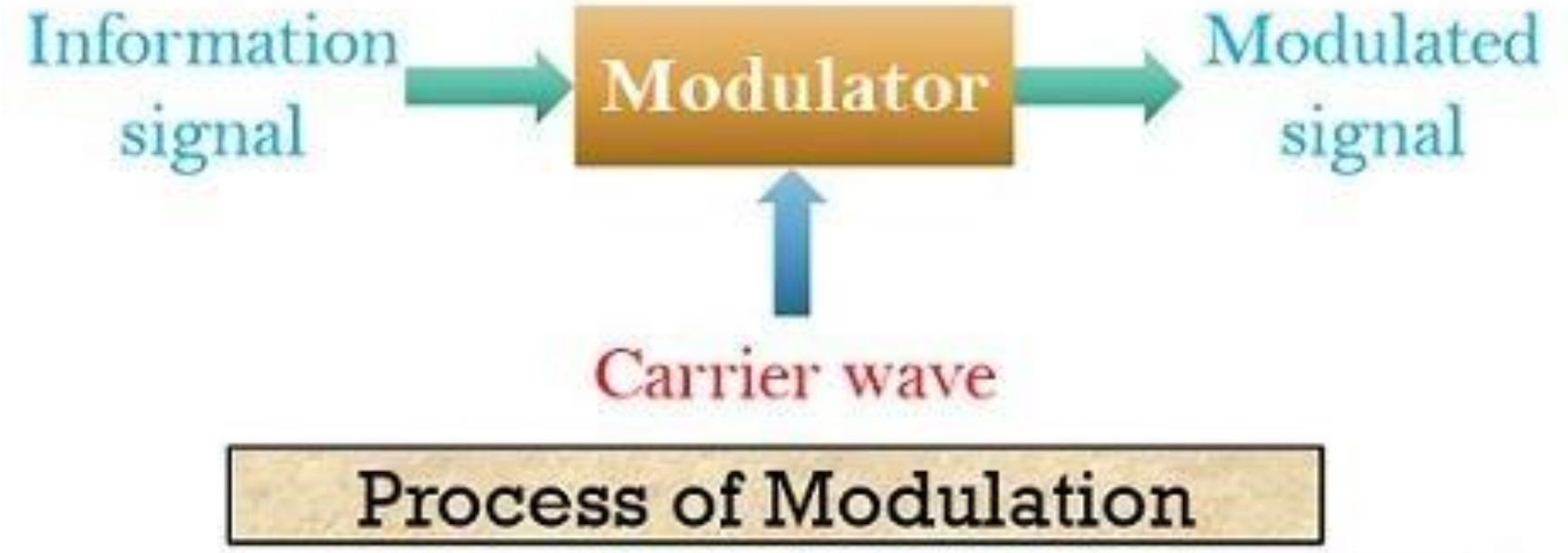
PART 2

TOPICS

1. Modulation techniques
2. Collision in Wireless Networks
3. Error Checking (Error Detection)
4. Main Idea of Routing
5. TCP/IP
6. Addresses on a Network
7. Cellular/Wireless Connectivity Protocols
8. Basic Network Tools
9. Various Protocols Used on Networks
10. How HTTP works – A Basic Idea
11. Working of Email
12. Secure Communication
13. Network Applications

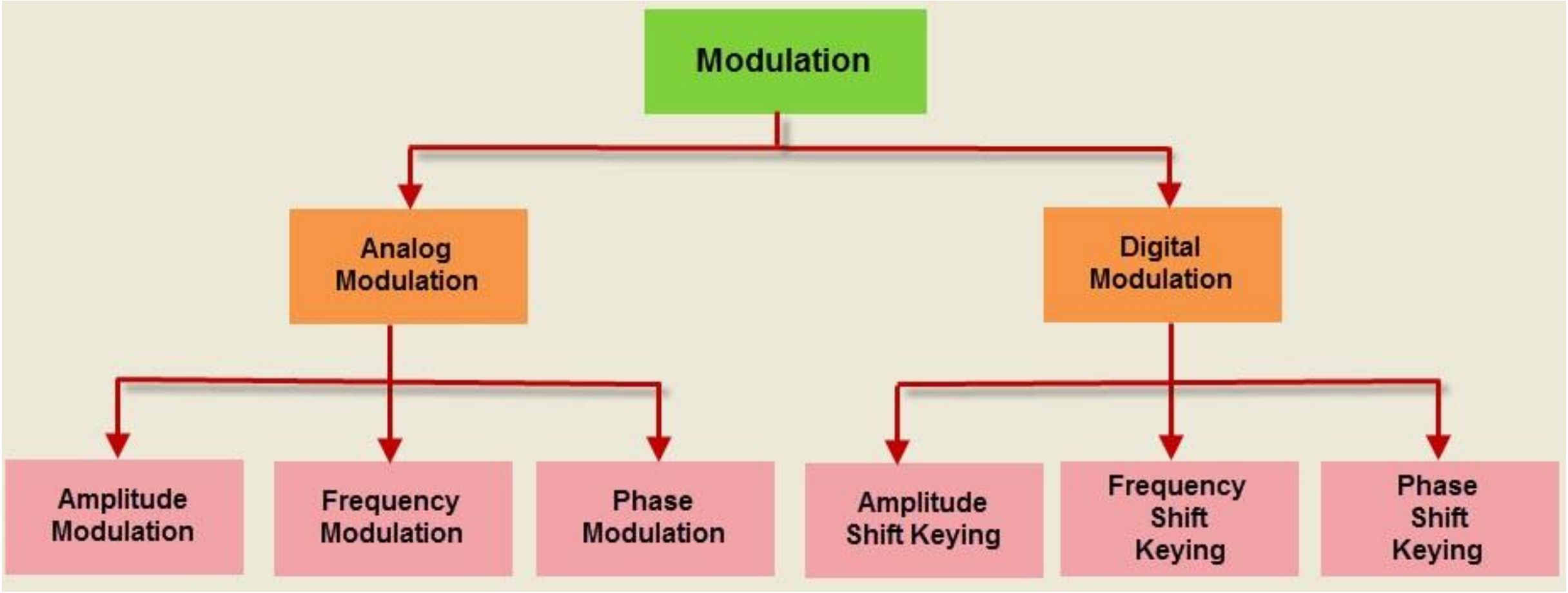
MODULATION TECHNIQUES

- Modulation is a process of changing the characteristics of the carrier wave by superimposing the message signal on a high frequency signal.

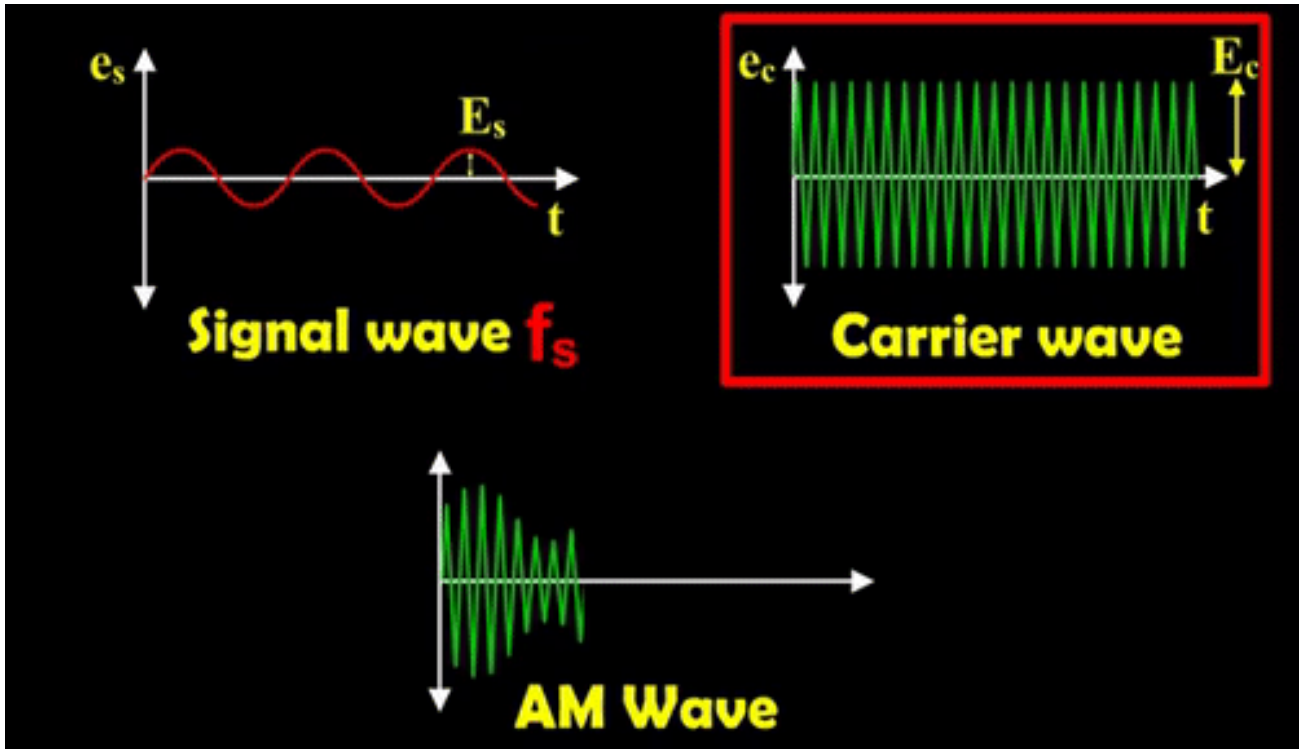


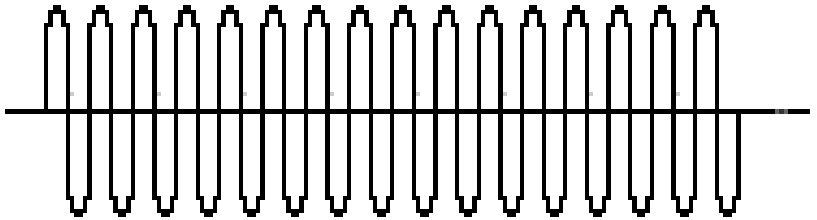
- A carrier wave by itself doesn’t carry much information that we can relate to (such as speech or data).
- To include a message (i.e., data or speech or image etc.), another wave, a message signal that carries the data to be transmitted, needs to be superimposed on top of the carrier signal.
- This process of termed as modulation.
- Modulation alters the shape of a carrier wave to encode somehow the speech or data information that is to be carried.
- Now this encoded form of wave (i.e., the speech/data merged with the carrier) will be transmitted.
- Thus, you can say that modulation is hiding a code inside the carrier wave.
- The main function of the carrier wave is to carry the audio or video signal from the transmitter to the receiver.
- The superimposition of message signal and carrier wave results into a new wave called the modulated wave.

- **Types of modulation:**

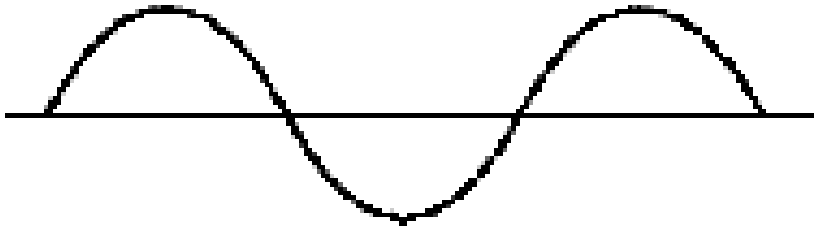


- **1. Amplitude modulation (AM):**
- The amplitude of a wave is the maximum disturbance from its undisturbed position. it is measured in the form of the height of the wave.
- In amplitude modulation the strength of the carrier signal i.e., the amplitude is varied as per the changes in the amplitude of the modulating signal.

