SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

ICT259 Computer Networking

Seminar 1: Fundamentals of Networking

Ms Wong Yoke Moon

Fundamentals of Networking

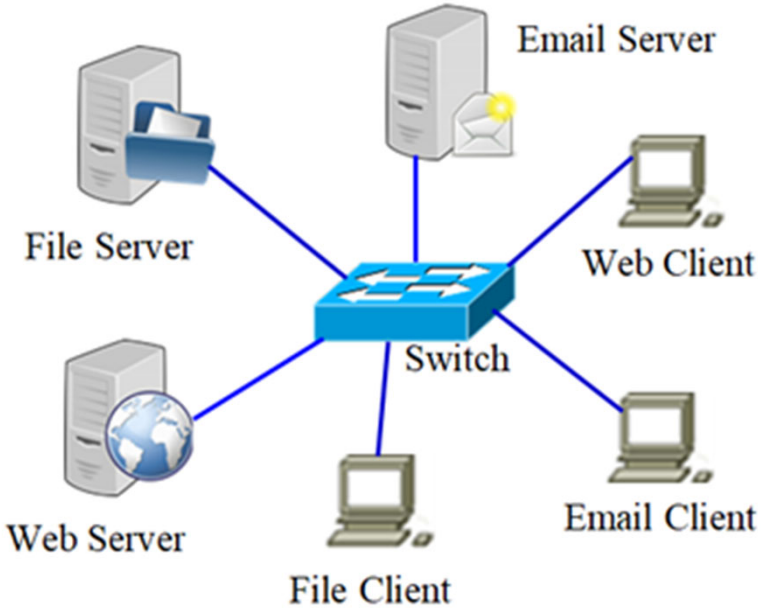
Objectives:

- Explain the differences between LAN and WAN topologies.
- Illustrate how LANs and WANs interconnect to the Internet.
- List the types of rules for successful communication.
- Describe the functions of each layer of the TCP/IP model.
- Describe the TCP/IP communication process.
- Compare the TCP/IP model with the OSI model.
- Describe the role of data encapsulation in enabling data to be transported across a network.
- Describe the process used by local hosts to access network resources

Definitions and Terminologies

Clients and Servers

- **Servers** are computers with software that **provide services** to other end devices.
- Each server has its **own server software**.
- **Clients** are computers with software installed that allow them to **request services** from the server.
- E.g. a client can use Microsoft Outlook to access email from an email server.

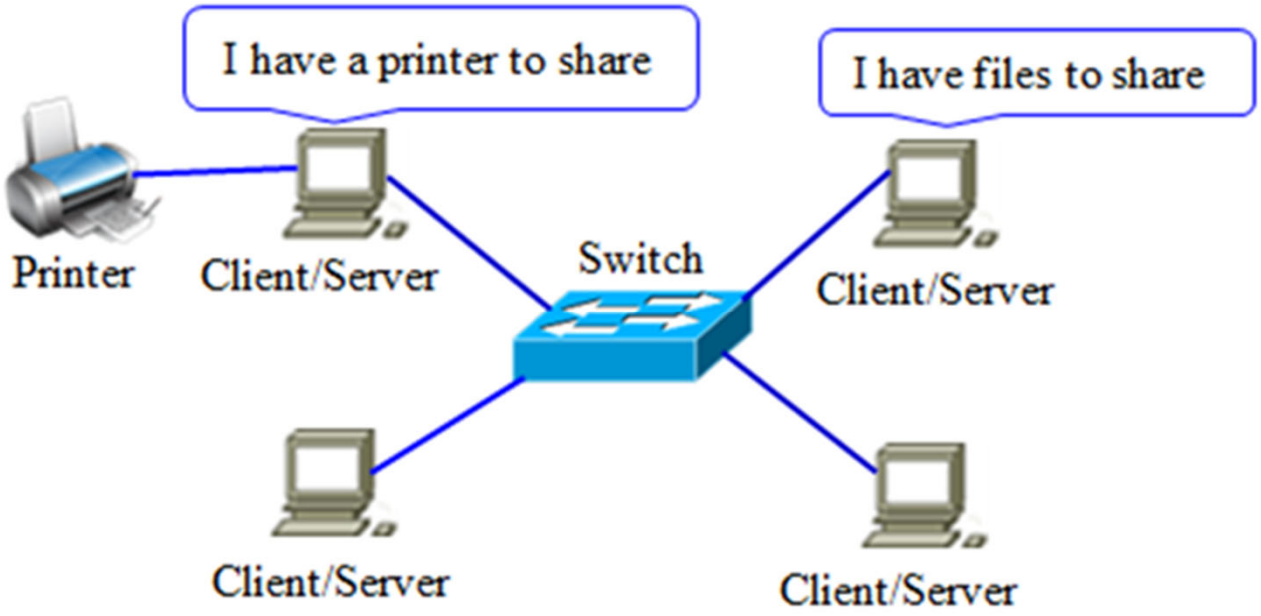


Client and Server Examples

Definitions and Terminologies

Peer-to-Peer (P2P)

- A peer-to-peer network has **no central server**.
- Each computer on the network **acts as a client as well as a server** and **shares its resources equally** with other computers



Peer-to-Peer Example

Definitions and Terminologies

Can you assign an IP Address to a switch ? Yes

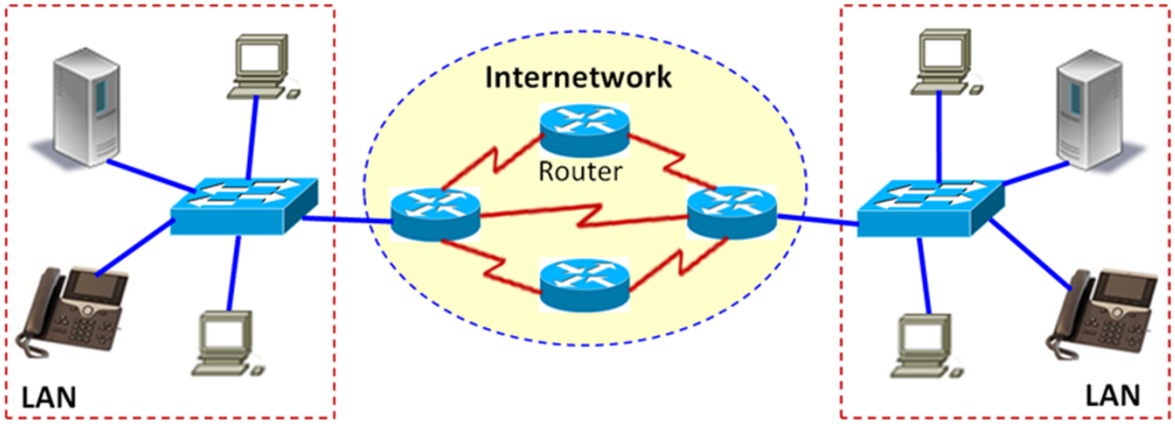
A host is any device that can take an IP address

End Devices and Hosts

- Network devices such as desktop computers, laptops, wireless tablets, smart phones, network printers, IP phones are end devices.
- All **end devices** that are connected to a network are called **hosts**.
- A **host** is also defined as a network node that is **assigned a network address**.

Intermediary Network Devices

- Intermediary network devices **connect end devices** to the network.
- It can also be used to **connect individual networks** to form an internetwork.
- E.g. of intermediary devices are switches, routers, wireless access points, modems and firewall appliances.

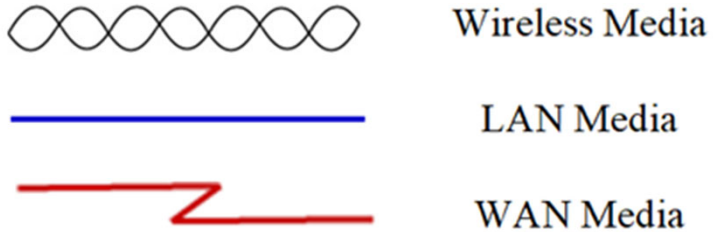


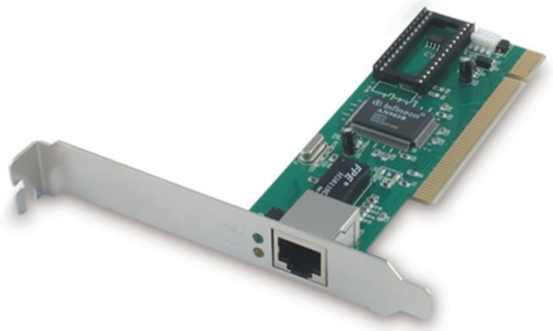
Interconnection of devices to an Internetwork

Definitions and Terminologies

Network Media

- A network media is the **path over which data travels** from source to destination.
- The path can be wired or wireless.
- Representations used in this course to distinguish the types of network connections.





Network Interface Card with a RJ45 Receptacle

Network Interface Card

- A Network Interface Card (NIC) or LAN adapter is a circuit board installed in an end device so that it can be connected to a network via a transmission media.

Physical Port and Interface

- A physical **port** on a router is referred to an **interface**.
- The NIC showed has a RJ45 receptacle or port.

Definitions and Terminologies

Local Area Network (LAN)

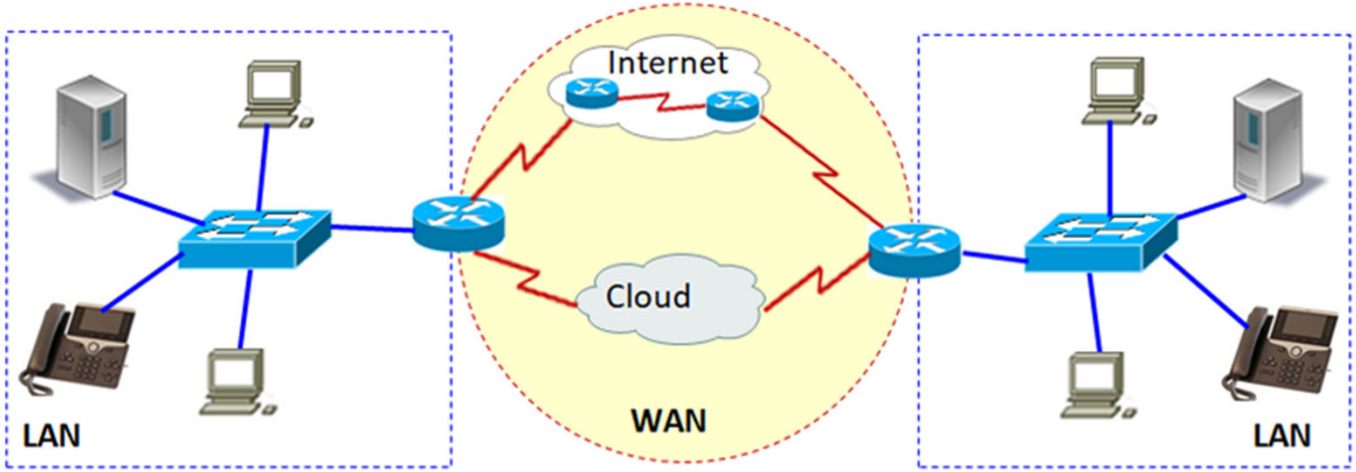
- A LAN is a network that links devices within a **small geographical area** such as a home, campus or an office building.
- The network is typically **owned and managed by an individual or organization**.

