TCP/IP Protocols

Layer	Protocols
Application	FTP, TFTP, DNS, HTTP(S), TLS/SSL, SSH, POP3, IMAP4, NTP, Telnet, SMTP, SNMP
Transport	TCP, UDP and Ports
Internet	IP Addressing (Routing), ICMP, ARP
Network Interface	Ethernet, Token Ring

These protocols work together to provide communication, management, diagnostics, and troubleshooting for a TCP/IP network.

Network Access Methods

CSMA

- Carrier Sense
  - Checks network for communication.
- Multiple Access
  - Multiple devices using the network.
- Collision Detection
  - Wired Network
- Collision Avoidance
  - Wireless Network

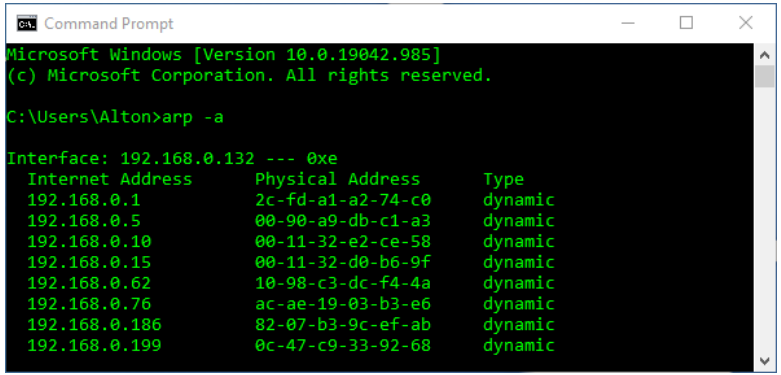
Token Ring

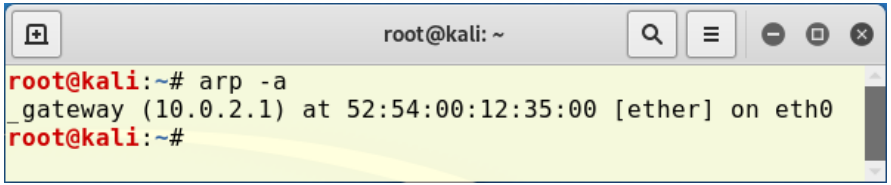
- The Token
  - Passed between devices on the network.
  - Only devices with the token can send data.
  - Token prevents network collisions.

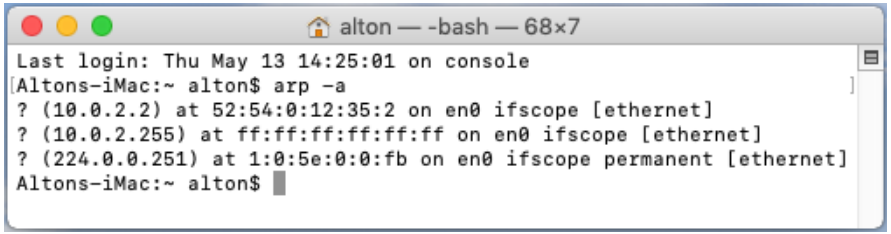
Address Resolution Protocol (ARP)

- Resolves IP address to MAC Addresses
- Finds the hardware address of a host from a know IP address
  - And vice versa (RARP)

