ACL:

Access Control List(ACL):

An ACL is a list configured on routers or firewalls to allow, deny, or control data packets and services between devices. It mainly works at the Network Layer (Layer 3) of the OSI model, and extended ACLs can also filter traffic at the Transport Layer (Layer 4).

Wildcard:

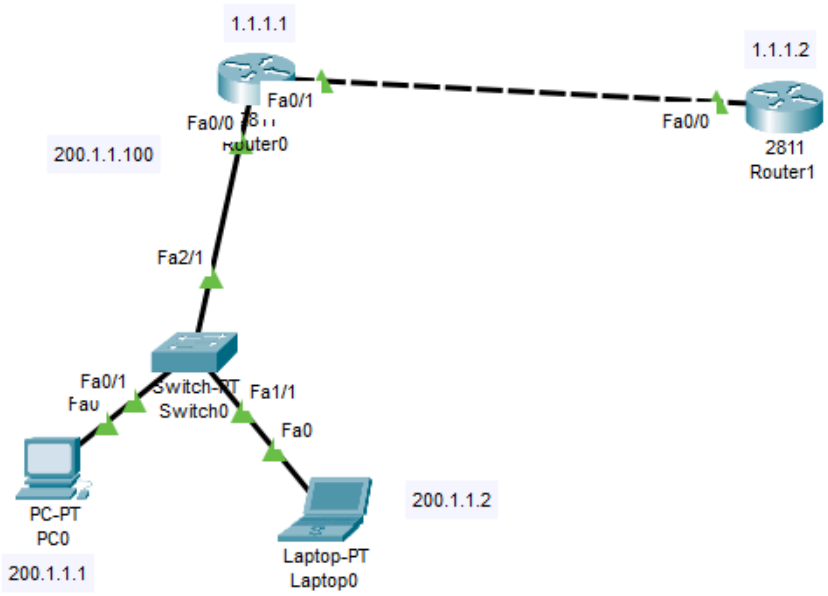
A **wildcard mask** tells the router **which bits in an IP address to check and which bits to ignore** when applying an ACL rule.

- **0** = Match exactly (must be the same).
- **1** = Ignore (don't care about this bit).

Easy Example

Suppose you have an IP: **192.168.1.0**

- Wildcard: **0.0.0.255**
  - Means: First three octets (192.168.1) must match exactly.
  - Last octet can be **anything (0–255)**.
  - This covers the whole subnet **192.168.1.0/24**.
- Wildcard: **0.0.0.0**
  - Means: Match the IP **exactly** (only one host).



Standard ACL:

It filters traffic based on IP address. It blocks every service from that particular IP. Its number range from (1-99).

access-list 5 deny 200.1.1.2 0.0.0.0

access-list 5 permit sny

int fast eth0/0

ip access group 5 in

exit

Extended ACL:

We can deny the specific source or service according to our needs. It filters traffic based on IP, port, and destination IP. It ranges from 100-199.

Router 2:

access-list 100(for extended access list)

access-list 100 deny ?

access-list 100 deny tcp ?

access-list 100 deny tcp 200.1.1.2 (laptop)

access-list 100 deny tcp 200.1.1.2 0.0.0.0 any (any destination)

(any will bloack all tcp traffic)

access-list 100 deny tcp 200.1.1.2 0.0.0.0 any eg 23(block only 23 port service)

access-list 108 permit ip any any(from any source to any destination)

int fast eth 0/0

ip access-group 108 in

exit

Command:

access-list 108 deny tcp 200.1.1.2 0.0.0.0 any eq 23

access-list 108 permit ip any any

int eth0/0

ip access-group 108 in

exit

How to edit ACL list?

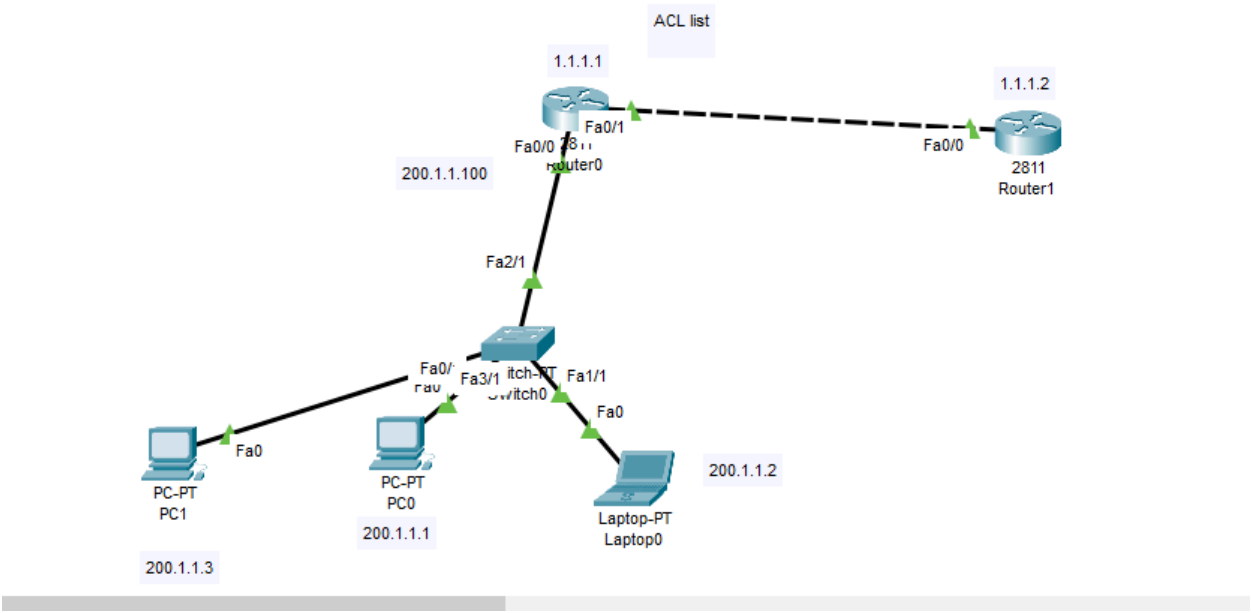
ip access-list extended 108

13 deny icmp 200.1.1.1 0.0.0.0 1.1.1.2 0.0.0.0 echo

exit

Activity:

I need to implement an extended access list.



Seq 10 block ping from R1 to R2
Seq 20 block telnet from pc2 to R2
Seq 30 perimit all
Seq 13 deny ping from pc1 to R2

for this, we need to do configuration of Access list in R2.

enable

config t

access-list 108 icmp 1.1.1.1 0.0.0.0 1.1.1.2 0.0.0.0 echo

access-list 108 tcp 200.1.1.3 0.0.0.0 1.1.1.2 0.0.0.0 eq 23

access-list 108 permit ip any any

exit

config t

ip access-list extended 108

13 deny icmp 200.1.1.1 0.0.0.0 1.1.1.2 0.0.0.0 echo

exit

int fast0/0

ip access goup 108 in

exit