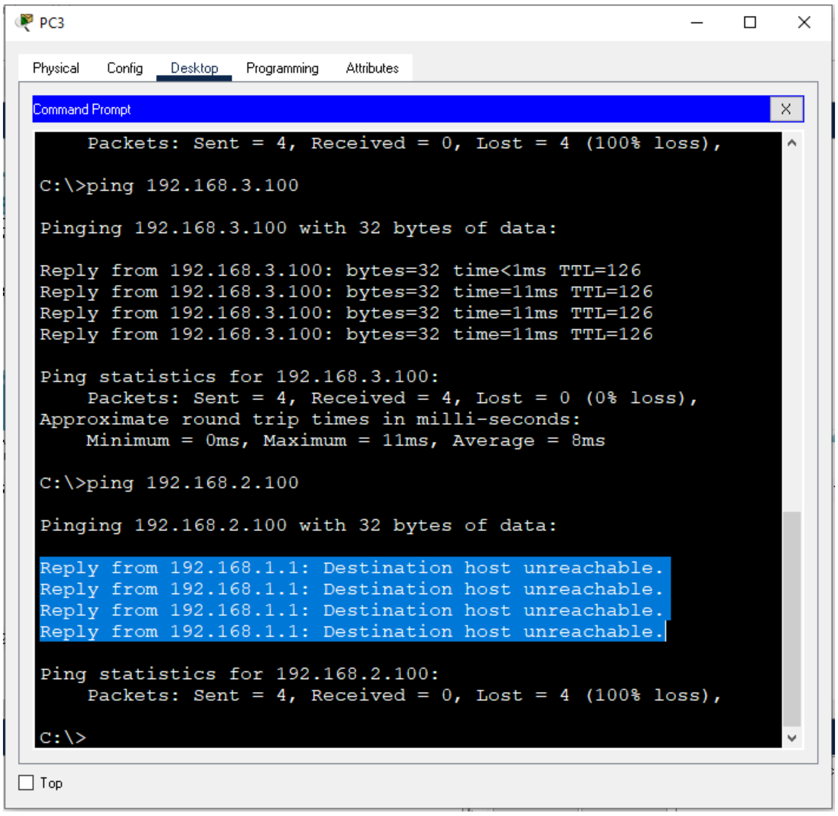


```
!
interface GigabitEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
```

Verify the Connectivity



```
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.100: bytes=32 time=10ms TTL=126
Reply from 192.168.3.100: bytes=32 time=10ms TTL=126
Reply from 192.168.3.100: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.100: bytes=32 time=11ms TTL=126
Reply from 192.168.2.100: bytes=32 time=11ms TTL=126
Reply from 192.168.2.100: bytes=32 time=30ms TTL=126

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 30ms, Average = 17ms

C:\>
```

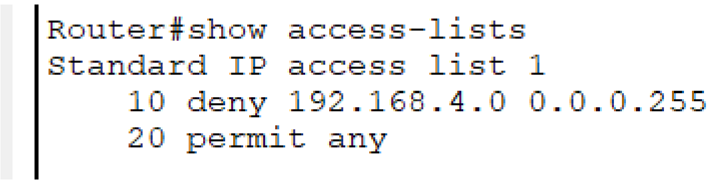


```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 192.168.3.100: bytes=32 time<1ms TTL=126
Reply from 192.168.3.100: bytes=32 time=11ms TTL=126
Reply from 192.168.3.100: bytes=32 time=11ms TTL=126
