LAN design

Typical hierarchical design:

- Access layer includes end devices. The main purpose is to connect devices and to control which ones are allowed to communicate on the network.
  - port security
  - VLANs
  - fast/gigabit ethernet
  - link aggregation
  - quality of service
- Distribution layer controls the flow of network traffic.
  - layer 3 support
  - high forwarding rate
  - 1/10 gigabit ethernet
  - renundancy
  - security policies
  - link aggregation
  - quality of service
- Core layer connects distribution layer devices and can have connection to internet resources.
  - layer 3 support
  - very high forwarding rate
  - 1/10 gigabit ethernet
  - redundancy
  - link aggregation
  - QoS

Benefits of hierarchical model:

- scalability
- redundancy
- performance (data is transmitted through high-performing switches)
- security (easy to manage)
- manageability (settings can be copied rapidly between switches)
- maintainability (scaling without increasing in complexity)

Network diameter is number of devices that a packet has to cross to its destination.

Device latency - time to handle incoming packet or frame.

Link aggregation - aggregating links between some devices to achieve higher throughput.

Redundancy:

- doubling connections
- doubling devices

Switch form factors:

- fixed configuration
- modular (line cards containing ports can be easily added)
- stackable (several switches operate as one large switch)

Port density - number of available ports.
Converging network design is combining data with voice and video on a common network.

Basic switch concepts

CSMA/CD:

- Carrier sense: devices that have messages must listen before transmitting.
- Multi-access
- Collision detection: registered when there is the amplitude increase.

Jamming signal notifies other devices about the collision.
Communications in LAN:

- unicast
- broadcast
- multicast (frame is sent to a specific group of devices, which are members of multicast group)

Ethernet frame:

- preamble and start frame delimiter (used for synchronization)
- destination MAC
- source MAC
- length/type field
- data and padding
- frame check sum

Duplex settings:

- half-duplex
  - unidirectional
  - hub connectivity
  - higher potential for collision
- full-duplex
  - point-to-point only
  - attached to switches

    - collision-free

Switch has MAC-addresses table. If there is no needed record, the frame is forwarded to all ports.
Collision domain - physical network segment.
Broadcast domain - collection of interconnected switches.
LANs should be segmented into smaller collision and broadcast domains using routers and switches.
Bottleneck - a place where high network congestion results in slow performance.
Forwarding methods:

- store-and-forward (also error checking)
- cut-through
    - fast-forwarding (as soon as destination address is read)
    - fragment-free (waiting for the first 64 bytes)

Asymmetric switching uses different bandwidth for different ports.
Memory buffering:

- port-based (queue for every income port)
- shared

Layered (OSI) switching:

- 2-layer (typical)
- 3-layer (IP addressing and routing functions)
    - don't support WAN interface cards
    - no advanced routing protocols
    - wire-speed routing

Switch loading process:

1. loading of boot loader from NVRAM
2. CPU initialization, POST, flash filesystem initialization, OS loading
3. running config.text from flash memory

Troubleshooting:

- MAC flooding
- spooning attacks (DHCP)
- CDP attack (gathering device info)
- telnet attack
    - Brute force password attack: guessing the password.
    - DoS: a lot of requests.

VLANs

Virtual LAN is logically separate IP subnetwork.
Benefits:

- security
- cost reduction (from less need to expensive network upgrades and more efficient use of bandwidth)
- higher performance (no unnecessary traffic)
- broadcast storm mitigation
- improved IT staff efficiency (minimal efforts to add new switch)
- simpler management

ID ranges:

- normal range (1-1005)
  - configuration is stored in vlan.dat in flash memory
  - 1 and 1002-1005 are automatically created and cannot be removed
  - suitable for VTP
- extended (1006-4094)
  - designed for service providers
  - stored in running config

VLAN types:

- data (only user-generated traffic)
- default (all ports after boot-up)
- native (all untagged traffic goes to it; assigned to 802.1Q trunk port)
- management (any configured vlan to access management capabilities)
- voice (can be configured with other type VLAN)

Network traffic types:

- IP telephony (signalling and voice traffic)
- IP multicast (e.g. TV broadcast)
- normal data
- scavenger (entertainment)

Switch port modes:

- static (manually assigned)
- dynamic (configured using special VLAN server)
- voice

Switch virtual interface (SVI) - logical interface that should be configured to switch between VLANs.

Trunk - point-to-point link between two network devices that carries more than one VLAN. Allows not to have separate link for each subnet.

