# Introduction to TCP/IP Internet Protocol

*by Sophia*

WHAT'S COVERED

In this lesson, you will learn about TCP/IP. Because TCP/IP is central to working with the internet and intranets, it is essential for you to understand it in detail. You will begin by understanding the background of TCP/IP and how it came about. You will then move on to understanding the important technical goals defined by the original designers. After that, you will discover how TCP/IP compares to a theoretical model—the open systems interconnection (OSI) model.

Specifically, this lesson will cover the following:



# 1. Introduction to TCP/IP

**Transmission Control Protocol/Internet Protocol (TCP/IP)** is a standard for computer network communication, used for the internet and most other modern networks as well. TCP/IP was originally developed by the **Internet Engineering Task Force (IETF)**, which is a standards organization for the internet responsible for the technical standards that comprise the TCP/IP protocol suite. TCP/IP is a suite of protocols that operate at Layers 3, 4, and 7 of the OSI model.

TERMS TO KNOW

**Transmission Control Protocol/Internet Protocol (TCP/IP)**
An IETF standard for computer network communication on an internetwork.

**The Internet Engineering Task Force (IETF)**
A standards organization for the internet that is responsible for the technical standards that comprise the TCP/IP protocol suite.

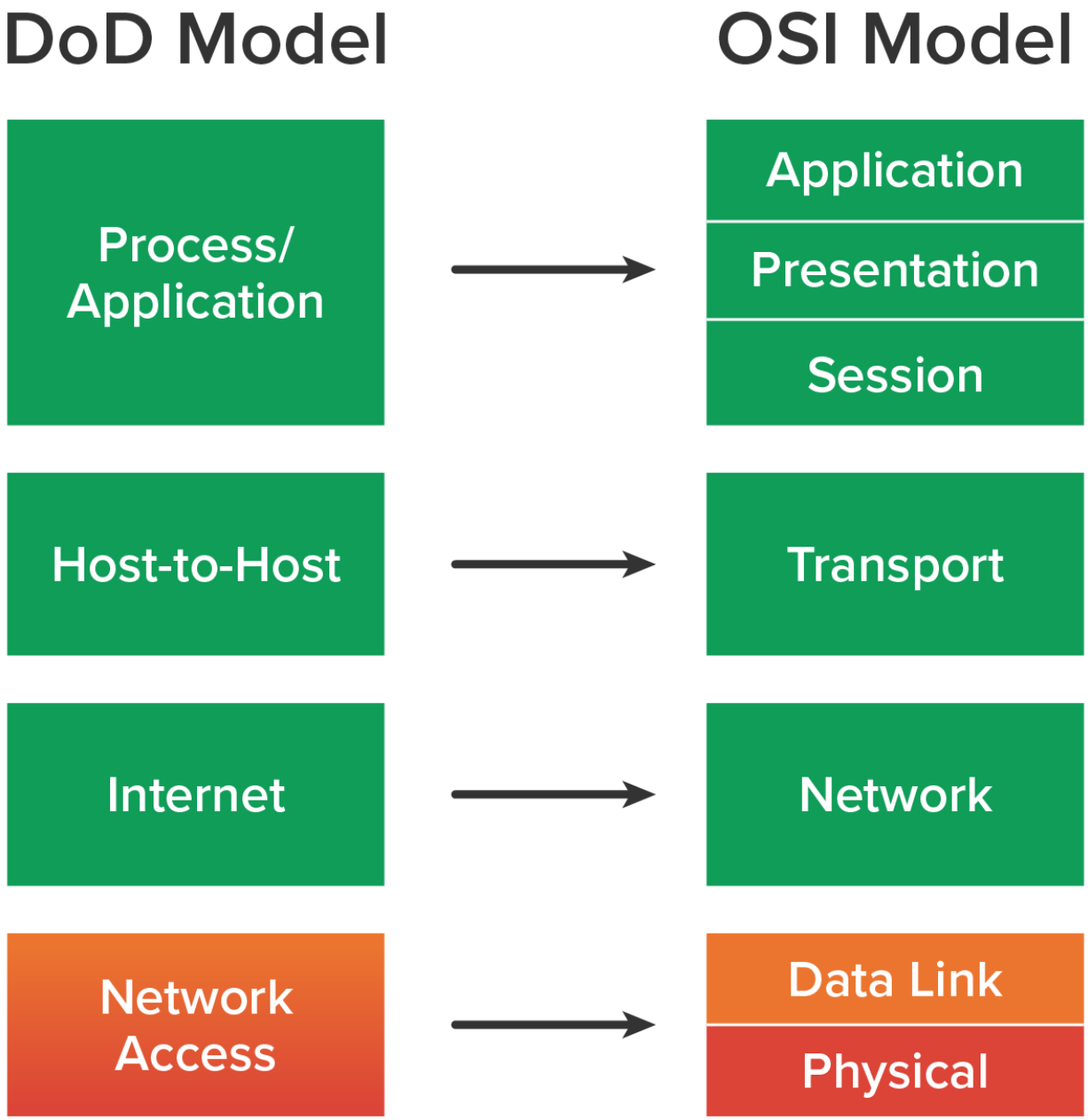
## 1a. TCP/IP and the DoD Model

TCP/IP maps to a U.S. Department of Defense (DoD) model that is similar to the OSI model. The DoD model is composed of four layers instead of seven:

- The process/application layer
- The host-to-host layer
- The internet layer
- The network access layer

KEY CONCEPT

The diagram below shows a comparison of the DoD model and the OSI reference model. The two are similar in concept, but each has a different number of layers with different names.



A vast array of protocols operate at the DoD model's process/application layer to integrate the various activities and duties that are the focus of the OSI's corresponding top three layers (application, presentation, and session). The process/application layer defines protocols for node-to-node application communication and also controls user interface specifications.

The host-to-host layer parallels the functions of the OSI's transport layer, defining protocols for setting up the level of transmission service for applications. It tackles issues such as creating reliable end-to-end communication and ensuring the error-free delivery of data. It handles packet sequencing and maintains data integrity.

