Information Technology Institute

ITI

Introduction to
Computer Networks & Cyber Security

Prepared By : Mohamed AboSehly

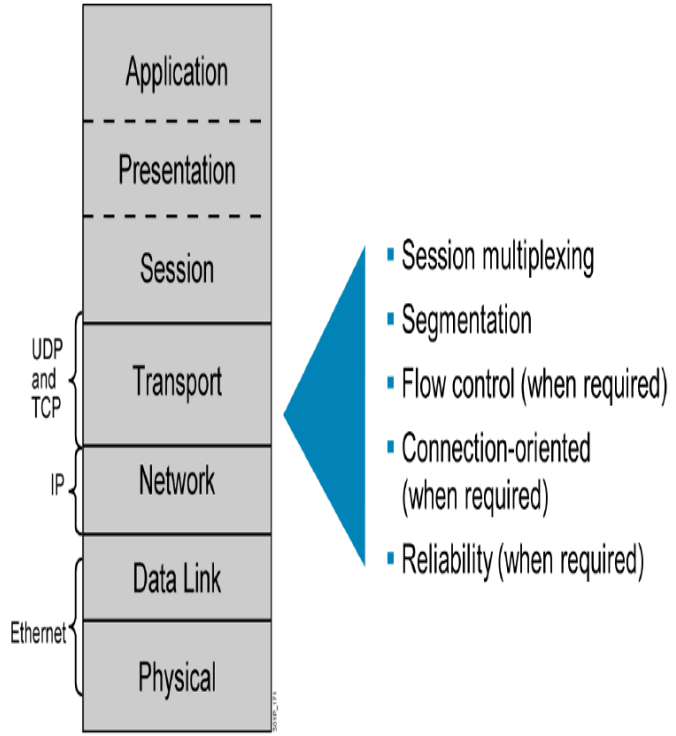
Transport Layer

Basic Network Elements (Software)

Transport Layer

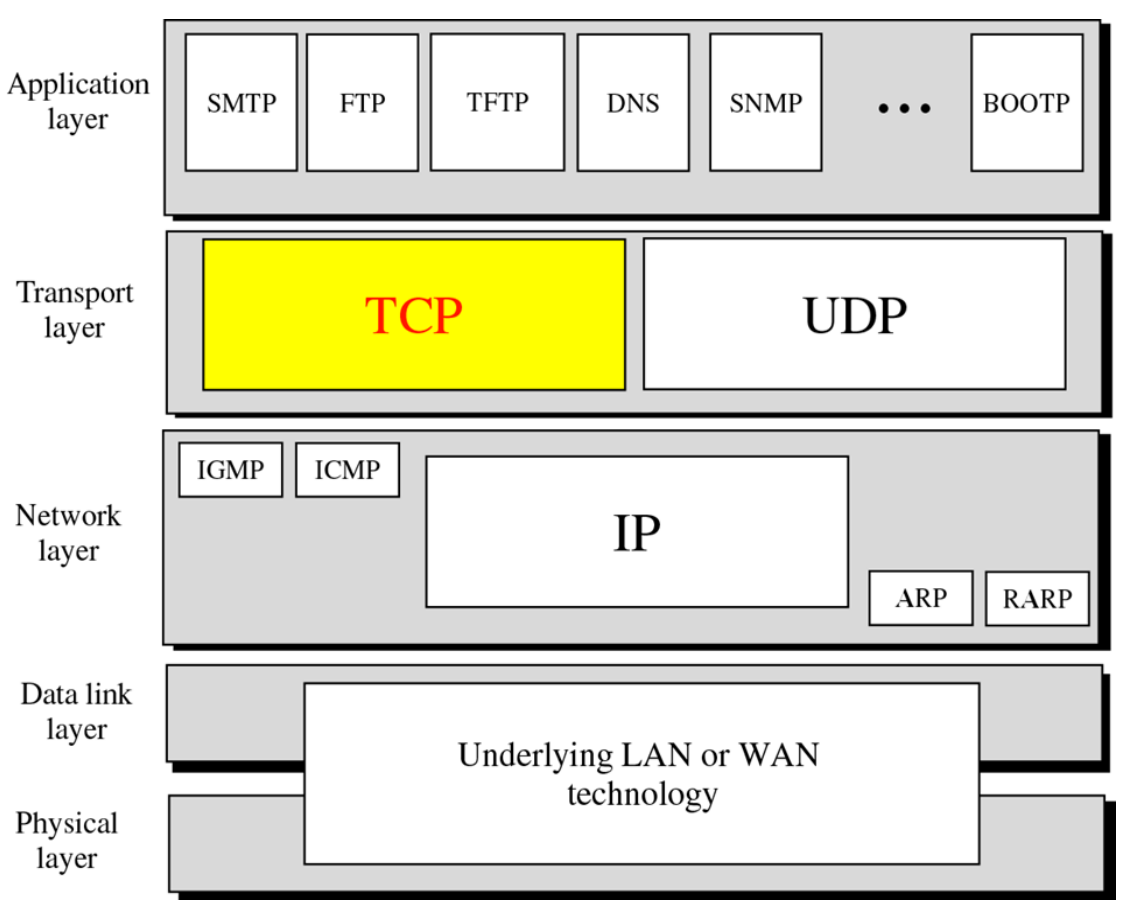
- **Session multiplexing:**
  - open **multiple sessions** using **UDP and TCP**

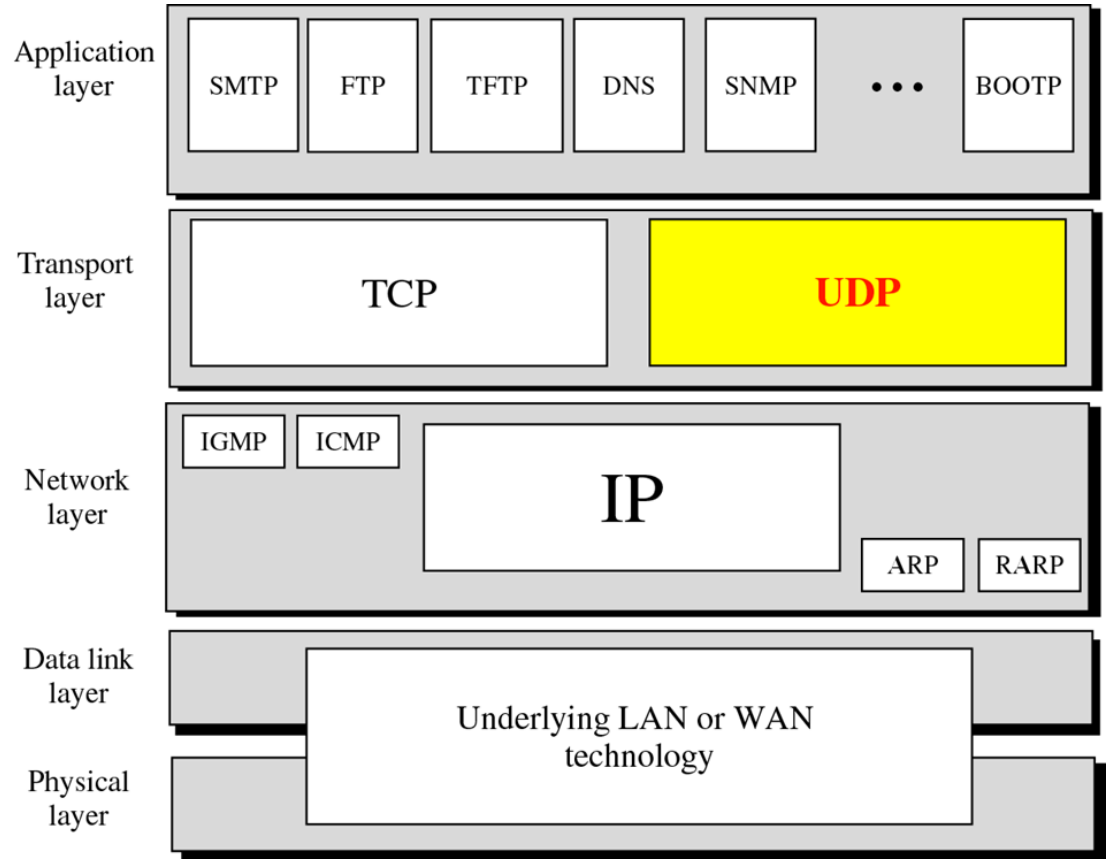
  Example : open **cisco.com & open facebook.com** you are the source using **port 49001** and another **port 49002** on the same machine (session multiplexing).
- **Segmentation:**
  - divided the data up to **multiple segments** to be easier in handling (the maximum performance 1518 byte)
- **Connection Oriented:**
  - To maintain the session with **acknowledgements** that the data are sent to the receiver then terminate the session
- **Reliability:**
  - **Data corrections** and **avoid** the **duplicate data** out of order and data arrangement.



Part 1 (TCP/IP Protocol Architecture)

TCP/IP Protocol Architecture





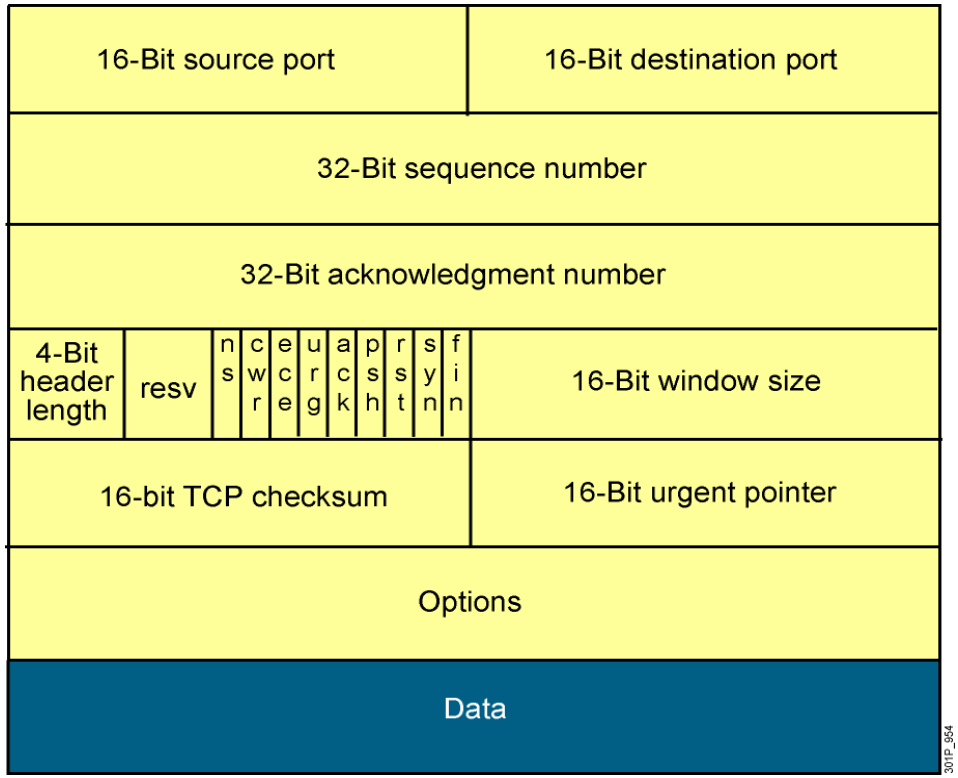
Part 1 (TCP/IP Protocol Architecture)

TCP Characteristics

- Transmission Control Protocol
- Transport layer protocol
- Use port numbers
- Reliable (Acknowledgement of receipt)
- **Connection oriented(**synchronization)
- **Full duplex**
- Error control(Error checking(checksum)
- **Flow control**
  - Data-recovery features
  - Sequencing of data packets

