Coursera : Connect & Protect : Networks and Network Security

Network components, devices, and diagrams

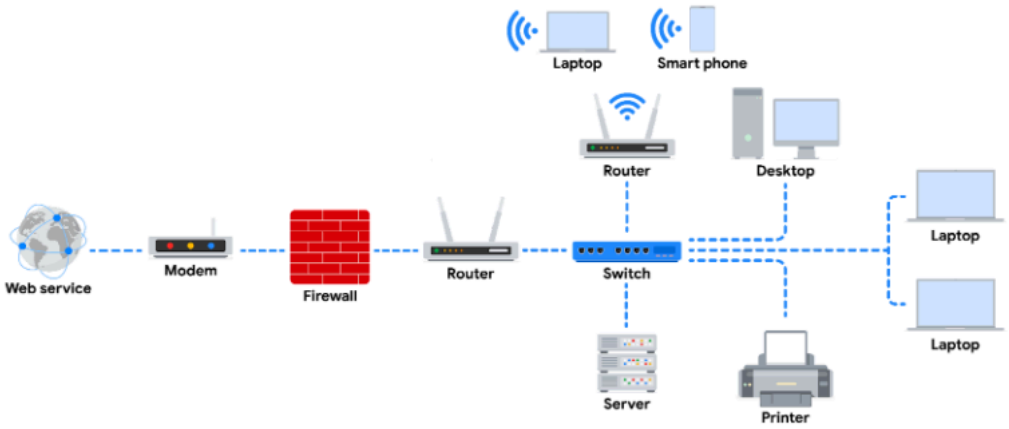
In this reading, you will review network devices and connections and investigate a simple network diagram similar to those used every day by network security professionals.

A foundational understanding of network architecture, sometimes referred to as network design, will help you as you learn about security vulnerabilities inherent in all networks and how malicious actors attempt to exploit them. Let’s get started!

Network devices

Network devices maintain information and services for users of a network. These devices connect over wired and wireless connections. After establishing a connection to the network, the devices send data packets. The data packets provide information about the source and the destination of the data. This is how the information is sent and received via different devices on a network.

The network is the overall infrastructure that allows devices to communicate with each other. Network devices are specialized vehicles like routers and switches that manage what is being sent and received over the network. Additionally, devices like computers and phones connect to the network via network devices.



Note: In this diagram, a router connects to the internet through a modem, which is provided by your internet service provider (ISP). The firewall is a security device that monitors incoming and outgoing traffic on your network. The router then directs traffic to the devices on your home network, which can include computers, laptops, smartphones, tablets, printers, and other devices. You can imagine here that the server is a file server. All devices on this network can access the files in this server. This diagram also includes a switch which is an optional device that can be used to connect more devices to your network by providing additional ports and Ethernet connections. Additionally, there are 2 routers connected to the switch here for load balancing purposes which will improve the performance of the network.

Devices and desktop computers

Most internet users are familiar with everyday devices, such as personal computers, laptops, mobile phones, and tablets. Each device and desktop computer has a unique MAC address and IP address, which identify it on the network. They also have a network interface that sends and receives data packets. These devices can connect to the network via a hard wire or a wireless connection.

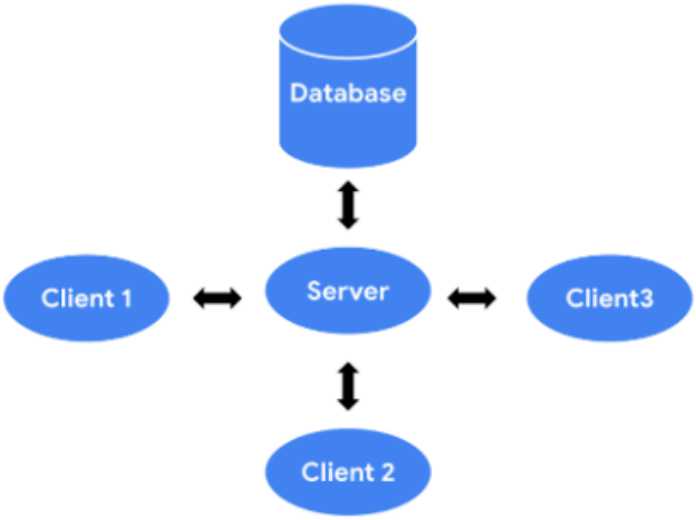
Firewalls

A firewall is a network security device that monitors traffic to or from your network. It is like your first line of defense. Firewalls can also restrict specific incoming and outgoing

network traffic. The organization configures the security rules of the firewall. Firewalls often reside between the secured and controlled internal network and the untrusted network resources outside the organization, such as the internet. Remember, though, firewalls are just one line of defense in the cybersecurity landscape.

Servers

Servers provide information and services for devices like computers, smart home devices, and smartphones on the network. The devices that connect to a server are called clients. The following graphic outlines this model, which is called the client-server model. In this model, clients send requests to the server for information and services. The server performs the requests for the clients. Common examples include DNS servers that perform domain name lookups for internet sites, file servers that store and retrieve files from a database, and corporate mail servers that organize mail for a company.



Hubs and switches

Hubs and switches both direct traffic on a local network. A hub is a device that provides a common point of connection for all devices directly connected to it. Hubs additionally repeat all information out to all ports. From a security perspective, this makes hubs vulnerable to eavesdropping. For this reason, hubs are not used as often on modern

networks; most organizations use switches instead. Hubs are more commonly used for a limited network setup like a home office.

