Module Six

CSG1105 Applied Communications

VLANs & DHCP

- This module covers two topics:
  1. VLANs - Virtual LANs: provide virtual broadcast domains
  2. DHCP - Dynamic Host Configuration Protocol: Automated TCP/IP configuration on hosts

Switched Routed Network 1

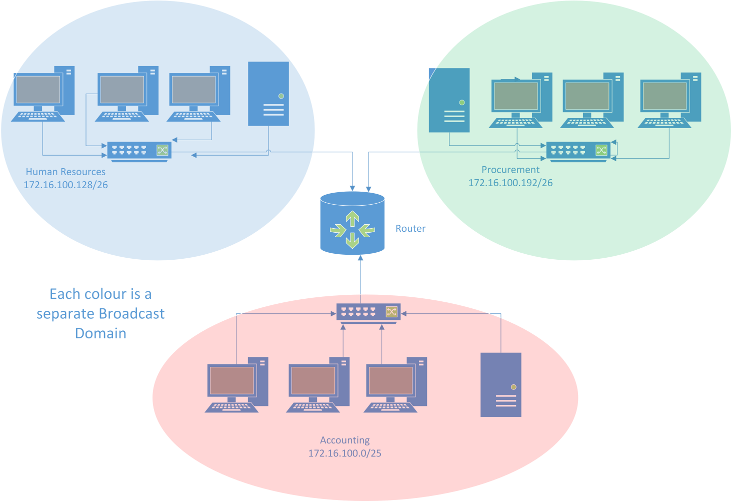

Figure 1: Switched/Routed Network

Switched Routed Network 2

- In Module Four, we looked at how a network could be divided into broadcast domains using a router (see previous slide)
- All resources of HR, Procurement and Accounting are grouped in close proximity and are able to use the same switch.
- It has the downside of co-locating the servers with the workgroup, moving them from a centralised, secured location.
- It also requires the users of the workstations to be in the one location
- There will be some latency on inter-subnet communications via the router
- The upside is decreased broadcasts
- While improving network broadcast performance , it may not fit well with the organisational structure

VLANs

- VLANs - Virtual LANs: provide virtual broadcast domains by
  1. Adding a VLAN tag field to an Ethernet frame to identify membership of a specific VLAN
  2. Ports on Managed switches being configured to be a member of a specific VLAN
  3. Frames are now delivered only to ports that have a matching VLAN tag as well as an entry in the MAC switching table

Destination MAC	Source MAC	802.1q Tag*	Ether Type	Payload	FCS
6 Bytes	6 Bytes	4 Bytes	2 Bytes	46-1500 Bytes	4

*Optional

Figure 2: Ethernet Frame

- The 802.1q tag contains a 12 bit field for the VLAN Identifier allowing values 1 through 4096
- Although there are 4096 possible values, generally only a small number are used. In CISCO devices, some of these values have special functions.

VLAN Connections 1

- When a port on a switch is configured for VLAN access it may be one of two types:

1. An Access Link or a
2. A Trunk Link

Access Links

- This link type is used to connect to a device that only supports the standard Ethernet frame format e.g. most PC NICs
- The ports connecting most workstations will be configured as Access Links
- An Access Link port only supports a single VLAN assignment
- If a switch is connected to an Access Link port, all devices connected to that port will be in the one broadcast domain

VLAN Connections 2

Trunk Links

- Ports configured as Trunk support multiple VLANs.
- Trunk Links are usually used to connect two switches or a switch to a VLAN capable router
- Trunks carry a *Logical* connection for each VLAN carried over a single *Physical* connection
- The 802.1q tags allow a receiving switch to select the destination port on
  1. VLAN ID
  2. MAC address

VLAN Network

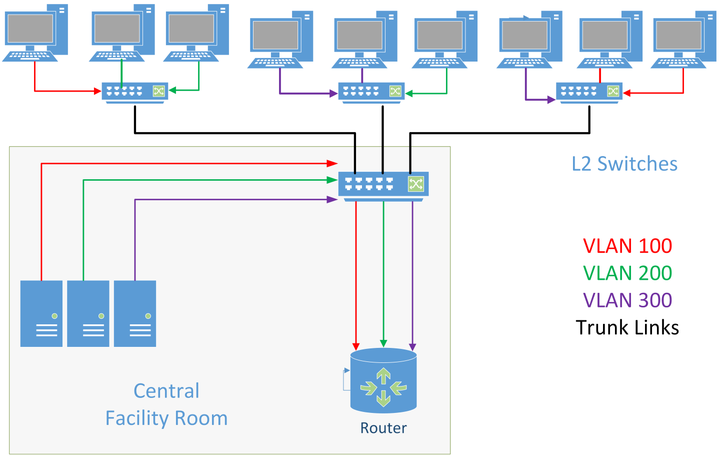

Figure 3: VLAN Network

VLAN Advantages

- Reduce the size of broadcast domains
- Per port configuration permits higher security. Users of each VLAN can't see broadcast traffic from other VLANs
- Location independence. Workstations and devices don't have to be connected to the same switch to be members of a subnet
- Users may be grouped by job category or security clearance rather than physical location
- Some switches can assign a higher priority to a specific VLAN