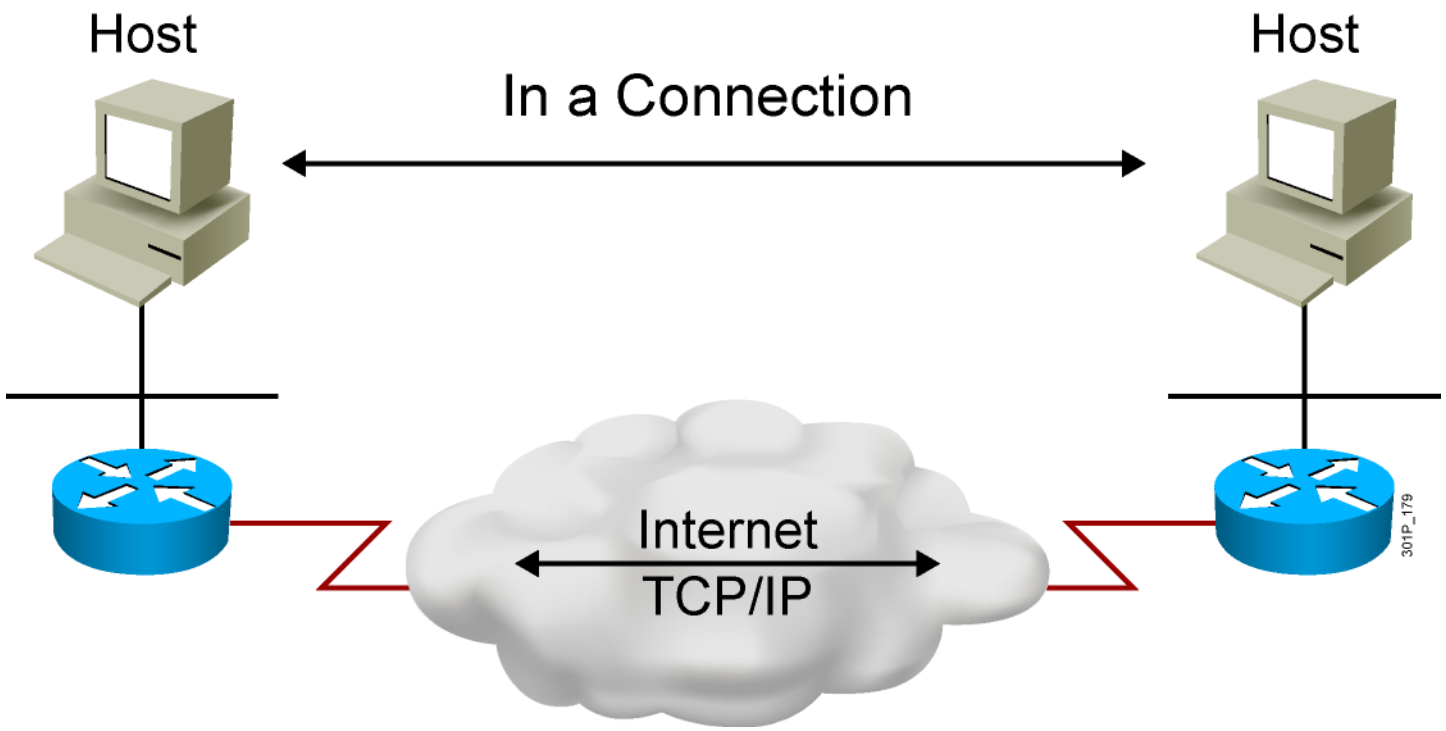
No internet

TCP Header



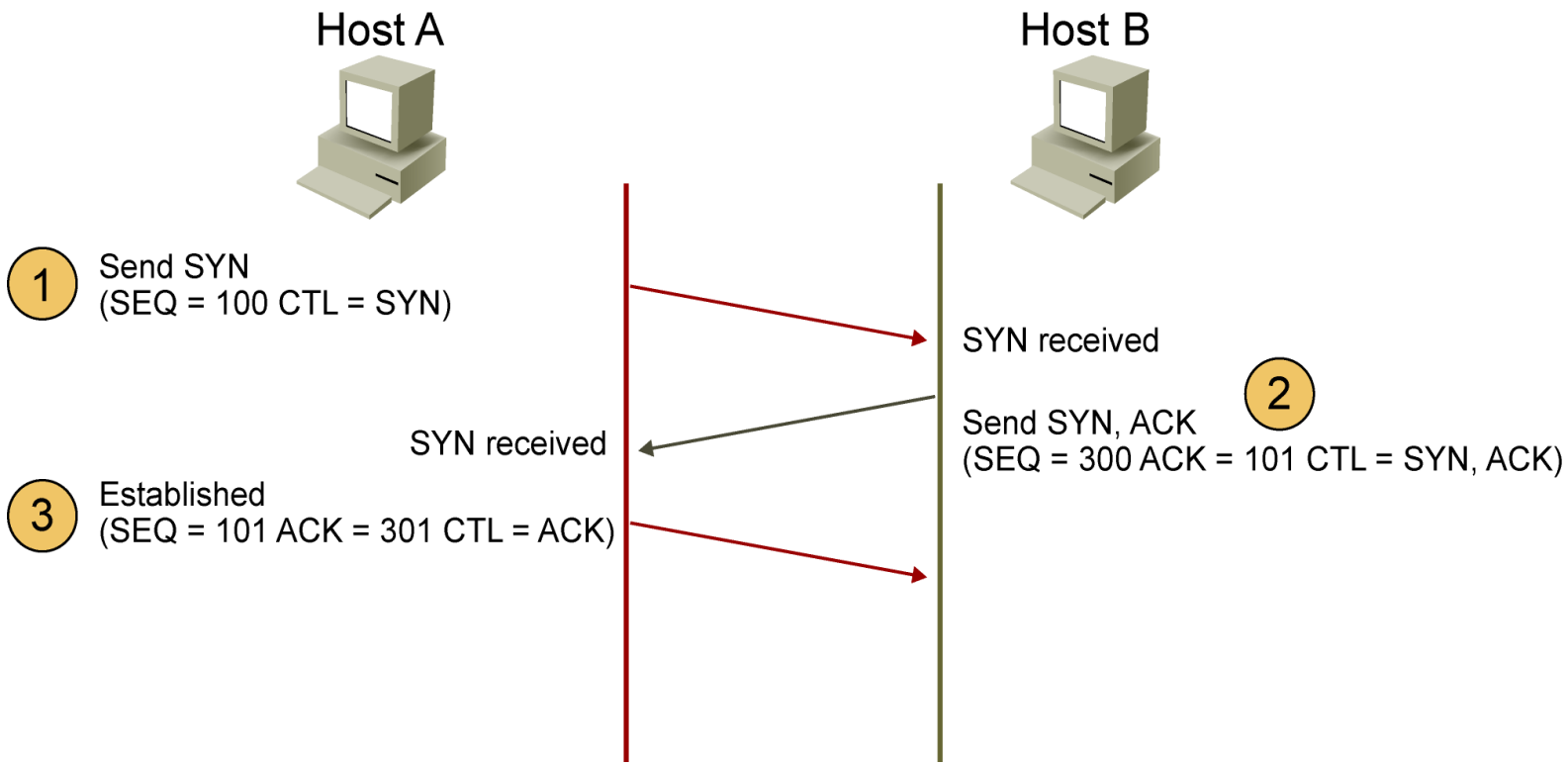
Part 1 (TCP/IP Protocol Architecture)

ESTABLISHING A CONNECTION



Part 1 (TCP/IP Protocol Architecture)

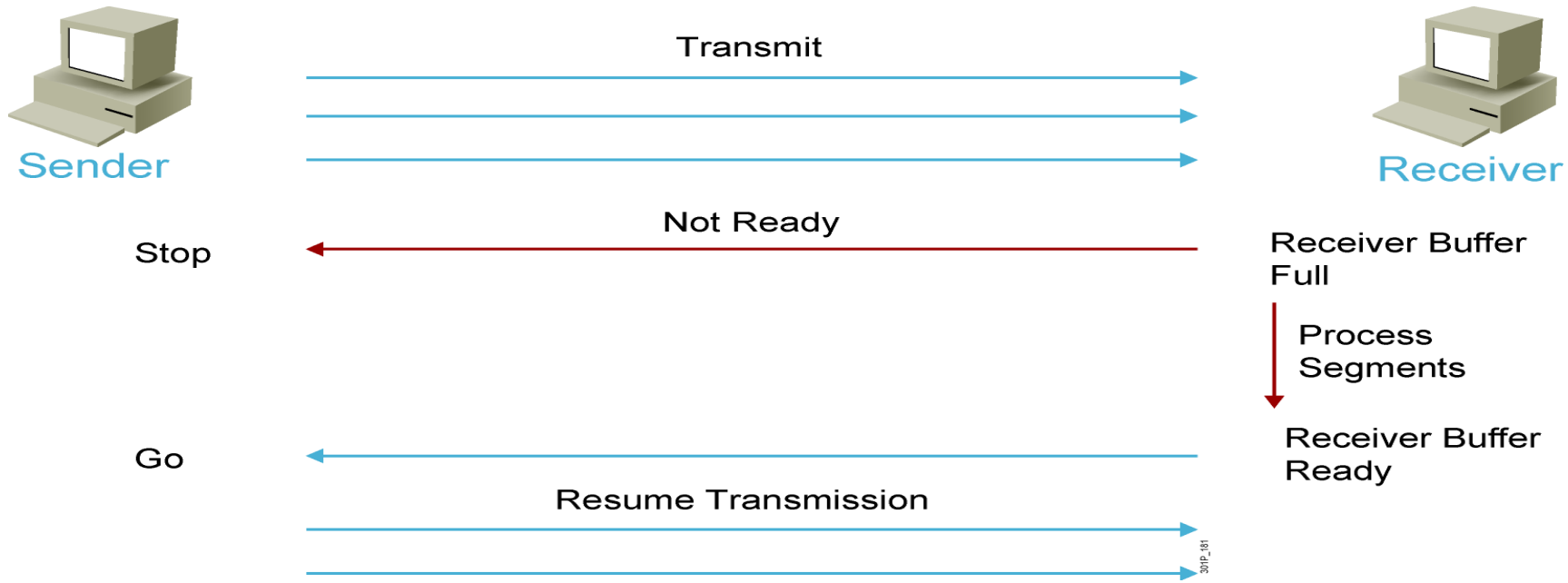
THREE-WAY HANDSHAKE



CTL = Which control bits in the TCP header are set to 1

Part 1 (TCP/IP Protocol Architecture)

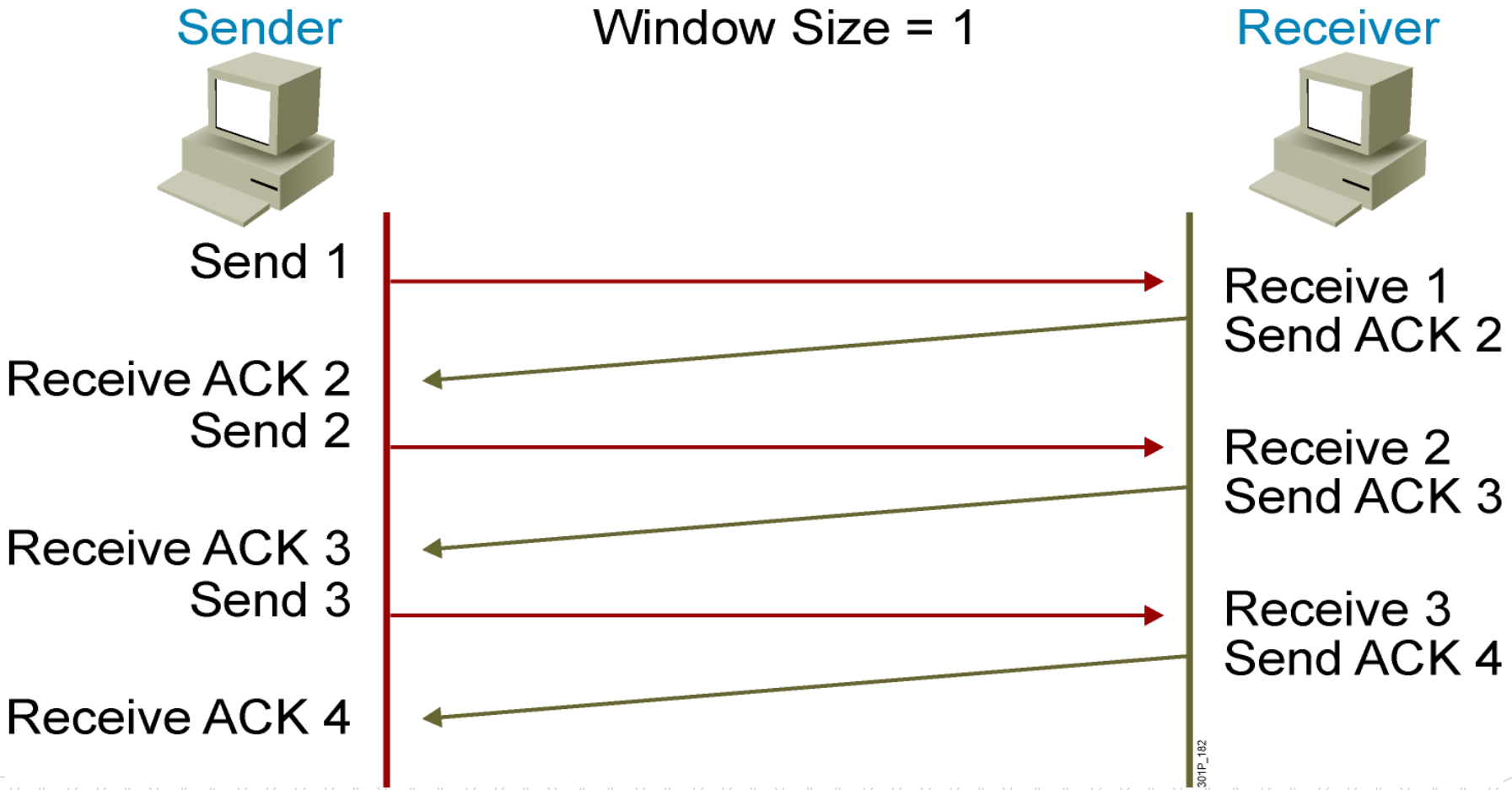
Flow Control



Flow Control:

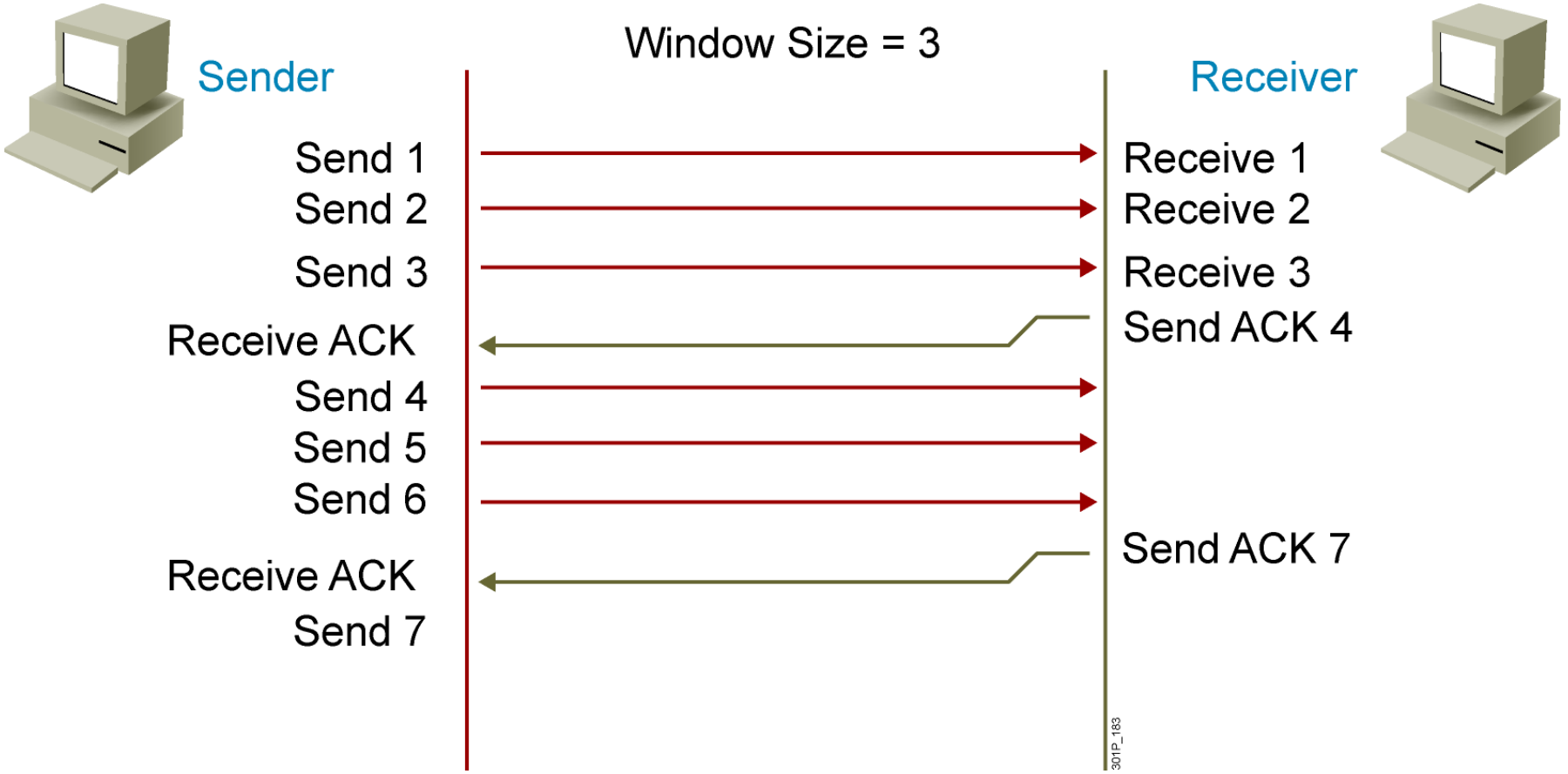
If the transmitter is sending data faster than the receiver so the receiver will drop the data and the retransmitting will waste time and network resources. The Round trip time will be very slow so we used **TCP windowing**

