Draft Documentation

The research paper I have used could unfortunately not be isolated from the journal, here is the citation and the page no. would be 81.
Virtual Local Area Network (VLAN): Segmentation and Security Abbas Mehdizadeha Kevin Suinggia Mojtaba Mohammadpoorb Harlina Haruna aDept. of Computing, Nilai University, 71800 Putra Nilai, Negeri Sembilan, Malaysia. bDept. of Computer & Electrical Eng., University of Gonabad, Gonabad, Iran. mehdiizadeh@ieee.org, kevingizxc@gmail.com, mohammadpur@gonabad.cac.ir, harlina@nilai.edu.my

Configuring VLANs

Here I will document all the steps that I take. I will be using Cisco Packet Tracer for the project.

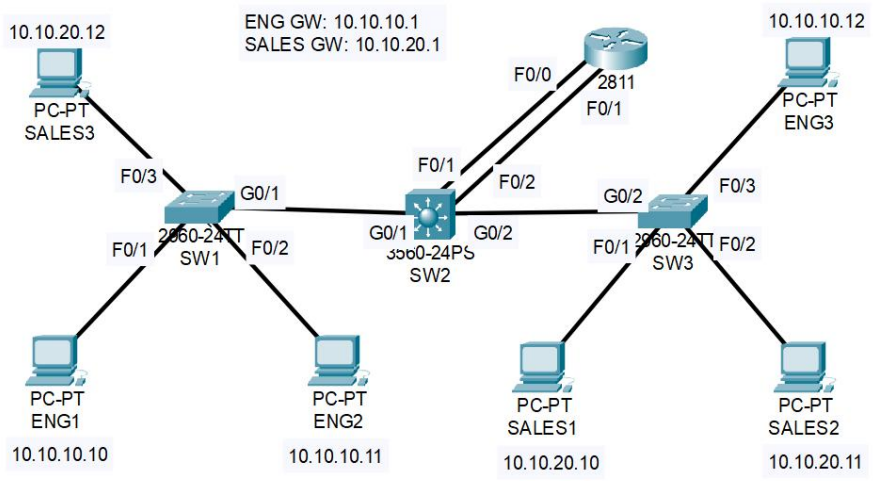


Fig 1

Step 1:
The switches and routers should all be in default state and have no vlans configured but I will still check using the command:
Show vlan brief

Step 2:
View the switchport status on the link from SW1 to SW2
Show int g0/1 switchport
We see that the trunking mode is set to dynamic auto and the interface is currently in the access port operational mode using the default vlan1.

Step 3:
Configure the links between switches as trunks

On SW1
Int g0/1
Switch mode trunk
On SW2
Int g0/1
Switch trunk encap dot1q
Switch mode trunk
Int g0/1
Switch trunk encap dot1q
Switch mode trunk
On SW3
Int g0/2
Switch mode trunk

Here to prevent **VLAN Hopping,**
Int g0/1
Switchport non negotiate

This disables DTP and prevents attackers from negotiating a trunk link.
We will also shut down all unused ports to access mode and disable them . This makes sure they are not exploited.
Interface range f0/5-24
switchport mode access
shutdown
exit

Step 4
Configure SW1 as a VTP server in vtp domain Project

On SW1
Vtp domain Project
Vtp mode server

Step 5
For additional security, SW2 must not synchronise its VLAN database with SW1
On SW2
Vtp mode transparent

Step 6
SW3 must learn information from SW1 but it should be edited on SW3 for security
Vtp mode client
Vtp domain Project

Step 7
Add engg, sales and native vlans on all switches
They only need to be configures on SW1 and SW2 as SW3 is a client
On SW1

Vlan 10
Name eng
Vlan 20
Name sales
Vlan 199
Name native

```
SW2(config-vlan)#do sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   eng                              active
20   sales                            active
199  native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW2(config-vlan)#
```

Then verify the vlan databases on each switch
Using
Sh vlan brief

For **ARP spoofing mitigation,**
ip dhcp snooping
ip dhcp snooping vlan 10,20
exit

Step 8
Configure the trunk links to use vlan 199 as the native vlan for better security against VLAN hopping. This prevents attackers from exploiting VLAN 1 as a default native vlan.

