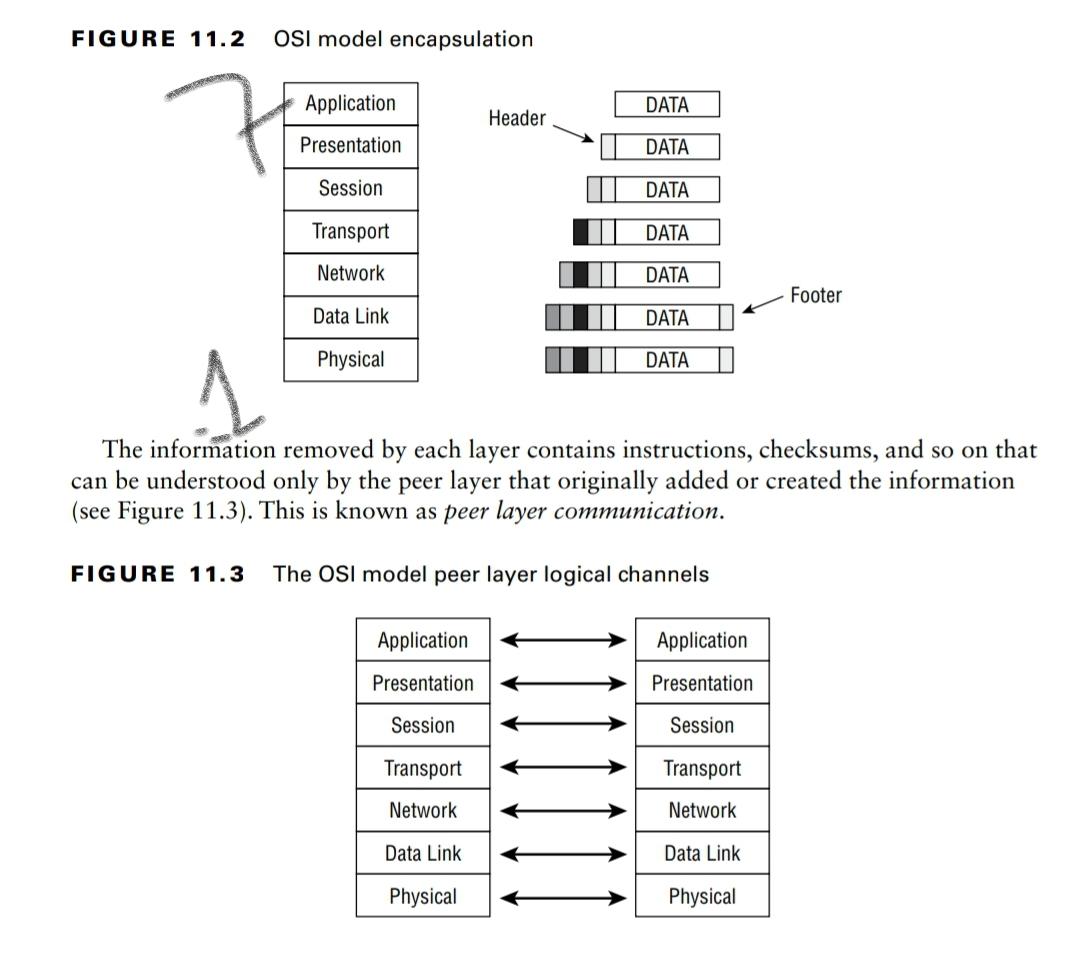
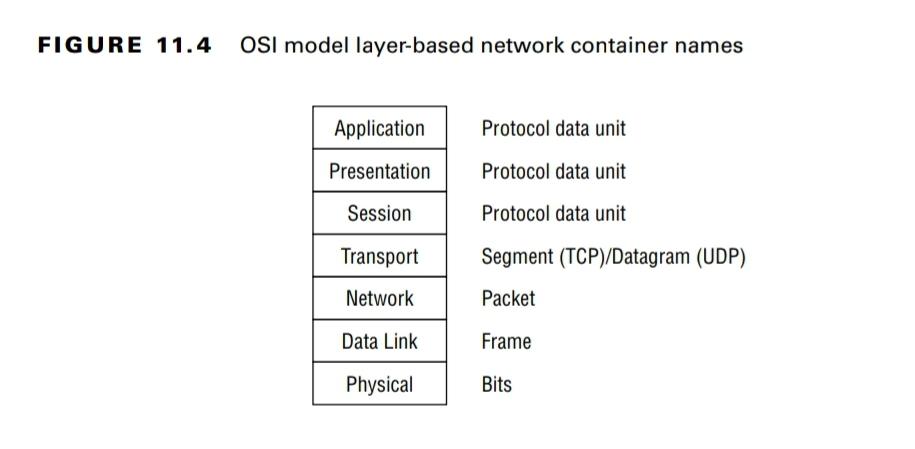
**Chapter 11: Secure Network Architecture and Components**