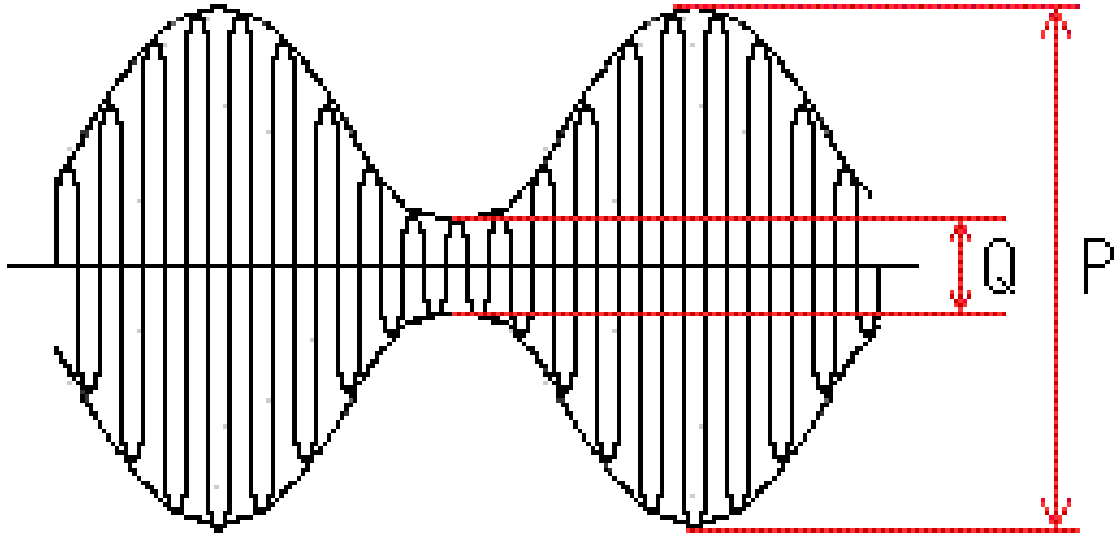




C Carrier
high frequency

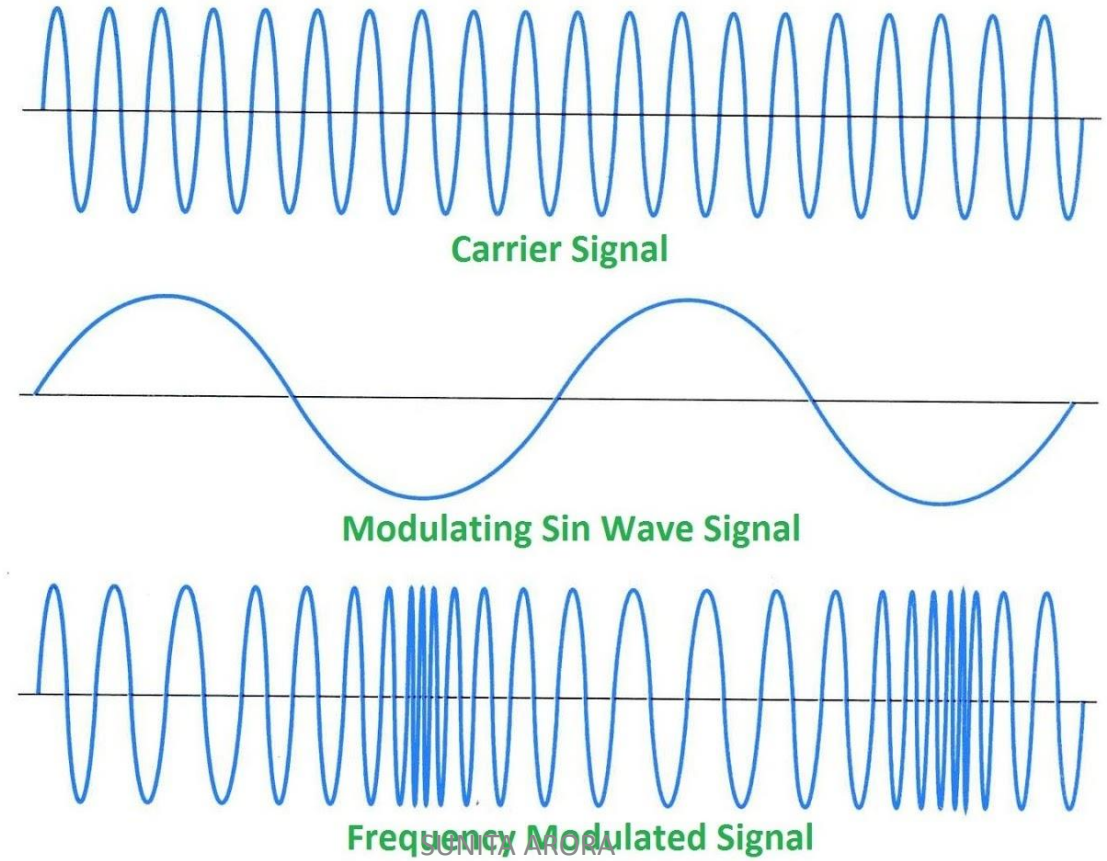


S Signal
audio frequency



D AM modulated waveform

- **2. Frequency modulation (FM):**
- Frequency of wave is the number of waves produced by a source, per second. It is measured as the number of waves that pass a certain point in one second.
- In frequency modulation, the frequency of the carrier signal is varied as per the changes in the frequency of the modulating signal.



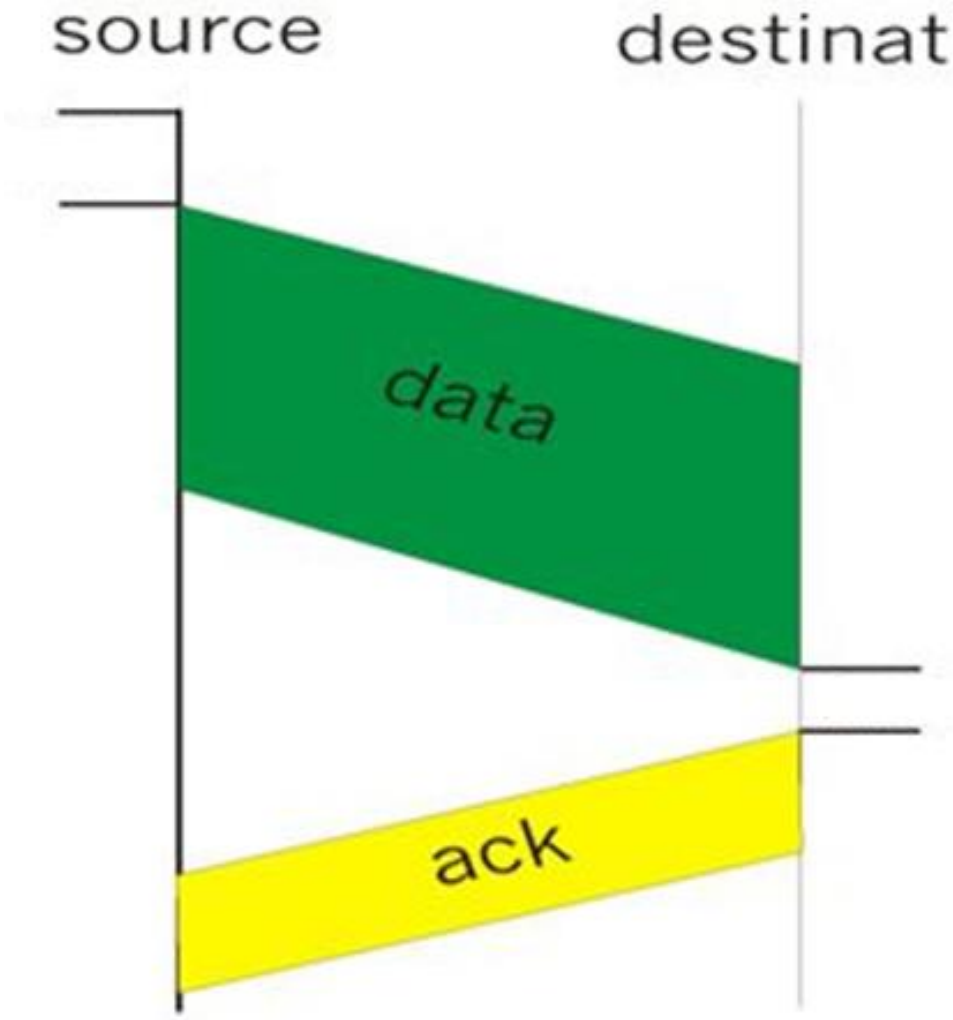
- **NOTE:**
- If the amplitude of the carrier wave is varied as per the message signal keeping other characteristics intact, it is the **amplitude modulation.**
- If the frequency of the carrier wave is varied as per the message signal keeping other characteristics intact, it is the **frequency modulation.**
- **Modulation** is the technique of changing the characteristics of the signal being transmitted so that it carries data.
- **Demodulation** is the reverse process of modulation where data is extracted from the received signal (ie., from the modulate wave).

COLLISION IN WIRELESS NETWORKS

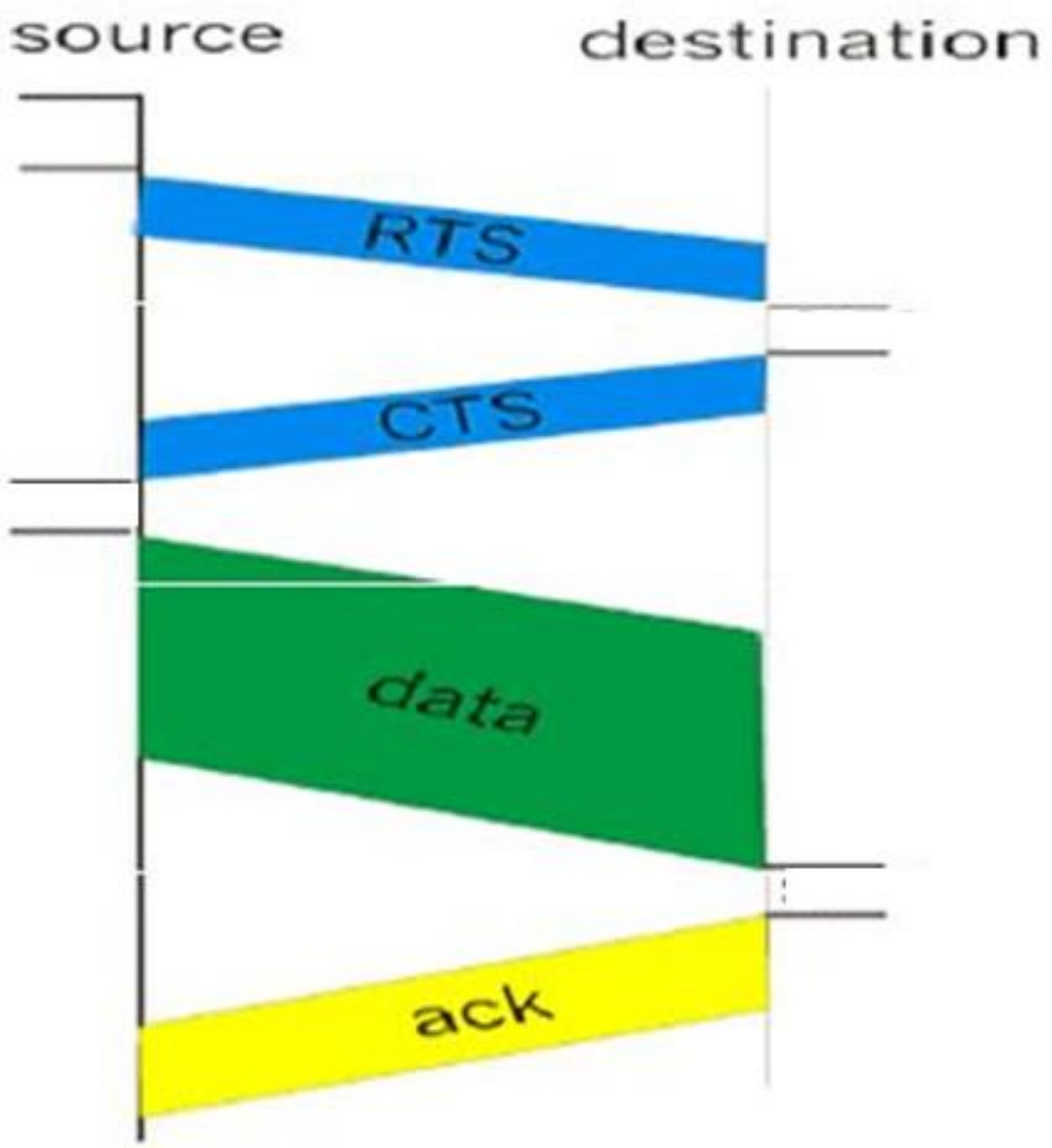
- Type of two-way communication where sending and receiving takes place simultaneously is called full duplex communication.
- Type of two-way communication where sending and receiving cannot take place simultaneously is called half duplex.

- Wireless networks use methods to ensure that collisions are avoided.
- But still, if collision occurs, the nodes wait for a random amount of time and retransmits data packet.
- In wireless networks, if collision occurs, the transmitting nodes cannot detect it. This is because the nodes in a wireless network cannot listen while transmitting (eg, half duplex).
- Thus, for wireless networks, strategies are adopted that avoid collision rather that detecting it.
- Wireless networks implement it using a special protocol called CSMA/CA.
- Wired networks use collision detection methods such as CSMA/CD as wired networks are full duplex.

- **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) working:**
- 1. Node ready to transmit/talk
- 2. Listen for other nodes, if any transmission is taking place. One of the two possibilities:
- 2.1 Busy. A transmission is taking place. Now do the following:
- 2.1.1 Increase back off or wait time (called BEB (binary Exponential Backoff))
- 2.1.2 Sleep as per BEB
- 2.1.3 wake up and go to step 1
- 2.2 Free. No transmission is taking place. Now do the following:
- 2.2.1 Send message
- 2.2.2 Verify it proper transmission has taken place using one of the following two methods:
- (a) ACK (Acknowledgement) method
- (b) Request to Send/Clear to Send (RTS/CTS) method.



CSMA/CA with ACK



CSMA/CA with RTS/CTS

- **1. CSMA/CA with ACK:**
- In this method, as soon as a node transmits data to another node, the receiving node must send an acknowledgement signal called ACK, once it has received the data.
- The ACK signal must reach to the sender node within a specified time-frame.
- If the sender node does not receive ACK in specified time, it considers it as a failed transmission and retransmits the data.
- The ACK signal is generated by the receiver node, only if the data frame is received in valid form.

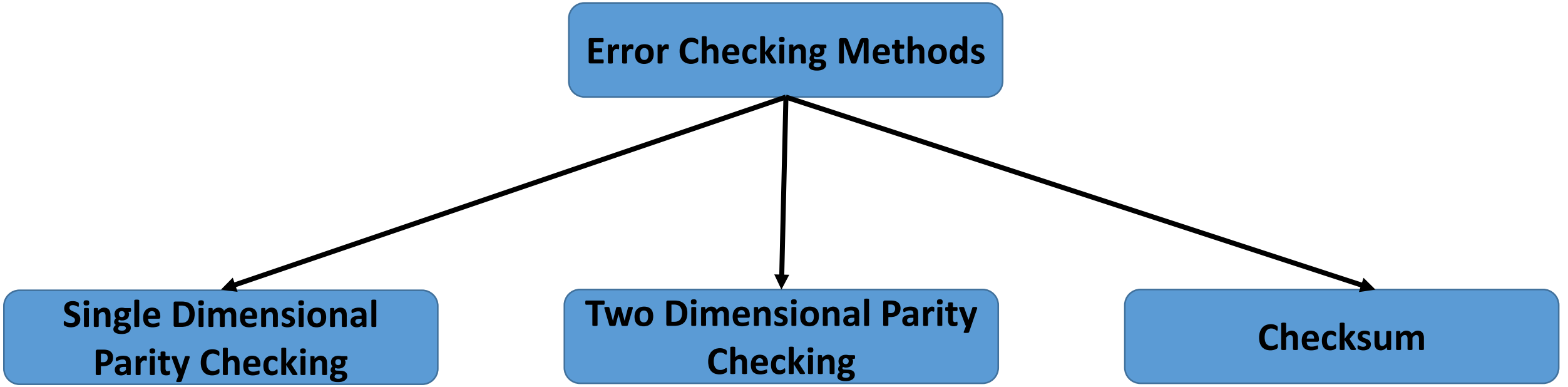
- **2. CSMA/CA with RTS/CTS:**
- In this method, the sender node first sends an RTS signal to its receiver. Receiver confirms its readiness to receive by sending a CTS signal to the sender as well as all other nodes.
- Other nodes upon receiving a CTS will now not transmit (will wait) as they now know that some transmission is taking place and communication channel is busy.
- The sender node upon receiving a CTS goes ahead with transmission.
- Once the transmission ends, the receiver nodes sends ACK signal to all nodes.

- Note: For smaller wireless networks, CSMA/CA with ACK is used, and for bigger wireless networks, CSMA/CA with RTS/CTS is used.

ERROR CHECKING (ERROR DETECTION)

- While transmitting data over networks, some errors may occur, and data may get corrupted, eg., if the sender is trying to send a data in binary form as 10110111 and the data received by the receiver as 10110101. This means that intended data has not reached the receiver node and hence it is an error.
- The errors can be one or more of following types:
- **1. Single bit error:** If only one bit of the transmitted data got changed from 1 to 0 or from 0 to 1.
- **2. Multiple bit errors:** If two or more non-consecutive bits in data got changed from 0 to 1 or from 1 to 0.
- **3. Burst error:** If two or more consecutive bits in data got changed from 0 to 1 or from 1 to 0.

