Assignment No: 3 Using a Network Simulator (e.g. packet tracer) Configure -A router using router commands, Access Control lists – Standard & Extended.

Theory:

- **Access control list:**

ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface.

When activating an ACL on an interface, you must specify in which direction the traffic should be filtered:

- **Inbound (as the traffic comes into an interface)**
- **Outbound (before the traffic exits an interface)**

Inbound ACLs: Incoming packets are processed before they are routed to an outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet will be discarded after it is denied by the filtering tests. If the packet is permitted by the tests, it is processed for routing.

Outbound ACLs: Incoming packets are routed to the outbound interface and then processed through the outbound ACL.

Universal fact about Access control list

1. ACLs come in two varieties : **Numbered and named**
2. Each of these references to ACLs supports two types of filtering: **standard and extended.**
3. Standard IP ACLs can filter only on the **source IP address** inside a packet.
4. Whereas an extended IP ACLs can filter on the **source and destination IP addresses** in the packet.
5. There are two actions an ACL can take: **permit or deny.**
6. Statements are processed top-down.
7. Once a match is found, no further statements are processed—therefore, order is important.
8. If no match is found, the imaginary **implicit deny statement at the end of the ACL** drops the packet.
9. An ACL should have at least one permit statement; otherwise, all traffic will be dropped because of the hidden implicit deny statement at the end of every ACL.

No matter what type of ACL you use, though, you can have only one ACL per protocol, per interface, per direction. For example, you can have one IP ACL inbound on an interface and another IP ACL outbound on an interface, but you cannot have two inbound IP ACLs on the same interface.

Access List Ranges

Type	Range
IP Standard	1–99
IP Extended	100–199

IP Standard Expanded Range	1300–1999
IP Extended Expanded Range	2000–2699

Standard ACLs

A standard IP ACL is simple; it filters based on source address only. You can filter a source network or a source host, but you cannot filter based on the destination of a packet, the particular protocol being used such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), or on the port number. You can permit or deny only source traffic.

Extended ACLs:

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.

Named ACLs

One of the disadvantages of using IP standard and IP extended ACLs is that you reference them by number, which is not too descriptive of its use. With a named ACL, this is not the case because you can name your ACL with a descriptive name. The ACL named Deny Mike is a lot more meaningful than an ACL simply numbered 1. There are both IP standard and IP extended named ACLs.

Another advantage to named ACLs is that they allow you to remove individual lines out of an ACL. With numbered ACLs, you cannot delete individual statements. Instead, you will need to delete your existing access list and re-create the entire list.

Configuration Guidelines

- Order of statements is important: put the most restrictive statements at the top of the list and the least restrictive at the bottom.
- ACL statements are **processed top-down until a match is found,** and then no more statements in the list are processed.
- If no match is found in the ACL, the packet is dropped (implicit deny).
- Each ACL needs either a unique number or a unique name.
- The router cannot filter traffic that it, itself, originates.
- You can have only one IP ACL applied to an interface in each direction (inbound and outbound)—you can't have two or more inbound or outbound ACLs applied to the same interface. (Actually, you can have one ACL for each protocol, like IP and IPX, applied to an interface in each direction.)
- Applying an empty ACL to an interface permits all traffic by default: in order for an ACL to have an implicit deny statement, you need at least one actual permit or deny statement.
- Remember the numbers you can use for IP ACLs.Standard ACLs can use numbers ranging **1–99 and 1300–1999,** and extended ACLs can use **100–199 and 2000–2699.**
- Wildcard mask is not a subnet mask. Like an IP address or a subnet mask, a wildcard mask is composed of 32 bits when doing the conversion; subtract each byte in the subnet mask from 255.

There are two special types of wildcard masks:

0.0.0.0 and 255.255.255.255

A 0.0.0.0 wildcard mask is called a host mask

255.255.255.255. If you enter this, the router will cover the address and mask to the keyword any.

Placement of ACLs

Standard ACLs should be placed as close to the destination devices as possible.

Extended ACLs should be placed as close to the source devices as possible.

