GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

The OSI Model: An Overview

Rachelle L. Miller

GSEC Practical Assignment Version 1.2e

The Open Systems Interconnection (OSI) reference model has served as the most basic elements of computer networking since the inception in 1984. The OSI Reference Model is based on a proposal developed by the International Standards Organization (ISO). The original objective of the OSI model was to provide a set of design standards for equipment manufacturers so they could communicate with each other. The OSI model defines a hierarchical architecture that logically partitions the functions required to support system-to-system communication.

The OSI model has seven layers, each of which has a different level of abstraction and performs a well-defined function. The principles that were applied to arrive at the seven layers are as follows (Feig)[1]:

- A layer should be created where a different level of abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessary, and small enough that the architecture does not become unwieldy.

The layered approach offers several advantages. By separating networking functions into logical smaller pieces, network problems can more easily be solved through a divide-and-conquer methodology. OSI layers also allow extensibility. New protocols and other network services are generally easier to add to a layered architecture.

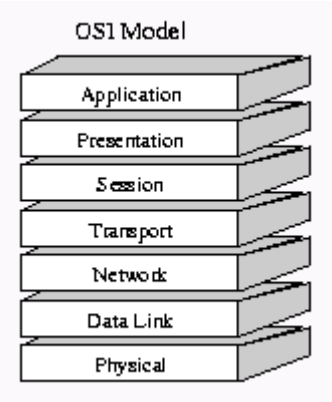
The seven OSI layers are defines as follows (Feig)[1]:

7. *Application*: Provides different services to the application
6. *Presentation*: Converts the information
5. *Session*: Handles problems which are not communication issues
4. *Transport*: Provides end to end communication control
3. *Network*: Routes the information in the network
2. *Data Link*: Provides error control
1. *Physical*: Connects the entity to the transmission media

(An acronym used to help remember the model from bottom to top is “Please Do Not Throw Sausage Pizza Away.” From top down the “All People Seem To Need Data Processing” acronym can be utilized.)

© SANS Institute 2000 - 2005 Author retains full rights.

The application, presentation, and session layers comprise the upper layers of the OSI Model. Software in these layers performs application specific functions like data formatting, encryption, and connection management. The transport, network, data link, and physical layers comprise the lower layers, which provide more primitive network-specific functions like routing, addressing, and flow controls.



(Mitchell)[2]

Application Layer (Layer 7)

The application layer is the top layer of the OSI model. It provides a set of interfaces for applications to obtain access to networked services as well as access to network services that support applications directly. This layer also provides application access security checking and information validation. The Application Layer provides the following functions (Tan Ten Hong)[3]:

- *File Transfer, Access and Management (FTAM):* Provides handling services in the network. This includes the movement of files between different systems, reading, writing and deletion of remote files, and management of remote file storage.
- *Virtual Terminal (VT):* Provides services to access applications in different remote computer systems through stimulating a real terminal.
- *Electronic Mail and Messaging Handling (MHS):* Facilitates the electronic exchange of documents.
- *Directory Services (DS):* Provides services with the ability to match names with addressing information.
- *Common management Information Protocol (CMIP):* Provides services for network management.

Distributed applications services, whether OSI or TCP/IP based, have some common characteristics (Tan Ten Hong)[3]:

- An end-user interface that provides a human or another application with the means to enter commands that direct the application to send files to and receive files from a remote host, list or change directories, rename or delete files, etc.
- The means of performing input to and output from mass storage devices.
- The means of transferring the files and file-related information between hosts.

© SANS Institute 2000 - 2005 Author retains full rights.

Presentation Layer (Layer 6)
The presentation layer is responsible for the format of the data transferred during network communications. This layer is concerned with the syntax and semantics of the information transmitted. For outgoing messages, it converts data into a generic format for the transmission. For the incoming messages, it converts the data from the generic form to a format understandable to the receiving application. Different computers have different codes for representing data. The presentation layer makes it possible for computers with different representation to communicate. The presentation layer provides common communication services such as encryption, text compression, and reformatting.

