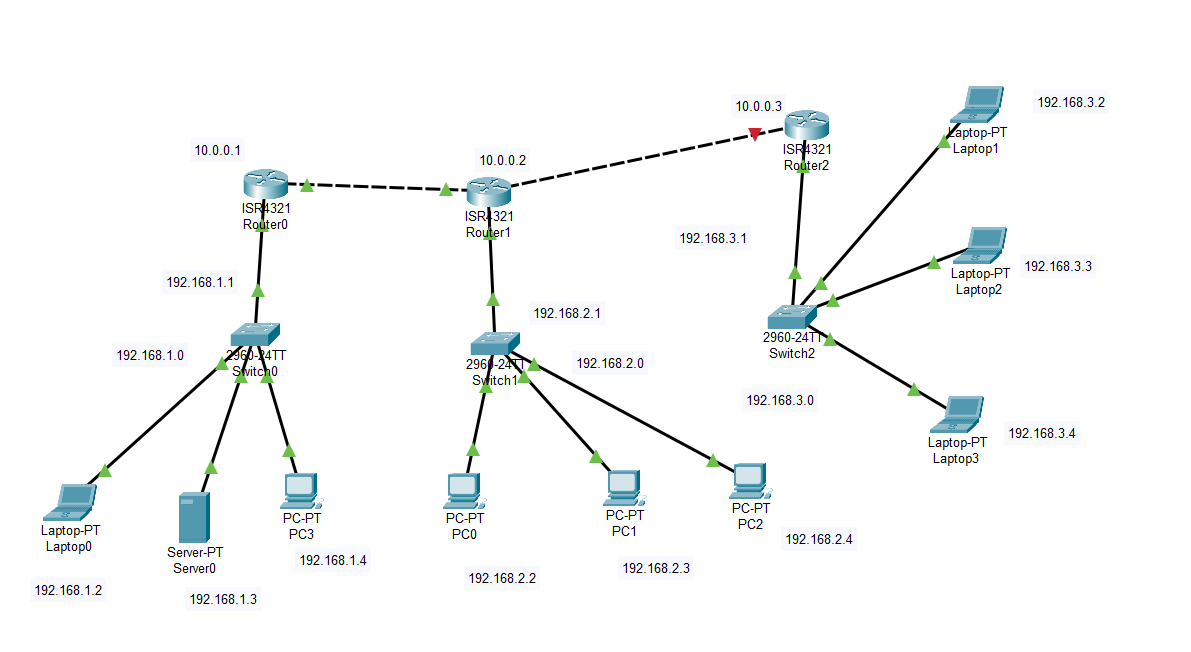
**Aryaman Mishra**

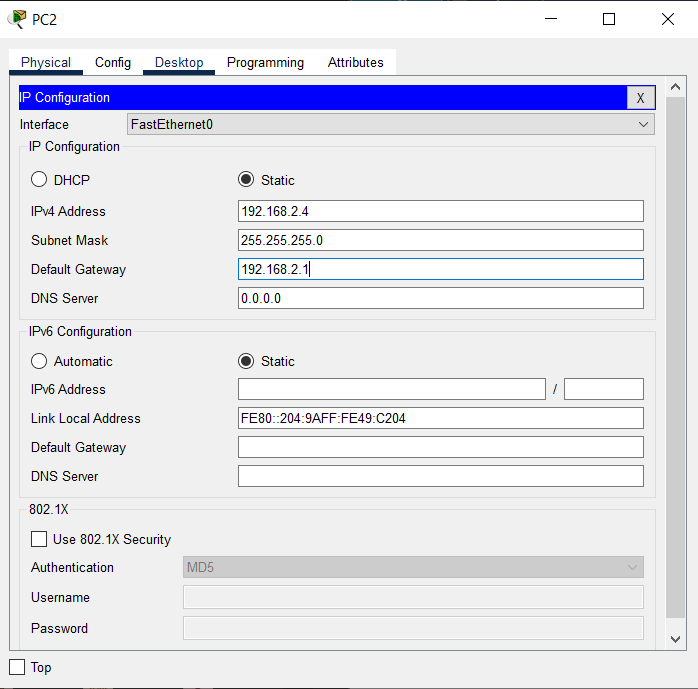
**19BCE1027**