Communications between computers over networks are made possible by protocols. A protocol is a set of rules and restrictions that define how data is transmitted over a network.

The OSI model divides networking tasks into seven layers. Communication between protocol layers occurs through encapsulation and deencapsulation (or decapsulation). Encapsulation is the addition of a header, and possibly a footer, to the data received by each layer from the layer above before it’s handed off to the layer below.





Application layer (layer 7) - responsible for interfacing user applications, network services, or the operating system with the protocol stack.

Presentation layer - responsible for encryption and compression.

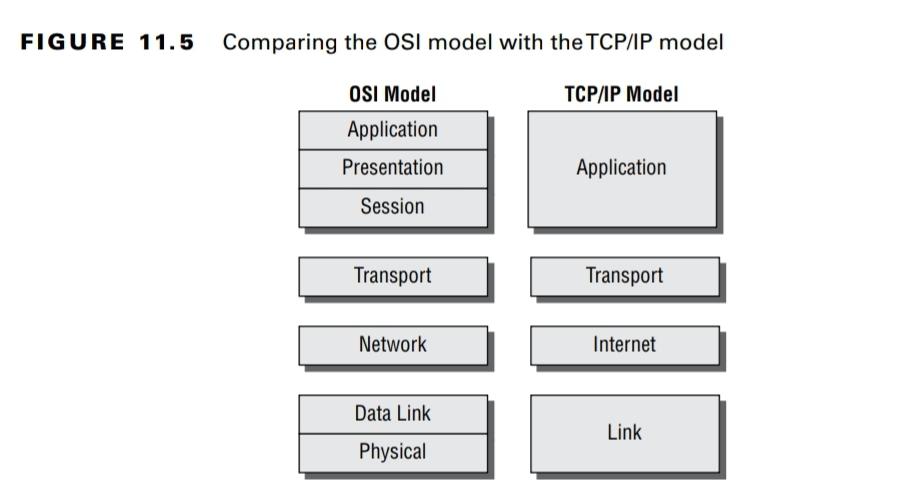
Session layer - responsible for establishing, maintaining, and terminating communication sessions between two computers (simplex, half-duplex, full-duplex).

Transport layer - responsible for managing the integrity of a connection and controlling the session. TLS, TCP and UDP operate at this layer.

Network layer - responsible for logical addressing and performing routing.

Data Link - responsible for formatting the packet for transmission. The proper format is determined by the hardware, topology, and the technology of the network, such as Ethernet.

Physical layer - converts a frame into bits for transmission over the physical connection medium, and vice versa for receiving communications.



Transmission Control Protocol (TCP) is a full-duplex connection-oriented protocol, whereas User Datagram Protocol (UDP) is a simplex connectionless protocol.

DNS poisoning is the act of falsifying the DNS information used by a client to reach a

desired system.

