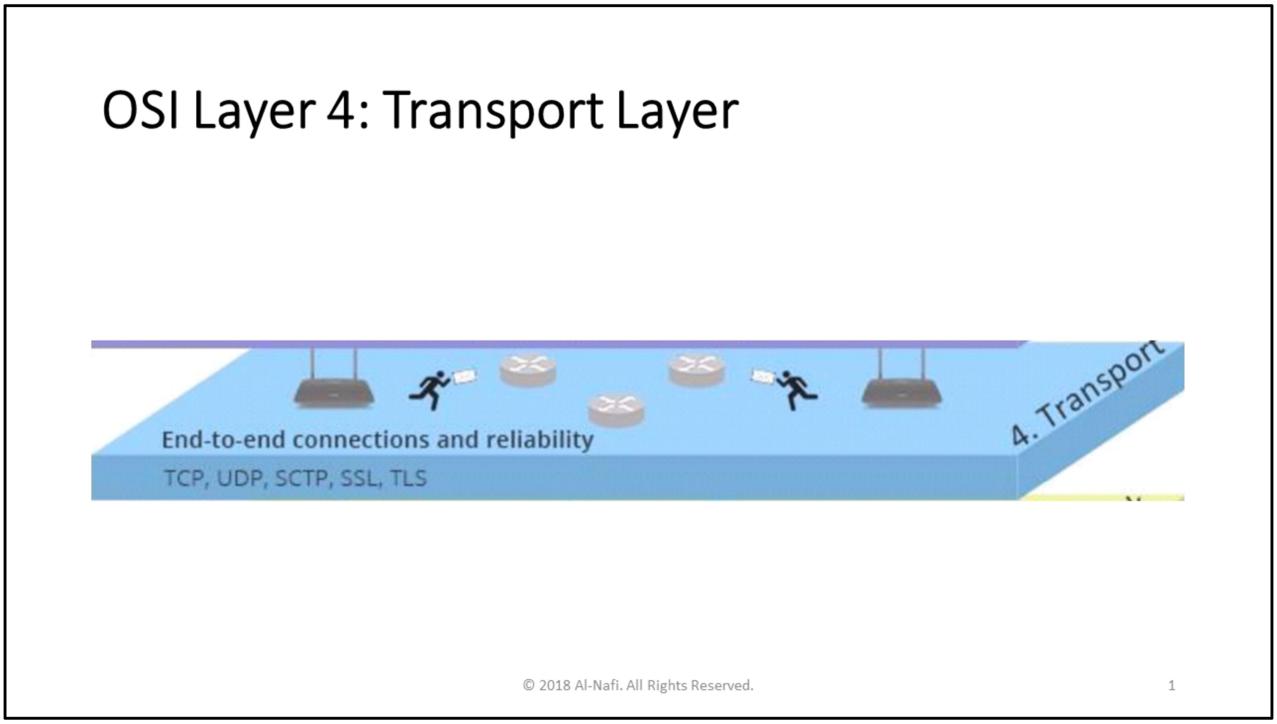
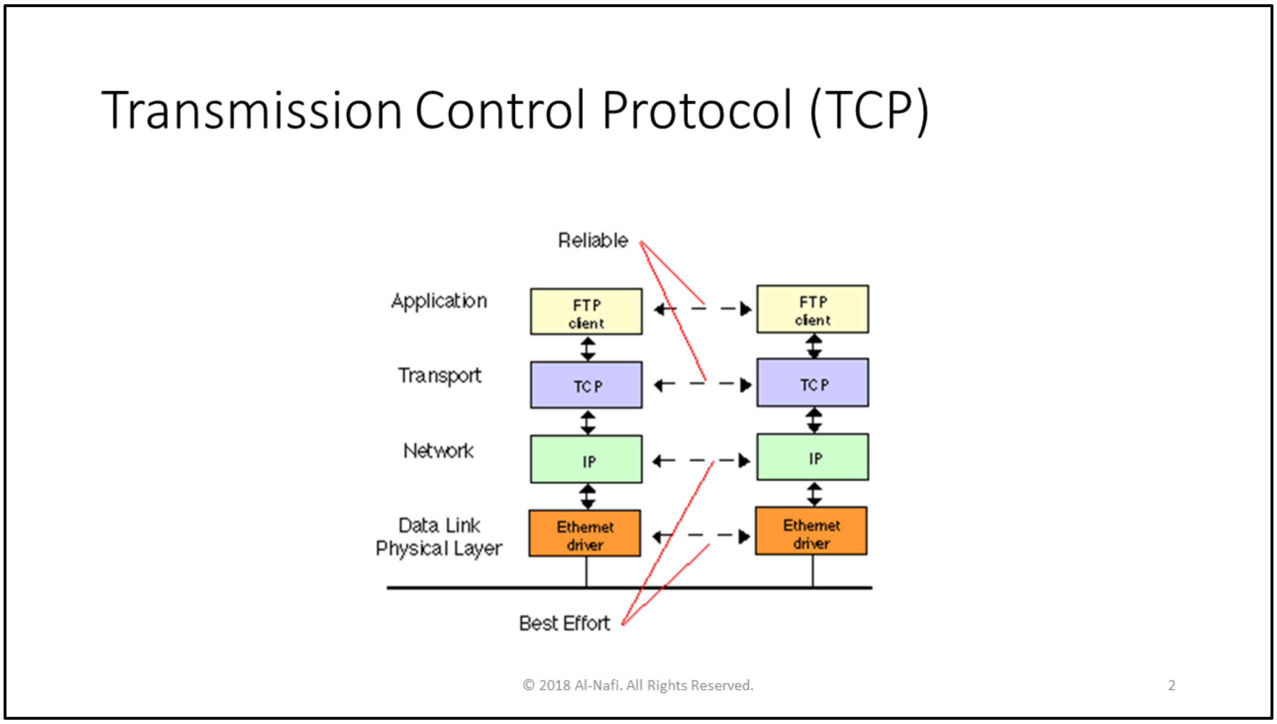


