Expert Reference Series of White Papers

The TCP/IP and OSI Models

The TCP/IP and OSI Models

Paul Simoneau, Global Knowledge Course Director, Network+, CCNA, CTP

Introduction

Two well-known protocol suites began working toward their standardization processes at about the same time. One was being developed under contracts to the Defense Advanced Research Projects Agency (DARPA). It eventually became TCP/IP, named for its core protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). Its cousin grew up under the watchful eyes of the International Organization for Standardization (ISO)1. Its name was more focused on its function: Open Systems Interconnection (OSI)[1]. OSI is composed of two parts. Part one, called the Basic Reference Model, is also known as the 7-layer model, or the OSI model. The other part is a set or suite of specific protocols for each layer.

History

In 1981, the Network Information Center (NIC) identified TCP/IP as its Internet standard in Request for Comments (RFC) 791 and 793. As of August, 1983, Department of Defense (DoD) set it as Military Specification 1778. In 1984, ISO specified OSI as ISO standard 7498. At the same time, the Consultative Committee on International Telephone and Telegraphy (CCITT), now known as the International Telecommunications Union Telecommunication Standardization Sector (ITU-T), designated the OSI Model as standard X.200. In 1987, after a subset of the OSI suite known as the Government Open Systems Interconnection Profile (GOSIP) became a Federal Information Processing Standard (FIPS), DoD sent out a letter declaring GOSIP "an experimental co-standard to the DoD protocols" as a result of the standards work done by the American National Standards Institute (ANSI) and the National Bureau of Standards (NBS). Though TCP/IP was and is in the public domain, and so free to use, GOSIP held the potential for large government contracts. This led to many companies wasting vast sums of money trying to produce OSI software while the networking community moved ahead with developing TCP/IP protocols, and then writing the standards. By 1994, after repeated attempts to make the GOSIP solution function, the OSI FIPS was finally rescinded.

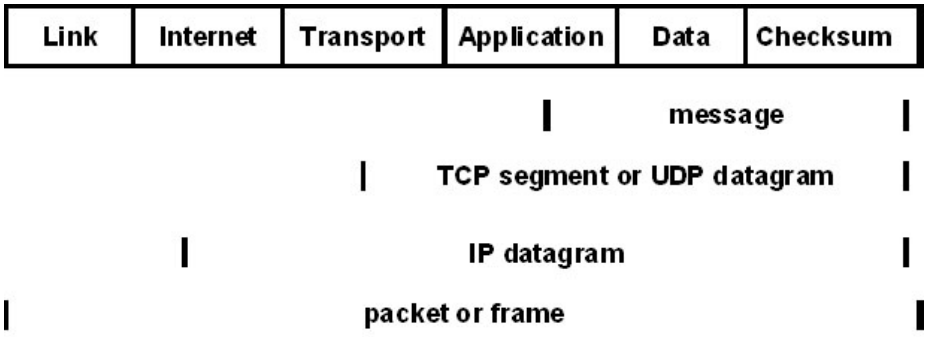
Similarities

- Both protocol suites (TCP/IP and OSI) use a layered approach.
- They are both designed to provide end-to-end communication.
- Both have similar Transport and Network layers.
- The suites both assume packets will be switched, meaning the packets can take different paths to their destination.
- Both solutions require that the network professionals using them must understand them in detail.
- With the common use of the OSI model as a way to describe the layers and their functions, network professionals must know both models.

Differences

- The application layer in TCP/IP handles the responsibilities of multiple layers in the OSI model.
- The OSI model numbers and names its layers, whereas the TCP/IP stack only names the layers.
- Unlike the transport layer in OSI, TCP/IP only guarantees reliable delivery of packets when TCP is the chosen protocol.
- OSI has much more complexity in its 7 layers than TCP/IP has in its 4 layers.
- In TCP/IP, protocols are deliberately designed to have more layer flexibility than the strict layers of the OSI model.
- TCP/IP functions are implemented, then standardized. OSI is standardized in concept only, though some functions work.
- OSI has more limited Network Management and Network Security.

TCP/IP Stack Layers



The four layers in TCP/IP are, from the top down: are as follows.

The **Application Layer** has the responsibility for authentication, data compression, and end-user services such as terminal emulation, file transfer, e-mail, web browsing/serving, and other network control and management services. An application header and following data are packaged as a message.

The **Transport Layer**, sometimes also called the **Host-to-Host Layer**, handles end-to-end communications, error handling, flow control, and connection-oriented or connectionless communication. An application message and a connection-oriented TCP header combine into a TCP segment. When a connectionless UDP header is attached to an application message, the result is a UDP datagram.

The **Internet Layer**, also known as the Internetwork Layer, does the heavy lifting for the network by supporting logical addressing, mapping logical addresses to physical addresses, routing decisions, subnetting, multicasting, logical error reporting, and network diagnostics. Adding an IP header to a TCP segment or a UDP datagram creates an IP datagram.