TCP Acknowledgment

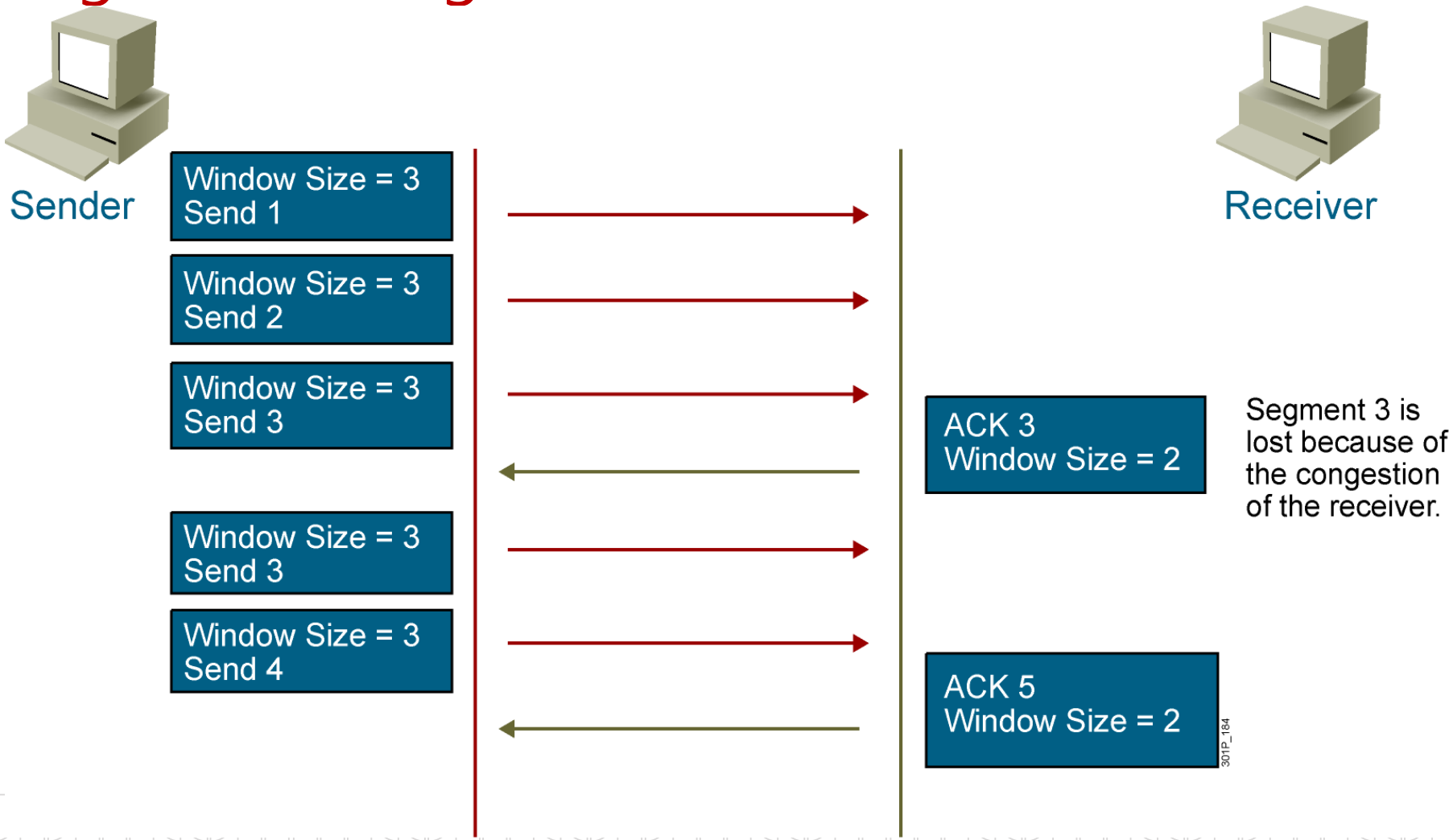


Part 1 (TCP/IP Protocol Architecture)

Fixed Windowing



TCP Sliding Windowing

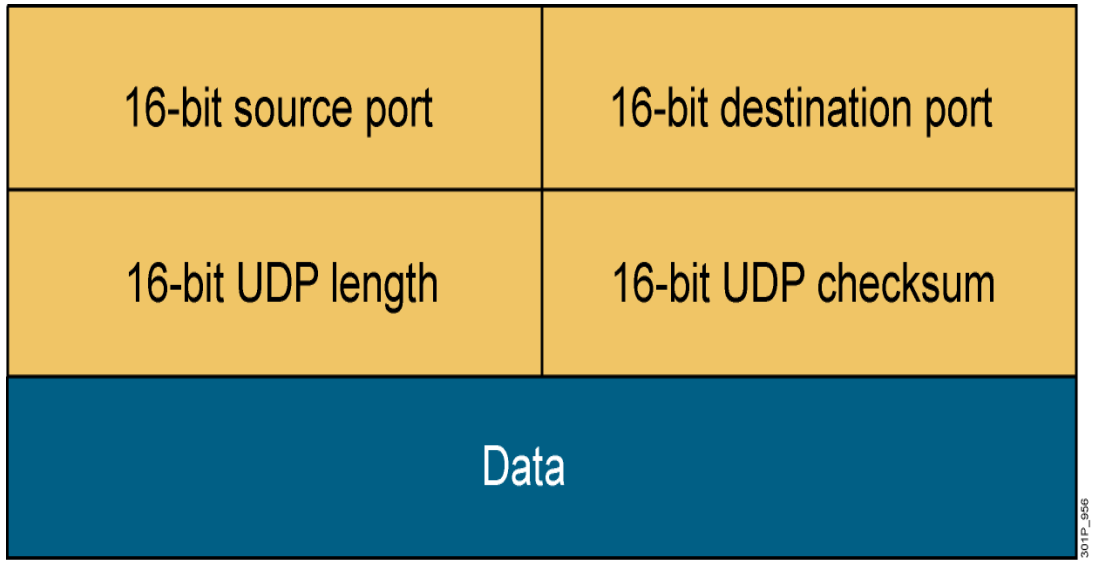


Part 1 (TCP/IP Protocol Architecture)

UDP Characteristics

- User Datagram Protocol / Transport layer protocol
- Process to process communication
  - Use port numbers
- **Connectionless** (no notification)
- Unreliable
- **Perform very limited error checking**
- Very simple using a minimum of overhead
- Provides best-effort delivery
    - The data may be dropped due to:
        - Routing Error,
        - Duplicate data due to redundancy
        - Data loss in its way due to TTL.
- **Has no data-recovery features**

UDP Header

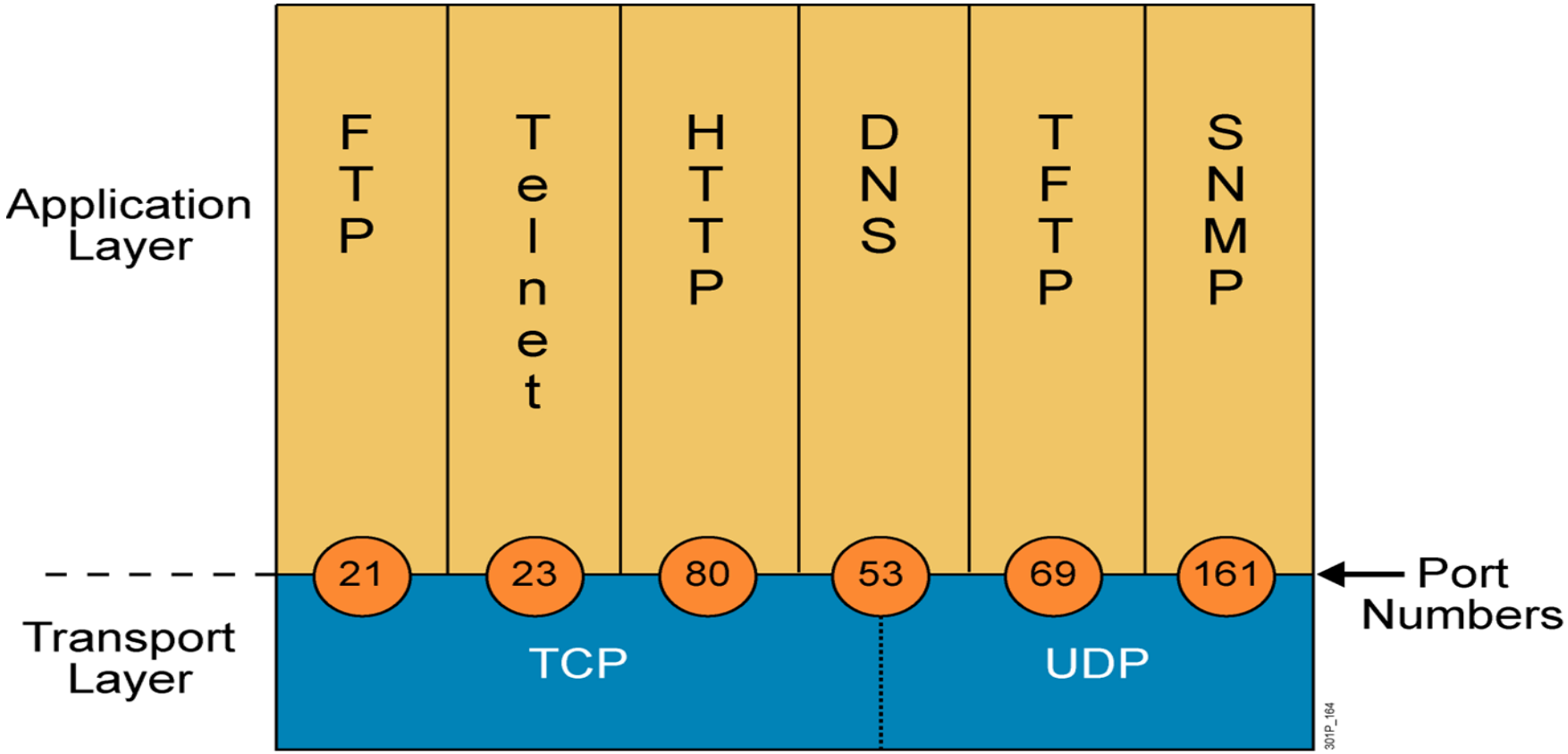


Part 1 (TCP/IP Protocol Architecture)

TCP (Reliable) vs. UDP (Best-Effort Comparison)

	Reliable	Best-Effort
Connection Type	Connection-oriented	Connectionless
Protocol	TCP	UDP
Sequencing	Yes	No
Uses	▪ E-mail ▪ File sharing ▪ Downloading	▪ Voice streaming ▪ Video streaming

Mapping Layer 4 to Applications

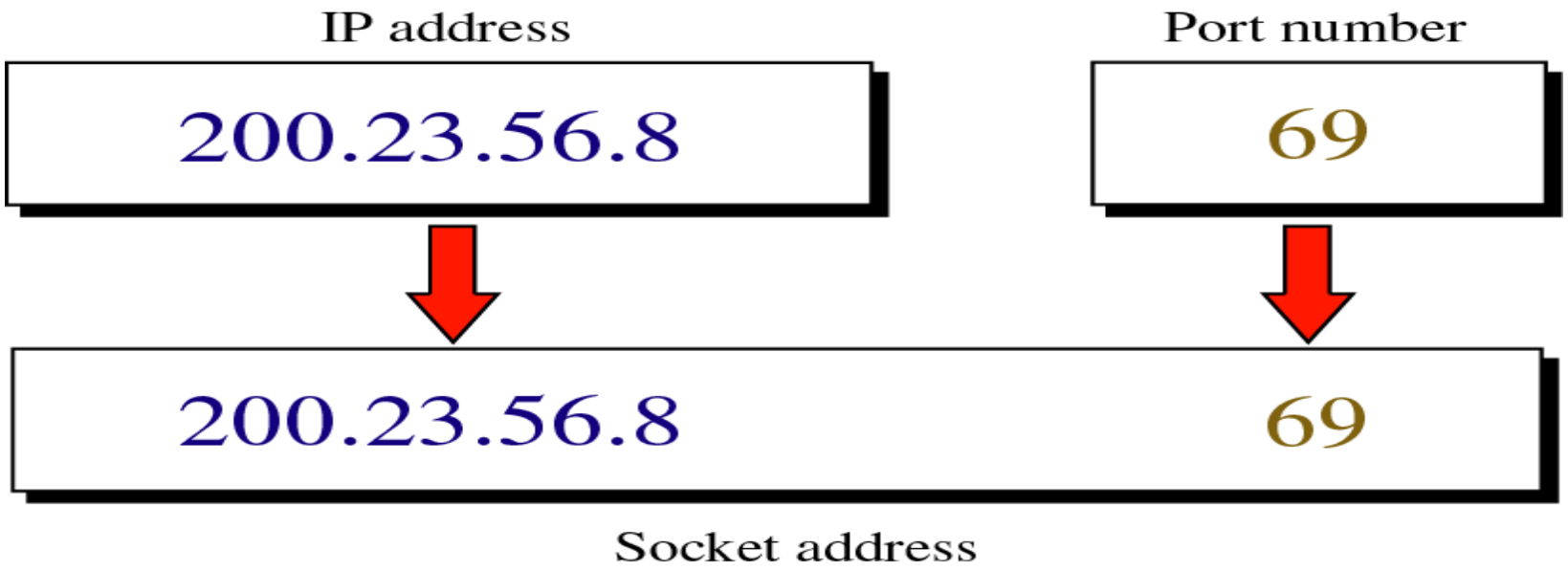


Port Numbers

- **Well Known ports**
  - Range from 0 to 1,023 are assigned and controlled by ICANN
- **Registered ports**
  - Range from 1,024 to 49,151 not assigned or controlled by ICANN but can be registered at ICANN to avoid duplication
- **Dynamic ports**
  - Range from 49,152 to 65,535 are neither controlled nor registered

- https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Socket Address



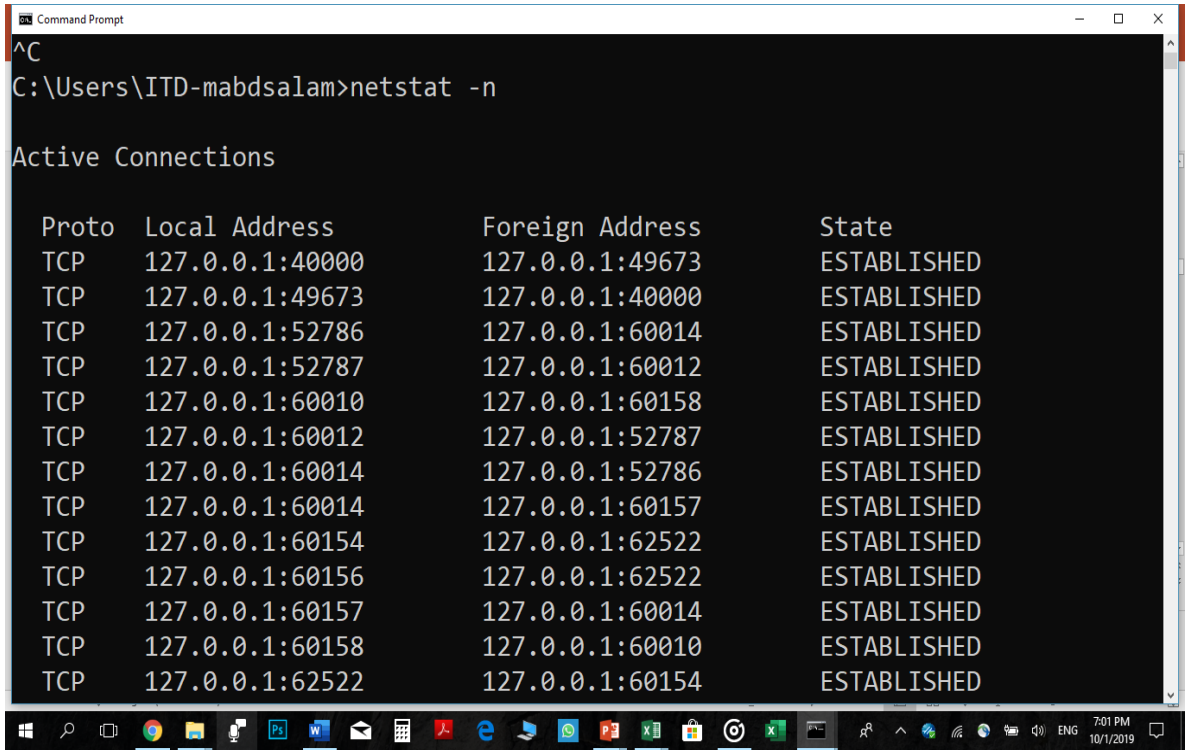
Part 1 (TCP/IP Protocol Architecture)- LAB

