Module 3: Protocols and Models

Introduction to Networks

Module Objectives

- Module Title: Protocols and Models
- Module Objective: Explain how network protocols enable devices to access local and remote network resources.

Topic Title	Topic Objective
3.1 The Rules	Describe the types of rules that are necessary to successfully communicate.
3.2 Protocols	Explain why protocols are necessary in network communication.
3.3 Protocol Suites	Explain the purpose of adhering to a protocol suite.
3.4 Standards Organizations	Explain the role of standards organizations in establishing protocols for network interoperability.
3.5 Reference Models	Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.
3.6 Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.
3.7 Data Access	Explain how local hosts access local resources on a network.

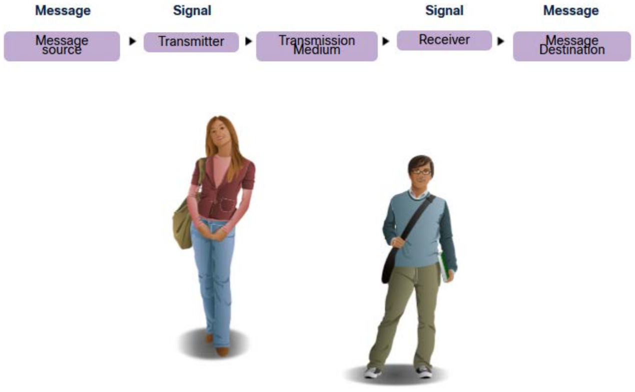
3.1 The Rules

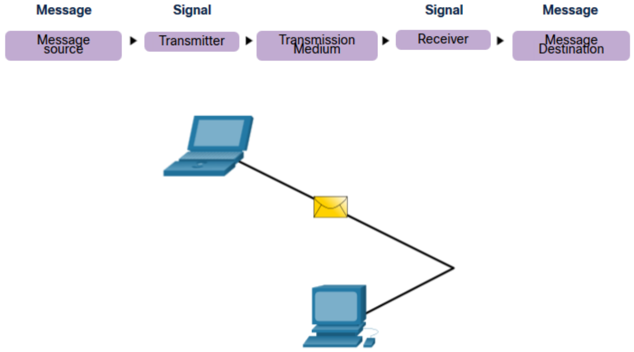
Communications Fundamentals

- Networks can vary in size and complexity. It is not enough to have a connection, devices must agree on “how” to communicate
- **Network protocols** define how messages are exchanged between the source and the destination.
- There are three elements to any communication:
  - There will be a source (sender).
  - There will be a destination (receiver).
  - There will be a channel (media) that provides for the path of communications to occur.

Communications Protocols

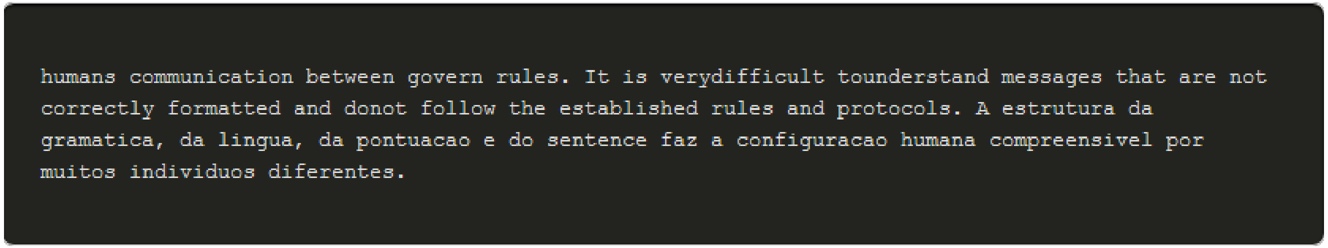
- All communications are governed by protocols.
- **Protocols** are the rules that communications will follow.
- These rules will vary depending on the protocol.
- All communication methods have elements in common:
  - Identify sender or source
  - Identify receiver or destination
  - Identify channel or media
  - Common language and grammar
  - Speed and timing of delivery
  - Confirmation or acknowledgment requirements



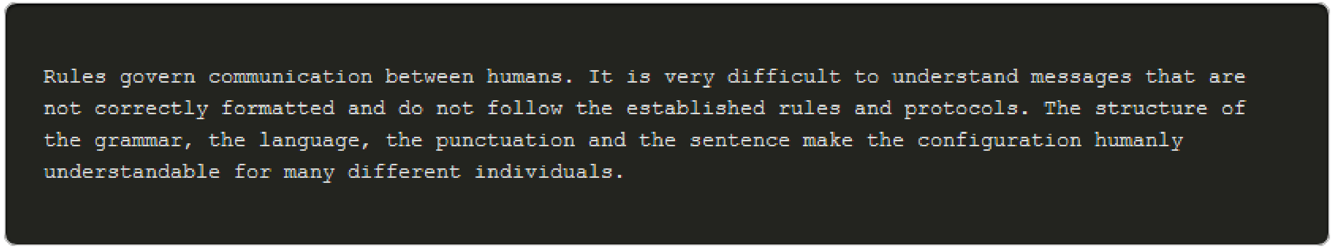


Rule Establishment

- Individuals must use established rules or agreements to govern the conversation.
- The first message is difficult to read because it is not formatted properly. The second shows the message properly formatted



humans communication between govern rules. It is verydifficult tounderstand messages that are not correctly formatted and donot follow the established rules and protocols. A estrutura da gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana compreensivel por muitos individuos diferentes.



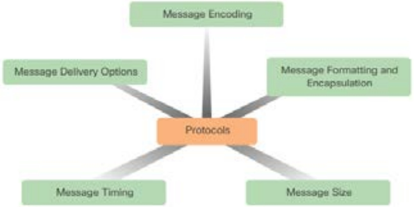
Rules govern communication between humans. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. The structure of the grammar, the language, the punctuation and the sentence make the configuration humanly understandable for many different individuals.

Rule Establishment

- Protocols must account for the following requirements:
  - An identified sender and receiver
  - Common language and grammar
  - Speed and timing of delivery
  - Confirmation or acknowledgment requirements

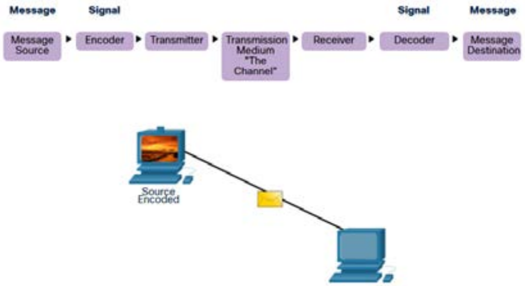
Network Protocol Requirements

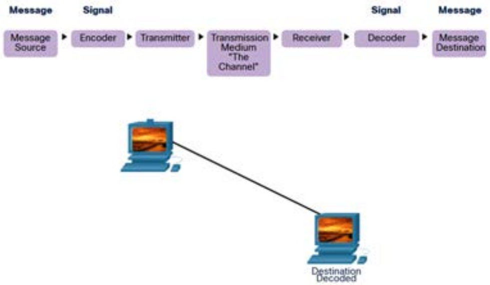
- Common computer protocols must be in agreement and include the following requirements:
  - **Message Encoding** – process of converting information into another acceptable form.
  - **Message Formatting** and **Encapsulation** – used to place one message inside another message for transfer from the source to the destination.
  - **Message Size** – process of breaking up a long message into individual pieces.
  - **Message Timing** – process of knowing when a message begins, how must can be received at a time, and how to respond back.
  - **Message Delivery Options** – who will receive the message and how will it be received.



Message Encoding

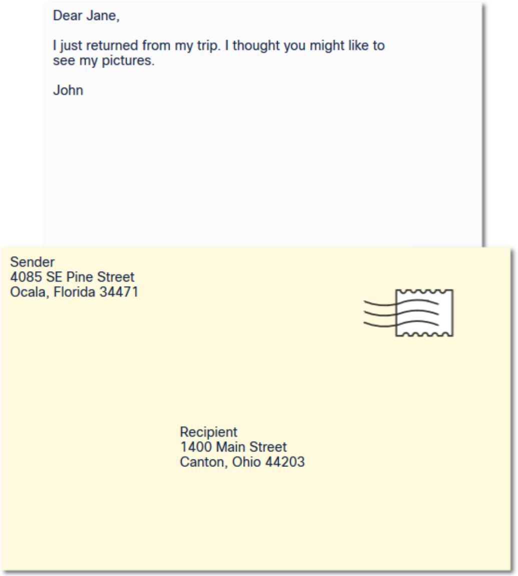
- **Encoding** is the process of converting information into another acceptable form for transmission.
  - Encoding between hosts must be in appropriate format for the medium
  - Messages are first converted into bits by the sending host
  - Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media
  - The destination host receives and decodes the signals in order to interpret the message
- **Decoding** reverses this process to interpret the information.





Message Formatting and Encapsulation

- When a message is sent, it must use a specific format or structure.
- Message formats depend on the type of message and the channel that is used to deliver the message.



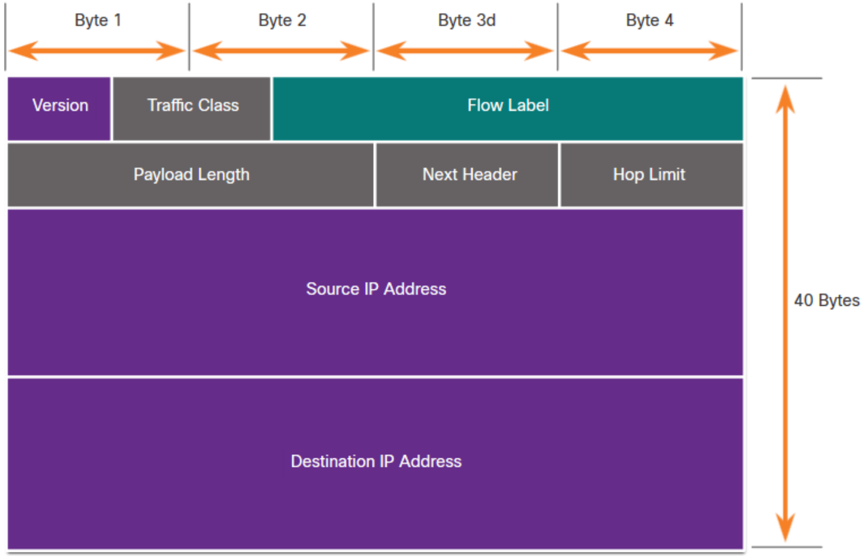
Dear Jane,

I just returned from my trip. I thought you might like to see my pictures.

