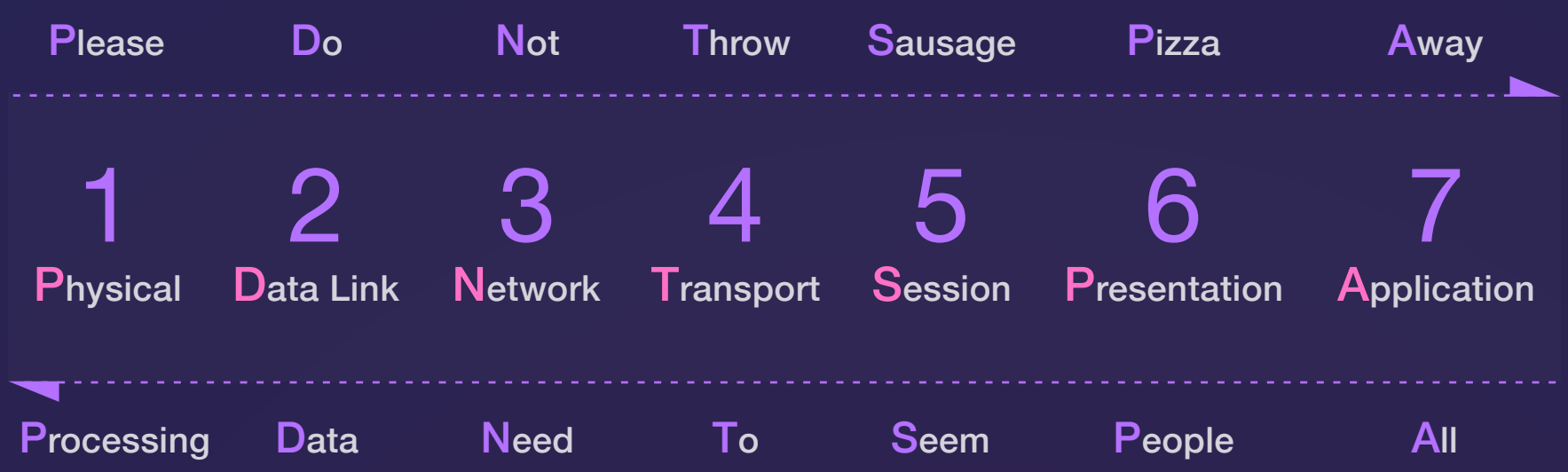
DESTINATION
CERTIFICATION

OSI Model Cheat Sheet

Summary of critical concepts, devices and protocols

OSI Model

Many people know the OSI model as simply a seven-word mnemonic that corresponds to its seven layers:



The Open Systems Interconnection (OSI) model is a structured, layered architecture comprising seven layers. It's important to know the seven layers, what happens at each of them, and where security fits in. Because it is a layered architecture, think of the seven layers of the OSI model as team members. Each member has responsibilities that allow the ultimate goal of communication to be accomplished. No layer can work on its own and accomplish this ultimate goal.

It's very important to know what security-specific features exist at different layers of the OSI model. The higher the layer, the more intelligent and the more functional the security features become, and more comprehensive controls can be implemented. However, at the higher layers, the functionality is accompanied with complexity, which reduces the speed and efficiency. At the lower layers, where complexity is minimized, speed and efficiency are improved.

While the OSI model consists of seven layers, the TCP/IP implementation consists of four layers. The top three layers of the OSI model are handled by the application layer of the TCP/IP model. The transport layer is the same in both models. The OSI network layer is called the internet layer in TCP/IP and then the bottom two layers of the OSI model are handled by TCP/IP's link layer.

Although a lot of people simply refer to every type of information as "packets," that is actually incorrect. Information within the uppermost three OSI layers (application, presentation, and session) is referred to as "data." When that data reaches the transport layer it is referred to as "segments." At Layer 3 (network), the term "packets" or "datagrams" is commonly used. Layer 2 (data link) uses the term "frames" while at Layer 1 (physical) everything is just referred to as bits (or 0s and 1s).