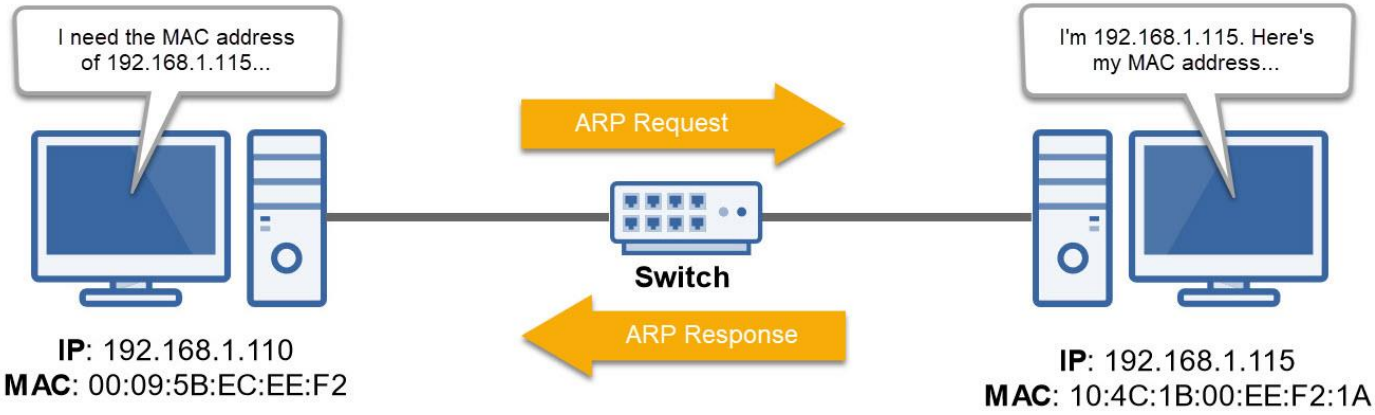
ARP Command: arp -a







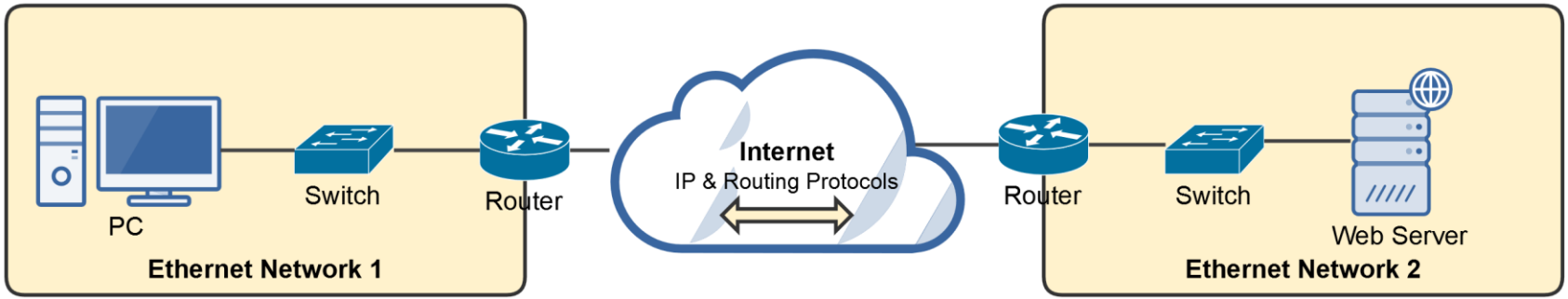
ARP Diagram



If a computer knows a device's IP address but not its MAC address, it'll send a **broadcast** message to all devices on the LAN asking which device is assigned that MAC address.

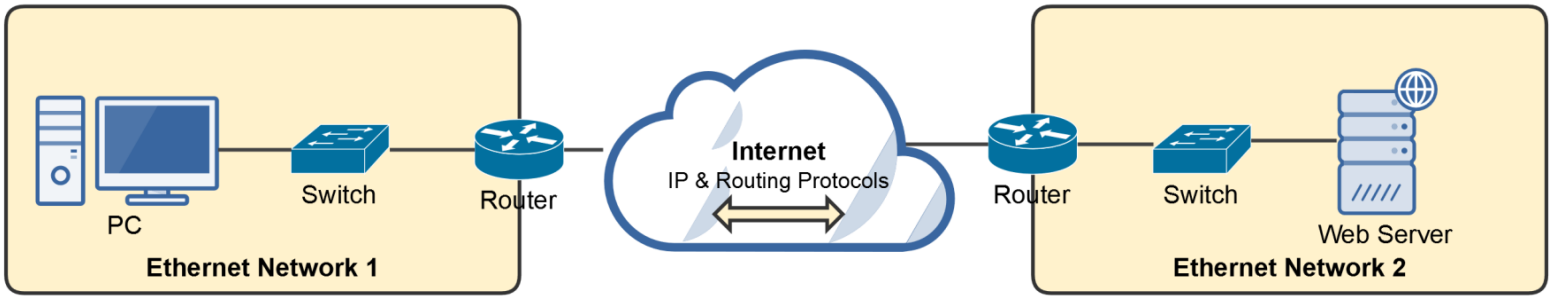
The Internet Protocol (IP)

