network1.png

- List item

  A network is a group of connected devices. At home, the devices connected to your network might be your laptop, cell phones, and smart devices, like your refrigerator or air conditioner. In an office, devices like workstations, printers, and servers all connect to the network. The devices on a network can communicate with each other over network cables, or wireless connections. Networks in your home and office can communicate with networks in other locations, and the devices on them.

  Devices need to find each other on a network to establish communications. These devices will use unique addresses, or identifiers, to locate each other. The addresses will ensure that communications happens with the right device. These are called the IP and MAC addresses.

  Devices can communicate on two types of networks: a local area network, also known as a LAN, and a wide area network, also known as a WAN.

  A local area network, or LAN, spans a small area like an office building, a school, or a home. For example, when a personal device like your cell phone or tablet connects to the WIFI in your house, they form a LAN. The LAN then connects to the internet.

  A wide area network or WAN spans a large geographical area like a city, state, or country. You can think of the internet as one big WAN. An employee of a company in San Francisco can communicate and share resources with another employee in Dublin, Ireland over the WAN.

  Now that you've learned about the structure and types of networks, meet me in an upcoming video to learn about the devices that connect to them.

A hub is a network device that broadcasts information to every device on the network. Think of a hub like a radio tower that broadcasts a signal to any radio tuned to the correct frequency.

Another network device is a switch. A switch makes connections between specific devices on a network by sending and receiving data between them. A switch is more intelligent than a hub. It only passes data to the intended destination. This makes switches more secure than hubs, and enables them to control the flow of traffic and improve network performance.

Another device that we'll discuss is a router. A router is a network device that connects multiple networks together.

For example, if a computer in one network wants to send information to a tablet on another network, then the information will be transferred as follows: First, the information travels from the computer to the router. Then, the router reads the destination address, and forwards the data to the intended network's router. Finally, the receiving router directs that information to the tablet.

Finally, let's discuss modems. A modem is a device that connects your router to the internet, and brings internet access to the LAN.

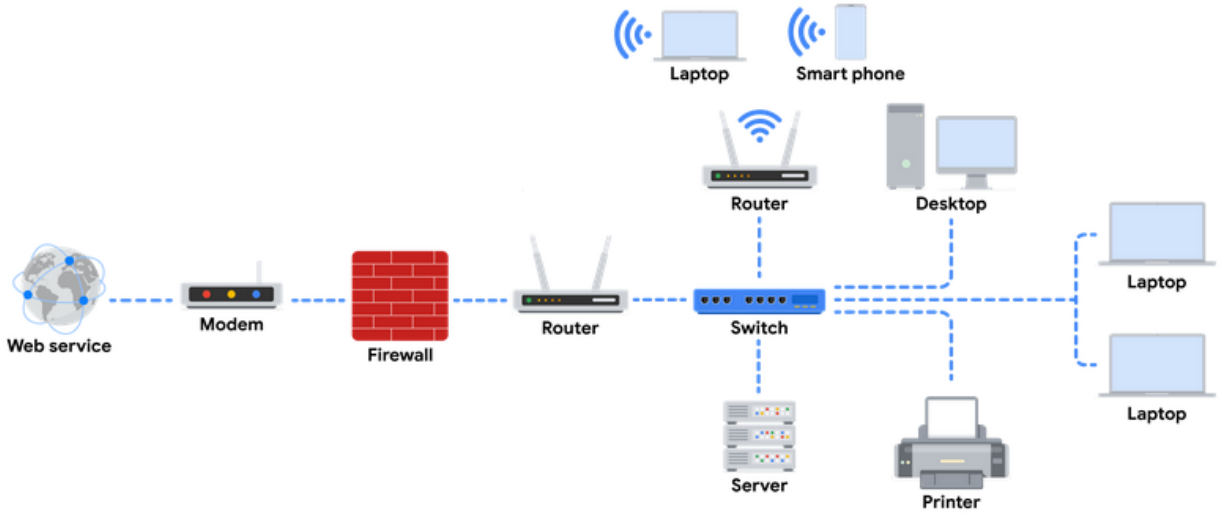
For example, if a computer from one network wants to send information to a device on a network in a different geographic location, it would be transferred as follows: The computer would send information to the router, and the router would then transfer the information through the modem to the internet. The intended recipient's modem receives the information, and transfers it to the router. Finally, the recipient's router forwards that information to the destination device.

