DTP (Dynamic Trunking Protocol):

- DTP Cisco proprietary protocol which stand for Dynamic Trunking Protocol.
- DTP is point-to-protocol negotiates common trunking mode between Switches.
- DTP is used to dynamically build trunk links between the two Cisco Switches.
- Which is used to automatically negotiate trunks between the Cisco Switches.
- DTP is used to negotiate & form trunk connection between switches dynamically.
- DTP can also be used for negotiating encapsulation type of either IEEE 802.1Q or ISL.
- Dynamic Trunking Protocol is Layer 2 (Data Link) protocol and is enabled by default.
- The default mode can be “Dynamic Auto” or “Dynamic Desirable” depend on Switches.
- A Non-Cisco Switches does not support Dynamic Trunking Protocol (DTP) only Cisco.
- Port configures as nonegotiate prevents generating Dynamic Trunking Protocol frames.
- DTP has two default timers that cannot be changed one is Hello & other is the timeout.
- Dynamic Trunking Protocol Hello frames being sent every 30 seconds to remote peer.
- And Dynamically formed Trunks via DTP will timeout after 300 seconds of the inactivity.
- We can configure the trunking in Cisco switches by two ways statically or dynamically.
- In static trunking method we need to configure trunking in interface statically.
- While in dynamic trunking mode it automatically done by a DTP trunking protocol.

Trunking Modes:

There are five different trunking modes or methods supported by Cisco Switches.

Access:

- The Access mode Puts the switch interface into permanent non-trunking mode.
- The Access mode negotiates to convert the link into a non-trunk link or interface.
- Interface becomes nontrunk even if neighboring interface does not agree to change.

Trunk:

- The Trunk mode puts the interface into permanent trunking mode in Switches.
- Th Trunk mode negotiates to convert the link or port into a trunk link or interface.
- Interface becomes a trunk even if neighboring interface does not agree to change.

Nonegotiation:

- Puts interface into permanent trunking mode but prevents interface sending DTP.
- Must configure neighboring interface manually trunk interface to establish trunk.
- Use this mode when connecting to a device that does not support DTP or non-Cisco.
- This mode is used to trunk connection between Cisco device and a non-Cisco device.

Dynamic Desirable:

- Interface will generate the DTP messages and send them to other end of switch.
- Interface will work as access link until it get replies from remote end of switch.
- If other end does not respond to DTP message, interface work as access link.
- If other end support DTP will change connection link in trunk from access link.
- The interface becomes a trunk interface if the neighboring interface is set to trunk.
- Interface becomes trunk if neighboring interface is set to desirable, or auto mode.

Dynamic Auto:

- In auto mode interface works as access link and passively listen for DTP messages.
- Dynamic Auto mode makes the interface willing to convert the link to a trunk link.
- The interface becomes a trunk interface if the neighboring interface is set to trunk
- The interface becomes a trunk interface if neighboring link set to desirable mode.
- Normally, this is the default mode for all Ethernet interfaces in Cisco IOS Switches.

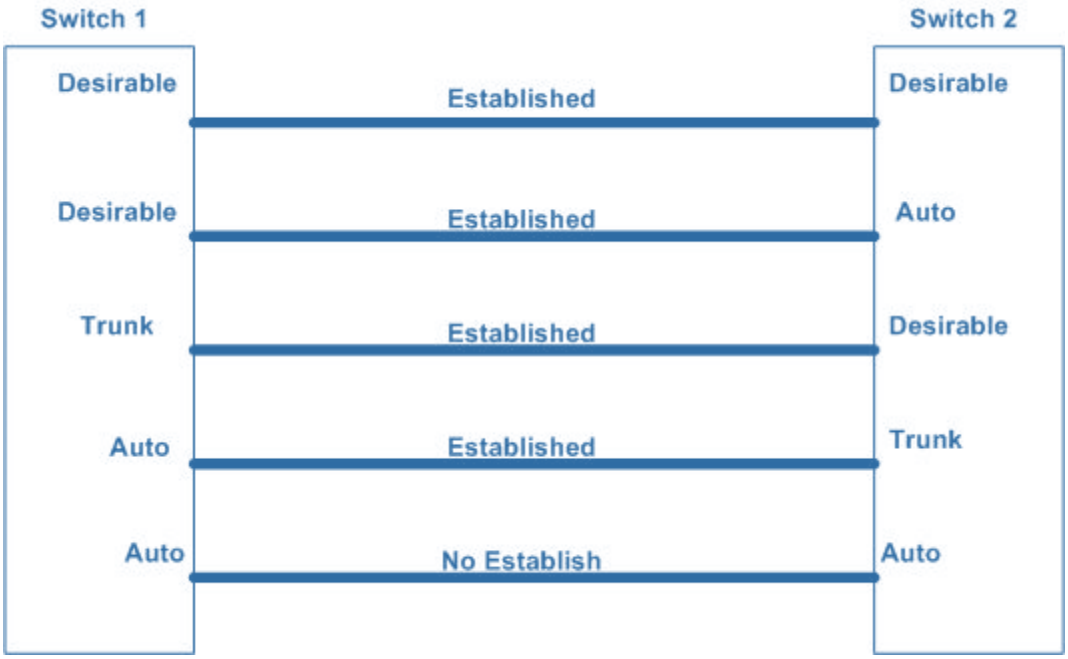
DTP On Mode:

- In ON mode interface is set to trunk, regardless remote end supports trunking or not.
- On mode cause interface to generate DTP messages & tag frames based on trunk type.
- Even if the neighboring ports are trunk or not that is why it is called DTP mode ON.

DTP Off Mode:

- DTP Off mode puts the Cisco switch interface into permanent non trunking mode.
- Whether the neighboring interface is trunk port or trying to become a trunk port.
- In DTP Off mode Cisco Switch port become a dedicated layer 2 access port or link.
- In Dynamic Trunking Protocol (DTP) off mode interface is configured as access-link.
- No Dynamic Trunking Protocol message will be generated, nor frames will be tagged.

Switchport Mode	Dynamic Desirable	Dynamic Auto	Trunk	Access
Dynamic Desirable	trunk	trunk	trunk	access
Dynamic auto	trunk	access	trunk	access
Trunk	trunk	trunk	trunk	Limited
Access	access	access	Limited	access



Manual (Static) Trunk Configuration:

- Manual configuration of trunk is performed by issuing the switchport mode trunk
- Interface configuration command on the desired Cisco switch port or Interface.
- This Switch command forces the port into a permanent (Static) trunking mode.
- Although Static configuration of a trunk link forces the switch to establish a trunk.
- Dynamic ISL & Dynamic Trunking Protocol packets will still be sent out of interface.
- Statically configured trunk link can establish trunk with neighboring that is using DTP.

S1(config)#interface Ethernet0/1
S1(config-if)#switchport
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk

```
S1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1
```

```
S1#show interfaces e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

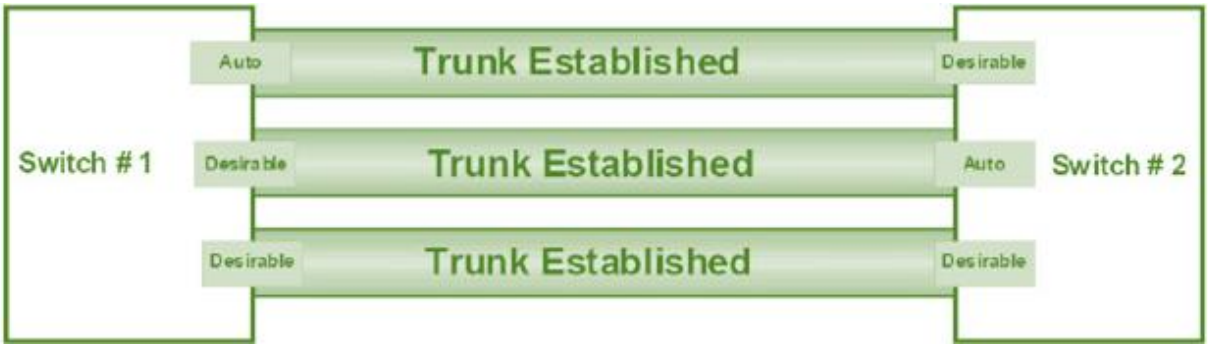
To turn off DTP on a switch port apply the following command under the interface commands.

S1(config)#interface e0/0
S1(config-if)#switchport nonegotiate

```
S1#show interfaces e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

Dynamic Trunk Configuration:

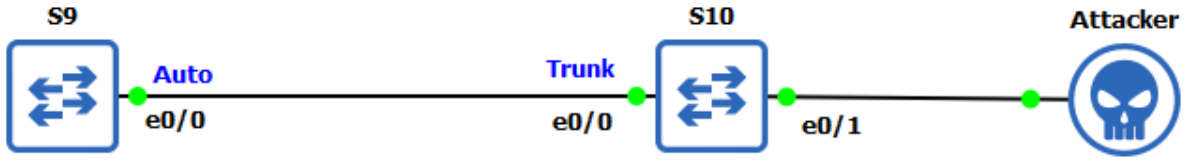
- While in dynamic trunking mode it automatically done by a DTP trunking protocol.
- Interface will generate the DTP messages and send them to other end of switch.
- Interface becomes trunk if one side is set to desirable & other side set to auto mode.
- Interface becomes trunk if one side is set to desirable & other side is also desirable.



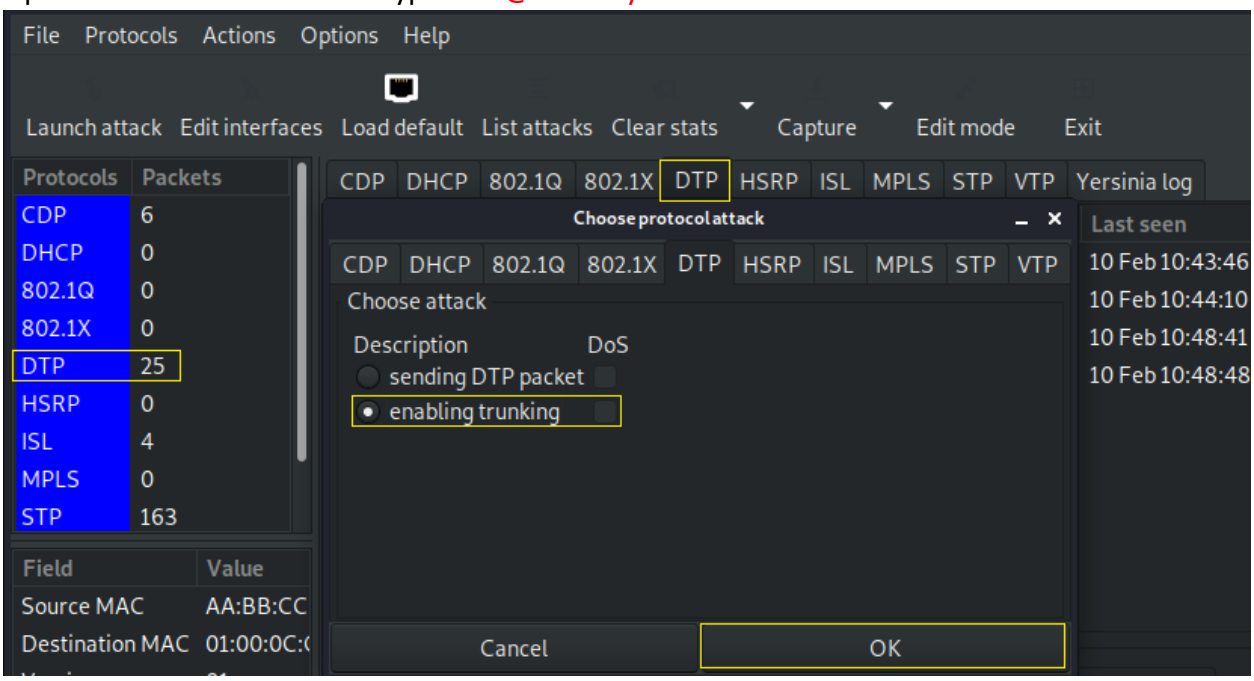

```
S9#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Et0/0       desirable    802.1q         trunking      1

S10#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Et0/0       auto         n-802.1q       trunking      1

S9#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Et0/0       desirable    802.1q         trunking      1
```

VLAN Hopping Attack:

- Attacker connects to a VLAN to gain access to traffic on other VLANs.
- Attacker send spoofed trunk negotiation & interface configured as a trunked.
- Disable any automated trunk negotiation (DTP) on Cisco Switches.
- Never leave a port in "dynamic desirable", "dynamic auto" or "trunk" mode.
- Hardcode all the access ports as access port and disable DTP everywhere.
- Shutdown all the interfaces in Cisco Switches which are not in use.



Open Yersinia from Terminal type root@kali:~# yersinia -G and lunch attack.




```
S10#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        n-802.1q       trunking      1
Et0/1       auto             n-802.1q       trunking      1
```