

# Access Control List

## Access Control List:

- ACL stand for Access Control List.
- ACL is set of statement which allow, deny network traffic from one router to other router.
- In other words, we can say it is filters which allow us to control traffic (Packets) flowing in network.
- It is Layer 3 security; we can control flow of traffic from one router to other router.
- ACLs are always processed from top to down in sequential order.
- A Packet is compared with ACL conditions until it finds a match.
- Once a match is found for packet, no further comparison will be done.
- Interface will take action based on match condition.
- There are two possible action permit and deny in ACL.
- If permit condition match, packet will be allowed to pass from interface.
- If deny condition match, packet will be destroyed immediately.
- Every ACL has a default deny statement at end of it.
- If a packet does not meet with any conditions, it will be destroyed by default deny.
- Empty ACL will permit all traffic by default.
- ACL can filter only the traffic passing from interface.
- Standard ACL can filter only the source IP address.
- Standard ACL should be placed near the destination devices.
- Extended ACL should be placed near the source devices.
- First, create an Access-List globally and then assign it to an interface.

## Different Types of ACL as given below:

- Standard (again it is divided into two name or number).
- Extended (again it is divided into two name or number).
- Time-Based ACL.

## Different between Standard and Extended ACL

Standard Access List	Extended Access List
The Access list number range from 1 to 99 or 1300-1999.	The Access list number range from 100 to 199 or 2000-2699.
Can block a host, network and subnet.	Can block a host, network, Subnet and Services.
Implemented Closest to the destination.	Implemented Closest to the Source.
Filtering is done based on only source IP address	Filtering can be done with source, destination, protocol, port number etc.
All Services are block	Selected Service can block.

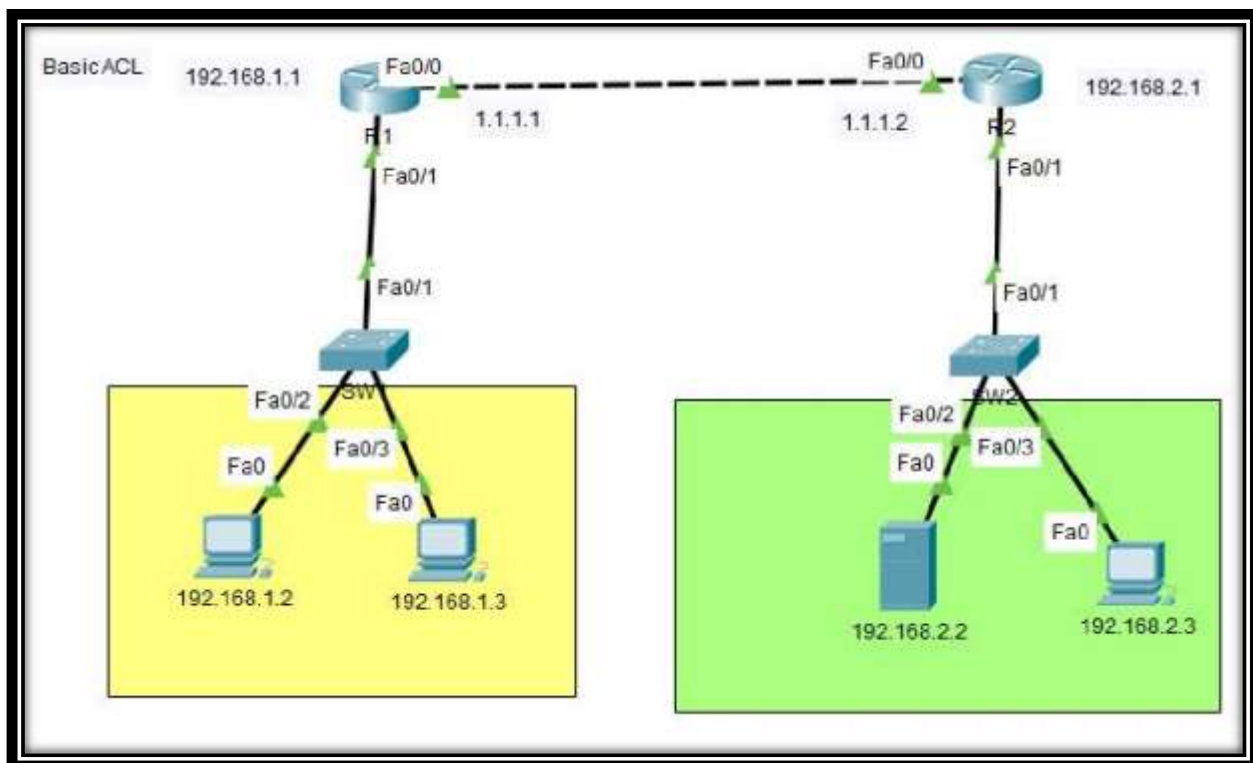
### Numbered Access List:

