3.1t Transcript

VLANs are separate layer 2 ethernet networks, created with switches that propagate broadcast traffic between the switches, this will not stop until it reaches the gateway routers, the borderline where the broadcasts stop, and as you can imagine through a lot of broadcast been sent over the network for services like ARP, DHCP, which creates a lot of traffic to 1 of the motivations for introducing VLANs is to is to split down these broadcast domains into smaller chunks. So basically, partitioning the LAN into multiple VLANs, each VLAN is its own broadcast domain and it has its own subnet associated with it.

VLANs are mutually isolated, so if a host is transmitting information in one VLAN, it cannot be received by a host in another VLAN without the intervention of a router to route between VLANs. If this is required, it is referred to as Inter-VLAN routing. VLANs are implemented in switches at layer 2 networks, partitioning is done inside the switch and different ports belong to VLANs. Host grouped within the VLAN don't even know the VLAN exists. VLANs only exist between switches and not between the switch and the router.

VLANs operate regardless of physical location. So, for example, we have a three-story building and VLANs IT, HR and the sales department are interspersed between these three floors, yet we can have VLANs which exist irrespective of physical location. Prior to VLANs been introduced, we usually had to situate a particular department in a particular location and isolate those networks. Now with VLANs, we don't have that restriction. It’s important to note that also that VLANs are usually also in different subnets at layer 3.

What are the other benefits of VLANs? Well security is an obvious one because traffic from one network can't talk to another. The added security reduces cost because you don't have to oversee requirement to move equipment about, you can just configure a port for a particular VLAN. This offers better performance, because you can shrink the broadcast domain size, therefore reducing the broadcast traffic, so you're reducing the clog on the network. Staff efficiency is improved because it's very straightforward and easy to move a particular machine from one VLAN to another.

There are numerous types of VLAN we see on networks today. Usually we will have a data VLAN, voice VLAN, a native VLAN and management VLAN, let's go through those one at a time. The data VLAN is basically any kind of standard data traffic such as web, email and so on, and basically what is not included in this is things like VoIP, which would be on a separate VLAN with higher priority quality of service. A default VLAN is basically VLAN 1, which is the default VLAN when the switch boots up in factory settings. A native VLAN is used to carry untagged traffic, this is traffic from legacy switches that don't support the VLAN tagging and any traffic on that basis has to be transported over the native VLAN. Lastly, the management VLAN is used, as it suggests, to manage the switch and it is assigned its own VLAN and IP address to manage the switch and other devices. VLAN 1, as mentioned previously, is the default VLAN when the switch boots up from cold, without any configuration on it, all the ports from the switch will be in the default VLAN and as we can see here, we do the show VLAN brief command then VLAN 1 are all members of this VLAN by default. VLANs also belonging VLAN 1 is also not a good practice from a security standpoint, so usually you would change that. It is important to note that VLAN 1 can't be renamed or deleted so it stays on the switch, even if there are no ports assigned to it. VLAN 1 will always exist.

Voice VLANS carry voice traffic and are time sensitive. Voice doesn't like delay or jitter and suffers badly if this is an issue on the network. It is therefore necessary to ensure there is enough bandwidth for voice quality to be sufficient to make a call. We do this by ensuring the voice traffic is prioritized over other types of traffic, this is known as Quality of Service. Voice traffic ideally should hold a delay of less than 150 ms across the network to enable good quality voice calls and basically enabling the voice VLAN enables this.

VLAN trunks only exist between switches and other switches or switches and routers. They don't exist between switches and hosts. Trunks are links that carry multiple VLANs rather than a single VLAN which a for example, A PC will be a member of a trunk link that is carrying multiple VLANs and this is usually between switches. So basically, if we have, for example, a PC on a particular connection to a particular switch and that's trunk to another switch, and a PC is connected to the adjacent switch, then both of those PCs in the same VLAN will be able to communicate because the frame will be tagged over the trunk link, so a VLAN trunk is not associated with a particular VLAN, it basically just carries all the VLANs, or a specified list of VLANs and neither of the trunk ports are used to establish the trunk link. There is a trunking protocol known as IEEE 802.1Q, which tags the frames going over the trunk link with a special header which identifies what VLAN the frames come from.