OSI Reference Model

7 layers, Allow changes between layers, Standard hardware/software interoperability.

Tip, OSI Mnemonics
All **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
Please **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

Layer	Data	Security
Application	Data	C, I, AU, N
Presentation	Data	C, AU, Encryption
Session	Data	N
Transport	Segment	C, AU, I
Network	Packets	C, AU, I
Data link	Frames	C
Physical	Bits	C

C=Confidentiality, AU=Authentication, I=Integrity, N=Non repudiation

Layer (No)	Functions	Protocols	Hardware / Formats
Physical (1)	Electrical signal Bits to voltage		Cables, HUB, USB, DSL Repeaters, ATM
Data Link Layer (2)	Frames setup Error detection and control Check integrity of packets Destination address, Frames use in MAC to IP address conversion.	PPP - PPTP - L2TP - - ARP - RARP - SNAP - CHAP - LCP - MLP - Frame Relay - HDLC - ISL - MAC - Ethernet - Token Ring - FDDI	Layer 2 Switch - bridges
Network layer	Routing, Layer 3 switching, segmentation, logical addressing. ATM. Packets.	ICMP - BGP - OSPF - RIP - IP - BOOTP - DHCP - ICMP	Layer 3 Switch - Router
Transport	Segment - Connection oriented	TCP - UDP datagrams. Reliable end to end data transfer - Segmentation - sequencing - and error checking	Routers - VPN concentrators - Gateway
Session Layer	Data, simplex, half duplex, full dupl Eg. peer connections.	TCP - UDP - NSF - SQL - RADIUS - and RPC - PPTP - PPP	Gateways
Presentation layer	Data compression/decompression and encryption/decryption	TCP - UDP messages	Gateways JPEG - TIFF - MID - HTML
Application layer	Data	TCP - UDP - FTP - TELNET - TFTP - SMTP - HTTP CDP - SMB - SNMP - NNTP - SSL - HTTP/HTTPS.	Gateways

TCP/IP Model

Layers	Action	Example Protocols
Network access	Data transfer done at this layer	Token ring • Frame Relay • FDDI • Ethernet • X.25
Internet	Create small data chunks called datagrams to be transferred via network access layer	IP • RARP • ARP • IGMP • ICMP
Transport	Flow control and integrity	TCP • UDP
Application	Convert data into readable format	Telnet • SSH • DNS • HTTP • FTP • SNMP • DHCP

TCP 3-way Handshake

SYN - SYN/ACK - ACK

LAN Topologies

Topology	Pros	Cons
BUS	• Simple to setup	• No redundancy • Single point of failure • Difficult to troubleshoot
RING	• Fault tolerance	• No middle point
Start	• Fault tolerance	• Single point of failure
Mesh	• Fault tolerance	• Redundant • Expensive to setup

Types of Digital Subscriber Lines (DSL)

Asymmetric Digital Subscriber Line (ADSL)	• Download speed higher than upload • Maximum 5500 meters distance via telephone lines. • Maximum download 8Mbps, upload 800Kbps.
Rate Adaptive DSL (RADSL)	• Upload speed adjust based on quality of the transmission line • Maximum 7Mbps download, 1Mbps upload over 5500 meters.
Symmetric Digital Subscriber Line (SDSL)	• Same rate for upstream and downstream transmission rates. • Distance 6700 meters via copper telephone cables • Maximum 2.3Mbps download, 2.3Mbps upload.
Very-high-bit-rate DSL (VDSL)	• Higher speeds than standard ADSL • Maximum 52Mbps download, 16 Mbps upload up to 1200 Meters
High-bit-rate DSL (HDSL)	T1 speed for two copper cables for 3650 meters
Committed Information Rate (CIR)	Minimum guaranteed bandwidth provided by service provider.

LAN Packet Transmission

Unicast	Single source send to single destination
Multicast	Single source send to multiple destinations
Broadcast	Source packet send to all the destinations.
Carrier-sense Multiple Access (CSMA)	One workstations retransmits frames until destination workstation receives.
CSMA with Collision Detection (CSMA/CD)	Terminates transmission on collision detection. Used by Ethernet.
CSMA with Collision Avoidance (CSMA/CA)	Upon detecting a busy transmission, pauses and then re-transmits delayed transmission at random interval to minimise two nodes re-sending at same time.
Polling	Sender sends only if polling system is free for the destination.
Token-passing	Sender can send only when token received indicating free to send.
Broadcast Domain	Set of devices which receive broadcasts.
Collision Domain	Set of devices which can create collisions during simultaneous transfer of data.
Layer 2 Switch	Creates VLANs
Layer 3 Switch	Interconnects VLANs

