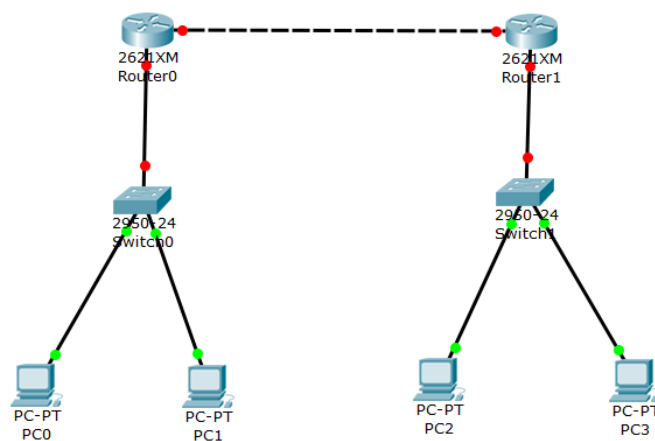


Network Analysis Project

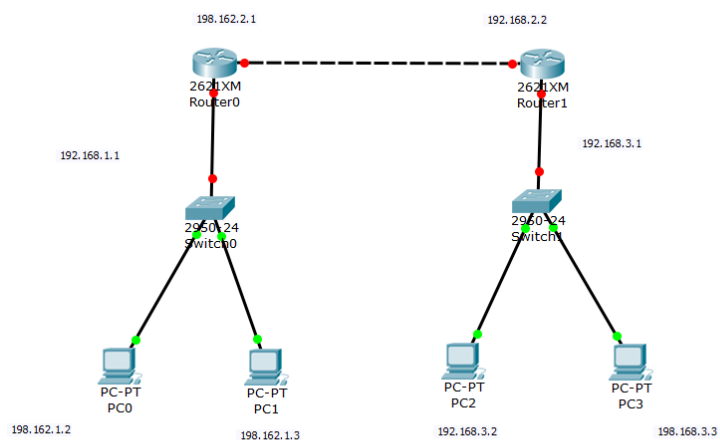
by Saurav Panigrahi

TOPIC – Controlling Traffic Using Access Control List

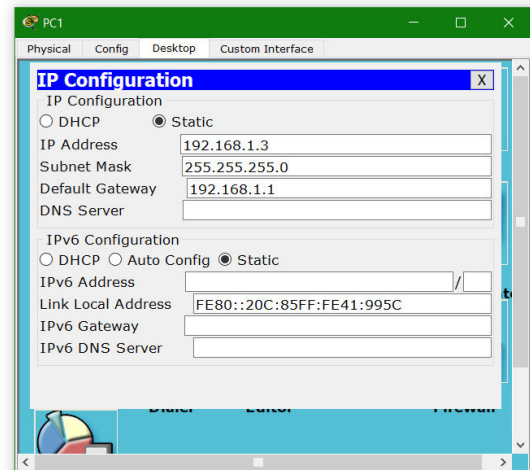
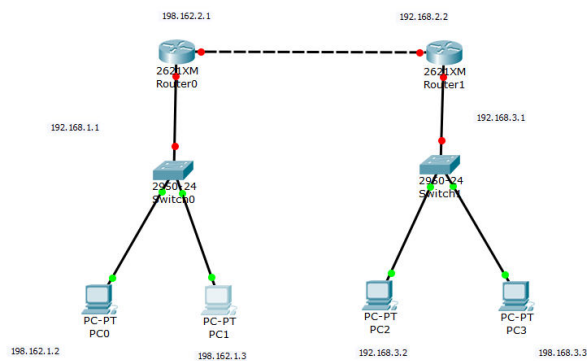
1. We setup the generic routers.
2. Next step is to setup the PCs and Switches.



3. Deciding the ip addresses of PCs and router.
4. The fa0/0 should have same ip network address
5. The fa0/1 should have different ip addresses.



