TCP/IP Model Layers

- Application Layer
- Transportation Layer
- Internet Layer
- Link Layer

Application Layer

Several protocols are available at the application layer. These include:

HTTP

PORT: 80

All web browsers use the HTTP protocol. The browser's job is to provide you with an interface for submitting web requests. The browser puts your request together and passes it to HTTP at the application layer.

HTTPS

PORT: 443

HTTPS is a more secure version of HTTP, it is used when you need the transaction to be encrypted and secured.

FTP and TFP

PORT: 20, 21

FTP is another Application layer protocol. There's also an unsecure version of it called TFTP. They're both used to send and receive files over a TCP/IP-based network.

Telnet

PORT: 23

Telnet is used to either remotely access applications off remote systems or get into a Cisco device to reconfigure it with remote access.

Transportation Layer

In this model, it consists of two primary protocols, TCP and UDP.

The Transport layer's main purpose is to identify the port numbering used by the Application layer protocols above it.

In our example, we're using HTTP as the Application layer protocol. HTTP uses port 80. As you create your request in the browser and that request is sent down to the Application layer, the HTTP protocol sends the data down to the Transport layer.

TCP

TCP is going to embed port 80 into the data's headers. This way, the internet knows which application to pass the request off to on the receiving side. This is a critical function of the Transport layer.

Beyond that, the differences between these two protocols are in security and reliability.

- Both TCP and UDP provide port numbering

TCP doesn't send data unless it knows the recipient is there and ready to receive it. It requires, ahead of time, some guarantee that the receiver is prepared for what it sends. This is called handshaking.

UDP

In UDP's case, there's no handshaking upfront whatsoever. It's considered a connectionless or a best-effort protocol. For that reason, TCP is considered more reliable.

Internet Layer

The next layer is the Internet layer. This layer's primary protocol is IP, the Internet Protocol, which provides the logical addressing required to locate your destination node. The IP address of that node is assigned at the Internet layer, and that's the first step in getting the data to the correct destination. This is called routing through the network.

On the Internet layer, every host is given a four-byte address that looks like this: **x.x.x.x**

- A portion of that address represents the network segment that you're on, and the rest of it represents your node.

Link Layer

The Link layer is concerned with physical addressing and transmitting bits on the wire or through wireless access. Everything that's been done up to now is passed down to this layer, and then the physical addresses, which we call Media Access Control, or MAC addresses, are added to the data.