John

Sender
4085 SE Pine Street
Ocala, Florida 34471

Recipient
1400 Main Street
Canton, Ohio 44203



Version | Traffic Class | Flow Label

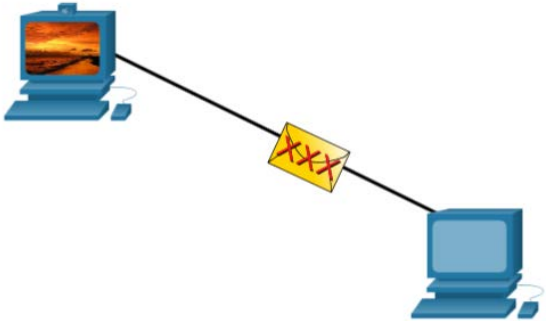
Payload Length | Next Header | Hop Limit

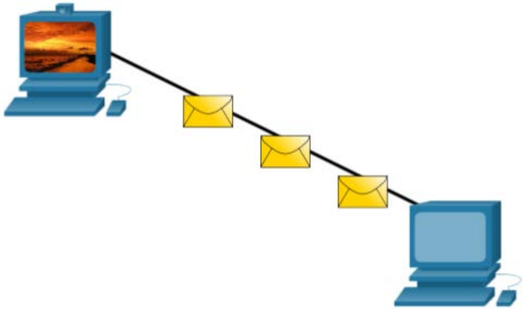
Source IP Address

Destination IP Address

Message Size

- Encoding between hosts must be in an appropriate format for the medium.
  - Messages sent across the network are converted to bits.
  - The bits are encoded into a pattern of light, sound, or electrical impulses.
  - The destination host must decode the signals to interpret the message.



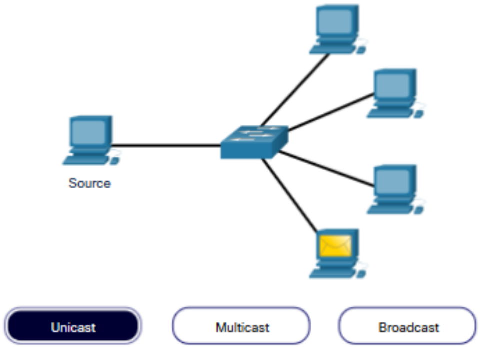


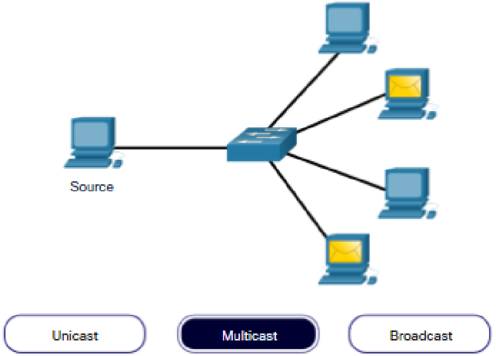
Message Timing

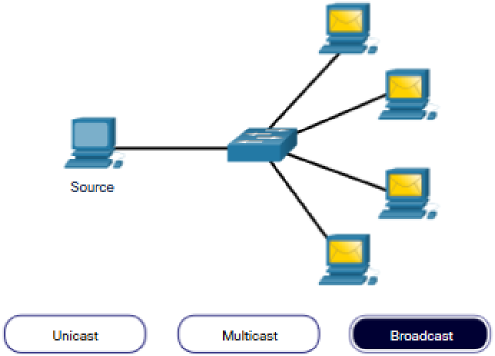
- Message timing includes the following:
  - **Flow Control** – Manages the rate of data transmission and defines how much information can be sent and the speed at which it can be delivered. Ensures packets are not dropped.
  - **Response Timeout** – Manages how long a device waits when it does not hear a reply from the destination.
  - **Access method** - Determines when someone can send a message.
    - There may be various rules governing issues like “collisions”. This is when more than one device sends traffic at the same time and the messages become corrupt.
    - Some protocols are proactive and attempt to prevent collisions; other protocols are reactive and establish a recovery method after the collision occurs.

Message Delivery Options

- Message delivery may one of the following methods:
  - **Unicast** – one to one communication
  - **Multicast** – one to many (select group of hosts), typically not all
    Broadcast – one to all
- Note: Broadcasts are used in IPv4 networks, but are not an option for IPv6. Later we will also see “**Anycast**” as an additional delivery option for IPv6.

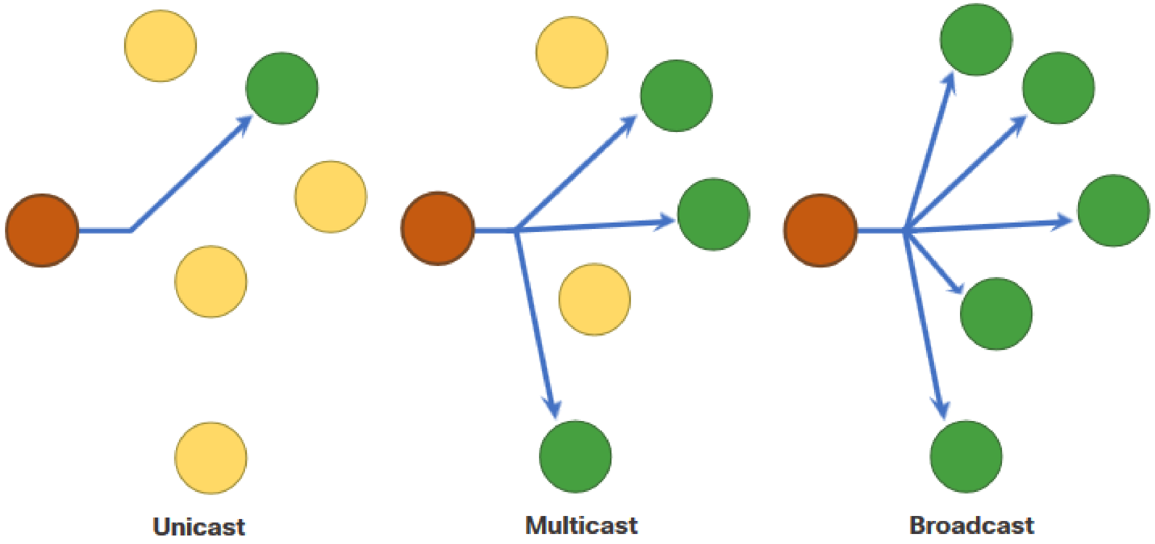






A Note About the Node Icon

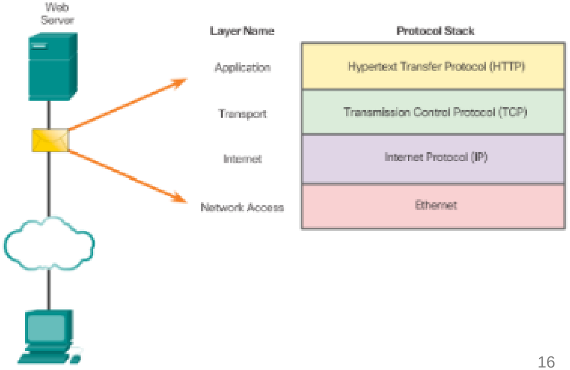
- Documents may use the node icon , typically a circle, to represent all devices.
- The figure illustrates the use of the node icon for delivery options.



3.2 Protocols

Network Protocols and Standards

- Rules that Govern Communications
  - May be specified by a standards organization or developed by a vendor
- Role of network protocols:
  - Define a common format and set of rules for exchanging messages between devices
  - Define how messages are exchanged between the source and the destination
  - How the message is formatted or structured
  - The process by which networking devices share information about pathways with other networks
  - How and when error and system messages are passed between devices
  - The setup and termination of data transfer sessions
- Protocol Interaction
  - Example: web server and client



Layer Name	Protocol Stack
Application	Hypertext Transfer Protocol (HTTP)
Transport	Transmission Control Protocol (TCP)
Internet	Internet Protocol (IP)
Network Access	Ethernet

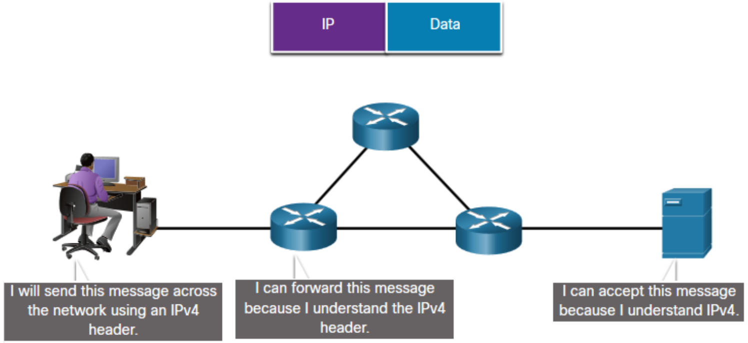
Network Protocol Overview

- Network protocols define a common set of rules.
- Can be implemented on devices in:
  - Software
  - Hardware
  - Both
- Protocols have their own:
  - Function
  - Format
  - Rules

Protocol Type	Description
Network Communications	enable two or more devices to communicate over one or more networks
Network Security	secure data to provide authentication, data integrity, and data encryption
Routing	enable routers to exchange route information, compare path information, and select best path
Service Discovery	used for the automatic detection of devices or services

Network Protocol Functions

- Devices use agreed-upon protocols to communicate .
- Protocols may have may have one or functions.



I will send this message across the network using an IPv4 header.

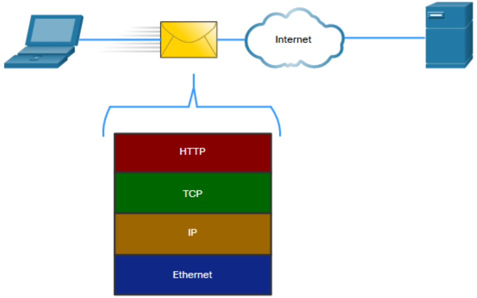
I can forward this message because I understand the IPv4 header.

I can accept this message because I understand IPv4.

Function	Description
Addressing	Identifies sender and receiver
Reliability	Provides guaranteed delivery
Flow Control	Ensures data flows at an efficient rate
Sequencing	Uniquely labels each transmitted segment of data
Error Detection	Determines if data became corrupted during transmission
Application Interface	Process-to-process communications between network applications

Protocol Interaction

- Networks require the use of several protocols.
- Each protocol has its own function and format.