Tag control information field (used in frames):

- 3 bits of priority
- 1 bit of Canonical format identifier
- 12 bits of VLAN ID

Trunk link is a link with trunk port on each end.

Trunking modes:

- 802.1Q: supports simultaneous traffic.
- ISL: all packets are expected to be encapsulated. Native frames are dropped.

Trunking modes (considering DTP):

- on
- dynamic auto
- dynamic desirable (request to go to trunk)
- off

Configuring overall steps:

- create VLANs
- assign switch ports to VLANs statically
- verify vlan configuration
- enable trunking on the inter-switch connections
- verify trunk configuration

Problems:

- native VLAN mismatch
- trunk mode mismatch
- IP subnets
- allowed VLANs on trunks

VTP

Benefits:

- configuration consistence across the network
- accurate tracking and monitoring of VLANs
- dynamic reporting of added VLANs across the network
- dynamic trunk configuration when VLANs are added

VTP domain consists of one or more interconnected switches that share configuration details and domain name. Separated by layer 3 devices.

VTP advertisements messages to distribute and synchronize VLAN configurations.

Switch modes:

- Server: advertising information; creating, deleting, changing VLANs. Information for entire domain is stored in NVRAM. Used by default.
- Client: the same as server, but cannot modify VLANs. Information for the entire domain is stored only when switch is on.
- Transparent: only advertisements forwarding. Created VLANs are only local.

VTP pruning increases bandwidth by restricting flooded traffic to specific trunks. Without it traffic is sent to all trunks that are configured on the appropriate VLAN.

Advertisements are multicasted using ethernet frames.

Ethernet frame:

- special multicast address
- LLC (destination service access point, source service access point)
- subnetwork access protocol (SNAP) (OUI=Cisco, PID=2003 for VTP)
- VTP header
  - domain name
  - domain name length
  - version
  - message type
  - revision number (shows the number of changes)
- VTP message
- FCS

Advertisements send global domain information:

- domain name
- updater notify and timestamp
- MD5 digest
- frame format

Advertisements sent this VLAN information:

- VLAN ID
- VLAN name
- VLAN type
- VLAN state
- additional configuration

VTP advertisements:

- Summary: domain name, revision number, etc
  - sent every 5 minutes to neighbors (client or server)
  - immediately after configuration change
- Subnet: VLAN information.
  - creating or deleting VLAN
  - suspending or activating
  - changing VLAN name
  - changing MTU
- Request: sent to server in order to get summary and subnet updates.
  - domain name change
  - receiving message with higher revision number
  - subnet advertisement is missed
  - switch reset

STP

Broadcast storm occurs when there are so many broadcast frames caught in layer 2 loop that all bandwidth is consumed.

Duplicate unicast frames are sent to loopes network where are duplicated.

STP intentionally blocks redundant paths that could cause a loop.

Bridge protocol data unit (BPDU) - hello packet.

Root bridge - switch with lowest bridge ID.

Port types:

- root (port with the lowest path cost to root bridge)
- designated (non-root ports permitted to forward traffic)
- non-designated (configured to be in blocking state)
- disabled (administratively down)

Bridge ID fields:

- priority

- extend system ID (old style; used for VLANs)
- switch MAC

BPDU format:

- protocol ID, version, message type, status flag
- root ID, cost of path, BID, port ID
- message age, max age, hello time, forward delay

Port states:

- blocking (non-designated) (receiving BPDUs)
- listening (receiving and processing BPDUs)
- learning (prepares to participate in forwarding and begin to populate MAC address table)
- forwarding
- disabled (no frames forwarding)

BPDU timers:

- hello (between sending BPDUs, 2s)
- forward delay (time spent in listening and learning state, 15s)
- maximum age (time for which BPDU information is stored)

Port fast techology is used on access ports and translates it from blocking to forwarding immediately.

STP convergence - time it takes to determine root bridge, go through different port states, and set all switches ports to final spanning-tree port roles.

- Electing a root bridge: after switch booting, it sends BPDU every 2 seconds. By default root ID matches local BID. If root ID in received BPDU is lower, root ID and cost are updated.
- Electing root ports: port with best cost becomes root port. If there is several paths, the port ID is used to break a tie: the one becomes root, other are non-designated.
- Electing designated and non-designated port: the switch with smaller BID wins the competition and sets port to designated while other becomes non-designated.

When topology changes (port is going down or transitions to forwarding), *topology change notification (TCN)* is sent to the root port. The answer is *topology change acknowledgement (TCA)*. Root bridge answers with *topology change (TC)* messages.