- These are the access list which cannot be deleted specifically one created.
- That is if we want to remove any rule from an Access-List then this is not permitted in the case of numbered access list.
- If we try to delete a rule from access list then the whole access list will be deleted.
- The numbered access list can be used with both Standard and Extended access list.

### Named Access List:

- In these types of access list, a name is assigned to identify an access list.
- It is allowed to delete a named access list unlike numbered access list.
- Like numbered ACL, these can be used with both standard and extended access list.

**Lab time:** Objective of Lab. :( Lab on Standard Access List Numbered)



Configuration for Router1	Configuration for Router2
<pre> en Config t hostname R1  int f0/0 ip add 1.1.1.1 255.0.0.0 no sh  int f0/1 ip add 192.168.1.1 255.255.255.0 no sh  router rip ver 2 no auto-summary  network 192.168.1.0 network 1.1.1.0 </pre>	<pre> en Config t hostname R2 int f0/0 ip add 1.1.1.2 255.0.0.0 no sh  int f0/1 ip add 192.168.2.1 255.255.255.0 no sh  router rip ver 2 no auto-summary network 192.168.2.0 network 1.1.1.0 </pre> <p><b>Standard ACL on R2 to deny PC1</b></p> <pre> access-list 10 deny host 192.168.1.2 access-list 10 permit any int f0/0  ip access-group 10 in </pre> <p>This is only for 1 PC if you need ACL with Complete Network then as given below.</p> <p><b>Standard ACL on R2 to deny Whole Network</b></p> <pre> access-list 10 deny 192.168.1.0 0.0.0.255 access-list 10 permit any int f0/0  ip access-group 10 in </pre>
To Check ACL we can type	Sh ip access list

**PC1 (192.168.1.2 is not able to ping 192.168.2.2 Because we Apply ACL:**

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC 192.168.1.3 is able to ping 192.168.2.2:

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

**The Table below lists many of popular port numbers and their related transport layer protocol and applications.**

Port Number(s)	Protocol	Application
20	TCP	FTP
21	TCP	FTP CONTROL
22	TCP	SSH
23	TCP	TELNET
25	TCP	SMTP
53	TCP, UDP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP(WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384-32,767	UDP	RTP-BASED VOICE AND VIDEO

**Extended ACLs:**

- Check based on the protocol, source address, destination address and port number
- Cisco expanded the original ACL Ranges
- Standard:1-99,1300-1999
- Extended:100-199, 2000-2699

### Example:

#### Creation of Extended Access List

Router(config)# access-list <acl no> <permit/deny> <protocol> <source address> <source wildcard mask> <destination address> <destination wildcard mask> <operator> <service>