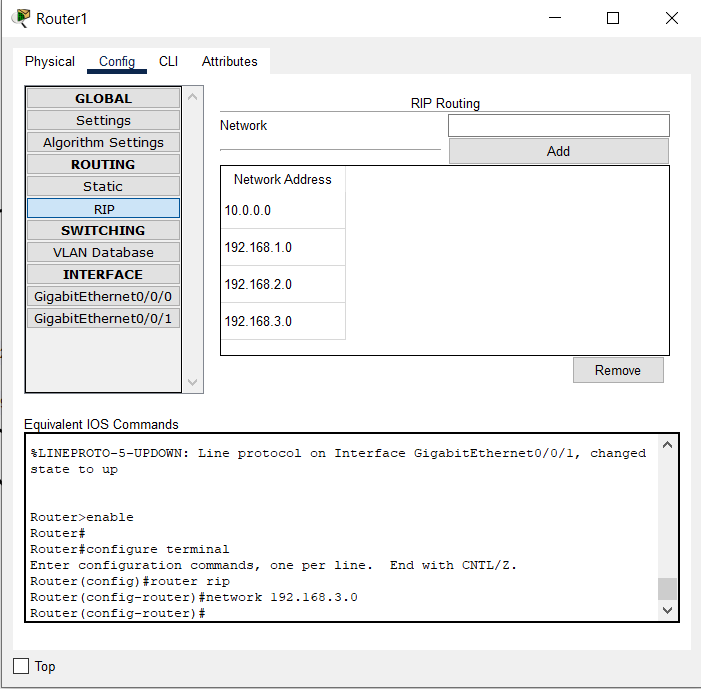
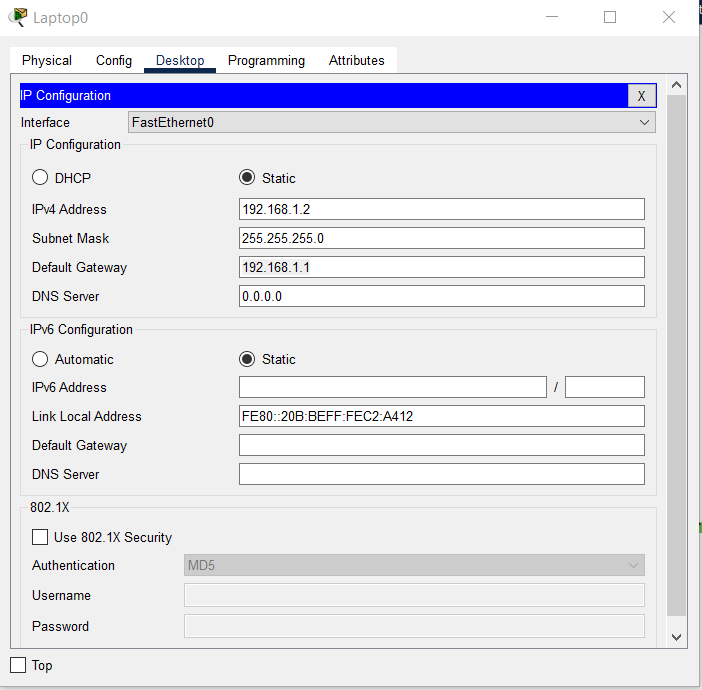
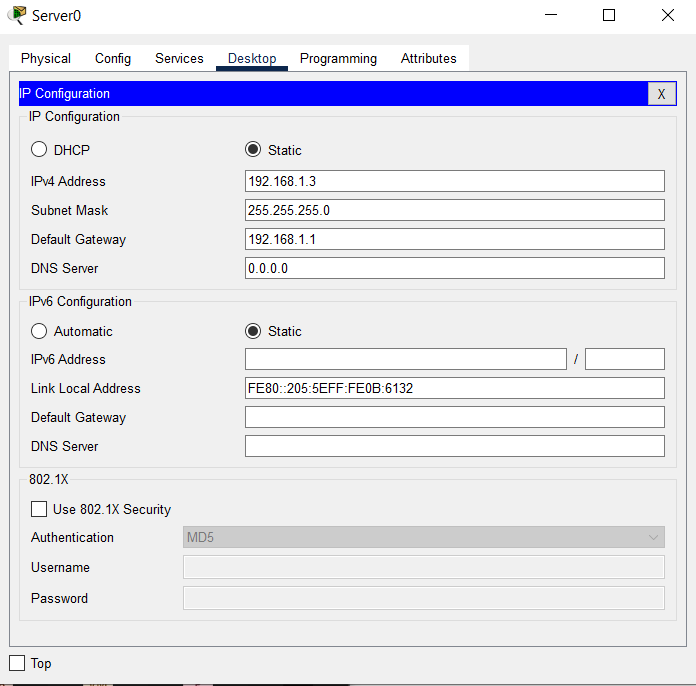
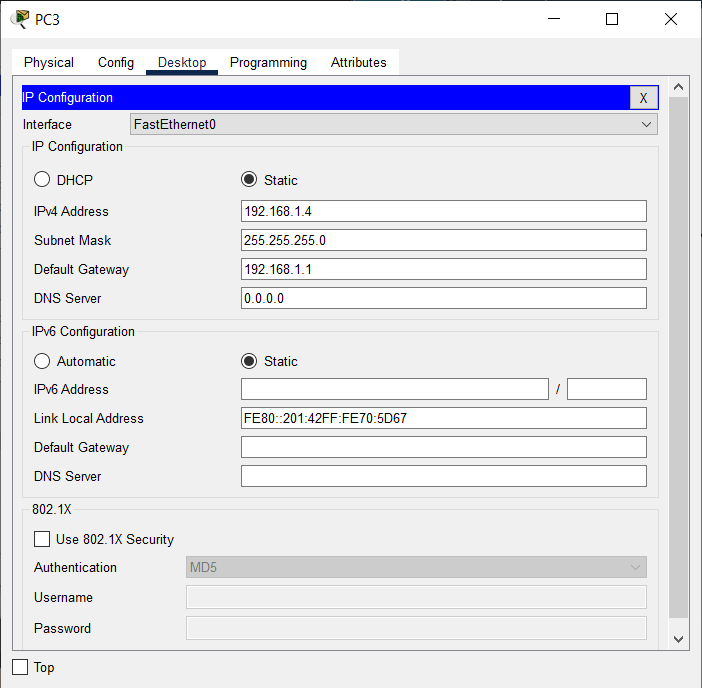