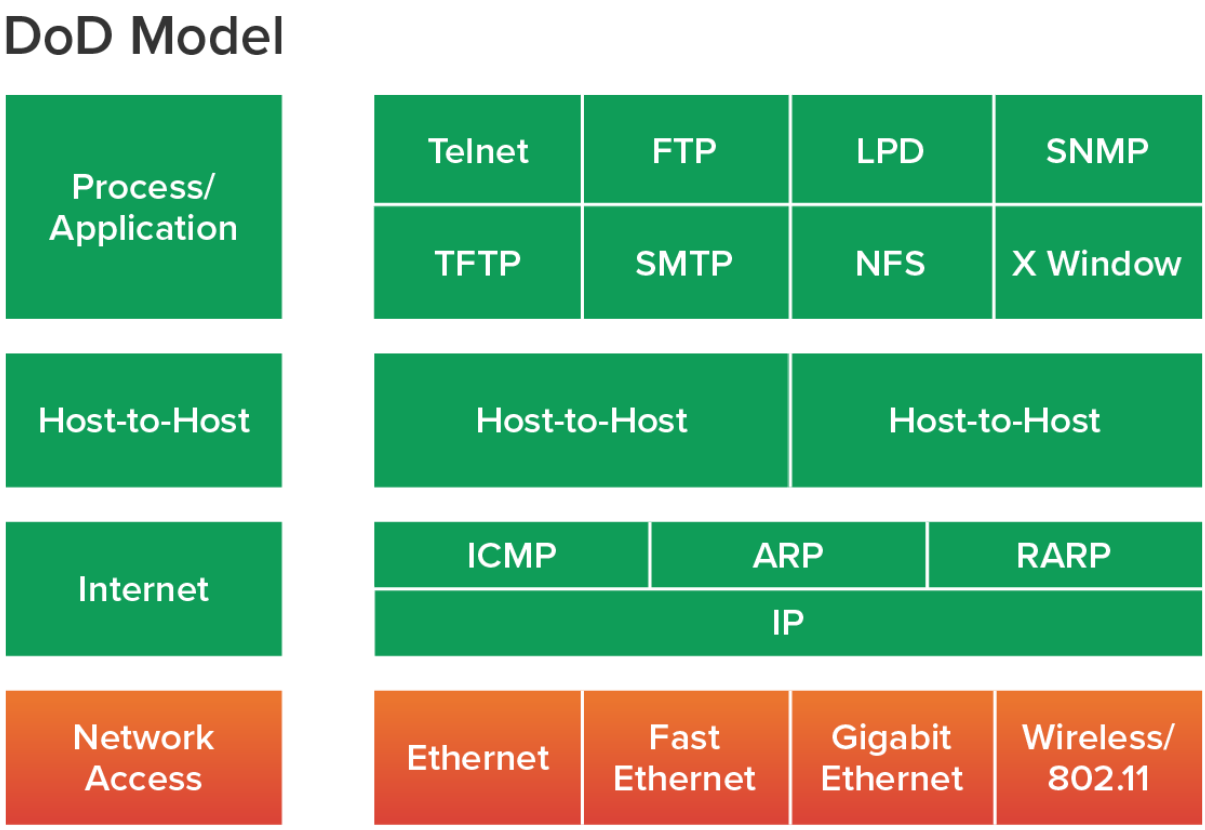
The internet layer corresponds to the OSI's network layer, which designates the protocols related to the logical transmission of packets over the entire network. It takes care of the logical addressing of hosts by giving them an IP address, and it handles the routing of packets among multiple networks.

At the bottom of the DoD model, the network access layer monitors the data exchange between the host and the network. The network access layer, the equivalent of the data link and physical layers of the OSI model, oversees hardware addressing and defines protocols for the physical transmission of data.

The DoD and OSI models are similar in design and concept and have similar functions in similar layers. The diagram below shows the TCP/IP protocol suite and how its protocols relate to the DoD model layers.

BIG IDEA

While the TCP/IP protocol suite maps directly to the four-layer DoD model, which is sometimes called the TCP/IP model, information technologists routinely refer to the seven layers of the OSI model to communicate their ideas about networking. So, when someone refers to Layer 3, for example, you can assume that they mean Layer 3 of the OSI model, not the third layer of the DoD model.




We will now look at various TCP/IP protocols in more detail, starting with the application layer protocols. You likely use many of these every day, while others are used primarily by information technologists who manage networks.

## 1b. The Process/Application Layer Protocols

In the following sections, we will describe the different applications and services typically used in IP networks and list their associated TCP or User Datagram Protocol (UDP) port numbers as well.

**Telnet (TCP 23)** supports terminal emulation. It allows a user on a remote client machine to access the resources of another machine, the Telnet server. Telnet enables the client machine to appear as though it were a terminal directly attached to the local network. Telnet offers no security or encryption and is a legacy protocol that has been replaced by Secure Shell (SSH).

**File Transfer Protocol (FTP), (TCP 20, 21)** is the protocol that lets you transfer files across an IP network, and it can accomplish this between any two machines that are using it. One common use of FTP is to use it to upload a revised website file to a web server.

HINT

The problem with FTP is that all data are sent in cleartext, just as with Telnet. If you need to make sure your FTP transfers are secure, then you will need to use SFTP.

**Secure File Transfer Protocol (TCP 22)**is used to transfer files over an encrypted connection. It uses an SSH session, which encrypts the connection; SSH uses port 22, hence the port number 22 for SFTP.

**Trivial File Transfer Protocol (TFTP), (UDP 69)** is a connectionless version of FTP that uses UDP instead of TCP at Layer 4, so there is no guarantee of delivery.

