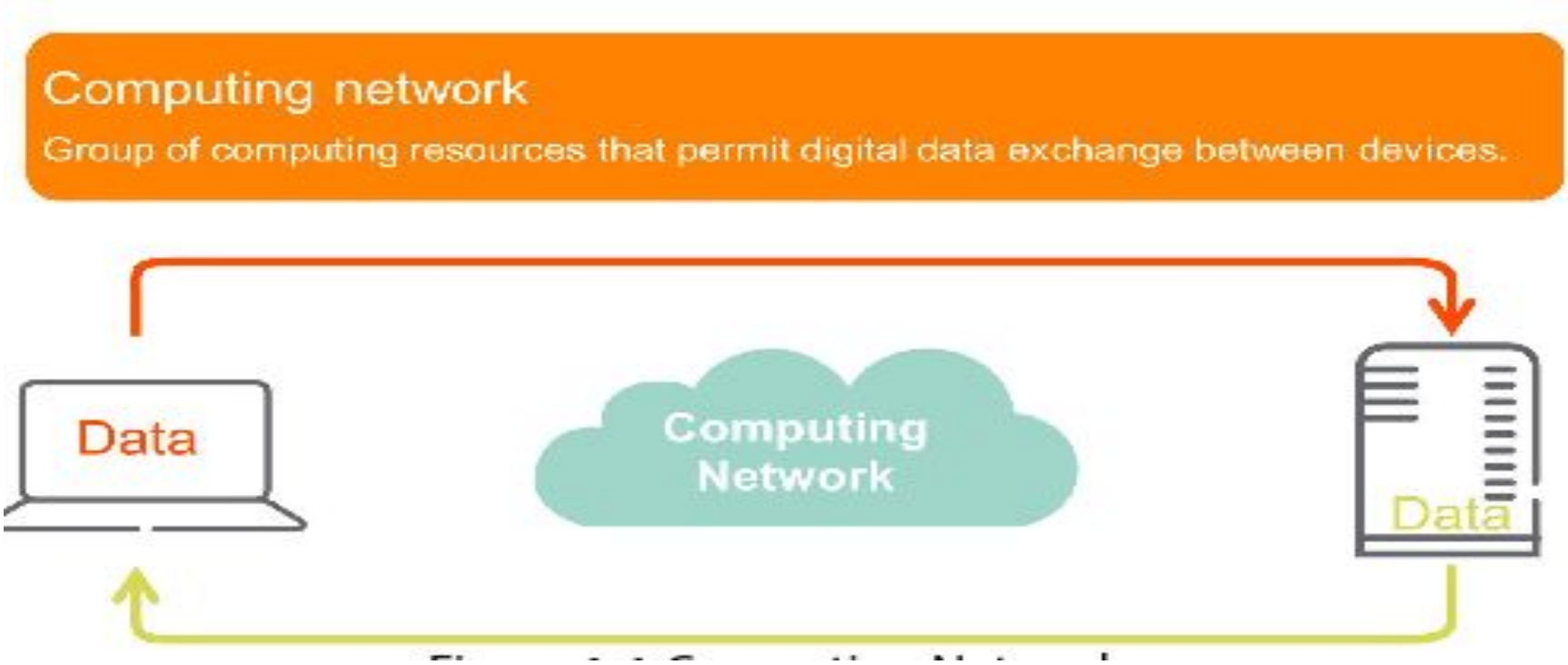
Лекція 1

Основи мережних технологій

Objectives

Основи мережних технологій

What is a Computing Network?



Network Classifications

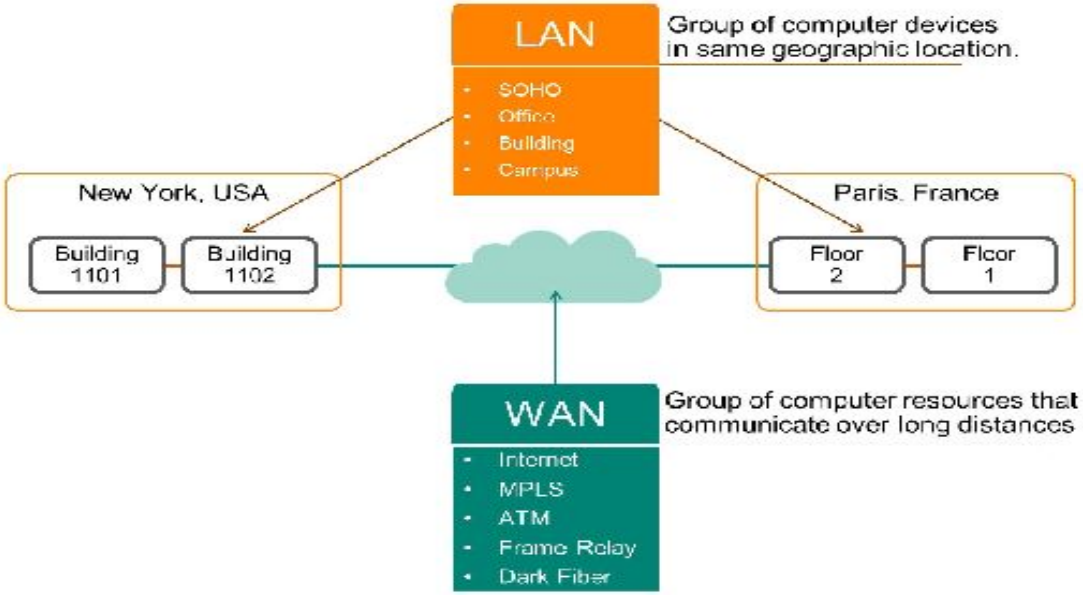
Local Area Network (LAN) Wide Area Network (WAN).

Local Area Network (LAN) - це група комп'ютерних пристроїв, які географічно розташовані в одному місці. Наприклад, групу пристроїв у будівлі можна вважати LAN.

LANs

:

- **Small Office/Home Office (SOHO)**
- **Office LANs**
- **Building LANs**
- **Campus LANs**



Wide Area Networks (WAN)

Wide Area Network (WAN)

Приклади технологій WAN включають наступне:

- **Internet**
- **Multi-Protocol Label Switching (MPLS)**
- **Asynchronous Transfer Mode (ATM)**
- **Frame Relay (largely obsolete)**
- **Dark fiber**

Differences between LAN and WAN

Local Area Network (LAN) має вищі показники пропускної здатності. Сучасна LAN працює зі швидкістю пропусканняи 100 Мбіт/с, 1 Гбіт/с або 10 Гбіт/с. WAN мають нижчий рівень пропускної здатності порівняно з LAN. Сучасні WAN працюють на пропускній здатності 20 Мбіт/с, 50 Мбіт/с або 100 Мбіт/с.

Для Local Area Network (LAN)

. Для

Wide Area Networks (WAN)

Ethernet

VPN

MPLS

Differences between LAN and WAN

Local Area Networks (LANs) є більш надійною і безпечною у порівнянні з Wide Area Networks (WANs).

Початкові витрати на налаштування для Local Area Networks (LANs) є низькими, оскільки пристрої, які необхідні для налаштування мереж, дешеві. Початкові витрати на налаштування для Wide Area Networks (WANs)

Local Area Networks (LANs
Wide Area Networks (WANs).

Wide Area Networks (WANs) є більш перевантажені ніж Local Area Networks (LANs).

Communication protocol

Протокол комунікації - **це система правил, яка дозволяє двом або більше об'єктам системи комунікації передавати інформацію за допомогою будь-якого варіанта фізичної величини. Протокол визначає правила, синтаксис, семантику та синхронізацію зкомунікації та можливі методи відновлення помилок.**

Типи протоколів комунікації	• Transmission Control Protocol (TCP) • Internet Protocol (IP) • User Datagram Protocol (UDP) • Post office Protocol (POP) • Simple mail transport Protocol (SMTP) • File Transfer Protocol (FTP) • Hyper Text Transfer Protocol (HTTP)
Кількість протоколів комунікації	• 65535 protocols
Найбільш важливі протоколи комунікації	• TCP, IP

Основи мережних технологій

OSI Model

International Organization for Standardization (ISO) вирішила проблему, представивши стандартну модель комунікації для обчислювальних пристроїв – модель Open Systems Interconnection (OSI).

Коли пристрій працює на певному рівні, це означає, що пристрій реалізує функціональність цього рівня, а також реалізує функціональність більш низьких рівнів.

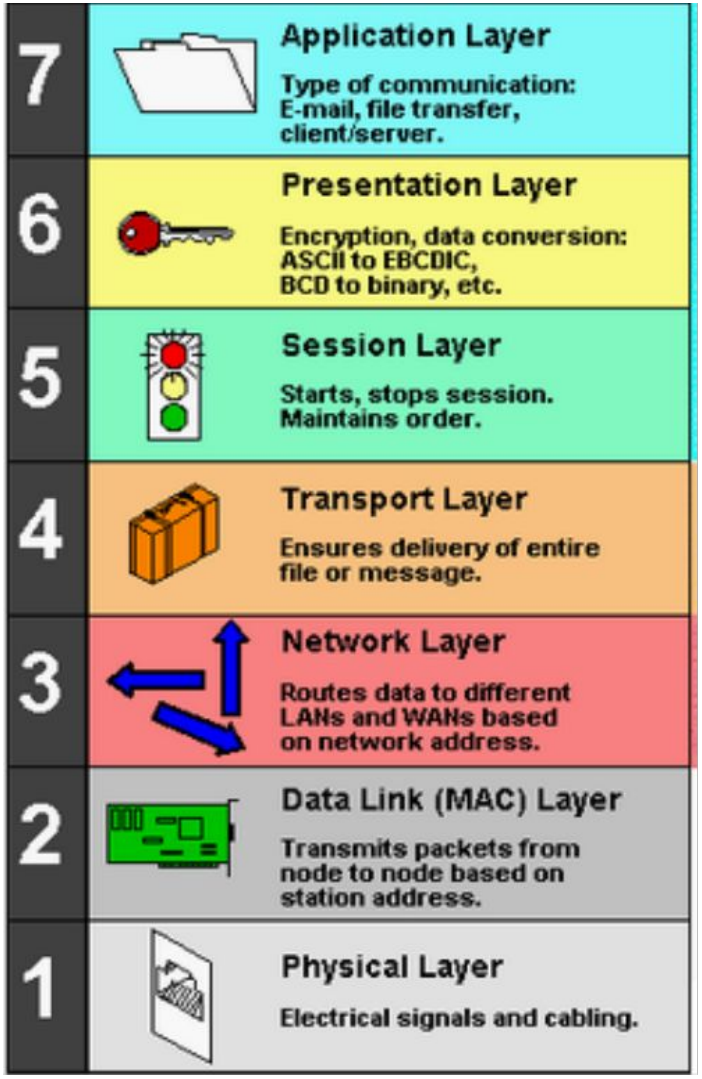
OSI Model

7	Application Layer	
6	Presentation Layer	
5	Session Layer	
4	Transport Layer	Segments
3	Network Layer	Packets
2	Data Link Layer	Frames
1	Physical Layer	Bits, wires, hardware, RF Signals

OSI Model

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

OSI Layer 1. Physical Layer



Physical layer

- **Середовище передачі**
- **З'єднувач**
- **Кодування та синхронізація даних**
- **Техніка передачі**

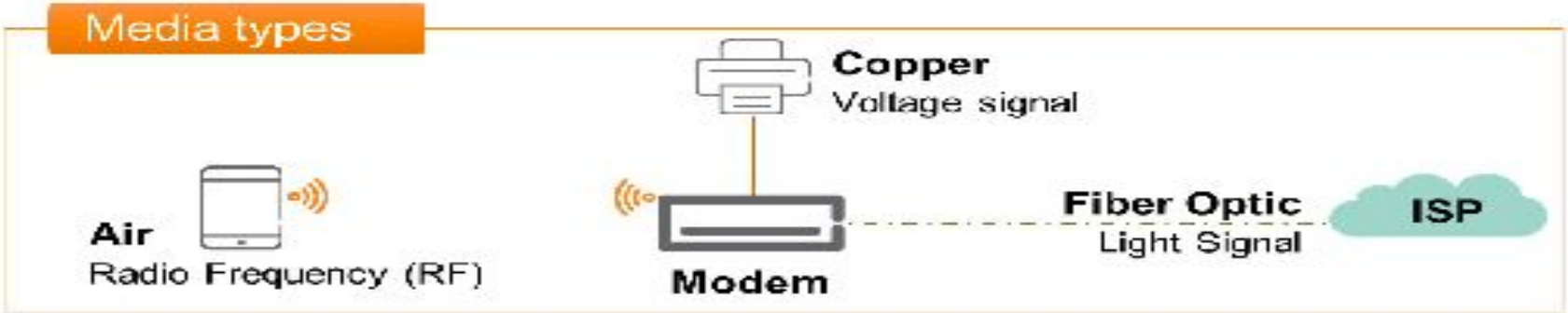
Transmission media

Цей рівень визначає характеристики матеріалу та компоненти, які слід використовувати для досягнення правильної передачі повідомлень.

Radio Frequency (RF) signals).

Fiber Optic cables)

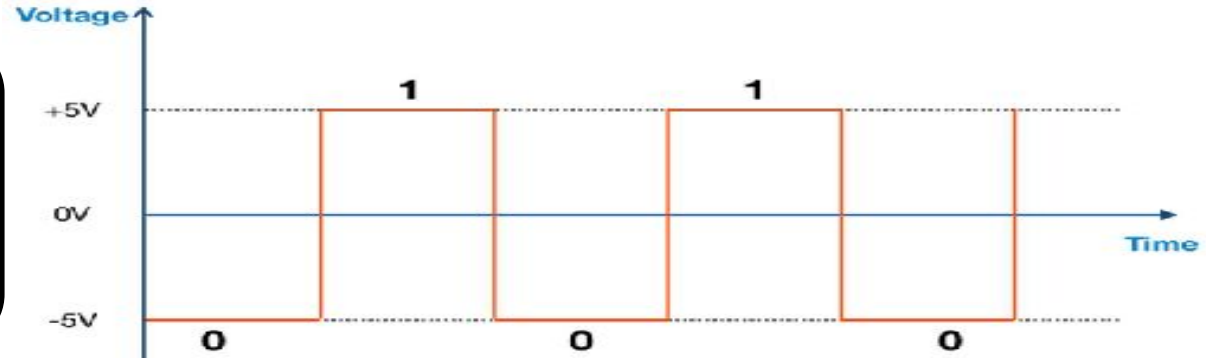
twisted pair copper patch cable)



Transmission media. Copper Cables

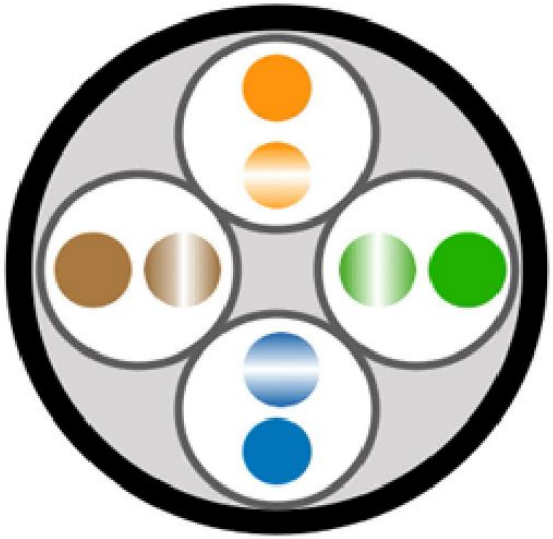
Twisted Pair)