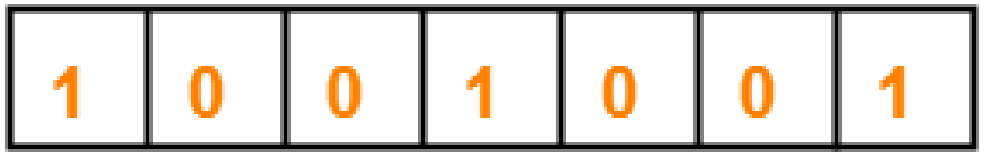
- To avoid such errors in transmission, some error detection or error checking methods are used in computer networks that ensure if the received packet is error free or not.



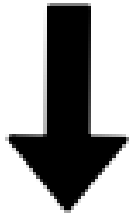
- **1. Single Dimensional Parity Checking:**
- Parity refers to an additional bit added to the actual data.
- Before transmission, at the sender node:
- i. Number of 1’s is counted in the actual data unit.
- Ii. Add an extra bit (either 0 or 1), called the parity bit to actual data so that the number of 1’s along with the extra bit, become even or remain even, i.e., for odd number of 1’s, add 1 as the parity bit and for even number of 1’s, add 0 as the parity bit.
- The data is now transmitted along with the parity bit.

- After transmission, at the receiver node:
- iii. From the received data, excluding the parity bit, once again determine the parity bit using the same process, i.e., by calculating the number of 1's in received data and compare it with the received parity bit. If the received bit matches with the calculated parity bit, data is considered as correct, otherwise the received data unit is considered as corrupted data and hence rejected.

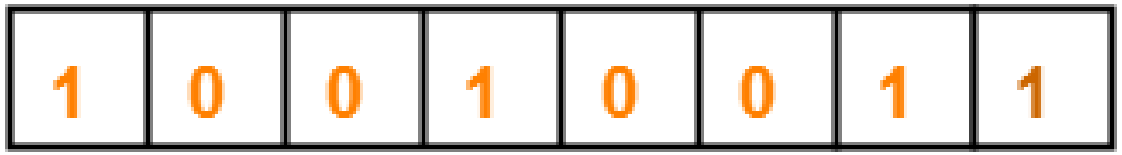
- Note: Since this parity check is based on making the number of bits as even, it is even parity checking. There is odd parity checking technique also, very similar to this – the only difference is that parity is calculated to make the number of bits odd.



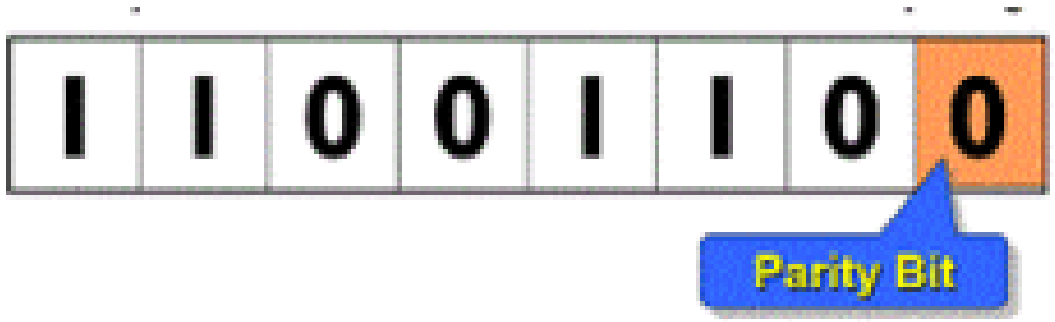
Original data unit

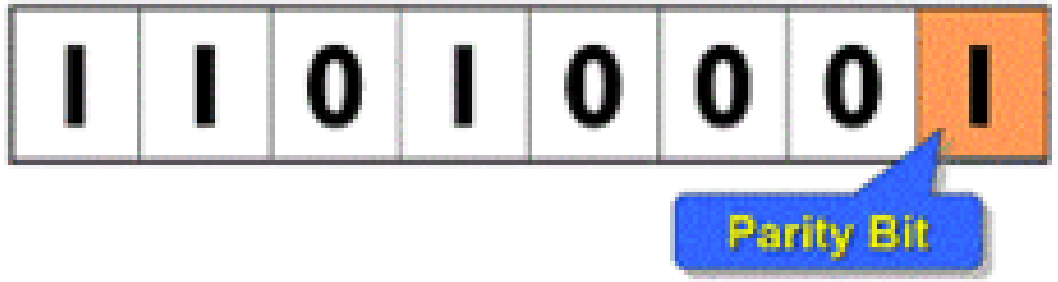


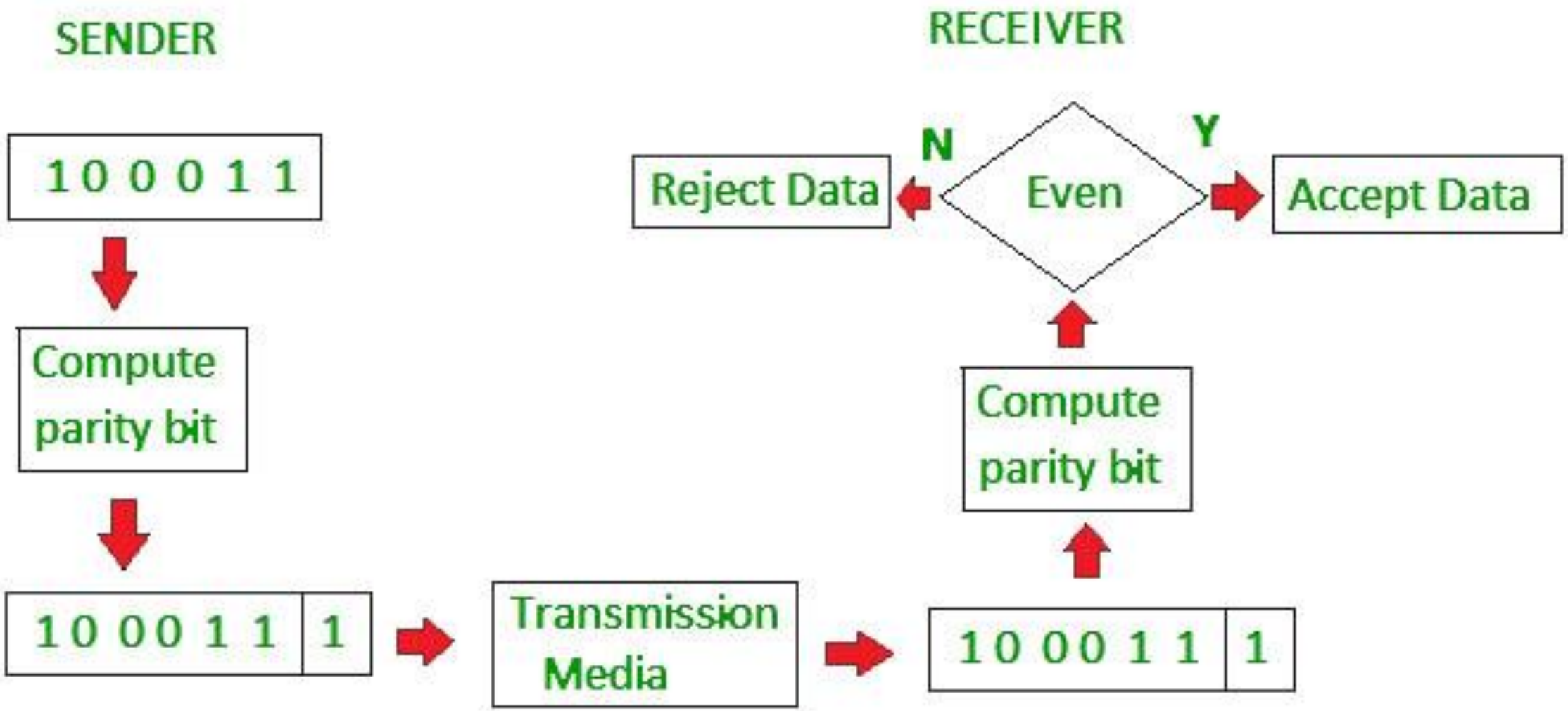
Parity bit



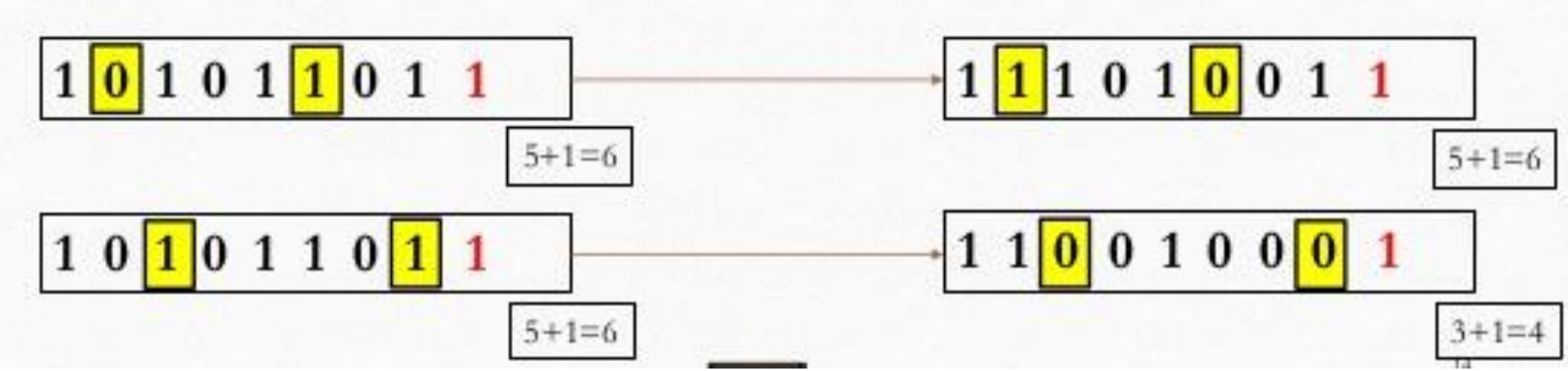
Transmitted data unit





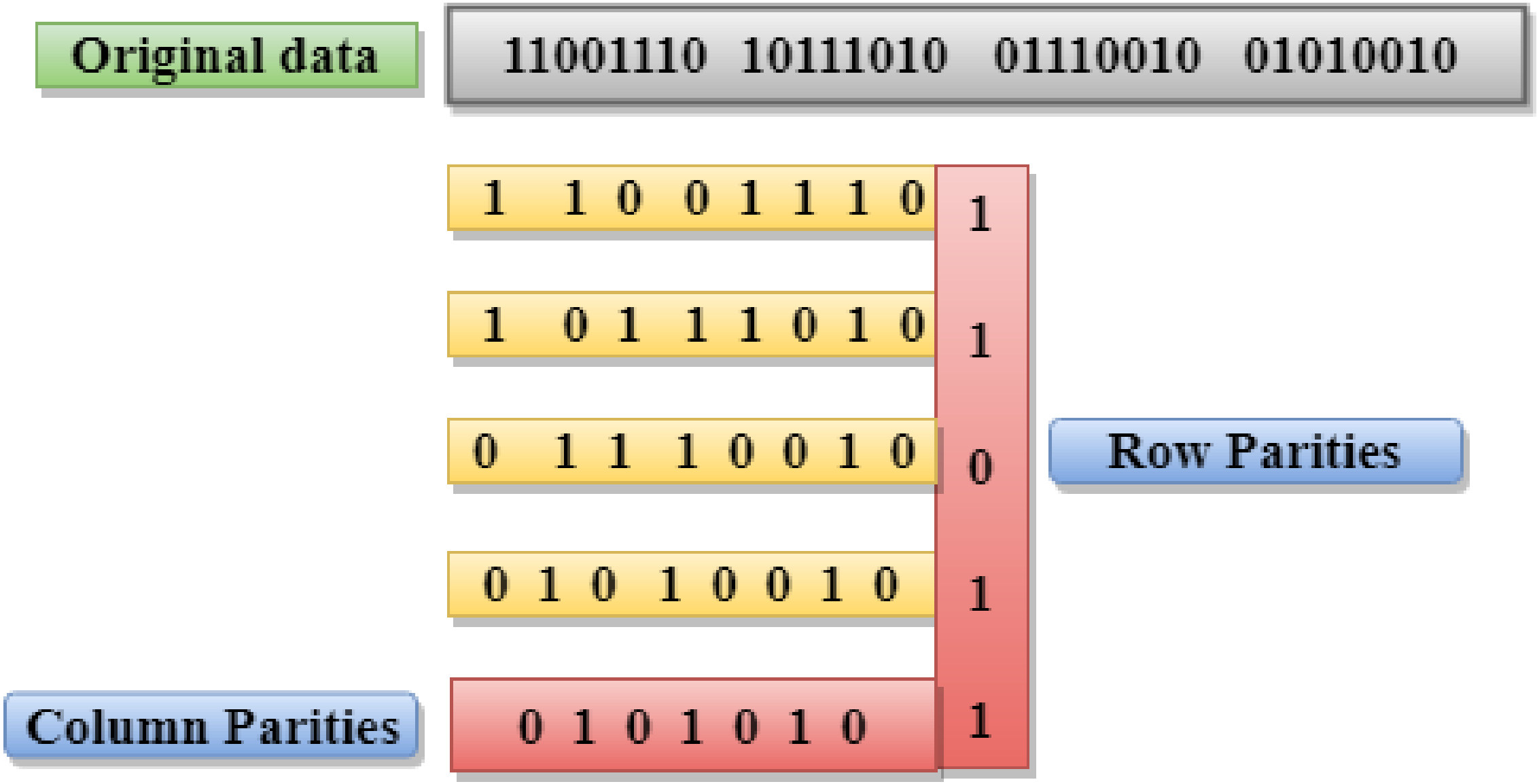

SENDER
RECEIVER
1 0 0 0 1 1
Compute parity bit
1 0 0 0 1 1 | 1
Transmission Media
1 0 0 0 1 1 | 1
Compute parity bit
N
Y
Even
Reject Data
Accept Data