Network tools such as hubs, switches, routers, and modems are physical devices. However, many functions performed by these physical devices can be completed by virtualization tools.

Virtualization tools are pieces of software that perform network operations. Virtualization tools carry out operations that would normally be completed by a hub, switch, router, or modem, and they are offered by Cloud service providers. These tools provide opportunities for cost savings and scalability. You'll learn more about them later in the certificate program.

Now you've explored some common devices that make up a network. Coming up, you're going to learn more about cloud computing, and how networks can be designed using cloud services.

Network devices are the devices that 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.



Devices and desktop computers

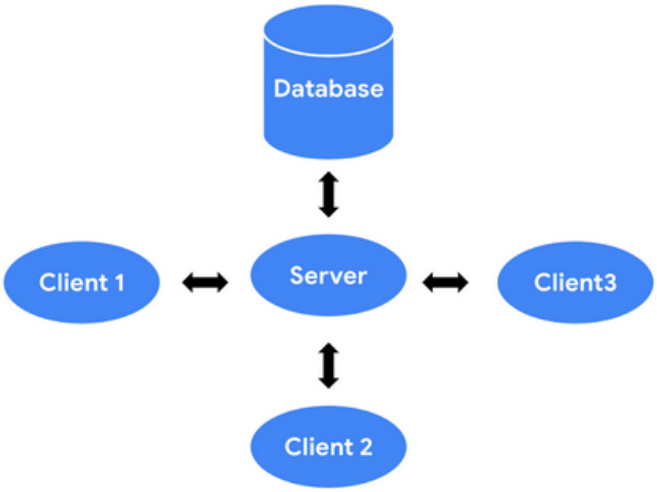
Most internet users are familiar with everyday devices, such as personal computers, laptops, mobile phones, and tablets. Each device and desktop computer has a unique MAC address and IP address, which identify it on the network, and a network interface that sends and receives data packets. These devices 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. Firewalls can also restrict specific incoming and outgoing network traffic. The organization configures the security rules. Firewalls often reside between the secured and controlled internal network and the untrusted network resources outside the organization, such as the internet.

Servers

Servers provide a service for other devices 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.

A switch forwards packets between devices directly connected to it. It maintains 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.

Routers

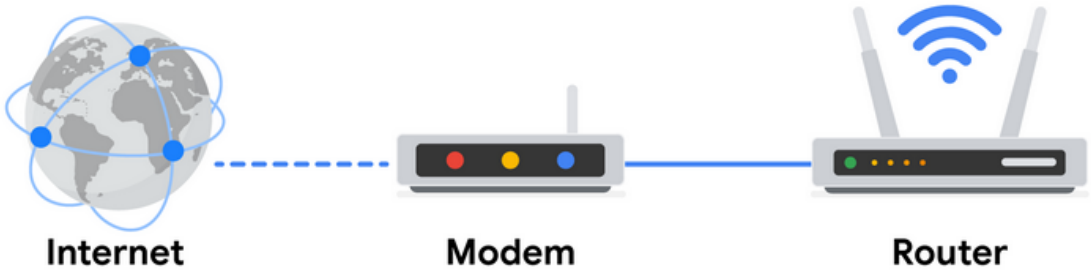
Routers sit between networks and direct traffic, based on the IP address of the destination network. The IP address of the destination network is contained in the IP header. The router reads the header information and forwards the packet to the next router on the path to the destination. This continues 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

