



# Security In Computing Practical's

## Objectives

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
- Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN

## Scenario

A company's network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15.

## Part 1: Configure Switch/Router

### Step 1: Configure secret

Execute command on all switches/router

```
SW/R1(config)# enable secret enpa55
```

### Step 2: Configure console password

Execute command on all switches/router

```
SW/R1(config)# line console 0
```

```
SW/R1(config-line)# password conpa55
```

```
SW/R1(config-line)# login
```

### Step 3: Configure SSH login

Execute command on all switches/router

```
SW/R1(config)# ip domain-name ccnasecurity.com
```

```
SW/R1(config)# username admin secret adminpa55
```

```
SW/R1(config)# line vty 0 4
```

# Security In Computing Practical's

SW/R1(config-line)# login local

SW/R1(config-line)# crypto key generate rsa

How many bits in the modulus [512]: 1024

## Part 2: Create VLAN and assign access mode and trunk mode to interfaces

### Step 1: Check existing VLAN

Execute command on all switches

SW# show vlan brief

### Step 2: Create new VLAN

Execute command on all switches

SW(config)# vlan 5

SW(config-vlan) # exit

SW(config)# vlan 10

SW(config-vlan) # exit

SW(config)# vlan 15

SW(config-vlan) # exit

### Step 3: Check the new VLAN

Execute command on all switches

SW# show vlan brief

### Step 4: Assign access mode to VLAN switch interfaces

Execute command on switches SWA/SWB

SWA(config)# int fa0/2

SWA(config-if)# switchport mode access

# Security In Computing Practical's

```
SWA(config-if)# switchport access vlan 10
```

```
SWA(config)# int fa0/3
```

```
SWA(config-if)# switchport mode access
```

```
SWA(config-if)# switchport access vlan 10
```

```
SWA(config)# int fa0/4
```

```
SWA(config-if)# switchport mode access
```

```
SWA(config-if)# switchport access vlan 5
```

```
SWB(config)# int fa0/1
```

```
SWB(config-if)# switchport mode access
```

```
SWB(config-if)# switchport access vlan 5
```

```
SWB(config)# int fa0/2
```

```
SWB(config-if)# switchport mode access
```

```
SWB(config-if)# switchport access vlan 5
```

```
SWB(config)# int fa0/3
```

```
SWB(config-if)# switchport mode access
```

```
SWB(config-if)# switchport access vlan 5
```

```
SWB(config)# int fa0/4
```

```
SWB(config-if)# switchport mode access
```

```
SWB(config-if)# switchport access vlan 10
```

## Step 5: Check the access mode allocations

```
SWA# show vlan brief
```

```
SWB# show vlan brief
```

## Step 6: Assign trunk mode to other switch interfaces

```
SWA(config)# int fa0/24
```

# Security In Computing Practical's

```
SWA(config-if)# switchport mode trunk
```

```
SWA(config-if)# switchport trunk native vlan 15
```

```
SWB(config)# int fa0/24
```

```
SWB(config-if)# switchport mode trunk
```

```
SWB(config-if)# switchport trunk native vlan 15
```

```
SW1(config)# int fa0/24
```

```
SW1(config-if)# switchport mode trunk
```

```
SW1(config-if)# switchport trunk native vlan 15
```

```
SW1(config)# int gig0/1
```

```
SW1(config-if)# switchport mode trunk
```

```
SW1(config-if)# switchport trunk native vlan 15
```

```
SW2(config)# int fa0/24
```

```
SW2(config-if)# switchport mode trunk
```

```
SW2(config-if)# switchport trunk native vlan 15
```

```
SW2(config)# int gig0/1
```

```
SW2(config-if)# switchport mode trunk
```

```
SW2(config-if)# switchport trunk native vlan 15
```

```
Central(config)# int range gig0/1-2
```

```
Central(config-if-range)# switchport mode trunk
```

```
Central(config-if-range)# switchport trunk native vlan 15
```

```
Central(config)# int fa0/1
```

```
Central(config-if)# switchport mode trunk
```

```
Central(config-if)# switchport trunk native vlan 15
```

# Security In Computing Practical's

## Step 7: Check the trunk mode allocations

Central# show int trunk

SW1/2# show int trunk

SWA/B# show int trunk

## Step 8: Create sub-interfaces on router to support VLAN

R1(config)# int gig0/0.1

R1(config - subif)# encapsulation dot1q 5

R1(config - subif)# ip address 192.168.5.100 255.255.255.0

R1(config)# int gig0/0.2

R1(config - subif)# encapsulation dot1q 10

R1(config - subif)# ip address 192.168.10.100 255.255.255.0

R1(config)# int gig0/0.15

R1(config - subif)# encapsulation dot1q 15

R1(config - subif)# ip address 192.168.15.100 255.255.255.0

## Part 3: Verify Connectivity

### Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).