Switches are the preferred choice for most networks. A switch forwards packets between devices directly connected to it. They analyze the destination address of each data packet and send it to the intended device. Switches maintain a MAC address table that matches MAC addresses of devices on the network to port numbers on the switch and forwards incoming data packets according to the destination MAC address. Switches are a part of the data link layer in the TCP/IP model. Overall, switches improve performance and security.

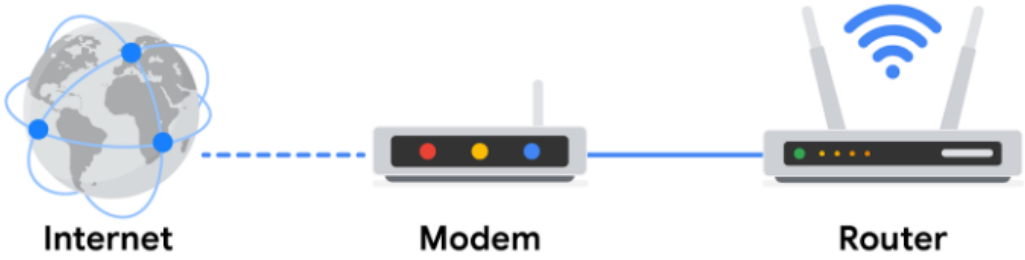
Routers

Routers connect networks and direct traffic, based on the IP address of the destination network. Routers allow devices on different networks to communicate with each other. In the TCP/IP model, routers are a part of the network layer. The IP address of the destination network is contained in the IP header. The router reads the IP header information and forwards the packet to the next router on the path to the destination. This continues until the packet reaches the destination network. Routers can also include a firewall feature that allows or blocks incoming traffic based on information in the transmission. This stops malicious traffic from entering the private network and damaging the local area network.

Modems and wireless access points

Modems usually connect your home or office with an internet service provider (ISP). ISPs provide internet connectivity via telephone lines, coaxial cables, or fiber optic cables. Modems receive transmissions or digital signals from the internet and convert them into a digital format compatible with the physical connection provided by your ISP. Usually, modems connect to a router that takes the decoded transmissions and sends them on to the local network.

Note: Enterprise networks used by large organizations to connect their users and devices often use other broadband technologies to handle high-volume traffic, instead of using a modem.



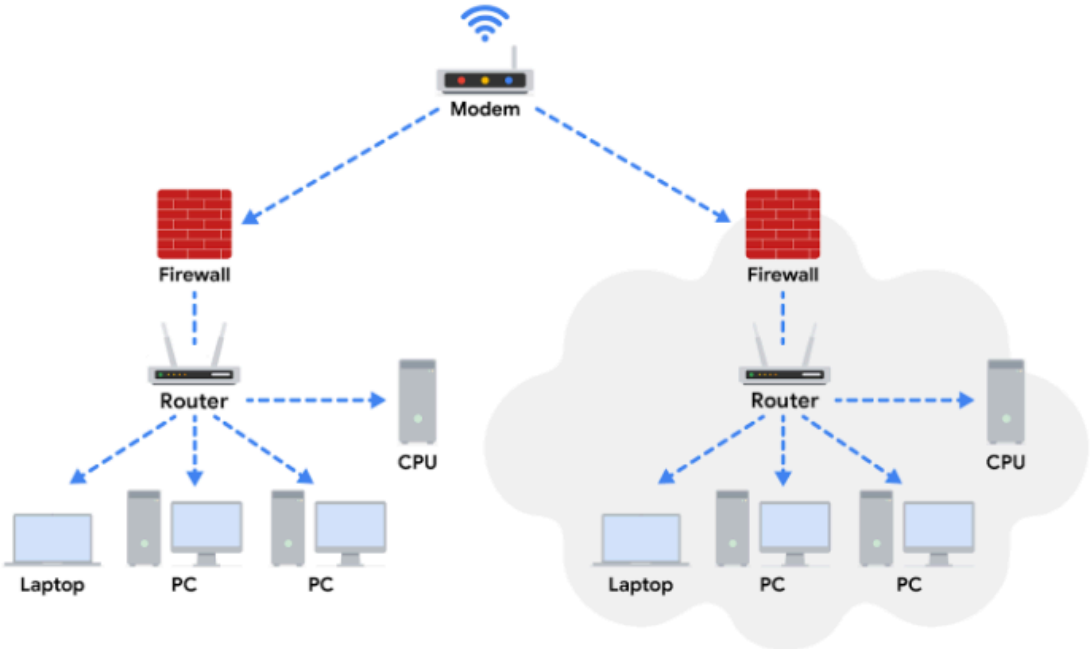
Wireless access point

A wireless access point sends and receives digital signals over radio waves creating a wireless network. Devices with wireless adapters connect to the access point using Wi-Fi. Wi-Fi refers to a set of standards that are used by network devices to communicate wirelessly. Wireless access points and the devices connected to them use Wi-Fi protocols to send data through radio waves where they are sent to routers and switches and directed along the path to their final destination.

Using network diagrams as a security analyst

Network diagrams allow network administrators and security personnel to imagine the architecture and design of their organization’s private network.