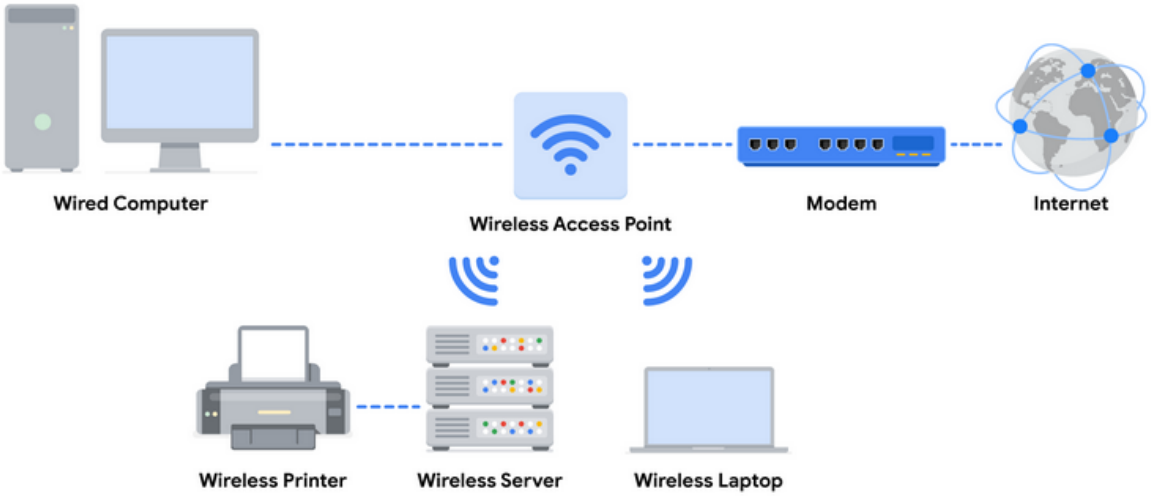
Modems usually interface with an internet service provider (ISP). ISPs provide internet connectivity via telephone lines, coaxial cables, fiber-optic cables, or satellites. Modems receive transmissions from the internet and translate them into digital signals that can be understood by the devices on the network. 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.

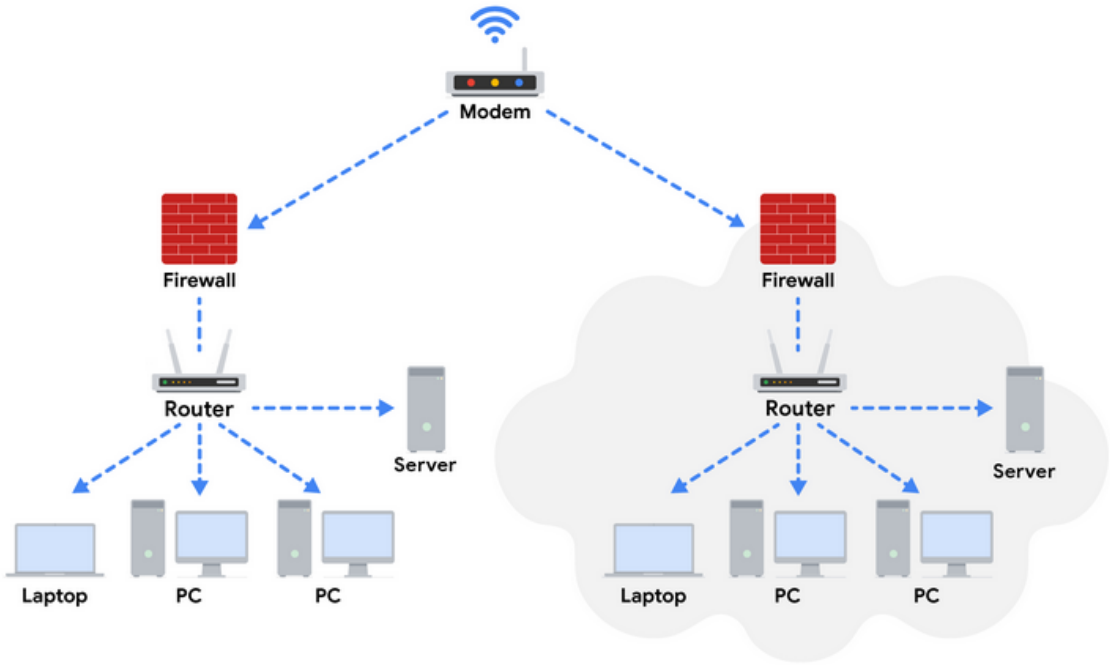
Network diagrams are topographical maps that show the devices on the network and how they connect. Network diagrams use small representative graphics to portray each network device and dotted lines to show how each device connects to the other. Security analysts use network diagrams to learn about network architecture and how to design networks.

Wireless Printer Wireless Server Wireless Laptop

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 topographical 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. Security analysts use network diagrams to learn about network architecture and how to design networks.