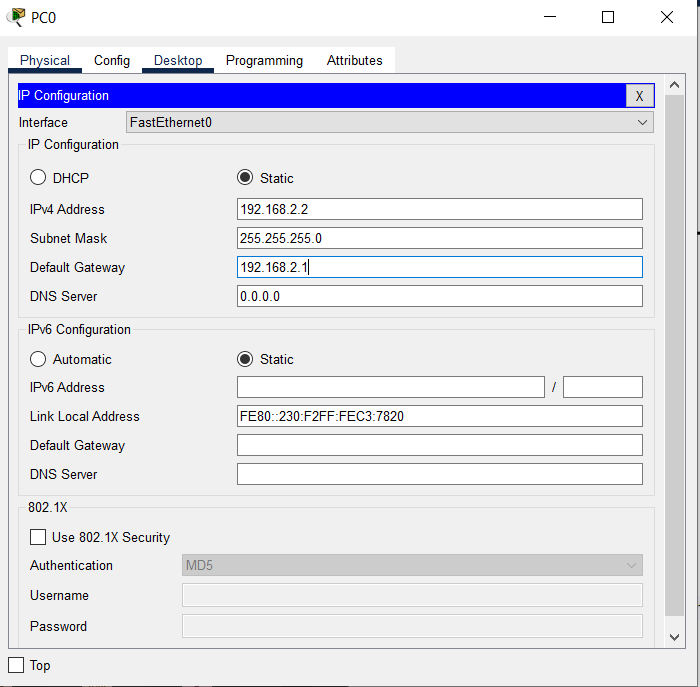
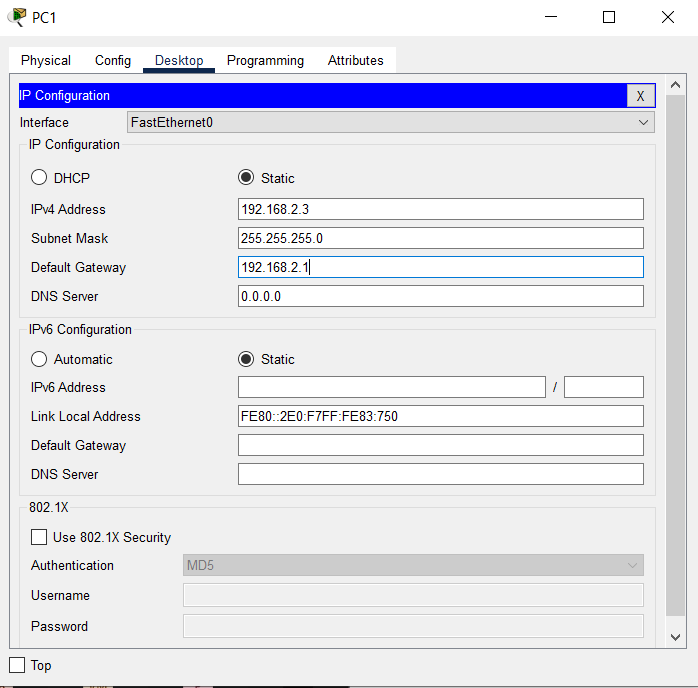
**EXPERIMENT 3:ACCESS CONTROL LISTS**