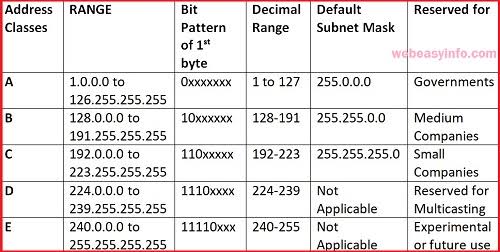
DNS Pharming is the malicious redirection of a valid website’s URL or IP address to a fake website. Usually, by modifying the local hosts file.

Typosquatting is a practice employed to take advantage of when a user mistypes the domain name or IP address of an intended resource.

Homograph attacks leverage similarities in character sets to register phony international domain names (IDNs) that to the naked eye appear legitimate.

Internet Protocol (IP) provides route addressing for data packets. Similar to UDP, IP is connectionless but works on "best effort" mechanism to deliver the data packets.

IPv4 uses a 32-bit addressing scheme, whereas IPv6 uses 128 bits for addressing.



Private IP addresses

**Class A**: 10.0. 0.0 to 10.255. 255.255.

**Class B**: 172.16. 0.0 to 172.31. 255.255.

**Class C**: 192.168. 0.0 to 192.168. 255.255.

TFTP is an unauthenticated ftp service used to store network devices config files for easy accessibility.

Address Resolution Protocol (ARP) resolves 32-bit IP addresses into 48-bit MAC addresses.

Internet Protocol Security (IPsec) uses public key cryptography to provide encryption, access control, nonrepudiation, and message authentication, all using IP-based protocols.

If a network blocks the use of FTP but allows HTTP, then tools such as HTTPTunnel can be used to bypass this restriction. This could result in an encapsulation structure such as this:

[ Ethernet [ IP [ TCP [ HTTP [ FTP [Payload] ] ] ] ]

WEP uses a predefined shared Rivest Cipher 4 (RC4) secret key for both authentication (i.e., SKA) and encryption. Due to flaws in its implementation of RC4, WEP is weak.

WPA separated authentication and encryption. WPA negotiates a unique key set for each host for the encryption process. WPA employs the Temporal Key Integrity Protocol (TKIP) which is a wrapper around the same RC4 algorithm defined for WEP.

WPA2 implements AES-CCMP instead of RC4. To date, no attacks have been successful against AES-CCMP encryption. But there have been exploitations of the WPA2 key exchange processes.

WPA3 replaces the pre-shared key authentication with Simultaneous Authentication of Equals (SAE). SAE performs a zero-knowledge proof process known as Dragonfly Key Exchange.

A captive portal is an authentication technique that redirects a newly connected client to a web-based portal access control page.

War driving is someone using a detection tool to look for wireless networking signals, often

ones they aren’t authorized to access.

A rogue Wireless Access Point (WAP) may be planted by an employee for convenience, installed internally by a physical intruder, or operated externally by an attacker. A rogue WAP or false WAP can be deployed by an attacker externally to target your existing wireless clients or future visiting wireless clients by offering plain text communication.

Evil twin is an attack in which a hacker operates a false access point that will automatically clone, or twin, the identity of an access point based on a client device’s request to connect.

Jamming is the transmission of radio signals to intentionally prevent or interfere with communications by decreasing the effective signal-to-noise ratio.

A replay attack is the retransmission of captured communications in the hope of gaining access to the targeted system. Replay attacks attempt to reestablish a communication session by replaying (i.e., retransmitting) captured traffic against a system.

**Firewalls**

* A static packet-filtering firewall (aka screening router) filters traffic by examining data from a message header. Usually, the rules are concerned with source and destination IP address (layer 3) and port numbers (layer 4). This is also a type of stateless firewall.
* Stateful inspection firewalls (aka dynamic packet filtering firewalls) evaluate the state, session, or context of network traffic.
* An application-level firewall filters traffic based on a single internet service, protocol, or application. Application-level firewalls operate at the Application layer (layer 7) of the OSI model. An example is the web application firewall (WAF).
* A next-generation firewall (NGFW) is a multifunction device (MFD) or unified threat management (UTM) composed of several security features in addition to a firewall.
* An internal segmentation firewall (ISFW) is a firewall deployed between internal network segments or company divisions.