LAN / WAN Media

Twisted Pair	Pair of twisted copper wires. Used in ETHERNET. Cat5/5e/6. Cat5 speed up to 100Mbps over 100 meters. Cat5e/6 speed 1000Mbps.
Unshielded Twisted Pair (UTP)	Less immune to Electromagnetic Interference (EMI)
Shielded Twisted Pair (STP)	Similar to UTP but includes a protective shield.
Coaxial Cable	Thick conduit instead of two copper wires. 10BASE-T, 100BASE-T, and 1000BASE-T.
Fiber Optic	Uses light as the media to transmit signals. Gigabit speed at long distance. Less errors and signal loss. Immune to EMI. Multimode and single mode. Single mode for outdoor long distance.
Frame Relay WAN	Over a public switched network. High Fault tolerance by relaying fault segments to working.

Secure Network Design - Components

Network address translation (NAT)	Hide internal public IP address from external internet
Port Address Translation (PAT)	Allow sharing of public IP address for internal devices and applications using a given single public IP address assigned by ISP
Stateful NAT	Keeps track of packets transfer between source and destinations
Static NAT	One to one private to public IP address assigned between two end devices
Dynamic NAT	Pool of internal IP maps one or several public IP address

Common TCP Protocols

Port	Protocol
20,21	FTP
22	SSH
23	TELNET
25	SMTP
53	DNS
110	POP3
80	HTTP
143	IMAP
389	LDAP
443	HTTPS
636	Secure LDAP
445	ACTIVE DIRECTORY
1433	Microsoft SQL
3389	RDP
137-139	NETBIOS

Attacks in OSI layers

Layer	Attack
Application	Phishing - Worms - Trojans
Presentation	Phishing - Worms - Trojans
Session	Session hijack
Transport	SYN flood - fraggle
Network	smurfing flooding - ICMP spoofing - DOS
Data link	Collision - DOS /DDOS - Eavesdropping
Physical	Signal Jamming - Wiretapping

Hardware Devices

HUB	Layer 1 device forward frames via all ports
Modem	digital to analog conversion
Routers	Interconnect networks
Bridge	Interconnect networks in Ethernet
Gateways	Inbound/outbound data entry points for networks
Switch	Frame forward in local network.
Load balancers	Share network traffic load by distributing traffic between two devices
Proxies	Hide internal public IP address from external public internet /Connection caching and filtering.
VPNs and VPN concentrators	Use to create VPN or aggregate VPN connections provide using different internet links
Protocol analyzers	Capture or monitor network traffic in real-time ad offline
Unified threat management	New generation vulnerability scanning application
VLANs	Create collision domains. Routers separate broadcast domains
IDS/IPS	Intrusion detection and prevention.

Firewall and Perimeter Security

DMZ (Demilitarized zone)	Secure network between external internet facing and internal networks.

Bastion Host - Dual-Homed - Three-Legged - Screened Subnet - Proxy Server - PBX - Honey Pot - IDS/IPS

IP Addresses

Public IPv4 address space	• Class A: 0.0.0.0 – 127.255.255.255 • Class B: 128.0.0.0 – 191.255.255.255 • Class C: 192.0.0.0 – 223.255.255.255
Private IPv4 address space	• Class A: 10.0.0.0 – 10.255.255.255 • Class B: 172.16.0.0 – 172.31.255.255 • Class C: 192.168.0.0 – 192.168.255.255
Subnet Masks	• Class A: 255.0.0.0 • Class B: 255.255.0.0 • Class C: 255.255.255.0
IPv4	32 bit octets
IPv6	128 bit hexadecimal

Network Types

Local Area Network (LAN)	Geographic Distance and are is limited to one building. Usually connect using copper wire or fiber optics
Campus Area Network (CAN)	Multiple buildings connected over fiber or wireless
Metropolitan Area Network (MAN)	Metropolitan network span within cities
Wide Area network (WAN)	Interconnect LANs over large geographic area such as between countries or regions.
Intranet	A private internal network
Extranet	connects external authorized persons access to intranet
Internet	Public network

