Day 19: DTP and VTP Protocols

CCNA 200-301 Study Guide: Cisco's DTP and VTP Protocols

1.0 Introduction: The Enduring Relevance of DTP and VTP

While DTP and VTP are no longer standalone topics in the current CCNA curriculum, they remain critical "under-the-hood" protocols. They govern the default behavior of Cisco Catalyst switches and can cause significant troubleshooting and security issues if left unmanaged.

Understanding these protocols is essential for interpreting switch behavior, securing networks against Layer 2 vulnerabilities, and ensuring stable trunking.

2.0 Dynamic Trunking Protocol (DTP)

DTP is a Cisco-proprietary protocol designed to automate the creation of trunk links. It negotiates whether a link should be an access port or a trunk and determines the encapsulation (typically 802.1Q).

2.1 DTP Administrative Modes

Mode	Behavior	Negotiation Stance
Access	Permanent access port.	Disables DTP.
Trunk	Permanent trunk port.	Actively sends DTP frames.
Dynamic Auto	Passive; becomes a trunk only if requested.	Listens only (Default for most switches).
Dynamic Desirable	Active; attempts to convert link to a trunk.	Actively negotiates.

2.2 DTP Negotiation Outcomes

Local Mode	Remote: Auto	Remote: Desirable	Remote: Trunk	Remote: Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Mismatch
Access	Access	Access	Mismatch	Access

The "Auto" Trap: If both switches are left in the default Dynamic Auto state, a trunk will never form. Both sides wait passively for the other to start the negotiation, resulting in a standard access link.

2.3 Security Risks: VLAN Hopping

A malicious actor can spoof DTP frames to trick a dynamic port into becoming a trunk. Once a trunk is formed, the attacker gains access to all VLANs allowed on that link, bypassing network segmentation.

Best Practices:

- End-User Ports: Always use switchport mode access to disable negotiation.
- Trunk Links: Hardcode using switchport mode trunk and disable negotiation with switchport nonegotiate.

3.0 VLAN Trunking Protocol (VTP)

VTP maintains a consistent VLAN database across a network. It allows an administrator to add, delete, or rename VLANs on one switch and have those changes propagate to all other switches in the domain.

3.1 VTP Operational Modes

1. Server (Default): Can create, modify, and delete VLANs. Changes are advertised to the domain and saved in NVRAM (vlan.dat).
2. Client: Cannot change VLANs locally. Synchronizes its database with the Server. In VTP v1/v2, changes are not saved to NVRAM (lost on reboot).
3. Transparent: Does not synchronize with the domain. It forwards VTP advertisements but does not process them. Local VLANs can be created but are not advertised. Configuration Revision is always 0.

3.2 The "VTP Bomb"

VTP uses a Configuration Revision Number to track updates. A switch will always overwrite its database if it receives an advertisement with a higher revision number.

The Risk: If you connect a repurposed switch with a high revision number and the same domain name, it can instantly overwrite the production VLAN database, potentially deleting all VLANs and causing a network-wide outage.

Safety Procedure to Reset Revision to 0:

1. Isolate the switch.
2. Change VTP mode to Transparent (this resets revision to 0).
3. Change VTP mode back to Client/Server.
4. Verify with show vtp status.

4.0 Configuration and Verification Command Reference

4.1 DTP Commands

Objective	Command
Set port to static access	switchport mode access

Set port to static trunk	switchport mode trunk
Disable DTP on interface	switchport nonegotiate
Verify interface status	show interfaces <id> switchport

4.2 VTP Commands

Objective	Command
Set VTP mode	vtp mode {server | client | transparent}
Set VTP domain	vtp domain <name>
Set VTP password	vtp password <pass>
Verify VTP status	show vtp status

5.0 Key Troubleshooting Insights

- VTP Version Limits: VTP v1 and v2 only synchronize Normal Range VLANs (1–1005). To sync Extended Range VLANs (1006–4094), you must use VTP v3 or Transparent mode.
- VTP Pruning: This feature prevents unnecessary broadcast traffic from flooding across trunks to switches that don't have active ports in those VLANs.
- Native VLAN Mismatch: DTP does not fix Native VLAN mismatches. If one side is VLAN 1 and the other is VLAN 99, you will receive CDP error messages and traffic will leak between VLANs.

Revision #1
Created 2026-03-14 19:26:15 UTC by Tony Utter
Updated 2026-03-14 19:26:39 UTC by Tony Utter