6. Assigning ip address to PCs



7. Configuring CLI Router0

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut

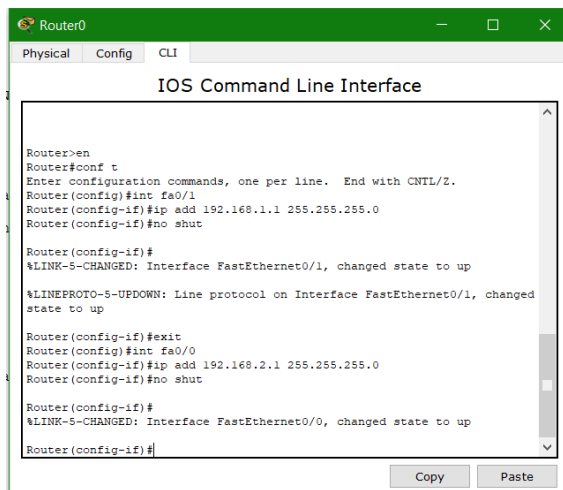
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shut

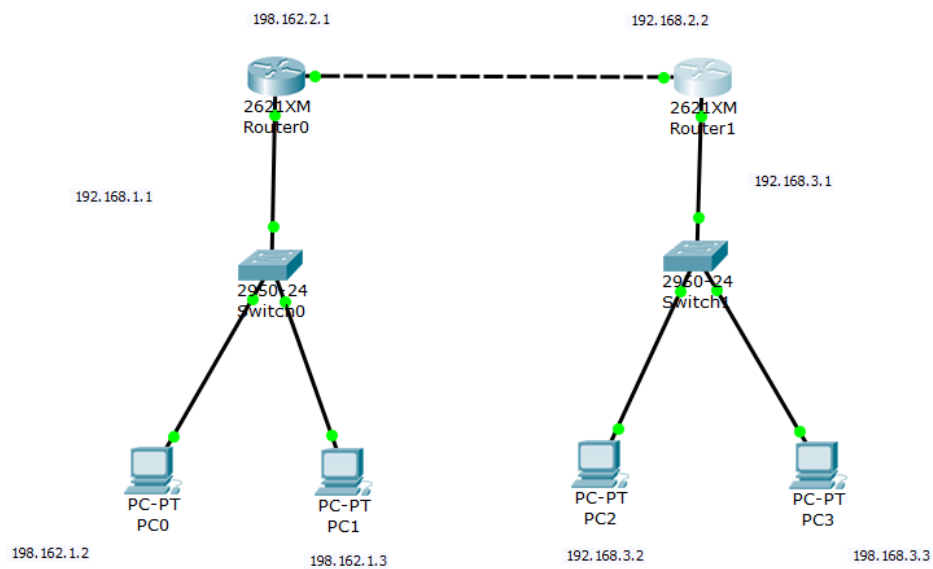
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#
```

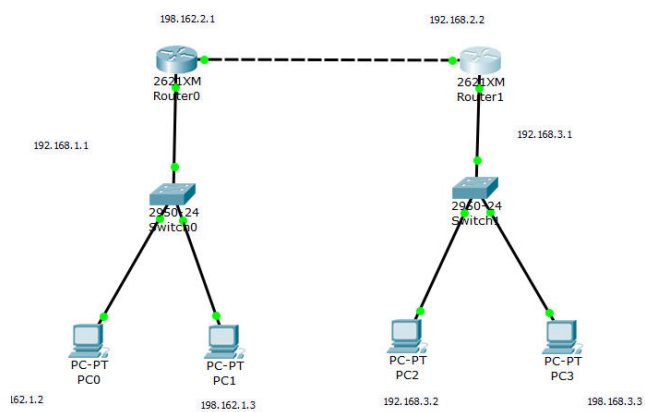


8. Repeat the CLI steps with Router1 but we should be careful about the ip address.

9. Connection is established.



10. Setting up the routing info



```
Router1
Physical Config CLI
IOS Command Line Interface

Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.2.2 255.255.255.0
Router(config-if)#no shut

