VLANs

- Routers operate at Layer 3 of the OSI stack
- Hosts in separate IP subnets must send traffic via a router to communicate
- Security rules on routers or firewalls can be used to easily control what traffic is allowed between different IP subnets at Layer 3
- Routers do not forward broadcast traffic by default
- They provide performance and security by splitting networks into smaller domains at Layer 3

- Switches operate at Layer 2 of the OSI stack
- They do forward broadcast traffic by default
- By default a campus switched network is one large broadcast domain
- Switches flood broadcast traffic everywhere, including between different IP subnets
- This raises performance and security concerns

The Problem

- Switches flood broadcast traffic everywhere, including between different IP subnets
- This affects security because the traffic bypasses router or firewall Layer 3 security policies
- It affects performance because every end host has to process the traffic
- It also affects performance by using bandwidth on links where the traffic is not required

Solution

- We can increase performance and security in the LAN by implementing VLANs on our switches
- VLANs segment the LAN into separate broadcast domains at Layer 2
- There is typically a one-to-one relationship between an IP subnet and a VLAN

VLAN Access Ports

- VLAN access ports are configured on switch interfaces where end hosts are plugged in
- Access ports are configured with one specific VLAN

- The configuration is all on the switch, the end host is not VLAN aware
- Switches only allow traffic within the same VLAN

SW1(config)#vlan 10
SW1(config-vlan)#name Eng
SW1(config)#interface FastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config)#interface range FastEthernet 0/3 - 5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10

SW1#show vlan brief
SW1#show interface FastEthernet 0/1 switchport

VLAN Trunk Ports

- An access port carries traffic for one specific VLAN
- Dot1Q trunks are configured on the links between switches where we need to carry traffic for multiple VLANs
- ISL (Inter-Switch Link) was a Cisco proprietary trunking protocol which is now obsolete
- When the switch forwards traffic to another switch, it tags the layer 2 Dot1Q header with the correct VLAN
- The receiving switch will only forward the traffic out ports that are in that VLAN
- The switch removes the Dot1Q tag from the Ethernet frame when it sends it to the end host

Trunk Port Configuration
SW1(config)#interface FastEthernet 0/24
SW1(config-interface)#description Trunk to SW2
SW1(config-interface)#switchport trunk encapsulation dot1q
SW1(config-interface)#switchport mode trunk

Allowed VLAN Configuration
SW1(config)#interface GigabitEthernet 0/1
SW1(config-if)#switchport trunk allowed vlan 10,30

Hypervisors - VLAN Aware Hosts

- End hosts are typically members of only one VLAN and are not VLAN aware

- A special case is virtualized hosts, where there are virtual machines in different IP subnets on the host
- In this case we need to trunk the VLANs down to the host

Voice VLAN Configuration
SW1(config)#interface FastEthernet 0/10
SW1(config-interface)#description IP Phone
SW1(config-interface)#switchport mode access
SW1(config-interface)#switchport access vlan 10
SW1(config-interface)#switchport voice vlan 20

The Native VLAN
- The switch needs to know which VLAN to assign to any traffic which comes in untagged on a trunk port
- This used to be required for when a switch was connected to a hub. Hubs are Layer 1 devices so are not VLAN aware
- The Native VLAN is used for this
- The default Native VLAN is VLAN 1
- There are some security issues with using VLAN 1 as the Native VLAN so best practice is to change it to an unused VLAN
- The Native VLAN must match on both sides of a trunk for it to come up

Native VLAN Configuration
SW1(config)#vlan 199
SW1(config-vlan)#name Native
SW1(config)#interface GigabitEthernet 0/1
SW1(config-interface)#description Trunk to SW2
SW1(config-interface)#switchport trunk encapsulation dot1q
SW1(config-interface)#switchport mode trunk
SW1(config-interface)#switchport trunk native vlan 199

SW1#show interface gig0/1 switchport

Dynamic Trunking Protocol DTP

DTP configuration:
- *Switchport mode dynamic auto*: will form a trunk if the neighbour switch port is set to trunk or desirable. Trunk will not be formed if both sides are set to auto. Default on newer switches.

