Lecture 1

Network Fundamentals

Objectives

Network Fundamentals

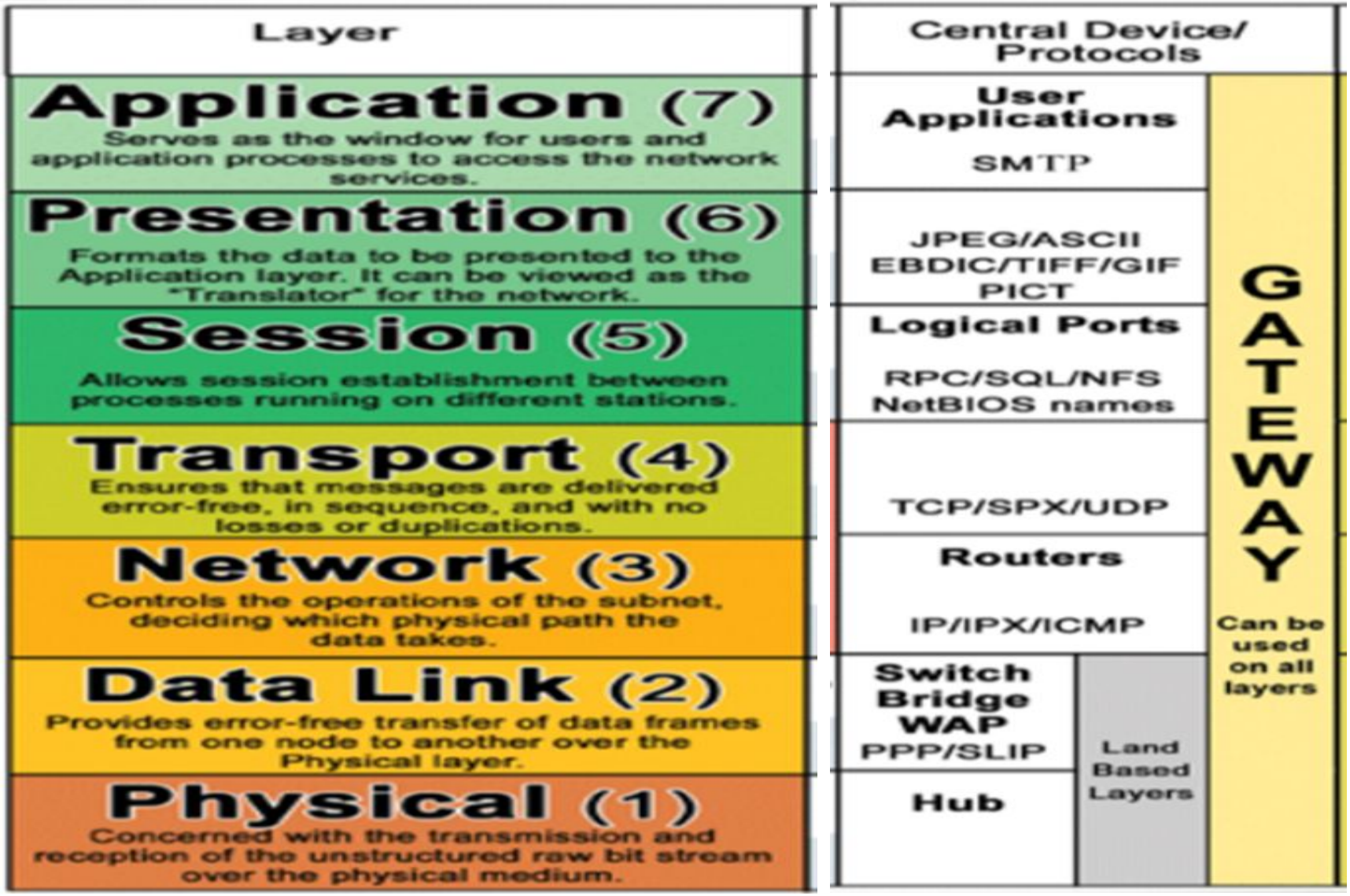
resolving the standards dilemma
multiple incompatible standards

standardizes the internal functions
partitioning it into abstraction layers

a device operates at a certain
layer
device implements the
functionality of that layer

The Open Systems Interconnection model (OSI)

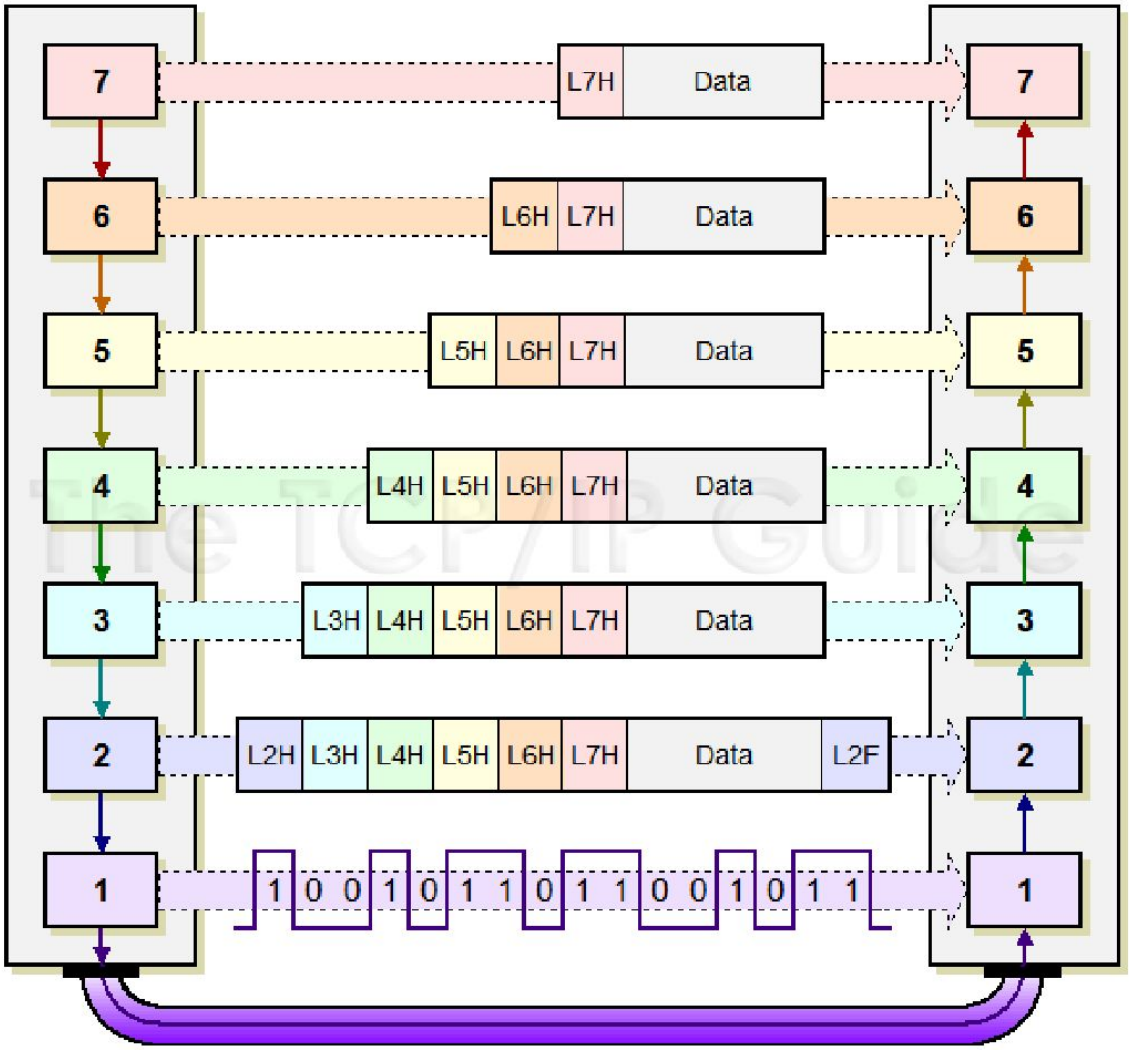
OSI Model


Layer
Application (7)
Serves as the window for users and application processes to access the network services.
Presentation (6)
Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.
Session (5)
Allows session establishment between processes running on different stations.
Transport (4)
Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.
Network (3)
Controls the operations of the subnet, deciding which physical path the data takes.
Data Link (2)
Provides error-free transfer of data frames from one node to another over the Physical layer.
Physical (1)
Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.
Central Device/ Protocols
User Applications
SMTP
JPEG/ASCII
EBDIC/TIFF/GIF
PICT
Logical Ports
RPC/SQL/NFS
NetBIOS names
TCP/SPX/UDP
Routers
IP/IPX/ICMP
Switch
Bridge
WAP
PPP/SLIP
Hub
Land Based Layers
GATEWAY
Can be used on all layers