- An OSI Layer 3 protocol that defines routing and logical addressing of packets that allow data to traverse WANs and the Internet.
- It specifies the formatting of packets and the logical addressing schema
  - **IP addresses**: IPv4 and IPv6
- Its job is to connect different OSI Layer 2 (switched) networks together.
- Provides end-to-end connectivity from one Layer 2 network to another via routers.



The Internet Protocol (IP)

- It's connectionless and, therefore, unreliable (similar to UDP).
  - No continued connection.
- Each packet sent is independent of each other packet.
  - TCP and other protocols provide a means to reassemble them properly.
- Packets don't always follow the same path to their destination.
  - They're sent via the most efficient route.
- Doesn't provide any error recovery or sequencing functionality.
  - That's the job of other protocols.



Internet Control Message Protocol (ICMP)

- OSI Layer 3 Internet Protocol (IP) companion “error reporting” protocol within the TCP/IP suite of protocols.
- Just like IP, it’s connectionless.
- Used to generate error messages to the source IP address when network issues prevent the delivery of a packet.
- Typically used by routers to report packet delivery issues, and, most importantly, it can report errors but not correct them.
- Commonly used by IT administrators to troubleshoot network connections with command-line utilities, including ping, pathping, and traceroute.
- For IPv6, it is also used for:
    - Neighbor Solicitation and Advertisement Messages (Similar to ARP)
    - Router Solicitation and Advertisement Messages

(Some) ICMP Message Types

- **Echo Request, Echo Reply**: Tests destination accessibility and status. A host sends an *Echo Request* and listens for a corresponding *Echo Reply*. Commonly done using the **ping** command.
- **Destination Unreachable**: Sent by a router when it can't deliver an IP packet.
- **Source Quench**: Sent by a host or router if it's receiving too much data than it can handle. The message requests that the source reduces its rate of data transmission.
- **Redirect Message**: Sent by a router if it receives a packet that should have been sent to a different router. The message includes the IP address to which future packets should be sent and is used to optimize the routing.
- **Time Exceeded**: Sent by a router if a packet has reached the maximum limit of routers through which it can travel.
- **Router Advertisement, Router Solicitation (IPv6)**: Allow hosts to discover the existence of routers. Routers periodically multicast their IP addresses via *Router Advertisement* messages. Hosts may also request a router IP address by broadcasting a *Router Solicitation* message, then wait for a router to reply with a *Router Advertisement*.

Understanding Protocols, Ports, and Sockets

Protocols

- Computers communicate with each other with network protocols.
- Protocols are rules governing how machines exchange data and enable effective communication.
- In an operating system (OS), a protocol runs as a process or service.

Ports

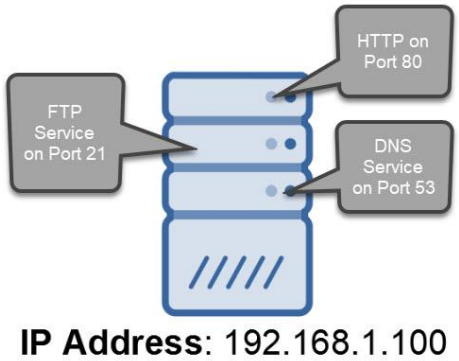
- Ports are logical constructs that bind a unique port number to a protocol process or service.

Sockets

- Sockets are a combination of an IP address and a port number, for example, 192.168.1.1:80.