C2> ping 192.168.10.2

(Successful)

### Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

PC2> ping 192.168.5.2

(Successful)

# Security In Computing Practical's

## Part 4: Create a Redundant Link between SW-1 and SW-2

### Step 1: Connect SW-1 and SW-2.

Using a crossover cable, connect port Fa0/23 on SW-1 to port Fa0/23 on SW-2.

### Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

(Execute command on SW- 1 and SW-2)

```
SW1/2(config)# int fa0/23
```

```
SW1/2(config-if)# switchport mode trunk
```

```
SW1/2(config-if)# switchport trunk native vlan 15
```

```
SW1/2(config-if)# switchport nonegotiate
```

## Part 5: Enable VLAN 20 as a Management VLAN

### Step 1: Enable a management VLAN (VLAN 20) on SW-A.

```
SW-A(config)# vlan 20
```

```
SW-A(config-vlan)# exit
```

```
SW-A(config)# int vlan 20
```

```
SW-A(config-if)# ip address 192.168.20.1 255.255.255.0
```

### Step 2: Enable the same management VLAN on all other switches

(Execute command on SW-B, SW-1, SW-2, and Central)

```
SW(config)# vlan 20
```

```
SW(config-vlan)# exit
```

***Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.***

```
SW-B(config)# int vlan 20
```

```
SW-B(config-if)# ip address 192.168.20.2 255.255.255.0
```

# Security In Computing Practical's

```
SW-1(config)#int vlan 20
```

```
SW-1(config-if)#ip address 192.168.20.3 255.255.255.0
```

```
SW-2(config)#int vlan 20
```

```
SW-2(config-if)#ip address 192.168.20.4 255.255.255.0
```

```
Central(config)# int vlan 20
```

```
Central(config-if)# ip address 192.168.20.5 255.255.255.0
```

## **Step 3: Connect and configure the management PC.**

*Connect the management PC using copper straight-through to SW-A port Fa0/1 and ensure that it is assigned an available IP address 192.168.20.50*

## **Step 4: On SW-A, ensure the management PC is part of VLAN 20.**

```
SW-A(config)# int fa0/1
```

```
SW-A(config)# switchport mode access
```

```
SW-A(config-if)# switchport access vlan 20
```

## **Step 5: Verify connectivity of the management PC to all switches.**

```
C1> ping 192.168.20.1 (SW-A)
```

(Successful)

```
C1> ping 192.168.20.2 (SW-B)
```

(Successful)

```
C1> ping 192.168.20.3 (SW-1)
```

(Successful)

```
C1> ping 192.168.20.4 (SW-2)
```

(Successful)



# Security In Computing Practical's

C1> ping 192.168.20.5 (Central)

(Successful)

## Part 6: Enable the Management PC to Access Router R1

### Step 1: Enable a new subinterface on router R1.

```
R1(config)# int gig0/0.3
```

```
R1(config-subif)# encapsulation dot1q 20
```

```
R1(config-subif)# ip address 192.168.20.100 255.255.255.0
```

### Step 2: Set default gateway in management PC.

C1 – 192.168.20.100

### Step 3: Verify connectivity between the management PC and R1.

C1> ping 192.168.20.100

(Successful)

### Step 4: Enable security.

```
R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255
```

```
R1(config)# access-list 101 permit ip any any
```

```
R1(config)# access-list 102 permit ip host 192.168.20.50 any
```

### Step 5: Apply ACL on correct interfaces

```
R1(config)# int gig0/0.1
```

```
R1(config-subif)# ip access-group 101 in
```

```
R1(config-subif)# int gig0/0.2
```

```
R1(config-subif)# ip access-group 101 in
```

```
R1(config-subif)# line vty 0 4
```

# Security In Computing Practical's

R1(config-line)# access-class 102 in

## Step 6: Verify connectivity between the management PC and SW-A, SW-B and R1

C1> ping 192.168.20.1 (SW-A)

(Successful)

C1> ping 192.168.20.2 (SW-B)

(Successful)

C1> ping 192.168.20.100 (R1)

(Successful)

## Step 7: Verify connectivity between the D1 and management PC.

D1>ping 192.168.20.50

(Unsuccessful – Destination host unreachable)

