Network Communication

- Introduction to network communication
- The TCP/IP model
- The four layers of the TCP/IP model
- Learn more about the TCP/IP model
- The OSI model
- Local and wide network communication
- Components of network layer communication
- Wrap-up
- Glossary terms from Course 3, Week 1

Introduction to network communication

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.

The TCP/IP model

Hello again. In this video, you'll learn more about communication protocols and devices used to communicate with each other across the internet. This is called the TCP/IP model.

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.

The four layers of 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.

---

what are the Layers of the TCP/IP model?

1. Network access layer
2. Internet layer
3. Transport layer
4. Application layer

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

Transmission Control Protocol

The 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

The UDP 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. 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.

Local and wide network communication

Let's learn about how IP addresses are used to communicate over a network. IP stands for internet protocol. An internet protocol address, or IP address, is a unique string of characters that identifies a location of a device on the internet. Each device on the internet has a unique IP address, just like every house on a street has its own mailing address.

There are two types of IP addresses: IP version 4, or IPv4, and IP version 6, or IPv6. Let's look at examples of an IPv4 address.

IPv4 addresses are written as four, 1, 2, or 3-digit numbers separated by a decimal point. In the early days of the internet, IP addresses were all IPV4. But as the use of the internet grew, all the IPv4 addresses started to get used up, so IPv6 was developed.

IPv6 addresses are made up of 32 characters. The length of the IPv6 address will allow for more devices to be connected to the internet without running out of addresses as quickly as IPv4.

IP addresses can be either public or private. Your internet service provider assigns a public IP address that is connected to your geographic location. When network communications goes out from your device on the internet, they all have the same public-facing address. Just like all the roommates in one home share the same mailing address, all the devices on a network share the same public-facing IP address.

Private IP addresses are only seen by other devices on the same local network. This means that all the devices on your home network can communicate with each other using unique IP addresses that the rest of the internet can't see.

Another kind of address used in network communications is called a MAC address. A MAC address is a unique alphanumeric identifier that is assigned to each physical device on a network. When a switch receives a data packet, it reads the MAC address of the destination device and maps it to a port. It then keeps this information in a MAC address table. Think of the MAC address table like an address book that the switch uses to direct data packets to the appropriate device.

In this video, you learned about IP version 4 and IP version 6 addresses. You learned how IP and MAC addresses are used in network communication and the difference between a public and a private IP address.

Components of network layer communication

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 and internet from the host device to the destination device. This includes directing the packets from one router to another router across the internet, based on 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; this is referred to as an IP packet or datagram. 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:

The size of the IP header ranges from 20 to 60 bytes. The header includes the IP routing information that devices use to direct the packet. The format of an IP packet header is determined by the IPv4 protocol.

The length of the data section of an IPv4 packet can vary greatly in size. However, the maximum possible size of an IP packet is 65,536 bytes. It contains the message being transferred to the transmission, like website information or email text.

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

Version: The first 4-bit header tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet.

IP Header Length (HLEN): 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: For IPv4 packets that are larger than 65, 535 bytes, 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 in the future. IPv6 was developed to mitigate IPv4 address exhaustion and other related concerns.

One of the key differences between IPv4 and IPv6 is the length of the addresses. IPv4 addresses are numeric, made of 4 bytes, and allow for up to 4.3 billion possible addresses. IPv4 addresses are made up of four strings and the numbers range from 0 to 255. An example of an IPv4 address would be: 198.51.100.0. IPv6 addresses are hexadecimal, made up of 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.

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 HLEN, Identification, and Flags fields, whereas the IPv6 does not. The IPv6 header introduces different fields not included in IPv4 headers, such as the Flow Label and Traffic Class.

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

Security analysts can use packet capturing tools, or PCAP, to inspect packets while they’re in transit. Analyzing the different fields in an IP address packet can be used to find out important security information about the packet. Some examples of security-related information found in IP address packets: where the packet is coming from, where it’s going, and which protocol it’s using. Understanding the data in an IPv4 data packet will allow you to make critical decisions about the security implications of packets that you inspect.

Wrap-up

Hey, you made it! Well done! Let's wrap up what you've learned in this section of the course.

We explored the structure of a network, including WANs and LANs. We also discussed standard networking tools like hubs, switches, routers, and modems. We briefly introduced cloud networks, and we discussed their benefits. We also spent some time on the TCP/IP model. As a reminder, technicians and security analysts often use this framework when communicating where network problems have occurred.

That wraps up this section. Next, you'll learn more about network operations and how data is transmitted over wireless networks.

bro i actuially listened to the extra reading like 5 times each

Glossary terms from Course 3, Week 1

Terms and definitions from Course 3, Week 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

Subnetting: The subdivision of a network into logical groups called subnets

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