On SW1
Int g0/1
Switch trunk native vlan 199

On SW2
Int g0/1
Switch trunk native vlan 199
Int g0/2
Switch trunk native vlan 199

On SW3
Int g0/2
Switch trunk native vlan 199

Also enable arp inspection on all,
Ip arp inspection vlan 10,20

Also mark trusted interfaces on the router;
Interface g0/1

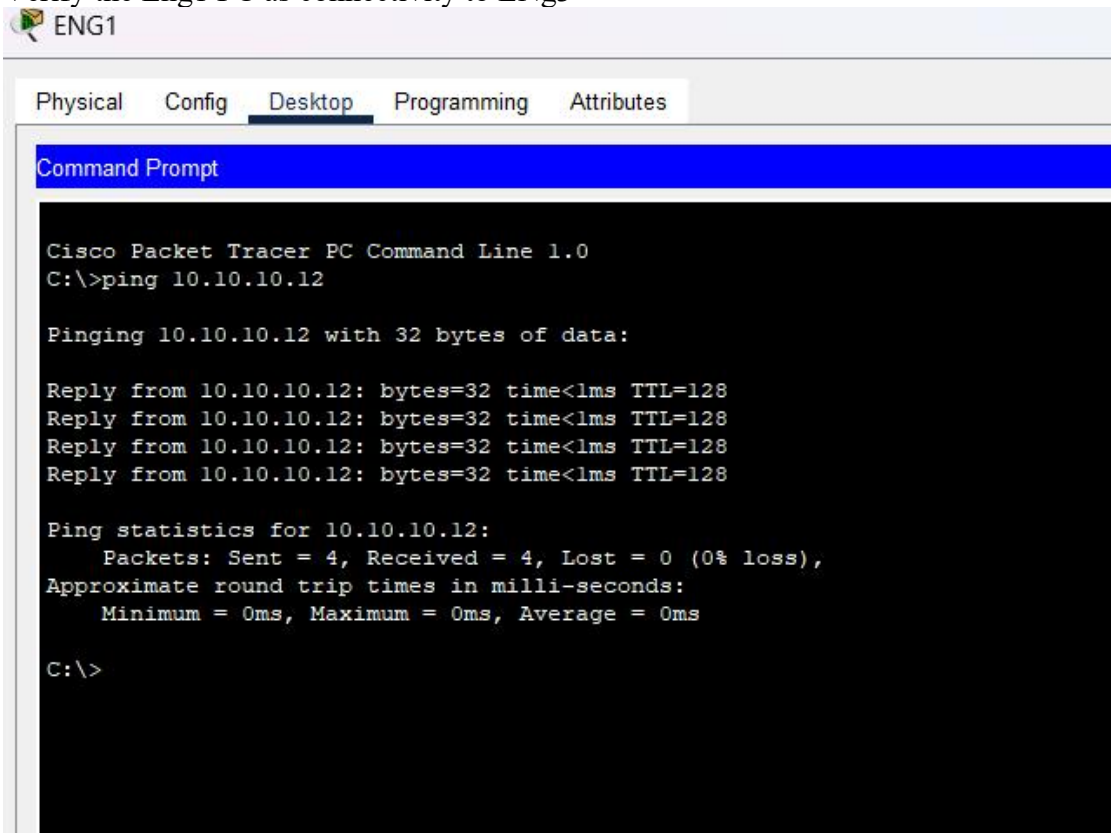
ip dhcp snooping trust
ip arp inspection trust
exit