Slowest → Fastest (Speed)

Most → Least (Intelligence)

Encapsulation ↓ Decapsulation

OSI	Description	Devices	Protocols	Common Attacks	Attack Mitigation	Data Format	TCP/IP
7 Application	Network capabilities of applications	• Application Firewall	• HTTP/S • DHCP • SSH • SNMP • SMTP • FTP • SIP • DNS	• DNS masquerading/ cache poisoning • Password exploitation • SNMP Community • String exploitation	• DNSSEC • AV software • Hardening • Patching • IDS/IPS • Encryption (prior to data entering network)	Data	4 Application
6 Presentation	Formatting of data, including encryption/ decryption and compression		• XML • JPEG • ANSI				
5 Session	Interhost communication	• Circuit Proxy Firewall	• PAP • CHAP • EAP • NetBIOS • RPC				
4 Transport	End-to-end connection with error correction and detection; encryption		• TCP/UDP • SRTP • iSCSI (SAN) • BGP	• SYN Flood • DoS/DDoS	• Encryption (SSL/TLS)	Segment	3 Transport
3 Network	Logical addressing, routing, and delivery of datagrams	• Routers • Packet Filtering & Stateful Inspection Firewalls • Layer 3 Switches	• IP addresses • IPSec • ICMP • NAT • RIP • OSPF		• Network Address Translation (NAT) • Encryption (VPN) • ACL • limit physical and logical access to router	Packet / Datagram	2 Network
2 Data Link	Physical addressing and reliable point-to-point connection	• Switches • Bridges	• MAC addresses • ARP/RARP • L2TP • PPTP	• ARP spoofing/ poisoning • MAC flood • Spanning tree attack	• VLAN • ARP inspection • Encryption (VPN and Wireless)	Frame	1 Link
1 Physical	Binary transmission of data across physical media (wire, fiber, etc.)	• Hubs • NICs • Repeaters • Concentrators	• Ethernet • Wireless	• Eavesdropping /tapping • Jamming • Floods • Power manipulation	• Encryption	Bits	

Term	Definition
Address Resolution Protocol (ARP)	Protocol which maps Layer 3 IP addresses to Layer 2 MAC addresses
Application Firewall	Operates at Layer 7 (Application), the most complicated / intelligent, slowest, highest latency, can inspect anything in the packet header and assemble a series of packets to inspect contents (e.g. for viruses)
Border Gateway Protocol (BGP)	Network protocol used to exchange routing and reachability information between routers - essentially the protocol looks at all of the available paths that a packet could travel and picks the best route based on numerous variables
Bridge	Device that creates a single aggregate network from multiple communication networks or network segments
Challenge-Handshake Authentication Protocol (CHAP)	Authenticates using a challenge / response method which prevents replay attacks. Should be used over PAP
Circuit Level Firewall	Operates at Layer 5 (Session), will allow a circuit / session to be established if it complies with rules
Concentrator	Device which aggregates and forwards data packets from multiple smaller networks across a single higher bandwidth connection
DNS Spoofing	(AKA DNS Cache Poisoning) corrupt data is provided to a DNS resolver's cache such that incorrect results are returned (e.g. a user is sent the wrong IP address for the provided domain name)
Domain Name System (DNS)	Protocol which is a hierarchical decentralized naming system. Primarily used to translate easily remembered domain names (google.com) into IP addresses (74.125.224.72)
Domain Name System Security Extensions (DNSSEC)	Set of extensions to DNS which attempt to provide security while maintaining backwards compatibility
Dynamic Host Configuration Protocol (DHCP)	Network protocol that enables a DHCP server to dynamically or statically assign IP addresses to devices as they are added to the network
Ethernet	Family of wired networking technologies used in local area networks (LANs), metropolitan area networks (MANs) and wide area networks (WANs)
Extensible Authentication Protocol (EAP)	Authentication framework, not a specific authentication mechanism. Enables authentication over wired or wireless networks using multiple different authentication methods (knowledge, ownership & characteristic)
Extensible Markup Language (XML)	Language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable
File Transfer Protocol (FTP)	Protocol which enables a client to get or put (save) a file on a remote server. FTP provides no encryption mechanisms
Hub	Device used to connect multiple network devices. Any packet sent to the hub is repeated to all other devices connected to the hub