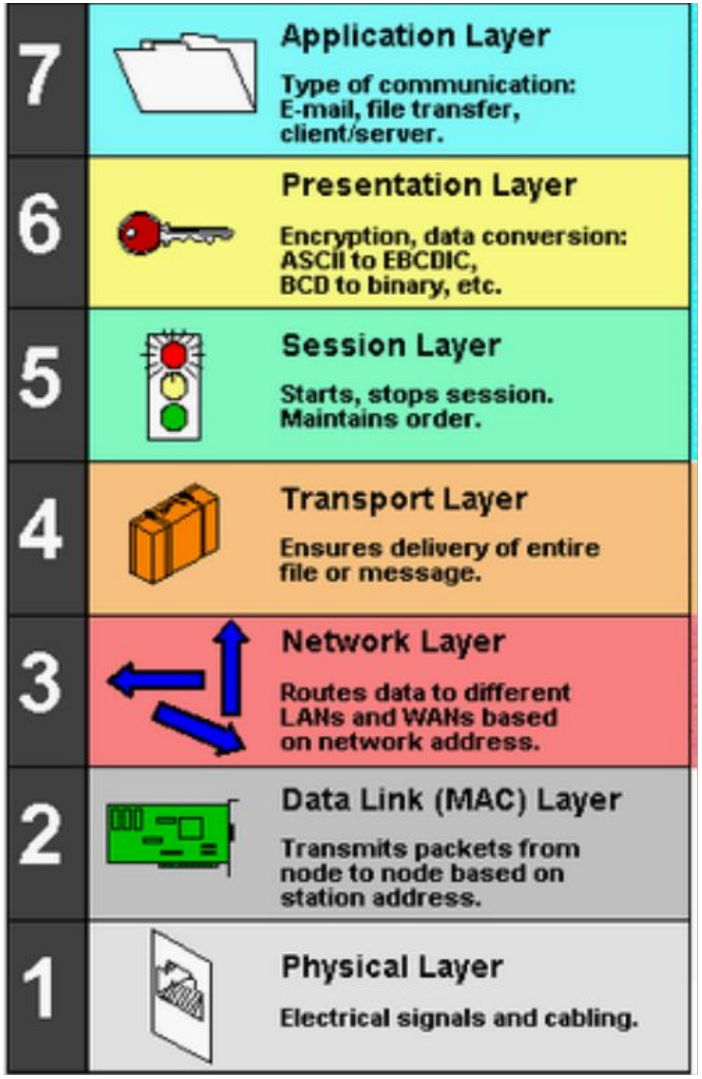
Communication between Layers

Moving from the top

Moving from the bottom



OSI Layer 1. Physical Layer



transmitting and receiving data over a transmission media

- **Transmission media**
- **Connector**
- **Data encoding and synchronization**
- **Transmission technique**

OSI Layer 1 functionality

Transmission medium

The path over which a data signal is carried. Transmission can be sent through a physical medium, such as copper wire or fiber optic cable, or it can be sent wirelessly using radio waves.

Connector

The Physical layer provides the direct connection between nodes (node - term used to refer to a connection point on a network, typically a computer or other network device).

OSI Layer 1 functionality

Data encoding

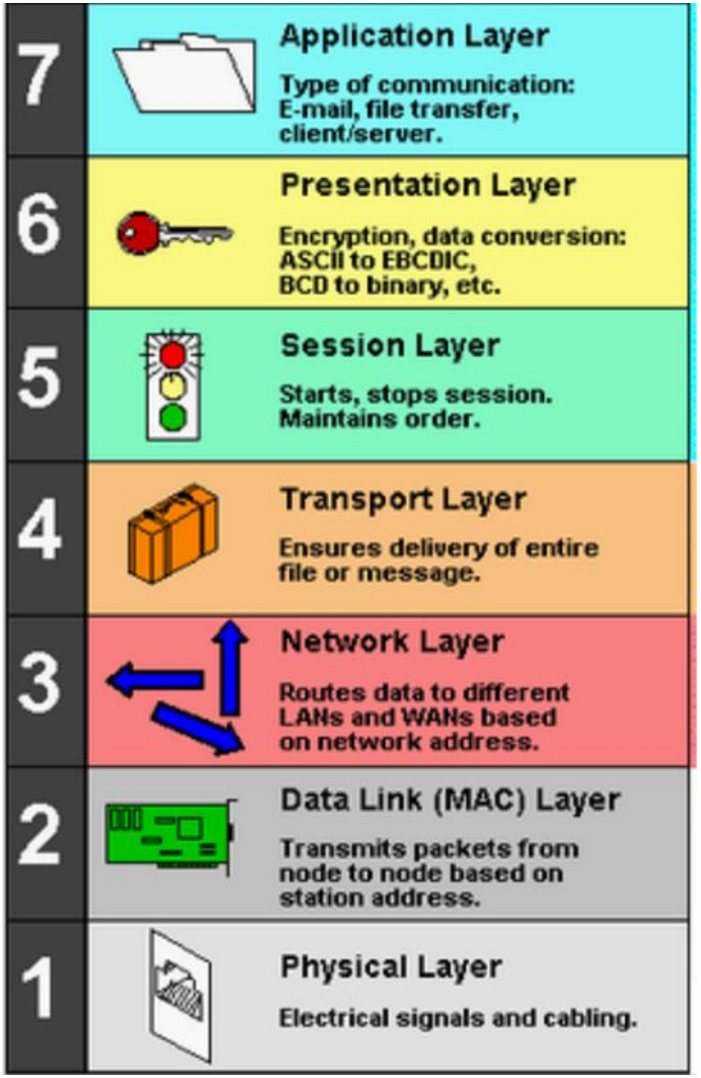
In the context of the Physical layer, it refers to converting data into a transmission format.

How to tell the start and end of a frame, and how data is synchronized.

Transmission technique

Physical layer also determine the transmission technique. Data can be sent using either a digital or analog transmission. Fiber optic transmissions, for example, are digital transmissions.

OSI Layer 2. Data Link Layer



ensuring that data is transmitted between nodes without errors

- **Link control**
- **Access management**
- **Traffic control**
  - Sequencing
    - Acknowledgement
      - Delimiting
        - Error correction

