TCP/IP Model and IP Addressing

TCP/IP Model

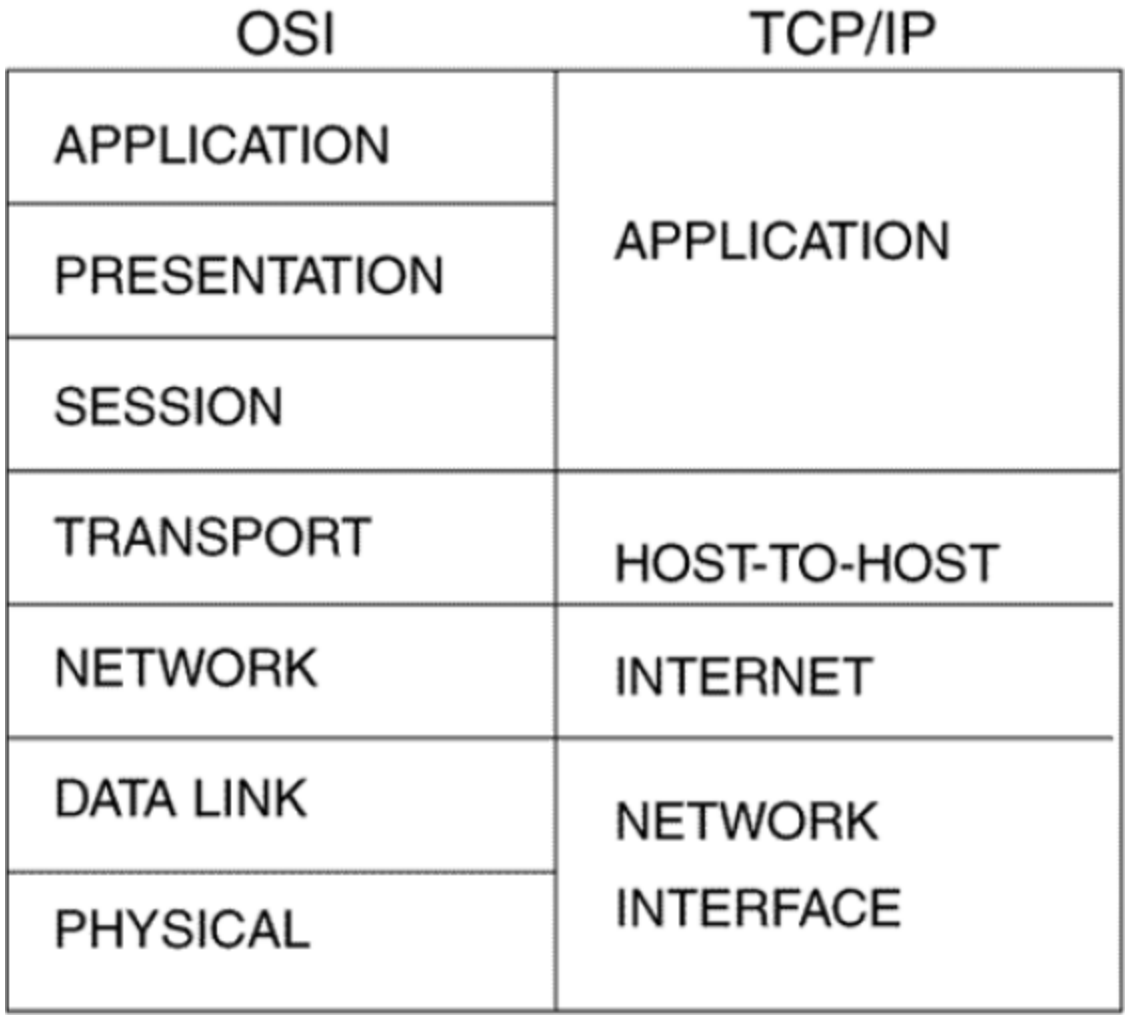
- This model has 4 layers compared to OSI which has 7 layers.
- It combines OSI's several layers to one layer.
- TCP/IP uses the client/server model of communication in which a user or machine by is provided a service by another computer in the network.
- Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continuously.
- The transport layer itself, however, is stateful . It transmits a single message, and its connection remains in place until all the packets in a message have been received and reassembled at the destination.
- TCP/IP grew out of U.S. Department of Defence networking research.
- TCP/IP is known as "the language of the Internet." If you want a computer to work on the Internet, you have to use TCP/IP.

Features of TCP/IP

- 1) **Multi-Vendor Support.** TCP/IP is implemented by many hardware and software vendors. It is an industry standard and not limited to any specific vendor.
- 2) **Interoperability.** Today we can work in a heterogeneous network because of TCP/IP. A user who is sitting on a Windows box can download files from a Linux machine, because both Operating Systems support TCP/IP. TCP/IP eliminates the cross-platform boundaries.
- 3) **Logical Addressing.** Every network adapter has a globally unique and permanent physical address, which is known as MAC address (or hardware address). The physical address is burnt into the card while manufacturing. Low-lying hardware-conscious protocols on a LAN deliver data packets using the adapter's physical address. The network adapter of each computer listens to every transmission on the local network to determine whether a message is addressed to its own physical address.