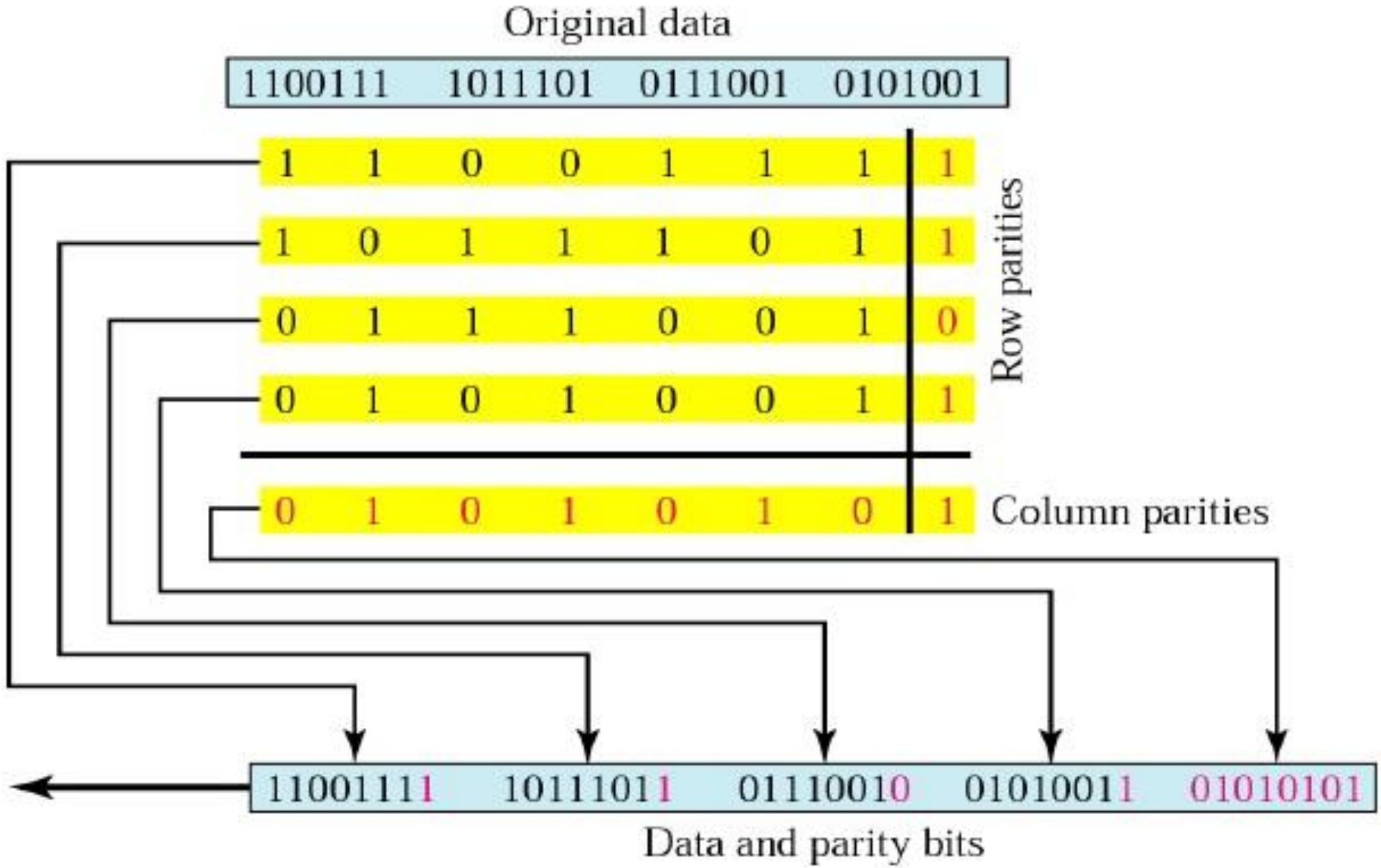
- **Advantages:**
- It is a simple mechanism which is easy to implement.
- It is an inexpensive technique for detecting the errors in data transmission.
- **Disadvantages:**
- It can detect only single bit errors which occur rarely.
- If, in the data transmitted, two bits get interchanged, then even though data gets affected, but the parity bit will remain correct. In such cases, this technique cannot detect the errors.



- **2. Two Dimensional Parity Checking:**
- This technique works with multiple data units simultaneously.
- At the sender node, before transmission:
- i. Organize all data units being sent, one below another so that it appears as table of bits.
- ii. Calculate parity bits for each data unit row-wise and column-wise.
- The data bits are now transmitted with the row parity bits and column parity bits.

- At the receiver end, after transmission:
- iii. The row parity and column parity bits are again recalculated using the received data parts only (excluding the parity bits) and compared with the received row parities and column parities. If these match, data is accepted, otherwise rejected, as this indicates error in transmission.

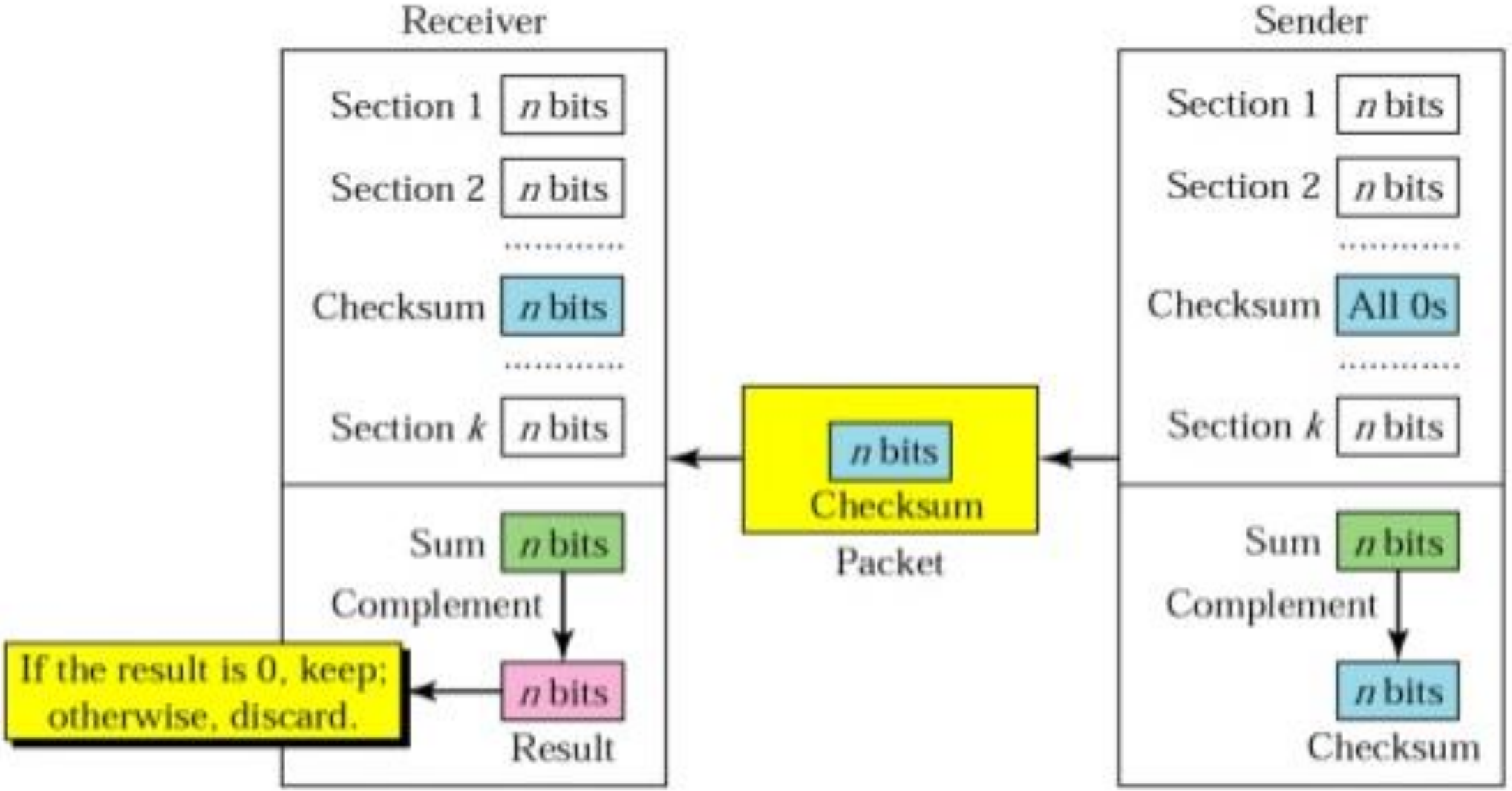

Original data
11001110 10111010 01110010 01010010
1 1 0 0 1 1 1 0
1
1 0 1 1 1 0 1 0
1
0 1 1 1 0 0 1 0
0
Row Parities
0 1 0 1 0 0 1 0
1
Column Parities
0 1 0 1 0 1 0
1


Original data
1100111 1011101 0111001 0101001
1 1 0 0 1 1 1 1
1 0 1 1 1 0 1 1
0 1 1 1 0 0 1 0
0 1 0 1 0 0 1 1
Row parities
0 1 0 1 0 1 0 1
Column parities
11001111 10111011 01110010 01010011 01010101
Data and parity bits

- **Advantages:**
- It is more efficient than single dimensional parity technique.
- It can detect multiple bit errors also.
- **Disadvantages:**
- It cannot detect compensating multiple bit errors. That means, if two bits in one data unit get corrupted and the two bits at the exact same position in another data unit also get corrupted so that they do not affect row and column parities, then such an error will go undetected.
- This technique cannot detect 4 – or more – bit errors in some cases.

- **3. Checksum:**
- The checksum refers to a sum of data bits calculated from digital data that is used to ensure the data integrity at the receiver's end.
- At the sender node, before transmission:
- i. The data being transmitted is divided into equal sized k number of segments, where each segment contains m number of bits.
- ii. The divided k segments are added using 1's complement arithmetic and extra bits (more than m bits) are added back to the sum (wrap-around).
- iii. The final sum's complement is calculated. This is the checksum.
- iv. Now all the data segments (k segments having m bits each) is sent along woth the checksum.

- At the receiver node, after transmission:
- v. Step ii is repeated at the receiver end, i.e., all the data segments are added using 1’s complement arithmetic (with extra bits wrapped around) to get the new sum.
- vi. This calculated new sum is added with the received checksum and then complemented.
- Now,
- A. If the result is all 0’s, the transmission is successful (i.e., no error) – Accept the data.
- B. If the result is not all 0’s, the transmission is erroneous – reject the data.


Receiver
Sender
Section 1
n bits
Section 2
n bits
Checksum
n bits
Section k
n bits
All 0s
Sum
Complement
Result
Checksum
Packet
If the result is 0, keep;
otherwise, discard.

Original Data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

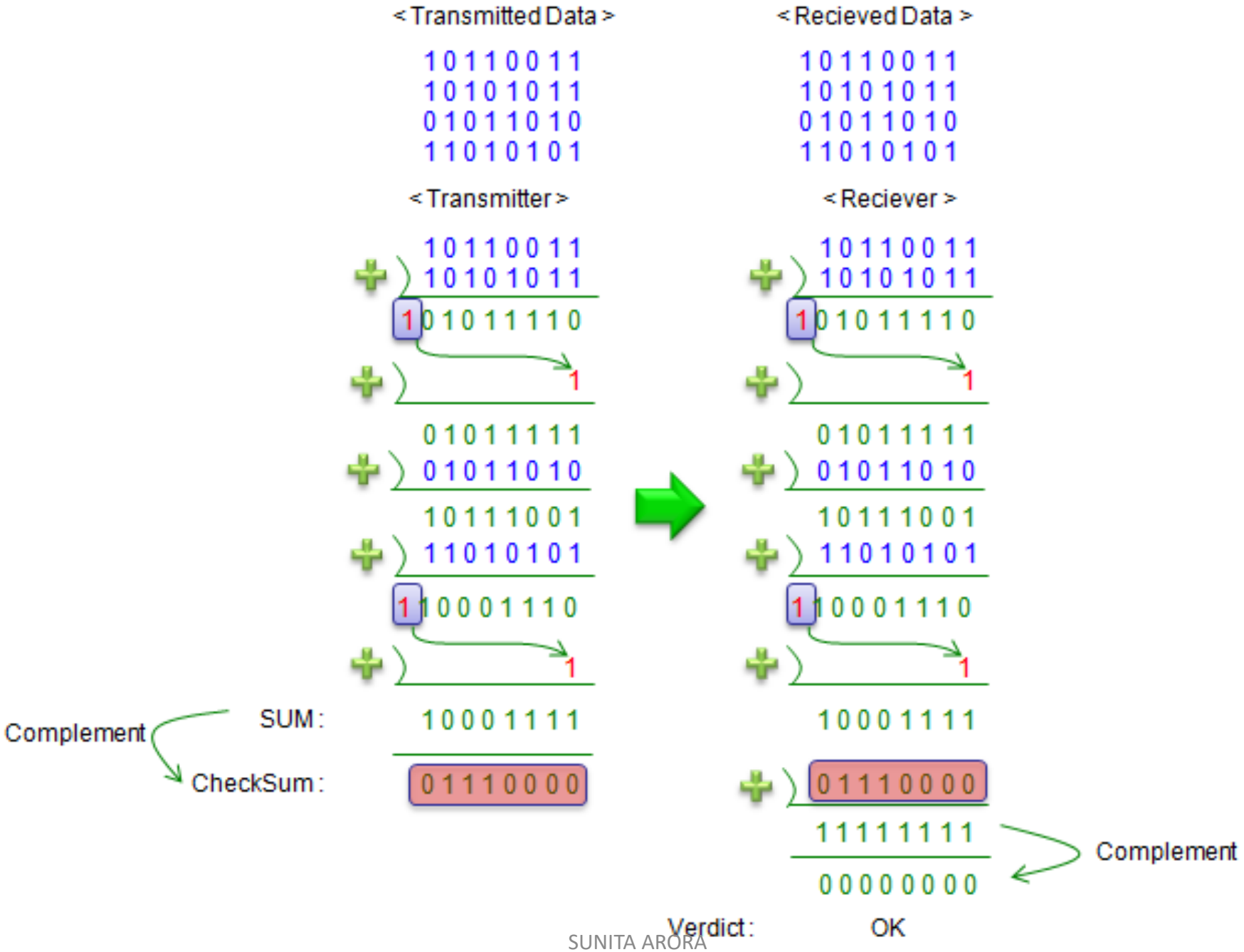
Sender

```
1   10011001
2   11100010
    --------
   (1)01111011
          1
    --------
    01111100
3   00100100
    --------
    10100000
4   10000100
    --------
   (1)00100100
          1
    --------
Sum: 00100101
CheckSum: 11011010
```

