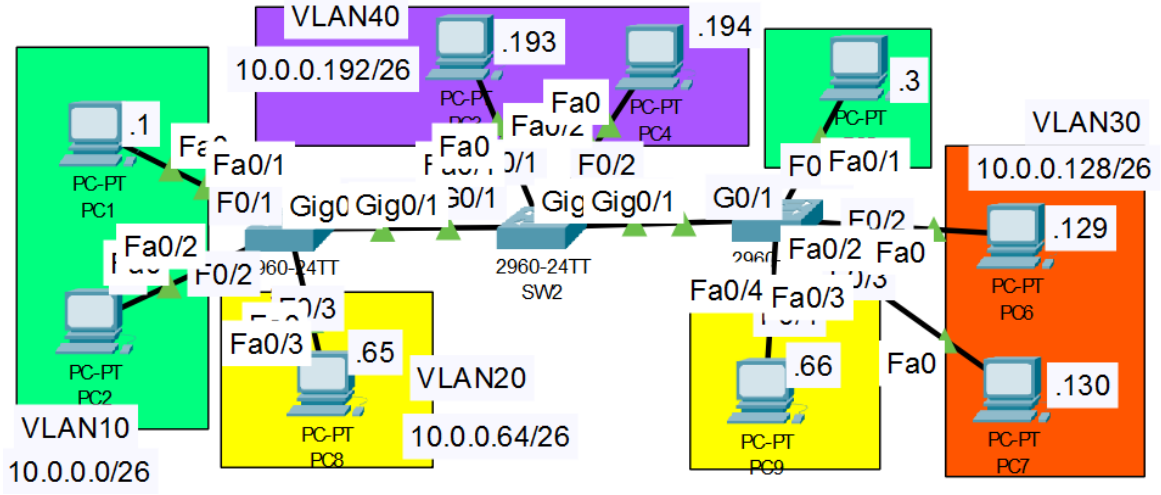
Configuring, Verifying, and Troubleshooting VTP and DTP

This document provides a cleaned-up, structured solution to *Jeremy's Free CCNA VTP/DTP Day 19 Lab*. It also includes additional configuration steps, verification commands, and security considerations that go beyond the original lab requirements.

Topology diagram

Figure 1.0: Network Topology from Jeremy's IT Lab Day 19



Network topology description

VLAN	Network	Default Gateway	Broadcast Address	VLAN Color	VLAN Host Range
10	10.0.0.0/26	10.0.062	10.0.063	GREEN	10.0.0.1 – 10.0.0.62
20	10.0.0.64/26	10.0.0.126	10.0.0.127	YELLOW	10.0.0.65 – 10.0.0.126
30	10.0.0.128/26	10.0.0.190	10.0.0.191	ORANGE	10.0.0.129 – 10.0.0.190
40	10.0.0.192/26	10.0.0.254	10.0.0.255	PURPLE	10.0.0.193 – 10.0.0.254

Step-by-step configurations

1. Solution 1: Configure trunk links between SW1 - SW3

SW1: Configure Gi0/1 as a static trunk and disable DTP

```
SW1> enable
SW1# configure terminal
SW1(config)# interface gigabitEthernet 0/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport nonegotiate
Verify trunk status:
SW1# show interfaces gigabitEthernet 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
```

SW2 connects to SW1 on Gi0/1 and to SW3 on Gi0/2:

SW2: Configure trunk ports and disable DTP

```
SW2> enable
SW2# configure terminal
SW2(config)# interface range gigabitEthernet 0/1 - 2
SW2(config-if-range)# switchport mode trunk
SW2(config-if-range)# switchport nonegotiate
```

Verify :

```
SW2# show interfaces gigabitEthernet 0/1 switchport
SW2# show interfaces gigabitEthernet 0/2 switchport
```

Both should show:

- Administrative Mode: trunk
- Operational Mode: trunk
- Negotiation of Trunking: Off

SW3: Configure trunk link with SW2 and disable DTP

```
SW3> enable
SW3# configure terminal
SW3(config)# interface gigabitEthernet 0/1
SW3(config-if)# switchport mode trunk
SW3(config-if)# switchport nonegotiate
```

Verify:

```
SW3# sh int gig0/1 sw
```

You should again see:

- Administrative Mode: trunk
- Operational Mode: trunk
- Negotiation of Trunking: Off

DTP summary

All inter-switch links (SW1–SW2, SW2–SW3) are configured as static 802.1Q trunks.

DTP negotiation is disabled (switchport nonegotiate) on all trunk ports, preventing unwanted dynamic trunking behavior.

