Access Control List (ACL)

What is an Access Control List (ACL)?

An Access Control List (ACL) is an ordered set of rules for filtering traffic. Access control lists can be used to filter incoming or outgoing packets on an interface to control traffic. Access lists also help in defining the types of traffic that should be allowed or blocked at device interfaces. For example, if you wish to permit e-mail traffic to be routed and block a specific host from entering a network, an Access Control List can be used. Access Control Lists play a major role in controlling bandwidth bottlenecks and is crucial for every organization to maintain a consistent network performance.

Access Control List (ACL) in Networking

In a network environment which consists of a large number of employees and network devices, there will be a lot of incoming and outgoing data traffic. This leads to bandwidth bottlenecks, which in turn affects the transmission of important data. In order to control this, you need to identify the network devices which consume a lot of bandwidth using a traffic monitoring tool. Once the devices are identified, you can apply the 'Access control list' (ACL) policies on the network devices to determine the priority of data during transmission.

ACL Configuration Guidelines

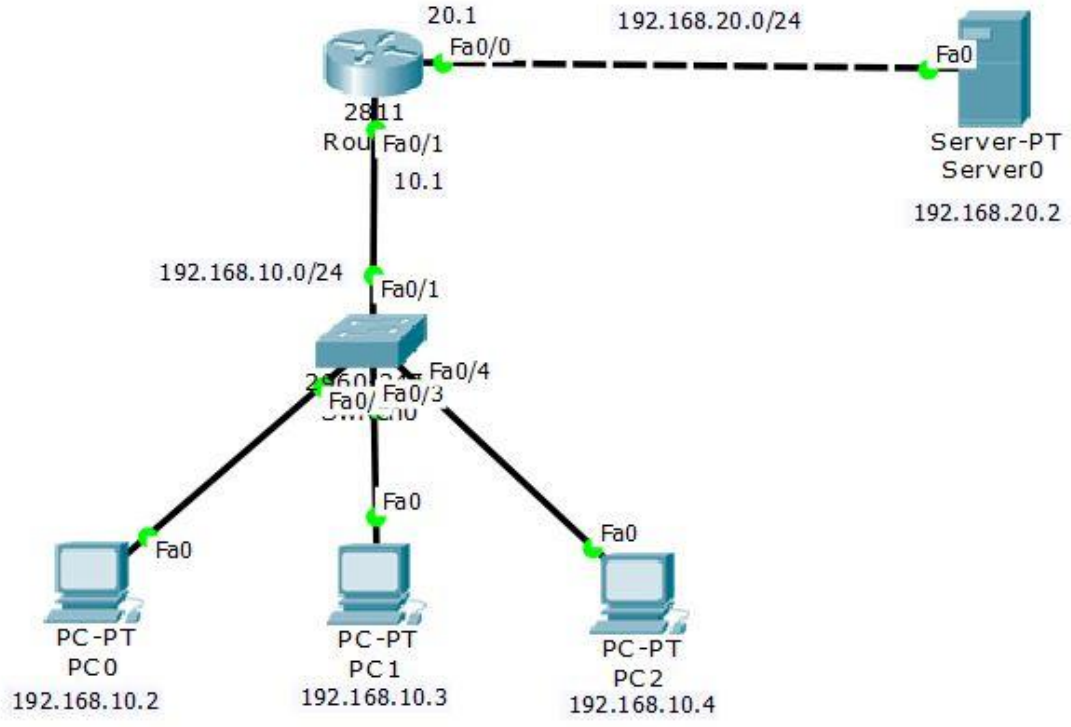
- Only one ACL per interface, per protocol, per direction is allowed.
- ACLs are created globally and then applied to interfaces.
- An ACL can filter traffic going through the router, or traffic to and from the router.

ACL Types:

- **Standard ACL**
    - Checks ACL source address
    - Permits or denies entire protocol suite
    - Range: 1–99 and 1300–1999

- **Extended ACL**
    - Checks source and destination address
    - Generally permits or denies specific protocols and applications
    - Source and destination TCP and UDP ports
    - Protocol type (IP, ICMP, UDP, TCP or protocol number)
    - Range: 100–199 and 2000–2699

Example 1



*****Configure Router & PC****

PERMIT SINGLE HOST:

Way1:

Router(config)#access-list 11 permit 192.168.10.3
Router(config)#int f0/1
Router(config-if)#ip access-group 11 in
Router(config-if)#exit

Way 2:

Router(config)#access-list 11 permit 192.168.10.3
Router(config)#int f0/0
Router(config-if)#ip access-group 11 out
Router(config-if)#exit

Show Access List:

Router#sh access-lists

Delete access-list:

Router(config)#no access-list 10

DENY SINGLE HOST:

Way 01:

```
Router(config)#access-list 10 deny  192.168.10.3
Router(config)#access-list 10 permit any
Router(config)#int f0/0
Router(config-if)#ip access-group 10 out
Router(config-if)#exit
```

