Building Cisco Multilayer Switched Networks (BCMSN)

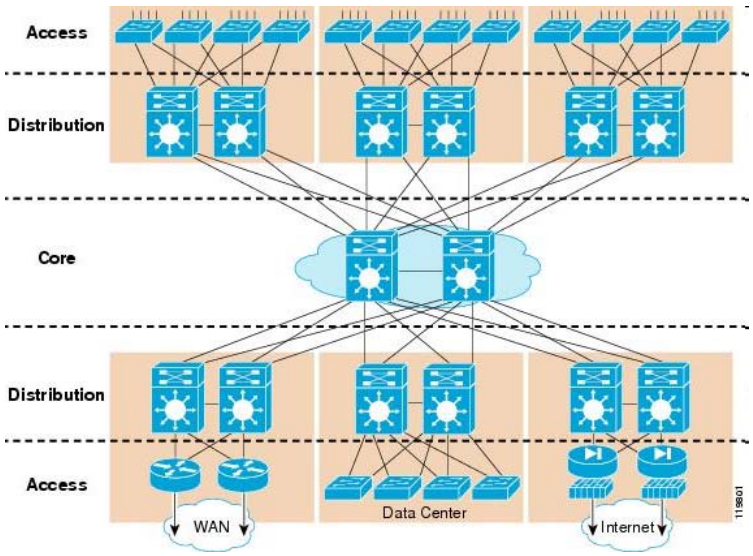
Hierarchical Campus Network Design Overview

http://www.INE.com

Hierarchical Campus Network Design Overview

- Per Cisco, a three layer "*hierarchical model to design a modular topology using scalable 'building blocks' that allow the network to meet evolving business needs. The modular design makes the network easy to scale, understand, and troubleshoot by promoting deterministic traffic patterns.*"
- The building blocks are…
  - Access layer
  - Distribution layer
  - Core (backbone) layer

Campus Network Example



Why Building Blocks?

- Easy to replicate, redesign, and expand
- No need to redesign entire network when a block is added or removed
- Can be added and removed without impacting the rest of the network
- Eases troubleshooting, fault isolation, and management

The Access Layer

- Point of entry for end nodes into the network
  - e.g. desktops, IP phones, printers, etc.
- Typically comprised of Layer 2 Switches, but can also be Layer 3 Switches
- Multiple connections to Distribution Layer for redundancy
- Offers services such as…
  - Broadcast domain segmentation (VLANs)
  - QoS (marking, policing, etc.)
  - Security (802.1x, port security, DAI, etc.)
  - Multicast traffic management (IGMP Snooping)
  - Inline power

The Distribution Layer

- Aggregates access layer switches
- Typically comprised of Layer 3 Switches
- Multiple connections to upstream to Core and downstream to Access
- Offers services such as
  - Gateway redundancy (HSRP/VRRP/GLBP)
  - Bandwidth aggregation (EtherChannel/802.3ad)
  - Load balancing
  - Topology summarization

The Core Layer

- Backbone of the network
  - Must be fast and reliable as all other blocks depend on it
- Typically hardware accelerated Layer 3 Switches
- Offers services such as
  - Wire speed forwarding
  - Fast convergence around a link or node failure
  - Efficient bandwidth utilization

Network Device Roles

- To understand how the layers interact, we must understand what role different devices play in the network
- Devices such as…
  - Hubs/Repeaters
  - Layer 2 Bridges/Switches
  - Layer 3 Routers
  - Layer 3/Layer 4 Switches

Hubs & Repeaters

- Work at layer 1 of OSI model
- When a frame is received it is sent back out all ports
  - i.e. “multiport repeater”
- Typically unintelligent and unmanaged
  - Does not inspect frame at all before forwarding
  - Accepts no user-defined configuration
- Devices connected to a hub are in the same…
  - Collision domain
    - i.e. Ethernet CSMA/CD Half-Duplex transmission
  - Broadcast domain

