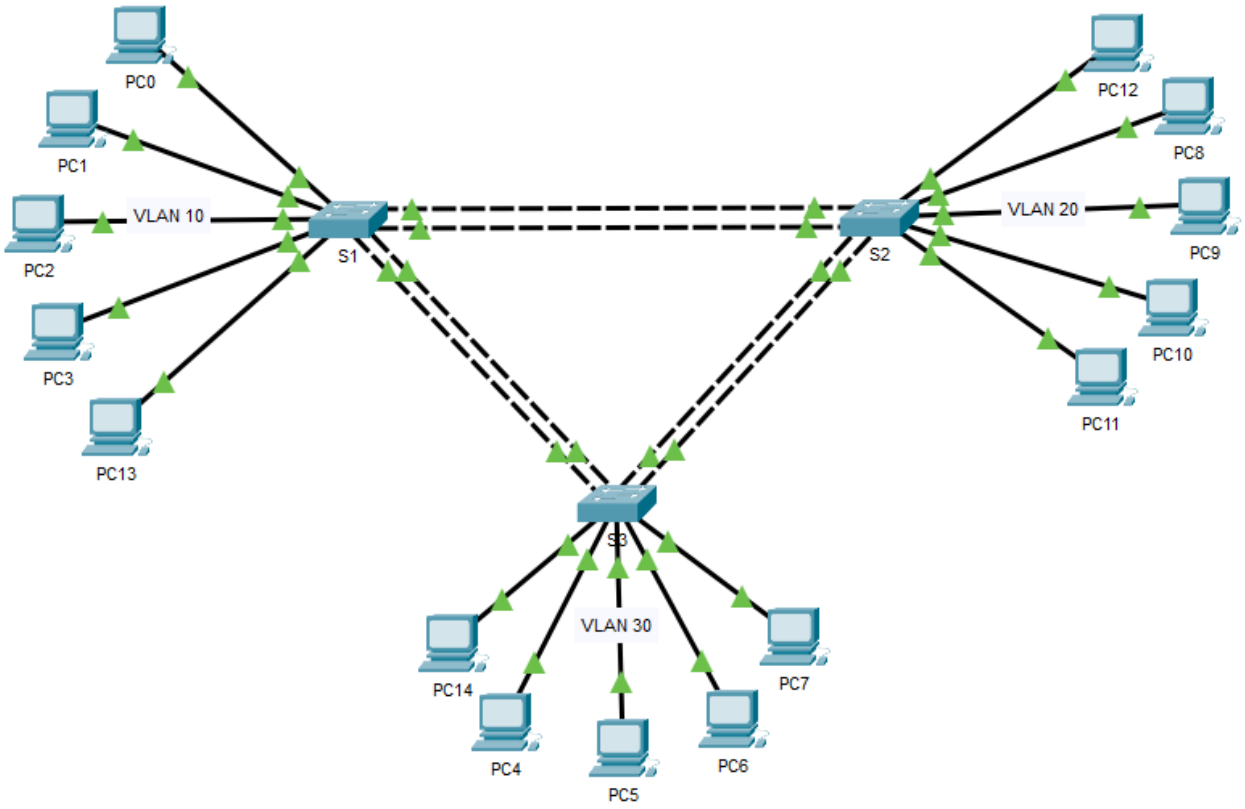
2024

Switchport Nonegotiate, Disable CDP

VLAN HOPING ATTACKS PREVENTION

INACIO ANDRE



- DTP, Dynamic Trunking Protocol, is a trunking protocol that is developed and proprietary to Cisco which is used to automatically negotiate trunks between Cisco switches. Trunk negotiations are managed by DTP only if the port is directly connected to each other.

- Ethernet trunk interfaces support various trunking modes. Those interfaces can be configured as a trunk or non-trunk, or to initiate negotiating trunking to a neighbor interface or is waiting to receive a trunking negotiation message from another directly connected interface. Most Cisco switches nowadays use IEEE 802.1Q as their trunking type of choice because of less overhead compared to Inter-Switch Link (ISL).

- DTP, Dynamic Trunking Protocol, negotiation involves the exchange of DTP frames between two neighboring interfaces. When an interface is configured in switchport dynamic auto or dynamic desirable modes, it will initiate DTP negotiation in order to select its own trunking operational mode.

- When an interface is statically configured in access mode or trunk mode, it will normally participate in the DTP process by responding to DTP frames if it receives any.

S1

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#vlan 10
S1(config-vlan)#name IT-Dept
S1(config-vlan)#exit
S1(config)#vlan 50
S1(config-vlan)#name NATIVE
S1(config-vlan)#exit
S1(config)#int range f0/1-20, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#switchport nonegotiate
S1(config-if-range)#exit
S1(config)#int range f0/21-24
S1(config-if-range)#switchport mode trunk
```

```
S1(config-if-range)#switchport trunk native vlan 50
S1(config-if-range)#switchport nonegotiate
S1(config-if-range)#exit
S1(config)#no cdp run
S1(config)#do wr
```

S2

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#vlan 20
S2(config-vlan)#name FIN-Dept
S2(config-vlan)#exit
S2(config)#vlan 50
S2(config-vlan)#name NATIVE
S2(config-vlan)#exit
S2(config)#int range f0/1-20, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#switchport nonegotiate
S2(config-if-range)#exit
S2(config)#int range f0/21-24
S2(config-if-range)#switchport mode trunk
```

```
S2(config-if-range)#switchport trunk native vlan 50
S2(config-if-range)#switchport nonegotiate
S2(config-if-range)#exit
S2(config)#no cdp run
S2(config)#do wr
```

S3

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#vlan 30
S3(config-vlan)#name ACC-Dept
S3(config-vlan)#exit
S3(config)#vlan 50
S3(config-vlan)#name NATIVE
S3(config-vlan)#exit
S3(config)#int range f0/1-20, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#switchport nonegotiate
S3(config-if-range)#exit
S3(config)#int range f0/21-24
S3(config-if-range)#switchport mode trunk
```

```
S3(config-if-range)#switchport trunk native vlan 50
S3(config-if-range)#switchport nonegotiate
S3(config-if-range)#exit
S3(config)#no cdp run
S3(config)#do wr
```

```
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
```

```
no cdp run
!
!
!
!
line con 0
!
```