Introduction to Network Services Name Resolution Name Resolution in Practice Dynamic Host Configuration Protocol Network Address Translation VPNs and Proxies **Graded Assessments** Reading: Module 4 Glossary
10 min Reading: Graded Plugin Quiz: Networking Services
 Simulation
 1 question Quiz: Networking Services 10 questions

Module 4 Glossary

New terms and their definitions: Course 2 Week 4 A record: The most common resource record, used to point a certain domain name at a certain IPv4 IP address Anycast: A technique that's used to route traffic to different destinations depending on factors like location, Automatic allocation: A range of IP addresses is set aside for assignment purposes 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 CNAME: A resource record used to map one domain to another **DHCP discovery:** The process by which a client configured to use DHCP attempts to get network configuration

Domain Name System (DNS): A global and highly distributed network service that resolves strings of letters, such as a 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 **Domain name:** A website name; the part of the URL following www. **Dynamic allocation:** A range of IP addresses is set aside for client devices and one of these IPs is issued to these

Fixed allocation: Requires a manually specified list of MAC address and the corresponding IPs Fully qualified domain name: When you combine all the parts of a domain together IP masquerading: The NAT obscures the sender's IP address from the receiver MX record: It stands for mail exchange and this resource record is used in order to deliver email to the correct server 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 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

Port forwarding: A technique where specific destination ports can be configured to always be delivered to specific Port preservation: A technique where the source port chosen by a client, is the same port used by the router Proxy service: A server that acts on behalf of a client in order to access another service Quad A (AAAA) record: It is very similar to an A record except that it returns in IPv6 address instead of an IPv4 address Recursive name servers: Servers that perform full DNS resolution requests 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

Round robin: It is a concept that involves iterating over a list of items one by one in an orderly fashion

Top Level Domain (TLD): The top level of the DNS or the last part of a domain name. For example, the "com" in Time-To-Live field (TTL): An 8-bit field that indicates how many router hops a datagram can traverse before it's **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 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 Zone Files: Simple configuration files that declare all resource records for a particular zone

Terms and their definitions from previous weeks

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 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 Application layer payload: The entire contents of whatever data applications want to send to each other Application layer: The layer that allows network applications to communicate in a way they understand 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

Bit: The smallest representation of data that a computer can understand Border Gateway Protocol (BGP): A protocol by which routers share data with each other Broadcast address: A special destination used by an Ethernet broadcast composed by all Fs Broadcast: A type of Ethernet transmission, sent to every single device on a LAN

Cable categories: Groups of cables that are made with the same material. Most network cables used today can be split Cables: Insulated wires that connect different devices to each other allowing data to be transmitted over them

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 Client: A device that receives data from a server 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 **CLOSE:** A connection state that indicates that the connection has been fully terminated, and that no further communication is possible Computer networking: The full scope of how computers communicate with each other 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 $\textbf{Copper cable categories:} \ \text{These categories have different physical characteristics like the number of twists in the pair} \\$ 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

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 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

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

Demarcate: To set the boundaries of something Demarcation point: Where one network or system ends and another one begins $\textbf{Demultiplexing:} \ Taking \ traffic \ that 's \ all \ aimed \ at \ the \ same \ node \ and \ delivering \ it \ to \ the \ proper \ receiving \ service$ $\textbf{Destination MAC address:} \ The \ hardware \ address \ of the \ intended \ recipient \ that \ immediately \ follows \ the \ start \ frame$

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 **Dotted decimal notation:** A format of using dots to separate numbers in a string, such as in an IP address Duplex communication: A form of communication where information can flow in both directions across a cable **Dynamic IP address:** An IP address assigned automatically to a new device through a technology known as Dynamic

ESTABLISHED: Status indicating that the TCP connection is in working order, and both sides are free to send each Ethernet frame: A highly structured collection of information presented in a specific order Ethernet: The protocol most widely used to send data across individual links EtherType field: It follows the Source MAC Address in a dataframe. It's 16 bits long and used to describe the protocol of $\textbf{Exterior gateway:} \ Protocols\ that\ are\ used\ for\ the\ exchange\ of\ information\ between\ independent\ autonomous\ systems$

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 $\textbf{FIN_WAIT:} \ A\ \mathsf{TCP}\ socket\ state\ indicating\ that\ a\ \mathsf{FIN}\ has\ been\ sent,\ but\ the\ corresponding\ ACK\ from\ the\ other\ end\ hasn't$ 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 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 $\textbf{Flag field:} \ \textbf{It is used to indicate if a datagram is allowed to be fragmented, or to indicate that the datagram has already} \\$ been fragmented

