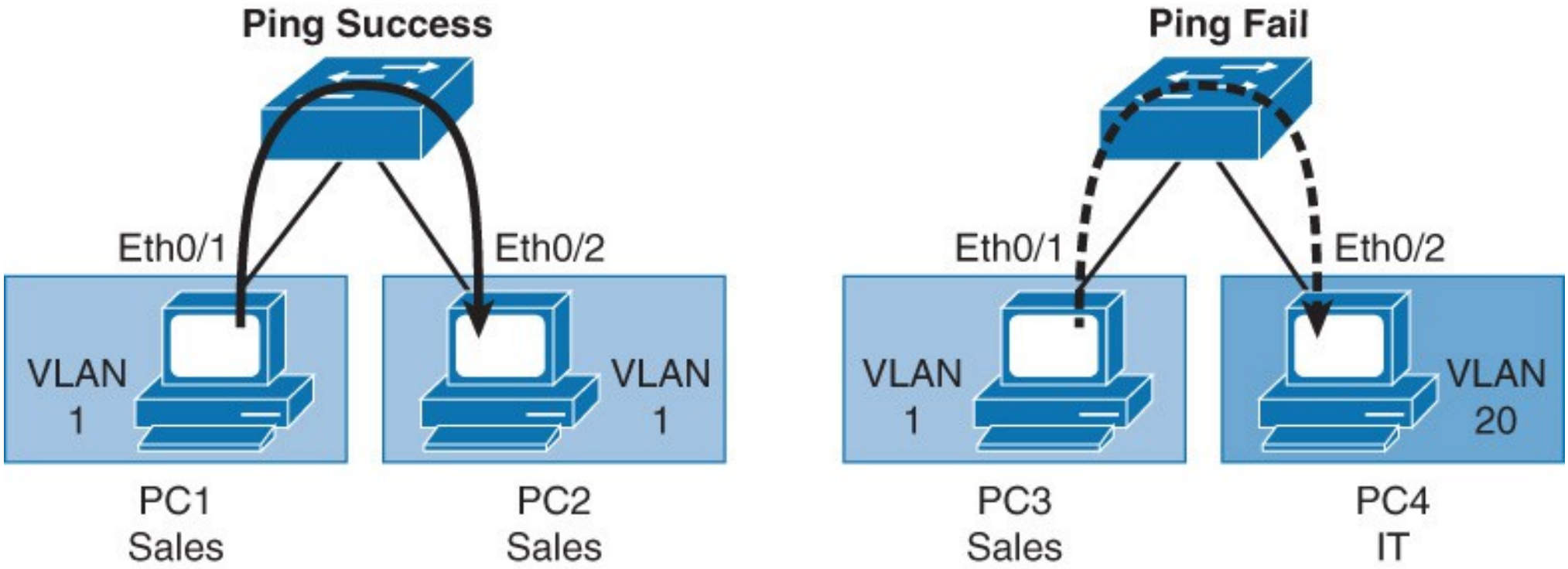
Extra (useful) details on **Campus Networks: VLANs, DTP, VTP, LAG (from NET3011 – 17W)**

VLANs: Avoiding a flat network

- VLANs isolate traffic and thus provide a logical broadcast domain
- Ports in the same VLAN share broadcasts; ports in different VLANs do not
- VLANs may exist on a single switch ("Local") or may span multiple physical LAN segments and switches ("End-to-end")
- VLANs are a L2 domain and thus every VLAN must terminate at (at least) one L3 routed port in order to go beyond the subnet

VLAN Operation



- VLAN is an independent LAN network.
- VLAN = broadcast domain.
- VLAN maps to logical network (subnet).
- VLANs provide segmentation, security, and network flexibility.