Reply from 192.168.3.100: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 8ms

C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

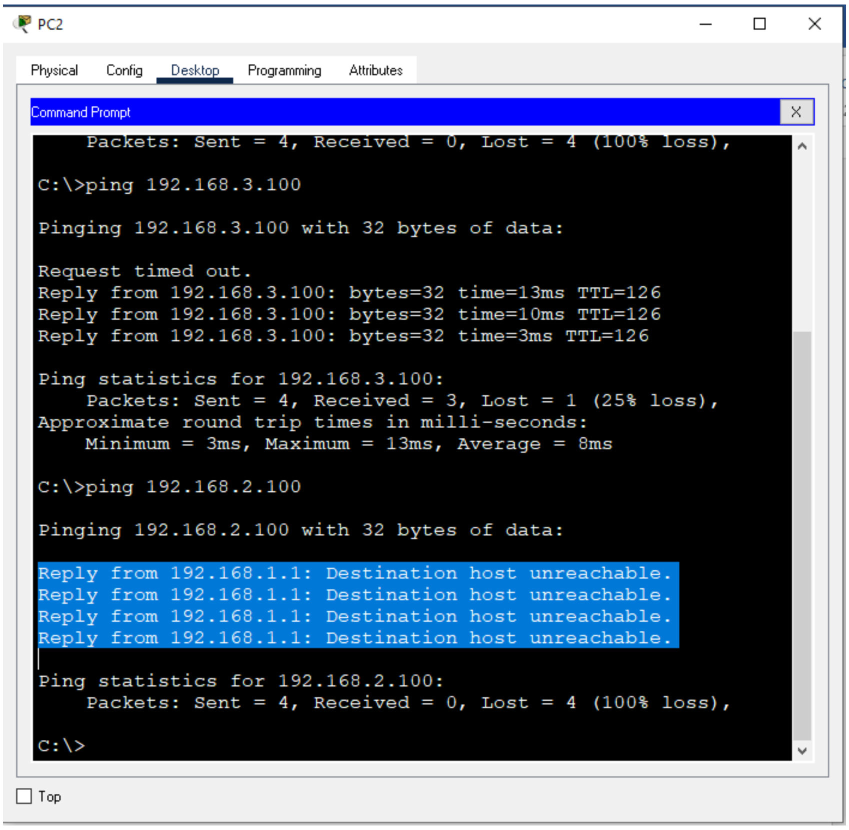
b. Blocking a Network (E.g 192.168.4.0)

We should use wild mask (0.0.0.255) for the Class C network when we need to block the whole network e.g 192.168.4.0.

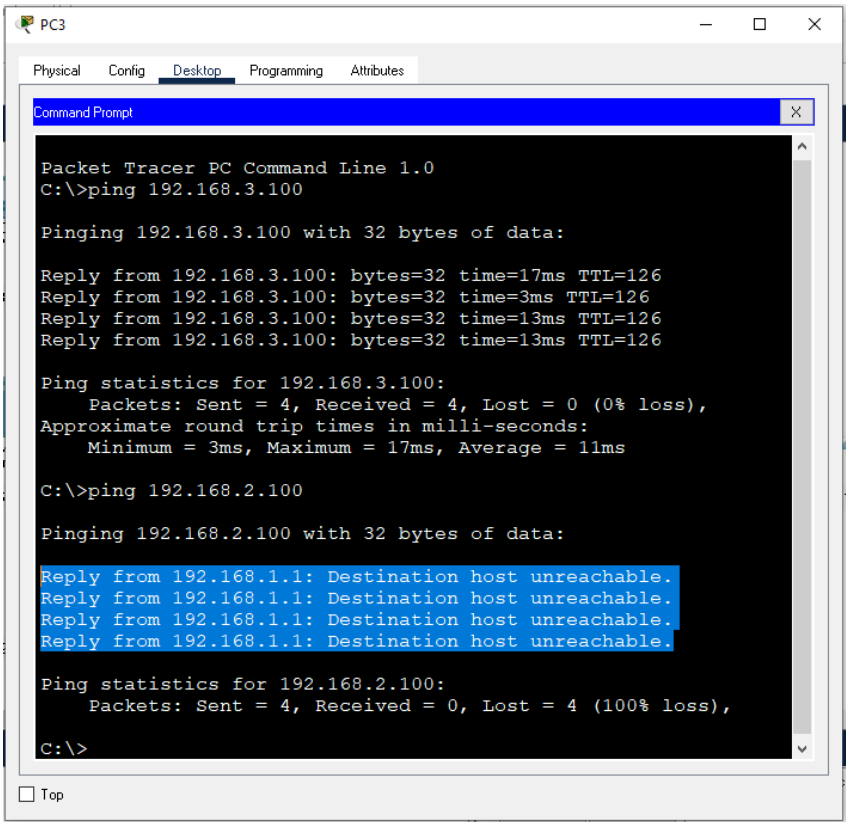
```
Router(config)#no access-list 1
Router(config)#access-list 1 deny 192.168.4.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#exit
Router#show access-lists
```



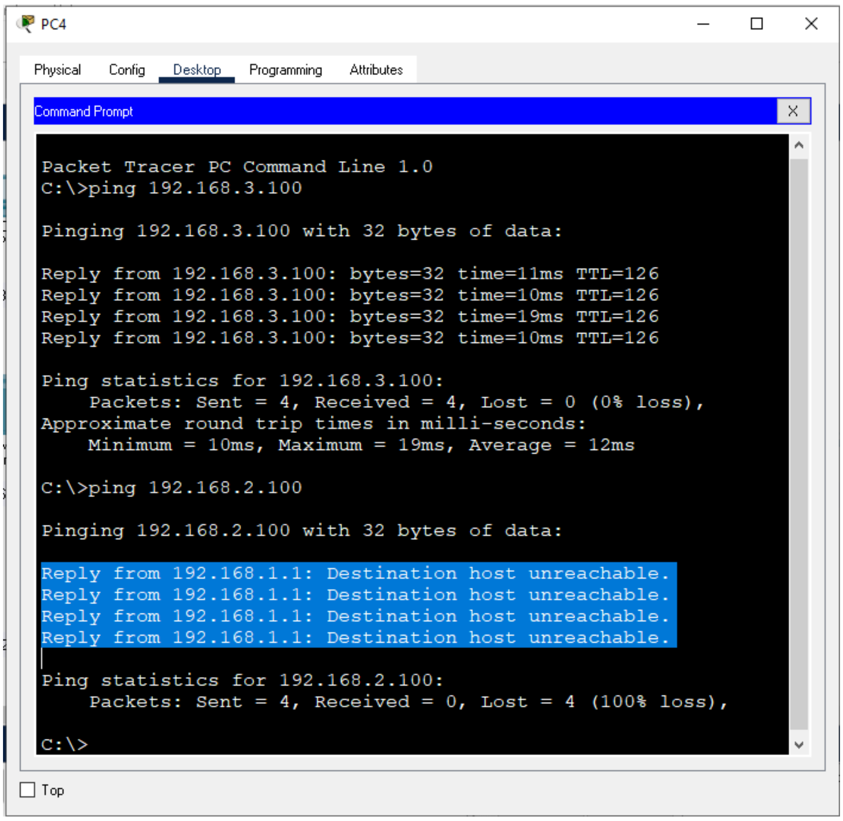
```
Router#show access-lists
Standard IP access list 1
    10 deny 192.168.4.0 0.0.0.255
    20 permit any
```



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

C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.100: bytes=32 time=13ms TTL=126
