Introduction to TCP/IP

CLARUSWAY©
WAY TO REINVENT YOURSELF

Table of Contents

CLARUSWAY©
WAY TO REINVENT YOURSELF

1 A Brief History of TCP/IP

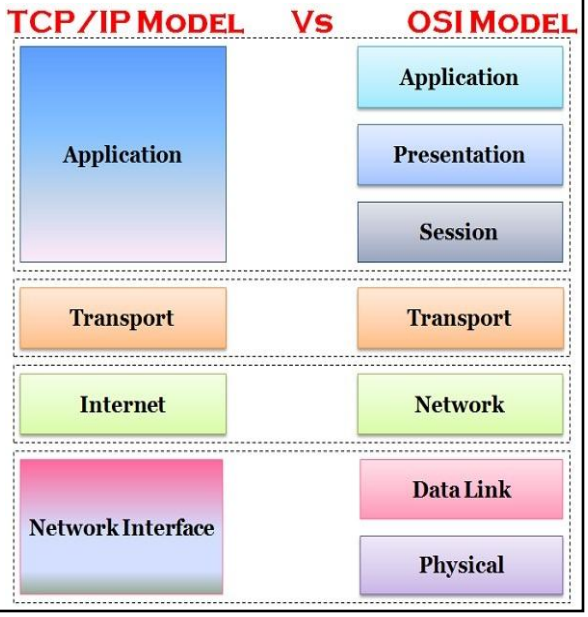
A Brief History of TCP/IP

- 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 officials means of data transport for ARPANet in 1983
- Mostly developed in UC Berkeley simultaneously with Berkeley version of UNIX (BSD)

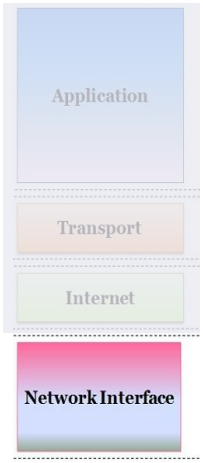
2 TCP/IP and the DoD Model

TCP/IP (DoD) and the OSI 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

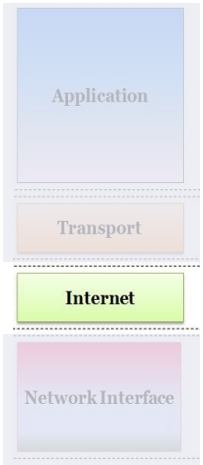


Network Access Layer

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

FDDI: Fiber Distributed Data Interface

TCP/IP and the DoD Model

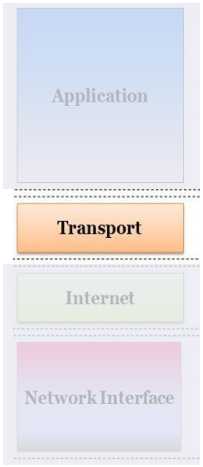


Internet Layer

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

IP: Internet Protocol
ICMP: Internet Control Message Protocol
ARP: Address Resolution Protocol
RARP: Reverse Address Resolution Protocol
IGMP: Internet Group Message Protocol

TCP/IP and the DoD Model

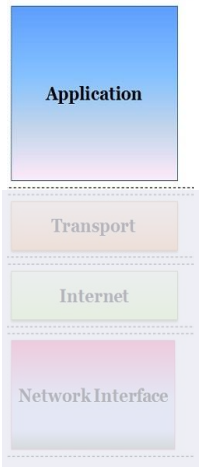


Host-to-Host Layer (Transport Layer)

- 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: Transmission Control Protocol
UDP: User Datagram Protocol

