Data Encapsulation & OSI & TCP/IP Models
Week 2

Lecturer: Lucy White lbwhite@wit.ie

Office : 324

Network Protocols

- **A protocol is a formal description of a set of rules and conventions that govern a particular aspect of how devices on a network communicate. Protocols determine the format, timing, sequencing, flow control and error control in data communication. Without protocols, the computer cannot make or rebuild the stream of incoming bits from another computer into the original format.**

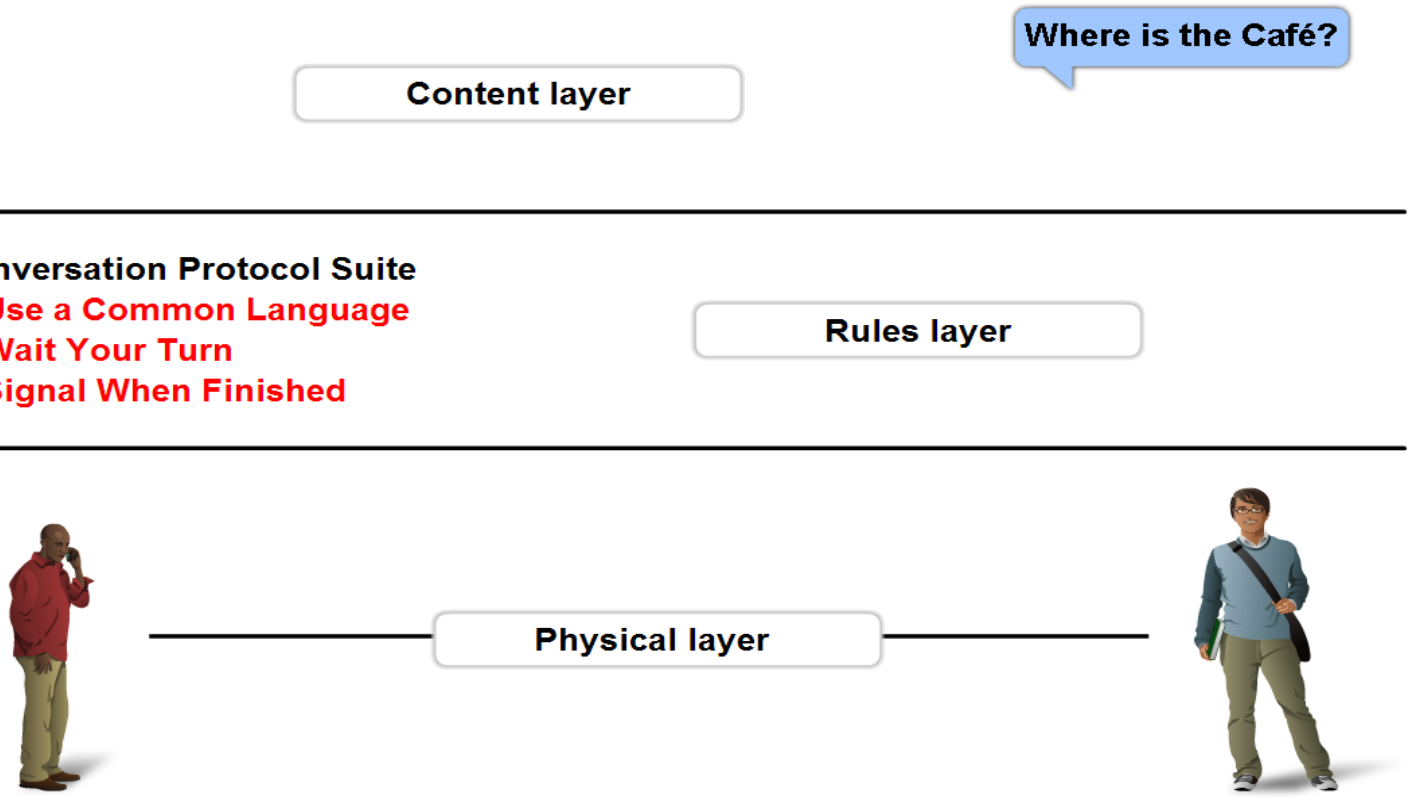
- **Protocols control all aspects of data communication, which include the following:**
  - **How the physical network is built**
  - **How computers connect to the network**
  - **How the data is formatted for transmission**
  - **The setting up and termination of data transfer sessions**
  - **How that data is sent**
  - **How to deal with errors**

Protocol Suites & Industry Standard

- Many of the protocols that comprise a protocol suite reference other widely utilized protocols or industry standards
- Institute of Electrical and Electronics Engineers (IEEE) or the Internet Engineering Task Force (IETF)
- The use of standards in developing and implementing protocols ensures that products from different manufacturers can work together for efficient communications

Function of Protocol in Network Communication

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

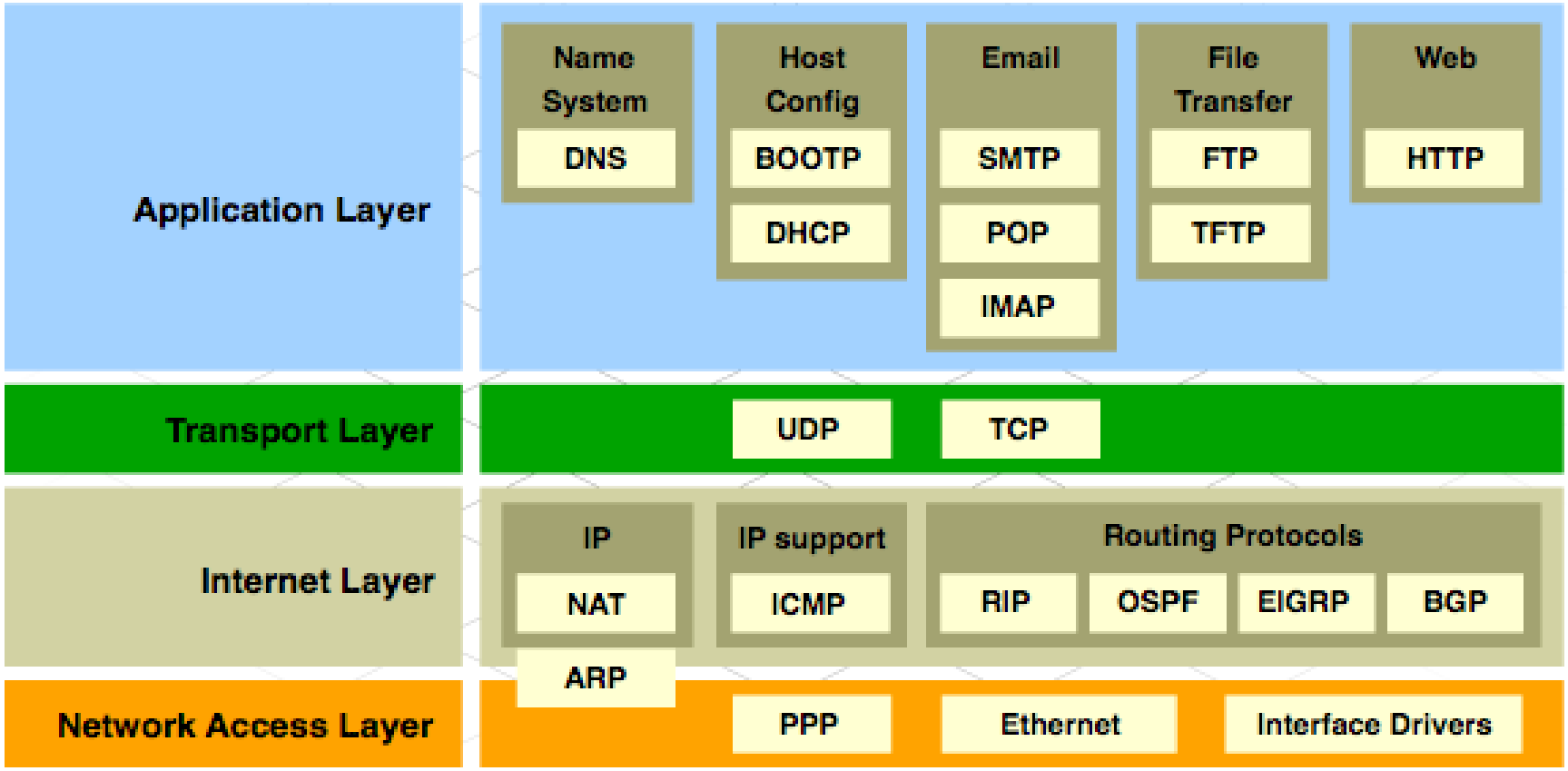


A standard is

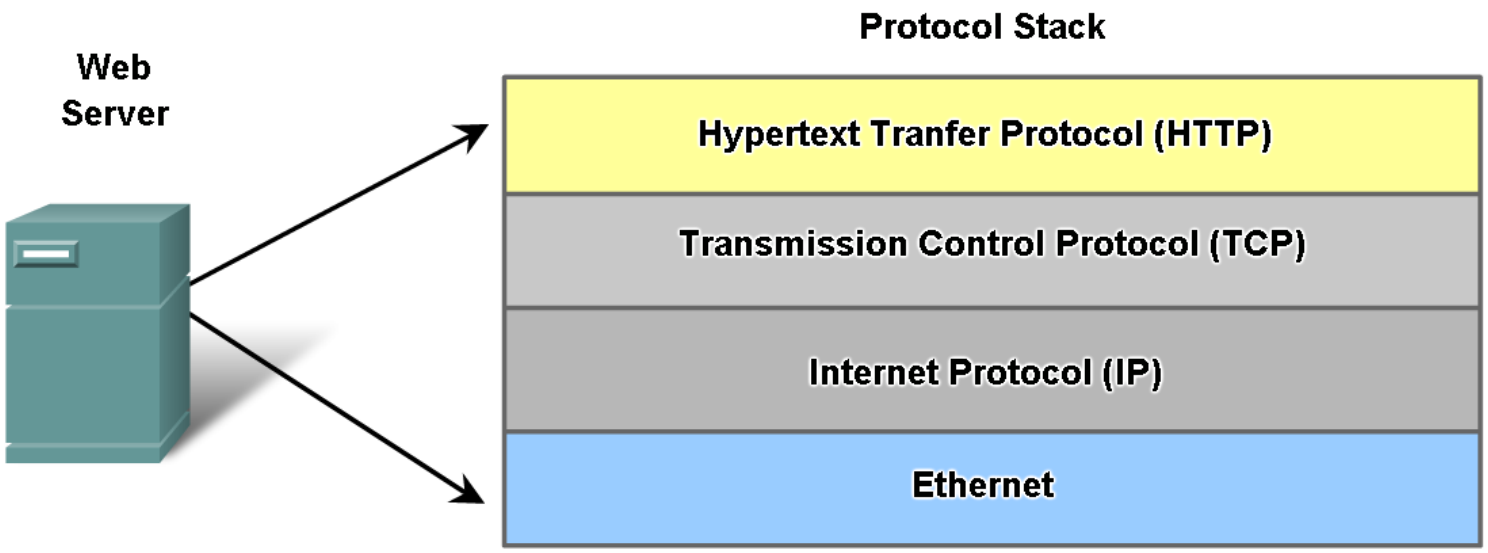
a process or protocol that has been endorsed by the networking industry and ratified by a standards organization