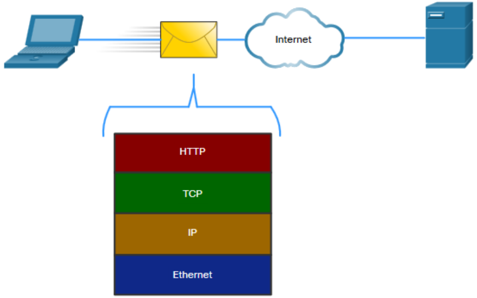
Protocol	Function
Hypertext Transfer Protocol (HTTP)	▪ Governs the way a web server and a web client interact ▪ Defines content and format
Transmission Control Protocol (TCP)	▪ Manages the individual conversations ▪ Provides guaranteed delivery ▪ Manages flow control
Internet Protocol (IP)	Delivers messages globally from the sender to the receiver
Ethernet	Delivers messages from one NIC to another NIC on the same Ethernet Local Area Network (LAN)

Interaction of TCP/IP Model Protocols

- Communication between a web server and web client is an example of an interaction between several protocols:
  - Application Layer – **Hypertext Transfer Protocol (HTTP)** – Defines the content and formatting of the requests and responses that are exchanged between the client and server.
  - Presentation Layer – **Hypertext Markup Language (HTML)** – Defines the syntax both sides of the communication must understand in order to communicate.
  - Transport Layer – **Transmission Control Protocol (TCP)** is responsible for controlling the size and rate of the HTTP messages exchanged between server and client. It segments the messages and manages the segments in the individual conversation between the host and destination.
  - Internet Layer – **Internet Protocol (IP)** or logical address is a unique host address for data communications at the internet layer
  - Network Access Layer – Describes two primary functions: 1) communication over a data link and 2) the physical transmission of data on the network media:
    - **Data-link** management protocols take the packets from IP and format them to be transmitted over the media.
    - **Physical** media standards and protocols govern how the signals are sent and how they are interpreted by the receiving clients

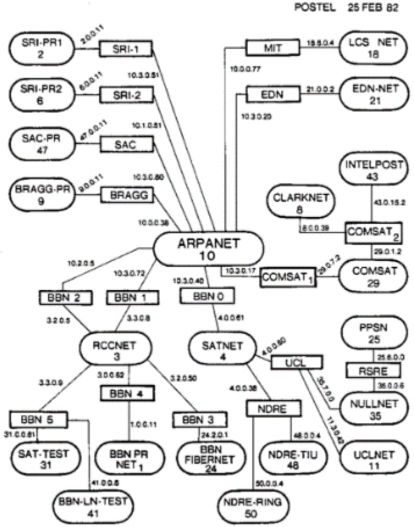
TCP/IP Communication Process

- From the user perspective, what is the correct order of the protocol stack that is used to prepare a web request for transmission?
  - **HTTP** (7) – Identifies the type of page that will be rendered
  - **HTML** (6) – Prepares the Hypertext Markup Language (HTML) page
  - **TCP** (4) – Breaks the data into segments and identifies each
  - **IP** (3) – The IP source and destination addresses are added, creating an IP Packet
  - **Ethernet** (2) – The Ethernet information is added creating the Ethernet Frame
    - This frame is delivered to the nearest router along the path towards the web client
    - Each router adds new data link information before forwarding the packet



Network Protocols

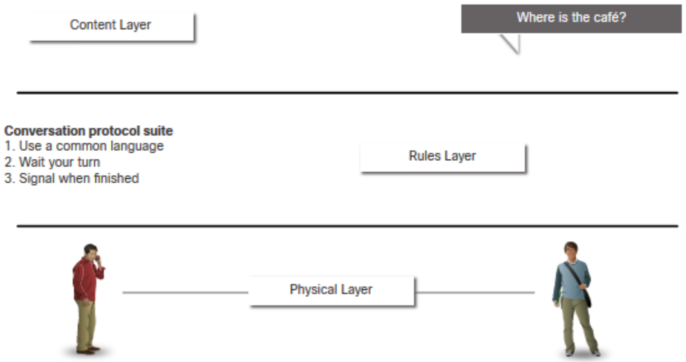
- **Address Resolution Protocol (ARP)** – used to discover the MAC address of any host on the local network
- **Reverse ARP** – Used to find the IP address of the local machine
- **Proprietary protocols** are developed by organizations who have control over their definition and operation
- Advantages of using standards to develop and implement protocols:
  - Products from different manufacturers can interoperate successfully
  - A host and a server running different operating systems can successfully exchange data



3.3 Protocol Suites

Network Protocol Suites

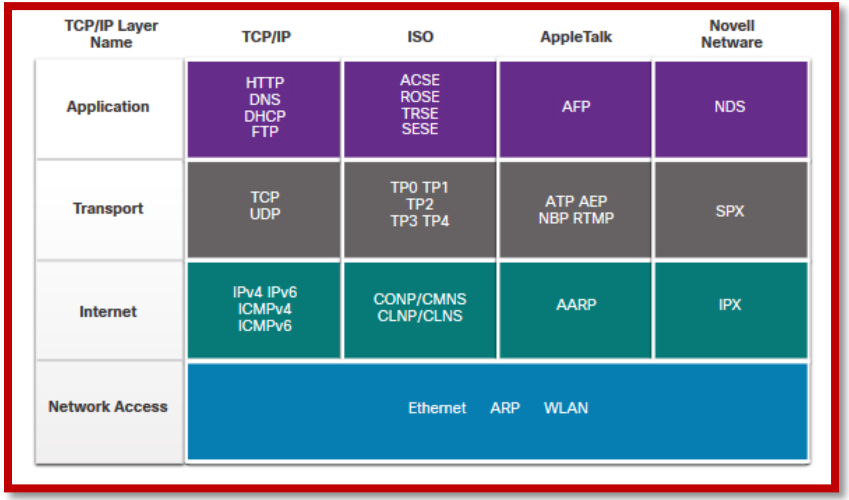
- Protocols must be able to work with other protocols.
- **Protocol suite**:
  - A group of inter-related protocols necessary to perform a communication function
  - Sets of rules that work together to help solve a problem
- The protocols are viewed in terms of layers:
  - Higher Layers
  - Lower Layers- concerned with moving data and provide services to upper layers



Protocol suites are sets of rules that work together to help solve a problem.

Evolution of Protocol Suites

- There are several protocol suites:
  - **Internet Protocol Suite or TCP/IP** – The most common protocol suite and maintained by the Internet Engineering Task Force (IETF)
  - **Open Systems Interconnection** (OSI) protocols – Developed by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU)
  - **AppleTalk** – Proprietary suite release by Apple Inc.
  - **Novell NetWare** – Proprietary suite developed by Novell Inc.



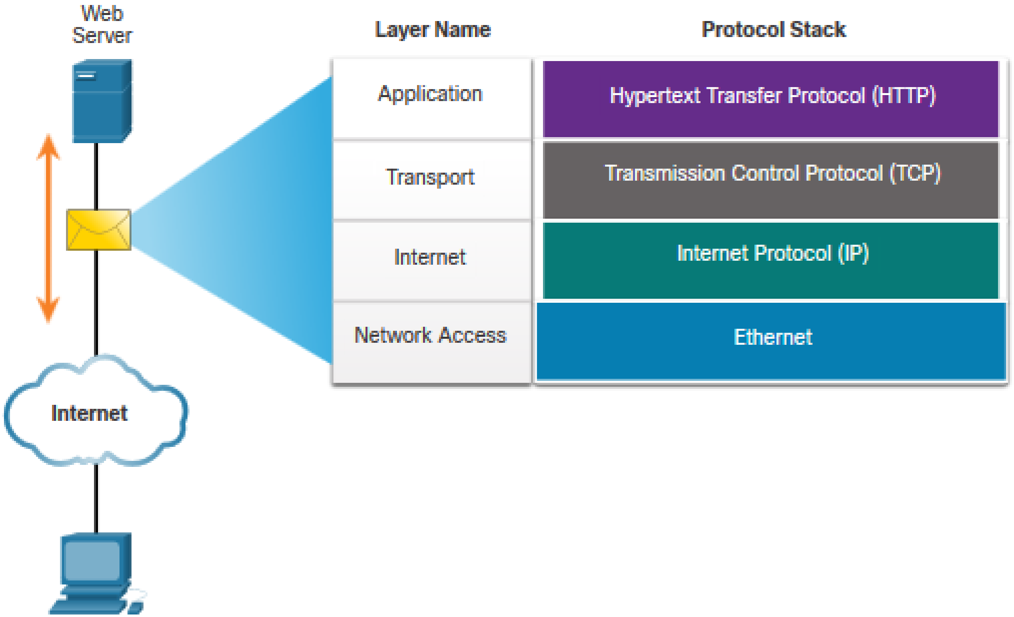
TCP/IP Layer Name	TCP/IP	ISO	AppleTalk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Network Access	Ethernet ARP WLAN			

International Organization for Standardization

- ISO is derived from the Greek isos, meaning equal.
- In 1946 when delegates from 25 countries met at the Institute of Civil Engineers in London and decided to create a new international organization “to facilitate the international coordination and unification of industrial standards”.
- ISO officially began operations on 23 February 1947.
- This organization is the largest developer of international standards in the world for a wide variety of products and services. It is known for its Open Systems Interconnection (OSI) reference model.
- ISO is an independent, non-governmental international organization with a membership of 164 national standards bodies.

TCP/IP Protocol Example

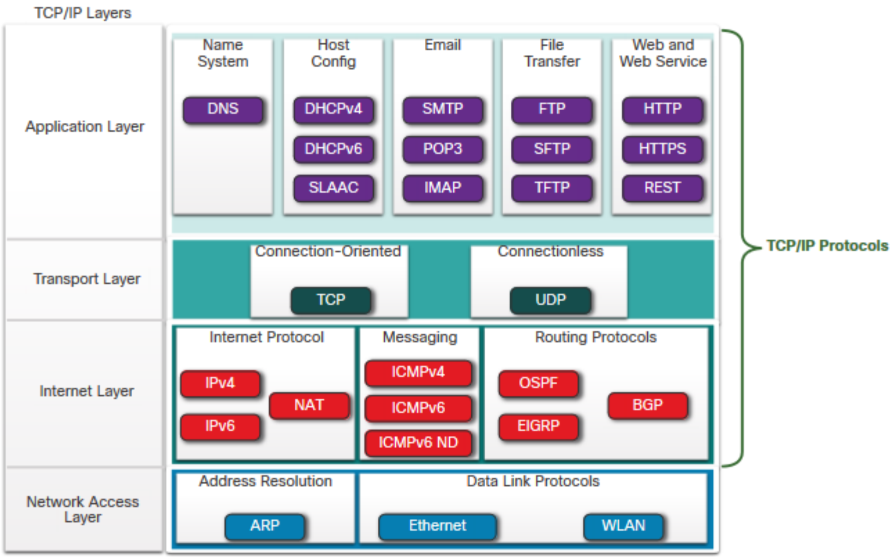
- TCP/IP protocols operate at the application, transport, and internet layers.
- The most common network access layer LAN protocols are Ethernet and WLAN (wireless LAN).