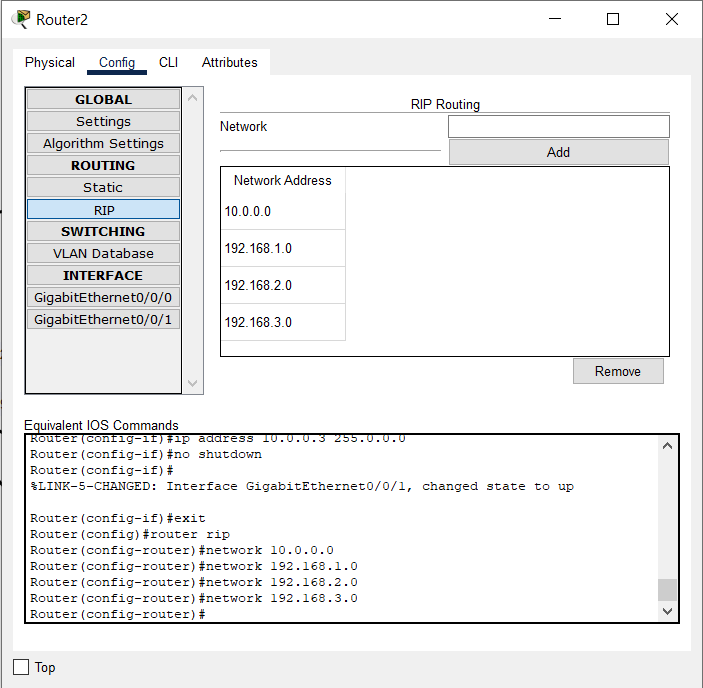
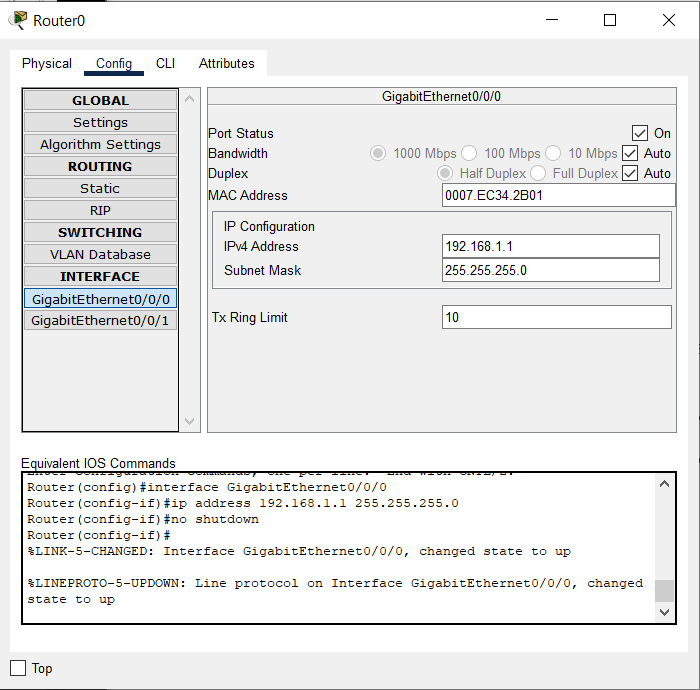
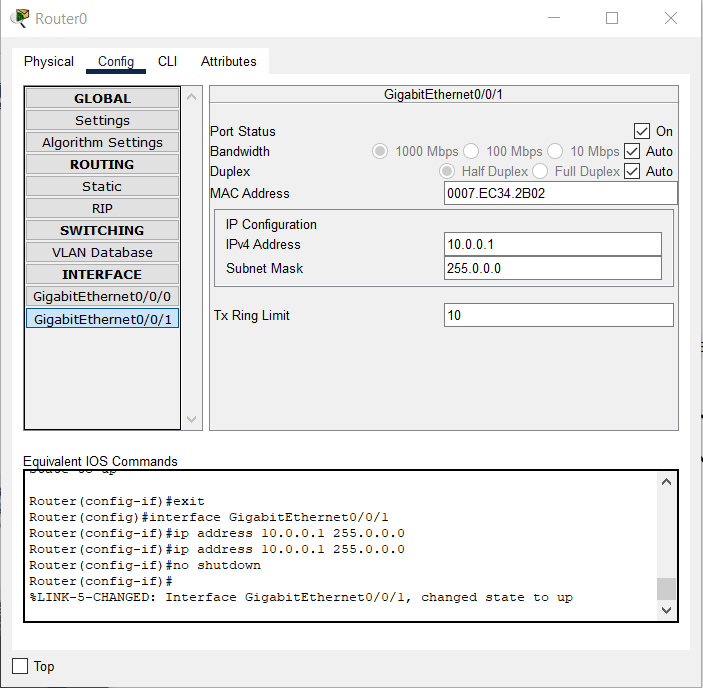
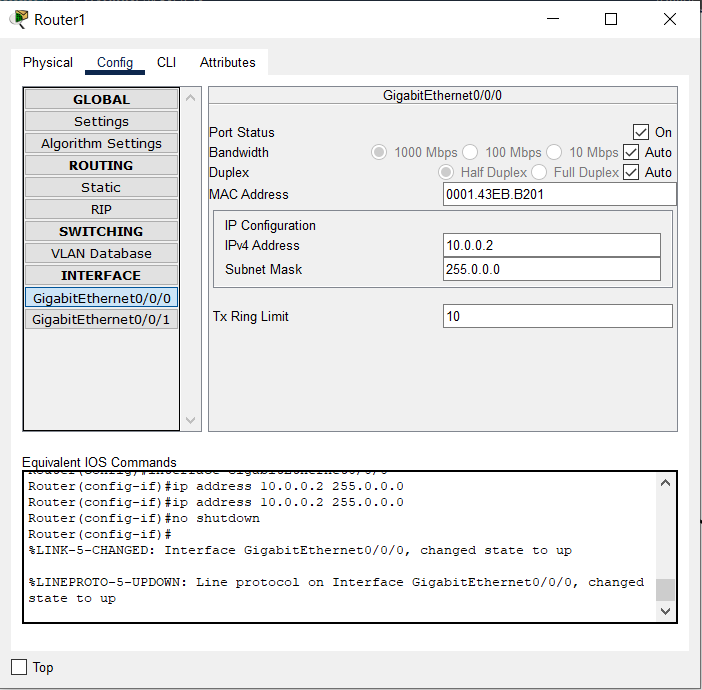
