OSI Model - 7 layers
L1 → Physical - RJ45,RS232...
L2 → Data Link -MAC/LLC - Eth,PPP,FR (MAC)
L3 → Network - IP,IPX (IP Address)
L4 → Transport - TCP/UDP (port)
L5 → Session - SQL,H.323
L6 → Presentation - formats (GIF,JPG,HTML)
L7 → Application - FTP,Telnet,SMTP

Communication → Peer-to-Peer vs. Client-Server

Ethernet
CSMA/CD - carrier sense multi access coll detect
XBase-T - UTP cabling, RJ45, 100M

Switching Bridging
CAM table - Content Addressable Memory
Cut-through, Store-and-Forward
Transparent Switching
Collision and Broadcast Domain
VLAN/trunking - 802.1Q, ISL
STP - STP/RSTP/PVSTP/MST
BPDU, Dis-List-Learn-Fwd-Block
root port, root cost, Bridge ID
EtherChannel - up to 8, LACP/PAgP

Internet Protocol (IP)
IP Address - 32b, 4 octets, ABCDE classes
10.0.0.0/8, 172.16.0.0/12,192.168.0.0/16
Header - Ver,ToS,Len,TTL,Proto,SRC/DST IP
CIDR - Classless Inter Domain Routing

Transmission Control Protocol (TCP)
TCP Header - SRC/DST Port,Seq,Ack,Window
3W Handshake - SYN,SYN/ACK,ACK

Routing Information Protocol (RIP)
AD120, ver 1/2,hop count
UDP520, 224.0.0.9
split-horizon, triggered updates
authentication - md5/cleartext

Enhanced Interior GW Routing Prot. (EIGRP)
AD90/170, 224.0.0.10
complex metric calculation - load,rel,bw,delay
Feasible distance, advertised distance
Feasible successor, Stuck In Active, DUAL
Active/Passive State
Authentication - md5/clear

Open Shortest Path First (OSPF)
AD110, 224.0.0.5,224.0.0.6
Link State, Backbone Area, Multi Area design
Cost, RouterID, Designated Router (high RID)
Area Border Router, AS Border Router
Virtual-link, authentication - null/md5/clear

Border Gateway Protocol (BGP)
AD20/200,TCP179,
Msg-Open,Keepalive,Update,Notification
Path-vector protocol,MD5 authentication
Attributes → Well-known, Optional,Transitive
BestPath Selection:
NH is reachable, weight, LP, local origin, ASP, MED, External, IGP Metric, RID

Generic Routing Encapsulation
IP protocol 47, header 24B
Encapsulates the payload, in case of IP:
IP--GRE--IP--IP_Payload
cfg → Source and Destination IP Address

Next Hop Resolution Protocol (NHRP)
In addition to mGRE (Multipoint GRE)
mapping of NBMA IP to the "inside" tunnel IP
Hub - NHS, spokes - clients
1- client sends a registration request
2- hub sends a registration reply
Phase 1
mGRE - hub=nhs, spokes=GRE
Phase 2
hub=mGRE, spokes=mGRE
Configuration:
```
ip nhrp nhs IP
ip nhrp map, ip nhrp net-id, ip nhrp authentication, ip nhrp holdtime
```

IPv6 Tunnel types
Manual → ipv6ip, IPv6 over GREv4
Automatic
6to4 - route 2002::/16 Tu0, 2001:IPv4::/48
```
tunnel mode ipv6ip 6to4
```
ISATAP - 64b IPv6 prefix + EUI64
```
tunnel mode ipv6ip isatap
```

IP Multicast - PIM
IP Class D, MAC 01:00:5E+IP
Protocol-Independent Multicast (PIM)
PIMv2 → protocol 103, 224.0.0.13
PIM-SM → shared tree, RP, Reg RegStop
RP - static,dynamic, BSR
PIM-DM → SPT, flooding
PIM-BIDIR → shared bidir tree

