

ABHISHEK KUMAR (RA2011030010089)

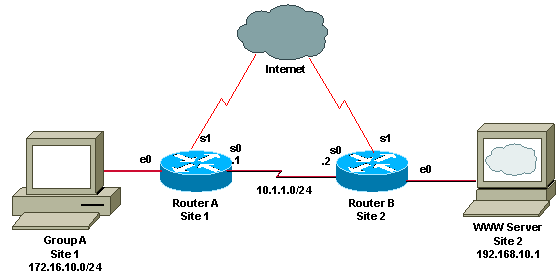
PRAKASH VERMA (RA2011030010175)

SHAIK MOHAMMED RAMIZ (RA2011030010112)

KAKARAPARTHI SAI SEETHA RAM (RA2011030010174)



**ACL (Access Control List) :-**

Access Control Lists “ACLs” are network traffic filters that can control incoming or outgoing traffic.

ACLs work on a set of rules that define how to forward or block a packet at the router’s interface.

An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination.

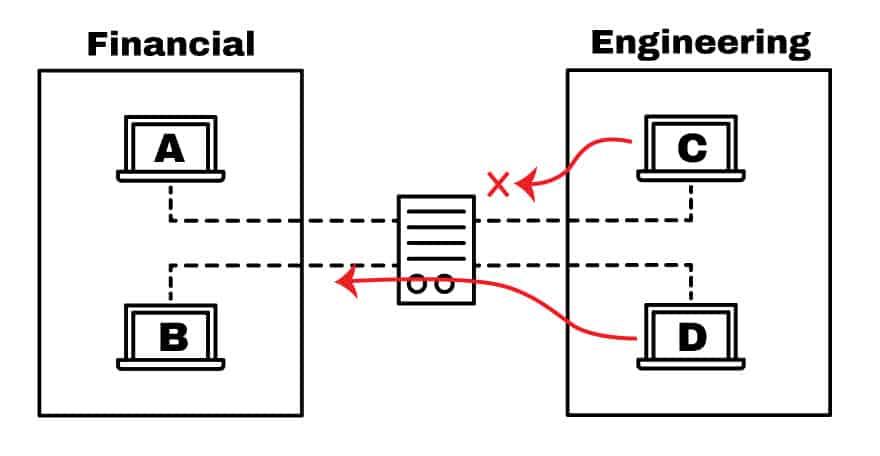
When you define an ACL on a routing device for a specific interface, all the traffic flowing through will be compared with the ACL statement which will either block it or allow it.

The criteria for defining the ACL rules could be the source, the destination, a specific protocol, or more information.

ACLs are common in routers or firewalls, but they can also configure them in any device that runs in the network, from hosts, network devices, servers, etc.

An access control list (ACL) contains rules that grant or deny access to certain digital environments. Every packet that attempts to enter or leave a router must be tested against each rule in the ACL until a match is found. If no match is found, then it will be denied.

when a packet is sent out, it must know where it's going (destination) and where it came from (source). So, it contains a source and destination IP address. The router looks at this information to determine if it matches any of the rules in its ACL.

If a router cannot find a match between the information in an ACL and the information in the packet that is attempting to enter it, the packet is denied .implicitly. 

There are two types of ACLs:

* Standard ACL
* Extended ACL

1. **Standard ACL** - Standard Access lists match only based on the source IP address of the packet.

1. **Extended ACL** - Extended Access lists can match on source and destination address, in addition to port, protocol, and many other fields.

## What Are The Components of An ACL?

The implementation for ACLs is pretty similar in most routing platforms, all of which have general guidelines for configuring them.