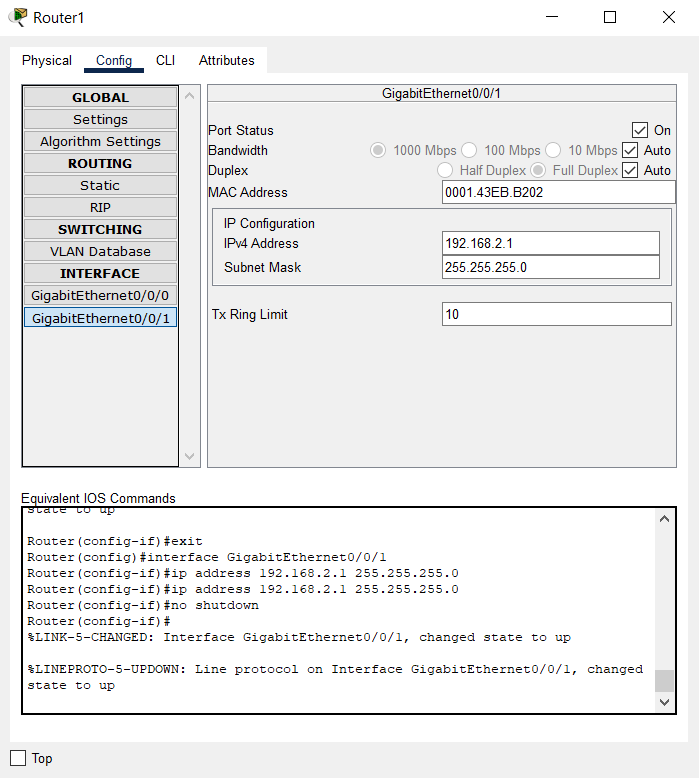
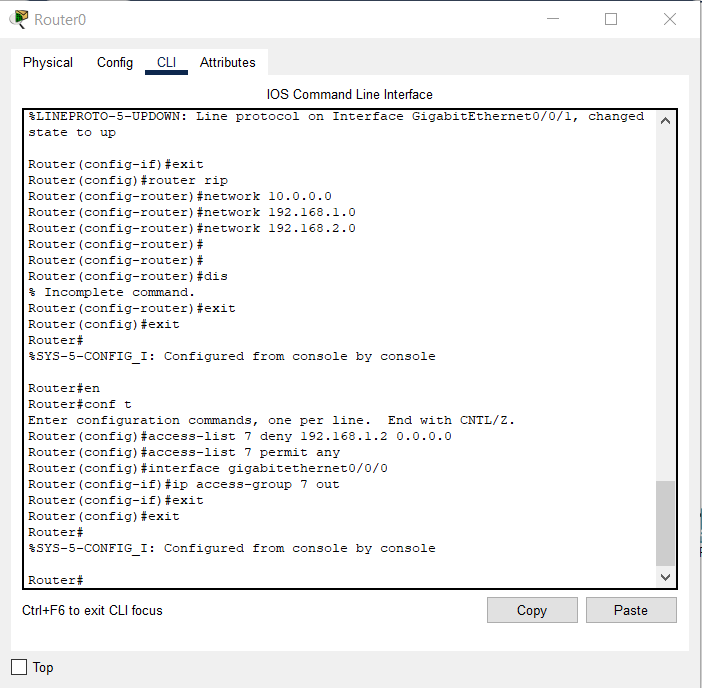
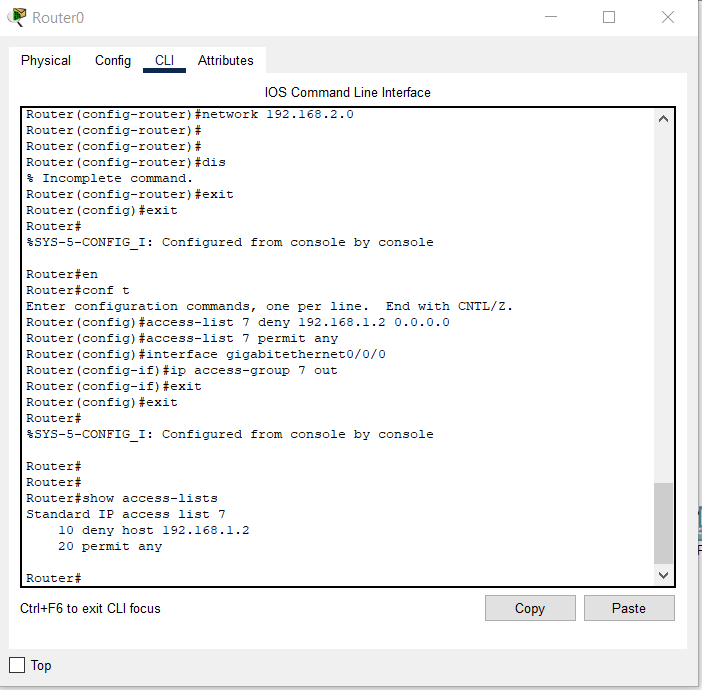
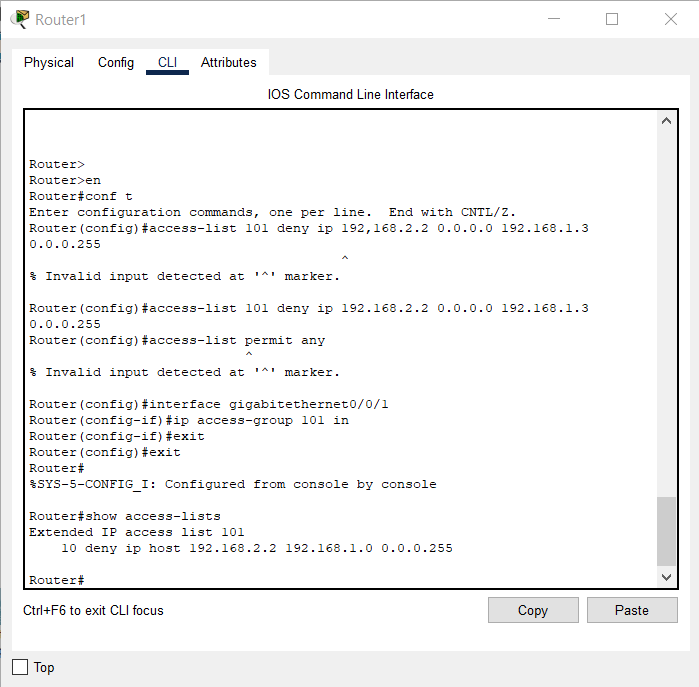
