Module3 Network Protocols-Short version

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protocols

Network Protocol Overview

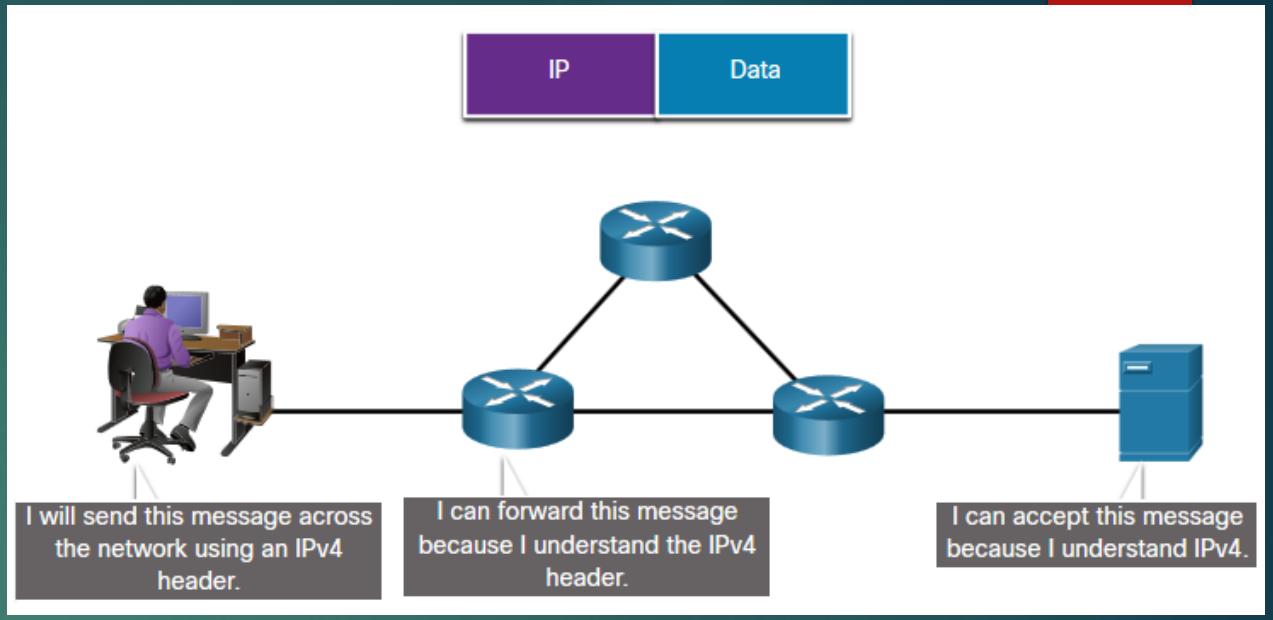
Network protocols define a common set of rules.

- 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

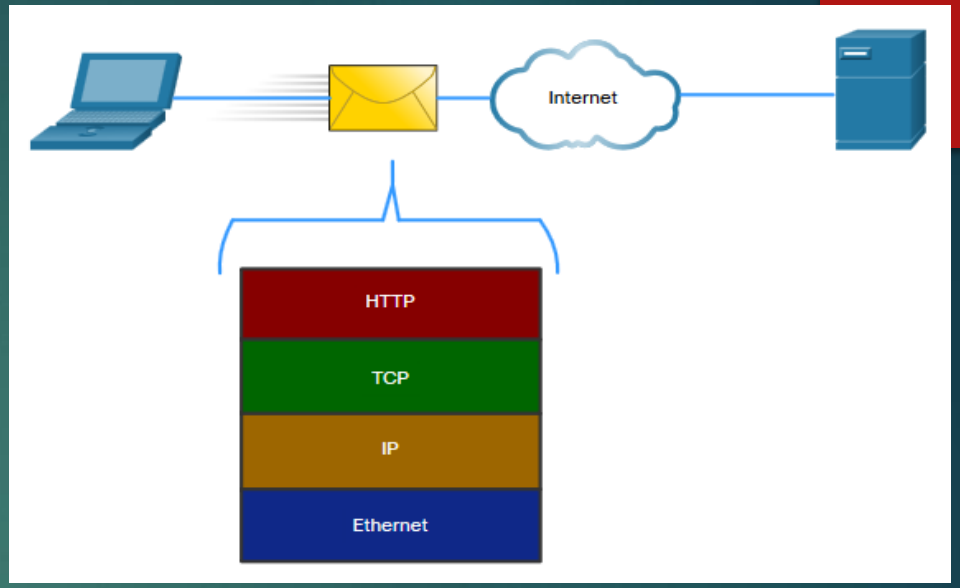
- Devices use agreed-upon protocols to communicate .
- Protocols may have may have one or functions.