The **Link Layer**, which is also called the **Network Interface Layer**, **Network Access Layer**, or **Local Link**, interfaces the rest of the protocol stack with the link protocols and the local communications hardware. It functions locally

and may be different along each network from one host or system to another. Unlike the other three layers, other standards organizations, like the Institute for Electrical and Electronics Engineers (IEEE), set the standards for this layer, for example, for Ethernet and Wi-Fi. Adding a link layer header to the front of an IP datagram and a checksum or Frame Check Sequence (FCS) to the end frames the data and is called a frame. Some other link layer protocols identify the created package by adding their header to the IP datagram as a packet. The generic name is also "packet," which is left from the early days of data communication.

While the first names given for each layer are the official names listed in the "Requirements for Internet Hosts," the alternate names are used in books and classrooms to explain the TCP/IP suite of protocols.

The OSI Model Layers

Layer 2	Layer 3	Layer 4	Layer 5	Layer 6	Layer 7	Data

The 7 layers of the OSI Protocol Stack are, in descending order, as follows:
Layer 7 is the Application Layer for supporting end user services such as terminal emulation, file transfer, em-ail, and web browsing.

- Layer 6 - the **Presentation Layer** that handles data encryption and data compression
- Layer 5 - the **Session Layer** for providing authentication and authorization
- Layer 4 - the **Transport Layer** that guarantees end-to-end delivery of packets
- Layer 3 - the **Network Layer** for doing packet routing
- Layer 2 - the **Data Link Layer** that transmits and receives packets
- Layer 1 - the **Physical Layer** that is the physical connection or cable

TCP/IP Suite Details[2] in the OSI Model Layers

Layer 7	IMAP4	FTP	Telnet	SMTP	HTTP	POP3	BGP4	DNS	DNS	DHCP	TFTP	SNMP	RIP2
Layer 6													
Layer 5													
Layer 4	TCP								UDP				
Layer 3	ARP			ICMP		IGMP		IPsec IP	OSPF			EIGRP	
Layer 2	SLIP			LLC MAC			Frame Relay		PPP				WLAN
Layer 1	UTP			RF			STP		OF				

Layer 7

IMAP4 - Internet Mail Access Protocol version 4 lets clients access an IMAP4 mail server to download their e-mail to a local computer program. It works using TCP as its transport protocol.

FTP - File Transfer Protocol uses TCP as transport and allows the transfer of files between two computer systems with login required by the requester.

Telnet – Sometimes incorrectly called Terminal Emulation across a network, it is used to remotely open a session on another computer acting as a server. It relies on TCP for transport.

SMTP - Simple Mail Transfer Protocol is a TCP-transported application layer protocol used to send electronic mail.

HTTP - Hypertext Transfer Protocol uses the TCP transport protocol to carry web browsing requests to a web server, and web pages from web servers to web browsers.

POP3 - Post Office Protocol version 3 uses TCP as a way to offer clients access to a POP3 mail server to transfer their e-mail to a local program on their computer.

BGP4 - Border Gateway Protocol version 4 is a routing protocol most often used between organizations. Two routers using BGP will establish a TCP connection to send each other their BGP routing tables. In that exchange is information about reachable networks including the full path to all BGP-known networks.

DNS[3] - Domain Names System provides the ability to refer to IP devices using names instead of numerical IP addresses. It lets Domain Name Servers resolve these names to their corresponding IP addresses.

DHCP - Dynamic Host Configuration Protocol uses UDP as its transport protocol to dynamically and automatically assign IP addresses and other networking configuration information to computers starting up on a given network.

TFTP - Trivial File Transfer Protocol is a UDP-transported protocol that allows file transfer between two computers with no login or user required for its limited use.

SNMP - Simple Network Management Protocol is used to manage all types of network elements based on various data sent and received using UDP as its transport protocol.

RIP2 - Routing Information Protocol is an internal routing protocol used to dynamically update router tables on internal organization networks. It uses UDP as its transport protocol.

Layer 6

Layer 5

Layer 4

TCP - Transmission Control Protocol is a reliable, connection-oriented protocol that supports application-level services between computer systems. Its reliability comes with more overhead, though with today's fast networks, it is almost as fast as UDP.

UDP - User Datagram Protocol is a less reliable, connectionless protocol that provides faster communication between computer systems than TCP due to far less overhead.

Layer 3

ARP - Address Resolution Protocol supports the packaging of IP data into Ethernet frames. It finds the local Ethernet (MAC) address that matches a specific local IP address.

ICMP[4] - Internet Control Message Protocol provides diagnostics and logical error reporting to help manage the sending of data between computers. Its best-known function is ping.

IGMP - Internet Group Management Protocol supports multicasting by letting multicast routers track group memberships on each of its connected networks.

IPsec - Internet Protocol Security is an end-to-end security scheme for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

IP[4] - Internet Protocol provides connectionless communication support for all protocols' data, except ARP, by packaging that data into an IP datagram.

OSPF - Open Shortest Path First is an internal routing protocol for use inside an organization. It checks the function of its link to each of its neighbor OSPF routers. Then, it sends the acquired routing information to those neighbor routers.

EIGRP - Enhanced Interior Gateway Routing Protocol is a local routing protocol that is proprietary to Cisco. It is an advanced distance-vector routing protocol that shares internal organizational routing information found in three tables.