Continue…

- 4) **Routability.** A router is a network infrastructure device which can read logical addressing information and direct data across the network to its destination.TCP/IP is a routable protocol, which means the TCP/IP data packets can be moved from one network segment to another.
- 5) **Name Resolution**. IP addresses are designed for the computers and it is difficult for humans to remember many IP addresses. TCP/IP allows us to use human-friendly names, which are very easy to remember (Ex. www.omnisecu.com). Name Resolutions servers (DNS Servers) are used to resolve a human readable name (also known as Fully Qualified Domain Names (FQDN)) to an IP address and vice versa.
- 6) **Error Control and Flow Control**. The TCP/IP protocol has features that ensure the reliable delivery of data from source computer to the destination computer. TCP (Transmission Control Protocol) defines many of these error-checking, flow-control, and acknowledgement functions.
- 7) **Multiplexing/De-multiplexing.** Multiplexing means accepting data from different applications and directing that data to different applications listening on different receiving computers. On the receiving side the data need to be directed to the correct application, for that data was meant for. This is called De-multiplexing. We can run many network applications on the same computer. By using logical channels called ports, TCP/IP provides means for delivering packets to the correct application. In TCP/IP, ports are identified by using TCP or UDP port numbers.


OSI
TCP/IP
APPLICATION
PRESENTATION
SESSION
APPLICATION
TRANSPORT
HOST-TO-HOST
NETWORK
INTERNET
DATA LINK
PHYSICAL
NETWORK
INTERFACE

TCP/IP Model Layers

- TCP/IP functionality is divided into 4 layers , each of which include specific protocols.
- **Application Layer :** It provides applications with standardized data exchange . Its protocols include Hypertext Transfer Protocol(HTTP), File Transfer Protocol(FTP),Post Office Protocol 3(POP3),Simple Mail Transfer Protocol(SMTP) and Simple Network Management Protocol(SNMP).
- **Transport Layer :** It is responsible for maintaining end-to-end communications across this network . TCP handles communications between hosts and provides flow control , multiplexing and reliability. The transport protocol includes TCP and UDP.
- **Network Layer :**It is also known as internet layer. It deals with packets and connects independent networks to transport the packets across network boundaries . The protocols at this layer are IP and Internet Control Messaging Protocol (ICMP), which is used for error reporting.
- **Network Interface Layer :** It consists of protocols that operate only on a link – the network component that interconnects nodes or hosts in the network . The protocols are Ethernet and Address Resolution Protocol (ARP).

Advantages of TCP/IP

- TCP/IP is non-proprietary and therefore not controlled by any single company.
- IP Suite can be modified easily.
- It is compatible with all Operating systems.
- IP Suite is also compatible with all types of computer hardware and networks.
- It can determine the most efficient path through the network.

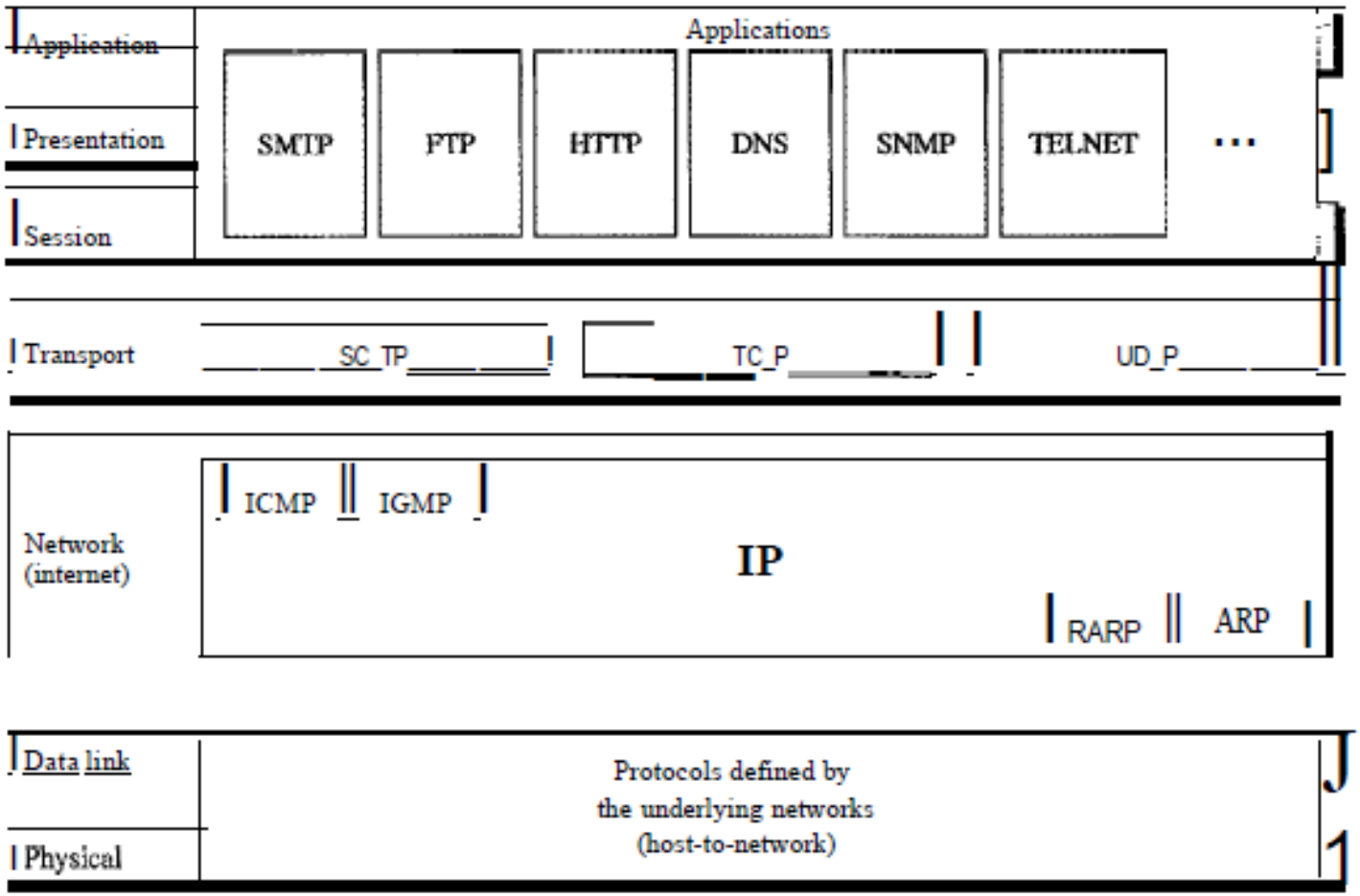
Similarities between TCP/IP model and OSI Model