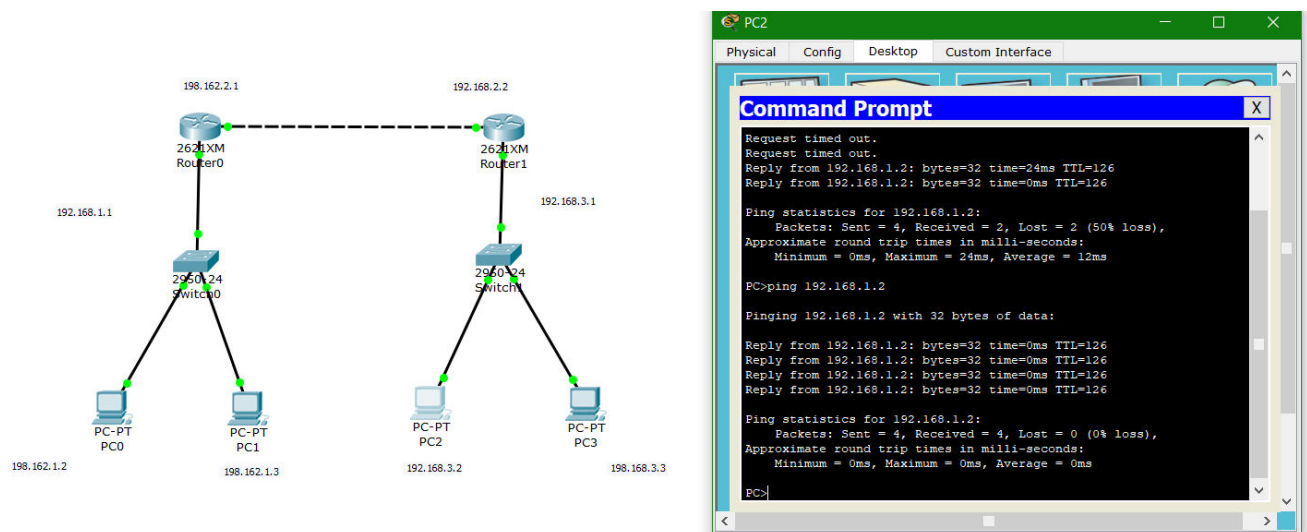
Router(config-if)#
%LINK-S-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