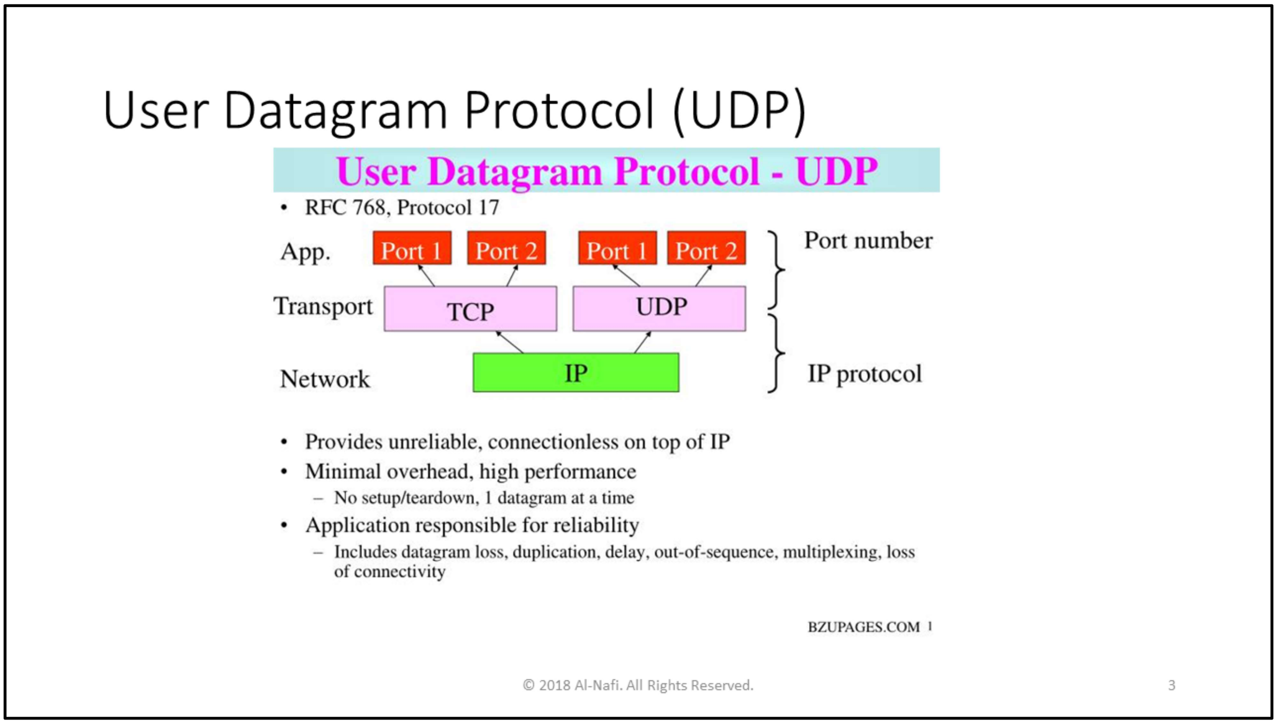
OSI Layer 4: Transport Layer

The transport layer delivers end-to-end services through segments transmitted in a stream of data and controls streams of data to relieve congestion through elements that include quality of service (QoS).



Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) provides connection-oriented data management and reliable data transfer.



User Datagram Protocol (UDP)

