Switch: Connects devices together on a Network. Note: if VLAN is involved then this definition changes: if devices are connected then they must be on the same network. Wrong…

Hub: Connects devices together on a network BUT it is dumb as it can only broadcast packets to all devices connected (IE repeater). Half duplex requires CS collision detection

Router: sends packets to devices on different networks or subnetworks**. (Refer to DataANS3 for definition in subnet context.)** The above is very basic one don't use

- The reason why it is also sub networks is because a network can have two mini networks in it and in order for devices on the two sub networks to communicate or forward packets it will need the use of router

Ethernet Switches: [When switches receive frame]

- Forward frames only to intended mac addresses
- Stores Mac addresses in a table which maps addresses of connected devices to ports on the switch
- Mapping created based on the source address of received frame
- If the switch were to receive a frame and it was for an unrecognised host, the switch would propagate the frame to all but the incoming port
- Types of Ethernet switching methods:
    - **Store and forward switching:**
        - Read *entire* frame into memory before forwarding
        - Higher Variable latency (slower) since entire frame must be recived
    - **Cut-through:**
        - Begin forwarding frame as soon as destination is known
        - Lower Variable latency (faster) but may result in errors since sending corrupt packet sent

Multilayer Switching: (no need for router)

- Switches are generally thought of as a layer 2 device but they do *support some routing* (Layer 3/Network layer)
- Usually Ethernet based switches and they are used to specifically do inter-vlan routing which is popular as it reduces the need of routers within the organisation
- Multilayer switches use info from layer 2 set up and optimisations to route at high speed

Address Resolution Protocol: Data link layer protocol (So when you ping a device it pings ip address not ip so this is the translation method of Ip to mac). <u>So when you send packets from host to host you need to know the Mac address of the destination</u>

- Host transmitting over local network are responsible for mapping Ip address → Mac addresses
- Address resolution protocol creates and maintains a list of mappings in ARP Table
- Host check their ARP table before transmitting packets bound for local network

- If No mapping then *Arp request* generated will be broadcasted
- The host with Ip address in the ARP request will transmit the ARP reply which is it's MAC address. The requesting host will receive the reply and enter it in it's ARP table for future purposes

Types of Transmission for Ethernet Frames:

- **Unicast:** transmit frames to single device using the destination Mac address
- **Multicast:** transmits frames to group of devices using multicast address
- **Broadcast:** transmit to all devices within broadcast domain using, **broadcast mac address**

Collision Domains: Logical network boundary inside which transmission occurring simultaneously will collide. **Think manly where it collides. A PC connected to switch will collide at switch with 1 link. But segments connect directly to hub will not collide**

- 1 Collision domain for all the lines connected to switch/router
- **Hub = 1 CD for everything connected to hub and the line coming out of hub**
    - **Everything coming out of hub + In hub = only 1**

    https://www.youtube.com/watch?v=_c1gqcr6Lcs

Broadcast domains: Logical network boundary inside which all devices can be reached by layer 2 broadcast. **THINK: How many networks are there? A router**

- **Router: separate broadcast domain/Networks ie:** turns 1 broadcast domain into two
- **Router to router = 1 network/Broadcast domain**

Straight through vs Cross over:

- Pairs 2 and 3 are swapped on one end
- Think straight through: all wires same on both ends
- Crossover: middle wires different on both ends