Term	Definition
Hypertext Transfer Protocol Secure (HTTPS)	Protocol which extends HTTP to enable encrypted communication with a web server. Encryption is provided via SSL/TLS protocol
Internet Control Message Protocol (ICMP)	Protocol which supports IP protocol by allowing network devices (e.g., routers) to send error and control messages and enables Ping & Traceroute utilities
Internet Protocol Security (IPSec)	Framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks
Internet Small Computer Systems Interface (iSCSI)	Protocol which enables clients to send and receive data from storage devices over an IP network
IP Addressing	Assigning source and destination IP addresses to each packet/datagram so that it can be routed across a network
Layer 2 Switch	Device used to connect multiple network devices. A packet sent to the switch is forwarded on only to the intended recipient based on destination MAC address in packet header
Layer 2 Tunneling Protocol (L2TP)	Tunneling protocol used to establish Virtual Private Network (VPN) connections over the Internet. Does not provide encryption on its own
Layer 3 Switch	Device used to connect multiple network devices. A packet sent to the switch is forwarded on only to the intended recipient based on destination IP address in packet header
Network Address Translation (NAT)	Method of remapping (swapping) an IP address to another by modifying the IP header of packets when they pass through a proxy. Typically remapping from an internal unrouteable IP address to a publicly routable address
Network Basic Input Output System (NetBIOS)	Protocol which allows applications on computers to communicate with one another over a LAN
Network Interface Card/Controller (NIC)	Hardware component that connects a computer to a network (wired or wireless)
Open Shortest Path First (OSPF)	Protocol which calculates the shortest route to a destination through a network based on an algorithm
Packet Filtering Firewall	Operates at Layer 3 (Network), the simplest, fastest, lowest latency firewall, inspects packets headers (e.g. source and destination IP address & ports) against a set of rules typically defined in an Access Control List (ACL)
Password Authentication Protocol (PAP)	Sends authentication credentials (username & password) in clear text across the network
Physical Addressing / Media Access Control (MAC) Address	Unique identifier (built-in address) associated with a network adapter that is used for identifying a device at Layer 2 of a network

Term	Definition
Point-to-Point Tunneling Protocol (PPTP)	Protocol for creating Virtual Private Networks (VPN)s which does not include encryption or authentication. Now considered an obsolete protocol due to many security vulnerabilities identified
Remote Procedure Call (RPC)	Protocol (Application layer in TCP/IP) which enables a client to send a request to a remote server to execute a specified procedure with supplied parameters
Repeater	Device which receives signals (wired or wireless) and re-transmits the signal to increase range of communications
Reverse Address Resolution Protocol (RARP)	Protocol which maps Layer 2 MAC addresses to Layer 3 IP addresses
Router	Device that forwards packets between different networks based on IP addresses
Routing Information Protocol (RIP)	Protocol which prevents routing loops by implementing a limit on the number of hops allowed by packet in a path from source to destination
Secure File Transfer Protocol (SFTP)	Protocol which enables a client to get or put (save) a file on a remote server. SFTP provides encryption
Secure Real-time Transport Protocol (SRTP)	Secure version (encryption, authentication, integrity & replay attack protection) of the Real-time Transport Protocol (RTP) which provides streaming audio and video over IP
Secure Shell (SSH)	Cryptographic protocol for using network services securely over an unsecured network (e.g., secure remote user login to a computer)
Session Initiation Protocol (SIP)	Signaling protocol used for initiating, maintaining, modifying and terminating real-time communications sessions between Internet Protocol (IP) devices. Used to establish voice & video calls.
Simple Mail Transfer Protocol (SMTP)	Standard for electronic mail (email) transmission. Typically, just used by clients to send emails to the server
Simple Network Management Protocol (SNMP)	Protocol for collecting data from, and managing configuration of network devices (e.g., switches & routers) across an IP network. Versions 1 & 2 provided no encryption. V3 incorporates encryption
Stateful Packet Filtering Firewall	Maintains a dynamic state table (simple memory / history of recent traffic) and uses the state table to help determine if packets are allowed through (e.g. if a request was sent out, reply will be allowed back in)
Transmission Control Protocol (TCP)	Protocol which provides reliable, ordered, and error-checked delivery of packets between applications running on hosts communicating via an IP network
User Datagram Protocol (UDP)	Protocol which provides speed / efficiency at the expense of a reliable connection and error correction (e.g. often used for video and audio streaming), jokingly referred to as: send and pray data arrives
Virtual Local Area Network (VLAN)	Abstracts the idea of the LAN; A VLAN might comprise a subset of the ports on a single switch or subsets of ports on multiple switches thus allowing systems to be logically separated / segmented into groups