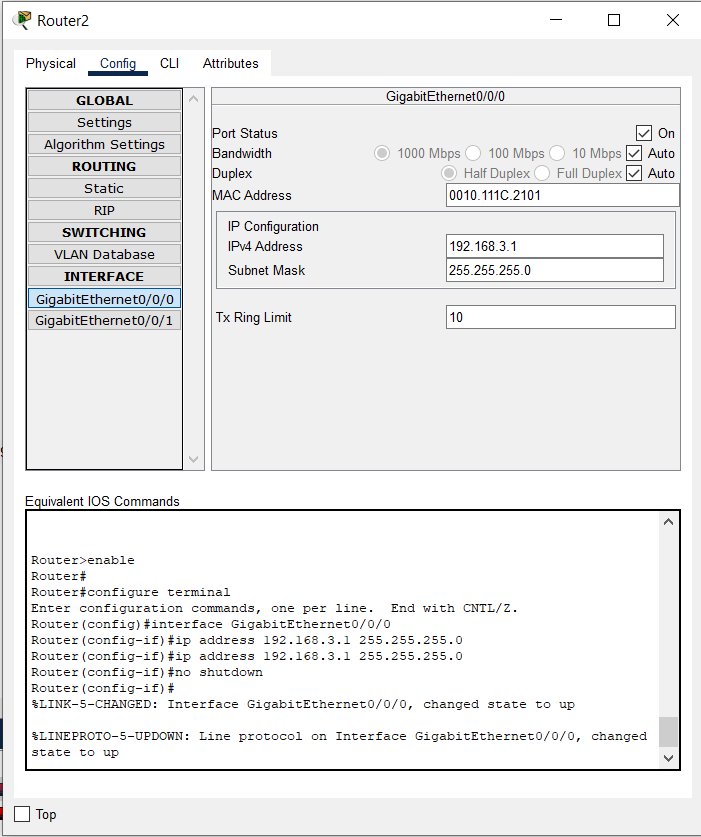
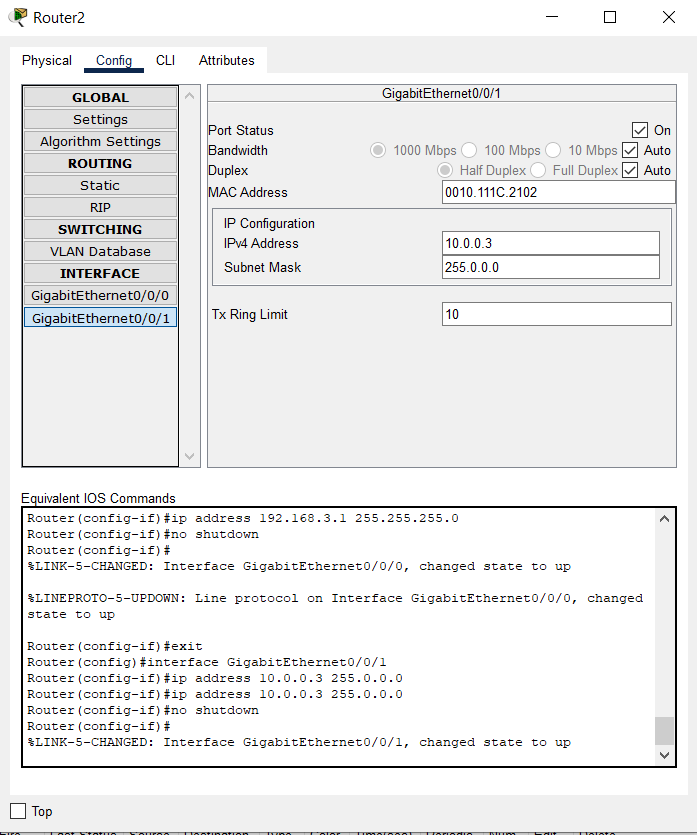
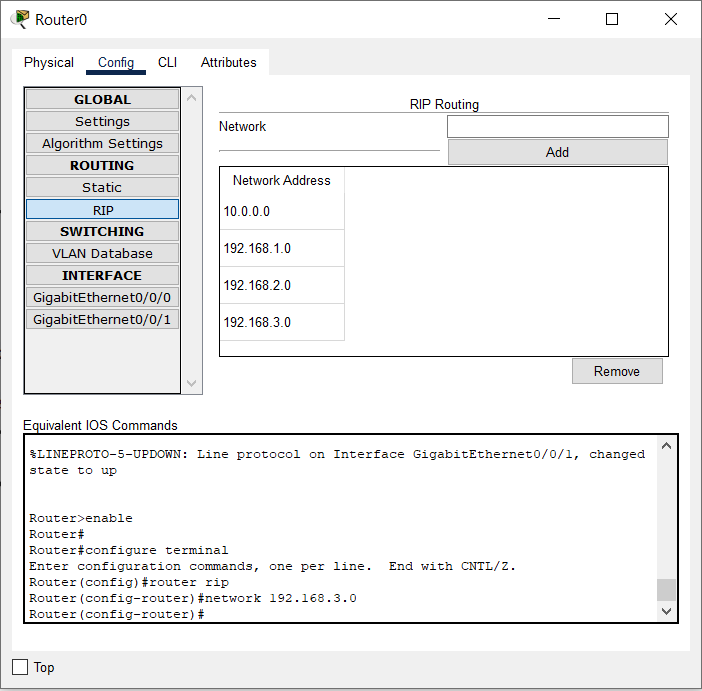
**Topology**