OSI Layer 2 functionality

Link control

terminates the link

Access management

OSI Layer 2 functionality

Traffic control

Sequencing

Acknowledgement

Delimiting

Error correction

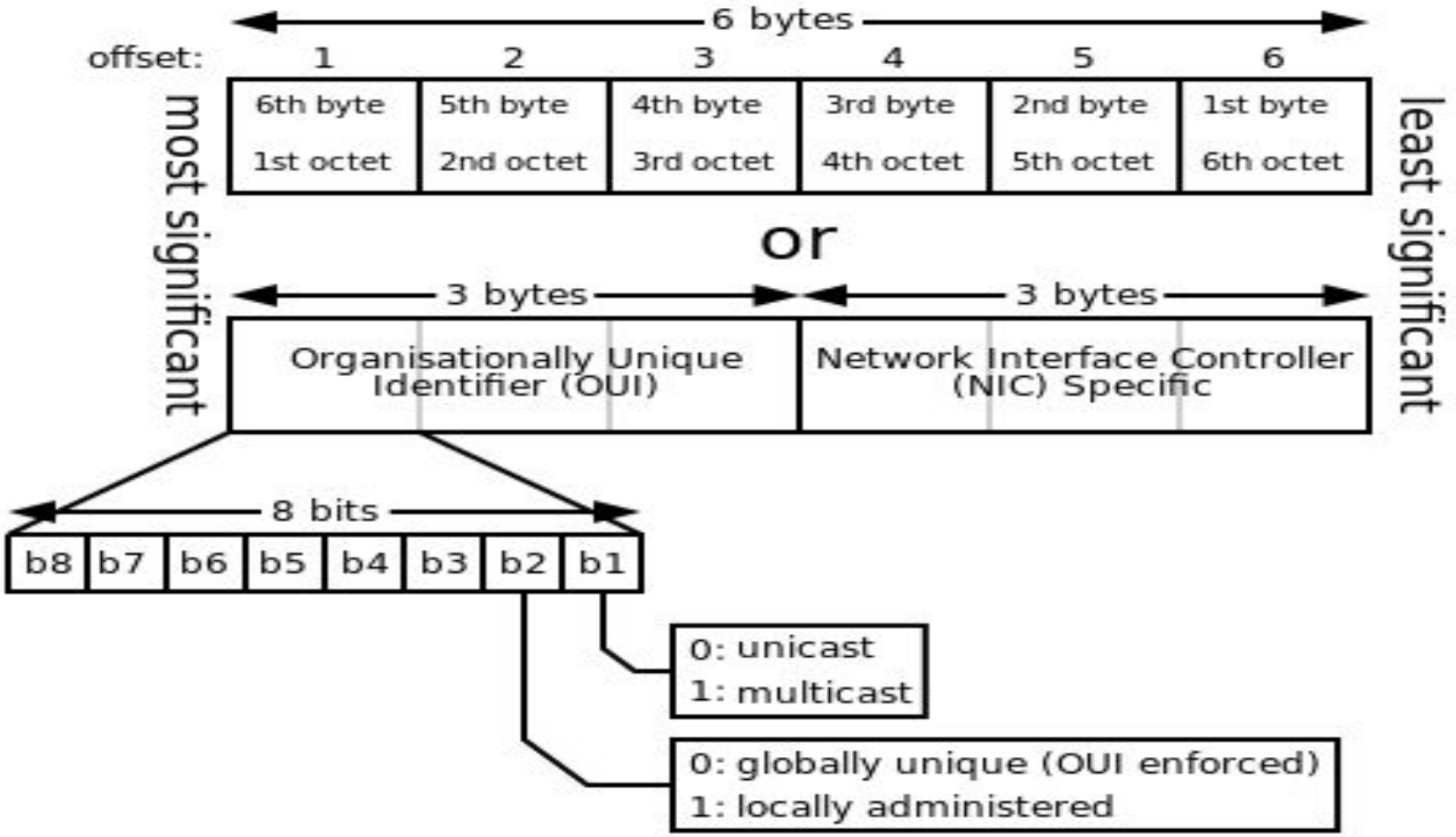
OSI Layer 2. MAC address

Media Access Control (MAC) address

The first three octets

The remaining three octets

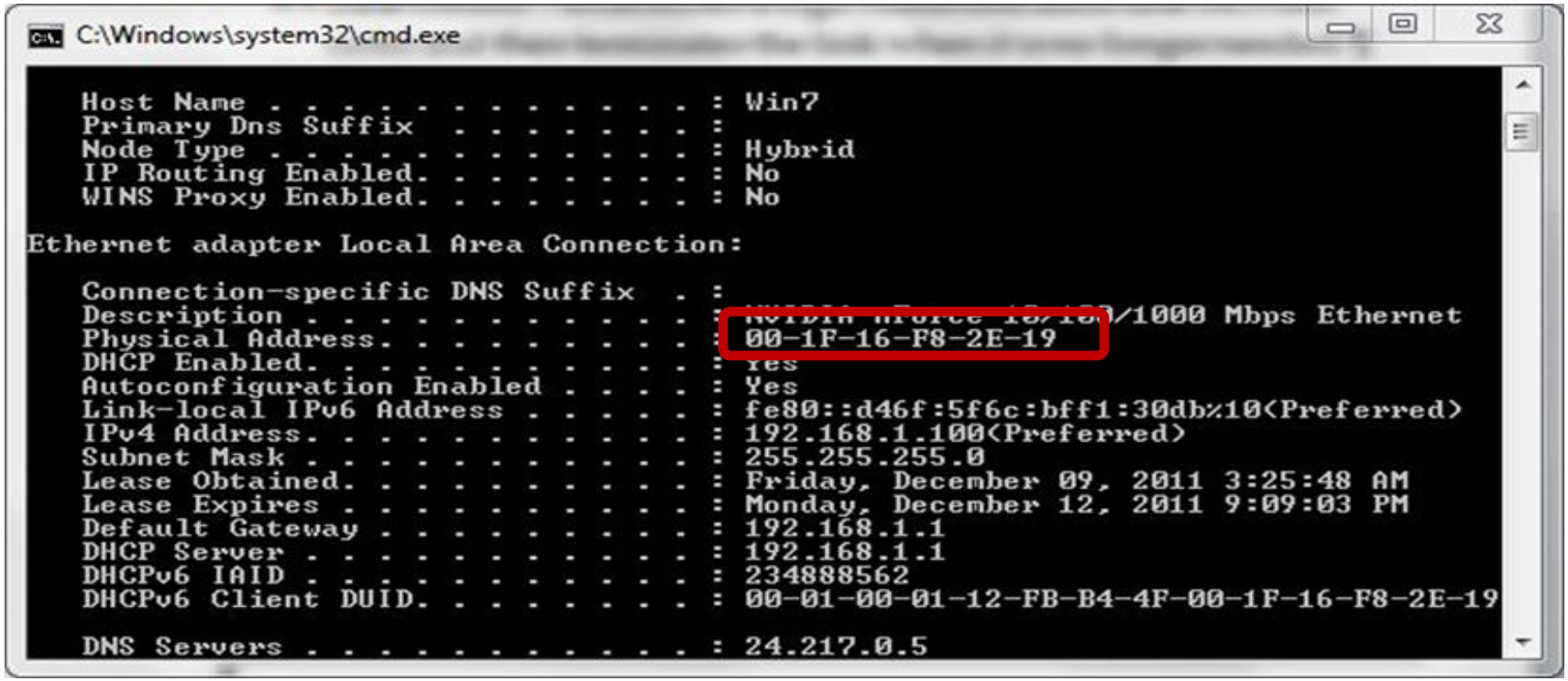
OSI Layer 2. MAC Address



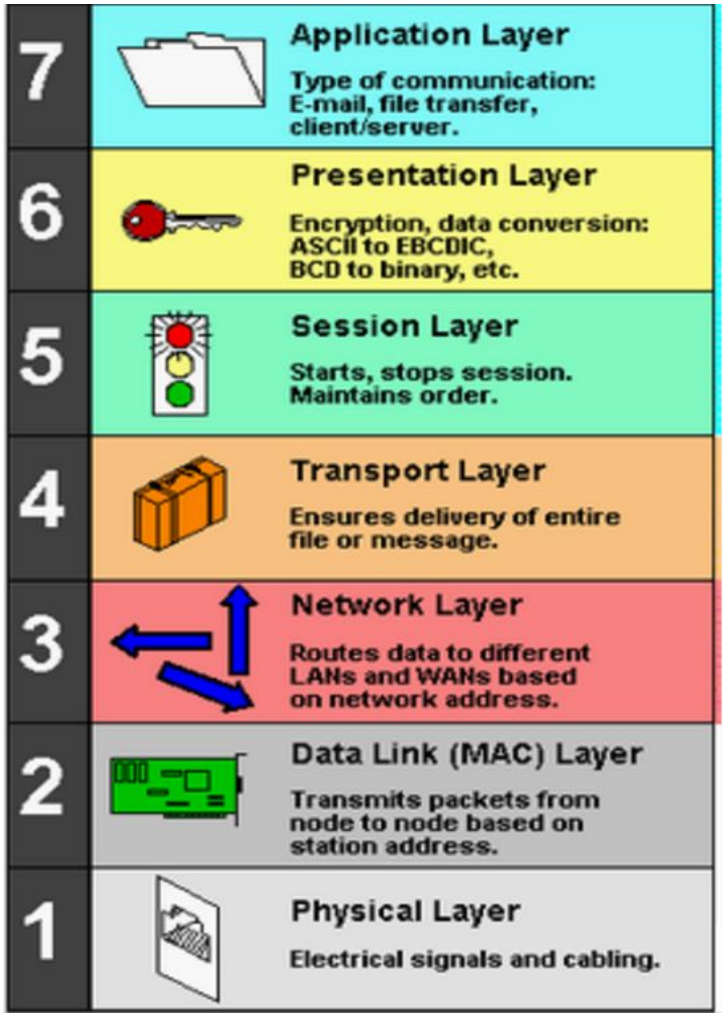
Adapter's physical address

ipconfig/all

adapter's physical address



OSI Layer 3. Network Layer



routed networks

- **Network address**
  - **Traffic routing**
    - **Fragmentation/ reassembly**