Reply from 192.168.3.100: bytes=32 time=10ms TTL=126
Reply from 192.168.3.100: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 13ms, Average = 8ms

C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 192.168.3.100: bytes=32 time=17ms TTL=126
Reply from 192.168.3.100: bytes=32 time=3ms TTL=126
Reply from 192.168.3.100: bytes=32 time=13ms TTL=126
Reply from 192.168.3.100: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 17ms, Average = 11ms

C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 192.168.3.100: bytes=32 time=11ms TTL=126
Reply from 192.168.3.100: bytes=32 time=10ms TTL=126
Reply from 192.168.3.100: bytes=32 time=19ms TTL=126
Reply from 192.168.3.100: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 19ms, Average = 12ms

C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

2. Extended ACL

a. Create an access-list (100-199)
- denies or permits port (service)
- denies or permits source IP Address
- denies or permits Destination IP Address

b. Apply the access-list to an interface (inbound)

Remove the Standard ACL from Router 1

Router 1

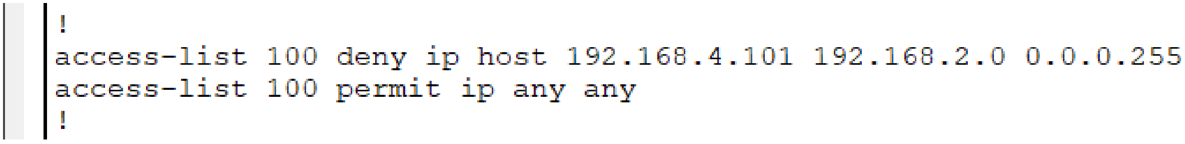
```
Router(config)#no access-list 1
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
```

Configure Extended ACL in Router 2

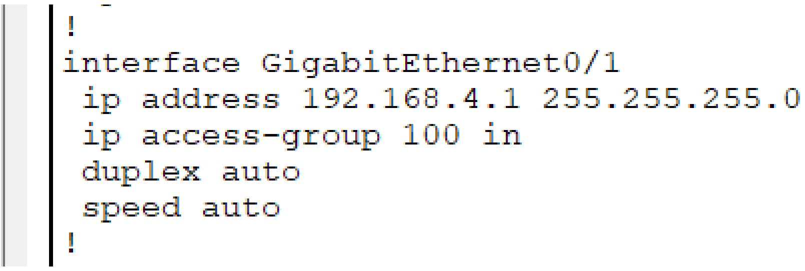
Router 2

- Deny (protocol-source-destination)
- Permit (protocol-any-any)
- There is implicit deny (protocol-any-any) at the end as the default which is not seen.

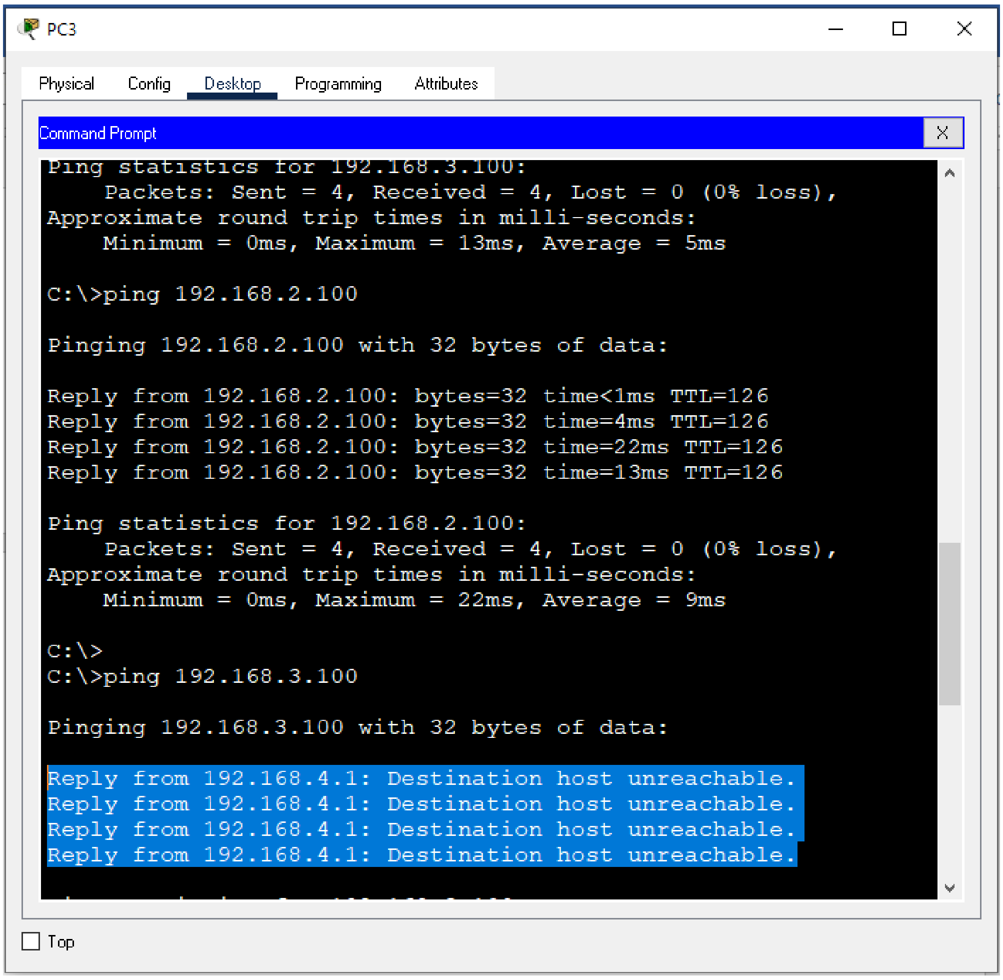
```
Router(config)#access-list 100 deny ip 192.168.4.101 0.0.0.0
192.168.4.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
Router(config)#exit
Router#

Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
```



```
!
access-list 100 deny ip host 192.168.4.101 192.168.2.0 0.0.0.255
access-list 100 permit ip any any
!
```



```
!
interface GigabitEthernet0/1
 ip address 192.168.4.1 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
!
```

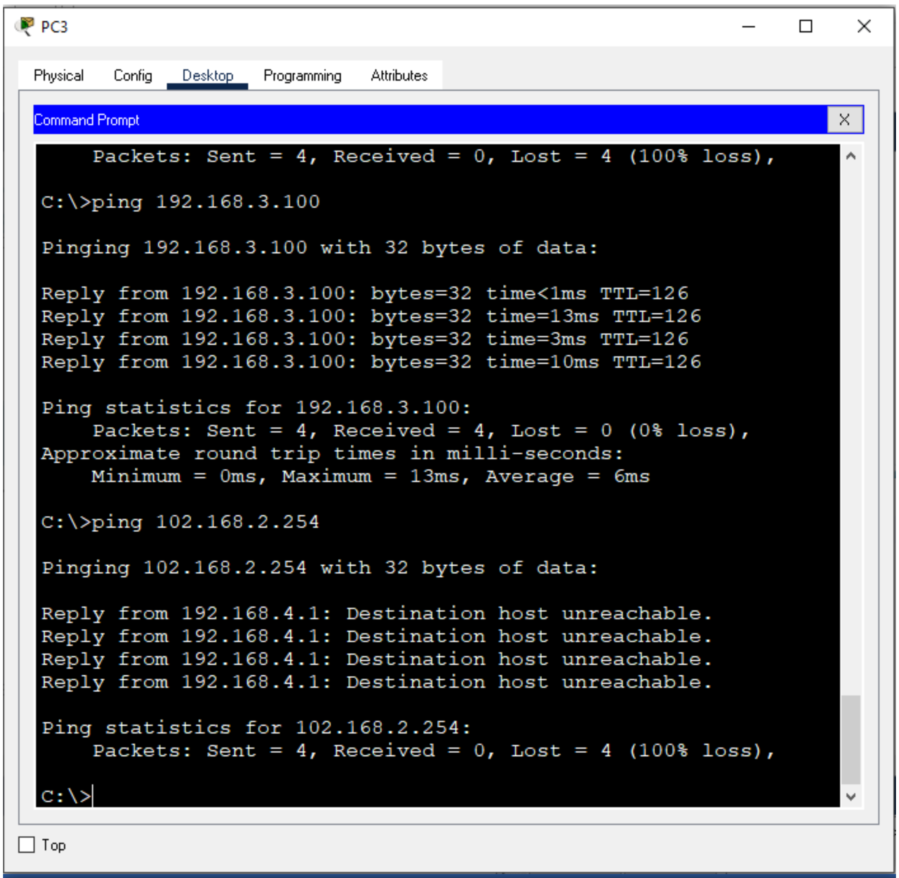


```
Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 5ms

C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.2.100: bytes=32 time<1ms TTL=126
Reply from 192.168.2.100: bytes=32 time=4ms TTL=126
Reply from 192.168.2.100: bytes=32 time=22ms TTL=126
Reply from 192.168.2.100: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 9ms

C:\>
C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
```

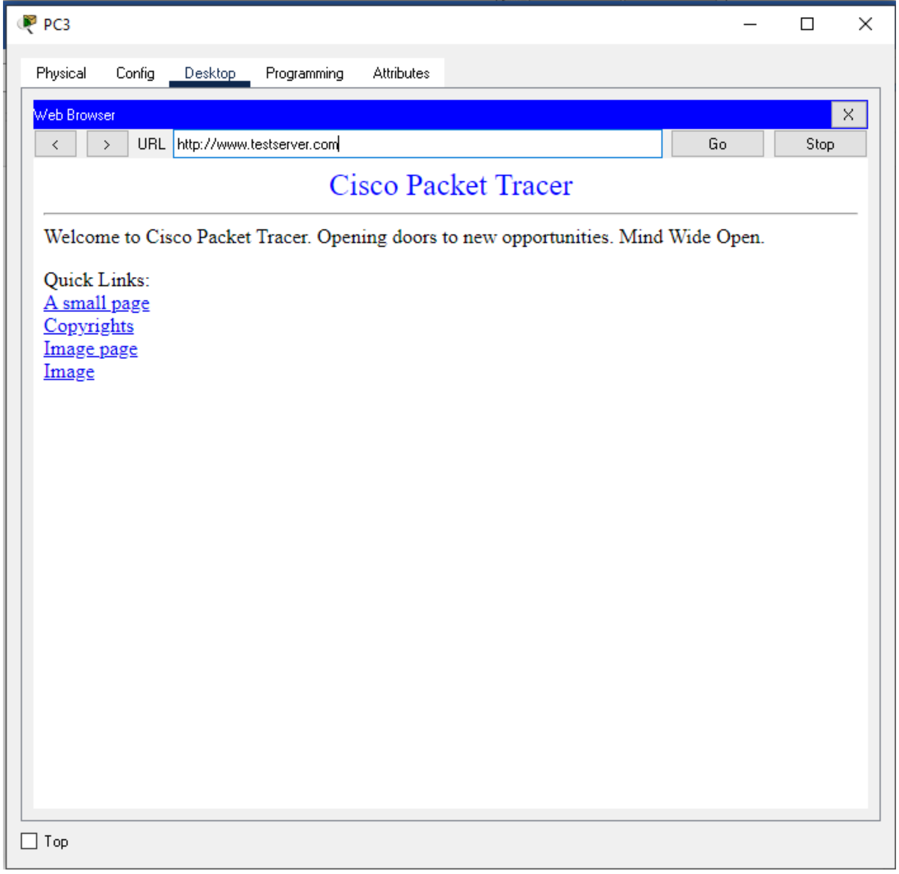
Allow HTTP traffic but block ICMP (ping)

```
Router(config)#no access-list 100
Router(config)#access-list 100 deny icmp 192.168.4.101 0.0.0.0
192.168.2.254 0.0.0.0
Router(config)#access-list 100 permit ip any any
Router(config)#
```

Verify ACLs



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

C:\>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:

Reply from 192.168.3.100: bytes=32 time<1ms TTL=126
Reply from 192.168.3.100: bytes=32 time=13ms TTL=126
Reply from 192.168.3.100: bytes=32 time=3ms TTL=126
Reply from 192.168.3.100: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 6ms

C:\>ping 102.168.2.254

Pinging 102.168.2.254 with 32 bytes of data:

Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.

Ping statistics for 102.168.2.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



URL http://www.testserver.com

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image