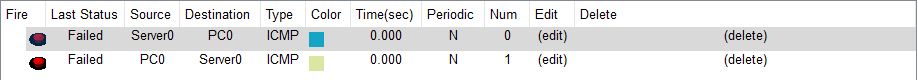
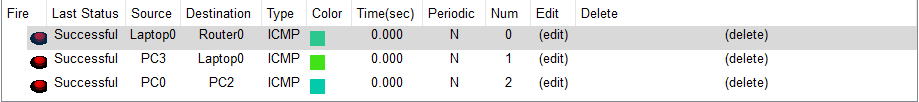
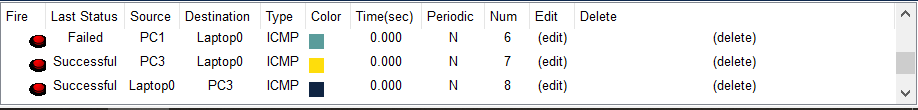
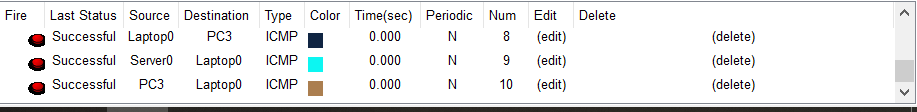
**System Configurations**