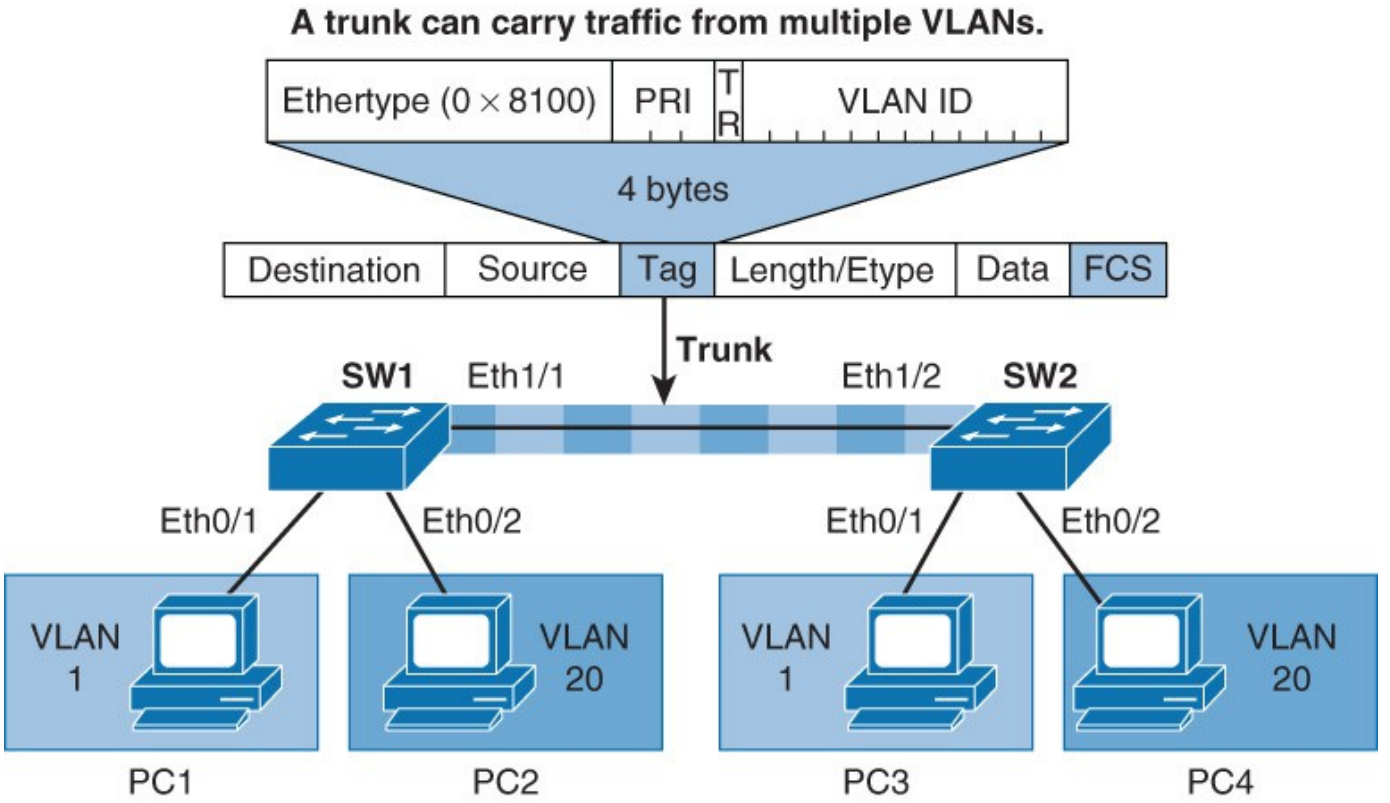
VLAN Organization

- ~~Five~~ ~~Six~~ ~~Seven~~ Eight generic types of VLANs:
  - **default** = VLAN 1 (also Native VLAN by default)
  - **native** = traffic on this VLAN isn't tagged
  - **data** = regular user traffic; may consist of many VLANs
  - **voice** = needed in modern campus networks (2001)
  - **wireless** = particularly for controller-based WLANs (2005)
  - **IoT** = extra protection for devices not often updated (2017)
  - **management** = for SSH, HTTPS, SNMP access
  - **garbage** or **black-hole** = for security purposes, a VLAN that is suspended and also never allowed on trunks; all un-used interfaces are placed in this VLAN.

Trunking Basics

- 2 methods of tagging: ISL and 802.1Q
- ISL is **dead**; you could forget about it *except* that many Cisco switches that (still) support it may need to have 802.1Q explicitly chosen in the configuration

Memorize the 802.1Q tag format!



Support for VLANs on Trunks

- Compare with Lotto 649 and Lotto MAX
- Now consider that different categories of switches (access, distribution) may be limited in the number of VLANs that can be "picked" simultaneously by the configuration.
- Examples:
  - 2960 can support 255 VLANs (250 + 5 std)
  - 3560 can support 1005 VLANs (1000 + 5 std)
  - 4000/6000 series supports 4094 VLANs (all)
- As a **separate** issue, number of simultaneous VLANs may be limited by STP ("Per VLAN STP")

Trunking Characteristics

- Trunk links have a *Native* VLAN which is the only VLAN whose traffic is ***not*** tagged;
  - by default = 1
  - best practice: choose & configure a native VLAN number that is unused for any other purpose
- Trunking *encapsulation* can be set, but only on Cisco switches that still support ISL; otherwise encapsulation is 802.1Q

Trunking Subtleties

- Interfaces are configured to strictly *access* mode, configured to strictly *trunk* mode, or configured for dynamic selection of either access or trunk mode
- *Describing* trunk characteristics is ***not*** the same as setting an interface to trunking mode! (Likewise, describing access mode characteristics does **not** configure an interface to access mode)
- *Unmanaged* switches completely ignore VLAN tags, which also means they will pass *all* traffic and thus can be used to join trunk links

Trunking and VLAN commands

- You hopefully remember the well-used commands:
  - show vlan [brief]
  - show interfaces trunk
- For additional details on a specific VLAN:
  - show vlan id {#}
  - show vlan name {vlan-name}
- Review all other VLAN and trunk configuration commands presented in the textbook(s)

DTP Basics

- Dynamic Trunking Protocol, a Cisco proprietary protocol (no known open standard equivalents)
- Only one purpose/function: negotiate the creation of trunk links dynamically, *if protocol is enabled*
- Has *nothing* to do with VTP
  … except Cisco mixed them together in one way: DTP won't work unless VTP domain names are identical on both sides of link ("null" can match)
- Exactly and only two options:
  – desirable = negotiate pro-actively
  – auto = negotiate passively ("Don't start nuthin!")

