|  |  |
| --- | --- |
| **Practicum Case** |  |
| CPEN6098 | CPEN6108 | CPEN6109  Computer Networks |
| **Computer Engineering** | **O1-CPEN6098-HP01** |
| ***Valid on*** *Even Semester Year 2018/2019* | **Revision 00** |

## Learning Outcomes

* Explain basic concepts of network

## Topic

* Session 05 - Access List

## Sub Topics

* Standard Access List
* Extended Access List
* Review

## Soal

*Case*

Access List is a list that stored in router to control the access to or from router with some available service. Access list determines which user and process system that are granted to access an object with some allowed operations for that object.

Access list has some functions, as follows:

* Limit the network traffic and improves network functionalities. Example, access list blocked the video traffic, so it can reduce the network load and improve the network performance.
* Manage traffic flow. Access list is able to block routing update. If the update is not needed because of network condition, the bandwidth can be saved.
* Capable to give basic security for accessing the network. Example, host A has no right to access the HRD network and host B has right to access that network.
* Disconnect which traffic type to be passed or blocked through router interface. Example, email traffic is served, telnet traffic is blocked.
* Control specific area where client can access network.
* Choose hosts that allowed or blocked when accessing network segment. Example, access list allow or block the FTP or HTTP.

Rules that used to create access list:

* Must have one access list per protocol for each direction.
* Standard access list must be applied to the nearest destination.
* Extended access list must be applied to nearest source.
* Inbound and outbound interface must be viewed from the direction of incoming router port.
* Access statement processed sequentially from top to bottom until it gets the suitable one. If none are match, then packet will be rejected and deleted.
* Have a **deny any** statement at the end of access list. (not visible in the configuration)
* Inputted access list must be sorted from specific to general order. Certain host must be rejected first and next process group then general.
* Suitable condition will be executed first. Allowed or rejected will be executed, if there is a suitable statement.
* Never work with an active access list.
* New row usually added at the end of the access list. **no access-list x** command will delete all list.
* Access list in the IP form will be sent as ICMP message host unreachable to sender and will be deleted.
* Access list must be deleted carefully. Some IOS versions will apply the default **deny any** to interface and all traffic will stop.

Access list is identified by number, although it can be identified by name. That number not only shows the specific access list, but also determines whether it is standard or extended access list.

|  |  |
| --- | --- |
| **Number Range** | **List Type** |
| 0-99 | Regular IP List |
| 100-199 | Extended IP List |

**Standard IP access lists**

* Filter on source address
* Log events (optional)

**Extended IP access lists (standard capabilities plus)**

* Filter on protocol
* Filter on destination address
* Filter on port number (both destination and source)

In TCP/IP, access list can be given to one or more interfaces and can filter the incoming or outgoing traffic using **ip access-group** command at interface configuration mode.

|  |
| --- |
|  |

Step by step to create access list:

1. Create the access list

**access-list 1 deny ip host 192.22.64.98 host 192.22.64.66**

Description:

1 : access list number

deny : access list type

192.22.64.98 : ip source

192.22.64.66 : ip destination

1. Give **permit** **any** access ( because the default at the end of access list is deny any)

**access-list 1 permit ip any any**

1. Go to interface destination

**interface fastEthernet 1/0**

1. Spceified the access control

**ip access-group 1 out**

**Access List Commands**

|  |  |
| --- | --- |
| **Command** | **Description** |
| show access-lists | Displays all access lists and their parameters configured on the router. This command doesn't show which interface the list is configured on. |
| show access-list [list #] | Shows only the parameters for the access list specified. This command does not show you the interface the list is configured on. |
| show ip access-list | Shows only the IP access lists configured on the router. |
| show ip interface | Shows which interfaces have IP access lists on them. |
| show running-config | Shows the access lists and which interfaces have access lists set. |
| any | Keyword used to represent all hosts or networks, replaces 0.0.0.0 255.255.255.255 in access list. |
| host | Keyword that specifies that an address should have a wildcard mask of 0.0.0.0 (i.e will match only 1 host) |
| clear access-list counter [list#] | Clears extended access lists counter of the number of matches per line of the access list. |
| ip access-group | Applies an IP access list to an interface. |

**If you don’t understand, please ask to your assistant!**