Topic 3 ACLs
V1.1

S2 2022

Addressing

- Network 145.60.0.0/16

- VLAN10 Marketing 80
- VLAN20 Sales 50 hosts

- Server Farm 20 hosts

- VLAN99 TechSupport 10 hosts
- Internal Serial Link 2 hosts

- Link to ISP 200.10.10.0/30

- R3 Loopback0 170.20.0.0/16 external site
- External Server Site 150.20.0.0/16

Subnetting Successful

Major Network: **145.60.0.0/16**
Available IP addresses in major network: **65534**
Number of IP addresses needed: **162**
Available IP addresses in allocated subnets: **234**
About **0%** of available major network address space is used
About **69%** of subnetted network address space is used

VLSM

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
VLAN10	80	126	145.60.0.0	/25	255.255.255.128	145.60.0.1 - 145.60.0.126	145.60.0.127
VLAN20	50	62	145.60.0.128	/26	255.255.255.192	145.60.0.129 - 145.60.0.190	145.60.0.191
Server Farm	20	30	145.60.0.192	/27	255.255.255.224	145.60.0.193 - 145.60.0.222	145.60.0.223
VLAN99	10	14	145.60.0.224	/28	255.255.255.240	145.60.0.225 - 145.60.0.238	145.60.0.239
Internal Serial	2	2	145.60.0.240	/30	255.255.255.252	145.60.0.241 - 145.60.0.242	145.60.0.243

Extended Named ACL For VLAN 10 on R1

1) Addresses

ISP Packet Tracer Server0 150.20.0.2
VLAN 10 145.60.0.0 /25 Mask 255.255.255.128 Wildcard (inverse of mask) 0.0.0.127

2) Rules for VLAN 10

Rule 1 - Deny ONLY HTTP access to ISP Packet Tracer Server0
Rule 2 - Permit ALL other access to ISP Packet Tracer Server0

3) ACL for VLAN 10

```
ip access-list extended ACLVLAN10
deny tcp 145.60.0.0 0.0.0.127 host 150.20.0.2 eq 80
permit ip any any
```

4) ACL Placement for VLAN 10

```
interface G0/0/1.10
ip access-group ACLVLAN10 in
```

Extended Named ACL For VLAN 20 on R1

1) Addresses

ISP Packet Tracer Server0 150.20.0.2
VLAN 20 145.60.0.128/26 Mask 255.255.255.192 Wildcard (inverse of mask) 0.0.0.63

2) Rules for VLAN 20

Rule 1 - Permit ONLY HTTP access to ISP Packet Tracer Server0
Rule 2 - Deny ALL other access to ISP Packet Tracer Server0
Rule 3 - Permit ALL other access

3) ACL for VLAN 20

ip access-list extended ACLVLAN20
permit tcp 145.60.0.128 0.0.0.63 host 150.20.0.2 eq 80
deny ip 145.60.0.128 0.0.0.63 host 150.20.0.2
permit ip any any

4) ACL Placement for VLAN 20

interface G0/0/1.**20**
ip access-group ACLVLAN**20** in

Extended Named ACL Structure

- **deny|permit *protocol* *source ip* *source wildcard* [operator operand] destination ip destination wildcard [operator operand]**
  - **protocol**
    - **ip** – Matches all protocols (includes IP,TCP, UDP, ICMP etc.)
    - **icmp** – Matches ICMP protocol
    - **tcp** – Matches TCP protocol
    - **udp** – Matches UDP protocol
  - **Source ip source wildcard**
    - Matches packet source IP Address
  - **Destination ip destination wildcard**
    - Matches packet destination IP Address

Extended Named ACL Structure

operator

- **eq, neq** – Port number equal or not equal to specified **operand**
- **lt, gt** – Port number less or greater than specified **operand**

and

operand

- Integer port number eg **80**, **20**, **23**
- Text representation of service name eg. **http**, **ftp**, **telnet**

Extended Named ACL

Create the ACL in Notepad, then paste into router config mode

no ip access-list extended ACLVLANXXX (Delete previous version of the ACL for VLAN XXX)

Ip access-list extended ACLVLANXXX (Self-documenting, the ACL for VLAN XXX, ! means comment)

ACL Case Sensitivity

- ACL names are case sensitive eg aclvlan70 and AclVlan70 are **different** ACLs
- Should decide to use either all uppercase - ACLVLAN70 or all lowercase – aclvlan70 names to reduce errors

ACL Rule Order

- ACL rules in the access list should be in order of most specific to least specific
- The last rule should be permit All other access

ACL Placement Rule

- Extended ACL – place as close as possible to source network or device, to block traffic early to reduce network congestion

Extended Named ACL Trouble Shooting

It is important to verify that the **ACL rules** actually work as intended, refer to the **steps** below:

1. Use show access-lists

- If all rules tested **go to 5**
- Else Identify which rule you want to test

2. Use clear access-list counters

- Clear any counts against the rules

3. Go to PC in VLAN<Id> perform test eg **Ping**, **Telnet**, **Browser** etc to trigger a match with the identified rule

4. Use show access-lists

Was the identified rule matched ?

- Yes – rule action correct, Repeat process, **go to 1**
- No – Debug
  - Was another rule matched ?
  - Where no rules matched ?
  - Check syntax and order of rules – make changes – Repeat process **go to 1**

5. Trouble Shooting completed

Standard Named ACL – Telnet Remote Access to R2

1) Addresses

VLAN 10 145.60.0.0 /25 Mask 255.255.255.128 Wildcard (inverse of mask) 0.0.0.127
VLAN 20 145.60.0.128/26 Mask 255.255.255.192 Wildcard (inverse of mask) 0.0.0.63
R2 S0/1/0 IP Address 145 .60.0.242

2) Rules for VLAN 10

Rule 1 - Deny Telnet Access to R2

3) Rules for VLAN 20

Rule 1 – Permit Telnet Access to R2

4) Configuration on R2

```
ip access-list standard ACLTELNETACCESS
! VLAN 10
deny 145.60.0.0 0.0.0.127
! VLAN 20
permit 145.60.0.128 0.0.0.63
```

5) ACL Placement on R2

```
line vty 0 4
  password cisco ←----------
  login
  access – class ACLTELNETACCESS in
```

i

Standard Named ACL

Create the ACL in Notepad, then paste into router config mode

no ip access-list standard **ACLTELNETACCESS**
! (Delete previous version of the ACL)
Ip access-list standard **ACLTELNETACCESS**
! (Self-documenting, the ACL for Telnet Access , ! means comment)

ACL Case Sensitivity

- ACL names are case sensitive
- Should decide to use either all uppercase or all lowercase names to reduce errors

ACL Rule Order

- ACL rules in the access list should be in order of most specific to least specific
- The last rule should be permit All other access

ACL Placement Rule

- Standard ACL – place as close as possible to destination network or device, to avoid unnecessarily blocking traffic