Assignment Number: 01

Using a Network Simulator (e.g. packet tracer) Configure Router

Using a Network Simulator (e.g. packet tracer) Configure Router

A] Configure a router using router commands and Configure Routing Information Protocol (RIP).

B] Configure Access Control lists – Standard & Extended.

C] Network Address Translation: Static, Dynamic & PAT (Port Address Translation)

Theory:

Router – Router is a network device that allows you to direct data traffic to an appropriate destination. Router maintain routing table that contain IP addresses of computers over the network. A router has different components that enable proper functioning.

Cisco IOS supports various command modes, among those followings are the main command modes.

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode
- Sub Interface Configuration Mode
- Setup Mode

Following table lists essential commands to navigate between different IOS modes.

Mode	**Prompt**	**Command to enter**	**Command to exit**
User EXEC	Router >	Default mode after booting. Login with password, if configured.	Use **exit** command
Privileged EXEC	Router #	Use **enable** command from user exec mode	Use **exit** command
Global Configuration	Router(config)#	Use **configure terminal** command from privileged exec mode	Use **exit** command
Interface Configuration	Router(config-if)#	Use **interface type *number*** command from global configuration mode	Use **exit** command to return in global configuration mode
Sub-Interface Configuration	Router(config-subif)	Use **interface type *sub interface number***command from global configuration mode or interface configure mode	Use **exit** to return previous mode. Use **end** command to return in privileged exec mode.

Some important router command

Command	**Description**
Router(config)#interface serial 0/0/0	Enter into serial interface 0/0/0 configuration mode
Router(config-if)#description Connected to interface	Optional command. It set description on interface that is locally significant
Router(config-if)#ip address 10.0.0.1 255.0.0.0	Assigns address and subnet mask to interface
Router(config-if)#clock rate 64000	DCE side only command. Assigns a clock rate for the interface
Router(config-if)#bandwidth 64	DCE side only command. Set bandwidth for the interface.
Router(config-if)#no shutdown	Turns interface on

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.

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.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a standards-based, distance-vector, interior gateway protocol (IGP) used by routers to exchange routing information. RIP uses hop count to determine the best path between two locations. Hop count is the number of routers the packet must go through till it reaches the destination network. The maximum allowable number of hops a packet can traverse in an IP network implementing RIP is 15 hops.

It has a maximum allowable hop count of 15 by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it's inefficient on large networks with slow WAN links or on networks with a large number of routers installed.

In a **RIP** network, each router broadcasts its entire RIP table to its neighboring routers every 30 seconds. When a router receives a neighbor's RIP table, it uses the information provided to update its own routing table and then sends the updated table to its neighbors.

Enabling RIP

To enable RIP, use the following commands beginning in global configuration mode:

	Command	**Purpose**
Step 1	Router(config)# **router rip**	Enables a RIP routing process, which places you in router configuration mode
Step 2	Router(config-router)# **network***ip-address*	Router(config-router)# **network***ip-address*

Network Address Translation (NAT)

NAT

There are several situations where we need address translation such as, a network which do not have sufficient public IP addresses want to connect with the Internet, two networks which have same IP addresses want to merge or due to security reason a network want to hide its internal IP structure from the external world. NAT (Network Address Translation) is the process which translates IP address. NAT can be performed at firewall, server and router. In this assignment we will understand how it is performed at Cisco router.

NAT Terminology

Before we understand NAT in details let's get familiar with four basic terms used in NAT.

Term	Description
Inside Local IP Address	Before translation source IP address located inside the local network.
Inside Global IP Address	After translation source IP address located outside the local network.
Outside Global IP Address	Before translation destination IP address located outside the remote network.
Outside Local IP Address	After translation destination IP address located inside the remote network.

Types of NAT

There are three types of NAT; Static NAT, Dynamic NAT and PAT. These types define how inside local IP address will be mapped with inside global IP address.

Static NAT

In this type we manually map each inside local IP address with inside global IP address. Since this type uses one to one mapping we need exactly same number of IP address on both sides.

Dynamic NAT

In this type we create a pool of inside global IP addresses and let the NAT device to map inside local IP address with the available outside global IP address from the pool automatically.

PAT

In this type a single inside global IP address is mapped with multiple inside local IP addresses using the source port address. This is also known as PAT (Port Address Translation) or NAT over load.

Advantages and disadvantages of NAT

Nat provides following advantages: -

- NAT solves IP overlapping issue.
- NAT hides internal IP structure from external world.
- NAT allows us to connect with any network without changing IP address.
- NAT allows us to connect multiple computers with internet through the single the public
IP address.

NAT has following disadvantages: -

- NAT adds additional delay in network.
- Several applications are not compatible with NAT.
- End to end IP traceability will not work with NAT.
- NAT hides actual end device.

Conclusion :

Thus we have successfully configured router with it’s command and with RIP protocol. Also we understand the use of standard and extended access control list and Network address translation (NAT).