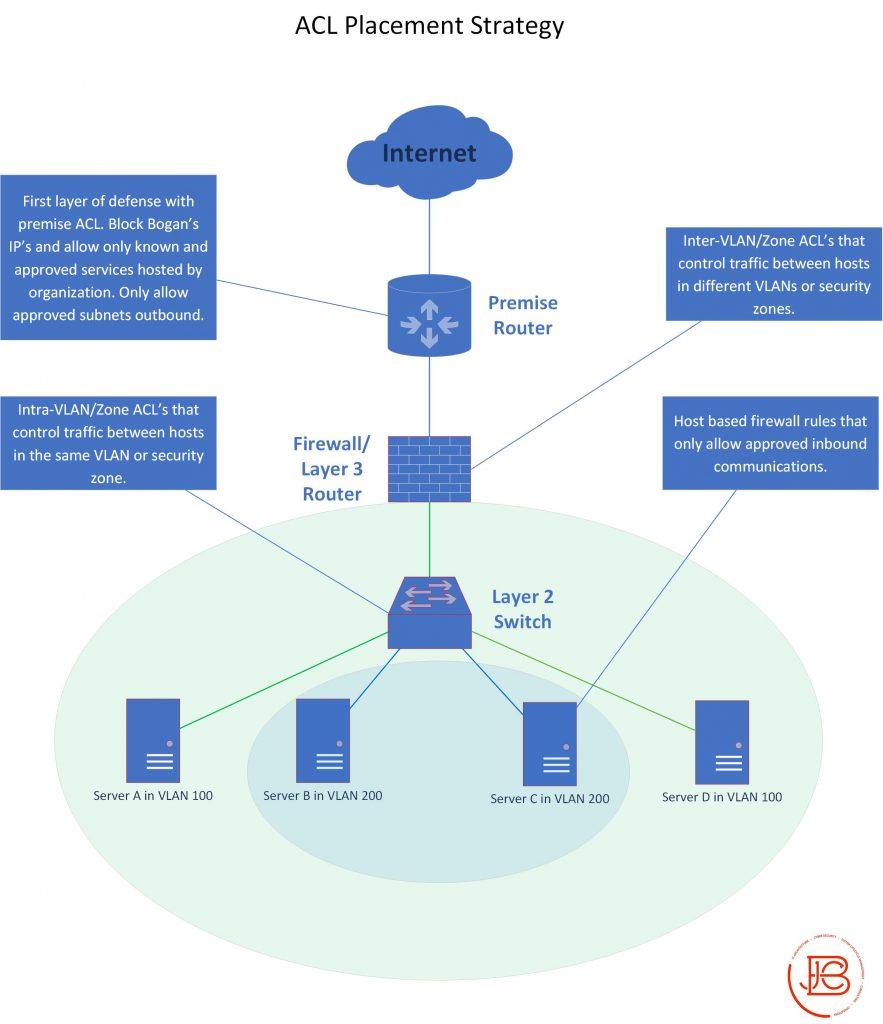
Remember that an ACL is a set of rules or entries. You can have an ACL with single or multiple entries, where each one is supposed to do something, it can be to permit everything or block nothing.

When you define an ACL entry, you’ll need necessary information.

1. **Sequence Number:**Identify an ACL entry using a number.
2. **ACL Name:**Define an ACL entry using a name. Instead of using a sequence of numbers, some routers allow a combination of letters and numbers.
3. **Remark:**  
   Some Routers allow you to add comments into an ACL, which can help you to add detailed descriptions.
4. **Statement:**Deny or permit a specific source based on address and wildcard mask. Some routing devices, such as Cisco, configure an implicit deny statement at the end of each ACL by default.
5. **Network Protocol:**Specify whether deny/permit IP, IPX, ICMP, TCP, UDP, NetBIOS, and more.
6. **Source or Destination:**Define the Source or Destination target as a Single IP, a Address Range (CIDR), or all Addresses.
7. **Log:**Some devices are capable of keeping logs when ACL matches are found.
8. **Other Criteria:**Advanced ACLs allow you to use control traffic through the Type of Service (ToS), IP precedence, and differentiated services codepoint (DSCP) priority.