(Unshielded Twisted Pair (UTP). Існують і інші варіації, наприклад Shielded or Foiled Twisted Pair (FTP) – яка зазвичай розгортається для забезпечення захисту від зовнішньої електромагнітної інтерференції

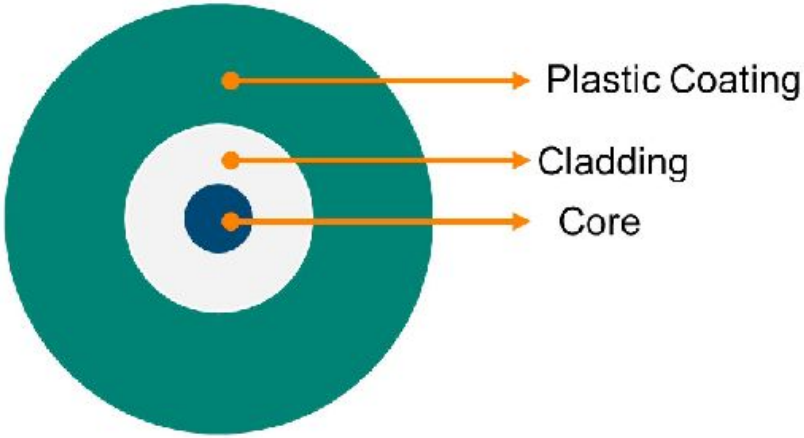


Transmission media. Copper Cables

RJ-45



Transmission media. Fiber Optic

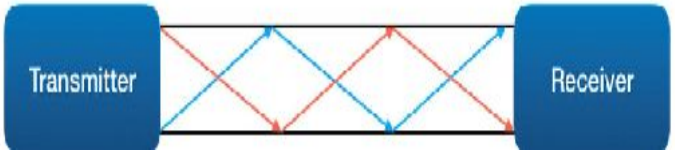


Transmission media. Fiber Optic

Transmission media. Fiber Optic

Multi mode (MM)

Multi Mode Fiber
Core size can be 50 or 62.5μm
Maximum distance: 600 meters (2000 feet)
Typical Data Rate: 10Gbps
Transceivers are based on LEDs



Transmission media. Fiber Optic

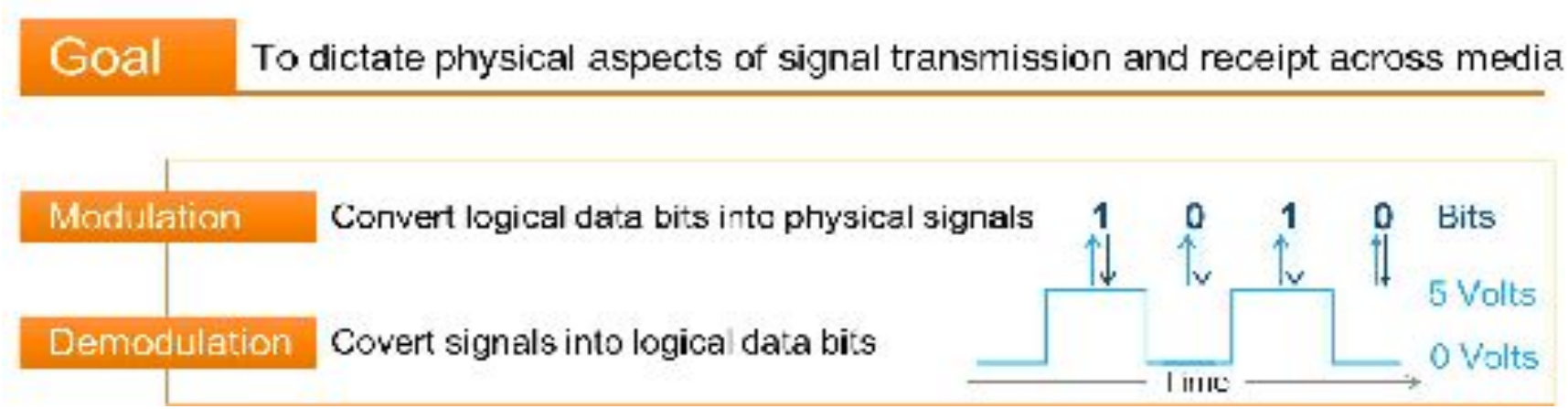
Single Mode (SM)

Single Mode Fiber
Core size is 9μm
Maximum distance: 40Km
Data Rates: Up to 40 and 400Gbps
Transceivers are based on LASERs

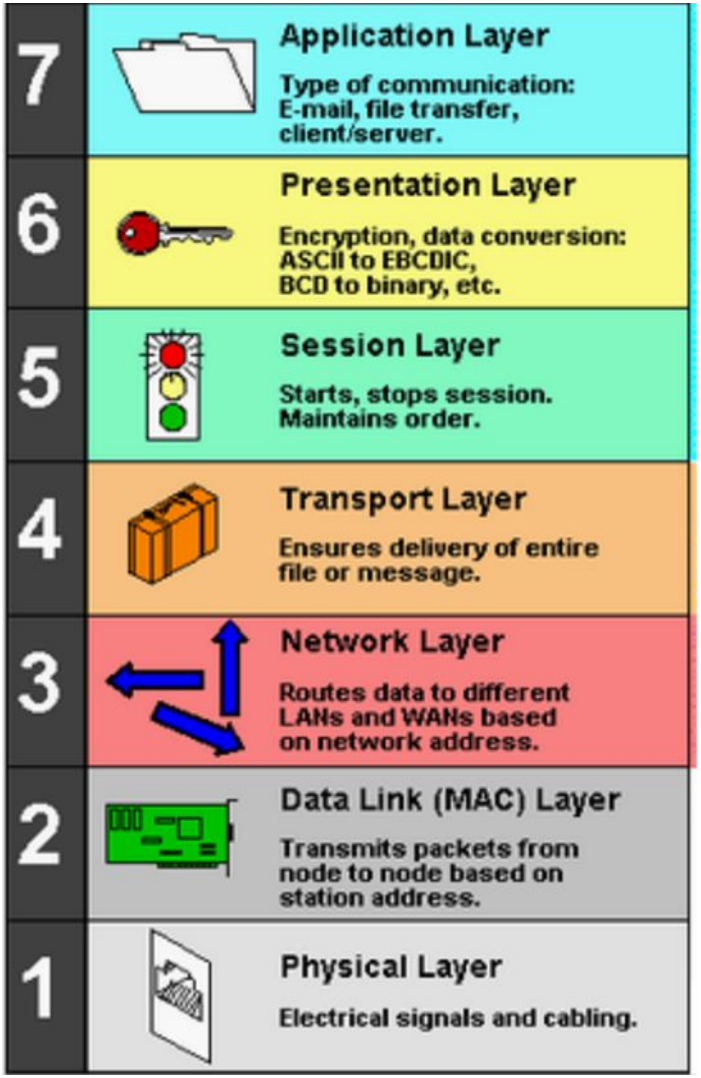
Transmission technique

Фізичний рівень диктує фізичні аспекти того, як сигнали передаються та приймаються через деякі носії.

Обчислювальні пристрої перетворюють біти логічних даних у правильний фізичний принцип залежно від використовуваного носія - цей процес відомий як модуляція. Зворотний процес, перетворення фізичних сигналів у логічні біти даних, відомий як демодуляція.



OSI Layer 2. Data Link Layer



Data Link layer

- **Контроль з'єднання**
- **Управління доступом**
- **Контроль трафіку (послідовність, підтвердження, делімітація, корекція помилок)**

OSI Layer 2. MAC address

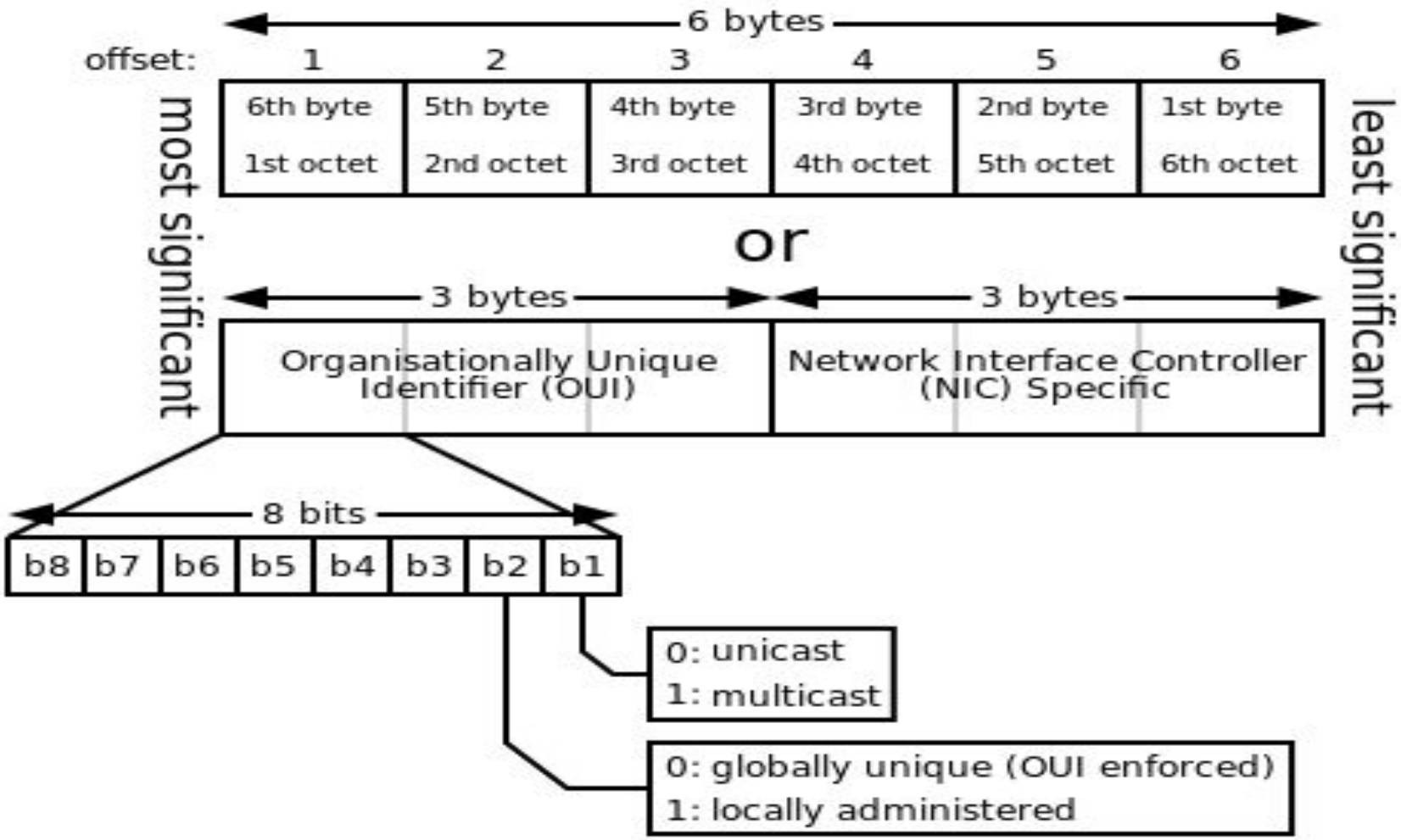
Media Access Control (MAC) address

Стандартний формат для друку MAC-адреси у зручній для людини формі - це шість груп із двох шістнадцяткових цифр (шість байтів), наприклад: 00-C0-26-A9-42-F7.

Перші три октети (байти) ідентифікують організацію, яка видала ідентифікатор і відомі як Organizationally Unique Identifier (OUI).

Решта три октети представляють унікальну адресу адаптера – Network Interface Controller (NIC) Specific.

OSI Layer 2. MAC Address



Adapter’s physical address

ipconfig/all.

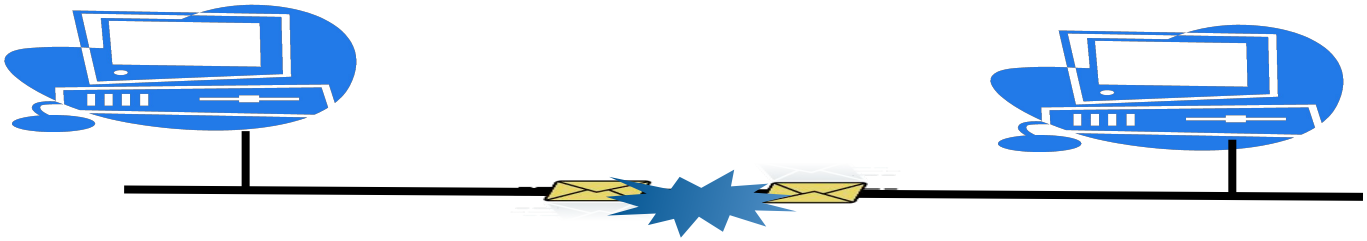
фізична адреса адаптера (physical address).

C:\Windows\system32\cmd.exe

```
   Host Name . . . . . . . . . . . . : Win7
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : NVIDIA nForce 10/100/1000 Mbps Ethernet
   Physical Address. . . . . . . . . : 00-1F-16-F8-2E-19
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d46f:5f6c:bff1:30db%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, December 09, 2011 3:25:48 AM
   Lease Expires . . . . . . . . . . : Monday, December 12, 2011 9:09:03 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 234888562
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-12-FB-B4-4F-00-1F-16-F8-2E-19

   DNS Servers . . . . . . . . . . . : 24.217.0.5
```

OSI Layer 2. Access management

CSMA/CD)

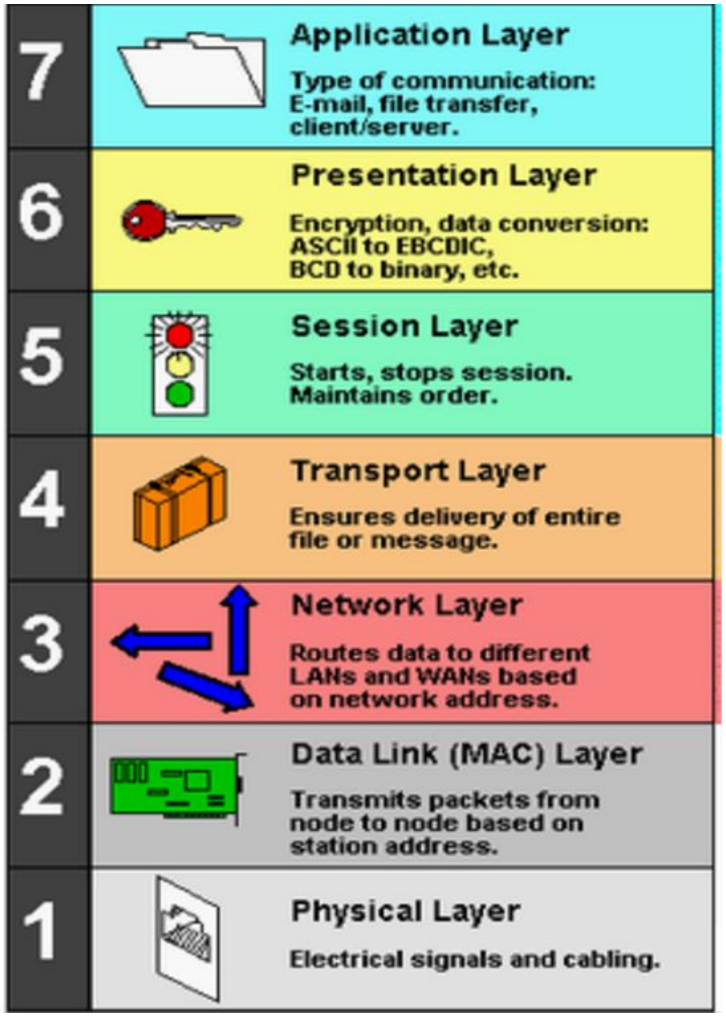


OSI Layer 2. Access management

Коли колізія виявляє-ться, то у цьому випадку:

- **Усі залучені хости припиняють передачу.**
- **Обидва кадри відкидаються.**
- **Обидві станції чекатимуть випадковий час і намагатимуться передати кадр без колізій, тобто передати успішно.**

OSI Layer 3. Network Layer



Network layer

- **Адресація мережі**
- **Маршрутизація трафіку**
- **Фрагментація/повторна збірка**

Network address. IPv4 and IPv6 Addresses

IPv4

- 32-bit address
- Up to 4,294,967,296 addresses
- Network and host address determined by subnet mask

IPv6

- 128-bit address
- Up to 340 undecillion addresses
- 64-bit network address/64-bit host address (18 446 744 073 709 551 616)

Network address. IPv4 Address

123.20.210.3

01111011 00010100 11010010 00000011

Subnet Mask

11000000 10101000 00000001 01100100
11111111 11111111 11111111 00000000

11000000 10101000 00000001 01100100

Network address

Host address

Subnet mask

- **Використовується для розмежування адрес мережі та хосту в адресі IPv4.**

Most significant bit

255.255.255.192

11111111 11111111 11111111 11000000

IPv4 Address Classes

Address class	First octet	Range	Default subnet mask	Hosts per network	Networks
Class A	01xxxxxx	0.0.0.0 to 127.255.255.255	255.0.0.0	16,777,216	128
Class B	10xxxxxx	128.0.0.0 to 191.255.255.255	255.255.0.0	65,536	16,384
Class C	110xxxxx	192.0.0.0 to 223.255.255.2255	255.255.255.0	256	2,097,152
Class D (multicast)	1110xxxx	224.0.0.0 to 239.255.255.255	undefined	undefined	undefined
Class E (reserved)	11110xxx	240.0.0.0 to 255.255.255.255	undefined	undefined	undefined

Private IP Address Ranges

У кожному класі адрес знаходиться діапазон адрес, зарезервований для використання в якості приватних адрес. Деякі IP -адреси є публічними і тому їх можна використовувати як у загальнодоступних мережах (Інтернет) так і в приватних мережах. Частіше приватні мережі використовують приватні IP-адреси. Інтернет не розпізнає приватні адреси. Для доступу до Інтернету хост з приватною адресою повинен пройти через пристрій NAT, де приватна адреса змінюється на публічну.

Address class	Private IP Address range	Full address range
Class A	10.0.0.0 – 10.255.255.255	0.0.0.0 - 127.255.255.255
Class B	172.16.0.0 – 172.31.255.255	128.0.0.0 - 191.255.255.255
Class C	192.168.0.0 – 192.168.255.255	192.0.0.0 - 223.255.255.2255
APIPA	169.254.0.0 – 169.254.255.255	

APIPA range address

- Наприклад, діапазон адрес 169.254.0.0 - 169.254.255.255 зарезервований як діапазон APIPA.

When a host is unable to obtain an IP address from a DHCP server, it will typically use an APIPA address until the problem is resolved.

Automatic Private IP Addressing (APIPA).

- Address generated for a host when it is unable to obtain an address from a DHCP server.

APIPA range address

- **Наприклад, діапазон адрес 169.254.0.0 - 169.254.255.255 зарезервований як діапазон APIPA.**

Automatic Private IP Addressing (APIPA).

- **Адреса, яка автоматично сформована для хоста, коли він не може отримати адресу з сервера DHCP.**

Коли хосту не вдається отримати IP-адресу з сервера DHCP, хост, як правило, використовує адресу APIPA, доки проблема не буде вирішена.

CIDR Format

Classless Inter-Domain Routing (CIDR).

- **Альтернативний метод виділення IP -адрес.**

192.168.040.0/24

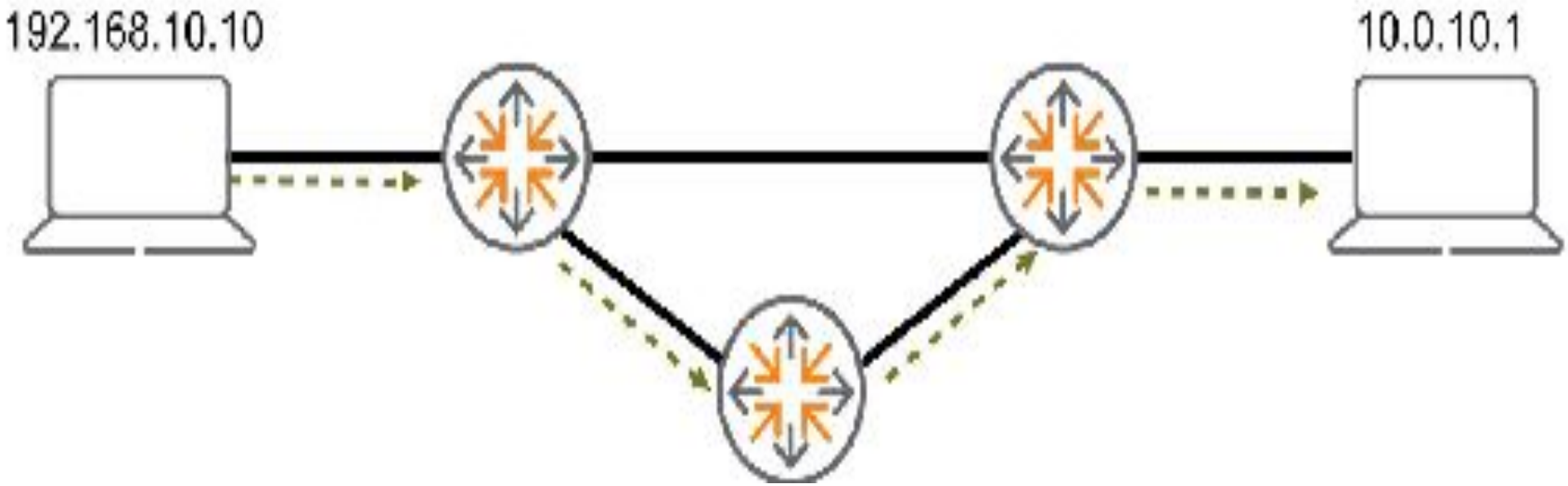
255.255.255.0

11111111 11111111 11111111 00000000

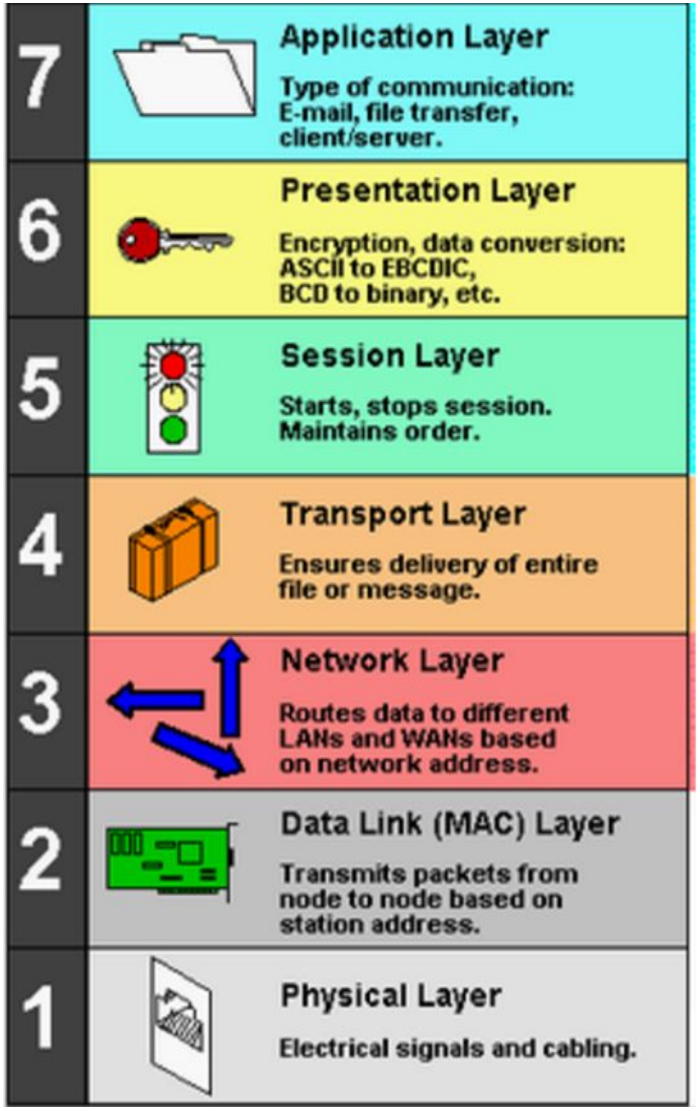
Traffic routing

Логічна адресація	• **Унікальний ідентифікатор Рівня-3 (Layer-3) для джерела та пункту призначення зберігається по всьому шляху.**
Відкриття і вибір шляху	• **Мережевий рівень запускає алгоритми та протоколи, щоб знайти всі можливі шляхи, а потім вибрати найкращий шлях. Пізніше на цьому курсі ви дізнаєтесь більше про такі протоколи як Routing Information Protocol (RIP) та Open Shortest Path First (OSPF).**

Traffic routing



OSI Layer 4. Transport Layer

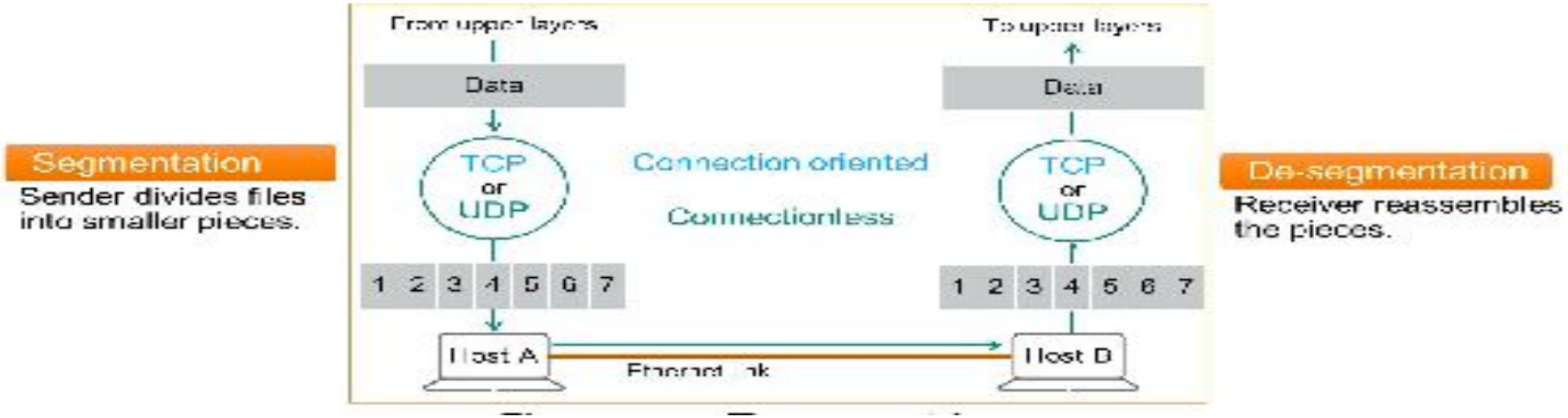


Transport layer

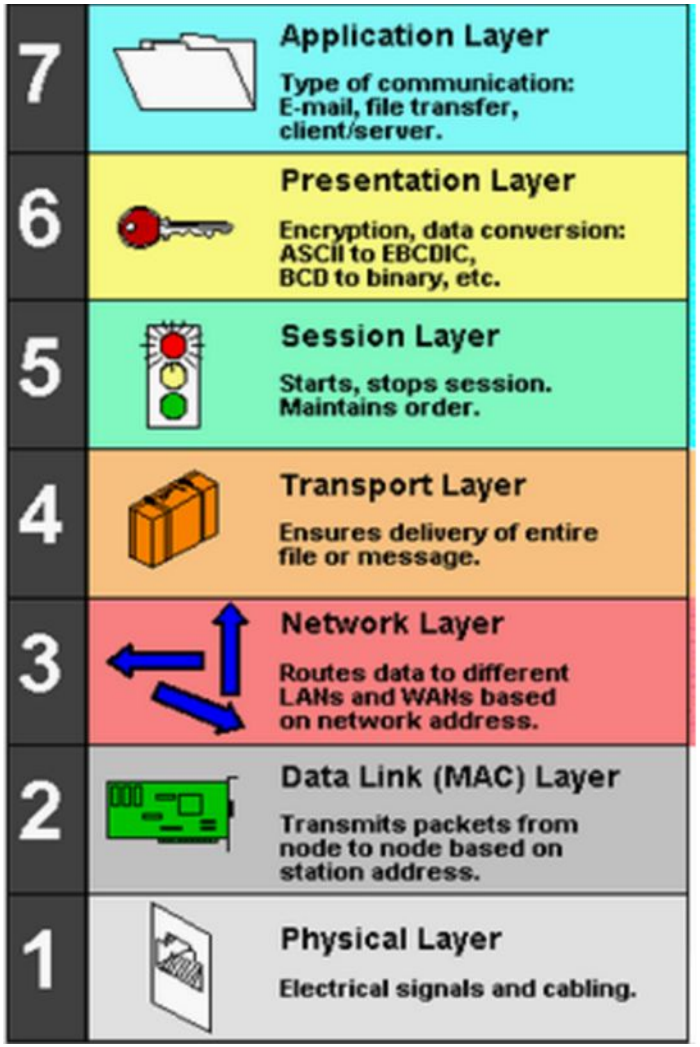
- **Сегментація**
  - **Підтвердження**
    - **Контроль трафіку**

Transport Layer

Транспортний рівень контролює надійність даного посилання шляхом сегментації, десегментації та контролю помилок. На цьому рівні деякі протоколи, такі як Transmission Control Protocol (TCP), орієнтовані на з'єднання. Це означає, що транспортний рівень може відслідковувати повідомлення та повторно передавати ті, які відправлені невдало. Інші протоколи, такі як User Datagram Protocol (UDP), не забезпечують з'єднання. Це означає, що транспортний рівень у цьому випадку не відстежує повідомлення. Перевага цього полягає в тому, що обробка цих з'єднань є відносно швидкою і простою для обчислення.



