Global Knowledge®

Expert Reference Series of White Papers

Foundational Focus: OSI Model – Breaking Down the Seven Layers

Foundational Focus: OSI Model – Breaking Down the Seven Layers

James Michael Stewart, CISSP, ISSAP, SSCP, CPTE, CDFE, Q/SA, Q/EH, CH, CHFI, Security+

Introduction

The OSI model has been the *de facto* reference model for networking protocols since the mid-1990s. The OSI model is formally known as Open Systems Interconnection (OSI) model ISO/IEC 7498-1. International Organization for Standardization (ISO), is a global standards-settings group comprised of members from various national standards groups. International Electrotechnical Commission (IEC) is another global standards-settings group; however, it focuses on electrical, electronic, and related technologies. The IEC works closely with ISO and other groups to establish standards for computers, networking, and communications. The OSI model is a conceptual model rather than a technical specification. This means it is used to discuss, describe, compare, and contrast actual technologies rather than directly mandating elements of technology.

The OSI model is comprised of seven layers, with layer one positioned at the bottom of the layer stack, and layer seven at the top. The layers have assigned names as well as number references.

Figure 1. The OSI Model

The OSI model is used to describe the function and purpose of the various elements in network communications. In theory, data is received by the protocol stack into layer 7, the application layer, from software. The received data is labeled as a service data unit (SDU). Each layer adds its own layer-specific header to the SDU, thus creating a payload data unit (PDU). The PDU is then passed down to the next layer below, where it becomes the SDU of that layer. This process of traversing down the layer stack is known as encapsulation. Once layer 1, the physical layer, receives the PDU from layer 2, the data link layer, the data is transmitted over the network medium (i.e., twisted pair cable, fiber optic cable, or wireless).

When a network interface receives a signal of data from the network medium, it processes the PDU in reverse. This reverse unpacking process is known as de-encapsulation. Each layer reads its corresponding header of the PDU, processes and removes the header from the PDU, creating an SDU, then passes the SDU to the layer above. This is repeated until layer 7, the application layer, receives its PDU and passes the actual data to software.

While the generic term for a header and payload data for a given layer is known as a PDU, some layers and/or protocols have unique names for this structure. These include:

- 4 - Transport - TCP - segment
- 4 - Transport - UDP - datagram
- 3 - Network - packet or datagram
- 2 - Data link - Frame

There are two additional oddities to the process of encapsulation. The first is that the data link layer often adds a header and footer to the SDU to create its PDU. For example, the most common data link layer technology is Ethernet. Ethernet adds a header containing the destination MAC address, source MAC address, and EtherType designation (i.e., identification of the type of payload), while the footer includes a checksum value to perform integrity checks. The second is that most layer 1 physical layer technologies do not add any headers (or footers) to the PDU from layer 2. Instead, start and stop delimiter bits might be used on asynchronous communication (i.e., not time-synched), but these are not considered to be part of the PDU, just part of the transmission technology.

The header added by a layer is configured to include information relevant to the same layer on the receiving system. This layer-to-layer communication via header (and footer) is known as peer layer communications. It is essential that headers (and payload) arrive uncorrupted and are unpacked (i.e., de-encapsulated) in the correct order. Fortunately, communication errors are rare, intentional corruption is detectable, and most systems use standardized protocol stacks, such as TCP/IP, thus peer-layer communication is generally flawless.

Layer 7 – Application

Layer 7, the application layer, is the interface between the protocol stack and application software. The software might be client utilities or server services. It is the ability of software to communicate with the standardized interface of application layer protocols that makes network communications possible. In fact, the use of common application layer protocols allows for fully interoperable computer communications. The application layer is assigned the responsibility to check whether a remote communication partner is available, confirm communications with that partner are possible, and evaluate whether or not there are sufficient resources to maintain a communication.

It is important to remember that software, like a Web browser or an e-mail server, is not part of the application layer; rather, they communicate with protocols in the application layer. Most applications have a specific protocol designed around their data types, functions, and features. These include many of the most commonly used application protocols such as:

- HTTP - hypertext transfer protocol
- FTP - file transfer protocol
- SMTP - simple mail transfer protocol
- POP3 - post office protocol
- IMAP - internet message access protocol
- DNS - domain name service
- Telnet

Layer 6 – Presentation

The presentation layer, or layer 6, establishes context between disparate application layer protocols. Effectively, the presentation layer adjusts syntax, semantics, data types, data formats, etc. This layer ensures that data sent by an application is compatible with the lower layers of network communication, and that data received from the network is acceptable to the receiving software.