User Datagram Protocol - UDP

- RFC 768, Protocol 17

App. Port 1 Port 2 Port 1 Port 2 Port number

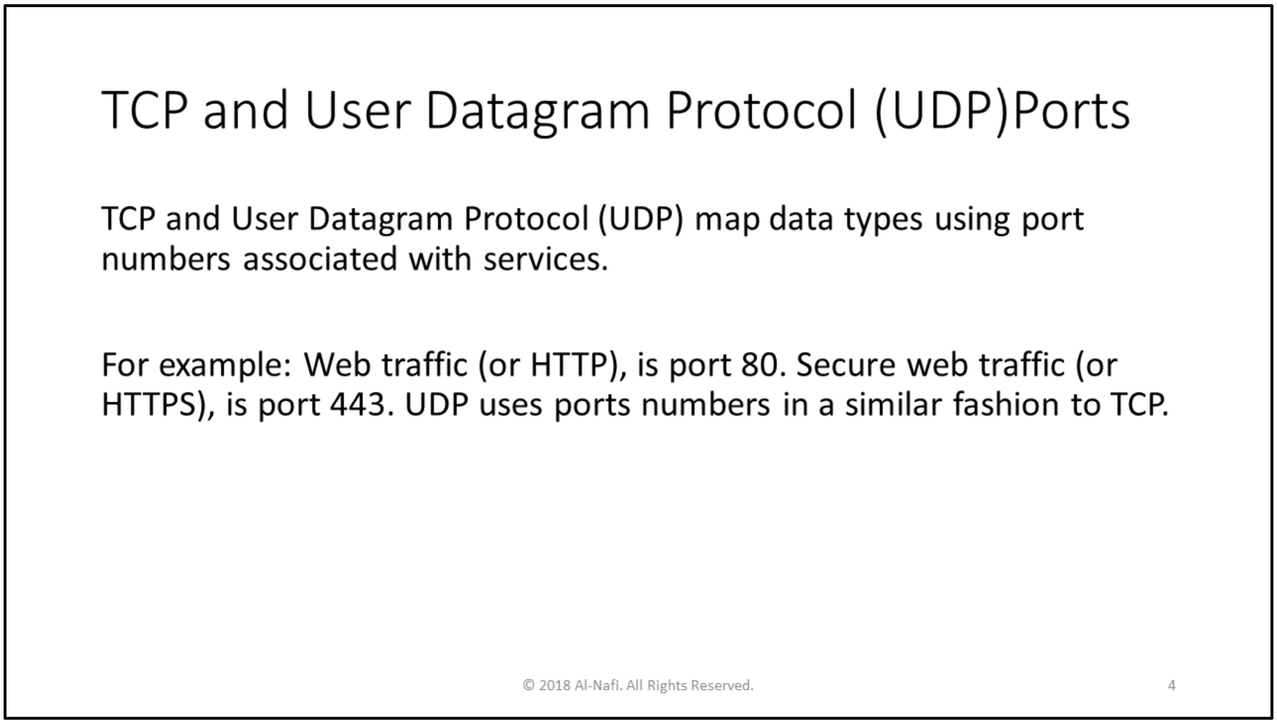
Transport TCP UDP

Network IP IP protocol

- Provides unreliable, connectionless on top of IP
- Minimal overhead, high performance
  - No setup/teardown, 1 datagram at a time
- Application responsible for reliability
  - Includes datagram loss, duplication, delay, out-of-sequence, multiplexing, loss of connectivity

BZUPAGES.COM 1

The UDP provides connectionless data transfer without error detection and correction. UDP uses port numbers in a similar fashion to TCP. As a connectionless protocol, UDP is useful for attacks as there is no state for routers or firewalls to observe and monitor.



TCP and User Datagram Protocol (UDP)Ports

TCP and User Datagram Protocol (UDP) map data types using port numbers associated with services.

For example: Web traffic (or HTTP), is port 80. Secure web traffic (or HTTPS), is port 443. UDP uses ports numbers in a similar fashion to TCP.

Well-Known Ports: Ports 0–1023

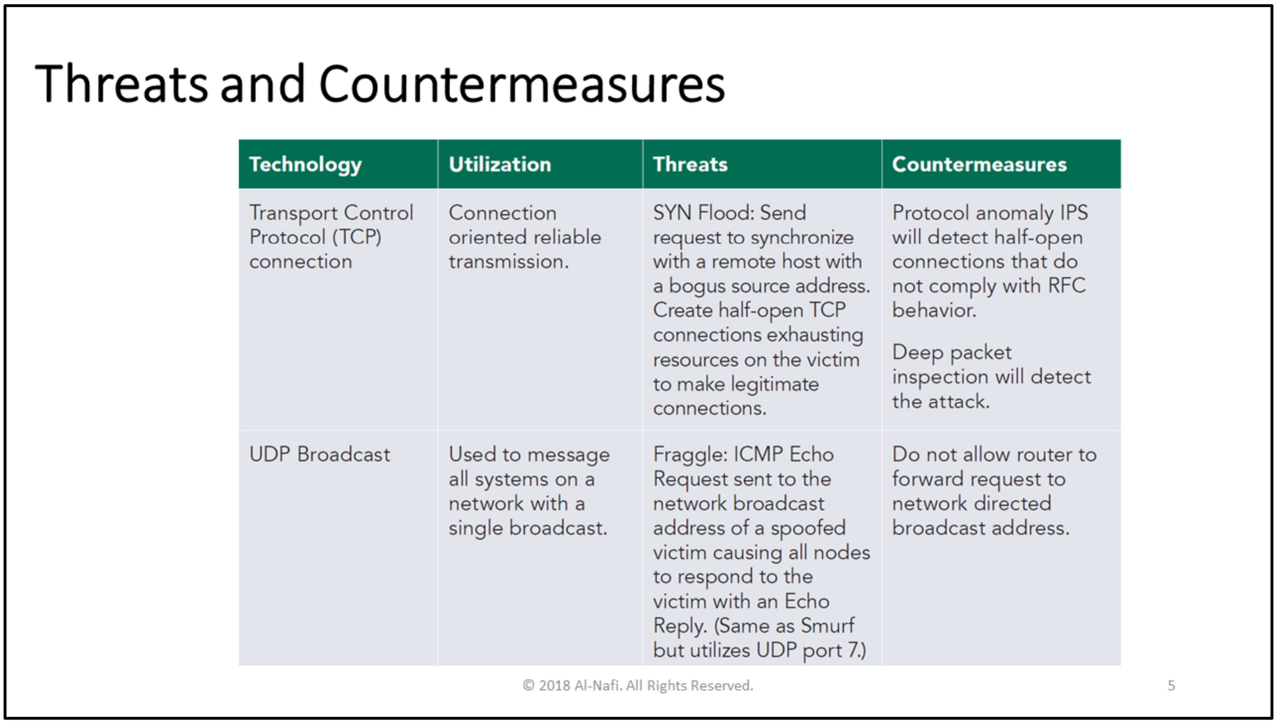
- These ports are related to the common protocols that are utilized in the underlying management of Transport Control Protocol/Internet Protocol (TCP/IP) system (Domain Name Service (DNS), Simple Mail Transfer Protocol (SMTP), etc.)

Registered Ports: Ports 1024–49151

- These ports typically accompany non-system applications associated with vendors and developers.