Layer Name	Protocol Stack
Application	Hypertext Transfer Protocol (HTTP)
Transport	Transmission Control Protocol (TCP)
Internet	Internet Protocol (IP)
Network Access	Ethernet

TCP/IP Protocol Suite

- TCP/IP is the protocol suite used by the internet and includes many protocols:
  - An open standard protocol suite that is freely available to the public and can be used by any vendor
  - A standards-based protocol suite that is endorsed by the networking industry and approved by a standards organization to ensure interoperability



TCP/IP Layers

Application Layer
- Name System: DNS
- Host Config: DHCPv4, DHCPv6, SLAAC
- Email: SMTP, POP3, IMAP
- File Transfer: FTP, SFTP, TFTP
- Web and Web Service: HTTP, HTTPS, REST

Transport Layer
- Connection-Oriented: TCP
- Connectionless: UDP

Internet Layer
- Internet Protocol: IPv4, IPv6, NAT
- Messaging: ICMPv4, ICMPv6, ICMPv6 ND
- Routing Protocols: OSPF, EIGRP, BGP

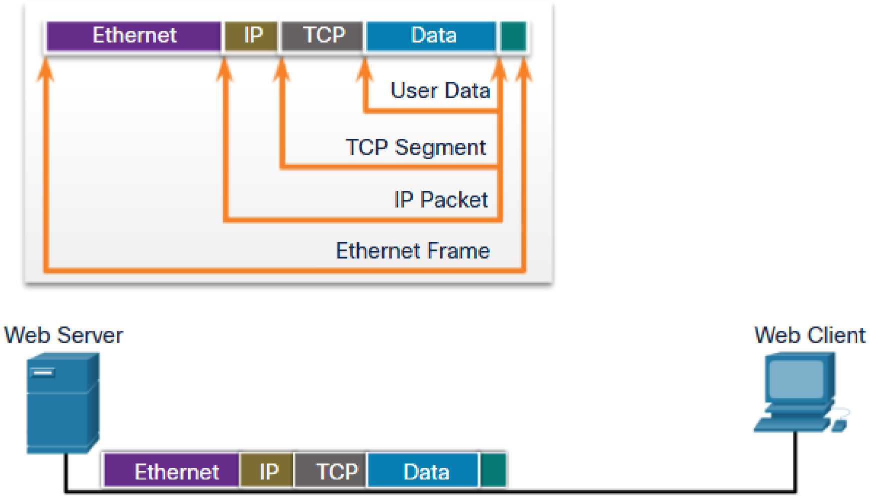
Network Access Layer
- Address Resolution: ARP
- Data Link Protocols: Ethernet, WLAN

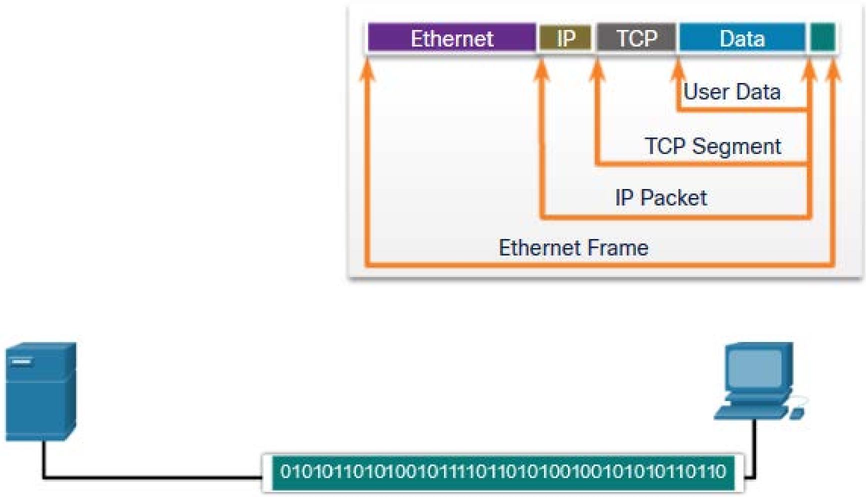
TCP/IP Protocols

TCP/IP Communication Process

A web server encapsulating and sending a web page to a client.

A client de-encapsulating the web page for the web browser





3.4 Standards Organizations

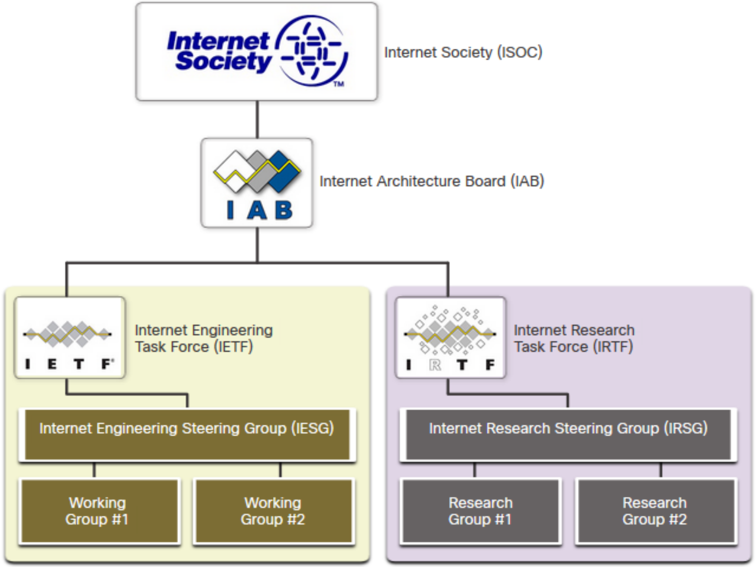
Open Standards

- Open standards encourage:
  - interoperability
  - competition
  - innovation
- A host and a server running different operating systems can successfully exchange data.
- Standards organizations are:
  - vendor-neutral
  - non-profit organizations
  - established to develop and promote the concept of open standards.

IEEE
IETF
iana
Internet Assigned Numbers Authority
ICANN
The Internet Corporation for Assigned Names and Numbers
ITU
TIA

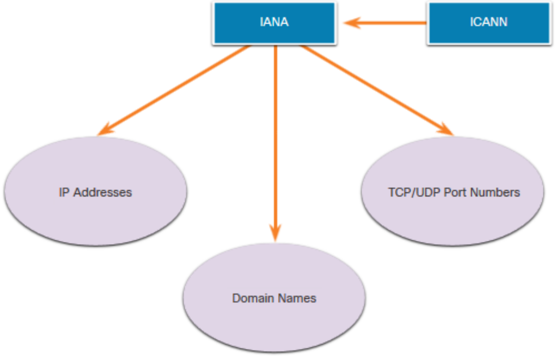
Internet Standards

- **Internet Society (ISOC)** - Promotes the open development and evolution of internet throughout the world.
- **Internet Architecture Board (IAB)** - Responsible for management and development of internet standards.
- **Internet Engineering Task Force (IETF)** - Develops, updates, and maintains internet and TCP/IP technologies.
- **Internet Research Task Force (IRTF)** - Focused on long-term research related to internet and TCP/IP protocols.


Internet Society
Internet Society (ISOC)
IAB
Internet Architecture Board (IAB)
IETF
Internet Engineering Task Force (IETF)
IRTF
Internet Research Task Force (IRTF)
Internet Engineering Steering Group (IESG)
Internet Research Steering Group (IRSG)
Working Group #1
Working Group #2
Research Group #1
Research Group #2

Internet Standards

- Standards organizations involved with the development and support of TCP/IP:
  - **Internet Corporation for Assigned Names and Numbers (ICANN)** - Coordinates IP address allocation, the management of domain names, and assignment of other information.
  - **Internet Assigned Numbers Authority (IANA)** - Oversees and manages IP address allocation, domain name management, and protocol identifiers for ICANN.

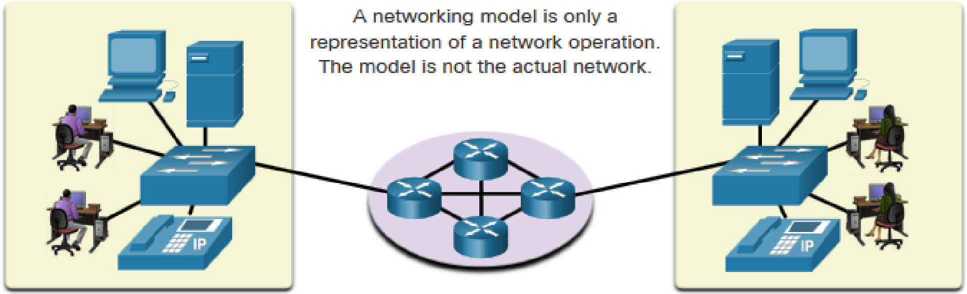


Electronic and Communications Standards

- **Institute of Electrical and Electronics Engineers** (**IEEE**, pronounced "I-triple-E") - dedicated to creating standards in power and energy, healthcare, telecommunications, and networking.
- **Electronic Industries Alliance (EIA)** - develops standards relating to electrical wiring, connectors, and the 19-inch racks used to mount networking equipment.
- **Telecommunications Industry Association (TIA)** - develops communication standards in radio equipment, cellular towers, Voice over IP (VoIP) devices, satellite communications, and more.
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T**) - defines standards for video compression, Internet Protocol Television (IPTV), and broadband communications, such as a digital subscriber line (DSL).

3.5 Reference Models

The Benefits of Using a Layered Model



A networking model is only a representation of a network operation. The model is not the actual network.

OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	Ethernet, WLAN, SONET, SDH	Network Access
Physical		

- Complex concepts such as how a network operates can be difficult to explain and understand. For this reason, a layered model is used.
- Two layered models describe network operations:
  - **Open System Interconnection (OSI) Reference Model**
  - **TCP/IP Reference Model**

The Benefits of Using a Layered Model

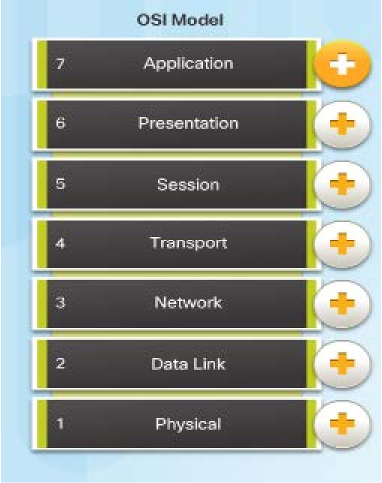
- These are the benefits of using a layered model:
  - Assist in protocol design because protocols that operate at a specific layer have defined information that they act upon and a defined interface to the layers above and below
  - Foster competition because products from different vendors can work together
  - Prevent technology or capability changes in one layer from affecting other layers above and below
  - Provide a common language to describe networking functions and capabilities

The OSI Reference Model

OSI Model Layer	Description
7 - Application	Contains protocols used for process-to-process communications.
6 - Presentation	Provides for common representation of the data transferred between application layer services.
5 - Session	Provides services to the presentation layer and to manage data exchange.
4 - Transport	Defines services to segment, transfer, and reassemble the data for individual communications.
3 - Network	Provides services to exchange the individual pieces of data over the network. Provides the logical addressing (IP).
2 - Data Link	Describes methods for exchanging data frames over a common media. Provides the physical addressing (MAC).
1 - Physical	Describes the means to activate, maintain, and de-activate physical connections.

OSI Reference Model

- **Layer 7** – The Application layer provides the means for end-to-end connectivity between individuals in the human network using data networks.
- **Layer 6** – The Presentation layer provides for common representation of the data transferred between application layer services.
- **Layer 5** – The Session layer provides services to the presentation layer to organize its dialogue and to manage data exchange.
- **Layer 4** – The Transport layer defines services to segment, transfer, and reassemble the data for individual communications between the end devices. It describes the ordered and reliable delivery of data between source and destination.
- **Layer 3** – The Network layer provides services to exchange the individual pieces of data over the network between identified end devices. IP or Logical addressing.
- **Layer 2** – The Data Link layer protocols describe methods for exchanging data frames between devices over a common media. MAC or physical addressing.
- **Layer 1** – The Physical layer protocols describe the mechanical, electrical, functional, and procedural means to activate, maintain, and de-activate physical-connections for bit transmission to and from a network device.



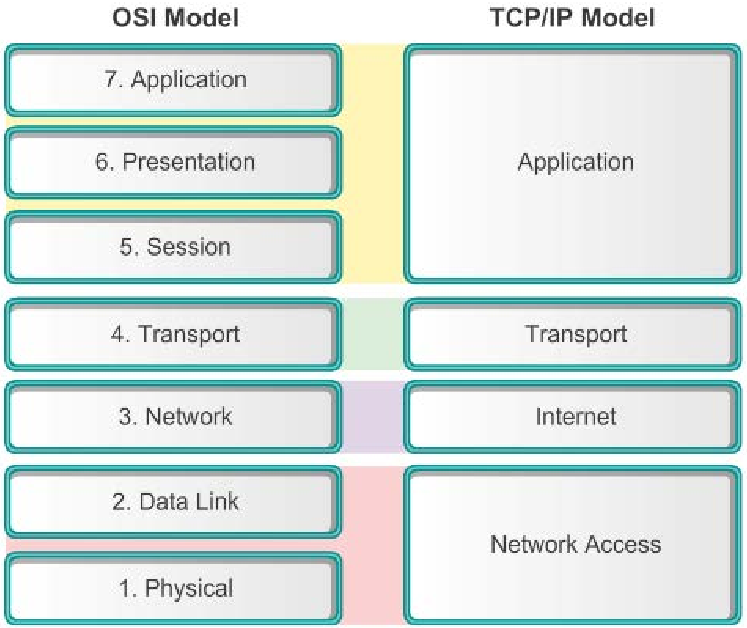
The TCP/IP Reference Model

- The TCP/IP Protocol Model
  - Created in the early 1970s for internetwork communications
  - Open Standard
  - Also called The TCP/IP Model or the Internet Model

TCP/IP Model Layer	Description
Application	Represents data to the user, plus encoding and dialog control.
Transport	Supports communication between various devices across diverse networks.
Internet	Determines the best path through the network. Responsible for routing messages through an internetwork
Network Access	Controls the hardware devices and media that make up the network.

OSI and TCP/IP Model Comparison

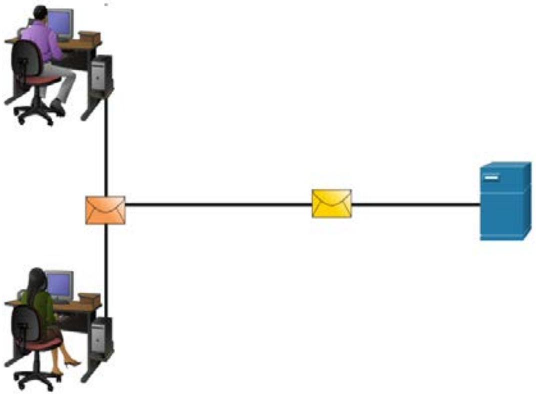
- Relationship between layers:
  - The TCP/IP Application layer combines layers 5-7 of the OSI model.
  - The TCP/IP Transport layer and OSI Transport layer provide similar services and functions.
  - The TCP/IP Network layer and OSI Internet layer provide similar services and functions.
  - The TCP/IP Network Access layer combines layers 1-2 of the OSI model.



3.6 Data Encapsulation

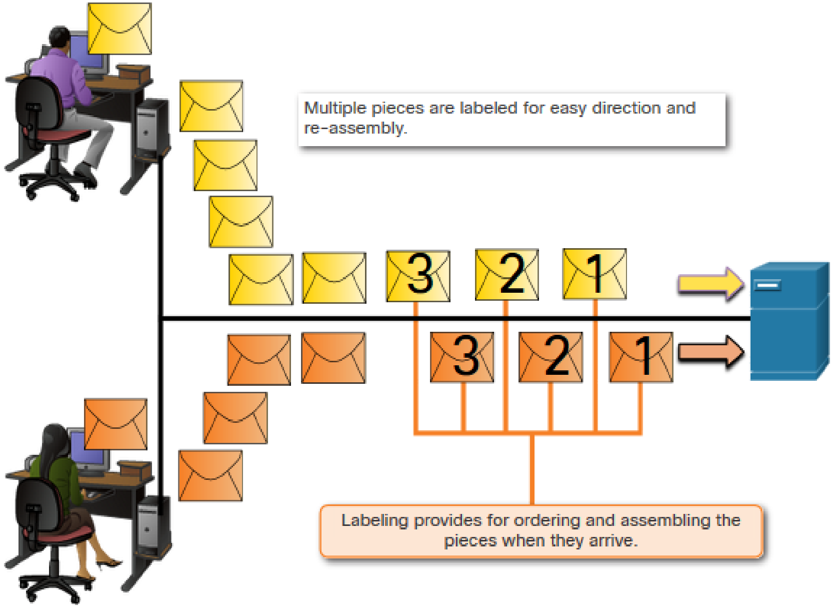
Segmenting Messages

- **Segmentation** is the process of breaking up messages into smaller units.
- **Multiplexing** is the processes of taking multiple streams of segmented data and interleaving them together.
- Segmenting messages has three primary benefits:
  - **Increases speed** - Large amounts of data can be sent over the network without tying up a communications link.
  - **Increases efficiency** - Only segments which fail to reach the destination need to be retransmitted, not the entire data stream.
  - **Increases reliability** of network communications.



Sequencing

- **Sequencing** messages is the process of numbering the segments so that the message may be reassembled at the destination.
- TCP is responsible for sequencing the individual segments.

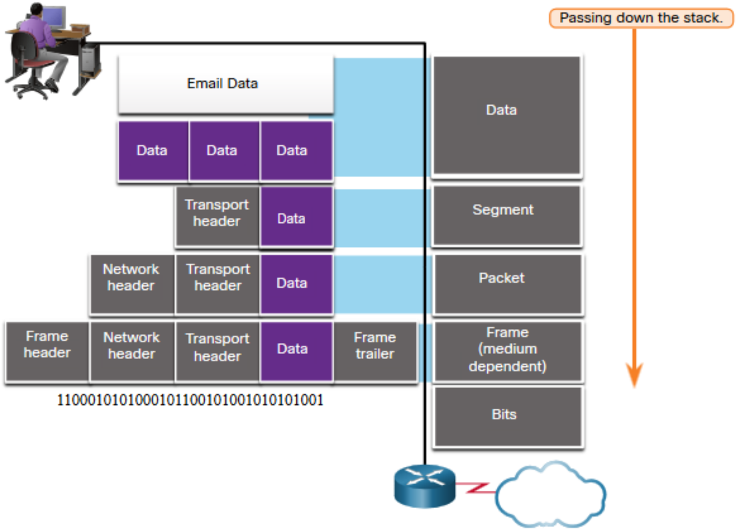


Multiple pieces are labeled for easy direction and re-assembly.

Labeling provides for ordering and assembling the pieces when they arrive.

Protocol Data Units

- **Encapsulation** is the process where protocols add their information to the data.
- At each stage of the process, a **Protocol Data Unit** (PDU) has a different name to reflect its new functions.
- There is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite.
- The level above does its process and then passes it down to the next level of the model. This process is repeated by each layer until it is sent out as a bit stream.



Passing down the stack.

Email Data

Data | Data | Data → Data

Transport header | Data → Segment

Network header | Transport header | Data → Packet

Frame header | Network header | Transport header | Data | Frame trailer → Frame (medium dependent)

1100010101000101100101001010101001 → Bits

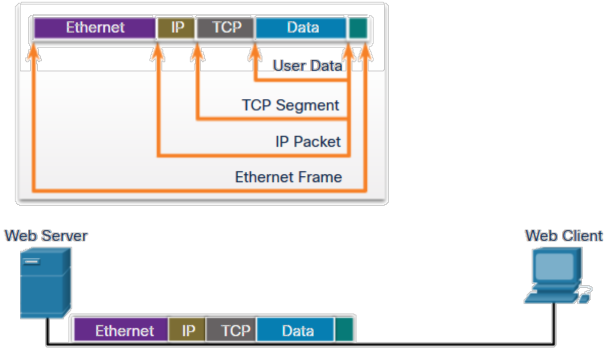
Encapsulation

- Each process is dependent of the layer directly above and below it.