Network Address

is specified through device configuration

identifies the node and the subnetwork

123.20.210.3

01111011 00010100 11010010 00000011

OSI Layer 3 functionality

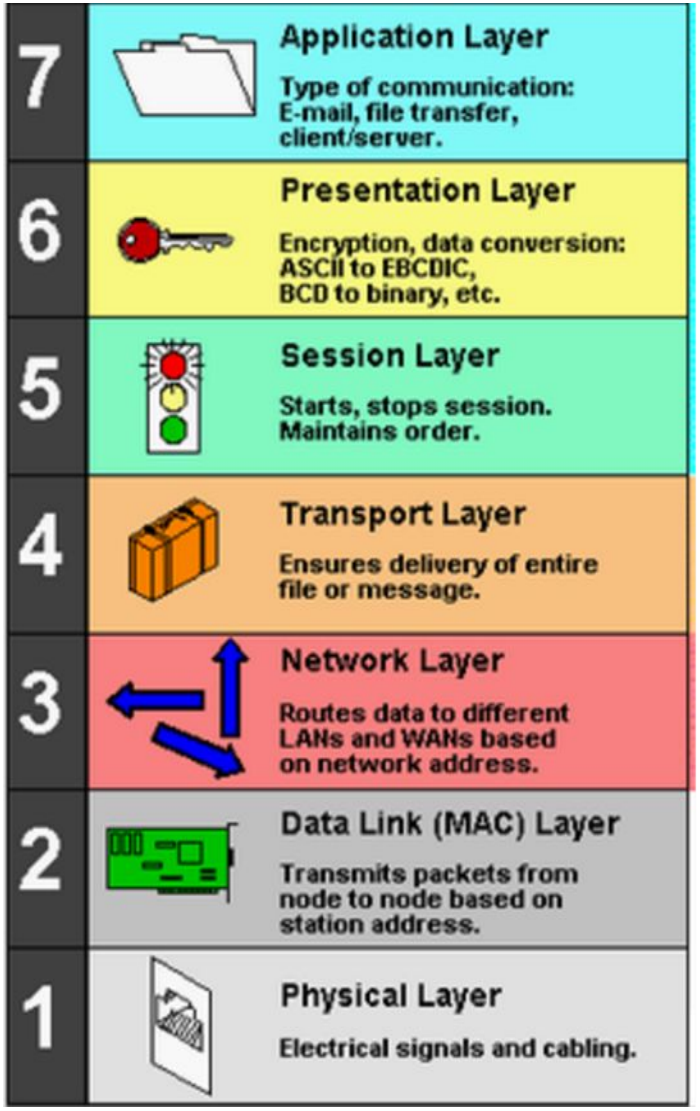
Traffic routing

for forwarding traffic between networks

Frag-men-tation/ reas-sembly

a smaller maximum transmission unit (MTU) size than others

OSI Layer 4. Transport Layer



layer is responsible for error-free delivery message

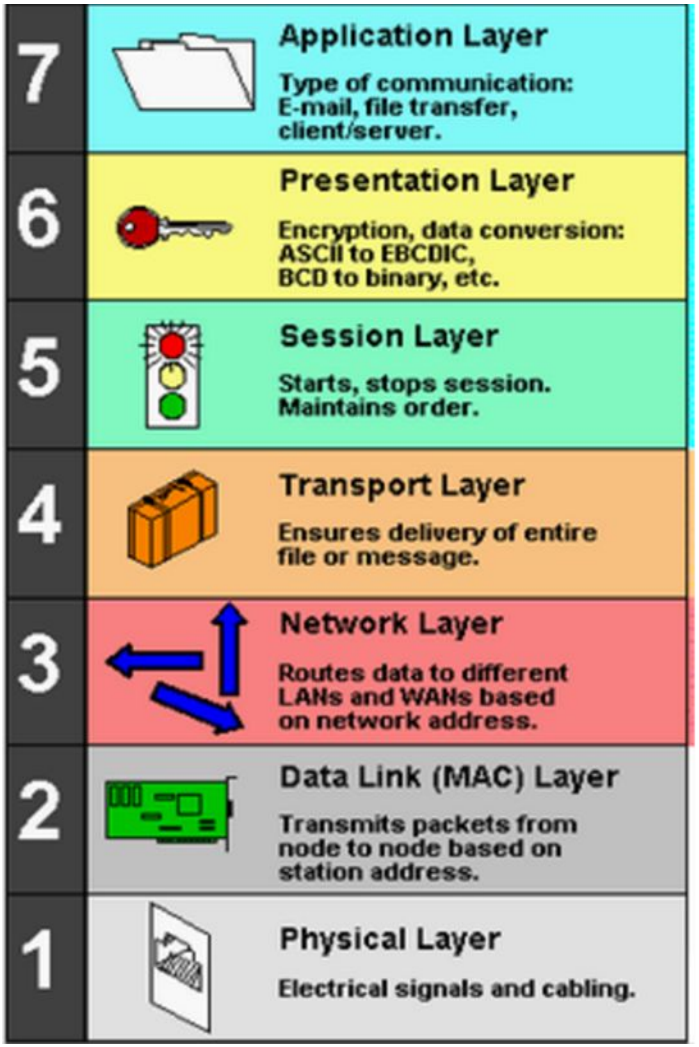
- **Segmentation**
- **Acknowledgement**
- **Traffic control**
- **Multiplexing**

Transport Layer functionality

Segmentation	• Splits the message (if necessary) for reassembly by the receiving Transport layer.
Acknowledgement	• Uses acknowledgements to provide reliable delivery.
Traffic control	• Enables transmission only when a message is available.
Multiplexing	• Manages transmission of multiple messages.

adds header information

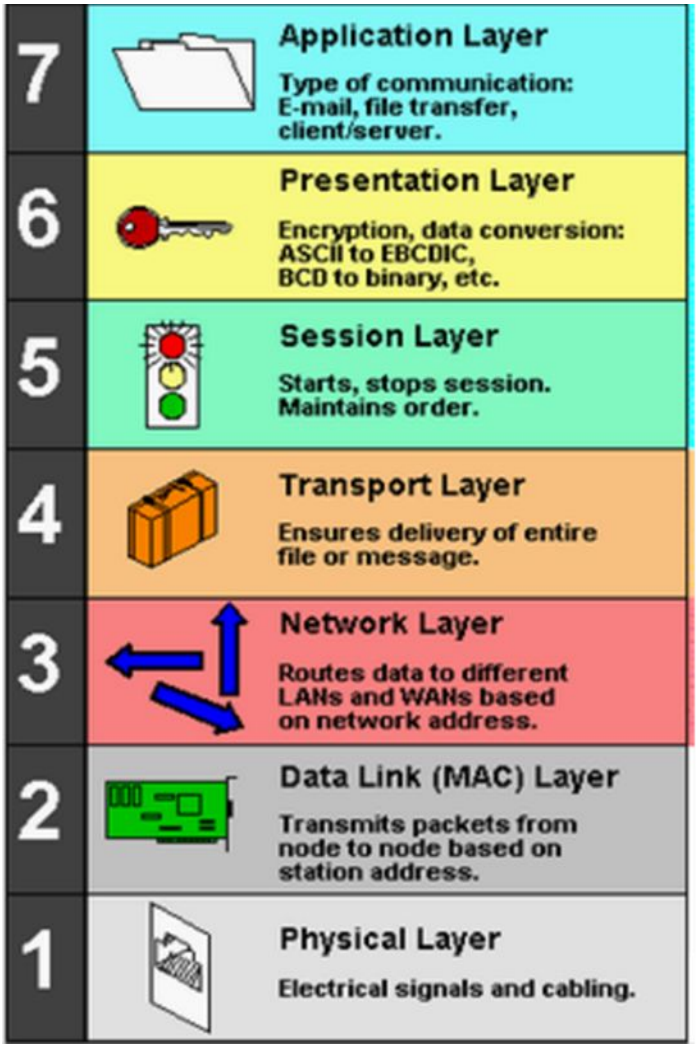
OSI Layer 5. Session Layer



to support the session

- Establishing sessions between hosts
- Managing/maintaining sessions
- Terminating sessions when it is no longer needed.

OSI Layer 6. Presentation Layer



layer is responsible for formatting data

- **Character translation**
  - ASCII
  - EBCDIC
- **Conversion**
- **Compression**
- **Encryption**

Presentation Layer functionality

Character translation

Typically American Standard Code for Information Interchange (ASCII) or Extended Binary Coded Decimal Interchange Code (EBCDIC).

Conversion

As necessary, including bit order, format-ti ng end of line, and so forth.

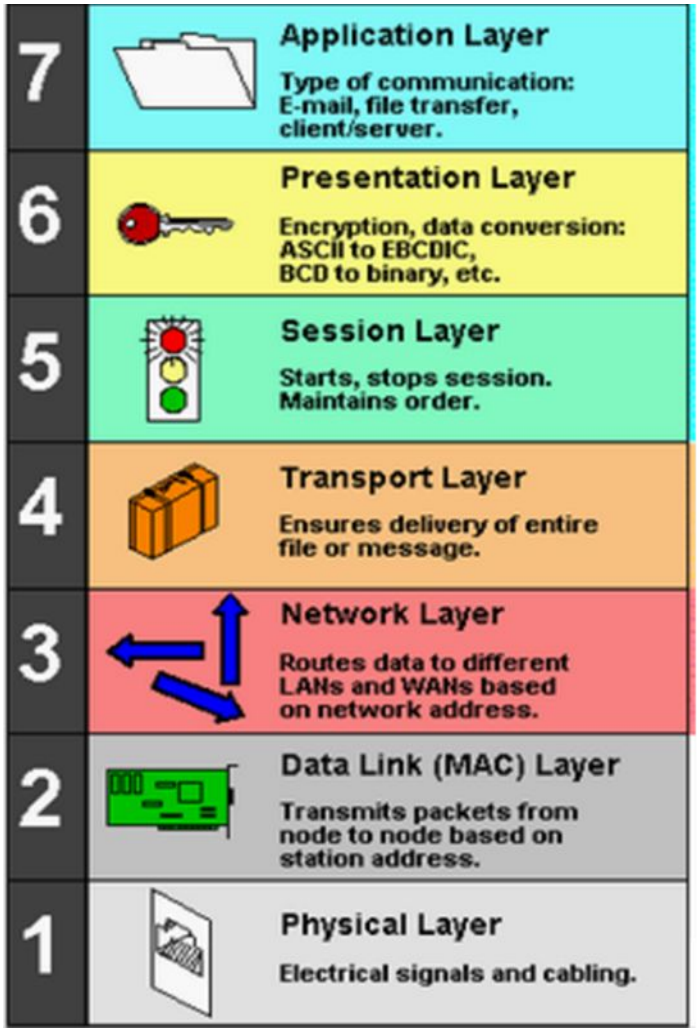
Compression

Applying data comp-ressi on algorithms to reduce the size of data being trans-mitt ed.

Encryption

Encryp-t ing/dec-r ypting data to provide data security.

OSI Layer 7. Application Layer



access to network services

- **Remote file and printer access**
- **Resource sharing**
- **Communications between processes**
- **Electronic messaging and e-mail**
- **Directory services**
- **Virtual devices and virtual communications**
- **Web browsing**

Summary

- **Layer 1, the Physical layer, is responsible for data transmission at the transmission media level.**
- **Layer 2, the Data Link layer, is responsible for low-level link control and traffic control.**
- **Layer 3, the Network layer, is responsible for network addressing and routing traffic through a network.**
- **Layer 4, the Transport layer, is responsible for ensuring error-free message delivery.**
- **Layer 5, the Session layer, establishes and manages communication sessions between hosts.**
- **Layer 6, the Presentation layer, is responsible for data translation and formatting.**
- **Layer 7, the Application layer, provides users and applications with access to networking functionality and network services.**

