



# 21AIE211

## Introduction to COMPUTER NETWORKS

### 2-0-3 3

Amrita Vishwa Vidyapeetham  
Amritapuri Campus





# Network Protocols

Dhivvya J P

Cisco Netacad Amritapuri Campus Instructor  
Amrita Vishwa Vidyapeetham

# Learning Objectives in Reliable Networks

- Network Trends
  - Online Collaboration
  - Cloud Computing
- Reliable Network features
  - Fault tolerance
  - Scalability
  - Quality of Service(QoS)
  - Security

# Network Trends

- Role of Network must adjust and continually transform to meet the user needs
- Networking trends that effect organizations and consumers:
  - Online Collaboration
  - Cloud Computing



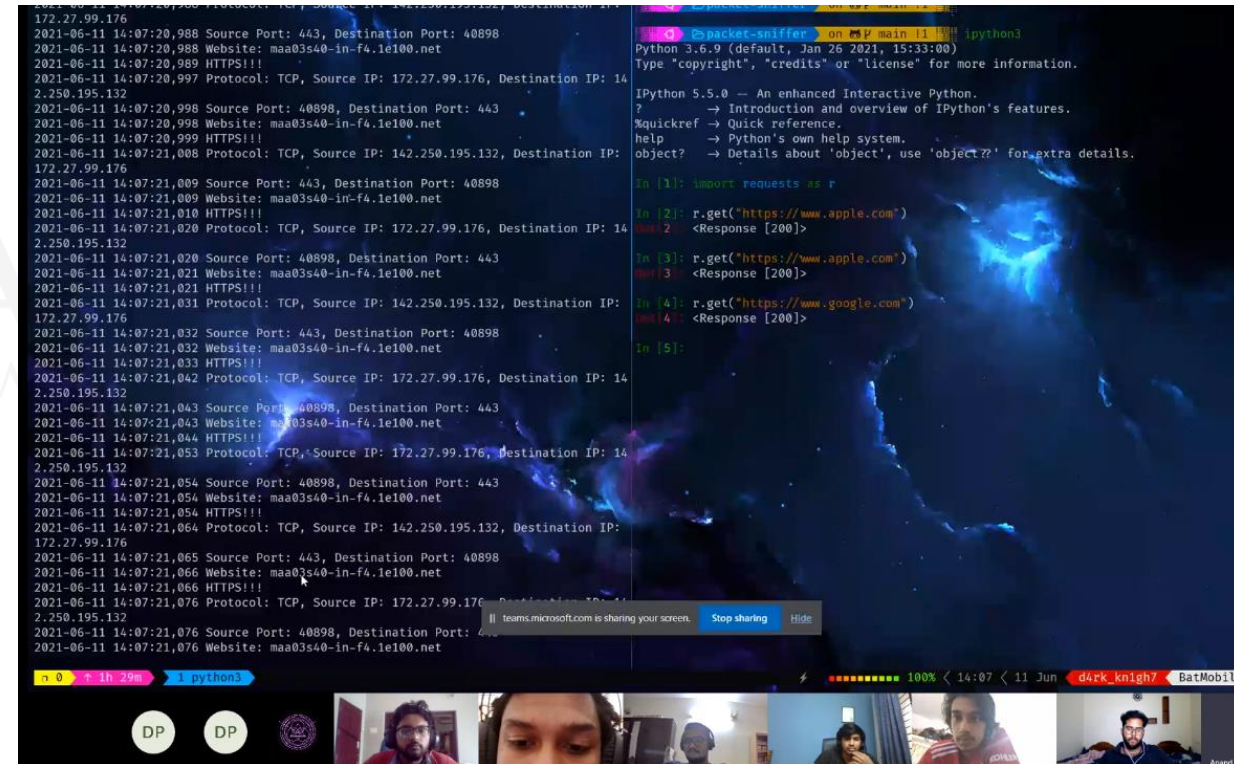
[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Ref: Cisco Netacad CCNA Introduction to Networks



# Online Collaboration

- Collaborate and work with others over the network on joint projects
- Collaboration tools are high priority in covid lockdowns for business and education
  - Ex: Skype, Microsoft teams, WebEx
- Multi-functional tools aiming at
  - Send instant messages
  - Post images, videos and links
  - Audio and Video call
  - Share screen



# Cloud Computing

- **Cloud Computing** allows us to store our data on the public servers
  - Helps to access shared data from multiple devices
  - Ex: Gmail Drive, Microsoft One Drive
- **Cloud Computing** is made possible by data centers
  - Companies not having data center can also borrow these services

Ref: Cisco Netacad CCNA Introduction to Networks



## Cloud Computing

*Having secure access to all your applications and data from any network device*

[This Photo](#) by Unknown Author is licensed under [CC BY](#)

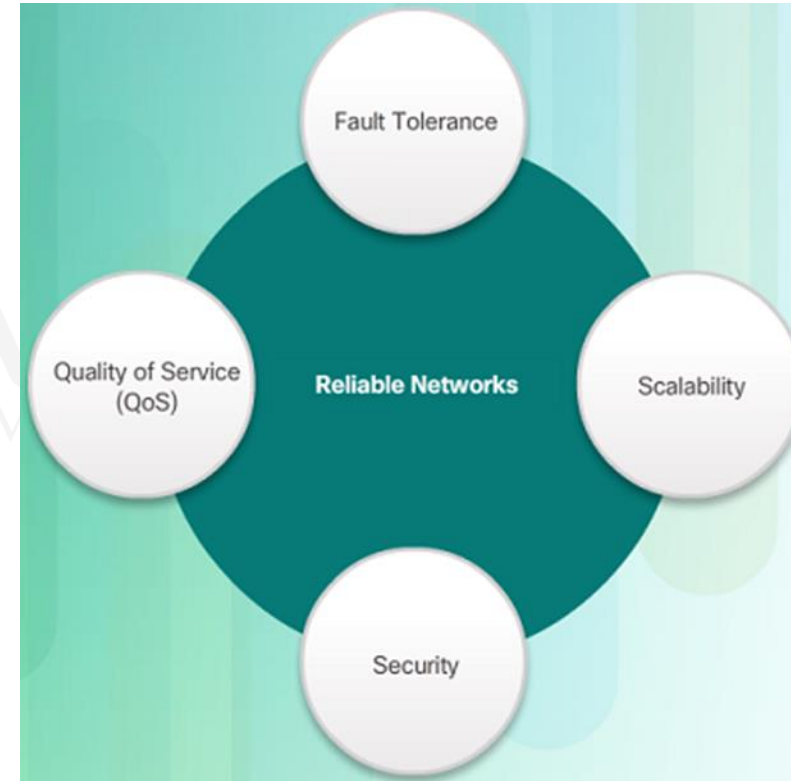
# Network Architecture

- Network Architecture is the **design of a computer network**
- Includes **hardware, software and connectivity**.
- Refers to the **technologies that support** the infrastructure that moves the data across the network
  - Network infrastructure to all the resources of a network that makes the network
- Responsible for **Standards and Frameworks** that can address various network types and solve problems to improve reliability

Ref: Cisco Netacad CCNA Introduction to Networks

# Reliable Networks

- User expect any designed network to be reliable in operation
- Reliability = continuity of service
- Four characteristic of any reliable network architectures are
  - ❖ Fault Tolerance
  - ❖ Scalability
  - ❖ Quality of Service (QoS)
  - ❖ Security

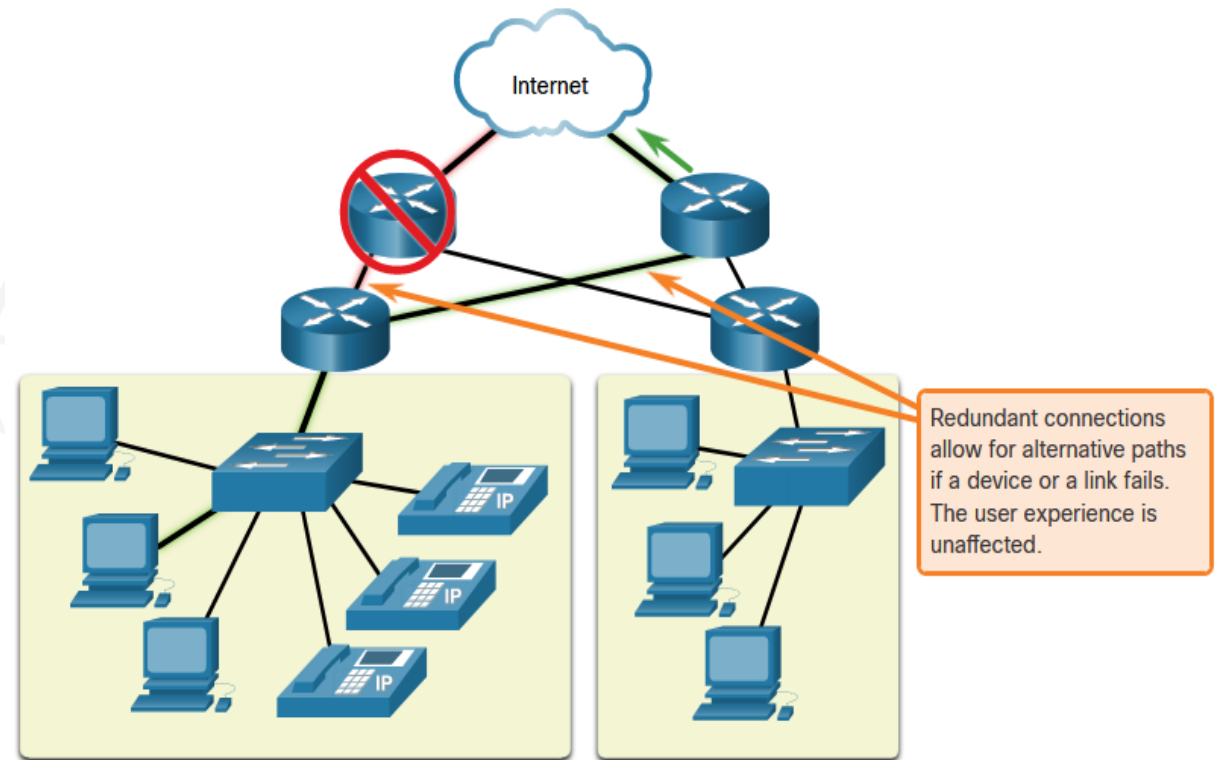


Ref: Cisco Netacad CCNA Introduction to Networks



# Fault tolerance

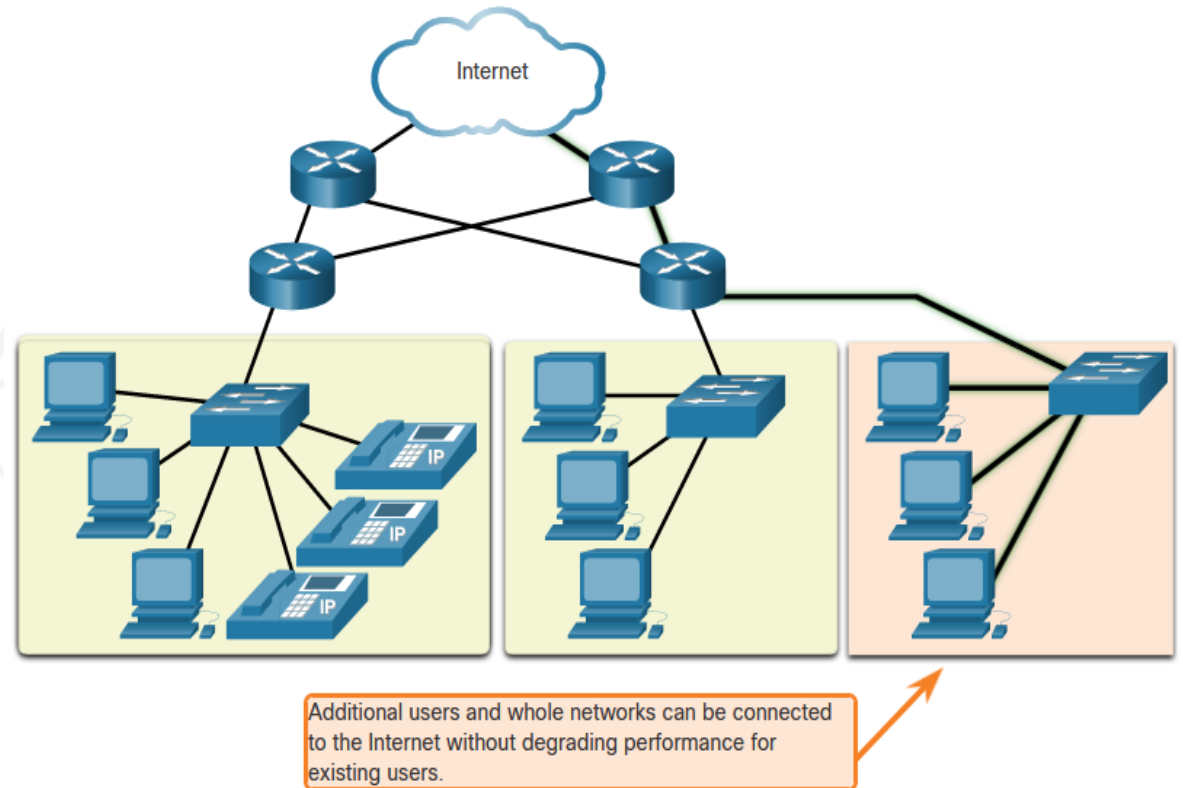
- Ability to provide continued operation in the presence of faults
- Problem: How to limit the impact of failure by limiting the number of affected devices?
- Solution: Introducing Redundancy



