Learn more about the TCP/IP model

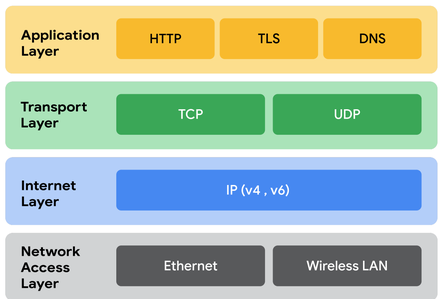
In this reading, you will build on what you have learned about the Transmission Control Protocol/Internet Protocol (TCP/IP) model, consider the differences between the Open Systems Interconnection (OSI) model and TCP/IP model, and learn how they're related. Then, you'll review each layer of the TCP/IP model and go over common protocols used in each layer.

As a security professional, it's important that you understand the TCP/IP model because all communication on a network is organized using network protocols. Network protocols are a language that systems use to communicate with each other. In order for two network systems to successfully communicate with each other, they need to use the same protocol. The two most common models available are the TCP/IP and the OSI model. These models are a representative guideline of how network communications work together and move throughout the network and the host. The examples provided in this course will follow the TCP/IP model.

The TCP/IP model

The **TCP/IP model** is a framework used to visualize how data is organized and transmitted across a network. This model helps network engineers and network security analysts conceptualize processes on the network and communicate where disruptions or security threats occur.

The TCP/IP model has four layers: network access layer, internet layer, transport layer, and application layer. When troubleshooting issues on the network, security professionals can analyze and deduce which layer or layers an attack occurred based on what processes were involved in an incident.



Network access layer

The **network access layer**, sometimes called the data link layer, organizes sending and receiving data frames within a single network. This layer corresponds to the physical hardware involved in network transmission. Hubs, modems, cables, and wiring are all considered part of this layer. The address resolution protocol (ARP) is part of the network access layer. ARP assists IP with directing data packets on the same physical network by mapping IP addresses to MAC addresses on the same physical network.

Internet layer

The **internet layer**, sometimes referred to as the network layer, is responsible for ensuring the delivery to the destination host, which potentially resides on a different network. The internet layer determines which protocol is responsible for delivering the data packets. Here are some of the common protocols that operate at the internet layer:

- **Internet Protocol (IP)**. IP sends the data packets to the correct destination and relies on Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to deliver them to corresponding service. IP packets allow communication between two networks. They are routed from the sending network to the receiving network. It retransmits any data that is lost or corrupt.

- **Internet Control Message Protocol (ICMP)**. ICMP shares error information and status updates of data packets. This is useful for detecting and troubleshooting network errors. ICMP reports information about packets that were dropped or disappeared in transit, issues with network connectivity, and packets redirected to other routers.

Transport layer

The **transport layer** is responsible for reliably delivering data between two systems or networks. TCP and UDP are the two transport protocols that occur at this layer.

Transmission Control Protocol

TCP ensures that data is reliably transmitted to the destination service. TCP contains the port number of the intended destination service, which resides in the TCP header of an TCP/IP packet.

User Datagram Protocol

UDP is used by applications that are not concerned with reliability of the transmission. Data sent over UDP is not tracked as extensively as data sent using TCP. Because UDP does not establish network connections, it is used mostly for performance sensitive applications that operate in real time, such as video streaming.

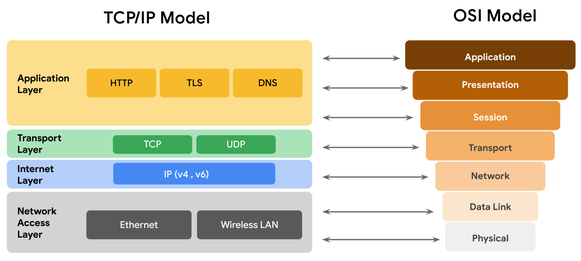
Application layer

The **application layer** in the TCP/IP model is similar to the application, presentation, and session layers of the OSI model. The application layer is responsible for making network requests or responding to requests. This layer defines which internet services and applications any user can access. Some common protocols used on this layer are:

- Hypertext transfer protocol (HTTP)
- Simple mail transfer protocol (SMTP)
- Secure shell (SSH)
- File transfer protocol (FTP)
- Domain name system (DNS)

Application layer protocols rely on underlying layers to transfer the data across the network.

TCP/IP model versus OSI model



The **OSI** visually organizes network protocols into different layers. Network professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.

The TCP/IP model combines multiple layers of the OSI model. There are many similarities between the two models. Both models define standards for networking and divide the network communication process into different layers. The TCP/IP model is a simplified version of the OSI model.

Key takeaways

Both the TCP/IP and OSI models are conceptual models that help network professionals visualize network processes and protocols in regards to data transmission between two or more systems. The TCP/IP model contains four layers, and the OSI model contains seven layers.

Mark as completed

Like **Dislike** **Report an issue**