Layer 2 Bridges & Switches

- Work at layer 2 of OSI model
- Can be managed or unmanaged
- For Ethernet, “frames” are forwarded based on destination layer 2 MAC address
  - “CAM” table used for decisions
  - Other types of switches such as Frame Relay & ATM use similar logic
- Does not rewrite anything in the frame when forwarding
- Switches are hardware accelerated bridges
  - ASICs for specific forwarding jobs
- Devices connected to a bridge/switch are…
  - in the same broadcast domain
  - *not* in the same collision domain
    - i.e. Full-Duplex transmission

Layer 2 Broadcast Domains

- Defines which devices can communicate directly at layer 2
- When a broadcast frame (i.e. FFFF.FFFF.FFFF) is received, it is sent out all ports in the "broadcast domain" except the one it came in on
- Unmanaged bridges/switches
  - All ports in the same broadcast domain
- Managed switches
  - Uses Virtual LANs (VLANs) to group ports into different broadcast domains
  - Frames within the same VLAN are Layer 2 switched
  - Packets between VLANs must be Layer 3 routed

Layer 2 Switching Design Problems

- Ethernet networks used to have scalability limitations based on the collision domain size
  - Half-Duplex CSMA/CD
  - Physical network delay vs. collision detection window
- Layer 2 switches segment the collision domain on a per-port basis to solve this
- Layer 2 switches still have scalability issues based on total hosts in the network and hosts per broadcast domain

CAM Table Limitations

- Switches use the MAC address (CAM) table to do destination based switching
- CAM table cannot be summarized like IP routing
  - 50,000 hosts in the network, 50,000 MAC addresses per CAM per switch
    - Even access layer switches!
- When CAM is full, switch acts like a hub
  - Forwards all new frames like broadcasts
  - Used in flooding attacks such as *macof*
- Layer 3 routing segments the MAC flooding domain

Broadcast Domain Limitations

- Devices in the same VLAN, or everyone in a flat network, are directly addressable via FFFF.FFFF.FFFF
- Larger the broadcast domain, more likelihood of a “broadcast storm”
  - So much broadcast traffic network is unusable
- Can happen for legitimate or illegitimate reasons
  - e.g. ARP storm vs. Fraggle attack
- Limiting hosts per VLAN limits broadcast domain size
  - Usually one VLAN per /24 IP subnet is a good rule

Layer 3 Routers

- Work at layer 3 of OSI model
- "Packets" are forwarded based on destination layer 3 address
  - e.g. IPv4 address, IPv6 address
  - routing table used for decisions
- Rebuilds layer 2 frame header at every hop
  - e.g. packet routed between Ethernet and HDLC
- Normally does not modify layer 3 packet header
  - Exceptions such as NAT
- All router links are in separate collision and broadcast domains
- Software based forwarding

Layer 3 Switches

- The same as Layer 3 Routers, but layer 2 packet rewrite is hardware accelerated with ASICs
- Rewrite process is called "switching path"
  - Process switching
    - CPU interrupt based (slowest)
  - Fast switching
    - Flow based rewrite cache
  - Netflow switching
    - Previously called Multi-Layered Switching (MLS)
  - Cisco Express Fowarding (CEF) switching
    - Pre-built adjacency table (fastest)
- Layer 3 Switching & MLS today is effectively hardware based CEF

Layer 3/Layer 4 Switches

- Layer 3 devices make decision based only on destination layer 3 address
- In some cases where multiple equal-cost paths are available, some paths are underutilized
  - AKA “CEF polarization”
- Layer 4 switching adds TCP/UDP src/dst port information into CEF input in order to vary output
  - e.g. HTTP flow vs. FTP flow between same 2 hosts can follow different forwarding path
- Still hardware accelerated for performance, but adds more optimal resource utilization

Further Reading

- Cisco Validated Design program
  - http://www.cisco.com/web/go/designzone
  - Previously SRNDs
- Enterprise Campus 3.0 Architecture: Overview and Framework
- Campus Network for High Availability Design Guide
- High Availability Campus Recovery Analysis Design Guide