What is the role of the router in a network ?

It is to connect networks

Wide Area Network (WAN)

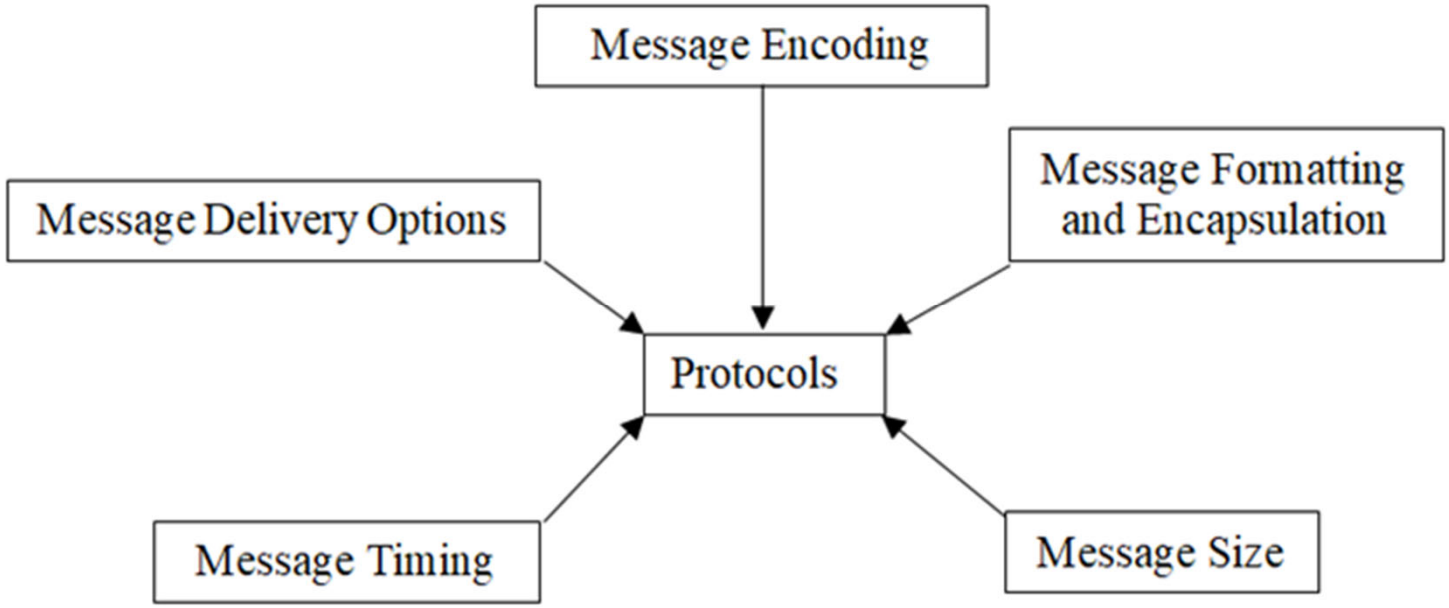
- A WAN is a network that spans over a **large geographical area** such as across cities, countries or continents.
- The network is typically **owned and managed by an Internet Service Provider**.



WAN interconnects LANs

Rules of Communication

- Protocols are **rules that govern the communication** between 2 communicating devices.
- Both devices must **use the same rules to communicate**.
- Common communication protocols have the following requirements:

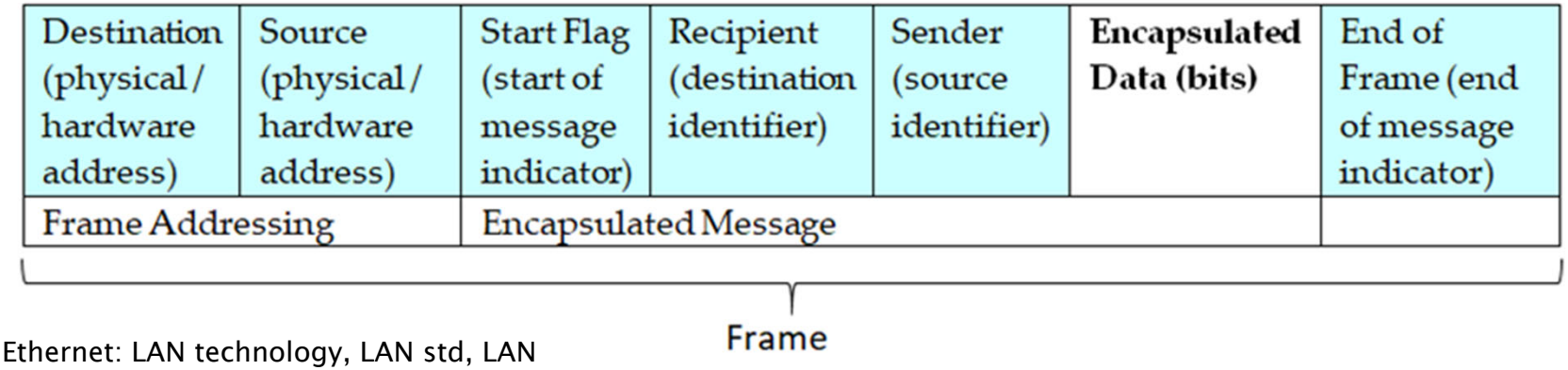


Protocol Requirements

Rules of Communication

Message Formatting and Encapsulation

- A message that is sent from source to destination must use a specific format.
- The **type of** message **format** to use **depends on** the **type of message** and the **channel** that is used to deliver the message.
- The data to be sent together with other information are **assembled into a frame**.
- **Encapsulation** is the process of **putting something around the data**, as shown by the shaded fields in Frame Format given below.
- **Decapsulation** occurs when the **process is reversed** by removing what have been added.



Ethernet: LAN technology, LAN std, LAN Architecture

Frame Format

Rules of Communication

Message Delivery Options

A broadcast is to all devices in the same network

There are three delivery options:

- **Unicast** – A **one-to-one** transmission, i.e. one source to one destination.

- **Multicast** – A one-to-many transmissions, i.e. **one** source **to a target group** of hosts simultaneously.

- **Broadcast** – A **one-to-all** transmissions, i.e. one source to all host in the network.

Network Protocols and Standards

Protocol Suites

- A *protocol suite* is a **set of related protocols** that **work together to perform a** communication **function**.
- Protocol suites are implemented by networking devices in **software**, **hardware**, or both.
- You can visualize a protocol suite as a **stack**, with **layers** of the stack **as protocols**.
- The interaction between layers of a protocol stack is called protocol interaction.
- There are a few industry protocol suites available.
- We will first examine the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

A protocol suite is a set of related protocols. Its a set.

It is a set put together to perform various functions

A protocol suite has horizontal and vertical interactions

TCP/IP Protocol Suite

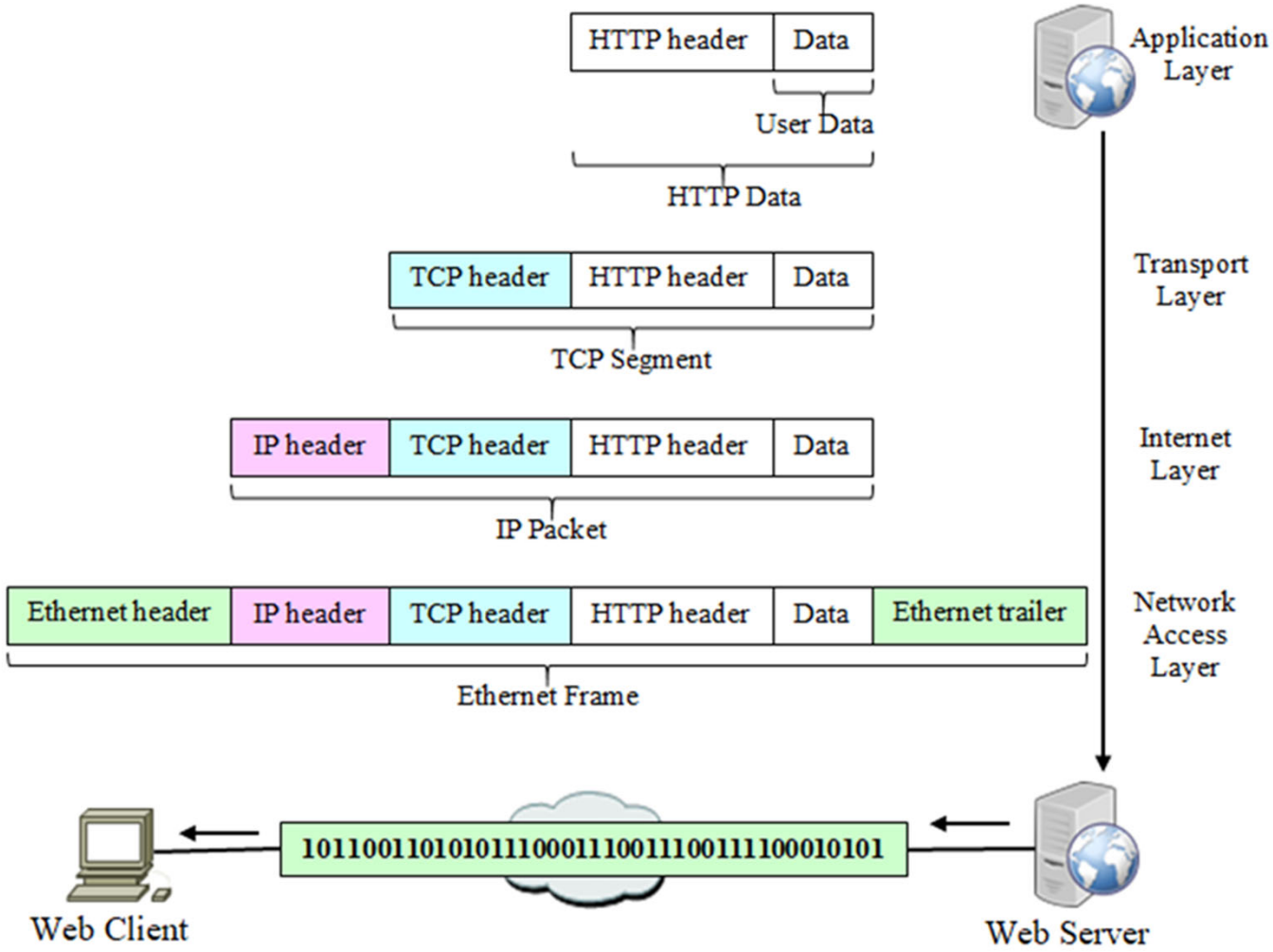
- The TCP/IP protocol suite is an **open standard**, meaning any vendor can freely implement these protocols on their hardware and/or software.
- **Standards** ensure that products developed based on the protocols can **interoperate successfully**.
- The TCP/IP protocol suite includes many protocols as shown below.