**Simple Mail Transfer Protocol (SMTP), (TCP 25)** enables the transfer of emails from email server to email server. It does not offer a server-to-client email service. SMTP carries, for example, email messages from a Gmail server to an Apple email server. Once delivered to either server, your login credentials for your server will allow you to access the message from the email client you use to access your email account.

**Post Office Protocol (POP), (TCP 110)**enables email transfer between an email server and an email client for client-side storage. When a client device connects to a POP3 server, messages addressed to that client are released for download.


It does not allow messages to be downloaded selectively, but once they are, the client–server interaction ends. A newer standard, IMAP, is typically used in place of POP3.

**Internet Message Access Protocol (IMAP), Version 4 (TCP 143)**enables email transfer between an email server and an email client for server-side storage. IMAP supports search commands used to look for messages based on their subject, header, or content. IMAP supports Kerberos authentication for security. IMAP is the protocol that your current email service uses to send messages to your computer.

**Remote Desktop Protocol (RDP), (TCP 3389)** is a protocol that allows you to connect to another computer and run programs. Clients exist for most versions of Windows, and Macs now come with a preinstalled RDP client.


RDP is an excellent tool for remote clients, allowing them to connect to their work computer from home, for example, and get their email or perform work on other applications without running or installing any of the software on their home computer.

Both **Transport Layer Security (TLS)** and its forerunner, Secure Sockets Layer (SSL), are cryptographic protocols for enabling secure online data transfer activities. Both use cryptography to authenticate the host they are communicating with and to exchange a key. This key is then used to encrypt data flowing between the hosts, which allows for data/message confidentiality, message integrity, and message authentication.

**Session Initiation Protocol (SIP)** is a signaling protocol used to enable multimedia communication sessions for many aspects like voice and video calls, videoconferencing, streaming multimedia distribution, instant messaging, presence information, and online games over the internet.


You likely use SIP when you use WhatsApp or Facetime to have a voice conversation.

**Real-Time Transport Protocol (RTP) (UDP 5004/TCP 5005)** describes a packet-formatting standard for delivering audio and video over the internet. It is commonly employed for streaming media, videoconferencing, and Voice over Internet Protocol (VoIP).

**Media Gateway Control Protocol (MGCP) (TCP 2427/2727)** is a standard protocol for handling the signaling and session management needed during a multimedia conference with multiple participants. The protocol defines a

means of communication between a media gateway, which converts data from the format required for a circuit-switched network to that required for a packet-switched network, and the media gateway controller.

**H.323 (TCP 1720)** is a protocol that provides a standard for video on an IP network that defines how real-time audio, video, and data information are transmitted. This standard provides signaling, multimedia, and bandwidth control mechanisms. H.323 uses the RTP standard for communication.

**Simple Network Management Protocol (SNMP), (UDP 161)** collects and manipulates valuable network information from network devices like routers and switches. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. The network uses agents, and when problems occur, the agents send an alert called a trap to the management station. SNMP enables the administration of a network.

**Secure Shell (SSH), (TCP 22)** protocol sets up a secure encrypted Telnet session over a standard TCP/IP connection and is used to securely log in to other systems, run programs on remote systems, and move files from one system to another.

**Hypertext Transfer Protocol (HTTP), (TCP 80)** is used to manage communications between web browsers and web servers, and it opens the right resource when you click a link, wherever that resource may reside. HTTP is the protocol that delivers webpages to your browser.

DID YOU KNOW

For many years, this was the dominant web protocol, but more and more sites are moving to the secure version, HTTPS.

**Hypertext Transfer Protocol Secure (HTTPS), (TCP 443)** is an encrypted version of HTTP that has security tools for keeping transactions between a web browser and a server secure. It is what your browser needs to fill out forms, sign in, authenticate, and encrypt an HTTP message when you make a reservation or buy something online.