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.

Companies have traditionally owned their network devices, and kept them in their own office buildings. But now, a lot of companies are using third-party providers to manage their networks.

Why? Well, this model helps companies save money while giving them access to more network resources. The growth of cloud computing is helping many companies reduce costs and streamline their network operations.

Cloud computing is the practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices.

Today, the number of businesses that use cloud computing is increasing every year, so it's important to understand how cloud networks function and how to secure them.

Cloud providers offer an alternative to traditional on-premise networks, and allow organizations to have the benefits of the traditional network without storing the devices and managing the network on their own.

A cloud network is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet. Because companies don't house the servers at their physical location, these servers are referred to as being "in the cloud".

Traditional networks host web servers from a business in its physical location. However, cloud networks are different from traditional networks because they use remote servers, which allow online services and web applications to be used from any geographic location. Cloud security will become increasingly relevant to many security professionals as more organizations migrate to cloud services.

Cloud service providers offer cloud computing to maintain applications. For example, they provide on-demand storage and processing power that their customers only pay as needed. They also provide business and web analytics that organizations can use to monitor their web traffic and sales.

With the transition to cloud networking, I have witnessed an overlap of identity-based security on top of the more traditional network-based solutions. This meant that my focus needed to be on verifying both where the traffic is coming from and the identity that is coming with it.

More organizations are moving their network services to the cloud to save money and simplify their operations. As this trend has grown, cloud security has become a significant aspect of network security.

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.

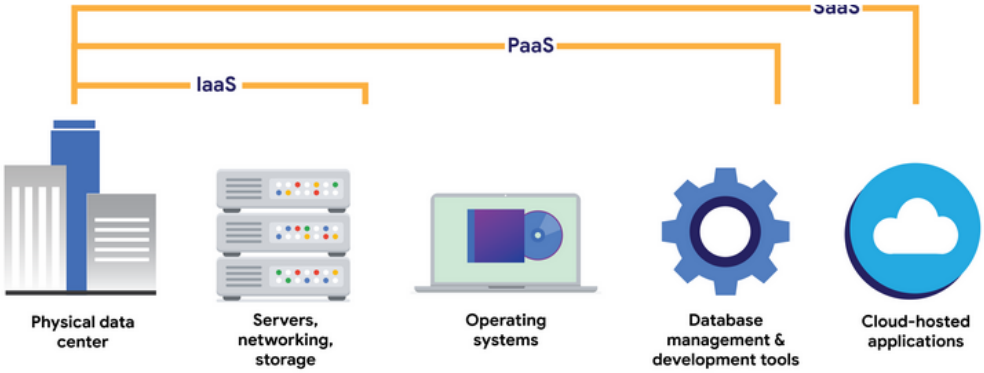
Computing processes in the cloud

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.

Resources for more information

For more information about cloud computing and the services offered, you can review Google Cloud (GC).

A network is a group of connected devices. At home, the devices connected to your network might be your laptop, cell phones, and smart devices, like your refrigerator or air conditioner. In an office, devices like workstations, printers, and servers all connect to the network. The devices on a network can communicate with each other over network cables, or wireless connections. Networks in your home and office can communicate with networks in other locations, and the devices on them.

Devices need to find each other on a network to establish communications. These devices will use unique addresses, or identifiers, to locate each other. The addresses will ensure that communications happens with the right device. These are called the IP and MAC addresses.

Devices can communicate on two types of networks: a local area network, also known as a LAN, and a wide area network, also known as a WAN.

A local area network, or LAN, spans a small area like an office building, a school, or a home. For example, when a personal device like your cell phone or tablet connects to the WIFI in your house, they form a LAN. The LAN then connects to the internet.

A wide area network or WAN spans a large geographical area like a city, state, or country. You can think of the internet as one big WAN. An employee of a company in San Francisco can communicate and share resources with another employee in Dublin, Ireland over the WAN.

Now that you've learned about the structure and types of networks, meet me in an upcoming video to learn about the devices that connect to them.

A hub is a network device that broadcasts information to every device on the network. Think of a hub like a radio tower that broadcasts a signal to any radio tuned to the correct frequency.

