Practical 5

Configure IPv6 ACL's

Part 1 - Configure, apply and verify an IPv6 ACL

Step 1 - Configure an ACL that will block HTTP (HTTPS) access

R1(config)# ipv6 access-list BLOCK-HTTP
R1(config-ipv6-acl)# deny tcp any host 2001:088:1:30::3 eq www.
R1(config-ipv6-acl)# deny tcp any host 2001:088:1:30::3 eq 443.

Step 2 - Allow the other IPv6 traffic to pass.

R1(config-ipv6-acl)# permit ipv6 any any

Step 3 - Apply ACL to an interface

R1(config)# interface g0/1
R1(config-if)# ipv6 traffic-filter BLOCK-HTTP in

Step 4 - Verify the ACLs implementation.

a) Open web browser of PC1 to http://2001:088:1:30::3
or
https://2001:088:1:30::130
The website should appear

b) Open the web browser of PC2 to
https://2001:088:1:30::30 or,
http://2001:088:1:30::30
the website should be blocked

a Ping from PC2 to 2001:088:1:30::30

the ping should succeed..

Part 2 - Configure, apply, verify a second IPv6 ACL

Step 1 - create an ACL to block ICMP.

R3(config)# ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)# deny icmp any any
R3(config-ipv6-acl)# permit ipv6 any any

Step 2 - Apply ACL to an interface

R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out

Step 3 - verify the ACL is working

a) Ping from PC1 to 2001:088:1:30::30 should fail
b) Ping from PC2 to 2001:088:1:30::30 should fail
c) Web browser from PC2 to 2001:088:1:30::30. the website should display