❖ NETSTATE

netstat –n

netstat -a

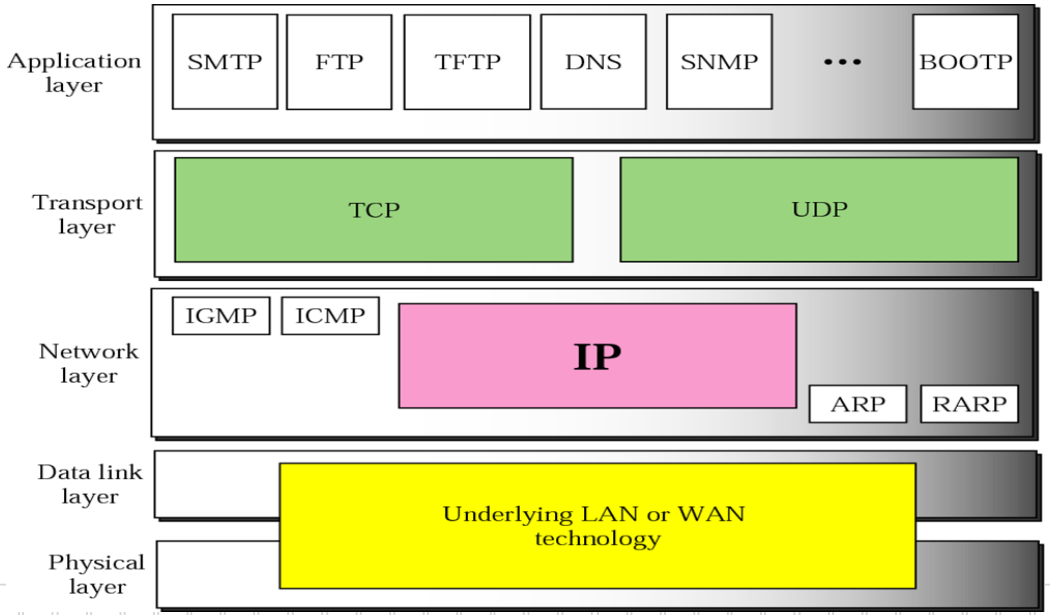
To know session and ports on your device

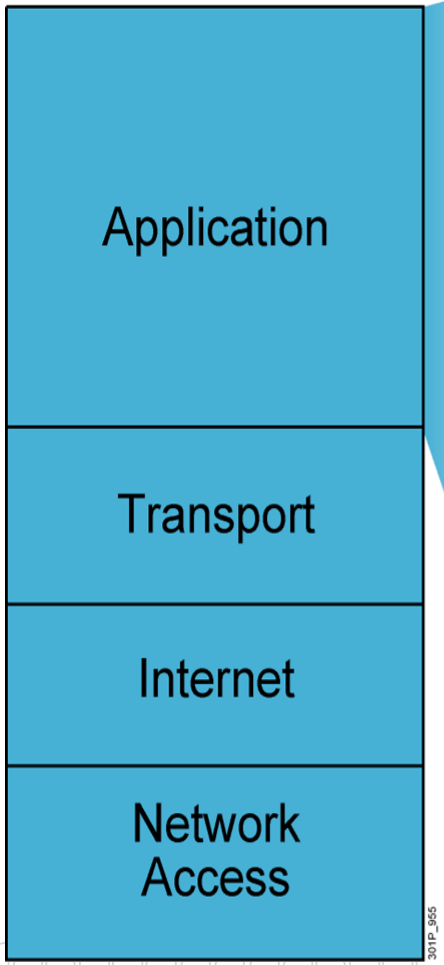


Application Layer

TCP/IP Protocol Architecture

- Application Layer
  - Communication between processes or applications





Application Layer Protocols

- File transfer
  - FTP
  - TFTP
  - Network File System
- E-mail
  - Simple Mail Transfer Protocol
- Remote login
  - Telnet
  - rlogin
- Network management
  - Simple Network Management Protocol
- Name management
  - Domain Name System

Part 1 (TCP/IP Protocol Architecture)

Internet Services (Client/Web Server)

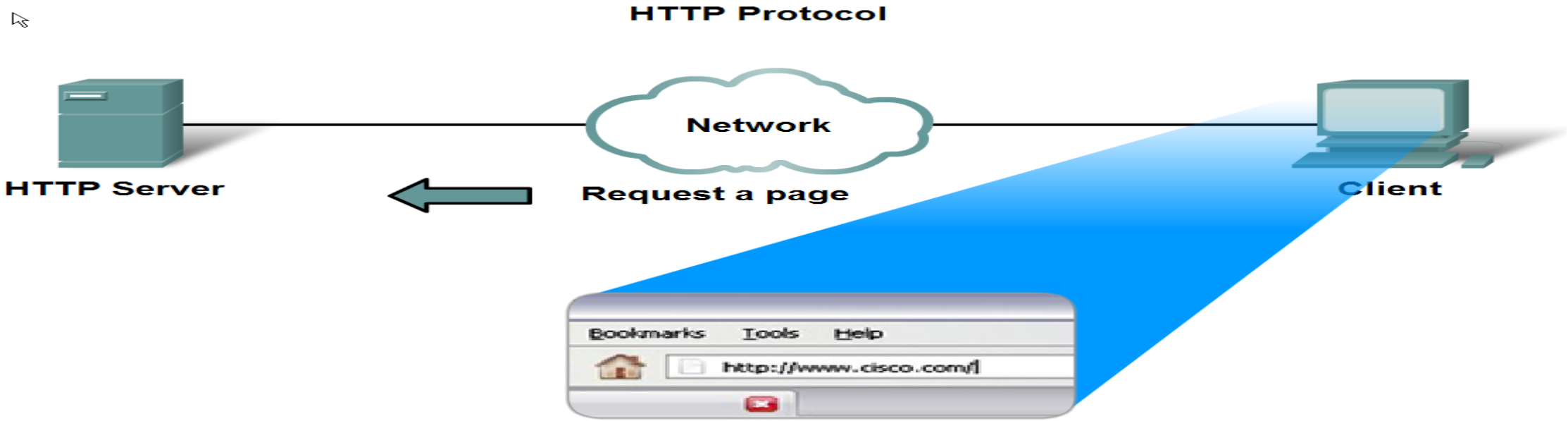
- The World Wide Web: HTTP
- Naming Service: DNS
- File Transfer: FTP
- Telnet Service
- Electronic Mail service: IMAP, POP3, SMTP

Client	Protocol	Server	Port No
Browser	HTTP	WEB	80
Browser	FTP	FTP	21
Browser Or Outlook Express Microsoft Outlook	HTTP SMTP POP3 IMAP4	Mail	110 143 25
Telnet	Telnet	Telnet	23

Part 1 (TCP/IP Protocol Architecture)

HTTP Protocol

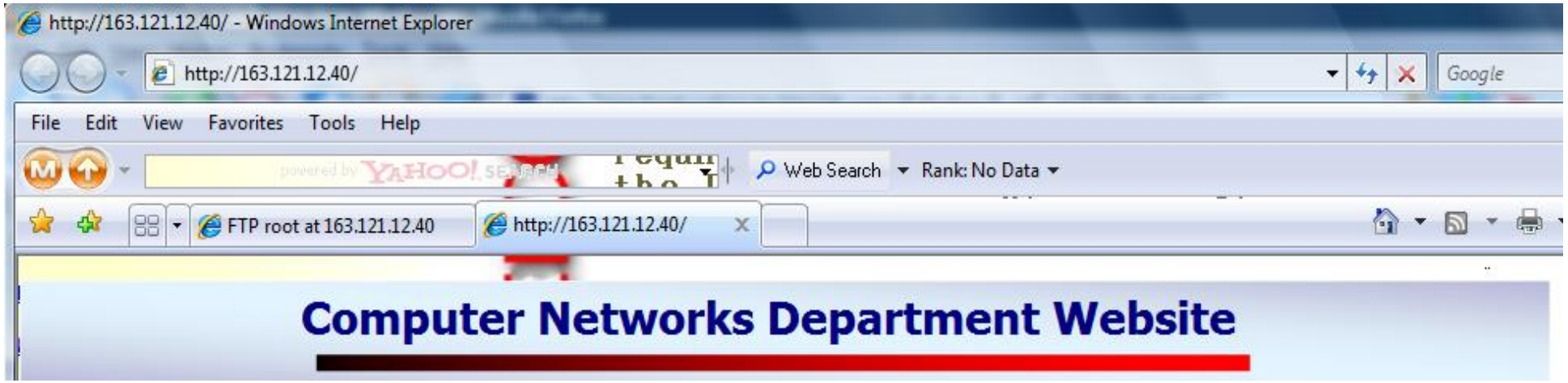
- Hyper Text Transfer Protocol
- Supports the delivery of web pages to the client



Part 1 (TCP/IP Protocol Architecture)

Browser as a web client

- Use Internet Browser as WEB client.



Part 1 (TCP/IP Protocol Architecture)

URL

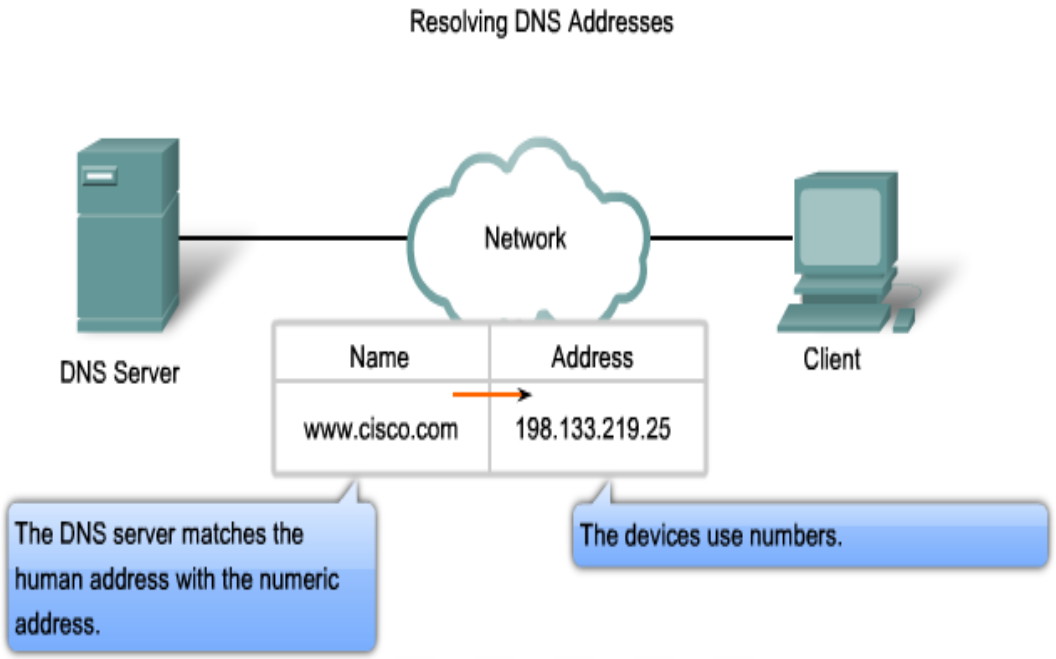
https://www.microsoft.com/ar-ww/microsoft-365/

- URL is **Universal Resource Locator**
- **Protocol** : HTTP, HTTPS or FTP
- **Host** : is the domain name of the computer on which the information is located .
- **Port**: The URL can optionally contain the port number of the server
- **Path**: is the pathname of the file where the information is located

Part 1 (TCP/IP Protocol Architecture)

DNS

- Domain Name Servers
  - Application specified in the TCP/IP suite
  - A way to translate **human-readable** names into **IP addresses**

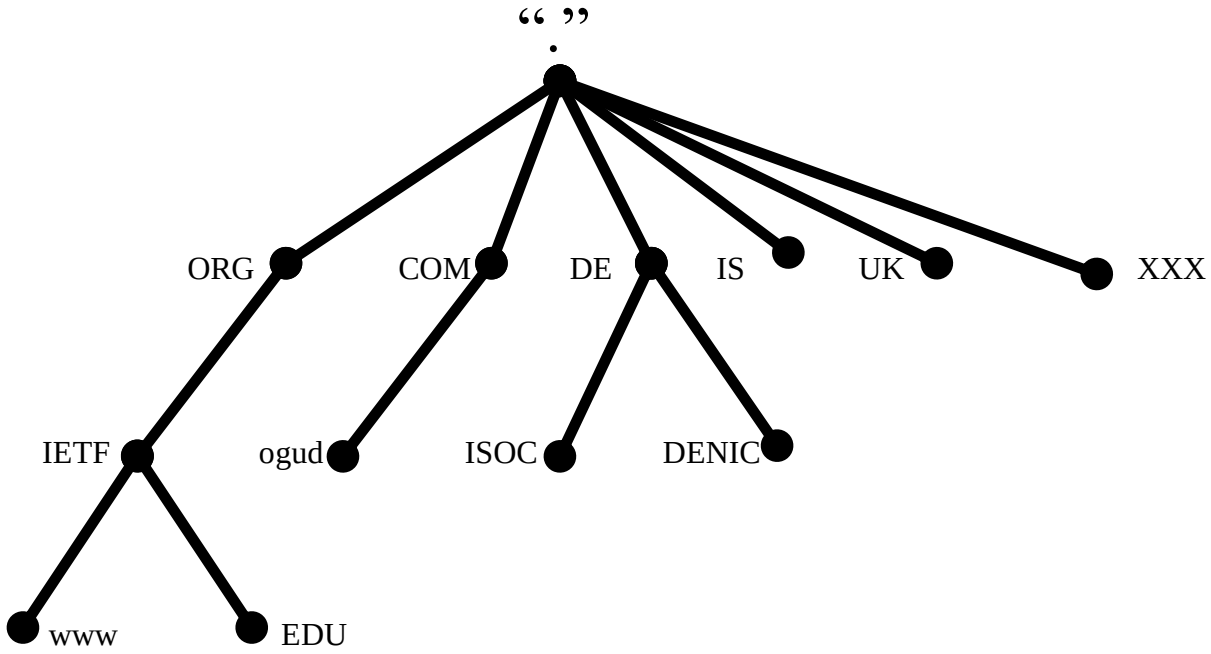


Part 1 (TCP/IP Protocol Architecture)