Protocol Suites

TCP/IP Protocol Suite and Communication



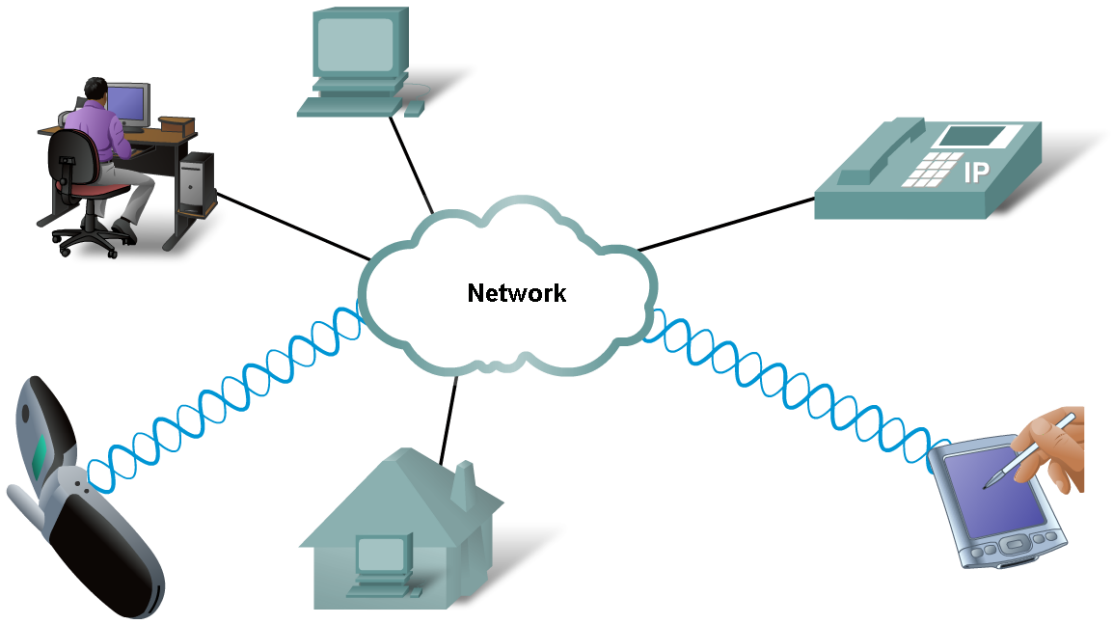
Function of Protocol in Network Communication



Function of Protocol in Network Communication

- **Technology independent Protocols**

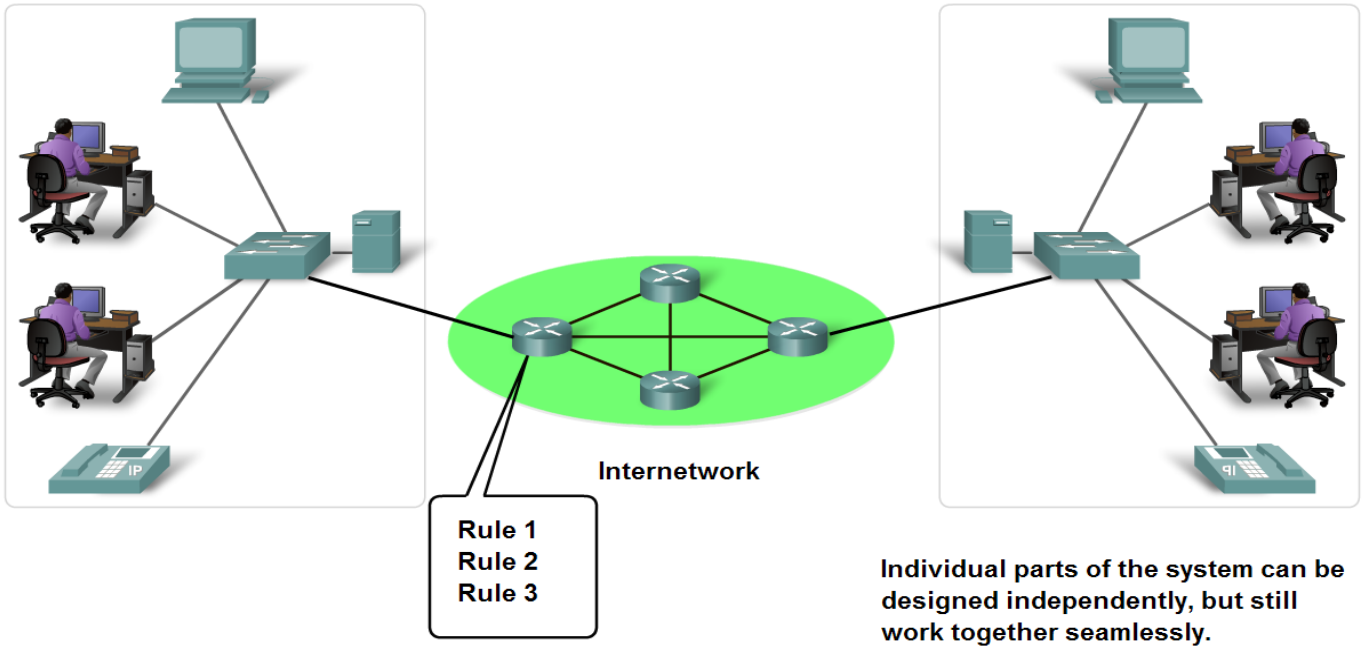
  -Many diverse types of devices can communicate using the same sets of protocols. This is because protocols specify network functionality, not the underlying technology to support this functionality.



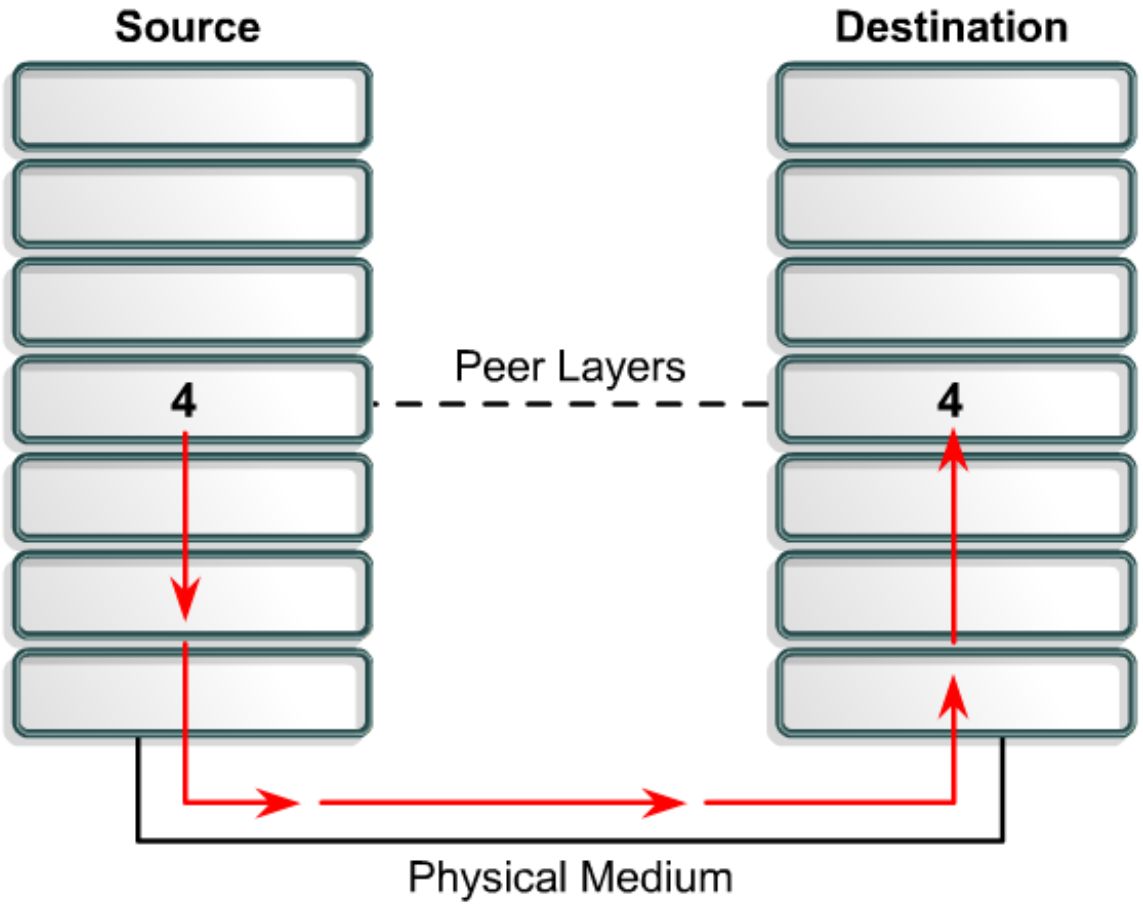
Layers with TCP/IP and OSI Model

- **Explain the benefits of using a layered model**
  - **–Benefits include**
    - **assists in protocol design**
    - **fosters competition**
    - **changes in one layer do not affect other layers**
    - **provides a common language**

Using a layered model helps in the design of complex, multi-use, multi-vendor networks.



