ACL Configuration using RIP Protocol:

What Is ACL ?

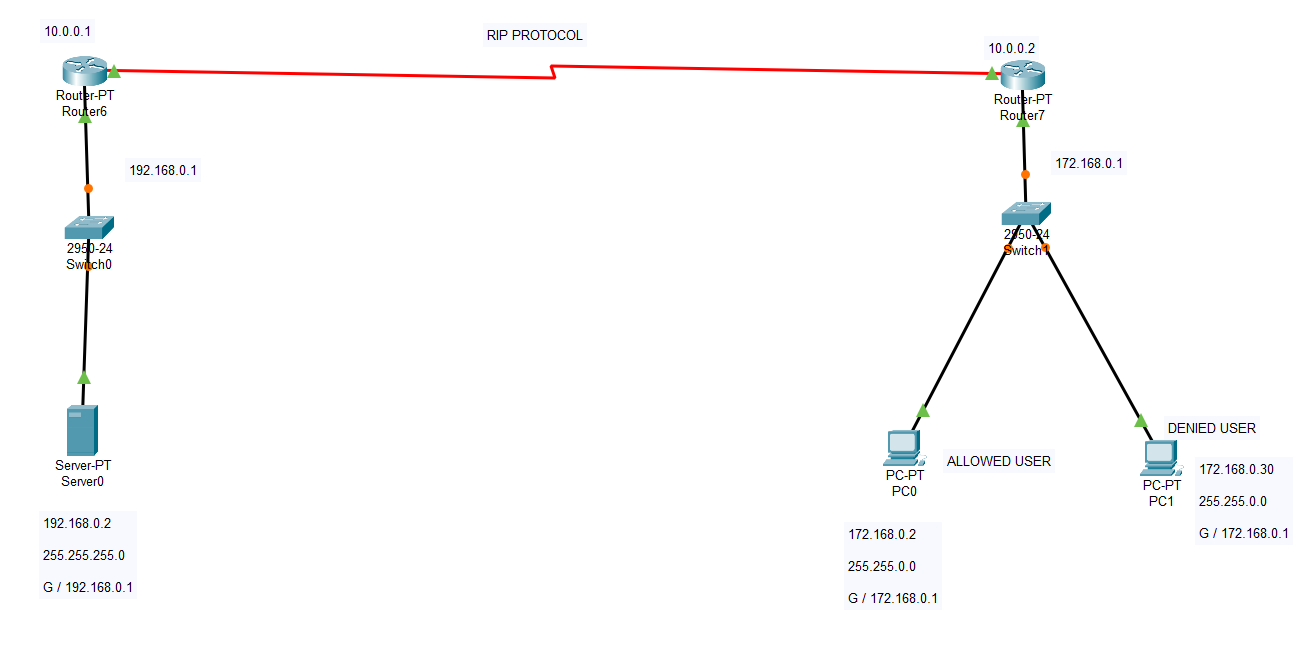
ACL (Access Control List)\*\* is a set of rules used in networking to control and filter traffic based on specified criteria, such as IP addresses, protocols, ports, etc. It is used on routers and firewalls to permit or deny data packets from traversing the network. By applying ACLs, you can:

1. Enhance security: by restricting access to certain parts of the network.

2. Control traffic: to and from specified hosts or networks.

3. Filter traffic: for specific applications, like blocking unwanted web traffic.

Here's a step-by-step note for configuring Access Control Lists (ACL) using the RIP (Routing Information Protocol):



---

1. Network Topology Setup

- Create a network topology with multiple routers connected via interfaces.

- Ensure that IP addressing is correctly assigned to all router interfaces and end devices.

2. Enable RIP Routing on Routers

- Use the following commands on each router:

```shell

Router> enable

Router# configure terminal

Router(config)# router rip

Router(config-router)# version 2 # Use RIP version 2

Router(config-router)# network [network\_address] # Add network(s) to RIP

```

- Replace `[network\_address]` with the actual network address directly connected to the router.

3. Verify RIP Configuration

- Check that RIP routes are propagating correctly:

```shell

Router# show ip route

Router# show ip protocols

```

4. Apply an Access Control List (ACL)

- ACLs can filter traffic and control data packets based on criteria such as IP addresses or protocols.

- Create a standard or extended ACL, for example:

- Standard ACL (Filters based on source IP only):

```shell

Router(config)# access-list [ACL\_NUMBER] permit/deny [source\_ip] [wildcard\_mask]

```

- Extended ACL (Filters based on source, destination, and protocol):\*\*

```shell

Router(config)# access-list [ACL\_NUMBER] permit/deny [protocol] [source\_ip] [source\_wildcard] [destination\_ip] [destination\_wildcard] [optional\_ports]

```

- Example (Standard ACL):

```shell

Router(config)# access-list 10 deny 192.168.1.0 0.0.0.255

Router(config)# access-list 10 permit any

```

5. Apply the ACL to an Interface

- Apply the ACL inbound or outbound on a specific interface:

```shell

Router(config)# interface [interface\_name]

Router(config-if)# ip access-group [ACL\_NUMBER] in/out

```

- Example:

```shell

Router(config)# interface FastEthernet0/0

Router(config-if)# ip access-group 10 in

```

6.Test ACL Functionality

- Use the `ping` and `traceroute` commands from connected devices to test if traffic is being allowed or denied as specified.

- Example:

```shell

Router# ping [destination\_ip]

Router# traceroute [destination\_ip]

```

7. View and Troubleshoot ACLs

- Verify the applied ACLs and their hit counts:

```shell

Router# show access-lists

Router# show running-config

```

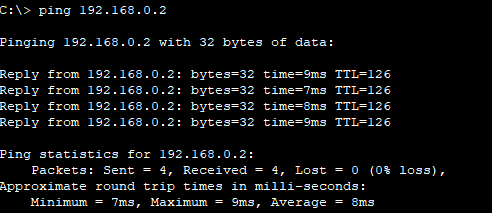
- Modify or remove ACLs as necessary:

```shell

Router(config)# no access-list [ACL\_NUMBER]

```

Output(Before ACL):



Output(After ACL):