- ## Standard access lists:

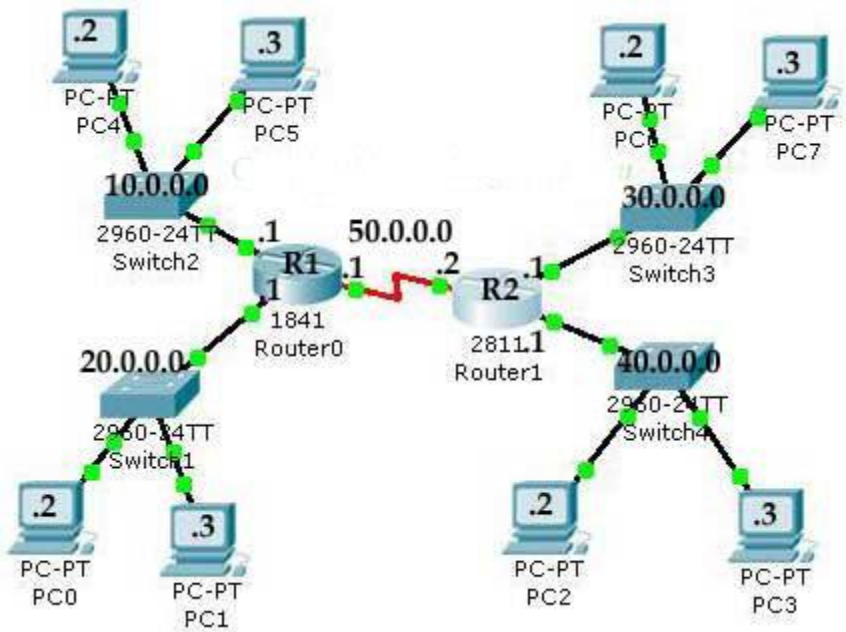
Because a standard access list filters only traffic based on source traffic, all you need is the IP address of the host or subnet you want to permit or deny. ACLs are created in global configuration mode and then applied on an interface. The syntax for creating a standard ACL is

access-list {1-99 | 1300-1999} {permit | deny} source-address
[wildcard mask]

In this article we will configure standard access list. If you want read the feature and characteristic of access list reads this previous article.

Access control list

In this article we will use a RIP running topology. Which we created in RIP routing practical.



Three basic steps to configure Standard Access List

- Use the access-list global configuration command to create an entry in a standard ACL.
- Use the interface configuration command to select an interface to which to apply the ACL.
- Use the ip access-group interface configuration command to activate the existing ACL on an interface.

With Access Lists you will have a variety of uses for the wild card masks, but typically For CCNA exam prospective you should be able to do following:

1. Match a specific host,
2. Match an entire subnet,
3. Match an IP range, or
4. Match Everyone and anyone

• Match specific hosts:

Task

You have given a task to block 10.0.0.3 from gaining access on 40.0.0.0. While 10.0.0.3 must be able to communicate with networks. Other computer from the network of 10.0.0.0 must be able to connect with the network of 40.0.0.0.

Decide where to apply ACL and in which directions.

Our host must be able to communicate with other host except 40.0.0.0 so we will place this access list on FastEthernet 0/1 of R2 (2811) connected to the network of 40.0.0.0. Direction will be outside as packet will be filter while its leaving the interface. If you place this list on R1(1841) then host 10.0.0.3 will not be able to communicate with any other hosts including 40.0.0.0.

To configure R2 double click on it and select CLI (Choose only one method result will be same)

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny host 10.0.0.3
R2(config)#access-list 1 permit any
R2(config)#interface fastEthernet 0/1
R2(config-if)#ip access-group 1 out

OR

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 10.0.0.3 0.0.0.0
R2(config)#access-list 1 permit any
R2(config)#interface fastEthernet 0/1
R2(config-if)#ip access-group 1 out
To test first do ping from 10.0.0.3 to 40.0.0.3 it should be request time out as this packet will filter by ACL. Then ping 30.0.0.3 it should be successfully replay.
PC>ping 40.0.0.3

Pinging 40.0.0.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

- **Configure Extended Access Lists**

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.

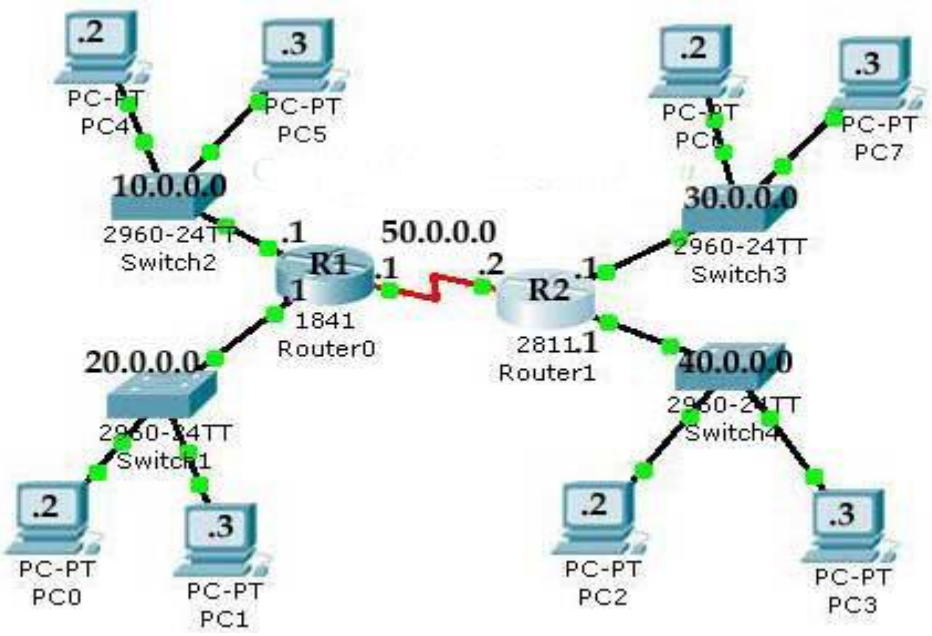
access-list access-list-number {permit | deny}
protocol source source-wildcard [operator port]
destination destination-wildcard [operator port]
[established] [log]