Encapsulation	TCP/IP Layer	OSI Layer
Data (Data Stream)	Application	Application Presentation Session
Segment (TCP/UDP)	Transport	Transport
Packet (IP)	Internet	Network
Frame (MAC)	Network Access	Data Link
Bits (Bit Stream)		Physical

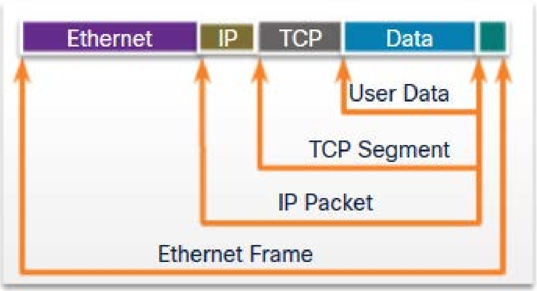
Encapsulation Example

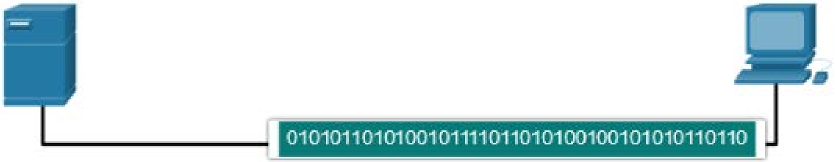
- Encapsulation is a top down process.
- PDUs passing down the stack are as follows:
  - **Data** – Provides raw data to the Transport layer.
  - **Segments** – Adds TCP/UDP header information, source & destination port numbers, sequence number, and acknowledgement numbers before passing to the Internet layer.
  - **Packets** – Adds IP header, source, and destination IP addressing before passing to the Network Access layer.
  - **Frames** – Adds Ethernet header, source and destination MAC addressing.
  - **Bits** – Encodes the PDU into a signal appropriate for the medium.



De-encapsulation Example

- Data is de-encapsulated as it moves up the stack.
- When a layer completes its process, that layer strips off its header and passes it up to the next level to be processed. This is repeated at each layer until it is a data stream that the application can process.
  - Received as Bits (Bit Stream)
  - Frame (Ethernet, MAC)
  - Packet (IP)
  - Segment (TCP/UDP)
  - Data (Data Stream like http)

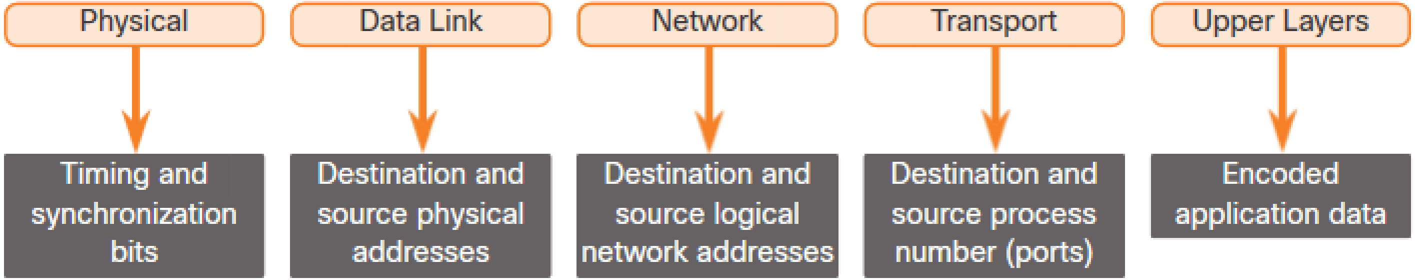




3.7 Data Access

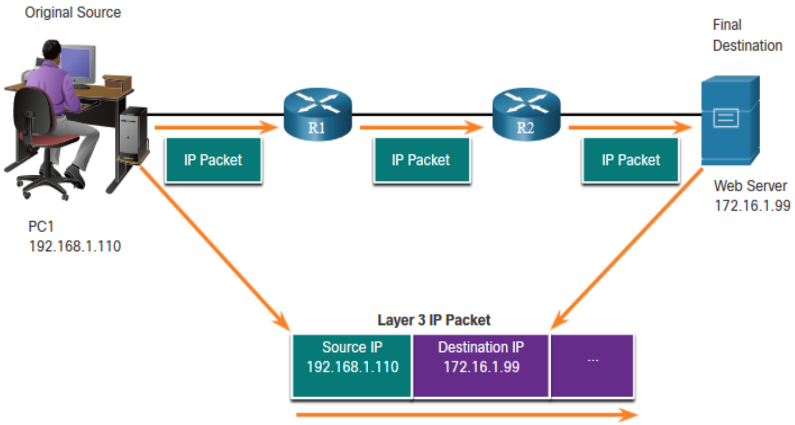
Addresses

- Both the data link and network layers use addressing to deliver data from source to destination:
  - **Network layer source and destination IP addresses** – Responsible for delivering the IP packet from original source to the final destination.
  - **Data link layer source and destination MAC addresses** – Responsible for delivering the data link frame from one Network Interface Card (NIC) to another NIC on the same network.


Physical
Data Link
Network
Transport
Upper Layers
Timing and synchronization bits
Destination and source physical addresses
Destination and source logical network addresses
Destination and source process number (ports)
Encoded application data

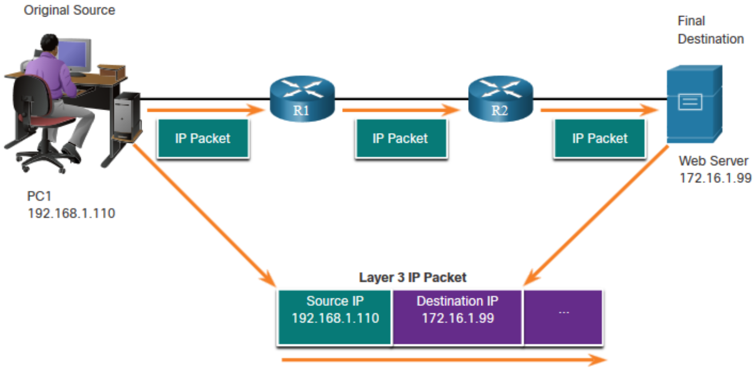
Layer 3 Logical Address

- The IP packet contains two IP addresses:
  - **Source IP address** – The IP address of the sending device, original source of the packet.
  - **Destination IP address** – The IP address of the receiving device, final destination of the packet.
- These addresses may be on the same link or remote.



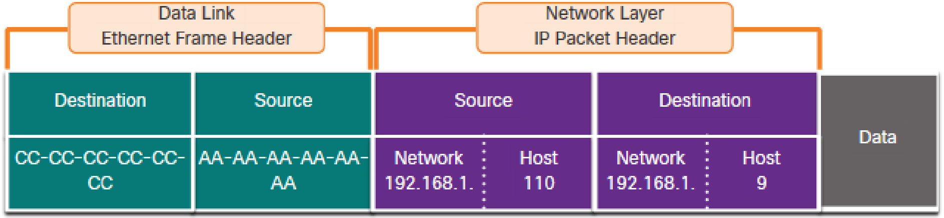
Layer 3 Logical Address

- An IP address contains two parts:
  - **Network portion (IPv4) or Prefix (IPv6)**
    - The left-most part of the address indicates the network group which the IP address is a member.
    - Each LAN or WAN will have the same network portion.
  - **Host portion (IPv4) or Interface ID (IPv6)**
    - The remaining part of the address identifies a specific device within the group.
    - This portion is unique for each device on the network.
- The **Subnet Mask (IPv4) or Network Prefix (IPv6)** identifies which part belongs to the network and which part belongs to the host.

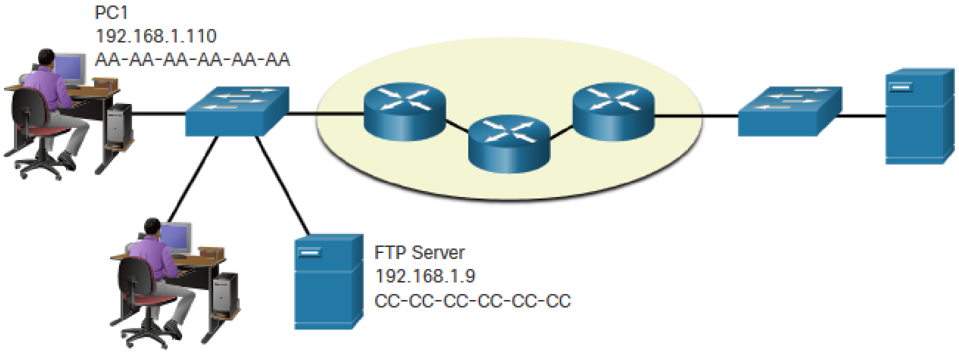


Devices on the Same Network

- When devices are on the same network the source and destination will have the same number in network portion of the address.
  - PC1 – 192.168.1.110
  - FTP Server – 192.168.1.9

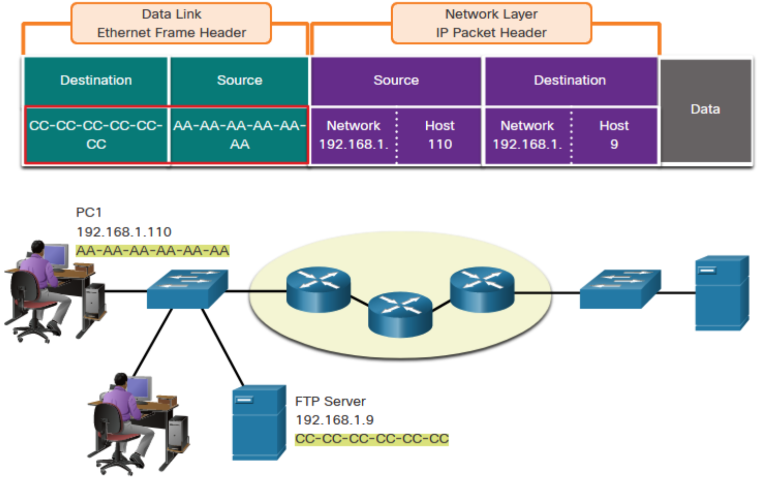


Data Link Ethernet Frame Header		Network Layer IP Packet Header		
Destination	Source	Source	Destination	Data
CC-CC-CC-CC-CC-CC	AA-AA-AA-AA-AA-AA	Network 192.168.1. Host 110	Network 192.168.1. Host 9	



Role of the Data Link Layer Addresses: Same IP Network

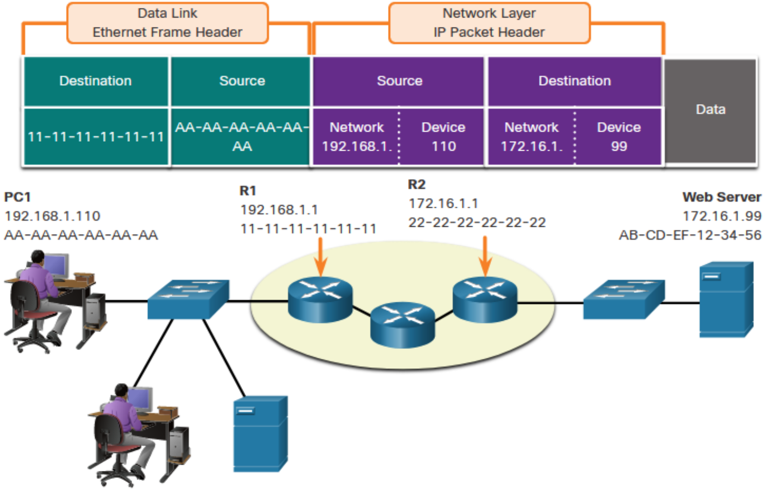
- When devices are on the same Ethernet network the data link frame will use the actual MAC address of the destination NIC.
- MAC addresses are physically embedded into the Ethernet NIC and are local addressing.
- The Source MAC address will be that of the originator on the link.
- The Destination MAC address will always be on the same link as the source, even if the ultimate destination is remote.