Networking Methods & Standards

Software defined networking (SDN)	Decoupling the network control and the forwarding functions. Features -Agility, Central management, Programmatic configuration, Vendor neutrality.
Converged protocols for media transfer	Transfer voice, data, video, images, over single network.
Fibre Channel over Ethernet (FCoE)	Running fiber over Ethernet network.
Multiprotocol Label Switching (MPLS)	Transfer data based on the short path labels instead of the network IP addresses. No need of route table lookups.
Internet Small Computer Interface (ISCI)	Standard for connecting data storage sites such as storage area networks or storage arrays. Location independent.
Multilayer Protocols	Encryption and different protocols at different levels. Disadvantages are hiding coveted channels and weak encryptions.
Voice over Internet Protocol (VoIP)	Allows voice signals to be transferred over the public Internet connection.
Asynchronous transfer mode (ATM)	Packet switching technology with higher bandwidth. Uses 53-byte fixed size cells. On demand bandwidth allocation. Use fiber optics. Popular among ISPs
X25	PTP connection between Data terminal equipment (DTE) and data circuit-terminating equipment (DCE)
Frame Relay	Use with ISDN interfaces. Faster and use multiple PVCs, provides CIR. Higher performance. Need to have DTE/DCE at each connection point. Perform error correction.
Synchronous Data Link Control (SDLC)	IBM proprietary protocol use with permanent dedicated leased lines.
High-level Data Link Control (HDLC)	Use DTE/DCE communications. Extended protocol for SDLC.
Domain name system (DNS)	Map domain names /host names to IP Address and vice versa.

Leased Lines

T1	1.544Mbps via telephone line
T3	45Mbps via telephone line
ATM	155Mbps
ISDN	64 or 128 Kbps REPLACED BY xDSL
Reserved	1024-49151
BRI B-channel	64 Kbps
BRI D-channel	16 Kbps
PRI B & D channels	64 Kbps

Network Attacks

Virus	Malicious software, code and executables
Worms	Self propagating viruses
Logic Bomb	Time or condition locked virus
Trojan	Code and/or executables that act as legitimate software, but are not legitimate and are malicious
Backdoor	Unauthorized code execution entry
Salami, salami slicing	A series of small attacks and network intrusions that culminate in a cumulative large scale attack
Data diddling	Alteration of raw data before processing
Sniffing	Unauthorized monitoring of transmitted data
Session Hijacking	Monitor and capture of authentication sessions with the purpose of finding and hijacking credentials
DDoS (Distributed Denial of Service)	Overloading a server with requests for data packets well beyond its processing capacity resulting in failure of service
SYN Flood	Combination of a DDoS attack and TCP 3-way handshake exploit that results in denial of service
Smurf	Particular kind of DDoS attack using large numbers of Internet Control Message Protocol (ICMP) packets
Fraggle	Smurf with UDP instead of TCP
LOKI	Uses the common ICMP tunnelling program to establish a covert channel on the network
Teardrop	A type of DDoS attack that exploits a bug in TCP/IP fragmentation reassembly by sending fragmented packets to exhaust channels
Zero-day	Exploitation of a dormant or previously unknown software bug
Land Attack	Caused by sending a packet that has the same source and destination IP
Bluejacking, Bluesnarfing	Anonymously sending malicious messages or injecting code via bluetooth to unprotected devices within range
DNS Spoofing, DNS Poisoning	The introduction of corrupt DNS data into a DNS servers cache, causing it to serve corrupt IP results
Session hijacking (Spoofing)	Change TCP structure of the packet to show the source as trusted to gain access to targeted systems.
A TCP sequence prediction / number attack	A successful attempt to predict a TCP number sequence resulting in an ability to compromise certain types of TCP communications

Email Security

LDAP (Lightweight Directory Access Protocol)	Active directory based certificate management for email authentication.
SASL (Simple Authentication and Security Layer)	Secure LDAP authentication.
Client SSL Certificates	Client side certificate to authenticate against a server.
S/MIME Certificates	Used for signed and encrypted emails in single sign on (SSO)
MOSS (MIME Object Security Services)	Uses the multipart/signed and multipart/encrypted framework to apply digital signatures.
PEM (Privacy-Enhanced Mail)	A sequence of RfCs (Request for Comments) for securing message authenticity.
DKIM (Domainkeys Identified Mail)	Technique for checking authenticity of original message.
OAuth	An open protocol to allow secure authorization using tokens instead of passwords.

Port Ranges

Point to Point Tunneling Protocol (PPTP)	Authentication methods: • PAP=Clear text, unencrypted • CHAP=unencrypted, encrypted • MS-CHAP=encrypted, encrypted
Challenge-Handshake Authentication Protocol (CHAP)	Encrypt username/password and re-authenticate periodically. Use in PPP.
Layer 2 Tunneling Protocol (L2TP)	Use with IPsec for encryption.
Authentication Header (AH)	Provide authentication and integrity, no confidentiality.
Encapsulating Security Payload (ESP)	Encrypted IP packets and preserve integrity.
Security Associations (SA)	Shared security attributes between two network entities.
Transport Mode	Payload is protected.
Tunnel Mode	IP payload and IP header are protected.
Internet Key Exchange (IKE)	Exchange the encryption keys in AH or ESP.
Remote Authentication Dial-In User Service (RADIUS)	Password is encrypted but user authentication with cleartext.
SNMP v3	Encrypts the passwords.
Dynamic Ports	49152 - 65535

Remote Access Services

Telnet	Username /Password authentication. No encryption.
Remote login (rlogin)	No password protection.
SSH (Secure Shell)	Secure telnet
Terminal Access Controller Access-Control System (TACACS)	User credentials are stored in a server known as a TACACS server. User authentication requests are handled by this server.
TACACS+	More advanced version of TACACS. Use two factor authentication.
Remote Authentication Dial-In User Service (RADIUS)	Client/server protocol use to enable AAA services for remote access servers.
Virtual private network (VPN)	Secure and encrypted communication channel between two networks or between a user and a network. Use NAT for IP address conversion. Secured with strong encryptions such as L2TP or IPSEC.