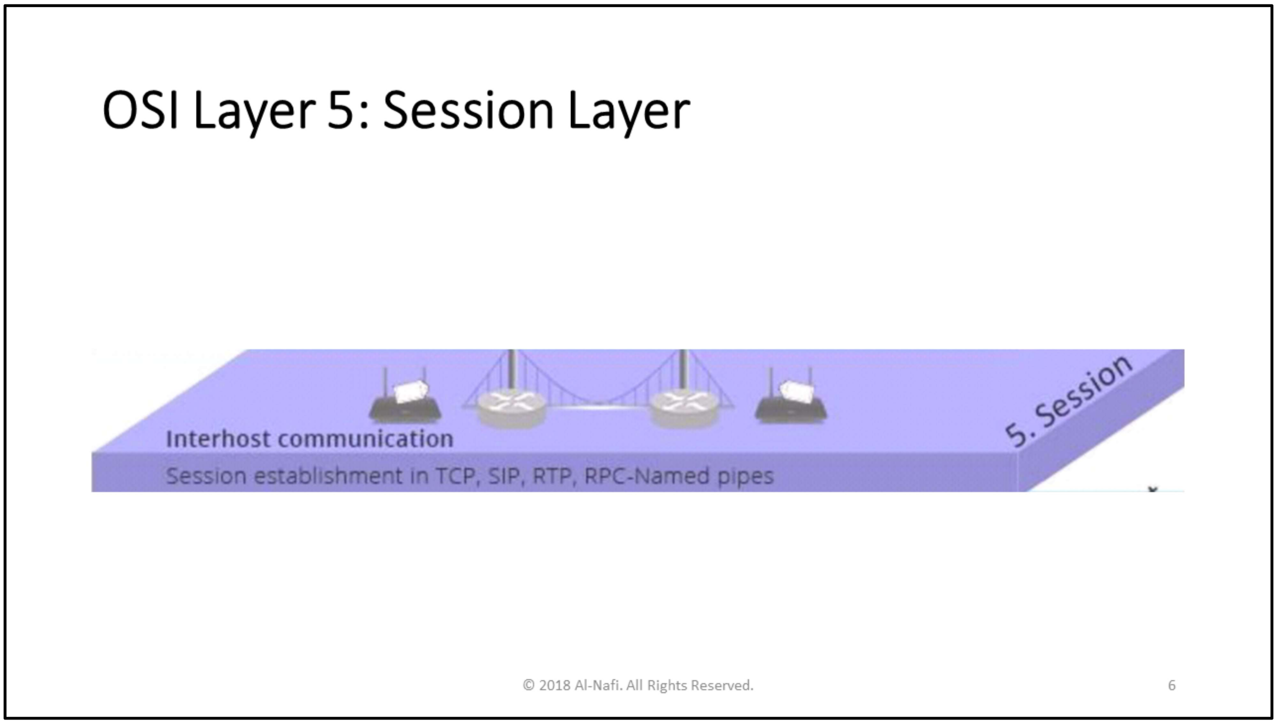
Dynamic or Private Ports: Ports 49152–65535

- Whenever a service is requested that is associated with Well-Known or Registered Ports those services will respond with a dynamic port.



Threats and Countermeasures

Technology	Utilization	Threats	Countermeasures
Transport Control Protocol (TCP) connection	Connection oriented reliable transmission.	SYN Flood: Send request to synchronize with a remote host with a bogus source address. Create half-open TCP connections exhausting resources on the victim to make legitimate connections.	Protocol anomaly IPS will detect half-open connections that do not comply with RFC behavior. Deep packet inspection will detect the attack.
UDP Broadcast	Used to message all systems on a network with a single broadcast.	Fraggle: ICMP Echo Request sent to the network broadcast address of a spoofed victim causing all nodes to respond to the victim with an Echo Reply. (Same as Smurf but utilizes UDP port 7.)	Do not allow router to forward request to network directed broadcast address.



OSI Layer 5: Session Layer

Interhost communication

Session establishment in TCP, SIP, RTP, RPC-Named pipes

5. Session

6

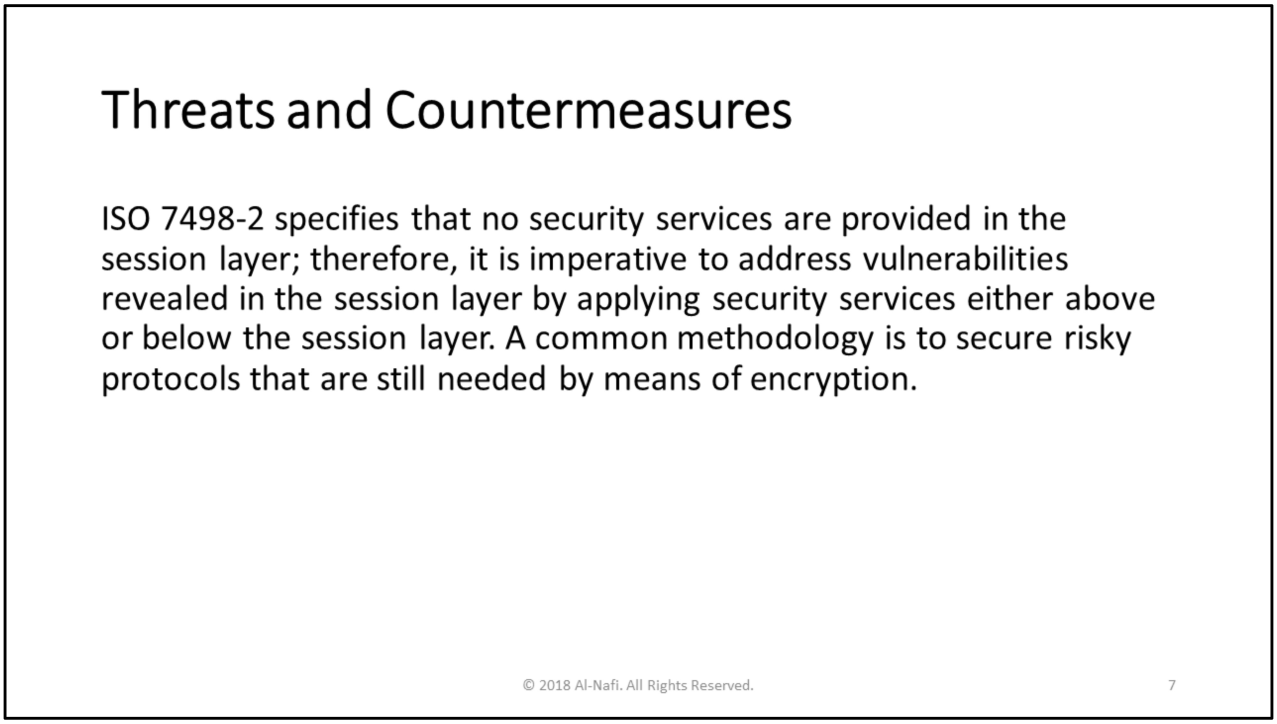
The session layer provides a logical persistent connection between peer hosts. The session layer is responsible for creating, maintaining, and tearing down the session.

