VLAN & Trunks – Summary Cheatsheet (ATech) – Part1

What is VLAN ??

"Logical division of a physical network into multiple logical networks irrespective of geographical conditions"

Advantages of VLANs

- ✓ Less Broadcast issues
- ✓ Improved Security
- ✓ Efficient Device Management
- ✓ Grouping by function instead of location
- ✓ Better Performance & Scalability
- ✓ Cost Reduction

VLAN ID Ranges

VLAN Range	Range	Detail
Normal VLANs	1 – 1005	*1=Default* *2-1001=Usable normal* *1002-1005 =Reserved/Defaults*
Extended VLANs	1006 – 4094	
Other VLANs	0, 4095	*Reserved*

VLAN Types

Type	Detail
Default VLAN	Assigned to every Port and are auto generated by Switch/System, Always 1. Carries STP Traffic as well.
Data VLAN	Carries user data traffic
Native VLAN	Assigned to every 802.1Q trunk port for backward compatibility. No tags.
Mgmt VLAN	Carries Network Management Traffic (ssh, Telnet). Defaults to 1.
Voice VLAN	Carries Voice Traffic only. Used for IP Phones mostly. No Tag & no priority usually.

Access Ports	Trunk Ports
✓ Access Ports belong to only one VLAN ✓ Access Ports are connected to end devices ✓ Access Ports don't modify the frames which pass through it	✓ Trunk Ports do not belong to any VLAN ✓ Trunk Ports can carry data with multiple VLANs ✓ Trunk Ports are used for connectivity between Switches

*Imp Points - VLANs

- ✓ All hosts in a subnet are always in the same subnet
- ✓ One VLAN = One Broadcast Domain
- ✓ The Switch keeps a separate MAC Table for each VLAN
- ✓ A Layer3 device is needed to route traffic b/w VLANs
- ✓ Layer2 Switches can't route the traffic between VLAN groups (they can route within one VLAN)

*Imp Points - Trunks

- ✓ Both ends of the Trunk Link must always be in the same native VLAN
- ✓ Manual and negotiated Trunking modes can't be mixed
- ✓ Subnetting and addressing must be correctly assigned
- ✓ The correct VLANs must be allowed on the trunk
- ✓ Always remove the extra VLANs from the allowed range