Layer 5 – Session

The session layer, or layer 5, manages the connections between computers. Connection management includes establishing, maintaining, and terminating the links between networked systems. This layer provides for full-duplex, half-duplex, and simplex communications (i.e., two-way simultaneous, two-way one-way-at-a-time, and one direction only). This layer also proves checkpoints or verification of delivered data, link recovery or re-establishment, and a graceful disconnect process.

Note: While the OSI model defines these features as part of the session layer, actual protocols, such as Transmission Control Protocol (TCP), exhibit many of the characteristics of both the transport layer and session layer.

Layer 4 – Transport

The transport layer, or layer 4, manages the integrity of a connection and controls the connection (at least as far as the connection or session is not being managed by the session layer). This layer potentially manages multiple connections simultaneously (often using a logical addressing scheme of ports on top of the network layer logical addresses). This layer defines the boundaries or rules of a connection, such as the size of data in each PDU, segmenting, sequencing, error checking, and how to determine if a PDU has been lost (or was not delivered). Many of these rules are defined uniquely for each connection during a session establishment handshake process. Two protocols commonly recognized as operating in this layer are TCP and User Datagram Protocol (UDP).

Layer 3 – Network

The network layer, or layer 3, provides for logical addressing and the management of communications between devices via service known as routing. While the network layer provides routing services and attempts to deliver

messages successfully, it does not guarantee delivery. This layer also includes error detection features. Internet Protocol (IP) is the most recognized protocol that operates at this layer. Currently, IPv4 is the most widely used version; however, IPv6 is quickly gaining in popularity. IPv6 got its official global Internet kick-off on June 6, 2012.

The OSI model also assigns the task of fragmentation to this layer; however, fragmentation is an often-abused feature of network layer protocols. For this reason, fragmentation is not supported in IPv6 and is generally blocked or filtered by firewalls on IPv4 connections.

Layer 2 - Data Link

The data link layer, or layer 2, formats the PDUs received from the network layer into the proper container for network transmission. On most networks, this proper container is the Ethernet frame. This layer also takes advantage of the hardware-assigned address of the physical interface card. This address is known as the media access control (MAC) address, or hardware address, or physical address. The most common standard technologies in use at the data link layer are Ethernet (IEEE 802.3) and Wireless (IEEE 802.11). The Address Resolution Protocol (ARP) is used at this layer (or between Layer 2 and Layer 3) to convert the destination IP address (logical) into a destination MAC address (physical).

Layer 1 - Physical

The physical layer, or layer 1, is the interface between the logical software of the network protocol and the hardware network interface card. It is at this layer that the conversion from the binary data of the layer 2 PDU occurs into the transmission technology encoding of the message bits, such as voltage variations, light pulses, or radio wave modulations. The devices at this layer manage transmission and reception of the bits, as well as physical-level synchronization, error detection, noise management, and contention media management.

TCP/IP Model

While the OSI model is the most widely used concept employed to compare and contrast networking concepts, there is a model derived directly from the most widely used protocol. The TCP/IP model was crafted directly from the TCP/IP protocol stack, and thus is a more true representation of the functions and operations of network protocols.

The TCP/IP model consists of only 4 layers and can be roughly mapped back to the OSI model for backwards referencing. The 4 layers of the TCP/IP model can be mapped to the OSI as follows:

- 4 - Process - OSI layers 5, 6,7
- 3 - Host-to-host - OSI layer 4
- 2 - Internetwork - OSI layer 3
- 1 - Link - OSI layers 1, 2

In spite of this being a more realistic and real-world model, it has not been adopted as a reference standard, or at least not to the extent of the OSI model. In most cases, layer references are still pointing to the OSI model.

Summary

The OSI model is a conceptual tool used to discuss and describe network functions. The use of a standard reference model is essential to communicating ideas as well as creating new technologies. It is a good idea to be familiar with the OSI model, the features assigned to each layer, and examples of common protocols or technologies associated with the OSI layers.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, Global Knowledge suggests the following courses:

Introduction to Information Technology (CompTIA Strata IT Fundamentals)

Network+ Prep Course (N10-005)

Understanding Networking Fundamentals

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart Has been working with computers for nearly thirty years. His work focuses on security, certification, and various operating systems Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author on the *CISSP Study Guide* 6th Edition, the *Security+ Review Guide* 2nd Edition (SYP-301), and *Network Security, Firewalls, and VPNs*. Michael has also contributed to many other security-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials, as well as presented materials in the classroom. Michael holds a variety of certifications, including CISSP, ISSAP, SSCP, CPTE, CDFE, Q/SA, Q/EH, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas a Austin with a bachelors degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by e-mail at michael@impactonline.com.