R1(config)#access-list 100 deny tcp host 192.168.1.2 host 192.168.2.2 eq 80

R1(config)#access-list 100 deny tcp host 192.168.1.3 host 192.168.2.3 eq 80

R1(config)#access-list 100 permit IP any any

#### Implementation of Extended Access List:

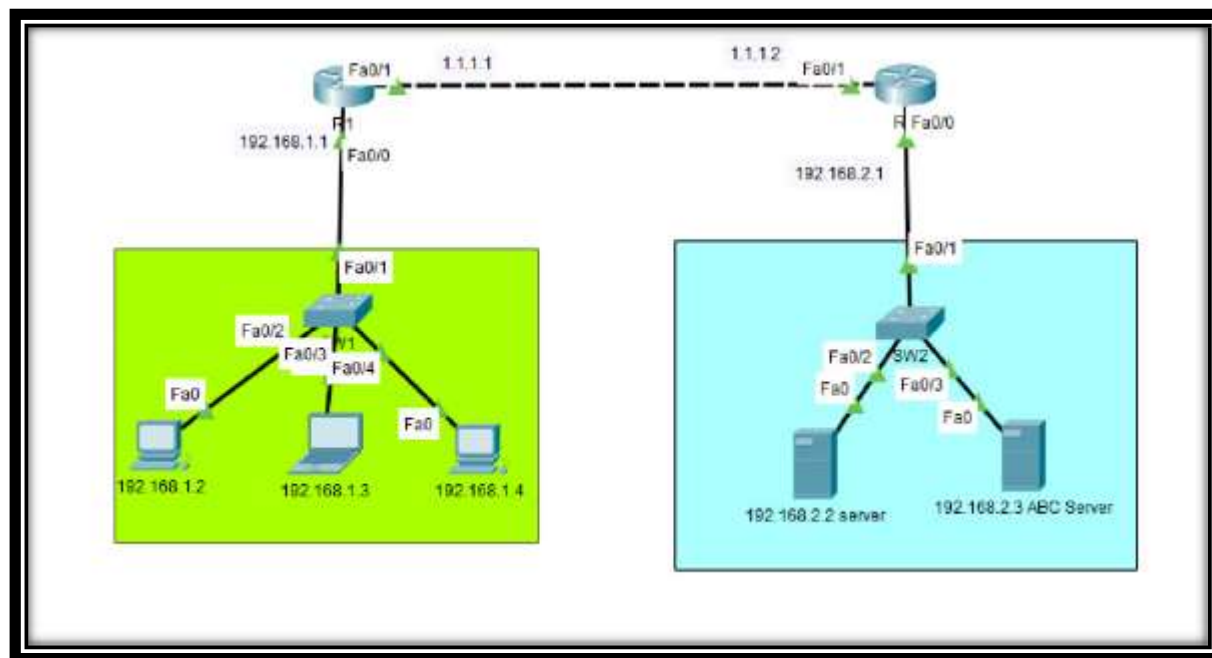
Router(config)#interface <interface type> <interface no>

