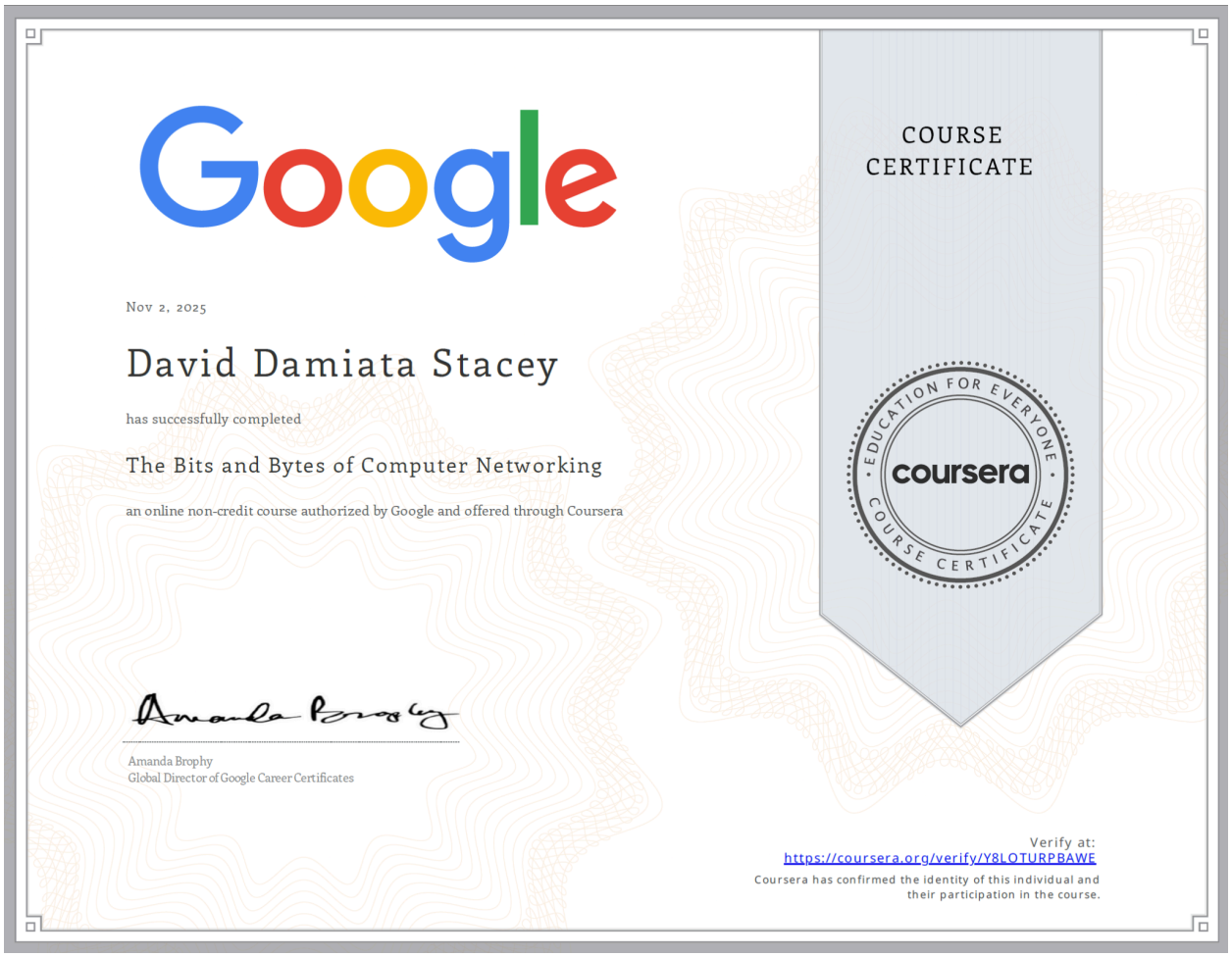
The Bits and Bytes of Computer Networking

Course 2 of the Google IT Support Professional Certificate

Completed on 11.2.2025



All associated videos are within **OneDrive/Coursera/Google IT Support/Networking_101**

Module 1 videos are labeled A01-A12.
Module 2 Videos are labeled B00-B12

Module 3 Videos are labeled C00-C09
Module 4 Videos are labeled D00-D12

Module 5 Videos are labeled E00-E14
Module 6 Videos are labeled F00-F14

Module 1 - Introduction to Networking

The TCP/IP Five-Layer Network Model

Physical Layer - Represents the physical devices that interconnect computers. Cables and their specifications.
- Older “hubs” were on the 1st layer.
- The physical layer is concerned with the transmission of raw bits

Data Link/Network Access Layer - Responsible for defining a common way of interpreting signals so network devices can communicate. Ethernet, standards that also define a protocol responsible for getting data to nodes on the same network or link.
- Switches are on layer 2.

Network/Internet Layer - Responsible for getting one node of data to another. Allows different networks to communicate with each other through devices known as routers. **Internetwork**: A collection of networks connected together through routers, the most famous of these being the internet. Packets/Datagram.
- Routers live on Layer 3.
    - **Border Gateway Protocol (BGP)**: Routers share data with each other via this protocol, which lets them learn about the most optimal paths to forward traffic.
- IP lives here.

Transport Layer - Sorts out which client and server programs are supposed to get that data. TCP and UDP *are* these layers.
- Provides end-to-end communication between processes on hosts, focusing on reliability and flow control, but it doesn't interpret the data for applications.
- Firewalls live here.

Application Layer - HTTP, SMTP... Messages and Client facing apps
- Specifically designed to provide services that applications can directly use, enabling them to communicate using protocols and data formats they understand

Supplemental Reading for Ethernet Over Twisted Pair Technologies

Ethernet Over Twisted Pair Technologies

In this reading, you will learn about the importance of Ethernet over twisted pair technologies. Twisted pair Ethernet cable is the most commonly used Ethernet cable in business and home networks. An internet connection to a building or home is normally delivered through a coaxial cable and/or fiber-optic cable from an internet service provider (ISP). This connection is fed into a gateway modem located inside the building or home (for home internet customers, this hardware is often provided by the ISP). The modem then passes the internet connection through a twisted pair Ethernet cable to a router or a single computer. The router uses twisted pair Ethernet cables to distribute wired network connections internally to the business or home. These network cables are also called CAT cables. It is possible that you have purchased an Ethernet CAT5 or CAT6 cable for your home internet connection. Some routers also have the capability to provide wireless network connections to the internal network. In addition, Ethernet over twisted pair technologies can also supply telephone and television services to businesses and homes.

Twisted pair cables

Originally, telephone and early data cables included two copper wires, one for transmitting data and one for receiving data. The two wires laid parallel to one another. This configuration was affected by electromagnetic interference (EMI), radio frequency interference (RFI), and crosstalk between the two copper wires. One of the initial engineering steps to resolve these issues involved twisting the wire pair together, which reduced some of the extra noise on the lines.
Twisted pair Ethernet cables are commonly used in LANs because:
- They offer multiple levels of protection against EMI, RFI, and crosstalk.
- The lower levels of interference protection provide low-cost options, which are generally more accessible to home users and small businesses.
- The cables are thin, light weight, and malleable enough to install and move easily.
- The transmission range of the cable is suitable for short distance connections inside of buildings and homes.
- The cable’s frequency range is able to transmit both data and telephone/voice communications.

UTP, STP, and FTP Ethernet cables

Twisted pair Ethernet cable uses four pairs of color-coded copper wires. Each colored pair, one solid and one striped, are twisted together. There are multiple types of twisted pair Ethernet cables available on the market.

These types fall into three main categories:

- Unshielded twisted pair (UTP) - The most common and least expensive type of Ethernet cable found in business and home networks. UTP cables offer very basic protection against EMI, RFI, and crosstalk interference.
- Shielded twisted pair (STP) - Used in environments where electromagnetic interference (EMI), radio frequency interference (RFI), and crosstalk with nearby cables have been identified as a problem for network communications. An STP cable uses a braided aluminum and/or copper shielding to encase the four twisted pairs underneath the outer jacket.
- Foiled twisted pair (FTP) - Also used in environments where EMI, RFI, and crosstalk are a problem. An FTP cable uses a thin foil shield that wraps around the bundle of twisted pair wires underneath the outer jacket.

The STP and FTP labels are often used interchangeably to reference shielded and/or foiled cables. STP and FTP braided and foiled shields can also exist together in the same cable for extra protection against interference. It is important to check the manufacturer's description of the Ethernet cable to determine which interference-reducing method was used in the manufacturing of the cable. UTP, STP, and FTP Ethernet cables can also be manufactured to have braided and/or foil shields around each of the four twisted pairs. This configuration further reduces crosstalk amongst the twisted pairs, but is the most expensive of the Ethernet cable options. A shielded with foiled twisted pair (SF/FTP) would most likely be used in an industrial environment where EMI and/or RFI is much higher than normal.

Straight-through cable

Straight-through cables are also known as patch cables. They are the primary type of Ethernet cable used in computer networks. Straight-through cables normally connect computers and routers to hubs and Ethernet switches. Ethernet cable can also connect servers to Ethernet switches.
Straight-through cables can be identified by comparing both ends of the cable with one another. The cable is a straight-through cable if the color and stripe order of the twisted pairs are in the same position on both ends of the cable. In a typical straight-through cable set-up, an orange-striped wire that appears in pin position 1 should also appear at that same position on the other end. This one-to-one pattern is continued for each color in pin positions 2-8. Ethernet cables that use 100Base-T standards (common for home networks) do not use blue and brown cables. Networks using gigabit Ethernet have the option to use blue and brown cables for Power over Ethernet (PoE).

Straight-through cable key:

- Computers and routers use:
    - Pins 1 & 2 - Orange wires for sending data
    - Pins 3 & 6 - Green wires for receiving data
- Hubs and switches use:
    - Pins 1 & 2 - Green wires for sending data
    - Pins 3 & 6 - Orange wires for receiving data

Supplemental Reading for Twisted Pair Ethernet: Crossover Cables

Twisted pair Ethernet: Crossover cable

Crossover cables

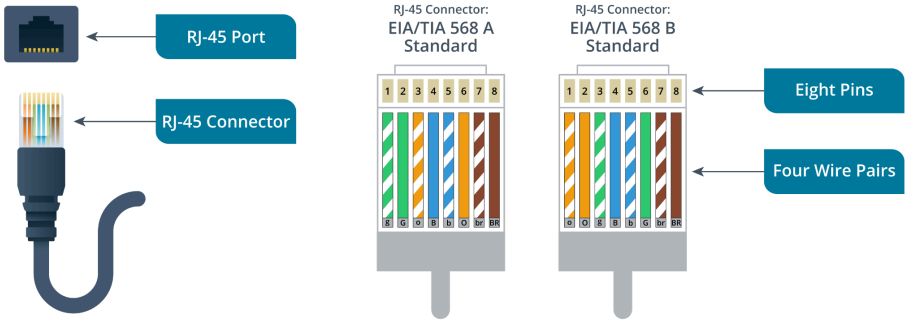
Crossover cables may still be in use in older network environments. This section provides information for working with crossover Ethernet cable for older Enterprise network devices. Note that most new Enterprise devices have the ability to detect Ethernet connection types and select the correct wires for sending and receiving data using Auto Medium Dependent Interface Crossover (Auto-MDI/MDIX) technology. The Auto-MDI/MDIX ports replace the crossover cable's function for connecting two devices that use the same sending and receiving wires for data communications.

Crossover cables are used to connect two computing devices directly to one another. As an IT Support specialist, you might use a short crossover cable to connect an IT administrator laptop directly to an Enterprise machine (e.g., server, switch, router, hub, etc.). This type of connection is normally used to update, repair, and perform other administrative tasks on the Enterprise machine. A crossover cable should be connected between the Ethernet port/Network Interface Card (NIC) on the IT administrative system and the management port of the Enterprise machine. This connection is then used to access the operating system and/or the management interface of the Enterprise machine. Additionally, crossover cables can connect two switches, two hubs, or a switch to a hub, as well as two routers, two PCs, or a router to a PC.

Like straight-through cables, crossover cables can also be identified by comparing both ends of the cable to one another. Crossover cable ends will have different patterns in the color order of the twisted pairs. The crossover cable key below describes a typical setup for a T-568-A. If the green wires appear in pin positions 1 and 2 on one side of the cable, on the opposite end of the cable, the green wires will appear in the pin positions 3 and 6. The orange wires will appear in positions 3 and 6 at one end of the cable, crossing over to the 1 and 2 positions at the opposite end.

For the T-568-B scheme, if you see orange wires start at pin positions 3 and 6, they should cross over to pin positions 1 and 2 at the opposite end of the cable. Green wires should start at pin positions 1 and 2, crossing over to 3 and 6 at the opposite end. This wiring crossover is needed to connect two computers that transmit and receive data on the same wires. Blue and brown wires do not cross over to different positions in this set-up.
Straight-through cables use the T568B wiring scheme, while crossover cables use both schemes.
Crossover cable key:

- Endpoint 1 of the Ethernet cable:
    - Pins 1 & 2 - Green wires for sending data
    - Pins 3 & 6 - Orange wires for receiving data
- Endpoint 2 of the Ethernet cable:
    - Pins 1 & 2 - Orange wires for sending data
    - Pins 3 & 6 - Green wires for receiving data



Unicast, Multicast, and Broadcast

A **unicast** transmission is always meant for just one receiving address.

- If the least significant bit in the **first octet** of a destination address is set to **zero**, it means that the ethernet frame is intended for only the destination address.
- If the least significant bit in the **first octet** of a destination address is set to **one**, it means you're dealing with a multicast frame.

A **multicast** transmission sends its information to all devices on the local Network segment.

An ethernet **broadcast** is sent to every single device on a LAN. This is accomplished by using a special destination known as a **broadcast address**. The ethernet broadcast address is all **F**'s.

- Used so that devices can learn more about each other.

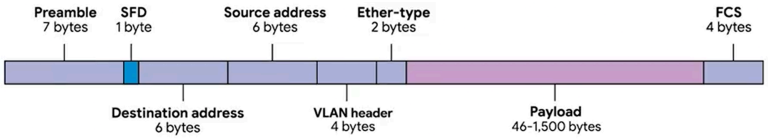
Dissecting an Ethernet Frame

Data packet - More of a concept than a literal term
An all-encompassing term that represents any single set of binary data being sent across a network link.

- Data packets at the Ethernet level are known as:

Ethernet frame
A highly structured collection of information presented in a specific order

- Enables network interfaces at the physical layer to convert a stream of bits traveling across a link into meaningful data, or vice versa.
- Almost all sections of an Ethernet frame are mandatory, and most of them have fixed size.



Preamble

8 bytes (or 64 bits) long, and can itself be split into two sections.

- **The first seven bytes** are a series of alternating **ones** and **zeros**. These act partially as a buffer between frames and can also be used by the network interfaces to synchronize internal clocks they use to regulate the speed at which they send data.
- **The last byte** in the preamble is known as the **SFD** or **Start frame delimiter**.

Star Frame Delimiter (SFD)

Signals to a receiving device that the preamble is over and that the actual frame contents will now follow.

Destination MAC address
The hardware address of the intended recipient.

- Each MAC address is **48 bits** or **6 bytes** long, or **6 octets**

Ether-type field
16 bits long and used to describe the protocol of the contents of the frame.

VLAN header
Indicates that the frame itself is what's called a VLAN frame.

Payload
In networking terms, is the actual data being transported, which is everything that isn't a header.

- Can be anywhere from 46 to 1500 bytes long.
- This contains all of the data from higher layers, such as the ip, transport and application layers, that's actually being transmitted.

Frame Check Sequence
A 4-byte (or 32-bit) number that represents a checksum value for the entire frame.

- Calculated by performing a CRC against the frame.