**Why do we use ACL’s?**

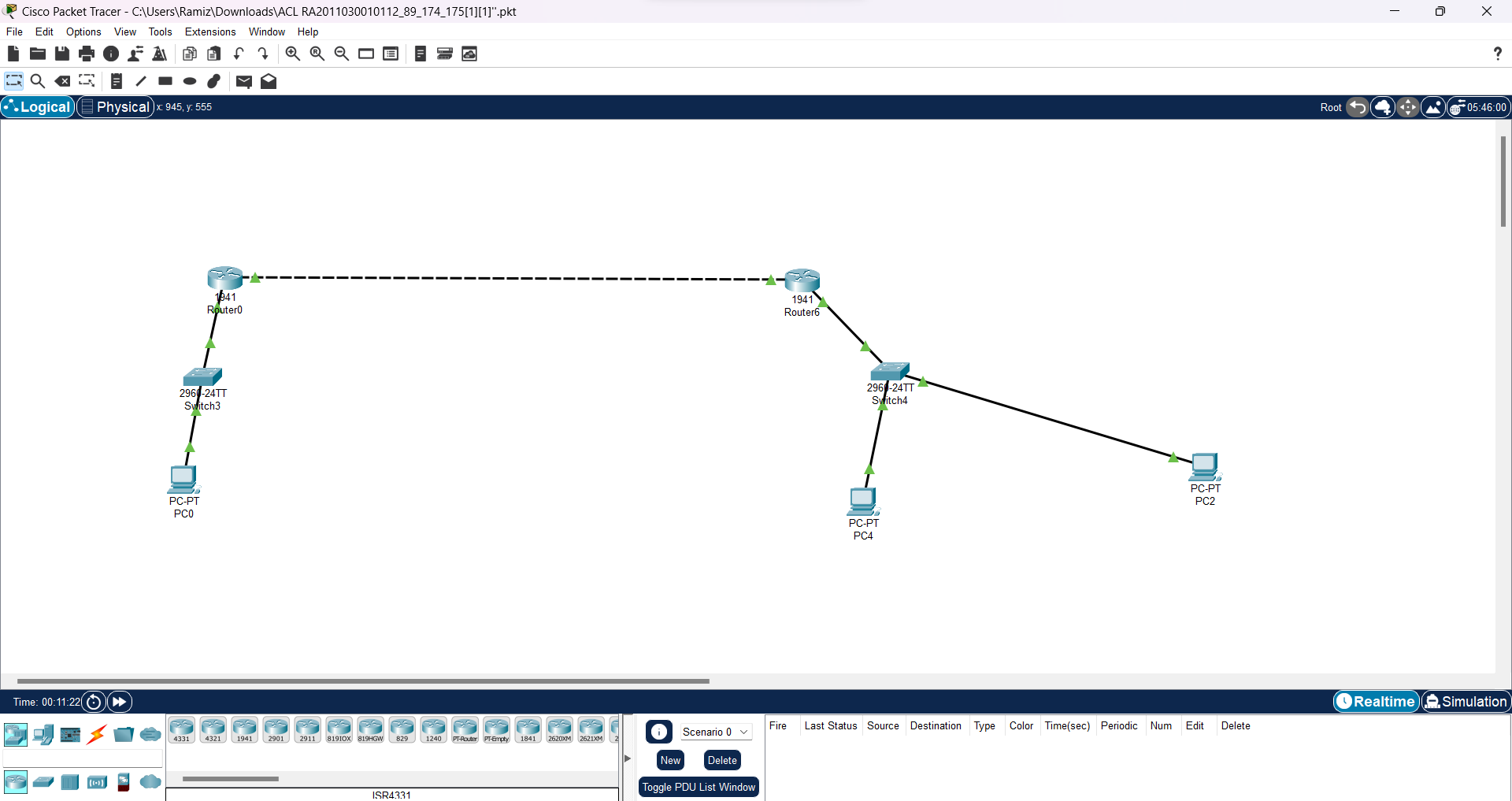
* They are used for controlling permissions to a computer system or computer network.
* They are used to filter traffic in and out of a specific device.
* Those devices can be network devices that act as network gateways or endpoint devices that users access directly.