Using layers to describe data communication



The OSI Model

• The OSI layer was introduced by the International Organization for Standardization (ISO) in 1984 in order to provide a reference model to make sure products of different vendors would interoperate in networks.

• OSI is short for Open Systems Interconnection.

• The OSI layer shows WHAT needs to be done to send data from an application on one computer, trough a network, to an application on another computer, not HOW it should be done.

• A layer in the OSI model communicates with three other layers: the layer above it, the layer below it, and the same layer at its communication partner.

• Data transmitted between software programs passes all 7 OSI layers.

OSI Layers

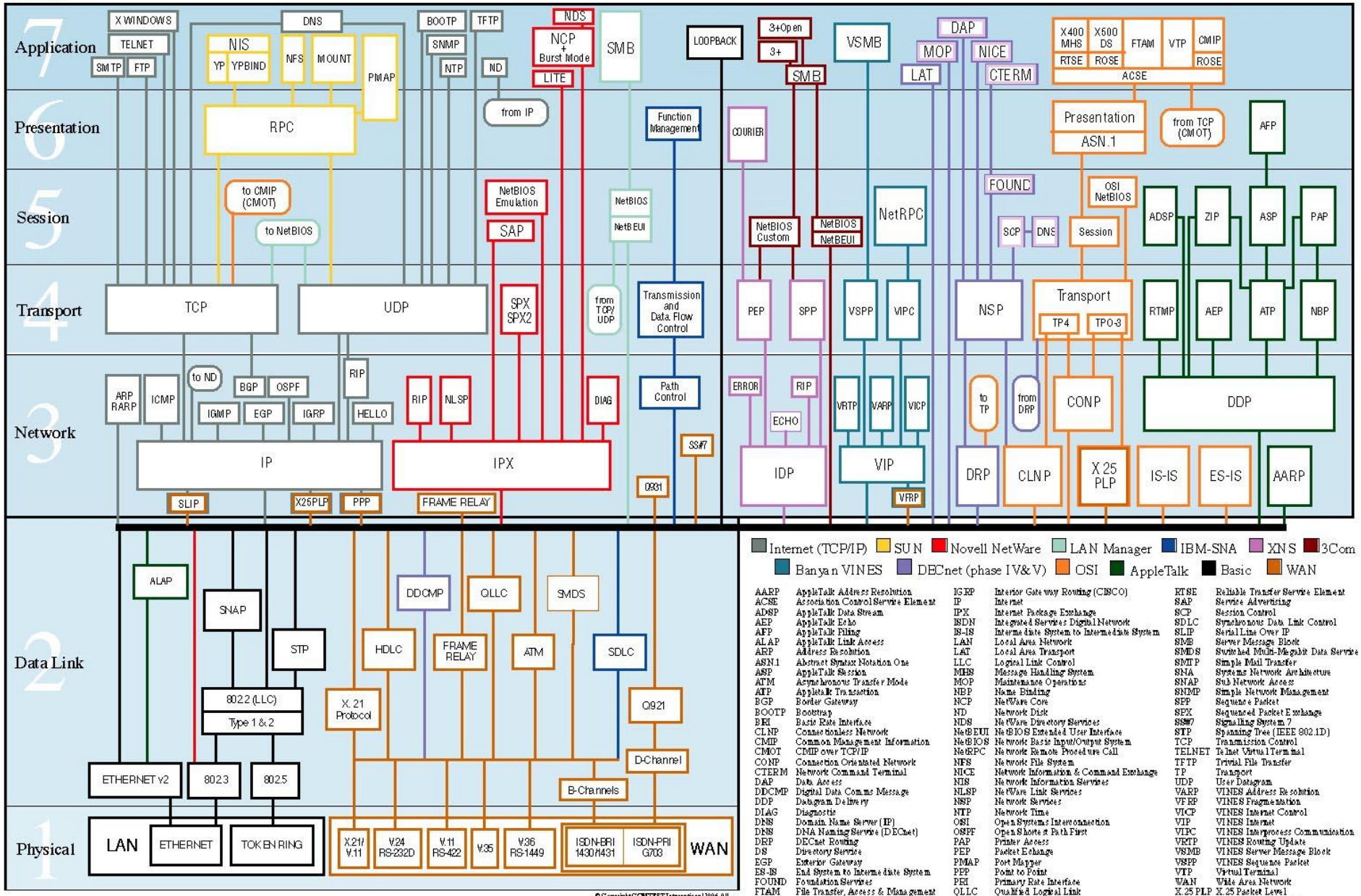
The OSI reference model is a framework that is used to understand how information travels throughout a network. The OSI reference model explains how packets travel through the various layers to another device on a network, even if the sender and destination have different types of network media.
In the OSI reference model, there are seven numbered layers, each of which illustrates a particular network function.

Dividing the network into seven layers provides the following advantages:

- It breaks network communication into smaller, more manageable parts.
- It standardizes network components to allow multiple vendor development and support.
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting other layers.
- It divides network communication into smaller parts to make learning it easier to understand.

Comtest LA Express
Comtest NM Elite
Comtest MDA

Comtest Network Services - protocol decode chart

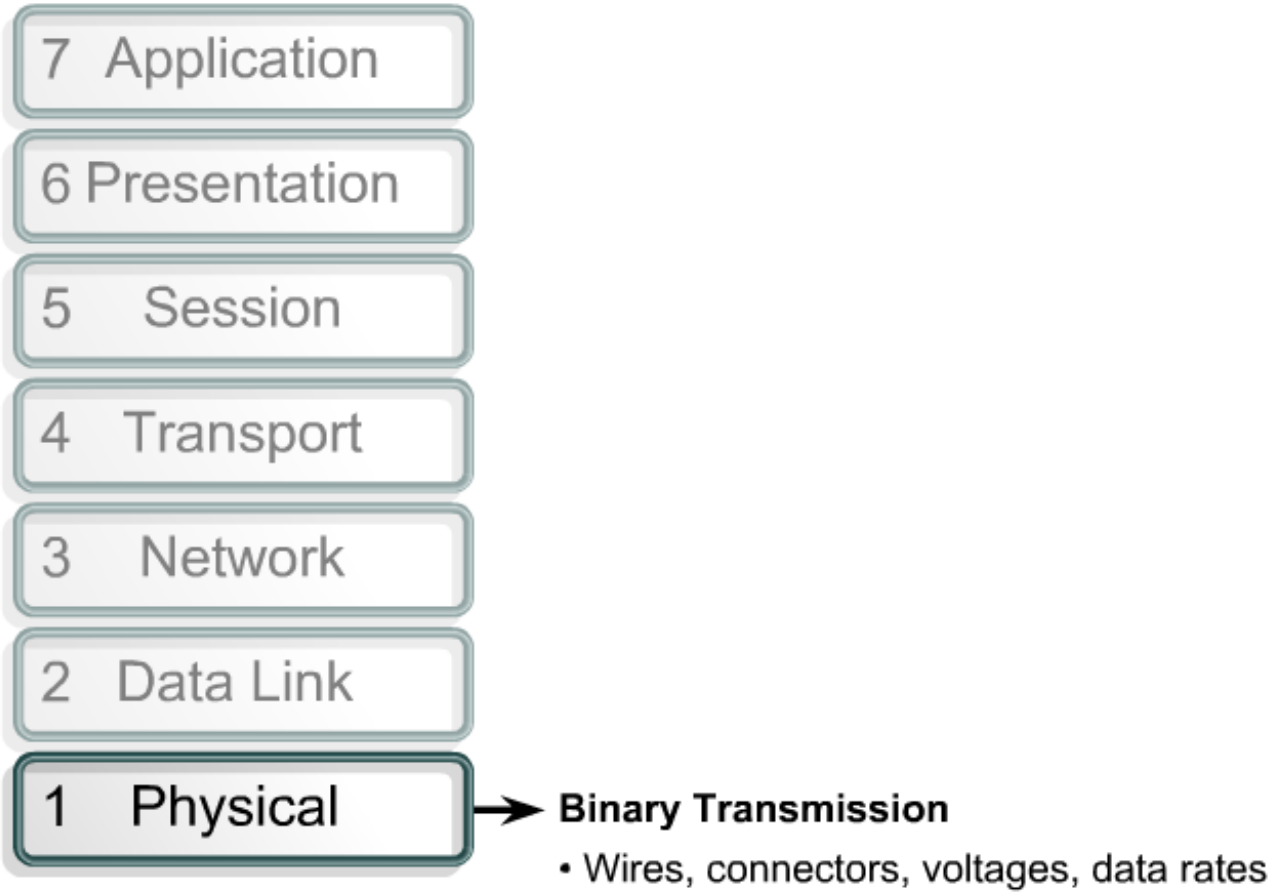


Internet (TCP/IP) SUN Novell NetWare LAN Manager IBM-SNA XNS 3Com
Banyan VINES DECnet (phase IV&V) OSI AppleTalk Basic WAN