Cyclical Redundancy Check (CRC)
An important concept for data integrity, and is used all over computing, not just network transmissions.

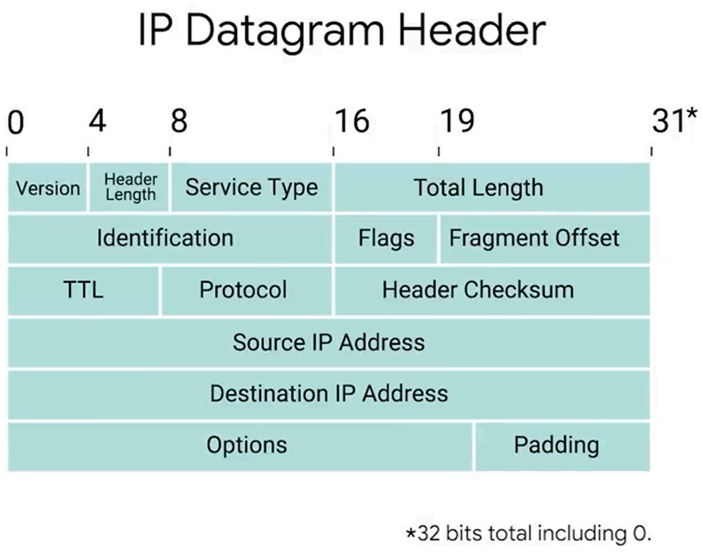
- A CRC is basically a mathematical transformation that uses polynomial division to create a number that represents a larger set of data.

Module 2: The Network Layer

IPv4 datagram

A highly structured series of fields that are strictly defined.

- The maximum size of a single datagram is the largest number you can represent with 16 bits: 65,535
- If the total amount of data that needs to be sent is larger than what can fit in a single datagram, the IP layer needs to split this data up into many individual packets.



Fragmentation
The process of taking a single IP datagram and splitting it up into several smaller datagrams.

Version
Indicates IPv4 or IPv6

Header
4-bit field, almost always 20 bytes in length in IPv4.

Service Type
These 8 bits can be used to specify details about quality of service (QoS) technologies.

Total Length
Indicates the total length of the IP datagram it's attached to.

Identification field
A 16-bit number that's used to group messages together

Flag field
Used to indicate if a datagram is allowed to be fragmented, or to indicate that the datagram has already been fragmented.

Fragment Offset
Contains values used by the receiving end to take all the parts of a fragmented packet and put them back together in the correct order.

Time to Live (TTL) field
An 8-bit field that indicates how many router hops a datagram can traverse before it's thrown away.

Protocol field
An 8-bit field that contains data about what transport layer protocol is being used.

Header Checksum
A checksum of the contents of the entire IP datagram header.

Source/Destination IP addresses
32-bit long each.

Options
An optional field and is used to set special characteristics for datagrams primarily used for testing purposes.

Padding
A series of zeroes used to ensure the header is the correct total size.

Address Resolution Protocol (ARP)
A protocol used to discover the hardware address of a node with a certain IP address

ARP Table
A list of IP addresses and the MAC addresses associated with them.
- Entries generally expire after a short amount of time to ensure changes in the network are accounted for.

Subnetting
The process of taking a large network and splitting it up into many individual and smaller subnetworks, or subnets.

Subnet Masks
32-bit numbers that are normally written out as four octets in decimal.

Demarcation Point
To describe where one network system ends and another one begins.

Routing Protocols
Special protocols routers use to speak to each other in order to share what information they might have. They fall into 2 main categories:
- Interior Gateway Protocols: Used by routers to share information within a single autonomous system.
    - **Link State Routing Protocols**: Link state protocols get their name because each router advertises the state of the link of each of its interfaces. These interfaces could be connected to other routers, or they could be direct connections to networks. The information about each router is propagated to every other router on the autonomous system. This means that every router on the system knows every detail about every other router in the system. Each router then uses this much larger set of information and runs complicated algorithms against it to determine what the best path to any destination network might be. Link state protocols require both more memory in order to hold all of this data, and also much more processing power. This is because it has to run algorithms against this data in order to determine the quickest path to update the routing tables. As computer hardware has become more powerful and cheaper over the years, link state protocols have mostly made distance-vector protocols outdated.
    - **Distance-vector protocols**: A router using a distance vector protocol basically just takes its routing table, which is a list of every network known to it and how far away these networks are in terms of hops. Then the router sends this list to every neighboring router, which is basically every router directly connected to it. In computer science, a list is known as a vector. This is why a protocol that just sends a list of distances to networks is known as a distance vector protocol.
- Exterior Gateway Protocols: Used for the exchange of information between independent autonomous systems. Exterior gateway protocols are used to communicate data between routers representing the edges of an autonomous system. Since routers sharing data using interior gateway protocols are all under control of the same organization, routers use exterior gateway protocols when they need to share information across different organizations. Exterior gateway protocols are really key to the Internet operating how it does today.

Autonomous System: A collection of networks that all fall under the control of a single network operator.

Internet Assigned Numbers Authority (IANA): A non-profit organization that helps manage things like IP address allocation. They are also responsible for **ASN**, or **Autonomous System Number** allocation.

Multiplexing
The process of combining multiple data streams into a single signal for transmission over a shared medium.

Demultiplexing
The process of taking the combined traffic arriving at the intended node and separating it to deliver it to the correct receiving application or service (often identified by port numbers).

Encapsulation
Adding control information (headers and trailers) to data as it moves through network layers.

Routing
Determines the best path for data packets to travel across networks to a destination host.

Supplemental Reading for Routing Protocol Examples

We've covered a few different routing protocol types, but we haven't discussed the details of how the actual implementation of these protocols might matter.

Many network protocols are implemented based on specifications published by the Internet Engineering Task Force (IETF). We'll cover this in more detail in a future lesson!

The most common distance vector protocols are RIP, or Routing Information Protocol (IETF RFC2453), and EIGRP, or Enhanced Interior Gateway Routing Protocol (Cisco documentation). The most common link state protocol is OSPF, or Open Shortest Path First (IETF RFC2328).

In terms of exterior gateway protocols, there is only one in use today. The entire Internet needs to agree on how to exchange this sort of information, so a single standard has emerged. This standard is known as BGP, or Border Gateway Protocol (IETF RFC4271).

Non-routable address space

Ranges of IPs set aside for use by anyone that cannot be routed to. Also known as "Private IP Addresses"

Supplemental Reading for RFCs and Standards

In the video about non-routable address space, we introduced the concept of an RFC, or Request for Comments. RFCs started as a way for academics to discuss how their computers might talk to each other.

An RFC would be published, people would leave comments, eventually a consensus would be formed, and a new standard would be developed.

Over many decades, RFCs have come to belong to the IETF, or Internet Engineering Task Force, which is an open community charged with developing and maintaining the standards required for the Internet to continue to operate.

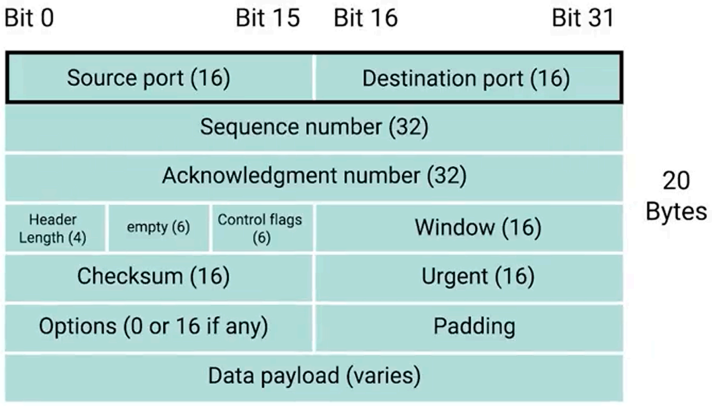
You can browse the impressively large collections of RFCs here.

By the way, RFCs have a long history of April Fool's Day jokes. My personal favorites are RFC 1149 and RFC 3514, both of which might be funnier once we've tackled the next module.

Module 3: The Transport and Application Layers

Port
A 16-bit number that's used to direct traffic to specific services running on a networked computer.

TCP Segment
Made up of a TCP header and a data section.



Source Port
A high-numbered port chosen from a special section of ports known as ephemeral ports.

Destination Port
The port of the service the traffic is intended for.

Sequence Number
A 32-bit number that's used to keep track of where in a sequence of TCP segments this one is expected to be.
- Indicates the order of bytes in the stream.
- Identifies the position of the first byte of data in the current segment being sent

Acknowledgement Number
The number of the next expected segment. Confirms the receipt of data from the other end of the connection. Used to inform the sending host which byte of data it should transmit next to continue the flow of communication, this field indicates the sequence number of the next byte the receiver expects to get.

Data Offset Field
A 4-bit number that communicates how long the TCP header for this segment is. To inform the receiving device precisely where the fixed-size header ends and the actual application data begins, the TCP header includes this specific field.
- The Data offset specifies the length of the TCP header, indicating where the actual data payload begins

Window
Specifies the range of sequence numbers that might be sent before an acknowledgement is required.(??? This is where the video in the course must have made mistakes, because they called this the "checksum" and so now there's 3 notes for Checksum).

Checksum
Specifies the range of sequence numbers that might be sent before an acknowledgement is required. It is used for error detection, ensuring the integrity of the TCP segment.

Urgent Pointer Field
Used in conjunction with one of the TCP control flags to point out particular segments that might be more important than others.

Options Field
Sometimes used for more complicated flow control protocols, but very rare.

Padding
Just a bunch of zeroes to make sure the **Data Payload** begins at the expected location.

Control Flags
1. **URG (urgent)**: A value of one here indicates that the segment is considered urgent and that the urgent pointer field has more data about this.
2. **ACK (acknowledged)**: A value of one in this field means that the acknowledgement number field should be examined.
3. **PSH (push)**: The transmitting device wants the receiving device to push currently-buffered data to the application on the receiving end as soon as possible.
4. **RST (reset)**: One of the sides in a TCP connection hasn't been able to properly recover from a series of missing or malformed segments. Used to abruptly terminate a connection, often due to an error.
5. **SYN (synchronize)**: It's used when first establishing a TCP connection and makes sure the receiving end knows to examine the sequence number field.

6. **FIN (finish)**: When this flag is set to one, it means the transmitting computer doesn't have any more data to send and the connection can be closed.

Socket
The instantiation of an end-point in a potential TCP connection.

Examples of **Socket States**:

LISTEN
A TCP socket is ready and listening for incoming connections.

SYN_SENT
A synchronization request has been sent, but the connection hasn't been established yet.

SYN-RECEIVED
A socket previously in a LISTEN state has received a synchronization request and sent a SYN/ACK back.

ESTABLISHED
The TCP connection is in working order and both sides are free to send each other data.

FIN_WAIT
A FIN has been sent, but the corresponding ACK from the other end hasn't been received yet.

CLOSE_WAIT
The connection has been closed at the TCP layer, but the application that opened the socket hasn't released its hold on the socket yet.

CLOSED
The connection has been fully terminated and no further communication is possible.

—----------

Connection-Oriented Protocol
Establishes a connection, and uses this to ensure that all data has been properly transmitted.

Supplemental Reading for System Ports versus Ephemeral Ports

System Ports versus Ephemeral Ports

Network services are run by listening to specific ports for incoming data requests. A port is a 16-bit number used to direct traffic to a service running on a networked computer. A "service" (or "server") is a program waiting to be asked for data. A "client" is another program that requests this data from the other end of a network connection. This reading explains how the Transmission Control Protocol (TCP) uses ports and sockets to establish a network connection and deliver data between services and clients.

TCP ports and sockets
Ports are used in the Transport Layer of the TCP/IP Five-Layer Network Model. At this layer, the TCP is used to establish a network connection and deliver data. A TCP "segment" is the code that specifies ports used to establish a network connection. It does this on the service side of the connection by telling a specific service to listen for data requests coming into a specific port. Once a TCP segment tells a service to listen for requests through a port, that listening port becomes a "socket." In other words, a socket is an active port used by a service. Once a socket is activated, a client can send and receive data through it.

Three categories of ports
Since a **16-bit number identifies ports**, there can be **65,535** of them. Given the number of ports available, they have been divided into three categories by the **Internet Assigned Numbers Authority (IANA)**: System Ports, User Ports, and Ephemeral Ports.

- **System/"well-known" Ports** are identified as **ports 0 through 1023**. System ports are reserved for common applications like FTP (port 21) and Telnet over TLS/SSL (port 992). *Many still are not assigned.*
    - Note: Modern operating systems do not use system ports for outbound traffic.
- **"Registered"/User Ports** are identified as **ports 1024 through 49151**. Vendors register user ports for their specific server applications. The **IANA** has *officially registered some but not all of them.*
- **Ephemeral Ports (Dynamic or Private Ports)** are identified as **ports 49152 through 65535**. Ephemeral ports are used as temporary ports for private transfers. Only clients use ephemeral ports.

Not all operating systems follow the port recommendations of the IANA, but the IANA registry of assigned port numbers is the most reliable for determining how a specific port is being used. You can access the IANA Service Name and Transport Protocol Port Number Registry here or check out this helpful list of commonly used ports.

How TCP is used to ensure data integrity

The TCP segment that specifies which ports are connected for a network data transfer also carries other information about the data being transferred (along with the requested data). Specifically, the TCP protocol sends acknowledgments between the service and client to show that sent data was received. Then, it uses checksum verification to confirm that the received data matches what was sent.

Port security

Ports allow services to send data to your computer but can also send malware into a client program. Malicious actors might also use port scanning to search for open and unsecured ports or to find weak points in your network security. To protect your network, you should use a firewall to secure your ports and only open sockets as needed.

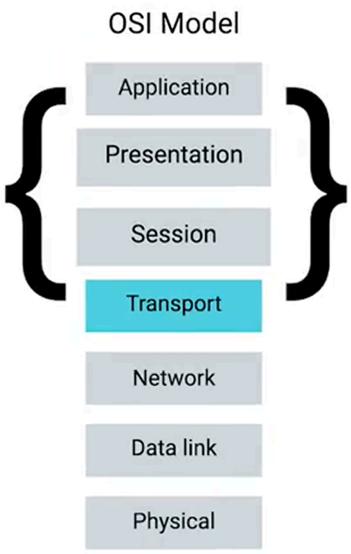
Key takeaways

Network services are run by listening to specific ports for incoming data requests.

- Ports are represented by a single 16-bit number (65535 different port ids)
- Ports are split up by the IANA (Internet Assigned Numbers Authority) into three categories: System Ports (ports 1-1023), User Ports (ports 1024-49151), and Ephemeral (Dynamic) Ports (ports 49152-65535).
- A socket is a port that a TCP segment has activated to listen for data requests.
- Ports allow services to send data to your computer but can also send malware into a client program. It's important to secure your ports.

—----------

The Application Layer and the OSI Model



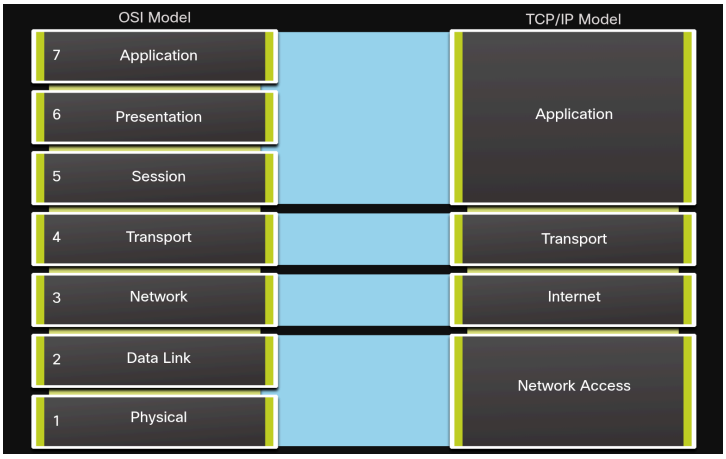
The OSI Model

The OSI model has seven layers and introduces two additional layers **between** our **transport layer** and our **application layer**.