Layer 2

SLIP - Serial Line Internet Protocol puts IP data into data frames for carrying across serial lines.

Frame Relay - Frame Relay is a standard packet switching solution designed for Wide Area Networking (WAN).

PPP - Point-to-Point Protocol is a variation of serial line data encapsulation that improved SLIP by supporting protocols other than IP and adding extra functions, including authentication.

LLC/MAC - Logical Link Control and **Media Access Control** work together to connect IP to the "physical" media (copper wire, fiber optic cable, or the air) by controlling the communication signal (electricity, light, or radio frequencies). The MAC sub layer provides access to the physical medium along with local link addressing, size indicator, and making sure the data sent is the data received. To do that, it also

communicates with the LLC sub-layer above it allowing it to access and speak to the upper-layer network protocols such as IP. Other communications methods such as Ethernet[5], WLAN[6], and Fiber Distributed Data Interface (FDDI) use LLC/MAC.

Layer 1

UTP - Unshielded Twisted Pair cables are the most common cables used in computer networking. They are copper wires grouped into sets of 4-pairs for Ethernet use, or 25-pairs for other communications such as WANs. Each wire pair is specified and twisted at a separate rate from other pairs to minimize cross communication (crosstalk) within a multiple-pair cable. Each wire is coated with an insulator to prevent direct contact with other wires.

RF - Radio Frequency is a shorthand term for using radio signals to send and receive communications. In this use, it encompasses the media for IEEE802.11 or WI-Fi, IEEE802.15 or Bluetooth, and IEEE802.16 or WiMAX.

STP - Shielded Twisted Pair cables are based on UTP cables with the variation that each pair includes metal or foil shielding to further protect its signals from electromagnetic interference (EMI).

OF - Optical Fiber cabling uses light to carry signaling. It comes in two main versions: Single Mode Fiber (SMF) and Multimode Fiber (MMF). SMF uses a laser as its light source while MMF uses a Light Emitting Diode (LED) to send its signals.

Conclusion

TCP/IP and OSI both seem to use a layered approach to computer networking. TCP/IP does so in four layers while OSI has seven layers that look a lot like the solution IBM developed when it moved to System Network Architecture (SNA). From there, the two "models" take quite different paths. TCP/IP began with protocols that had been discussed, developed, tested, implemented, and then presented as a proposed standard. This gave TCP/IP much more flexibility and less reliance on layers than OSI. ISO developed the OSI model as a structure for protocols that would be developed at the designated layer for the specific purpose that performs only at that particular layer. The layer responsibilities are more structured in the OSI scheme.

The greater complexity of OSI and a wide-spread desire to have simplified standards made TCP/IP the choice for networking. The clear, layered structure and detail of the OSI model has made it the way most network technical staff members describe network activity, especially for installing, managing, and troubleshooting today's digital networks.

To understand what "techies" are talking about requires detailed knowledge of networking terms and how they fit into the OSI model, as well as how TCP/IP and its protocols do what they do. It also requires an understanding of how TCP/IP and its protocols fit into the OSI model.

NOTES:

1) "Because "International Organization for Standardization" would have different acronyms in different languages ("IOS" in English, "OIN" in French for Organisation internationale de normalisation), its founders decided to give it also a short, all-purpose name. They chose "ISO", derived from the Greek isos, meaning,

"equal". Whatever the country, whatever the language, the short form of the organization's name is always ISO." http://www.iso.org/iso/about/discover-iso_isos-name.htm

2) The TCP/IP details here are limited, for space reasons, to the best known and most used protocols.

3) DNS operates over TCP to update one server with another server's information. DNS operates over UDP to support a quick request and response to lookup names and get IP addresses.

4) IP and ICMP both work together in either version 4 or in version 6 depending on the network.

5) Ethernet comes in two flavors: Ethernet II and IEEE 802.3. Ethernet II is the de facto standard while IEEE802.3 is the standard de jure Both operate at multiple different speeds: 10Mbps, 100Mbps, 1000Mbps, 10Gps, 40Gbps, and 100Gbps. Mbps is million bits per second. Gbps is billion bits per second (in US measurement).

6) A wireless local area network links two or more devices using radio communications. It usually offers a connection to a wired network and the Internet. This may also be known as Wi-Fi or by its official name IEEE802.11

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

TCP/IP Networking
Understanding Networking Fundamentals
Voice over IP Foundations

For more information or to register, visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

Paul Simoneau has over 37 years of experience in working with multiple aspects of computers and data communications. He is the founder and president of NeuroLink, Ltd., an international coaching and education company specializing in professional development. NeuroLink's client list includes Cisco, AT&T, Lucent, Citibank, Quest Communications, Hewlett-Packard, Sprint, Verizon, all branches of the US Armed Forces, and many others.

He is also a senior instructor and course director with Global Knowledge, the blended solutions training company. In that role, he has authored and managed two highly successful courses—Hands-on Internetworking with TCP/IP and Network Management Essentials. Both courses are offered world-wide in Classroom, Virtual Classroom, and Self-directed formats. In support of these and other courses, he actively participates in Global Knowledge's e-mentoring programs.

His is author of the books ***Hands-On TCP/IP*** and ***SNMP Network Management***.