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)

Protocol Suites

Network Protocol Suites

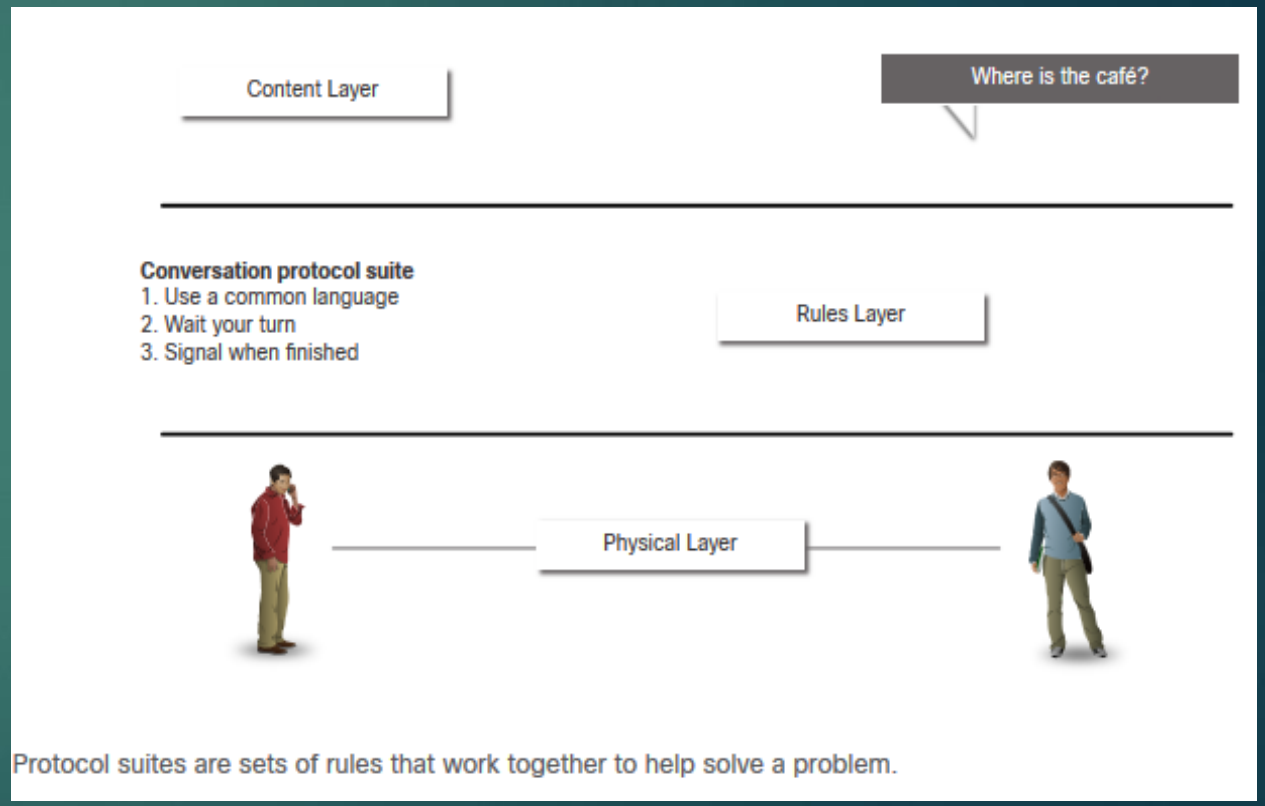
Protocols must be able to work with other protocols.