Step 10:
Configure the switchports connected to PCs with the correct vlan config

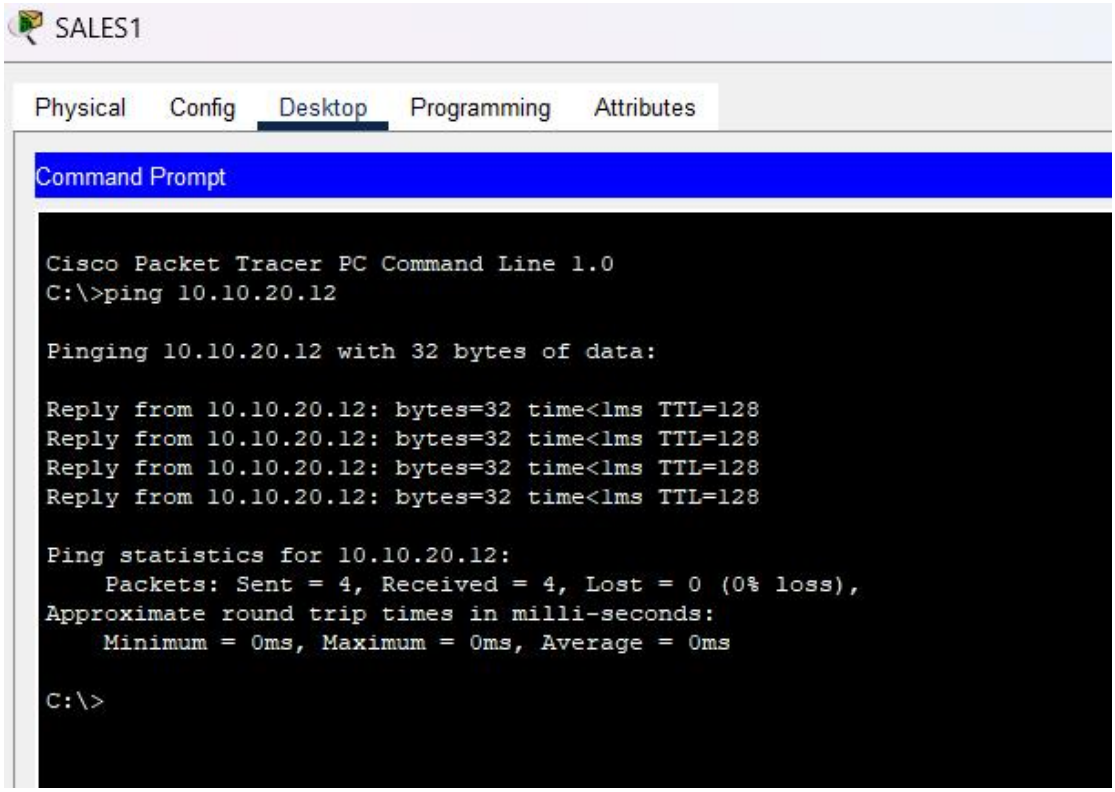
Eng PCs should be in vlan 10 and sales PCs should be in vlan 20

On SW1
Int range f0/1-2
Switchport mode access
Switch access vlan 10
Int f0/3
Switch mode access
Switch access vlan 20
On SW3
Int range f0/1-2
Switchport mode access
Switch access vlan 20
Int f0/3
Switch mode access
Switch access vlan 10

Step 11:
Verify the Eng1 PC as connectivity to ENg3



Step 12
Verify the Sales1 PC as connectivity to Sales3



Inter- VLAN routing: Separate interfaces on router

1. Configure interface f0/0 on r2 as the default gatway for eng pcs
On R1
Int f0/0
Ip add 10.10.10.1 255.255.255.0
No shut
2. Configure interface f0/1 on r2 as the default gatway for salespcs
On R1
Int f0/1
Ip add 10.10.20.1 255.255.255.0
No shut
3. Configure sw2 to support inter-vlan routing using r1 as the default gatway.
Int f0/1
Switchport mode access
Switchport access vlan 10
Int f0/2
Switchport mode access
Switchport access vlan 20

4. Verify the eng1 pc has connectivity to the vlan 20 int on R1

Here, I encountered a problem where the ping was failing, after troubleshooting using various commands, the interface cable was not properly connected.

```
C:\>ping 10.10.20.1

Pinging 10.10.20.1 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 10.10.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Then using command “Sh ip int brief” and “Sh interfaces” on router and switch respectively and even checking for MTU mismatch etc, I figured it was a physically connection problem and remade the cable connection.