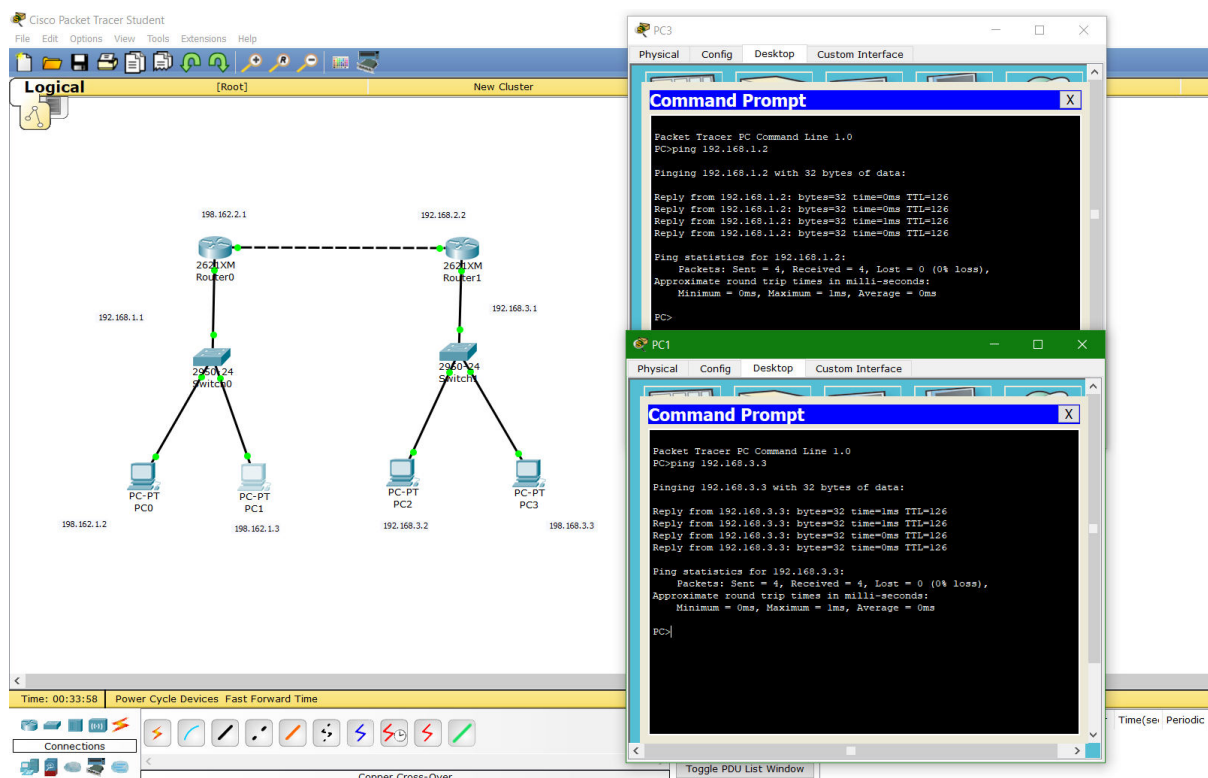
Router(config-if)#exit
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#exit
Router(config)#int fa 0/0
Router(config-if)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
Router(config)#
```

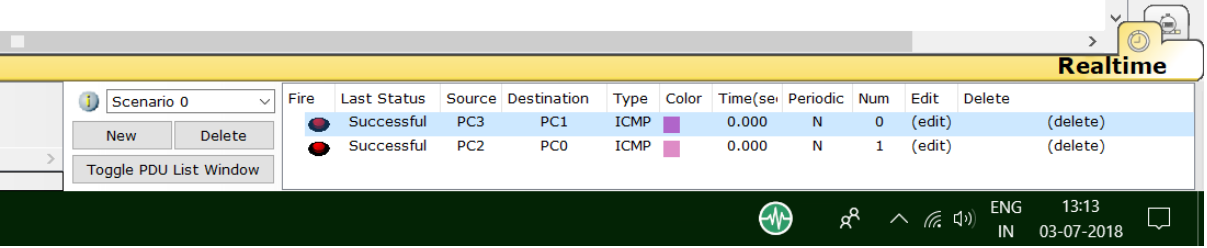
11. Now we have to check our connection if messages are being sent to other systems or not.



12. Similarly for other PCs.



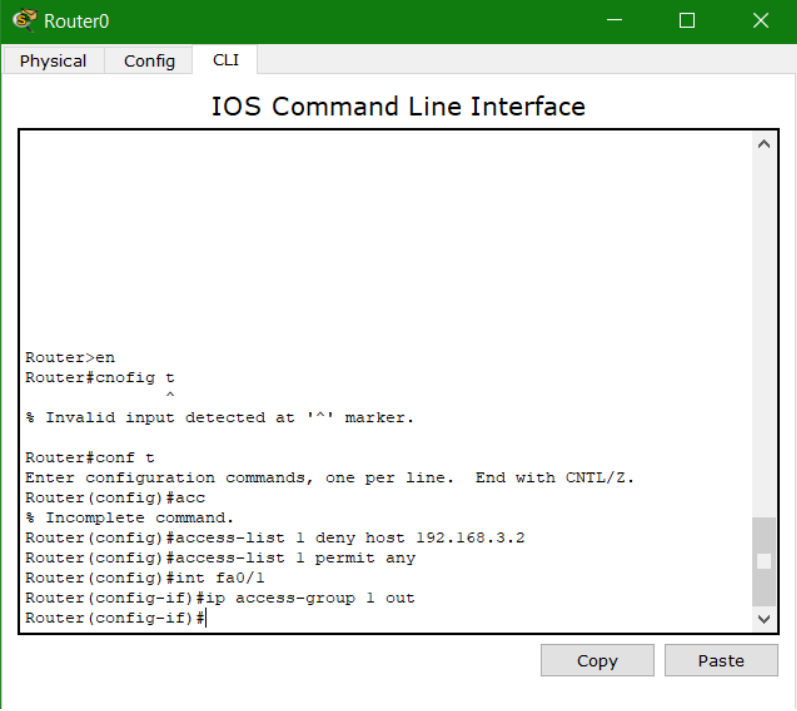
13. Checking the connections with message packets



The screenshot shows a 'Realtime' packet capture window. It has a table with columns: Fire, Last Status, Source, Destination, Type, Color, Time(se), Periodic, Num, Edit, and Delete. There are two rows of data, both with a status of 'Successful' and Type of 'ICMP'.

Fire	Last Status	Source	Destination	Type	Color	Time(se)	Periodic	Num	Edit	Delete
	Successful	PC3	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC0	ICMP		0.000	N	1	(edit)	(delete)

14. Now we have to apply ACL on our network

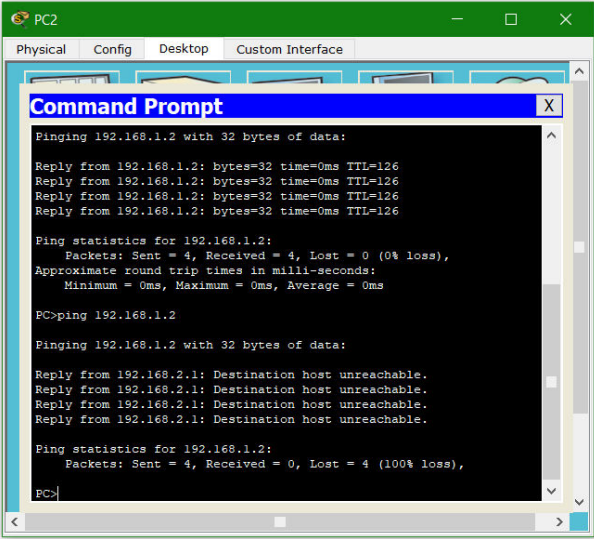


The screenshot shows the 'Router0' CLI window with the 'CLI' tab selected. The title is 'IOS Command Line Interface'. The command history shows the user entering 'en' to enter enable mode, then 'conf t' to enter configuration mode. They then configure an access list 1 to deny traffic from 192.168.3.2 and permit any other traffic. Finally, they apply this access list to the output of interface fa0/1.