<table>
<tr><td>TCP/IP Protocol Suite</td><td colspan="5">Protocols</td></tr>
<tr><td>Layer Name</td><td>Name System</td><td>Host Config</td><td>Email</td><td>File Transfer</td><td>Web</td></tr>
<tr><td>Application Layer</td><td>DNS</td><td>BOOTP
DHCP</td><td>SMTP
POP
IMAP</td><td>FTP
TFTP</td><td>HTTP</td></tr>
<tr><td>Transport Layer</td><td colspan="2">UDP</td><td colspan="3">TCP</td></tr>
<tr><td>Internet Layer</td><td>IP
NAT</td><td>IP Support
ICMP</td><td colspan="3">Routing Protocols
OSPF RIP</td></tr>
<tr><td>Network Access Layer</td><td>ARP</td><td>PPP</td><td>Ethernet</td><td colspan="2">Interface Drivers</td></tr>
</table>

- Protocols in the **Application**, **Transport** and **Internet** layers are **specific to TCP/IP**.
- The **Network Access** layer protocols are responsible for **delivering** the message **over the physical medium**.
- **Network Access** layer protocols are developed by **various standards organizations**.

TCP/IP Communication Process

- The complete communication process of a web server transmitting data to a web client.



TCP/IP Communication Process

Steps of Communication Process

1. The web server prepares the Hypertext Markup Language (HTML) page as user data to be sent.

2. At the Application layer, the application protocol HTTP header is added to the front of the HTML data.

3. The HTTP application layer protocol delivers the HTML web page data to the Transport layer.

4. At the Transport layer, the TCP protocol adds a TCP header to the HTTP data to form the TCP segment. The function of the transport layer protocol is to support communication between devices, in this case the web server and web client. Next, the TCP protocol delivers the TCP segment to the Internet layer.

5. At the Internet layer, the IP protocol adds an IP header to the TCP segment to form the IP packet. The IP protocol assigns appropriate source and destination IP addresses and placed these information in the IP header. Next, the IP protocol delivers the IP packet to the Network Access layer.

TCP/IP Communication Process

Steps of Communication Process

6. At the Network Access layer, the Ethernet protocol adds an Ethernet header and an Ethernet trailer to the IP packet to form the Ethernet frame. This Ethernet frame which consists of a series of binary bits is transmitted across the internetwork to the web client. As mentioned previously, encapsulation is the process of adding something around some data. As data moved from the Application layer down to the Network Access layer, encapsulation takes place at each layer as header is added. For the Network Access layer, a trailer is also added.

7. At the Network Access layer, the web client receives the Ethernet frame in binary form. To get to the user data or HTML web page, a de-capsulation is performed at each layer in reverse order as it moves from Network Access layer to Application layer. First, the Ethernet header and trailer are processed and removed, then the IP header, the TCP header, and finally the HTTP header.

8. Finally, the web page information is passed on to the web client's web browser software.

Reference Models

- A reference model is a conceptual **framework for understanding relationships between** various **protocols**.
- The two primary models used in networking are:
  1. Open Systems Interconnection (OSI) Model
  2. TCP/IP Model

Benefits of Using a Layered Reference Model

- **Easier standardization**: Each layer focuses on specific functions, making the development of standards easier.

- **Lower dependence**: Changes in one layer will not affect other layers; protocols or functions of each layer can be independently developed.

- **Ensure interoperability**: Products from different vendors can work together.

- **Easier to understand**: Layering protocols and functions make it clearer for people to study and research networks.

OSI Reference Model

- The OSI model has seven layers.
- Each layer has its functions and services and it interacts with layers directly above and below.

Layer No.	Layer Name	Description
7	Application	Contains protocol used for process-to-process communications.
6	Presentation	Provides data representation to ensure the application layer of one device can identify and understand the data generated by the application layer of another device.
5	Session	Provides services to the presentation layer to establish, manage, and terminate communication sessions between two parties, and determine whether a party can initiate communication.
4	Transport	Provides transparent transfer of data between end devices, responsible for end-to-end error recovery, flow control and reassembly of data.
3	Network	Provides node-to-node transmission over the network between identified end devices based on network layer address.
2	Data Link	Describes methods for exchanging data frames between devices over a physical media.
1	Physical	Describes the mechanical, electrical, functional and procedural means to activate, maintain, and de-activate physical connections for bit transmission to and from a network device.

TCP/IP Model

- The TCP/IP model is sometimes referred to as the **Internet model**.
- The table below lists the functions of each layer of the TCP/IP.

Layer Name	Function
Application	Represents data to the user, perform encoding and dialog control. User typically interact with application program (e.g. to retrieve web page) to get work done.
Transport	Controls the flow of information between the application program running the client and the application program running the server.
Internet	Determines the best path through the network.
Network Access	Controls the hardware devices and media that make up the network.

OSI Model and TCP/IP Model Comparison

- The main difference between the OSI model and the TCP/IP model, and **how they are divided**, is **due to the protocols they use**.
- The suite of protocols used in the TCP/IP model is shown below, but not for the OSI model as the OSI protocol suite will not be emphasized in this course.
- Another reason is that most **Internet and network designers** opted for the **TCP/IP model**.

OSI Model	TCP/IP Model	TCP/IP Protocol Suite
7. Application	Application	HTTP, DNS, DHCP, FTP
6. Presentation		
5. Session		
4. Transport	Transport	TCP, UDP
3. Network	Internet	IPv4, IPv6, ICMPv4, ICMPv6
2. Data Link	Network Access	PPP, Frame Relay, Ethernet
1. Physical		

OSI Model and TCP/IP Model Comparison

- OSI layers 5, 6, and 7 maps to the application layer of the TCP/IP model.
- OSI layers **5, 6, and 7** are used as references **for application software developers** to develop network products.
- **TCP/IP** application layer protocols **provide specific functions** to a variety of end user applications, like HTTP, DNS, DHCP and FTP.

- OSI **layer 4**, the transport layer, maps directly to the transport layer of the TCP/IP model.
- The function of this layer is to **provide ordered and reliable transmission** between source and destination devices.

OSI Model	TCP/IP Model	TCP/IP Protocol Suite
7. Application	Application	HTTP, DNS, DHCP, FTP
6. Presentation		
5. Session		
4. Transport	Transport	TCP, UDP
3. Network	Internet	IPv4, IPv6, ICMPv4, ICMPv6
2. Data Link	Network Access	PPP, Frame Relay, Ethernet
1. Physical		

OSI Model and TCP/IP Model Comparison

- OSI **layer 3**, the network layer, maps directly to the Internet layer of the TCP/IP model.
- This layer describes protocols for **addressing and routing messages** through an internetwork.

- OSI **layers 1 and 2** describe the procedures to **access the media** and the **physical means to transmit** the data over a network.
- At the **network access** layer, the TCP/IP protocol suite **does not specify** which **protocols** to use **to send data over a physical medium**. The protocol to use **depends on the physical network**.

OSI Model	TCP/IP Model	TCP/IP Protocol Suite
7. Application	Application	HTTP, DNS, DHCP, FTP
6. Presentation		
5. Session		
4. Transport	Transport	TCP, UDP
3. Network	Internet	IPv4, IPv6, ICMPv4, ICMPv6
2. Data Link	Network Access	PPP, Frame Relay, Ethernet
1. Physical		

Data Transfer in the Network

Data Encapsulation

- To transmit data over the network, data must be **encapsulated with appropriate addressing and control information** so that it can go from source to destination.

- The **type of information** required depends on whether the **destination** is within a **local** or in a **remote** network.

Message Segmentation

- For delivery efficiency, before a message is sent from source to destination, it is **divided into smaller** manageable **pieces**.

- This division of a message into smaller pieces is called ***segmentation***.

- **Each piece** or segment of the message **must go through the same process** to get to the destination.

- When all the pieces **arrived at the destination**, it is **reassembled** into the original message.

Data Transfer in the Network

Protocol Data Units (PDUs)

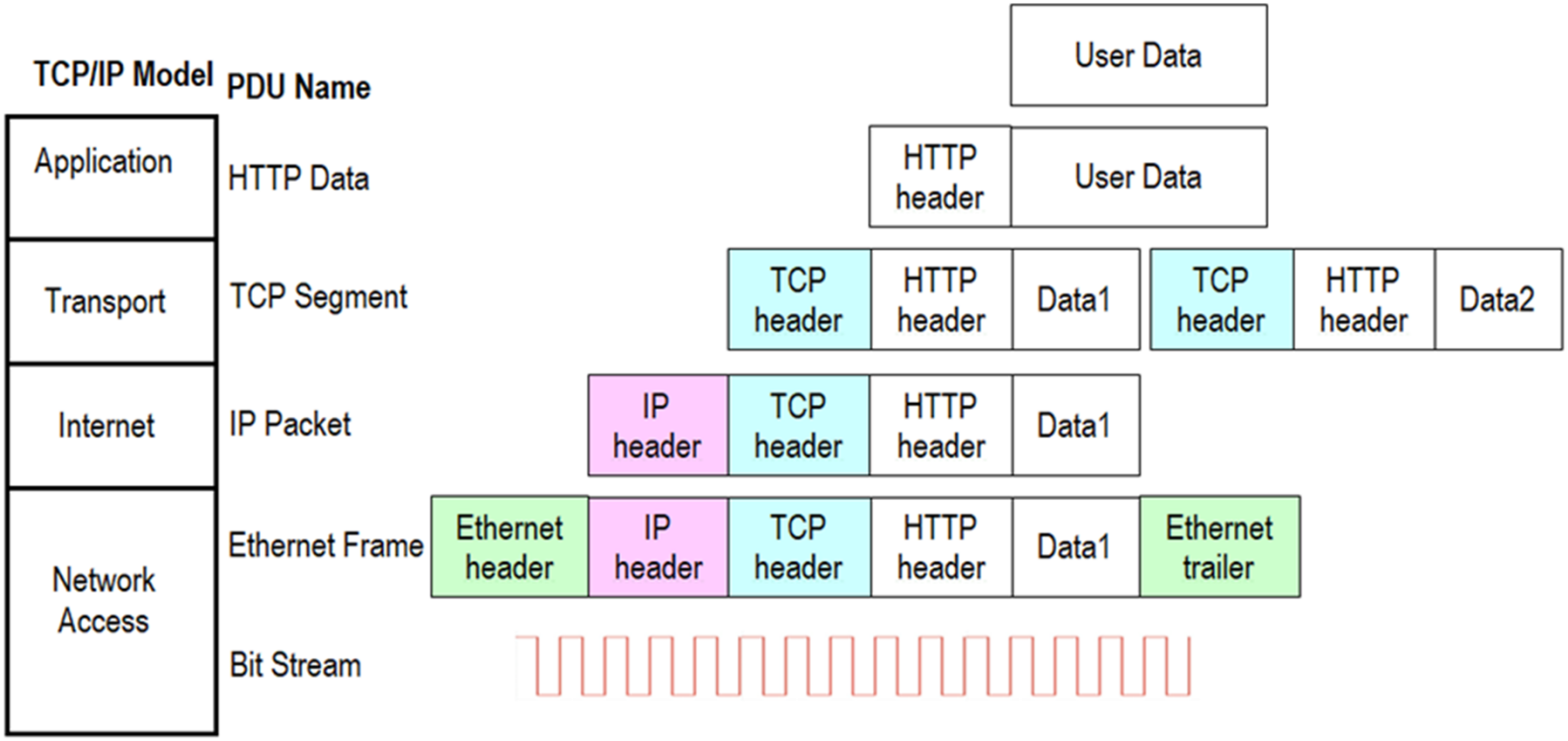
- PDU is used to describe the **data unit** of each layer of the model.
- In the OSI model, the **lower four layers are given specific names**.
- The **upper three layers** are just called '**Data**'.
- Sometimes, the data unit can be referred to by the name of the layer.