Fragmentation offset field: It contains values used by the receiving end to take all the parts of a fragmented packet Fragmentation: The process of taking a single IP datagram and splitting it up into several smaller datagrams Frame check sequence: It is a 4-byte or 32-bit number that represents a checksum value for the entire frame FTP: An older method used for transferring files from one computer to another, but you still see it in use today Full duplex: The capacity of devices on either side of a networking link to communicate with each other at the exact

Half-duplex: It means that, while communication is possible in each direction, only one device can be communicating **Handshake:** A way for two devices to ensure that they're speaking the same protocol and will be able to understand $\textbf{Header checksum field:} \ \textbf{A checksum of the contents of the entire IP datagram header}$ **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 **Hub:** It is a physical layer device that broadcasts data to everything computer connected to it

IANA: The Internet Assigned Numbers Authority, is a non-profit organization that helps manage things like IP address Identification field: It is a 16-bit number that's used to group messages together 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 Interior gateway: Interior gateway protocols are used by routers to share information within a single autonomous Internet Service Provider (ISP): A company that provides a consumer an internet connection $\textbf{Internetwork:} \ \textbf{A } \textbf{collection of networks connected together through routers-the most famous of these being the all the properties of the properti$

IP datagram: A highly structured series of fields that are strictly defined IP options field: An optional field and is used to set special characteristics for datagrams primarily used for testing

Line coding: Modulation used for computer networks 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 MAC(Media Access Control) address: A globally unique identifier attached to an individual network interface. It's a 48bit number normally represented by six groupings of two hexadecimal numbers **Modulation:** A way of varying the voltage of a constant electrical charge moving across a standard copper network

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

Network Address Translation (NAT): A mitigation tool that lets organizations use one public IP address and many **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 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-routable address space: They are ranges of IPs set aside for use by anyone that cannot be routed to

Octet: Any number that can be represented by 8 bits 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

Padding field: A series of zeros used to ensure the header is the correct total size Patch panel: A device containing many physical network ports Payload: The actual data being transported, which is everything that isn't a header Physical layer: It represents the physical devices that interconnect computers Port: It is a 16-bit number that's used to direct traffic to specific services running on a networked computer **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 Protocol field: A protocol field is an 8-bit field that contains data about what transport layer protocol is being used $\textbf{Protocol:} \ \textbf{A} \ \textbf{defined set} \ \textbf{of} \ \textbf{standards} \ \textbf{that} \ \textbf{computers} \ \textbf{must} \ \textbf{follow} \ \textbf{in} \ \textbf{order} \ \textbf{to} \ \textbf{communicate} \ \textbf{properly} \ \textbf{is} \ \textbf{called} \ \textbf{a} \ \textbf{protocol} \ \textbf{a} \ \textbf{a} \ \textbf{protocol} \ \textbf{a} \ \textbf{a} \ \textbf{protocol} \ \textbf{a} \ \textbf{$ **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 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 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 Sequence number: A 32-bit number that's used to keep track of where in a sequence of TCP segments this one is

Server or Service: A program running on a computer waiting to be asked for data Server: A device that provides data to another device that is requesting that data, also known as a client 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 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 $\textbf{Source MAC address:} \ The \ hardware \ address \ of \ the \ device \ that \ sent \ the \ ethernet \ frame \ or \ data \ packet. \ In \ the \ data$ Source port: A high numbered port chosen from a special section of ports known as ephemeral ports 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 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 $\textbf{Subnetting:} \ \text{The process of taking a large network and splitting it up into many individual smaller sub networks or a subnetwork of the process of taking a large network and splitting it up into many individual smaller subnetworks or a subnetwork of the process of taking a large network and splitting it up into many individual smaller subnetwork or a subnetwork of the process of taking a large network and splitting it up into many individual smaller subnetwork or a subnetwork of the process of taking a large network and splitting it up into many individual smaller subnetwork or a subnetwork of the process of taking a large network and splitting it up into many individual smaller subnetwork or a subnetwork of the process of taking a large network of taking a large netw$ **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

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 **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 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

 $\textbf{SYN_SENT:} \ A \ \mathsf{TCP} \ socket \ state \ that \ means \ that \ a \ synchronization \ request \ has \ been \ sent, \ but \ the \ connection \ hasn't$

Twisted pair cable: The most common type of cabling used for connecting computing devices. It features pairs of Unicast transmission: A unicast transmission is always meant for just one receiving address $\textbf{URG flag:} \ \textbf{One of the TCP control flags.} \ \textbf{URG is short for urgent.} \ \textbf{A value of one here indicates that the segment is}$ considered urgent and that the urgent pointer field has more data about this 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

Transport layer: The network layer that sorts out which client and server programs are supposed to get the data

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 Virtual LAN (VLAN): It is a technique that lets you have multiple logical LANs operating on the same physical VLAN header: A piece of data that indicates what the frame itself is. In a data packet it is followed by the EtherType

Mark as completed

been established yet

🖒 Like 🖓 Dislike 🏳 Report an issue