The presentation layer is also concerned with other aspects of information representation. Data compression can be used to reduce the number of bits that have to be transmitted. Cryptography is frequently required for privacy and authentication.

Session Layer (Layer 5)
The session layer permits two parties to hold ongoing communications called a session across a network. The applications on either end of the session can exchange data or send packets to another for as long as the session lasts. The session layer handles session setup, data or message exchanges, and tear down when the session ends. It also monitors session identification so only designated parties can participate and security services to control access to session information. A session can be used to allow a user to log into a remote time-sharing system or transfer a file between two machines. (Tan Ten Hong)[3]

The session layer has the option of providing one-or-two-way communication called dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time. Token management may be used to prevent both sides from attempting the same operation at the same time. To manage these activities, the session layer provides tokens that can be exchanged. Only the side holding the token is permitted to perform the critical operation.

Another session service is synchronization. Consider the problems that occur when transferring a file between two machines and the system crashes not being able to complete the transfer. This process must be restarted from the beginning. To avoid this problem, the session layer provides a way to insert checkpoints into the data stream, so that after a crash, only the data after the last checkpoint has to be repeated.

Transport Layer (Layer 4)
The basic function of the transport layer is to accept data from the session layer, split it up into smaller units, pass it to the network layer, and ensure that the bits delivered are the same as the bits transmitted without modification, loss or duplication.

If an error occurs during transmission, the transport layer must correct it. There is a set

© SANS Institute 2000 - 2005 Author retains full rights.

of rules to follow that detail the handling of the error and how to correct it. The correction may mean re-sending just the damaged data or restarting from the beginning. This can be achieved because the transport layer protocol includes the capability to acknowledge the receipt of a packet. "If no acknowledgement is received, the transport layer can retransmit the packet or time-out the connection and signal an error. The transport protocol can also mark packets with sequencing information so that the destination system can properly order the packets if they are received out of order." (Tan Ten Hong)[3]

If the transport connection requires a high throughput, the transport layer might create multiple network connection by dividing the data among the network connections to improve the throughput. However, the transport layer might multiplex several transport connections onto the same network to reduce costs. This multiplexing is transparent to the session layer.

"Transport protocols provide the capability for multiple application processes to access the network by using individual local addresses to determine the destination process for each data stream. These addresses are often referred to as ports and connection opened to these ports as sockets." (Tan Ten Hong)[3]

Network Layer (Layer 3)

The network layer controls the operation of a sub-net, provides routing, congestion control and accounting. The network layer provides both connectionless and connection-oriented services. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are within the network and rarely change. They could also be determined at the start of each conversion. Finally, they could be highly dynamic, being newly determined for each packet to reflect the current network load. It is up to the network layer to allow heterogeneous networks to be interconnected. The IP protocol resides in this layer. All routers in the network are operating at this level.

If too many packets are present in the sub-net at the same time, bottlenecks will form. The network layer helps to control this congestion. An accounting function is built into the network layer to ensure that the number of bits sent is the number of bits received.

Controls over network connections, logical channels, segmenting and sequencing, and data flow can be placed in this layer.

Data Link Layer (Layer 2)

The main task of the data link layer is to take a raw transmission and transform it into a line that appears free of transmission errors in the network layer. It accomplishes this task by having the sender break the input data up into data frames, transmit the frames sequentially, and process the acknowledgment frames sent back by the receiver. The protocol packages the data into frames that contain source and destination addresses. These frames refer to the physical hardware address of each network card attached to

© SANS Institute 2000 - 2005 Author retains full rights.

the network cable. Ethernet, Token Ring, and ARCnet are examples of LAN data link protocols. If communication extends beyond the LAN onto the Internet, the network might use other data link protocols, such as Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP).