Ref: Cisco Netacad CCNA Introduction to Networks

# Scalability

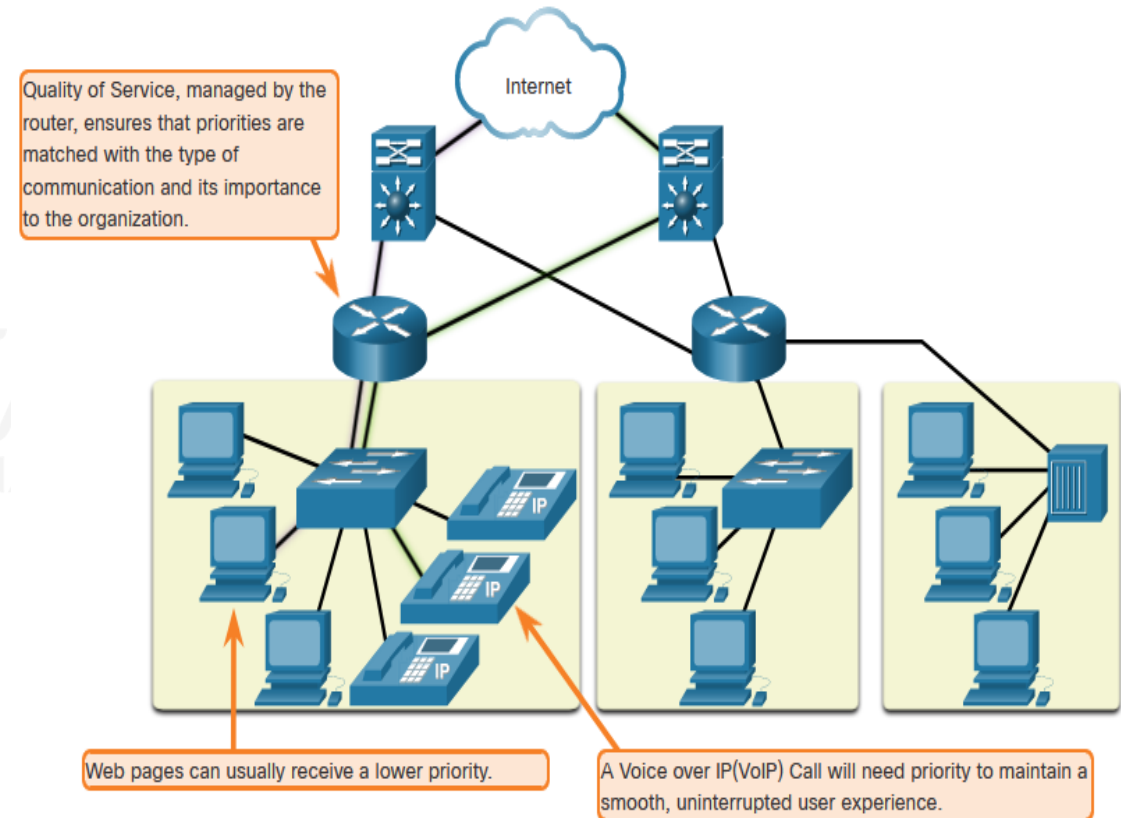
- **Problem:** How to expand the network or services without affecting the existing one?
- **Solution:** Hardware or software expansion
- **Additional** users and whole networks can be connected to the internet without degrading performance for existing users.



Ref: Cisco Netacad CCNA Introduction to Networks

# Quality of Service(QoS)

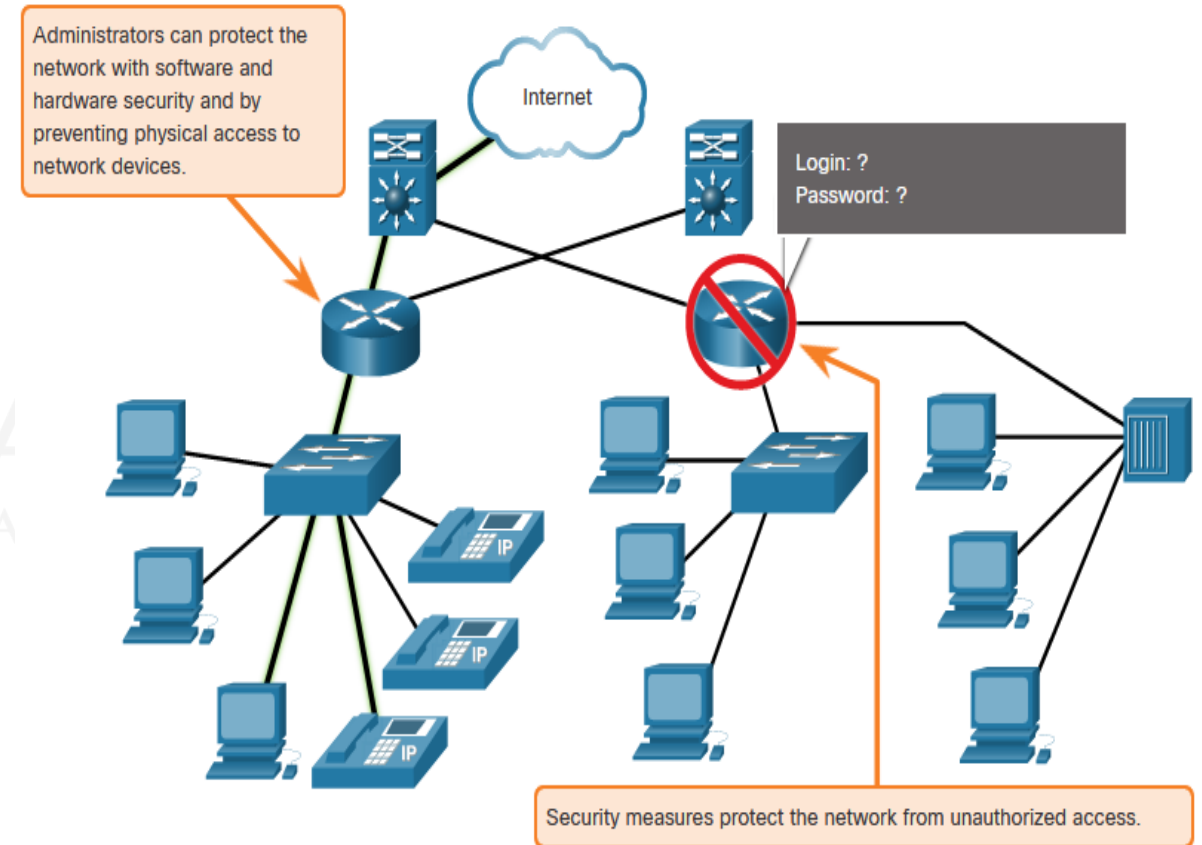
- **Problem:** Watching live video with constant breaks do not meet the user needs
- **Solution:** QoS is the primary mechanism used to ensure reliable delivery for all users
- With **QoS policy**, routers give **priority** to voice traffic packets compared to data traffic packets



Ref: Cisco Netacad CCNA Introduction to Networks

# Network Security

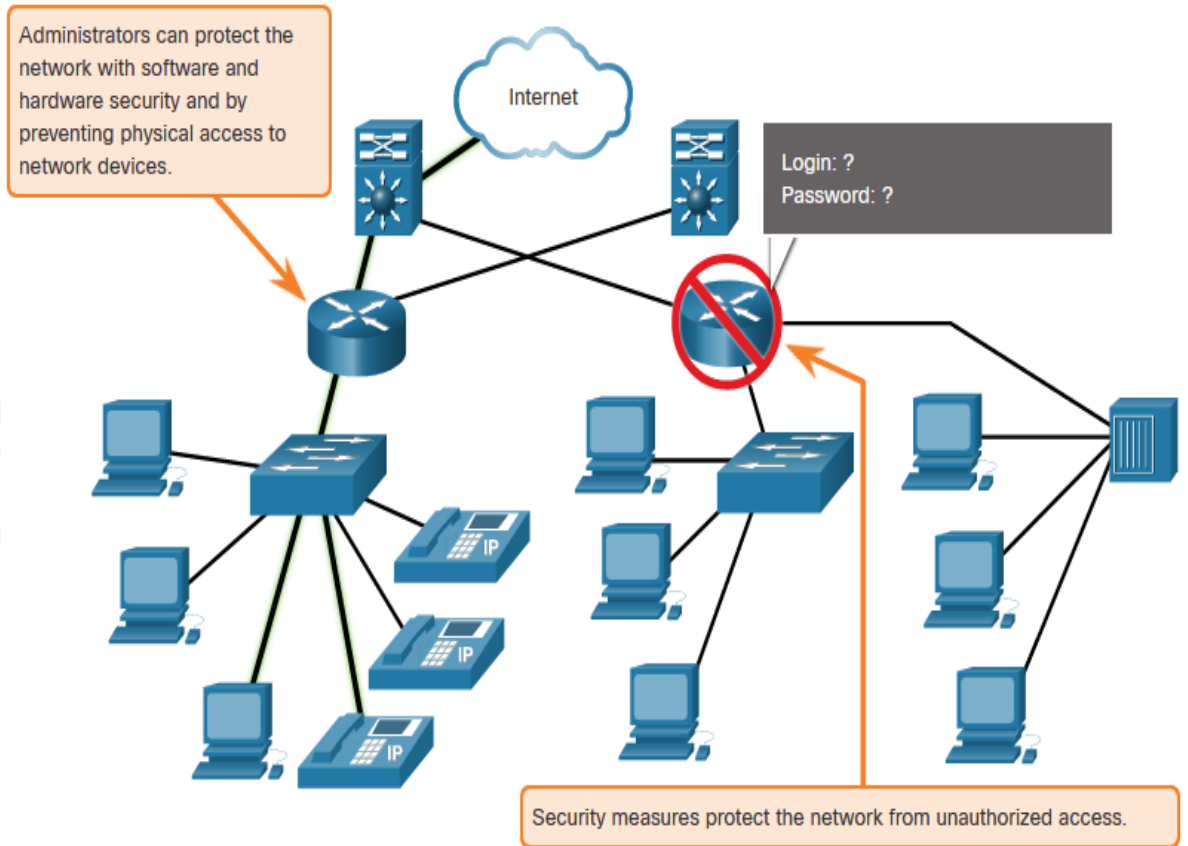
- Two main types of network security to be addressed
  - Network Infrastructure Security
    - Physical security of network devices
    - Preventing unauthorized access to the devices
  - Information Security
    - Protection of the information or data transmitted over the network



Ref: Cisco Netacad CCNA Introduction to Networks

# 3 Goals of Network Security

- **Confidentiality** – only intended users can access the data
- **Integrity** – assurance that the data has not altered with during transmission
- **Availability** – assurance of timely and reliable access to data for authorized users



Ref: Cisco Netacad CCNA Introduction to Networks



# Summary

- Network Trends
  - Online Collaboration
  - Cloud Computing
- Network Architecture
- Reliable Network Characteristics
  - Fault tolerance
  - Scalability
  - Quality of Service (QoS)
  - Network Security
- Next lecture discussion
  - Protocols



AMRITA  
VISHWA VIDYAPEETHAM | Online

# Network Protocols basics

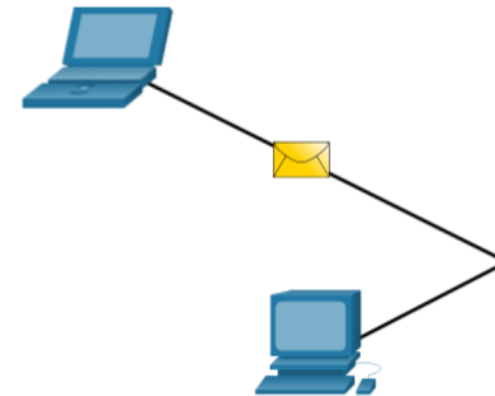


# Key points to discuss in Protocols

- Rules for Communication
- Network Protocols
- Protocol Suite
- Communication Process
  - Sender side
  - Receiver side

# Rules for Communication

- Set of rules needed for any communication to be effective
- Sender/Transmitter transmits signal from message source
- Receiver receives signal and becomes the message destination



Ref: Cisco Netacad CCNA Introduction to Networks

# Rules for Communication

## Human Protocols



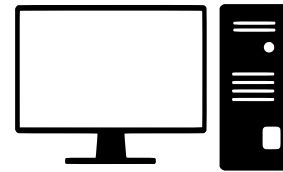
Namah Shivaya! Welcome to Networks course

Namaskar

Did you understand internet?

