

Introduction to TCP/IP



CLARUSWAY©
WAY TO REINVENT YOURSELF

A Brief History of TCP/IP

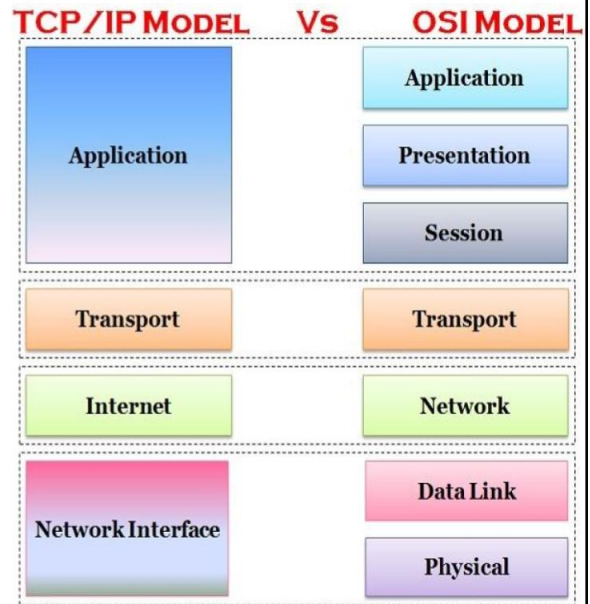
- TCP/IP (*Transmission Control Protocol/Internet Protocol*) is a set of network protocols (*Protocol Suite*) that enable communication between computers
- TCP first came on the scene in 1974
- Divided into two distinct protocols, TCP and IP in 1978
- Became the official means of data transport for ARPANet in 1983
- Mostly developed in UC Berkeley simultaneously with Berkeley version of UNIX (BSD)

CLARUSWAY©
WAY TO REINVENT YOURSELF

TCP/IP and the DoD Model



- The DoD (*Department of Defense*) created TCP/IP to ensure and preserve data integrity
- The DoD model is a condensed version of the OSI model



TCP/IP and the DoD Model



Process/Application layer

- Enables applications to communicate with each other.
- Provides access to the services that operate at the lower layers of the DoD model.
- It contains a protocol that implements user-level functions such as mail delivery, file transfer, and remote login.
- Includes all higher-level protocols: DNS, HTTP, Telnet, SSH, FTP, SNMP, DHCP, etc.

DNS: Domain Name Service
 HTTP: Hyper-text Transfer Protocol
 SSH: Secure Shell
 FTP: File Transfer Protocol
 SNMP: Simple Network Management Protocol
 DHCP: Dynamic Host Configuration Protocol

TCP/IP and the DoD Model

Host-to-Host Layer (Transport Layer)

- Permits devices on the source and destination to carry on a conversation
- Defines the level of service and status of the connection used when transporting data
- Main protocols are TCP and UDP

TCP/IP and the DoD Model

Internet Layer

- Packs data into data packets known as IP datagrams
- Responsible for routing of IP datagrams
- Main protocols are IP, ICMP, ARP, RARP, and IGMP

► TCP/IP and the DoD Model

Network Access Layer

- Defines details of how data is physically sent through the network
- Main protocols are Ethernet, Token Ring, FDDI, X.25, and Frame Relay

► The Process/Application Layer Protocols

Telnet (TCP 23): Allows a user on a remote client machine to access the resources of another machine.

SSH (TCP 22): Secure Shell Protocol sets up a secure session that's similar to Telnet over a standard TCP/IP connection and is employed for doing things like logging into systems, running programs on remote systems and moving file from one system to another system.

▶ The Process/Application Layer Protocols »

FTP (TCP 20, 21): File Transfer Protocol lets us transfer files between any two machines. FTP functions are limited to listing and manipulating directories, typing file contents, and copying files between hosts.

SFTP (TCP 22): Same as FTP but Secure FTP uses an encrypted connection through an SSH session, which encrypts the connection, and SSH uses port 22.

TFTP (UDP 69): Trivial FTP is the stripped-down, stock version of FTP. TFTP is fast and so easy to use. It can only send and receive files.

▶ The Process/Application Layer Protocols »

POP (TCP 110): Post Office Protocol gives us a storage facility for incoming mail (the latest version is POP3). A newer standard, IMAP, is being used more and more in place of POP3.

IMAP (TCP 143): Internet Message Access Protocol makes it so you get control over how you download your mail, with it, you also gain some much-needed security. It has some serious authentication features. IMAP4 is the current version.