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

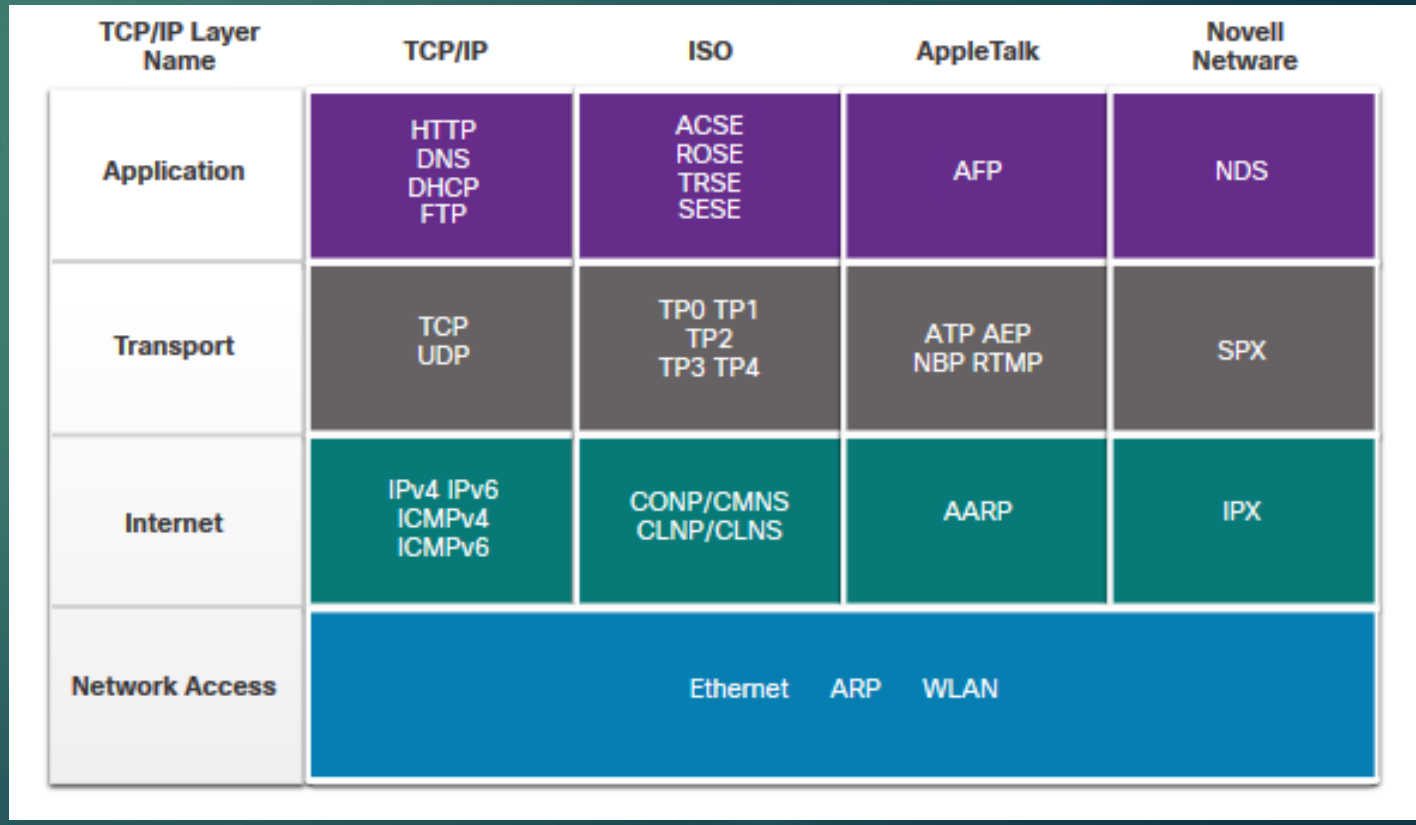


Protocol Suites

Evolution of Protocol Suites

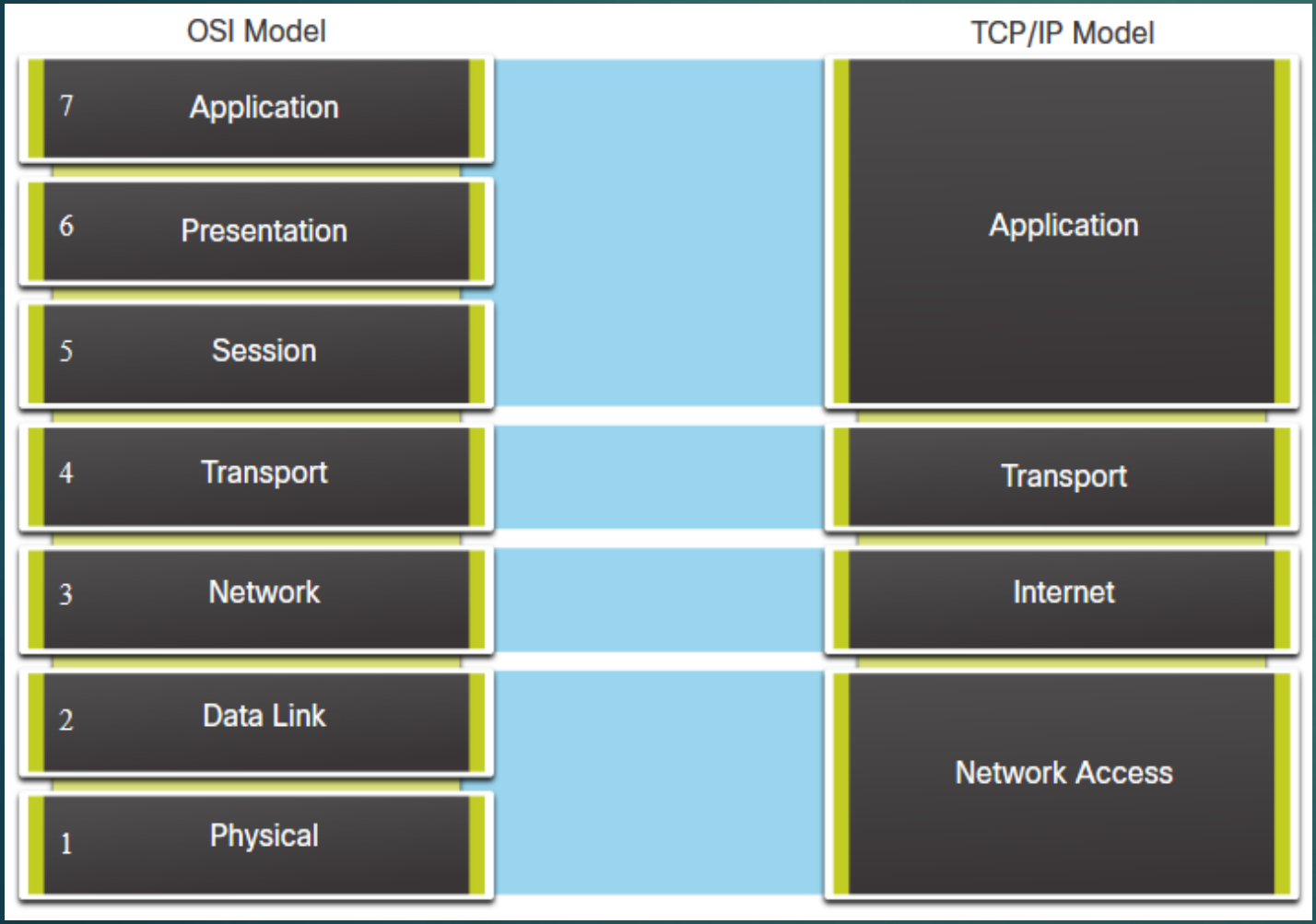
There are several protocol suites.

