Lab-8: Objective:
Part A: Configure Standard Access Control List (ACL) on given network.
Part B: Configure Extended Access Control List (ACL) on given network

Lab-8
Standard & Extended Access Control List

Part A: Configure Standard Access Control List (ACL) on given network in figure 18 so that only authorized departments can communicate with attached server.

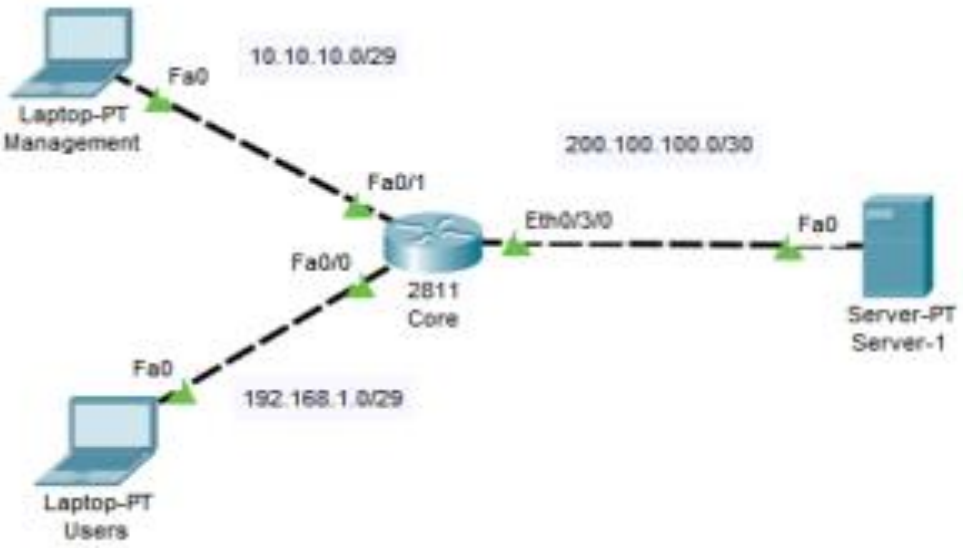

Figure 18

Access Control List (ACL)

An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each

system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program).

In the computer networking world, an ACL is one of the most fundamental components of security. An Access Control Lists "ACL" watches incoming and outgoing traffic and compares it with a set of defined statements.

Access Control List (ACL) are filters that enable you to control which routing updates or packets are permitted or denied in or out of a network.
They are specifically used by network administrators to filter traffic and to provide extra security for the network. This can be applied to routers (Cisco).

ACLs provide a powerful way to control traffic into and out of your network; this control can be as simple as permitting or denying network hosts or addresses. You can configure ACLs for all routed network protocols.

The most important reason to configure ACLs is to provide security for your network. However, ACLs can also be configured to control network traffic based on the TCP port being used.

How ACLs works.

A router acts as a packet filter when it forwards or denies packets according to filtering rules. As a Layer 3 device, a packet-filtering router uses rules to determine whether to permit or deny traffic based on source and destination IP addresses, source port and destination port, and the protocol of the packet. These rules are defined using access control lists or ACLs.

Standard access-list

Standard access lists create filters based on source addresses and are used for server-based filtering. Address-based access lists distinguish routes on a network you want to control by using network address number (IP).
Address-based access lists consist of a list of addresses or address ranges and a statement as to whether access to or from that address is permitted or denied.

Standard ACL has two different ranges which are, 1-99 and 1300-1999.

Example of the command syntax for configuring a standard numbered IP ACL:

Access-list {1-99} {permit | deny} source-address [source-wildcard]

- The first value {1-99} specifies the standard ACL number range.
- The second value specifies whether to permit or deny the configured source IP address traffic.
- The third value is the source IP address that must be matched.

- The fourth value is the wildcard mask to be applied to the previously configured IP address to indicate the range.

Task 1, Assign the IP address on Core Router

Core>enable

Core#configure terminal

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

Core(config)#interface fa 0/1

Core(config-if)#ip address 10.10.10.1 255.255.255.248

Core(config-if)#no shutdown

Core(config-if)#exit

Core (config)#interface fa 0/0

Core (config-if)#ip address 192.168.1.1 255.255.255.248

Core (config-if)#no shutdown

Core (config-if)#exit

Core (config)#interface ethernet 0/3/0

Core (config-if)#ip address 200.100.100.1 255.255.255.252

Core (config-if)#no shutdown

Core (config-if)#exit

Task 2, Configure OSPF-70 on attached Router

Core(config)#router ospf 70

Core(config-if)#network 10.10.10.0 0.0.0.7 area 0

Core(config-if)#network 192.168.1.0 0.0.0.7 area 0

Core(config-if)#network 200.100.100.0 0.0.0.3 area

Core(config-if)#exit

Task 3, Configure Standard ACL 49

We want to allow traffic from the management LAN to the server S1. First, we need to write an ACL to permit traffic from LAN 10.10.10.0/29 to S1. We can use the following command on R1:

Core (config)#access-list 49 permit 10.10.10.0 0.0.0.7

The command above permits traffic from all IP addresses that begin with 10.10.10.0. We could also target the specific host by using the host keyword:

Core (config)#access-list 49 permit host 10.10.10.1

Next, we will deny traffic from the Users LAN (192.168.1.0):

Core (config)#access-list 49 deny 192.168.1.0 0.0.0.7

Next, we need to apply the access list to an interface. It is recommended to place the standard access lists as close to the destination as possible. In our case, this is the Ethernet 0/3/0interface on core router. Since we want to evaluate all packets trying to exit out Ethernet 0/3/0, we will specify the outbound direction with the out keyword:

Core (config)#Ethernet 0/3/0

Core (config-if)#ip access-group 49 out

Core (config-if)#exit

Extended Access Control List (ACL)

Part B: Configure Extended Access Control List (ACL) on given network in figure 19, so that only User-A can access Web Server while users B and C should be restricted. You can configure any routing protocol before applying ACL.

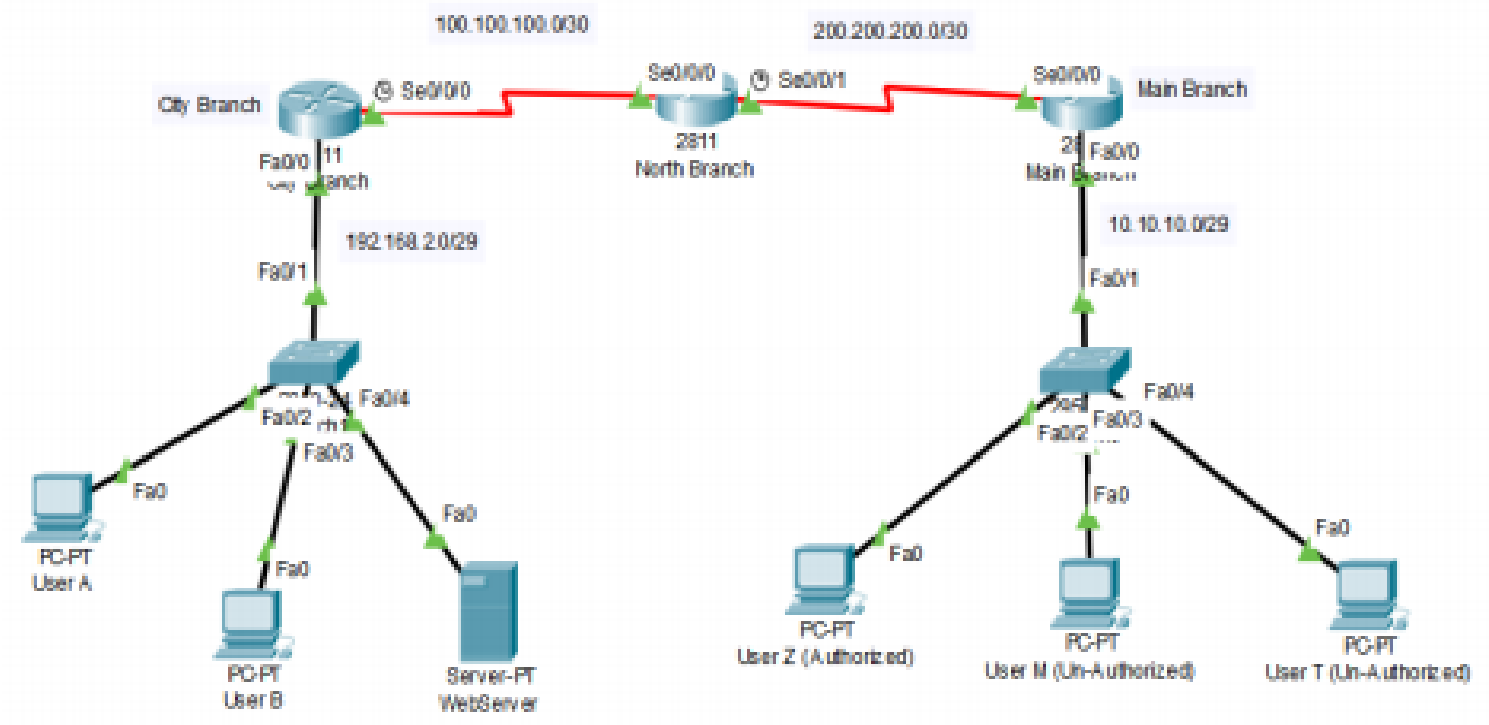

Figure 19

Extended Access Control List (ACL)

Extended access lists create filters based on source addresses, destination addresses, protocol, port number and other features and are used for packet-based filtering for packets that traverse the network.