OSI Layer 5. Session Layer

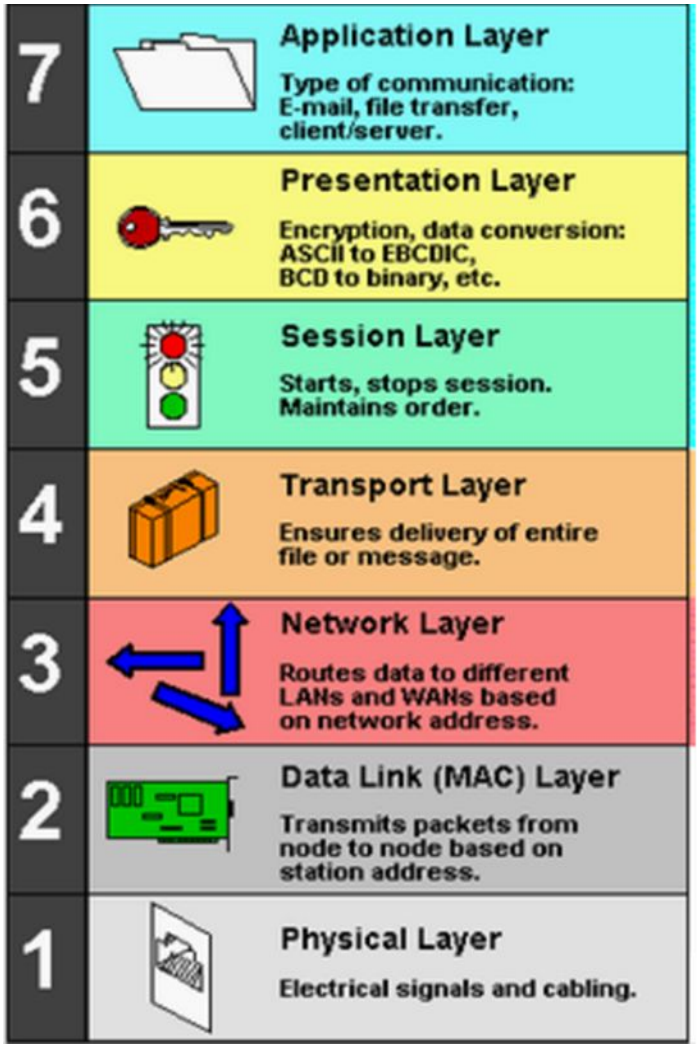


Session Layer

- **Встановлення сеансів між хостами**
- **Управління/підтримка сеансів**
- **Припинення сеансів, коли це більше не потрібно.**

Session Layer

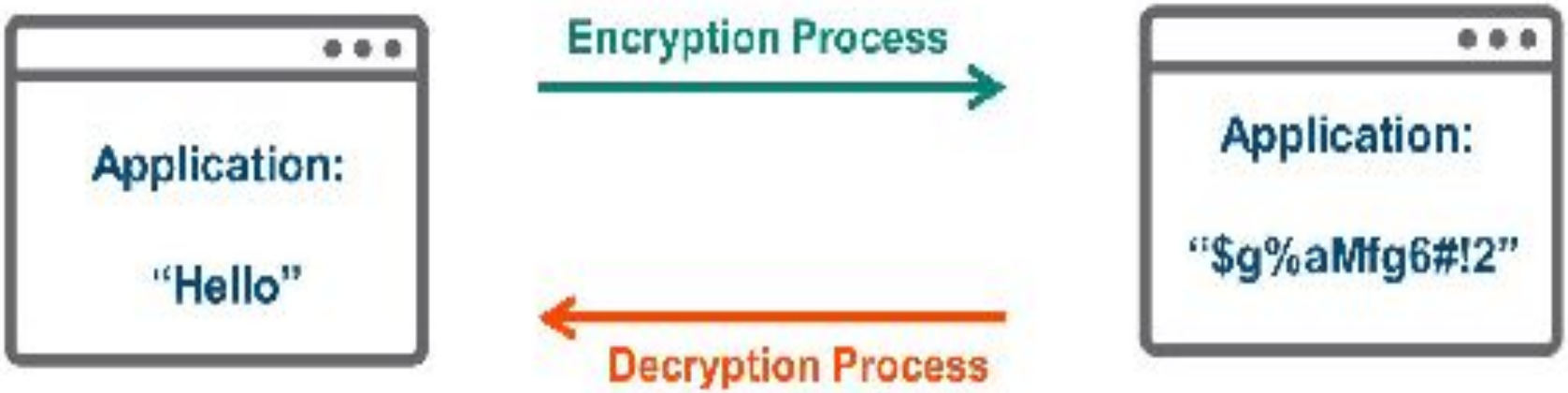
OSI Layer 6. Presentation Layer



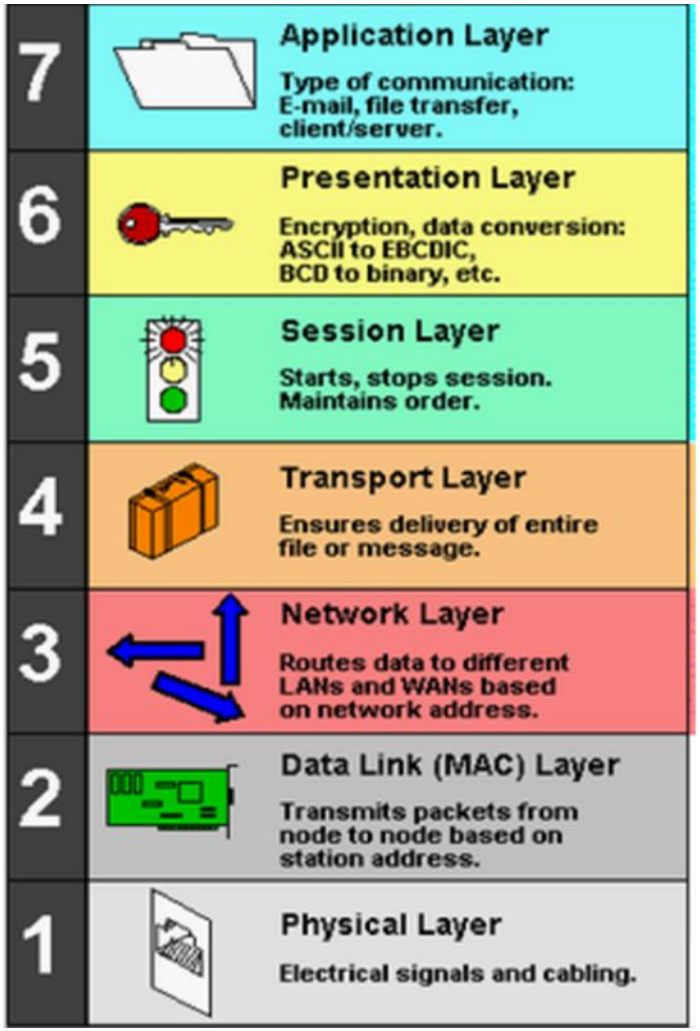
Рівень Презентації (Presentation layer) відповідає за форматування даних із Прикладного рівня так, щоб дані могли передаватися або щоб дані були розпізнані Прикладним рівнем.

- **Переклад символів**
  - ASCII
  - EBCDIC
- **Перетворення**
- **Стиснення**
- **Шифрування**

Presentation Layer



OSI Layer 7. Application Layer



- Віддалений доступ до файлів і принтерів
- Обмін ресурсами
- Зв'язок між процесами
- Електронні повідомлення та електронна пошта
- Каталогічні послуги
- Віртуальні пристрої та віртуальні комунікації
- Перегляд веб-сторінок

Application Layer

Прикладний рівень включає наступні функції:

- **Прикладний рівень визначає ідентичність та наявність партнерів програми із даними для передачі.**
- **Цей рівень забезпечує мережеві послуги для користувацьких програм, таких як передача файлів, електронна пошта, відеоконференції та багато інших .**

Layer Headers

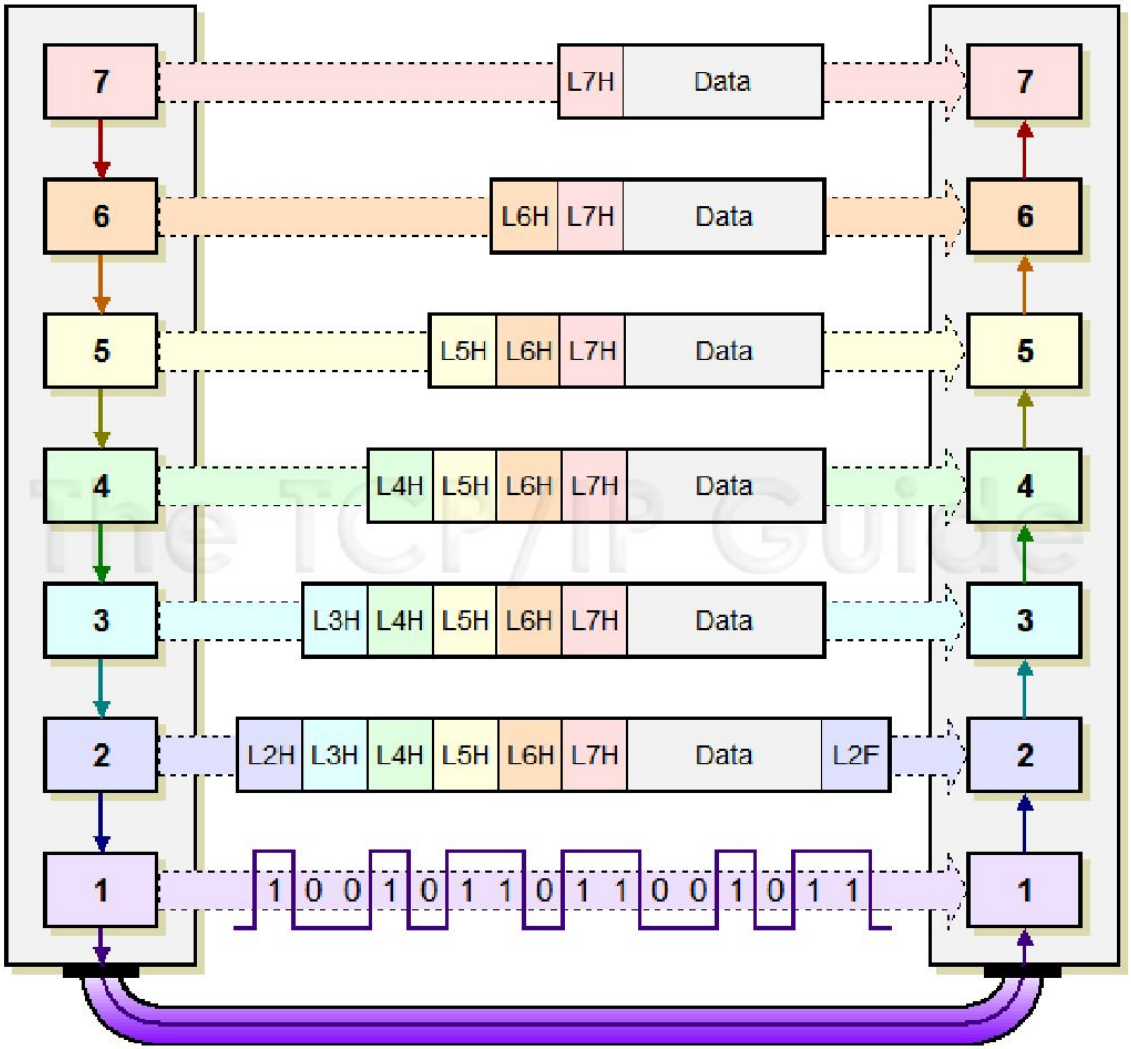
- **Це процес, коли кожен рівень OSI додає заголовок. Цей процес завжди виконується пристроєм-відправником.**

- **Is the process to read and interpret the header information. This process is always done by the receiver device.**

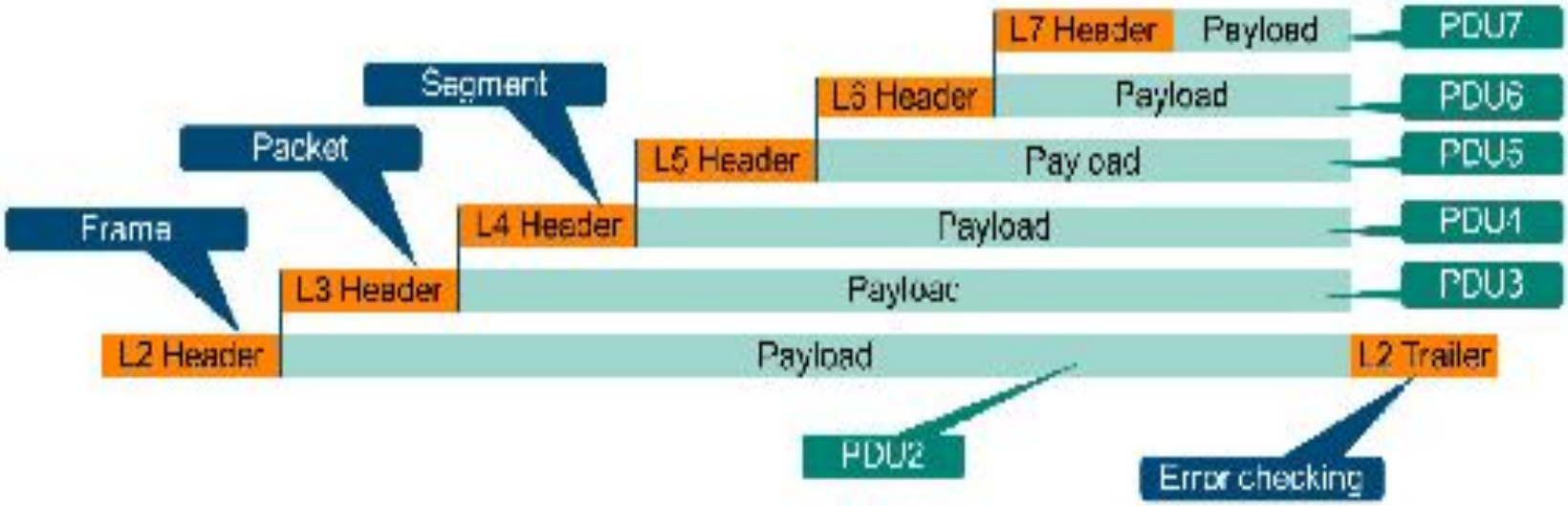
Communication between Layers

Moving from the top)

Moving from the bottom)



Protocol Data Units (PDUs)



Protocol Data Units (PDUs)

Segment.	• **Відноситься до інкапсуляції, яка виконується на Рівні-4. Сегмент еквівалентний PDU4. Відповідно в мережі це сегмент TCP або сегмент UDP .**
Packet.	• **Відноситься до інкапсуляції, яка виконується на Рівні-3. Пакет еквівалентний PDU3. Можна говорити про пакети IP Рівня-3.**
Frame.	• **Відноситься до інкапсуляції, яка виконується на Рівні-2. Кадр еквівалентний PDU2. Можна говорити про фрейми Ethernet або Wi-Fi.**

“L2 Trailer”.