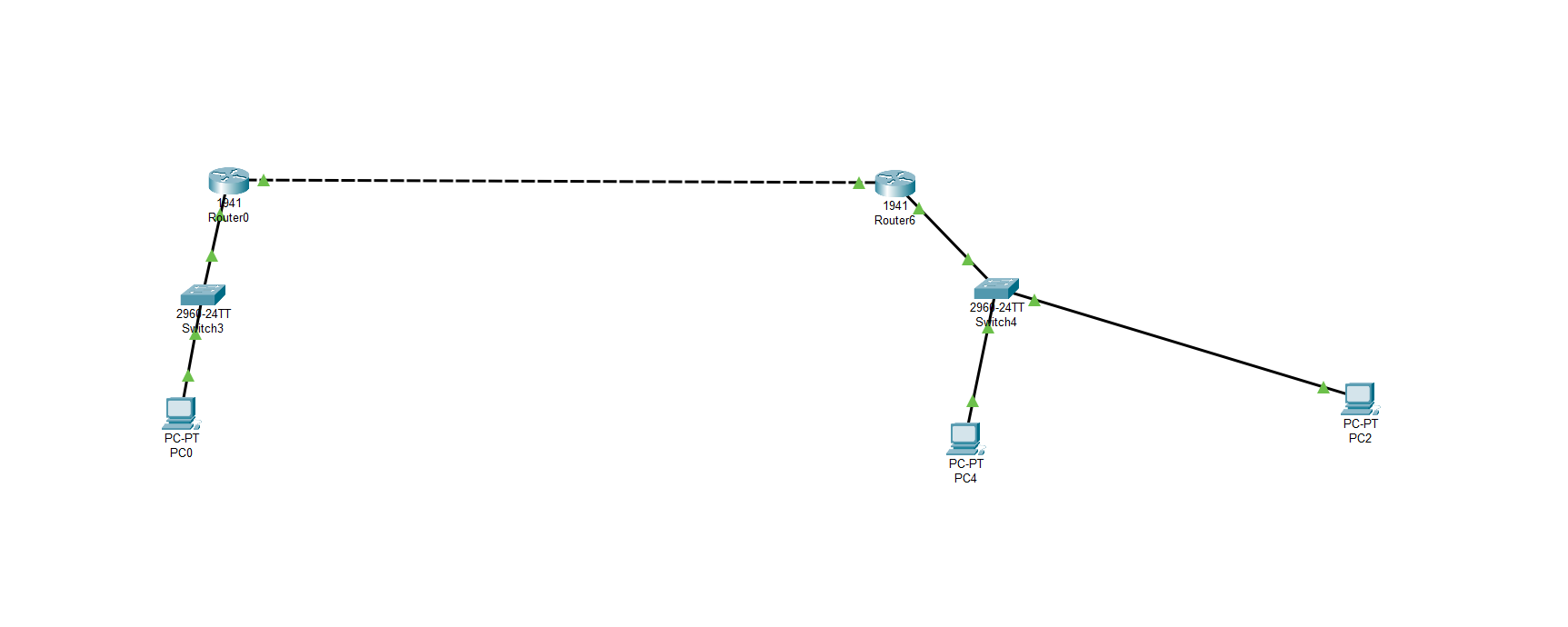


**Routing Table:**

|  |  |  |
| --- | --- | --- |
| **Device / Interface** | **IP Address** | **Connected with** |
| Router0 (Fa0/0) | 192.168.3.1 | Switch0 |
| Router0 (Fa0/1) | 192.168.1.1 | Switch0 |
| PC0 | 192.168.1.10 | Switch0 |
| PC1 | 192.168.1.20 | Switch0 |
| Router1 (Fa0/0) | 192.168.3.2 | Switch1 |
| Router1 (Fa0/1) | 192.168.2.1 | Switch1 |
| PC2 | 192.168.2.42 | Switch1 |