**Results:**



**Inference:**

Access Control Lists (ACL) are used to filter network traffic on Cisco routers. In order to filter network traffic, ACLs control if routed packets have to be forwarded or blocked at the ingress or egress router interface. The router checks each packet to determine whether to forward or drop the packet based on the criteria specified in the ACL applied to the interface.

IP ACL types

Two types of IP ACL can be configured in Cisco Packet Tracer 7.2 :

* Standard ACLs : This is the oldest ACL type which can be configured on Cisco routers. Traffic is filtered based on the source IP address of IP packets. The access-list number can be any number from 1 to 99. This kind of ACL has to be placed near the destination to avoid blocking legitimate trafic from the source.

access-list 1 permit 10.2.25.0 0.0.0.255  
access-list 1 deny any

* Extended ACLs : Introduced in IOS version 8.3, the extended ACLs are more complex and allow filtering of the IP traffic based on a combination of multiple criterias : source IP address, destination IP address, TCP or UDP port, protocol, .... In numbered ACLs, the access-list number can be any number from 100 to 199 or 2000 to 2699 (available in IOS versions >12.0.1). Such ACLs can also be named access lists in which the ACL number is replaced by a keyword. This kind of ACL has to be placed near the source as it allows fine grained control to ressources accessed. Placing the ACL near the destination will make the trafic travel through the network before beeing blocked, resulting in bandwidth waste.

access-list 1 permit ip 10.2.25.0 0.0.0.255 10.1.0.0 0.0.255.255  
access-list 101 permit icmp any 10.1.0.0 0.0.255.255 echo  
access-list 1 deny ip any any

A wildcard mask is a [mask](https://en.wikipedia.org/wiki/Mask_(computing)) of [bits](https://en.wikipedia.org/wiki/Bit) that indicates which parts of an [IP address](https://en.wikipedia.org/wiki/IP_address) are available for examination. In the [Cisco IOS](https://en.wikipedia.org/wiki/Cisco_IOS), they are used in several places, for example:

* To indicate the size of a network or subnet for some routing protocols, such as [OSPF](https://en.wikipedia.org/wiki/OSPF).
* To indicate what IP addresses should be permitted or denied in [access control lists](https://en.wikipedia.org/wiki/Access_control_list) (ACLs).

A wildcard mask can be thought of as an inverted [subnet mask](https://en.wikipedia.org/wiki/Subnet_mask). For example, a subnet mask of 255.255.255.0 (binary equivalent = 11111111.11111111.11111111.00000000) inverts to a wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111).

A wild card mask is a matching rule.[[2]](https://en.wikipedia.org/wiki/Wildcard_mask#cite_note-matching-2) The rule for a wildcard mask is:

* 0 means that the equivalent bit must match
* 1 means that the equivalent bit does not matter

Any wildcard bit-pattern can be masked for examination. For example, a wildcard mask of 0.0.0.254 (binary equivalent = 00000000.00000000.00000000.11111110) applied to IP address 10.10.10.2 (00001010.00001010.00001010.00000010) will match even-numbered IP addresses 10.10.10.0, 10.10.10.2, 10.10.10.4, 10.10.10.6 etc. Same mask applied to 10.10.10.1 (00001010.00001010.00001010.00000001) will match odd-numbered IP addresses 10.10.10.1, 10.10.10.3, 10.10.10.5 etc.

A network and wildcard mask combination of 1.1.1.1 0.0.0.0 would match an interface configured exactly with 1.1.1.1 only, and nothing else.

Wildcard masks are used in situations where subnet masks may not apply. For example, when two affected hosts fall in different subnets, the use of a wildcard mask will group them together.

**CONCLUSION:**

**ACCESS CONTROL LOSTS HAVE BEEN SUCCESFULLY IMPLEMENTED IN CISCO PACKET TRACER.**