**Network Time Protocol (NTP), (UDP 123)** works to ensure that all the computers on a given network are set to the same time. This is important because many of the transactions done today are time stamped and date stamped.

**Lightweight Directory Access Protocol (LDAP), (TCP 389)**enables access to computer directories. Its third version is most commonly used today and is described in RFC 3377.

**Internet Group Management Protocol (IGMP)** is the TCP/IP used for managing IP multicast sessions. IGMP messages support active multicast streams. IGMP works at the network layer and does not use port numbers.

**Network Basic Input/Output System (NetBIOS) and (UDP 137–139)** provides an interface for separate computers running Windows to communicate over a network.

**Server Message Block (SMB), (TCP 445)** is used for sharing access to files and printers and other communications between hosts on a Microsoft Windows network.

**Domain Name Service (DNS), (TCP and UDP 53)** resolves hostnames to their corresponding IP addresses. DNS allows you to use a domain name to specify an IP address.

HINT

When you type “www.google.com,” DNS is that protocol that tells your computer the IP address of Google’s web server.

BIG IDEA

Of all the TCP/IP application protocols listed above, the chances are high that you are using SMTP, IMAP, TLS/SSL, SIP, HTTP, HTTPS, DNS, and H.323 to engage in your routing online activities. All the other protocols discussed are generally used by information technologists to manage networks.

TERMS TO KNOW

**Telnet**
A Layer 7 protocol that supports terminal emulation.

**File Transfer Protocol (FTP)**
A Layer 7 protocol that enables the transfer of files across an IP network.

**Secure File Transfer Protocol (SFTP)**
A Layer 7 protocol that is used to transfer files over an encrypted connection.

**Trivial File Transfer Protocol (TFTP)**
A Layer 7 protocol that is a connectionless version of FTP that uses UDP instead of TCP at Layer 4.

**Simple Mail Transfer Protocol (SMTP)**
A Layer 7 protocol that enables the transfer of emails from email server to email server.

**Post Office Protocol (POP)**
A legacy Layer 7 protocol that enables email transfer between an email server and an email client for client-side storage.

**Internet Message Access Protocol (IMAP)**
A Layer 7 protocol that enables email transfer between an email server and an email client for server-side storage.

**Remote Desktop Protocol (RDP)**
A Layer 7 protocol that allows you to connect to another computer and run programs.

**Transport Layer Security (TLS)**
A Layer 7 protocol that is a cryptographic protocol for enabling secure online data transfer activities.

**Session Initiation Protocol (SIP)**
A Layer 7 protocol used to enable multimedia communication sessions.

**Real-Time Transport Protocol (RTP)**

A Layer 7 protocol that describes a packet-formatting standard for delivering audio and video over the internet.

**Media Gateway Control Protocol (MGCP)**

A Layer 7 protocol that is a standard protocol for handling the signaling and session management needed during a multimedia conference.

**H.323**

A Layer 3 protocol that provides a standard for video on an IP network that defines how real-time audio, video, and data information are transmitted.

**Simple Network Management Protocol (SNMP)**

A Layer 7 protocol that collects and manipulates valuable network information from network devices like routers and switches.

**Secure Shell (SSH)**

A Layer 7 protocol that sets up a secure encrypted Telnet session over a standard TCP/IP connection.

**Hypertext Transfer Protocol (HTTP)**

A Layer 7 protocol that is used to manage communications between web browsers and web servers.

**Hypertext Transfer Protocol Secure (HTTPS)**

A Layer 7 protocol that is an encrypted version of HTTP and has security tools for keeping transactions between a web browser and a server secure.

**Network Time Protocol (NTP)**

A Layer 7 protocol that ensures all the computers on a given network are set to the same time.

**Lightweight Directory Access Protocol (LDAP)**

A Layer 7 protocol that enables access to computer directories.

**Internet Group Management Protocol (IGMP)**

A Layer 7 protocol used for managing IP multicast sessions.