AARP	AppleTalk Address Resolution
ACSE	Association Control Service Element
ADSP	AppleTalk Data Stream
AEP	AppleTalk Echo
AFP	AppleTalk Filing
ALAP	AppleTalk Link Access
ARP	Address Resolution
ASN.1	Abstract Syntax Notation One
ASP	AppleTalk Session
ATM	Asynchronous Transfer Mode
ATP	AppleTalk Transaction
BGP	Border Gateway
BOOTP	Bootstrap
BRI	Basic Rate Interface
CLNP	Connectionless Network
CMIP	Common Management Information
CMOT	CMIP over TCP/IP
CONP	Connection Orientated Network
CTERM	Network Command Terminal
DAP	Data Access
DDCMP	Digital Data Comms Message
DDP	Datagram Delivery
DIAG	Diagnostic
DNS	Domain Name Server (IP)
DNS	DNA Naming Service (DECnet)
DRP	DECnet Routing
DS	Directory Service
EGP	Exterior Gateway
ES-IS	End System to Intermediate System
FOUND	Foundation Services
FTAM	File Transfer, Access & Management
FTP	File Transfer
HDLC	High-Level Data Link Control
ICMP	Internet Control Message
IDP	Internetwork Datagram
IGMP	Internet Group Management
IGRP	Interior Gateway Routing (CISCO)
IP	Internet
IPX	Internet Package Exchange
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
LAN	Local Area Network
LAT	Local Area Transport
LLC	Logical Link Control
MHS	Message Handling System
MOP	Maintenance Operations
NBP	Name Binding
NCP	NetWare Core
ND	Network Disk
NDS	NetWare Directory Services
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
NetRPC	Network Remote Procedure Call
NFS	Network File System
NICE	Network Information & Command Exchange
NIS	Network Information Services
NLSP	NetWare Link Services
NSP	Network Services
NTP	Network Time
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Printer Access
PEP	Packet Exchange
PMAP	Port Mapper
PPP	Point to Point
PRI	Primary Rate Interface
QLLC	Qualified Logical Link
RARP	Reverse ARP
RIP	Routing Information
ROSE	Remote Operations Service Element
RPC	Remote Procedure Call
RTMP	Routing Table Maintenance
RTSE	Reliable Transfer Service Element
SAP	Service Advertising
SCP	Session Control
SDLC	Synchronous Data Link Control
SLIP	Serial Line Over IP
SMB	Server Message Block
SMDS	Switched Multi-Megabit Data Service
SMTP	Simple Mail Transfer
SNA	Systems Network Architecture
SNAP	Sub Network Access
SNMP	Simple Network Management
SPP	Sequence Packet
SPX	Sequenced Packet Exchange
SS#7	Signalling System 7
STP	Spanning Tree (IEEE 802.1D)
TCP	Transmission Control
TELNET	Telnet Virtual Terminal
TFTP	Trivial File Transfer
TP	Transport
UDP	User Datagram
VARP	VINES Address Resolution
VFRP	VINES Fragmentation
VICP	VINES Internet Control
VIP	VINES Internet
VIPC	VINES Interprocess Communication
VRTP	VINES Routing Update
VSMB	VINES Server Message Block
VSPP	VINES Sequence Packet
VTP	Virtual Terminal
WAN	Wide Area Network
X.25 PLP	X.25 Packet Level
XNS	Xerox Network System
YP	Yellow Pages (NIS)
YPBIND	Binder Program (NIS)
ZIP	Zone Information

www.comtest-int.com

OSI Layers


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Binary Transmission
• Wires, connectors, voltages, data rates

OSI Layers

Direct Link Control, Access to Media

- Provides reliable transfer of data across media
- Connectivity and path selection between host systems

OSI Layers

Network Address and Best Path Determination

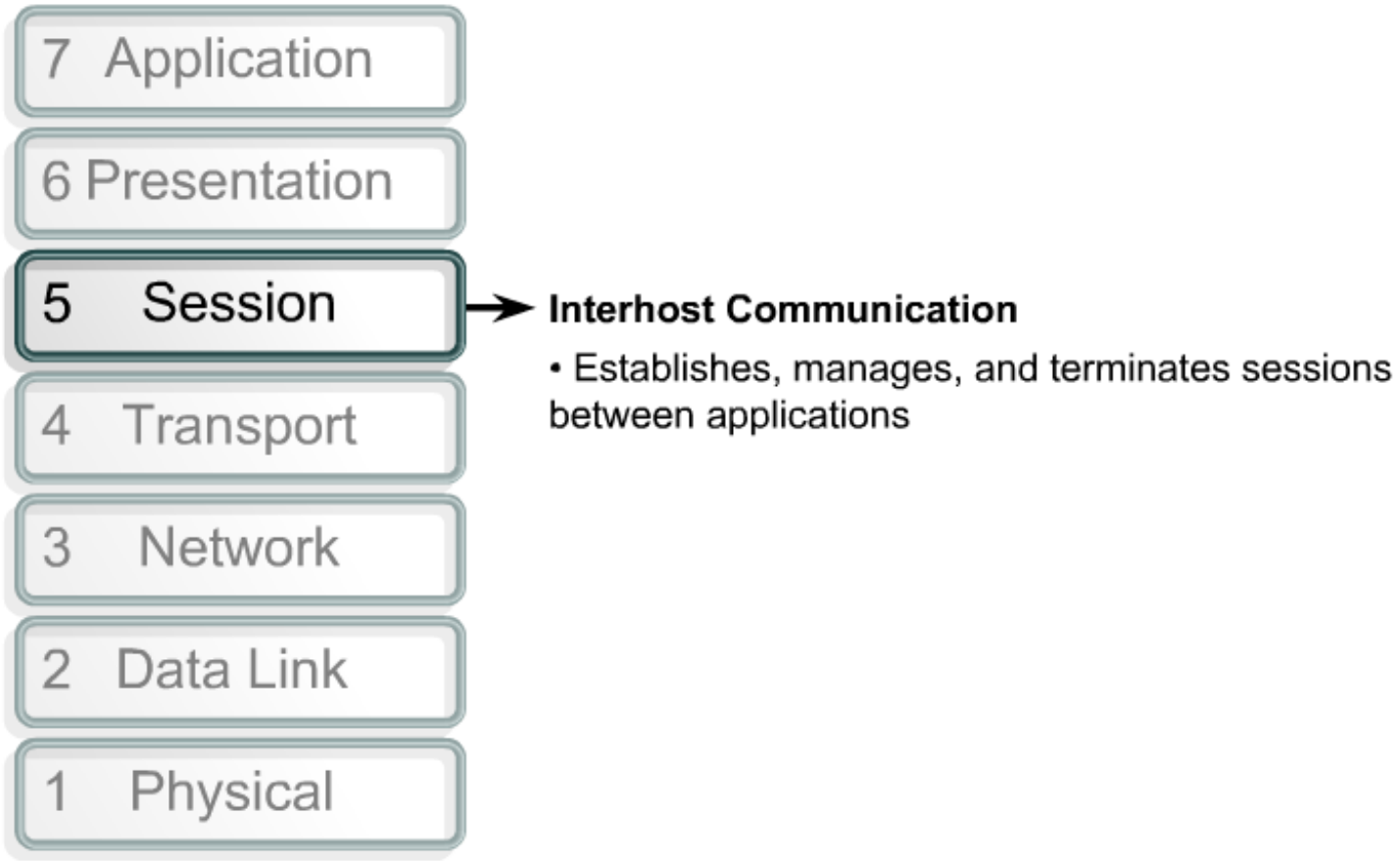
- Provides reliable transfer of data across media
- Connectivity and path selection between host systems
- Logical addressing
- Best effort delivery

OSI Layers

End-to-end Connections

- Concerned with transportation issues between hosts
- Data transport reliability
- Establish, maintain, terminate virtual circuits
- Fault detection and recovery information flow control

OSI Layers


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Interhost Communication
• Establishes, manages, and terminates sessions between applications

OSI Layers

Data Representation

- Ensure data is readable by receiving system
- Format of data
- Data structures
- Negotiates data transfer syntax for application layer

OSI Layers

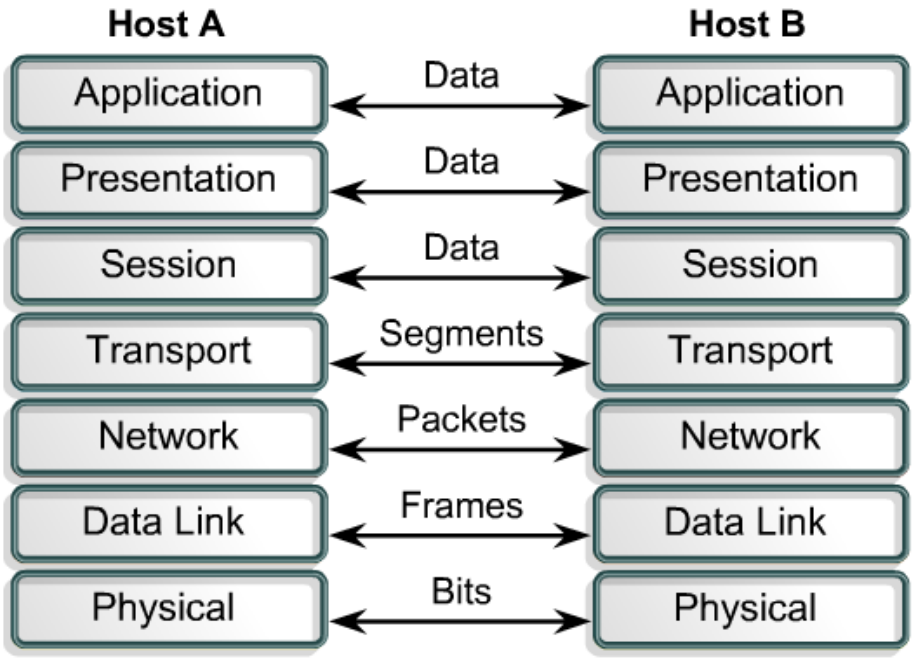
Network Processes to Applications

- Provides network services to application processes, such as electronic mail, file transfer, and terminal emulation

OSI Layers – Remembering Them!

