**Standard Access Control List   
Intended Learning Outcome:**a. To understand the properties of Standard Access Control List.  
b. To analyze how Standard Access Control List is used for forwarding the packets.

**Expected skills:**The basic concepts IP address and Subnet mask.   
  
**Tools Required:**Cisco Packet Tracer Simulation Software  
  
**Session Detail:**

**Configure Standard Access Control List**

ACL-Access Control List (Named Access List and Number Access List).If we use numbers to refer access list it is numbered access list. If we use Name to refer access list it is named access list. We are using access list to permit or deny ip packets based on our requirements. There are two types,

# Standard Access List 2.Extended Access List

Here we are going to see how to configure standard access list with a simple topology in a packet tracer,

Step 1: Create a topology

Step 2: Configure router with ip address that i have given in topolgy. Assign ip address to all PC and server like in topology.

# In Router,global configuration

**Router(config)#interface fastethernet0/0 Router(config-if)#ip address 10.0.0.1 255.0.0.0 Router(config-if)#no shutdown**

**Router(config-if)#exit Router(config)#interface fastethernet1/0 Router(config-if)#ip address 20.0.0.1 255.0.0.0 Router(config-if)#no shutdown**

Step 3: Three steps to configure access list on router,

# Creating Standard Access List

* 1. **Choosing an Interface for Binding**
  2. **Choosing In/Out**

Step 4: Create an Standard Ip access list to deny a host 10.0.0.3 to server.

In standard access list, it filters based on source ip address. we can't deny of permit packets to destination or particular ports for that we have use extended access list later we see this, Now let’s we create a standard access list based on above statement i have given.

# Create Access List:

**Router(config)#access-list 1 deny host 10.0.0.3 (or)**

**Router(config)#access-list 1 deny 10.0.0.3 0.0.0.0 Router(config)#access-list 1 permit any**

where '1' is a number. It refers, this as a Standard accesss control list. It can be '1 to 99' and '1300 to 1999'.

'Deny' Allows router to deny the packet that matches this statement. 'Host 10.0.0.3' when we configure like this it refers 'Only this host will be permitted or denied' or we should configure with wild card mask '0.0.0.0' it means router checks for entire four octets if matched then it will process based on access list.

'Implicit deny' at bottom of all access list so we have to give permit any command at last otherwise ip address that doesn't match above statement will be denied. Access list always proccesed from top to bottom so we should configure access list in order. We should not configure 'permit any' statement first and then deny, If we configure permit any statement first, access list will check first statement if matches it will forward the packet and it won't go for next statement that 'deny'. Always we should configure 'deny' statement first.

Choose Interface for Binding whether In or Out:

Always we have to choose an interface near to the source as much as possible. Sometime based on some access list statement we need to choose interface that packets go out of the router. We should try to use router interface that receives a packet from PC in a LAN.

So, I am going to choose 'interface fastethernet0/0' .Before that i am going to check access list status for this interface.

# In Privileged Mode,

**Router#show ip interface fastethernet0/0**

**FastEthernet0/0 is up, line protocol is up (connected)**

**Internet address is 10.0.0.1/8**

**Broadcast address is 255.255.255.255**

**Address determined by setup command**

**MTU is 1500**

**Helper address is not set**

**Directed broadcast forwarding is disabled**

**Outgoing access list is not set**

**Inbound access list is not set**

**Proxy ARP is enabled**

**In global configuration,**

**Router(config)#interface fastethernet0/0 Router(config-if)#ip access-group 1 in Router(config-if)#exit**

where '1' refers access list 1 and packets that comes into the router will be filtered based on access list.

Now, Check the access list status on this interface.