List of Top Level Domains (TLDs)

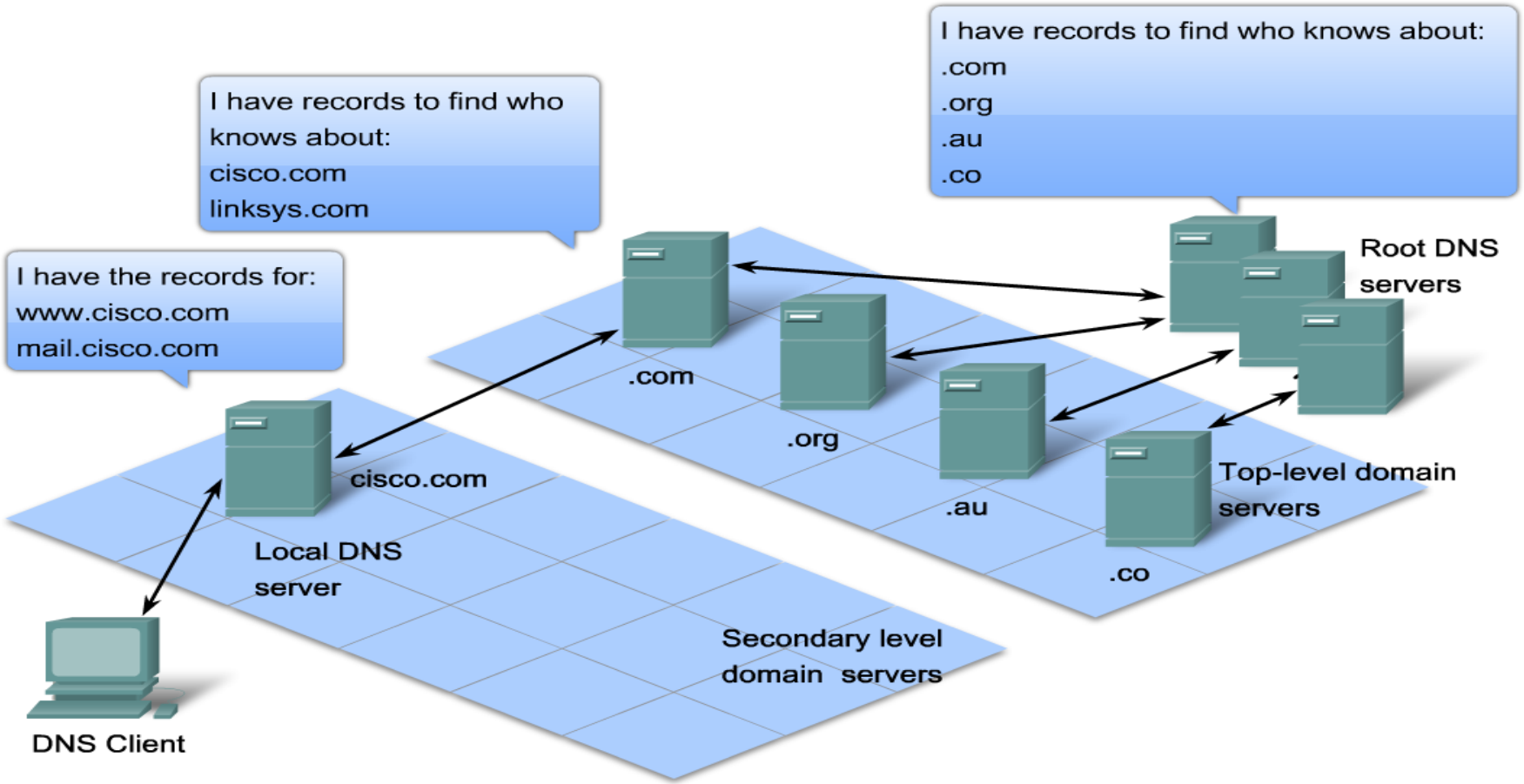
Domain Name	Assigned To
com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military group
net	Major network support center
org	Organization other than those above
country code	A country

DNS Tree



Part 1 (TCP/IP Protocol Architecture)

DNS Query



A hierarchy of DNS servers contains the resource records that match names with addresses.

How DNS works?

- At the beginning they use Hosts file, It maps the IP addresses to host names
- It is found at C: Windows\System32\drivers\etc
  - **Problems**:
    - Huge number of hosts
    - Update very dynamic
    - Searching will be too slow
- **So hosts file can be used in local networks**

- DNS Server is used for **centralize** the Domain Name Servers.
- DNS are used to convert the **addresses** into **IP addresses and vice versa**

Part 1 (TCP/IP Protocol Architecture)_Lab

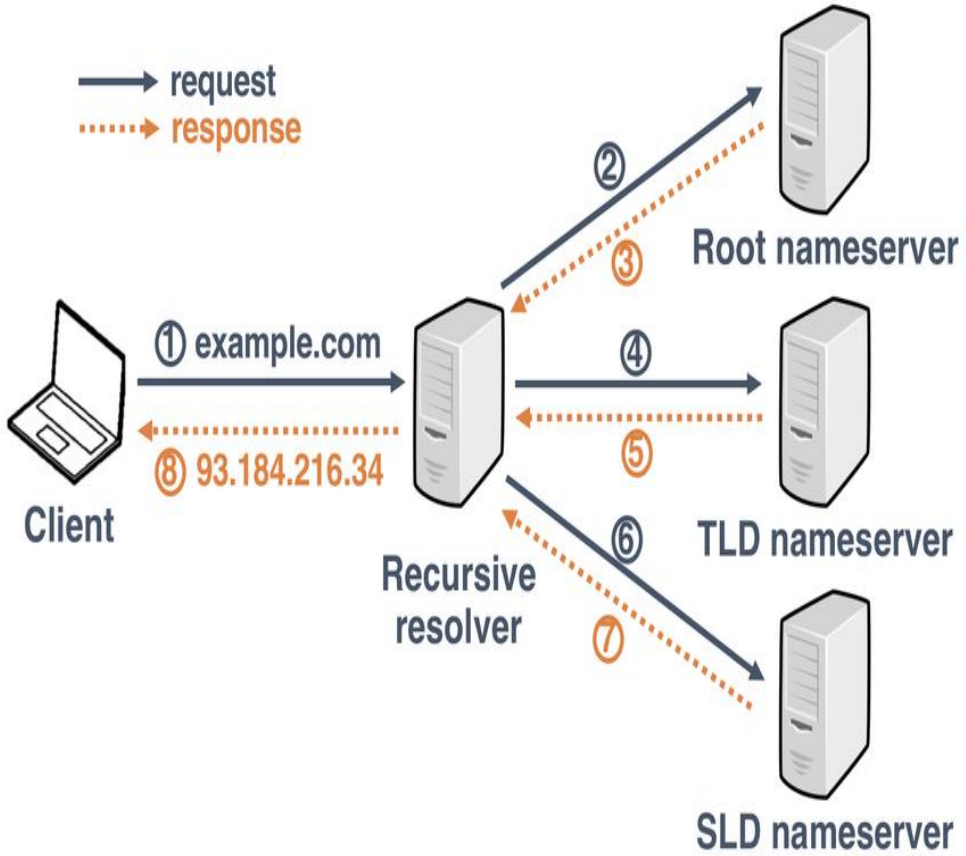
DNS Lookup

How the client get the website:

1- check the cash

2- check the hosts file

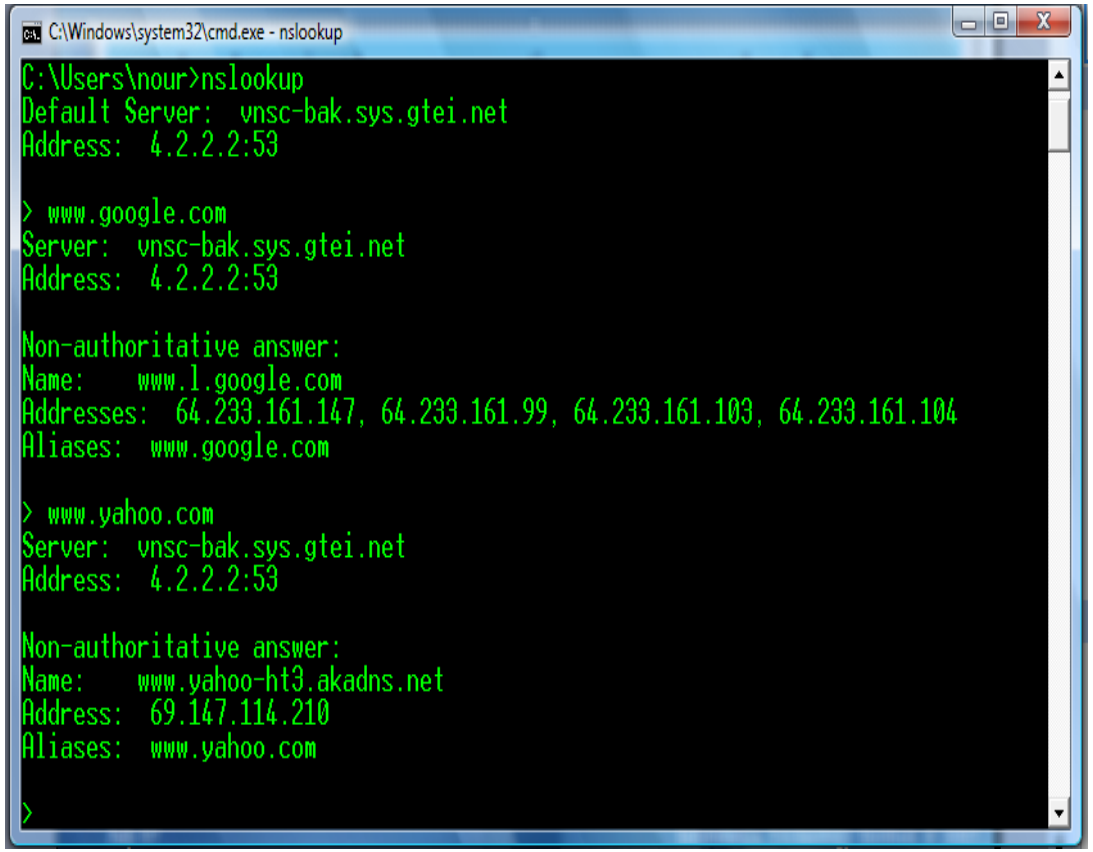
3- Ask DNS server



Basic Network Elements (Software) - Lab

Nslookup

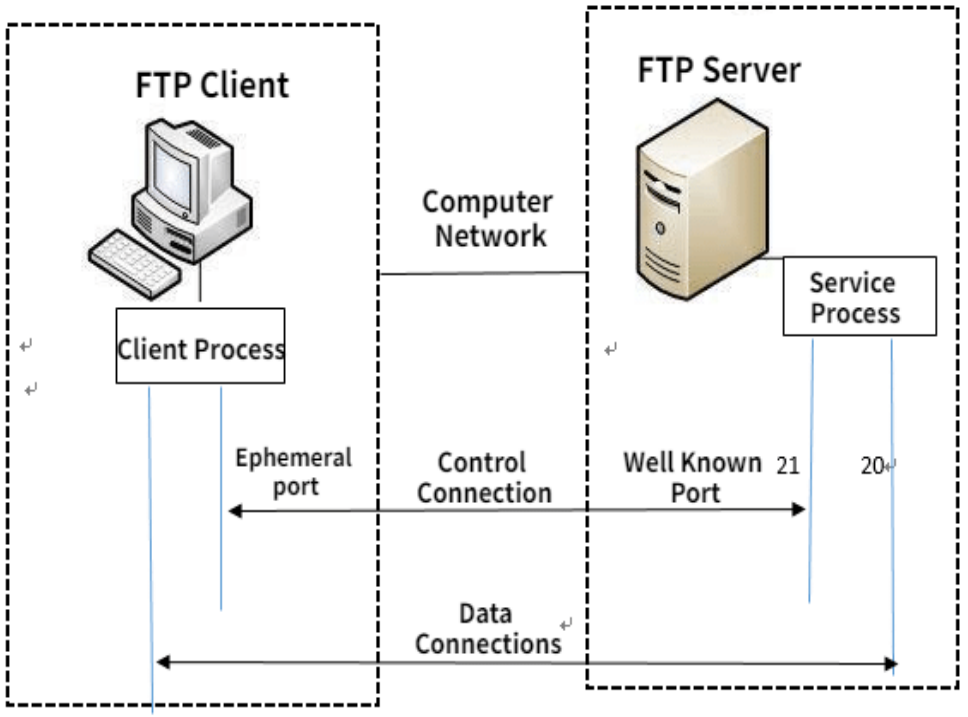
- nslookup is the name of a program that lets you to **enter a host name** and **find** out the **corresponding IP address**



Part 1 (TCP/IP Protocol Architecture)

FTP

- File Transfer Protocol
- a transmission protocol that provides **reliable data transfer between hosts**.
- **The default FTP port is**
  - **Port 21** for command and control,
  - **Port 20** for data transport.