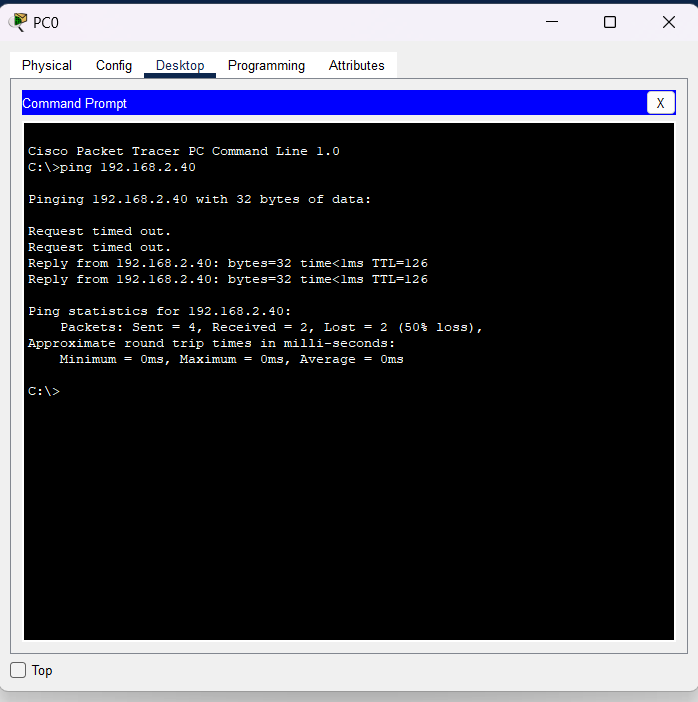
**ACL Design:**



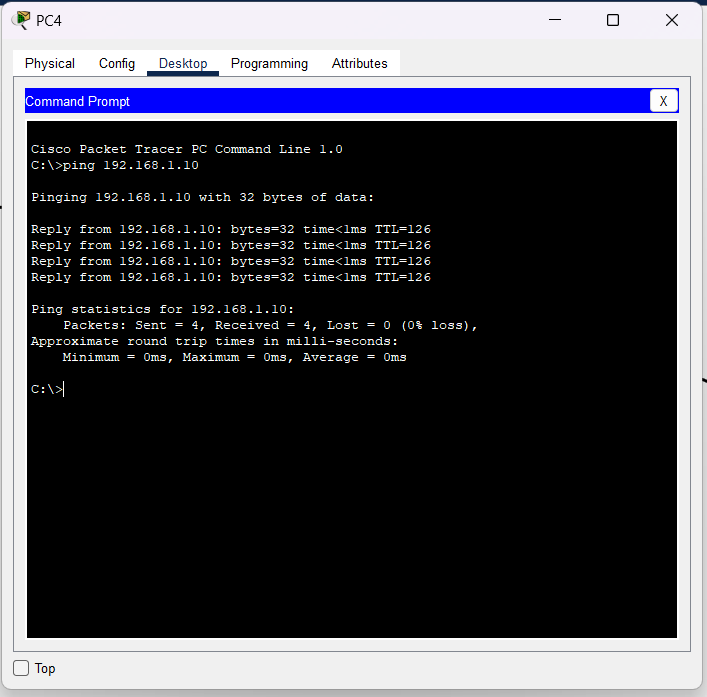
****

**Before ACL:**

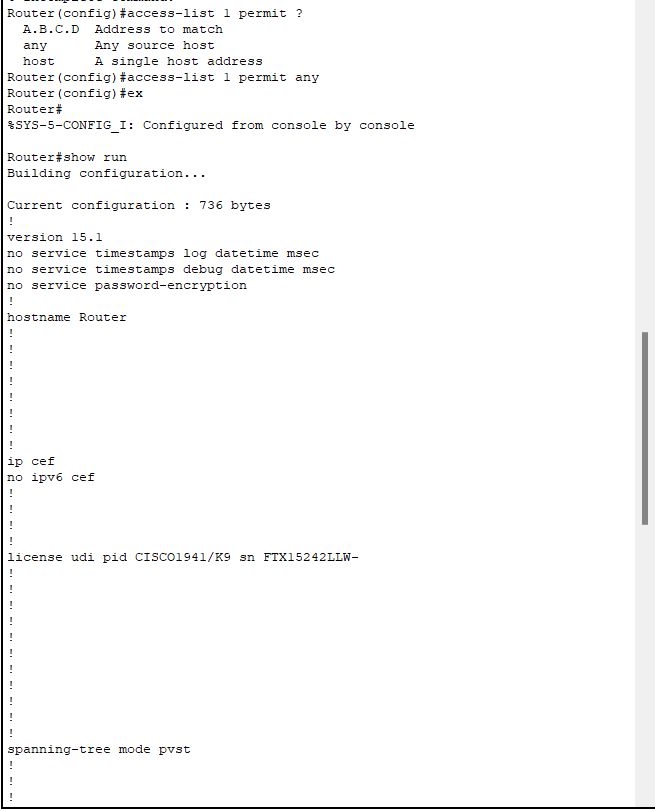