Yes. Network of Networks

## Network Protocols



TCP Connection Request

TCP Connection Response

HTTP Web page URL Request  
Ex: <http://amrita.edu>

HTTP Web page 200 Ok

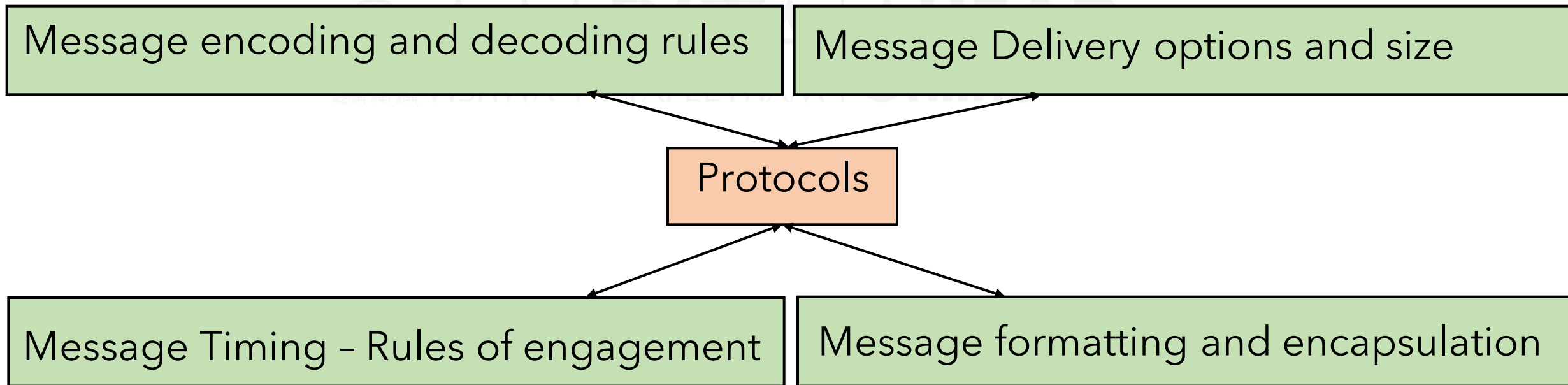
Time





# Network Protocol Requirements

- **Protocols** = set of rules
- Protocols should meet these requirements to send the message



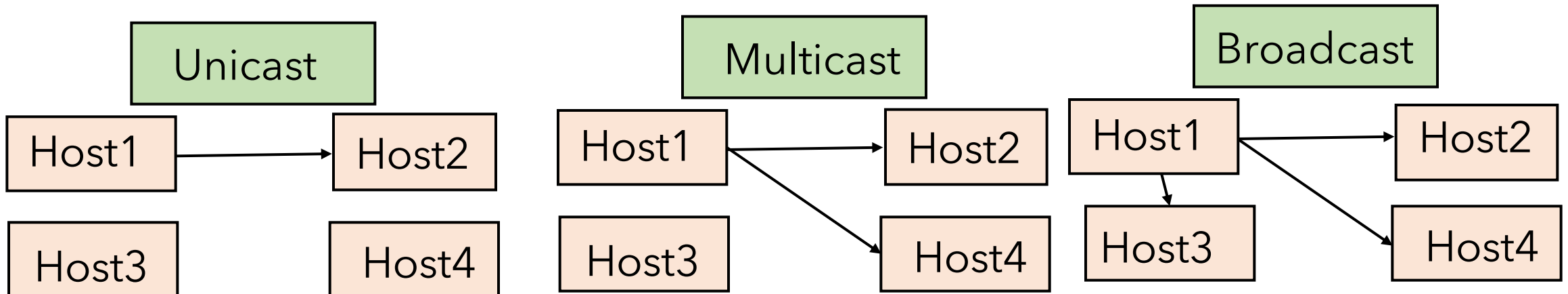
# Message Encoding

- **Encoding** is the process of converting information into another acceptable form for transmission.
  - **Sender** encodes the message source to signal to get transmitted in the Communication medium.
- **Decoding** reverses this process to interpret the information.
  - **Receiver** decodes the signal to the message



# Message Delivery Options & Size

- Different delivery options in the same network
  - **Unicast** : One Sender -> One Receiver
  - **Multicast** : One Sender -> Group of Receivers
  - **Broadcast**: One Sender -> All Receivers
- Message size restricted depending on Media/link capacity



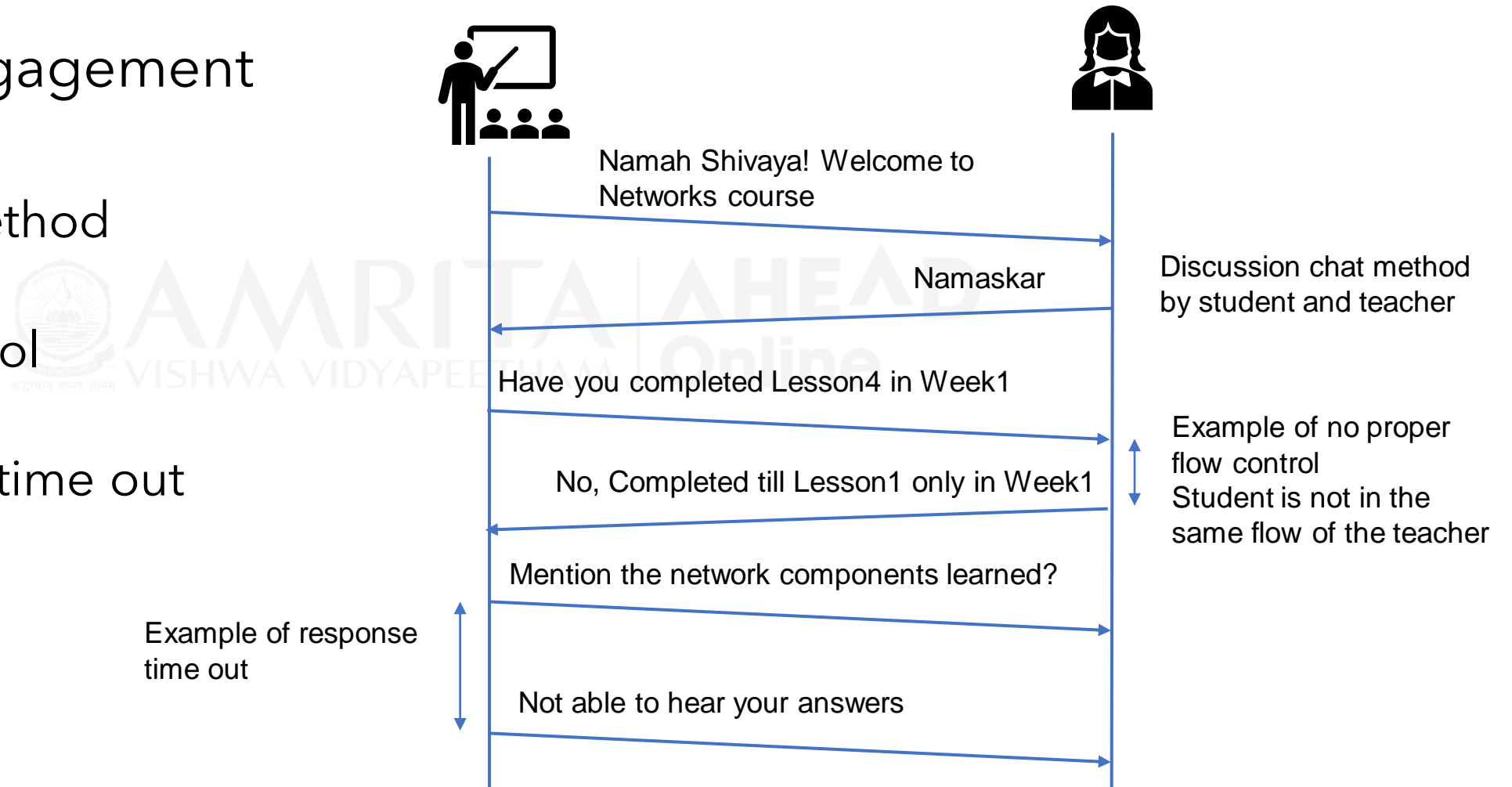
# Message Timing

- Rules of Engagement

- Access Method

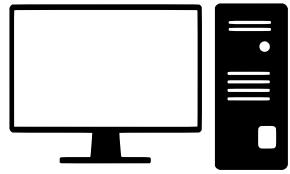
- Flow control

- Response time out



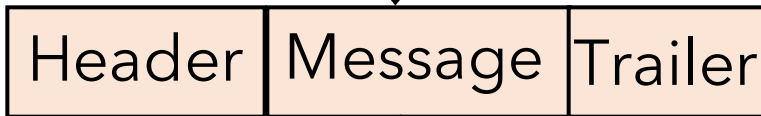
# Message Formatting & Encapsulation

- Body of the letter is encapsulated with the envelope cover having destination address



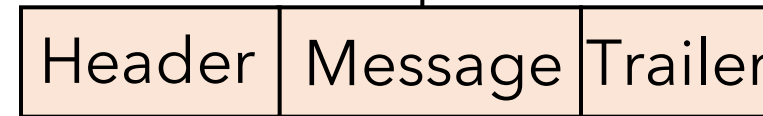
Message

Encapsulation



Message

De-Encapsulation



10001...00010..1111

Communication Medium



# Network Protocol Types

- Protocols can be implemented on devices in software, hardware or both

Protocol Types	Description	Example
Network Communications	Enable two or more devices to communicate over one or more network	HTTP, TCP, IP
Network Security	Secure data to provide authentication, data integrity and data encryption	TLS, SSH, SSL
Routing	Enable routers to exchange route information and thus helps to select best path for packets to move forward	OSPF, BGP
Service discovery	Used for automatic detection of devices or services	DNS, DHCP

# Network Protocol Functions

- Protocols have their own Format, Function and Rules

Protocol Function	Description	Example
Addressing	Identifies sender and receiver	IP, Ethernet
Reliability	Provides guaranteed delivery	TCP
Flow control	Ensures data flows at an efficient rate	TCP
Sequencing	Uniquely labels each transmitted segment of data	TCP
Error detection	Determines if data becomes corrupted during transmission	TCP, IP, Ethernet
Application interface	Process-to-process communication between network applications	HTTP, HTTPS

# Summary

- Rules of Communication
- Network Protocols
- Protocol Requirements
  - Message Encoding
  - Message delivery options and size
  - Message timing
  - Message formatting and encapsulation
- Next lecture discussion
  - Protocol suite



AMRITA  
VISHWA VIDYAPEETHAM | Online

# Protocol suite and Standards

Reference: CCNA ITN Ch3.1, 3.2 Protocol rules



# Key points in Protocol Suite & Internet Standards

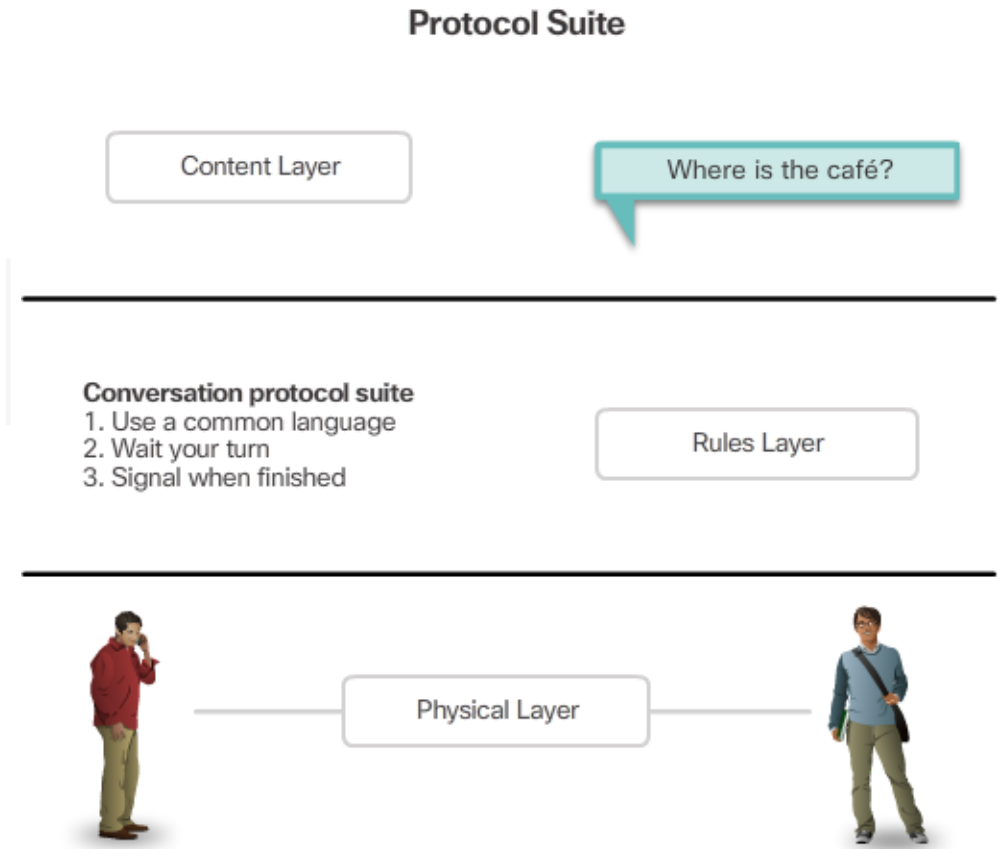
- What is **protocol suite**?
- Analyze **Evolution** of **Protocol suites**
  - Open
  - Proprietary
- Analyze **Internet Standards** and Organizations
  - IP Addressing
  - Communication protocols





# Protocol Suite

- Protocol suite?
  - Group of inter-related protocols necessary to perform a communication function
  - set of protocols that work together to solve a problem
- Protocols are viewed in terms of layers
  - @Sender: Content Layer -> Rules Layer -> Physical Layer
  - @Receiver: Physical Layer -> Rules Layer -> Content Layer



Ref: CCNA Introduction to Networks from Cisco Netacad

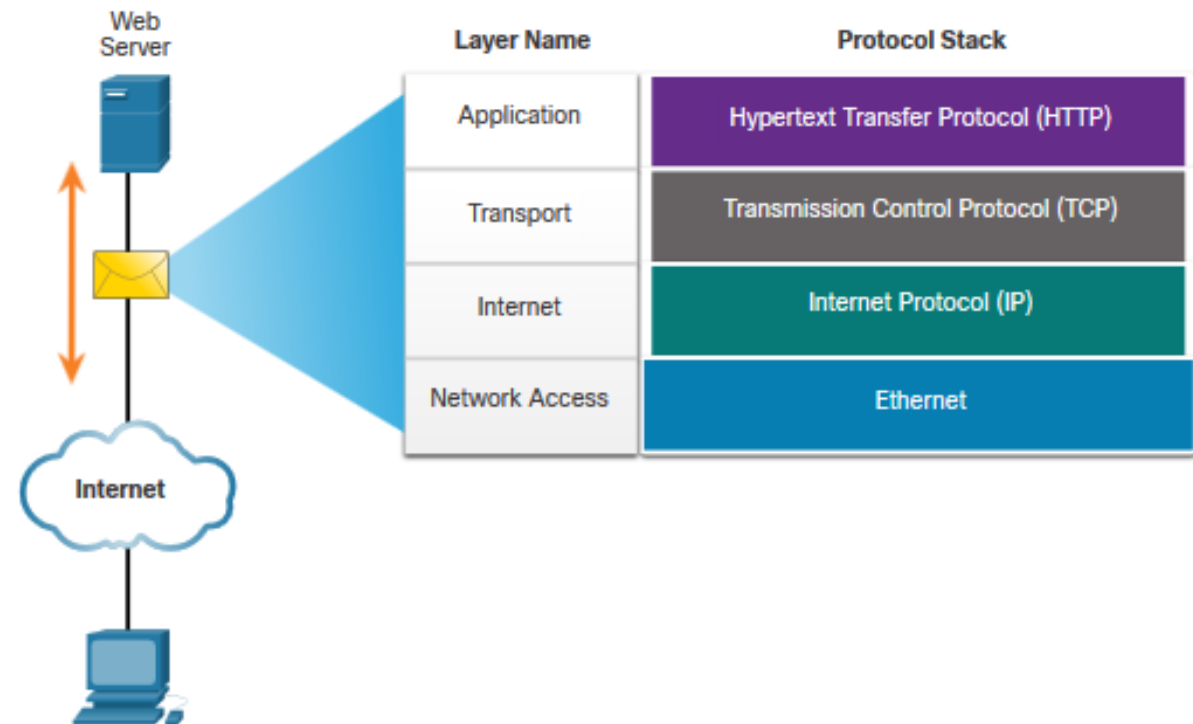
# Evolution of Protocol Suites

- Several **competing protocol suites** providing comprehensive network communication services
- Open Standards
  - TCP/IP
  - OSI
- Proprietary
  - AppleTalk
  - Novell Netware