Command Parameters	Descriptions
access-list	Main command
access-list-number	Identifies the list using a number in the ranges of 100–199 or 2000–2699.
permit | deny	Indicates whether this entry allows or blocks the specified address.
protocol	IP, TCP, UDP, ICMP, GRE, or IGRP.
source and destination	Identifies source and destination IP addresses.
source-wildcard and destination-wildcard	The operator can be lt (less than), gt (greater than), eq (equal to), or neq (not equal to). The port number referenced can be either the source port or the destination port, depending on where in the ACL the port number is configured. As an alternative to the port number, well-known application names can be used, such as Telnet, FTP, and SMTP.
established	For inbound TCP only. Allows TCP traffic to pass if the packet is a response to an outbound-initiated session. This type of traffic has the acknowledgement (ACK) bits set. (See the Extended ACL with the Established Parameter example.)
log	Sends a logging message to the console.

Before we configure Extended Access list you should cram up some important port number

Well-Known Port Numbers and IP Protocols

Port Number	IP Protocol
20 (TCP)	FTP data
21 (TCP)	FTP control
23 (TCP)	Telnet
25 (TCP)	Simple Mail Transfer Protocol (SMTP)
53 (TCP/UDP)	Domain Name System (DNS)
69 (UDP)	TFTP
80 (TCP)	HTTP



Three basic steps to configure Extended Access List

- Use the access-list global configuration command to create an entry in a Extended ACL.
- Use the interface configuration command to select an interface to which to apply the ACL.
- Use the ip access-group interface configuration command to activate the existing ACL on an interface.

With Access Lists you will have a variety of uses for the wild card masks,

1. Block host to host
2. Block host to network
3. Block Network to network
4. Block telnet access for critical resources of company
5. Limited ftp access for user
6. Stop exploring of private network form ping
7. Limited web access
8. Configure established keyword

• Block host to host

Task

You are the network administrator at ComputerNetworkingNotes.com. Your company hire a new employee and give him a pc 10.0.0.3. your company's critical record remain in 40.0.0.3. so you are asked to block the access of 40.0.0.3 from 10.0.0.3. while 10.0.0.3 must be able connect with other computers of network to perform his task.

Decide where to apply ACL and in which directions.

As we are configuring Extended access list. With extended access list we can filter the packed as soon as it generate. So we will place our access list on F0/0 of Router1841 the nearest port of 10.0.0.3

To configure Router1841 (Hostname R1) double click on it and select CLI

R1>enable

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#access-list 101 deny ip host 10.0.0.3 40.0.0.3 0.0.0.0

R1(config)#access-list 101 permit ip any any
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip access-group 101 in
R1(config-if)#exit
R1(config)#

Verify by doing ping from 10.0.0.3 to 40.0.0.3. It should be request time out. Also ping other computers of network including 40.0.0.2. ping should be successfully.

- **Block host to network**

Task

Now we will block the 10.0.0.3 from gaining access on the network 40.0.0.0. (if you are doing this practical after configuring pervious example don't forget to remove the last access list 101.

With no access-list command. Or just close the packet tracer without saving and reopen it to be continue with this example.)
R1(config)#access-list 102 deny ip host 10.0.0.3 40.0.0.0 0.255.255.255
R1(config)#access-list 102 permit ip any any
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip access-group 102 in
R1(config-if)#exit
R1(config)#

Verify by doing ping from 10.0.0.3 to 40.0.0.3. and 40.0.0.2.It should be request time out. Also ping computers of other network. ping should be successfully.

Conclusion:

We have configured router, standard and extended access control list on router successfully.