Why We Need Ports and Sockets

- Computers require ports because of network application multitasking.
- Because a computer may have only one IP address, it needs ports to differentiate network protocols and services running on it.
- TCP/IP has 65,536 ports available



Port Type	Port Numbers	Description
Well Known Ports	0 – 1023	Assigned to well-known protocols.
Registered Ports	1024 – 49,151	Registered to specific protocols.
Dynamic Ports	49,152 – 65,535	Not registered and used for any purpose.

Protocols & Port Numbers

Service, Protocol, or Application	Port Number(s)	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
Secure FTP (SFTP)	22	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System)	53	UDP
DHCP (Dynamic Host Configuration Protocol)	67, 68	UDP
TFTP (Trivial File Transfer Protocol)	69	UDP
HTTP (Hypertext Transfer Protocol)	80	TCP
POP3 (Post Office Protocol version 3)	110	TCP

Protocols & Port Numbers

Service, Protocol, or Application	Port Number(s)	TCP or UDP
NTP (Network Time Protocol)	123	UDP
IMAP4 (Internet Message Access Protocol version 4)	143	TCP
SNMP (Simple Network Management Protocol)	161	UDP
LDAP (Lightweight Directory Access Protocol)	389	TCP
HTTPS (Hypertext Transfer Protocol Secure)	443	TCP
Server Message Block (SMB)	445	TCP
LDAPS (Lightweight Directory Access Protocol Secure)	636	TCP
RDP (Remote Desktop Protocol)	3389	TCP
ITU Telecommunication Standardization Sector A/V Recommendation (H.323)	1720	TCP
Session Initiation Protocol (SIP)	5060, 5061	TCP

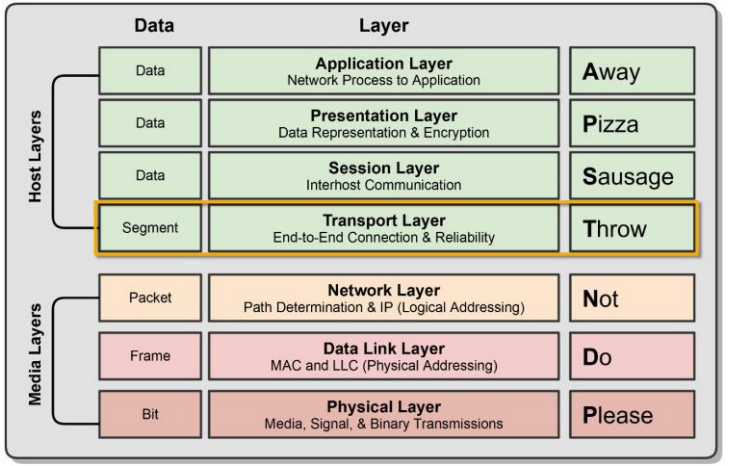
TCP vs. UDP

Transport Layer Protocols

- **TCP** (Transmission Control Protocol): Connection-Oriented
- **UDP** (User Datagram Protocol): Connectionless

TCP is the most widely used Transport Layer protocol because it is connection-oriented, which provides packet delivery reliability, i.e., guaranteed delivery.

UDP, being connectionless, is considered to be unreliable; however, it is more lightweight than TCP and often used for streaming or real-time data.