- The **session layer**, the fifth layer in the OSI model. The concept of the session layer is that it's responsible for things like facilitating the communication between actual applications and the transport layer.
    - It's the part of the operating system that takes the application layer data that's been unencapsulated from all the layers below it and hands it off to the next layer in the OSI model, the presentation layer.
    - The layer specifically tasked with establishing, managing, and terminating the communication dialogue or "session" between two applications, thereby orchestrating their interaction and ensuring proper synchronization before handing off to or receiving from the transport layer
- **The presentation layer** is responsible for making sure that the unencapsulated application layer data is actually able to be understood by the application in question. This is the part of an operating system that might handle encryption or compression of data.
    - focuses on data formatting, encryption, and compression to ensure data is understandable

– – Continued – –

Because TCP/IP is the protocol suite in use for internet communications, why do we need to learn the OSI model as well?



The TCP/IP model is a method of visualizing the interactions of the various protocols that make up the TCP/IP protocol suite. It does not describe general functions that are necessary for all networking communications. It describes the networking functions specific to those protocols in use in the TCP/IP protocol suite. For example, at the network access layer, the TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium, nor the method of encoding the signals for transmission. OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

The protocols that make up the TCP/IP protocol suite can be described in terms of the OSI reference model. The functions that occur at the internet layer in the TCP/IP model are contained in the network layer of the OSI Model, as shown in the figure. The transport layer functionality is the same between both models. However, the network access layer and the application layer of the TCP/IP model are further divided in the OSI model to describe discrete functions that must occur at these layers.

Module 3: Networking Services

DNS (Domain Name Service)

DNS generally prefers UDP over TCP.

Name Resolution
The process of using DNS to turn a domain name into an IP address and vice-versa

There are 5x primary types of DNS servers:

1. **Caching name servers**: These store known domain name lookups for a certain amount of time.
2. **Recursive name servers**: Performs full DNS resolution requests.
3. **Root name servers**: Responsible for directing queries toward the appropriate TLD name server.
    - Originally there were 13 total root servers.
    - Better defined as 13 authorities that provide root name lookups as a service.
    - Will respond to a DNS lookup with the TLD name server that should be queried.
    - Responsible for the "root zone".
4. **TLD name servers**: "Top-Level Domain"; represents the top of the hierarchical DNS resolution systems.
    - The .com or .net part of a web address
5. **Authoritative name servers**: Responsible for responding to name resolution requests for specific domains.
    - Responsible for specific DNS zones.

All domain names in the global DNS system have a TTL

TTL (Time to Live)
A value, in seconds, that can be configured by the owner of a domain name for how long a name server is allowed to cache an entry before it should discard it and perform a full resolution again.

Anycast
A technique that's used to route traffic to different destinations depending on factors like location, congestion, or link health.

Resource Record Types

A Record
Used to point to a certain domain name at a certain IPv4 IP address.

AAAA Record
Used to point to a certain domain name at a certain IPv6 IP address.

CNAME Record
Used to redirect traffic from one domain name to another.

MX (Mail exchange) Record
Used in order to deliver email to the correct server.

SRV (Service) Record
Used to define the location of very specific services.

TXT (Text) Record
Originally intended to be used only for associating some descriptive text with a domain name for human consumption.

Round Robin
A concept that involves iterating over a list of items one by one in an orderly fashion.

Anatomy of a Domain Name

TLD (Top Level Domain)
The last part of a domain name, like .com or .net .

Domain
Used to demarcate where control moves from a TLD name server to an authoritative name server.

Sub-Domain

Fully Qualified Domain Name (FQDN)
When all parts of a Domain Name are resolved.

- DNS can support 127 levels of domain in total for a single FQDN.

ICANN
The Internet Corporation for Assigned Names and Numbers

- ICANN is a sister organization to the iana, and together they help define and control both the global IP spaces along with the global DNS system.

DNS Zones
Allows for easier control over multiple levels of a domain.

Zone Files
Simple configuration files that declare all resource records for a particular zone.

Start of Authority (SOA)
Declares the zone and the name of the name server that is authoritative for it.

NS Records
Indicate other name servers that might also be responsible for this zone.

Pointer Record (PTR)
Resolves an IP to a name

Overview of DHCP

Dynamic Host Configuration Protocol (DHCP)
An **application layer** protocol that automates the configuration process of hosts on a network.

Dynamic Allocation
A range of IP addresses is set aside for client devices and one of these IPs is issued to these devices when they request one.

Automatic Allocation
A range of IP addresses is set aside for assignment purposes.

Fixed Allocation
Requires a manually specified list of MAC addresses and their corresponding IPs.

DHCP in Action

DHCP Discovery
The process by which a client configured to use DHCP attempts to get network configuration information. There are 4 steps to the process:

1. The DHCP client sends out a **DHCPDISCOVER** message out onto the network.
    a. Since the machine doesn't have an IP and it doesn't know the IP of the DHCP server, a specially crafted broadcast message is formed instead. DHCP listens on UDP port 67, and DHCP discovery messages are always sent from UDP port 68. The DHCP discover message is encapsulated in a UDP datagram with a destination port of 67 and a source port of 68. This is then encapsulated inside of an IP datagram with a destination IP of 255.255.255.255, and a source IP of 0.0.0.0. This broadcast message would get delivered to every node on the local area network, and if a DHCP server is present, it would receive this message.
2. The response would be sent as a **DHCPOFFER** message
    a. It will contain a destination port of 68, a source port of 67, a destination broadcast IP of 255.255.255.255, and its actual IP as the source. Since the DHCP offer is also a broadcast, it would reach every machine on the network. The original client would recognize that this message was intended for itself. This is because the DHCP offer has the field that specifies the MAC address of the client that sent the DHCP discover message. The client machine would now process this DHCP offer to see what IP is being offered to it. Technically, a DHCP client could reject this offer.
3. The DHCP client would then respond to the DHCPOFFER message with a **DHCPREQUEST** message.
    a. "Yes, I would like to have an IP that you offered to me." Since the IP hasn't been assigned yet, this is again sent from an IP of 0.0.0.0, and to the broadcast IP of 255.255.255.255.
4. Finally, the DHCP server receives the DHCP request message and responds with a **DHCPACK** or DHCP acknowledgment message.
    a. This message is again sent to a broadcast IP of 255.255.255.255, and with a source IP corresponding to the actual IP of the DHCP server.

Basics of NAT

Network Address Translation (NAT)
A technology that allows a gateway, usually a router or firewall, to rewrite the source IP of an outgoing IP datagram while retaining the original IP in order to rewrite it into the response.

IP Masquerading
When a gateway rewrites an IP address to hide the original IP from clients.

1-to-Many NAT
Where a single router hides the IPs of all the local computers, potentially hundreds or thousands.

NAT at the Transport Layer

Port Preservation
A technique where the source port chosen by a client is the same port used by the router.

Port Forwarding
A technique where specific destination ports can be configured to always be delivered to specific nodes.

Supplemental Reading for IPv4 Address Exhaustion

IPv4 Address Exhaustion

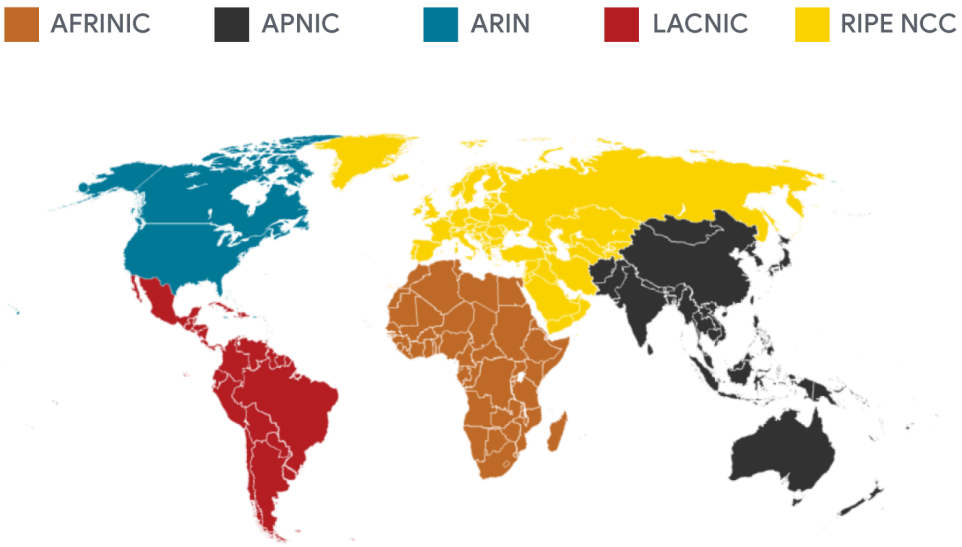
IT professionals are responsible for troubleshooting network connections. If a device cannot connect to the network, the IP address is used as a part of a command line to test if the device is the issue. The Internet Assigned Numbers Authority (IANA) distributes IP addresses, so unique addresses are used when connecting to the internet. Since 1988 IANA has assigned IP addresses, but the internet has expanded drastically, requiring billions of IP addresses. The possible combinations of numbers (4.2 billion) have almost run out. This reading will explain the structure for the distribution of IP addresses and how IPv6 is being used to solve the limited number of IP addresses available.

Regional internet registries (RIRs)

IANA assigns IP address blocks to the five regional internet registries (RIRs). An RIR is an organization that manages internet number resources within a geographical region. IANA is responsible for assigning address blocks to five Regional Internet Registries (RIRs):

- AFRINIC - Africa
- ARIN - USA, Canada, and parts of the Caribbean
- APNIC - Most of Asia, Australia, New Zealand, and Pacific Island nations
- LACNIC - Central America, South America, and the remaining parts of the Caribbean not covered by ARIN
- RIPE - Europe, Russia, Middle East, and portions of Central Asia

Your computer gets its IP address directly from an RIR, not the IANA.



Timeline for IPv4 address exhaustion

On February 3, 2011, IATA assigned the last unallocated /8 of the 4.2 billion possible combinations of IPv4 addresses. In some regions, you use a recycled number as a new IP address due to reaching IP exhaustion. The RIRs exhausted the following blocks by date:

- APNIC reached its final /8 addresses in April 2011.
- RIPE reached its final /8 addresses in September 2012.
- LACNIC reached its final /10 addresses in June 2014.
- ARIN exhausted its list of free IPv4 addresses in September 2015.
- AFRINIC entered IPv4 Exhaustion Phase 2 in January 2020.

IPv6

IPv6 will replace IPv4, using 128-bit addresses. IPv6 provides an identification and location system for computers on networks and routes traffic across the internet. The 128-bit addresses used by IPv6 provide a practically inexhaustible number of addresses. While IPv6 will solve many IPv4 address exhaustion issues, 99% of the devices in use today still use IPv4. IT professionals should be aware of IPv6 as it begins to take effect over the coming years and the structure of IP addresses changes.

Key takeaways

The current system used for IP addresses, IPv4, has exhausted the combinations of numbers possible.

- IPv4 has nearly exhausted the 4.2 billion IP addresses.
- Regional Internet Registries assign IP addresses to devices in their physical area.
- IPv6 provides significantly more IP addresses and will solve the IPv4 address exhaustion issues over time. However, 99% of devices as of today use IPv4 addresses.

Virtual Private Networks
A technology that allows for the extension of a private or local network to hosts that might not work on that same local network.

Proxy Service
A server that acts on behalf of a client in order to access another service.

- Anonymity
- Security
- Content Filtering
- Increased Performance

Reverse Proxy
A service that might appear to be a single server to external clients, but actually represents many servers living behind it.

Module 5: Connecting to the Internet

Dial-Up Modems

Baud Rate
A measurement of how many bits can be passed across a phone line in a second.

T-Carrier Technologies

Originally invented by AT&T in order to transmit multiple phone calls over a single link.

- **T1 (Transmission System 1)**
  - Allowed for up to 24 simultaneous phone calls on a single twisted-pair copper.
  - Up to 1.544 Mb/s

- A **T3** line is 28x T1s multiplexed
  - Up to 44.7736 Mb/s

Digital Subscriber Lines (DSL)

DSLAM (Digital Subscriber Line Access Multiplexers)
Modem devices that establish data connections across long-running phone lines.

- **ADSL (Asymmetric Digital Subscriber Line)**:
  - Feature different speeds for outbound and inbound speeds.
  - Ideal for home users, with high download needs.
- **SDSL (Symmetric Digital Subscriber Line)**:
  - The inbound and outbound speeds are the same.
  - Becoming more common for both home and business.
- **HDSL (High-Bit-Rate Digital Subscriber Line)**:
  - DSL technologies that provision speeds above 1.544 mb/s

Fiber Connections

FttN - Fiber to the Neighborhood

FttB - Fiber to the Building/Business/Basement

FttH - Fiber to the Home

FttP - Fiber to the Premises

ONT (Optical Network Terminator) - Converts data from protocols the fiber network can understand to those that more traditional twisted pair copper can understand.

Supplemental Reading for Broadband Protocols

Broadband Protocols

Broadband communications require a set of instructions, rules, and communication to various network layer protocols to support operation. Point to Point Protocol (PPP) for broadband communications is a set of instructions used to transmit data between two directly connected devices. This reading will cover the definitions, structures, and details of Point to Point Protocol (PPP) and Point to Point Protocol over Ethernet (PPPoE).

Point to Point Protocol (PPP)

Point to Point Protocol (PPP) is a byte-oriented protocol broadly used for high-traffic data transmissions. PPP functions at the data link layer, which transmits data between two devices on the same network. PPP is designed to link devices, so the endpoints do not need to be the same vendor to work.

Configuring PPP

When configuring PPP for the devices on your network, you have the following options:

- **Multilink** connection provides a method for spreading traffic across multiple distinct PPP connections.
- **Compression** increases throughput by reducing the amount of data in the frame.
- **Authentication** occurs when connected devices exchange authentication messages using one of two methods:
    - **Password Authentication Protocol (PAP)** is a password authentication option that is hard to obtain plaintext from if passwords are compromised.
    - **Challenge Handshake Authentication Protocol (CHAP)** is a three-way handshake authentication that periodically confirms the identity of the clients.
- **Error detection** includes Frame Check Sequence (FCS) and looped link detection.
    - **Frame Check Sequence (FCS)** is a number included in the frame calculated over the Address, Control, Protocol, Information, and Padding fields used to determine if there has been data loss during transmission.
    - **Looped link detection** in PPP detects looped links using magic numbers. A magic number is generated randomly at each end of the connection, so when a looped message is received, the device checks the magic number against its own. If the line is looped, the number will match the sender's magic number, and the frame is discarded.

Sub-protocols for PPP

In addition, two sub-protocols for PPP occur on the network layer when the network decides what physical path the information will take. These protocols use the configuration options you set for the endpoints.

- **Network Control Protocol (NCP)** will be used to negotiate optional configuration parameters and facilities for the network layer. There is an NCP for each higher layer protocol used by the PPP.
- **Link Control Protocol (LCP)** initiates and terminates connections automatically for hosts. It automatically configures the interfaces at each end like magic numbers and selects for optional authentication.

Data is sent using PPP in a frame. A frame is a collection of data sent to a receiving point.