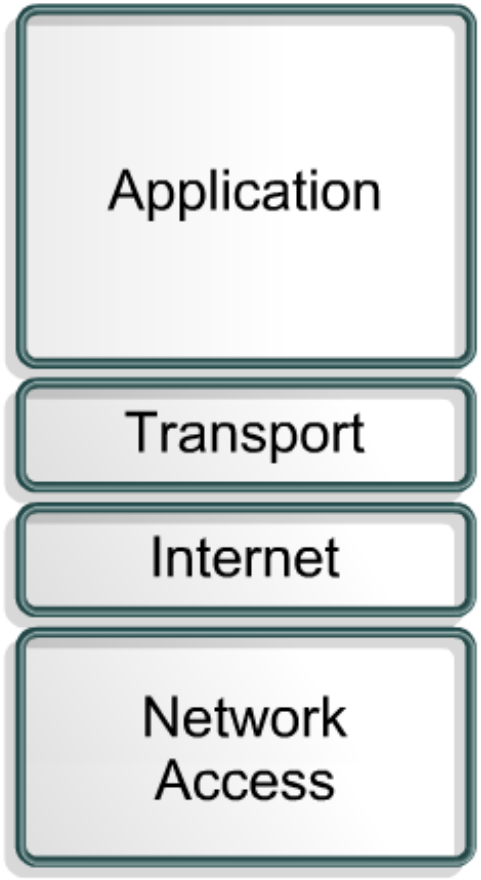
• Away	7 - Application
• Pizza	6 - Presentation
• Sausage	5 - Session
• Throw	4 - Transport
• Not	3 - Network
• Do	2 - Data Link
• Please	1 - Physical

Peer-to-Peer Communications



• In order for data to travel from the source to the destination, each layer of the OSI model at the source must communicate with its peer layer at the destination. This form of communication is referred to as peer-to-peer. During this process, the protocols of each layer exchange information, called protocol data units (PDUs). Each layer of communication on the source computer communicates with a layer-specific PDU, and with its peer layer on the destination computer.

TCP/IP Model



- The TCP/IP reference model is the historical and technical standard of the Internet.
- The U.S. Department of Defense (DoD) created the TCP/IP reference model, because it wanted to design a network that could survive any conditions, including a nuclear war.
- TCP/IP was developed as an open standard. This meant that anyone was free to use TCP/IP. This helped speed up the development of TCP/IP as a standard.
- Although some of the layers in the TCP/IP model have the same name as layers in the OSI model, the layers of the two models do not correspond exactly.
- The relationship between IP and TCP is an important one. IP can be thought to point the way for the packets, while TCP provides a reliable transport.

TCP/IP Model

Similarities include:

- Both have layers.
- Both have application layers, though they include very different services.
- Both have comparable transport and network layers.
- Both models need to be known by networking professionals.
- Both assume packets are switched.

TCP/IP Model

Differences include:

- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears simpler because it has fewer layers.
- TCP/IP protocols are the standards around which the Internet developed, so the TCP/IP model gains credibility just because of its protocols. In contrast, networks are not usually built on the OSI protocol, even though the OSI model is used as a guide.

TCP/IP Model

Although TCP/IP protocols are the standards with which the Internet has grown, we will also use the OSI model for the following reasons:

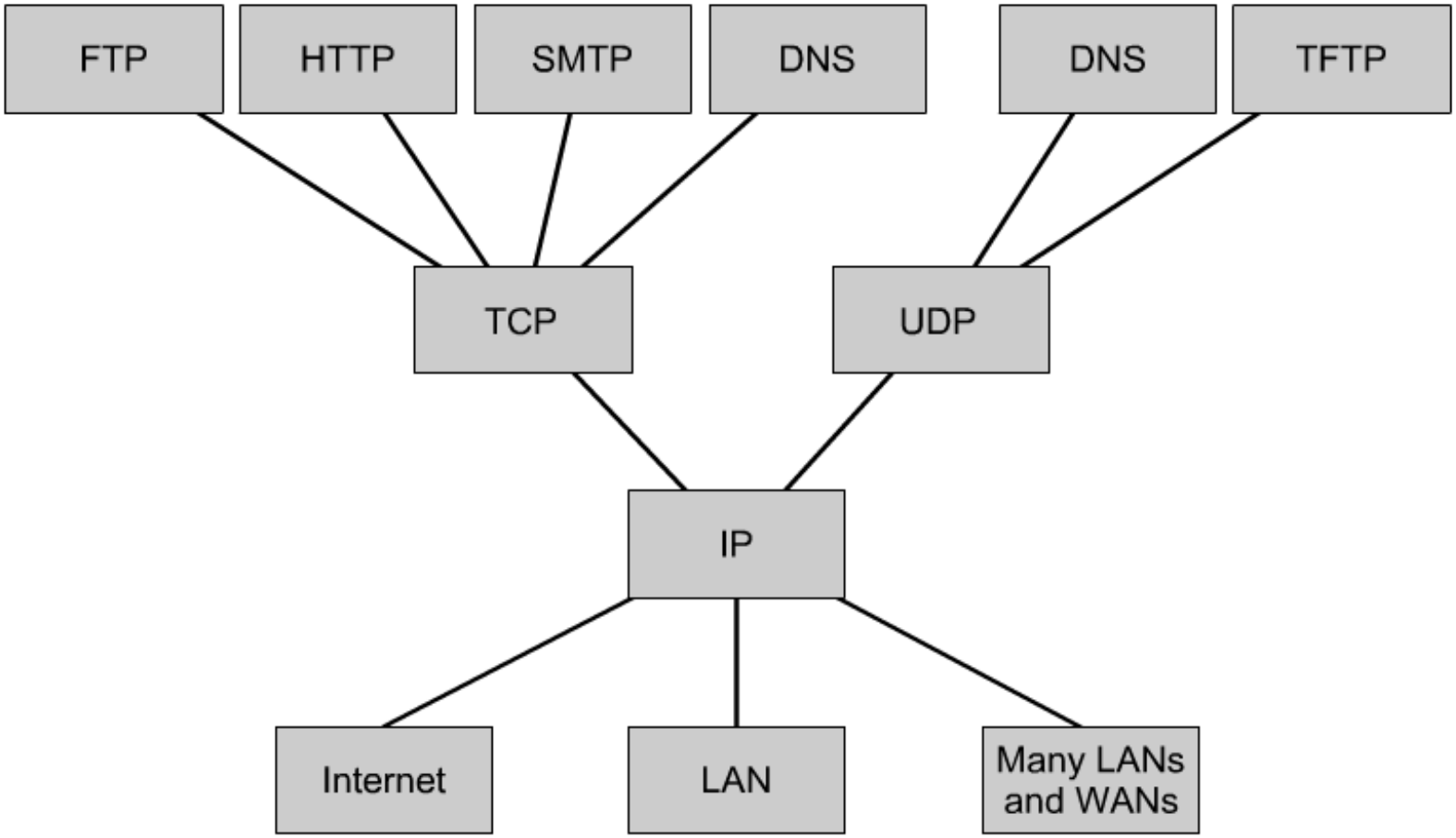
- It is a generic, protocol-independent standard.
- It has more details, which make it more helpful for teaching and learning.
- It has more details, which can be helpful when troubleshooting.

Networking professionals differ in their opinions on which model to use. Due to the nature of the industry it is necessary to become familiar with both. Both the OSI and TCP/IP models will be referred to with the focus on the following:

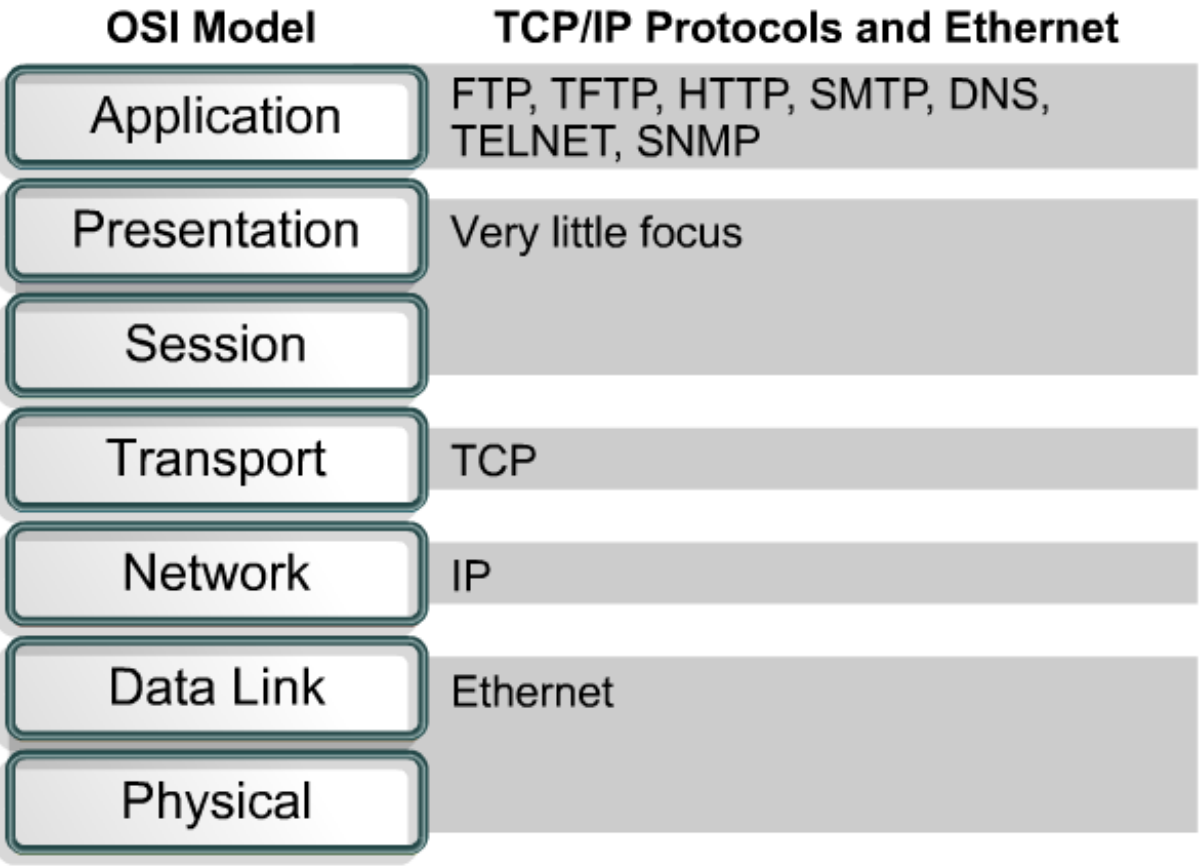
- TCP as an OSI Layer 4 protocol
- IP as an OSI Layer 3 protocol
- Ethernet as a Layer 2 and Layer 1 technology

Remember that there is a difference between a model and an actual protocol that is used in networking. The OSI model will be used to describe TCP/IP protocols.