Ethernet Traffic Types

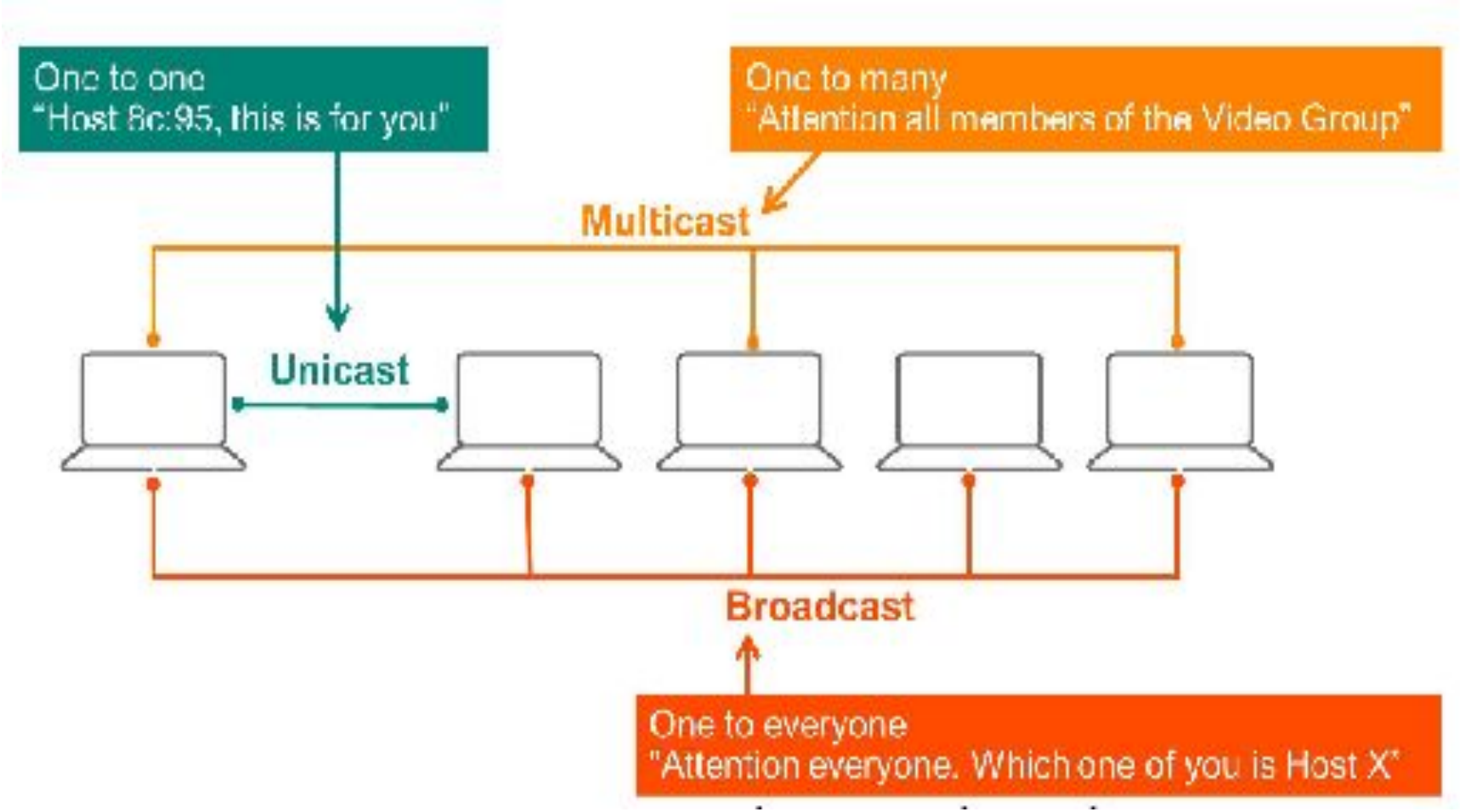
Unicast

Broadcast

Multicast

Anycast

Ethernet Traffic Types



Full Duplex and Half Duplex

Full duplex (EDX) та Half duplex (HDX)

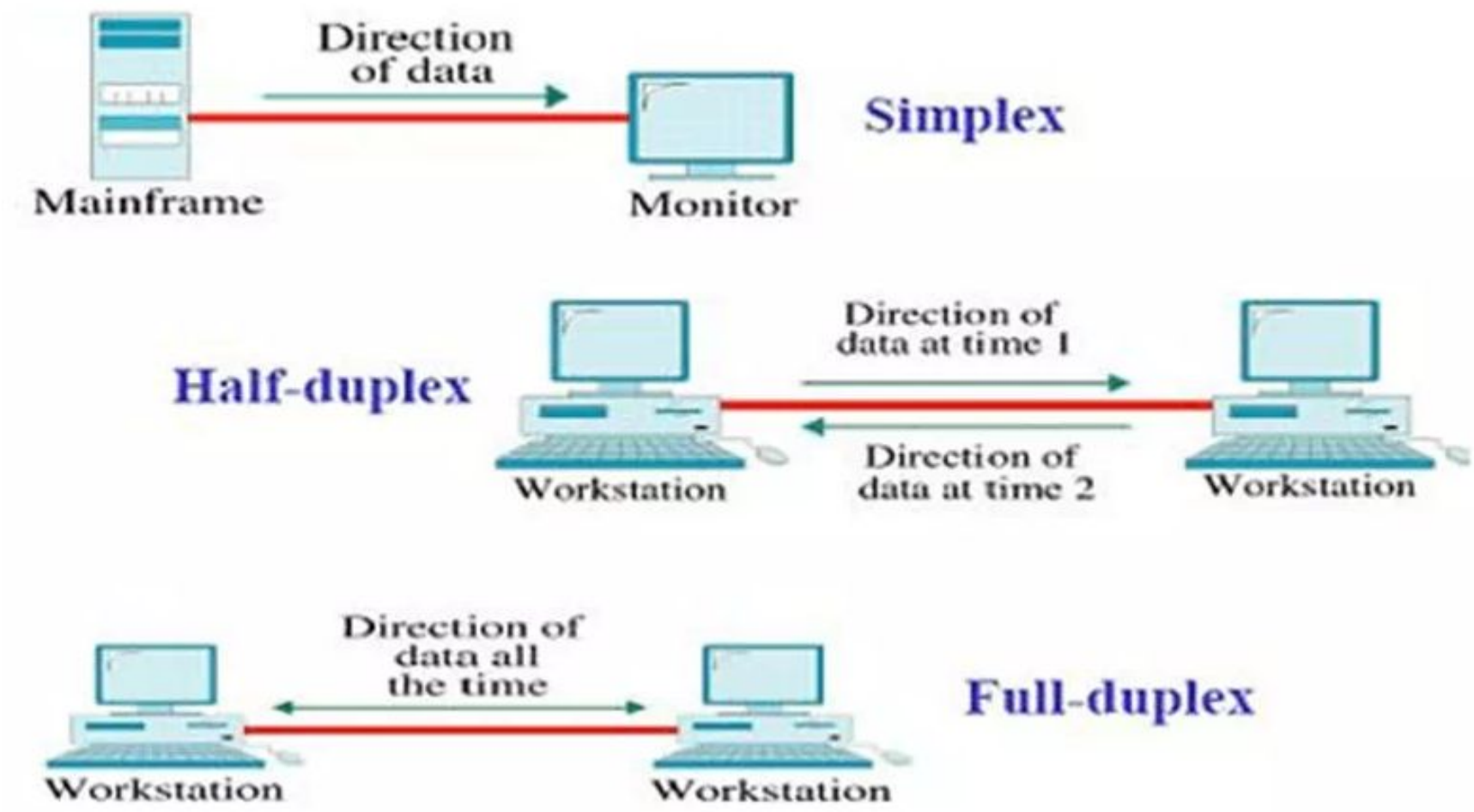
Full Duplex:

- **Обидві сторони можуть спілкуватися один з одним одночасно. Прикладом повного дуплексу є телефон; сторони на обох кінцях можуть говорити і чути іншу сторону одночасно.**

Half Duplex:

- **Обидві сторони можуть спілкуватися між собою, але не одночасно; спілкування спочатку із одним напрямком, а потім з іншим.**

Full Duplex and Half Duplex

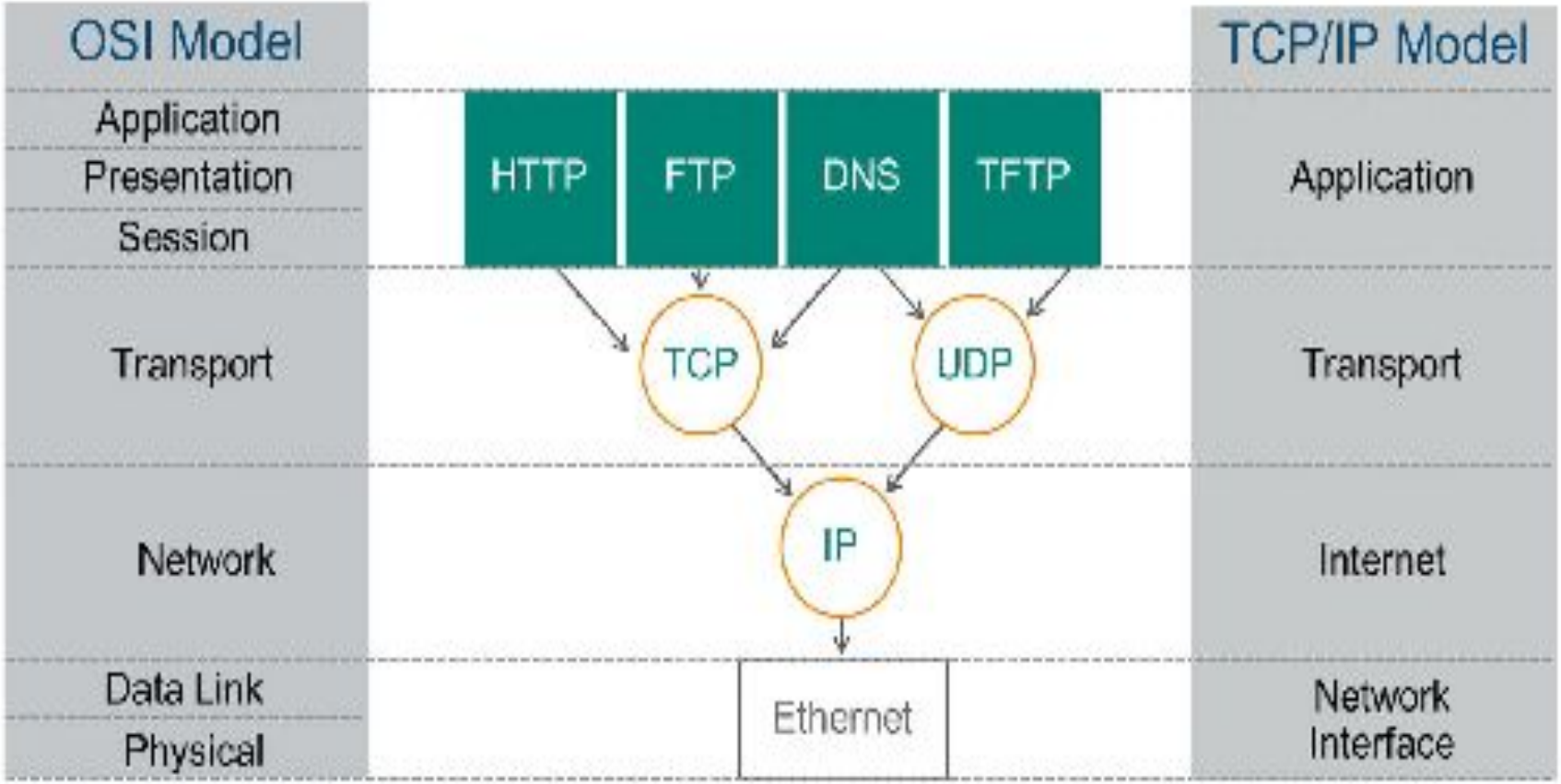


Основи мережних технологій

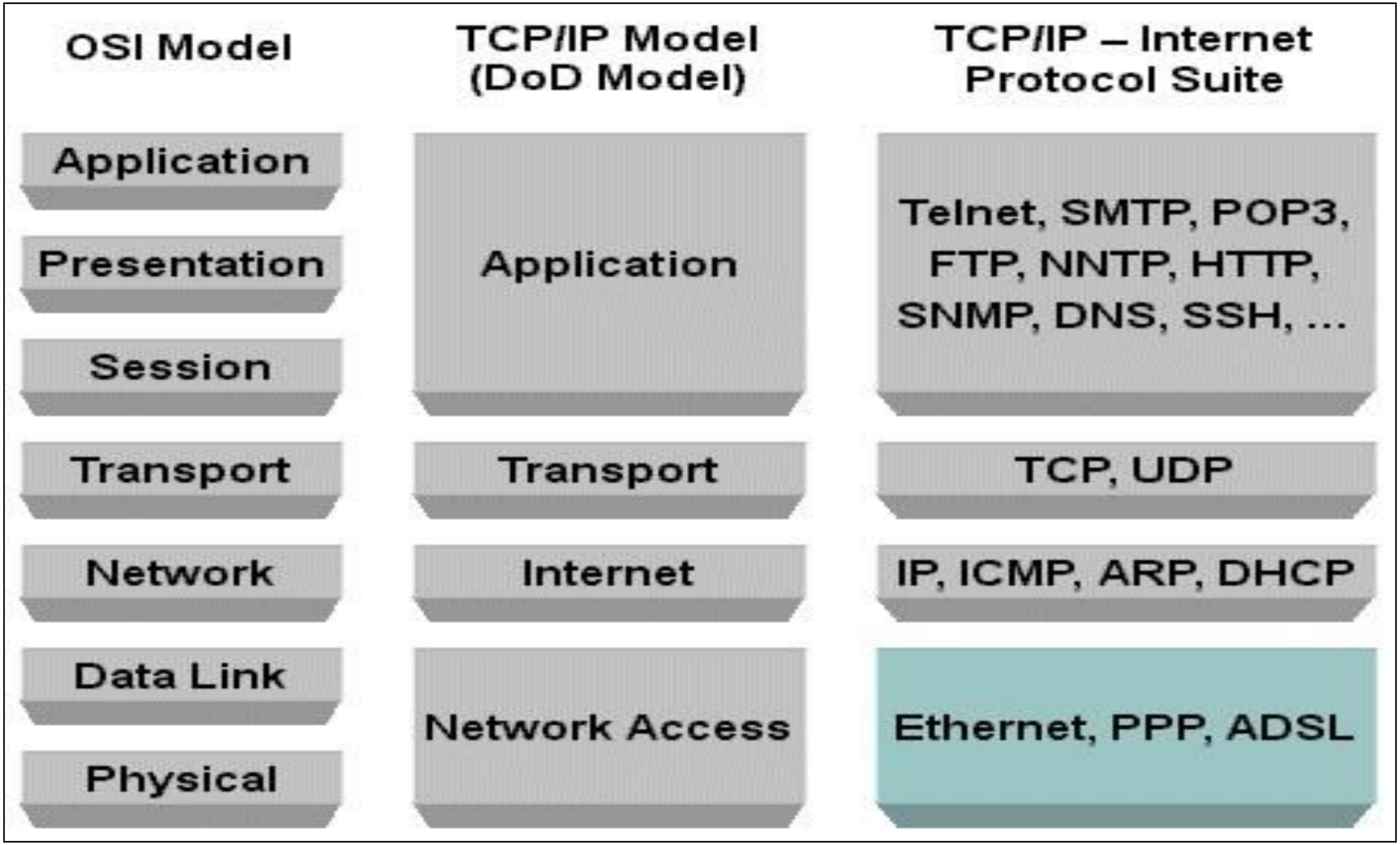
TCP/IP Model

Стек Інтернет протоколів - це концептуальна модель і набір протоколів, що використовуються в Інтернеті та обчислювальних мережах.