- **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.



Reference Models

OSI and TCP/IP Model Comparison



- The OSI model divides the network access layer and the application layer of the TCP/IP model into multiple layers.
- The TCP/IP protocol suite does not specify which protocols to use when transmitting over a physical medium.
- OSI Layers 1 and 2 discuss the necessary procedures to access the media and the physical means to send data over a network.

Reference Models

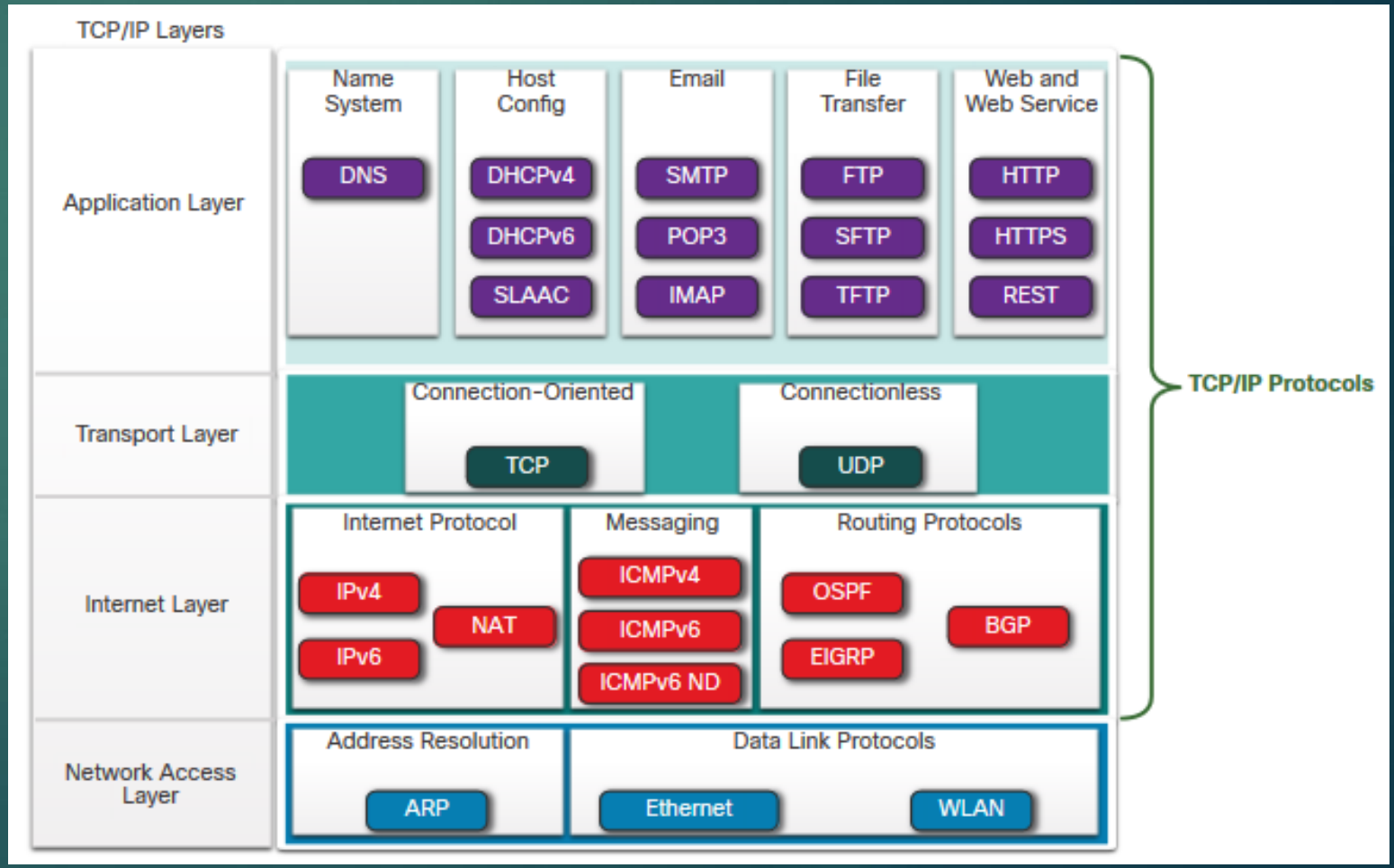
The TCP/IP Reference Model

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.
Network Access	Controls the hardware devices and media that make up the network.