Technology and Implementation

Session layer protocols include the following:

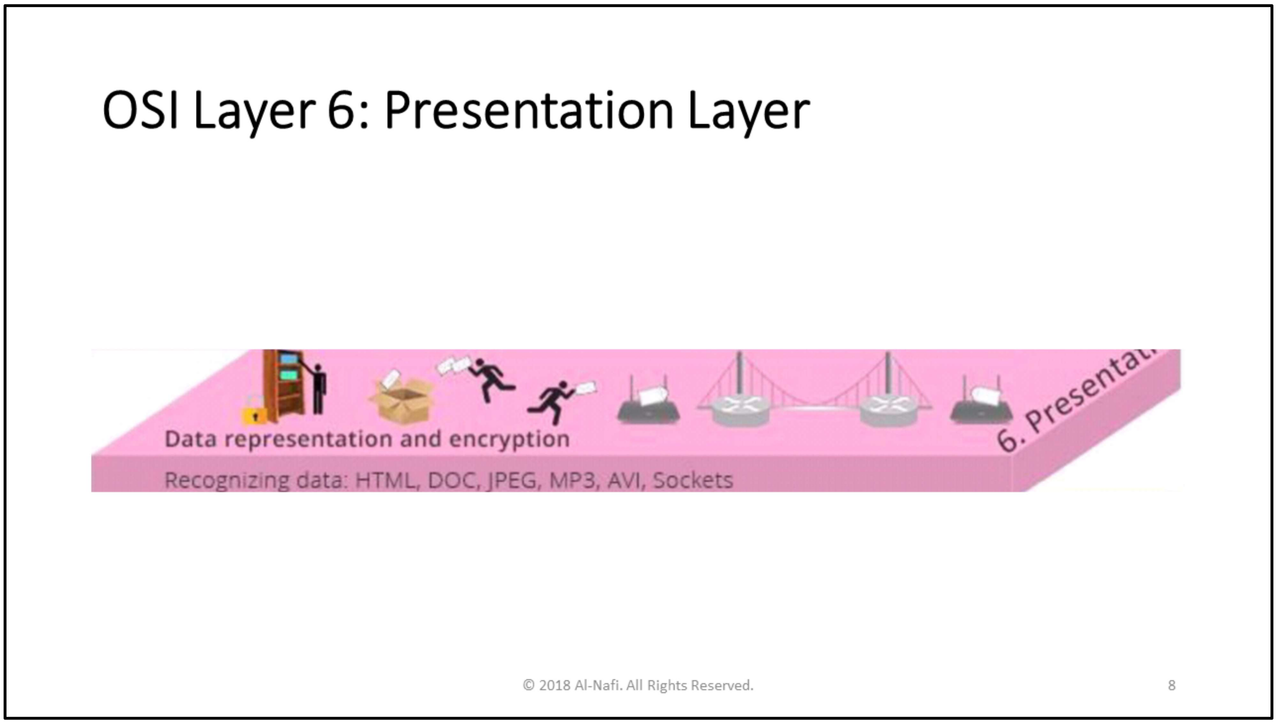
- PAP – password authentication protocol
- PPTP – Point-to-Point Tunneling Protocol
- RPC – remote procedure call protocol

RPCs represent the ability to allow for the executing of objects across hosts with a client sending a set of instructions to an application residing on a different host on the network. It is important to note that RPC does not in fact provide any services on its own; instead, it provides a brokering service by providing (basic) authentication and a way to address the actual service.



Threats and Countermeasures

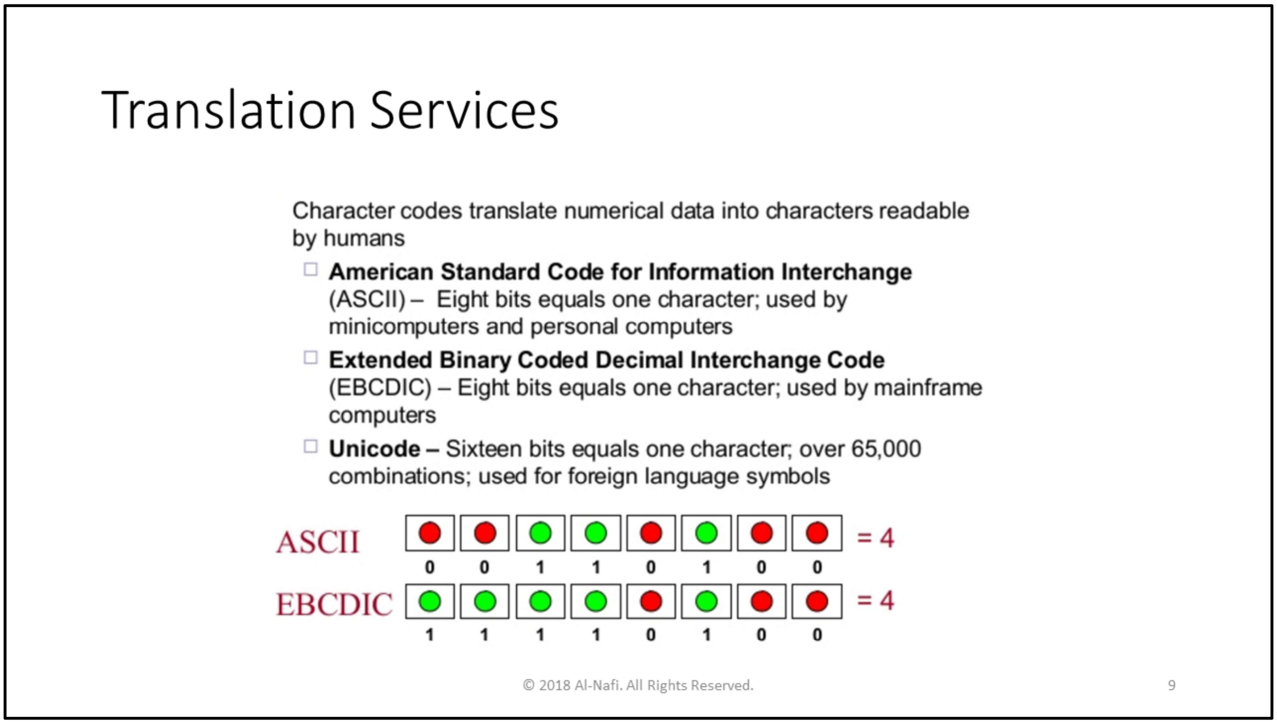
ISO 7498-2 specifies that no security services are provided in the session layer; therefore, it is imperative to address vulnerabilities revealed in the session layer by applying security services either above or below the session layer. A common methodology is to secure risky protocols that are still needed by means of encryption.



