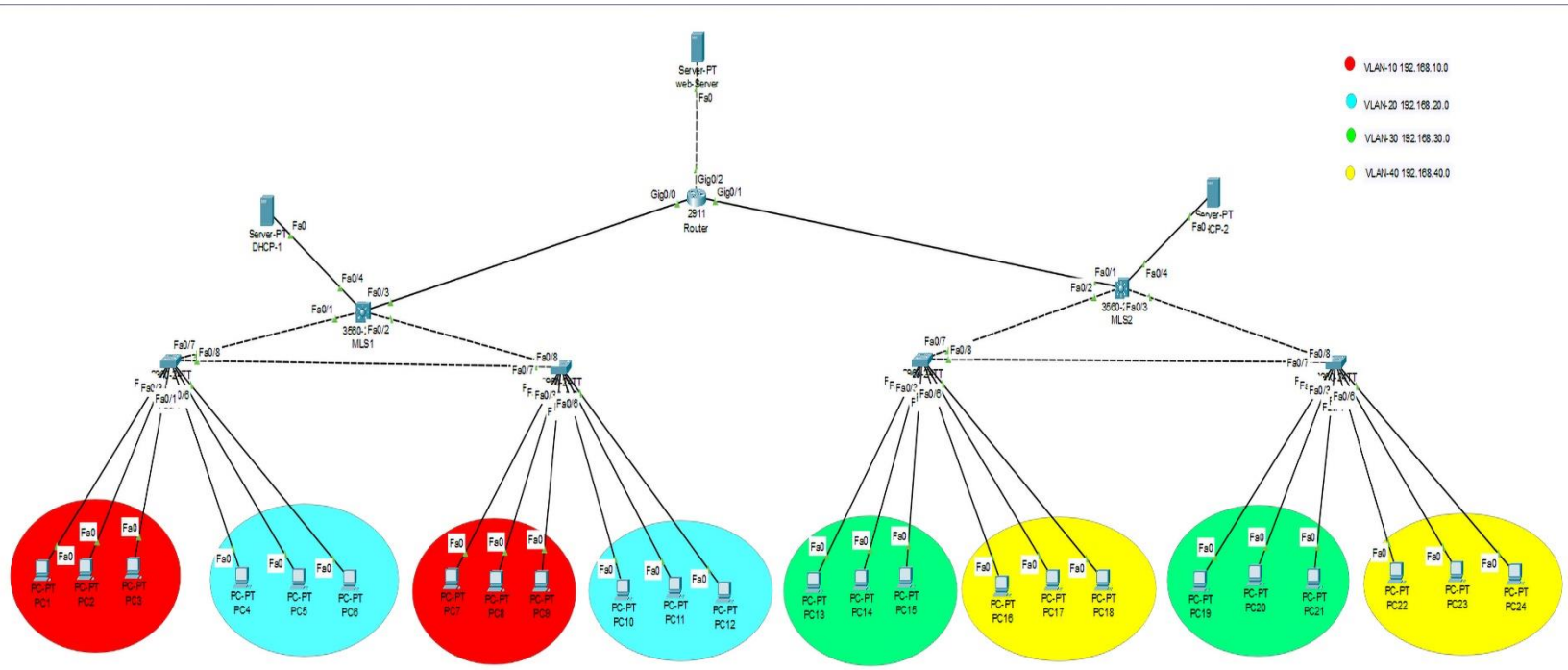
Secure a Network Using Cisco Security Features



Overview

The goal is to ensure efficient communication between different VLANs while maintaining security through various mechanisms such as

1- ACLs
2- DHCP Snooping
3- Dynamic ARP Inspection (DAI)
4- Port Security
5- IP source guard

And

1- Disable CDP on ports connected to end device
2- use NTP
3- SSH
4- Make passwords

VLAN and IP Assignments

1. **VLAN 10:**
    - **Switch 1:** Ports f0/1-3
    - **Switch 2:** Ports f0/1-3
    - **Subnet:** 192.168.10.0/24
2. **VLAN 20:**
    - **Switch 1:** Ports f0/4-6
    - **Switch 2:** Ports f0/4-6
    - **Subnet:** 192.168.20.0/24
3. **VLAN 30:**
    - **Switch 3:** Ports f0/1-3
    - **Switch 4:** Ports f0/1-3
    - **Subnet:** 192.168.30.0/24
4. **VLAN 40:**
    - **Switch 3:** Ports f0/4-6
    - **Switch 4:** Ports f0/4-6
    - **Subnet:** 192.168.40.0/24