1. **From PC0**

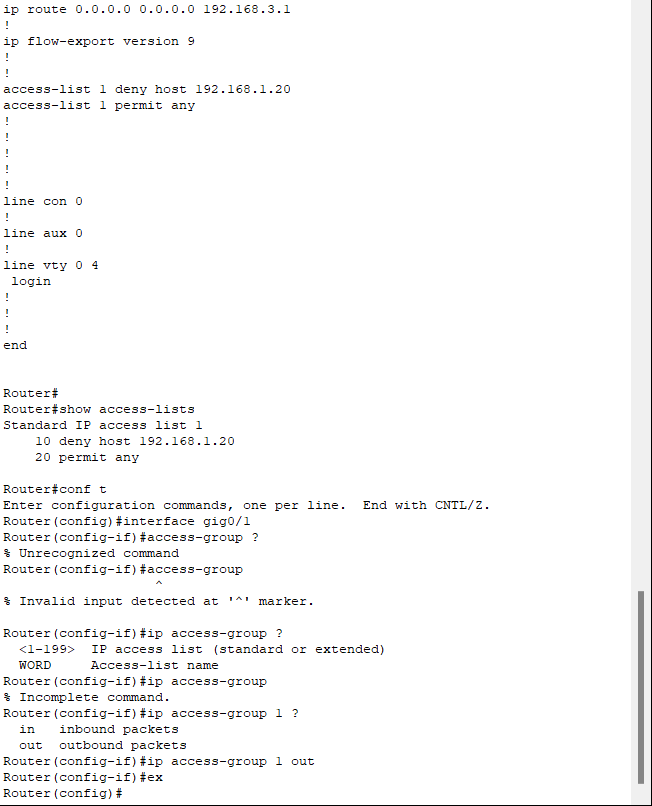
****

# From PC1

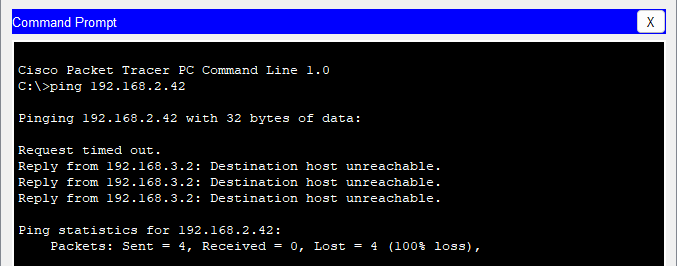


**ACL Implementation:**

****



**1. Access Denied:**

****