Protocol Suites

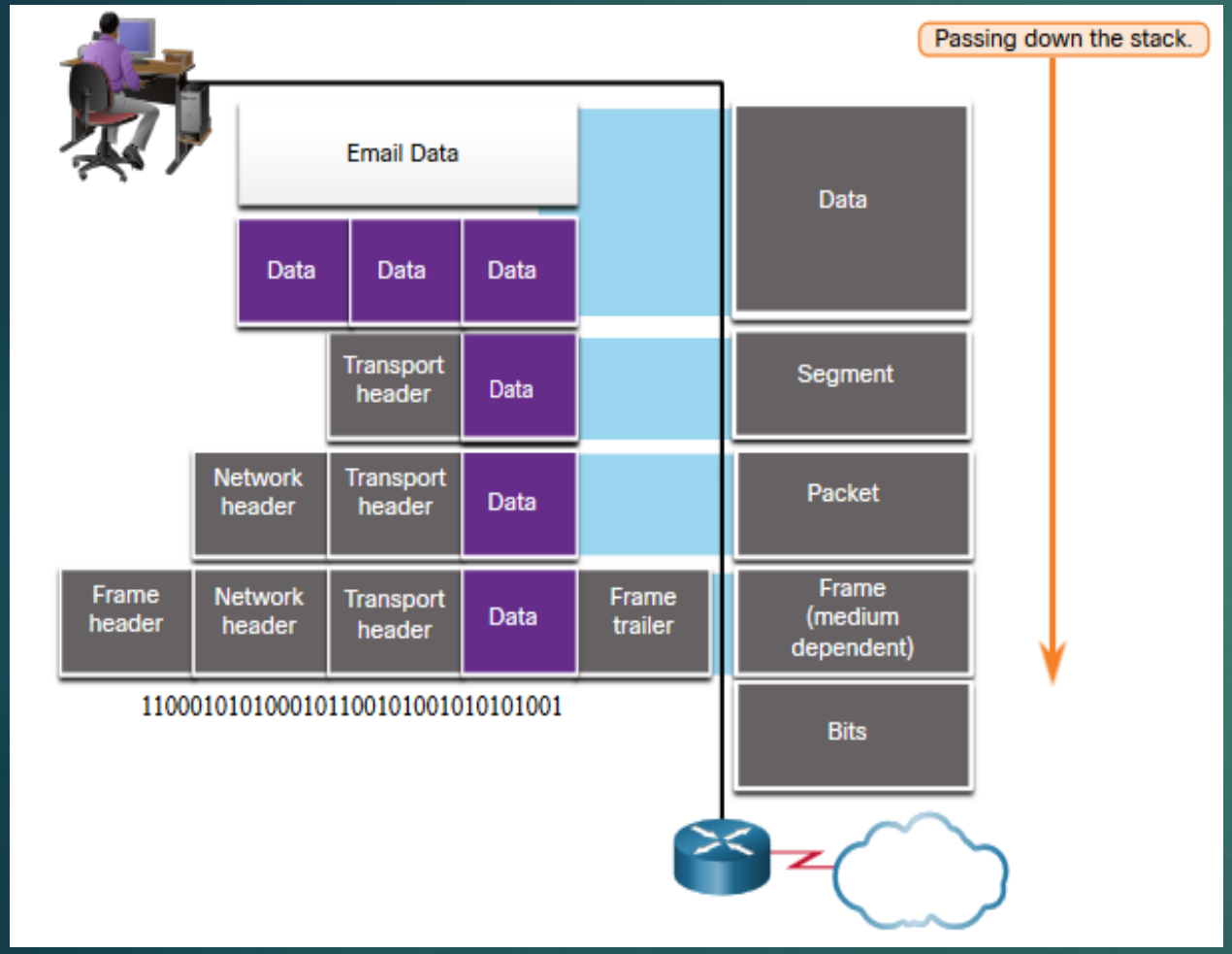
TCP/IP Protocol Suite

- TCP/IP is the protocol suite used by the internet and includes many protocols.
- TCP/IP is:
  - 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