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			

# TCP/IP Protocol example

- Interaction of protocols in communication between a web server and web client uses **TCP/IP protocol suite**.
- **TCP/IP protocol suite** is used in the internet and an open standard maintained by Internet Engineering Task Force (IETF)
  - Standards based protocol suite endorsed by networking industry and approved by standards organizations



Ref: CCNA Introduction to Networks from Cisco Netacad

# Open Standards

- Open standards encourage:
  - Interoperability
  - Competition
  - Innovation
- Standards organizations are
  - Vendor neutral
  - Non profit organizations
  - Established to develop and promote the concept of open standards



Ref: CCNA Introduction to Networks from Cisco Netacad

# Network protocols -> Layered Models

- **Network protocols** is Set of rules defined in the software process for
  - How are messages formatted or structured?
  - How and when error and system messages are passed between devices?
  - Setup and termination of data transfer session
- Networks are complex with many components. Organizing network structure better is possible by **Layered models**

Ref: J. Kurose and K. Ross 2012, Computer Network, 6th ed.

# Summary

- Protocol Suite and concept of layers
- Different Protocol suites evolution
  - Open - TCP/IP, OSI
  - Proprietary - Apple, Novel
- Internet Standards
  - IETF, IANA etc
- Next lecture discussion
  - Layered Models

AMRITA | AHEAD  
VISHWA VIDYAPEETHAM | Online



AMRITA  
VISHWA VIDYAPEETHAM | Online

# Layered Models

Reference: CCNA ITN Ch3.5 Layered models





# Key points to discuss in Layered Models

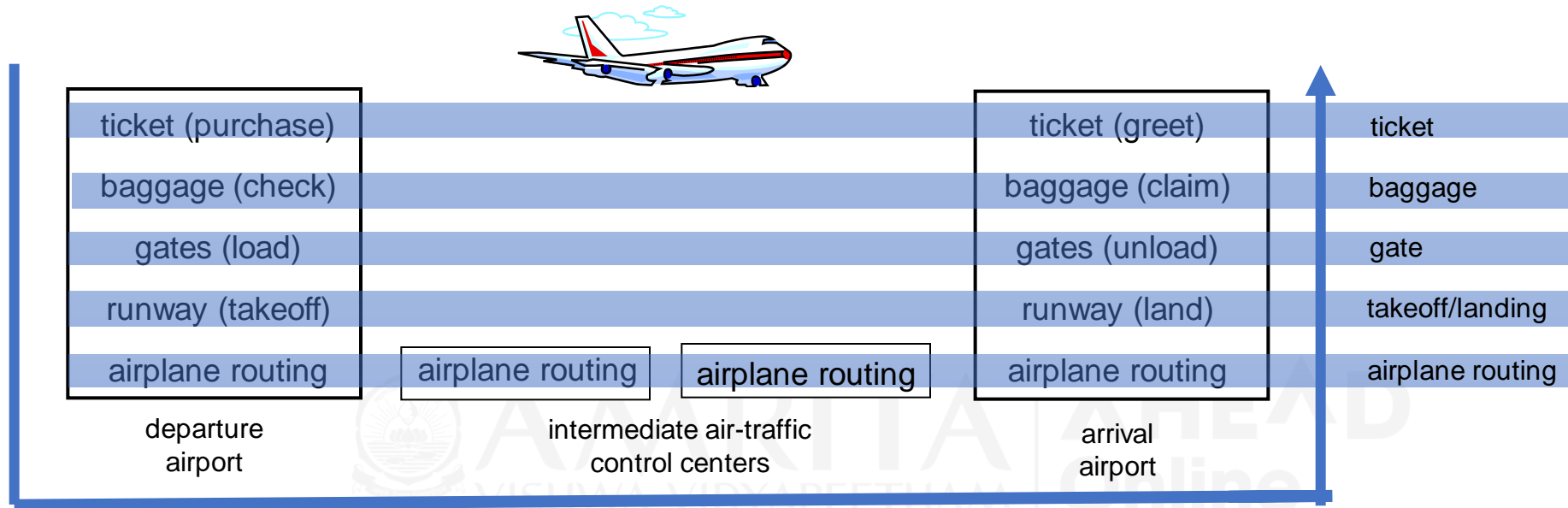
- Why Layering?
- What is layered approach?
- Benefits of Layered models
- Protocol model
  - TCP/IP Implemented Model
  - OSI Reference Model
- Protocol stack in sending and receiving a message

# Protocol “Layers”

- Networks are complex with many hardware and software components
  - End Devices – Laptop, Mobile etc.
  - Intermediary Devices – Switch, routers etc.
  - Media – Wired: Copper, Fiber etc. Wireless: Radio, microwave
  - Applications – provides human interface
  - Protocols – set of rules for network communication
  - Services – follow protocols to prepare data for the network
- Protocol “layers” helps in organizing the structure of the complex systems like network.

Ref: CCNA Introduction to Networks from Cisco Netacad

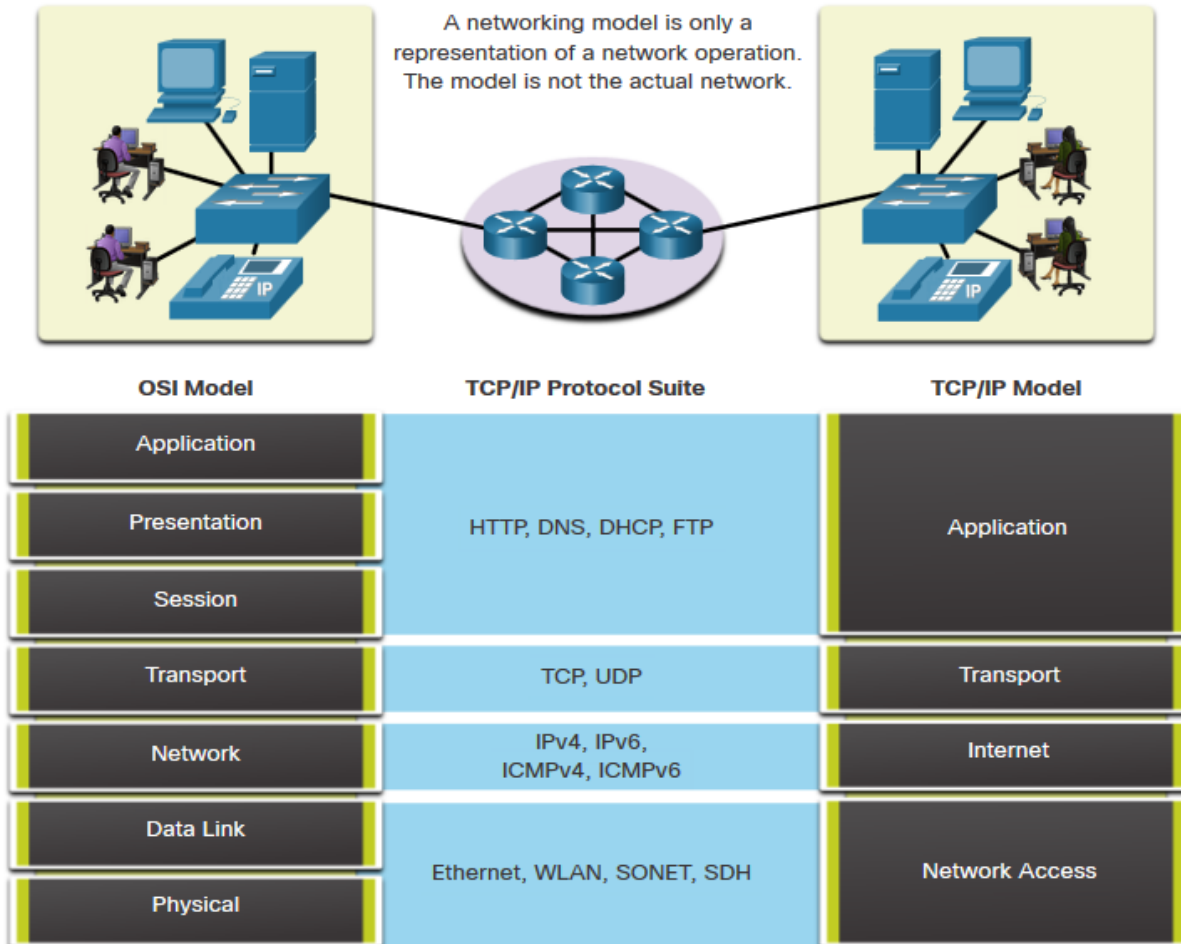
# Layered approach analogy



- Analogy – Organization of air travel – series of steps
- Layers: each layer implements a service
  - Via its own internal-layer actions (Ex: at the gate layer, loading & unloading)
  - Relying on services provided by layer below (Ex: in the gate layer, using the takeoff/landing service)

Ref: J. Kurose and K. Ross 2012, Computer Network, 6th ed.

# Why Layered Model ?



- Used to easily explain/understand complex concepts such as how network operates (or how airline system works)
- TCP/IP and OSI models describe network operation
- Modularization eases maintenance, updating of system
  - Ex: change in services of one layer doesn't affect other layers

Ref: CCNA Introduction to Networks from Cisco Netacad

# Benefits of using a layering 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

Ref: CCNA Introduction to Networks from Cisco Netacad

# Protocol stack

- Network designers organize protocols in layers
  - Each protocol belongs to one of the layers
- Each layer provides its services by
  - Performing actions specific to the layer
  - Use the services of the layer directly below it. Ex: HTTP uses the TCP service
- Layer N protocol distributed among the end system, switches and other network components
  - Each component performs layer N services. Ex: Router = Layer 3
- When taken together, the protocols of various layers are called protocol stack

Ref: CCNA Introduction to Networks from Cisco Netacad

# Internet Protocol stack = TCP/IP model

5. Application	Support network applications like web, email	HTTP, SMTP
4. Transport	Process-to-process data transfer	TCP, UDP
3. Network	Routing packets to destination	IP, OSPF etc.
2. Data Link	Data transfer between neighbouring devices	HDLC, PPP
1. Physical	Bits as signals on the wire	Ethernet

Ref: CCNA Introduction to Networks from Cisco Netacad



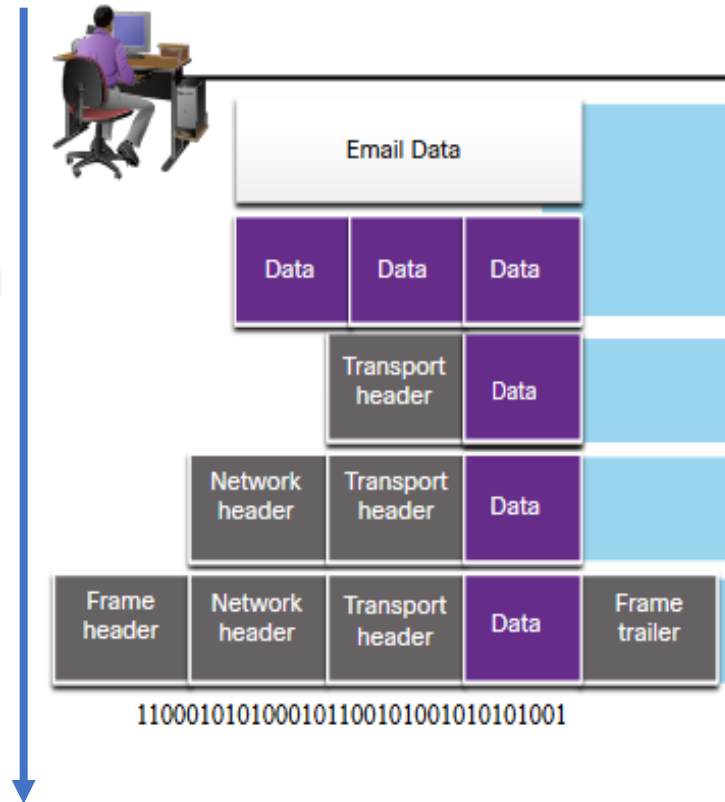
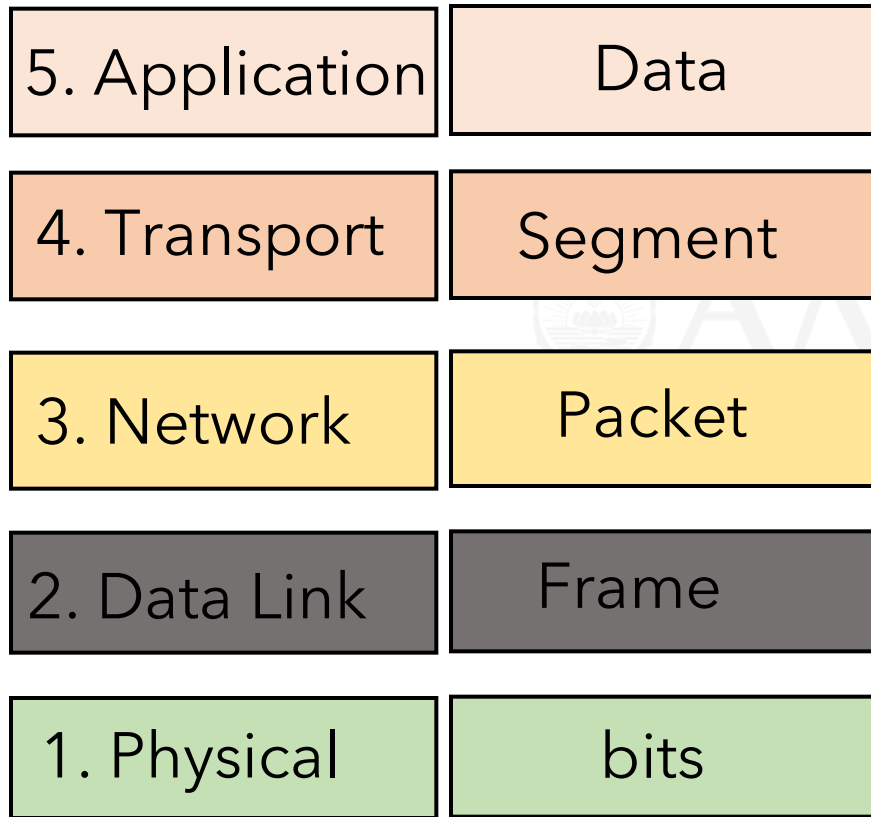
# OSI Reference Model