Network Fundamentals

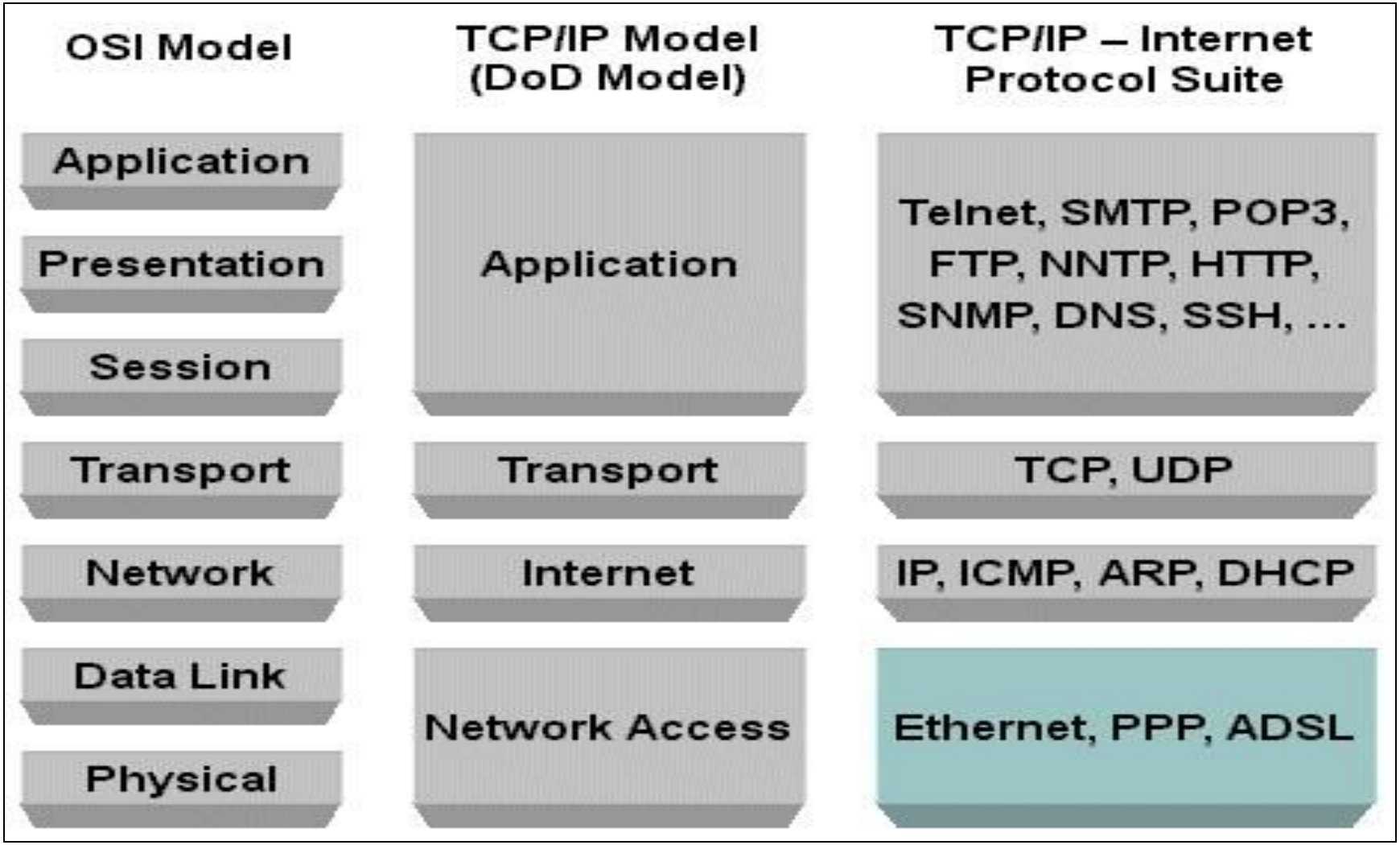
DARPA (Defense Advanced Research Projects Agency) model

Internet Protocol Suite

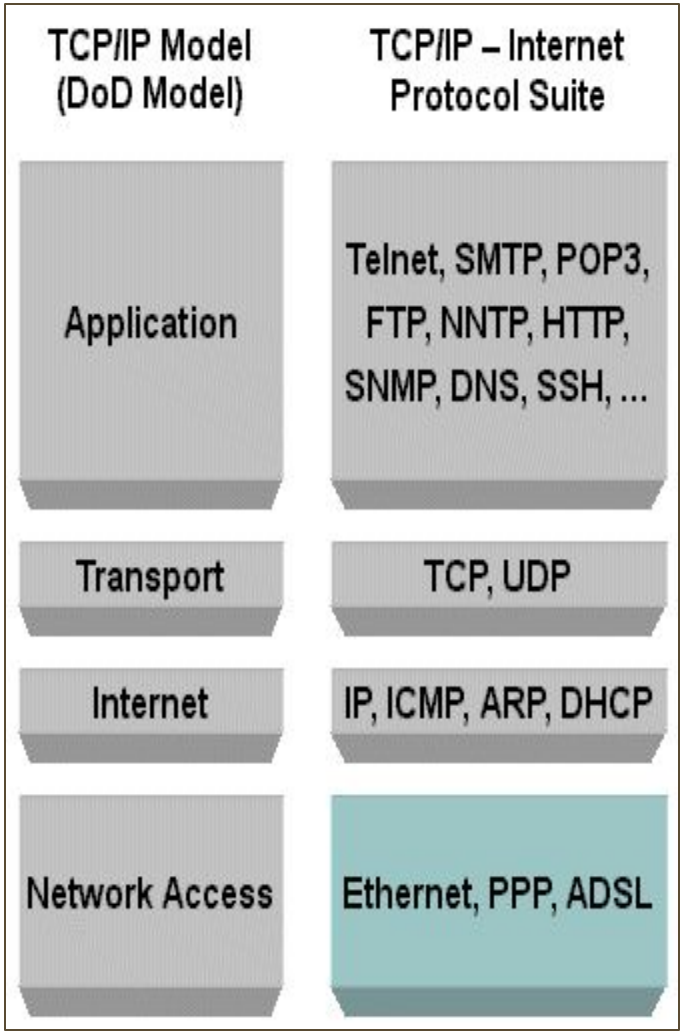
four abstraction layers

The Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP Model


OSI Model
TCP/IP Model (DoD Model)
TCP/IP – Internet Protocol Suite
Application
Presentation
Session
Application
Telnet, SMTP, POP3, FTP, NNTP, HTTP, SNMP, DNS, SSH, …
Transport
Transport
TCP, UDP
Network
Internet
IP, ICMP, ARP, DHCP
Data Link
Physical
Network Access
Ethernet, PPP, ADSL

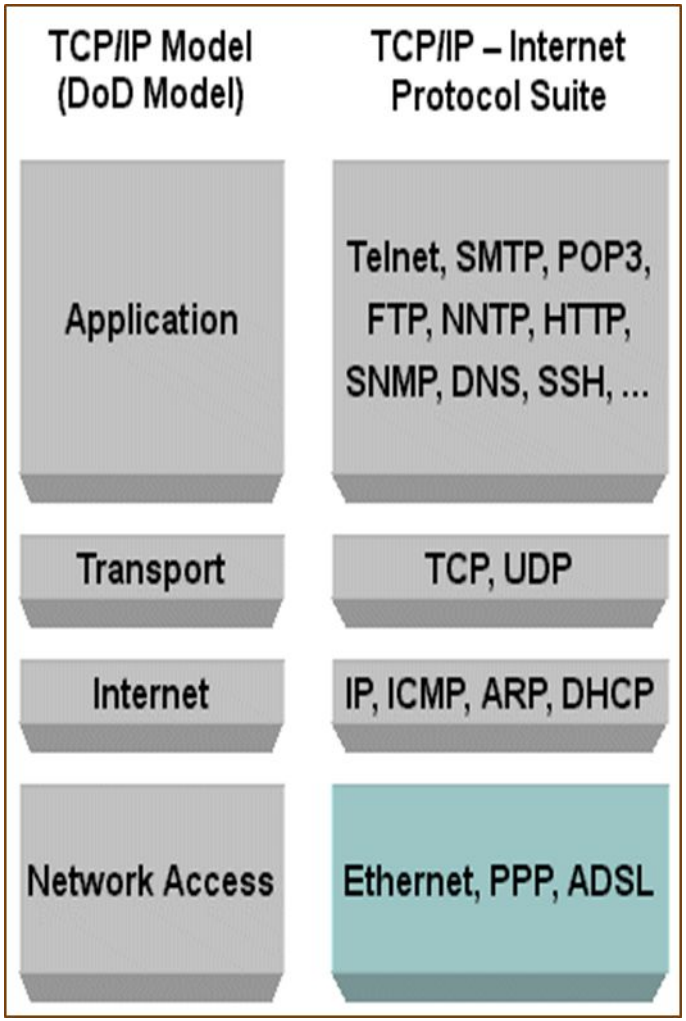
TCP/IP Model. Network Access Layer



- **Implementation of OSI Physical and Data Link layers.**
- **Hosts identified by MAC address.**
- **A wide range of low-level protocols.**

- **Sequencing**
- **Acknowledgement**

TCP/IP Model. Internet Layer



- **network addressing**
- **host addressing**
- **routing**
- **packaging data for transmission**
- **fragmenting packets for transmission and reassembling packets**

Internet Protocol version 4 (IPv4)

It is responsible for addressing and routing packets.

It is responsible for delivering packets from the source host to the destination host solely based on the IP addresses.

It is a connectionless protocol, so it does not establish a connection between the source and destination hosts.