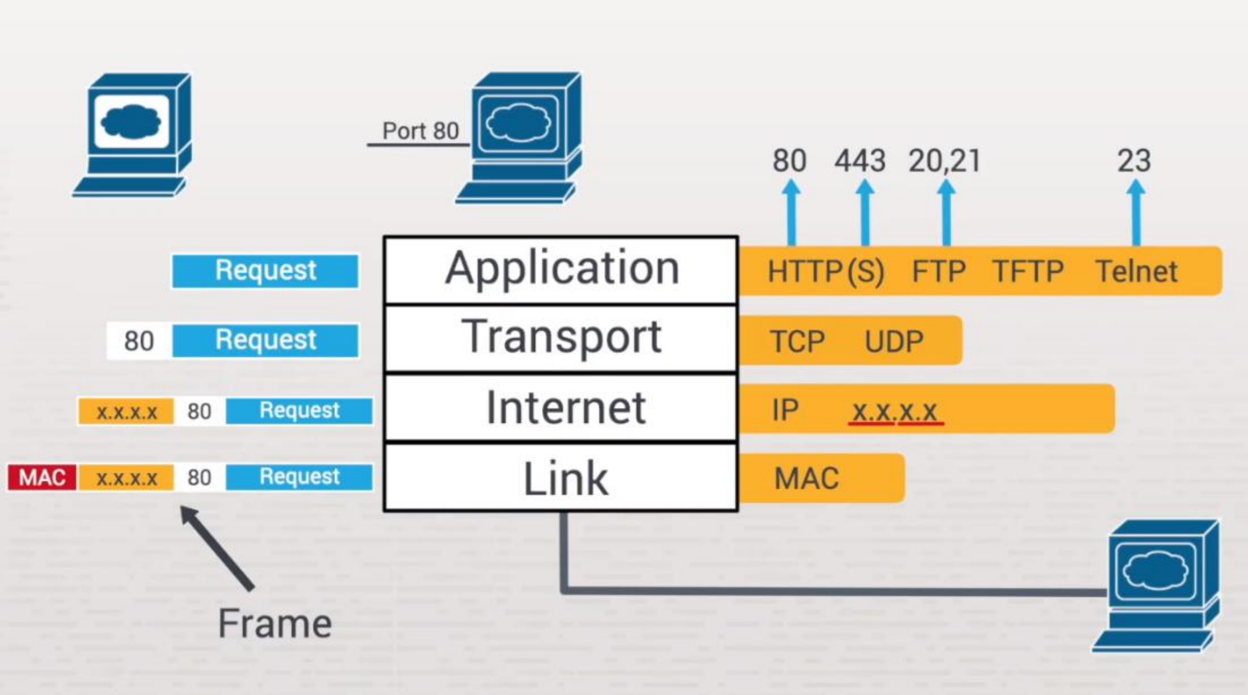
MAC Addresses

MAC addresses are physical in nature, meaning the network port in your workstation is going to have a physical address associated with it. Then two MAC addresses are added to the data from the Internet layer: your address, and the address of closest system you need to pass data through.

Physical Transmission of Bits

Frame: What you end up with is called a frame. Once you have a frame, the only thing left to do is take all the 1s and 0s in the frame, which is all the information you're trying to send, and encode them on the wire.

This is where the physical transmission of bits occurs. Your information is converted to electricity or radio waves and then sent out on the network.



TCP/IP Model Overview Facts

TCP/IP model is commonly used when learning about and referring to TCP/IP protocols. It is a theoretical, layered model that classifies and organizes the tasks hosts perform to prepare data for transport across the network. The TCP/IP model is a widely used method for understanding and talking about network communications. However, remember that it is only a theoretical model that defines standards for programmers and network administrators. It is not a model of actual physical layers.

TCP/IP Model Overview

The TCP/IP model performs the following functions when discussing networking concepts:

- Provides a common language or reference point for network professionals.
- Divides networking tasks into logical layers for easier comprehension.
- Allows specialization of features at different levels.
- Aids in troubleshooting.
- Promotes standards and interoperability between networks and devices.
- Provides modularity in networking features that allows developers to change features without changing the entire approach.

However, you must remember the following limitations of the TCP/IP model:

- TCP/IP layers are theoretical and do not actually perform real functions.
- Industry implementations rarely have a layer-to-layer correspondence with the TCP/IP layers.
- Different protocols within the stack perform different functions, which help send or receive the overall message.
- A particular protocol implementation may not represent every layer or it may spread across multiple layers.

TCP/IP Model Layers

The layers of the TCP/IP model are described in the following table.

Layer	Description
Application layer	The Application layer, also called the Process-to-Process layer, corresponds to the Session, Presentation, and Application layers of the OSI model.
Transport layer	The Transport layer, also called the Host-to-Host layer, is comparable to the Transport layer of the OSI model. It is responsible for error-checking and reliable packet delivery. The Transport layer breaks the data stream into segments and assigns sequence numbers so that the segments can be reassembled correctly at the destination.
Internet layer	The Internet layer is comparable to the Network layer of the OSI model. It is responsible for moving packets through a network. This involves addressing and making routing decisions to identify how the packet traverses the network.

Link layer	The Link layer corresponds to the functions of the Physical and Data Link layers of the OSI model. It is responsible for describing the physical layout of the network and how messages are formatted on the transmission medium. Sometimes this layer is divided into the Data Link and the Physical layers.

The TCP/IP model focuses specifically on the functions in the Internet layer and the Transport layer. All other functions of the traditional OSI model are encompassed in the first and fourth layers.