Router(config-if)#ip access-group <number> <out/in>

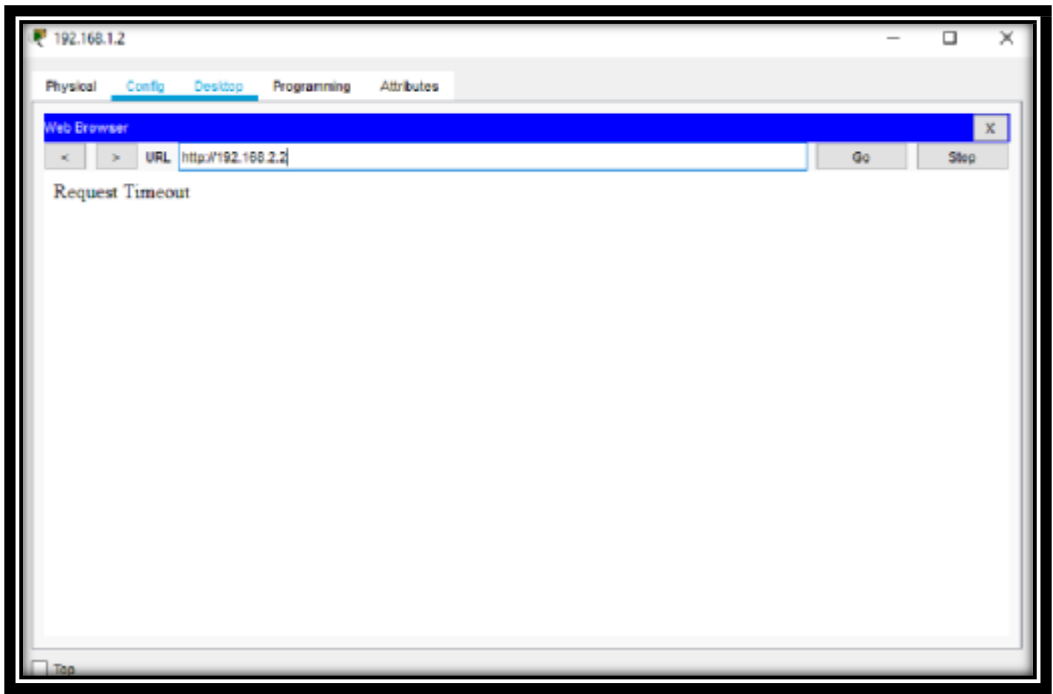
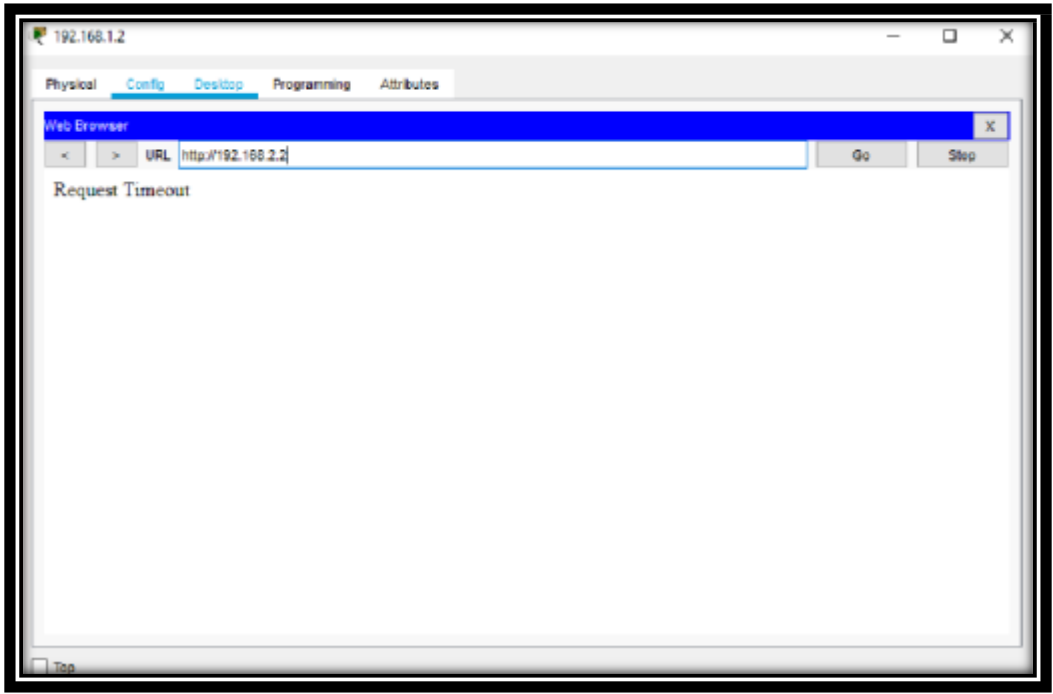
R1(config)#int fa0/0

R1(config-if)#ip access-group 100 in

#### So let see lab for this



R1 Configuraiton:	R2 Configuration:
<pre> en config t hostname R1 int f0/0 ip add 192.168.1.1 255.255.255.0 no sh  int f0/1 ip add 1.1.1.1 255.0.0.0 no sh  router rip ver 2 no auto-summary network 192.168.1.0 network 1.1.1.0  access-list 100 deny tcp host 192.168.1.2 host 192.168.2.2 eq 80 access-list 100 deny tcp host 192.168.1.3 host 192.168.2.3 eq 80 access-list 100 permit IP any any  int fa0/0 ip access-group 100 in </pre>	<pre> en config t hostname R2 int f0/0 ip add 192.168.2.1 255.255.255.0 no sh  int f0/1 ip add 1.1.1.2 255.0.0.0 no sh  router rip ver 2 no auto-summary network 192.168.2.0 network 1.1.1.0 </pre>





### **Creation of Extended Named Access List Syntax:**

ip access-list extended <name>

<permit/deny> <protocol> <source address> <source wildcard mask> <destination address> <destination wildcard mask> <operator> <service>