Another network device is a switch. A switch makes connections between specific devices on a network by sending and receiving data between them. A switch is more intelligent than a hub. It only passes data to the intended destination. This makes switches more secure than hubs, and enables them to control the flow of traffic and improve network performance.

Another device that we'll discuss is a router. A router is a network device that connects multiple networks together.

For example, if a computer in one network wants to send information to a tablet on another network, then the information will be transferred as follows: First, the information travels from the computer to the router. Then, the router reads the destination address, and forwards the data to the intended network's router. Finally, the receiving router directs that information to the tablet.

Finally, let's discuss modems. A modem is a device that connects your router to the internet, and brings internet access to the LAN.

For example, if a computer from one network wants to send information to a device on a network in a different geographic location, it would be transferred as follows: The computer would send information to the router, and the router would then transfer the information through the modem to the internet. The intended recipient's modem receives the information, and transfers it to the router. Finally, the recipient's router forwards that information to the destination device.

Network tools such as hubs, switches, routers, and modems are physical devices. However, many functions performed by these physical devices can be completed by virtualization tools.

Virtualization tools are pieces of software that perform network operations. Virtualization tools carry out operations that would normally be completed by a hub, switch, router, or modem, and they are offered by Cloud service providers. These tools provide opportunities for cost savings and scalability. You'll learn more about them later in the certificate program.

Now you've explored some common devices that make up a network. Coming up, you're going to learn more about cloud computing, and how networks can be designed using cloud services.

Networks help organizations communicate and connect. But communication makes network attacks more likely because it gives a malicious actor an opportunity to take advantage of vulnerable devices and unprotected networks.

Communication over a network happens when data is transferred from one point to another. Pieces of data are typically referred to as data packets.

A data packet is a basic unit of information that travels from one device to another within a network. When data is sent from one device to another across a network, it is sent as a packet that contains information about where the packet is going, where it's coming from, and the content of the message.

Think about data packets like a piece of physical mail. Imagine you want to send a letter to a friend. The envelope will need to have the address where you want the letter to go and your return address. Inside the envelope is a letter that contains the message that you want your friend to read.

A data packet is very similar to a physical letter. It contains a header that includes the internet protocol address, the IP address, and the media access control, or MAC, address of the destination device. It also includes a protocol number that tells the receiving device what to do with the information in the packet. Then there's the body of the packet, which contains the message that needs to be transmitted to the receiving device. Finally, at the end of the packet, there's a footer, similar to a signature on a letter, the footer signals to the receiving device that the packet is finished.

The movement of data packets across a network can provide an indication of how well the network is performing. Network performance can be measured by bandwidth.

Bandwidth refers to the amount of data a device receives every second. You can calculate bandwidth by dividing the quantity of data by the time in seconds. Speed refers to the rate at which data packets are received or downloaded. Security personnel are interested in network bandwidth and speed because if either are irregular, it could be an indication of an attack. Packet sniffing is the practice of capturing and inspecting data packets across the network.

Communication on the network is important for sharing resources and data because it allows organizations to function effectively. Coming up, you'll learn more about the protocols to support network communication.

TCP/IP stands for Transmission Control Protocol and Internet Protocol. TCP/IP is the standard model used for network communication. Let's take a closer look at this model by defining TCP and IP separately.

First, TCP, or Transmission Control Protocol, is an internet communication protocol that allows two devices to form a connection and stream data. The protocol includes a set of instructions to organize data, so it can be sent across a network. It also establishes a connection between two devices and makes sure that packets reach their appropriate destination.

The IP in TCP/IP stands for Internet Protocol. IP has a set of standards used for routing and addressing data packets as they travel between devices on a network. Included in the Internet Protocol (IP) is the IP address that functions as an address for each private network. You'll learn more about IP addresses a bit later.

When data packets are sent and received across a network, they are assigned a port.

Within the operating system of a network device, a port is a software-based location that organizes the sending and receiving of data between devices on a network. Ports divide network traffic into segments based on the service they will perform between two devices. The computers sending and receiving these data segments know how to prioritize and process these segments based on their port number.

This is like sending a letter to a friend who lives in an apartment building. The mail delivery person not only knows how to find the building, but they also know exactly where to go in the building to find the apartment number where your friend lives.