Data Encapsulation

Protocol Data Units



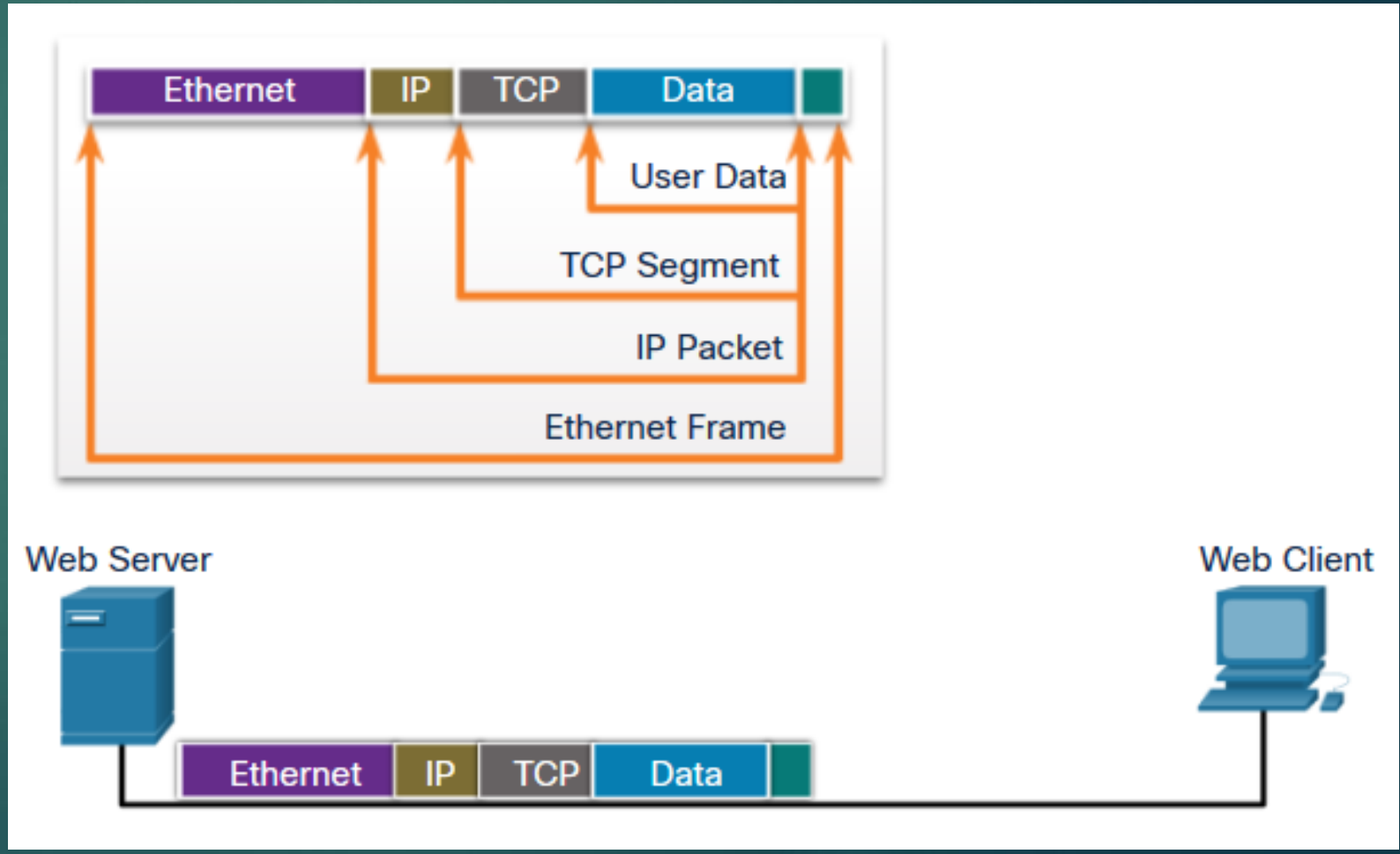
Encapsulation is the process where protocols add their information to the data.

- At each stage of the process, a 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.
- PDUs passing down the stack are as follows:
  1. Data (Data Stream)
  2. Segment
  3. Packet
  4. Frame
  5. Bits (Bit Stream)

Data Encapsulation

Encapsulation Example

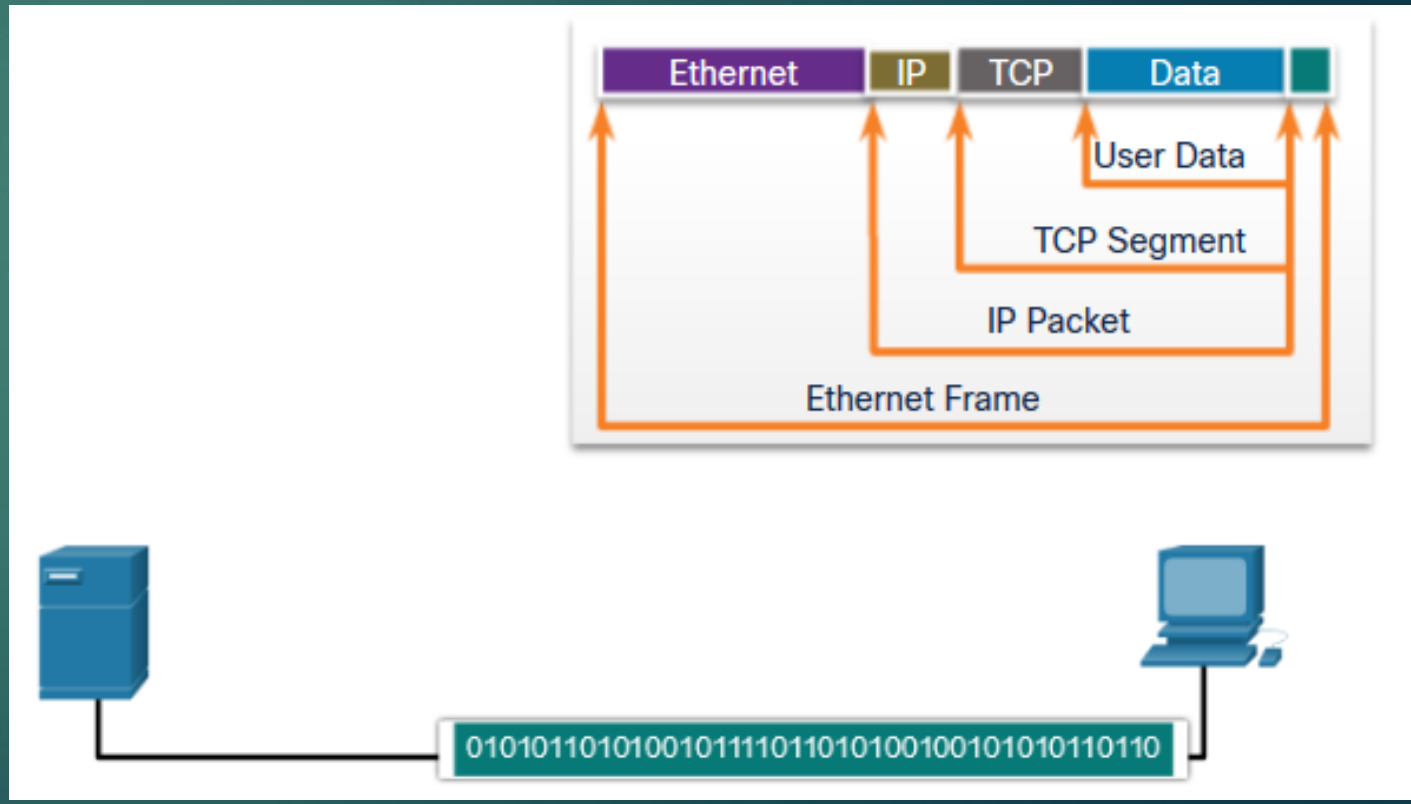
- Encapsulation is a top down process.
- The level above does its process and then passes it down to the next level of the model. This process is repeated by each layer until it is sent out as a bit stream.