# In Privileged Mode,

**Router#show ip interface fastethernet0/0**

**FastEthernet0/0 is up, line protocol is up (connected)**

**Internet address is 10.0.0.1/8**

**Broadcast address is 255.255.255.255**

**Address determined by setup command**

**MTU is 1500**

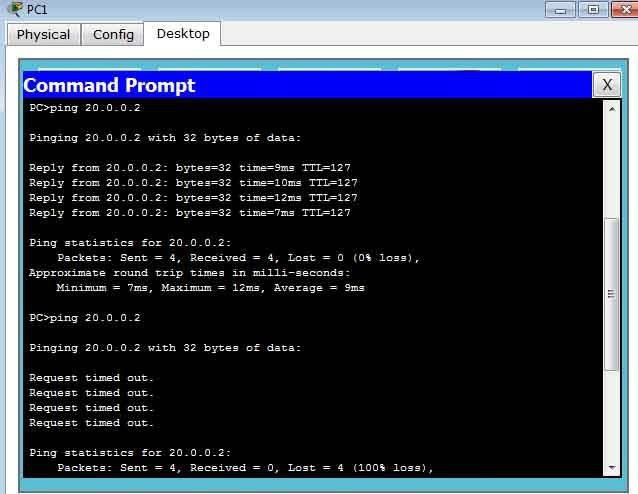
**Helper address is not set**

**Directed broadcast forwarding is disabled**

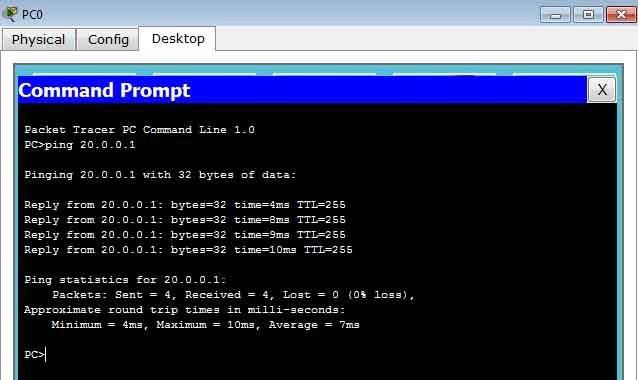
**Outgoing access list is not set**

**Inbound access list is 1**

Now , go to the host that configured with ip address 10.0.0.3 and try to ping 20.0.0.2.This is the response i have got before and after configure access list.



This is the response for other host.



To deny whole network,

**Router(config)#access-list 1 deny 10.0.0.0 0.255.255.255**

Here we are permitting whole network that 1,67,77,216 ip address

To permit one host others should be denied,i am going to pemit 10.0.0.2

# Router(config)#access-list 1 permit 10.0.0.2 0.0.0.0

(or)

# Router(config)#access-list 1 permit host 10.0.0.2

Here,Implicit deny in all access list will deny other host.

To permit a series of ip address,i am going permit 10.0.0.0 to 10.0.0.3 other ip address others should be blocked.

# Router(config)#access-list 1 permit 10.0.0.0 0.0.0.3

'0.0.0.3' by this router knows that the next ip address from 10.0.0.0 should be pemitted others blocked.Total ip address 4. Some more example for subnetted Networks,

# Router(config)#access-list 1 permit 10.0.0.0 0.0.0.255

Here, From 10.0.0.0-10.0.0.255 will be permitted,Total ip address 256 Network 10.0.0.0/24 Range of ip's 10.0.0.0 -10.0.0.255

# Router(config)#access-list 1 permit 10.0.0.0 0.0.1.255

Network 10.0.0.0/23 Range of ip's 10.0.0.0 -10.0.1.255

Here,From 10.0.0.0-10.0.1.255 will be permitted,Total ip address 512

# Router(config)#access-list 1 permit 10.0.32.0 0.0.15.255

Here , From 10.0.0.0 -10.0.15.255 will be permitted,Total ip address 4096.This is the network subnetted from Class A network.

Network 10.0.32.0/20, Range of Ip's 10.0.32.0-10.0.47.255

So, from 10.0.32.0- 10.0.47.255 ip address are belongs to this network. Here we are permitting whole subnetted network. Now, we see how to pemit or deny some of the network ip address from this subnet.

# Router(config)#access-list 1 deny 10.0.32.0 0.0.3.255 Router(config)#access-list 1 permit any

Here ,Ip from 10.0.32.0 - 10.0.35.255 will be denied other ip address will be permitted.i.e from 10.0.36.0-10.0.47.255 will be permitted.

# Trouble Shooting Commands,

**Router#show ip access-lists 1 Standard IP access list 1**

**deny host 10.0.0.3 permit any**

**Router#show access-lists , 'To see all access list'.**

**Router#show access-lists <WORD> , '<WORD> name we use for access list'.**

**Post Lab Exercise:**

Project Complete and demostration.

**Further Readings:**

http://www.computernetworkingnotes.com/ccna-study-guide/configure-standard-access-control-list-step-by-step-guide.html