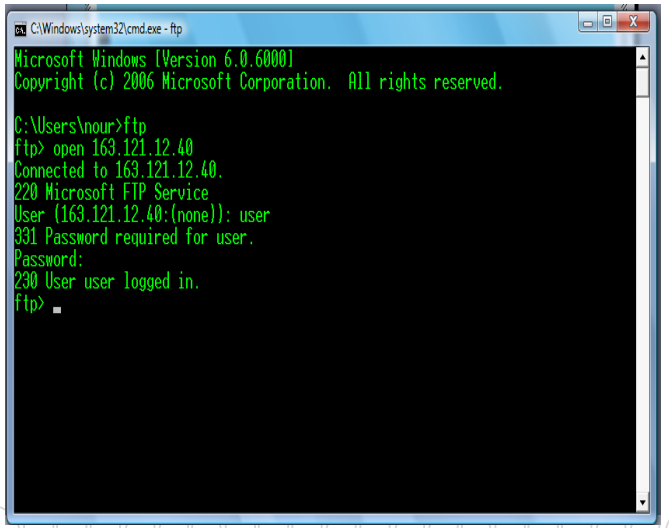
Working Principle of FTP

Part 1 (TCP/IP Protocol Architecture)_Lab

FTP

FTP Client

- Browser as a FTP client
  - **Use Internet Browser as FTP client.**
  - Using **MS Windows** built-in FTP client (CLI)
  - Third party programs “FileZilla *FTP*”



open

ls

cd

bin

get

mget

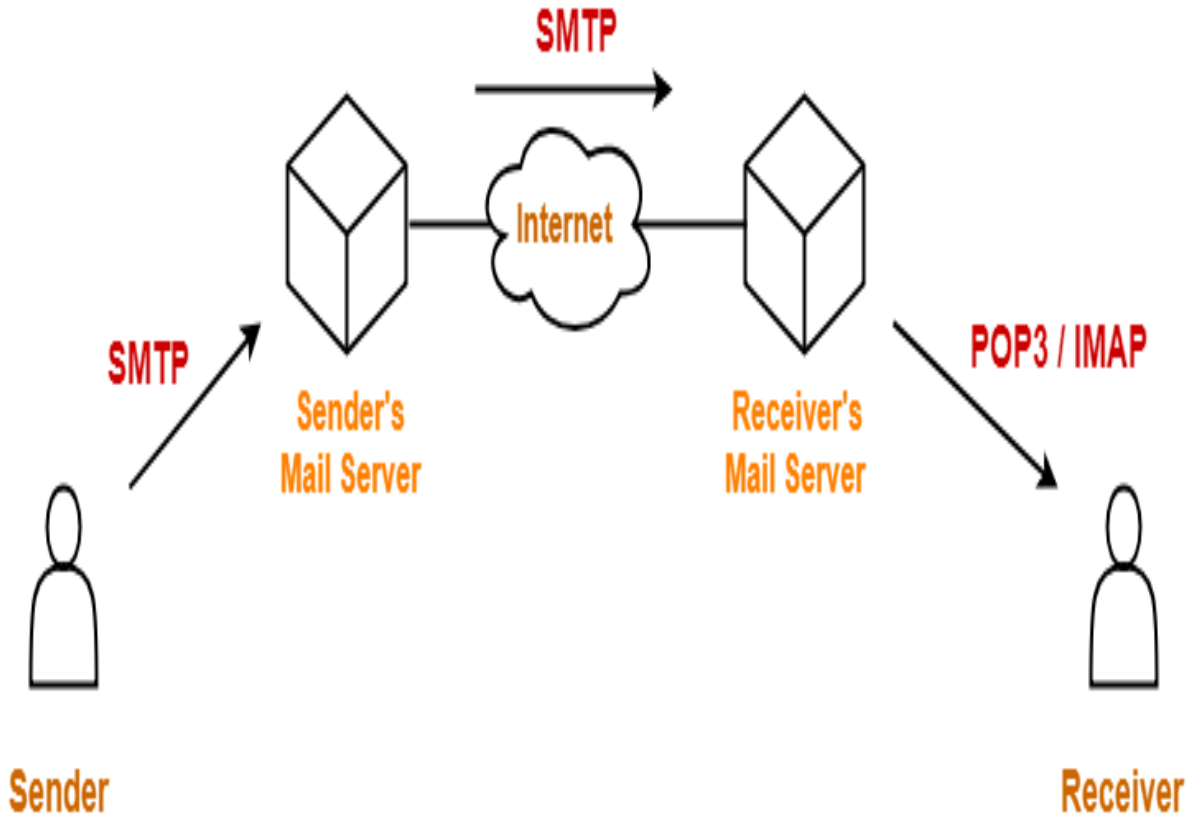
Put

bye

Part 1 (TCP/IP Protocol Architecture)_Lab

Mail Server and Clients

- Mail Clients
  - **Web based**
    - Hotmail
    - gmail
  - **Non web based**
    - Microsoft Outlook



Part 1 (TCP/IP Protocol Architecture)_Lab

Mail Protocols

- **SMTP (send mail transfer Protocol)**
  - It is the common language used by the majority of Mail Servers to send messages back and forth to other Mail Servers or Email Clients
- **POP3 “Post Office Protocol version 3”**
  - In order to collect email messages from the Mail Server, the Email Client contacts the Mail Server.
  - Download messages on the hard disk
  - You can work Offline
  - Keep the user’s quota on the server
- **IMAP4 “Internet Message Access Protocol version 4”**
  - Retrieve only message header

Part 1 (TCP/IP Protocol Architecture)

Telnet (23)/SSH(22)

- Telnet/ssh is a user command and an underlying TCP/IP protocol for accessing remote computers.
- Through Telnet/ssh, an administrator can access someone else's computer remotely

Telnet client (not secure)

- Built in MS-Windows Telnet client
- Third party programs

Part 1 (TCP/IP Protocol Architecture)_lab

- **RDP**
  - **Remote Desktop Protocol (RDP)** is a Microsoft proprietary protocol that enables remote connections to other computers,

Part 1_Network Elements (Hardware)

Network Hardware

Devices

Medium

Part 1_Network Devices (Hardware)

❖Computers / Peripherals

Any device that can connect to network with NIC

Ex: Computer

- ✓ Mobile
- ✓ Laptop-
- ✓ Printers-
- ✓ Cameras
- ✓ smart TV
- ✓ - …..etc

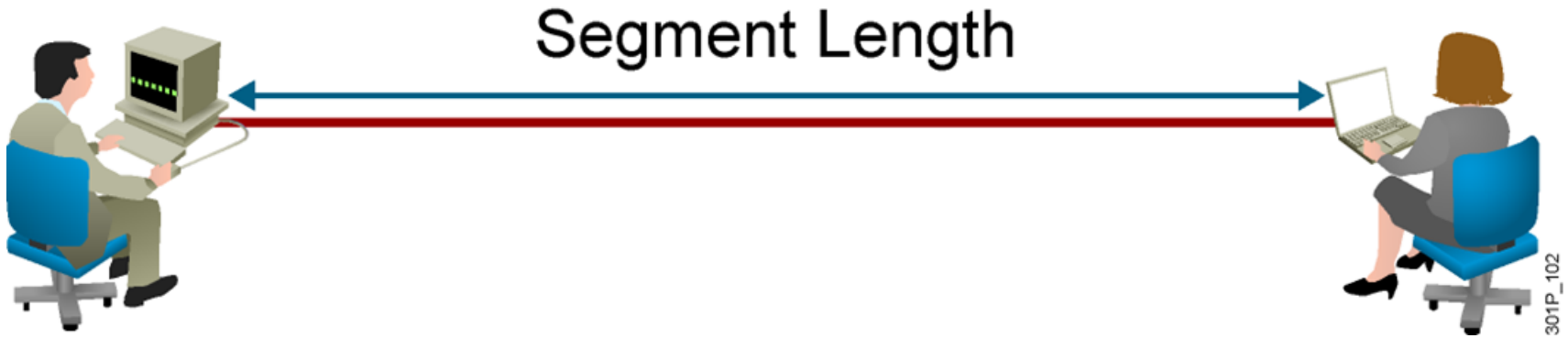
Part 1_Network Devices (Hardware)

NIC (Network Interface Card)

- Called network interface controller, network adapter or LAN adapter.

- Operate at **the physical layer of OSI/RM**
- hardware component without a computer cannot be connected over a network cable (interface between the PC and the network)
- Resides in the motherboard of the PC
  - **Internal NIC** (plugs into the motherboard directly)
  - **External NIC** (Wireless and USB based)
- Have A physical Address burned on the card called Mac.

LAN Segment Limitations



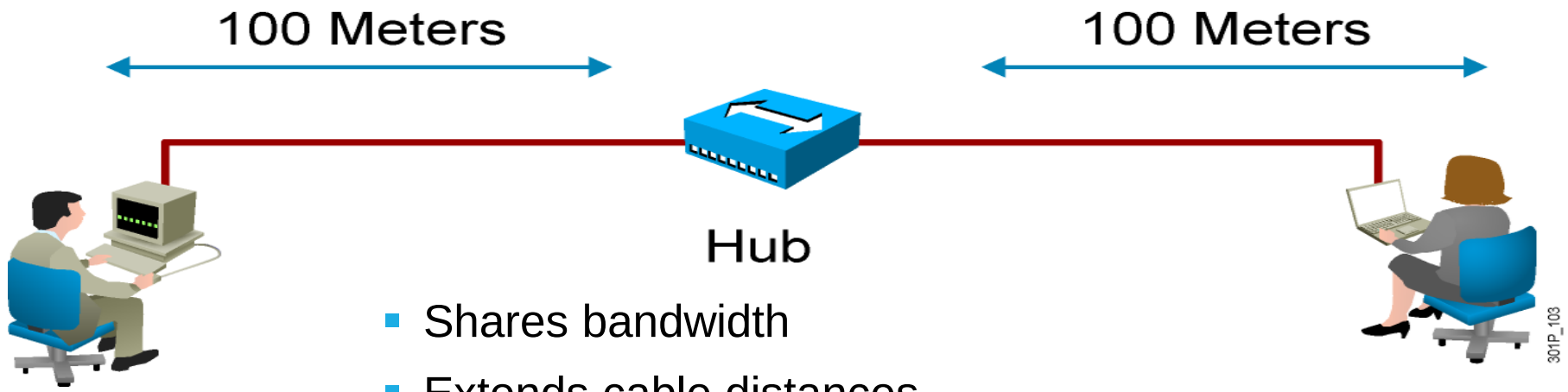
- Signals degrade with transmission distance.
- Each Ethernet type has a maximum segment length.

Part 1_Network Devices (Hardware)

❖Repeater

- Operates at the **physical layer**.
- **Regenerate** the **signa**l over the **same network** before the signal becomes too **weak or corrupted**
- Only extend the length of the signal to its original strength
- Does not amplify the signal.
- 2 port device.

Extending LAN Segments

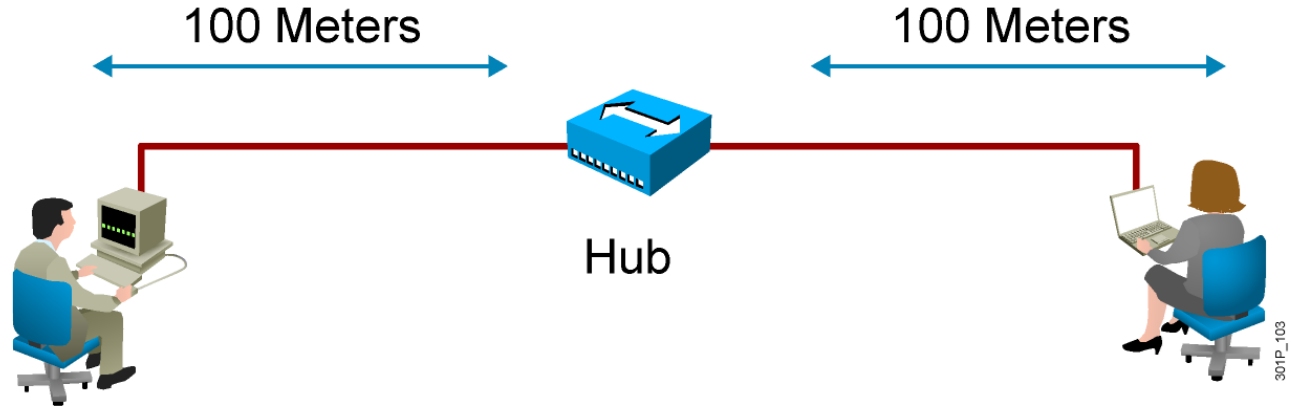


- Shares bandwidth
- Extends cable distances
- Repeats or amplifies signal
- **It is layer 1 device**
- It work only with bits
- Must work with **half duplex** communication

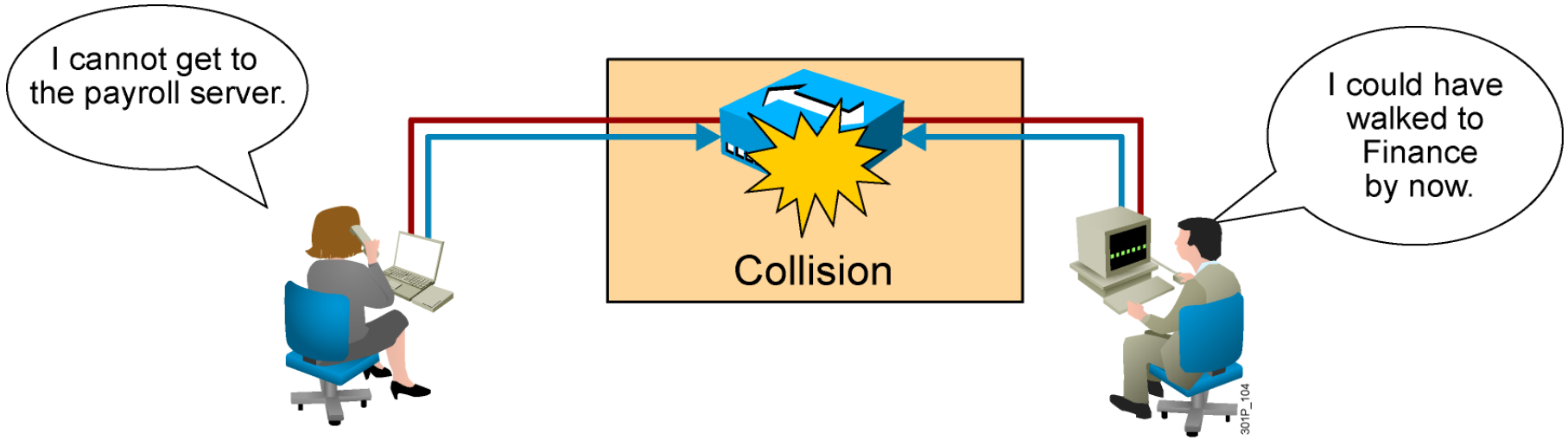
Part 1_Network Devices (Hardware)

❖ Hub

- It is **multi port repeater**
- Shares bandwidth
- Extends cable distances
- Repeats or amplifies signal
- It is **layer 1 device**
- It work **only with bits**
- Must work with **half duplex** communication
- It works by **flooding**



Part 1_Network Devices (Hardware)



- All ports of the hub have the same collision domain and broadcast domain.
- **Collisions** makes the network very **slow and congested**

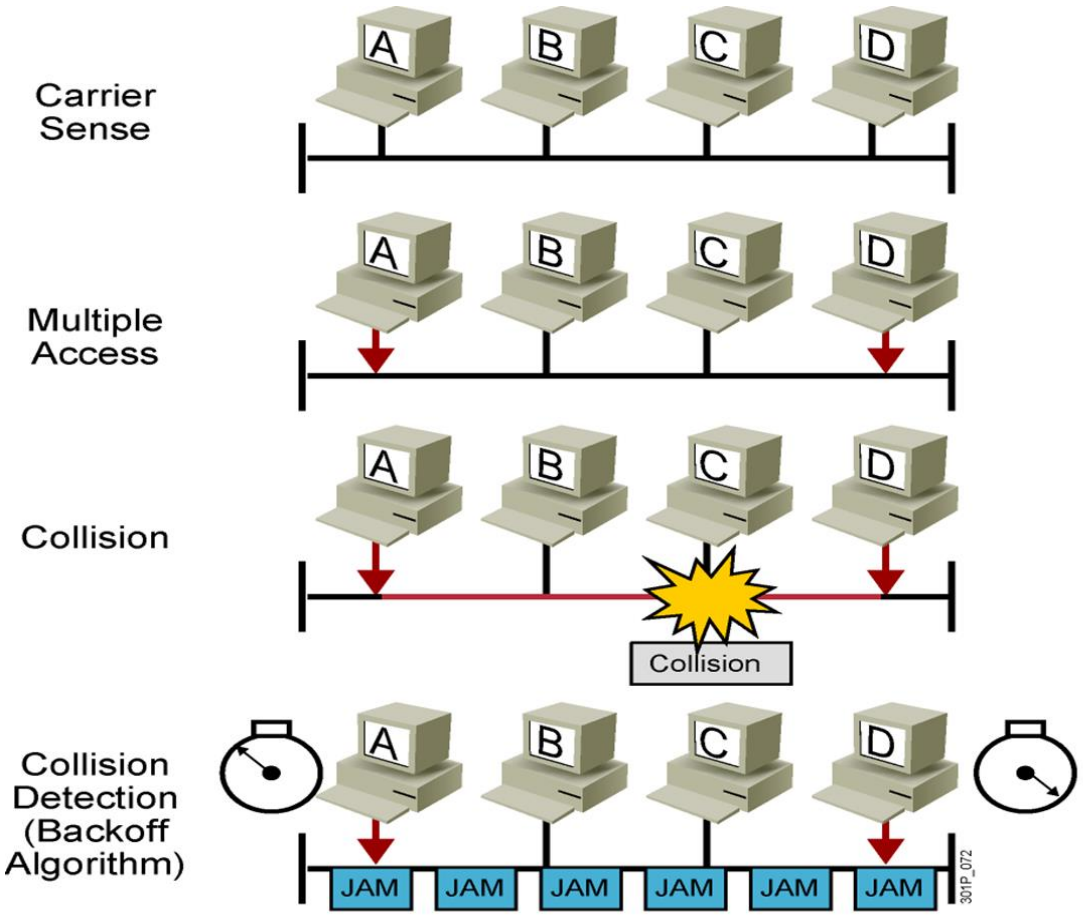
Part 1_Network Devices (Hardware)

CSMA/CD

Carrier sense
Each station continuously listens for traffic on the medium to determine when gaps between frame transmissions occur.