Reciever

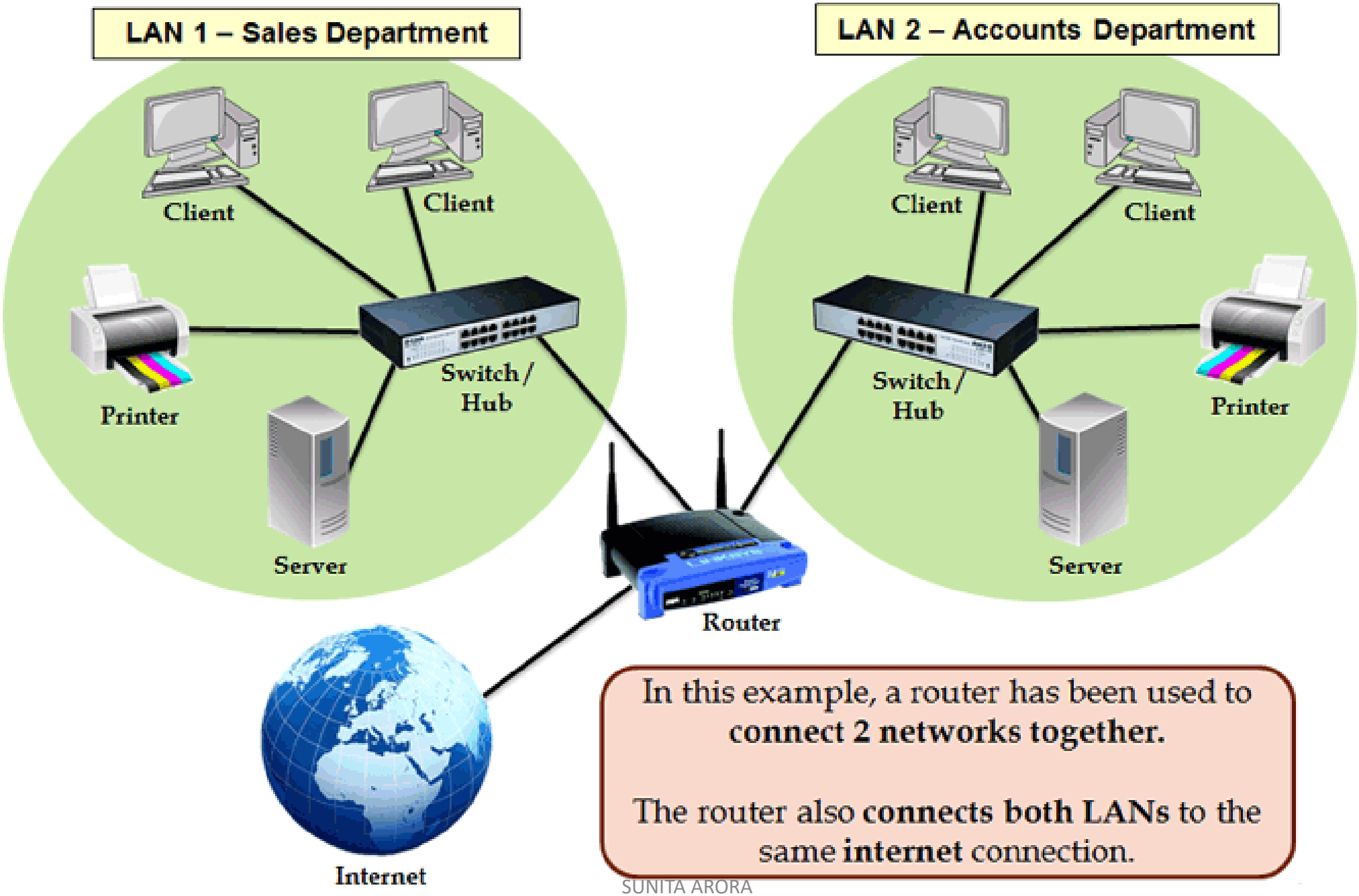
```
1   10011001
2   11100010
    --------
   (1)01111011
          1
    --------
    01111100
3   00100100
    --------
    10100000
4   10000100
    --------
   (1)00100100
          1
    --------
    00100101
    11011010
    --------
Sum: 11111111
Complement: 00000000
```

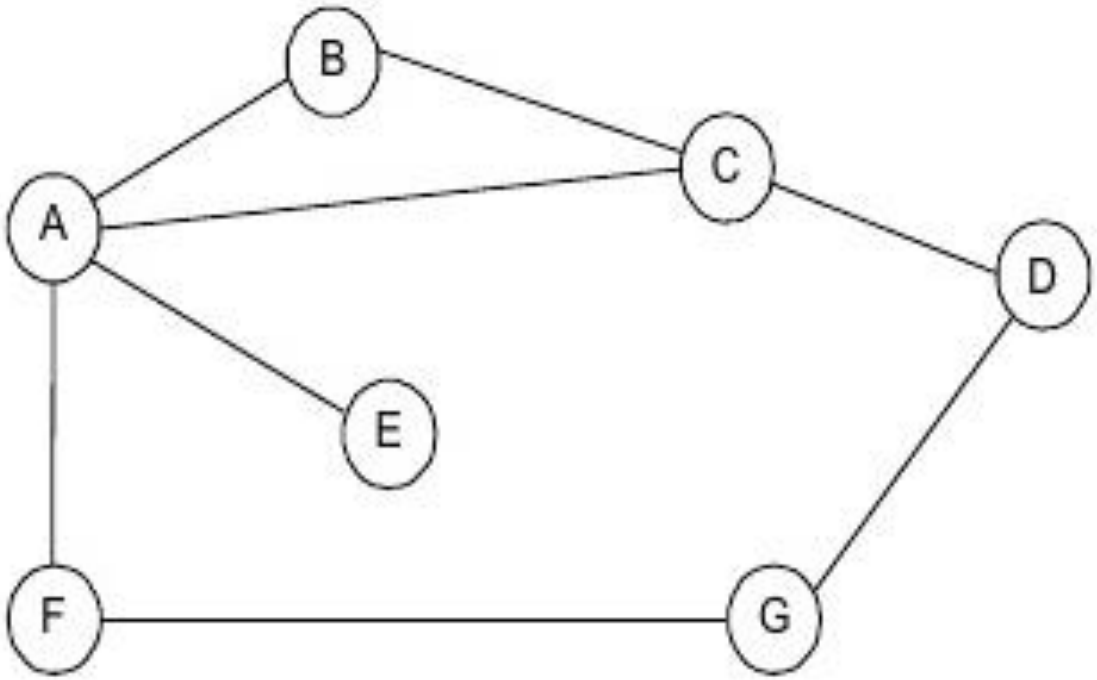
Conclusion: Accept Data


<Transmitted Data>
10110011
10101011
01011010
11010101
<Transmitter>
10110011
10101011
10101111 10
1
01011111
01011010
10111001
11010101
11000111 10
1
10001111
SUM:
Complement
CheckSum:
01110000
<Recieved Data>
10110011
10101011
01011010
11010101
<Reciever>
10110011
10101011
10101111 10
1
01011111
01011010
10111001
11010101
11000111 10
1
10001111
01110000
11111111
Complement
00000000
Verdict:
OK

MAIN IDEA OF ROUTING

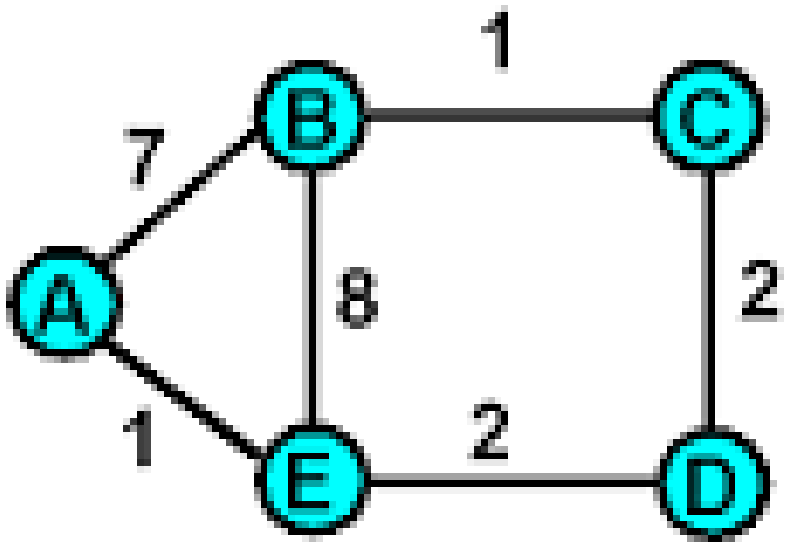
- The job done by a router is known as routing.
- Routing is the process of efficiently selecting a path in a network along which the data packets will travel to their destination.
- A router maintains a table called the routing table that stores routing information based on which the router determines the best path to a network.
- As various networks are connected to one another like a graph, there are multiple paths from one network to another, and router keeps track of best path to reach to another network.
- Router of one network is connected to routers of other networks and they keep exchanging information such as which networks they can reach etc.
- Every router maintains a table called routing table that stores the best paths to reach to other networks starting from it.
- Routers work with one goal: Find the best route for every destination.


LAN 1 – Sales Department
LAN 2 – Accounts Department
Client
Client
Client
Client
Printer
Switch / Hub
Switch / Hub
Printer
Server
Server
Router
Internet
In this example, a router has been used to connect 2 networks together.
The router also connects both LANs to the same internet connection.



Routing table for B

Destination	Cost	Next Hop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A



$D^E(\ )$		cost to destination via A	B	D
destinat.	A	(1)	14	5
	B	7	8	(5)
	C	6	9	(4)
	D	4	11	(2)

TCP/IP

- TCP/IP suite is the standard for both local and wide area networking.
- TCP/IP is used as a primary or sole communication protocol on nearly all new computer network installations.
- Currently, the Internet fully supports TCP/IP version 4 (IPv4).
- Internet has started adapting to TCP/IP version 6 (IPv6).
- TCP/IP is not tied to any one vendor, and therefore allows heterogeneous networks to communicate efficiently.

How TCP/IP Works

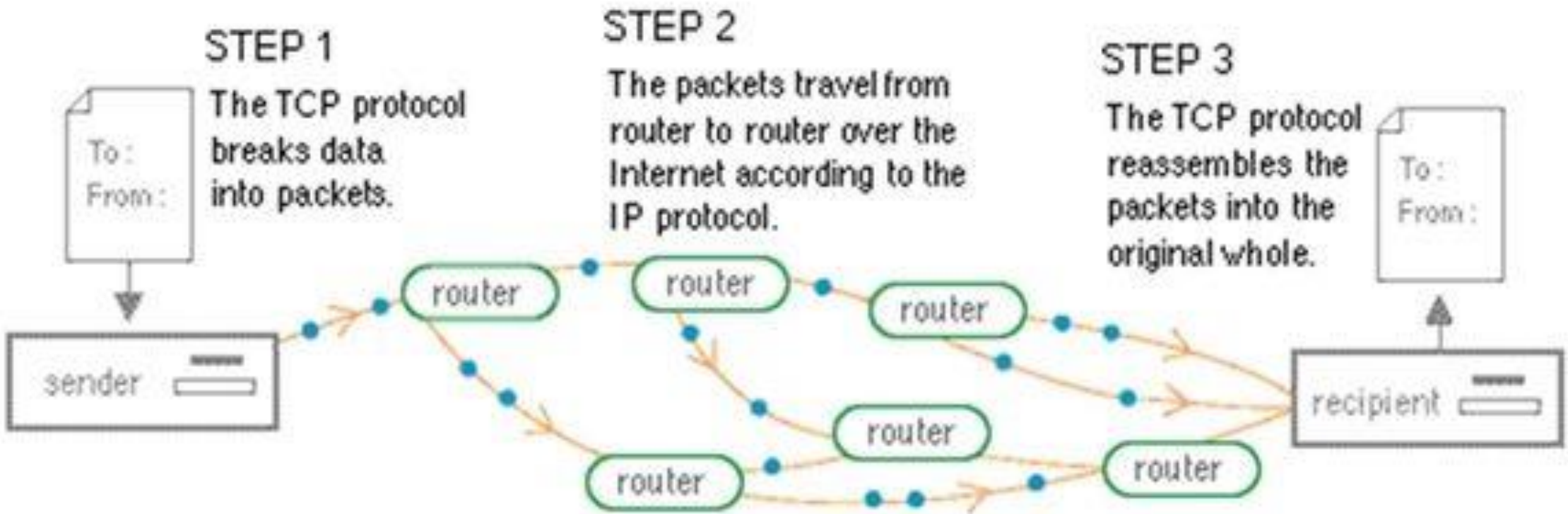
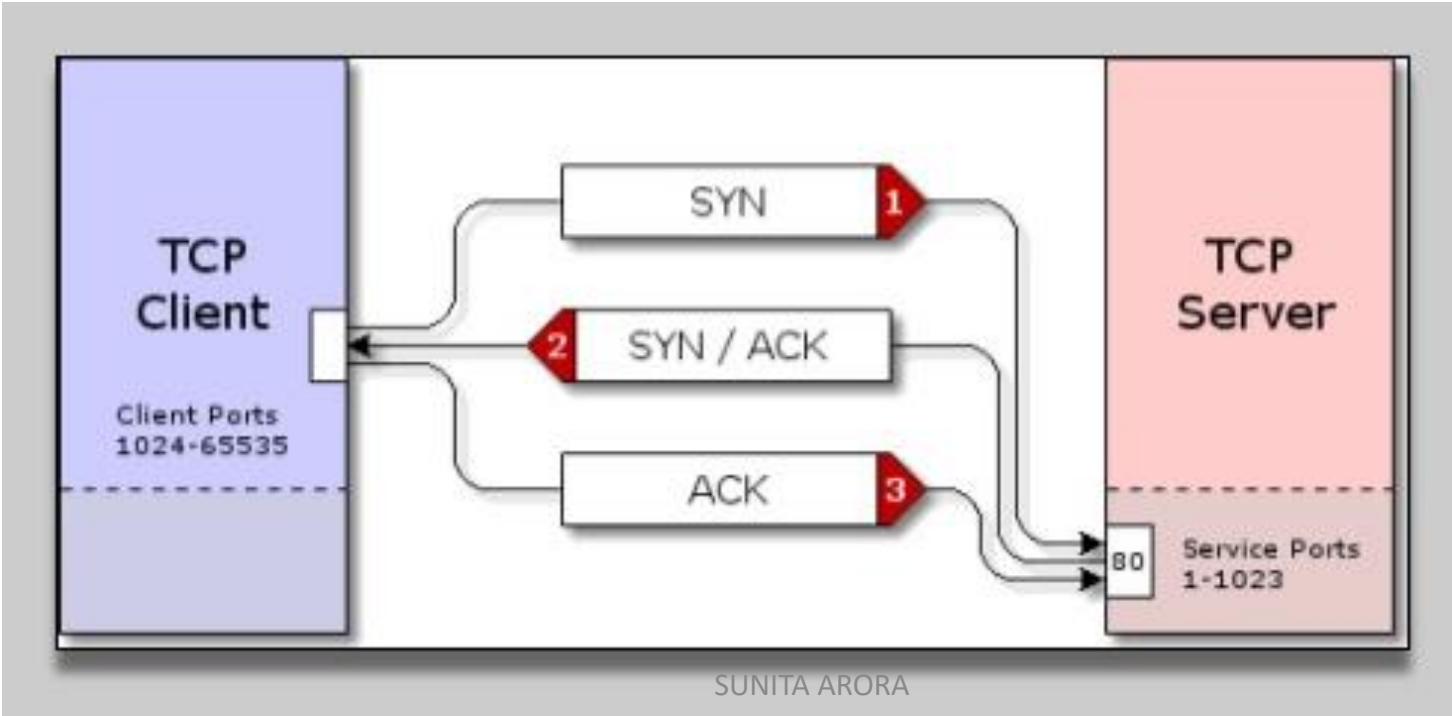
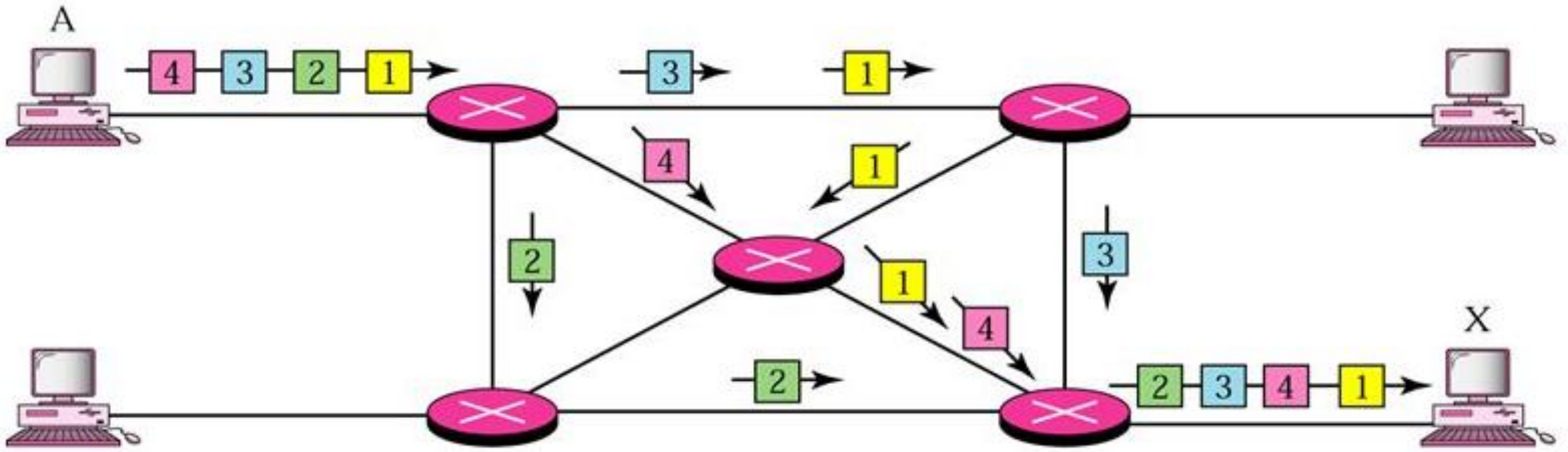