```
Router>en
Router#conf t
^
% Invalid input detected at '^' marker.

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#acc
% Incomplete command.
Router(config)#access-list 1 deny host 192.168.3.2
Router(config)#access-list 1 permit any
Router(config)#int fa0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

15. We can see the result



The screenshot shows the 'PC2' window with the 'Command Prompt' tab selected. It displays the results of two ping commands. The first ping is to 192.168.1.2 and is successful. The second ping is to 192.168.2.1 and fails with 'Destination host unreachable'.

```
PC2
Physical Config Desktop Custom Interface

Command Prompt

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.2

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

16. The destination host is not reachable since we have used ACL to restrict it.(PC2)

```
PC>ping 192.168.1.2

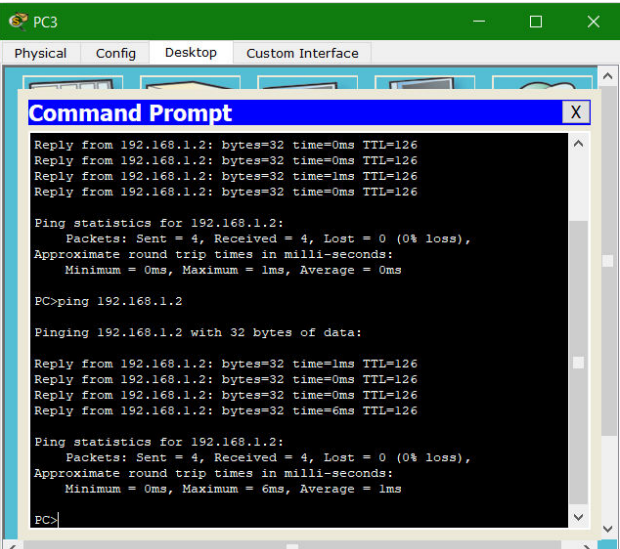
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

17. The host 192.168.3.2 has no access to other networks that is ip address of PC2.

18. But PC3 with ip address 192.168.3.3 has still access to send messages as it is not in access list.



```
PC3
Physical Config Desktop Custom Interface
Command Prompt
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

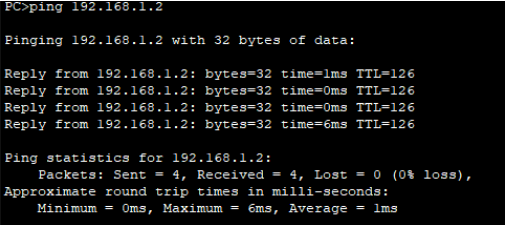
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

PC>
```



```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=0ms TTL=126
Reply from 192.168.1.2: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

So basically this is the way ACL works which permits and denies the communication between the systems .