Multiple access
Stations may begin transmitting any time they detect that the network is quiet (there is no traffic).

Collision detect
This means that if any collision occurs, it will be detected immediately



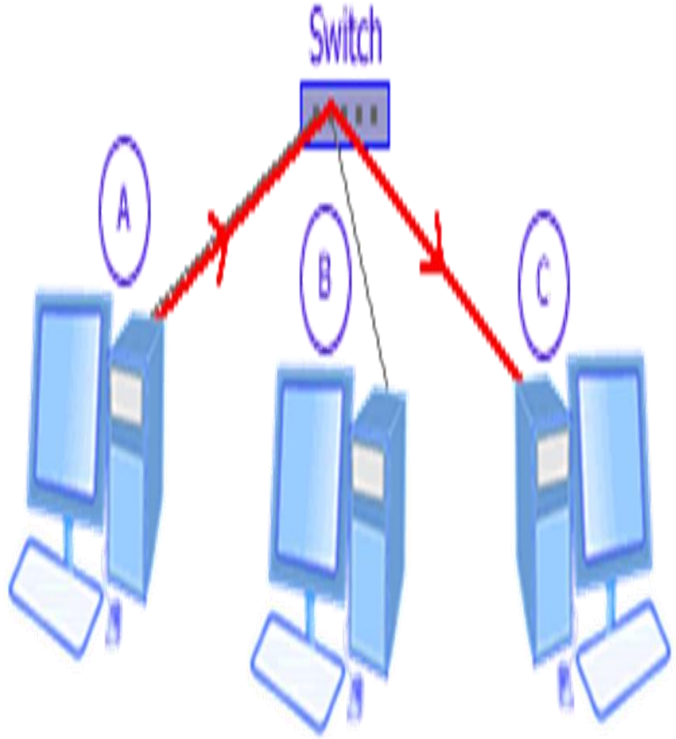
Carrier Sense Multiple Access Collision Detection (CSMA/CD)

Part 1_Network Devices (Hardware)

❖Switch

– Allow different nodes to communicate with each other at the same time without slowing each other down.

- Imply less traffic and high performance and effective.
- Switch is data link layer device.
- The switch can perform error checking before forwarding data.
- less collision domain of hosts



Part 1_Network Devices (Hardware)

❖Switch

- **Layer 2 switch**
  - LAN switch
  - Forwards traffic based on the MAC address
- **Layer 3 switch**
  - Routing switch
  - Forwards traffic based on IP Address
  - Used for Inter-VLAN routing
  - Don’t have WAN connectivity

Part 1_Network Devices (Hardware)

❖Router

- Allow different **networks** to communicate with each other (redirect packets between networks)
- Routes data packets based on their IP addresses.
- Routers are protocol dependent
- Operate at Network Layer device.
- Normally connect LANs and WANs together
- have a dynamically updating routing table based on which they make decisions on routing the data packets.

Part 1_Network Devices (Hardware)

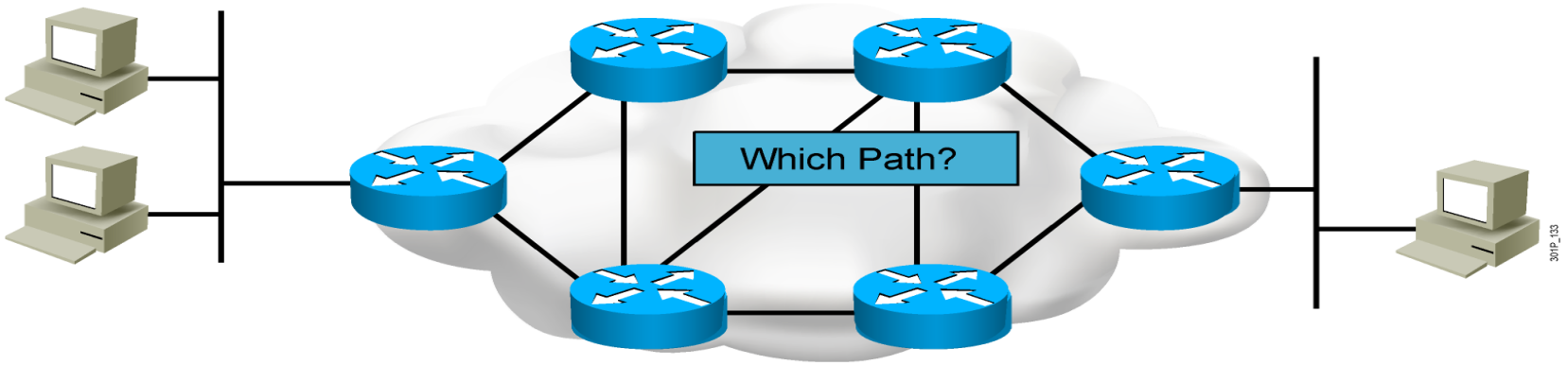
❖Router

– Path Determination :

- Getting update about the networks and send its updates to the other routers using the routing protocol configured

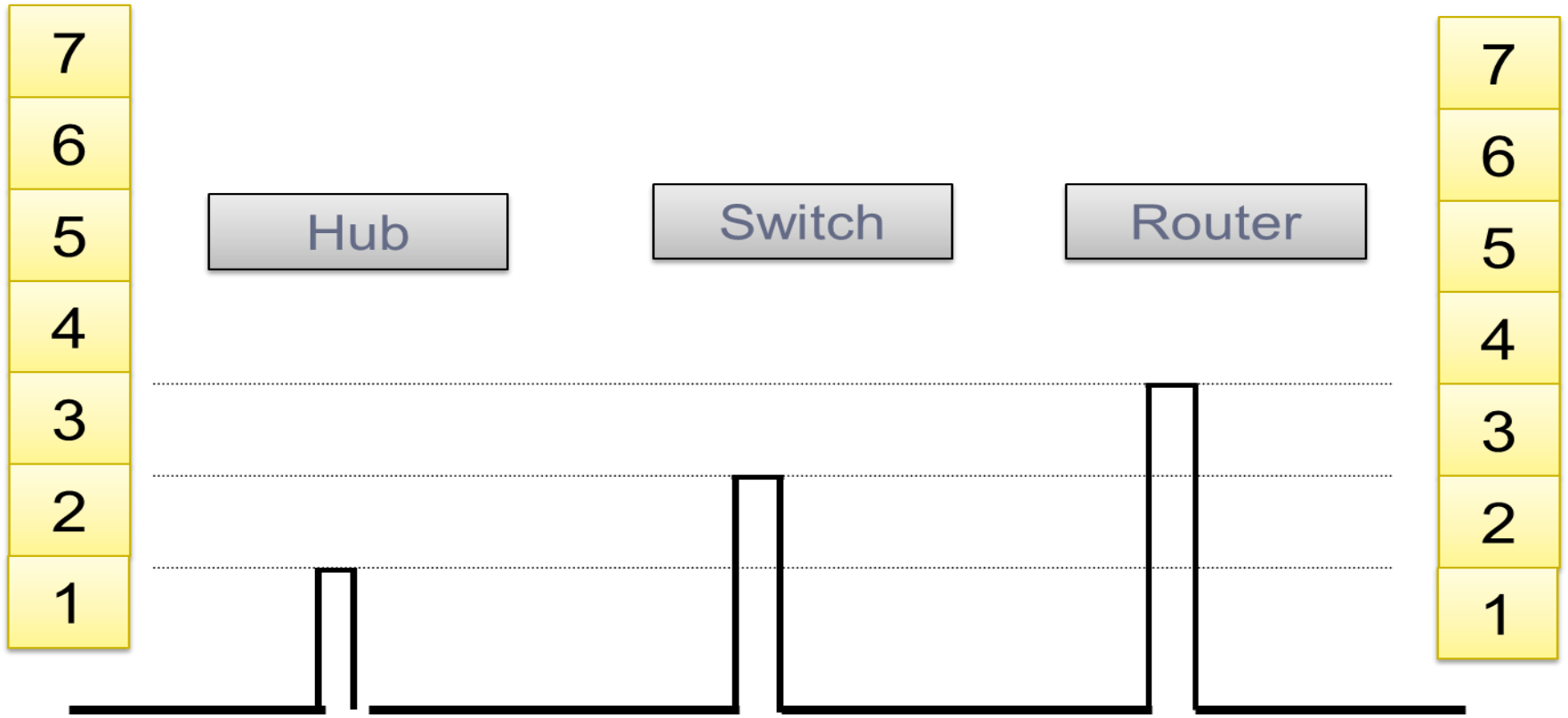
– Packet forwarding:

- Routers use the routing table to know where to forward packets using the best path out of its serial interfaces.



Part 1_Network Devices (Hardware)

❖Hub, Switch, Router Layers



Part 1_Network Devices (Hardware)

❖Splitter

- is a device that divides a telephone signal into two or more signals,
- each carrying a selected frequency range
- can also reassemble signals from multiple signal sources into a single signal

Part 1_Network Devices (Hardware)

❖Your Home “Router”

- Main Function is Routing
- Act as Switch
- Act as DHCP
- Act as Firewall
- Act As Access point

Part 1_Network Media (Hardware)

Network Transmission Media

Wired Media

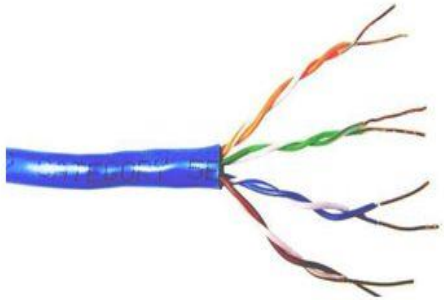
Wireless Media

Part 1_Network Media (Hardware)

Network Transmission Media

- **Cable Media**
  - Twisted Pair Cables
    - UTP
    - STP
    - Coaxial Cables
  - Fiber Optic Cables
- **Wireless Media**
  - WIFI
  - Infra red
  - Microwave
  - Bluetooth

- Unshielded twisted pair (UTP)



- Shielded twisted pair (STP)

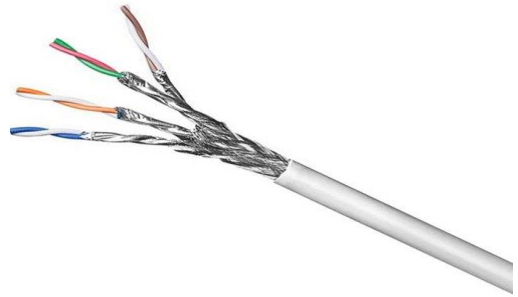
- Coaxial cable

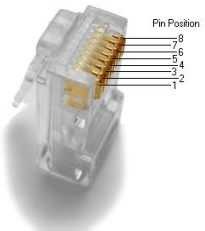
- Fiber optic

Part 1_Network Media (Hardware)

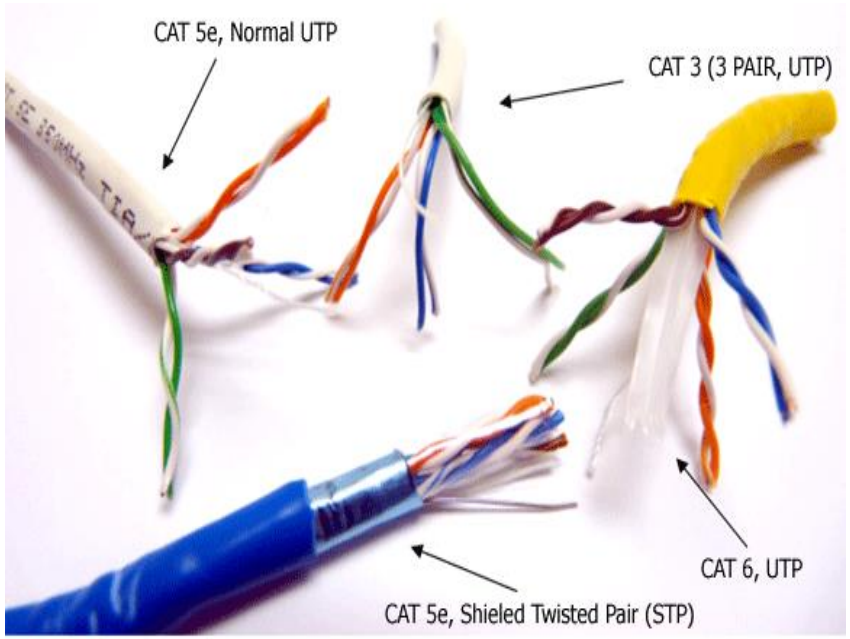
Network Transmission Media -Twisted pair cable

- Most widely used (Ethernet networks)
- Two basic types
  - STP
    - Shielded twisted pair
    - Protected
    - Hard to install
  - UTP
    - Unshielded twisted pair
    - Most common
    - Easy to install
    - Less expensive
    - Effected By electromagnetic interference
- Use RJ-45 connectors
- Crimper tool attach the twisted pair cable to RJ-45