TCP/IP and the DoD Model



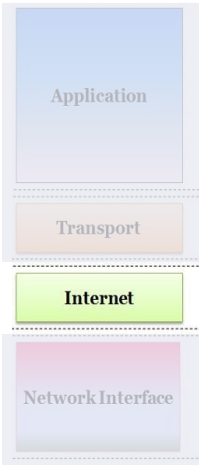
Process/Application layer

- 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

5 The Internet Layer Protocols

The Internet Layer Protocols

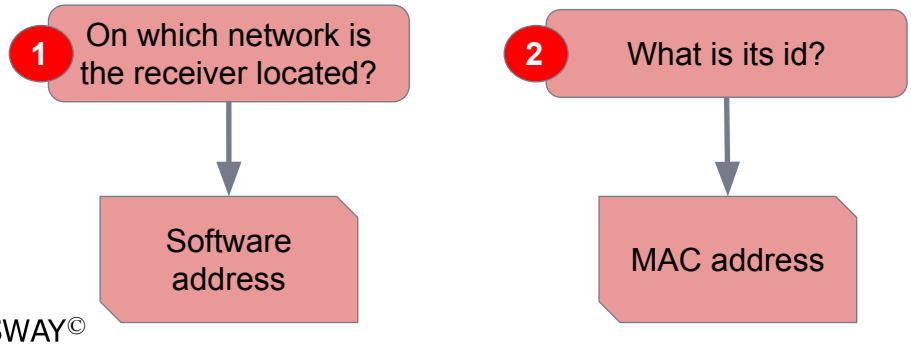


- Main functions: routing and providing a single network interface to upper layers

- Main protocols:
  - Internet Protocol (IP)
  - Internet Control Message Protocol (ICMP)
  - Address Resolution Protocol (ARP)
  - Reverse Address Resolution Protocol (RARP)

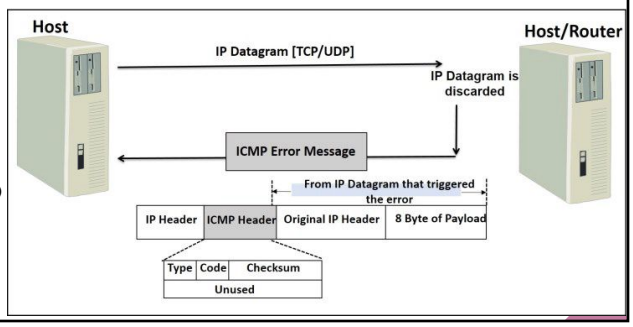
The Internet Layer Protocols

- **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:



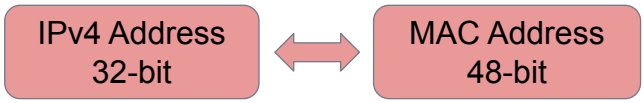
The Internet Layer Protocols

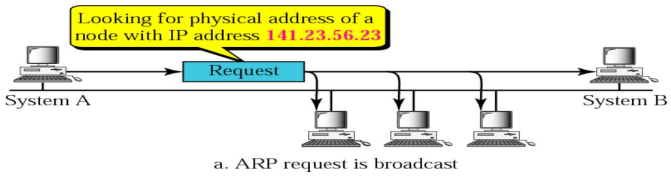
- **Internet Control Message Protocol (ICMP)** is a management protocol and messaging service provider for IP
- **ICMP** messages are sent as IP packets
- Common events that **ICMP** relates to:
  - Destination unreachable
  - Buffer full
  - Hops
- **Ping** and **Traceroute** use **ICMP**



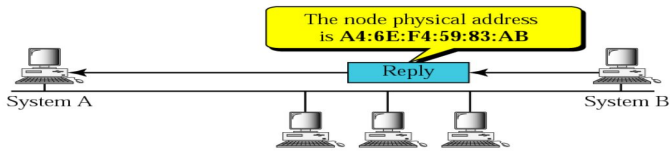
The Internet Layer Protocols

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





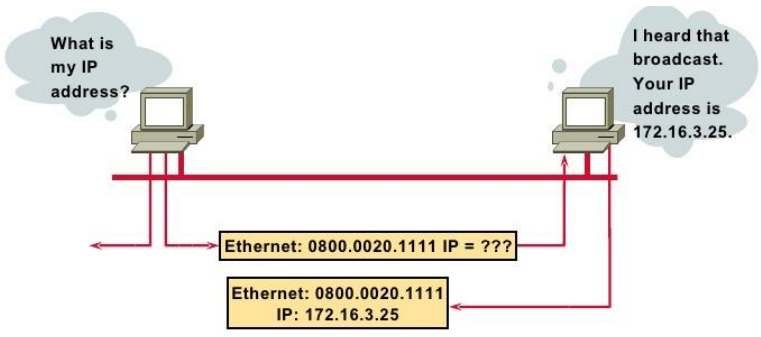
a. ARP request is broadcast



b. ARP reply is unicast

The Internet Layer Protocols

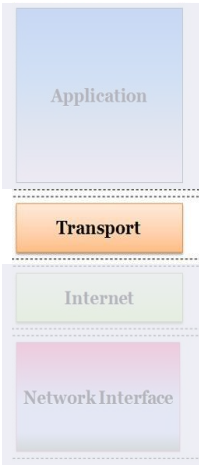
- Host machines that don't know their own IP address can use the **Reverse ARP (RARP)** protocol for discovery



