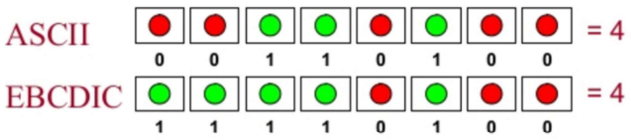
OSI Layer 6: Presentation Layer

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

Translation Services

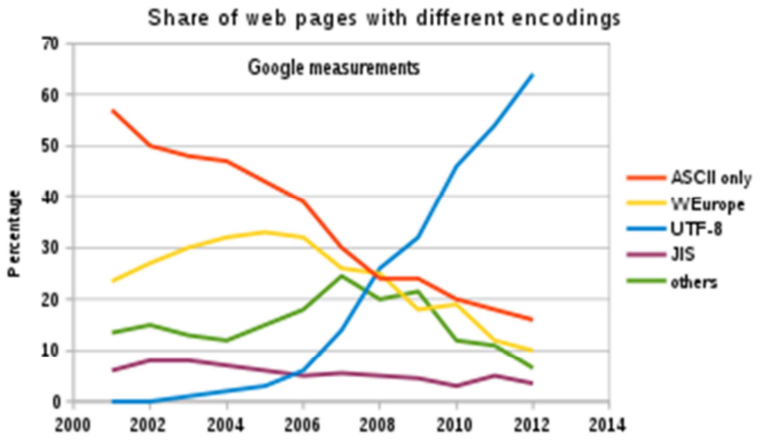
Character codes translate numerical data into characters readable by humans

- **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



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



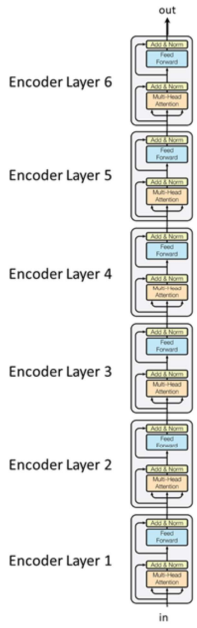
Translation services are also necessary when considering that different computer platforms (Macintosh and Windows personal computers) may exist within the same network and could be sharing data. The presentation layer is needed to translate the output from unlike systems to similar formats.

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.

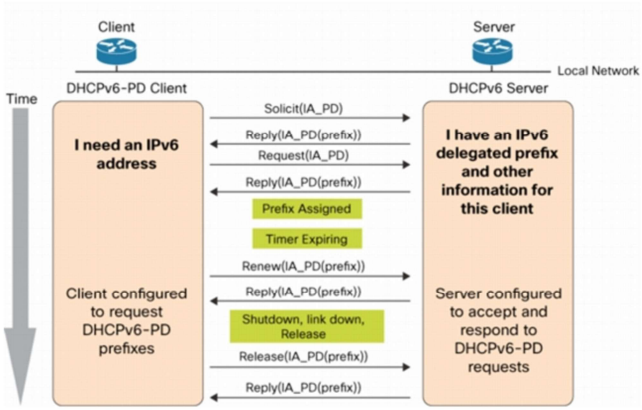
Threats and Countermeasures

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.

OSI Layer 7: Application Layer

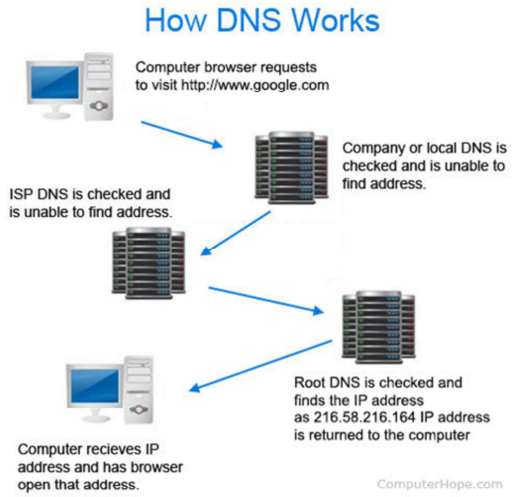
The application layer supports or hosts the function of applications that run on a system. All manner of a human supported interfaces, messaging, systems control, and processing occur at the application level. While the application layer itself is not the application it is where applications run.

Dynamic Host Configuration Protocol (DHCP/DHCPV6)



DHCP is a client/server application that is designed to assign IP addresses from a pool of pre-allotted addresses on a DHCP server. Based upon the specifications in RFC 2131, the client transmits on port 67 and the server responds on port 68. The client sends out a broadcast with a DHCPDISCOVER packet. The server responds with a DHCPOFFER giving the client an available address to use. The client responds back with DHCPREQUEST to use the offered address, and the server sends back a DHCPACK allowing the client to bind the requested address to the network interface card (NIC). If a DHCP server doesn't respond in a predetermined time, then the DHCP client self-assigns an IP address in the 169.254.x.x range based upon IPv4 Link-Local Addresses based upon RFC 3927.

Domain Name System (DNS)



DNS resolves Fully Qualified Domain Names (FQDN) to IP addresses and transmits data on port 53. According to RFC 1035, the local user, or client, queries an agent known as a Resolver that is part of the client operating system. DNS is used to resolve a FQDN to an IP address. Network nodes automatically register this resolution in the DNS server's database. To resolve any external domain name, each DNS in the world must hold a list of these root servers. Various extensions to DNS have been proposed to enhance its functionality and security, for instance, by introducing authentication using DNS Security Extensions (DNSSEC), multicasting, or service discovery.