7. Application	Support network applications like web, email
6. Presentation	Provides for common representation of the data
5. Session	Managed data exchange sessions
4. Transport	Process-to-process data transfer
3. Network	Determine the best path through the network
2. Data Link	Data transfer between neighbouring devices
1. Physical	Bits as signals on the communication medium

Ref: CCNA Introduction to Networks from Cisco Netacad

# Internet Protocol stack = TCP/IP model

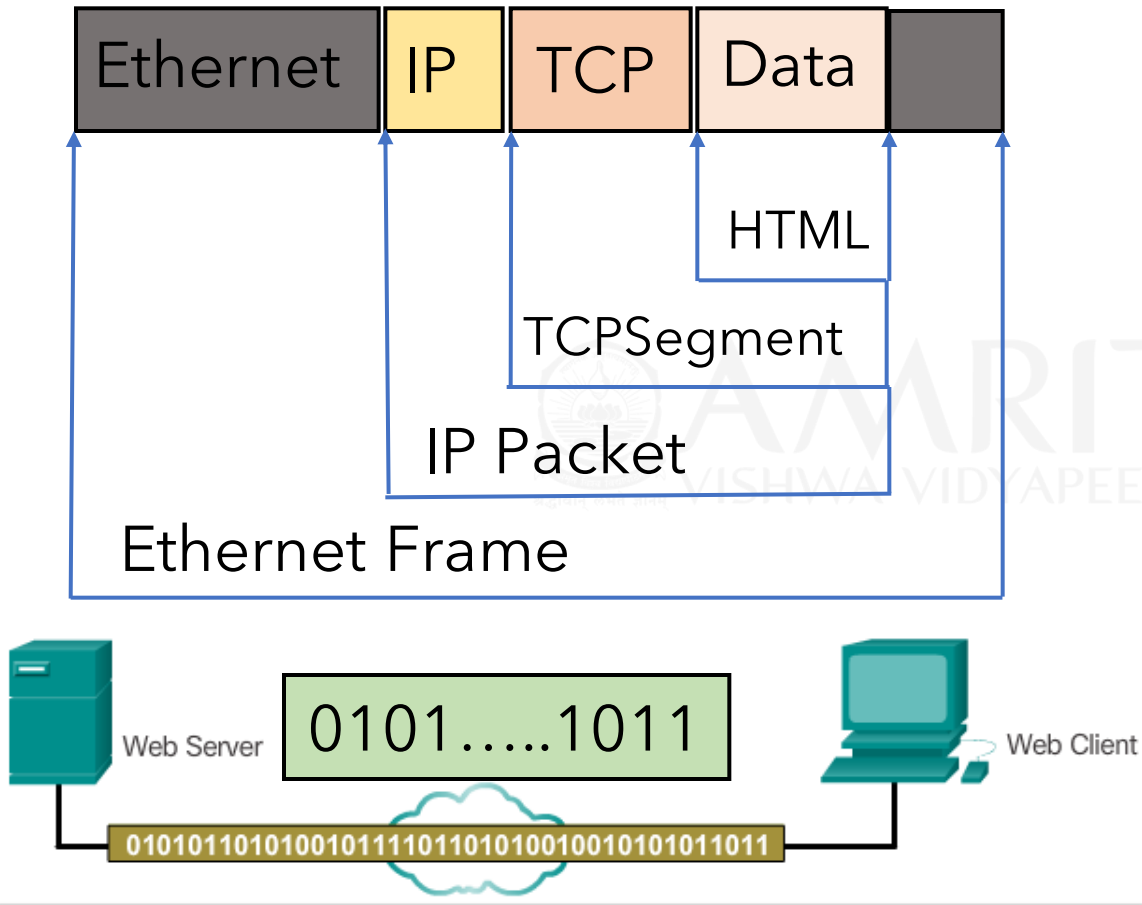
Pushing down the stack



- **Encapsulation** = process where protocols add their information to the data.
- At each layer, a **protocol data unit** has a different name to reflect its new functions.

Ref: CCNA Introduction to Networks from Cisco Netacad

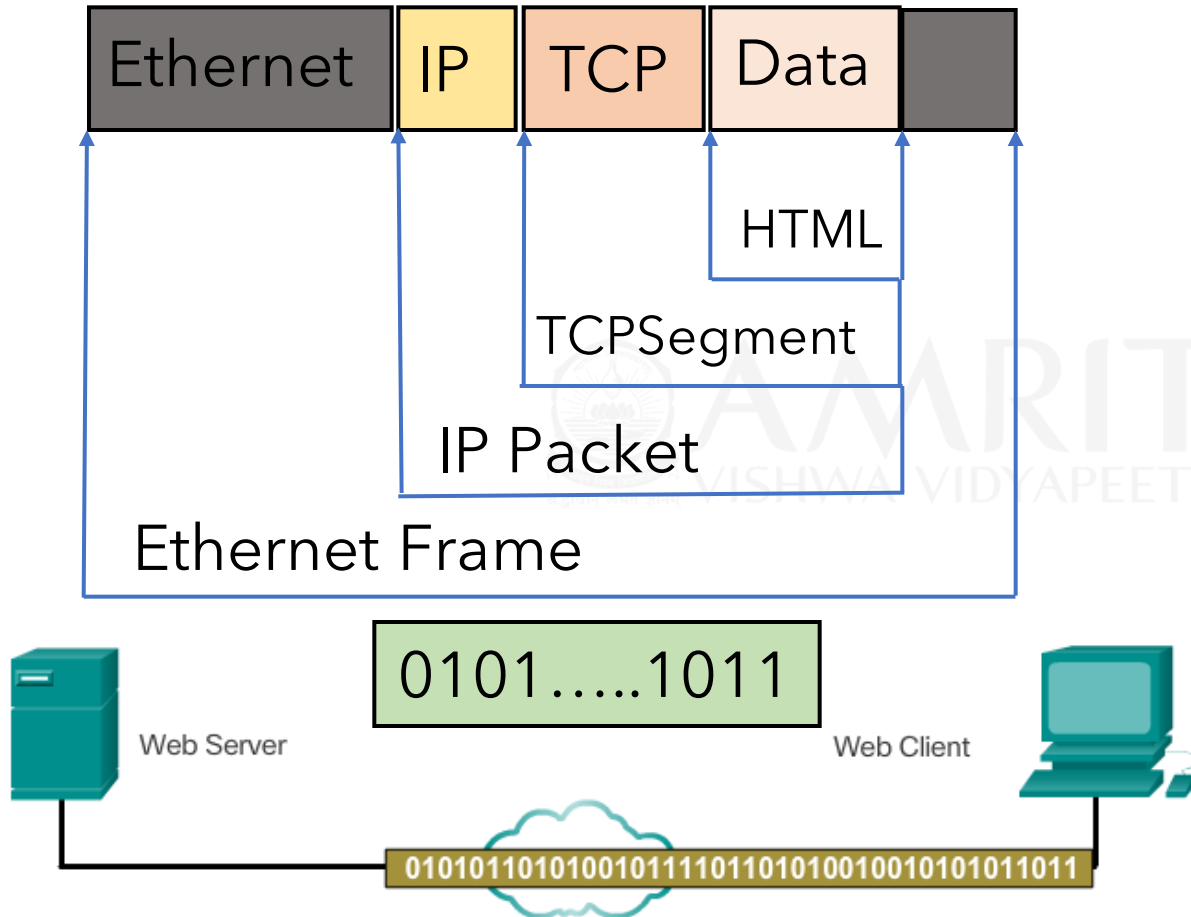
# Sending message - Internet protocol stack



Ref: CCNA Introduction to Networks from Cisco Netacad

- Data are pushed down in protocol stack in sending a message in **TCP/IP Communication process**
- **Encapsulation** is adding control or header information along with the User data
- Encapsulation takes place in the **sender side**
- Ex: Web server sending web page (HTML)

# Protocols in Receiving a message



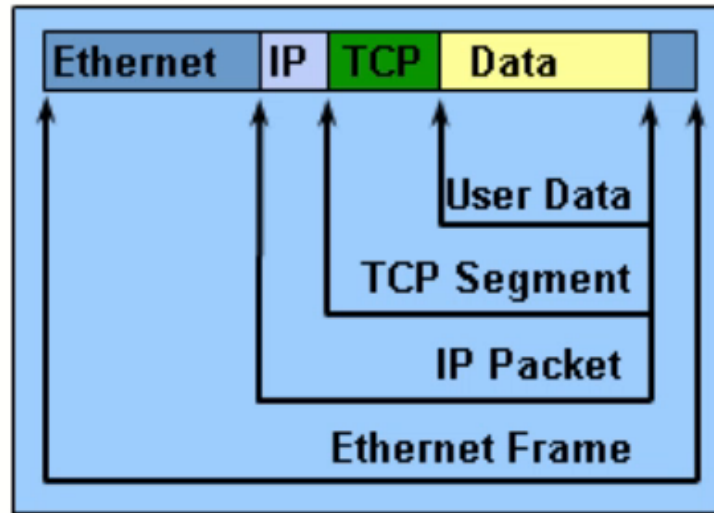
Ref: CCNA Introduction to Networks from Cisco Netacad

- Data is popped out from protocol stack in Receiving a Message in **TCP/IP Communication process**
- **De-Encapsulation** is removing control or header information from the User data
- De-Encapsulation takes place in the **receiver side**
- Ex: Web Client receiving web page from web server

# Protocol Operation

## Protocol Operation of Sending and Receiving a Message

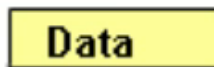
### Protocol Encapsulation Terms



Web  
server



Data



Web  
Client

# Summary

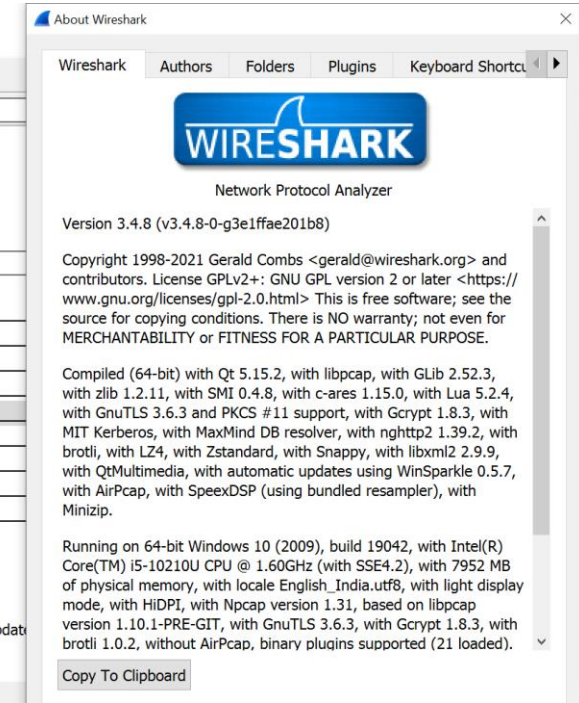
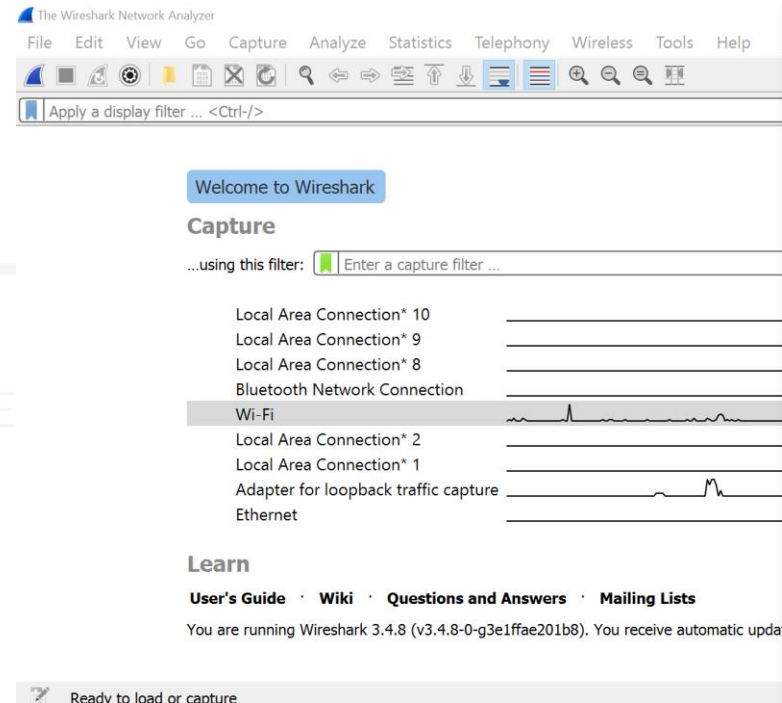
- Need for Layered approach
- Protocol models
  - TCP/IP
  - OSI
- TCP/IP Communication process
  - Encapsulation @ sender
  - De-encapsulation @ Receiver
- Next lecture discussion
  - Practical session - Wireshark