DTP Combinations

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Problem! ~~Limited Connectivity~~
Access	Access	Access	Problem! ~~Limited Connectivity~~	Access

Source: p. 54 of FLG, except caption is wrong there!

VTP Characteristics

- VTP is a Cisco proprietary protocol;
  GVRP and MVRP are open standard equivalents
- VTP will **only** communicate over trunk links.
- VTP always sends advertisements over *VLAN 1*,
  every 5 minutes or *whenever there's a change*,
  to a fixed multicast address (01:00:0C:CC:CC:CC),
  using an 802.3 frame (not Ethernet II)
- Key parameters for accepting a message:
  – version – revision number
  – domain name – password
  – MD5 hash (for above fields)

VTP Characteristics

- Versions 1, 2, 3 exist; each ver. has new features
  - ver 1 is **not** compatible with ver 2, but will "jump"
  - ver 3 **is** backwards compatible with ver 2, but not ver 1
- Ver 1: Basic protocol to dynamically xfer VLANs
- Ver 2: Several enhancements
- Ver 3: Covered briefly in NET3011-Advanced Sw

VTP modes

- Client: receive-only; cannot make any changes
  - but can *shutdown* a VLAN (!)
  - relays all messages from same domain
  - may adopt domain name from server if no password configured (but not in v3)
- Server: can make all changes (add/del/modify)
  - relays all messages from same domain
  - can *shutdown* and *suspend* a VLAN
  - may adopt domain name from server if no password configured (but not in v3)
  - v3 adds *Primary Server*, the only that can make changes
- Transparent: like server but with separate VLAN database
  - won't adopt domain name from any other server
- Off: like Transparent, except no forwarding; totally isolated!
  (on *Cisco* equipment, only available for IOS's that support VTP v3)

VTP Idiosyncracies

- Highest revision **trumps** all, regardless of mode!
- Ver 3: provides extended VLANs, but doesn't have 100% support (can't *shutdown* or *prune* them)
- *Ver 3: Primary Server*
  - configured in privilg'd exec and *not* global config
  - so not saved in either config or vlan.dat
  - so doesn't survive a reboot
- *Ver 3: only* the Primary Server can make changes
  - but must be manually configured *after* reboot
  - let's hope that no admins are in "panic" mode after a network crash, so that they don't make any mistakes!!

Beware: VLAN Nastiness with Cisco

- On Cisco switches, Server mode stored in vlan.dat trumps Transparent mode from startup-config !
- or: When trying to load a config with VTP Transparent mode, check for an existing vlan.dat because it will over-rule the Transparent mode!
- Check the log entries generated during bootup (ie. **`show logging`**)

Supplemental to textbook material!

```
...
Mar  1 00:00:43.889: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
Mar  1 00:00:47.588: VTP mode mismatches between startup-config: transparent,
                     vlan database: server.
Mar  1 00:00:47.596: %SW_VLAN-4-BAD_STARTUP_VLAN_CONFIG_FILE:
                     Failed to configure VLAN from startup-config.  Fallback to use VLAN
                     configuration file from non-volatile memory
Mar  1 00:00:47.596: %SYS-5-CONFIG_I: Configured from memory by console
Mar  1 00:00:48.528: %SYS-5-RESTART: System restarted –
...
```

VTP Messages

1.VTP Summary advertisement

Version (1 byte)	Type (Summary Adv) (1 byte)	Number of subset advertisements to follow (1 byte)	Domain name length (1 byte)
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number (4 bytes)			
Updater Identity (orginating IP address: 4 bytes)			
Update Time Stamp (12 bytes)			
MD5 Digest hash code (16 bytes)			

Source: Official Cert Guide, p. 129

VTP Messages

2.VTP Subset advertisment

0	1	2	3
Version (1 byte)	Type (Subset Adv) (1 byte)	Subset sequence number (1 byte)	Domain name length (1 byte)
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number (4 bytes)			
VLAN Info Field 1 (see below)			
VLAN Info Field ...			
VLAN Info Field N			

0	1	2	3
Info Length	VLAN Status	VLAN Type	VLAN Name Length
VLAN ID		MTU Size	
802.10 SAID			
VLAN Name (padded with zeros to multiple of 4 bytes)			

Source: Official Cert Guide, p. 130

VTP Messages

3.Advertisement Request

0	1	2	3
Version (1 byte)	Type (Adv request) (1 byte)	Reserved (1 byte)	Domain name length (1 byte)
Management Domain Name (zero-padded to 32 bytes)			
Starting advertisement to request			

4.Mystery message: propagates VTP pruning option