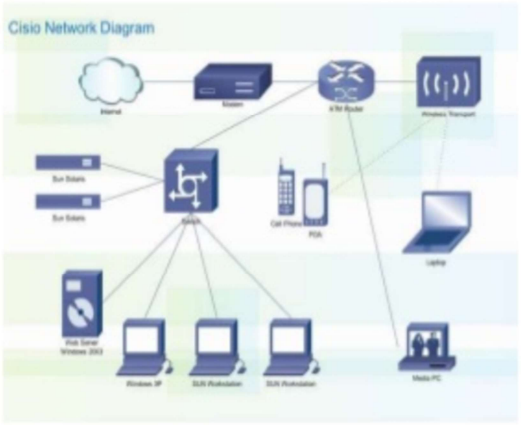
DNS maintains a directory of zones that have a hierarchical superior known as the root that are represented by an administrative (".") that is appended to the end of a FQDN. The root servers (at the initial printing of this publication there are 13) carry references to what is known as Top Level Domains (TLDs). A few examples of TLDs are .com; .edu; .gov; etc. The TLDs contain references to sub zones know as second level domain. A few examples of second level domains include amazon.com; microsoft.com; ibm.com; etc. The subzones can continue with third or fourth level domains that are typically tied to a specific service.

When a resolver connects to a DNS server, the default specifications state that it will do so with an iterative lookup. This means that the DNS server will hand the lookup to the resolver after making the first query. In a recursive lookup, the DNS server will return with a response of the FQDN to the original resolver after managing the lookup from the root servers until the last answer.
The following records are necessary for the DNS server to be operational.

- Host (A)
- Start of Authority (SOA)
- Name Server (NS)
- Pointer (PTR)
- Mail Exchange (MX)

Simple Network Management Protocol (SNMP)

- ❑ ...all SNMP compatible devices.
  - ✓servers
  - ✓workstations
  - ✓routers
  - ✓switches
  - ✓printers
  - ✓...many more.



 10

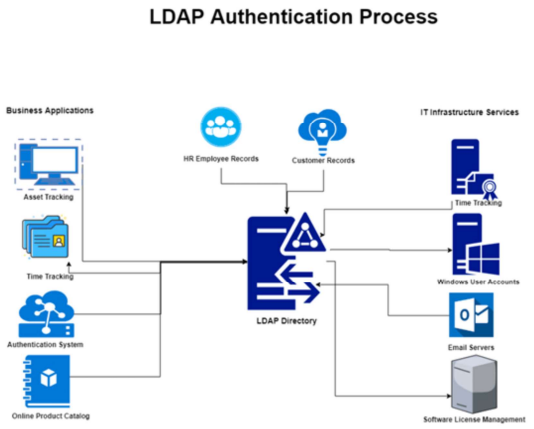
SNMP is designed to manage network infrastructure. SNMP architecture consists of a management server (called the manager in SNMP terminology) and a client usually installed on network devices, such as routers and switches, called an agent. SNMP allows the manager to retrieve “get” values of variables from the agent, as well as “set” variables. Such variables could be routing tables or performance-monitoring information. Probably the most easily exploited SNMP vulnerability is a brute-force attack on default or easily guessable SNMP passwords known as “community strings” often used to manage a remote device. Given the scale of SNMP v1 and v2 deployment, combined with a lack of clear direction from the security professional with regards to the risks associated with using SNMP without additional security enhancements to protect the community string, it is certainly a realistic scenario and a potentially severe but easily mitigated risk. Until version 2, SNMP did not provide any degree of authentication or transmission security. Authentication consists of an identifier, called a community string, by which a manager will identify itself against an agent (this string is configured into the agent) and a password sent with a command. As a result, passwords can be easily intercepted that could then result in commands being sniffed and potentially faked. Like the previous problem, SNMP

version 2 did not support any form of encryption so that passwords (community strings) were passed as cleartext. SNMP version 3 addresses this weakness with encryption
for passwords.

These are the primary components of SNMP:

- Network management systems
- Management information base
- Managed devices
- Agents

Lightweight Directory Access Protocol (LDAP)



LDAP uses a hierarchical tree structure for directory entries. Like X.500, LDAP entries support the DN and RDN concepts. DN attributes are typically based on an entity's DNS name. Each entry in the database has a series of name/value pairs to denote the various attributes associated with each entry.

Common attributes for an LDAP entry include the following:

- Distinguished Name (DN)
- Relative Distinguished Name (RDN)
- Common Name (CN)
- Domain Component (DC)
- Organizational Unit (OU)

LDAP operates in a client/server architecture. Clients make requests for access to LDAP servers, and the server responds back to the client with results of that request. LDAP typically runs over unsecured network connections using TCP port 389 for communications. If advanced security is required, version 3 of the LDAP protocol supports using TLS to encrypt communications.

Threats and Countermeasures continued…

Technology	Utilization	Threats	Countermeasures
DHCP	Dynamic assignment of IP addresses on a network.	Rogue DHCP service.	Port authentication of MAC addresses for all workstations.
DNS	Resolve web names to IP addresses.	Poisoning of DNS server records. Redirect resolvers to erroneous DNS services.	Utilize DNSSEC and harden DNS servers and related services to mitigate erroneous assignment of DNS services.
DNS	Resolve web names to IP addresses.	Amplification: Turn small queries into oversized payloads to exhaust victim DNS servers. Reflection: Use spoofed victim addresses to receive query responses.	Manages Black/ Whitelist (untrusted/ trusted) DNS servers, establish rate limiting responses. Deep packet inspection to detect malicious traffic.
HTTP	Resolve web page URL request from server to client.	Text traversing the internet is in plaintext and can be read and manipulated.	Utilize SSL or TLS - HTTPS.
LDAP	Directory service protocol for managing and organizing systems and services.	Injection for unauthorized query or content modification.	Utilize input validation for queries and strong authentication and encryption.
SNMP	Monitor enterprise system performance and health.	Sensitive system and information disclosure.	Utilize SNMP V3 only with strong encryption.