PPP Frame

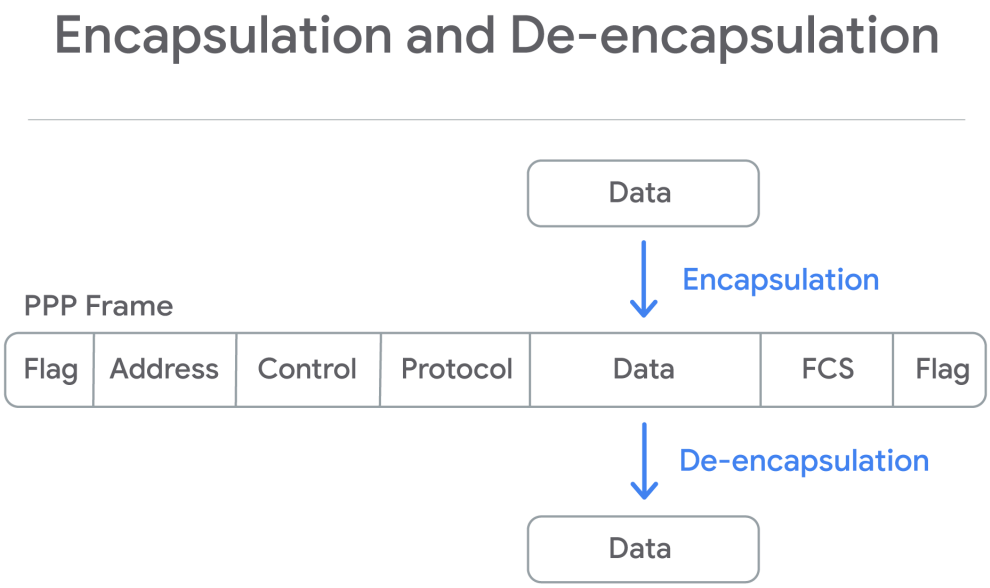
PPP uses the following frame format:

- **Flag** is a single byte and lets the receiver know this is the beginning of the frame. Depending on the encapsulation, there may or may not be a start flag or an end flag.
- **Address** is a single byte, and it contains the broadcast address.
- **Control** is a single byte required for various purposes but also allows a connectionless data link.
- **Protocol** varies from one to three bytes which identify the network protocol of the datagram.
- **Data** is where the information you need to transmit is stored and has a limit of 1500 bytes per frame.
- **Frame check sequence (FCS)** is 2 or 4 bytes and is used to verify data is intact upon receipt at the endpoint.

When the data is packaged in a frame, it undergoes **encapsulation**.

Encapsulation

Encapsulation is the process by which each layer takes data from the previous layer and adds headers and trailers for the next layer to interpret.



These frames are sent to the other endpoint where the process is reversed, which is called De-encapsulation.

PPP can get expensive and hard to manage due to all the direct cables and links required. In this case, you may want to switch to a **multi-access Ethernet solution**. Point to Point Protocol over Ethernet is a protocol made to bridge the gap between directly connected endpoints and other devices.

Point to Point Protocol over Ethernet (PPPoE)

PPPoE is a way of encapsulating PPP frames inside an ethernet frame. PPPoE is a solution for tunneling packets over the DSL connection service provider's IP network and from there to the rest of the Internet. Like PPP, PPPoE provides authentication, encryption, and compression, though it primarily uses **Password Authentication Protocol (PAP)** for authentication.

A common use case is PPPoE using DSL services where a PPPoE modem-router connects to the DSL service or when a PPPoE DSL modem is connected to a PPPoE-only router using an Ethernet cable.

PPP is strictly point-to-point, so frames can only go to the intended destination. PPPoE requires a new step because ethernet connections are multi-access enabled (every node connects to another). This requires an additional step called the discovery stage. The discovery stage establishes a session ID to identify the hardware address. This stage ensures data gets routed to the correct place.

PPPoE is an encapsulation of PPP inside an ethernet frame. PPPoE retains the same architecture, configuration options, and frame data as PPP but with one extra layer of ethernet encapsulation.

Key takeaways
Broadband internet requires several protocols to make sure different connected devices can communicate with each other.

- Point to Point Protocol (PPP) encapsulates data, so any PPP configured devices can communicate without issue.
- Point to Point over Ethernet (PPPoE) is an extra layer of encapsulation for standard PPP frames, to enable data to be sent over ethernet connections.

Supplemental Reading for WAN Protocols

Wan Protocols V2

In this reading, you will continue learning about the various components of Wide Area Networks (WANs). WAN configurations are important for IT Support professionals to understand when working with the geographically dispersed networks of large organizations. WANs can be connected through the Internet with connections provided by Internet Service Providers (ISPs) in each locale. Regional WANs can also be formed by connecting multiple Local Area Network (LAN) sites using equipment and cables leased from a regional ISP. Security for WANs across the public Internet can be configured through Virtual Private Networks (VPNs).

Physical versus software-based WANs

- **WAN router**: Hardware devices that act as intermediate systems to route data amongst the LAN member groups of a WAN (also called WAN endpoints) using a private connection. WAN routers may also be called border routers or edge routers. These routers facilitate an organization's access to a carrier network. WAN routers have a digital modem interface for the WAN, which works at the **OSI link layer**, and an Ethernet interface for the LAN.
- **Software-Defined WAN (SD-WAN)**: Software developed to address the unique needs of cloud-based WAN environments. SD-WANs can be used alone or in conjunction with a traditional WAN. SD-WANs simplify how WANs are implemented, managed, and maintained. An organization's overall cost to operate a cloud-based SD-WAN is significantly less than the overall cost of equipping and maintaining a traditional WAN. One of the ways that SD-WANs help reduce operational costs is by replacing the need for expensive lines leased from an ISP by linking regional LANs together to build a WAN.

WAN optimization

There are multiple techniques available to optimize network traffic and data storage on a WAN:

- **Compression**: Reducing file sizes to improve network traffic efficiency. There are many compression algorithms available for text, image, video, etc. The sender and the receiver will need apps that offer the same compression/decompression algorithm to encode and decode the compressed files.
- **Deduplication**: Prevents files from being stored multiple times within a network to avoid wasting hard drive space. One copy of the file is kept in a central location. All other "copies" are actually file pointers to the single copy of the file. This saves valuable hard drive space, makes performing data backups more efficient, and reduces the amount of time needed to recover from data loss disasters.
- **Protocol Optimization**: Improves the efficiency of networking protocols for applications that need higher bandwidth and low latency.
- **Local Caching**: Storing local copies of network and internet files on a user's computer to reduce the need to resend the same information across the network every time the file is accessed. Some WAN optimization products can cache shared files at one physical LAN location when groups of employees at the location tend to request the same set of files frequently. Traffic Shaping: Optimizing network performance by controlling the flow of network traffic. Three techniques are commonly used in traffic shaping:
    - **bandwidth throttling** - controlling network traffic volume during peak use times
    - **rate limiting** - capping maximum data rates/speeds
    - **use of complex algorithms** - classifying and prioritizing data to give preference to more important traffic (e.g., an organization might want to prioritize private LAN-to-LAN traffic within the organization's WAN and give a lower priority to employees accessing the public Internet).

– – Continued – –

WAN Protocols

WAN Internet Protocols are used in conjunction with WAN routers to perform the task of distinguishing between a private LAN and the related public WAN. Several WAN protocols have been developed over the decades for this task, as well as other purposes, including:

- **Packet switching**: A method of data transmission. In packet switching, messages are broken into multiple packets. Each packet contains a header that includes information on how to reassemble the packets, as well as the intended destination of the packets. As a measure to prevent data corruption, the packets are triplicated. The triplicated packets are sent separately over optimal routes through the internet. Then, once the packets reach their destination, they are reassembled. The triplicate copies are compared with one another to detect and correct any data corruption that occurred during transmission (at least two of the three copies should match). If the data cannot be reassembled and/or data corruption is evident in all three copies, the destination will make a request to the origin to resend the packet.
- **Frame relay**: Also a method of data transmission. Frame relay is an older technology originally designed for use on **Integrated Services Digital Network (ISDN)** lines. However, the technology is now used in other network interfaces. Frame relays are used to transmit data between endpoints of a WAN through a packet switching method that works at the **OSI data link and physical layers**. A fast data communications network, called a **Frame Relay Network**, is used to transport data packets in frames. The reliability of Frame Relay Networks minimizes the need for error checking. The frames include routing address information for the destination.
    - **Permanent Virtual Circuits (PVCs)** - Used for long-term data connections. Stays open even when data is not being transmitted.
    - **Switched Virtual Circuits (SVCs)** - Used in temporary session connections for sporadic communications.
- **Asynchronous Transfer Mode (ATM)**: ATM is an older technology that encodes data using asynchronous time-division multiplexing. The encoded data is packaged into small, fixed-sized cells. ATM can send the cells over a long distance, which makes it useful for WAN communications. ATMs use routers as end-points between ATM networks and other networks. ATM technology has been replaced for the most part by **Internet Protocol (IP)** technologies.
- **High Level Data Control (HLDC)**: An encapsulation or data link protocol that delivers data frames through a network. The frames include multiple fields that can hold information about start and end flags, controls, Frame Check Sequence (FCS), and protocol used. HLDC was developed to use multiple protocols to replace Synchronous Data Link Control (SLDC), which used only one protocol. HLDC includes error correction, flow control, and data transmission through polling. HLDC has three modes to define the relationship between two devices, or nodes, during communications:
    - **Normal Response Mode (NRM)** - Primary node must give permission to the secondary node to transmit.
    - **Asynchronous Response Mode (ARM)** - Primary node allows the secondary node to initiate communication.
    - **Asynchronous Balanced Mode (ABM)** - Both nodes can act as either the primary or secondary nodes. They can each initiate communications without permission.
- **Packet over Synchronous Optical Network (SONET)** or **Synchronous Digital Hierarchy (SDH)**: A communication protocol used for WAN transport. The SONET or SDH communication protocols define how point-to-point links communicate over fiber optics cables.
- **Multiprotocol Label Switching (MPLS)**: A technique for optimizing network routing. MPLS replaces inefficient table lookups for long network addresses with short path labels. These labels direct data from node to node.

Introduction to Wireless Networking Technologies

The most common specifications for how wireless networking devices should communicate are defined by the IEEE 802.11 Standards.

- In North America, FM radio transmissions operate between 88 and 108 MHz.
- Wi-Fi networks operate on the 2.4, 5 and 6 GHz bands.

Frame Control Field:
16-bits long and contains a number of subfields that are used to describe how the frame itself should be processed.

Duration/ID:
Specifies how long the total frame is, so the receiver knows how long it should expect to have to listen to this transmission.

4 Address Fields, each 6 bytes long:

- **Source Address Field**: Represents the MAC address of the sending device.
- **Intended destination** on the network.
- **Receiving address**: The MAC address of the access point that should receive the frame.
- **Transmitter address**: The MAC address of whatever has just transmitted the frame.

Sequence Control Field
16-bits long and mainly contains a sequence number used to keep track of the ordering of frames.

Wireless Access Point
A device that bridges the wireless and wired portions of a network.

Data Payload:
All of the data of the protocols further up the stack.

Frame Check Sequence Field:
Contains a checksum for a cyclical redundancy check.

Wi-Fi 6

Wi-Fi 6, formerly known as 802.11ax, is one of the largest leaps in Wi-Fi technology since its introduction. This reading will introduce you to the benefits and technology used in Wi-Fi 6.

Benefits of Wi-Fi 6

The Wi-Fi 6 network protocol is faster and more efficient for networks with a larger number of connected devices.

Key benefits of Wi-Fi 6 technology include:

- **Higher data rates**: Band splitting or increased client group sizes allow for uploading and downloading greater amounts of data.
- **Increased band capacity**: Band utilization increased from 80mHz to 160mHz, creating a faster connection from the router to connected devices.
- **Better performance**: The input/output streams are doubled from the 4 by 4 allowed by Wi-Fi 5, to 8 by 8 in Wi-Fi 6, allowing more clients to be grouped.
- **Improved power efficiency**: Devices only connect to the network when sending or receiving data, increasing battery life.

Capabilities of Wi-Fi 6

Wi-Fi 6 technology improves functionality and connectivity.

- **Channel sharing** for better efficiency and shortens the time it takes to send data once a user gives the send command.
- **Target Wake Time (TWT)** improves the network speed and increases battery life by allowing battery-powered devices to sleep when not in use.
- **Multi-user MIMO (Multiple Input, Multiple Output)** wireless technology allows more data to be transferred simultaneously. This ability increases capacity and efficiency in high bandwidth applications like voice calls or video streaming.
- **160 MHz channel utilization** gives more space for transmitting data and increases bandwidth capability.
- **1024 Quadrature amplitude modulation** combines two signals into a single channel, so more data is encoded.
- **Orthogonal Frequency Division Multiple Access (OFDMA)** allows for bandwidth splitting, which is assigned dynamically by the access point to separate devices.
- **Transmit beamforming** is a technique that sends signals that allow for more efficient higher data rates by targeting each connected device.

Wi-Fi 6E extends Wi-Fi 6 into 6 GHz

Wi-Fi 6E is an additional certification for Wi-Fi 6 that has all of the features of Wi-Fi 6 but adds a third 6 GHz band.

Wi-Fi 6E has more channels to use to broadcast, including **14 more 80MHz channels** and **seven more 160MHz channels**. The additional channels allow networks with Wi-Fi 6E for better performance even when streaming high-definition video or using virtual reality devices.

Key takeaways

- Wi-Fi technology will continue to change as the needs of companies and users change. Wi-Fi 6 improves the quality of networks with faster speeds and energy-saving technology.
- Wi-Fi 6 uses technologies like channel sharing, Target Wake Time, Multi-user MIMO, channel utilization, amplitude modulation, OFDMA, and transmit beamforming to increase the quality of a Wi-Fi network.
- Wi-Fi 6E is an additional certification of Wi-Fi 6 that has even faster speeds and stronger performance.

Resource for more information

For more information about Wi-Fi 6, read this article by the Wi-Fi Alliance: Wi-Fi CERTIFIED 6.

Supplemental Reading for Alphabet Soup

Alphabet Soup: Wi-Fi Standards

As an IT Support specialist, you may be responsible for supporting wireless technologies. In this reading, you will learn about the 802.11 Wireless-Fidelity (Wi-Fi) standards, including the alphabet-coded updates: a, b, g, n, ac, ad, af, ah, ax, ay, and az. You will also learn about the differences between the 2.4 gigahertz (GHz) and 5 GHz Wi-Fi frequencies.

You may already be familiar with selecting from the 2.4 GHz and 5 GHz frequency options on your home Wi-Fi router. Perhaps you also noticed the 802.11 specifications on the packaging for your Wi-Fi router when you purchased it. Have you wondered what these numbers and letters mean?

Wi-Fi 2.4 GHz and 5 GHz frequencies

There are multiple wireless technologies available today that use various frequencies ranging from radio to microwave bands. These wireless technologies include Wi-Fi, Z-Wave, ZigBee, Thread, Bluetooth, and Near Field Communication (NFC). Radio and microwave frequency bands each have specific ranges that are divided into channels. Wi-Fi uses the 2.4 GHz and 5 GHz microwave radio frequency band ranges for sending and receiving data. Some Wi-Fi routers use multiple channels within each range to avoid signal interference and to load-balance network traffic. Wi-Fi is commonly used for wireless local area networks (WLANs).

The following is a comparison of the performance characteristics between the 2.4 GHz and 5 GHz frequency bands:

2.4 GHz

- Advantages:
  - Has the longest signal range from 150 feet (45 meters) indoors to 300 feet (92 meters) outdoors.
  - Can pass through walls and other solid objects.
- Disadvantages:
  - The long signal range also increases the chances of Wi-Fi traffic being intercepted by cybercriminals.
  - Includes a limited number of channels. Can range from 11 to 14 channels, depending on regulations in the country of use.
  - Can experience network traffic congestion and interference with other Wi-Fi networks and wireless technologies, such as BlueTooth, that overlap the 2.4 GHz frequency bands.
  - Microwave ovens also work in the 2.4 GHz frequency band and can cause Wi-Fi interference.
  - Under specific conditions, the maximum achievable data rate is 600 Mbps.