Figure 2. How data travels over the Net.

- TCP/IP is a collection of protocols that includes Transmission Control Protocol and Internet Protocol.
- TCP ensures reliable communication and uses ports to deliver packets. It is a connection-oriented protocol. In TCP, a connection must be built using a handshake process before information is sent or received. A handshake process means establishing a direct connection between sender and receiver with start signal, acknowledgement signals etc.

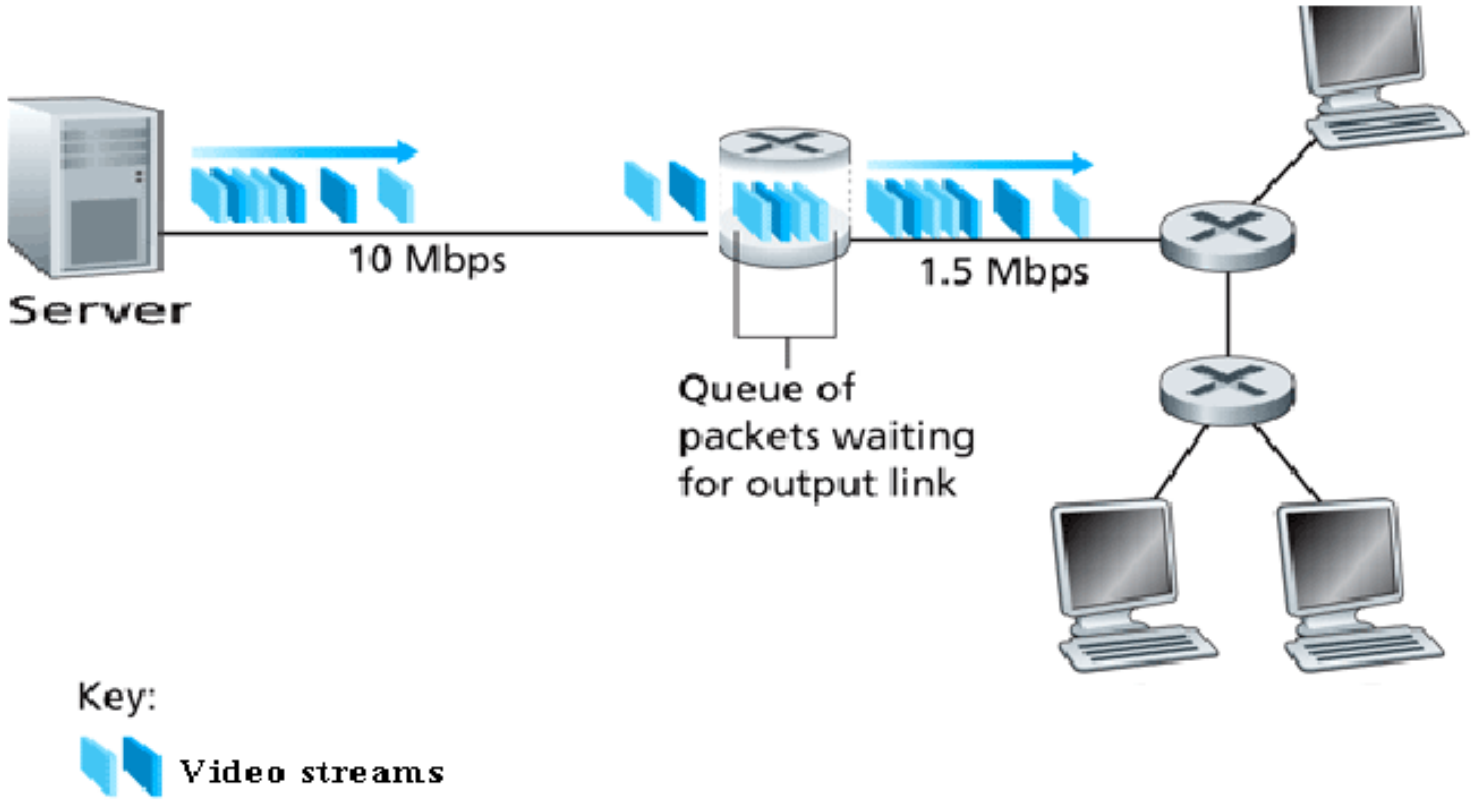


- IP is a connectionless protocol responsible for providing addresses of each computer and perform routing.



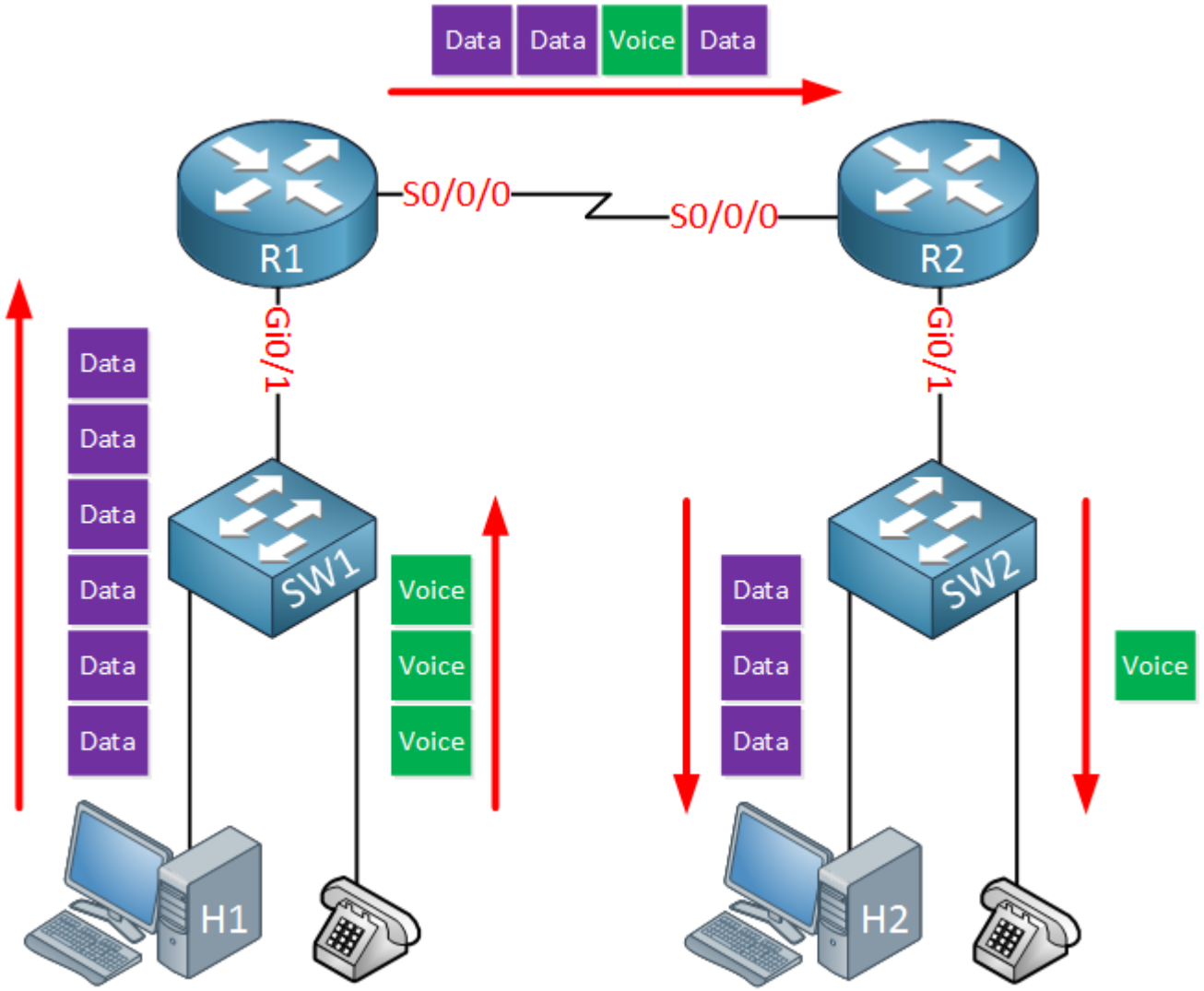
NETWORK CONGESTION AND RETRANSMISSION IN TCP

- Network congestion is a specific condition in a network when more data packets are coming to network devices than they can handle and process at a time.



- Network congestion results in many problems:
- 1. The receiving network device (such as router) cannot send acknowledgment signal (ACK signal) in time even if they have received the data.
- 2. The sender node retransmits the data when it does not receive the ACK signal and, this further increases the network traffic, causing more congestion.
- 3. It reduces the network throughput. Throughput is a measure of a network's performance.

- Symptoms of network congestion:
- 1. Excessive packet delay
- 2. Loss of data packets
- 3. Retransmission



- How network congestion is handled? (Analogy to road network congestion)
- The metering technique is implemented to control network congestion in the following ways:
- 1. It ensures that the sender does not overflow the network and it is done by controlling the flow of data packets (rate modulation of data packets). With this measure, the sender maintains a value indicating the limit of data that can be sent into the network without being acknowledged.
- 2. It ensures that the routers along the path work as per their capacity to handle network traffic and do not become overflowed. It includes strategies like:
- A. Rerouting the data packets.
- B. Informing the senders about the congestion to control the transmission rate.
- C. Delaying the transmission/retransmission depending upon the congestion levels.

