Vlans – David Bombal Course
VLAN = broadcast domain = logical network (subnet)

A group of hosts with a common set of requirements (project teams, departments, etc), attached to the same broadcast domain regardless of where the are physically located (hosts in a VLAN can be spanned to multiple switches, but still belong the same subnet/broadcast domain. Though this is not recommended today).

VLAN advantages

- Segmentation (VLAN for HR, VLAN for Accounting, VLAN for Sales)
- Flexibility – you can change what subnet a host is one without changing cable physically.
- Security – users can be set to separate VLANs from servers or you can limit access to hosts with an ACL
- VOIP – you can put your IP Phones into a separate VLAN from other hosts, this provides security so the host connected to the VOIP phone cannot retrieve packets and listen in to calls, as host and phone are on separate subnets. QoS can assign priority to the Voice VLAN.

Assigning VLANs

- Statically – done by an administrator – Sw1(config-if)#switchport access vlan 20
- Dynamically – using a VLAN Management Policy Server (VMPS) – the assignment is based on the mac address of the host. For example, a CEO could take his laptop to the boardroom and plug into a switch in the boardroom, the VMPS would recognize this mac and give an IP within the VLAN assigned for the CEO. A manager could plug his laptop into the same switchport the next day and be assigned to a different VLAN, based on the VMPS config.
- Voice VLAN – used for IP Phones, for security and QoS priority

VTP (VLAN Trunking Protocol

- Cisco Proprietary
- Layer 2 protocol
- Allows for propagation of VLAN information
  - Addition, deletion and renaming of VLANs on one switch which updates the others
- Propagation across Trunk Links (can only be sent across trunk links)
- VTP can save time, but can also cause the VLAN database to be wiped out across all switches, if a new switch is added to the network improperly (with VTP enabled you must follow a specific procedure when adding a new switch, as the new switch will have no VLANs by default and a higher revision number)
  As such, many cisco net admins do not use VTP
- VTP messages are sent to this MAC address 01-00-0C-CC-CC-CC (floods CDP and VTP protocols)
- Messages:
  - Summary Advertisements
  - Subset Advertisements
  - Advertisement requests
- When setting up VTP devices by default will belong to null domain, for VTP to work you need to put devices into a specific VTP domain (only devices in the VTP domain will be updated with VLAN info)
- A switch can only belong to one VTP domain at a time
- VTP will not traverse a router, and only trunk links on a switch3
- Revision Numbers (increment by 1), when a change to the VLAN database is made on a Switch, the VTP rev # increments by 1, the change is sent to all the other switches in the VTP domain and they acquire that new rev #)

- VTP does not put ports into a specific VLAN, it just updates the VLAN db across devices

VTP Messages (in detail)

Summary Advertisements

- Sent every 5 min
- or whenever there is a change
- Informs other switches of the current VTP domain and configuration number

Summary Requests

- Switch has been reset
- VTP domain name has been changed
- Switch has received a VTP summary advertisement with a high rev # (asking for the changes to the VLAN db)

Subset advertisement

- Contains a list of VLAN information
- If there are several VLANs, more than one subset advertisement may be required

VTP Modes

Server – (default mode)

- a VTP switch in server mode can create, delete, or modify VLANs
- Sends and Forwards advertisements
- Synch's Database
- Saves VLAN configuration data locally

Client

- cannot create, delete, or modify VLANs
- Sends and Forwards advertisements
- Synch's Database (this leads to a VTP issue – where a new VTP client switch added to the topology has a high revision number from another VTP domain (its old deployment) and this client ends up replacing the VLAN db with its own configuration.

Transparent

Can create and

Administrative Mode	access	dynamic auto	dynamic desirable	trunk
access	access	access	access	misconfig
dynamic auto	access	access	trunk	access
dynamic desirable	access	trunk	trunk	access
trunk	misconfig	access	access	trunk