Network diagrams are maps that show the devices on the network and how they connect. Network diagrams use small representative graphics to portray each network device and dotted lines to show how each device connects to the other. By studying network diagrams, security analysts develop and refine their strategies for securing network architectures.



Key takeaways

In the client-server model, the client requests information and services from the server, and the server performs the requests for the clients. Network devices include routers, workstations, servers, hubs, switches, and modems. Security analysts use network diagrams to visualize network architecture.

Cloud computing and software-defined networks

In this section of the course, you've been learning the basic architecture of networks. You've learned about how physical network devices like workstations, servers, routers, and switches connect to each other to create a network. Networks may cover small geographical areas, as is the case in a local area network (LAN). Or they may span a large geographic area, like a city, state, or country, as is the case in a wide area network (WAN). You also learned about cloud networks and how cloud computing has grown in recent years.

In this reading, you will further examine the concepts of cloud computing and cloud networking. You'll also learn about hybrid networks and software-defined networks, as well as the benefits they offer. This reading will also cover the benefits of hosting networks in the cloud and why cloud-hosting is beneficial for large organizations.

Computing processes in the cloud

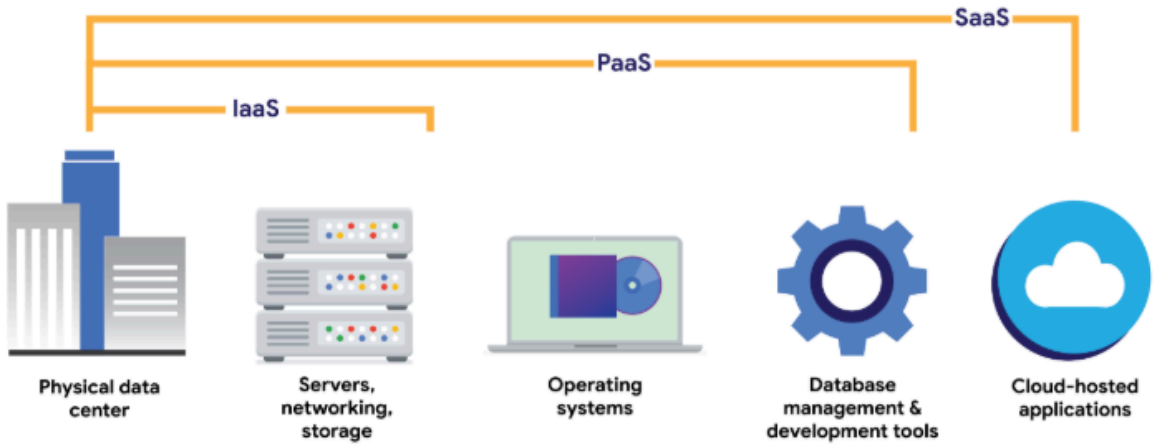
Traditional networks are called on-premise networks, which means that all of the devices used for network operations are kept at a physical location owned by the company, like in an office building, for example. Cloud computing, however, refers to the practice of using remote servers, applications, and network services that are hosted on the internet instead of at a physical location owned by the company.

A cloud service provider (CSP) is a company that offers cloud computing services. These companies own large data centers in locations around the globe that house millions of servers. Data centers provide technology services, such as storage, and

compute at such a large scale that they can sell their services to other companies for a fee. Companies can pay for the storage and services they need and consume them through the CSP's application programming interface (API) or web console.

CSPs provide three main categories of services:

- Software as a service (SaaS) refers to software suites operated by the CSP that a company can use remotely without hosting the software.
- Infrastructure as a service (IaaS) refers to the use of virtual computer components offered by the CSP. These include virtual containers and storage that are configured remotely through the CSP's API or web console. Cloud-compute and storage services can be used to operate existing applications and other technology workloads without significant modifications. Existing applications can be modified to take advantage of the availability, performance, and security features that are unique to cloud provider services.
- Platform as a service (PaaS) refers to tools that application developers can use to design custom applications for their company. Custom applications are designed and accessed in the cloud and used for a company's specific business needs.



Hybrid cloud environments

When organizations use a CSP's services in addition to their on-premise computers, networks, and storage, it is referred to as a hybrid cloud environment. When organizations use more than one CSP, it is called a multi-cloud environment. The vast majority of organizations use hybrid cloud environments to reduce costs and maintain control over network resources.

Software-defined networks

CSPs offer networking tools similar to the physical devices that you have learned about in this section of the course. Next, you'll review software-defined networking in the cloud. Software-defined networks (SDNs) are made up of virtual network devices and services. Just like CSPs provide virtual computers, many SDNs also provide virtual switches, routers, firewalls, and more. Most modern network hardware devices also support network virtualization and software-defined networking. This means that physical switches and routers use software to perform packet routing. In the case of cloud networking, the SDN tools are hosted on servers located at the CSP's data center.

Benefits of cloud computing and software-defined networks

Three of the main reasons that cloud computing is so attractive to businesses are reliability, decreased cost, and increased scalability.

Reliability

Reliability in cloud computing is based on how available cloud services and resources are, how secure connections are, and how often the services are effectively running. Cloud computing allows employees and customers to access the resources they need consistently and with minimal interruption.

Cost

Traditionally, companies have had to provide their own network infrastructure, at least for internet connections. This meant there could be potentially significant upfront costs for companies. However, because CSPs have such large data centers, they are able to offer virtual devices and services at a fraction of the cost required for companies to install, patch, upgrade, and manage the components and software themselves.