The following table compares the functions performed at each TCP/IP model layer:

Layer	Description
Application (Process-to-Process)	The Application layer contains high-level protocols used by processes (applications) running on a host for network communications. The Application layer integrates network functionality into the host operating system and enables network services. The Application layer does not include specific applications that provide services, but rather provides the capability for services to operate on the network. Processes operating at the Application layer on the source host send data to other processes running on a destination host at the Application layer. For example, a web browser on a client system can send an HTTP GET request to the web service running on a network server to request that it send a particular web page. Processes running on the source host produce the data to be transmitted and encode it using the appropriate Application layer protocol. Some commonly-used Application layer protocols include FTP, HTTP, Telnet, SMTP, DNS, and SSH. Once encoded, the data is then sent to the Transport layer where it is encapsulated using the appropriate Transport layer protocol. The Application layer in the TCP/IP model corresponds to the Session, Presentation, and Application layers of the OSI model.

Transport (Host-to-Host)	The Transport layer is responsible for error checking and reliable delivery. The Transport layer provides the following key functions: ● The sending Transport layer receives a stream of information from the Application layer and breaks it into smaller chunks called *segments*. Segmentation is necessary to enable the data to meet network size and format restrictions. ● The receiving Transport layer uses packet sequence numbers to reassemble segments into the original message. ● The Transport layer establishes a communication channel that can be used to transfer data to a remote host. Protocols that are associated with the Transport layer include: ● Transport Control Protocol (TCP) ○ TCP creates a connection-oriented communication channel. Prior to transmission, TCP negotiates a connection with the remote host using a three-way handshake: ■ The source host sends the destination host a TCP SYN message. ■ The destination host responds with TCP SYN/ACK message. ■ The source host responds with a TCP ACK message. ○ TCP uses acknowledgements after each packet is transmitted to ensure that the data arrived correctly. Any missing, damaged, or discarded packets are retransmitted. ○ TCP ensures a high degree of reliability. However, it also incurs a degree of latency, due to the extra overhead required to ensure data integrity. ○ TCP is most appropriate for communications where data integrity is more important than transmission speed. For example, when saving a file on a network server using the SMB protocol, a few milliseconds of latency is of little concern, but the integrity of the data is critical. ● User-Datagram Protocol (UDP): ○ UDP uses connectionless communications. ○ Unlike TCP, UDP does not set up a connection, nor does it use acknowledgements to ensure the data arrived properly. ○ UDP assumes that lower-level protocols can reliably deliver packets to the destination host.

- This protocol is most appropriate for application-level processes that require low-latency transmissions and can tolerate a degree of missing or out-of-sequence packets.
- UDP is commonly used by streaming audio, streaming video, and Voice over IP (VoIP) applications.

The Transport layer uses ports to enable application-to-application communications between hosts. A port number is logically assigned to each service running on a system. Using ports allows a network host with a single IP address to provide multiple services, each sending and receiving data on its own port. The Transport layer header applied to each segment before transmission identifies the source port on the sending host as well as the destination port on the receiving host. Standardized port numbers have been defined for well-known services. For example:

Service	Port Number
FTP	20 and 21
SSH	22
SMTP	25
DNS	53
HTTP	80
POP3	110
IMAP	143

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>HTTPS</td><td>443</td></tr>
</table>

The Transport layer is comparable to the Transport layer of the OSI model.
</td>
</tr>
<tr>
<td>Internet</td>
<td>The Internet layer is responsible for forwarding packets through multiple networks. This process is called *routing*. The Internet layer manages host addressing and routing decisions to identify how packets traverse networks. Protocols that reside at the Internet layer include:

- Internet Protocol (IP)
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)

The Internet layer uses logically-assigned IP addresses to uniquely identify networks and network hosts. Each address assigned to a host identifies:

- The network the host resides on.
- The host's unique identity on that network.

