**Assignment No:3**

[**https://www.slideshare.net/raghukiran735/acl-35752640**](https://www.slideshare.net/raghukiran735/acl-35752640) **:Slides**

**Using a Network Simulator (e.g. packet tracer) Configure A router using router commands, Access Control lists – Standard & Extended**

In this lesson we will see **Cisco Standard ACL Configuration** and how to configure **Standart Access-List** in Packet Tracer.  
There are **three types** **Access Lists** in common. Thse access list types are :

* **Standard Access List https://www.youtube.com/watch?v=ytS55tg73TQ,** **https://www.youtube.com/watch?v=j70vcgCLOJE**
* [**Extended Access List**](https://ipcisco.com/lesson/extended-access-list-configuration-with-packet-tracer-2/)
* **Named Access List**

**Types of access control lists**

* Standard access control list

Filter packets based on source P address

The access control list number of the standard access control list is 1 ~ 99

* Extended access control list

Filter packets based on source P address, destination P address, specified protocol, port and flag

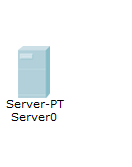
The access control list number of the extended access control list is 100 ~ 199

* Named access control list

Named access control lists allow the use of names instead of table numbers in standard and extended access control lists

1. **Standard Access-Lists**

* are the simplest one. With **Standard Access-List** you can check only the source of the IP packets. On the other hand, with **Extended Access-Lists**, you can check source, destination, specific port and protocols. Lastly, with **Named Access-Lists**, you can use names instead of the numbers used in standard and extended ACLs.
* A standard ACL can be used for several purpose. In this tutorial we will see how it can be used in controlling the unwanted network traffic. With standard ACL, we can define certain conditions for the network traffic passing through the router. Once defined, Standard ACL works like a gate keeper that will allow only the authorized people (packets). All unwanted people (packets) are kicked out from the gate.
* For demonstration purpose I will use packet tracer network simulator software. You can use it or can use any other network simulator software such as Boson, NetSim, GNS etc.

-🡪 End devices🡪3 rd Generic

* Router>enable
* Router#config
* Configuring from terminal, memory, or network [terminal]?
* Enter configuration commands, one per line. End with CNTL/Z.
* Router(config)#host R1
* R1(config)#interface Fa0/0
* R1(config-if)#ip address 192.168.23.1 255.255.255.0

[**https://www.youtube.com/watch?v=FIVJUx1k3xA**](https://www.youtube.com/watch?v=FIVJUx1k3xA) **Extended ACL Link:**

* Extended Access Control Lists (ACLs) act as the gatekeeper of your network
* Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or out going of the network.
* **Extended Access-list –**It is one of the types of Access-list which is mostly used as it can distinguish IP traffic therefore the whole traffic will not be permitted or denied like in standard access-list .
* These are the ACL which uses both source and destination IP address and also the port numbers to distinguish IP traffic. In these type of ACL, we can also mention which IP traffic should be allowed or denied .
* These use range 100-199 and 2000-2699.

**Features –**

1. Extended access-list is generally **applied close to the source** but not always.
2. In Extended access-list, packet filtering takes place on the basis of **source IP address, destination IP address, Port numbers.**
3. In extended access-list, particular services will be **permitted or denied .**
4. Extended ACL is created from 100 **– 199 & extended range 2000 – 2699.**
5. **If numbered with extended Access-list** is used then remember rules can’t be deleted. If one of the rule is deleted then the whole access-list will be deleted.
6. **If named with extended Access-list** is used then we have the flexibility to delete a rule from access-list.

Two steps are required to configure an extended access list:

1. Configure an extended access list using the following command:

(config) access list NUMBER permit|deny IP\_PROTOCOL SOURCE\_ADDRESS WILDCARD\_MASK [PROTOCOL\_INFORMATION] DESTINATION\_ADDRESS WILDCARD\_MASK PROTOCOL\_INFORMATION

192.168.1.0 255.255.255.0 0.0.0.255

2. Apply an access list to an interface using the following command:

(config) ip access-group ACL\_NUMBER in | out

Router R0:

R0(config)#access-list 1 deny host 192.168.2.100

R0(config)#access-list 1 deny host 192.168.2.101

R0(config)#access-list 1 permit any

R0(config)#interface fa0/0

R0(config-if)#ip access-group 1 out

**From 192.168.2.100**

PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.