OSI Layer	PDU Name	PDU Name based on layer
7. Application	Data	Application Data Unit
6. Presentation	Data	Presentation Data Unit
5. Session	Data	Session Data Unit
4. Transport	Segment	Transport Data Unit
3. Network	Packet	Network Data Unit
2. Data Link	Frame	Data Link Data Unit
1. Physical	Bit	Physical Data Unit

Data Transfer in the Network

Encapsulation

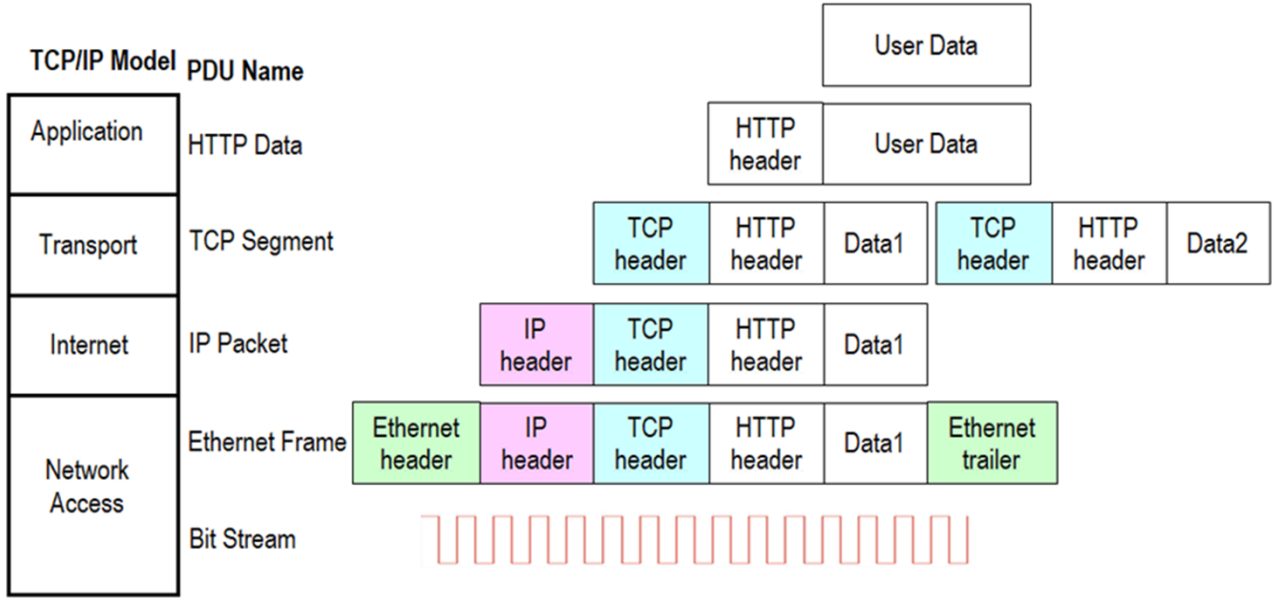
- When sending data on a network, the encapsulation process works from top to bottom by adding a header to the data unit from the upper layer before passing it down to the lower layer.
- Figure below shows the encapsulation process of the previously mentioned **web server example**. Note: The segmentation at the Transport layer.



Data Transfer in the Network

Encapsulation

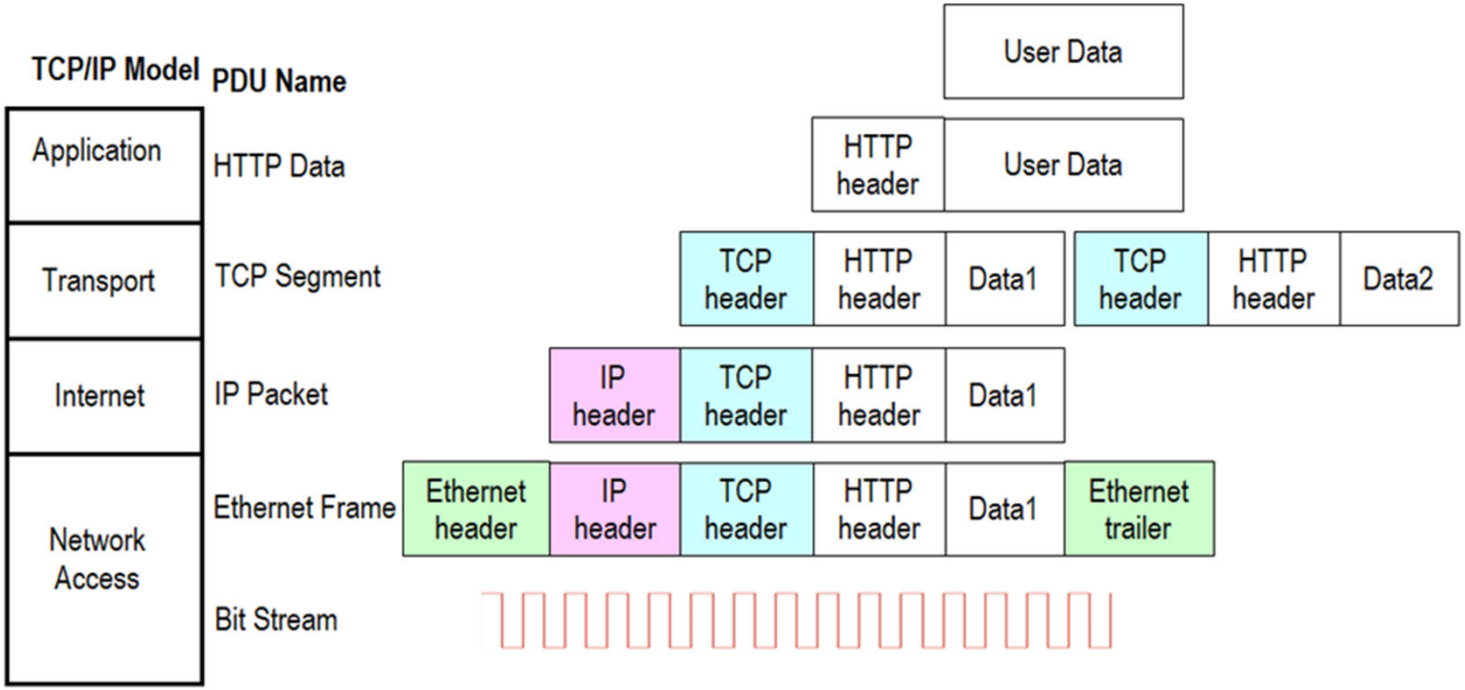
- The data the web server wanted to send to the web client will be **encapsulated through the layers** on the web server.
- The **application layer** will **add a HTTP header** to the original data to form the HTTP data.
- Since the **HTTP data is too long**, it will be **segmented** into two pieces (Data 1 and Data2) at the transport layer.
- At the transport layer, a TCP header is added to the front of each piece to form two **TCP segments**.
- Each piece is **delivered** to the destination **separately**.
- This example shows only the complete encapsulation process for Data1.



Data Transfer in the Network

Encapsulation

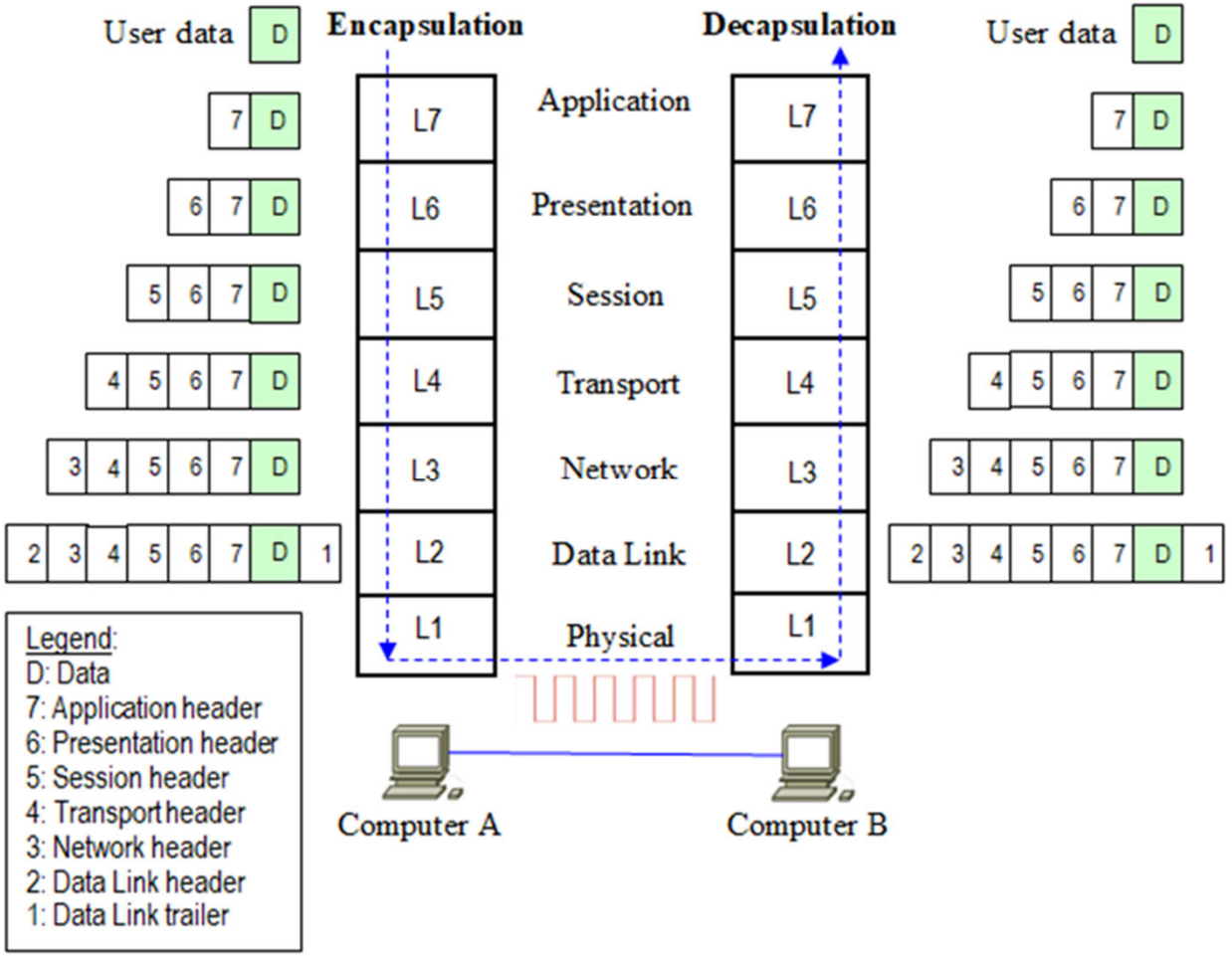
- At the Internet layer, an IP header is added to the front of each TCP segment to form an **IP packet**.
- When the IP packet arrives at the Network Access layer, assuming this layer is using **Ethernet technology**, it will add an Ethernet header and trailer to the IP packet, forming the **Ethernet frame**.
- Finally, this Ethernet frame is converted to a **bit stream** for transmission **over the physical media** to the web client.