**Network Basic Input/Output System (NetBIOS)**

A legacy Layer 7 protocol that provides an interface for separate computers running Windows to communicate over a network..

**Server Message Block (SMB)**

A Layer 7 protocol that is used for sharing access to files and printers and other communications between hosts on a Microsoft Windows network.

**Domain Name Service (DNS)**

A Layer 7 protocol that resolves hostnames to their corresponding IP addresses.

## SUMMARY

In this lesson, you learned how **TCP/IP** maps to the OSI model and learned about a large set of TCP/IP

applications used to facilitate network communications and services.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

## TERMS TO KNOW

**Domain Name Service (DNS)**
A Layer 7 protocol that resolves hostnames to their corresponding IP addresses.

**File Transfer Protocol (FTP)**
A Layer 7 protocol that enables the transfer of files across an IP network.

**H.323**
A Layer 3 protocol that provides a standard for video on an IP network that defines how real-time audio, video, and data information are transmitted.

**Hypertext Transfer Protocol (HTTP)**
A Layer 7 protocol that is used to manage communications between web browsers and web servers.

**Hypertext Transfer Protocol Secure (HTTPS)**
A Layer 7 protocol that is an encrypted version of HTTP and has security tools for keeping transactions between a web browser and a server secure.

**Internet Group Management Protocol (IGMP)**
A Layer 7 protocol used for managing IP multicast sessions.

**Internet Message Access Protocol (IMAP)**
A Layer 7 protocol that enables email transfer between an email server and an email client for server-side storage.

**Lightweight Directory Access Protocol (LDAP)**
A Layer 7 protocol that enables access to computer directories.

**Media Gateway Control Protocol (MGCP)**
A Layer 7 protocol that is a standard protocol for handling the signaling and session management needed during a multimedia conference.

**Network Basic Input/Output System (NetBIOS)**
A legacy Layer 7 protocol that provides an interface for separate computers running Windows to communicate over a network.

**Network Time Protocol (NTP)**
A Layer 7 protocol that ensures all the computers on a given network are set to the same time.

**Post Office Protocol (POP)**

A legacy Layer 7 protocol that enables email transfer between an email server and an email client for client-side storage.

**Real-Time Transport Protocol (RTP)**

A Layer 7 protocol that describes a packet-formatting standard for delivering audio and video over the internet.

**Remote Desktop Protocol (RDP)**

A Layer 7 protocol that allows you to connect to another computer and run programs.

**Secure File Transfer Protocol (SFTP)**

A Layer 7 protocol that is used to transfer files over an encrypted connection.

**Secure Shell (SSH)**

A Layer 7 protocol that sets up a secure encrypted Telnet session over a standard TCP/IP connection.

**Server Message Block (SMB)**

A Layer 7 protocol that is used for sharing access to files and printers and other communications between hosts on a Microsoft Windows network.

**Session Initiation Protocol (SIP)**

A Layer 7 protocol used to enable multimedia communication sessions.

**Simple Mail Transfer Protocol (SMTP)**

A Layer 7 protocol that enables the transfer of emails from email server to email server.

**Simple Network Management Protocol (SNMP)**

A Layer 7 protocol that collects and manipulates valuable network information from network devices like routers and switches.

**Telnet**

A Layer 7 protocol that supports terminal emulation.

**The Internet Engineering Task Force (IETF)**

A standards organization for the internet that is responsible for the technical standards that comprise the TCP/IP protocol suite.

**Transmission Control Protocol/Internet Protocol (TCP/IP)**

An IETF standard for computer network communication on an internetwork.

**Transport Layer Security (TLS)**

A Layer 7 protocol that is a cryptographic protocol for enabling secure online data transfer activities.

**Trivial File Transfer Protocol (TFTP)**

A Layer 7 protocol that is a connectionless version of FTP that uses UDP instead of TCP at Layer 4.