Solution 2: VTP Configuration and VLAN Synchronization Across SW1, SW2, and SW3

2.1. Verify Initial VTP Status on All Switches

SW1

```
SW1# show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
```

SW2

```
SW2# show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
```

SW3

```
SW3# show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
```

Initial Observations

- All switches are in **VTP Server mode**
- No VTP domain name is configured
- Revision number is **0** on all switches
- Only default VLANs exist (1, 1002–1005)

Verify VLANs on either Switch:

```
SW3# show vlan brief
VLAN Name                             Status    Ports
1    default                          active    Fa0/1–Fa0/24, Gi0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

2.2. Configure VTP Domain and VLANs on SW1

Set VTP Domain Name

```
SW1# configure terminal
SW1(config)# vtp domain CCNA
%SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
```

Create VLANs 10, 20, and 30

```
SW1(config)# vlan 10
SW1(config-vlan)# vlan 20
SW1(config-vlan)# vlan 30
```

Verify VTP Update on SW1

```
SW1# show vtp status
VTP Version                     : 1
Configuration Revision          : 3
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : CCNA
```

Updated Parameters

- Revision number increased to 3
- VLAN count increased to 8 (default VLANs + 10, 20, 30)
- Domain name now set to CCNA

2.3. Verify VTP Synchronization on SW2 and SW3

SW2

```
SW2# show vtp status
Configuration Revision          : 3
Number of existing VLANs        : 8
VTP Domain Name                 : CCNA
```

SW3

```
SW3# show vtp status
Configuration Revision          : 3
Number of existing VLANs        : 8
VTP Domain Name                 : CCNA
```

Both switches successfully synchronized with SW1.

2.4. Verify VLAN Database on SW2 and SW3

```
SW2 VLANs

SW2# show vlan brief
VLAN Name                              Status
1    default                           active
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002–1005 legacy VLANs                 active


SW3 VLANs


SW3# show vlan brief
VLAN Name                              Status
1    default                           active
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002–1005 legacy VLANs                 active
```

Observations:

- VLANs **10, 20, and 30** were automatically added to SW2 and SW3 via VTP.
- All switches remain in **VTP Server mode**.
- Synchronization occurred because SW1 had the **highest revision number**.

Important note to know:

Switches in VTP Server or Client mode will automatically update their VLAN database when they receive a VTP advertisement with a higher revision number within the same domain. Switches in Transparent mode do not update their VLAN database but still forward VTP advertisements.

Solution 3: Configure SW2 in VTP Transparent Mode and Test VLAN Propagation

3.1. Configure SW2 in VTP Transparent Mode

Changing SW2 from VTP Server mode to VTP Transparent mode.

```
SW2> enable
SW2# configure terminal
SW2(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

3.2. Verify SW2 VTP Operating Mode

```
SW2(config)# do show vtp status
VTP Version                     : 1
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Transparent
VTP Domain Name                 : CCNA
```

Key Observations

- SW2 is now operating in VTP Transparent mode.
- The configuration revision resets to 0, which is expected when switching to Transparent mode.
- Transparent mode forwards VTP advertisements but does not participate in VLAN synchronization.

3.3. Add VLAN 40 Locally on SW2

Since Transparent mode does not sync VLANs, VLANs must be created manually.

```
SW2(config)# vlan 40
SW2(config-vlan)# do show vlan brief
```

Output:

```
VLAN Name                              Status
1    default                           active
10   VLAN0010                          active
20   VLAN0020                          active
30   VLAN0030                          active
40   VLAN0040                          active
1002–1005 legacy VLANs                active
```

VLAN 40 is successfully added **locally** on SW2.

3.4. Verify Whether VLAN 40 Propagated to SW1 and SW3

SW1 VLAN Database

```
SW1# show vlan brief
VLANs present: 1, 10, 20, 30, 1002–1005
SW3 VLAN Database
SW3# show vlan brief
VLANs present: 1, 10, 20, 30, 1002–1005
```

Observation:

- VLAN 40 does NOT appear on SW1 or SW3.
- This behavior is correct and expected.

Explanation

Switches in VTP Transparent mode behave differently from Server and Client modes:

- They do not update their VLAN database based on VTP advertisements.
- They do not advertise their own VLAN changes to other switches.
- They do forward VTP messages, allowing the rest of the domain to function normally.

It is for these reasons:

VLAN 40 remains local to SW2 and is not synchronized to SW1 or SW3.

This confirms correct VTP Transparent mode behavior.

