VLANS

LAN (Local Area Network)—All devices in the same broadcast domain (the set of devices that receive a copy of a broadcast frame sent by any of the others). Normally (without VLANs), this would be all interfaces on a switch.

VLANs (Virtual LANs)—allow you to divide the ports of a switch between different L2 broadcast domains, so you don't need a separate switch for each. A router is required to forward traffic between the VLANs at L3.

VLANs create more broadcast domains, each of which is smaller. Advantages include:

- Improved efficiency by reducing the number of broadcasts each host has to process
- Improved security by limiting exposure of devices to flooded frames (broadcasts, multicasts, and unicasts to MAC addresses that a switch doesn't recognize)
- Improved security by separating hosts that send sensitive data from the rest of the net—the payroll check printer can be on a separate VLAN
- Ability to group users by needs rather than location
- Rapid problem solving—often failure domains mirror broadcast domains
- Simplify STP (Spanning Tree Protocol) by limiting a L2 VLAN to a single switch. *STP is explained in CCNA 200-105 Chapter 3.*
- Savings on cost and space—several logical LANs can share the same hardware

TRUNKING

Trunking allows traffic from multiple VLANs to share the same connection between switches and to routers. This is good when the same VLAN exists across multiple switches. Frames are tagged with their VLAN ID before being sent over the trunk. When they arrive, the tag is removed.

ISL (Inter-Switch Link)—An old Cisco trunking protocol not supported in 2960 switches

802.1Q—The IEEE trunking standard. Inserts a 4-byte tag inside the frame header and calculates a new Frame Check Sequence (FCS). The maximum frame size is increased by 4 bytes to cope. The only part of this tag that we care about is the 12-bit VLAN ID, providing 4096 values divided into normal and extended ranges:

VLAN	Description
0	Reserved
1-1005	Normal (1002-1005 are pre-named and used for special non-Ethernet purposes)
1006-4094	Extended
4095	Reserved

Native VLAN—Frames from the native VLAN aren't given an 802.1q tag when they're sent across a trunk. In theory, this supports devices that don't understand trunking. On arrival, all untagged frames are placed in the native VLAN.

INTER-VLAN ROUTING

One subnet per VLAN. Data is *routed* between VLANs at L3 (IP), either using a router or a layer 3 switch instead of being *switched* at L2 (Ethernet).

Router-on-a-Stick—A trunk connects all of a switch's VLANs to a router over one physical link.

Layer-3 Switch—The L3 routing happens inside the switch hardware without slowing down for a trunk to a separate router.

CONFIGURING VLANS ON A SWITCH

```
SW(config)# vlan 2
SW(config-vlan)# name MY_VLAN

SW(config)# interface fa0/1
SW(config-if)# switchport mode access
SW(config-if)# switchport access vlan 2
```

As long as you didn't care about naming your VLAN (above), this would create it automatically

```
SW# show vlan brief
SW# show vlan id 2
```

VTP

VTP (VLAN Trunking Protocol)—A Cisco protocol that advertises VLANs from one switch to another. Mostly saved for ICND2.

VTP On	VTP Off or Transparent
Normal VLANs (1-1005) available	Normal and Extended (1006-4094) VLANs available
VLAN configurations stored in vlan.dat	VLAN configurations stored in running-config
Only VTP server switches can configure VLANs	Any switch can create VLANs
VTP server and client switches learn VLANs from each other, even having their VLANs remotely deleted.	VLANs are not learned or shared

Best practice for us is to turn VTP off until ICND2, or at least make each switch transparent to it.

```
SW(config)# vtp mode transparent
SW(config)# vtp mode off
SW# show vtp status
```

TRUNK CONFIGURATION & DTP

DTP (Dynamic Trunking Protocol)—can allow two switches to negotiate the trunking encapsulation (802.1Q or ISL) and whether to trunk at all.

```
SW(config-if)# switchport trunk encapsulation { dot1q | isl | negotiate }
```

If negotiate (dynamic) is chosen, DTP will choose an encapsulation that both switches support. If they both support both options, ISL will be used. (Just remember that they're Cisco's switches choosing Cisco's protocol.)

```
SW(config-if)# switchport mode {access | trunk | dynamic desirable | dynamic auto}
```

Switchport modes

Switchport Mode	Description
access	
trunk	
dynamic desirable	Actively tries to convince the other side to trunk
dynamic auto	(Default) Willing to trunk but won't initiate negotiations.

Trunking Outcomes—Notice that two "autos" won't trunk. Both will accept it; neither will cause it.

	Access	Trunk	Dyn. Desirable	Dynamic Auto
Access	Access	—	Access	Access
Trunk	—	Trunk	Trunk	Trunk
Dyn. Desirable	Access	Trunk	Trunk	Trunk
Dynamic Auto	Access	Trunk	Trunk	Access

Troubleshooting—for exam, be able to interpret "show interfaces switchport" and know if the interface should operationally trunk based on its administrative mode. [See CCNA notes, section 1-4(A) for exmple output of the following two commands]

```
SW# show interfaces switchport
```
Administrative Mode: What you configured, e.g. Dynamic Auto
Operational Mode: Actual status of the interface, i.e. outcome of the negotiations, if any
Administrative Trunking Encapsulation: what you set, e.g. dot1q
Operational Trunking Encapsulation: Actual state. May say "native," which on a 2960 is 802.1q

```
SW# show interfaces trunk
```
Only shows information about interfaces that are operation mode trunking.
Tells admin mode ("mode"), operational mode ("status"), encapsulation (e.g. 802.1q), native VLAN, and information about allowed, pruned, and STP forwarding VLANs.

Cisco's best practice is to disable negotiation for better security.

```
SW(config-if)# switchport nonegotiate
```
Notice that it's not "switchport mode nonegotiate."

Voice VLANs

Cisco IP phones include a switch that allows you to connect a desktop PC to the phone. The main Cisco switch has two VLANs on each interface. The voice VLAN is 802.1Q tagged, the PC receives the untagged "native" data VLAN traffic.

```
interface fa0/1
 switchport mode access
 switchport access vlan 10
 switchport voice vlan 15
```

```
SW# show interfaces fa0/4 switchport
```
Tells both the data and voice VLANs.

```
SW# show interfaces trunk
```
Shows our voice VLAN access port (fa0/1) as an access port, but in the 3 "VLANs allowed on trunk" sections, mentions that 2 VLANs, not just one are allowed on it. Without a voice VLAN, an access port would never be mentioned in those three sections.