permit IP any any

Then

### **Implementation of Extended Named Access List:**

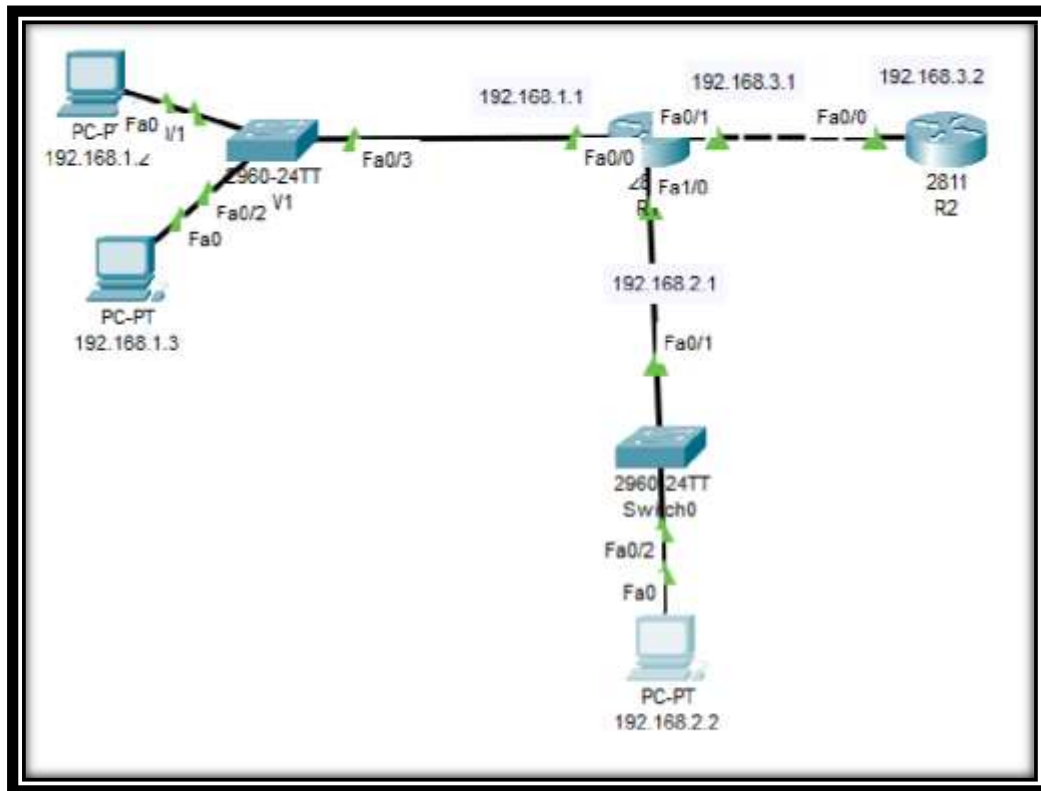
interface <interface type> <interface no>

ip access-group <ACL Name> <out/in>

### **Lab time:**

#### **ACL Configuration Lab Exercise:**

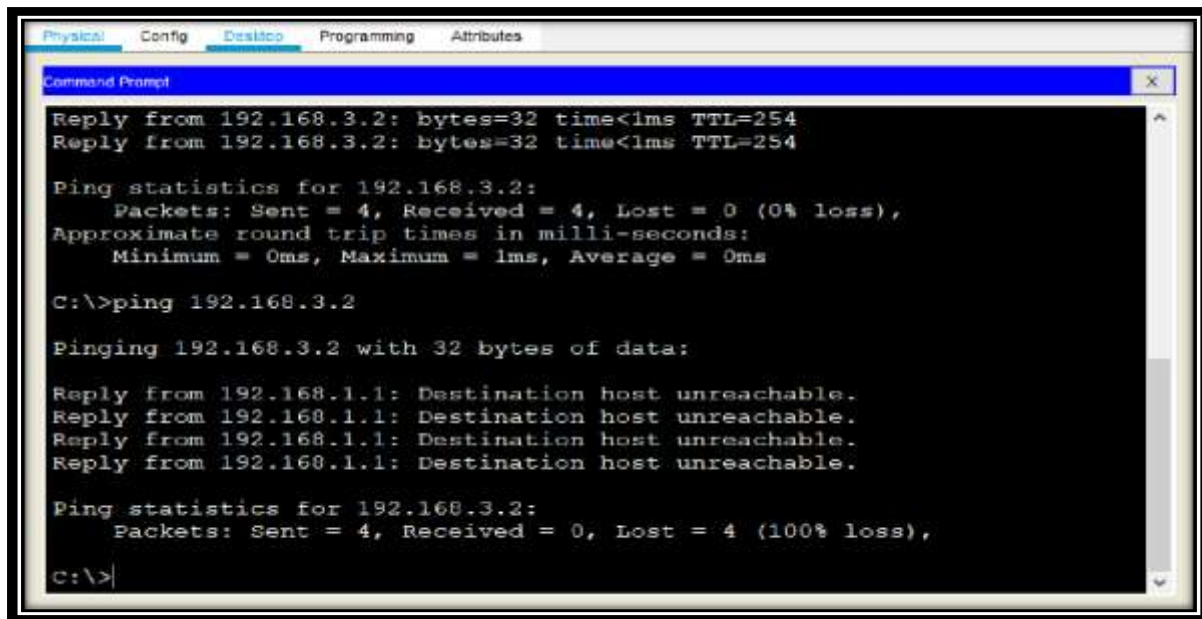
1. Configure Telnet in R2
2. Check All PC can Telnet to R2 and Ping R1 and R2
3. Configure and Apply named extended ACL on R1 as follow
  - a) Permit Telnet from PC1 to R2. Telnet to R2 must be denied for all other pcs in the network.
  - b) Permit ping from PC2 to R2. Ping to R2 must be denied for all other pcs in the network.