OSI Layer 6: Presentation Layer

Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
6. Presentati

The presentation layer maintains that communications delivered between sending and receiving computer systems are in a common and discernable system format.



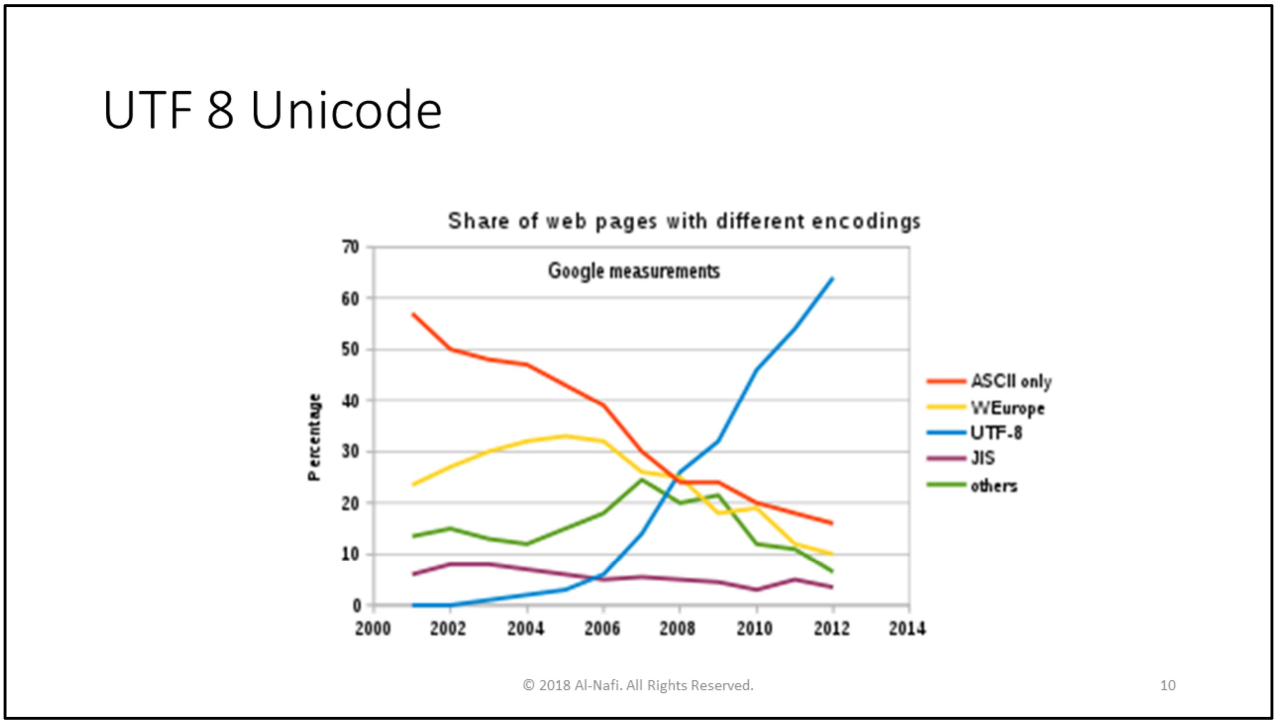
Translation Services

Character codes translate numerical data into characters readable by humans

- □ **American Standard Code for Information Interchange** (ASCII) – Eight bits equals one character; used by minicomputers and personal computers
- □ **Extended Binary Coded Decimal Interchange Code** (EBCDIC) – Eight bits equals one character; used by mainframe computers
- □ **Unicode –** Sixteen bits equals one character; over 65,000 combinations; used for foreign language symbols