- TCP/IP model was created in 1970’s while OSI Model was created in 1980’s.
- IP corresponds to a subset of OSI Layer 3.
  - IP Describes only the protocol used for internet ,while OSI Layer 3 also encompasses non-internet protocols such as Datagram Delivery Protocol.
- TCP corresponds to OSI Layer 4 and some functions of Layer 5.
  - OSI Layer 4 ensures delivery of data from one node to another by doing things like assigning sequential numbers to packets , checking to make sure all sent packets arrive and retransmitting lost or damaged packets . TCP is responsible for these functions as well.
  - OSI Layer 5 sets up and terminates connections between nodes as TCP but also handles authentication and authorization.

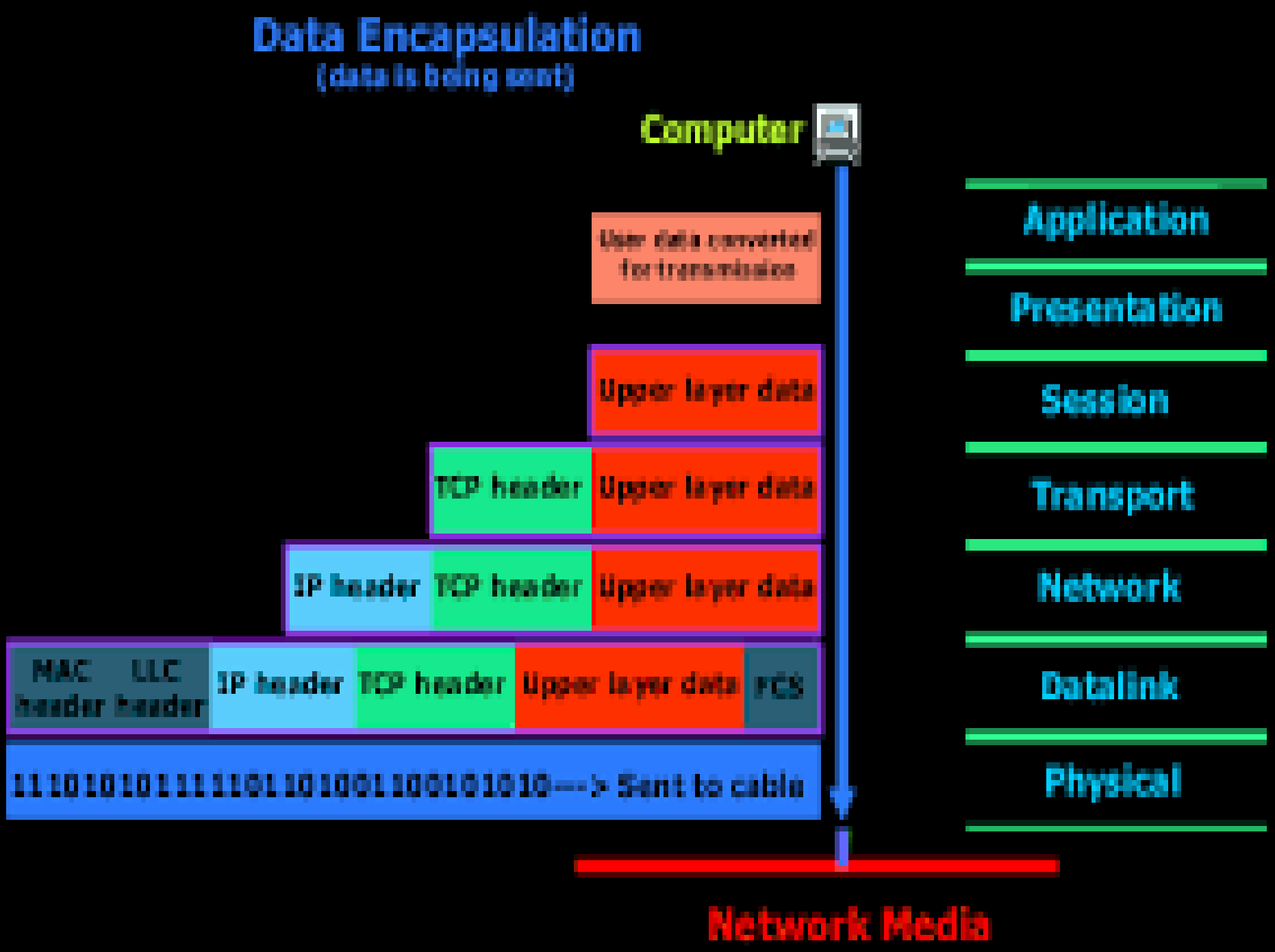
Protocols at Every Layer

OSI Model	TCP/IP Model	PDU	Protocols	Network Devices
7. Application	Application	Data	HTTP, SMTP, FTP, Telnet, SSH, DNS, DHCP, POP, IRC, SMB	
6. Presentation			.jpg, .zip, ASCII, .mp3	
5. Session				
4. Transport	Transport	Segments	TCP, UDP Port Numbers	Layer 4 Switches
3. Network	Internet	Packets	IP Addresses Logical Addressing	Routers
2. Data Link	Network Access	Frames	MAC Addresses Physical Addressing	Nics, Switches, Bridges
1. Physical		Bits	Media, Medium	Nics, Hubs, Cables, Wires, Radiowaves

Protocols at Every Layer



Telnet	Allows users to access resources on another machine. All data is seen in clear text (not recommended for use)
Secure Shell (SSH)	Similar to Telnet but it sets up a secure session (recommended over telnet). All data is encrypted during the session
File Transfer Protocol (FTP)	Allows users to transfer files between two hosts. Users must use some type of Authentication, also includes advance file search features
Trivial File Transfer Protocol (TFTP)	Allows users to transfer files between two hosts. Users does not need Authentication, also you lose a lot of functions such as directory browsing abilities
Simple Network Management Protocol (SNMP)	Pulls data from networking devices to verify status information / error messages, etc.
Hyper Text Transfer Protocol (HTTP)	Allows you to display graphics, text, and links correctly. manages communication between web browsers and web servers
Hyper Text Transfer Protocol Secure (HTTPS)	Allows you to display graphics, text, and links correctly. Manages communication between web browsers and web servers. This version make sure your web communication is secure using SSL
Network Time Protocol (NTP)	Synchronize devices to ensure that all computer on the network has the correct time
Domain Name Services (DNS)	Resolves hostnames on a network
Dynamic Host Configuration Protocol (DHCP/BOOTP)	Assigns IP configurations to hosts on a network **DHCP Conflicts:** two hosts have the same IP information. If conflict is detected it is removed from the pool and the will not be assigned until the admin resolves the conflict by hand. **APIPA** - clients can automatically self-configure an IP address and subnet mask. This will allow communication if you have no DHCP available. Address: 169.254.0.1 - 169.254.255.254