Data Link Ethernet Frame Header		Network Layer IP Packet Header		
Destination	Source	Source	Destination	Data
CC-CC-CC-CC-CC-CC	AA-AA-AA-AA-AA-AA	Network 192.168.1. : Host 110	Network 192.168.1. : Host 9	

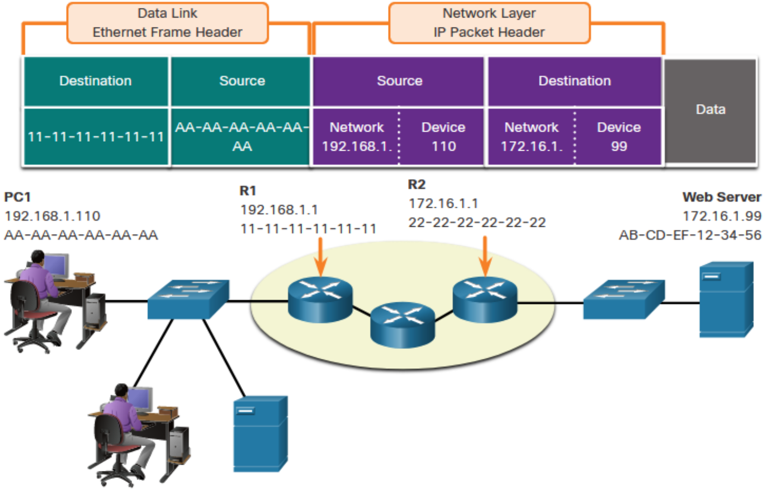
Devices on a Remote Network

- What happens when the actual (ultimate) destination is not on the same LAN and is remote?
- What happens when PC1 tries to reach the Web Server?
- Does this impact the network and data link layers?



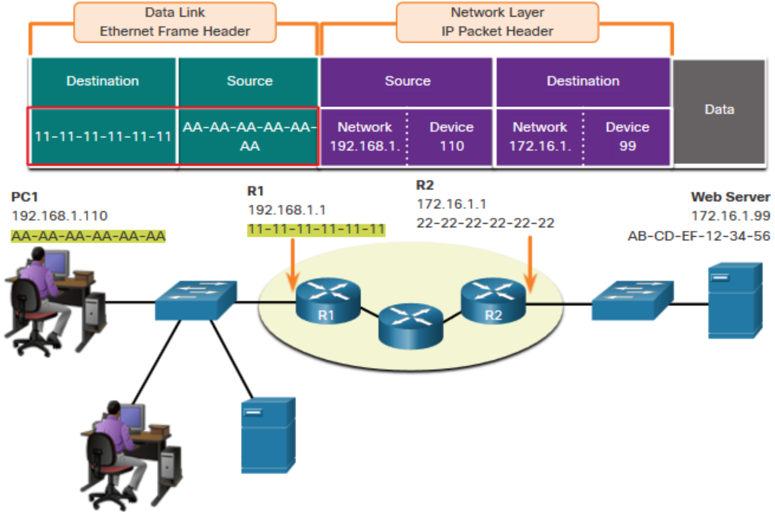
Role of the Network Layer Addresses

- When the source and destination have a different network portion, this means they are on different networks.
  - PC1 – 192.168.1.110
  - Web Server – 172.16.1.99



Role of the Data Link Layer Addresses: Different IP Networks

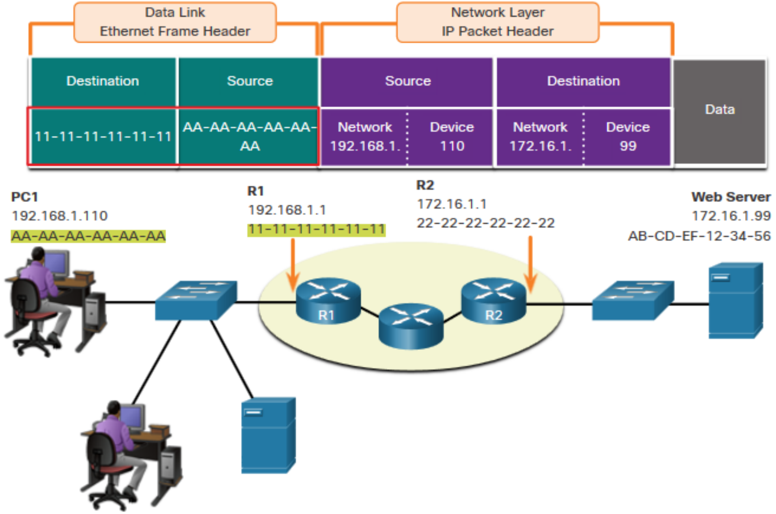
- When the final destination is remote, Layer 3 will provide Layer 2 with the local default gateway IP address, also known as the **router address**.
- The **default gateway** (DGW) is the router interface IP address that is part of this LAN and will be the “door” or “gateway” to all other remote locations.
- All devices on the LAN must be told about this address or their traffic will be confined to the LAN only.
- Once Layer 2 on PC1 forwards to the default gateway (Router), the router then can start the routing process of getting the information to actual destination.



Data Link Ethernet Frame Header		Network Layer IP Packet Header				
Destination	Source	Source		Destination		Data
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	Network 192.168.1.	Device 110	Network 172.16.1.	Device 99	

Role of the Data Link Layer Addresses: Different IP Networks

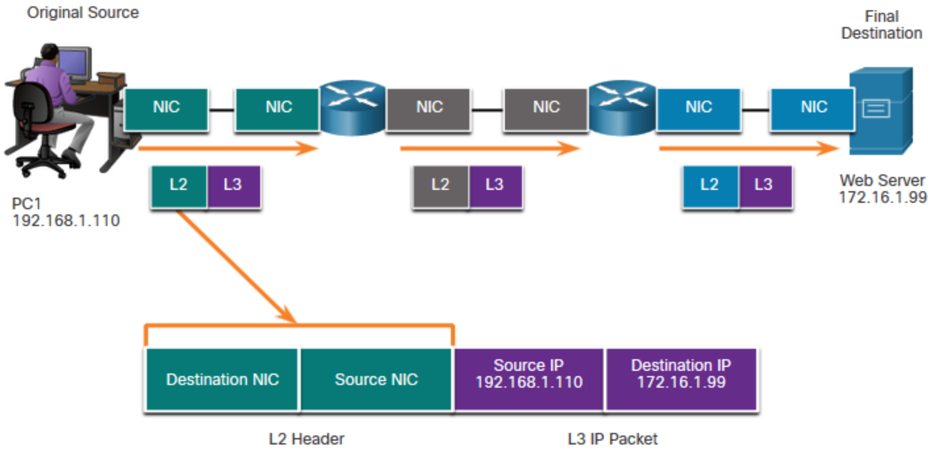
- The data link addressing is local addressing so it will have a source and destination for each link.
- The MAC addressing for the first segment is :
  - Source – AA-AA-AA-AA-AA-AA (PC1) Sends the frame.
  - Destination – 11-11-11-11-11-11 (R1- Default Gateway MAC) Receives the frame.
- Note: While the L2 local addressing will change from link to link or hop to hop, the L3 addressing remains the same.



Data Link Ethernet Frame Header		Network Layer IP Packet Header				
Destination	Source	Source		Destination		Data
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	Network 192.168.1.	Device 110	Network 172.16.1.	Device 99	

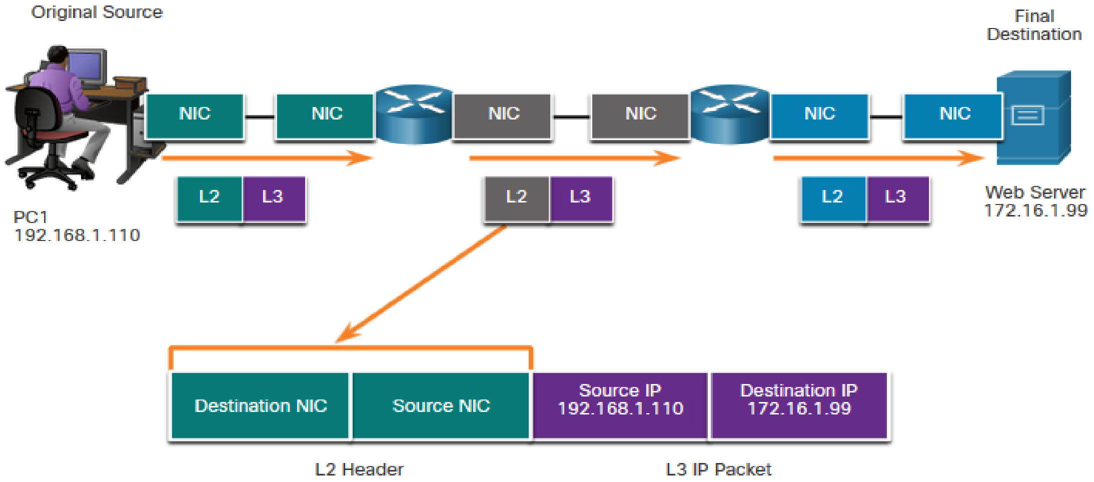
Data Link Addresses

- Since data link addressing is local addressing, it will have a source and destination for each segment or hop of the journey to the destination.
- The MAC addressing for the first segment is:
  - Source – (PC1 NIC) sends frame
  - Destination – (First Router- DGW interface) receives frame



