

*There is nothing new in chapter 1 of the CCNA 200-105 book by Wendell Odom. It is entirely a reprint of CCENT 100-105 Chapter 11, covering the concepts and configuration of VLANs and trunks. What follows is taken entirely from Chapter 4 ("LAN Troubleshooting") of the CCNA 200-105 book.*

## ASSIGNING FRAMES TO VLANS

As a frame enters a switch, it is assigned to a VLAN which will limit which ports it can exit.

- If the frame enters an access port, its VLAN will be the access VLAN of that port
- If the frame enters on trunked interface, its VLAN will be in its trunking header. If it lacks a trunking header, then it is assigned to the native VLAN of that trunk
- If the port happens to have both an access VLAN and a voice VLAN, any frames from an attached IP phone will be assigned to the voice VLAN. This is easy because the phone will give its frames an 802.1Q trunking header, perhaps even using CDP to know which VLAN to use. If any untagged frames arrive from a PC or printer attached to the phone, they will be assigned to the port's access VLAN.

## VLAN TROUBLESHOOTING

Frame forwarding on a Cisco switch is per-VLAN, as if there were a separate MAC address table for each VLAN. For a switch to forward data in a VLAN,

- The VLAN must exist on the switch—If a trunk brings in frames tagged with a VLAN that doesn't exist on the switch, they die. Check each switch along a path to ensure that the VLAN exists there
- The VLAN must be active on the switch—not shutdown
- If the exit interface is a trunk, that trunk must allow that VLAN—check the "allowed" config at *both* ends of the trunk



Check that access interfaces are in the correct VLAN. Don't rely on "show running-config."

```
S1# show vlan brief
```

*Ports default to VLAN 1. Trunks like fa0/12 aren't listed under any VLAN.*

VLAN	Name	Status	Ports
1	default	active	Fa0/11, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gi0/1, Gi0/2
10	TEN	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
20	TWENTY	active	

S1# show vlan id 10

VLAN Name	Status	Ports
10 TEN	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/12

S1# show interfaces fa0/1 switchport

Name: Fa0/1  
Switchport: Enabled  
Administrative Mode: static access  
Operational Mode: static access  
Administrative Trunking Encapsulation: negotiate  
Operational Trunking Encapsulation: native  
Negotiation of Trunking: Off  
Access Mode VLAN: 10 (TEN)  
Trunking Native Mode VLAN: 1 (default)  
Administrative Native VLAN tagging: enabled  
Voice VLAN: none

S1# show mac address-table [ dynamic ]  
Mac Address Table

Vlan	Mac Address	Type	Ports
All	000c.85ca.e280	STATIC	CPU
All	000c.85ca.e281	STATIC	CPU
<i>These "CPU" ports are MAC addresses for our own switch There are lots of these, two for each interface in my case. Most omitted. Using the "dynamic" option would only skip them, giving us only the two lines we care about.</i>			
All	0180.c200.0010	STATIC	CPU
1	000d.29a1.868c	DYNAMIC	Fa0/12
10	000f.8f4b.b4a0	DYNAMIC	Fa0/1
<i>This is our access port in VLAN 10.</i>			

Total Mac Addresses for this criterion: 50

S1# show interfaces status

*Author Odom doesn't mention this command, but it's my favorite.*

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		connected	10	a-full	a-100	10/100BaseTX
Fa0/2		notconnect	10	auto	auto	10/100BaseTX
Fa0/3		notconnect	10	auto	auto	10/100BaseTX
Fa0/4		notconnect	10	auto	auto	10/100BaseTX
Fa0/5		notconnect	10	auto	auto	10/100BaseTX
Fa0/6		notconnect	10	auto	auto	10/100BaseTX
Fa0/7		notconnect	10	auto	auto	10/100BaseTX
Fa0/8		notconnect	10	auto	auto	10/100BaseTX
Fa0/9		notconnect	10	auto	auto	10/100BaseTX
Fa0/10		notconnect	10	auto	auto	10/100BaseTX
Fa0/11		notconnect	1	auto	auto	10/100BaseTX
Fa0/12		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/13		notconnect	1	auto	auto	10/100BaseTX

Check for shutdown VLANs.

S1(config)# vlan 20  
S1(config-vlan)# shutdown  
S1(config)# shutdown vlan 10

*Two different ways to shutdown (or "no shutdown") a VLAN.*

```
S1# show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/11, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gi0/1, Gi0/2
10 TEN	act/lshut	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
20 TWENTY	act/lshut	

```
S1#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		connected	10	a-full	a-100	10/100BaseTX
<i>The interface status stays connected even though it's in a shutdown VLAN that can't pass frames.</i>						
Fa0/2		notconnect	10	auto	auto	10/100BaseTX
Fa0/3		notconnect	10	auto	auto	10/100BaseTX
Fa0/4		notconnect	10	auto	auto	10/100BaseTX

## M I S C O N F I G U R E D T R U N K I N G

Check for misconfigured trunking (both ends of the link). One easy mistake (or test question) involves setting both ends of the link to DTP mode "dynamic auto." Since neither end of the link "actively desires" ("dynamic desirable" or "trunk") a trunk, it'll stay an access port. See CCENT, chapter 11 for details, specifically page 3 of my notes.

```
S1(config)# interface fa0/12
S1(config-if)# switchport mode dynamic auto
```

```
S1# show interfaces trunk
```

*The complete lack of output to this command tells us we have no operating trunks.*

```
S1# show interfaces fa0/12 switchport
```

```
Name: Fa0/12
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
```

If one end of the trunk link is mode "trunk" and the other "access," then both ends will be up/up but only traffic from the trunk's native VLAN will pass. The native VLAN works because its traffic is untagged. All other VLANs have a 4-byte tag inserted into the ethernet header and when the non-trunking side sees that header, the frame is discarded as illegal (bad ethertype field value).

Best commands to learn the operational (actual) trunking status on each side:

```
S1# show interfaces trunk
S1# show interfaces [ fa0/1 ] switchport
```

## U N S U P P O R T E D V L A N S O N A T R U N K

To pass over a trunk, a VLAN must be

- Existing and active on the switch (show vlan brief)
- One of the VLANs allowed across the trunk (default all)
- Not pruned on that trunk by VTP (see chapter 5)
- In an STP forwarding state (show spanning-tree vlan #)

The "show interfaces trunk" command displays three increasingly restrictive lists of VLANs. Only VLANs in the third list actually meet all the criteria to traverse the trunk.

```
S1# show interfaces fa0/12 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/12	on	802.1q	trunking	1

```
Port      Vlans allowed on trunk
Fa0/12    1-4094
```

```
Port      Vlans allowed and active in management domain
Fa0/12    1,10
```

*VLAN 20 is shutdown on S1, so doesn't make this list  
All the other VLANs were never created on S1*

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/12    1,10
```

*Only these will actually cross. Be aware that STP is slow and it can take time (30 secs. default) for a VLAN to show on this list after you fix a problem like the VLAN being shut down.  
Also, to successfully enter the other switch, VLAN 10 will need to exist there (it doesn't, but you can't tell from this end).*

#### D I F F E R I N G N A T I V E V L A N S

When frames within a trunk's native VLAN cross that trunk, they don't receive a trunking header telling the receiving switch which VLAN they're in. Since a trunk's native VLAN is configured on the interfaces at each end, they don't have to match. If S1 names VLAN 10 as its native VLAN and S2 names VLAN 20, then frames from VLAN 10 on S1 will enter the trunk untagged and be placed in VLAN 20 when they arrive at S2.