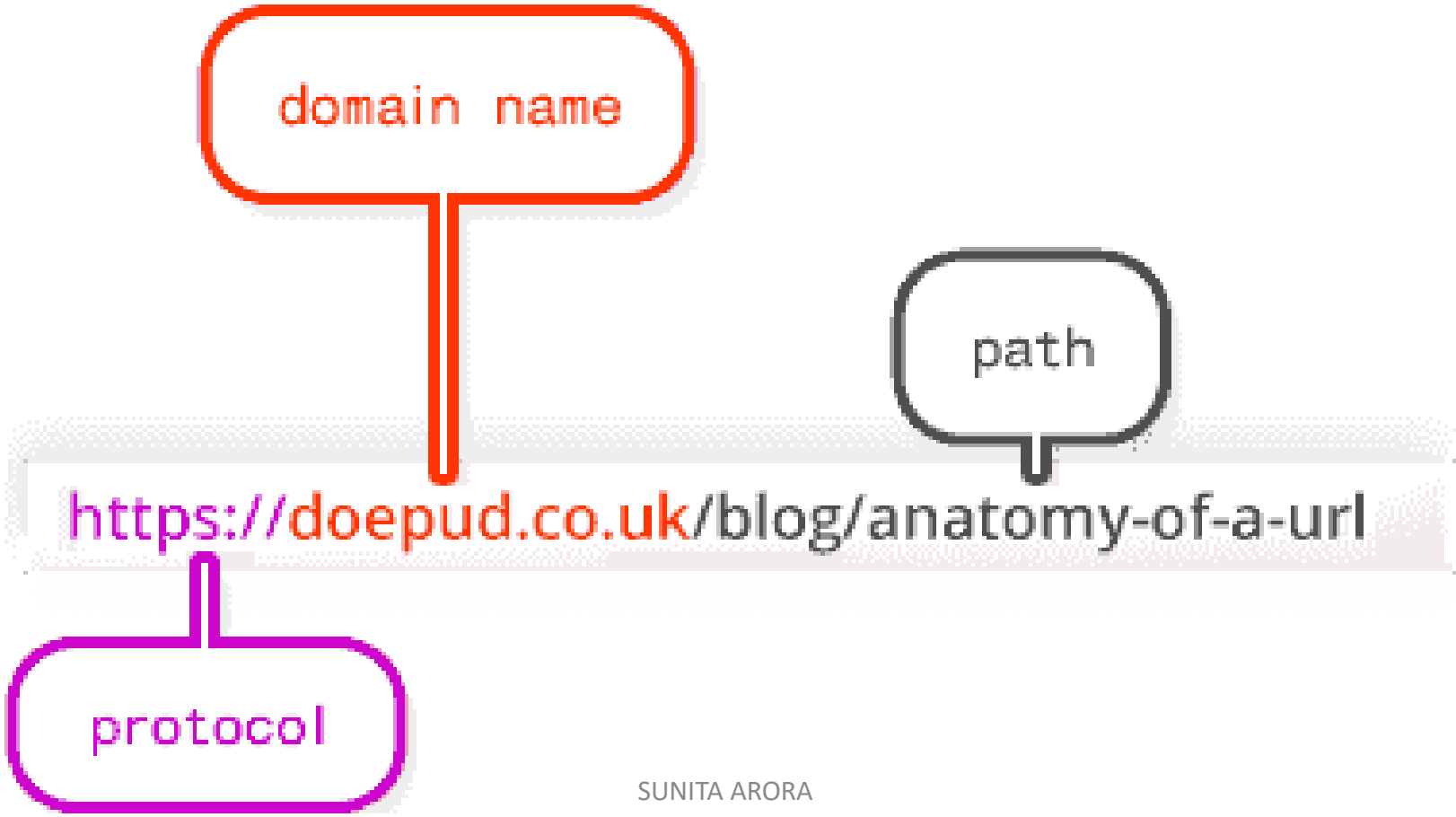
ADDRESSES ON A NETWORK

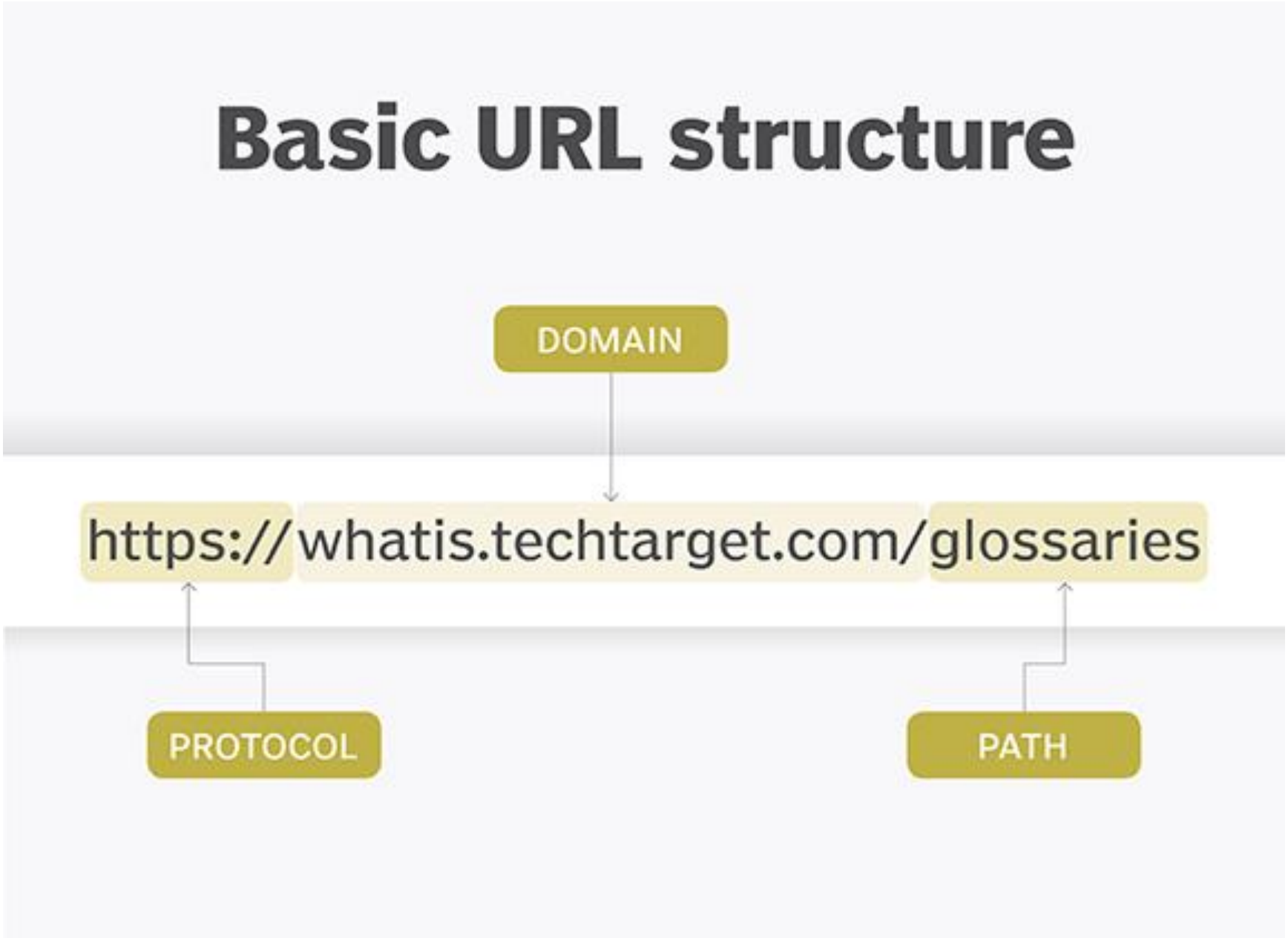
- Different addresses used on a network are:
- 1. Web Address (URL)
- 2. IP Address

Both the IP address and domain name URL can be used to connect to the same web server:

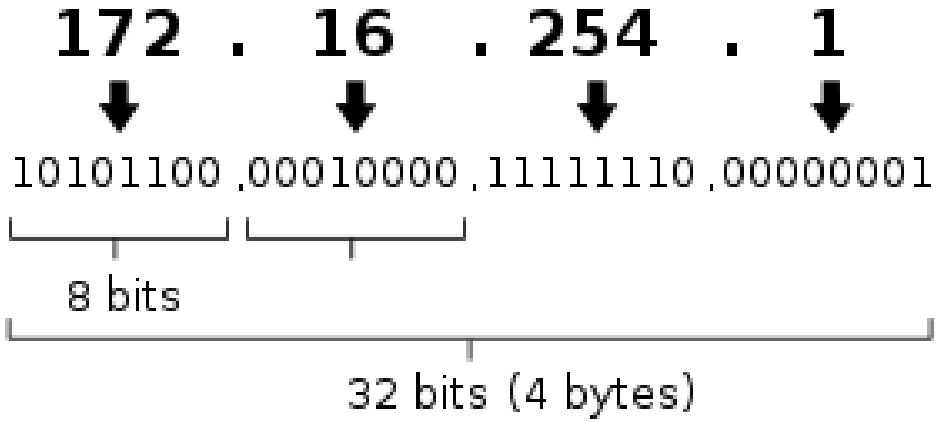
- e.g. 72.246.51.15 = www.nasa.gov
- e.g. 152.91.56.138 = www.gov.au
- e.g. 208.185.127.40 = www.about.com

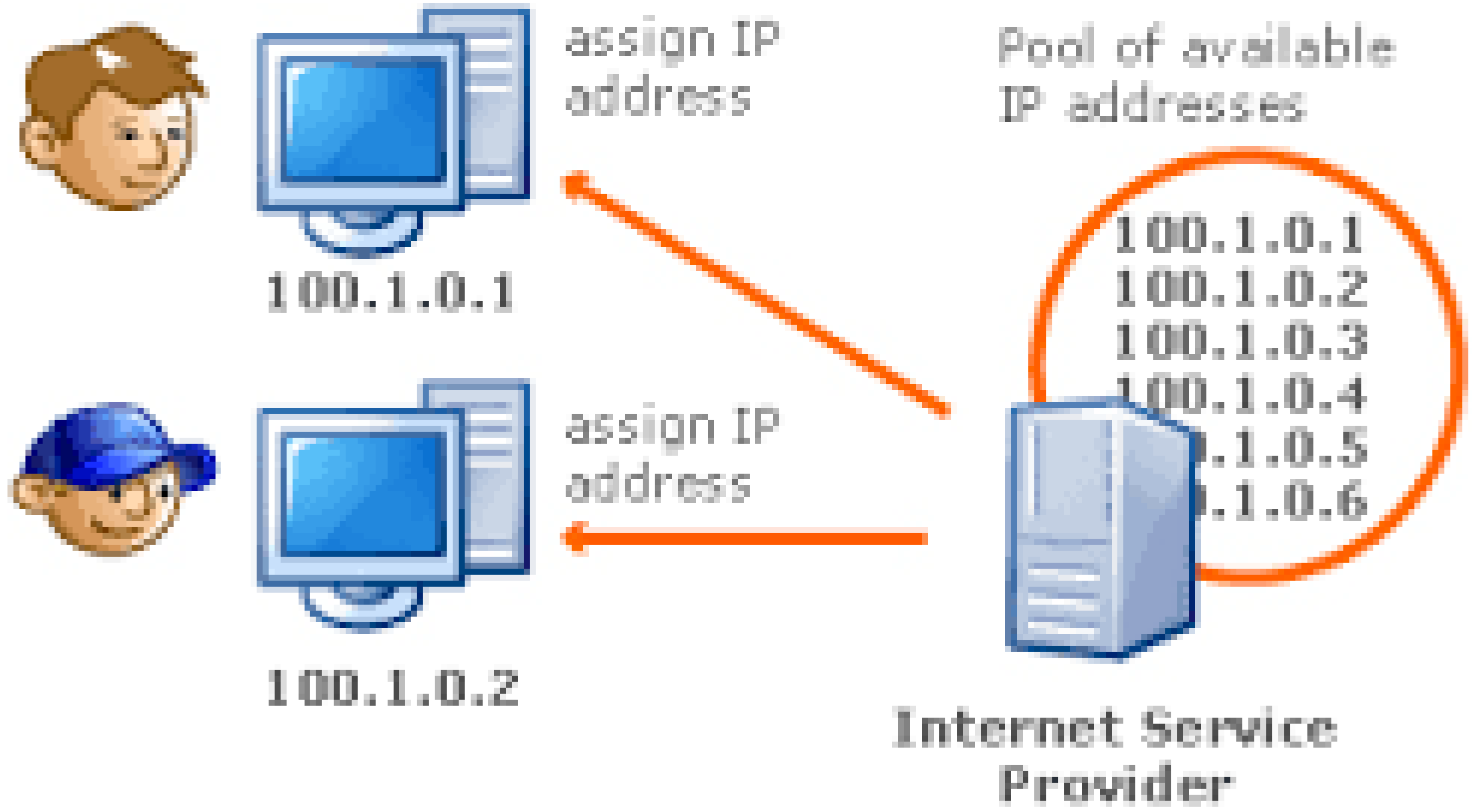
- **Web Address (URL):**
- A location on the net server is called a website.
- Each website has a unique address called URL (Uniform Resource Locator).
- A URL is an address of a file on Internet.




Basic URL structure
DOMAIN
https://whatis.techtarget.com/glossaries
PROTOCOL
PATH

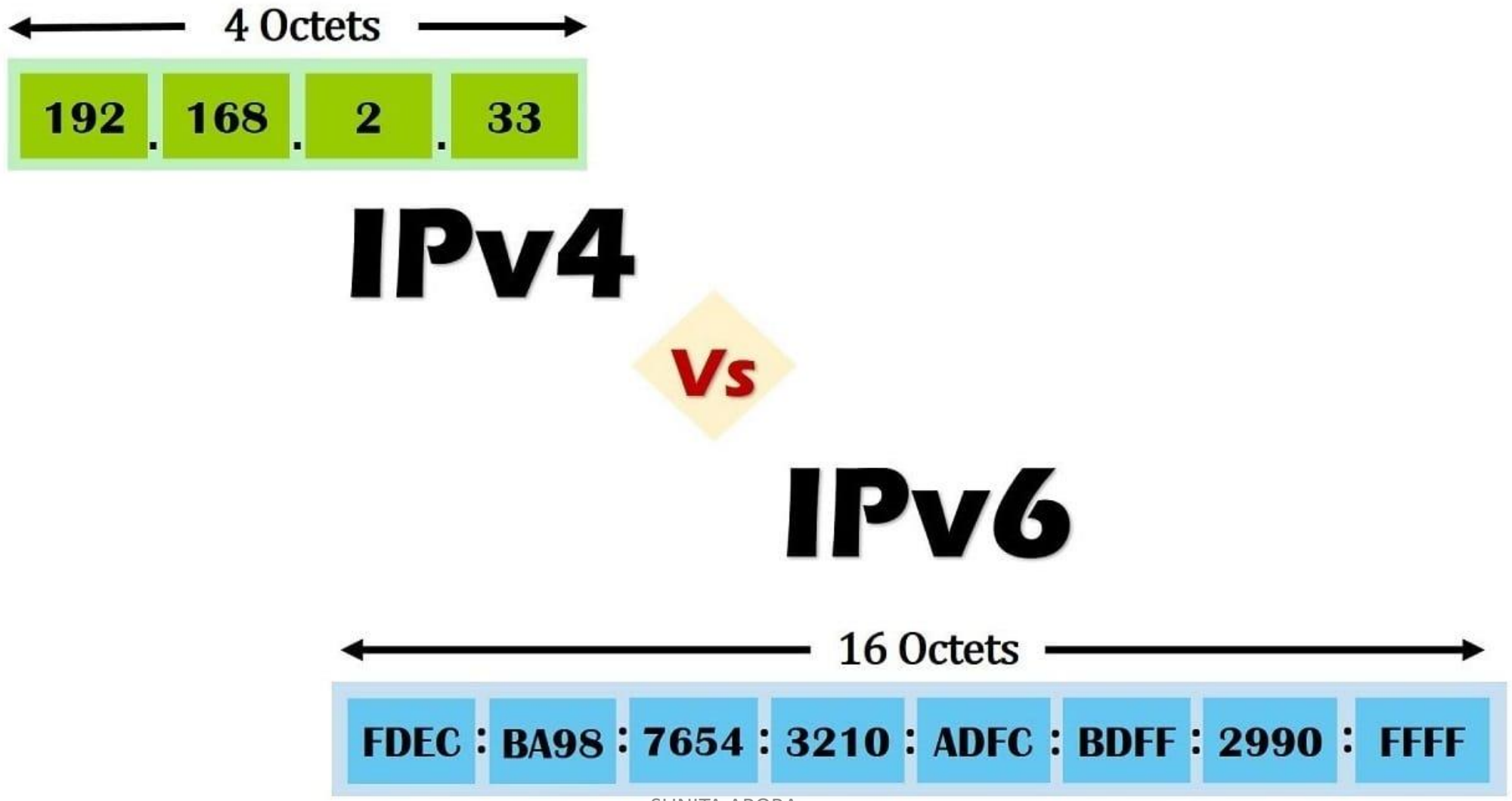
- **IP Address:**
- IP address is a unique numerical label as a string of numbers separated by dots, used to identify a device on the Internet.
- Each network device (a computer or any other network device) on a TCP/IP network needs to have a unique address on the network. This unique address on a TCP/IP network is the IP address.
- IP addresses are needed so that different networks can communicate with each other.
- Each IP address is actually a series containing four numbers separated by dots or periods e.g., 192.168.1.1 is an IP address.
- IP addresses are normally written in dotted decimal form but computers internally convert them into binary form.




assign IP address
Pool of available IP addresses
100.1.0.1
100.1.0.2
100.1.0.3
100.1.0.4
100.1.0.5
100.1.0.6
100.1.0.1
assign IP address
100.1.0.2
Internet Service Provider

IP ADDRESS	MAC ADDRESS
Internet Protocol Address.	Media Access Control Address.
It is called as logical address.	It is called as Physical Address.
It Is assigned by User/Administrator or ISP.	It is assigned at the time Hardware Is manufactured.
It is Software address.	It is hardware address.
Can be changed.	Can never be changed.
It is a numerical label that is assigned to a device participating in a computer network.	It is a unique 12 digit hexadecimal number assigned to each Network Interface card.
Ex: 192.168.0.2	Ex: 00:A0:C9:14:C8:35

- Internet Protocol (IP) Versions:
- There are currently two versions of IP.