Solution 4: Configure SW3 in VTP Client Mode and Test VLAN Creation

4.1. Configure SW3 in VTP Client Mode

```
SW3# configure terminal
SW3(config)# vtp mode client
Setting device to VTP CLIENT mode.
```

4.2. Verify SW3 VTP Operational mode

```
SW3(config)# do show vtp status
VTP Version                     : 1
Configuration Revision          : 3
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
```

Key Observations

- SW3 is now operating in **VTP Client mode**.
- The switch retains the **revision number of 3**, inherited from SW1.
- As a VTP client, SW3 **cannot create, modify, or delete VLANs**.
- SW3 will only learn VLANs from VTP servers in the same domain.

4.3. Attempt to Create VLAN 50 on SW3

```
SW3(config)# vlan 50
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

Result

- The attempt to create VLAN 50 fails, as expected because VTP Client mode does not permit any VLAN database changes. Only VTP Server switches can create or modify VLANs in the domain.

Solution 5: Configure All Switchports Connected To Host In The Correct VLAN | Manually Configure Them As Access Ports. | Verify Whether DTP Is Still Enabled On The. Switchports

5.1 Configure all Switchports to host to their appropriate VLAN

SW1

```
SW1>ena
SW1#
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#swi
SW1(config-if)#switchport ac
SW1(config-if)#switchport access vl
SW1(config-if)#switchport access vlan 10
SW1(config-if)#
SW1(config-if)#int fa0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#
SW1(config-if)#int fa0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#
```

Configure other switchports using the same commands.

5.2. Observe and verify that SW1 interfaces are configured to the correct VLANs

```
SW1(config-if)#
SW1(config-if)#do show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Gig0/2
10   VLAN0010                         active    Fa0/1, Fa0/2
20   VLAN0020                         active    Fa0/3
30   VLAN0030                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW1(config-if)#
```

The show vlan brief command confirms SW1 interfaces are now added to their respective VLANs. Verify the same for other switchports.

5.3 Verify that DTP is still enabled on the switchports connected to the host VLANs

```
W1(config-if)#
SW1(config-if)#
SW1(config-if)#
SW1(config-if)#do sh int fa0/1 switch
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
```

SW1 interface fa0/1 is operating in static access mode, and DTP is still enabled. DTP may remain enabled on interfaces on dynamic auto, dynamic desirable and dynamic access unless the switchport nonegotiate command is used.

Security Advise: DTP should be disabled using the ***switchport nonegotiate*** command on switchports on the mentioned DTP modes, to avoid the switch from sending DTP messages trying to form trunk connection with switches.

Beyond The LAB Tasks:

Simplified summary of DTP and VTP:

VTP protocol helps you create and manage VLAN from one central switch (server mode). Imagine you have many switches, and you want them all to know the same VLANs. Instead of configuring VLANs on every switch manually, VTP lets one switch spread the VLAN information to the others.

Risk:

It is dangerous if misused (wrong revision number can wipe VLANs). A new switch with a higher revision number and outdated VLAN database can override the VLAN database causing the network to lose connection.

DTP helps two switches decide whether a link should be an access port or a trunk port without manual configuration.

Risk(s):

It is recommended to disable DTP in switches to avoid unauthorize switches forming trunk connection with the switch. Trunk mode automatically turns off DTP negotiations, while dynamic auto and dynamic desirable have it on. it should be manually disabled using the ***switchport nonegotiate*** command.

Further Security enhancement:

configuring the native VLAN to an unused VLAN, and the trunk ports to only allow traffics for VLAN active and on the switch. If there is an unauthorize connection to the switch interface, that connection by default will be in the VLAN1, which is the native VLAN, changing the native VLAN to an unused VLAN protects the networks and discard unknown traffic from that interface.

Changing the native vlan on all Switch trunk interface to 99:

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#vlan 99
SW1(config)# int gig0/1
SW1(config-if)#switchport trunk native vlan 99
```

Observe if the Vlan 99 was created:

```
SW1(config-if)#do show vlan br
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Gig0/2
10   VLAN0010                         active    Fa0/1, Fa0/2
20   VLAN0020                         active    Fa0/3
30   VLAN0030                         active
99   VLAN0099                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW1(config-vlan)#
SW1(config-vlan)#
SW1(config-vlan)#^Z
SW1#
```

Note: SW3 will ADD VLAN99 to VLAN database, however SW2 will not, because SW2 is on VTP TRANSPARENT MODE. This will cause SW1 to display the below error message:

```
%SYS-5-CONFIG_I: Configured from console by console

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (99),
with SW2 GigabitEthernet0/1 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (99),
with SW2 GigabitEthernet0/1 (1).
```

A quick look on SW2 VLAN databas:

```
SW2>
SW2>ena
SW2#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active    Fa0/1, Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
```

```
1004 fddinet-default                active
1005 trnet-default                  active

SW2#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 99 on
GigabitEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/1 on VLAN0001. Inconsistent local
vlan.
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1),
with SW1 GigabitEthernet0/1 (99).
```

SW2 has not added the VLAN 99 to it's database, and there is an error message warning for inconsistency with SW1 native VLAN, that the port is blocking the gig0/1 interfaces on VLAN001.