- *Switchport mode dynamic desirable*: will form a trunk if the neighbour switch port is set to trunk, desirable or auto. Default on older switches.
- *Switchport nonegotiate*: disables DTP

It is however recommended to manually configure switch ports

- Manual configuration:
  - *switchport mode access*
  - *switchport mode trunk*

VLAN Trunking Protocol VTP

- The VLAN Trunking Protocol (VTP) allows you to add, edit or delete VLANs on switches configured as VTP Servers, and have other switches configured as VTP Clients synchronise their VLAN database with them
- This can be convenient if you manage a large campus
- You will still need to perform port level VLAN configuration on the switches

VTP Modes

- VTP Server: Can add, edit or delete VLANs. A VTP Server will synchronise its VLAN database from another Server with a higher revision number.
- VTP Client: Cannot add, edit or delete VLANs. A VTP Client will synchronise its VLAN database from the Server with the highest revision number.
- VTP Transparent: Does not participate in the VTP domain. Does not advertise or learn VLAN information but will pass it on. Can add, edit or delete VLANs in its own local VLAN database.

SW1(config)#vtp domain Flackbox
SW1(config)#vtp mode server
or
SW1(config)#vtp mode client
or
SW1(config)#vtp mode transparent
SW1(config)#vlan 20
SW1(config-vlan)#name sales
(Cannot add VLAN if VTP Client)

SW1#show vtp status

Inter-VLAN Routing

1. Router with separate interfaces
2. Router on a stick
3. Layer 3 switch

VLANs and IP subnets in the LAN

- There is typically a one-to-one relationship between an IP subnet and a VLAN in the LAN campus
- For example Engineering hosts are in IP subnet 10.10.10.0/24 and VLAN 10, and Sales hosts are in IP subnet 10.10.20.0/24 and VLAN 20
- Hosts are segregated at Layer 3 by being in different IP subnets, and at Layer 2 by being in different VLANs
- Hosts in different IP subnets need to send traffic via a router to communicate with each other

R1(config)#interface FastEthernet 0/1
R1(config-interface)#ip address 10.10.10.1 255.255.255.0
R1(config)#interface FastEthernet 0/2
R1(config-interface)#ip address 10.10.20.1 255.255.255.0
R1(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.2

SW1(config)#interface FastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config)#interface FastEthernet 0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20

Router on a Stick

- You do not need a separate physical interface for every VLAN – you are less likely to run out of interfaces
- Traffic being routed within the campus has to go up and down the same physical Ethernet cable to the router – there is more contention for bandwidth than when using separate interfaces

R1(config)#interface FastEthernet 0/1
R1(config-interface)#no ip address
R1(config-interface)#no shutdown
R1(config)#interface FastEthernet 0/1.10

R1(config-interface)#encapsulation dot1q 10
R1(config-interface)#ip address 10.10.10.1 255.255.255.0
R1(config)#interface FastEthernet 0/1.20
R1(config-interface)#encapsulation dot1q 20
R1(config-interface)#ip address 10.10.20.1 255.255.255.0
R1(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.2

SW1(config)#interface FastEthernet 0/1
SW1(config-if)#switchport mode trunk

Layer 3 Switch

- Traffic being routed within the campus is routed across the switch backplane, it does not need to travel over physical cables to an external router
- You may still need an external router for WAN connectivity and services

Inter-VLAN Routing Configuration
SW1(config)#ip routing
SW1(config)#interface vlan 10
SW1(config-if)#ip address 10.10.10.1 255.255.255.0
SW1(config)#interface vlan 20
SW1(config-if)#ip address 10.10.20.1 255.255.255.0

WAN Routing Configuration
SW1(config)#interface FastEthernet 0/1
SW1(config-if)#no switchport
SW1(config-if)#ip address 10.10.100.1 255.255.255.0
SW1(config)#ip route 0.0.0.0 0.0.0.0 10.10.100.2

R1(config)#interface FastEthernet 0/1
R1(config-interface)#ip address 10.10.100.2 255.255.255.0
R1(config)#interface FastEthernet 0/2
R1(config-interface)#ip address 203.0.113.1 255.255.255.0
R1(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.2
R1(config)#ip route 10.10.0.0 255.255.0.0 10.10.100.1