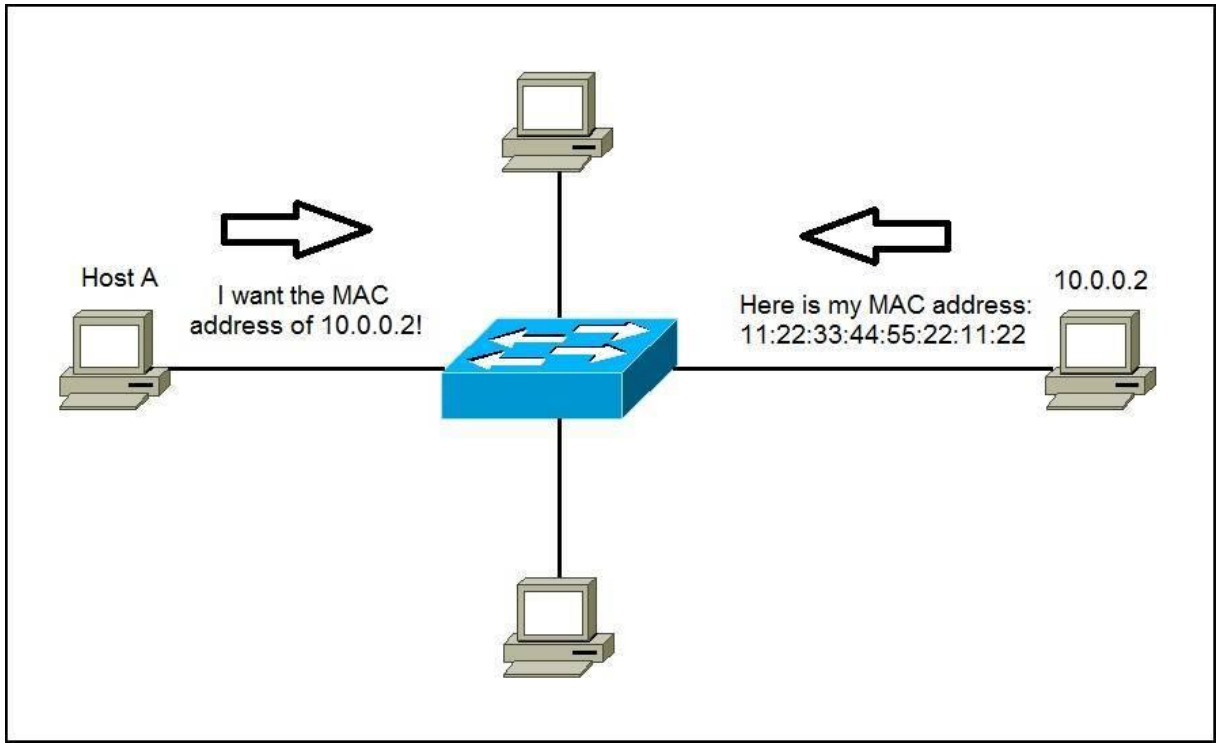

Data Encapsulation
(data is being sent)
Computer
User data converted for transmission
Upper layer data
TCP header
Upper layer data
IP header
TCP header
Upper layer data
MAC header
LLC header
IP header
TCP header
Upper layer data
FCS
11101010111101101001101010 ---> Sent to cable
Application
Presentation
Session
Transport
Network
Datalink
Physical
Network Media

Internetworking Protocol

- The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
- IP provides no error checking or tracking therefore it is unreliable.
- IP transports data in packets called datagrams, each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be
- duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

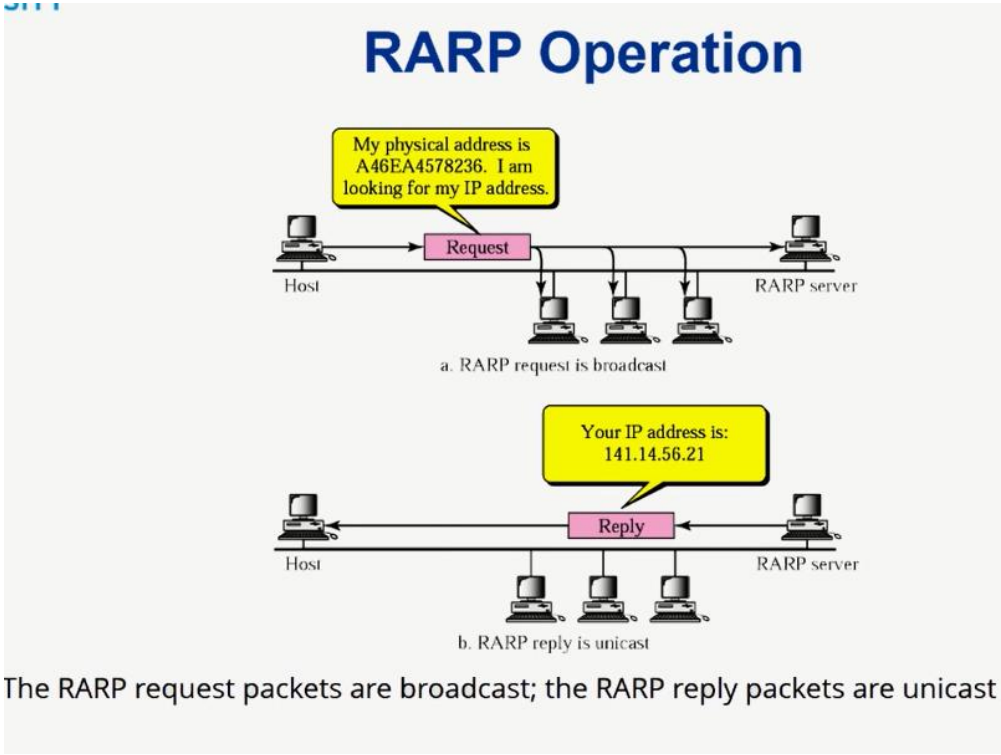
Address Resolution Protocol

- ARP is used to associate a logical address with a physical address.
- On a physical network, such as LAN , each device on a link is identified by a physical or station address , usually imprinted on NIC.
- ARP is used to find the physical address of the node when its Internet address is known.