# Objectives – Protocol Analyzer Tool

- Understanding Protocol analyzer tool
- Explore the logical and physical address in laptop for internet access
- Install & launch Wireshark in the laptop having internet access
- Explore the basic Wireshark features

# Protocol analyzer tool?

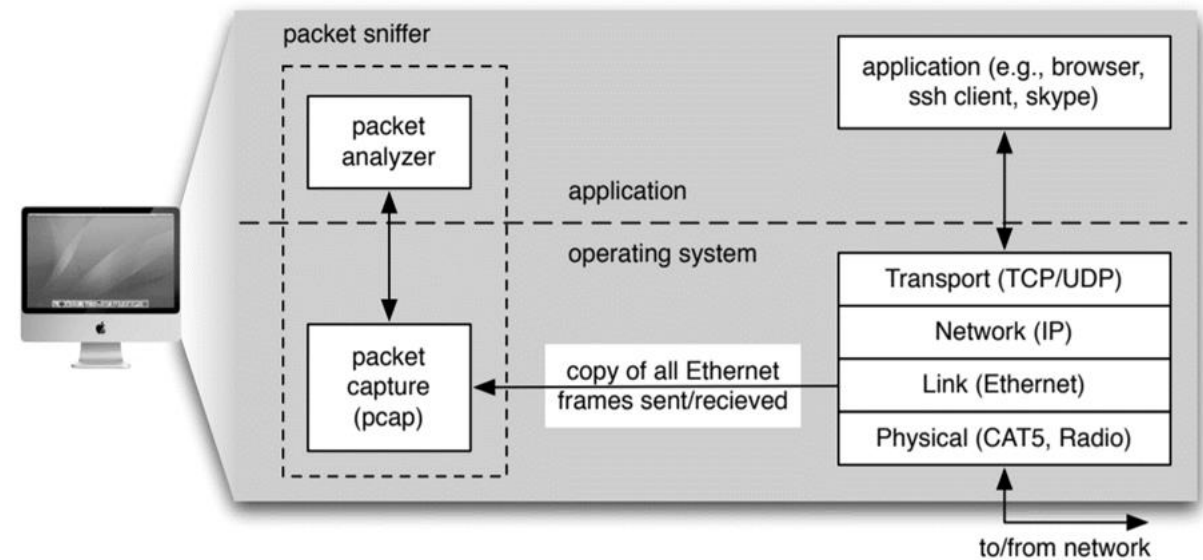
- **Wireshark tool** used for network troubleshooting, protocol analysis, decode and analyze protocol data unit in each layers
- **Open-source packet sniffer software** used by network engineers
- It can **capture** incoming frames and outgoing frames **from an interface**.  
Ex: Wi-Fi





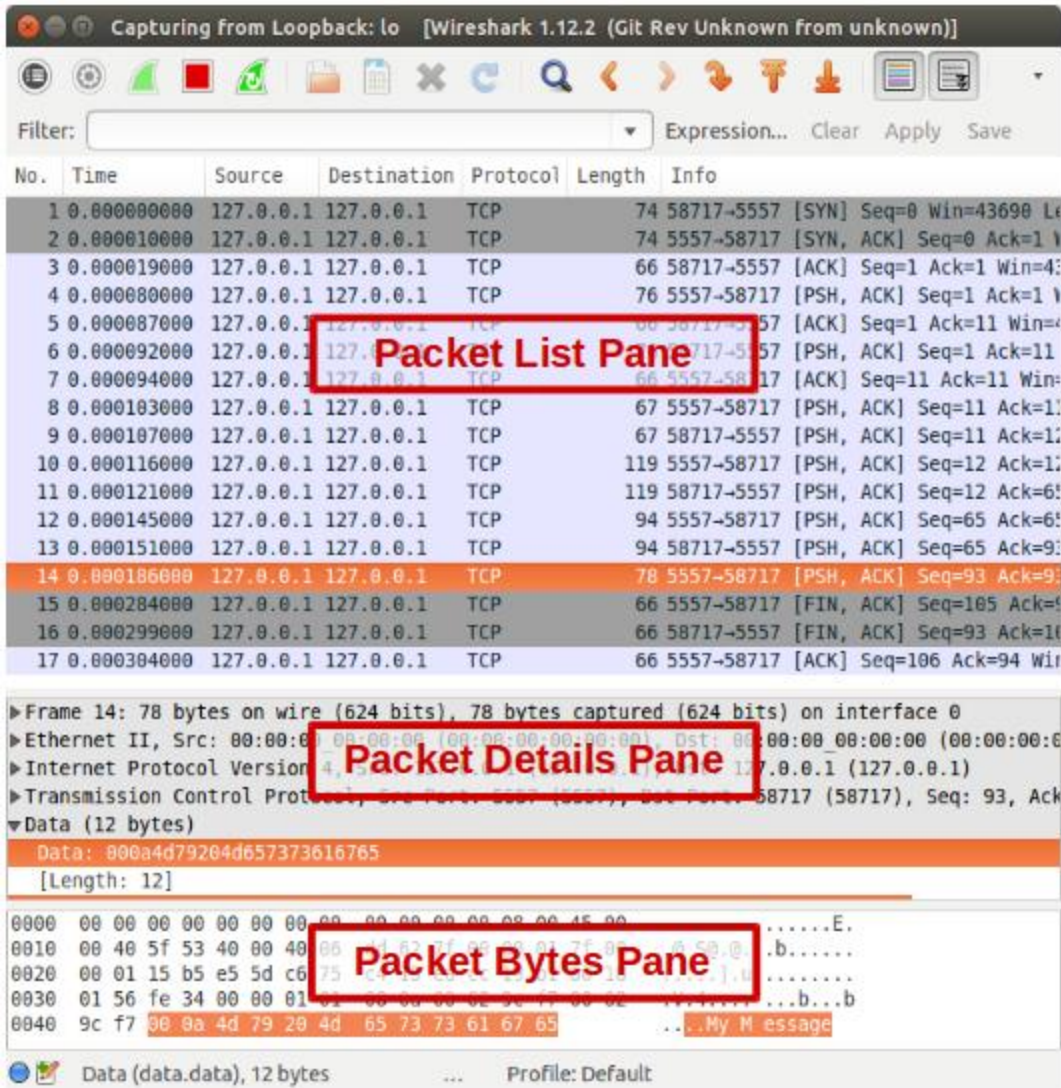
# Packet Sniffer tool?

- **Packet Sniffers tool** are used to observe the messages on the network
- Packet sniffer **captures ("sniffs") messages** being sent/received from/by our laptop
- **Packet capture** library receives copy of frame sent from or received by your laptop
- **Packet analyzer** displays the content of all fields within a protocol message



Ref: J. Kurose and K. Ross 2012, Computer Network, 6th ed.

# View Protocol Data Units in Wireshark



- **Wireshark** is programmed to recognize the structure of different network protocols.
- This enables to **display the encapsulation** and individual fields of a Protocol Data Unit (PDU) to help in interpretation.
- Useful tool for those working with networks and can be used for **data analysis and troubleshooting**.

[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

# Examine Logical IPv4 Address

- Analyze the end-device connectivity to the network in our laptop/PC is required to troubleshoot issues in the internet access
- How to gather TCP/IP configuration of an end device?
  - Use the start menu and go the command prompt
    - Type **ipconfig** and press the **Enter** key.
    - Note: **ifconfig** is the command in **Ubuntu machine**
    - It is short for IP Configuration.
- **ipconfig** command provides IP address, subnet mask and default gateway.
- The **IP address and the default gateway should be in the same network** or subnet, otherwise this host would not be able to communicate outside the network

```
C:\Windows\system32\cmd.exe

C:\Users\amrita>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : am.amrita.edu

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : am.amrita.edu
    Link-local IPv6 Address . . . . . : fe80::f83b:35a7:75bb:4752%16
    IPv4 Address. . . . . : 10.110.25.25
    Subnet Mask . . . . . : 255.255.128.0
    Default Gateway . . . . . : 10.110.0.1

Ethernet adapter Bluetooth Network Connection:
```

# Physical MAC Address

```
C:\Windows\system32\cmd.exe

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : am.amrita.edu
    Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
    Physical Address. . . . . : 6C-94-66-63-E0-C5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f83b:35a7:75bb:4752%16(Preferred)
    IPv4 Address. . . . . : 10.110.25.25(Preferred)
    Subnet Mask . . . . . : 255.255.128.0
    Lease Obtained. . . . . : 27 September 2021 18:52:05
    Lease Expires . . . . . : 01 October 2021 15:53:55
    Default Gateway . . . . . : 10.110.0.1
    DHCP Server . . . . . : 192.168.0.251
    DHCPv6 IAID . . . . . : 275551334
    DHCPv6 Client DUID. . . . . : 00-01-00-01-28-BF-9A-19-C0-25-A5-77-56-17
    DNS Servers . . . . . : 192.168.0.250
                           192.168.0.251
    NetBIOS over Tcpi. . . . . : Enabled

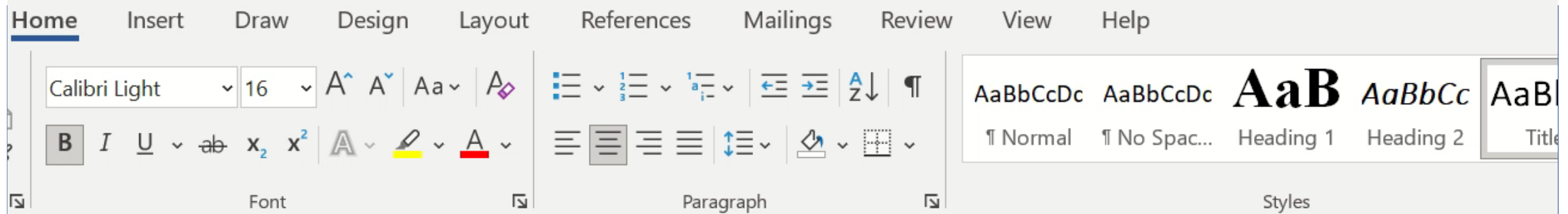
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address. . . . . : 6C-94-66-63-E0-C9
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

C:\Users\amrita>ipconfig /all
```

- **ipconfig /all** command is used to know the physical address
- **Medium Access Control(MAC)** address or Physical address refers the same
- **Wireless NIC card** MAC address is involved in communication if internet access it through Wi-Fi.
- **Ethernet NIC card** MAC address is involved in communication for accessing internet via wired LAN.





## Analyzing the End Device connectivity to the Network

### Part1: Gather basic TCP/IP configuration information

Use the Start menu to open the Command Prompt, an MS-DOS-like window. Press **Start Programs > Accessories > Command Prompt** or **Start > Programs > Command Prompt**.