Scalability

Another challenge that companies face with traditional computing is scalability. When organizations experience an increase in their business needs, they might be forced to buy more equipment and software to keep up. But what if business decreases shortly after? They might no longer have the business to justify the cost incurred by the upgraded components. CSPs reduce this risk by making it easy to consume services in an elastic utility model as needed. This means that companies only pay for what they need when they need it.

Changes can be made quickly through the CSPs, APIs, or web console—much more quickly than if network technicians had to purchase their own hardware and set it up. For example, if a company needs to protect against a threat to their network, web application firewalls (WAFs), intrusion detection/protection systems (IDS/IPS), or L3/L4 firewalls can be configured quickly whenever necessary, leading to better network performance and security.

Key takeaways

In this reading, you learned more about cloud computing and cloud networking. You learned that CSPs are companies that own large data centers that house millions of servers in locations all over the globe and then provide modern technology services, including compute, storage, and networking, through the internet. SDNs are an approach to network management. SDNs enable dynamic, programmatically efficient network configurations to improve network performance and monitoring. This makes it more like cloud computing than traditional network management. Organizations can

improve reliability, save costs, and scale quickly by using CSPs to provide networking services instead of building and maintaining their own network infrastructure.

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.

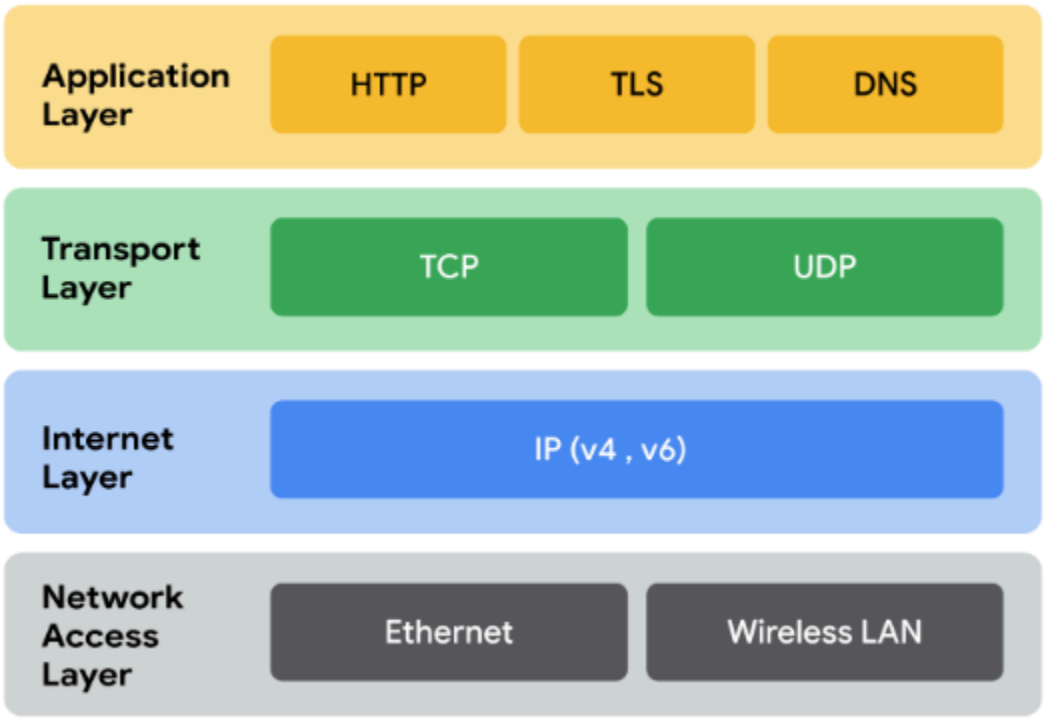
As a security professional, it's important that you understand the TCP/IP model because it describes the functions of various network protocols. The TCP/IP model is based on the TCP/IP protocols suite that includes all network protocols that support the main TCP/IP protocol. To reiterate from previous lessons, a network protocol, also known as an internet protocol, is a set of standards used for routing and addressing data packets as they travel between devices on a network. In this reading, you will learn which network protocols operate on which communication layers of the TCP/IP model. The two most common models available are the TCP/IP and the OSI model. These models are a representative guideline of how hosts communicate across a network. 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: the network access layer, internet layer, transport layer, and application layer. When troubleshooting issues on the network, security professionals can analyze which layers were impacted by an attack based on what processes were involved in an incident.



Network access layer

The network access layer, sometimes called the data link layer, deals with the creation of data packets and their transmission across a 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. Since MAC addresses are used to identify hosts on the same

physical network, ARP is needed to map IP addresses to MAC addresses for local network communication.

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. It ensures IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also determines which protocol is responsible for delivering the data packets and ensures the delivery to the destination host. 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 the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to deliver them to the corresponding service. IP packets allow communication between two networks. They are routed from the sending network to the receiving network. TCP in particular retransmits any data that is lost or corrupt.
- Internet Control Message Protocol (ICMP). The ICMP shares error information and status updates of data packets. This is useful for detecting and troubleshooting network errors. The ICMP reports information about packets that were dropped or that disappeared in transit, issues with network connectivity, and packets redirected to other routers.

Transport layer

The transport layer is responsible for delivering data between two systems or networks and includes protocols to control the flow of traffic across a network. TCP and UDP are the two transport protocols that occur at this layer.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is an internet communication protocol that allows two devices to form a connection and stream data. It 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 a TCP/IP packet.

