Glossary

Address Resolution Protocol (ARP) A protocol for determining the hardware address of a computer or other device based on its IP address.

application layer The topmost layer of the networking protocol stack. This layer consists of data formats and protocols specific to a given application. For example, the HTTP (hypertext transport protocol) standard is an application-layer protocol.

broadcast address A special address that sends a packet simultaneously to every device on a local area network.

core router A router that provides service for major Internet backbone routes. Core routers are powerful devices that must handle a large volume of traffic and usually must manage a large number of simultaneous routes. Core routers participate in route advertisements to discover or announce changes in the network topology.

default gateway The default router used for outgoing traffic if there is no explicit route for the destination IP in the system's routing table.

domain name A human-readable name that identifies an Internet or intranet site; for example, developer.apple.com is a domain name.

By resolving a domain name, an application can obtain a corresponding IP address that is suitable for sending data to that site.

edge router A router that provides connectivity between a customer site and an upstream ISP. Edge routers generally route between only two or three different networks, and thus usually do not participate in route advertisements.

encapsulation The act of wrapping one packet inside another packet (usually of a different type).

For example, on a local area network, your IP packets are encapsulated within Ethernet packets. The Ethernet packets provide information about their destination within the local area network. The IP packets inside them provide information about what to do with the packets once they reach the public Internet.

firewall A router that limits the type of traffic that can pass. A firewall may block certain ports, perform network address translation to hide the IP addresses of hosts on one side, block malformed packets, or perform various other packet rewriting operations.

fragmentation The process of breaking up a packet into smaller pieces to accommodate network connections with a smaller maximum packet size (referred to as the maximum transmission unit, or MTU).

header In the context of packets, the first part of a packet (before the actual payload) that contains information about where the packet should be sent.

In the context of HTTP, a series of values that provide information about the content of a request or reply, such as the hostname, caching policies, and so on.

hop Any one of a series of physical links that make up the route from one host to another.

host Any device that is connected to a network. It may be a client computer, a server, a mobile phone, or even a network-attached printer.

hostname (or host name) A DNS name that points to a specific host (or a group of hosts that mimic a single host).

infrastructure device Any device that provides support for a network's basic operation—for example, a router, a Wi-Fi access point, or an Ethernet switch.

Internet Control Message Protocol (ICMP) A low-level networking protocol that provides out-of-band control messages that are used by the operating system when making TCP connections.

ICMP is used mainly to deliver connection failure notifications—"connection refused" and "host unreachable" messages, for example. However, it is also used by some network diagnostic tools, such as `ping` and `traceroute`.

IP (Internet Protocol) layer The networking layer that provides basic transport of packets across the Internet. It sits above the physical layer (hardware interconnects) and below the transport layer (TCP and UDP, for example).

IP address A number that uniquely identifies a single host on the Internet (short for Internet Protocol address). An IP address can be in one of two forms: an IPv4 address or an IPv6 address.

IPv4 address An IP address consisting of four 8-bit numbers (for a total of 32 bits). For example, the IP address for developer.apple.com is 17.254.2.129.

IPv6 address An IP address consisting of eight groups of 16-bit hexadecimal numbers (for a total of 128 bits). If several groups in a row are all zero, you can omit those groups and replace them with a double colon (but only once per IP address).

For example, the IPv6 address for example.com is 2001:500:88:200::10.

latency The amount of time it takes for a packet to reach its destination, usually measured in milliseconds. Latency is usually expressed as round-trip latency, which refers to the amount of time for a packet to reach its destination and for the response packet to reach the original host. Latency is important for two reasons. First, it increases the amount of time it takes to establish a connection. Second, it dramatically reduces performance when using protocols that require the client to wait for a response before sending subsequent requests.

link A physical connection between two hosts on a network (or a virtual connection that emulates a physical connection) with no intermediate routers (except for link-layer switches).

link layer The lowest layer of the network protocol stack. This layer provides support for the physical transport of packets from one host to another across a local area network or other physical link.

listening socket (or listen socket) A socket configured to listen for incoming connections.