The following figure shows the Command screen.

```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

# Instructions to install Wireshark

- **Step1: Download Wireshark**
  - Based on your PC, choose 32 bit or 64 bit OS Windows installer
- **Step2: Install Wireshark**
  - Downloaded file is named **Wireshark-win64-x.x.x.exe**, where x represents version number
  - To capture live network data, same x version of **Ncap is required.**
  - Recommended to uninstall old and update it with version of Ncap x.x.x same as wireshark done by clicking next to continue.
  - USBPcap is experimental, and it would cause USB problems on your laptop. So, **do not select the checkbox to install USBPcap.**
  - Click **Next** and **Finish** to complete the installation process.

Ref: CCNA Introduction to Networks from Cisco Netacad

# Launch Wireshark

- Search for **Wireshark** application
- Look for the list of **network** interfaces in the lower part of Wireshark. Choose your **active interface**. Double click on the active interface.
- Open your browser, e.g. Microsoft Edge and **pick a URL & fetch** it e.g. <http://www.bettertechnology.in>". Stop capturing as soon as the page is displayed
- Close unnecessary browser tabs and windows. By **minimizing browser activity**, we can stop computer from fetching unnecessary web content.
- Ensure that **browser cache is deleted**, so that web pages comes from web server

AutoSave Off Wireshark explore -... Search Dhivvy J P

File Home Insert Draw Design Layout References Mailings Review View Help

Paste Times New Roma 12 A A Aa A AaBbCcDc AaBbCcDc AaBbCc AaBbCc AaBbCc 1 Normal 1 No Spac... Heading 1 Heading 2 Title

Clipboard Font Paragraph Styles Editing Voice Editor Reuse Files

I

**Understanding the TCP/IP protocol stack using Wireshark**

1. Open Packet sniffer [Wirehark] Application and Capture the Wi-Fi/Ethernet Interface
2. Do this activity and capture frames.
  - a. Request for a web page from webserver
3. Briefly explain the Encapsulation process in at least one http request frame of the protocol analyzed. Also explain the PDU contents in each layer.

Layer	Protocol	Important Contents	Purpose
Application	http	GET Request for a <i>given URL</i>	

Page 6 of 6 726 words English (United States)

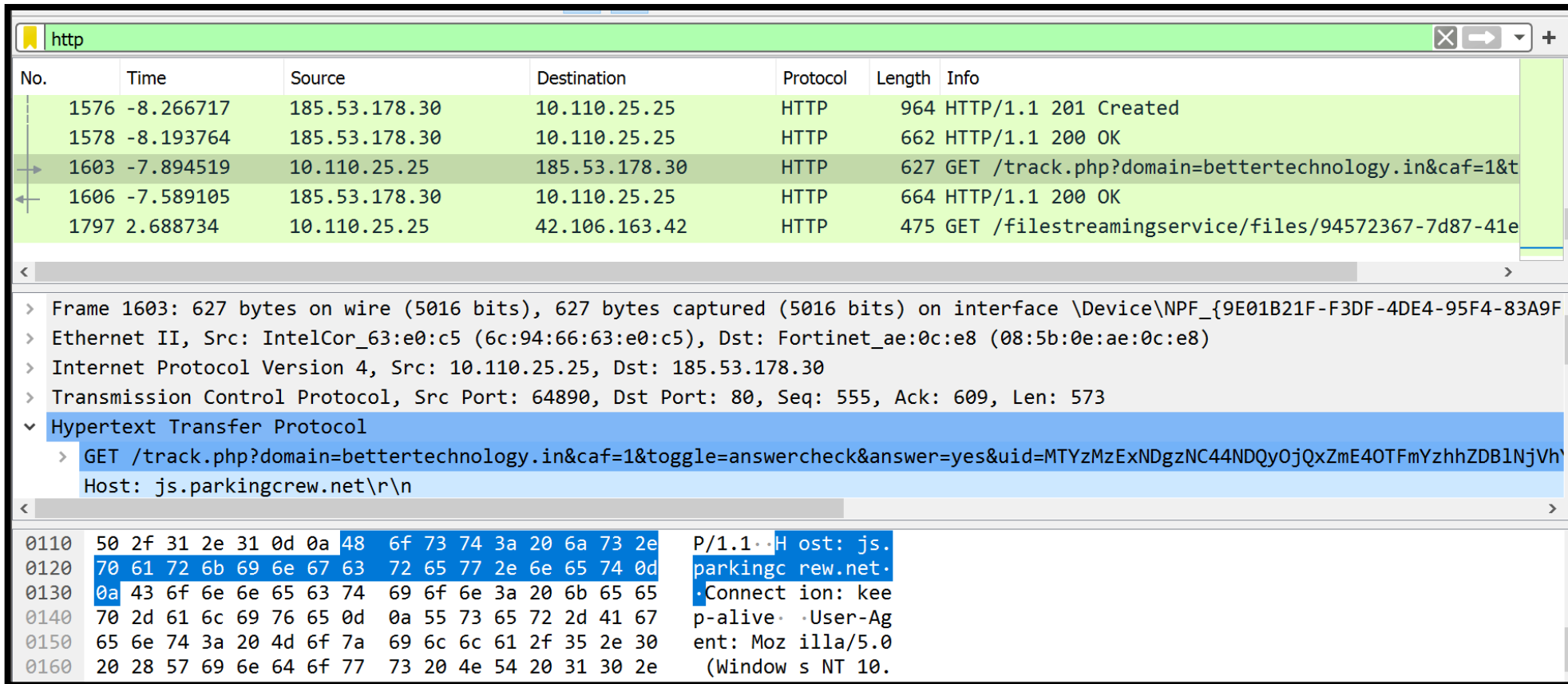
Focus 100%

Type here to search 27°C 12:29 AM 02-10-2021



# Encapsulation in requesting a web page

- **Application Layer** – host address (js.parkingcrew.net)
- **Host server** having the web page with URL bettertechnology.in



The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets, with packet 1603 selected. The middle pane shows the details of packet 1603, highlighting the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1576	-8.266717	185.53.178.30	10.110.25.25	HTTP	964	HTTP/1.1 201 Created
1578	-8.193764	185.53.178.30	10.110.25.25	HTTP	662	HTTP/1.1 200 OK
1603	-7.894519	10.110.25.25	185.53.178.30	HTTP	627	GET /track.php?domain=bettertechnology.in&caf=1&t
1606	-7.589105	185.53.178.30	10.110.25.25	HTTP	664	HTTP/1.1 200 OK
1797	2.688734	10.110.25.25	42.106.163.42	HTTP	475	GET /filestreamingservice/files/94572367-7d87-41e

Frame 1603: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF\_{9E01B21F-F3DF-4DE4-95F4-83A9F}

Ethernet II, Src: IntelCor\_63:e0:c5 (6c:94:66:63:e0:c5), Dst: Fortinet\_ae:0c:e8 (08:5b:0e:ae:0c:e8)

Internet Protocol Version 4, Src: 10.110.25.25, Dst: 185.53.178.30

Transmission Control Protocol, Src Port: 64890, Dst Port: 80, Seq: 555, Ack: 609, Len: 573

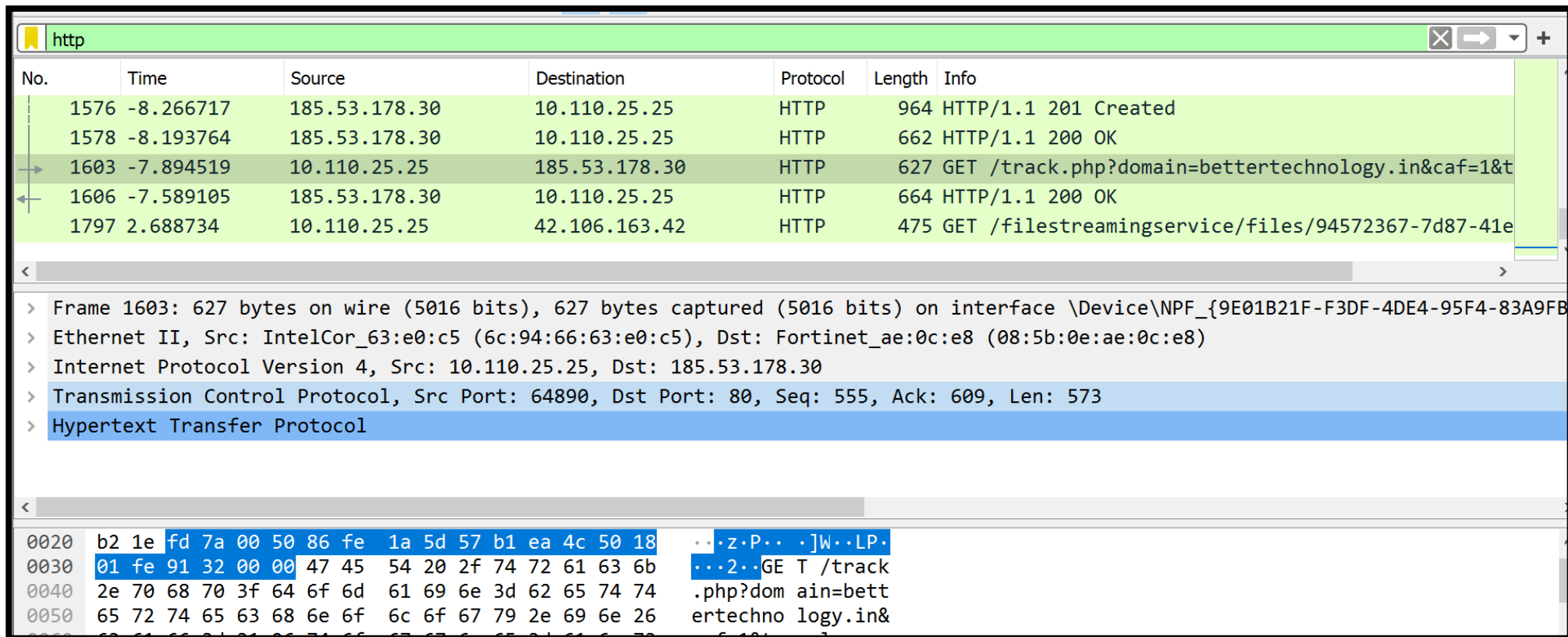
Hypertext Transfer Protocol

GET /track.php?domain=bettertechnology.in&caf=1&toggle=answercheck&answer=yes&uid=MTYzMzExNDgzNC44NDQyOjQxZmE4OTFmYzhkZDBlNjVh Host: js.parkingcrew.net\r\n

0110 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6a 73 2e P/1.1..H ost: js.  
0120 70 61 72 6b 6e 67 63 72 65 77 2e 6e 65 74 0d parkingc rew.net.  
0130 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 .Connect ion: kee  
0140 70 2d 61 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 p-alive· ·User-Ag  
0150 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0  
0160 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e (Window s NT 10.

# Encapsulation in requesting a web page

- Transport Layer – Port address
- Source port (my laptop as client)– 64890
- Destination port (web server) - 80



The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 1603 is selected, showing an HTTP GET request from 10.110.25.25 to 185.53.178.30. The bottom pane shows the details of packet 1603, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1576	-8.266717	185.53.178.30	10.110.25.25	HTTP	964	HTTP/1.1 201 Created
1578	-8.193764	185.53.178.30	10.110.25.25	HTTP	662	HTTP/1.1 200 OK
1603	-7.894519	10.110.25.25	185.53.178.30	HTTP	627	GET /track.php?domain=bettertechnology.in&caf=1&t
1606	-7.589105	185.53.178.30	10.110.25.25	HTTP	664	HTTP/1.1 200 OK
1797	2.688734	10.110.25.25	42.106.163.42	HTTP	475	GET /filestreamingservice/files/94572367-7d87-41e

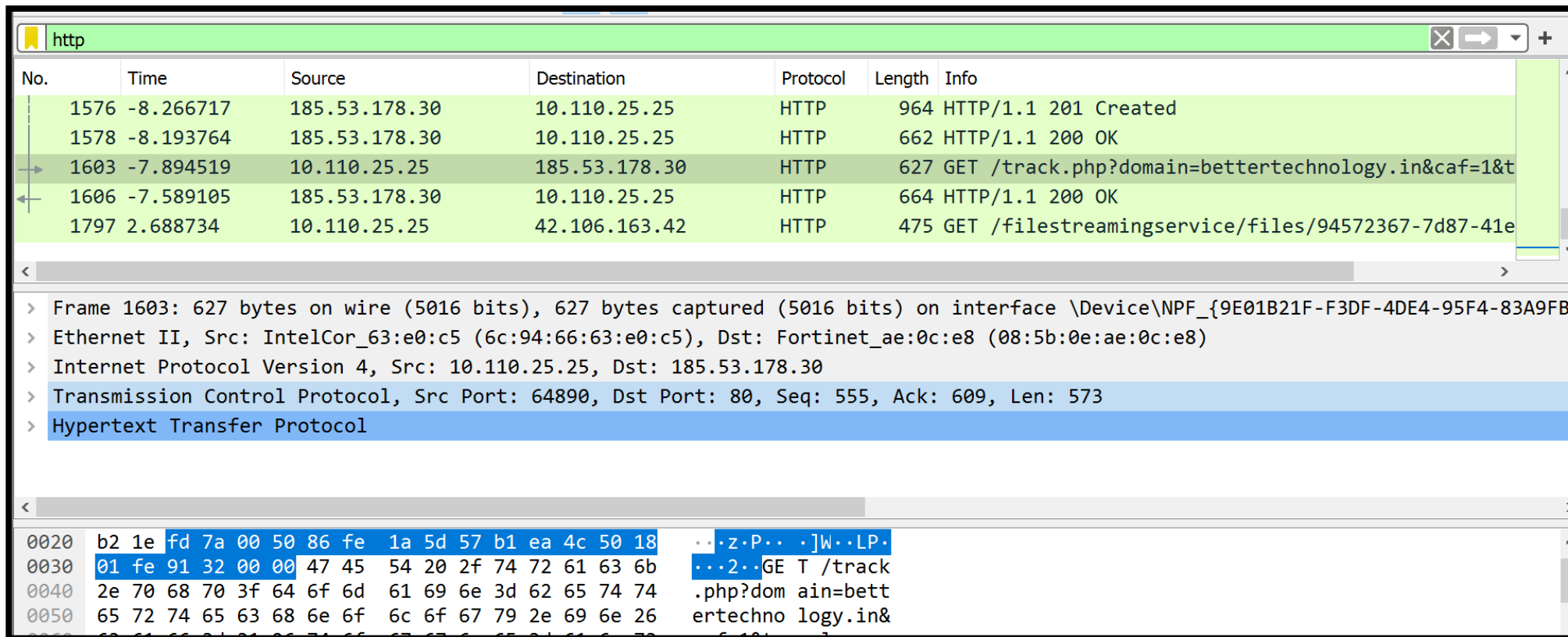
Frame 1603: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{9E01B21F-F3DF-4DE4-95F4-83A9FB}	
Ethernet II, Src: IntelCor_63:e0:c5 (6c:94:66:63:e0:c5), Dst: Fortinet_ae:0c:e8 (08:5b:0e:ae:0c:e8)	
Internet Protocol Version 4, Src: 10.110.25.25, Dst: 185.53.178.30	
Transmission Control Protocol, Src Port: 64890, Dst Port: 80, Seq: 555, Ack: 609, Len: 573	
Hypertext Transfer Protocol	

Offset	Hex	ASCII
0020	b2 1e fd 7a 00 50 86 fe 1a 5d 57 b1 ea 4c 50 18	...z.P... ]W..LP.
0030	01 fe 91 32 00 00 47 45 54 20 2f 74 72 61 63 6b	...2...GE T /track
0040	2e 70 68 70 3f 64 6f 6d 61 69 6e 3d 62 65 74 74	.php?dom ain=bett
0050	65 72 74 65 63 68 6e 6f 6c 6f 67 79 2e 69 6e 26	ertechno logy.in&

# Encapsulation in requesting a web page

- **Network Layer** – Internet Protocol (IP) address
- **Source IP:** 10.110.25.25 (laptop – ipconfig)
- **Destination IP:** 185.53.178.30 (web server)