Data packets include instructions that tell the receiving device what to do with the information. These instructions come in the form of a port number. Port numbers allow computers to split the network traffic and prioritize the operations they will perform with the data. Some common port numbers are: port 25, which is used for e-mail, port 443, which is used for secure internet communication, and port 20, for large file transfers.

As you've learned in this video, a lot of information and instructions are contained in data packets as they travel across a network. Coming up, you'll learn more about the TCP/IP model.

Now that we've discussed the structure of a network and how communications takes place, it's important for you to know how the security professionals identify problems that might arise.

The TCP/IP model is a framework that is used to visualize how data is organized and transmitted across the network. The TCP/IP model has four layers. The four layers are: the network access layer, the internet layer, the transport layer, and the application layer.

Knowing how the TCP/IP model organizes network activity allows security professionals to monitor and secure against risks.

Let's examine these layers one at a time.

Layer one is the network access layer. The network access layer deals with creation of data packets and their transmission across a network. This includes hardware devices connected to physical cables and switches that direct data to its destination.

Layer two is the internet layer. The internet layer is where IP addresses are attached to data packets to indicate the location of the sender and receiver. The internet layer also focuses on how networks connect to each other. For example, data packets containing information that determine whether they will stay on the LAN or will be sent to a remote network, like the internet.

The transport layer includes protocols to control the flow of traffic across a network. These protocols permit or deny communication with other devices and include information about the status of the connection. Activities of this layer include error control, which ensures data is flowing smoothly across the network.

Finally, at the application layer, protocols determine how the data packets will interact with receiving devices. Functions that are organized at application layer include file transfers and email services.

Now you have an understanding of the TCP/IP model and its four layers. Meet you in the next video.

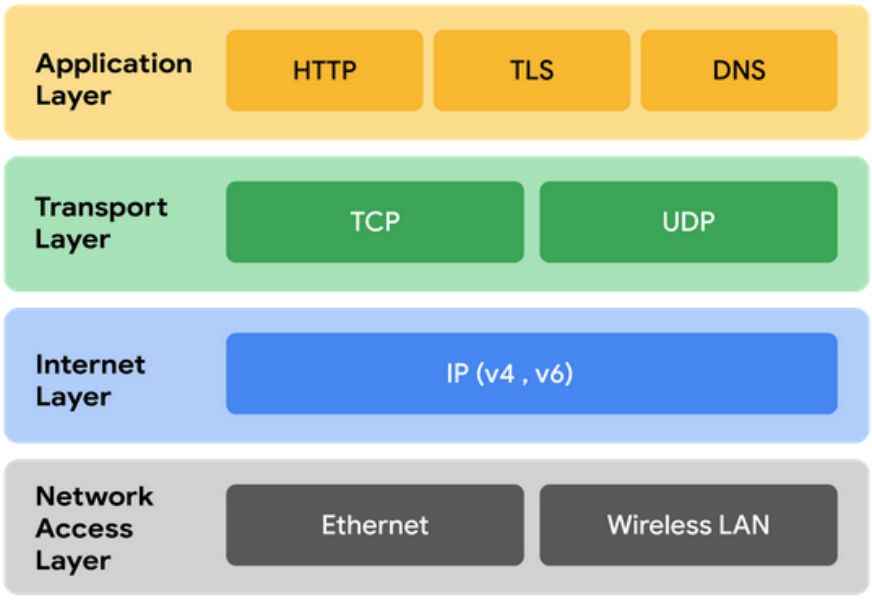
In this reading, you will build on what you have learned about the Transmission Control Protocol/Internet Protocol (TCP/IP) model, consider the differences between the Open Systems Interconnection (OSI) model and TCP/IP model, and learn how they're related. Then, you'll review each layer of the TCP/IP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