DHCP Servers

- **On VLAN 100 : IP Address:** 192.168.100.2

  -VLAN 10 pool :

  Default-gateway: 192.168.10.1

  Start IP: 192.168.10.4

  Subnet-Mask: 255.255.255.0

  Maximum number of users : 32

  -VLAN 20 pool :

  Default-gateway: 192.168.20.1

  Start IP: 192.168.20.4

  Subnet-Mask: 255.255.255.0

  Maximum number of users : 32

- **On VLAN 101 : IP Address:** 192.168.101.2

  -VLAN 30 pool :

  Default-gateway: 192.168.30.1
  Start IP: 192.168.30.4

  Subnet-Mask: 255.255.255.0

  Maximum number of users : 32

  -VLAN 40 pool :

  Default-gateway: 192.168.40.1

  Start IP: 192.168.40.4

  Subnet-Mask: 255.255.255.0
  Maximum number of users : 32

Management VLANs (SSH Access)

- **VLAN 5:** Switch 1 SSH - IP Address: 192.168.5.2

- **VLAN 6:** Switch 2 SSH - IP Address: 192.168.6.2
- **VLAN 7:** Switch 3 SSH - IP Address: 192.168.7.2
- **VLAN 8:** Switch 4 SSH - IP Address: 192.168.8.2

Loopback Addresses for SSH

- **MLS1 Loopback:** SSH IP Address: 192.168.2.1
- **MLS2 Loopback:** SSH IP Address: 192.168.3.1
- **Router Loopback:** SSH IP Address: 192.168.4.1

Interconnect Networks

- **Between MLS1 and Router:** Subnet 10.10.10.0/24
- **Between MLS2 and Router:** Subnet 10.10.20.0/24
- **Router and Web Server:**
    - **Router IP:** 30.0.0.1
    - **Web Server IP:** 30.0.0.2

Router IDs

- **MLS1 Router ID:** 50.0.0.1
- **MLS2 Router ID:** 60.0.0.1
- **Main Router ID:** 70.0.0.1

OSPF

- **OSPF Configuration** between MLS1, Router and MLS2.

Default static route:

Configured for potential future use : serial0/0/0 is used

VLANs and routing:

SW1(config)#vlan 10

SW1(config)#vlan 20

SW1(config)#vlan 5

SW1(config)#ip default-gateway 192.168.5.1

SW1(config)#int vlan 5

SW1(config-if)#ip address 192.168.5.2 255.255.255.0

SW1(config)#interface range f0/1-3

SW1(config-if-range)#switchport mode access

SW1(config-if-range)#switchport access vlan 10

SW1(config)#interface range f0/4-6

SW1(config-if-range)#switchport mode access

SW1(config-if-range)#switchport access vlan 20

SW1(config)#interface range f0/7-8

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

Apply similar configurations on SW2 but on SW3,4 change vlans

MLS1(config)#ip routing

MLS1 (config)#vlan 5

MLS1 (config)#vlan 6

```
MLS1(config)#vlan 10
MLS1(config)#vlan 20
MLS1(config)#vlan 100
MLS1(config)#int vlan 5
MLS1(config-if)#ip address 192.168.5.1 255.255.255.0
MLS1(config)#int vlan 6
MLS1(config-if)#ip address 192.168.6.1 255.255.255.0
MLS1(config)#int vlan 10
MLS1(config-if)#ip address 192.168.10.1 255.255.255.0
MLS1(config-if)#ip helper-address 192.168.100.2
MLS1(config)#no shutdown
MLS1(config-if)#int vlan 20
MLS1(config-if)#ip address 192.168.20.1 255.255.255.0
MLS1(config-if)#ip helper-address 192.168.100.2
MLS1(config-if)#no shutdown
MLS1(config-if)#int vlan 100
MLS1(config-if)#ip address 192.168.100.1 255.255.255.0
MLS1(config-if)#int f0/4
MLS1(config-if)#switchport mode access
MLS1(config-if)#switchport access vlan 100
MLS1(config-if)#int rang f0/1-2
MLS1(config-if-range)#switchport mod trunk
MLS1(config-if)#int loopback 1
MLS1(config-if)#no shutdown
MLS1(config-if)#ip address 192.168.2.1 255.255.255.0
MLS1(config-if-range)#int f0/3
MLS1(config-if)#no switchport
```

