ACL Laboratory Experiment 9.1.1

WEB / MANAGEMENT / DHCP Access

Overview: The purpose of this lab is to examine using Access Control lists in IPv4, to permit or deny access to router management (Telnet), and to server services (WEB / DHCP) using both standard and extended named ACL's

Equipment: Cisco Packet Tracer® 6.0.1

Optional Equipment:

Cisco 2911 Router

Cisco 2960 Switch

Windows Server with both WEB and DHCP services active

Two (2) generic PC's

Assorted cables

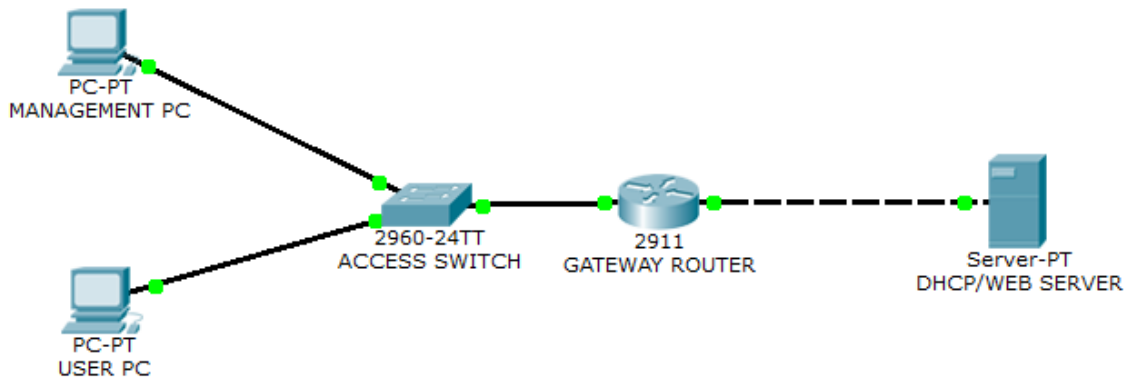
Construction:

1. Construct the following circuit in Cisco Packet Tracer® (PT)

   Select in PT a 2911 router, 2960 switch, tow generic PC's and server, and place as shown in the diagram. The equipment may or may not be named for easier recognition.

2. Connect a straight-through cable from one of the PC's FastEthernet0 to any port on the switch.
3. Connect a straight-through cable from the other PCs FastEthernet0 to any free port on the switch.
4. Connect a third straight-through cable from any free port on the switch to the routers GigaBitEthernet 0/0 (G0/0) port
5. Connect a Cross-over cable from the routers GigaBitEthernet 0/1 (G0/1) port to the servers FastEthernet0 port

Diagram:



Addressing:

Addressing Table			
Device	**IP Address**	**Subnet Mask**	**Default-Gateway**
Management PC	10.1.0.1	255.255.255.0	10.1.0.254
User PC	10.1.0.2	255.255.255.0	10.1.0.254
Gateway Router G0/0	10.1.0.254	255.255.255.0	
Gateway Router G0/1	10.2.0.254	255.255.255.0	
DHCP / WEB server	10.2.0.1	255.255.255.0	10.2.0.254

Configuration:

1. Program the router with basic set-up instructions as follows:

    Router>**enable**

    Router#**config t**

    Router(config)#**enable secret cisco**

    Router(config)#**line vty 0 4**

    Router(config-line)#**password class**

    Router(config-line)#**login**

Router(config-line)**#exit**

Router(config)**#int g0/0**

Router(config-if)**#ip address 10.1.0.254 255.255.255.0**

Router(config-if)**#no shut**

Router(config)**#int g0/1**

Router(config-if)**#ip address 10.2.0.254 255.255.255.0**

Router(config-if)**#no shut**

Router(config-if)**#end**

Router**#copy run start**

2. Program the two (2) PC's and the Server with the address from the Addressing Table.
3. Using the "ping" command, verify full-connectivity from the PC's to the server.
4. Use the web browser in either PC to connect to the server and verify web page connectivity.

Part I

Procedure:

1. Construct a standard named ACL to limit access to the router and place appropriately. Note: All proper names, such as TELNET, should be all capitalized to facilitate easier recognition.