5 GHz

- Advantages:
  - Includes significantly more channels than 2.4 GHz.
  - Experiences fewer interference problems and less wireless network traffic congestion than 2.4 GHz.
  - Can achieve over 2 Gbps data transfer speeds under specific conditions.
- Disadvantages:
  - The wireless range is limited to 50 feet (12 meters) indoors and 100 feet (30 meters) outdoors.
  - Does not penetrate walls and other solid objects as well as 2.4 GHz.

IEEE 802.11 standards

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) ratified the first 802.11 standard for wireless fidelity (later branded as Wi-Fi). The standard was first published for use by computer device manufacturers to use as a common protocol for wireless communications. The IEEE has amended the 802.11 specifications multiple times over the years with updates and additional enhancements to 802.11 Wi-Fi. The IEEE names each new amendment with one or two letters appended to 802.11 (e.g., 802.11n or 802.11ax). The IEEE plans to continue updating the 802.11 specifications until a new technology replaces Wi-Fi.

The majority of wireless networks use the IEEE 802.11 standards for Wi-Fi. Wi-Fi networks include client devices (e.g., laptops, tablets, smartphones, IoT devices, etc.) that are configured to connect to wireless access points. This configuration is referred to as “infrastructure mode”. Access points can serve both wireless and wired network traffic. For wired traffic, the access point works as a bridge between wireless devices and a wired network. The access point connects to an Ethernet switch through a wired Ethernet cable.

The various amended 802.11 specifications use the same fundamental data link protocol. However, some characteristics may vary at the OSI physical layer, including:

- signal ranges
- modulation techniques
- transmission bit rates
- frequency bands
- channels

Note that countries around the world may impose different regulations on channel usage, power limitations, and Wi-Fi ranges. A technology called dynamic frequency selection (DFS) is also required to prevent 5 GHz Wi-Fi signals from interfering with local radar and satellite communications.

– – Continued – –

A comparison of the frequencies, maximum data rates, and maximum signal ranges for each 802.11 update over the years is detailed below:

Year Ratified	IEEE 802.11 Standard	Marketing Name	Frequency	Maximum Range Indoors - Outdoors	Maximum Data Rate
1997	-	Wi-Fi 0	2.4 GHz	20-100 meters	2 Mbps
1999	a	Wi-Fi 2	5 GHz	35-120 meters	54 Mbps
1999	b	Wi-Fi 1	2.4 GHz	40-140 meters	11 Mbps
2003	g	Wi-Fi 3	2.4 GHz	40-140 meters	54 Mbps
2009	n	Wi-Fi 4	2.4 & 5 GHz	70-250 meters	600 Mbps
2015	ac wave 2	Wi-Fi 5	5 GHz	80-120 meters	6.9 Gbps
2019	ax	Wi-Fi 6	2.4 & 5 GHz	50-300 meters	10 Gbps
2021	ax	Wi-Fi 6e	6 GHz	Varies	10 Gbps
2024	be	Wi-Fi 7	6 GHz	TBD	46 Gbps

IEEE 802.11 major updates list:

- **802.11a (1999) - Wi-Fi 2**
  - Designed for 5 GHz frequency band only
  - Offered a maximum data rate of 54 Mbps
  - Offered a maximum signal range of 400 feet (120 m)
  - Defined 23 non-overlapping channels at 20 MHz wide
- **802.11b (1999) - Wi-Fi 1**
  - Designed for 2.4 GHz frequency band only
  - Offered a maximum data rate of 11 Mbps
  - Offered a maximum signal range of 450 feet (140 m)
  - Defined 14 overlapping channels (frequent cause of interference)
- **802.11g (2003) update to 802.11b - Wi-Fi 3**
  - Improved 2.4 GHz frequency band only
  - Increased the maximum data rate to 54 Mbps
- **802.11n (2009) bandwidth increase - Wi-Fi 4**
  - Improved both 2.4 GHz and 5 GHz frequency bands
  - Access points could offer “dual-band” support with each band implemented by a separate radio.
  - Increased bandwidth and reliability with “multiple input multiple output" (MIMO) technology.
  - Allowed “channel bonding” for 5 GHz (two adjacent channels could be combined).
  - Increased the maximum data rate to 72 Mbps per stream and 150 Mbps per stream for bonded channels. With specific configurations, the maximum data rate could be as high as 600 Mbps.
  - Increased maximum signal range of 825 feet (250 m)
- **802.11ac (2014) and Wave 2 (2015) bandwidth increases - Wi-Fi 5**
  - Improved the 5 GHz frequency band only, though access points could still offer dual band support for older 2.4 GHz specifications.
  - Access points could offer triband support (one 2.4 GHz and two 5 GHz radios).
  - Supported wider bonded channels at 80 and 160 MHz.
  - Allowed up to eight streams with each 80 MHz channel.
  - Increased maximum data rates to 1 Gbps and could be as high as 2.2 Gbps for specific configurations. Wave 2 increased the maximum data rate to 6.9 Gbps.
  - Increased sent data transmissions to up to 4 clients at the same time. This was achieved by allowing access points to use multiple antennas through downlink multiuser MIMO (DL MU-MIMO) technology.
- **802.11ax (2019) bandwidth increases - Wi-Fi 6**
  - Improved data stream rates to 600 Mbps per 80 MHz channel, with combined data rates of over 1 Gbps for the 2.4 GHz frequency and 4.8 Gbps for the 5 GHz frequency.
  - Increased sent data transmissions to up to 8 clients at the same time with downlink MU-MIMO.
  - Added support for full-duplex MU-MIMO to receive uplink data from multiple client devices.
  - Added support for “orthogonal frequency division multiple access” (OFDMA), which works with MU-MIMO to sustain high data rates during periods of high client device traffic.
  - Requires all client devices to use WPA3 security protocols.
- **Wi-Fi 6e (2020) bandwidth increases**
  - Added support for a new 6 GHz frequency band, which has a combined maximum data rate speed of 10 Gbps (shared by multiple devices).
  - Added new channels to reduce interference.
  - Improved frequency space for 80 and 160 MHz channels.

Resources for more information

For more information about Wi-Fi standards, please visit:

- Official IEEE 802.11 Working Group Project Timelines - An IEEE published table detailing each update to the 802.11 standards.

Supplemental Reading for IoT Data Transfer Protocols

IoT Data Transfer Protocols

In this reading, you will learn how Internet of Things (IoT) devices send and receive data across networks. As an IT Support specialist, you may need to support data collection from IoT devices. For example, you may work for a company that uses an array of IoT sensors in a manufacturing setting to help with the remote monitoring and proactive maintenance of industrial machines. You may need to manage the software applications and data transfer protocols that support automated and human interaction with the IoT devices and the data they collect.

Data protocol models used with IoT

There are two common data protocol models to illustrate how low-power IoT devices share data:

- **Request/Response model**: Often used in distributed systems where the communication flow between servers and clients consists of requests and responses for data. Examples include HTTP and CoAP (described in the "IoT data protocols at the application layer" section below)
- **Publish/Subscribe model**: A framework for message exchanges between publishers (hosts) and subscribers (clients) that are routed through a broker. Subscribers can sign up to a channel to receive notices through the broker when the publisher releases new messages. Examples: MQTT and AMQP (described in the "IoT data protocols at the application layer" section below).

IoT data protocols at the application layer

IoT devices can collect **environmental data around their physical location** (e.g., temperature), **equipment data** (e.g., maintenance status), and **metered data** (e.g., electricity usage). Data protocols are needed to transfer and format the data for use by applications that interface with either humans or automated systems. IoT devices can be configured to use various data transfer and formatting protocols at the **OSI application/software layer** of communication.

Most IoT devices can use at least one of the following data transfer protocols:

- **HyperText Transfer Protocol / Secure (HTTP/HTTPS)**: HTTP and HTTPS are the most widely used information transfer protocols across the World Wide Web (WWW). The protocols define how information is formatted and transmitted. HTTP/HTTPS uses ASCII formatting, has a header size of 8 bytes, and is designed for transmitting documents. HTTP/HTTPS use either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) for sending information across the internet. HTTP/HTTPS uses the request/response model. When a website address is entered into a browser, HTTP/HTTPS sends a request to the site's web server, which then returns an HTTP/HTTPS formatted response to the browser. The protocols use ports 80 or 8080 and data security is provided on the HTTPS version of the protocol. HTTP is supported by Google Cloud IoT Core for device-to-cloud communication.
- **Machine-to-Machine (M2M) Communication Protocols**: A set of direct communication methods for low-power devices, machines, and systems. There are three primary architectural and protocol groups in M2M electronic communications:
    - **Representational State Transfer (REST)**: An architectural style for communication amongst web accessible systems.
    - **Service-oriented Architectures (SOA)**: An architecture for data exchanges in industrial automation systems.
    - **Message Oriented Protocols**: A protocol for asynchronous data transfers for distributed systems.
- **Message Queue Telemetry Transport (MQTT)**: An IoT data-centric interaction protocol for M2M that uses a simple publish-subscribe model. MQTT supports Quality of Service (QoS), uses TCP for sending information, and utilizes Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for security. MQTT using binary format and **2-byte header sizes** for efficient messaging. MQTT is supported by Google Cloud IoT Core for device to cloud communication.
- **Constrained Application Protocol (CoAP)**: A web transfer protocol for IoT constrained nodes and networks designed for M2M applications. CoAP is used for IoT applications like building automation and smart energy management. CoAP is very similar to HTTP: both are based on the REST model and both place resources on a server that is accessible to clients via a URL.
- **Advanced Message Queuing Protocol (AMQP)**: An open standard for messaging amongst applications in different organizations and/or platforms. Its purpose is to remove vendor lock-in for app communication. In addition to interoperability, AMQP also offers reliability and security.
- **Extensible Messaging and Presence Protocol (XMPP)**: A decentralized, open standard for chat, messaging, video and voice calls, collaboration tools, and more. Built upon Jabber, XMPP offers a proven communication technology that is extensible, flexible, and diverse.

- **Data Distribution Service (DDS)**: An API standard and middleware protocol from the Object Management Group. Middleware exists in the OSI applications layer, between software and the operating system. DDS uses the publish-subscribe communications model. DDS is also data-centric, provides low-latency data connectivity, and helps the devices in an IoT ecosystem share data more efficiently. DDS is reliable, scalable, and provides control of QoS parameters, including bandwidth and resource limits.

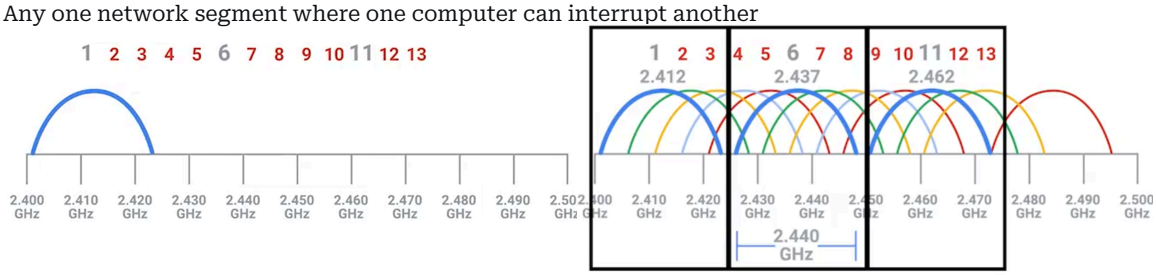
Wireless Network Configurations.

Mesh Networks: Utilizing multiple connected wireless access points to increase performance and range of a SOHO.
Ad-hoc Networks: No real supporting network infrastructure.
WLANS (Wireless LANs): Consists of one or more Access Points that act as bridges between the wireless and wired internet.

Wireless Channels

Individual, smaller sections of the overall frequency band used by a wireless network.

Collision Domain
Any one network segment where one computer can interrupt another



For example: Dealing with an 802.11B network.

Channel 1 operates at **2412MHz**.
But since the channel width is 22 MHz, the signal really lives between **2401MHz** and **2423MHz**.

Channels 1, 6, and 11 are the optimal channels within the 2.4GHz range because they don't overlap with each other.

Wireless Security

WEP (Wired Equivalent Privacy)

An encryption technology that provides a very low level of privacy.
- Very weak encryption.
- Only uses 40 bits for its encryption keys, which can be cracked in a few moments

WPA

- Uses a 128-bit key

WPA2

- Uses a 256-bit key

WPA3

- Discussed below

MAC filtering

When the user configures their access points to only allow for connections from a specific set of MAC addresses belonging to devices you trust.

Protocols & Encryption

WPA3 Protocols & Encryption

Protocols and encryption are vital components in cybersecurity. Network security continues to evolve along with technological innovations and ever-increasing computing power. You have learned about WPA2 and how it improved the security of the **Wi-Fi Protected Access (WPA) protocol**. In this reading, you will explore **WPA3**, the third iteration of WPA wireless security. You will also learn about various internet connectivity technologies, as well as the basics of wireless and cellular networking.

WPA3 is built upon the WPA2 protocol and is intended to replace WPA2. The WPA3 protocol introduces new features and methods to repair the security weaknesses of WPA2. The benefits of this advancement in Wi-Fi security include:

- Simplified wireless security
- Stronger authentication
- Powerful encryption
- Stable business continuity
- Enhanced security methods
- Replacement for legacy protocols
- Protected Management Frames (PMF) requirement for enterprise networks

WPA3 offers two versions, a personal and an enterprise version.

WPA3-Personal

WPA3-Personal is intended for individual users and personal/home Wi-Fi networks. This protocol addresses common cybersecurity weaknesses that affect consumers' wireless devices. It also simplifies Wi-Fi security for users.

The improvements to WPA3-Personal include:

- **Natural password selection**: Gives users the ability to set passwords that are easier for the user to remember.
- **Increased ease of use**: Users do not need to change the way they connect to Wi-Fi to benefit from WPA3's improved security.
- **Forward secrecy**: If a password is stolen, WPA3 can continue to protect data that is transmitted.
- **Simultaneous Authentication of Equals (SAE)**: WPA3-Personal improves upon the WPA2-Personal Pre-Shared Key (PSK) handshake protocol. SAE uses PSK to generate a Pairwise Master Key (PMK). The PMK uses password-based authentication and is shared between a Wi-Fi access point and a wireless device. The pair use a complex, multi-stage process for proving to one another that they each possess the PMK. This complex handshake makes it extremely difficult for cybercriminals to intercept packets in order to extract an identifiable authentication key. If the SAE transaction is successful, the wireless device will pass the authentication stage and gain access to the secured Wi-Fi network.

The SAE authentication **also reduces the probability of successful dictionary and brute force attacks**, in which cybercriminals try to crack short, weak, and commonly used passwords. Additionally, SAE corrects a weakness exploited by cybercriminals who could perform **key reinstallation attacks (KRACKs)** when in close proximity to a Wi-Fi user. This type of attack could decrypt data and expose passwords, credit card information, photos, chats, emails, and more.