Reverse Address Resolution Protocol

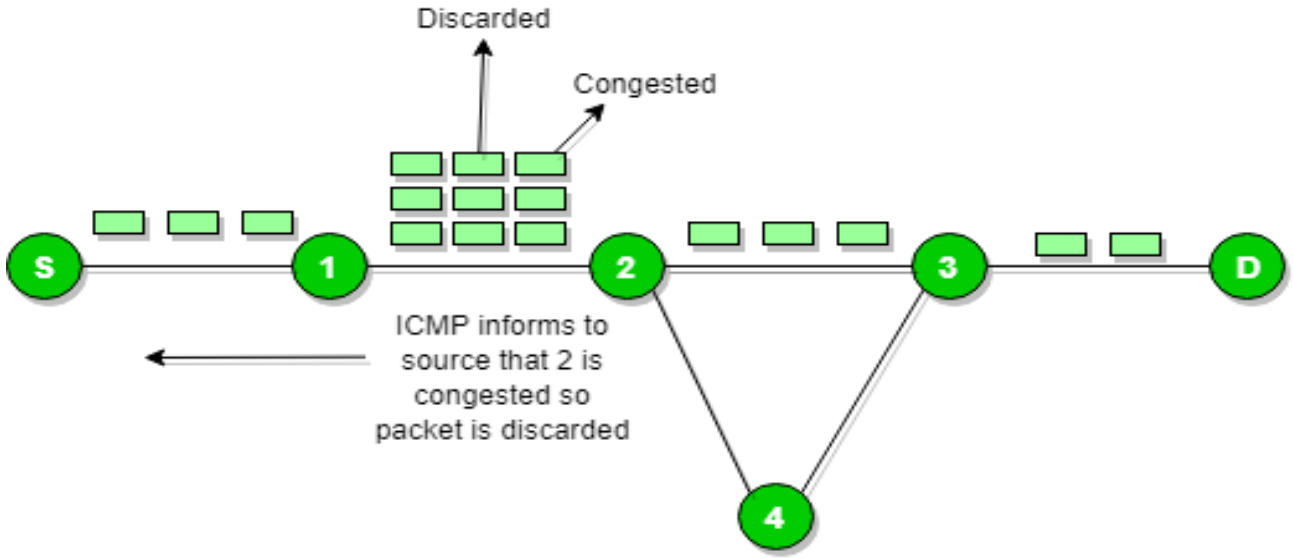
- The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.
- It is used when a computer is connected
- to a network for the first time or when a diskless computer is booted.



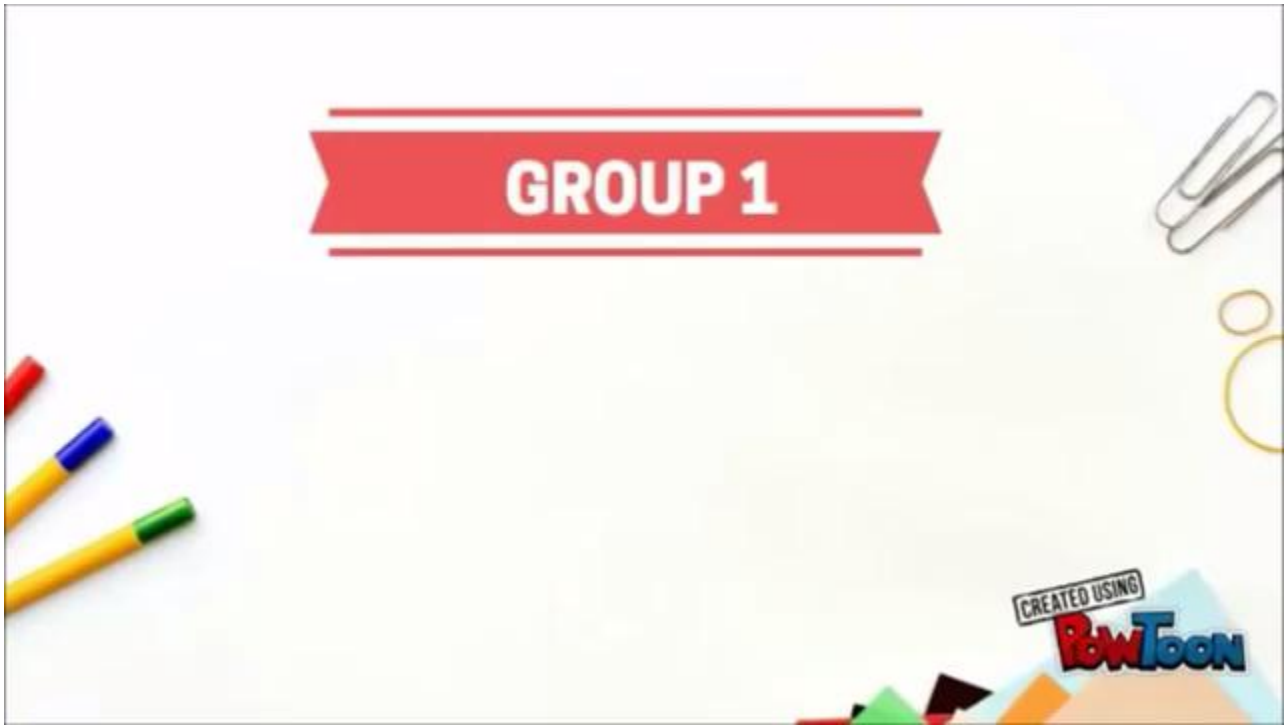
The RARP request packets are broadcast; the RARP reply packets are unicast

Internet Control Message Protocol

- The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
- ICMP sends query and error reporting messages.