TCP/IP Model


OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
HTTP
FTP
DNS
TFTP
TCP
UDP
IP
Ethernet
TCP/IP Model
Application
Transport
Internet
Network Interface

TCP/IP Model


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

TCP/IP Model

Прикладний рівень TCP/IP

Транспортні рівні кожної із моделей

TCP/IP Model

Міжмережевого інтерфейсу **TCP/IP.**

рівень
Доступу до мережі. Цей рівень містять протоколи, що стосуються фізичного середовища зв'язку (мідні проводи, оптоволокно та радіохвилі). Контроль доступу до фізичних носіїв також відбувається на цьому рівні. Ethernet і Wi-Fi-це загальні протоколи, які працюють на цьому рівні Доступу до мережі

TCP/IP Model. Network Access Layer

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

- **Імплементація Фізичного та Канального рівнів моделі OSI.**
- **Ідентифікація хостів за MAC - адресою.**
- **Широкий спектр протоколів низького рівня (Ethernet).**

802.3 Ethernet

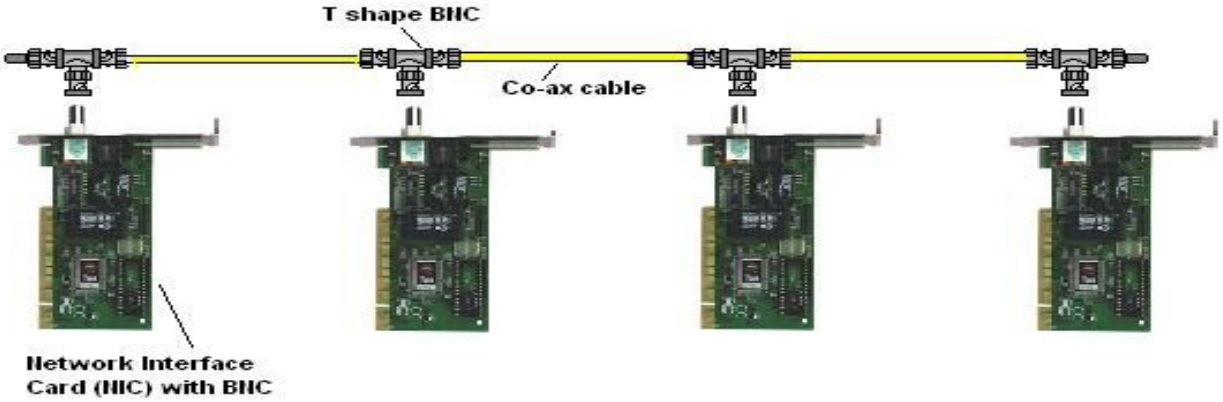
Ethernet - це сімейство комп'ютерних мережевих технологій для

IEEE 802.3

До 1980 року Ethernet став явним переможцем і сьогодні інші протоколи низького рівня рідко можна побачити, крім дуже спеціалізованих додатків.

802.3 Ethernet

- 10Base5 – Товстий Ethernet
- 10Base2 – Тонкий Ethernet



802.3 Ethernet

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**

802.3 Ethernet

Standard	Description
802.3	10BASE5 (Thick Ethernet)
802.3a	10BASE2 (Thin Ethernet)
802.3i	10BASE-T (Twisted pair)
802.3j	10BASE-F (Fiber optic)
802.3u	Fast Ethernet
802.3z	Gigabit Ethernet
802.3ab	1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s)

Standard	Description
802.3x	Full Duplex and flow control;
802.3ac	Max frame size extended to 1522 bytes ("Q-tag")
802.3ad	Link aggregation
802.3ae	10 Gigabit Ethernet over fiber
802.3af	Power over Ethernet
802.3bm	100G/40G Ethernet for optical fiber

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 →						

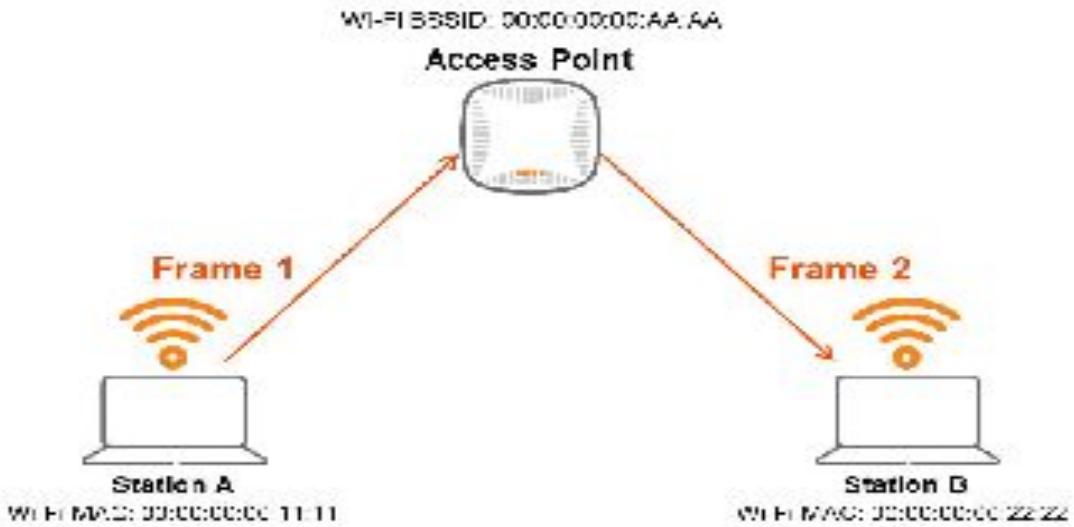
Wi-Fi Frames

Wi-Fi Header								Wi-Fi Trailer
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Payload	FCS
2 Bytes	2 Byte	6 Bytes	6 Bytes	6 Bytes	2 Bytes	6 Bytes	46 – 1500 Bytes	4 Bytes

Ethernet Frame

Frame Control.	• Вказує на тип фрейму (контроль, управління або дані), а також містить інформацію про фрагментацію та конфіденційність.
Duration/Con-nection ID.	• Якщо використовується, вказує час у мікросекундах, який буде виділено каналу для успішної передачі контрольного кадру.
Addresses.	• MAC-адреси для пристроїв, які беруть участь у зв'язку. Кількість адрес залежить від типу кадру та контексту. Як правило, використовуються лише перші три поля адреси.
Sequence Control.	• Це поле містить інформацію про фрагментацію та повторну збірку .

Understanding the Wi-Fi Header



	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
Frame 1	BSSID (AP) 00:00:00:00:AA:AA	MAC of Station A 00:00:00:00:11:11	MAC of Station B 00:00:00:00:22:22	Not Used
Frame 2	MAC of Station B 00:00:00:00:22:22	BSSID (AP) 00:00:00:00:AA:AA	MAC of Station A 00:00:00:00:11:11	Not Used

Understanding the Wi-Fi Header

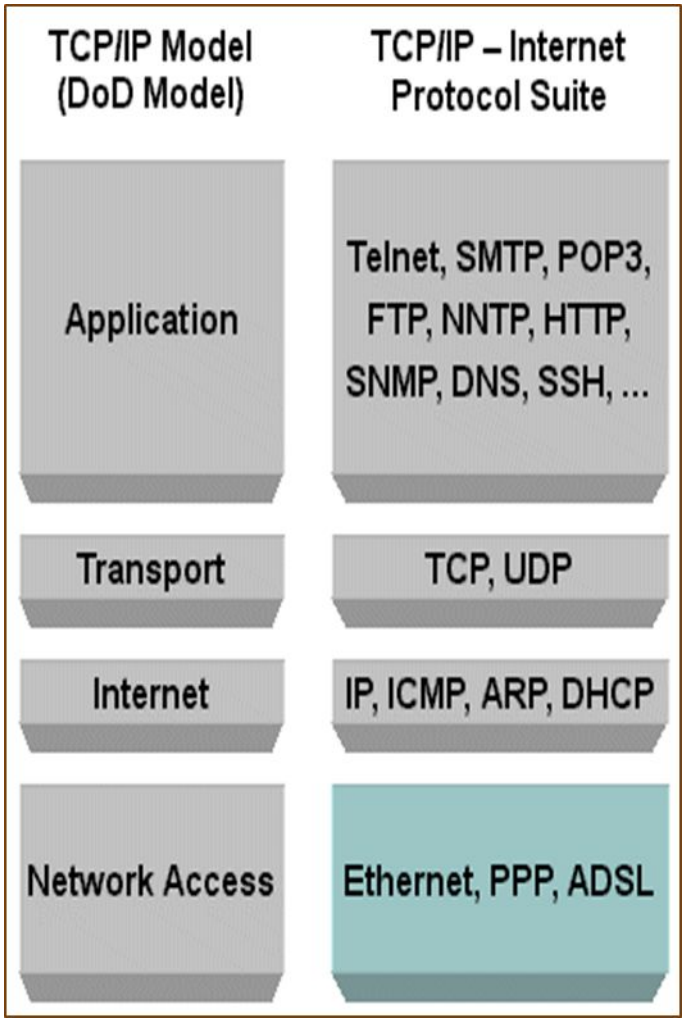
Wireless Networking

Визначається стандартами 802.11. Стандарти сімейства 802.11 визначають радіо-інтерфейс між безпроводовим клієнтом і точкою доступу (AP) або між двома безпроводовими клієнтами.

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 (WiFi 5)	5 GHz	Up to 1.3 Gbps
802.11 ax (WiFi 6)	1-7 GHz	Up to 7 Gbps

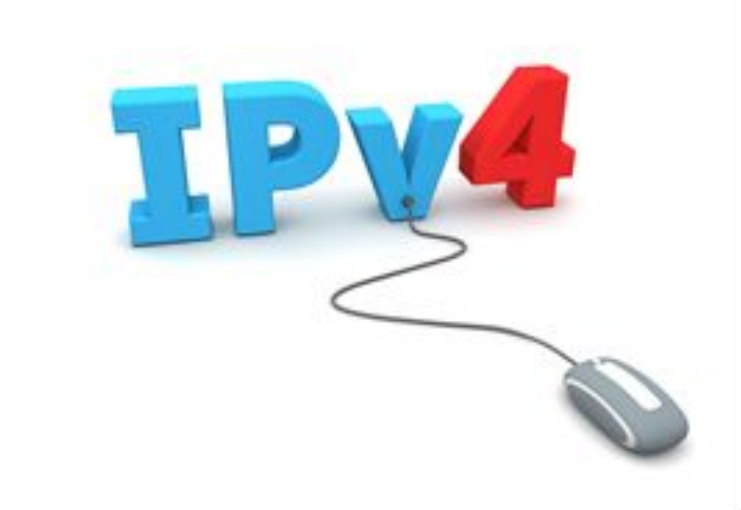
TCP/IP Model. Internet Layer



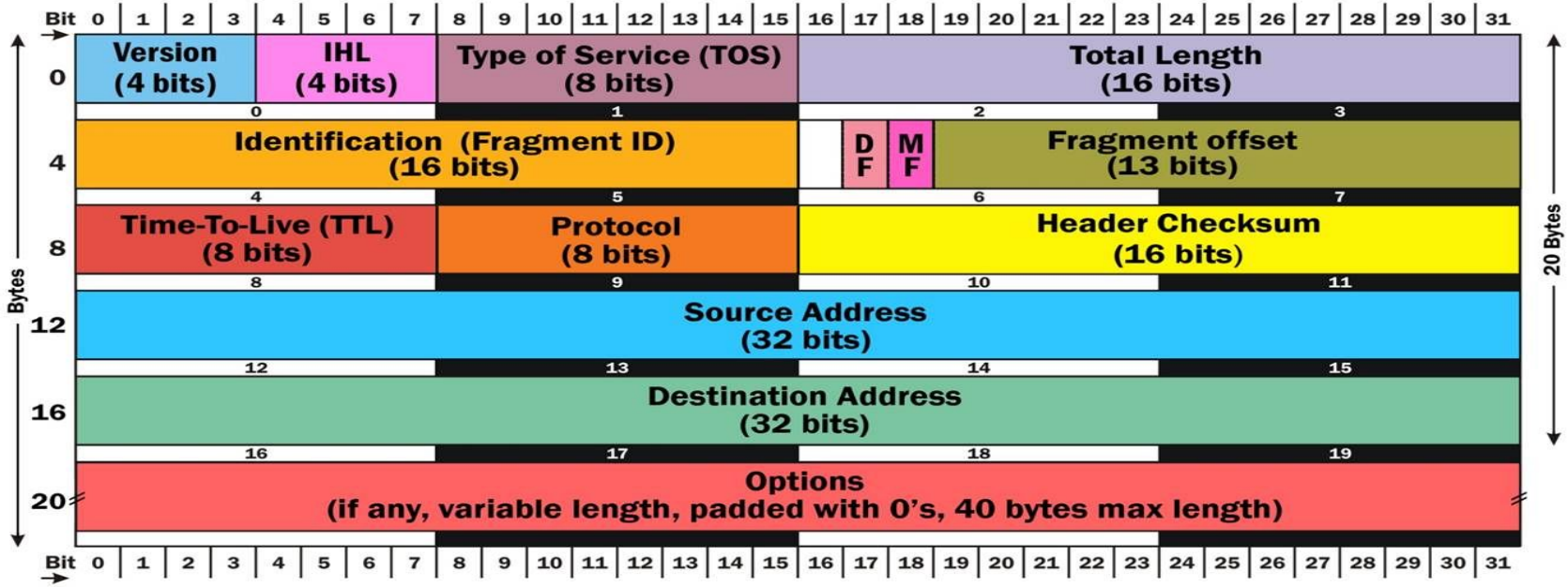
- мережева адресація
- адресація хоста
- маршрутизація
- упаковка даних для передачі
- фрагментація пакетів для передачі та повторної збірки пакетів

IPv4 Protocols

Відповідає за адресацію та маршрутизацію пакетів.



IPv4 Packet Header



Real life example IPv4 Packet Header

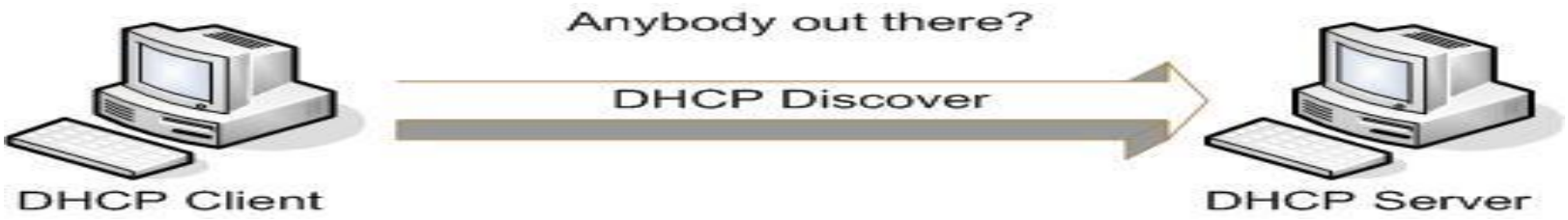
```
⊟ Internet Protocol Version 4, Src: 192.168.82.147 (192.168.82.147), Dst: 192.243.232.2 (192.243.232.2)
    Version: 4
    Header Length: 20 bytes
  ⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 1155
    Identification: 0x69de (27102)
  ⊟ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊟ Header checksum: 0xd064 [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 192.168.82.147 (192.168.82.147)
    Destination: 192.243.232.2 (192.243.232.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Transmission Control Protocol, Src Port: 57487 (57487), Dst Port: 80 (80), Seq: 1102, Ack: 883, Len: 1115
```

DHCP

- **Список адрес, доступних для призначення. Область також може включати адреси, зарезервовані для конкретних комп'ютерів, та інші параметри конфігурації TCP/IP.**

DHCP Discover message

DHCP Discover.