Data Encapsulation

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.
  1. Received as Bits (Bit Stream)
  2. Frame
  3. Packet
  4. Segment
  5. Data (Data Stream)



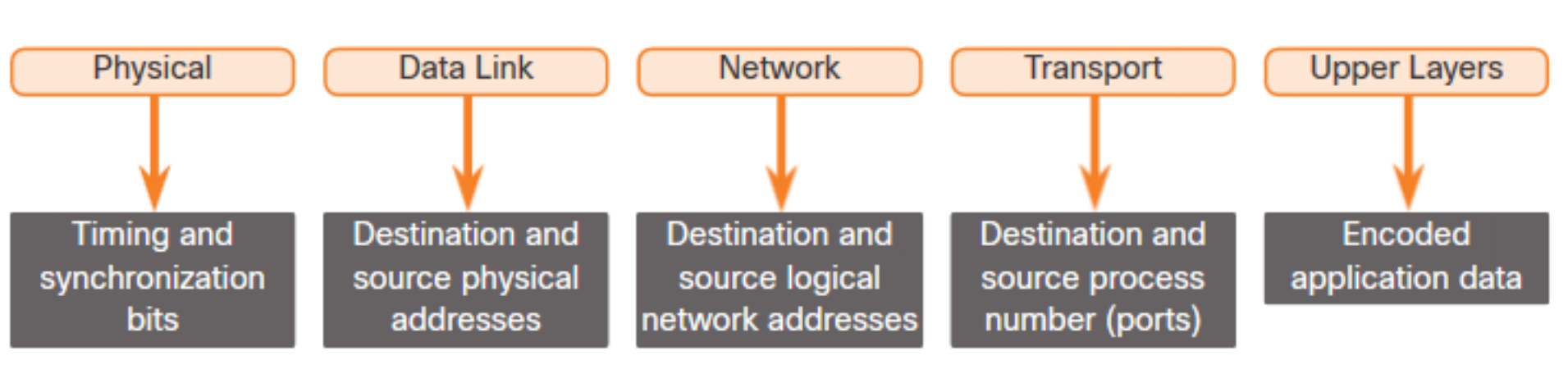
Data Access

Addresses

Both the data link and network layers use addressing to deliver data from source to destination.

Network layer source and destination addresses - Responsible for delivering the IP packet from original source to the final destination.

Data link layer source and destination addresses – Responsible for delivering the data link frame from one network interface card (NIC) to another NIC on the same network.