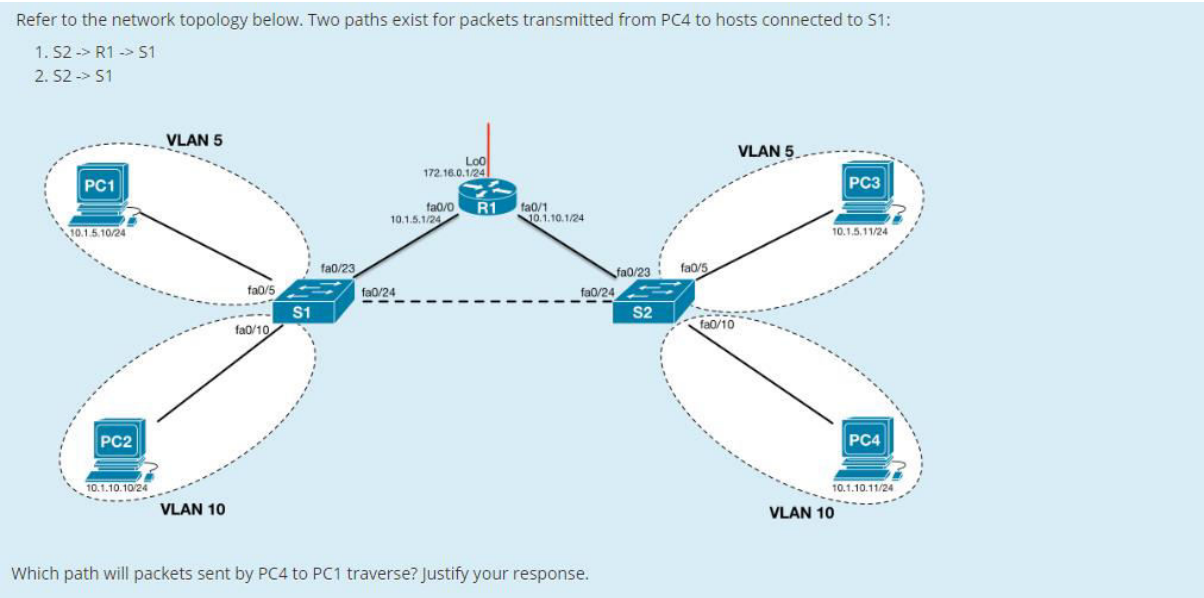
Structured Cabling Types:

- Horizontal cable: cables running between PC to Local Switch (In between the two should be a patch panel usually)
- Patch Panels: physical layer devices that provide cable extension
- Backbone/vertical cabling: cables running between telecommunication closets (usually between intermediately devices)

Vlan (Virtual LAN): ie divide devices on the single switch into networks.

- Two devices on the **same** vlan can communicate even if they are on different switches
- Logical networks that enable hosts in different physical locations to communicate as though they were on same network segment
- Enables the network administrator to create a smaller networks on one single switch
- Each Vlan becomes their own logical network and identifies vlan using Vlan ID
    - Vlan Id
- So two devices on same VLAN can communicate with each other

Picture Explain:



- Firstly to tell if devices is on the same network you need to look at the host identification. (10.1.5 or 10.1.10)
    - The subnet mask identifies the host identification
- As you can see the host identification for PC1/3 are the same (10.1.5) but PC2/4 (10.1.10) are different.

    - For understanding purposes: Since all devices are in the same broadcast domain (1 router) then we can assume we are dealing with sub networks or since all devices have **10.1**

- This suggest those groups are on different ~~**(sub [understanding purposes])**~~ network due to the implementation of a VLAN
- The router therefore is needed in order to send packets devices on different networks

***NOTE DON'T OVER Complicate things DON'T THINK IN TERMS OF SUB NETWORKS JUST THINK in terms of NETWORK. Assume NETWORK = SUB NETWORK**

Advantages of Vlan:

- Reduced equipment cost: A single switch can now be used for multiple networks
- Improved security: traffic can be isolated based on vlan tags
- Reduces Performance overhead: broadcast are contained within a vlan
- Simplified network management: configuration changes can be applied to all the users on a vlan as they share similar requirements/roles

Vlan Trunking: (So in order to connect 2 vlan networks you need lots of wires so use vlan trank)

- Links that can carry traffic for multiple VLANS
- Ethernet frames must be tagged before switches receive so they can identify where it belongs
- Tagging done using 802.1Q

Default vlan: where all ports on switch are going to be on Vlan 1 by default

Native vlan:

Inter-Vlan:

- Vlans are individual Ip subnets so hosts on different vlan can't communicate with each other so we use inter-vlan. Allows two vlan to communicate with each other
- Normally one switch and one router interface per vlan. Different approaches
- **Router-on-a-stick:**
    - Single trunk link carries traffic for multiple vlans between a switch and router
    - But requires a physical router (think single trunk between router and switch)
    - Router uses 802.1Q tags to determine how packets should be routed
- **Multilayer switching:**

Spaning tree protocol:

- Networks to be designed to be more fault tolerant (think if switch goes down then its fine). Therefore Redundant links between switches are used/created so that fewest users are effected by any outage

- Disadvantage: creates loops in switched network this means that packets may loop around and in some cases if the packet keeps looping past Time to live then it will be dropped or if Ethernet will loop forever wasting bandwidth. Therefore use **spanning tree protocol**

- So spanning tree protocol will prevent switching loops by disabling redundant links until they are needed in which they are activated.
- Creates a logical tree structure consisting of loop free leaves and branches.

***Add tagging/understand it?**