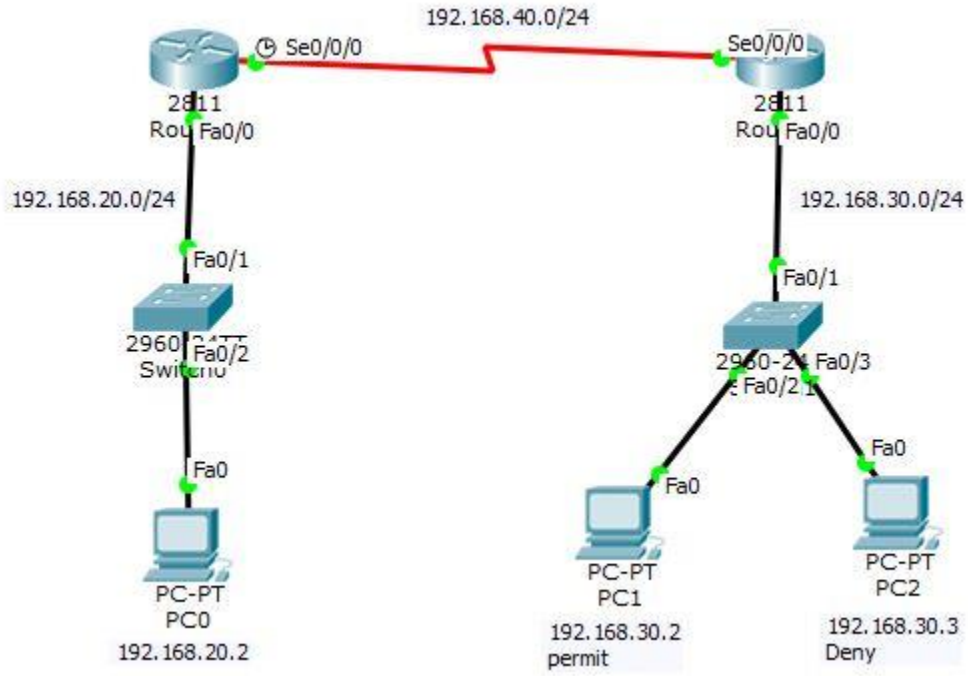
Way 02:

```
Router(config)#access-list 10 deny  192.168.10.3
Router(config)#access-list 10 permit any
Router(config)#int f0/1
Router(config-if)#ip access-group 10 in
Router(config-if)#exit
```

DENY WHOLE NETWORK:

```
Router(config)#access-list 13 deny   192.168.10.0
Router(config)#int f0/1
Router(config-if)#ip access-group 13 in
Router(config-if)#exit
```

Example 2



*****Configure Router & PC*****
*****Configure RIP*****

Way 01:
Router 0->
Router(config)#access-list 11 permit 192.168.30.2
Router(config)#int f0/0
Router(config-if)#ip access-group 11 out
Router(config-if)#ex

Router(config)#no access-list 11

Way 02:
Router(config)#access-list 11 permit 192.168.30.2
Router(config)#int s0/0/0
Router(config-if)#ip access-group 11 in
Router(config-if)#ex

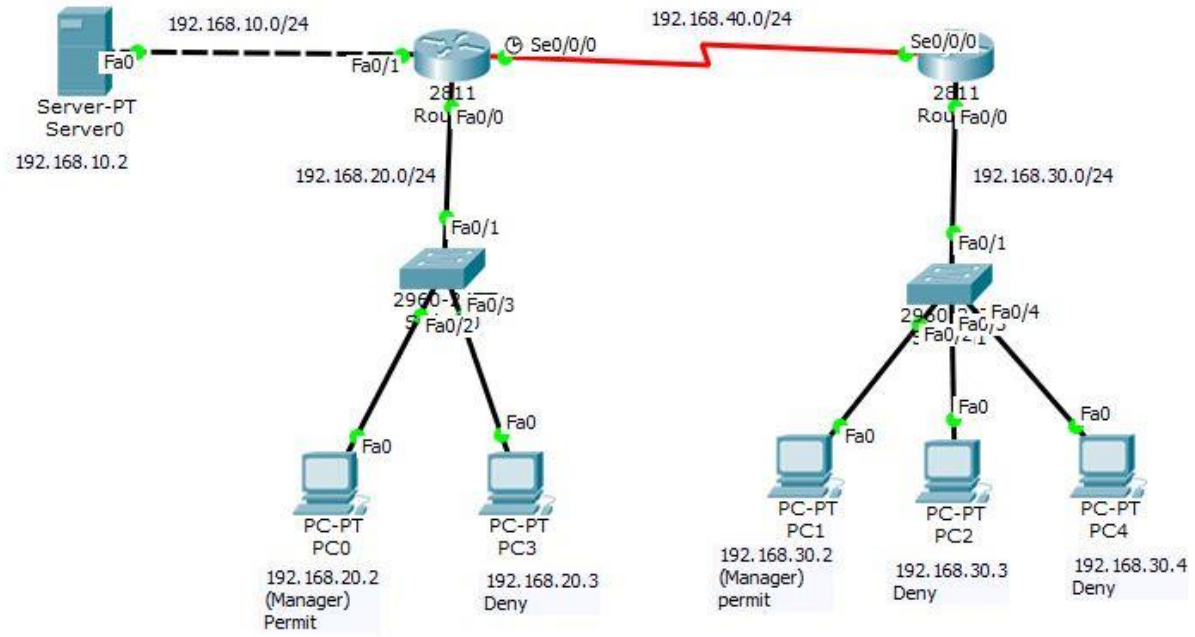
Way 03:
Router 1->
Router(config)#access-list 12 permit 192.168.30.2
Router(config)#int f0/0
Router(config-if)#ip access-group 12 in
Router(config-if)#ex

Router(config)#no access-list 12

Way 04:

Router(config)#access-list 12 permit 192.168.30.2
Router(config)#int s0/0/0
Router(config-if)#ip access-group 12 out
Router(config-if)#ex

Example 4



*****Configure Router & PC*****

*****Configure RIP*****

Router 0->
Router(config)#access-list 13 permit 192.168.20.2
Router(config)#access-list 13 permit 192.168.30.2
Router(config)#int f0/1
Router(config-if)#ip access-group 13 out
Router(config-if)#exit