With this in mind we have to locally create the vlan 99 in SW2 and manually configure the native vlan to use vlan99. we have to manually configure SW3 trunk port native vlan to 99 too.

```
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#vlan 99
SW2(config-vlan)#
SW2(config-vlan)#
SW2(config-vlan)#do show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active    Fa0/1, Fa0/2
99   VLAN0099                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

W2(config-vlan)#
SW2(config-vlan)#int gig0/1
SW2(config-if)#swi
SW2(config-if)#switchport tr
SW2(config-if)#switchport trunk na
SW2(config-if)#switchport trunk native v
SW2(config-if)#switchport trunk native vlan 99
SW2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on VLAN0099.
Port consistency restored.
```

```
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on VLAN0001. Port
consistency restored.
```

After configuring the correct native VLAN99 on SW2 we get a message that the port consistency has been restored.

The same configuration on SW3:

Verify existence of vlan 99 on SW3:

```
SW3#
SW3#show vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    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
                                                 Gig0/2
10   VLAN0010                          active    Fa0/1
20   VLAN0020                          active    Fa0/4
30   VLAN0030                          active    Fa0/2, Fa0/3
99   VLAN0099                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
SW3#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 99 on
GigabitEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/1 on VLAN0001. Inconsistent local
vlan.


%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1),
with SW2 GigabitEthernet0/2 (99).
```

Configure SW3 Trunk native VLAN to VLAN99:

```
SW3#
SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#int gig0/1
SW3(config-if)#swi
SW3(config-if)#switchport vl
SW3(config-if)#switchport tr
SW3(config-if)#switchport trunk na
SW3(config-if)#switchport trunk native vl
```

```
SW3(config-if)#switchport trunk native vlan 99
SW3(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on VLAN0099.
Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking GigabitEthernet0/1 on VLAN0001. Port
consistency restored.
```

LAST TASK IS TO ENSURE THAT SWITCHES ONLY FORWARD TRUSTED VLAN TRAFFIC ON THEIR TRUNK PORTS:

Until now, all traffic will go through the trunk ports, lets verify this on SW1:

```
SW1#
SW1#
SW1#show int tru
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      1,10,20,30,99
```

observing the row ***vlans allowed on trunk port:***

This means all traffic for VLAN in the range 1-1005 will be allowed on the trunk port. SW2 will allow an additional VLAN40. We have to configure the trunk port to only allow the configured VLANs and the Trunk native VLAN.

Configure allowed VLANs on trunk ports:

```
SW1#
SW1#
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#int gig0/1
SW1(config-if)#swi
SW1(config-if)#switchport tr
SW1(config-if)#switchport trunk all
SW1(config-if)#switchport trunk allowed vl
SW1(config-if)#switchport trunk allowed vlan 99,10,20,30
SW1(config-if)#
```

Observe the trunk allowed VLAN list again on SW1:

```
SW1#
SW1#show int tr
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/1      10,20,30,99

Port        Vlans allowed and active in management domain
Gig0/1      10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,30,99
```

Observation:

Native VLAN is now 99 and only the allowed VLANs can access trunk.

Hurray! we have secured our ports and VLANs, the same configuration should be done on SW2 and SW3, ensure that only the VLANs active in managements should be allowed in the trunk port. Use the ***show interfaces trunk*** command to confirm VLANs active in that switch.

PERFORM PING TEST AND OBSERVE:

Hosts belonging to specific VLANs can ping each other, but cannot ping host in other VLANs. Also, you should notice the segregation of the VLANs into separate broadcast domains. Traffic coming to a VLAN belonging to a different subnet must pass through a Router.

Thank you for staying though this Step by Step guild on VTP and DTP troubleshooting. I love sharing what I have learnt and this is just one of many labs and guilds which will be uploaded to my portfolio on GitHub: hub.com/Cokode/portfolio

Credit to Jeremy's IT LAB for this and other wonderful and challenging LAB Task