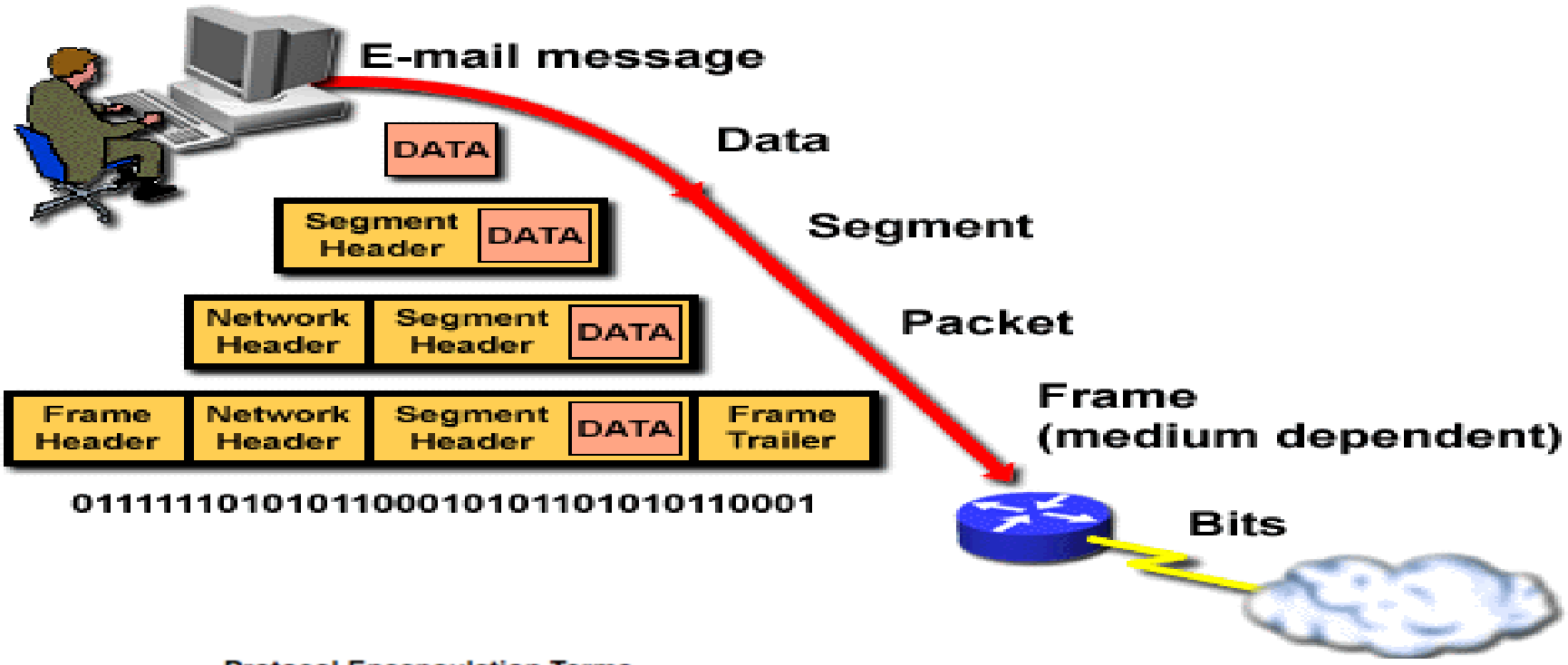
TCP/IP Model

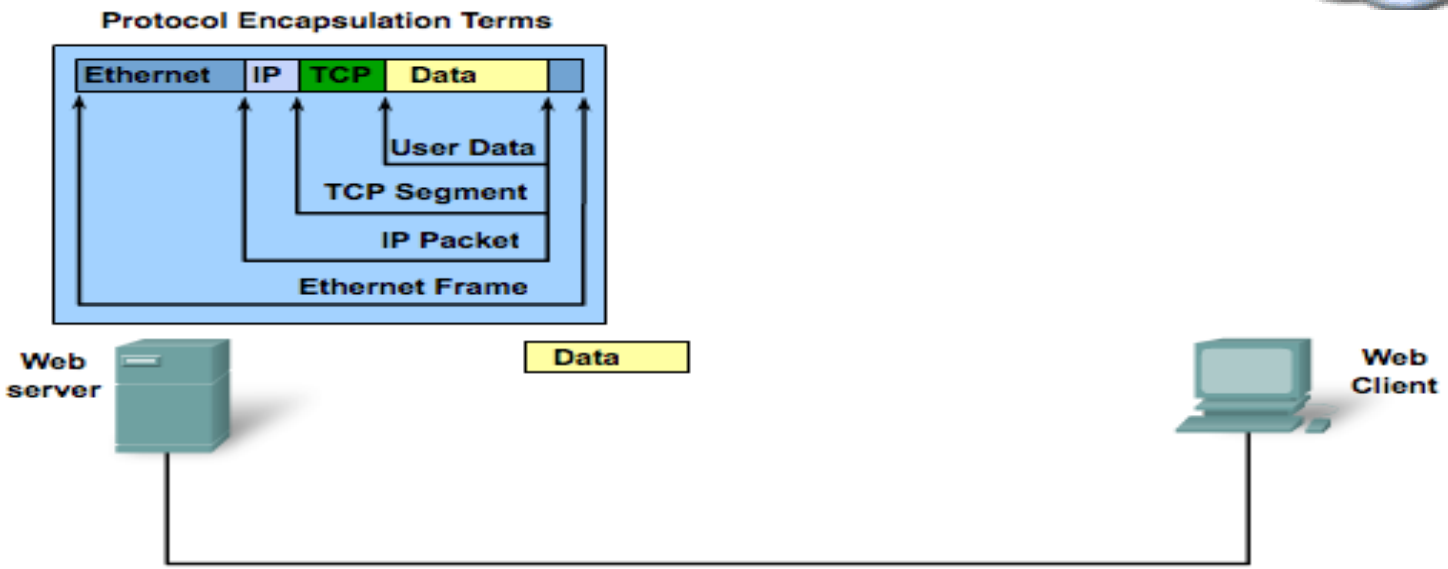

FTP
HTTP
SMTP
DNS
DNS
TFTP
TCP
UDP
IP
Internet
LAN
Many LANs and WANs

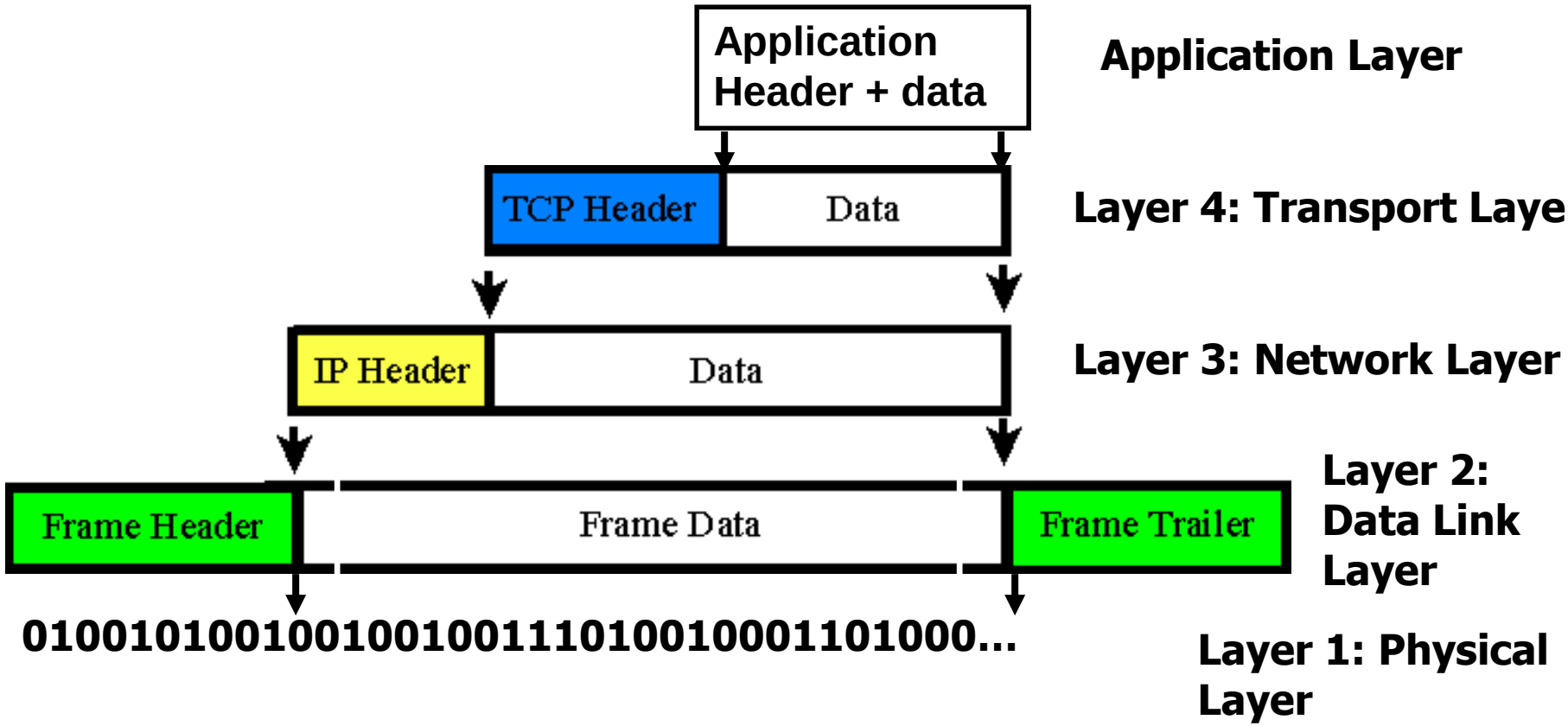
TCP/IP Model


OSI Model
TCP/IP Protocols and Ethernet
Application
FTP, TFTP, HTTP, SMTP, DNS, TELNET, SNMP
Presentation
Very little focus
Session
Transport
TCP
Network
IP
Data Link
Ethernet
Physical