Internet Protocol version 4 (IPv4)

uses a 32-bit address

192.168.10.42

Internet Protocol version 6 (IPv6)

extend the address space

fe80:bde1:d46f:5f6c:bff1:30db

Address Resolution Protocol (ARP)

deserves special mention is ARP

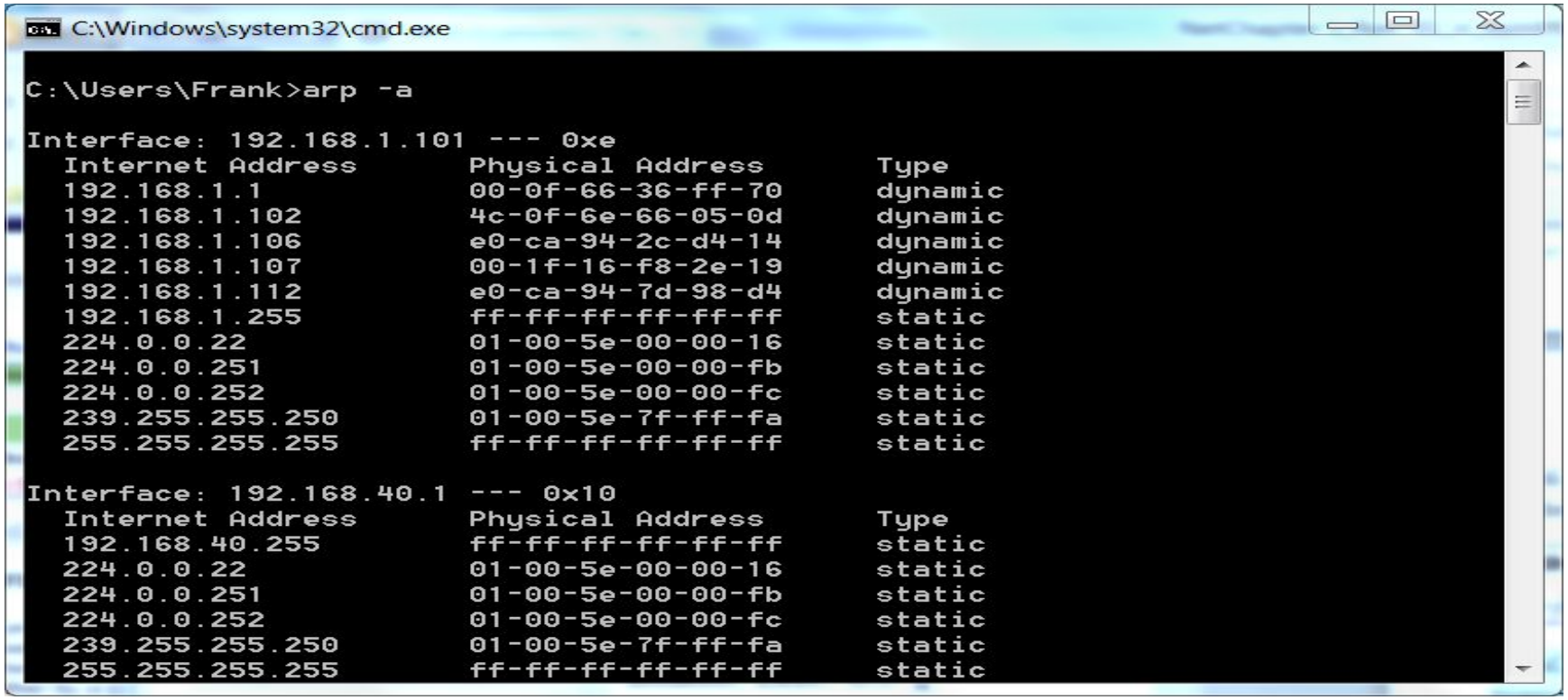
map IP addresses to MAC addresses

MAC address information is collected through the use of broadcast transmissions

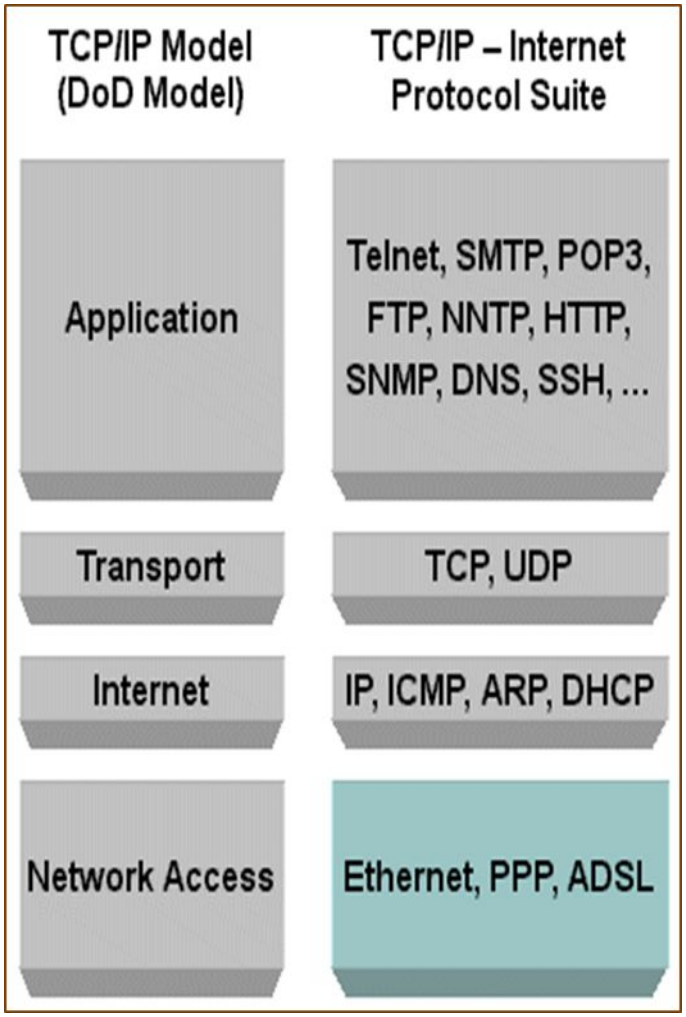
is maintained dynamically as the result of ARP broadcasts

ARP Command

arp -a



TCP/IP Model. Transport Layer



Provides datagram services for Application

TCP

- **Establishes connection between hosts**
- **Provides sequencing and acknowledgement**
- **Recovers lost packets through retransmission**

UDP

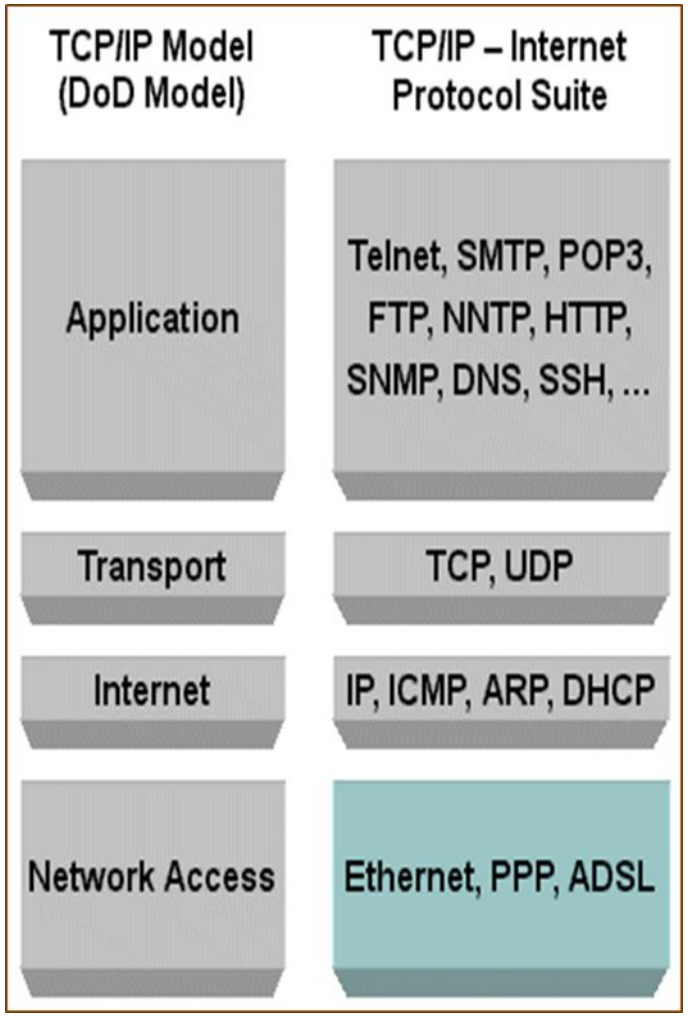
- **One-to-one or one-to-many transmissions**

TCP and UDP protocols

Transmission Control Protocol (TCP) is a connection-oriented protocol

User Datagram Protocol (UDP) is a connectionless protocol

TCP/IP Model. Application Layer



It is the interface between a computer's users and applications

Application layer protocols:

- **Telnet, SSH, SNMP (Simple Network Management Protocol), FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol) , DNS (Domain Naming System), DHCP (Dynamic Host Configuration Protocol).**