**Cables**

Coaxial cable has a center core of copper wire surrounded by a layer of insulation,

which is in turn surrounded by a conductive braided shielding and encased in a final insulation sheath. The design of coaxial cable makes it fairly resistant to electromagnetic interference (EMI) and able to support high bandwidths. It's costly as compared to twisted pair cable.

Baseband cables can transmit only a single

signa at a time, and broadband cables can transmit multiple signals simultaneously.

10Base2 - 10 Mbps baseband cable can be used for 200 meters max distance

100BaseT - 100 Mbps baseband Twisted pair cable

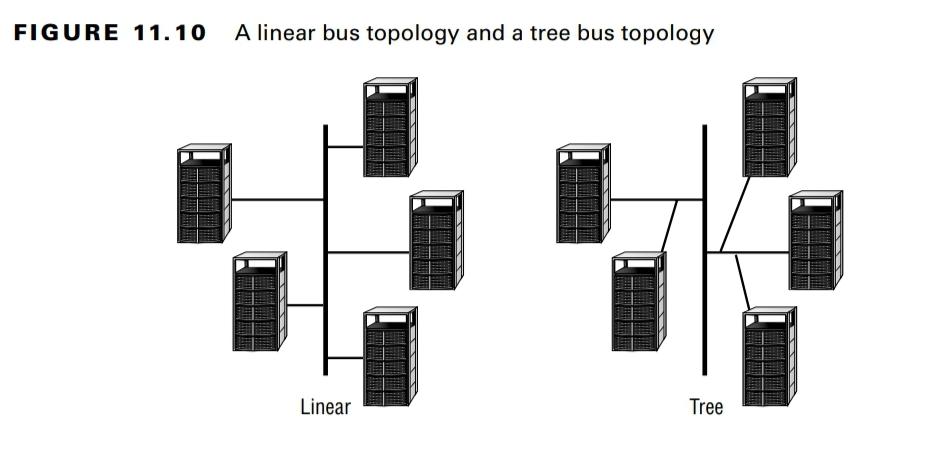
Twisted pair cable consists of four pairs of wires that are twisted around each other and then sheathed in a PVC insulator. If there is a metal foil wrapper around the wires underneath the external sheath, the wire is known as shielded twisted-pair (STP). Twisted pair cables became very popular due to the cheap cost.

Fiber-optic cables transmit pulses of light rather than electricity. This gives fiber-optic cable the advantage of being extremely fast and nearly impervious to tapping and interference.

**Network Topologies**

A ring topology connects each system as points on a circle. Transmission is unidirectional, Only one system can transmit data at a time. Traffic management is performed by a token.

A bus topology connects each system to a trunk or backbone cable. All systems on the bus can transmit data simultaneously, which can result in collisions.



Star topology employs a centralized connection device. This device can be a simple hub or switch. Each system is connected to the central hub by a dedicated segment.

A mesh topology connects systems to other systems using numerous paths. A full-mesh topology connects each system to all other systems on the network.

Dual stack implies systems operate both IPv4 and IPv6 and use the appropriate protocol for each conversation.

Tunneling allows most systems to operate a single stack of either IPv4 or IPv6 and use an encapsulation tunnel to access systems of the other protocol.

NAT-PT (NAT Protocol Translation) can be used to convert between IPv4 and IPv6 network segments similar to how NAT converts between internal and external addresses.

Zigbee is an IoT equipment communications concept that is based on Bluetooth. Zigbee communications are encrypted using a 128-bit symmetric algorithm.

Deduplication replaces multiple copies of a file with a pointer to one copy. If the original file is damaged, then all of the linked copies are damaged.

The goals of Network access control (NAC) are to detect/ block rogue devices, prevent or reduce zero-day attacks, confirm compliance with updates and security settings, enforce security policy throughout the network, and use identities to perform access control.