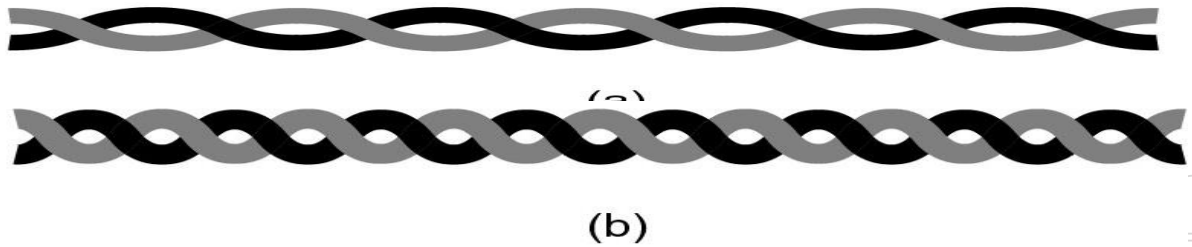
UTP Categories



Type	Use
Category 1	Voice Only (Telephone Wire)
Category 5	Data to 100 Mbps (Fast Ethernet)
Category 5e	Data to 1 Gbps (Giga Ethernet)
Category 6	Data to 1 – 10 Gbps (Giga Ethernet)

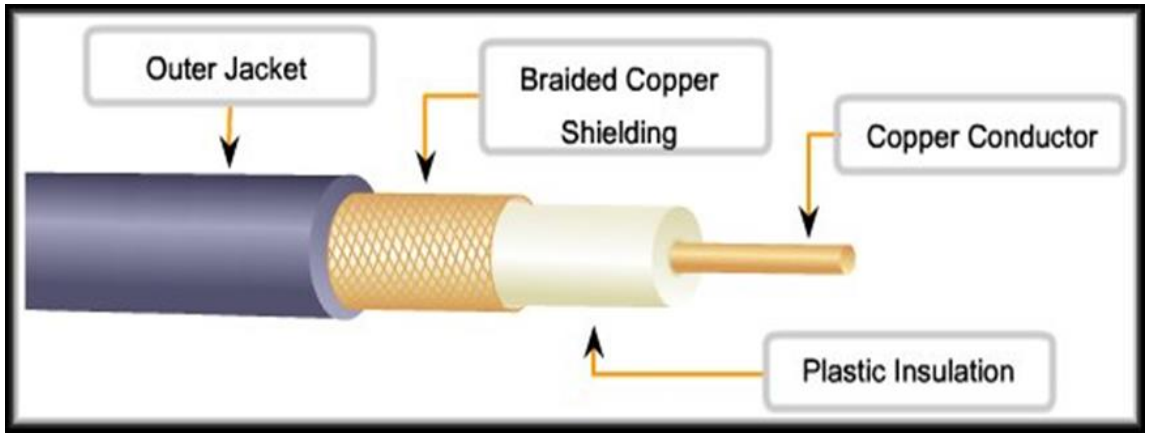
(a) Category 3 UTP.

(b) Category 5 UTP.



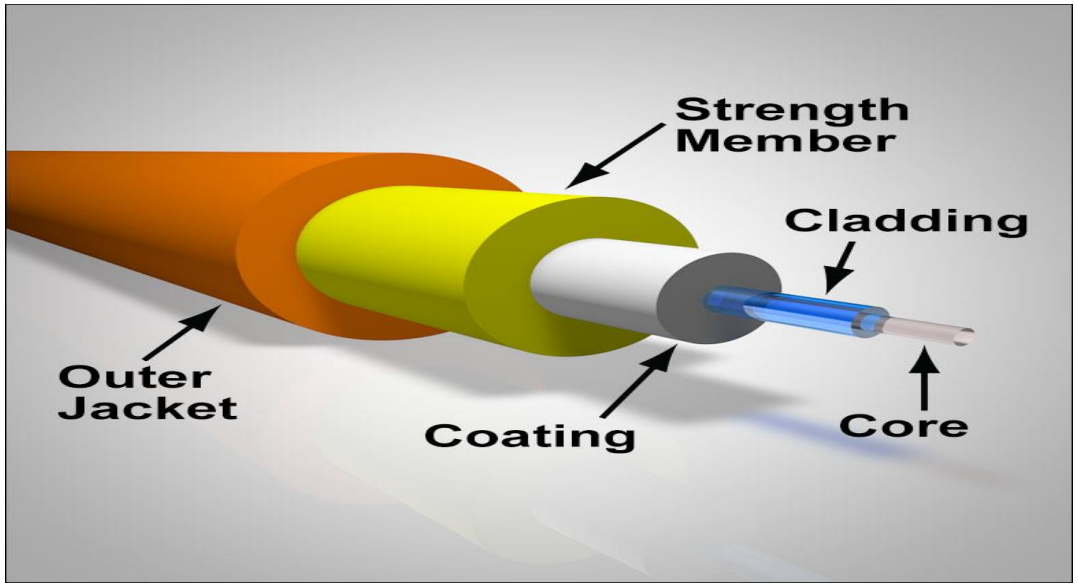
Coaxial Cable

- High capacity cable
- Used for video transfer
- Has two types
  - Thick coaxial cable (Thicknet)
    - ½ inch diameter
  - Thin coaxial cable (Thinnet)
    - ¼ inch diameter
- Use BNC connector



Fiber optic

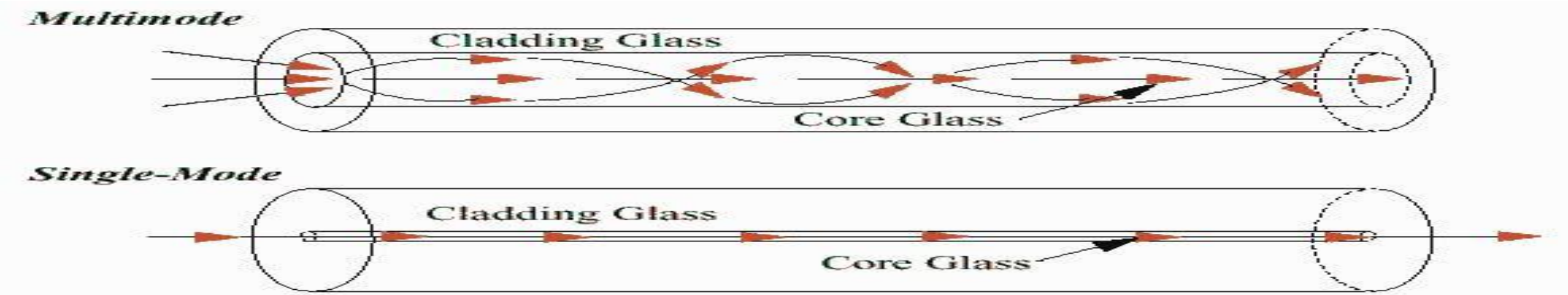
- Fiber optic cabling is composted of the following components:
  - The core that carries the signals. It is made of plastic or glass
  - The cladding maintains the signal in the center of the core as the cable bends.



Part 1_Network Media (Hardware)

Fiber Optic Types

Type	Description
Single Mode	• Transfer data through the core using a single light ray • The core diameter is around 9 microns • Supports a large amount of data • Cable length can extended a great distance
Multi-Mode	• Transfers the data through the core using multiple light rays • The core diameter is around 50 to 50 microns • Cable length are limited in distance compared to single mode

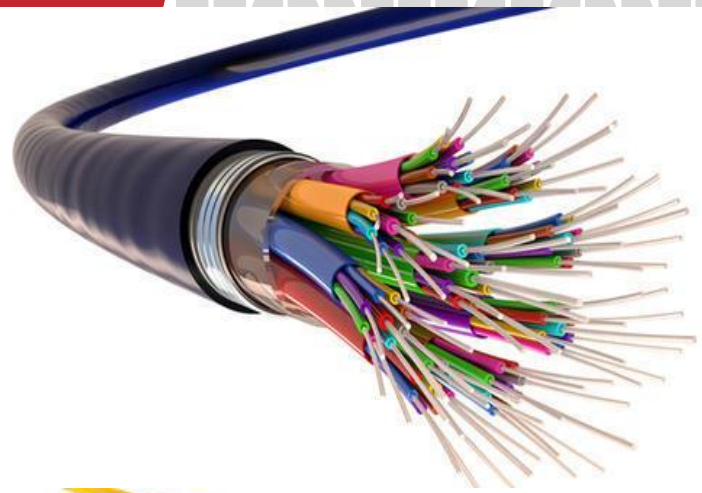


Part 1_Network Media (Hardware)

Fiber Optic advantages

- Advantages
  - Faster than twisted pair and coaxial
  - Send data as light pulses over glass medium
  - Free of electromagnetic interference
  - Highly resistance to Eavesdropping
  - Support extremely high data transfer rate
  - Allow grater cable distances without repeater

- Disadvantages
  - Expensive
  - Hard to install

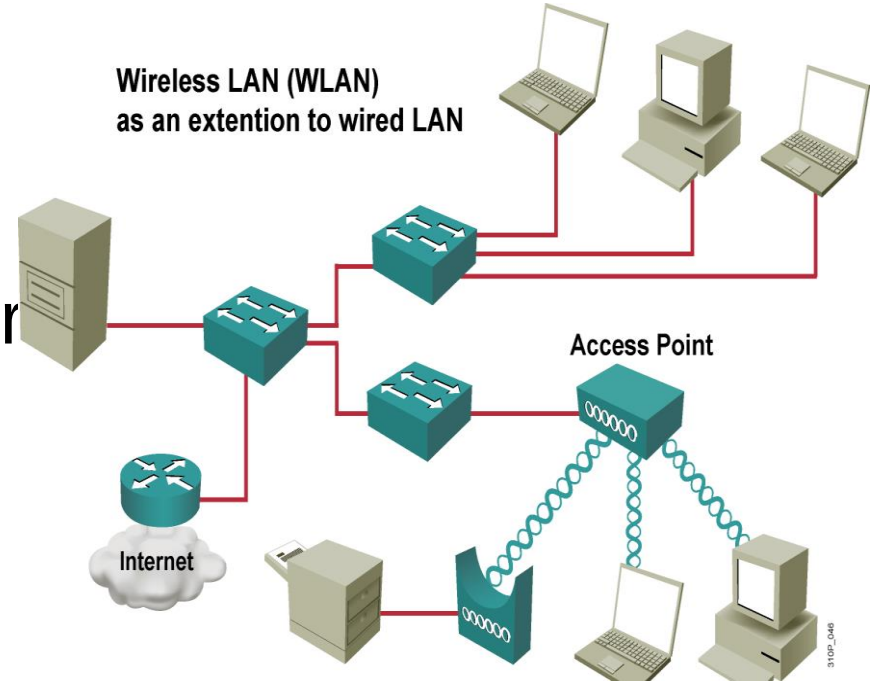


Wireless Media

- Flexible (Used in areas where it is hard to install cables)
- Used in wireless LANs
- Hybrid environment is one which wireless components communicate with a network that use cables

Part 1_Wireless Communication

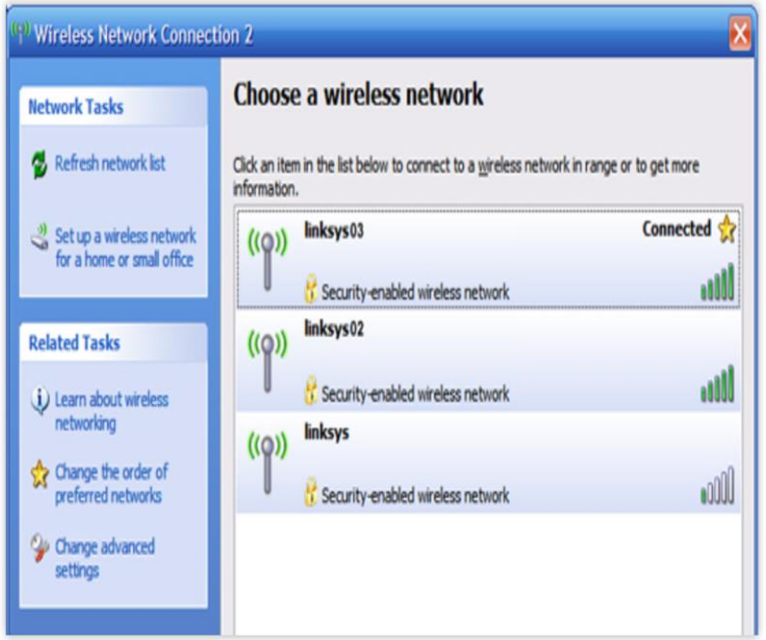
- Transmits data over the air vs. data over the wire
- Looks like a wired network to the user
- Defines physical and data link layer
- Uses MAC addresses
- The same protocols/applications run over LANs.
  - IP (network layer)
  - Web, FTP, SNMP (applications)



Service Set Identifier (SSID)

- **Unique identifier** that client devices use to distinguish between multiple wireless networks in the same vicinity (separate WLANs)
- Alphanumeric, case-sensitive entry from 2 to 32 characters long.

- The SSID is configured on the AP and can be either **broadcasted** to the outside world or **hidden.**
- The SSID must match on client and access point.
- Access point broadcasts one SSID in beacons.
- Client cannot be configured without SSID.



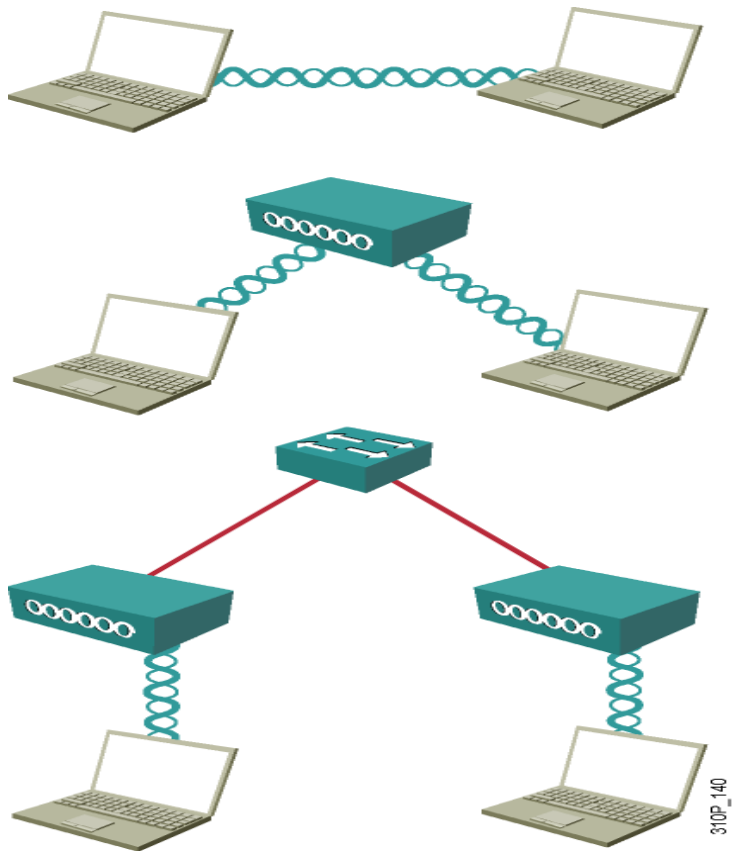
Service Modes

Independent Mode:

- Mobile clients connect directly without an intermediate access point.
- Ad hoc mode

Infrastructure Mode:

- Mobile clients use a single access point for connecting to each other or to wired network resources.



PART 1_WIRELESS COMMUNICATION

- **Advantages**
  - Provide the **ability to work anywhere** within range of your access points
  - **Extends the range of your network without running additional wires**
- **Disadvantages**
  - Introduces serious **security concerns**
  - provides **much less bandwidth** than wired devices

Thank You