Summary

Network Fundamentals

Ethernet

family of computer networking technologies

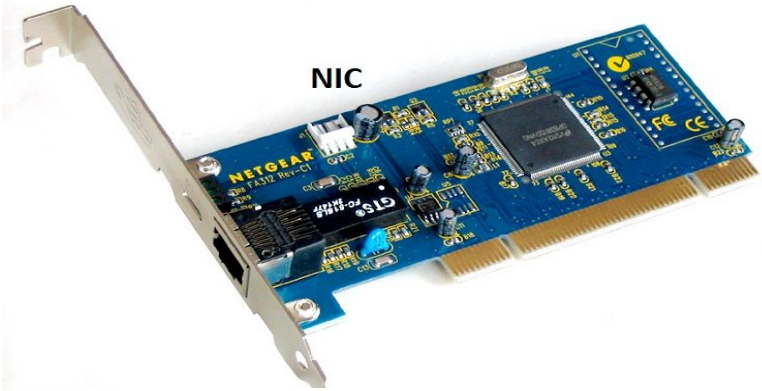
a low-level communication protocol

IEEE 802.3 standard

Ethernet History

was the clear winner

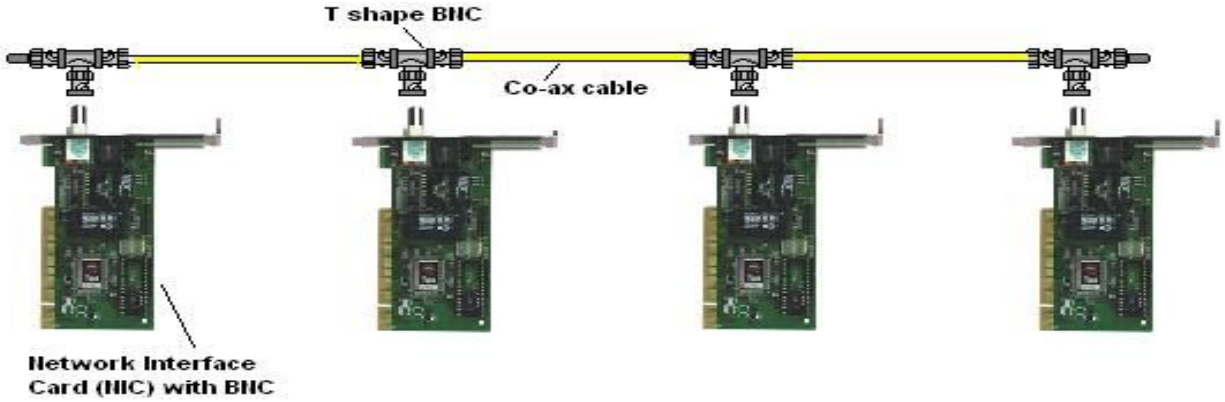
NIC



- **Transmission media and Connector types;**
- **Cable segment lengths;**
- **Transmission signals;**
- **Frame format;**
- **Network access method.**

Ethernet specifications

- **10Base5 – Thick Ethernet or thicknet**
- **10Base2 – Thin Ethernet or thinnet**



Current Ethernet standard

Name	Data rate	Standard	Note
10BaseT	**10 Mbps**	**802.3i**	**Requires two twisted pairs**
100BaseT	**100 Mbps**	**802.3u**	**Requires two twisted pairs**
1000BaseT	**1 Gbps**	**802.3ab**	**Requires four twisted pairs**
10GBaseT	**10 Gbps**	**802.3an**	**Requires four twisted pairs**

Ethernet Frame

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46(42)[b]–1500 octets	4 octets	12 octets
		← 64–1518(1522) octets →						

source and destination MAC addresses

1500 bytes of payload

entire frame size is 1518 bytes

Ethernet Traffic Types

Unicast

Broadcast

Multicast

Anycast

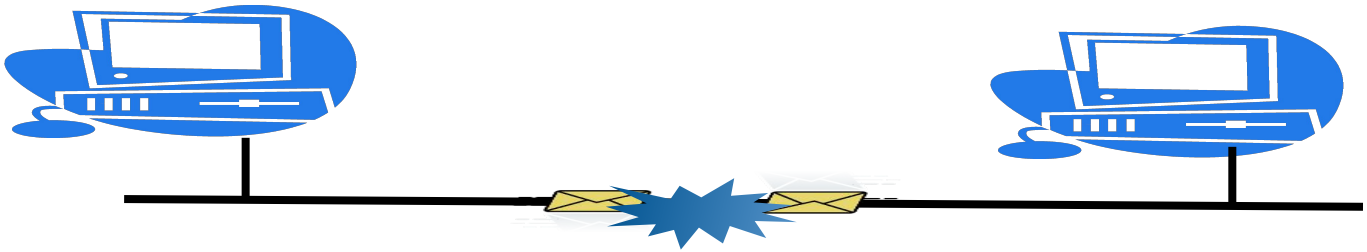
CSMA/CD

more than one host trying to transmit at the same time

collision

in older Ethernet networks

CSMA/CD



When a collision occurs:

- **All involved hosts will stop transmitting.**
- **Both frames are discarded.**
- **Both stations will wait a random time and attempt to transmit until successful.**

with a maximum transmission attempt count.

are built with switches

through the appropriate port at the switch

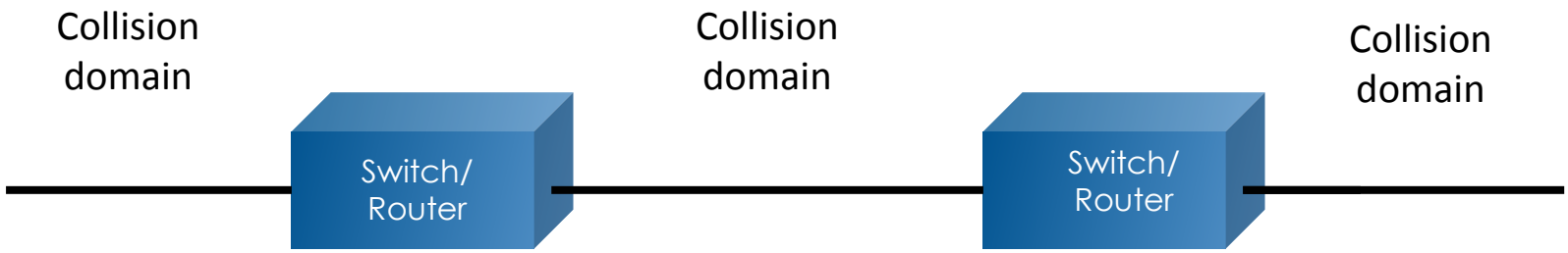
Collision Domain

network traffic communication devices

can control and segregate through

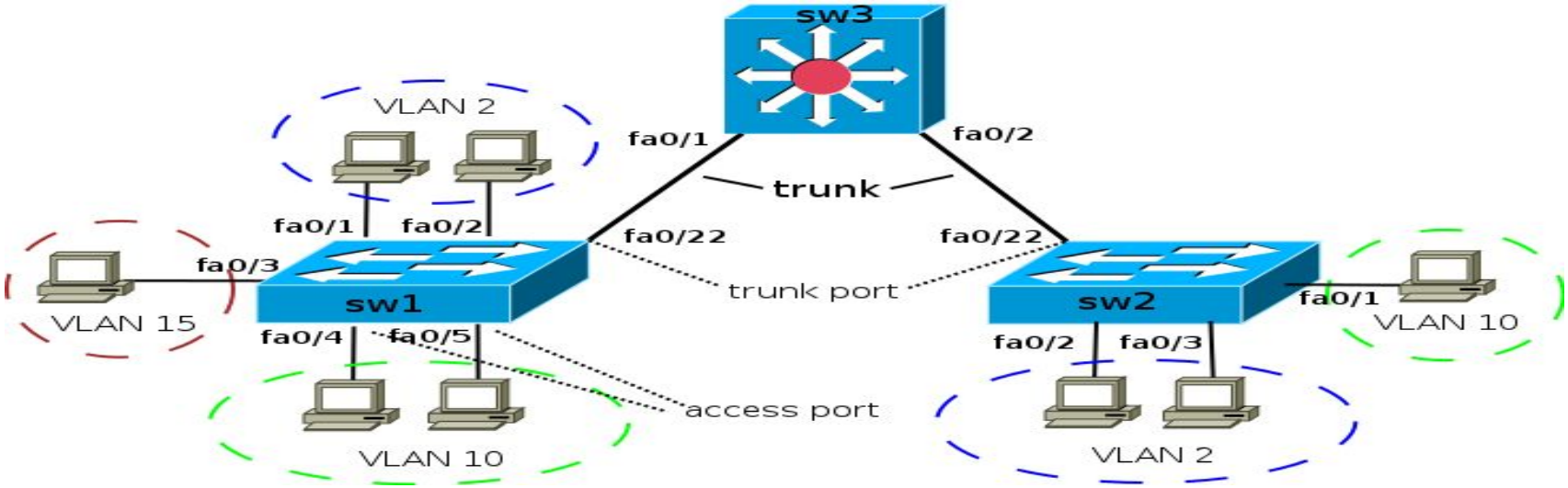
- Devices that operate at the Data Link layer manage traffic based on the MAC address.

- Devices that operate at the Network layer manage traffic based on the network address. IP address.