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

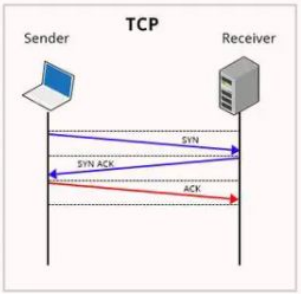
4 The Transport Layer Protocols

The Transport Layer Protocols



- **TCP** and **UDP** are the main protocols for Transport Layer
- Transport layer defines a **protocol** as well as a **port**

The Transport Layer Protocols

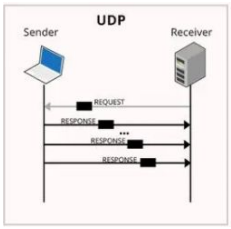


TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

- **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

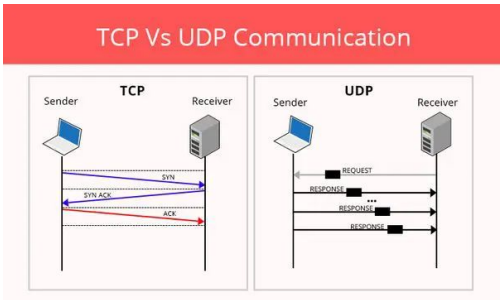


UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

- **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 Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

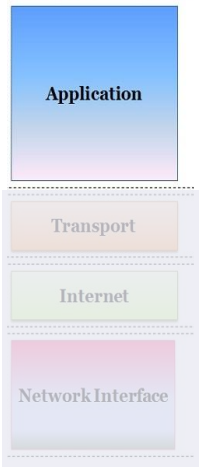
Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

The Transport Layer Protocols

TCP	UDP
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 byte header	8 byte header

3 The Process/Application Layer Protocols

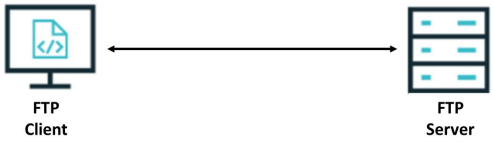
Application Layer



- There are many application layer protocols:
  - Remote access (SSH, RDP, ...)
  - File Transfer (FTP, FTPS, SFTP, ...)
  - Email (POP, IMAP, SMTP, ...)
  - Web (HTTP, HTTPS)

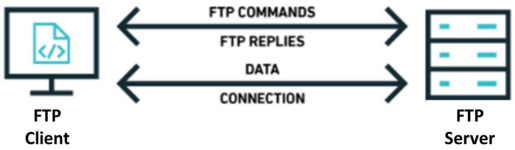
FTP Protocol

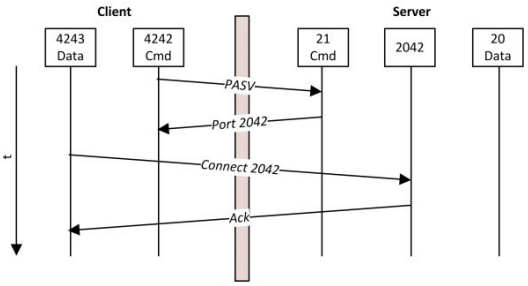
- **F**ile **T**ransfer **P**rotocol lets us transfer files between any two machines.
- Uses TCP protocol on port 20 and 21
- FTP functions are limited to listing and manipulating directories, typing file contents, and copying files between hosts.



FTP Protocol Elements

- **Channels**
  - Data
  - Connection (control)
- **Data Structures**
  - File, Record, Page
- **FTP Commands**
  - USER
  - PASS
  - LIST
  - MKD
  - ...
- **FTP Replies**
  - 200 - Okay
  - 530 - Not logged in
  - 225 - Data connection open; no transfer in progress
  - ...