Advanced layer 3 switches can:

- build a forwarding table
- receive packets and route to the correct interface

Per-VLAN STP (PVST) - spanning tree for each VLAN. Load balancing on 2 layer. Uses ISL. Includes extensions like BackconeFast, UplinkFast, PortFast.

PVST+ supports 802.1Q. BPDU guard and Root guard extensions. In BID priority field is reduced to 4 bits, 12 bits for VLAN.

Multiple STP enables ms to be mapped in the same spanning-tree.

RSTP

RSTP uses flag byte in BPDU:

- bits 0 and 7 for topology change and ack
- 1 and 6 for proposal agreement process
- 2-5 encode the role and state of the port

Edge port is port that is never intended to be connected to switch. Immediately transitions to forwarding. When it receives BPDU it becomes normal spanning-tree port.

Non-edge ports can be point-to-point or shared.

Port states:

- Discarding: in both stable and synchronization steps. Prevents data forwarding.
- Learning: also in both steps. Accepting data frames to populate MAC table.
- Forwarding: only when stable.

Port roles:

- Root: on every non-root bridge that is the chosen path to the root.
- Alternate: offers an alternate path toward root bridge, assumes discarding state.
- Backup: additional port with redundant link. Higher priority, assumes discarding state.
- Designated: assumes the forwarding state. Only one per segment.

RSTP is faster because it converges on link-by-link basis and does not rely on timers. Also there are alternate ports.

Inter-VLAN routing

Router-on-a-stick is a router in which a single interface routes traffic between multiple VLANs.

Subinterfaces - multiple virtual interfaces associated with one physical interface.

Switch configuration issues:

- Ports are in VLAN 1 by default.
- The switch interface connected to router-on-a-stick must be in trunk mode (if using subinterfaces)

Router configuration issues:

- connecting to ports with appropriate VLAN
- correct encapsulation number

IP addressing issues:

- correct IP and subnet mask

EtherChannel is used to reduce the risk of failed inter-switch link.

Wireless concepts

Clients connect to the network through wireless *access points (AP)*. It operates at data link layer.

802.11 standards differences:

- Band (5.7 or 2.4 GHz): smaller frequency signals have better range and less absorbed by obstacles, but larger antennas.
- Modulation techniques: direct sequence spread spectrum (DSSS) is worse than orthogonal frequency division multiplexing (OFDM).

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CD): devices must sense the medium for energy and wait until the medium is free before sending.

In small business and homes wireless router act as AP, switch and router.

Shared service set identifier (SSID) - unique identifier used by clients to distinguish between WLANs in the same vicinity.

The band is broken into several channels with a separator between center frequences of successive channels. No overlapped channels are preferred.

Service sets:

- ad hoc networks (without access point)
- basic service sets (single AP)
- extended service sets

The common distribution system allows multiple APs to be in single BSS.

Primary components of 802.11:

- beacon (frame to advertise the presence)
- probe (used by clients to find their networks)
- authentication
- association (establishing a data link)

Process before sending data:

1. Client sends SSID and supported rates, AP responses the same fields and security implementation.
2. Authentication is based on wired equivalency protection (WEP).
   (a) authentication request by client
   (b) response a text
   (c) client encrypts the text using shared key and sends to AP
   (d) decrypting and answering
3. Associate stage: client learns BSSID which is AP MAC, AP maps a logical port (AID) to the client.

AAA - authentication (client identification), authorization (checking special credentials) and accounting (holding logs).

Threads to wireless security:

- war driving (simply exploiting open networks)
- hackers (exploit weak privacy measures)
- using client's data in open networks
- man-in-the-middle
- denial of service

Steps to secure WLAN:

1. SSID (open, not secure)
2. WEP (static, breakable keys, not scalable)
3. WPA (strong user-based authentication)
4. WPA2 (AES, dynamix key management)

Extensible authentication protocol (EAP) is a framework for authenticating network access.

1. identify request (from AP)
2. identify response
3. EAP request (from authentication server)
4. EAP response
5. successful

TKIP is the encryption method certified as WPA.

AES has the same functions as TKIP, but uses additional data from MAC header to recognize tampering and also adds sequence number to header.

Methods of access controlling:

- disabling SSID broadcasts
- MAC filtering
- WPA2

Standard troubleshooting practice:

1. Eliminate a client device as problem source.
2. Confirm the physical status of devices.
3. Inspect wired links.

Channel overlapping may cause problems.

Other devices can "hog" some channels.

Orientation of antenna can reduce coverage in some places.