Router**#config t**

Router(config)**#ip access-list standard TELNET**

Router(config-std-nacl)**#10 permit host 10.1.0.1**

Router(config-std-nacl)**#exit**

Router(config)**#line vty 0 4**

Router(config-line)#**access-class TELNET in**

Router(config-line)#**end**

2. Show the ACL you just constructed.

Router#**sh access-lists**

Router#sh access-lists

Standard IP access list TELNET

10 permit host 10.1.0.1

During configuration the ACL line entries may or may not be numbered to facilitate editing at a later time.

3. Test your ACL by using telnet from the MANAGEMENT PC to the router.

PC>telnet 10.1.0.254
Trying 10.1.0.254 …Open

User Access Verification

Password:
Router>ena
Password:
Router#exit

[Connection to 10.1.0.254 closed by foreign host]
PC>

4. Test telnet connectivity from the USER PC to the router.

   PC>telnet 10.1.0.254
   Trying 10.1.0.254 …
   % Connection refused by remote host
   PC>

5. Did your ACL successfully block telnet access? (yes / no)
6. Now it is necessary to restrict only web traffic to the server, by constructing an extended ACL.

   Router**#config t**

   Router(config)**#ip access-list extended SERVER**

   Router(config-ext-nacl)**#remark Allow WEB Access**

   Router(config-ext-nacl)**#10 permit tcp 10.1.0.0 0.0.0.255 eq 80 host 10.2.0.1 eq 80**

   Router(config-ext-nacl)**#exit**

   Router(config)**#int g0/1**

   Router(config-if)**#ip access-group SERVER out**

   Router(config-if)**#exit**

7. Test web connectivity to the server.
    a. Was it successful? (yes/no)
    b. If you were not successful, why?

        _____
        _____
        _____

    c. The reason that your ACL blocked the web request was that in the ACL the source port for web traffic was specified.

        10 permit tcp 10.1.0.0 0.0.0.255 **eq 80** host 10.2.0.1 eq 80

        Normally a PC will use a dynamic port for the connection.

8. Modify the ACL to permit a dynamic port.

    Router**#config t**

    Router(config)**#ip access-list extended SERVER**

    Router(config-ext-nacl)**#no 10 permit tcp 10.1.0.0 0.0.0.255 eq 80 host 10.2.0.1 eq 80**

    Router(config-ext-nacl)**#10 permit tcp 10.1.0.0 0.0.0.255 host 10.2.0.1 eq 80**

    Router(config-ext-nacl)**#end**

    Notice that it was not necessary to eliminate the entire ACL as with a numbered ACL, in a named ACL a line may be identified by its line number and replaced.

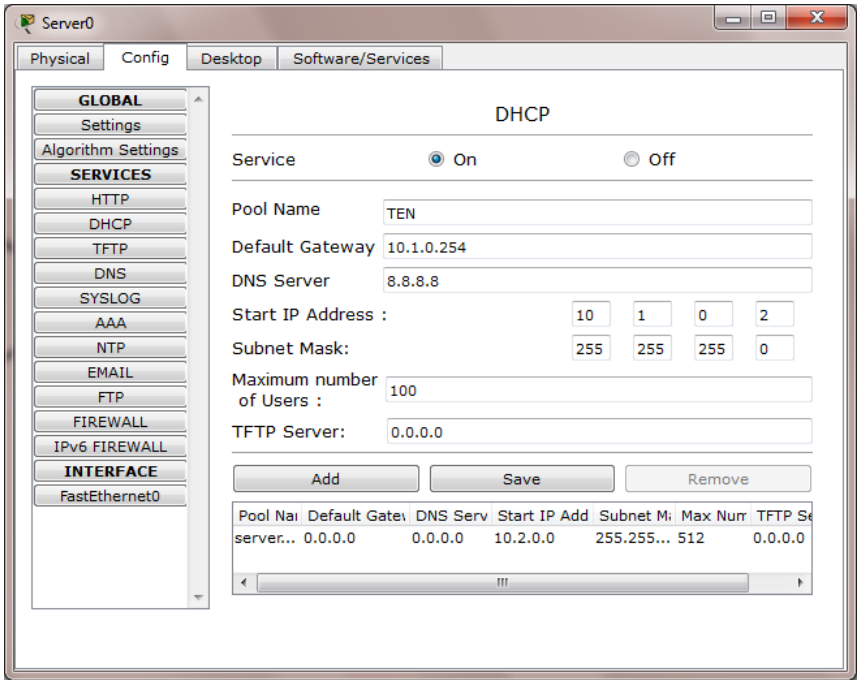
9. Test web connectivity to the server.
    a. Was it successful? (yes/no)