R1 Configuration	R2 Configuraiton
<pre> en config t hostname R1  int f0/0 ip add 192.168.1.1 255.255.255.0 no sh  int f0/1 ip add 192.168.3.1 255.255.255.0 no sh  int f1/0 ip add 192.168.2.1 255.255.255.0 no sh </pre>	<pre> en config t hostname R2  int f0/0 ip add 192.168.3.2 255.255.255.0 no sh  enable secret cisco username admin password admin  line vty 0 4 login local  router ospf 1 </pre>

<pre> username admin password admin  router ospf 1 int f0/0 ip ospf 1 area 0  int f1/0 ip ospf 1 area 0  int f0/1 ip ospf 1 area 0  IP access list Extended abc   permit tcp host 192.168.1.2 host 192.168.3.2 eq telnet   deny tcp 192.168.1.0 0.0.0.255 host 192.168.3.2 eq telnet   deny tcp 192.168.2.0 0.0.0.255 host 192.168.3.2 eq telnet   permit icmp host 192.168.1.3 host 192.168.3.2 echo   permit icmp host 192.168.1.3 host 192.168.3.2 echo-reply   deny icmp 192.168.1.0 0.0.0.255 host 192.168.3.2 echo   deny icmp host 192.168.2.2 host 192.168.3.2 echo   permit ip any any  int f0/1 ip access-group abc out </pre>	<pre> int f0/0 ip ospf 1 area 0 </pre>
--	--

**PC1 (192.168.1.2) is not able to ping 192.168.3.2 After ACL apply but he can telnet.**



The screenshot shows a Cisco Packet Tracer window with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the results of a ping command to 192.168.3.2. The first ping is successful, showing 0% loss. The second ping is failed, showing 100% loss.

```
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.3.2: bytes=32 time<1ms TTL=254
Reply from 192.168.3.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

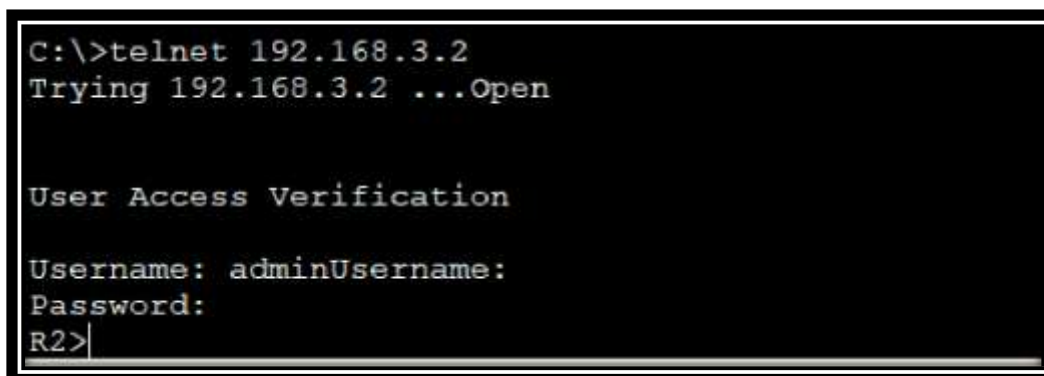
C:\>ping 192.168.3.2

Pinging 192.168.3.2 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 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



The screenshot shows a Command Prompt window with the following text:

```
C:\>telnet 192.168.3.2
Trying 192.168.3.2 ...Open

User Access Verification

Username: adminUsername:
Password:
R2>
```

Thanks & regards

Palyam Ajay