Maximum Transmission Unit (MTU) The largest packet size that can be delivered across a particular link. The MTU is limited by the actual communication hardware, and usually represents the maximum payload size supported by the largest physical packet that the hardware supports. However, in some cases (such as gigabit Ethernet), the default MTU may be further limited in software to maintain backwards compatibility with legacy hardware that does not support larger packets.

multicast A special type of packet that is simultaneously delivered to a multitude of hosts on the network, but not to every host (broadcast).

neighbor discovery protocol (NDP) A protocol used by IPv6 over Ethernet to learn about other devices on the physical network. Among other things, neighbor discovery can be used to learn the hardware addresses of nearby devices, discover routers and name servers, and determine information about upstream links, such as their Maximum Transmission Unit (MTU).

netblock See subnet.

netmask A collection of bits indicating which portion of an IPv4 address is the network part and which portion is the host part.

If the network part of the destination address is the same as the network part of the source address, the two hosts are considered to be within the same subnet.

network address A special reserved address within each IPv4 network in which the host part is all zeros. This address was used by older operating systems as the broadcast address, so for historical compatibility reasons, this number is reserved.

network address translation (NAT) A form of packet rewriting performed by a firewall in which packets are modified to contain a different source or destination IP address before passing them on. NAT is most commonly used to make traffic from multiple devices appear to come from a single device, often for security or load balancing purposes.

network interface A piece of hardware (or virtual hardware) that represents the endpoint of a link.

packets A discrete unit of data that is sent across a computer network.

path MTU discovery A process by which one host determines the largest packet that can be sent to a destination without fragmenting it. This allows the host to fragment the data ahead of time, which prevents packets from potentially being fragmented more than once before reaching their final destination.

Path MTU discovery works by sending packets with the “Don't Fragment” bit set. If any router along the path responds by sending an ICMP packet with the Fragmentation Needed bit set, the host then tries progressively smaller sizes until the packet reaches its destination successfully.

See also Maximum Transmission Unit (MTU).

payload The data contents of a packet (as distinct from the structure of the packet itself).

physical layer See link layer.

port numbers A number that uniquely identifies a particular service on a given host. Port numbers are further divided according to whether they are TCP or UDP ports.

recursion The use of recursive queries. A recursive query asks the domain name server to perform recursion on the client’s behalf. If the domain name server allows recursive queries, it then sends a query to the root name server asking which server knows the answer, then asks that server, and so on, until it reaches a server that actually knows the answer to the query.

See also recursion.

route The path that packets take from one host to another host. If the two hosts are on the same physical network, the route consists of a single link; if not, it passes through one or more routers.

router A device that routes packets between two or more networks. A router determines which network should receive each packet based on a set of routing rules.

Most routers also communicate with other routers to optimize those rules as network links are added and removed.

router address The IP address of your router.

routing The process of taking a packet on one physical network and retransmitting it on a different physical network, using a set of rules to determine which network should receive each packet. A device that performs routing is called a router.

shared network A network in which every packet is received by every device on the network. This is the opposite of a switched network.

subnet A range of IP addresses in which packets from one host can be sent directly to another host without going through an intermediate router.

switched network A physical network in which an infrastructure device (called a switch) directs packets based on their destination. This improves network performance by ensuring that only the hosts that need to receive a given packet actually see it. This is the opposite of a shared network.

trailer The last part of a packet (after the payload) that usually contains a checksum of the payload data.

Transmission Control Protocol (TCP) A transport-layer protocol that provides bidirectional, stream-based delivery of data, with flow control and delivery guarantees (automatic retry). Contrast with User Datagram Protocol (UDP).

transport layer The networking layer that sits on top of the IP layer and can provide such features as port numbers, delivery guarantees, flow control, and checksums. The two most common transport-layer protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

User Datagram Protocol (UDP) A transport-layer protocol that provides unidirectional, packet-based delivery of data, with best-effort delivery (no retransmission). Contrast with Transmission Control Protocol (TCP).