VLAN

segmentation through VLANs



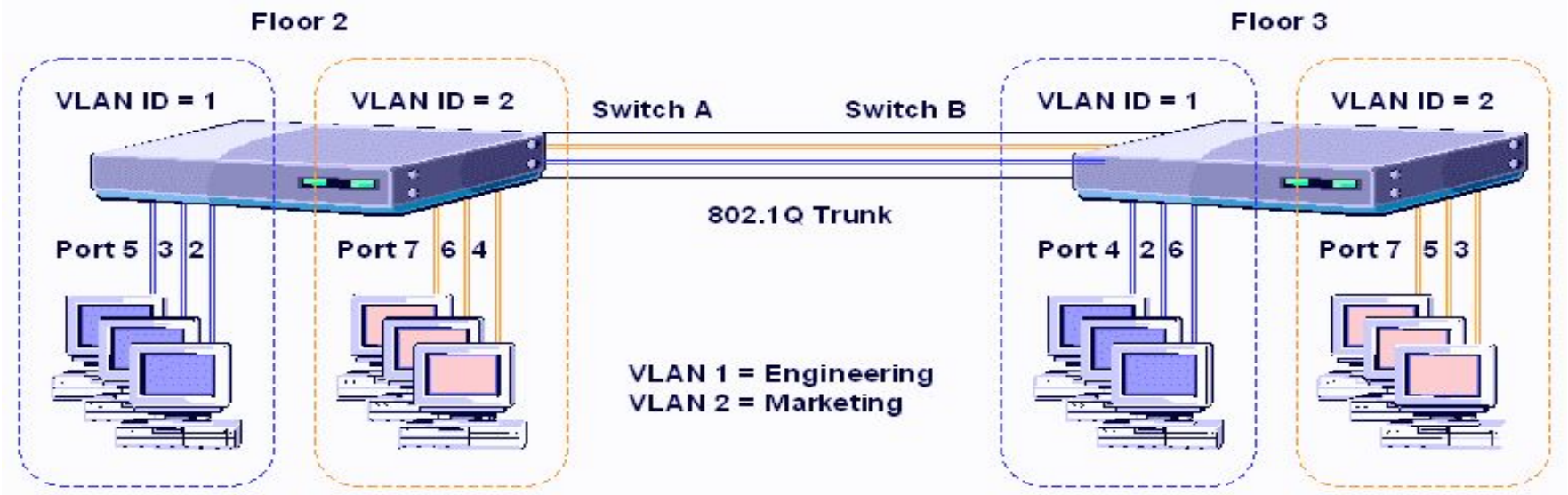
static VLAN

dynamically

VLAN and Ethernet

each frame

includes an 802.1Q tag



Summary

Network Fundamentals

Wireless Networking

that uses wireless data connections

using radio communication

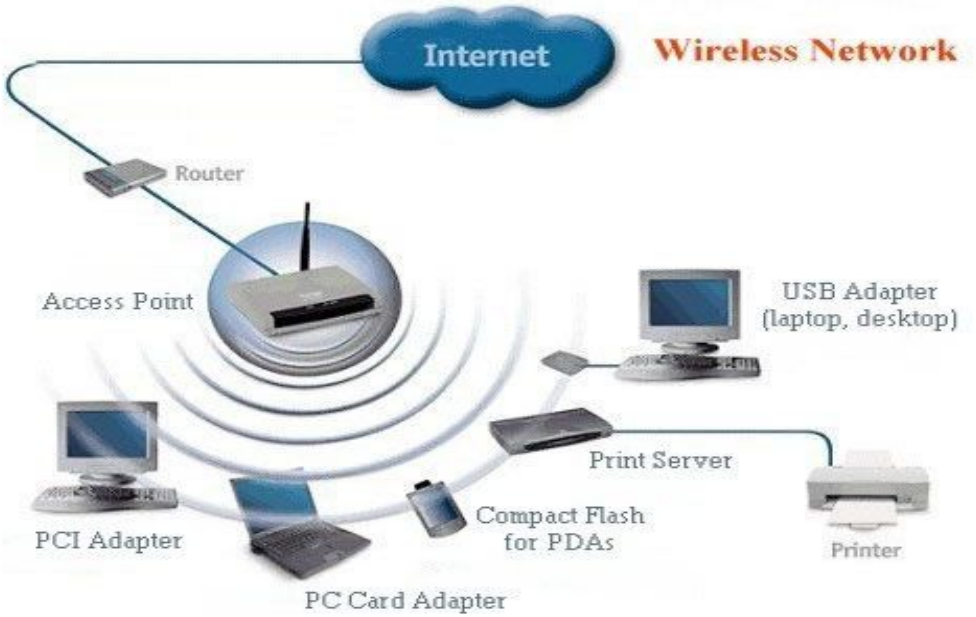
Defined by 802.11 standards

Current Wireless Standards

Standard	Frequency	Maximum data rate
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4/5 GHz	Up to 600 Mbps
802.11ac	5 GHz	Up to 1.3 Gbps

Wireless adapters

Access points



Most 802.11 wireless network configurations are based around one or more access points (APs).

Access method

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

to ensure the availability of the channel

Summary

Network Fundamentals

Security Basics

- **Authentication and resource access**
- **Data and communication security**

Authentication and resource access

Authentication	• Identify verification
Authorization	• Access control and access permissions
Accounting	• Tracking access to resources

AAA framework

Authentication Forms

logged onto a computer

you have taken part in an authentication process

Something you know	• Password or PIN
Something you have	• Smart card, ID badge, etc.
Something you are	• Biometric information

Authorization

access control and access permissions

level of access

Most security systems also support explicitly denied permissions, which block access to an object.

Accounting

Accounting systems could be used to track the amount of time that a user is connected or the amount of data uploaded or downloaded by the user

to collect data for network planning

RADIUS

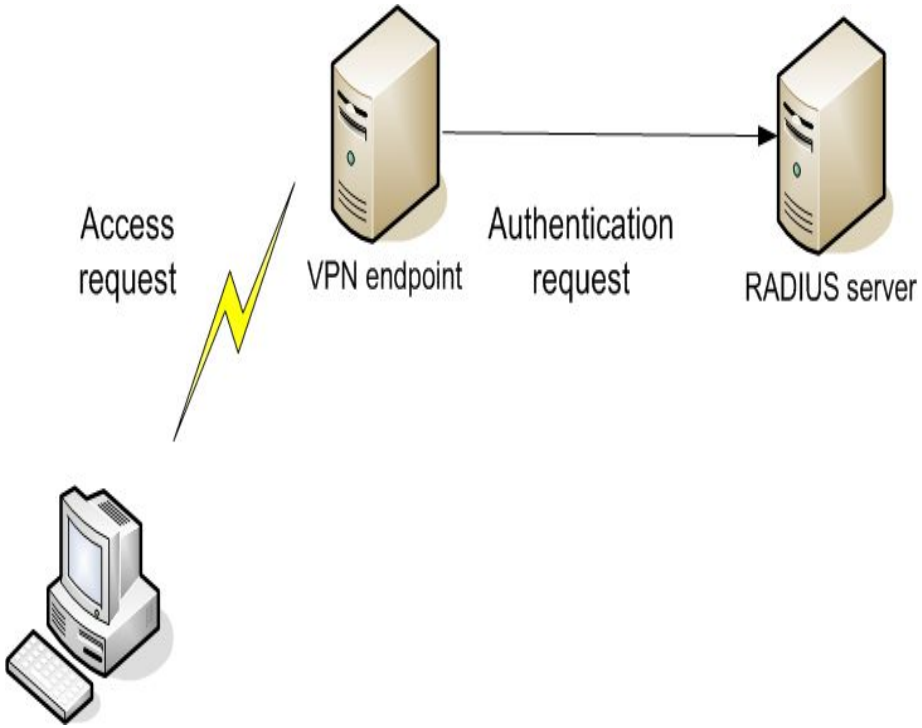
(RADIUS)
manage centralized

be used to provide AAA support for Internet sites, internal wired networks, and wireless networks.

RADIUS

the request is forwarded to the RADIUS server for authentication

on a database maintained by the RADIUS server



Data Integrity Technology

for keeping data safe and secure

Integrity

- **Making sure that unauthorized changes are not made to your data. For example, preventing a hacker from intercepting a file, making changes to the file, and then passing it on to its destination.**

Data Integrity Technology

is the use of data encryption.

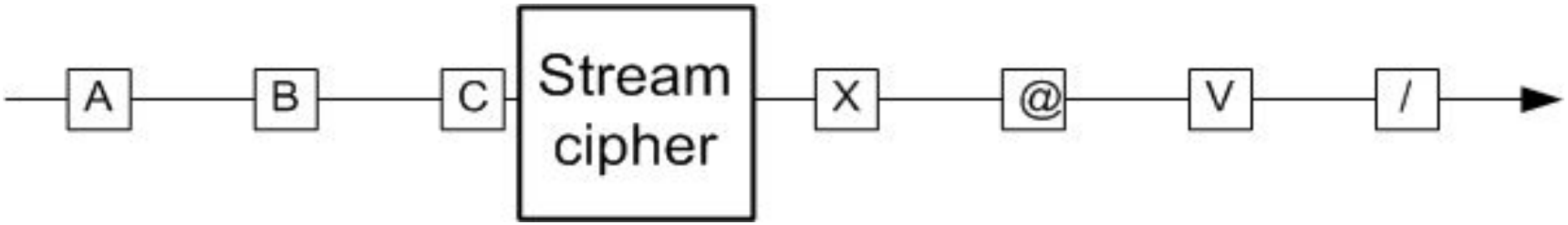
A special value, known as a key, is used to encrypt and decrypt the data

Symmetric encryption	• **Encryption method in which the same key is used to encrypt and decrypt data.**
Asymmetric encryption	• **Encryption method based on using two different keys, one for data encryption and one for decryption.**

Symmetric Encryption

- **Stream cipher**
- **Block cipher**

stream cipher is RC4.



Block cipher

- **Advanced Encryption Standard (AES)**
- **Data Encryption Standard (DES)**
- **Triple DES (3DES)**

Asymmetric Encryption

a private key

and a public key.

The public key is used

The private key

Private key	•Asymmetric encryption key used by the key owner to decrypt data that was originally encrypted using the corresponding public key.
Public key	•Asymmetric encryption key used to encrypt data. The data can only be decrypted using the corresponding private key.

Summary