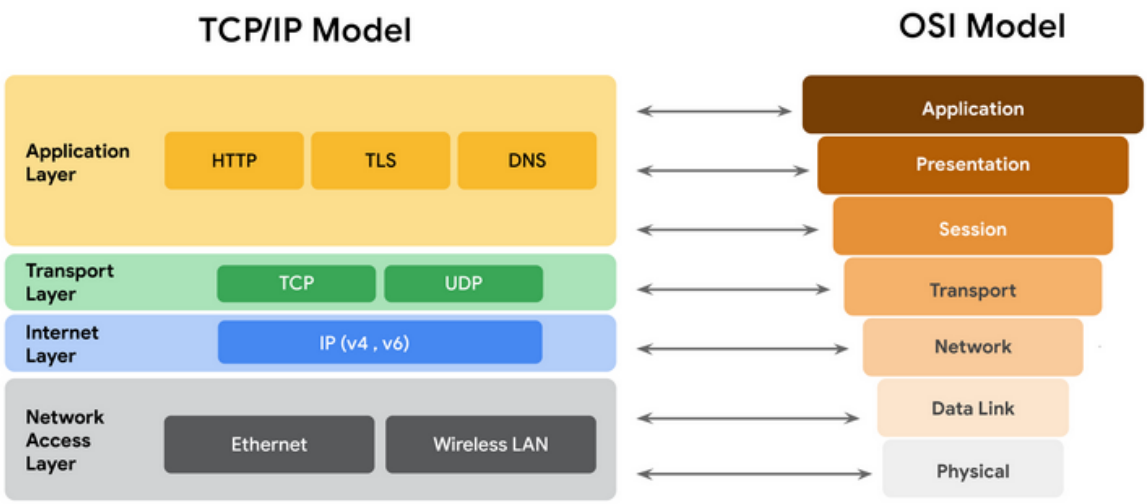
Application layer

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 network communication occurs across a network.

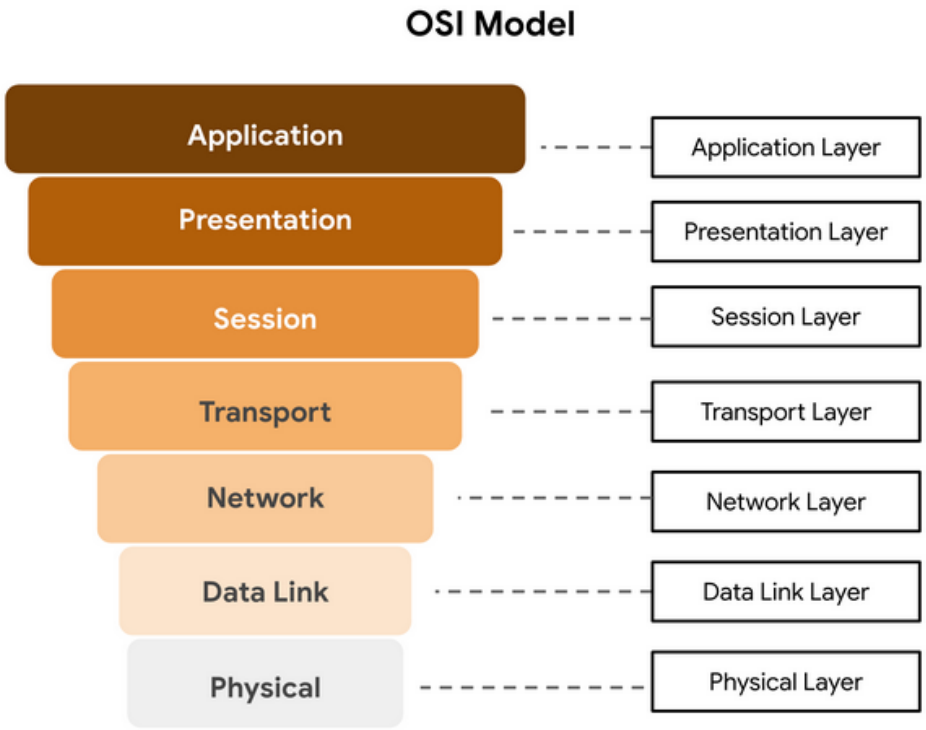
All communication on a network is organized using network protocols. Previously, you learned about the Transmission Control Protocol (TCP), which establishes connections between two devices, and the Internet Protocol (IP), which is used for routing and addressing data packets as they travel between devices on a network. This reading will continue to explore the seven layers of the Open Systems Interconnection (OSI) model and the processes that occur at each layer. We will work backwards from layer seven to layer one, going from the processes that involve the everyday network user to those that involve the most basic networking components, like network 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 network security analysts design the data network and 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 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 network 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 occur to 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 in regards to data transmission between two or more systems. The OSI model contains seven 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.