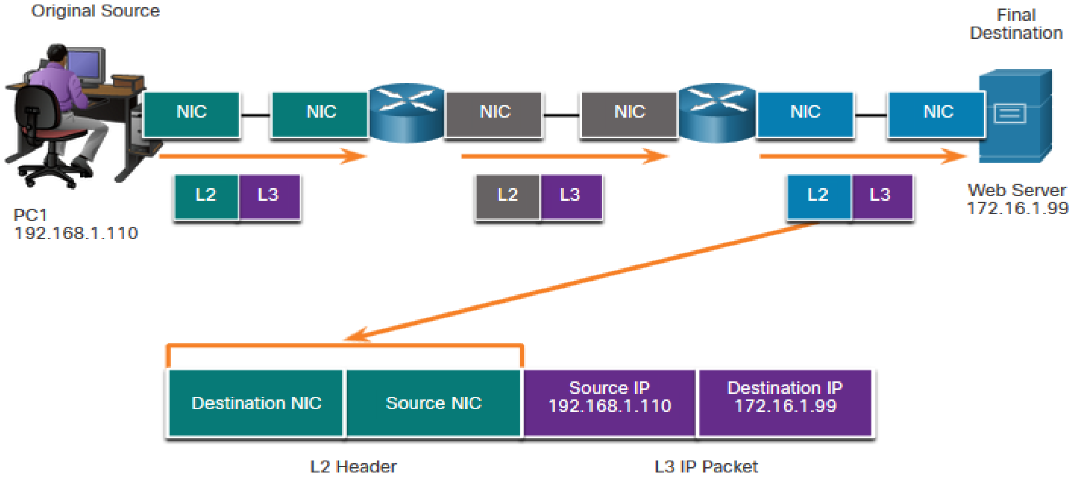
Data Link Addresses

- The MAC addressing for the second hop is:
  - Source – (First Router- exit interface) sends frame
  - Destination – (Second Router) receives frame



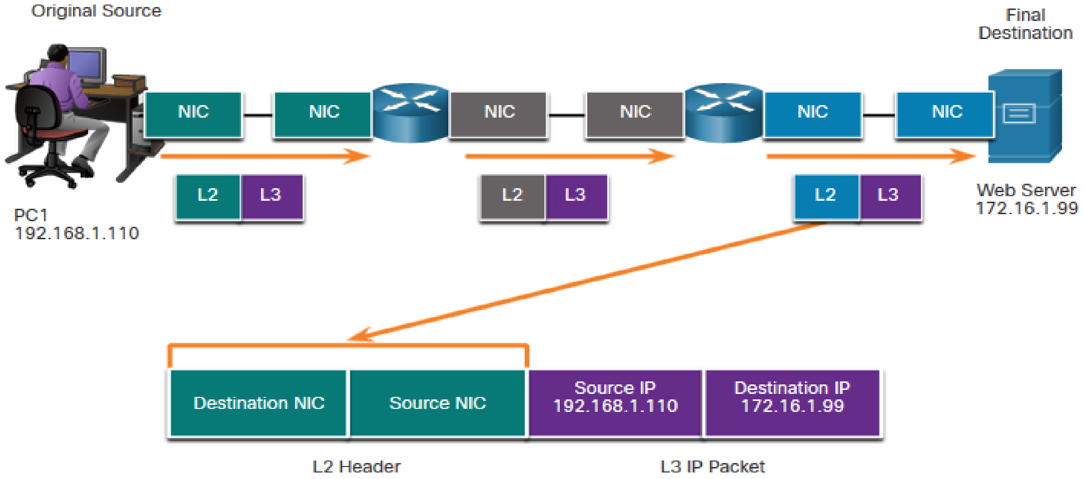
Data Link Addresses

- The MAC addressing for the last segment is:
  - Source – (Second Router- exit interface) sends frame
  - Destination – (Web Server NIC) receives frame

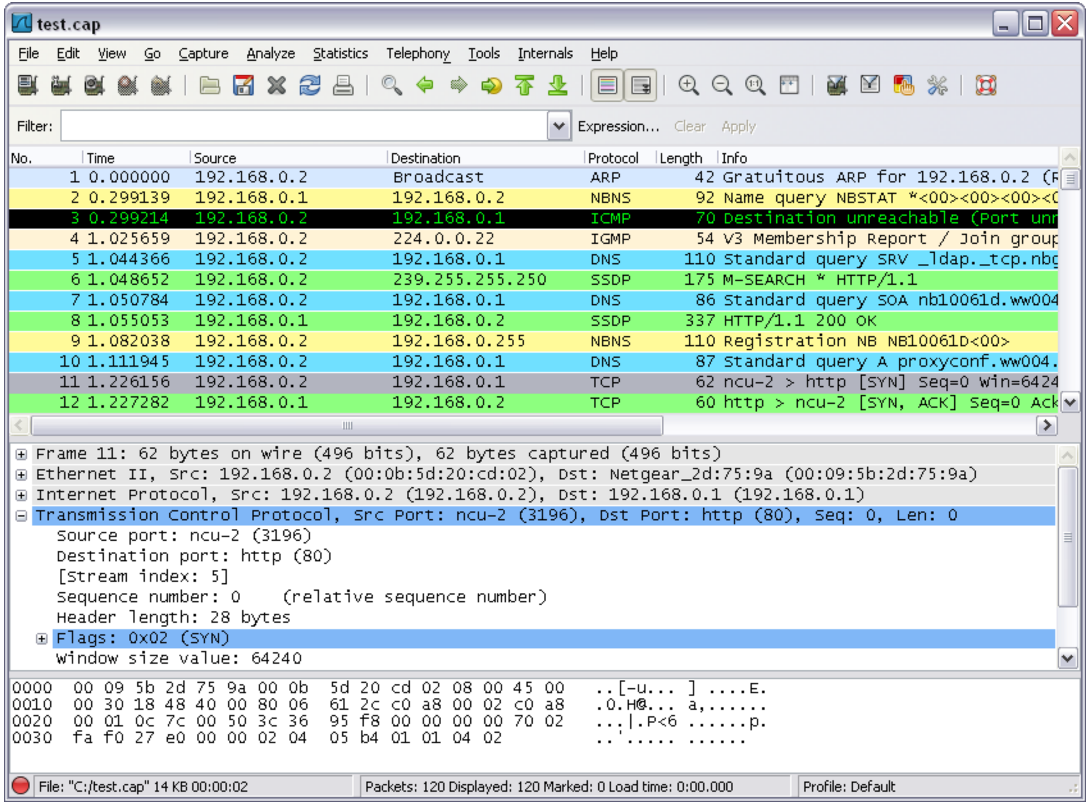


Data Link Addresses

- Notice that the packet is not modified, but the frame is changed, therefore the L3 IP addressing does not change from segment to segment like the L2 MAC addressing.
- The L3 addressing remains the same since it is global and the ultimate destination is still the Web Server.



Using Wireshark to View Network Traffic



test.cap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.    Time      Source           Destination      Protocol Length Info
     1 0.000000  192.168.0.2      Broadcast        ARP         42 Gratuitous ARP for 192.168.0.2 (R
     2 0.299139  192.168.0.1      192.168.0.2      NBNS        92 Name query NBSTAT *<00><00><00><0
     3 0.299214  192.168.0.2      192.168.0.1      ICMP        70 Destination unreachable (Port unr
     4 1.025659  192.168.0.2      224.0.0.22       IGMP        54 V3 Membership Report / Join group
     5 1.044366  192.168.0.2      192.168.0.1      DNS        110 Standard query SRV _ldap._tcp.nbg
     6 1.048652  192.168.0.2      239.255.255.250  SSDP       175 M-SEARCH * HTTP/1.1
     7 1.050784  192.168.0.2      192.168.0.1      DNS         86 Standard query SOA nb10061d.ww004
     8 1.055053  192.168.0.1      192.168.0.2      SSDP       337 HTTP/1.1 200 OK
     9 1.082038  192.168.0.2      192.168.0.255    NBNS       110 Registration NB NB10061D<00>
    10 1.111945  192.168.0.2      192.168.0.1      DNS         87 Standard query A proxyconf.ww004.
    11 1.226156  192.168.0.2      192.168.0.1      TCP         62 ncu-2 > http [SYN] Seq=0 Win=6424
    12 1.227282  192.168.0.1      192.168.0.2      TCP         60 http > ncu-2 [SYN, ACK] Seq=0 Ack
```

```
⊞ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊟ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size value: 64240
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "C:/test.cap" 14 KB 00:00:02 | Packets: 120 Displayed: 120 Marked: 0 Load time: 0:00.000 | Profile: Default

Warriors of the Net

- The animated video below will help you visualize networking concepts.
  http://www.warriorsofthe.net/

3.8 Module Practice and Quiz

What did I learn in this module?

- **The Rules**
  - Protocols must have a sender and a receiver.
  - Common computer protocols include these requirements: message encoding, formatting and encapsulation, size, timing, and delivery options.
- **Protocols**
  - To send a message across the network requires the use of several protocols.
  - Each network protocol has its own function, format, and rules for communications.
- **Protocol Suites**
  - A protocol suite is a group of inter-related protocols.
  - TCP/IP protocol suite are the protocols used today.
- **Standards Organizations**
  - Open standards encourage interoperability, competition, and innovation.

What did I learn in this module?

- **Reference Models**
  - The two models used in networking are the TCP/IP and the OSI model.
  - The TCP/IP model has 4 layers and the OSI model has 7 layers.
- **Data Encapsulation**
  - The form that a piece of data takes at any layer is called a *protocol data unit (PDU)*.
  - There are five different PDUs used in the data encapsulation process: data, segment, packet, frame, and bits
- **Data Access**
  - The Network and Data Link layers are going to provide addressing to move data through the network.
  - Layer 3 will provide IP addressing and layer 2 will provide MAC addressing.
  - The way these layers handle addressing will depend on whether the source and the destination are on the same network or if the destination is on a different network from the source.

New Terms and Commands

- encoding
- protocol
- channel
- flow control
- response timeout
- acknowledgement
- unicast
- multicast
- broadcast
- protocol suite
- Ethernet
- standard
- proprietary protocol
- 802.3 (Ethernet)
- 802.11 (wireless Ethernet)
- segmentation
- default gateway
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP)
- Transmission Control Protocol (TCP)
- transport
- data link
- network access
- Advanced Research Projects Agency Network (ARPANET)

New Terms and Commands

- Internet Message Access Protocol (IMAP)
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- Network Address Translation (NAT)
- Internet Control Messaging Protocol (ICMP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Address Resolution Protocol (ARP)
- Dynamic Host Configuration (DHCP)
- encapsulation
- de-encapsulation
- protocol data unit (PDU)
- segment
- packet
- frame

cisco

Elk Technologies

https://elktech.org

Scott Stephenson