```
C:\>ping 10.10.20.1

Pinging 10.10.20.1 with 32 bytes of data:

Reply from 10.10.20.1: bytes=32 time<1ms TTL=255
Reply from 10.10.20.1: bytes=32 time<1ms TTL=255
Reply from 10.10.20.1: bytes=32 time<1ms TTL=255
Reply from 10.10.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

5. Verify eng1 pc has connectivity to sales1

```
C:\>ping 10.10.20.10

Pinging 10.10.20.10 with 32 bytes of data:

Request timed out.
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127
Reply from 10.10.20.10: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.20.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

6. Since I will do two more configurations here,let me clean up
On R1
Int f0/1
Shut

Inter-Vlan Routing : Router on a stick

1. Configure sub interfaces on Fast 0/0 on R1 as the default gatewat for the eng and sales pc
On R1
Int f0/0
No ip address
No shut
Int f0/0.10
Encapsulation dot1q 10
Ip add 10.10.10.1 255.255.255.0
Int f0/0.20
Encapsulation dot1q 20
Ip add 10.10.20.1 255.255.255.0

2. Now for ACLs,We will control traffic between VLANS we allow VLAN 10 (engg) to access only 10.10.20.10 in VLAN 20 (sales).The second line blocks all other traffic from VLAN 10 to VLAN 20.
The third line permits all other traffic, ensuring the router functions properly.

access-list 101 permit ip 10.10.10.0 0.0.0.255 host 10.10.20.10
access-list 101 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255
access-list 101 permit ip any any
interface f0/0.10
ip access-group 101 out

3. Configure SW2 to support inter-vlan routing using R1 as default gateway

Int f0/1
Switch trunk encap dot1q
Switchport mode trunk

4. Verify the eng1 PC has connectivity to vlan 20 int on r1

```
C:\>ping 10.10.20.1

Pinging 10.10.20.1 with 32 bytes of data:

Reply from 10.10.20.1: bytes=32 time<1ms TTL=255
Reply from 10.10.20.1: bytes=32 time<1ms TTL=255
Reply from 10.10.20.1: bytes=32 time=10ms TTL=255
Reply from 10.10.20.1: bytes=32 time=17ms TTL=255

Ping statistics for 10.10.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 6ms

C:\>
```

5. Verify eng1 pc has connectivity to sales1

```
C:\>ping 10.10.20.10

Pinging 10.10.20.10 with 32 bytes of data:

Request timed out.
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.20.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

6. Verify eng1 pc can't connect to sales2 because of the access list.

```
C:\>ping 10.10.20.11

Pinging 10.10.20.11 with 32 bytes of data:

Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 10.10.20.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

7. Clean up: Shut down int f0/0 on R1
int f0/0
Shut

Inter VLAN routing: Layer 3 switch

1. Enable layer 3 routing on SW2
ip routing

2. Configure SVIs on SW2 to support inter vlan routing between the eng and sales vlans
Int vlan 10
Ip add 10.10.10.1 255.255.255.0
Int vlan 20
Ip add 10.10.20.1 255.255.255.0

2. Configuring ACLs for Inter-VLAN Routing
To restrict traffic between VLANs:
Allow VLAN 10 (engg) devices to communicate only with host `10.10.20.10` in VLAN 20 (sales). Block all other traffic from VLAN 10 to VLAN 20.

access-list 102 permit ip 10.10.10.0 0.0.0.255 host 10.10.20.10
access-list 102 deny ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255

access-list 102 permit ip any any
interface vlan 10
ip access-group 102 in

3. Verify eng1 pc has connectivity to vlan 20 int on sw2

```
C:\>ping 10.10.20.1

Pinging 10.10.20.1 with 32 bytes of data:

Request timed out.
Reply from 10.10.20.1: bytes=32 time<1ms TTL=255
Reply from 10.10.20.1: bytes=32 time<1ms TTL=255
Reply from 10.10.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.20.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4. Verify the Eng1 has connectivivty to sales 1

```
C:\>ping 10.10.20.10

Pinging 10.10.20.10 with 32 bytes of data:

Request timed out.
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127
Reply from 10.10.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.20.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5. Verify no one from engg can reach anyone else on the sales vlan because of the access list

```
C:\>ping 10.10.20.11

Pinging 10.10.20.11 with 32 bytes of data:

Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 10.10.20.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```