User Datagram Protocol

The User Datagram Protocol (UDP) is a connectionless protocol that does not establish a connection between devices before transmissions. It is used by applications that are not concerned with the 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.

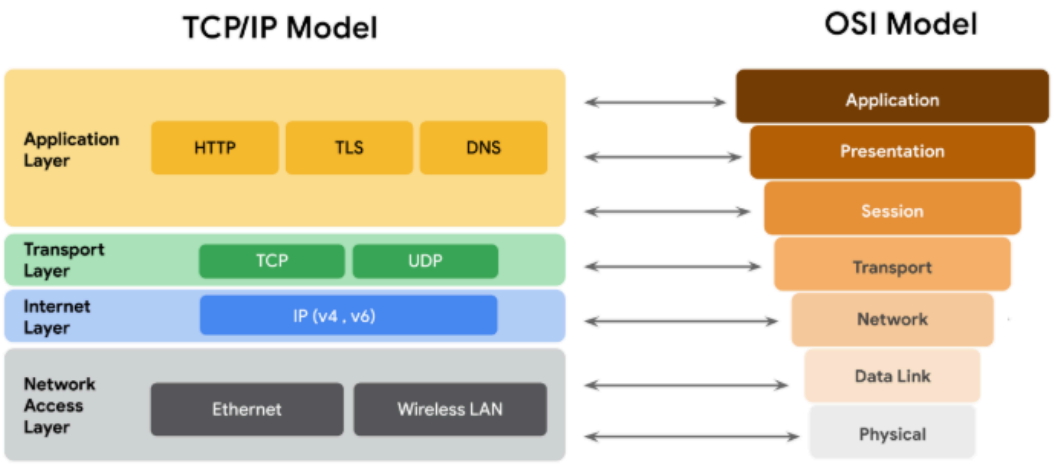
Application layer

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. Protocols in the application layer determine how the data packets will interact with receiving devices. 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.

The OSI model

So far in this section of the course, you learned about the components of a network, network devices, and how communication occurs across a network. You also studied the TCP/IP model to understand how network communication is organized across different layers of the internet.

All communication on a network is organized using network protocols. Previously, you learned about the Transmission Control Protocol (TCP), which establishes connections between two devices, and the Internet Protocol (IP), which is used for routing and addressing data packets as they travel between devices on a network. These protocols are used on specific internet layers in the TCP/IP model. The 4-layer TCP/IP model is a condensed form of the OSI (open Systems Interconnection) model, which is made up of 7 layers. The OSI model will provide a more in depth understanding of the processes that occur at each layer. We will work backwards from layer seven to layer one, going from the processes that involve direct user interaction with the network to those that involve the physical connection to the internet via network components like cables and switches. This reading will also review the main differences between the TCP/IP and OSI models.

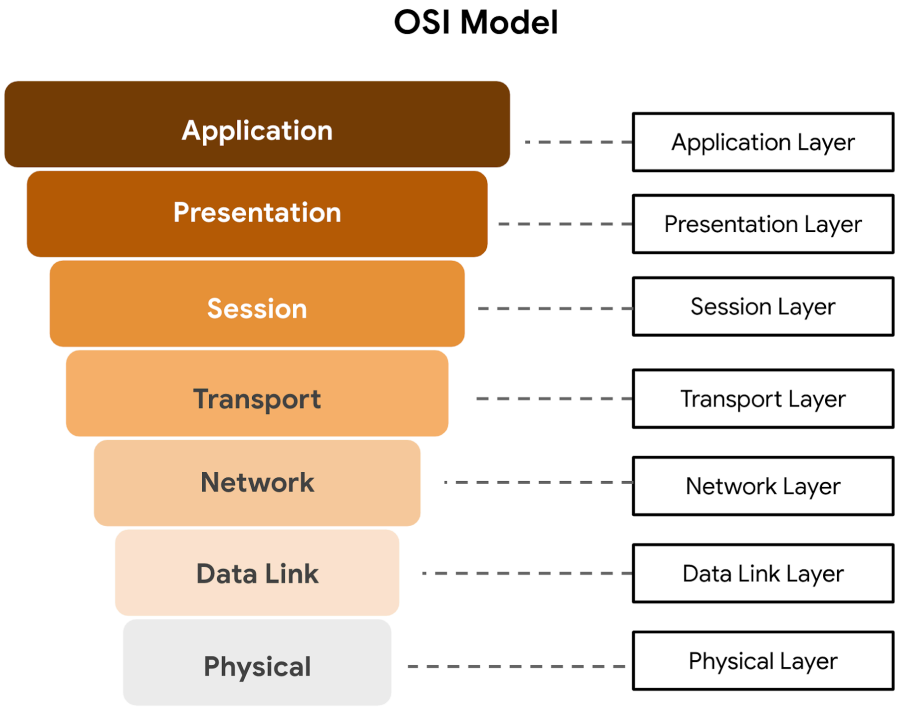
The TCP/IP model vs. the OSI model

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 security analysts conceptualize processes on the network and communicate where disruptions or security threats occur.

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

The OSI model is a standardized concept that describes the seven layers computers use to communicate and send data over the network. Network and security

professionals often use this model to communicate with each other about potential sources of problems or security threats when they occur.