Example of the command syntax for configuring an extended numbered IP ACL:

Access-list {100-199} {permit | deny} protocol source-address [source-wildcard] [operator operand] destination-address [destination-wildcard] [operator operand] [established]

-Like the standard ACLs, the first value {100-199 or 2000 – 2699} specifies the ACL number range.
- The next value specifies whether to permit or deny according to the criteria that follow.
- The third value specifies protocol type (IP, TCP, UDP, or other specific IP sub-protocols).

The source IP address and wildcard mask determine traffic source. The destination IP address and its wildcard mask are used to indicate the final destination of the network traffic. When the destination IP address and mask are configured, the port number must be specified to match, either by number or by a well-known port name, otherwise, all traffic to that destination will be dropped.

Standard and Extended access lists can be applied base on the use of ip access-list command.

Access lists uses deny or **permit** statement to define which packet is allowed or denied entry into a server or network.

Task 1, Assign the IP address on each Router

Router City Branch:

City Branch >enable

City Branch #configure terminal

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

City Branch (config)#interface serial 0/0/0

City Branch (config-if)#ip address 100.100.100.1 255.255.255.252

City Branch (config-if)#clock rate 64000

City Branch (config-if)#no shutdown

City Branch (config-if)#exit

City Branch (config)#interface fa 0/0

City Branch (config-if)#ip address 192.168.2.1 255.255.255.248

City Branch (config-if)#no shutdown

City Branch (config-if)#exit

Router North Branch:

North Branch >enable

North Branch #configure terminal

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

North Branch (config)#interface serial 0/0/0

North Branch (config-if)#ip address 100.100.100.2 255.255.255.252

North Branch (config-if)#no shutdown

North Branch (config-if)#exit

North Branch (config)#interface serial 0/0/1

North Branch (config-if)#ip address 200.200.200.1 255.255.255.252

North Branch (config-if)#clock rate 64000

North Branch (config-if)#no shutdown

North Branch (config-if)#exit

Router Main Branch:

Main Branch >enable

Main Branch #configure terminal

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

Main Branch (config)#interface serial 0/0/0

Main Branch (config-if)#ip address 200.200.200.2 255.255.255.252

Main Branch (config-if)#clock rate 64000

Main Branch (config-if)#no shutdown

Main Branch (config-if)#exit

Main Branch (config)#interface fa 0/0

Main Branch (config-if)#ip address 10.10.10.1 255.255.255.248

Main Branch (config-if)#no shutdown

Main Branch (config-if)#exit

Task 2, Configure EIGRP-50 on each Router

Router City Branch:

City Branch (config)#router eigrp 50

City Branch (config-if)#network 192.168.2.0 0.0.0.7

City Branch (config-if)#network 100.100.100.0 0.0.0.3

City Branch (config-if)#no auto-summary

City Branch (config-if)#exit

Router North Branch:

North Branch (config)#router eigrp 50

North Branch (config-if)# network 100.100.100.0 0.0.0.3

North Branch (config-if)# network 200.200.200.0 0.0.0.3

North Branch (config-if)#no auto-summary

North Branch (config-if)#exit

Router Main Branch:

Main Branch (config)#router eigrp 50

Main Branch(config-if)# network 200.200.200.0 0.0.0.3

Main Branch(config-if)# network 10.10.10.0 0.0.0.7

Main Branch(config-if)#no auto-summary

Main Branch(config-if)#exit

Task 3, Configure Extended ACL 199

Main Branch (config)# access-list 199 permit tcp host 10.10.10.2 host 192.168.2.4 eq www

Main Branch (config)# access-list 199 deny tcp any host 192.168.2.4 eq www

Main Branch (config)# access-list 199 permit ip any any

Main Branch (config)# interface Serial0/0/0

Main Branch (config-if)# ip address 200.200.200.2 255.255.255.252

Main Branch (config-if)# ip access-group 199 out

Main Branch (config-if)#exit

Lab-8Exercise:

Configure Extended Access Control List (ACL) on a 3 routers bus network. Also attach 3 PC's with all 3 routers. At the end of the configuration any 2 of the authorized users can send and receive email to each other while unauthorized users should be restricted. You have to configure EIGRP on this network and must use your SID as EIGRP Process ID.