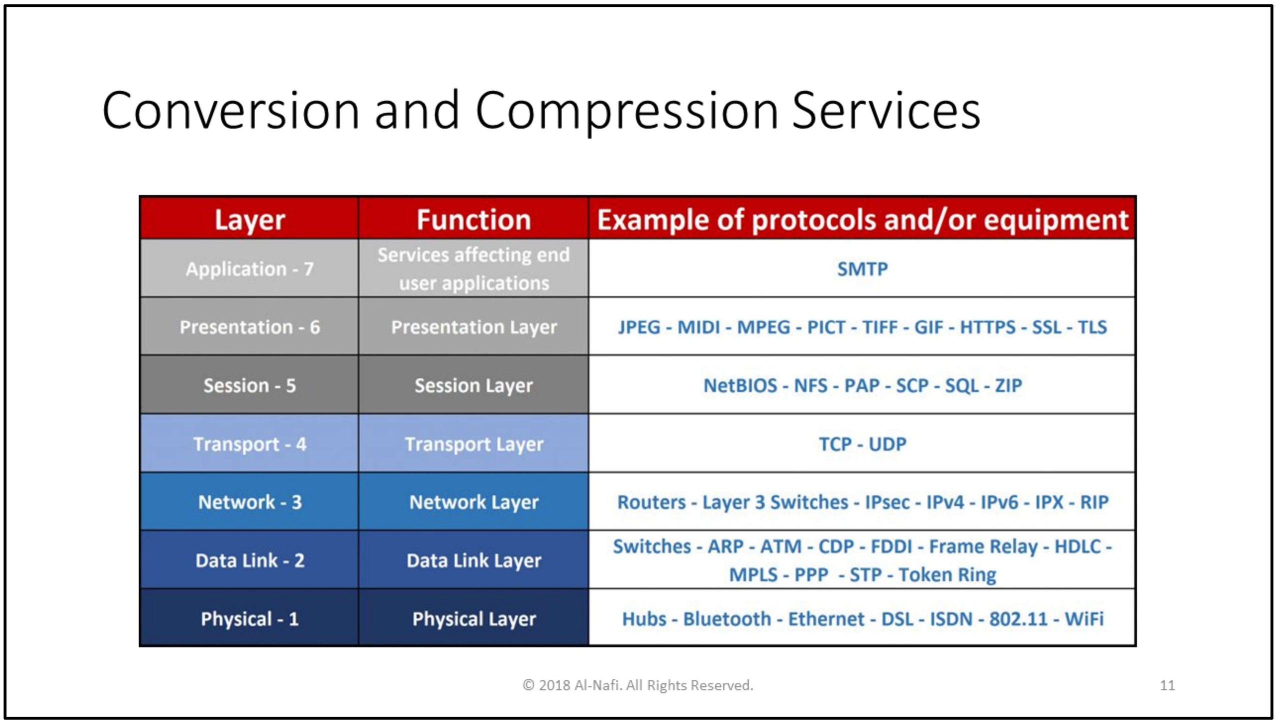
ASCII	🔴	🔴	🟢	🟢	🔴	🟢	🔴	🔴	= 4
	0	0	1	1	0	1	0	0	
EBCDIC	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🔴	= 4
	1	1	1	1	0	1	0	0	

To provide a reliable syntax, systems processing at the presentation layer will use American Standard Code for Information Interchange (ASCII) or Extended Binary Coded Decimal Interchange Code (EBCDIC) to translate from Unicode. In 2016 the W3C Internationalization Working Group estimated that 86 percent of all web pages sampled showed that they are using UTF 8 Unicode character encoding. It further states, “Not only are people using UTF-8 for their pages, but Unicode encodings are the basis of the Web itself. All browsers use Unicode internally, and convert all other encodings to Unicode for processing. As do all search engines. All modern operating systems also use Unicode internally. It has become part of the fabric of the Web.”



UTF 8 Unicode

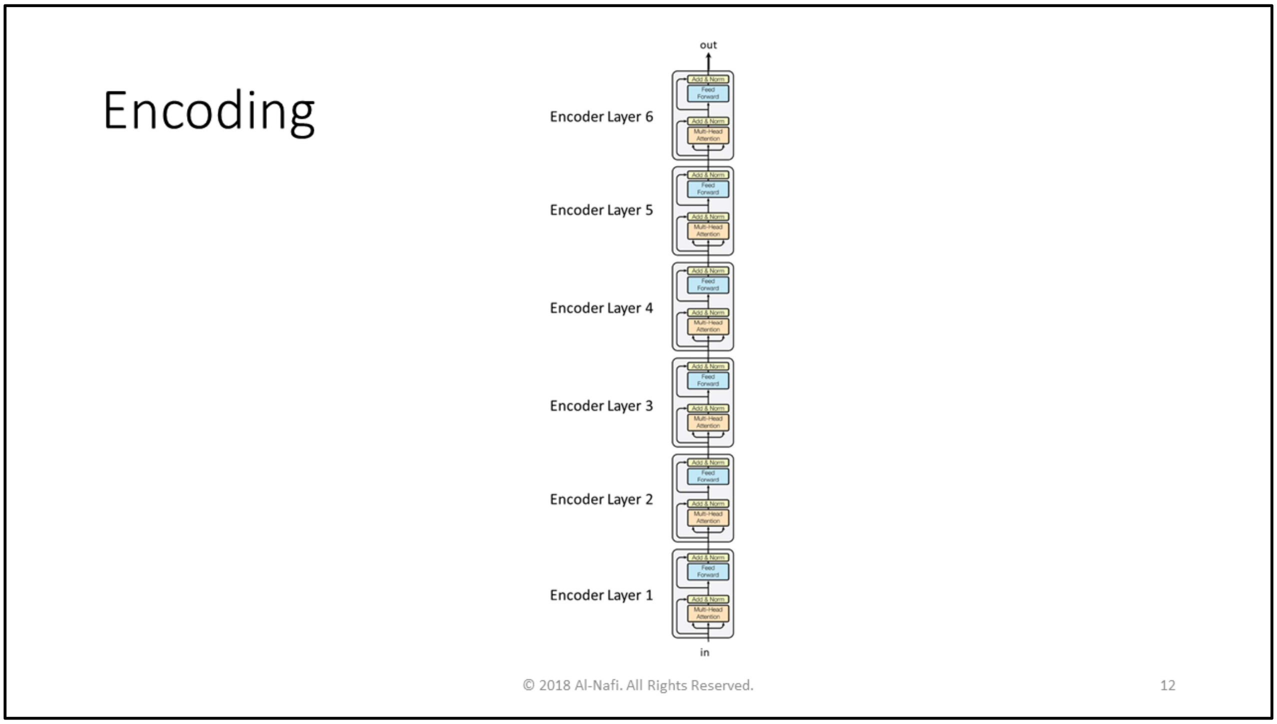
Translation services are also necessary when considering that different computer platforms (Macintosh and Windows personal computers) may exist within the same network and could be sharing data. The presentation layer is needed to translate the output from unlike systems to similar formats.