The data link layer sends blocks of data with the necessary synchronization, bit error detection/correction error control, and flow control. This control of data flow controls approximately 70 percent of all error handling. Since the physical layer merely accepts and transmits a stream of bits without any regard to the meaning of the structure, it is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

Encryption can be used to protect the message as it flows between each network node. Each node then decrypts the message received and re-encrypts it for transmission to the next node.

Physical Layer (Layer 1)

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions are how many volts should be used to represent a 1 and how many for a 0, how many microseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established and how it is torn down when both sides are finished, and how may pins the network connector has and what each pin is used for. The design issues deal largely with mechanical, electrical, functional, and procedural interface.

The physical layer describes some type of cabling system as the transmission media. It also describes the network topology and how the transmission media is to be distributed. Some examples include the bus, star, and ring topologies.

Concepts

Three concepts are central to the OSI model:

1. Services
2. Interfaces
3. Protocols

Information from each layer passes up to the next layer, so that a protocol operating at a given layer can access all the information the protocols below it collect or prepare. Each layer performs some services for the layer above it. The service definition tells what the layer does, not how entities above it access or how the layer works. A layer's interface tells the processes above it how to access it. It specifies what the parameters are and what results to expect. The layer can use any protocols as long as it provides the offered services.

© SANS Institute 2000 - 2005 Author retains full rights.

OSI versus TCP/IP

TCP/IP has four layers in its transport model instead of the seven that the OSI reference model lays out. When compared to the OSI reference model, the TCP/IP model combines the application, presentation, and session layers into a single top layer, called the application layer, and combines the data-link and physical layers into a bottom layer, called the network interface layer.

OSI	***TCP/IP***
Application (Layer 7)	Application
Presentation (Layer 6)	
Session (Layer 5)	
Transport (Layer 4)	Transport
Network (Layer 3)	Internet
Data Link (Layer 2)	Subnet
Physical (Layer 1)	

Summary

- The application layer is the layer at which a user and a computer interface to a network to view a message, data request, or response. It contains a variety of commonly used protocols, such as file transfer, virtual terminal, and email.
- The presentation layer converts incoming and outgoing data from one presentation format to another. It manages the syntax and semantics of the information transmitted between two computers.
- The session layer manages the establishment of a continuing series of requests and responses between the applications at each end. It establishes and manages sessions, conversions, and dialogues between two computers.
- The transport layer manages the end-to-end control and error checking.
- The network layer handles the routing of the data. It controls the operation of a packet from one network to another.
- The data link layer provides error control and synchronization for the physical level
- The physical layer conveys the bit stream through the network at the electrical and mechanical level. It physically transmits signals across a communication medium.

Conclusion

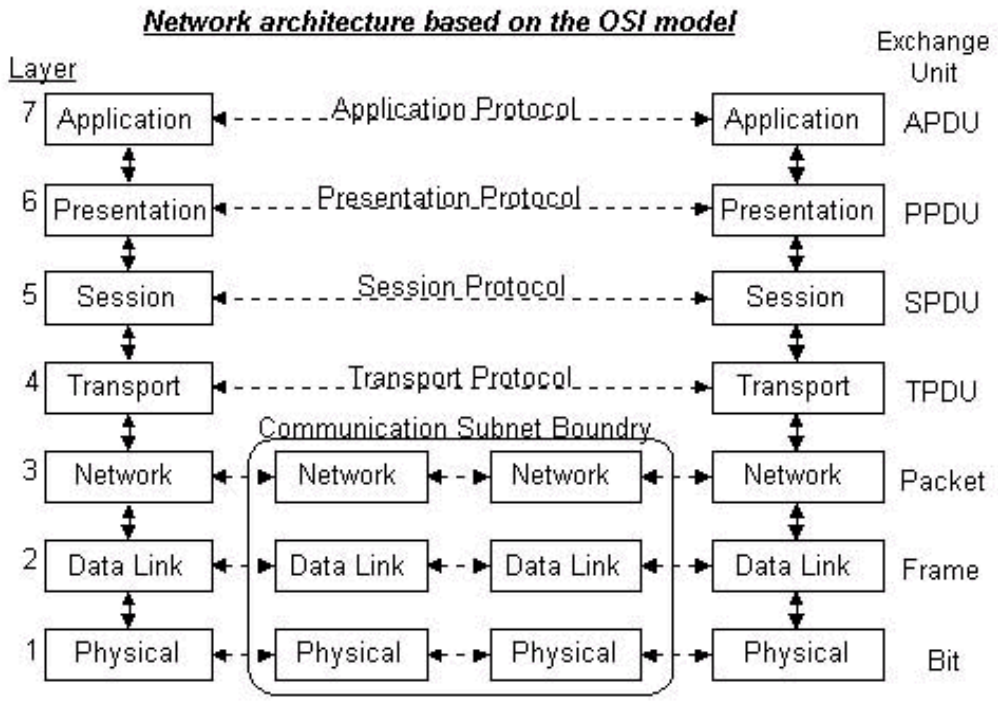
Not every network uses all of the model's layers. ISO's intent in creating the OSI model wasn't to describe every network but to give protocol designers a map to follow to aid in design. This model is useful for conceptualizing network components to demonstrate how they fit together to help the computers within the network communicate.