VPN encryption options

Point-to-Point Tunneling Protocol (PPTP)	• PPP for authentication • No support for EAP • Dial in • Connection setup uses plaintext • Data link layer • Single connection per session
Layer 2 Tunneling Protocol (L2TP)	• Same as PPTP except more secure • Commonly uses IPsec to secure L2TP packets
Internet Protocol Security (IPsec)	• Network layer • Multiple connection per session • Encryption and authentication • Confidentiality and integrity

Communication Hardware Devices

Concentrator	Divides connected devices into one input signal for transmission over one output via network.
Multiplexer	Combines multiple signals into one signal for transmission.
Hubs	Retransmit signal received from one port to all ports.
Repeater	Amplifies signal strength.

WAN Transmission Types

Circuit-switched networks	• Dedicated permanent circuits or communication paths required. • Stable speed. Delay sensitive. • Mostly used by ISPs for telephony.
Packet-switched networks	• Fixed size packets are sending between nodes and share bandwidth. • Delay sensitive. • Use virtual circuits therefore less expensive.

Wireless Networking

Wireless personal area network (WPAN) standards

IEEE 802.15	Bluetooth
IEEE 802.3	Ethernet
IEEE 802.11	Wi-Fi
IEEE 802.20	LTE

Wi-Fi

Standard	Speed	Frequency (GHz)
802.11a	54 Mbps	2.4
802.11b	11 Mbps	5
802.11g	54 Mbps	2.4
802.11n	200+ Mbps	2.4/5
802.11ac	1Gbps	5

• 802.11 use CSMA/CA protocol as DSSS or FHSS
• 802.11b uses only DSSS

Wireless Security Protocols

Ad-hoc Mode	Directly connects peer-to-peer mode clients without a central access point.
Infrastructure Mode	Clients connect centrally via access point.
WEP (Wired Equivalent Privacy)	Confidentiality, uses RC4 for encryption.
WPA (Wi-Fi Protected Access)	Uses Temporal Key Integrity Protocol (TKIP) for data encryption.
WPA2	Uses AES, key management.
WPA2-Enterprise Mode	Uses RADIUS
TKIP (Temporal Key Integrity Protocol)	Uses RC4 stream cipher.
EAP (Extensible Authentication Protocol)	Utilizes PPP and wireless authentication. Compatible with other encryption technologies.
PEAP (Protected Extensible Authentication Protocol)	Encapsulates EAP within an encrypted and authenticated TLS tunnel.
Port Based Authentication	802.1x, use with EAP in switching environment

Wireless Spread Spectrum

FHSS (Frequency Hopping Spectrum System)	Uses all available frequencies, but only a single frequency can be used at a time.
DSSS (Direct Sequence Spread Spectrum)	Parallel use of all the available frequencies leads to higher throughput of rate compared to FHSS.
OFDM (Orthogonal Frequency-Division Multiplexing)	Orthogonal Frequency-Division Multiplexing

Firewall Generation Evolution

First Generation Firewalls	• **Packet Filter Firewalls:** Examines source/destination address, protocol and ports of the incoming packets. And deny or permit according to ACL. Network layer, stateless.
Second Generation Firewalls	• **Application Level Firewall / Proxy Server:** Masks the source during packet transfer. Operating at Application layer, stateful.
Third Generation Firewalls	• **Stateful Inspection Firewall:** Faster. State and context of the packets are inspected.
Fourth Generation Firewalls	• **Dynamic Packet Filtering Firewall:** Dynamic ACL modification • **Packet Filtering Routers:** Located in DMZ or boundary networks. Includes packet-filter router and a bastion host. Packet filtering and proxy • **Dual-homed Host Firewall:** Used in networks facing both internal and external • **Screened-subnet Firewall:** Creates a Demilitarized Zone (DMZ) - network between trusted and untrusted
Fifth Generation Firewalls	• **Kernel Proxy Firewall:** Analyzes packets remotely using virtual network
Next-generation Firewalls (NGFW)	• **Deep packet inspection (DPI) with IPS:** Integrated with IPS/IDS