

Fundamentals

Basic elements Layer 1, contention-based (unorderly transmission)

CSMA/CD Carrier Sense Multiple Access / Collision Detect

Carrier Sense Listen to the wire, verify if busy

Multiple Access all devices have access at any time

Collision Detect if collision occurs, wait random time, try again

Collision Domain /CDO all devices on an internet segment (same cable or hub)

half duplex, operates CSMA/CD

Switches creates multiple CDOs, 1port=1CDO
-> no chance of collision, full-duplex capability

Limitations

SPEED

Ethernet 10Mbps

Fast Ethernet 100Mbps

Gigabit Ethernet 1000Mbps / 1Gbps

10-Gigabit Ethernet 10Gbps

100-Gigabit Ethernet 100Gbps

DISTANCE (memo)

Copper 100m

CAT6 100m@1Gbps / 55m@10Gbps

CAT8 30m

MMF (T, TX,FX, SR, SX) short range (200-500m)

SMF (LX, LR, ZX) long range (in km)

Infrastructure devices

Collision domain /CD network segment where packets collide. Collision detection/avoidance can be set

Broadcast domain /BD domain where broadcast packets are diffused. The smaller the better

Hub multiport repeater with or without amplification (passive/active/smart)

Infrastructure devices (cont)

Bridge analyse source MAC adr & populates table. Separates collision domains

Switch combination of hub and bridge

- layer 2 all ports belong to broadcast domain

- layer 3 creates one *BD* per port. Makes routing decisions, interconnect entire NW

Router connects NW together, makes *fw* decisions. Separates *CD* and *BD*

Other Features

Link Aggregation 802.3ad combines multiple connect° into a single logical connect°

increased bandwidth, congestion lowered

PoE, PoE+ 802.3af/at electrical power over Ethernet, Cat5 mini, 15.4W/25.5W

Port monitoring network sniffer plugged on a hub - analyse purpose

Port mirroring copy all traffic to another port

User Auth. 802.1x once auth., a key is generated and shared

Management SSH for remote access, **console port** for local admin.

Out-of-Band NW conf. devices on a separate NW

First-Hop Redundancy creates a stand-by router in case the active router fails

MAC Filtering filters connect° based on MAC adr

Traffic Filtering filters connect° based on IP adr

QoS forwards traffic according to priority markings



Spanning Tree Protocol STP 802.1D

Role redundant links btw switches, prevent traffic loops.
Without STP, MAC table can be corrupted

Broadcast Storms

when a switches broadcasts btw each other in loop. Multiple copies are forwarded in loop. NW becomes saturated

Root Bridge reference bridge for spanning tree. defined with BID (lower BID) - made of *priority value* and MAC adr.

Non-Root Bridge all other switches

Root Port on N-RB, closest port to the RB

Designated Port port with the lowest cost index to route to the RB. RB has only designated ports

Non-Des. Port all other ports. Block traffic to avoid loops

Port states

- *Blocking* BPDU recieved but not forwarded

- *Listening* idem+ but populates MAC adr table

- *Learning* process BPDU, switch tries to determine its role

- *Forwarding* full ops

Link Costs speed of a link. Lower the speed, higher the cost

ex: Fast Ethernet :19, GB Ethernet : 4

Long STP from 2.000.000 to 2.

Virtual LAN (VLAN)

Principle allows different logical NWs with a single hardware.

How ? use certain ports to separate broadcast domains

VLAN Trunking multiple VLAN using same phy. cable

TPI Tag Protocol Identifier

TCI Tag Control Identifier

VLAN 0 Native VLAN left untagged

Specialized Equipment

VPN virtual tunnel over untrusted NW/Internet

VPN concentrator tunnel traffic to a single location

VPN headend

Firewalls softw or hardw, allows some outcome traffic, blocks some inbound traffic

NGFW packet inspection at layer 7 (App lvi). much more powerful

IDS/IPS *Intrusion Detection/Prevention System*
recognizes attacks and can respond

Proxy content filter server

Content/C-aching Engine caching service for a proxy

Load Balancer distributes request across a server farm