Data Encapsulation Example



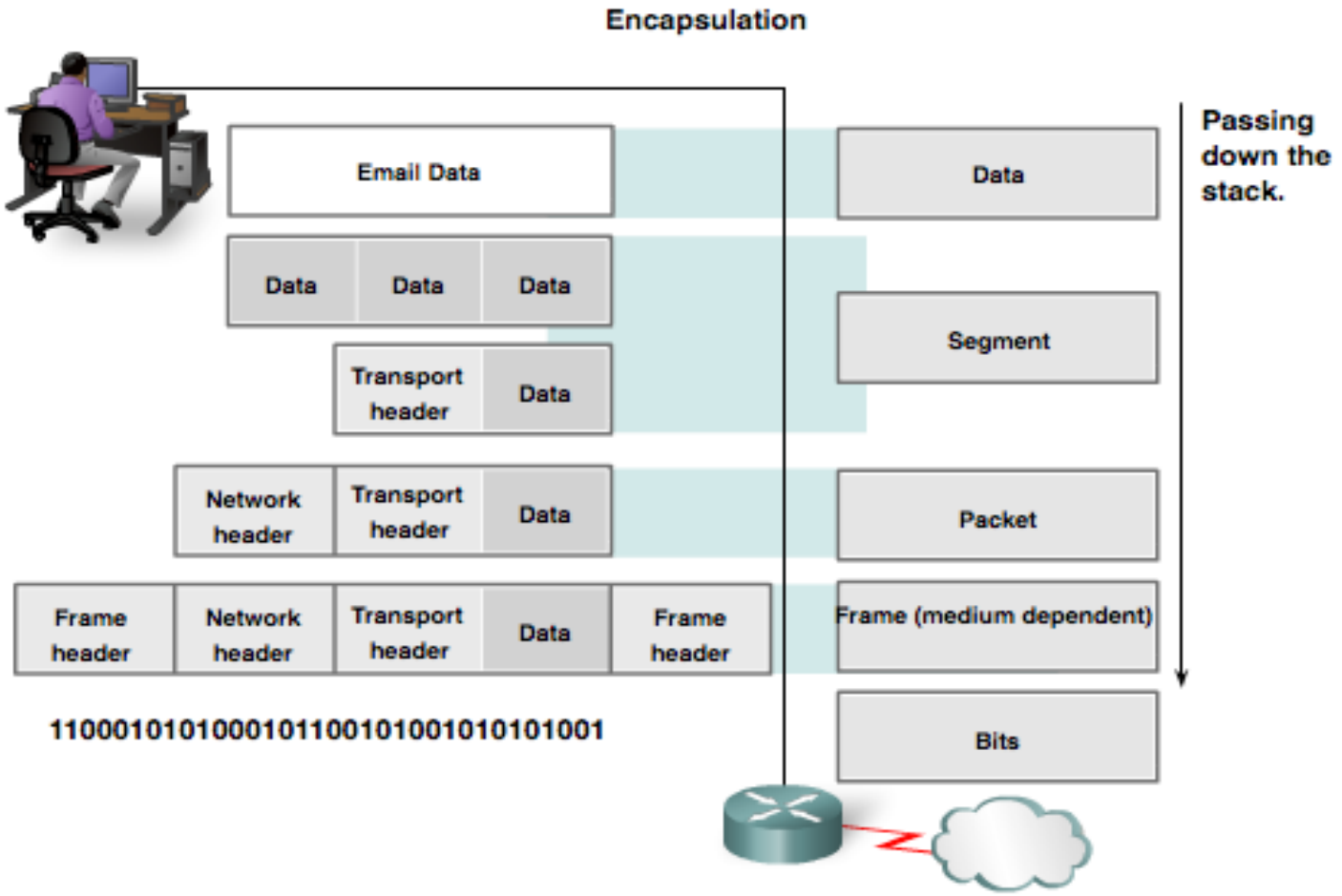



Application Header + data
Application Layer
TCP Header
Data
Layer 4: Transport Layer
IP Header
Data
Layer 3: Network Layer
Frame Header
Frame Data
Frame Trailer
Layer 2: Data Link Layer
0100101001001001001110100100011010000...
Layer 1: Physical Layer

Data Encapsulation

Protocol Data Units (PDUs)

- Data
- Segment
- Packet
- Frame
- Bits

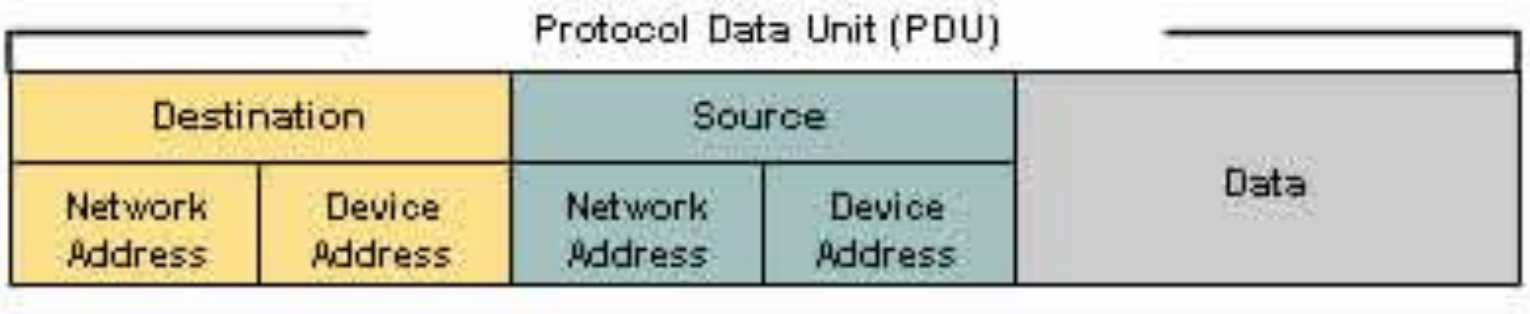


Getting Data to the End Device

- The host physical address, is contained in the header of the Layer 2 PDU, called a frame.
- Layer 2 is concerned with the delivery of messages on a single local network.
- The Layer 2 address is unique on the local network and represents the address of the end device on the physical media.
- In a LAN using Ethernet, this address is called the Media Access Control (MAC) address.
- When two end devices communicate on the local Ethernet network, the frames that are exchanged between them contain the destination and source MAC addresses.
- Once a frame is successfully received by the destination host, the Layer 2 address information is removed as the data is decapsulated and moved up the protocol stack to Layer 3.

Getting the Data Through the Internetwork

- Layer 3 protocols are primarily designed to move data from one local network to another local network within an internetwork.
- Layer 3 addresses must include identifiers that enable intermediary network devices to locate hosts on different networks
- At the boundary of each local network, an intermediary network device, usually a router, decapsulates the frame to read the destination host address contained in the header of the packet, the Layer 3 PDU
- Routers use the network identifier portion of this address to determine which path to use to reach the destination host.

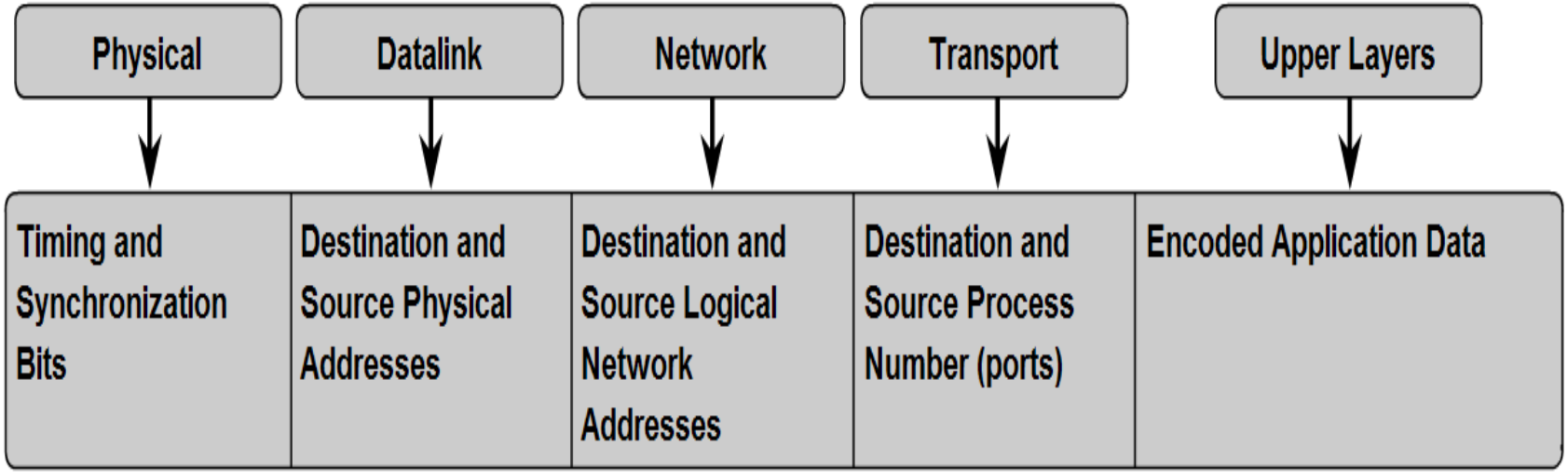


Getting Data to the Right Application

- Think about a computer that has only one network interface on it. How to differentiate various type of data?
- Each application or service is represented at Layer 4 by a port number
- When the data is received at the host, the port number is examined to determine which application or process is the correct destination for the data
- Example of popular port numbers?