The image shows a Wireshark packet capture window. The top pane displays a list of network packets. Packet 1603 is selected, showing an HTTP GET request from 10.110.25.25 to 185.53.178.30. The bottom pane shows the detailed structure of this packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The raw packet data is also visible at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
1576	-8.266717	185.53.178.30	10.110.25.25	HTTP	964	HTTP/1.1 201 Created
1578	-8.193764	185.53.178.30	10.110.25.25	HTTP	662	HTTP/1.1 200 OK
1603	-7.894519	10.110.25.25	185.53.178.30	HTTP	627	GET /track.php?domain=bettertechnology.in&caf=1&t
1606	-7.589105	185.53.178.30	10.110.25.25	HTTP	664	HTTP/1.1 200 OK
1797	2.688734	10.110.25.25	42.106.163.42	HTTP	475	GET /filestreamingservice/files/94572367-7d87-41e

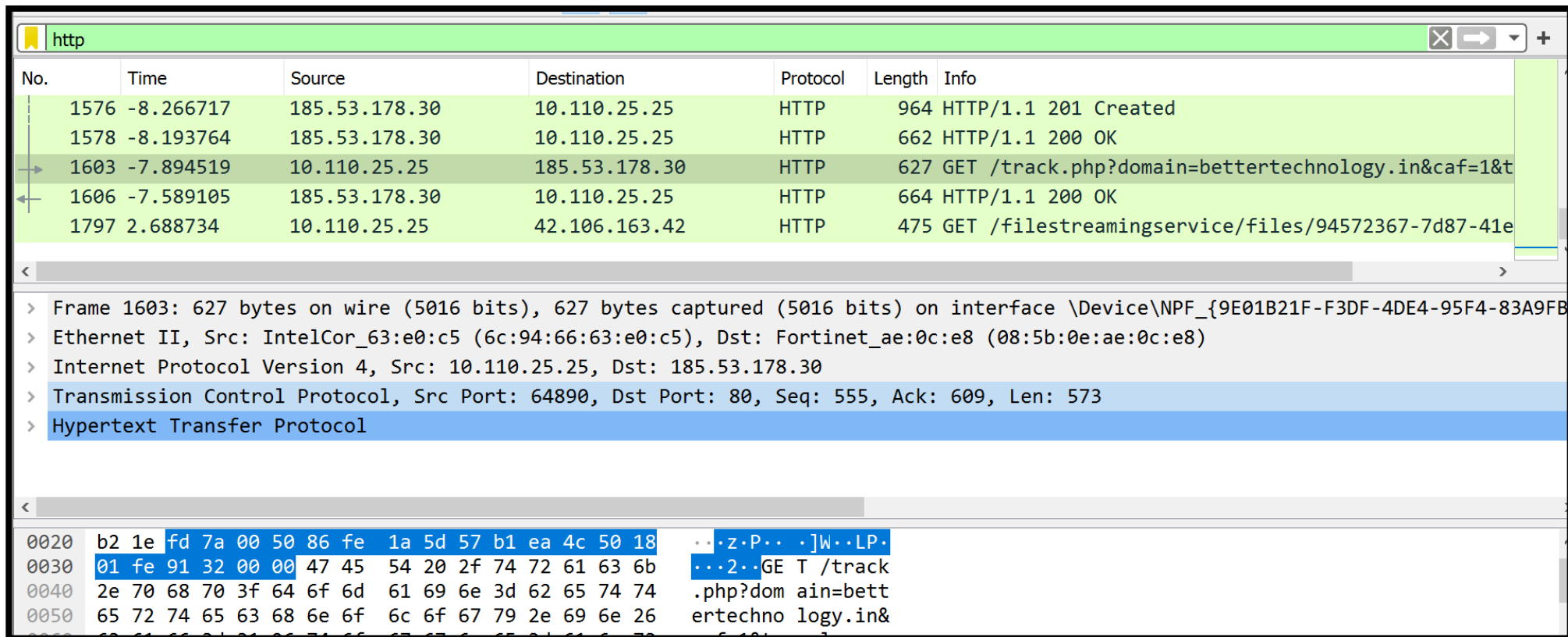
Frame 1603: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{9E01B21F-F3DF-4DE4-95F4-83A9FB}	
Ethernet II, Src: IntelCor_63:e0:c5 (6c:94:66:63:e0:c5), Dst: Fortinet_ae:0c:e8 (08:5b:0e:ae:0c:e8)	
Internet Protocol Version 4, Src: 10.110.25.25, Dst: 185.53.178.30	
Transmission Control Protocol, Src Port: 64890, Dst Port: 80, Seq: 555, Ack: 609, Len: 573	
Hypertext Transfer Protocol	

Offset	Hex	ASCII
0020	b2 1e fd 7a 00 50 86 fe 1a 5d 57 b1 ea 4c 50 18	...z.P... ]W..LP.
0030	01 fe 91 32 00 00 47 45 54 20 2f 74 72 61 63 6b	...2...GE T /track
0040	2e 70 68 70 3f 64 6f 6d 61 69 6e 3d 62 65 74 74	.php?dom ain=bett
0050	65 72 74 65 63 68 6e 6f 6c 6f 67 79 2e 69 6e 26	ertechno logy.in&

# Encapsulation in requesting a web page

- **Data Link Layer** – Physical (MAC) address
- **Source MAC:** 6c:94:66:63:e0:c5 (laptop – ipconfig/all)
- **Destination MAC:** 08:5b:0e:ae:0c:e8 (default gateway)



The image shows a Wireshark packet capture window. The top pane displays a list of network packets. Packet 1603 is selected, showing an HTTP GET request from 10.110.25.25 to 185.53.178.30. The bottom pane shows the detailed structure of this packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers. The raw packet data is visible at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
1576	-8.266717	185.53.178.30	10.110.25.25	HTTP	964	HTTP/1.1 201 Created
1578	-8.193764	185.53.178.30	10.110.25.25	HTTP	662	HTTP/1.1 200 OK
1603	-7.894519	10.110.25.25	185.53.178.30	HTTP	627	GET /track.php?domain=bettertechnology.in&caf=1&t
1606	-7.589105	185.53.178.30	10.110.25.25	HTTP	664	HTTP/1.1 200 OK
1797	2.688734	10.110.25.25	42.106.163.42	HTTP	475	GET /filestreamingservice/files/94572367-7d87-41e

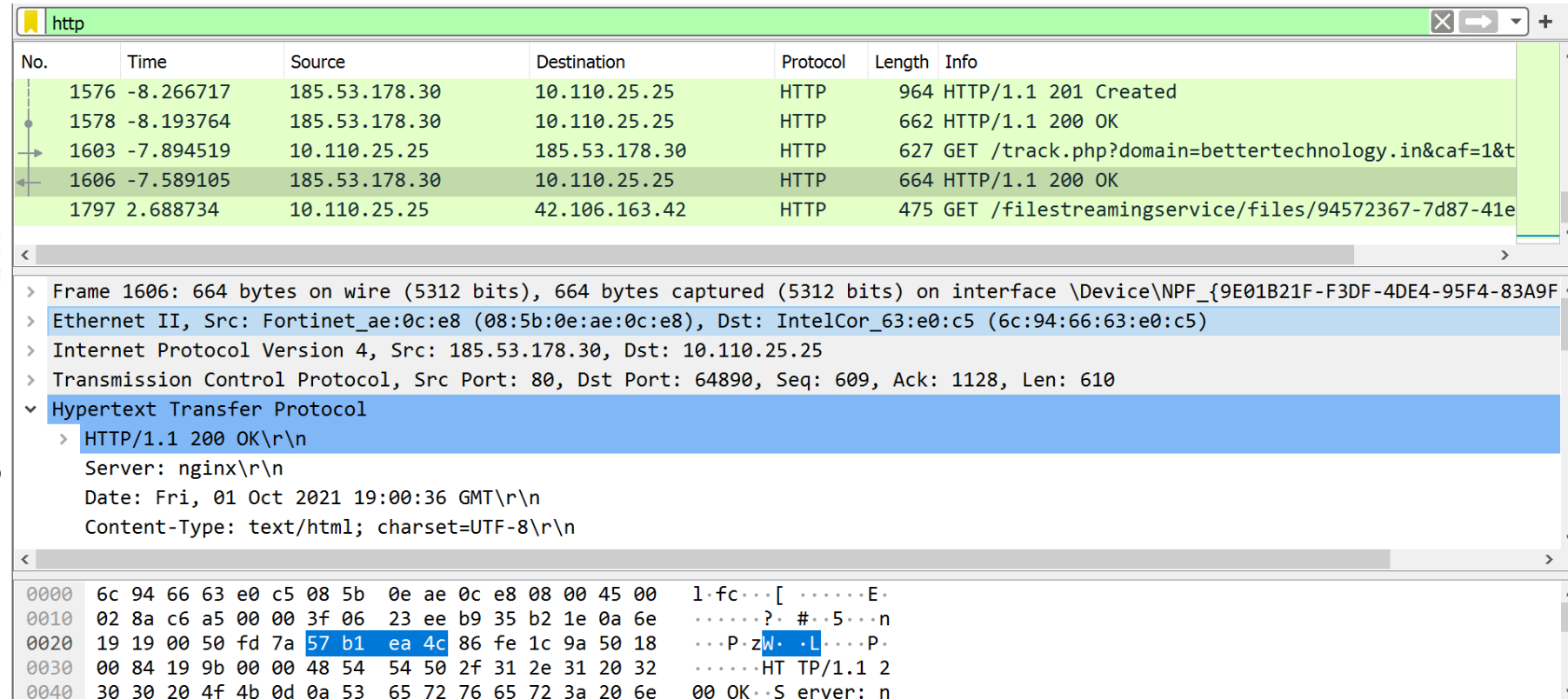
Frame 1603: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{9E01B21F-F3DF-4DE4-95F4-83A9FB}	
Ethernet II, Src: IntelCor_63:e0:c5 (6c:94:66:63:e0:c5), Dst: Fortinet_ae:0c:e8 (08:5b:0e:ae:0c:e8)	
Internet Protocol Version 4, Src: 10.110.25.25, Dst: 185.53.178.30	
Transmission Control Protocol, Src Port: 64890, Dst Port: 80, Seq: 555, Ack: 609, Len: 573	
Hypertext Transfer Protocol	

Offset	Hex	ASCII
0020	b2 1e fd 7a 00 50 86 fe 1a 5d 57 b1 ea 4c 50 18	...z.P... ]W..LP.
0030	01 fe 91 32 00 00 47 45 54 20 2f 74 72 61 63 6b	...2...GE T /track
0040	2e 70 68 70 3f 64 6f 6d 61 69 6e 3d 62 65 74 74	.php?dom ain=bett
0050	65 72 74 65 63 68 6e 6f 6c 6f 67 79 2e 69 6e 26	ertechno logy.in&

# De-Encapsulation in received webpage

- Application - Received webpage successfully by response code 200 ok in the laptop
- Transport - Source and destination port of request are exchanged in response
  - Src: 80
  - Dst: 64890
- Network - also Exchanged
  - Src: 185.53.178.30
  - Dest: 10.110.25.25
- Ethernet - MAC address also exchanged



The image shows a Wireshark packet capture of an HTTP response. The top table lists several packets, with packet 1606 being the focus. Below this, the packet details pane shows the de-encapsulation layers for packet 1606: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1576	-8.266717	185.53.178.30	10.110.25.25	HTTP	964	HTTP/1.1 201 Created
1578	-8.193764	185.53.178.30	10.110.25.25	HTTP	662	HTTP/1.1 200 OK
1603	-7.894519	10.110.25.25	185.53.178.30	HTTP	627	GET /track.php?domain=bettertechnology.in&caf=1&t
1606	-7.589105	185.53.178.30	10.110.25.25	HTTP	664	HTTP/1.1 200 OK
1797	2.688734	10.110.25.25	42.106.163.42	HTTP	475	GET /filestreamingservice/files/94572367-7d87-41e

Frame 1606: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface \Device\NPF_{9E01B21F-F3DF-4DE4-95F4-83A9F}
Ethernet II, Src: Fortinet_ae:0c:e8 (08:5b:0e:ae:0c:e8), Dst: IntelCor_63:e0:c5 (6c:94:66:63:e0:c5)
Internet Protocol Version 4, Src: 185.53.178.30, Dst: 10.110.25.25
Transmission Control Protocol, Src Port: 80, Dst Port: 64890, Seq: 609, Ack: 1128, Len: 610
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: nginx\r\n
Date: Fri, 01 Oct 2021 19:00:36 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n

0000	6c 94 66 63 e0 c5 08 5b 0e ae 0c e8 08 00 45 00	l.fc...[ .....E.
0010	02 8a c6 a5 00 00 3f 06 23 ee b9 35 b2 1e 0a 6e	.....?..#..5...n
0020	19 19 00 50 fd 7a 57 b1 ea 4c 86 fe 1c 9a 50 18	...P.zW..L...P.
0030	00 84 19 9b 00 00 48 54 54 50 2f 31 2e 31 20 32	.....HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 6e	00 OK..S erver: n

# Protocol Data Unit Analysis

- We will **analyze now** the protocol data units(**PDU**) in web page request and response packets together

Layer	Protocol	Web page request frame	Web page response frame
Application	HTTP	Host: js.parkingcrew.net	200 ok [web page confirmed]
Transport	TCP	Src port: 64890 Dest Port: 80	Src port: 80 Dest Port: 64890
Network	IP	Src IP: 10.110.25.25 Dest IP: 185.53.178.30	Src IP: 185.53.178.30 Dest IP: 10.110.25.25
Data Link & Physical	Ethernet	Src MAC: 6c:94:66:63:e0:c5 Dest MAC: 08:5b:0e:ae:0c:e8	Src MAC: 08:5b:0e:ae:0c:e8 Dest MAC: 6c:94:66:63:e0:c5

# Summary

- Examined the IP address & MAC address of our laptop
- Install & launch Wireshark in the laptop having internet access
- Analyze the protocols in the packet sniffer tool for web page request and response
  - Viewed Protocol Data Units