Data Transfer in the Network

Encapsulation and Decapsulation

- Decapsulation is the **reverse process** of encapsulation.
- When the bit stream arrives at the receiving device, **protocol header is removed** as it moves up the stack toward the end-user application.



Data Access

- To transmit data from source to destination, the data must be **encapsulated** with the correct **source** and **destination addresses**.

- Two types of addresses with different purposes are needed for transmission of data over a network.

Ethernet MAC Addresses

- Every network interface card (NIC) has an unique Media Access Control (MAC) address, which is **48 bits** or 6 bytes in length.

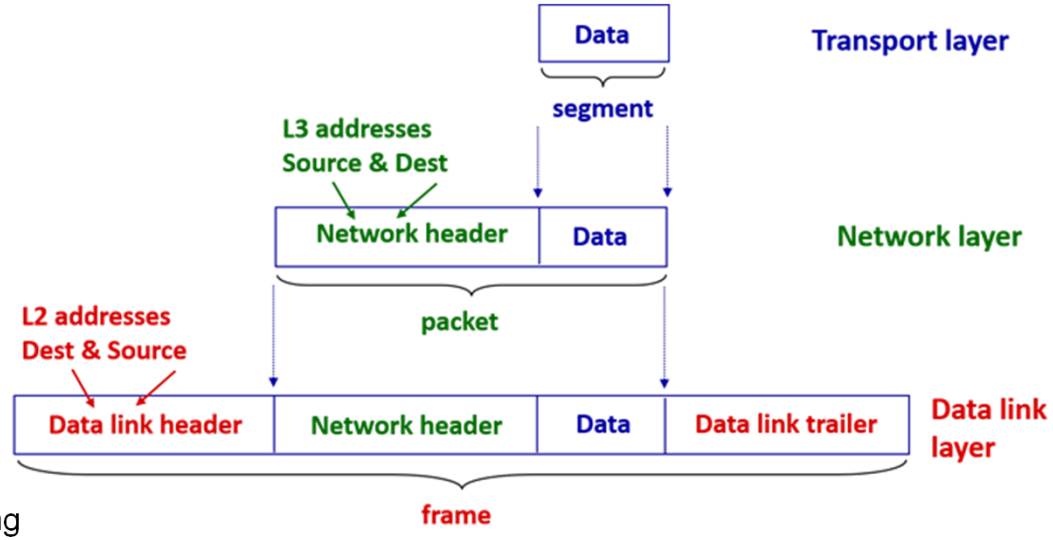
- It is usually expressed in **12 hexadecimal digits**.

- It is also referred to as the **physical or hardware address** of the NIC.

Data Access

Network and Data Link Addresses

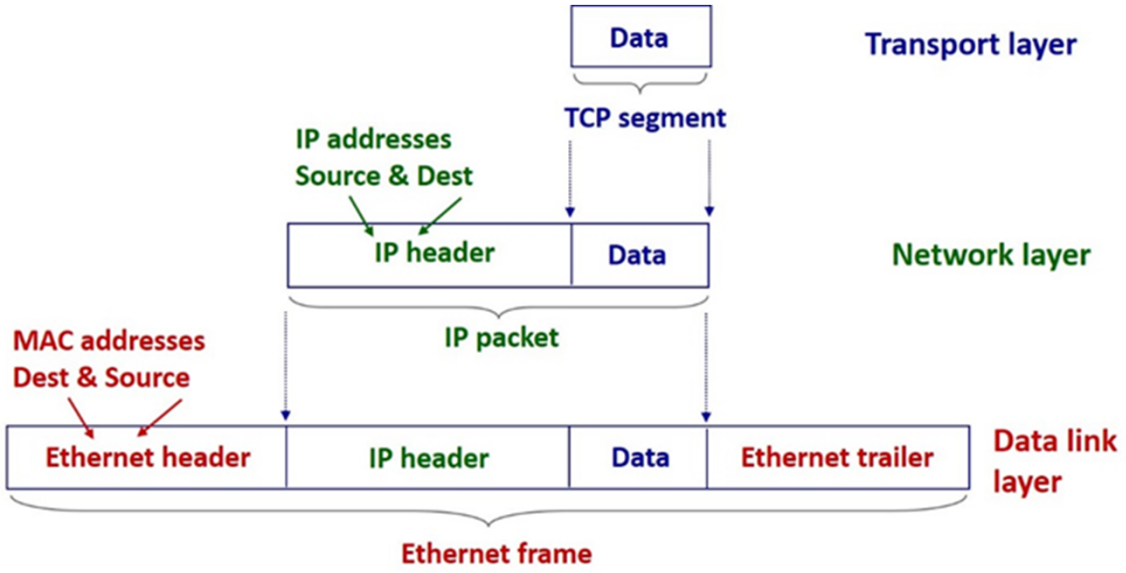
- Two types of addresses needed for transmission of data over a network are:
  1. **Network or Layer 3 addresses**, also known as ***end-to end*** addresses – The network layer source and destination addresses are responsible for delivering packet from the **original source** to the **end destination**, either on the same network or to a remote network.
  2. **Data Link or Layer 2 addresses**, also known as ***point-to point*** addresses – The data link layer source and destination addresses are responsible for delivering data link frame from one network interface card (**NIC**) to another **NIC** on the same network.
- Layer 2 (L2) and Layer 3 (L3) addresses are encapsulated in a frame.



Data Access

Network and Data Link Addresses

- If the **Layer 2** protocol is **Ethernet** and the **Layer 3** protocol is **IP**, then the Layers 2 and 3 addresses are **MAC** and **IP** respectively.
- Network addresses are known as *end-to-end* addresses because the **network source address** is the network address of the **device initiating the transmission**, and the **network destination address** is the network address of the **target device** that is destined to receive the message, regardless of whether the two devices are directly connected, separated by many intermediary devices, or in a remote network.
- For data link addresses, it is handled **differently** for devices on the **same network** and for devices on **different networks**.



Data Access

Data Link Addresses for Devices on the Same Network

- For devices on the same network, the data link **source address** is the data link address of the **device initiating the transmission**, and the data link **destination address** is the data link address of **target device** that is destined to receive the message.
- The end-to-end devices is the same as the point-to-point devices, as illustrated in the example given below.

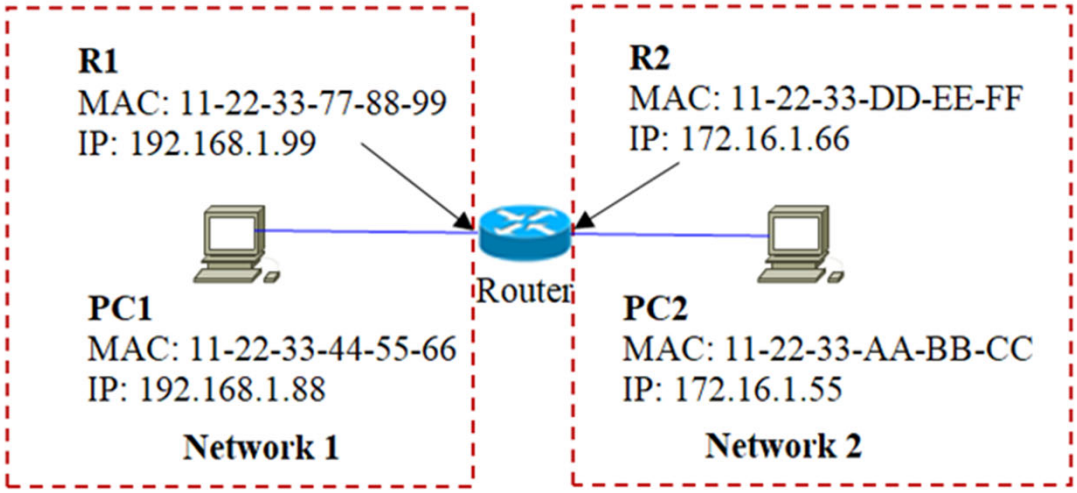
PC1
MAC: 11-22-33-44-55-66
IP: 192.168.1.88

PC2
MAC: 11-22-33-AA-BB-CC
IP: 192.168.1.99

L2 Source address:	11-22-33-44-55-66
L2 Destination address:	11-22-33-AA-BB-CC
L3 Source address:	192.168.1.88
L3 Destination address:	192.168.1.99

Data Link Addresses for Devices on Different Networks

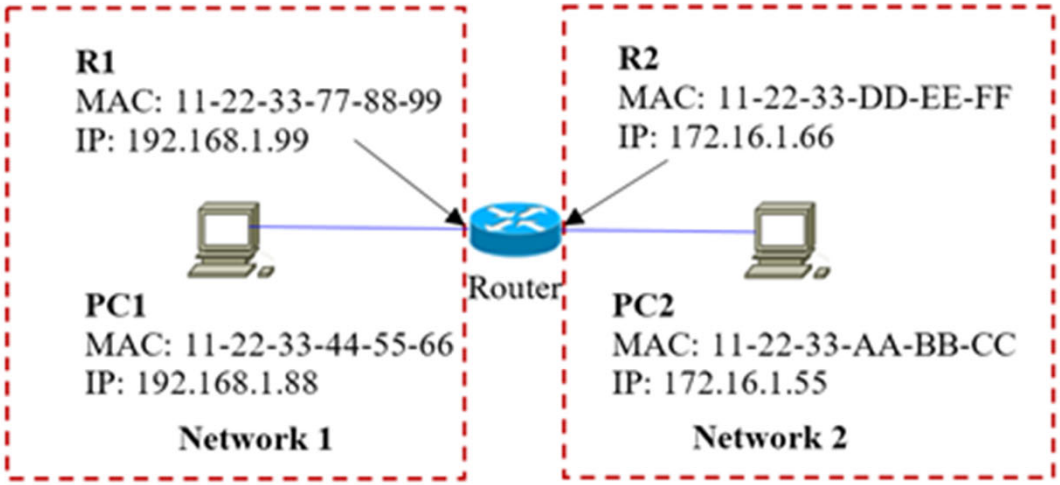
- Since the source and destination devices are on different networks, the data needs to traverse through at least two or more networks.
- To exit its own network and move on to another network, the data must traverse from **source NIC** to the **NIC of the exit device**, which is usually the router or default gateway.
- Upon arriving at the next network, the data will have to transmit from **one NIC** to **another NIC** on the same network on its way to the destination.
- The **data link source and destination addresses** will **change from network to network**.



