Days 16, 17, 18: VLANs

CCNA 200-301 Study Guide: VLANs, Trunking, and DTP

1.0 Foundational Concepts: Introduction to VLANs

Virtual LANs (VLANs) provide the mechanism for network segmentation at Layer 2. By creating distinct broadcast domains, administrators can logically group users regardless of their physical location on the switch.

1.1 The Metaphor: The Soundproof Office

Think of a large, open-plan office where everyone is shouting. This is a single broadcast domain; the noise (broadcast traffic) makes it hard for anyone to focus. Implementing VLANs is like building soundproof glass walls. People in the "Sales" room can talk to each other without distracting the "Finance" room, even though they are all in the same building (on the same physical switch).

1.2 Core Benefits

- Broadcast Containment: ARP requests and other broadcasts are limited to a single VLAN.
- Enhanced Security: Users in different VLANs cannot communicate at Layer 2. Inter-VLAN communication requires a Layer 3 device (Router or Multilayer Switch).
- Improved Performance: Reduces CPU overhead on host devices by eliminating irrelevant broadcast processing.

1.3 VLAN Ranges

Cisco switches support two ranges of VLAN IDs:

VLAN Range	Numeric Range	Storage Location	Notes
Normal	1 – 1005	vlan.dat (Flash)	VLANs 1002–1005 are reserved for legacy tech.
Extended	1006 – 4094	running-config (NVRAM)	Requires VTP Transparent mode on older switches.

1.4 Basic VLAN Configuration

- # 1. Create and name the VLAN
- Switch(config)# vlan 10
- Switch(config-vlan)# name SALES
-
- # 2. Assign a port to the VLAN (Access Port)
- Switch(config)# interface g0/1
- Switch(config-if)# switchport mode access
- Switch(config-if)# switchport access vlan 10

2.0 Inter-Switch Communication: VLAN Trunking

Trunking allows a single physical link to carry traffic for multiple VLANs between switches.

2.1 The 802.1Q Tagging Protocol

IEEE 802.1Q (Dot1q) is the industry-standard protocol for trunking. It inserts a 4-byte (32-bit) tag into the Ethernet header to identify the VLAN ID.

- TPID: Set to 0x8100 to identify a tagged frame.
- VLAN ID: A 12-bit field, allowing for 2^{12} (4,096) unique VLANs.

2.2 The Native VLAN

By default, traffic on the Native VLAN is sent across a trunk untagged.

- Security Risk: VLAN 1 is the default native VLAN and a target for "VLAN hopping" attacks.
- Best Practice: Change the native VLAN to an unused ID (e.g., 999) and ensure it matches on both ends of the link.

2.3 Trunk Configuration

- Switch(config)# interface g0/1
- # Switch(config-if)# switchport trunk encapsulation dot1q (Required on older hardware)
- Switch(config)# switchport mode trunk
- Switch(config)# switchport trunk native vlan 99
- Switch(config)# switchport trunk allowed vlan 10,20,30 # VLAN Pruning

3.0 Automated Negotiation: Dynamic Trunking Protocol (DTP)

DTP is a Cisco proprietary protocol that automates the formation of trunk links. While convenient, it is considered a security risk in modern networks.

3.1 DTP Operational Modes

- Access: Permanent non-trunking state.
- Trunk: Permanent trunking state; actively negotiates with the neighbor.
- Dynamic Auto: Passive; becomes a trunk only if the neighbor is set to Trunk or Desirable.
- Dynamic Desirable: Active; attempts to convert the link to a trunk.
- No-Negotiate: Disables DTP advertisements entirely (switchport nonegotiate).

3.2 DTP Negotiation Outcomes

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

4.0 Verification and Best Practices

4.1 Key Verification Commands

Command	Purpose
show vlan brief	Lists all active VLANs and their assigned access ports.
show interfaces trunk	Shows active trunks, encapsulation, and allowed/native VLANs.
show interface [ID] switchport	Displays administrative vs. operational modes (e.g., DTP status).

4.2 Security Best Practices

1. Disable DTP: Use switchport mode access and switchport nonegotiate on user-facing ports.
2. Hard-code Trunks: Never rely on Dynamic Auto; use switchport mode trunk.
3. VLAN Pruning: Only allow necessary VLANs across a trunk to save bandwidth.
4. Secure the Native VLAN: Move the native VLAN away from VLAN 1 and use a dedicated "dummy" VLAN.

TL;DR Summary

- VLANs break one large broadcast domain into multiple smaller logical ones.
- 802.1Q is the standard for trunking; it uses tags to keep traffic separated on inter-switch links.
- Native VLAN traffic is untagged; mismatches cause traffic "leaking" and security issues.
- DTP should be disabled on all production ports to prevent unauthorized trunking and VLAN hopping.

Revision #1
Created 2026-03-14 19:21:56 UTC by Tony Utter
Updated 2026-03-14 19:22:35 UTC by Tony Utter