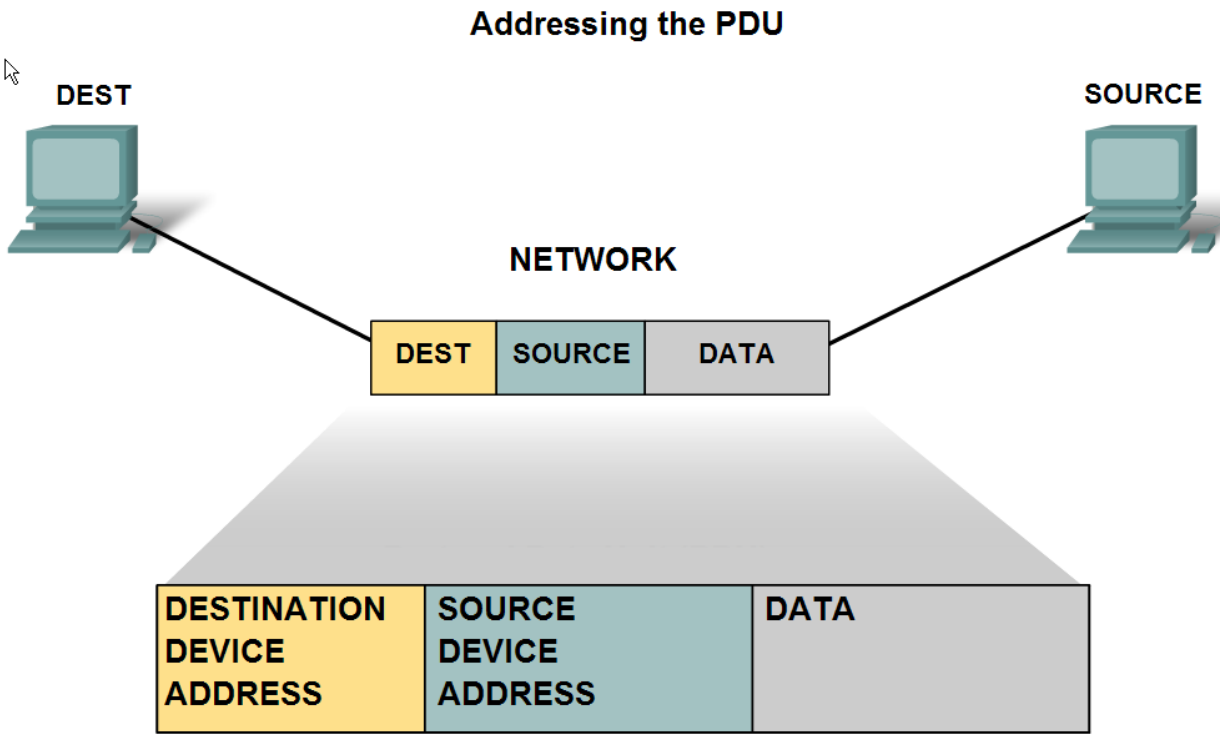
Addressing and Naming Schemes

- **How are labels in encapsulation headers are used to manage communication in data networks**



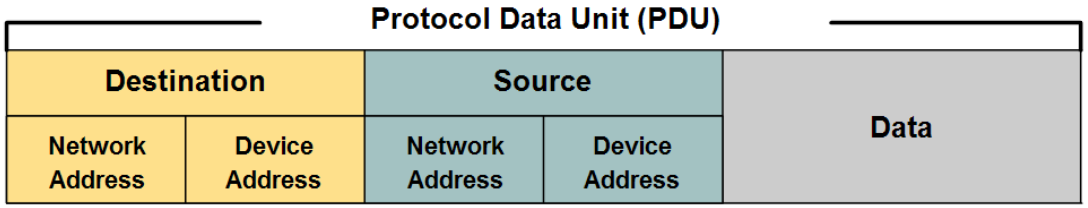
Addressing and Naming Schemes

- **Describe examples of Ethernet MAC Addresses, IP Addresses, and TCP/UDP Port numbers**

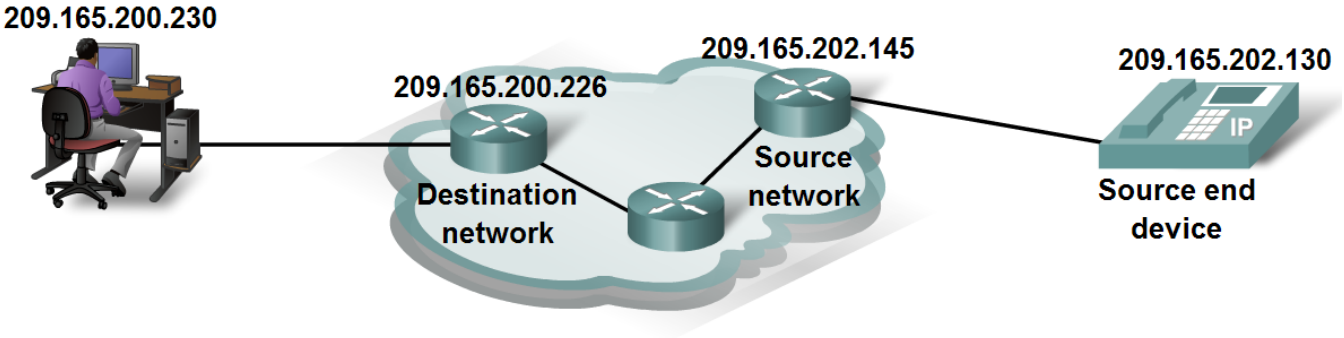


Addressing and Naming Schemes

- **Labels are used in encapsulation headers to manage communication in data networks**

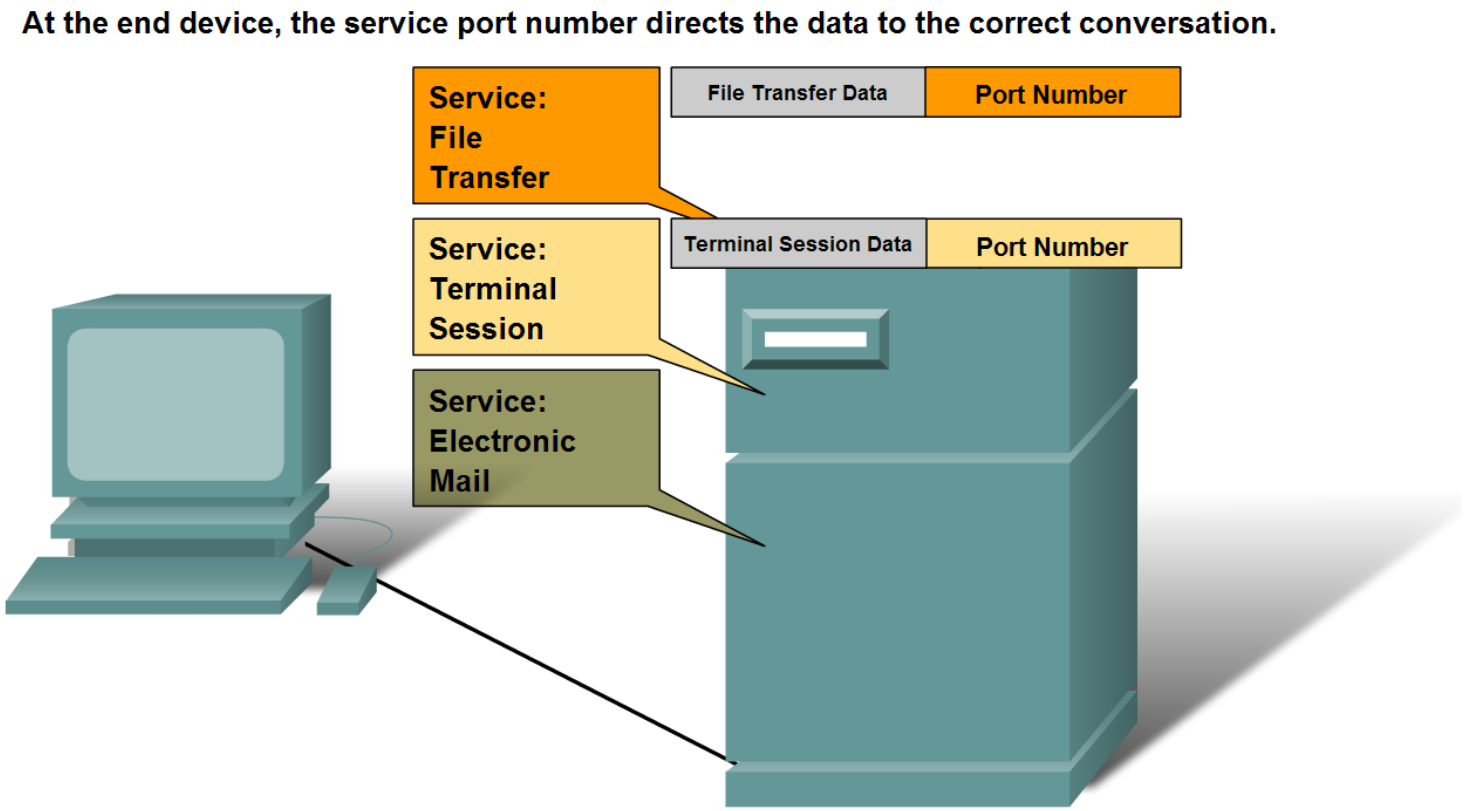


The Protocol Data Unit header also contains the network address.



Addressing and Naming Schemes

- **Information in the encapsulation header is used to identify the source and destination processes for data communication**



Questions ?

- **Today there are fewer commonly used protocols at the transport, network and data link layers than during the 90s. Why do you think this has happened ?**
- **Today there are more commonly used protocols at the application layer than during the 90s. Why do you think this has happened ?**

References

- **Cisco Internetworking Technologies Handbook**
  http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html

- **IBM Redbook - TCP/IP Tutorial**
  http://www.redbooks.ibm.com/abstracts/gg243376.html

- **Introduction to Networking on Youtube**

http://www.youtube.com/watch?v=rL8RSFQG8do&feature=related

LIBRARY BOOKS

Computer Networking – A Top-Down Approach Featuring the Internet, International Ed., Kurose & Ross, 0-321-22735-2

Distributed Systems and Networks William Buchanan McGraw Hill 0-07-709583-9

Computer Networks and Internets D.Comer

Any CCNA Book/Study guide