▶ The Process/Application Layer Protocols »

RDP (TCP 3389): Remote Desktop Protocol is a proprietary protocol developed by Microsoft. It allows you to connect to another computer and run programs. Clients exist for most versions of Windows, and Macs now come with a preinstalled RDP client.

TLS/SSL (TCP 995/465): Both Transport Layer Security and its forerunner, Secure Sockets Layer, are cryptographic protocols that are useful for enabling secure online data-transfer activities like browsing the Web, instant messaging, Internet faxing, and so on.

▶ The Process/Application Layer Protocols »

SIP (VoIP) (TCP or UDP 5060/TCP 5061): Session Initiation Protocol is a hugely popular protocol used to construct and deconstruct multimedia communication sessions for many things like voice and video calls, videoconferencing, streaming multimedia distribution, instant messaging, presence information, and online games over the Internet.

RTP (VoIP) (UDP 5004/TCP 5005): Real-time Transport Protocol describes a packet-formatting standard for delivering audio and video over the Internet.

▶ The Process/Application Layer Protocols »

MGCP (Multimedia) (TCP 2427/2727): Media Gateway Control Protocol is a standard protocol for handling the signaling and session management needed during a multimedia conference.

H.323 (Video) (TCP 1720): H.323 is a protocol that provides a standard for video on an IP network that defines how real-time audio, video, and data information is transmitted.

Cl
wa

▶ The Process/Application Layer Protocols »

SNMP (UDP 161/TCP 25): Simple Network Management Protocol collects and manipulates valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. This protocol can also stand as a watchdog over the network, quickly notifying managers of any sudden turn of events. Besides, SNMP can help simplify the process of setting up a network as well as the administration of your entire internetwork.

▶ The Process/Application Layer Protocols »

HTTP (TCP 80): Hypertext Transfer Protocol is used to manage communications between web browsers and web servers.

HTTPS (TCP 443): HTTP Secure uses the Secure Socket Layer (SSL). It is the secure version of the HTTP.

NTP (UDP 123): Network Time Protocol is used to synchronize the clocks on our computer to one standard time source. This protocol works by synchronizing devices to ensure that all the computers on a given network agree on the time.

▶ The Process/Application Layer Protocols »

LDAP (TCP 389): Lightweight Directory Access Protocol standardizes how you access directories.

IGMP: Internet Group Management Protocol is the TCP/IP protocol used for managing IP multicast sessions. It accomplishes this by sending out unique IGMP messages over the network to reveal the multicast-group landscape and to find out which hosts belong to which multicast group. IGMP works at the Network layer and doesn't use port numbers.

▶ The Process/Application Layer Protocols »

DHCP (UDP 67/68): Dynamic Host Configuration Protocol assigns IP Address to hosts. It allows for easier administration and works well in small to very large network environments. Many types of hardware can be used as a DHCP Server, including a Cisco Router. There is a lot of information a DHCP server can provide to a host when the host is requesting an IP address from DHCP Server like

- IP Address
- Subnet Mask
- Domain Name
- Default Gateways
- DNS Server Address

▶ The Transport Layer Protocols »

- **TCP** and **UDP** are the main protocols for Transport Layer
- **TCP** is full-duplex, connection-oriented, reliable and accurate protocol
- In order to send information, TCP establishes a connection with the receiving host (connection-oriented)
- **TCP** takes information and breaks it into segments
- **TCP** sends this segments in the order that application intended
- After segments are sent **TCP** waits for the acknowledgement for each segment
- Retransmits the segments that aren't acknowledged (reliable)



The Transport Layer Protocols

- **UDP** uses less bandwidth compared to **TCP**
- **UDP** transports data much faster than **TCP**
- **UDP** doesn't care the order of the segments
- **UDP** doesn't care if the segment is received by the recipient (no acknowledgement) (*not reliable*)
- **UDP** doesn't establish a connection with the receiver (*connectionless protocol*)
- Mostly used while speed is more important than reliability (like video teleconferencing or SNMP)