Some organizations rely heavily on the TCP/IP model, while others prefer to use the OSI model. As a security analyst, it's important to be familiar with both models. Both the TCP/IP and OSI models are useful for understanding how networks work.

Layer 7: Application layer

The application layer includes processes that directly involve the everyday user. This layer includes all of the networking protocols that software applications use to connect a user to the internet. This characteristic is the identifying feature of the application layer—user connection to the internet via applications and requests.

An example of a type of communication that happens at the application layer is using a web browser. The internet browser uses HTTP or HTTPS to send and receive information from the website server. The email application uses simple mail transfer protocol (SMTP) to send and receive email information. Also, web browsers use the

domain name system (DNS) protocol to translate website domain names into IP addresses which identify the web server that hosts the information for the website.

Layer 6: Presentation layer

Functions at the presentation layer involve data translation and encryption for the network. This layer adds to and replaces data with formats that can be understood by applications (layer 7) on both sending and receiving systems. Formats at the user end may be different from those of the receiving system. Processes at the presentation layer require the use of a standardized format.

Some formatting functions that occur at layer 6 include encryption, compression, and confirmation that the character code set can be interpreted on the receiving system. One example of encryption that takes place at this layer is SSL, which encrypts data between web servers and browsers as part of websites with HTTPS.

Layer 5: Session layer

A session describes when a connection is established between two devices. An open session allows the devices to communicate with each other. Session layer protocols keep the session open while data is being transferred and terminate the session once the transmission is complete.

The session layer is also responsible for activities such as authentication, reconnection, and setting checkpoints during a data transfer. If a session is interrupted, checkpoints ensure that the transmission picks up at the last session checkpoint when the connection resumes. Sessions include a request and response between applications. Functions in the session layer respond to requests for service from processes in the presentation layer (layer 6) and send requests for services to the transport layer (layer 4).

Layer 4: Transport layer

The transport layer is responsible for delivering data between devices. This layer also handles the speed of data transfer, flow of the transfer, and breaking data down into smaller segments to make them easier to transport. Segmentation is the process of dividing up a large data transmission into smaller pieces that can be processed by the receiving system. These segments need to be reassembled at their destination so they can be processed at the session layer (layer 5). The speed and rate of the transmission also has to match the connection speed of the destination system. TCP and UDP are transport layer protocols.

Layer 3: Network layer

The network layer oversees receiving the frames from the data link layer (layer 2) and delivers them to the intended destination. The intended destination can be found based on the address that resides in the frame of the data packets. Data packets allow communication between two networks. These packets include IP addresses that tell routers where to send them. They are routed from the sending network to the receiving network.

Layer 2: Data link layer

The data link layer organizes sending and receiving data packets within a single network. The data link layer is home to switches on the local network and network interface cards on local devices.

Protocols like network control protocol (NCP), high-level data link control (HDLC), and synchronous data link control protocol (SDLC) are used at the data link layer.

Layer 1: Physical layer

As the name suggests, the physical layer corresponds to the physical hardware involved in network transmission. Hubs, modems, and the cables and wiring that connect them are all considered part of the physical layer. To travel across an ethernet

or coaxial cable, a data packet needs to be translated into a stream of 0s and 1s. The stream of 0s and 1s are sent across the physical wiring and cables, received, and then passed on to higher levels of the OSI model.

Key takeaways

Both the TCP/IP and OSI models are conceptual models that help network professionals design network processes and protocols with regards to data transmission between two or more systems. The OSI model contains seven communication layers. Network and security professionals use the OSI model to communicate with each other about potential sources of problems or security threats when they occur. Network engineers and network security analysts use the TCP/IP and OSI models to conceptualize network processes and communicate the location of disruptions or threats.

Components of network layer communication

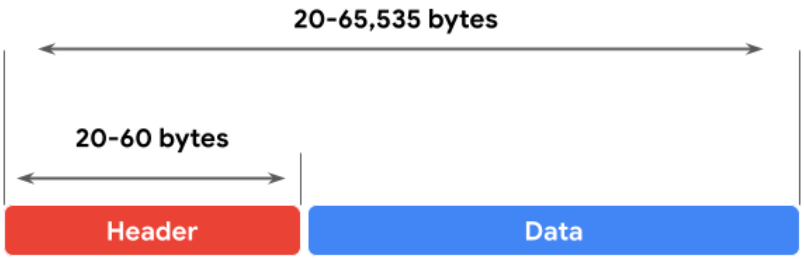
In the reading about the OSI model, you learned about the seven layers of the OSI model that are used to conceptualize the way data is transmitted across the internet. In this reading, you will learn more about operations that take place at layer 3 of the OSI model: the network layer.

Operations at the network layer

Functions at the network layer organize the addressing and delivery of data packets across the network from the host device to the destination device. This includes directing the packets from one router to another router across the internet, till it reaches the internet protocol (IP) address of the destination network. The destination IP address is contained within the header of each data packet. This address will be stored for future routing purposes in routing tables along the packet's path to its destination.