Data Access

Data Link Addresses for Devices on Different Networks

- For each network, the **data link source and destination addresses** are the addresses of the **source and destination NICs** respectively, as it traverses through the network, as illustrated below.
- R1 and R2 are **Ethernet interfaces** of the router, each has its **own MAC and IP addresses**.



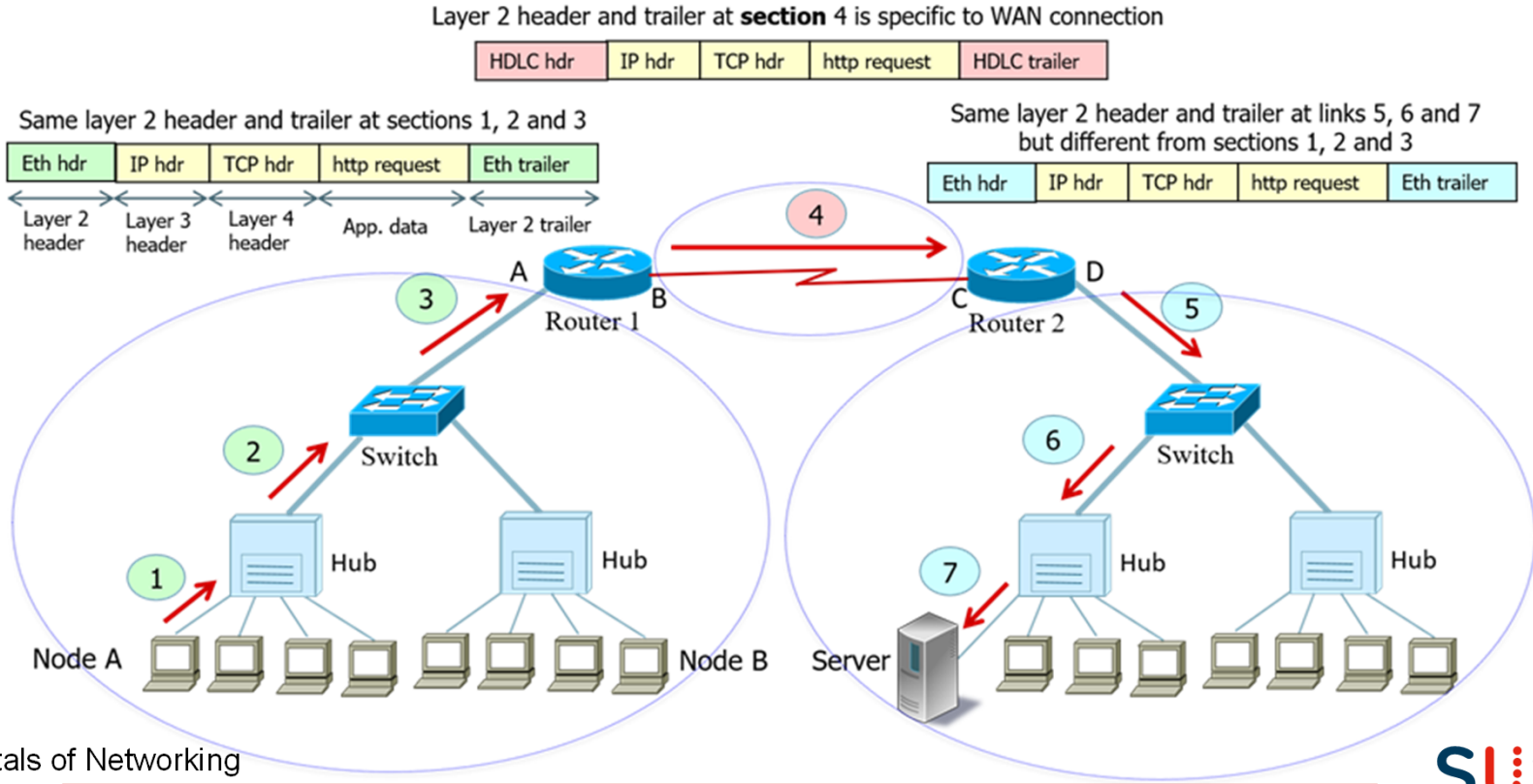
Network 1	
L2 Source address:	11-22-33-44-55-66
L2 Destination address:	11-22-33-77-88-99
L3 Source address:	192.168.1.88
L3 Destination address:	172.16.1.55

Network 2	
L2 Source address:	11-22-33- DD-EE-FF
L2 Destination address:	11-22-33-AA-BB-CC
L3 Source address:	192.168.1.88
L3 Destination address:	172.16.1.55

Data Access

Remote Network Communication Example

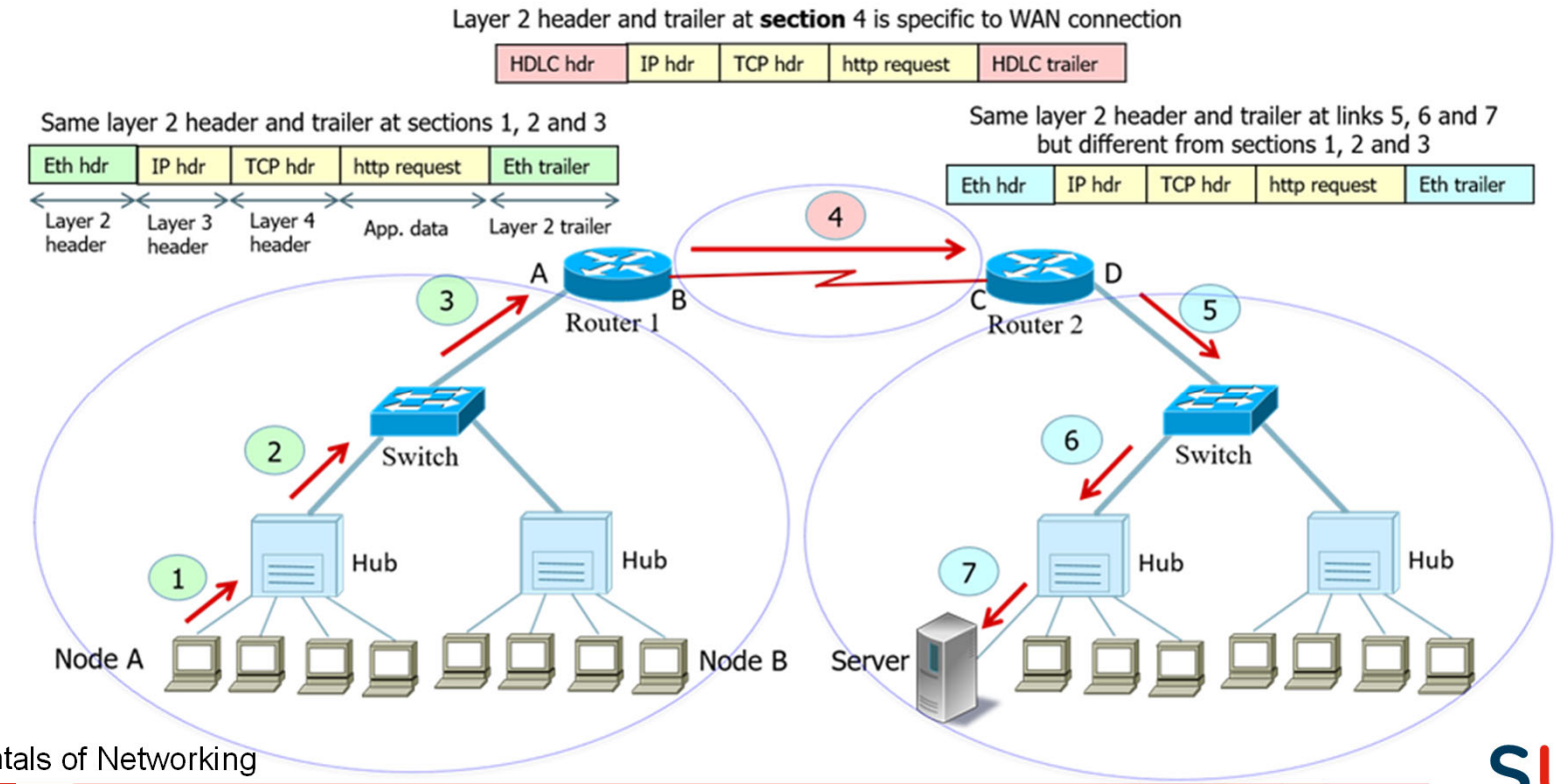
- **Node A** is sending a HTTP request to a **server** in another network.
- Assume the **data link protocol** for **LAN is Ethernet** and for **WAN is** High-Level Data Link Control (**HDLC**).
- The protocols at the **network** and **transport** layers are **IP** and **TCP** respectively.