Layer Three - 1

- Each VLAN is a broadcast domain and therefore will be an IP subnet
- Communication between subnets requires a routing device
- Any communications between VLANs, even on the same switch will require to be routed at layer three.
- If the router is not aware of 802.1q tags, there will need to be a physical connection for each VLAN, each switch connection to the router will be configured in access mode
- This is not a big issue if there are a small number of subnets, but for larger numbers of subnets, many cables and expensive router ports are required

Layer Three - 2

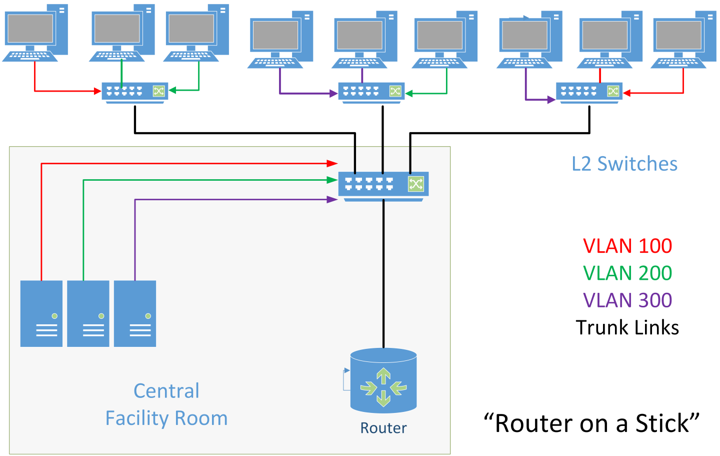

Figure 4: 802.1q aware Router

Layer Three - 3

- One solution is a “Router on a Stick”
- This requires a router that understands 802.1q tagging
- A trunk connection exists between a core switch and the router
- On the router, logical “sub-interfaces” are associated with each VLAN
- Each sub-interface is assigned an IP address
- Each sub-interface becomes default gateway for appropriate VLAN/IP subnet

Layer Three - 4

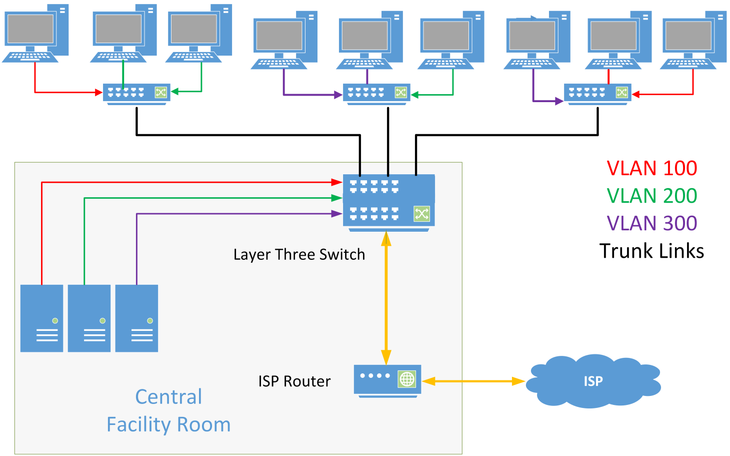

Figure 5: Layer Three Switch

Layer Three - 5

- Previous module discussed switch vs router performance - “switch where you can, route where you must”
- Switches have higher performance than routers
- A *Multi-Layer* switch can use ASIC circuitry to either switch **frames** at **layer 2** *or* switch **packets** at **layer 3**
- The administrator creates an **SVI** (switched virtual interface), associated with a VLAN and assigns it an IP address. This becomes the default gateway for the subnet associated with that VLAN
- The switch is able to interpret the destination IP address in a packet and switch it to the appropriate SVI
- Using a multi-layer switch eliminates the link to a router and removes the requirement that occurs in the router of L2-L3-L2 as the packet moves between interfaces.

Layer Three - 6

- So, do we still need routers?
- Yes, Multi-layer switches operate within a LAN
- For protocol conversion, access control, NAT and WAN/Internet links a router is still required
- Multi-layer switch may be used for internal subnets
- A router with fewer ports may be used for external network access.