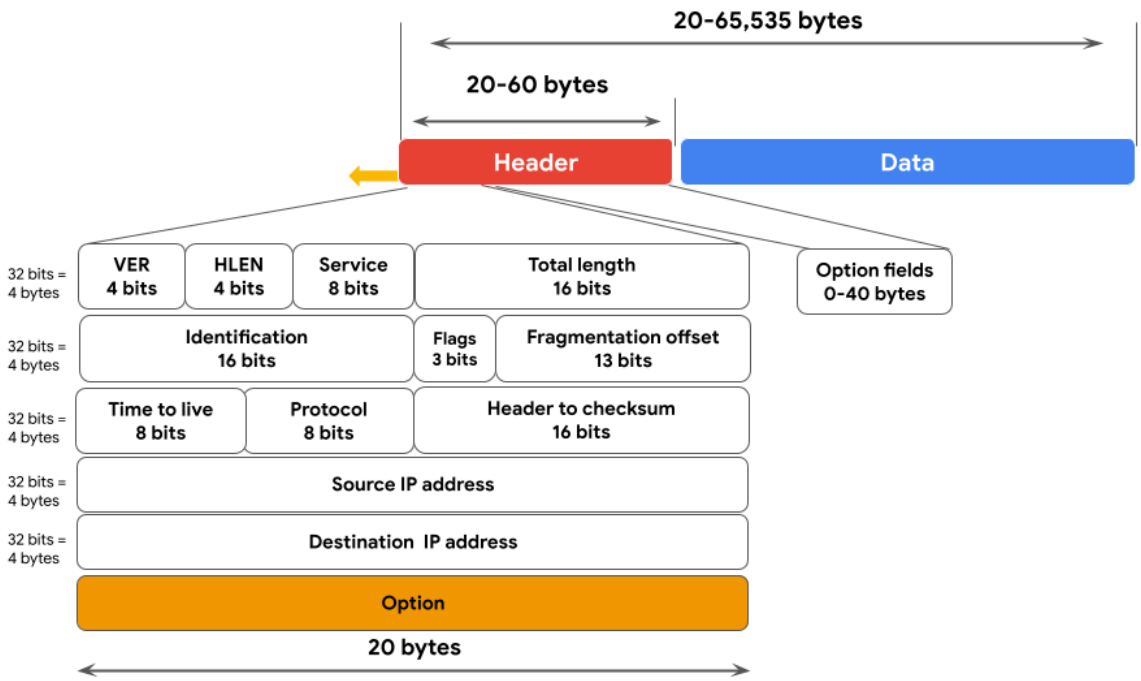
All data packets include an IP address. A data packet is also referred to as an IP packet for TCP connections or a datagram for UDP connections. A router uses the IP address to route packets from network to network based on information contained in the IP header of a data packet. Header information communicates more than just the address of the destination. It also includes information such as the source IP address, the size of the packet, and which protocol will be used for the data portion of the packet.

Format of an IPv4 packet



Next, you can review the format of an IP version 4 (IPv4) packet and review a detailed graphic of the packet header. An IPv4 packet is made up of two sections, the header and the data:

- An IPv4 header format is determined by the IPv4 protocol and includes the IP routing information that devices use to direct the packet. The size of the IPv4 header ranges from 20 to 60 bytes. The first 20 bytes are a fixed set of information containing data such as the source and destination IP address, header length, and total length of the packet. The last set of bytes can range from 0 to 40 and consists of the options field.
- The length of the data section of an IPv4 packet can vary greatly in size. However, the maximum possible size of an IPv4 packet is 65,535 bytes. It contains the message being transferred over the internet, like website information or email text.



There are 13 fields within the header of an IPv4 packet:

- Version (VER): This 4 bit component tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet.
- IP Header Length (HLEN or IHL): HLEN is the packet's header length. This value indicates where the packet header ends and the data segment begins.
- Type of Service (ToS): Routers prioritize packets for delivery to maintain quality of service on the network. The ToS field provides the router with this information.
- Total Length: This field communicates the total length of the entire IP packet, including the header and data. The maximum size of an IPv4 packet is 65,535 bytes.
- Identification: IPv4 packets can be up to 65, 535 bytes, but most networks have a smaller limit. In these cases, the packets are divided, or fragmented, into smaller IP packets. The identification field provides a unique identifier for all the fragments of the original IP packet so that they can be reassembled once they reach their destination.
- Flags: This field provides the routing device with more information about whether the original packet has been fragmented and if there are more fragments in transit.
- Fragmentation Offset: The fragment offset field tells routing devices where in the original packet the fragment belongs.
- Time to Live (TTL): TTL prevents data packets from being forwarded by routers indefinitely. It contains a counter that is set by the source. The counter is decremented by one as it passes through each router along its path. When the TTL counter reaches zero, the router currently holding the packet will discard the packet and return an ICMP Time Exceeded error message to the sender.
- Protocol: The protocol field tells the receiving device which protocol will be used for the data portion of the packet.
- Header Checksum: The header checksum field contains a checksum that can be used to detect corruption of the IP header in transit. Corrupted packets are discarded.
- Source IP Address: The source IP address is the IPv4 address of the sending device.

- Destination IP Address: The destination IP address is the IPv4 address of the destination device.
- Options: The options field allows for security options to be applied to the packet if the HLEN value is greater than five. The field communicates these options to the routing devices.