ARP ,RARP and ICMP Explained



IP Addressing

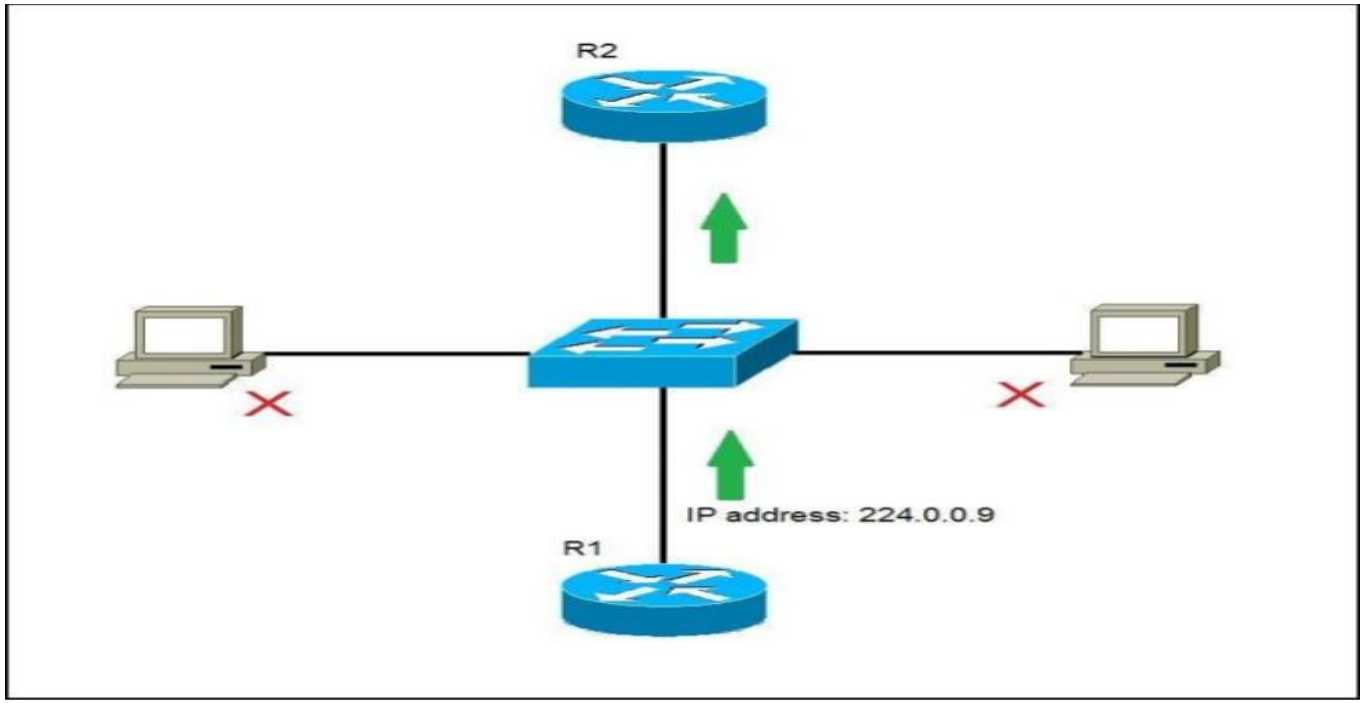
- **Address -** The unique number ID assigned to one host or interface in a network.
- **Subnet -** A portion of a network that shares a particular subnet address.
- **Subnet mask -** A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.
- **Interface -** A network connection.
- An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask.
- The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot)
- For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary..

Types of IP addresses

- **Unicast IP Addresses** – an address of a single interface. The IP addresses of this type are used for one-to-one communication. Unicast IP addresses are used to direct packets to a specific host.