Part II

Procedure:

1. Enable DHCP services on the server and create a pool of addresses for the 10.1.0.0 network.

2. Name the pool TEN and use a starting address of 10.1.0.2 (10.1.0.1 is the management PC) with a maximum number of leased addresses of one-hundred (100) and a DNS server address of 8.8.8.8 (Google)



3. Select the "ADD" button to add the pool. Make sure the DHCP service is enabled with the "ON" radio button.

4. Remove the static ip address on the USER PC and set it to DHCP.

   a. Does the PC get an address from the server? (yes/no)
   b. The reason that it should not get an address at this time is two-fold.
      1. IP helper was not configured on GigabitEthernet 0/0 pointing to the server
      2. The ACL has an implicit deny any statement.

5. Establish the ip-helper address on interface G0/0

   Router**#config t**

   Router(config)**#int G0/0**

   Router(config-if)**#ip helper-address 10.2.0.1**

   Router(config-if)**#end**

6. Modify the ACL to allow DHCP requests which originate from ports UDP 68 the DHCP server will respond using port UDP 67. Since the ACL is applied in the outbound direction it is only necessary to add port UDP 68

   Router**#config t**

   Router(config)# **ip access-list extended SERVER**

   Router(config-ext-nacl)**#remark Allow DHCP Access**

   Router(config-ext-nacl)**#20 permit udp host 10.1.0.254 host 10.2.0.1 eq 68**

   Although it was not necessary the originating ip-address of the interface was specified (10.1.0.254) to further secure the network.

Part III

Procedure:

1. Verify that the server can contact the inside hosts using the "ping" command.

   Was the "ping" successful? (yes/no)

   The server should not have been able to ping the inside PC's because echo-reply was never allowed to exit the interface to the Server

2. Modify the ACL named "SERVER" to allow echo-reply

   Router**#config t**

   Router(config)# **ip access-list extended SERVER**

   Router(config-ext-nacl)**#remark Allow echo-reply**

   Router(config-ext-nacl)**#30 permit icmp 10.1.0.0 0.0.0.255 host 10.2.0.1 echo-reply**

3. Verify that the server can contact the inside hosts using the "ping" command.

   Was the "ping" successful? (yes/no)

4. Verify that the inside hosts can contact the Server using the "ping" command.

   Was the "ping" successful? (yes/no)

   The inside hosts should not have been able to ping the server because echo was never permitted to exit the interface to the Server.

5. Edit the ACL named "SERVER" to allow echo

   Router**#config t**

   Router(config)**# ip access-list extended SERVER**

   Router(config-ext-nacl)**#remark Allow echo**

   Router(config-ext-nacl)**#40 permit icmp 10.1.0.0 0.0.0.255 host 10.2.0.1 echo**

6. Use the "ping" command to verify full connectivity.

   Was connectivity verified (yes/no)

Part 4

Procedure:

1. Create an ACL to apply to the G0/1 interface to only allow permitted services and block all others.

   Router**#config t**

   Router(config)**#ip access-list extended OUTSIDE**

   Router(config-ext-nacl)**#remark Allow WEB Traffic**

   Router(config-ext-nacl)**#10 permit tcp host 10.2.0.1 eq 80 10.1.0.0 0.0.0.255**

   Router(config-ext-nacl)**#remark Permit DHCP response**

   Router(config-ext-nacl)**#20 permit udp host 10.2.0.1 eq 67 host 10.1.0.254**

   Router(config-ext-nacl)**#remark Permit Echo Request**

   Router(config-ext-nacl)**#30 permit icmp host 10.2.0.1 10.1.0.0 0.0.0.255 echo**

   Router(config-ext-nacl)**#exit**

   Router(config)**#int g0/1**

   Router(config-if)**#ip access-group OUTSIDE in**

   Router(config-if)**#exit**

2.
3. Verify that WEB, Ping and DHCP services function normally.

   Did all services function normally? (yes/no)

4. Remove the ACL from the VTY line.

   Router(config)**#line vty 0 4**

   Router(config-line)**#no access-class TELNET in**

5. Verify that the server cannot telnet into the router.

   Was the Telnet secession successful? (yes/no)

   The Telnet secession should not have been successful because Telnet was not allowed to enter by the "OUTSIDE" ACL.