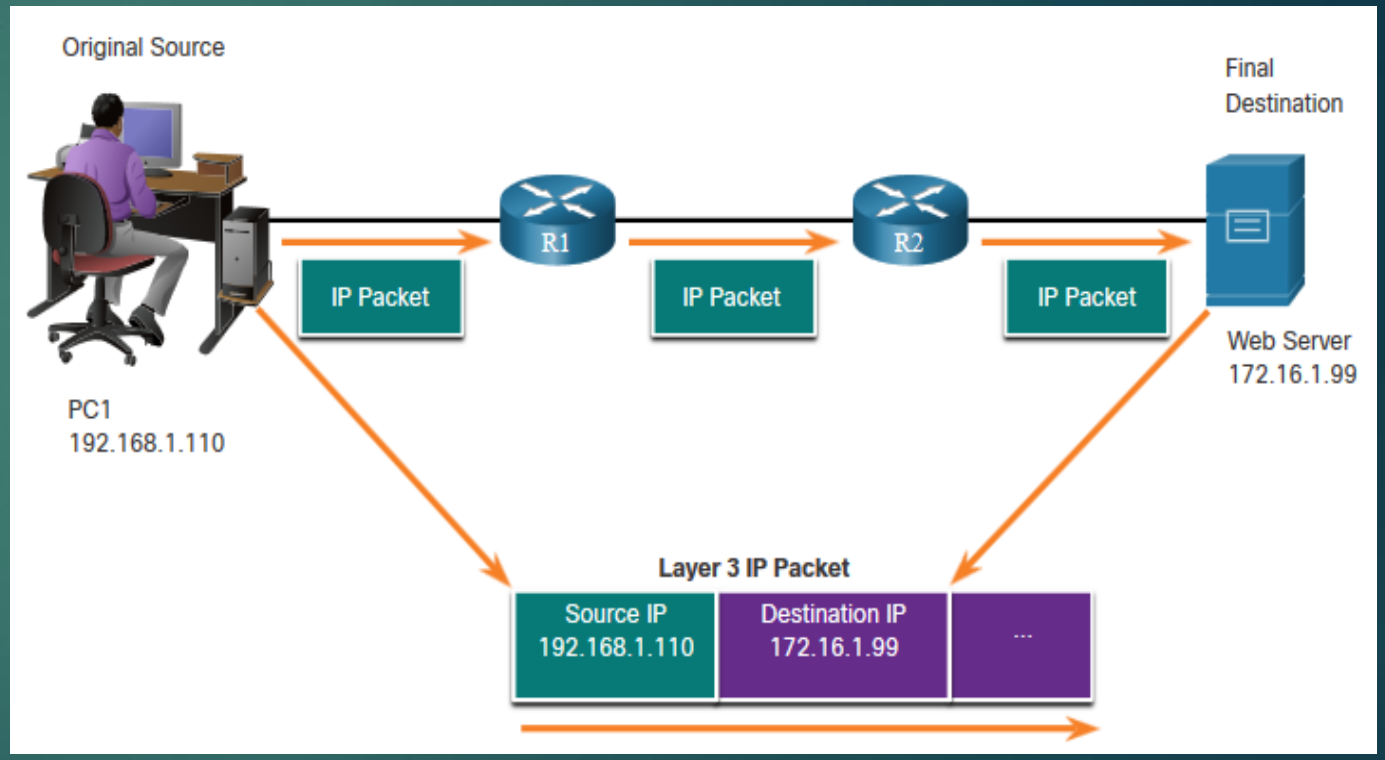
Data Access

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.

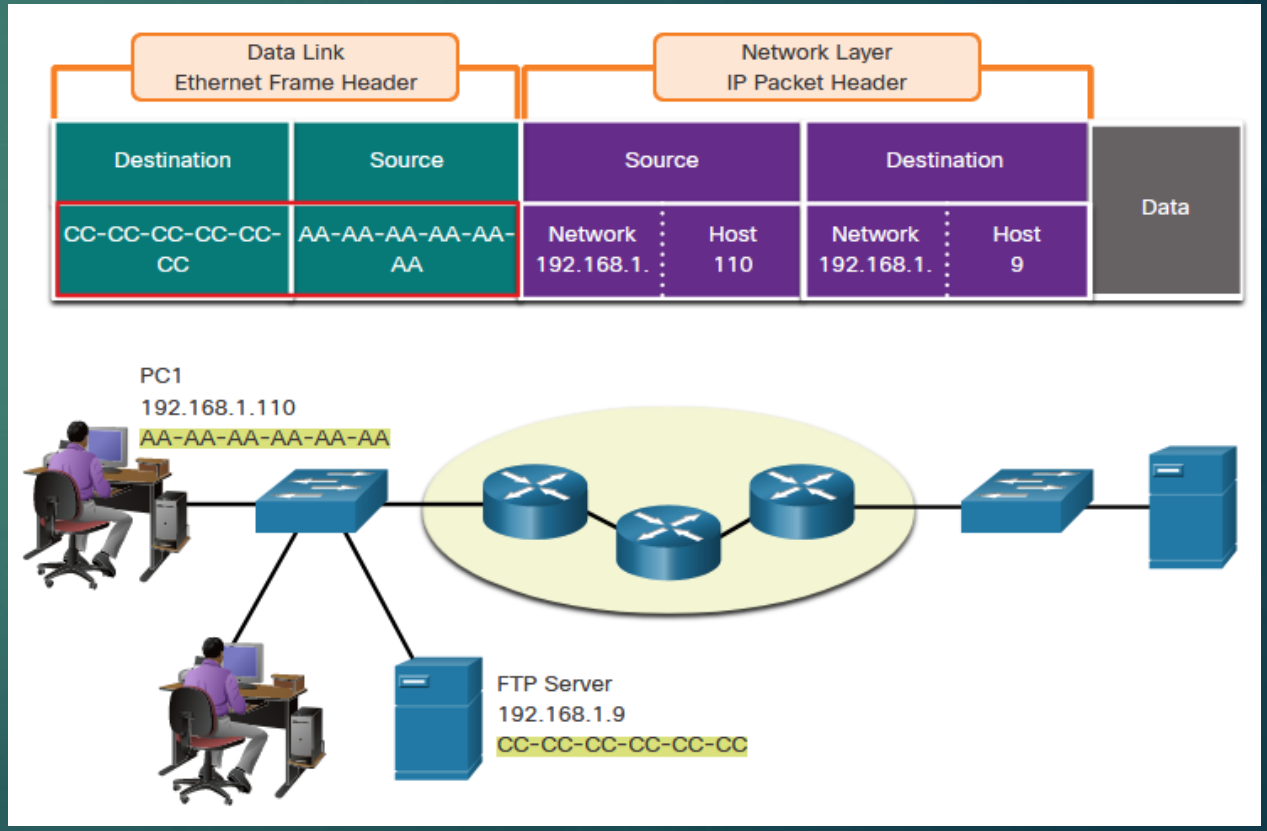


Role of the Data Link Layer Addresses: Same IP Network

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.



Demo

- Using Wireshark to Examine TELNET, SSH, HTTP, DNS traffic
- Using Packet Tracer to simulate network