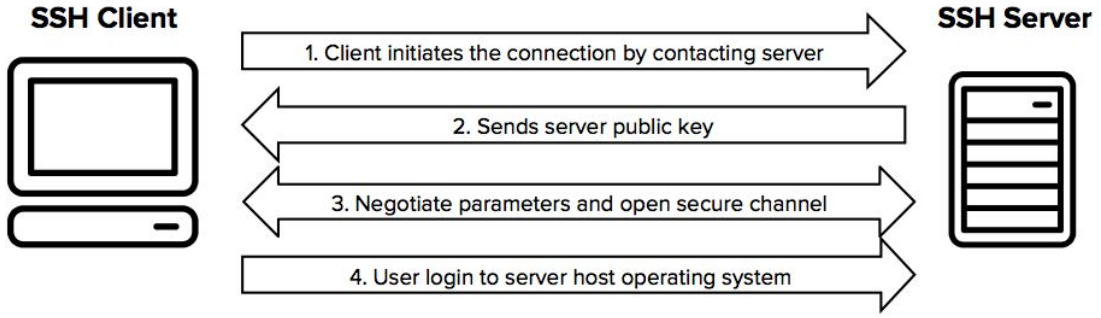


Other File Transfer Protocols

Name	TCP/UDP	Port	Description
FTPS	TCP	20/21	**FTP Secure** is an extension of FTP that adds support for TLS encryption.
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.
SFTP	TCP	22	Same as FTP but **Secure FTP** uses an encrypted connection through an SSH session, which encrypts the connection.

SSH Protocol

- **S**ecure **Sh**ell protocol creates a secure connection to enable users to execute commands on remote machines
- Uses TCP Port 22

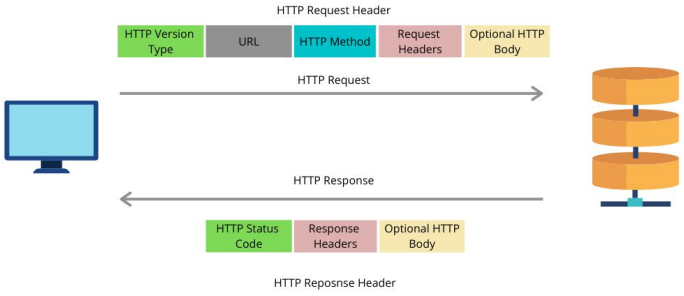


Other Remote Access Protocols

Name	TCP/UDP	Port	Description
Telnet	TCP	23	**Teletype Network Protocol** allows a user on a remote client machine to access the resources of another machine. Uses plain text communication.
RDP	TCP	3389	**Remote Desktop Protocol** is a proprietary protocol developed by Microsoft. It allows you to connect to another computer and run programs. Windows, and Macs now come with a preinstalled RDP client.

HTTP and HTTPS Protocols

- **Hypertext Transfer Protocol** (HTTP) is used for communication between clients and web servers
- Uses TCP Port 80
- HTTPS adds encryption via TLS (or SSL) and instead uses port 443
- Example Methods:
  - GET
  - POST
  - ...
- Example Response Codes
  - 200: The request was successful
  - 404: Page not found



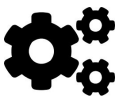
Email Protocols

Name	TCP/UDP	Port	Description
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.

Multimedia Protocols

Name	TCP/UDP	Port	Description
SIP (VoIP)	TCP or UDP	5060 or 5061	**Session Initiation Protocol** is a popular protocol used to for multimedia communication sessions for many things like voice and video calls, streaming, instant messaging, and online games over the Internet.
RTP (VoIP)	UDP TCP	5004 5005	**Real-time Transport Protocol** describes a packet-formatting standard for delivering audio and video over the Internet.
MGCP	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	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.

Utility Protocols



Name	TCP/UDP	Port	Description
SNMP	UDP TCP	161 25	**Simple Network Management Protocol** collects and manipulates valuable network information. It gathers data by polling the devices on the network. This protocol can also stand as a watchdog over the network or simplify network management.
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.

DHCP

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

LDAP

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

Encryption Protocols

TLS/SSL: 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.

THANKS!

Any questions?

You can find me at:

- @Altaz - Instructor
- altaz@clarusway.com