IP Multicast - MSDP
Interconnects multiple PIM-SM domains
MSDP session between RPs, TCP/639
→ RP redundancy → Anycast RP
MSDP for v6 → MLD
RP sends PIM-join (SRC-Active) to MSDP peer
```
ip msdp peer X connect-source IF
```

IP Multicast - IGMP
MCast protocol between hosts and SW/R
IP protocol 2
Packets:
Gen Query → to all hosts 224.0.0.1
Leave → to all routers 224.0.0.2
Group-Query,Membership Report
IGMP Snooping - VLAN flood avoidance (L2)
CGMP - Cisco proprietary
between R and SW
packets: Join or Leave

IP Multicast - MLD
MLD → for IPv6
replaces IGMP and MSDP
using ICMPv6 to carry data
Messages: Query, Report, Done
Anycast RP → PIMv6 Anycast RP
```
ipv6 pim anycast-RP rp-add peer-add
```

Wireless
SSID → Service Set Identifier
Service Set → group of devices on WLAN
up to 32B, hiding SSID (not-broadcast)
Rogue AP → non-authorized AP on WLAN
WIPS to prevent, radio scan
Session Establishment
LWAPP - prot to manage more APs
Control/analyze multiple AP
L4 UDP 12222 (Data)/12223(Control)
CAPWAP - based on LWAPP
Adding DTLS tunnel
L4 UDP 5246 (Control)/5247 (Data)
Authentication
Static MAC filtering
WEP - Wireless Equivalent Protection
24b IV, RC4, manual
WPA - WiFi Protected Access
personal (PSK) vs. enterprise (EAP)
TKIP - dynam 48b IV, RC4
WPA2
RC4/TKIP replaced by CCMP/AES

Authentication and Authorization
SSO (Single Sign On)
one password for all accesses
often based on LDAP/AD database
One-Time Password (OTP)
pswd valid for one login or period of time
multifactor - something you have
physical keyring - RSA, software ID
often linked with the PIN/password
important - time sync
Lightweight Directory Access Prot (LDAP)
open system - IETF/RFC
contact details, permissions, passwords
based on X.500
TCP/389, TCP636 (Secure LDAP)
Distinguisher Name, RDN, CN ... LDIF
Active Directory
Microsoft stuff, using LDAPv2,3
Domain services → Domain, user, privileges
Federation → SSO for AD
object → resource or security principle
Domain → logical group of PCs/devices
Tree → collection of one or more domains
Forrest → set of trees, same schema
Organisational Unit (OU) - PC subgroup
Role-Based Access Control (RBAC)
system of restriction per user/rights
MAC → Mandatory Access Control
DAC → Discretionary Access Control
Subject, Role, Permission, Session

Virtual Private Network

Layer 2 VPN
L2 frames are delivered directly
L2TPv3 → direct L2 site-to-site tunnel
need to have IP-based network
multiprotocol → Eth,PPP,FR,HDLC...
PPTP
Microsoft L2, client-server
ATOM - Any Transport over MPLS
VPWS - Virtual Private Wire Service (PtP)
VPLS - Virtual Private LAN Service (PtMP)
need to have MPLS-based network

Layer 3 VPN
MPLS VPN
PtMP, LDP/TDP switching, LDP table
LFIB/LIB/FIB
PE,CE,P routers → RD/RT
IPSec VPN
using any other IP transport
tunneled VPN → PtP or PtMP (DMVP)
crypto session → IPSec
ISAKMP (Phase1) - policy, auth, integrity
IPSec (Phase 2) - transform-set, hash
crypto-map, GRE over IPSec, tunnel/trans

Remote Access VPN
Allow mobile users access the resources
usually via the public service
originally L2VPN, then IPSec, today SSL
client (PC/router)-server (router/fw)

Mobile IP
IETF/RFC based, one mobile user same IP
keeping all the sessions when move to net
mobile IP has two addresses:
CoA - Care of Address, Provider-based
HAdd - Home Address, permanent
Home Agent (HA) and Foreign Agent (FA)