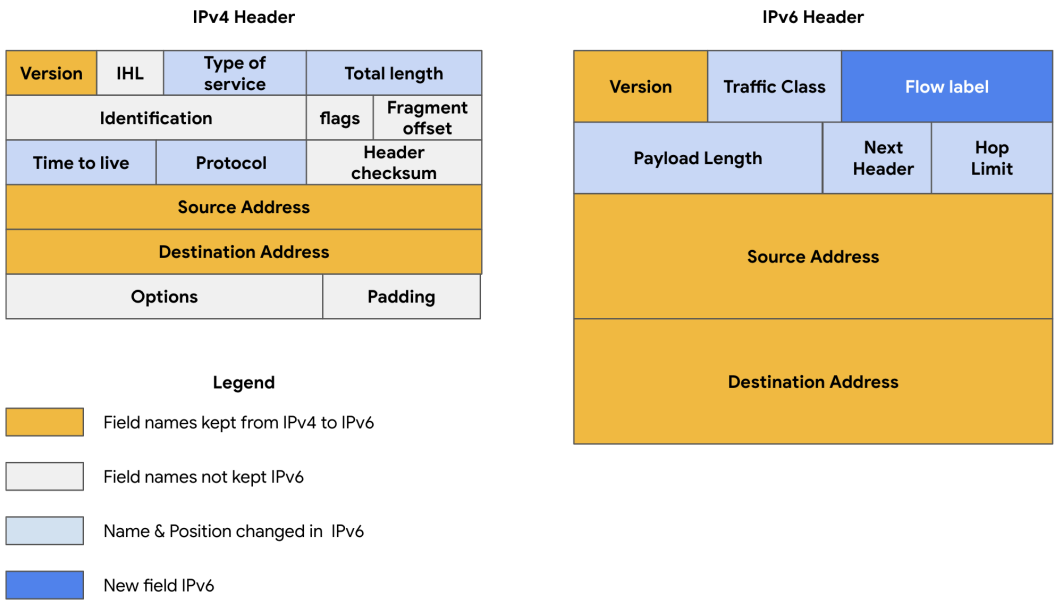
Difference between IPv4 and IPv6

In an earlier part of this course, you learned about the history of IP addressing. As the internet grew, it became clear that all of the IPv4 addresses would eventually be depleted; this is called IPv4 address exhaustion. At the time, no one had anticipated how many computing devices would need an IP address. IPv6 was developed to mitigate IPv4 address exhaustion and other related concerns.

Some of the key differences between IPv4 and IPv6 include the length and the format of the addresses. IPv4 addresses are made up of four decimal numbers separated by periods, each number ranging from 0 to 255. Together the numbers span 4 bytes, and allow for up to 4.3 billion possible addresses. An example of an IPv4 address would be: 198.51.100.0. IPv6 addresses are made of eight hexadecimal numbers separated by colons, each number consisting of up to four hexadecimal digits. Together, all numbers span 16 bytes, and allow for up to 340 undecillion addresses (340 followed by 36 zeros). An example of an IPv6 address would be: 2002:0db8:0000:0000:0000:ff21:0023:1234.

*Note: to represent one or more consecutive sets of all zeros, you can replace the zeros with a double colon "::", so the above IPv6 address would be "*2002:0db8::ff21:0023:1234."

There are also some differences in the layout of an IPv6 packet header. The IPv6 header format is much simpler than IPv4. For example, the IPv4 Header includes the IHL, Identification, and Flags fields, whereas the IPv6 does not. The IPv6 header only introduces the Flow Label field, where the Flow Label identifies a packet as requiring special handling by other IPv6 routers.



There are some important security differences between IPv4 and IPv6. IPv6 offers more efficient routing and eliminates private address collisions that can occur on IPv4 when two devices on the same network are attempting to use the same address.

Key takeaways

Analyzing the different fields in an IP data packet can be used to find out important security information about the packet. Some examples of security-related information found in IP address packets are: where the packet is coming from, where it's going, and which protocol it's using. Understanding the data in an IP data packet will allow you to make critical decisions about the security implications of packets that you inspect.

Glossary terms from module 1

Terms and definitions from Course 3, Module 1

Bandwidth: The maximum data transmission capacity over a network, measured by bits per second

Cloud computing: The practice of using remote servers, application, and network services that are hosted on the internet instead of on local physical devices

Cloud network: A collection of servers or computers that stores resources and data in remote data centers that can be accessed via the internet

Data packet: A basic unit of information that travels from one device to another within a network

Hub: A network device that broadcasts information to every device on the network

Internet Protocol (IP): A set of standards used for routing and addressing data packets as they travel between devices on a network

Internet Protocol (IP) address: A unique string of characters that identifies the location of a device on the internet

Local Area Network (LAN): A network that spans small areas like an office building, a school, or a home

Media Access Control (MAC) address: A unique alphanumeric identifier that is assigned to each physical device on a network

Modem: A device that connects your router to the internet and brings internet access to the LAN

Network: A group of connected devices

Open systems interconnection (OSI) model: A standardized concept that describes the seven layers computers use to communicate and send data over the network

Packet sniffing: The practice of capturing and inspecting data packets across a network

Port: A software-based location that organizes the sending and receiving of data between devices on a network

Router: A network device that connects multiple networks together

Speed: The rate at which a device sends and receives data, measured by bits per second

Switch: A device that makes connections between specific devices on a network by sending and receiving data between them

TCP/IP model: A framework used to visualize how data is organized and transmitted across a network

Transmission Control Protocol (TCP): An internet communication protocol that allows two devices to form a connection and stream data

User Datagram Protocol (UDP): A connectionless protocol that does not establish a connection between devices before transmissions

Wide Area Network (WAN): A network that spans a large geographic area like a city, state, or country