Reply from 192.168.3.1: Destination host unreachable.

Reply from 192.168.3.1: Destination host unreachable.

Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

**From 192.168.2.102**

PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Reply from 192.168.1.100: bytes=32 time=2ms TTL=126

Reply from 192.168.1.100: bytes=32 time=9ms TTL=126

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 9ms, Average = 3ms

* **Static Routes:**

R1(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.1

R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1

R0(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

R1:

R1#show access-lists

Extended IP access list 100

10 deny ip host 192.168.2.100 192.168.1.0 0.0.0.255 (4 match(es))

20 permit ip any any

R1#show access-lists

Extended IP access list 100

10 deny ip host 192.168.2.100 192.168.1.0 0.0.0.255 (4 match(es))

20 permit ip any any

R1(config)#no access-list 100

R1(config)#access-list 100

% Incomplete command.

Accsss-list 100 deny 192.168.2.100 0.0.0.0

R1(config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.254 ?

dscp Match packets with given dscp value

eq Match only packets on a given port number

established established

gt Match only packets with a greater port number

lt Match only packets with a lower port number

neq Match only packets not on a given port number

precedence Match packets with given precedence value

range Match only packets in the range of port numbers

<cr>

R1(config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.254 eq 80

R1(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

R1(config)#interface fa0/0

R1(config-if)#ip access-group 100 in

R1(config-if)#exit

R1(config)#exit

R1#

%SYS-5-CONFIG\_I: Configured from console by console

R1#show run

Building configuration...

Current configuration : 991 bytes

!

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R1

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface FastEthernet0/0

ip address 192.168.2.1 255.255.255.0

ip access-group 100 in

duplex auto

speed auto

!

interface FastEthernet1/0

no ip address

duplex auto

speed auto

shutdown

!

interface Serial2/0

ip address 192.168.3.2 255.255.255.0

!

interface Serial3/0

no ip address

clock rate 2000000

shutdown

!

interface FastEthernet4/0

no ip address

shutdown

!

interface FastEthernet5/0

no ip address

shutdown

!

ip classless

ip route 192.168.1.0 255.255.255.0 192.168.3.1

ip route 192.168.4.0 255.255.255.0 192.168.3.1

!

ip flow-export version 9

!

!

access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.254 eq www

access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end

R1#config

Configuring from terminal, memory, or network [terminal]?

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

R1(config)#show access-lists

^

% Invalid input detected at '^' marker.

R1(config)#

R1(config)#show access-lists 100

^

% Invalid input detected at '^' marker.

R1(config)#show access-lists 100?

% Unrecognized command

R1(config)#exit

R1#

%SYS-5-CONFIG\_I: Configured from console by console

R1#show access-lists 100

Extended IP access list 100

permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.254 eq www (332 match(es))

permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255 (4 match(es))

**Standard ACL:**

* **Static Routes:**

R0:

Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

R1:

Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1

Otherwise it Shows message :**Destination Unreachable**

**PC0:**

PC>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Reply from 192.168.2.100: bytes=32 time=1ms TTL=126

Reply from 192.168.2.100: bytes=32 time=12ms TTL=126

Reply from 192.168.2.100: bytes=32 time=6ms TTL=126

Reply from 192.168.2.100: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 12ms, Average = 7ms

**PC1:**

PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Reply from 192.168.1.100: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

**Standard Access List:**

* **Steps:**
  1. **Create the standard Access List**
  2. **Apply the access list to an interface (inbound or outbound)**
* **Standard ACL: (1-99)**
* **Applied closest to destination.**

**Router 0:**

Router(config)#

Router(config)#hostname R0

Router(config)#access-list 1 ?

deny Specify packets to reject

permit Specify packets to forward

remark Access list entry comment

Router(config)#access-list 1 deny 192.168.2.101 0.0.0.0 (Wildcard Mask)

If you want to block complete network

Router(config)#access-list 1 deny 192.168.2.0 0.0.0.255 (Wildcard Mask)

Router(config)#access-list permit any

Router(config)#interface se2/0

Router(config-if)#ip access-group ?

<1-199> IP access list (standard or extended)

WORD Access-list name

Router(config)#interface fa0/0

Router(config-if)#ip access-group 1 out