MLS1(config-if)#ip address 10.10.10.2 255.255.255.0

MLS1(config-if)#no shutdown

Apply similar configurations on MLS2 but change vlans and ip

OSPF

MLS1(config)#router ospf 1

MLS1(config-router)#router-id 50.0.0.1

MLS1(config-router)#network 192.168.5.0 0.0.0.255 area 0

MLS1(config-router)#network 192.168.6.0 0.0.0.255 area 0

MLS1(config-router)#network 192.168.10.0 0.0.0.255 area 0

MLS1(config-router)#network 192.168.20.0 0.0.0.255 area 0

MLS1(config-router)#network 192.168.2.0 0.0.0.255 area 0

MLS1(config-router)#network 10.10.10 0   0.0.0.255 area 0

Apply similar configurations on MLS2 and Router but by its networks

Default Static Route:

MLS1(config)#ip route 0.0.0.0   0.0.0.0 f0/3

MLS2(config)#ip route 0.0.0.0   0.0.0.0 f0/1

Security Configuration

DHCP Snooping

To mitigate the risk of rogue DHCP servers, DHCP Snooping is enabled on the layer 2 switches:

- **SW4 Configuration:**

SW4(config)#ip dhcp snooping

SW4(config)#ip dhcp snooping vlan 30,40

SW4(config)#int f0/7

SW4(config-if)#ip dhcp snooping trust

SW4(config)#int range f0/1-6

SW4(config-if-range)#ip dhcp snooping limit rate 4

SW4(config)#no ip dhcp snooping information option

- **Repeat similar configuration for SW1,SW2,SW3**

MLS DHCP Snooping

On the MLS:

MLS2(config)#ip dhcp snooping

MLS2(config)#ip dhcp snooping vlan 30,40,101

MLS2(config)#int f0/4

MLS2(config-if)#ip dhcp snooping trust

Apply similar configurations on MLS1

Dynamic ARP Inspection (DAI)

Enable ARP Inspection based on the DHCP Snooping Binding Table to prevent ARP spoofing attacks:

SW1(config)#ip arp inspection vlan 10,20

SW4(config)#ip arp inspection vlan 30,40

Apply similar configurations on SW2 and SW3.

NTP Configuration

Enable Network Time Protocol (NTP) to ensure time synchronization across devices:

Router(config)#ntp master 1

Router# clock set hh:mm:ss Day Month Year

…….

SW1(config)#ntp server [Router Loopback IP]

Repeat similar configuration for all network devices

Port Security Configuration

Implement Port Security to limit the number of MAC addresses per port:

SW1(config)#int range f0/1-6

SW1(config-if-range)#switchport port-security

SW1(config-if-range)#switchport port-security maximum 1

SW1(config-if-range)#switchport port-security mac-address sticky

SW1(config-if-range)#switchport port-security violation shutdown

- **Repeat for SW2, SW3, and SW4.**

ACL Configurations

1. **Only permit vlan10 to access other devices via ssh**

   SW1(config)#ip access-list extended ssh

SW1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 22

SW1(config-ext-nacl)#den tcp any any eq 22

SSW1(config-ext-nacl)#permit ip any any

Apply ACL to VLAN interfaces:

SW1(config)#line vty 0 4

SW1(config-line)#access-class ssh in

- **Apply similar configurations on all network devices**

2. ### Deny VLAN 30 from Reaching Web Server

MLS2(config)#ip access-list extended deny-vlan30-web

MLS2(config-ext-nacl)#deny tcp 192.168.30.0 0.0.0.255 host 30.0.0.2 eq 80

MLS2(config-ext-nacl)#deny tcp 192.168.30.0 0.0.0.255 host 30.0.0.2 eq 443

MLS2(config-ext-nacl)#permit ip any any

Apply ACL to VLAN 30 interface:

MLS2(config)#int vlan 30

MLS2(config-if)#ip access-group deny-vlan30-web in

Additional Configurations

CDP Configuration

Disable CDP on selected interfaces to enhance security:

SW1(config)#int range f0/1-6

SW1(config-if-range)#no cdp enable

- **Repeat for SW2, SW3, SW4, and Router g0/2.**

Passwords:

SW4(config)#enable secret Cisco2@#

SW4(config)#line console 0

SW4(config-line)#password Cisco1@#

SW4(config-line)#login

SW4(config)#service password-encryption

Apply similar configurations on all network devices

SSH

SW4(config)#username cisco secret Cisco3@#

SW4(config)#ip domain-name cisco.com

SW4(config)#crypto key generate rsa

1024

SW4(config)#line vty 0 4

SW4(config-line)#login local

SW4(config-line)#transport input ssh

Apply similar configurations on all network devices

IP Source Guard

To prevent IP spoofing, enable IP Source Guard on access ports:

```
SW1(config)#int range f0/1-6
SW1(config-if-range)#ip verify source
```