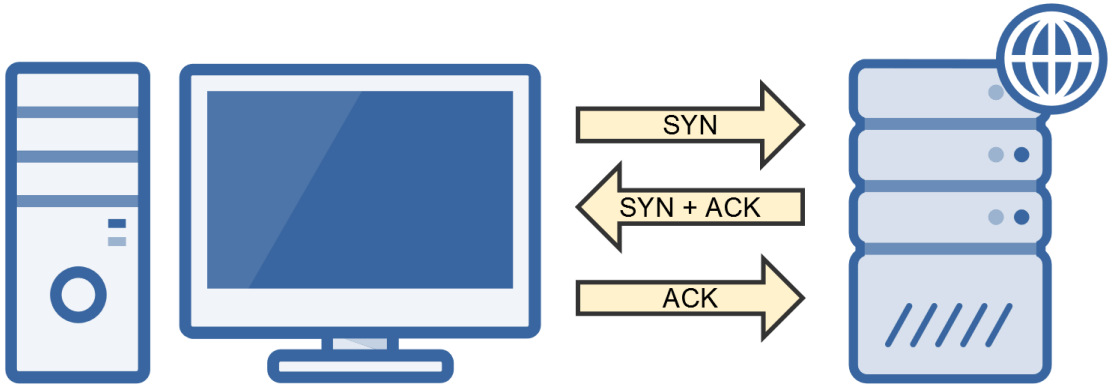
TCP Reliability

- TCP utilizes the following features to ensure reliable delivery of data.
  - **3-Way Handshake** creates a virtual connection between the source and destination before data is sent.
  - **Acknowledgment** is required before the next segment is sent.
  - **Checksum** that detects corrupted data.
  - **Sequence Numbers** that detect missing data and reassemble them in the correct order.
  - **Retransmission** that will retransmit lost or corrupt data.

- **Note**: TCP header is 20 bytes in size, whereas the UDP header is only 8 bytes.

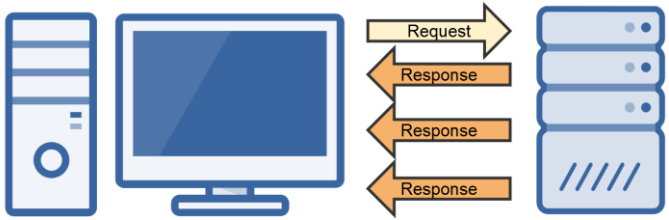
TCP Three-Way Handshake

- A connection must be established before data is transmitted, called the three-way handshake.
  - SYN → SYN / ACK → ACK
- Creates a Virtual Connection Between 2 Devices



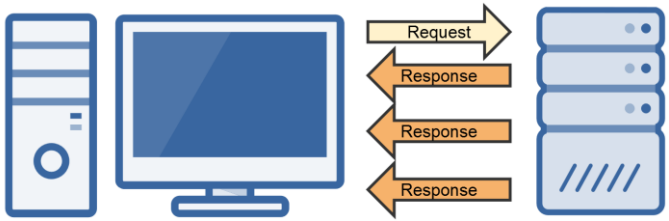
“Best Effort” UDP

- A scaled-down, economic version of TCP
  - Connectionless & Unreliable
  - No Data Retransmissions
  - “Best Effort”
- Faster than TCP
  - Smaller Header & Connectionless
- Primarily used for protocols that favor:
  - Low-Latency, i.e., Faster Speeds
  - Can Tolerate Data Loss



"Best Effort" UDP

- Example UDP Use-Cases
  - VoIP Phone Calls
  - Live Video Streams
  - Live Audio Streams
  - Online Gaming
  - Certain Network Management Protocols
    - DNS
    - DHCP
    - NTP



Application Layer Management Protocols

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)
- Simple Network Management Protocol (SNMP)
- Lightweight Directory Access Protocol (LDAP)
- LDAP Secure (LDAPS)
- Server Message Block (SMB)

Domain Name System (DNS)

Port: 53 **Transport Layer Protocol:** UDP

- Protocol that is used to resolve a domain name to its corresponding IP address
  - InstructorAlton.com → 162.0.232.236
- Uses TCP port 53 by default
- We'll be discussing DNS in detail in the **DNS Network Services** section of this course:
  - DNS Hierarchy
  - DNS Record Types
  - Name Resolution

Dynamic Host Configuration Protocol (DHCP)

Ports: 67, 68 **Transport Layer Protocol:** UDP

- Protocol that automatically assigns IP address configurations to devices on a network:
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS Server
- We'll be discussing how DHCP works in detail in the **Assigning IP Addresses** section of this course
- Uses two UDP ports 67 and 68 by default

Network Time Protocol (NTP)

Port: 123 **Transport Layer Protocol:** TCP

- Protocol that automatically synchronizes a system's time with a network time server.
  - Important for time-dependent network applications and protocols.
  - If a system is configured with the incorrect time, it may not be able to access network services.
  - Authentication will often fail if time isn't properly synchronized between devices.
- Uses TCP port 123 by default.