– – Continued – –

WPA3-Enterprise

WPA3-Enterprise is intended for business networks with multiple users. This protocol addresses the WPA2-Enterprise weaknesses that cybercriminals have been able to exploit. In addition to the WPA3-Personal SAE improvements, the WPA3-Enterprise security improvements and options include:

- **Galois/Counter Mode Protocol (GCMP-256)**: The Advanced Encryption Standard (AES) with GCMP-256-bit encryption replaces the WPA2 128-bit AES-Counter Mode Protocol (CCMP) Cipher Block Chaining Message Authentication Code (CBC-MAC). **GCMP provides data integrity and confidentiality.** The GCMP-256-bit encryption strength takes significantly more computing power for cybercriminals to crack than 128-bit encryption. The average person would not have access to that level of computing power. GCMP-256-bit encryption provides a stronger security protocol and makes it harder for cybercriminals to perform Meddler-in-the-Middle attacks.
- **Opportunistic Wireless Encryption (OWE)**: OWE improves upon the WPA2 wireless encryption standard of 802.1x Open Authentication and Extensible Authentication Protocol (EAP). In WPA2, EAP required additional support to help it encrypt and authenticate login credentials. In the WPA3 protocol, OWE replaces EAP with a solution that encrypts and authenticates all wireless traffic. It also replaces Wi-Fi passwords by assigning a unique key to each device that has permission to access the network. This technology repairs a weakness Wi-Fi users experience in open networks, which are often found in restaurants, coffee shops, hotels, airports, malls, and more.
- **Wi-Fi Device Provisioning Protocol (DPP)**: DPP improves upon the WPA2 Wi-Fi Protected Setup (WPS) encryption technology between wireless devices and routers. WPA3's DPP uses QR codes or NFC tags to grant passwordless Wi-Fi access to wireless devices.
- **384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA)**: HMAC creates hash code from a secret key. This hash code is sent with each message passed between a Wi-Fi access point and a user's device. The hash code from the origin of the message is compared to the hash code from the receiver of the message to determine if the hash codes match. A discrepancy between the two hashes would indicate that the message was compromised or corrupted during transmission.
- **Elliptic Curve Diffie-Hellman Exchange (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA)**: In WPA3, key management and authentication use the ECDHE protocol and ECDSA encryption for faster performance. The protocol is supported by most browsers. This key management technology replaces the WPA2 4-way handshake.

Key takeaways

As the tech industry develops more powerful computers, cybercriminals will use them to crack older encryption standards. The need to create more complex encryption algorithms will always be present in order to stay ahead of the evolving tools used by cybercriminals.

For WPA3-Personal, some of the new features include:

- Natural password selection
- Increased ease of use
- Forward secrecy
- Simultaneous Authentication of Equals (SAE)

For WPA3-Enterprise, some of the new features include:

- Galois/Counter Mode Protocol (GCMP-256)
- Opportunistic Wireless Encryption (OWE)
- Wi-Fi Device Provisioning Protocol (DPP)
- 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA)
- Elliptic Curve Diffie-Hellman Exchange (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA)

Supplemental Reading for Mobile Device Networks

Wireless Network Protocols for IoT

In this reading, you will learn how Internet of Things (IoT) devices connect to wireless networks. As an IT Support specialist, you may need to support wireless IoT devices in a networked environment. For example, you may have a client who needs to install a smart, wireless security system for their home or office. The client might need assistance with connecting the security system to a private network for onsite monitoring and/or to the internet for remote monitoring. Understanding the properties of wireless IoT networks will help you select appropriate network protocols for various IoT applications.

IoT wireless network protocols at the physical layer

IoT devices can use both wired and wireless methods to connect to the Internet. For wireless connections, there are multiple network protocols that manufacturers configure IoT devices to use. Some of these network protocols support global internet connectivity, while others are intended for short-distance Personal Area Networks (PANs). Network protocols connect at the **OSI physical layer.**

Most IoT devices can use at least one of the following network protocols:

- **Wireless-Fidelity (Wi-Fi)**: Wi-Fi is the more familiar brand name for the IEEE 802.11 standard for wireless networks. Wi-Fi is the most common wireless protocol across the world, with billions of devices capable of using Wi-Fi, including many IoT devices. Wi-Fi is a great option when needing to integrate IoT devices into an existing IP network that is connected to the internet. Wi-Fi 6 can support up to 500 Mbps data transfer speeds, for fast performance with large amounts of data. IoT networks often include a hub or a control system that uses Wi-Fi to facilitate wireless networking.

  As you have learned previously, Wi-Fi networks communicate on radio frequencies 2.4 GHz and 5 GHz. The 2.4 GHz frequency extends to 150 feet (45 meters) indoors and 300 feet (92 meters) outdoors. However, the 2.4 GHz frequency can experience congestion due to a limited number of channels. Plus, 2.4 GHz is more likely to experience interference from other nearby devices that use the same frequency, like microwaves. The 5 GHz frequency provides a stronger signal than 2.4 GHz and has more channels to handle more traffic. The 5 GHz drawback is that its range is limited to 50 feet (12 meters) indoors and 100 feet (30.6 meters) outdoors.

- **IEEE 802.15.4**: An inexpensive, low-power wireless access technology intended for IoT devices that operate on battery power. IEEE 802.15.4 uses the 2.4 GHz or lower radio band frequencies. IEEE 802.15.4 is normally used for **low-rate wireless personal area networks (LR-WPANs)** and uses a **128-bit encryption**. Examples of IoT technologies that use IEEE 802.15.4 network connections include:
  - **ZigBee**: An LR-WPAN intended for smart home use. However, ZigBee has also been adopted globally for commercial IoT products. ZigBee includes a universal language that facilitates the interoperability of smart objects through a self-healing mesh network. **ZigBee LR-WPAN networks can be accessed through Wi-Fi or Bluetooth.**
- **Thread**: A low-latency wireless mesh networking protocol based on IPv6 addressing and existing open standards and technologies. These characteristics make thread networks compatible with a broad spectrum of IoT ecosystems. Thread devices do not use proprietary gateways or translators, making them inexpensive and easier to implement and maintain than other wireless technologies. **Thread is used by the Google Nest Hub Max.**
- **Z-Wave**: An interoperable, wireless mesh protocol (described below) that is based on low powered radio frequency (RF) communications. The **Z-Wave protocol uses an RF signal on the 908.2MHz frequency band and extends 330 feet.** Z-Wave allows users to control and monitor IoT smart devices. *Z-Wave is inexpensive, reliable, and simple to use*. The Z-wave protocol supports a closed network for security purposes. Over 3300 types and models of home and business IoT devices are certified to use Z-Wave technology, with more than 100 million devices in use worldwide.
- **Wireless mesh network (WMN)**: Mesh networks are used by many popular wireless IoT network protocols, like Zigbee and Z-Wave, for device communication. Wireless mesh networks use less power than other wireless connectivity options. Wireless mesh is a decentralized network of connected wireless access points (WAP), also called nodes. Each WAP node forwards data to the next node in the network until the data reaches its destination. This network design is "self-healing," meaning the network can recover on its own when a node fails. The other nodes will reroute data to exclude the failed node. Wireless mesh is a good option for high reliability and low power consumption, which is better for battery powered IoT devices. Wireless mesh networks can be configured to be full or partial mesh:
  - **Full mesh network**: Every node can communicate with all of the other nodes in the network.
  - **Partial mesh network**: Nodes can only communicate with nearby nodes.
- **Bluetooth**: Bluetooth is a widely used wireless network that operates at a 2.45 GHz frequency band and facilitates up to **3 Mbps connections** among computing and IoT devices. Bluetooth has a range of **up to 100 feet (30.6 meters)** and can accommodate multiple paired connections. It is a good choice for creating a short distance wireless connection between Bluetooth enabled devices. Bluetooth is often used by computing devices to manage, configure, control, and/or collect small amounts of data from one or more close range IoT devices. For example, Bluetooth may be used to control smart home lighting or thermostat IoT devices from a smartphone.

- **Near-Field Communication (NFC)**: NFC is a short-range, low data, wireless communication protocol that operates on the 13.56 MHz radio frequency. NFC technology requires a physical chip (or tag) to be embedded in the IoT device. NFC chips can be found in credit and debit cards, ID badges, passports, wallet apps on smartphones (like Google Pay), and more. A contactless NFC scanner, like a Point-of-Sale (PoS) device, is used to read the chip. This scanner communication connection often requires the IoT device to be within 2 inches (6 cm) of the scanner, but some NFC chips have an 8 inch (20 cm) range. This short-distance range helps to limit wireless network security threats. However, criminals can carry a portable NFC scanner into a crowded area to pick up NFC chip data from items like credit cards stored inside purses and wallets. To protect against this type of data theft, the cards should be placed inside special NFC/RFID sleeves that make the chips unreadable until they are removed from the sleeves. NFC technology may also be used in the pairing process for Bluetooth connections.
- **Long Range Wide Area Network (LoRaWan)**: LoRaWan is an open source networking protocol designed to connect battery powered, wireless IoT devices to the Internet for widely dispersed networks.

Module 6: Troubleshooting and the Future of Networking

Introduction to Troubleshooting and the Future of Networking

Error Detection
The ability for a protocol or program to determine that something went wrong.

Error Recovery
The ability for a protocol or program to attempt to fix it.

Ping: Internet Control Message Protocol

ICMP (Internet Control Message Protocol)
Mainly used by a router or remote host to communicate why a transmission has failed back to the origin of the transmission.

Type Field
8-bits long, specifies what type of message is being delivered.

Code Field
Indicates a more specific reason for the message than just the type.

Checksum
16-bit

Rest of Header
32-bit field, optionally used by some of the specific types and codes to send more data.

Data Section
The payload for an ICMP packet exists entirely so that the recipient of the message knows which of their transmissions caused the error being reported.

- Contains the entire IP header.
- Contains 1st 8-bytes of the data payload section of the offending packet.
- Not developed for humans to interact with.

Ping
Lets you send a special type of ICMP message called an **Echo Request**.

- If the destination is up and running and able to communicate on the network, it'll send back an ICMP **Echo Reply**.

Traceroute
A utility that lets you discover the path between two nodes, and gives you information about each hop along the way.

Traceroute uses the TTL field by first setting it to 1 for the first packet, then 2 for the second, 3 for the third, and so on. By doing this clever little action, traceroute makes sure that the very first packet sent will be discarded by the first router hop. This results in an ICMP time exceeded message. The second packet will make it to the second router, the third will make it to the third, and so on. This continues until the packet finally makes it all the way to its destination. For each hop, traceroute will send three identical packets.

mtr is a similar command on Linux and macOS, runs in real time and continually updates its output with current aggregate data about the traceroute.

pathping is a similar command on Windows, runs for 50 seconds and then displays the final aggregate data all at once.

Testing Port Connectivity

netcat - Linux/macOS, can be run through the command $ nc , has two mandatory arguments, a host, and a port.

- Running **$ nc google.com space80** would try to establish a connection on port 80 to google.
- If the command fails, the command will exit.
- If it succeeds, you'll see a blinking cursor waiting for more input.
- Running the command with the **-z** flag will run it in **zero input output mode**
- Running the command with the **-v** flag will run it in verbose mode, which is more useful for human eyes.

```
Example: $ nc -z -v google.com 80
         Connection to google.com 80 port (tcp/http] succeeded!
          $ _
```

Test-NetConnection - Windows

- If you run the command with **-port** flag, you can ask it to test connectivity to a specific port.

```
Example: > Test-NetConnection google.com
         Computer Name..
         RemoteAddress..
         InterfaceAlias..
         SourceAddress..
         PingSucceeded..
         PingReplyDetails (RTT)..
          >
```

Testing Port Connectivity

Grow with Google: IT Support Certificate

netcat

The following commands are used on Linux and MacOS devices. The letters nc are used for the netcat command along with a host and a port. Net stands for networking. Cat comes from the Unix command line program cat, short for concatenate, which means to link things together in a chain or series.

nc [options] <host> <port>

Example command: **nc google.com 80**

This command tries to establish a transmission control protocol (TCP) connection to the host <google.com> on the specified port <port 80>.

The host can be a website or a targeted IP address.
The port can be a specific port or a range of port numbers.

Listed below are some of the options available for you to use in testing port connectivity:

nc -u <host> <port>

Tells netcat to open a user datagram protocol (UDP) connection, instead of a TCP connection.

> Example: Certain network protocols use UDP for speed or efficiency purposes. To test them, you will open a UDP connection by using nc -u and identify the host and port the data needs to be sent to.

nc -z <host> <port>

Stands for zero input/output and tells it to scan for open ports.

> Example: You can use nc -z to scan for unneeded services that could be listening into a network without sending any data to them. This can be combined with using a range of port numbers instead of just a single port.

nc -v <host> <port>
Stands for verbose and gives extended output text important for debugging and troubleshooting.

Example: You want to run a scan looking for listening devices and adds -v so that it will return lists of ports and statuses on the network or website being scanned.

nc -vv <host> <port>
Stands for very verbose and gives more output text than just verbose

Example: The IT administrator has asked for a very detailed report of all ports and their statuses within the company network. A netcat command can be run with -vv to get the robust information on all ports and their statuses.

nc -p <localport> <host> <port>
Refers to a local port for a connection. Some protocols require a specific source port to work properly, this lets you specify what port to connect from.

nc -e <program> <host> <port>
Executes a program after a connection is established. This option is not supported by all versions of netcat, but you can also use standard unix command line pipelines to pass network input to or from other programs.

nc -n <addr> <port>
prevents domain name server (DNS) lookup. Use this when you have an IP address and numeric port to use for the connection and you want to avoid the overhead of DNS or if it is not working properly.

These command-line options can be used independently or combined with one another.

> Example: An IT administrator wants to evaluate the network for open doors or weak connections that would allow someone to hack into the network. To discover this you run nc -v -z google.com 80 to determine if a connection to the port 80 is possible to google.com.

Test-NetConnection

The following commands are used on Windows PowerShell devices. The command, Test-NetConnection is case sensitive and uses capitals unlike netcat.

Test-NetConnection <host> <port>
Example command: **Test-NetConnection -ComputerName google.com -Port 80**

Tests ping connectivity and displays diagnostic information for a connection from the host google.com on port 80

Test-NetConnection -InformationLevel "Detailed"
Tests ping connectivity with detailed results.

Example: A data transfer on the network is moving very slowly. In order to check the quality of the connection an you runs
Test-NetConnection -InformationLevel “Detailed” to view details about the connection. This will connect to a default address from microsoft.

Test-NetConnection -ComputerName [remote host]
Tests a connection to a remote host.

Test-NetConnection -ComputerName [remote host] -Port [port number]
Tests TCP connectivity to a specific host and port. This can be combined with the display detailed results option:

Example:
PS C:\> Test-NetConnection -ComputerName www.google.com -Port 80 -InformationLevel Detailed

Test-NetConnection -ComputerName [remote host] -DiagnoseRouting
Performs route diagnostics to connect to a remote host. This can require administrator privileges, so you may have to run your powershell window as administrator.

Test-NetConnection -ComputerName [remote host] -constrainInterface [interface number] -DiagnoseRouting -InformationLevel "Detailed"
Performs route diagnostics to connect to a remote host with routing constraints.

Example: An employee is having trouble connecting to a specific website from their computer, but other sites are loading fine in the browser. You can try connecting to the website directly with:
Test-NetConnection -ComputerName www.example.com -Port 80 -InformationLevel Detailed

Name Resolution Tools

nslookup
Used to verify name resolution using either IP or FQDN
- By not entering any argument, nslookup will enter interactive mode.
- Entering **> set type=MX** tells nslookup to ask for specific records like the MX one in this example.
- Entering **> set debug** tells nslookup to display the full response packets, including any intermediary requests and all of their contents.

Public DNS Servers

Level 3 Communications - One of the largest ISPs in the world
- Other ISPs often connect to Level 3
- The IP addresses for Level 3's public DNS servers are **4.2.2.1** to **4.2.2.6**

Google's Public DNS
- Public name servers on the IPs **8.8.8.8** and **8.8.4.4**

DNS Registration and Expiration

Registrar
An organization responsible for assigning individual domain names to other organizations or individuals.

The most notable was a company named Network Solutions Inc. It was responsible for the registration of almost all domains that weren't country specific. As the popularity of the Internet grew, there was eventually enough market demand for competition in this space. Finally, the United States government and Network Solutions Inc came to an agreement to let other companies also sell domain names. Today, there are hundreds of companies like this all over the world.

Hosts Files
A flat file that contains, on each line, a network address followed by the host name it can be referred to as.