Double Tagging

- Some ISPs now provide the capability of using Ethernet as a WAN protocol
- The customer's LAN device adds a C-Tag (Customer Tag)which is used internally as described above
- The ISP adds a second tag called a S-Tag (Service Tag) that allows the ISP to switch traffic within it's network
- This would allow VLAN tagged traffic to be moved between sites owned by the same customer
- The Double Tagging standard is documented in IEEE 802.1ad (also known as Q-in-Q)

Configuring IP Networks

- We've seen in previous modules that each host on a network needs to be configured with a number of parameters in order to participate in TCP/IP connections
- The parameters we have seen are:
  1. IP Address
  2. Subnet Mask
  3. Default Gateway
- Setting these parameters is not an issue in a small network, but is a major task in a large network
- Some of the issues are:
  - Ensuring there are no duplicate IP addresses within a subnet
  - Track IPs and workstations in use and those retired to reuse IPs
  - Assigning temporary IPs to devices that are not always present, such as mobile phones, tablets and laptop PCs

DHCP - Dynamic Host Configuration Protocol

- DHCP is a method for automating the IP network configuration of a device
- Devices requiring configuration run a **DHCP Client** which generally on OS startup request an IP address and other configuration data
- Each IP subnet requires access to a **DHCP Server** that will assign and track allocated IP addresses
- If a DHCP server is unavailable, workstations will self-assign an IP address using **APIPA**

DHCP Server

- A DHCP Server is configured with a pool of IP addresses and other configuration data for each of the subnets it services
- When requested, it will allocate an IP to a client using one of three methods:
  1. Dynamic Allocation - allocates an IP **lease**. If the lease period expires without the client renewing, the IP address is returned to the available pool
  2. Automatic Allocation - Assigns an IP from the available pool, but will remember which client requested the IP and reallocate it to that client
  3. Manual Allocation (reservations) - allocates an IP based on the client's MAC address from settings created by the server's administrator
- On home networks, the ISP Router/Modem is usually also the DHCP server
- On large networks, a central DHCP server not directly connected to the subnet may be reached by using a **DHCP Relay Agent**

DHCP Protocol

- The DHCP protocol uses **UDP** on port 67 for the server and port 68 for the client
- The communication between client and server consists of four steps
  1. **D**iscover
  2. **O**ffer
  3. **R**equest
  4. **Acknowledge**
- The mnemonic DORA is used to summarise the steps

DORA 1

Discover

- At the time of the Discovery message, the DHCP Client is unaware of the Server's MAC or IP address
- The Discovery message is a **Broadcast** either to 255.255.255.255 (which will translate to MAC FF:FF:FF:FF:FF:FF). If the client has retained any settings from a previous session, it may use a directed broadcast using the subnet broadcast address (e.g 192.168.0.255). It may also include a request for a previously used IP address

Offer

- On receipt of a DHCPDiscover request, a DHCP Server reserve an IP will respond with
  - the IP address
  - the subnet mask
  - the lease duration
  - the IP address of the Server

DORA 2

Request

- Based on the DHCPOffer message, a DHCP Client will
  - respond to **a single** DHCP Server. (It is possible to have multiple DHCP servers on a subnet)
  - reply with a request that includes the IP address of the server
  - broadcast the reply to inform other servers their offered IP is not needed

Acknowledge

- Based on the DHCPRequest message, a DHCP Server will
  - reply with a DHCPACK message
  - send the lease duration and any other configuration data requested

DHCP Configuration - Other

- In addition to the IP Address, the DHCP Server provides:

1. DHCP Server Identifier
2. IP Address Lease Time
3. Subnet Mask
4. Router address (default gateway)
5. DNS Server address
6. A default domain name
7. A client identifier (MAC address)

- There are other options that may be configured for delivery fro the DHCP server

DHCP Servers

- A DHCP Server can:
  1. be a router. ISP provided routers contain a DHCP server for the internal network, serving addresses from a private IP range. Commercial routers like CISCO products may be configured to provide a DHCP server
  2. be any host. Any computer with a NIC may be configured to run a DHCP server. Recall that a DHCP client broadcasts a DHCPDiscover message and may be responded to by more than one DHCP server. This has the potential to permit a “Man in the Middle” attack
  3. be a host, not necessarily connected to a local subnet. As long as there is a DHCP Relay on the local subnet that can forward requests to the remote DHCP Server
  4. be configured with redundancy. Two DHCP servers with a split pool of addresses. If one becomes unavailable, the other can continue to serve IP addresses from a distinct range.
  5. be used by ISPs to provide you with your external IP address

APIPA - Automatic Private IP Addressing

- In RFC3927, the IETF reserved the range 169.254.0.0/16 for **link-local** addressing
- If a DHCP server is unavailable, the client randomly assigns an address in the above range
- It then uses an ARP broadcast to check that the address is not already in use by another device
- If no reply from the ARP broadcast, the address is given to the workstation
- APIPA addresses can only be used within the subnet and may allow limited communications within the subnet
- APIPA addresses, like private IP addresses cannot be used for external IP connections