The OSI reference model was formulated as a template for the structure of communications systems. It was not intended that there should be standard protocols associated with each layer. Instead, a number of different protocols have been developed each offering a different functionality. There are three major international

© SANS Institute 2000 - 2005 Author retains full rights.

organizations developing standards and protocols for communications including:

- International Standards Organization (ISO)
- American Institute of Electrical Engineers (IEEE) – produces standards for use by computer manufacturers
- International Telecommunications Union – Telecommunications Sector (ITU-T) – produces standards for connecting different types of national and international public networks



(Feig)[1]

Work Cited

© SANS Institute 2000 - 2005 Author retains full rights.

1. Feig, Rami. "Computer Networks: The OSI Reference Model." URL: http://www.rad.com/networks/1994/osi/intro.htm (31 July 2001).

2. Mitchell, Bradley. "Basic Network Design – The OSI Model." URL: http://compnetworking.about.com/library/weekly/aa052800a.htm (31 July 2001).

3. Tan Teng Hong, Andrew; Chee Meng, Mah; Yew Wai, Chee; Yoke Chuan, Tan; Kim Ming, Cheong; "Comparing OSI and TCP/IP." URL: http://members.tripodasia.com.sg/osi/home.htm (31 July 2001).

References

Anderson, Christa. "Mapping Practice to Theory: NT Networking and the OSI Model." Windows 2000 Magazine. 1 March 1999. URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=4912 (15 August 2001).

Briscoe, Neil. "Understanding The OSI 7-Layer Model." PC Network Advisor Issue 120 (July 2000): 13 - 14.

Feig, Rami. "Computer Networks: The OSI Reference Model." URL: http://www.rad.com/networks/1994/osi/intro.htm (31 July 2001).

Mitchell, Bradley. "Basic Network Design – The OSI Model." URL: http://compnetworking.about.com/library/weekly/aa052800a.htm (31 July 2001).

Rohlin, Robert W. "OSI Model: Upper Layers". URL: http://www.rohlin.com/helpdesk//CCNA/upper_layers.htm (31 July 2001).

Tan Teng Hong, Andrew; Chee Meng, Mah; Yew Wai, Chee; Yoke Chuan, Tan; Kim Ming, Cheong; "Comparing OSI and TCP/IP." URL: http://members.tripodasia.com.sg/osi/home.htm (31 July 2001).

"OSI Model Layers."
URL: http://www.geocities.com/SiliconValley/Monitor/3131/ne/osimodel.html (31 July 2001).

"Understanding the OSI Reference Model."
URL: www.msic.com/tech_resources/osi_info.html (15 August 2001).

Zhou, Tao, "ISO/OSI, IEEE 802.2, and TCP/IP." URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=22

© SANS Institute 2000 - 2005, Author retains full rights.