Conversion and Compression Services

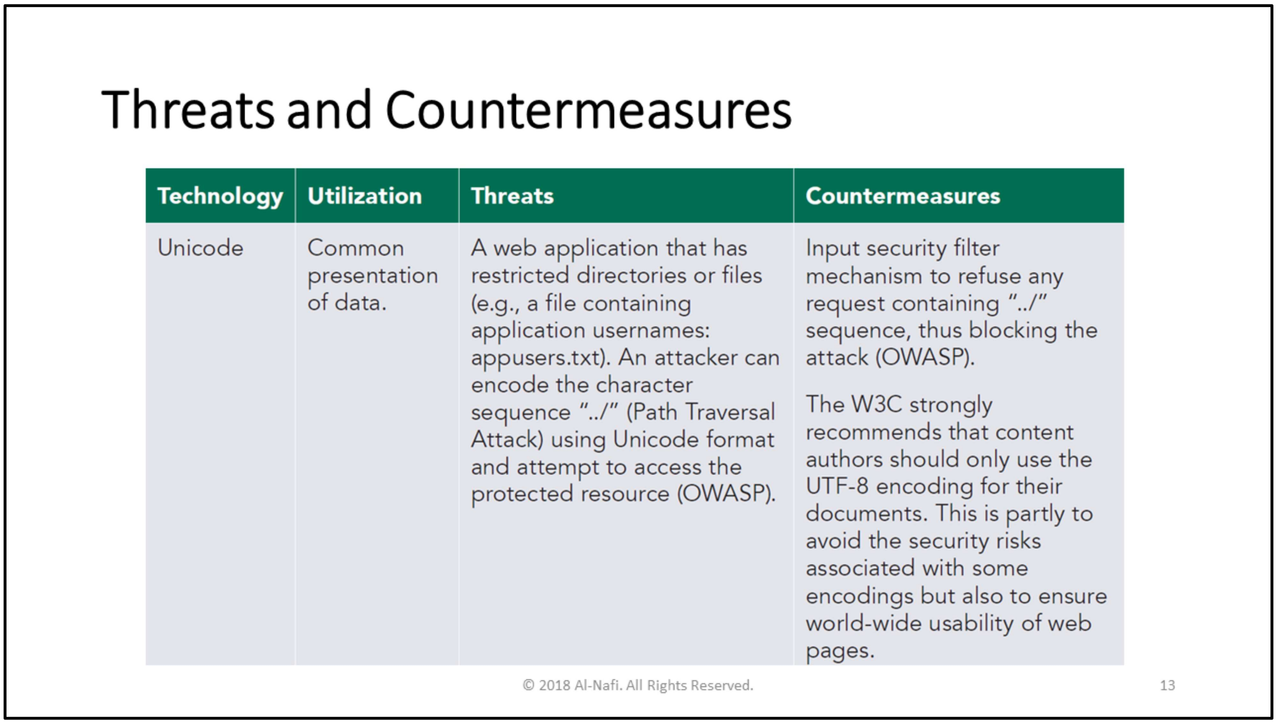
Layer	Function	Example of protocols and/or equipment
Application - 7	Services affecting end user applications	SMTP
Presentation - 6	Presentation Layer	JPEG - MIDI - MPEG - PICT - TIFF - GIF - HTTPS - SSL - TLS
Session - 5	Session Layer	NetBIOS - NFS - PAP - SCP - SQL - ZIP
Transport - 4	Transport Layer	TCP - UDP
Network - 3	Network Layer	Routers - Layer 3 Switches - IPsec - IPv4 - IPv6 - IPX - RIP
Data Link - 2	Data Link Layer	Switches - ARP - ATM - CDP - FDDI - Frame Relay - HDLC - MPLS - PPP - STP - Token Ring
Physical - 1	Physical Layer	Hubs - Bluetooth - Ethernet - DSL - ISDN - 802.11 - WiFi

Data conversion or bit order reversal and compression are other functions of the presentation layer. As an example, an MPEG-1 Audio Layer-3 (MP3) is a standard audio encoding and compression algorithm that creates a file with a bitrate of 128kbit/s. The Waveform Audio File Format (WAVE) with Linear PCM bitstream is another standard audio encoding and compression that creates a file with a bitrate of 44.1khz. The compression for both formats is accomplished at the presentation layer. If a tool is used to convert one format into another, this is also accomplished at the presentation layer.



Encoding

Encryption services such as TLS/SSL are managed below, above, and within the presentation layer. At times, the encoding capabilities that are resident at the presentation layer are inappropriately conflated with a specific set of cryptographic services. Abstract Syntax Notation (ASN.1) is an ISO standard that addresses the issue of representing, encoding, transmitting, and decoding data structures. The transfer of data entities between two points of communication could appear as nonsensical or encoding if a nonparticipating (eavesdropping) third party wasn't aware of the standard being used in transmission.



Threats and Countermeasures

Technology	Utilization	Threats	Countermeasures
Unicode	Common presentation of data.	A web application that has restricted directories or files (e.g., a file containing application usernames: appusers.txt). An attacker can encode the character sequence "../" (Path Traversal Attack) using Unicode format and attempt to access the protected resource (OWASP).	Input security filter mechanism to refuse any request containing "../" sequence, thus blocking the attack (OWASP). The W3C strongly recommends that content authors should only use the UTF-8 encoding for their documents. This is partly to avoid the security risks associated with some encodings but also to ensure world-wide usability of web pages.