Loopback Address
A way of sending network traffic to yourself.
- IPv4: **127.0.0.1**
- IPv6: **::1**
- Almost every host file in existence will, in the very least, contain a line that contain a line that reads **127.0.0.1 localhost**
    - Most likely followed by **::1 localhost**

What is The Cloud?

Cloud Computing
A technological approach where computing resources are provisioned in a shareable way so that lots of users get what they need, when they need it.

Virtualization
A single physical machine, called a host, could run many individual virtual instances, called guests.

Hypervisor
A piece of software that runs and manages virtual machines, while also offering these guests a virtual operating platform that's indistinguishable from actual hardware.

Public Cloud
A large cluster of machines run by another company.

Private Cloud
Used by a single large corporation and generally physically hosted on its premises.

Hybrid Cloud
Used to describe situations where companies might run things like their most sensitive proprietary technologies on a private cloud, while entrusting their less-sensitive servers to a public cloud.

Cloud Computing
A new model in computing where large clusters of machines let us use the total resources available in a better way.

Everything as a Service

Infrastructure as a Service (IaaS)
Abstract away the physical infrastructure you need for a Desktop.

Platform as a Service (PaaS)
A subset of cloud computing where a platform is provided for customers to run their services. It abstracts away the server instances you need.

Software as a Service (SaaS)
A way of licensing the use of software to others while keeping that software centrally hosted and managed.
- Gmail for Business
- Office 365 Outlook

Cloud Storage
A customer contracts a Cloud storage provider to keep their data secure, accessible and available.
- It's up to the provider to keep the underlying physical hardware running.
- Grows with the customer's needs.
- Cloud Storage should always be the *LAST* backup option after all physical/local options have been exhausted.

IPv6 Addressing and Subnetting

Multicast: A way of addressing groups of hosts all at once.

Link-Local Unicast Addresses: Allows for local network segment communications and are configured based upon a host's MAC address.

IPv5 was an experimental protocol that introduced the concept of connections.

IPv6 are **128 bits**, which creates an "undecillion" number of numbers, or 2^128 (39-digits long)
340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6 is written out as **8** groups of **16 bits** each.
Each group is made up of **4 hexadecimal numbers**.
2001:0db8:0000:0000:0000:ff00:0012:3456

- Every IPv6 that starts with **2001:0db8** has been reserved for documentation and education or for books and courses.
  - OVER 18 quintillion addresses, larger than the entire IPv4 address space.
- Any IPv6 that begins with **FF00::** is used for multicast.
- Any IPv6 that begins with **FF80::** is used for Link-local unicast.
- Any IPv6 that begins with **5x 0's** is used for IPv4 aliasing
  0:0:0:0:0:ffff:c0a8:0101 = 192.168.1.1

2 Rules to shortening an IPv6 address:

1. You can **remove any leading zeros** from a group.
2. Any number of consecutive groups composed of just zeros can be replaced with **2 colons (:)**

	Network ID	**Host** ID	Over 9 quintillion host addresses!
IPv6	2001:0db8:0000:0000::0000:ff00:0012:3456		
Rule 1	2001: db8: 0: 0:: 0:ff00: 12:3456		
Rule 2	2001:db8::ff00:12:3456		

IPv6 Loopback Address:
0000:0000:0000:0000:0000:0000:0000:0001 -or- **::1**

IPv6 Headers

Version Field
A 4-bit field that defines what version of IP is in use.

Traffic Class Field
An 8-bit field that defines the type of traffic contained within the IP datagram and allows for different classes of traffic to receive different priorities.

Flow Label Field
A 20-bit field that's used in conjunction with the traffic class field for routers to make decisions about the quality of service level for a specific datagram.

Payload Length Field
A 16-bit field that defines how long the data payload section of the datagram is.

Next Header Field
Optional headers that allow for a chain of headers to be formed if there's a lot of optional configuration.

Hop Limit Field
An 8-bit field that's identical in purpose to the TTL field in an IPv4 header.

Source Field
A 128-bit field.

Destination Field
A 128-bit field

Data Payload

IPv6 and IPv4 Harmony

Any IPv6 that begins with **5x 0's** is used for IPv4 aliasing
0:0:0:0:0:ffff:c0a8:0101 = **192.168.1.1**

IPv6 Tunnels
Servers take incoming IPv6 traffic and encapsulate it within traditional IPv4 datagram

IPv6 Tunnel Broker
Companies that provide IPv6 tunneling endpoints for you, so you don't have to introduce additional equipment to your network.

Supplemental Reading for IPv6 and IPv4 Harmony

IPv6 and IPv4 harmony

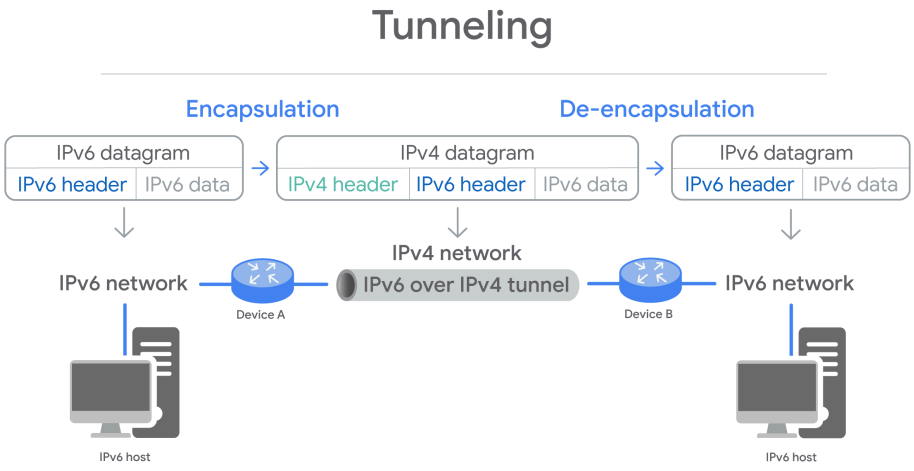
At the network layer of the TCP/IP Five-Layer Network Model, nodes connect through the internet protocol (IP) and the IP addresses that come along with it. The most common version of IP is version four (IPv4), but version six (IPv6) is rapidly seeing more widespread adoption.

This reading covers key differences between IPv6 and IPv4 and the methods that allow them to work together.

When IPv4 was first developed, a 32-bit number was chosen to represent the address for a node on a network. This means there can be around 4.2 billion individual IPv4 addresses. But this just isn't enough addresses for the number of Internet-connected devices we have in the world today. IPv6 was developed to provide plenty of addresses for all of our Internet connected devices. While IPv4 represents addresses with a 32-bit number, IPv6 represents addresses with 128 bits. This 128-bit update allows for a practically unlimited number of IPv6 addresses, 340 trillion trillion trillion addresses to be exact!

IPv4 and IPv6 require a different structure for each version's datagrams. This means the IPv4 and IPv6 networks speak different languages. For IPv6 data to travel over an IPv4 network, the IPv6 datagram has to be translated into something IPv4 can understand. Since it's not possible for the entire Internet and all connected networks to switch to IPv6 all at once, IPv6 tunneling protocols are used to allow IPv6 traffic to travel over the remaining IPv4 network.

Tunneling
Tunneling protocols allow users to carry IPv6 traffic across an IPv4 network. Tunnels are created using IPv6 servers on either end of a network connection. A tunnel server at one end takes incoming IPv6 traffic and encapsulates it within a traditional IPv4 datagram. Encapsulation is the process of transporting a data packet inside the payload of another packet.



IPv6 data that's encapsulated within an IPv4 datagram can then be delivered across the IPv4 network and received by another IPv6 tunnel server. The receiving server de-encapsulates the datagram and passes the IPv6 traffic further along the IPv6 network.

Three types of tunnels

Since IPv6 tunneling is still an evolving technology, there are several competing protocols used to establish IPv6 tunnels.

Here are three commonly used tunnel protocols:

- 6in4/manual protocol encapsulates IPv6 packets immediately inside an IPv4 packet, without using additional headers to configure the setup of the tunnel endpoints. Setup is configured manually instead. This makes performance predictable and easy to debug. Unfortunately, this protocol often will not function if the host uses network address translation (NAT) technology to map its IPv4 address. This makes the 6in4/manual protocol difficult to deploy.
- Tunnel Setup Protocol (TSP) specifies rules for negotiating the setup parameters between tunnel endpoints. This allows for a variety of tunnel encapsulation methods and wider deployment than is possible with the 6in4/manual protocol.
- Anything in Anything (AYIYA) protocol defines a method for encapsulating any protocol in any other protocol. AYIYA was developed for tunnel brokers, a service which provides a network tunnel. This protocol specifies the encapsulation, identification, checksum, security, and management operations that can be used once the tunnel is established. A key advantage of AYIYA is that it can provide a stable tunnel through an IPv4 NAT. It allows users behind a NAT or a dynamic address to maintain connectivity even when roaming between networks.

Each protocol has its pros and cons, depending on the nature of the communicating endpoints of the IPv6 connection.

Key takeaways

As IPv6 becomes more widely adopted, IPv6 traffic needs a way to travel over the IPv4 network.

- Tunneling protocols allow users to carry IPv6 traffic across an IPv4 network.
- Since IPv6 tunneling is still an evolving technology, there are several competing protocols used to establish IPv6 tunnels.
- Each protocol has its pros and cons, depending on the nature of the communicating endpoints of the IPv6 connection.

– – fin – –

Glossary

Terms and definitions from Course 2

A

A record: The most common resource record, used to point a certain domain name at a certain IPv4 IP address
ACK flag: One of the TCP control flags. ACK is short for acknowledge. A value of one in this field means that the acknowledgment number field should be examined
Acknowledgement number: The number of the next expected segment in a TCP sequence
Ad-Hoc network: A network configuration without supporting network infrastructure. Every device involved with the ad-hoc network communicates with every other device within range, and all nodes help pass along messages
Address class system: A system which defines how the global IP address space is split up
Address Resolution Protocol (ARP): A protocol used to discover the hardware address of a node with a certain IP address
Anycast: A technique that's used to route traffic to different destinations depending on factors like location, congestion, or link health
Application layer: The layer that allows network applications to communicate in a way they understand
Application layer payload: The entire contents of whatever data applications want to send to each other
ARP table: A list of IP addresses and the MAC addresses associated with them
ASN: Autonomous System Number is a number assigned to an individual autonomous system
Asymmetric Digital Subscriber Line (ADSL): A device that establishes data connections across phone lines and different speeds for uploading and downloading data
Automatic allocation: A range of IP addresses is set aside for assignment purposes

B

Baud rate: A measurement of how many bits could be passed across a phone line in a second
Bit: The smallest representation of data that a computer can understand
Bluetooth: The most common short range wireless network

Border Gateway Protocol (BGP): A protocol by which routers share data with each other
Broadband: Any connectivity technology that isn't dial-up Internet
Broadcast: A type of Ethernet transmission, sent to every single device on a LAN
Broadcast address: A special destination used by an Ethernet broadcast composed by all Fs

C

Cable categories: Groups of cables that are made with the same material. Most network cables used today can be split into two categories, copper and fiber

Cable modem termination system: Connects lots of different cable connections to an ISP's core network

Cable modem: A device that sits at the edge of a consumer's network and connects it to the cable modem termination system

Cables: Insulated wires that connect different devices to each other allowing data to be transmitted over them

Caching and recursive name servers: They are generally provided by an ISP or your local network, and their purpose is to store domain name lookups for a certain amount of time

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD): CSMA/CD is used to determine when the communications channels are clear and when the device is free to transmit data

Channels: Individual, smaller sections of the overall frequency band used by a wireless network

Client: A device that receives data from a server

CLOSE: A connection state that indicates that the connection has been fully terminated, and that no further communication is possible

CLOSE_WAIT: A connection state that indicates that the connection has been closed at the TCP layer, but that the application that opened the socket hasn't released its hold on the socket yet

Cloud computing: The concept and technological approach of accessing data, using applications, storing files, etc. from anywhere in the world as long as you have an internet connection

CNAME: A resource record used to map one domain to another

Collision domain: A network segment where only one device can communicate at a time

Computer networking: The full scope of how computers communicate with each other

Connection-oriented protocol: A data-transmission protocol that establishes a connection at the transport layer, and uses this to ensure that all data has been properly transmitted

Connectionless protocol: A data-transmission protocol that allows data to be exchanged without an established connection at the transport layer. The most common of these is known as UDP, or User Datagram Protocol

Copper cable categories : These categories have different physical characteristics like the number of twists in the pair of copper wires. These are defined as names like category (or cat) 5, 5e, or 6, and how quickly data can be sent across them and how resistant they are to outside interference are all related to the way the twisted pairs inside are arranged
Crosstalk: Crosstalk is when an electrical pulse on one wire is accidentally detected on another wire
Cyclical Redundancy Check (CRC): A mathematical transformation that uses polynomial division to create a number that represents a larger set of data. It is an important concept for data integrity and is used all over computing, not just network transmissions

D

Datalink layer: The layer in which the first protocols are introduced. This layer is responsible for defining a common way of interpreting signals, so network devices can communicate
Data offset field: The number of the next expected segment in a TCP packet/datagram
Data packet: An all-encompassing term that represents any single set of binary data being sent across a network link

Data payload section: Has all of the data of the protocols further up the stack of a frame
Demarcate: To set the boundaries of something
Demarcation point: Where one network or system ends and another one begins
Demultiplexing: Taking traffic that's all aimed at the same node and delivering it to the proper receiving service
Destination MAC address: The hardware address of the intended recipient that immediately follows the start frame delimiter
Destination network: The column in a routing table that contains a row for each network that the router knows about
Destination port: The port of the service the TCP packet is intended for
DHCP: A technology that assigns an IP address automatically to a new device. It is an application layer protocol that automates the configuration process of hosts on a network
DHCP discovery: The process by which a client configured to use DHCP attempts to get network configuration information
Dial-up: Uses POTS for data transfer, and gets its name because the connection is established by actually dialing a phone number
DNS zones: A portion of space in the Domain Name System (DNS) that is controlled by an authoritative name server
Domain: Used to demarcate where control moves from a top-level domain name server to an authoritative name server
Domain name: A website name; the part of the URL following www.
Domain Name System (DNS): A global and highly distributed network service that resolves strings of letters, such as a website name, into an IP address
Dotted decimal notation: A format of using dots to separate numbers in a string, such as in an IP address
DSL: Digital subscriber line was able to send much more data across the wire than traditional dial-up technologies by operating at a frequency range that didn't interfere with normal phone calls
DSLAM: Digital Subscriber Line Access Multiplexers are devices that connect multiple DSL connections to a high-speed digital communications channel
Duplex communication: A form of communication where information can flow in both directions across a cable
Duration field: Specifies how long the total frame is
Dynamic allocation: A range of IP addresses is set aside for client devices and one of these IPs is issued to these devices when they request one
Dynamic IP address: An IP address assigned automatically to a new device through a technology known as Dynamic Host Configuration Protocol

E

Error detection: The ability for a protocol or program to determine that something went wrong
Error recovery: The ability for a protocol or program to attempt to fix an error
ESTABLISHED: Status indicating that the TCP connection is in working order, and both sides are free to send each other data
Ethernet: The protocol most widely used to send data across individual links
Ethernet frame: A highly structured collection of information presented in a specific order
EtherType field: It follows the Source MAC Address in a dataframe. It's 16 bits long and used to describe the protocol of the contents of the frame
Exterior gateway: Protocols that are used for the exchange of information between independent autonomous systems