Data Access

Remote Network Communication Example

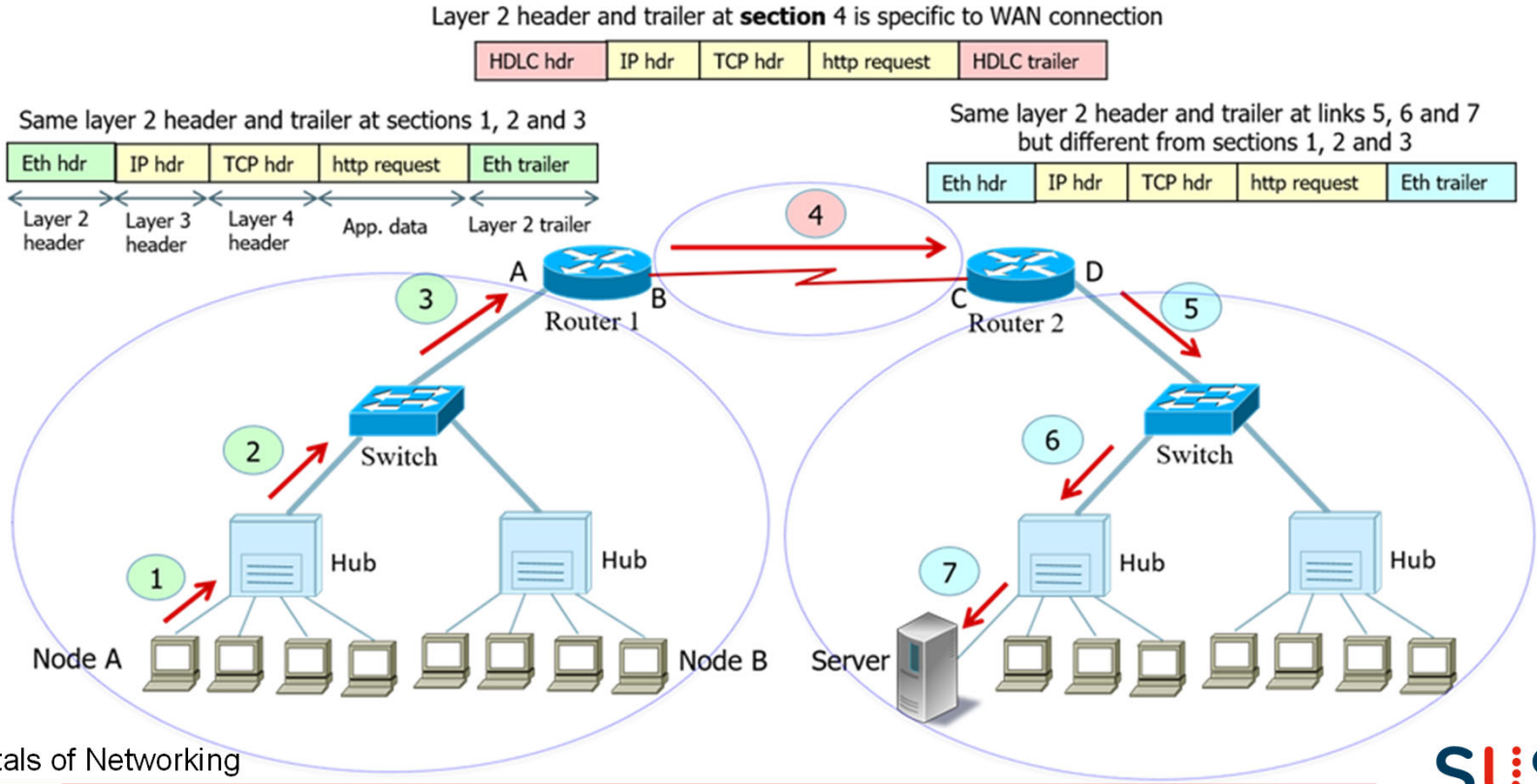
- There are 3 networks as indicated by circled ovals.
- Recall: Layer 2 addressing is point-to-point and layer 3 addressing is end-to-end.
- The layer 3 addressing is from Node A to Server.
- The layer 2 addressing has 3 sections, from Node A to point A, from point B to point C, and from point D to Server.



Data Access

Remote Network Communication Example

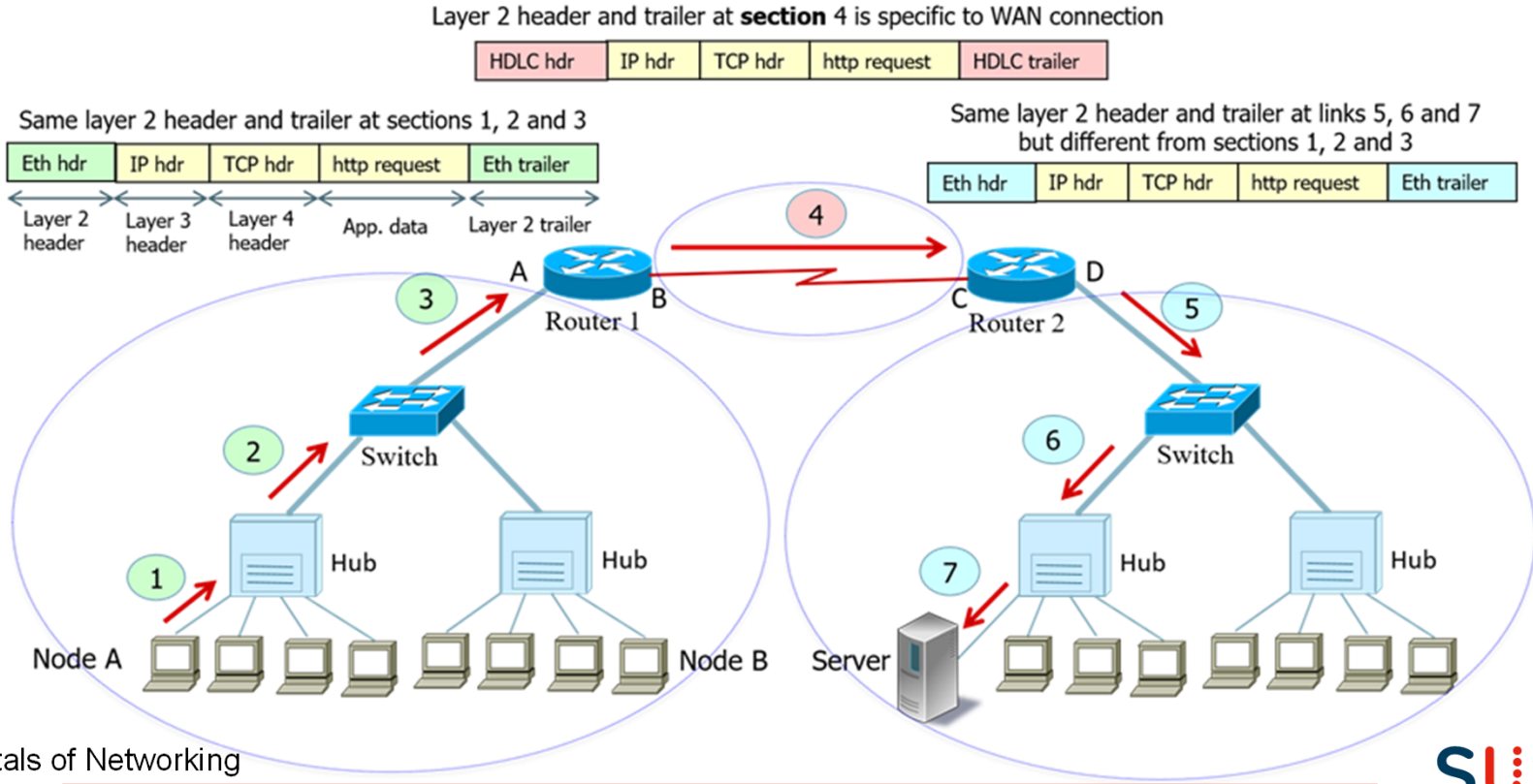
- The HTTP request is encapsulated at Node A with:
  1. **TCP header** to indicate it is a web request (**port number** = 80). Port number will be discussed in a later chapter.
  2. **IP header** to indicate the **source** IP address of **Node A** and the **destination** IP address of **Server**.



Data Access

Remote Network Communication Example

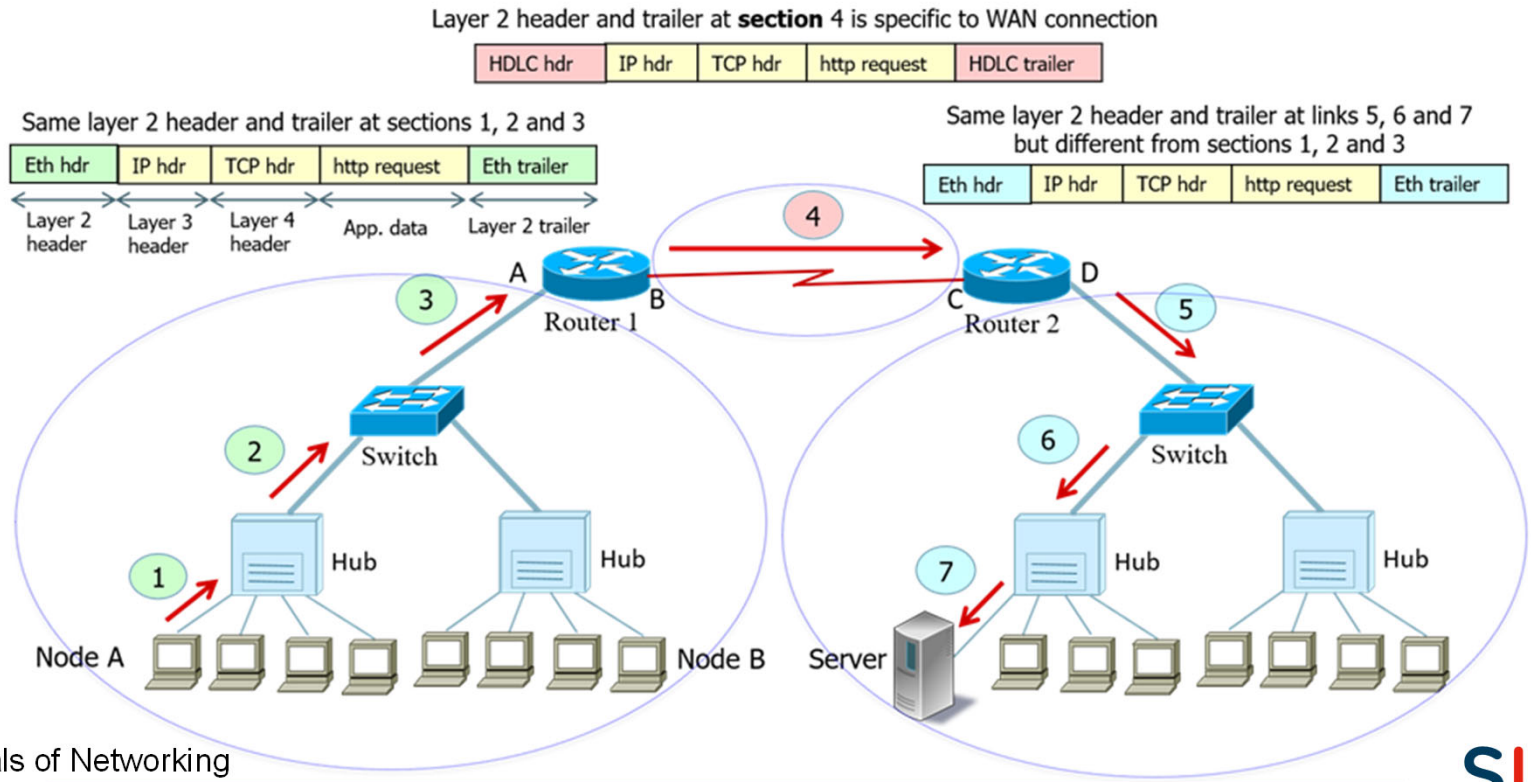
- The HTTP request is encapsulated at Node A with:
  3. **Ethernet header** to indicate the **source MAC address of Node A** and **destination MAC address** of **interface A of Router 1**.
  4. Ethernet trailer for error checking, which will be discussed in a later chapter.