DHCP Offer

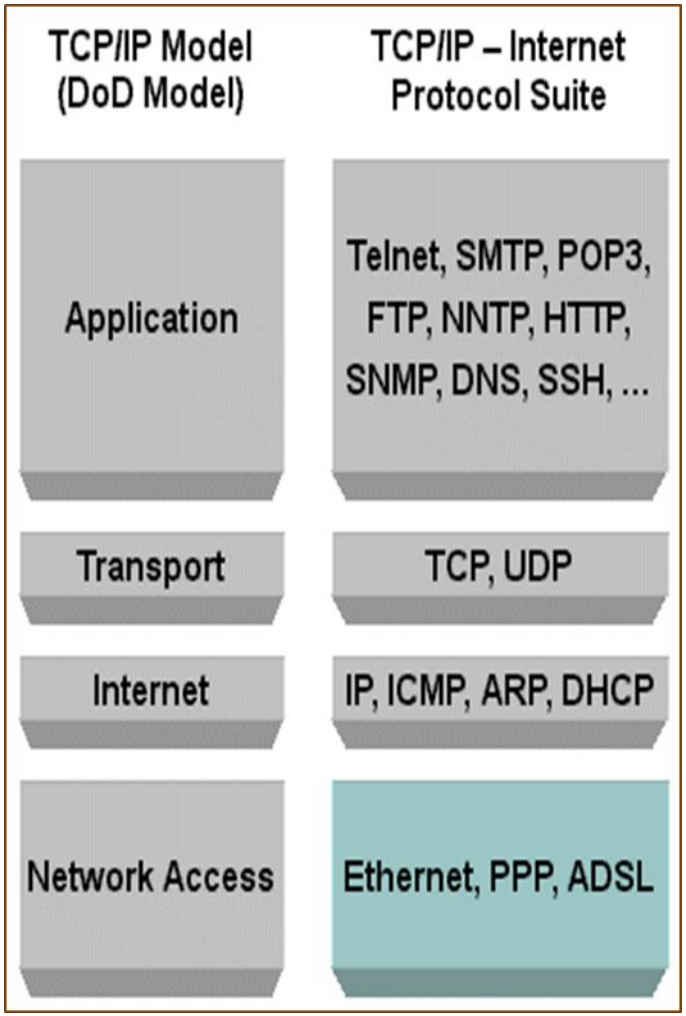
DHCP Request message

DHCP Ack

DHCP

UDP 67
I need IP address settings
DHCP Client
DHCP Server
UDP 68
I can offer to you:
• IP address
• Subnet Mask
• Default Gateway
• DNS server IP

TCP/IP Model. Transport Layer



Надає послуги дейтаграм (пакет даних, що містять інформацію призначення та маршрутизації) для протоколів Прикладного рівня.

TCP

- **Встановлює зв'язок між хостами**
- **Забезпечує послідовність та підтвердження**
- **Відновлює втрачені пакети шляхом повторної передачі**

UDP

- **Протокол без з'єднання, який надсилає дані лише в надії на їх отримання.**

Transport Layer

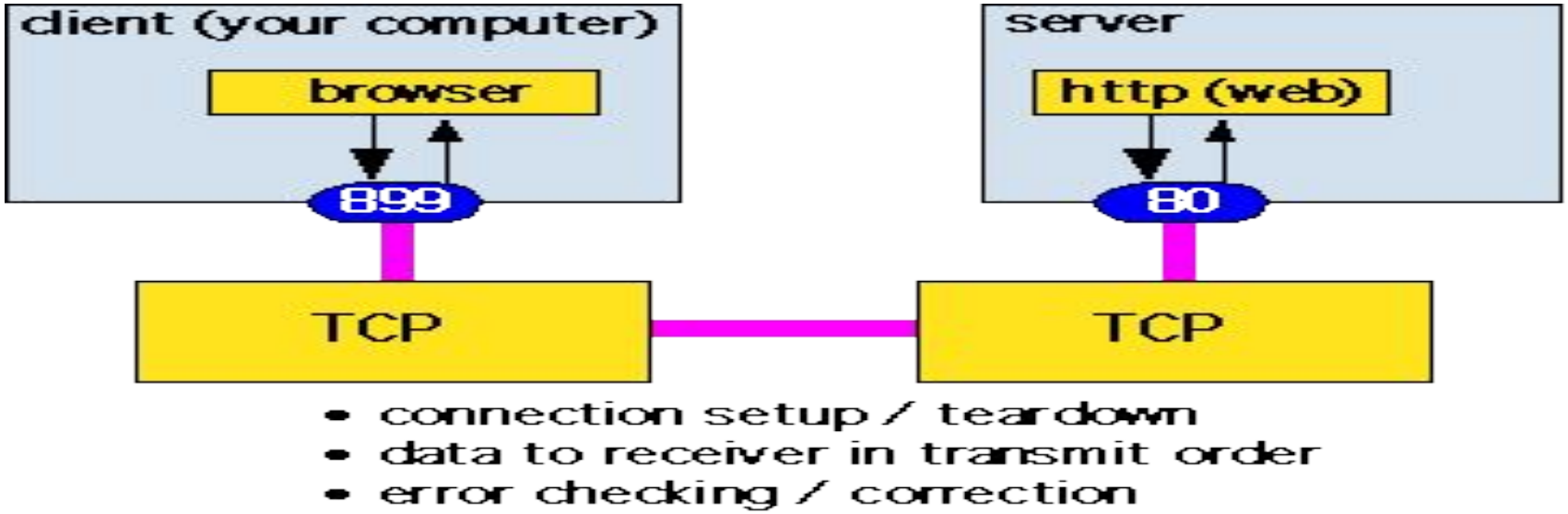
Транспортний рівень може підготувати дейтаграми для передачі без з'єднання або орієнтованого на з'єднання.

Транспортний рівень забезпечує доставку повідомлень у порядку їх надсилання та відсутності втрат чи дублювання.

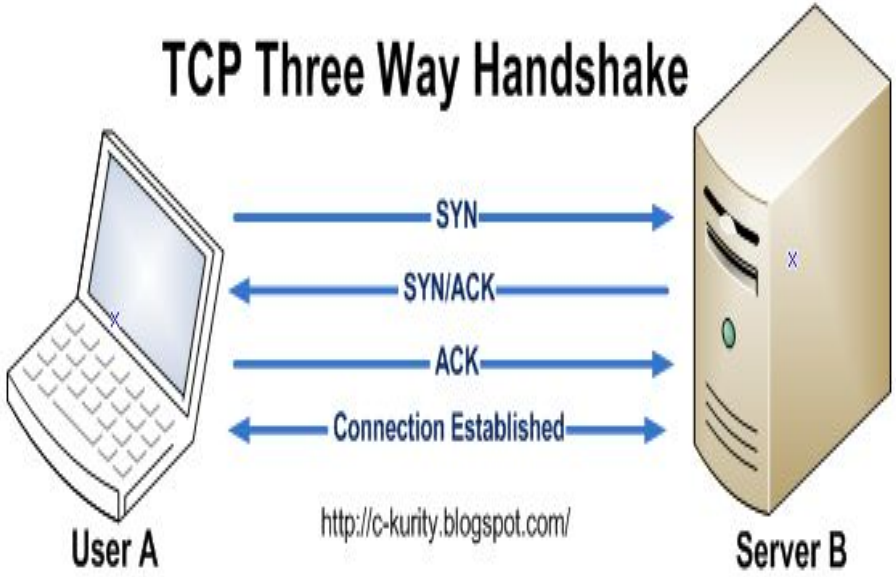
- **TCP - це протокол, орієнтований на з'єднання, який встановлює сеанс зв'язку між відправником і одержувачем.**
- **UDP - це протокол без з'єднання, який надсилає дані лише в надії на їх отримання.**
- **TCP і UDP можуть передавати дейтаграми для IPv4 та IPv6 у відповідний час.**

Transmission Control Protocol (TCP)

- **Встановлення з'єднання між двома хостами.**
- **Передача даних. Послідовність і підтвердження пакетів.**
- **Повторна відправка пакетів у відповідь на помилки.**
- **Розрив з'єднання.**

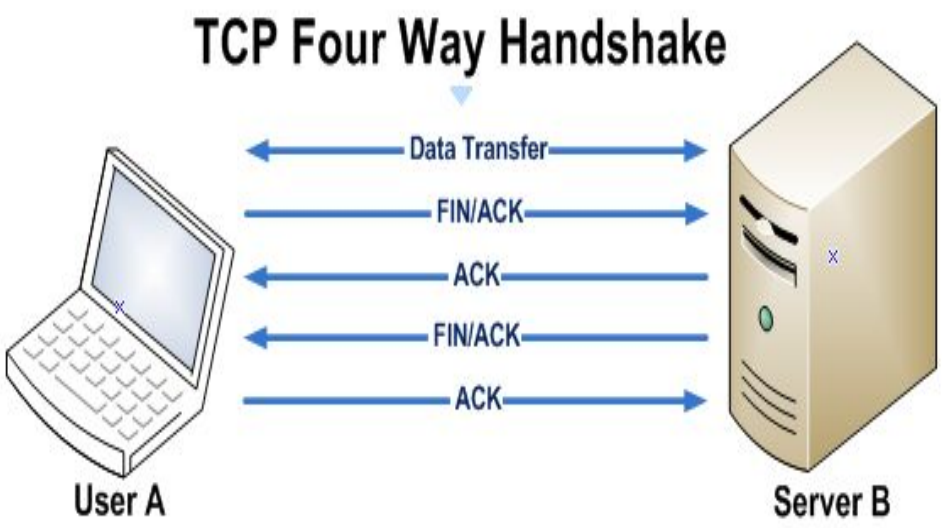


Establish connection



EVENT
Host A **sends** a TCP **SYN**chronize packet to Host B
Host B receives A's **SYN**
Host B **sends** a **SYN**chronize-**ACK**nowledgement
Host A receives B's **SYN-ACK**
Host A **sends** **ACK**nowledge
Host B receives **ACK**. *TCP socket connection is **ESTABLISHED**.*

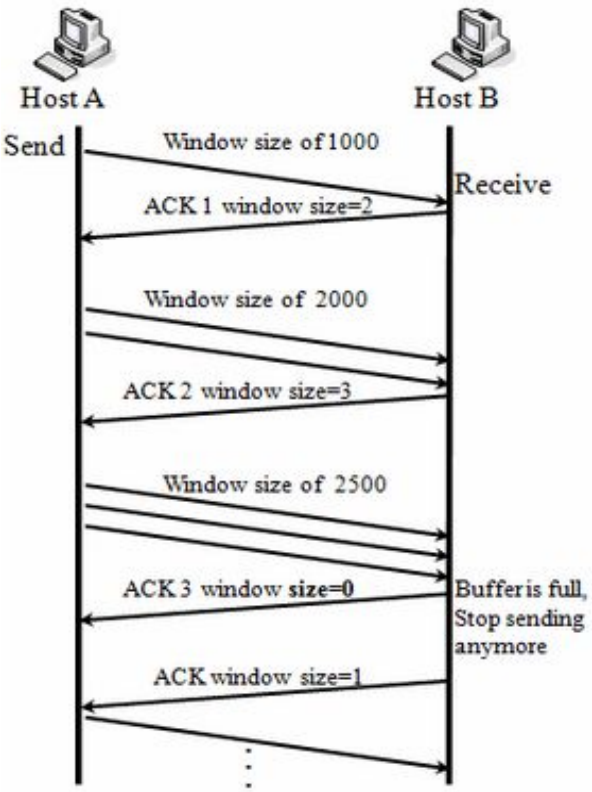
Termination connection



- FIN bit says no more data to send
  - Caused by close() or shutdown() on other end
- Both sides must send FIN to terminate a connection
- Typical teardown exchange:
  - A → B: FIN, seq S_A, ack S_B
  - B → A: ack S_{A+1}
  - B → A: FIN, seq S_B, ack S_{A+1}
  - A → B: ack S_{B+1}
- Can also have simultaneous close
- Can A and B forget about closed socket after final message?

Data transmission

Коли з'єднання встановлено, одержувач вказує поле вікна (window field) (див. формат заголовка TCP) у кожному кадрі TCP. Віконний механізм використовується для управління потоком даних. Розмір вікна являє собою кількість прийнятих даних, які одержувач готовий зберігати в буфері. розмір вікна (у байтах) надсилається відправнику разом із підтвердженнями.



TCP Header

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			N S	C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20	160	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.)																															
...	...	...																															

Destination port address

- **Well Known Ports** є такими у діапазоні **0-1024**.
- **Registered Ports** є такими у діапазоні **1025-49151.**
- **Private Ports** є такими у діапазоні **49152-65535.**

Commonly Used Port Numbers

Port Number	Protocol	Function
21	TCP	FTP (File Transfer Protocol)
22	TCP/UDP	SSH (ssh,scp copy or sftp)
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP (for sending outgoing emails)
43	TCP	WHOIS function
53	TCP/UDP	DNS Server (Domain name service for DNS requests)
67	UDP	DHCP Server
68	TCP	DHCP Client
70	TCP	Gopher Protocol
79	TCP	Finger protocol
110	TCP	POP3 (for receiving email)
119	TCP	NNTP (Network News Transfer Protocol)
143	TCP/UDP	IMAP4 Protocol (for email service)
194	TCP	IRC
389	TCP/UDP	LDAP (light weight directory access)
443	TCP	Secure HTTP over SSL (https)
465	TCP	Secure SMTP (email) using SSL
990	TCP/UDP	Secure FTP using SSL
993	TCP	Secure IMAP protocol over SSL (for emails)
1433	TCP/UDP	Microsoft SQL server port

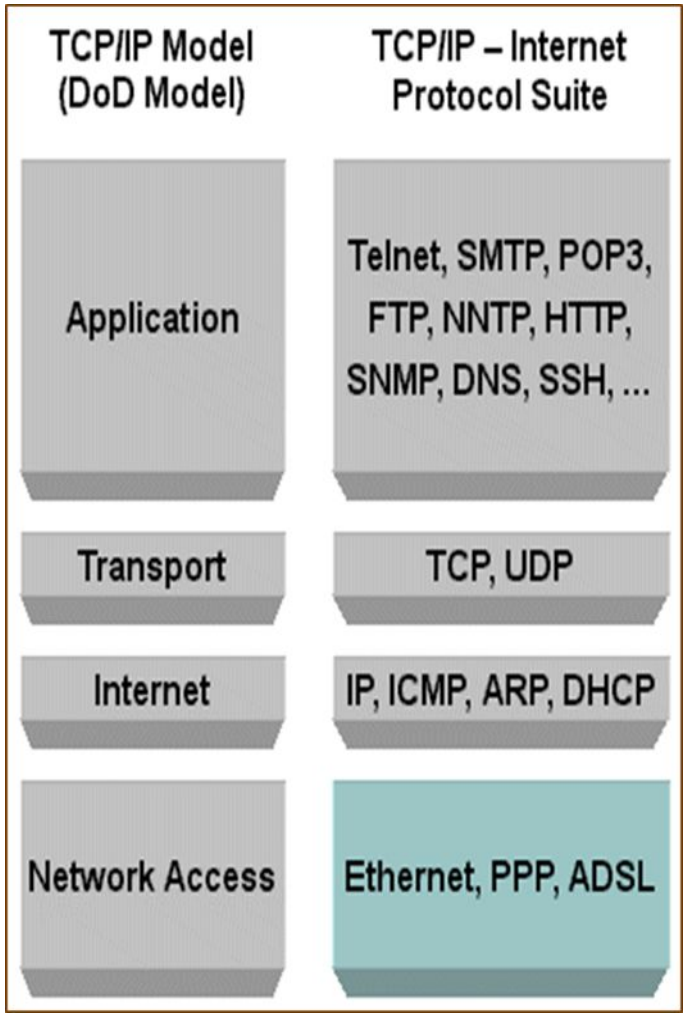
User Datagram Protocol (UDP)

User Datagram Protocol (UDP)

UDP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															

TCP/IP Model. Application Layer



Протоколи Прикладного рівня:

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

Telnet and SSH

Telnet

```
6300 Login: admin
Password: admin
6300>
```

Telnet and SSH

HTTP

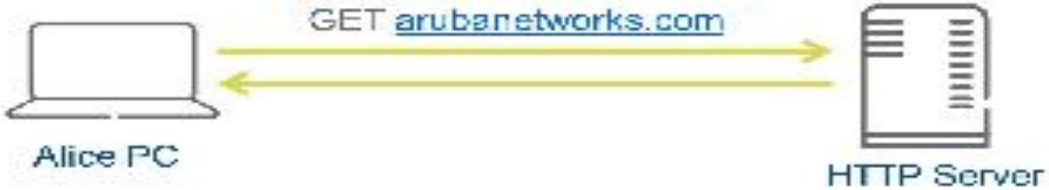
Ease and flexibility

- Users can easily interact with server-provided data
- No special application required – just a simple browser

GET:	Client requests objects
DELETE:	Client requests object deletion
POST:	Servers accept client data
PUT:	Server request write data

TCP 80: Unsecured HTTP

TCP 443: Secure HTTPS



HTTP

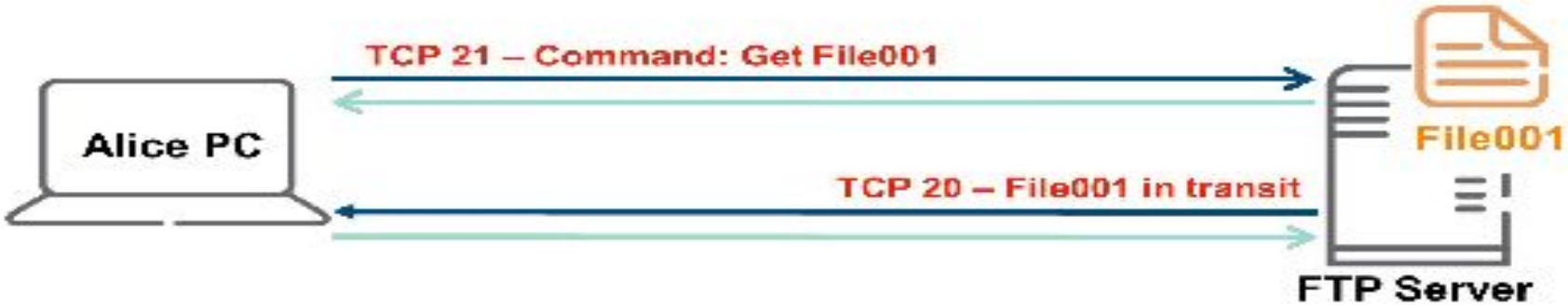
80

443

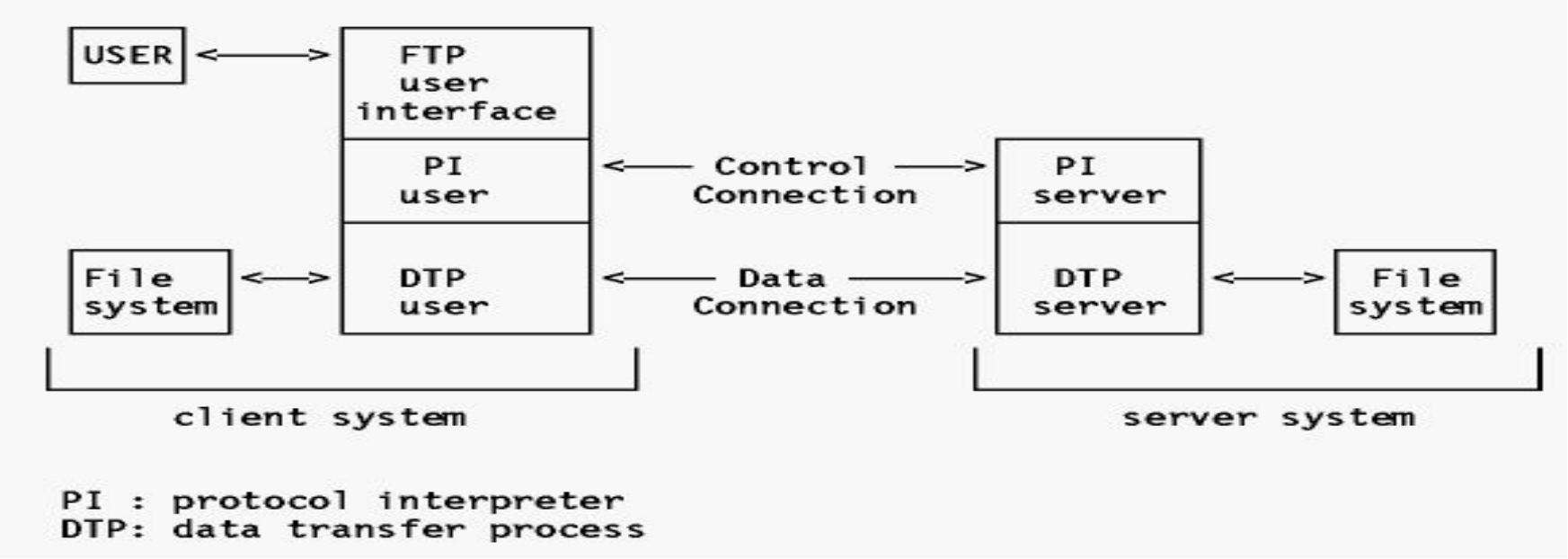
Domain Name Service (DNS)

FTP

Variations	TFTP: Simple, low overhead	UDP port 69
	SFTP: Encryption/Security	TCP port 22



FTP



- **DTP (Data Transfer Process) - це процес, який відповідає за встановлення з'єднання та управління каналом даних.**
- **PI (Protocol Interpreter) - інтерпретує протокол, що дозволяє управляти DTP за допомогою команд, отриманих по каналу управління.**

FTP

- **ASCII (American standard code for information interchange) mode: Використовується для тексту. Перед передачею дані перетворюються з представлення символів відправляючого хоста у "8-розрядний ASCII" .**
- **Binary mode: Машина-відправник посилає кожен байт файлу за байтом, а одержувач зберігає байтовий потік по мірі його отримання .**
- **EBCDIC (Extended Binary Coded Decimal Interchange Code) mode: Використовується для простого тексту між хостами за допомогою набору символів EBCDIC .**

- **Stream mode: Дані надсилаються як безперервний потік, звільняючи FTP від виконання будь-якого процесу .**
- **Block mode: FTP розбиває дані на кілька блоків (заголовок блоку, кількість байтів і поле даних), а потім передає їх TCP .**
- **Compressed mode: Дані стискаються за допомогою простого алгоритму (зазвичай це кодування довжини виконання).**

TFTP

- **Завантажувальні файли для пристроїв без локального сховища**
- **Використовується з мережевим протоколом завантаження Preboot Execution Environment (PXE)**
- **Системи встановлення на основі мережі**

SFTP

Secure File Transfer Protocol (SFTP)

Secure Shell (SSH).

- **Протокол, що забезпечує безпечну автентифікацію та передачу зашифрованих даних для інших протоколів додатків.**

Основи мережних технологій

Switches

- Spanning Tree Protocol (STP)
- Link Layer Discovery Protocol (LLDP)
- 802.1Q tagging protocol

Switches

Multiple ports connect endpoints

- PCs, printers, cameras, and more
- Commonly 8, 24, 48, or more physical ports
- Transparent to endpoints

Special L2 protocols

Performance, reliability, security

- STP
- LLDP
- 802.1q

MAC Address	Port
90:...:01	1
90:...:03	2

Routers

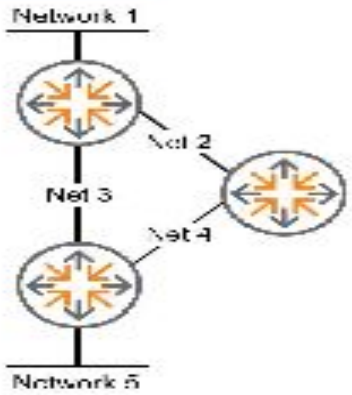
Functionality and features

- Connect separate networks into an inter-network
- Offer WAN connectivity to networks

L3 routing protocols

Learn all possible paths, then choose a best path

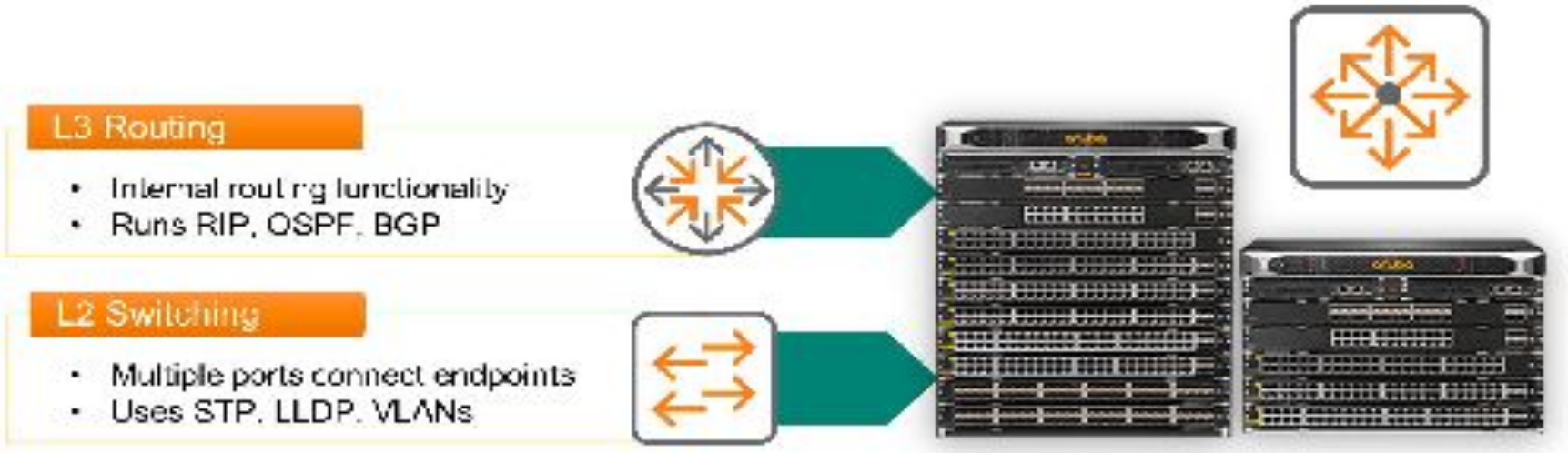
- RIP
- OSPF
- BGP



Routers

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)

Multi-Layer Switch



Multi-Layer Switch

Wireless Access Points

Functionality

- Bridges wireless devices and wired networks.
- Transform Ethernet into Wi-Fi frames and back

Varieties of APs

- Internal or external antennas
- One or Dual Ethernet Ports
- Indoor or outdoor
- Autonomous or Controller-based

Wireless Access Points

Wireless Access Points

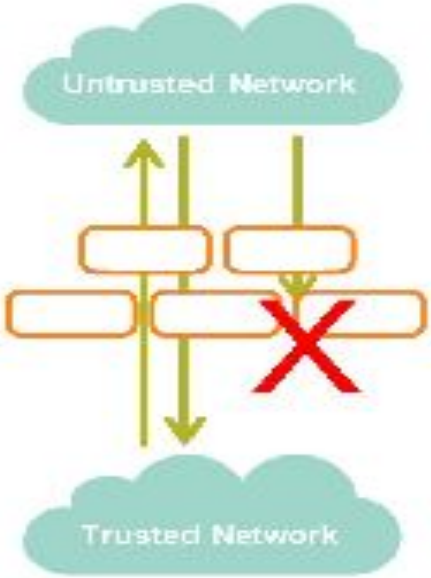
Firewalls

Functionality

- First line of defense between trusted and untrusted networks
- Deep Packet Inspection analyses all OSI layers

Additional features

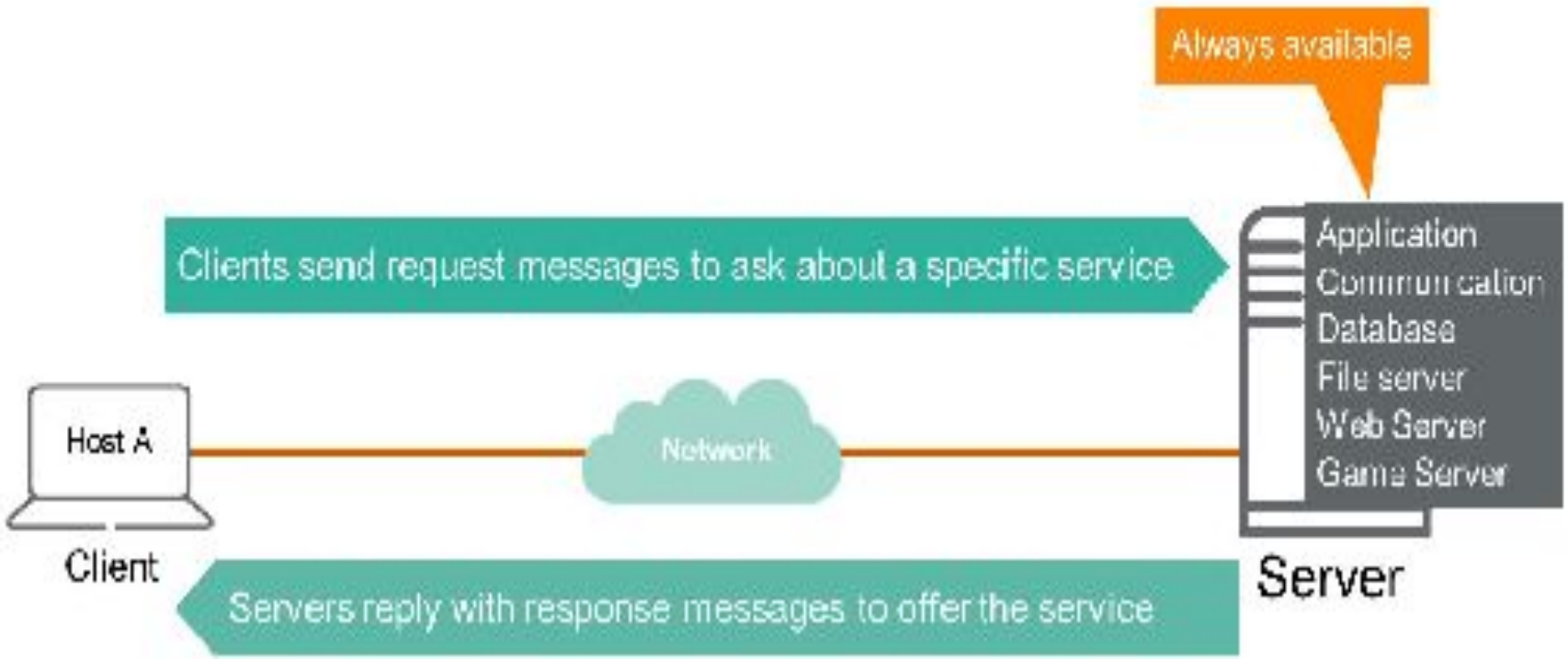
- IDS and IPS
- VPN concentrator
- SSL Proxy



Firewalls

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- VPN Concentrators
- SSL proxy

Servers


Always available
Clients send request messages to ask about a specific service
Application
Communication
Database
File server
Web Server
Game Server
Host A
Network
Client
Server
Servers reply with response messages to offer the service

Servers

- Application Servers
- Communication Servers
- Database Servers
- File Servers
- Web Servers
- Game Servers