The Internet layer header applied to each packet before transmission includes the source IP address of the sending host and the destination IP address of the receiving host. When transmitting data, the Internet layer uses the source and destination network addresses to determine whether the hosts reside on the same network or on different networks:

- If they reside on the same network, the data can be sent directly to the destination host.
- If they reside on different networks, the Internet layer forwards packets from router to router until the packets reach the appropriate destination host.

Key Internet layer functions include:

- Maintaining addresses of neighboring routers.
- Maintaining a list of known networks.
- Determining the next network point to which data should be sent. Routers use a routing protocol to take into account</td>
</tr>
</table>

	various factors, such as the number of hops in the path, link speed, and link reliability to select the optimal path for data. The Internet layer is not concerned with reliable delivery of information. Instead, it relies on the Transport layer to establish a host-to-host communication channel and ensure information arrives correctly at the destination host. The Internet layer is comparable to the Network layer of the OSI model.
Link	The Link layer is responsible for describing the physical layout of the network and how messages are electrically transmitted. It is used to move information between hosts by controlling how individual bits are transmitted and received on the network medium. Each host is uniquely identified at the Link layer using a Media Access Control (MAC) address. Every network interface has a physical MAC address assigned to it by the manufacturer. This address is stored in the firmware of the network interface itself. Theoretically, no two network interfaces in the world should have the same MAC address assigned. Unlike an IP address, a MAC address only identifies the host. It does not identify the network where the host resides. As a result, the link layer is not concerned with which network the sending and receiving hosts reside on. It simply transmits data from interface to interface using electrical signals on the network medium. The Link layer converts the data to be transmitted into frames by adding a Link layer header, which includes physical device addressing information. Each frame processed by the Link layer includes the source MAC address and the destination MAC address. The Link layer then converts the frames into bits for transmission across the network media. The Link layer corresponds to the functions of the Physical and Data Link layers of the OSI model.

TCP and UDP Port Numbers

Network ports are logical connections, provided by the TCP or UDP protocols at the Transport layer. Port numbers are used by protocols in the upper layers of the OSI model.

The TCP/IP protocol stack uses port numbers to determine the protocol incoming traffic should be directed to. Below are a few characteristics of ports:

- Ports allow a single host with a single IP address to run network services. Each port number identifies a separate service.
- Each host can have over 65,000 ports per IP address.
- Port use is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN).

ICANN specifies three port categories:

Category	Characteristics
Well-known	A well-known port is: ● Assigned for specific protocols and services. ● Has port numbers ranging from 0 to 1023.
Registered	A registered port: ● Is assigned by ICANN for a newly created network service. ● Has port numbers ranging from 1024 to 49151.
Dynamic (private or high)	A dynamic port: ● Is assigned when a network service establishes contact and released when the session ends. ● Allows applications to listen to the assigned port for other incoming requests. Traffic for a protocol can be received through a port other than the port which the protocol is assigned. This requires that the destination application or service is listening for that type of traffic on that port. ● Has port numbers ranging from 49,152 to 65,535.

The following table lists the well-known ports that correspond to common internet services:

Protocol(s)	Port(s)	Service

TCP	20, 21	File Transfer Protocol (FTP)
TCP, UDP	22	Secure Shell (SSH)
TCP, UDP	23	Telnet
TCP, UDP	25	Simple Mail Transfer Protocol (SMTP)
TCP, UDP	53	Domain Name Server (DNS)
UDP	67, 68	Dynamic Host Configuration Protocol (DHCP)
UDP	69	Trivial File Transfer Protocol (TFTP)
TCP	80	Hypertext Transfer Protocol (HTTP)
TCP	110	Post Office Protocol (POP3)
TCP	119	Network News Transport Protocol (NNTP)
UDP	123	Network Time Protocol (NTP)
TCP	143	Internet Message Access Protocol (IMAP4)
TCP	161, 162	Simple Network Management Protocol (SNMP)
TCP	389	Lightweight Directory Access Protocol (LDAP)
TCP	443	HTTP with Secure Sockets Layer (SSL)