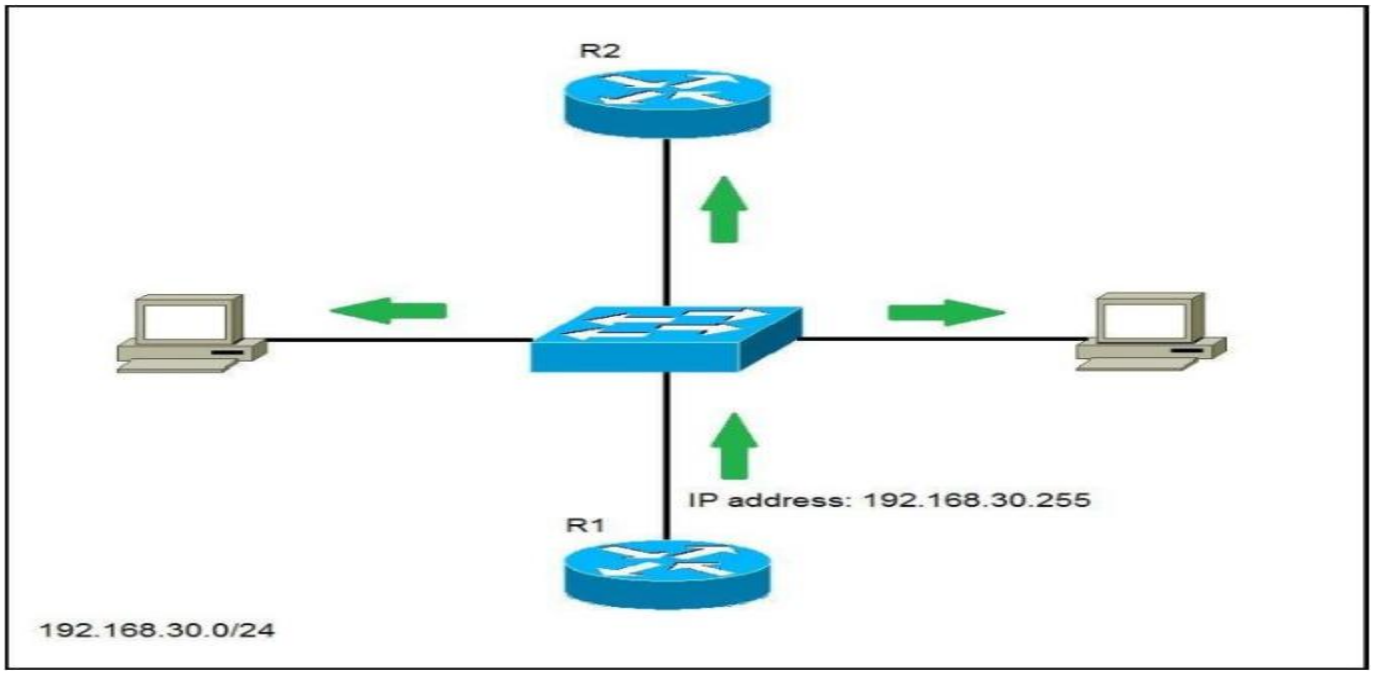
Continue…

- **Multicast IP Addresses** – used for one-to-many communication. Multicast messages are sent to IP multicast group addresses. Routers forward copies of the packet out to every interface that has hosts subscribed to that group address. Only the hosts that need to receive the message will process the packets. All other hosts on the LAN will discard them.



Continue…

- **Broadcast IP Addresses** – used to send data to all possible destinations in the broadcast domain (the one-to-everybody communication). The broadcast address for a network has all host bits on. For example, for the network **192.168.30.0 255.255.255.0** the broadcast address would be **192.168.0.255**. Also, the IP address of all 1's (**255.255.255.255**) can be used for local broadcast.



IPv4 and IPv6 Addresses

- IPv4 addresses are 32 bits long (four bytes). An example of an IPv4 address is **216.58.216.164.**
- The maximum value of a 32-bit number is 2^{32}, or 4,294,967,296. So the maximum number of IPv4 addresses, which is called its address space, is about **4.3 billion**. In the 1980s, this was sufficient to address every networked device, but scientists knew that this space would quickly become exhausted.
- A major advantage of IPv6 is that it uses 128 bits of data to store an address, permitting 2^{128} unique addresses, or 340,282,366,920,938,463,463,374,607,431,768,211,456. The size of IPv6's address space — 340 duodecillion — is much, much larger than IPv4.

Classes of IP Addresses

- There are five classes of IP Addresses:
  - Class A
  - Class B
  - Class C
  - Class D
  - Class E
- The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for the small number of networks with a very large number of hosts, the Class A was created. The Class C was created for numerous networks with small number of hosts.
- For the IP addresses from Class A, the first 8 bits (the first decimal number) represent the network part, while the remaining 24 bits represent the host part. For Class B, the first 16 bits (the first two numbers) represent the network part, while the remaining 16 bits represent the host part. For Class C, the first 24 bits represent the network part, while the remaining 8 bits represent the host part.

Special IP Address Range

- Special IP address ranges that are used for special purposes are:
- **0.0.0.0/8** – addresses used to communicate with the local network
- **127.0.0.0/8** – loopback addresses
- **169.254.0.0/16** – link-local addresses (APIPA)

Classes with their Range

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or research and development purposes.

Static vs. Dynamic IP Addresses

- IP addresses are assigned in two different ways. They may be dynamically assigned (they can change automatically) or statically assigned (they're intended not to change, and must be changed manually). Most home networks use **dynamic allocation**. Your router uses DHCP to temporarily assign, or "lease," an IP address to your device. After a period of time, this lease "expires," and the router renews your old address or assigns you a new one, depending on the needs of the network and the configuration of the router.

192.168.1.0	This number, called the **network number**, identifies the network as a whole, and is not assigned to a device.
192.168.1.1	The common default address assigned to the gateway device. In most home networks, the gateway is the router itself.
192.168.1.2	Another common gateway address. Or, it may be assigned to a device on the network.
192.168.1.3–254	Assigned to devices on the network.
192.168.1.255	The broadcast address of the network. Data sent to this address is automatically broadcast to addresses 1–254.

Binary to Decimal Conversion

- The right most bit, or least significant bit, of an octet holds a value of 2^0.
- The bit just to the left of that holds a value of 2^1.
- This continues until the left-most bit, or most significant bit, which holds a value of 2^7.
- if all binary bits are a one, the decimal equivalent would be 255 as shown here:

```
  1   1   1   1 1 1 1 1
128  64  32  16 8 4 2 1 (128+64+32+16+8+4+2+1=255)
```

Here is a sample octet conversion when not all of the bits are set to 1.

```
0   1 0 0 0 0 0 1
0  64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)
```

And this sample shows an IP address represented in both binary and decimal.

```
      10.       1.      23.      19 (decimal)
00001010.00000001.00010111.00010011 (binary)
```

Subnetting

- **Subnetting** is the practice of dividing a network into two or more smaller networks. It increases routing efficiency, enhances the security of the network and reduces the size of the broadcast domain.