Data Access

Remote Network Communication Example

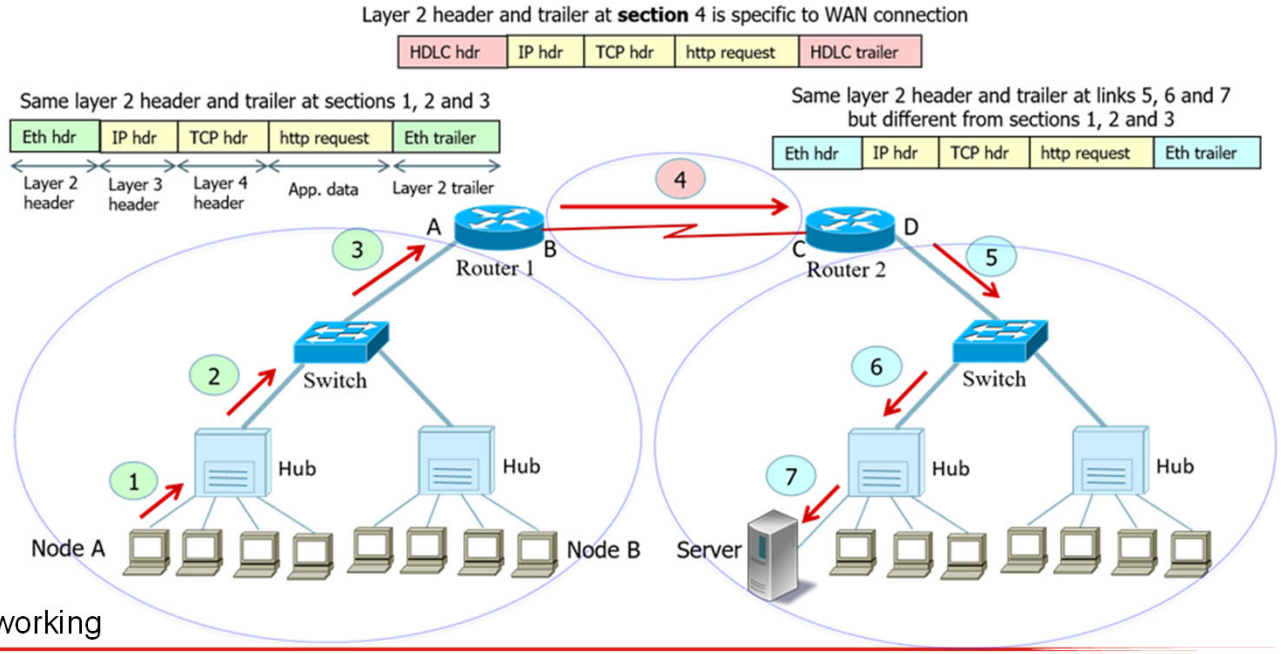
- The **hub and switch do not alter** the source and destination **MAC addresses** in the Ethernet header.
- The **hub has no intelligent** and the switch examines the destination MAC address to switch it correctly. **The switch does not alter its contents**. The **header contents are adjusted at the routers**.



Data Access

Remote Network Communication Example

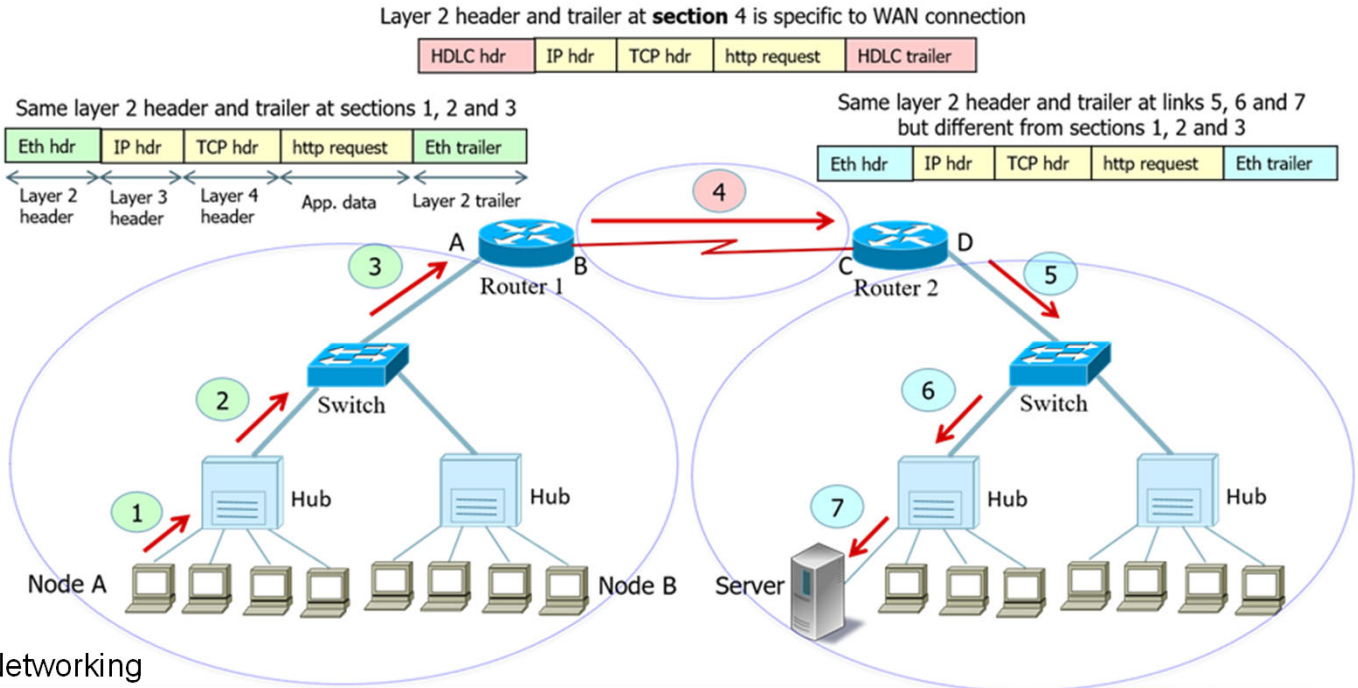
- As the Ethernet frame reaches Router 1, the destination IP address is examined, and the router's intelligence is consulted:
  1. Router 1 decides that it must send the request to Router 2.
  2. As this link is a HDLC WAN link, it must strip the Ethernet header and trailer, encapsulate with a HDLC header and trailer. The source layer 2 address of interface B and the destination layer 2 address of interface C are indicated in the header.
  3. The layer 3 and 4 headers as well as the HTTP request remain unchanged.



Data Access

Remote Network Communication Example

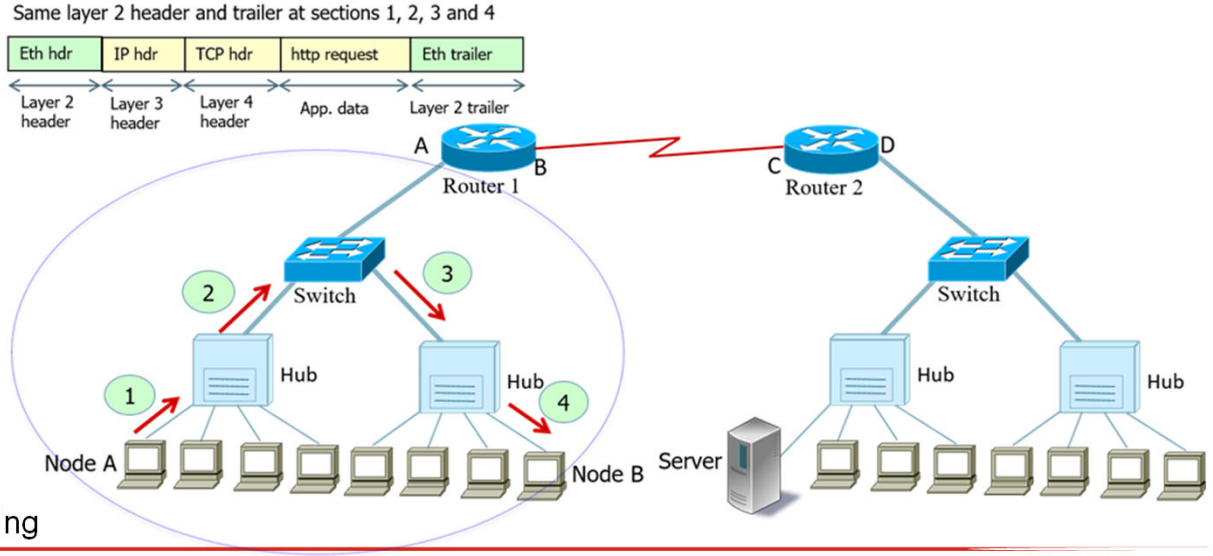
- As the HDLC frame reaches Router 2:
  1. The HDLC header and trailer are removed.
  2. Router 2 examines the destination IP address, consults its intelligence, and decides that it must be forwarded into the network containing the Server.
  3. The IP packet is encapsulated with an Ethernet header and trailer. The source MAC address at interface D of Router 2 and the destination MAC address of the Server are indicated in the header.



Data Access

Same Network Communication Example

- Node A transmits a frame to a station in the same network, say to Node B.
- Since they are in the **same network**, the **end-to-end** devices is the **same as** the **point-to-point** devices.
- There is **no change to any header** once it is encapsulated at Node A.
- The Ethernet header contains the **source MAC address of Node A** and the **destination MAC address of Node B**.
- The IP header contains the **source IP address of Node A** and the **destination IP address of Node B**.
- The encapsulated frame will be sent from **Node A to Node B without any change to its contents**.



Summary

- Differences between LAN and WAN
- Rules for successful communication
- Functions of each layer of the TCP/IP model
- TCP/IP Communication Process
- Comparison between OSI model and TCP/IP model
- Role of data encapsulation in enabling data transfer in the network
- Role of Layer 2 and Layer 3 addressing in data transmission

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Thank You.