The Transport Layer Protocols

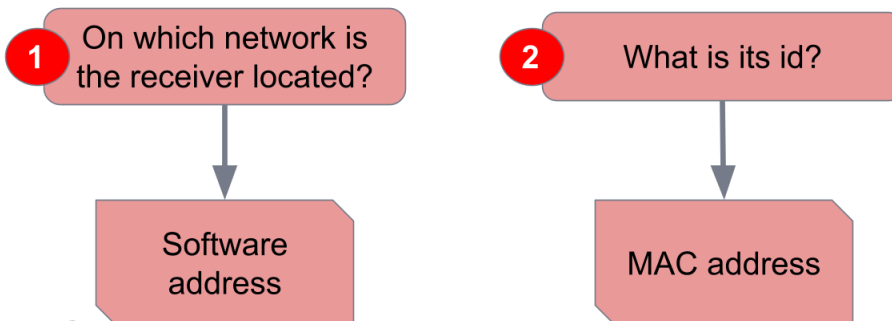
| TCP | UDP |
|-------------------------|--------------------|
| Secure | Unsecure |
| Connection-oriented | Connectionless |
| Slow | Fast |
| Guaranteed transmission | No guarantee |
| Flow control | No flow control |
| Reliable | Unreliable |
| Virtual circuit | No virtual circuit |
| Acknowledgement | No acknowledgement |
| 20 bytes header | 8 bytes header |

The Internet Layer Protocols

- Main functions: routing and providing a single network interface to upper layers
- Main protocols:
 - Internet Protocol (IP)
 - Internet Control Message Protocol (ICMP)
 - Address Resolution Protocol (ARP)
 - Reverse Address Resolution Protocol (RARP)

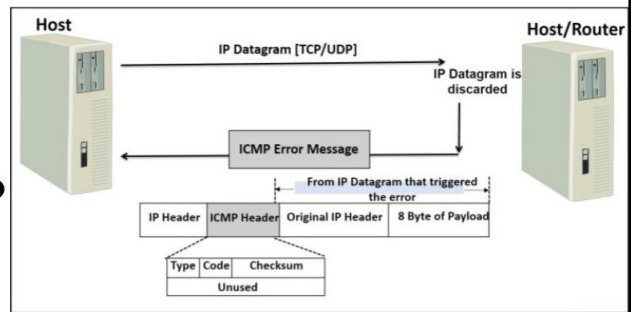
The Internet Layer Protocols

- **Internet Protocol (IP)** looks at each packet's destination address, then, using a routing table, it decides where a packet is to be sent next, choosing the best path.
- To find the receiver host, sender has to find out:



The Internet Layer Protocols

- **Internet Control Message Protocol (ICMP)** is a management protocol and messaging service provider for IP
- **ICMP** messages are sent as IP packets
- Common events that **ICMP** relates to:
 - Destination unreachable
 - Buffer full
 - Hops
- **Ping** and **Traceroute** use **ICMP**



CLARUSWAY©
WAY TO REINVENT YOURSELF

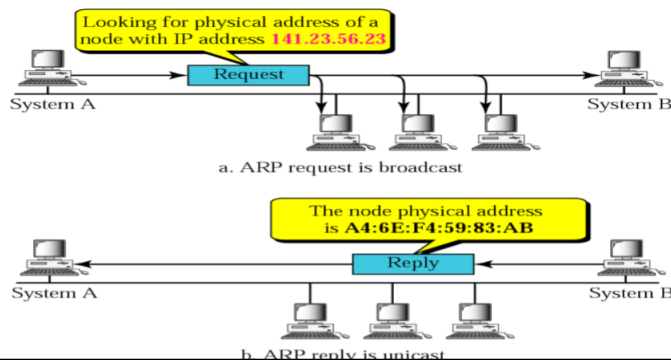
The Internet Layer Protocols

- **Address Resolution Protocol (ARP)** is a procedure for mapping a dynamic **IP address** to a permanent physical machine address in a LAN
- Essentially matches

IPv4 Address
32-bit

↔

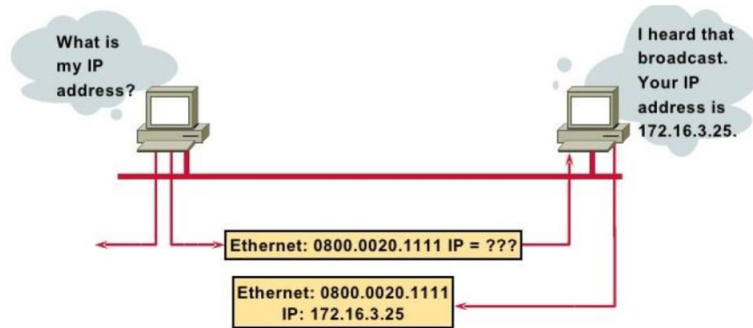
MAC Address
48-bit



CLARUSWAY©
WAY TO REINVENT YOURSELF

The Internet Layer Protocols

- Host machines that don't know their own IP address can use the **Reverse ARP (RARP)** protocol for discovery



- ARP is replaced by **Neighbor Discovery Protocol** with the use of IPv6