F

Fiber cable: Fiber optic cables contain individual optical fibers which are tiny tubes made of glass about the width of a human hair. Unlike copper, which uses electrical voltages, fiber cables use pulses of light to represent the ones and zeros of the underlying data
FIN: One of the TCP control flags. FIN is short for finish. When this flag is set to one, it means the transmitting computer doesn't have any more data to send and the connection can be closed
FIN_WAIT: A TCP socket state indicating that a FIN has been sent, but the corresponding ACK from the other end hasn't been received yet
Firewall: It is a device that blocks or allows traffic based on established rules
Five layer model: A model used to explain how network devices communicate. This model has five layers that stack on top of each other: Physical, Data Link, Network, Transport, and Application
Fixed allocation: Requires a manually specified list of MAC address and the corresponding IPs
Flag field: It is used to indicate if a datagram is allowed to be fragmented, or to indicate that the datagram has already been fragmented
Flat file: A collection of records/information that follow a consistent format with rules around stored values. On a host computer, one use is to have a list of network address and host name pairs (a hosts file)
Flow label field: 20-bit field that's used in conjunction with the traffic class
field for routers to make decisions about the quality of service level for
a specific datagram

Fragmentation: The process of taking a single IP datagram and splitting it up into several smaller datagrams

Fragmentation offset field: It contains values used by the receiving end to take all the parts of a fragmented packet and put them back together in the correct order

Frame check sequence: It is a 4-byte or 32-bit number that represents a checksum value for the entire frame
Frame control field: 16 bits long, it contains a number of sub-fields that are used to
describe how the frame itself should be processed

Frequency band: A certain section of the radio spectrum that's been agreed upon to be used for certain communications
FTP: An older method used for transferring files from one computer to another, but you still see it in use today
FTTB: Fiber to the building, fiber to the business or even fiber to the basement, since this is generally where cables to buildings physically enter. FTTB is a setup where fiber technologies are used for data delivery to an individual building
FTTH: Fiber to the home. This is used in instances where fiber is actually run to each individual residents in a neighborhood or apartment building
FTTN: Fiber to the neighborhood. This means that fiber technologies are used to deliver data to a single physical cabinet that serves a certain amount of the population
FTTP: Fiber to the premises. FTTH and FTTB may both also be referred to as FTTP
FTTX: Stands for fiber to the X, where the X can be one of many things
Full duplex: The capacity of devices on either side of a networking link to communicate with each other at the exact same time
Fully qualified domain name: When you combine all the parts of a domain together

H

Half-duplex: It means that, while communication is possible in each direction, only one device can be communicating at a time
Handshake: A way for two devices to ensure that they're speaking the same protocol and will be able to understand each other
HDSL: High Bit-rate Digital Subscriber Lines. These are DSL technologies that provision speeds above 1.544 megabits per second
Header checksum field: A checksum of the contents of the entire IP datagram header
Header length field: A four bit field that declares how long the entire header is. It is almost always 20 bytes in length when dealing with IPv4
Hexadecimal: A way to represent numbers using a numerical base of 16
Hop limit field: An 8-bit field that's identical in purpose to the TTL field in an IPv4 header
Host file: It is a flat file that contains, on each line, a network address followed by the host name it can be referred to as
Hub: It is a physical layer device that broadcasts data to everything computer connected to it
Hybrid cloud: Used to describe situations where companies might run things like
their most sensitive proprietary technologies on a private cloud or on premise while entrusting their less sensitive servers to a public cloud

Hypervisor: A piece of software that runs and manages virtual machines while also
offering guests a virtual operating platform that's indistinguishable from actual hardware

I

IANA: The Internet Assigned Numbers Authority, is a non-profit organization that helps manage things like IP address allocation

ICMP: Internet control message protocol is used by router or remote hosts to
communicate error messages when network problems prevent delivery of IP packets

ICMP payload: Piece of the packet which lets the recipient of the message knows which of their transmissions caused the error being reported

Identification field: It is a 16-bit number that's used to group messages together

Infrastructure as a Service (IaaS): A subset of cloud computing where a network and servers are provided for customers to run their services

Instantiation: The actual implementation of something defined elsewhere

Interface: For a router, the port where a router connects to a network. A router gives and receives data through its interfaces. These are also used as part of the routing table

Interior gateway: Interior gateway protocols are used by routers to share information within a single autonomous system
Internet Protocol (IP): The most common protocol used in the network layer
Internet Service Provider (ISP): A company that provides a consumer an internet connection
Internetwork: A collection of networks connected together through routers - the most famous of these being the Internet
IP datagram: a highly structured series of fields that are strictly defined
IP masquerading: The NAT obscures the sender's IP address from the receiver
IP options field: An optional field and is used to set special characteristics for datagrams primarily used for testing purposes
IPv6 tunnel: IPv6 tunnel servers on either end of a connection take incoming IPv6 traffic and encapsulate it within traditional IPv4 datagrams
IPv6 tunnel brokers: Companies that provide IPv6 tunneling endpoints for you, so you don't have to introduce additional equipment to your network
L
Line coding: Modulation used for computer networks
Link-local unicast address: Allow for local network segment communications and
are configured based upon a host's MAC address

Listen: It means that a TCP socket is ready and listening for incoming connections

Local Area Network (LAN): A single network in which multiple devices are connected
Loopback address: An IP address that always points to itself. This type of address is used to test internal pathing through the TCP/IP protocols
M
MAC(Media Access Control) address: A globally unique identifier attached to an individual network interface. It's a 48-bit number normally represented by six groupings of two hexadecimal numbers
MAC filtering: Access points are configured to only allow for connections from a specific set of MAC addresses belonging to devices you trust
Mesh networks: Like ad-hoc networks, lots of devices communicate with each other device, forming a mesh if you were to draw lines for all the links between all the nodes
Metered connection: An internet connection where all data transfer usage is tracked. Cell phone plans that have a limit on data usage per month or that charge based on usage are examples of metered connections
Modulation: A way of varying the voltage of a constant electrical charge moving across a standard copper network cable
Multicast: A way of addressing groups of hosts all at once
Multicast frame: If the least significant bit in the first octet of a destination address is set to one, it means you're dealing with a multicast frame. A multicast frame is similarly set to all devices on the local network signal, and it will be accepted or discarded by each device depending on criteria aside from their own hardware MAC address
Multiplexing: It means that nodes on the network have the ability to direct traffic toward many different receiving services
MX record: It stands for mail exchange and this resource record is used in order to deliver email to the correct server
N
Name resolution: This process of using DNS to turn a domain name into an IP address
Network Address Translation (NAT): A mitigation tool that lets organizations use one public IP address and many private IP addresses within the network
Network layer: It's the layer that allows different networks to communicate with each other through devices known as routers. It is responsible for getting data delivered across a collection of networks
Network port: The physical connector to be able to connect a device to the network. This may be attached directly to a device on a computer network, or could also be located on a wall or on a patch panel
Network switch: It is a level 2 or data link device that can connect to many devices so they can communicate. It can inspect the contents of the Ethernet protocol data being sent around the network, determine which system the data is intended for and then only send that data to that one system
Next header field: Defines what kind of header is immediately after this current one
Next hop: The IP address of the next router that should receive data intended for the destination networking question or this could just state the network is directly connected and that there aren't any additional hops needed. Defined as part of the routing table
Node: Any device connected to a network. On most networks, each node will typically act as a server or a client
Non-metered connection: A connection where your data usage is not tracked or limited, instead you are charged a flat fee for unlimited and unrestricted usage. A Wi-Fi connection is an example of a non-metered connection
Non-routable address space: They are ranges of IPs set aside for use by anyone that cannot be routed to
NS record: It indicates other name servers that may also be responsible for a particular zone
NTP servers: Used to keep all computers on a network synchronized in time
O
Octet: Any number that can be represented by 8 bits
Optical Network Terminator: Converts data from protocols the fiber network can
understand to those that are more traditional twisted pair copper networks can understand

Options field: It is sometimes used for more complicated flow control protocols

Organizationally Unique Identifier (OUI): The first three octets of a MAC address
OSI model: A model used to define how network devices communicate. This model has seven layers that stack on top of each other: Physical, Data Link, Network, Transport, Session, Presentation, and Application
P
Padding field: A series of zeros used to ensure the header is the correct total size
Pairing: When a wireless peripheral connects to a mobile device, and the two devices exchange information, sometimes including a PIN or password, so that they can remember each other
Patch panel: A device containing many physical network ports
Payload: The actual data being transported, which is everything that isn't a header
Payload length field: 16-bit field that defines how long the data payload section of the datagram is
Physical layer: It represents the physical devices that interconnect computers
Platform as a service: A subset of cloud computing where a platform is provided for customers to run their services
Point-To-Point VPN: Establishes a VPN tunnel between two sites but VPN tunneling logic is handled by network devices at either side, so that users don't all have to establish their own connections

Pointer resource record: It resolves an IP to a name
Port: It is a 16-bit number that's used to direct traffic to specific services running on a networked computer
Port forwarding: A technique where specific destination ports can be configured to always be delivered to specific nodes
Port preservation: A technique where the source port chosen by a client, is the same port used by the router
Preamble: The first part of an Ethernet frame, it is 8 bytes or 64 bits long and can itself be split into two sections
Presentation layer: It is responsible for making sure that the unencapsulated application layer data is actually able to be understood by the application in question
Private cloud: When a company owns the services and the rest of the cloud infrastructure, whether on-site or in a remote data center
Protocol: A defined set of standards that computers must follow in order to communicate properly is called a protocol
Protocol field: A protocol field is an 8-bit field that contains data about what transport layer protocol is being used
Proxy service: A server that acts on behalf of a client in order to access another service
PSH flag: One of the TCP control flags. PSH is short for push. This flag means that the transmitting device wants the receiving device to push currently- buffered data to the application on the receiving end as soon as possible
Public cloud: The cloud services provided by a third party
Public DNS servers: Name servers specifically set up so that anyone can use them for free

Q

Quad A (AAAA) record: It is very similar to an A record except that it returns in IPv6 address instead of an IPv4 address

R

Receiving address: The MAC address of the access point that should receive the frame
Recursive name servers: Servers that perform full DNS resolution requests
Registrar: An organization responsible for assigning individual domain names to other organizations or individuals
Reverse lookup zone files: They let DNS resolvers ask for an IP, and get the FQDN associated with it returned
Reverse proxy: A service that might appear to be a single server to external clients, but actually represents many servers living behind it
Round robin: It is a concept that involves iterating over a list of items one by one in an orderly fashion
Router: A device that knows how to forward data between independent networks
Routing protocols: Special protocols the routers use to speak to each other in order to share what information they might have
RST flag: One of the TCP control flags. RST is short for reset. This flag means that one of the sides in a TCP connection hasn't been able to properly recover from a series of missing or malformed segments

S

Sequence control field: A field that is 16 bits long and mainly contains a sequence number used to keep track of ordering the frames
Sequence number: A 32-bit number that's used to keep track of where in a sequence of TCP segments this one is expected to be
Server: A device that provides data to another device that is requesting that data, also known as a client
Server or Service: A program running on a computer waiting to be asked for data
Service type field: A eight bit field that can be used to specify details about quality of service or QoS technologies
Session layer: The network layer responsible for facilitating the communication between actual applications and the transport layer
Short-range wireless network: It is what mobile devices uses to connect to their peripherals

Simplex communication: A form of data communication that only goes in one direction across a cable
Socket: The instantiation of an endpoint in a potential TCP connection
Software as a Service (SaaS): A way of licensing the use of software to others while keeping that software centrally hosted and managed
Source MAC address: The hardware address of the device that sent the ethernet frame or data packet. In the data packet it follows the destination MAC address
Source port: A high numbered port chosen from a special section of ports known as ephemeral ports
SRV record: A service record used to define the location of various specific services
Start Frame Delimiter (SFD): The last byte in the preamble, that signals to a receiving device that the preamble is over and that the actual frame contents will now follow
Start of authority: A declaration of the zone and the name of the name server that is authoritative for it
Static IP address: An IP address that must be manually configured on a node
Subnet mask: 32-bit numbers that are normally written as four octets of decimal numbers
Subnetting: The process of taking a large network and splitting it up into many individual smaller sub networks or subnets
Symmetric Digital Subscriber Line (SDSL): A device that establishes data connections across phone lines and has upload and download speeds that are the same
SYN flag: One of the TCP flags. SYN stands for synchronize. This flag is used when first establishing a TCP connection and make sure the receiving end knows to examine the sequence number field
SYN_RECEIVED: A TCP socket state that means that a socket previously in a listener state, has received a synchronization request and sent a SYN_ACK back
SYN_SENT: A TCP socket state that means that a synchronization request has been sent, but the connection hasn't been established yet

T

T-Carrier technologies: Technologies Invented to transmit multiple phone calls over a single link. Eventually, they also became common transmission systems to transfer data much faster than any dial-up connection could handle
TCP checksum: A mechanism that makes sure that no data is lost or corrupted during a transfer
TCP segment: A payload section of an IP datagram made up of a TCP header and a data section
TCP window: The range of sequence numbers that might be sent before an acknowledgement is required
Time-To-Live field (TTL): An 8-bit field that indicates how many router hops a datagram can traverse before it's thrown away
Top Level Domain (TLD): The top level of the DNS or the last part of a domain name. For example, the “com” in www.weather.com
Total hops: The total number of devices data passes through to get from its source to its destination. Routers try to choose the shortest path, so fewest hops possible. The routing table is used to keep track of this
Total length field: A 16-bit field that indicates the total length of the IP datagram it's attached to
Traffic class field: An 8-bit field that defines the type of traffic contained within the IP datagram and allows for different classes of traffic to receive different priorities

Transmission Control Protocol (TCP): The data transfer protocol most commonly used in the fourth layer. This protocol requires an established connection between the client and server
Transmitter address: The MAC address of whatever has just transmitted the frame
Transport layer: The network layer that sorts out which client and server programs are supposed to get the data
TTL: The lifetime limit of data given in seconds. This number can be configured by the owner of a domain name for how long a name server is allowed to cache in entry before it should discard it and perform a full resolution again
Twisted pair cable: The most common type of cabling used for connecting computing devices. It features pairs of copper wires that are twisted together
Two-factor authentication: A technique where more than just a username and password are required to authenticate. Usually, a short-lived numerical token is generated by the user through a specialized piece of hardware or software
TXT record: It stands for text and was originally intended to be used only for associating some descriptive text with a domain name for human consumption
Types of DNS servers: There are five primary types of DNS servers; caching name servers, recursive name servers, root name servers, TLD name servers, and authoritative name servers

U

Unicast transmission: A unicast transmission is always meant for just one receiving address
Urgent pointer field: A field used in conjunction with one of the TCP control flags to point out particular segments that might be more important than others
URG flag: One of the TCP control flags. URG is short for urgent. A value of one here indicates that the segment is considered urgent and that the urgent pointer field has more data about this

User Datagram Protocol (UDP): A transfer protocol that does not rely on connections. This protocol does not support the concept of an acknowledgement. With UDP, you just set a destination port and send the data packet

V

Version field: First field in an IP header that specifies the version of IP
Virtual LAN (VLAN): It is a technique that lets you have multiple logical LANs operating on the same physical equipment
Virtual Private Network (VPN): A technology that allows for the extension of a private or local network, to a host that might not work on that same local network
Virtualization: A single physical machine called a host runs many individual virtual instances called guests
VLAN header: A piece of data that indicates what the frame itself is. In a data packet it is followed by the EtherType

W

Wide area network: Acts like a single network but spans across multiple physical locations. WAN technologies usually require that you contract a link across the Internet with your ISP
Wi-Fi Protected Access (WPA): A security program that uses a 128-bit key to protect wireless computer networks, which makes it more difficult to crack than WEP
Wired Equivalence Privacy (WEP): An encryption technology that provides a very low level of privacy. WEP should really only be seen as being as safe as sending unencrypted data over a wired connection
Wireless access point: A device that bridges the wireless and wired portions of a network
Wireless LANS (WLANS): One or more access points act as a bridge between a wireless and a wired network
Wireless networking: Networks you connect to through radios and antennas

Z

Zone Files: Simple configuration files that declare all resource records for a particular zone