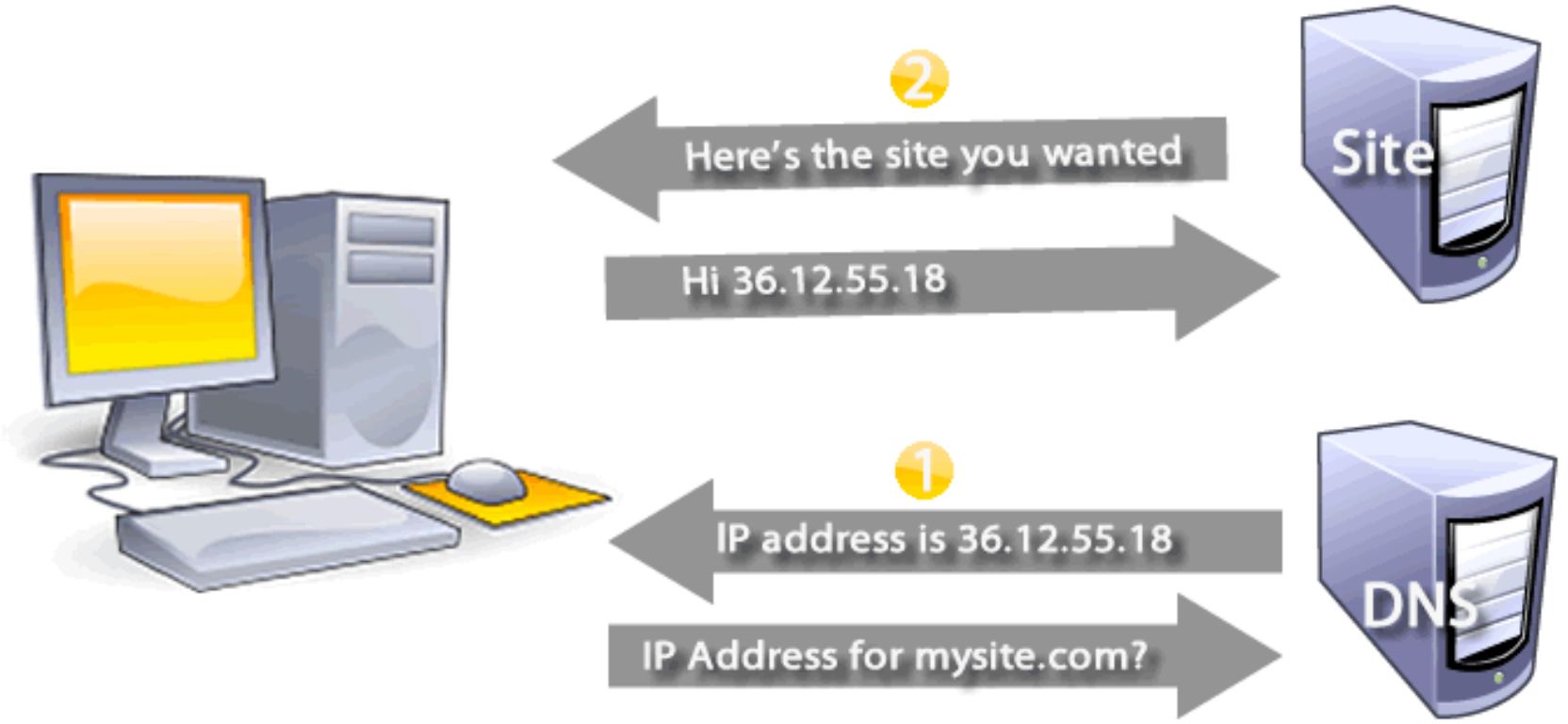


	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 199.43.0.202	Hexadecimal Notation: 2001:500:4:1::80
Number of Addresses	2^{32} = ~4 billion addresses	2^{128} = ~16 billion-billion addresses

- **Domain Name and DNS (Domain Name System):**
- Every computer connected to internet has an IP address.
- Different websites on internet also have their unique IP addresses.
- Domain name is the unique name assigned to a website.
- A domain name is also known as DNS name i.e, Domain Name System name.
- A domain name consists of 3 parts: 1. www 2. name describing website's purpose. 3. TLD (top level domain) such as .net, .org, .edu, .ca, .in.
- Few TDL's are: .com -> commercial business, .edu-> educational institutions, .gov-> government agencies, .mil-> military, .net-> network organizations, .org-> organizations (non-profit) country.
- The complete unique address of the page on the website is called URL (Uniform Resource Locator).


www.Google.com
173.194.36.51
Google
DNS Server

- **Domain Name Resolution:**
- Domain name resolution refers to the process of obtaining corresponding IP address from a domain name.
- A domain name is also known as DNS name i.e Domain Name System name.



CELLULAR/WIRELESS CONNECTIVITY PROTOCOLS

- Modern age cellular or wireless networks depend heavily on wireless connectivity protocols such as 2G, 3G, 4G etc.
- In networking, bandwidth refers to the transmission capacity of a computer or a communications channel.
- It is stated in megabits per second (Mbps).
- Higher frequencies offer higher bandwidth. It means they can handle more users, more data at the same time.
- **2G GSM (1992) – the Second Generation:**
- 2G, more familiarly known as GSM was introduced back in 1992 and is a fully digital technology. It allowed some data along with calls in the form of text messages.
- GSM can handle data speeds of upto 250 Kbps.
- The GSM standard is transmitted at frequency between 900 Mhz and 1800 Mhz.

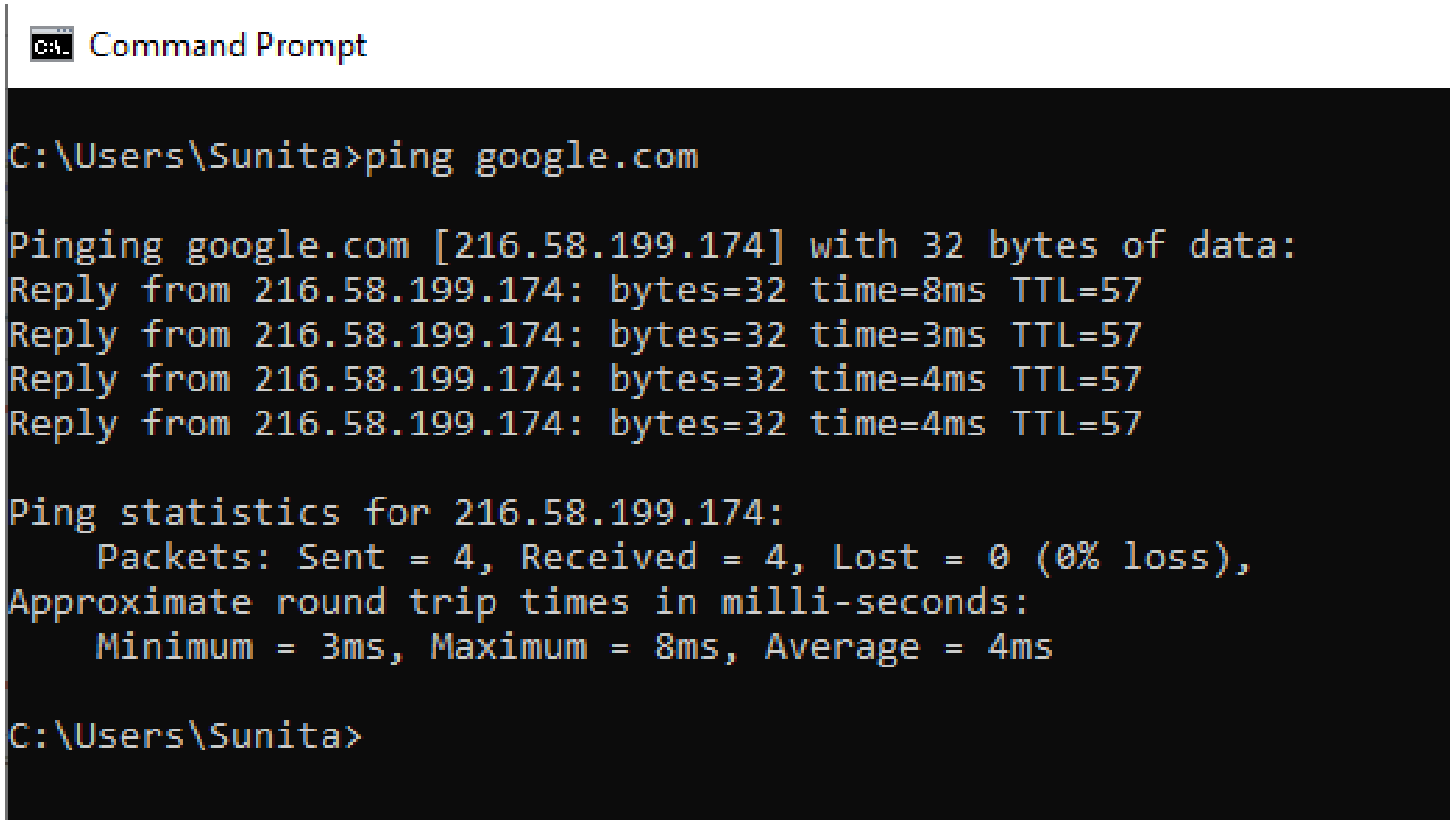
- **3G (2000) – the Third Generation Standard:**
- 3G was introduced to cater to increasing demand for data by consumers.
- 3G initially offered speeds of 500 Kbps to 2 Mbps, but over the years, it is now as high as 20 Mbps.
- It can handle data in the form of text messages and multimedia such as audio/video messages along with voice calls.
- 3G is transmitted at frequency 2100 Mhz.

- **4G (2013) – the Fourth Generation:**
- 4G offers data speeds in the range of 10-15 Mbps, which can go upto 50 Mbps and even higher depending on the technology.
- The operators use many different frequencies for 4G.
- In India the frequency range for 4G (LTE) is 1800 Hz to 2300 Hz.

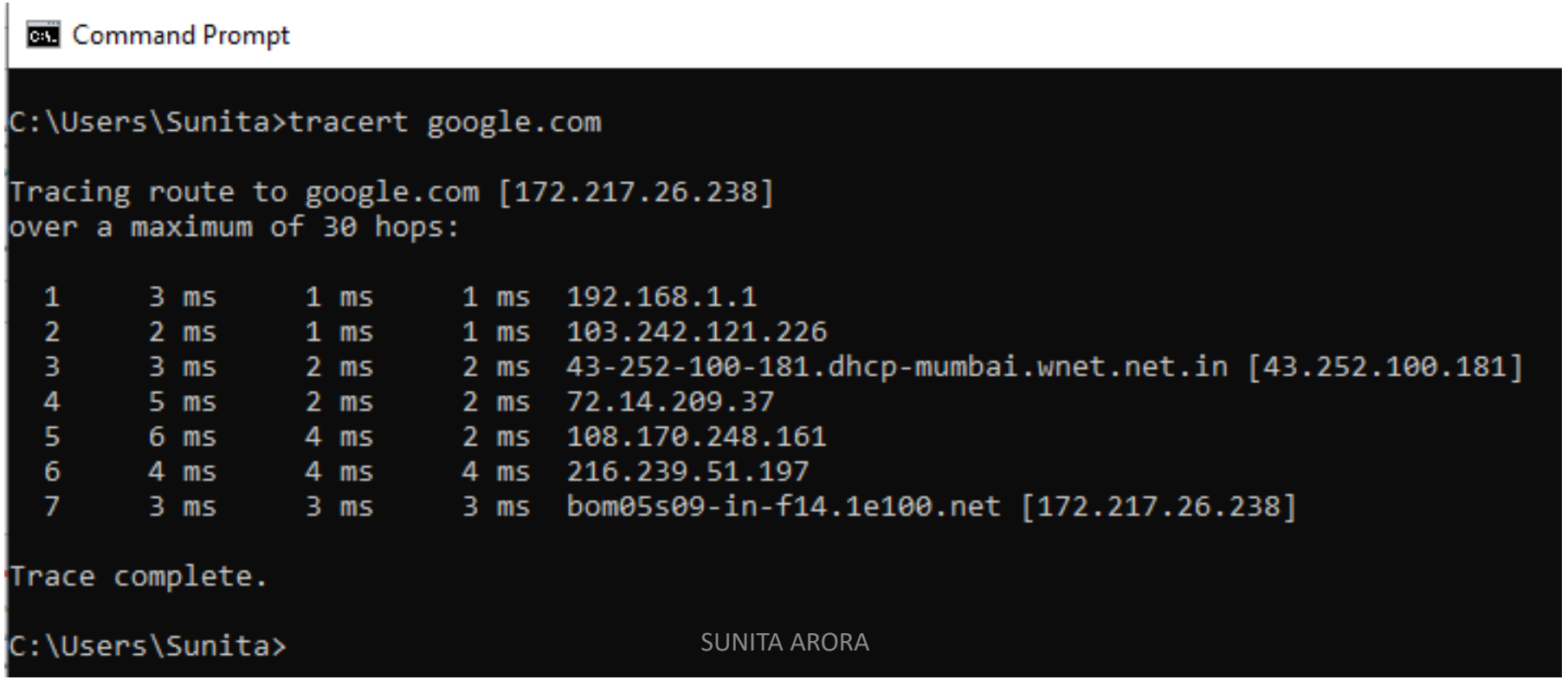
- **Wi-Fi:**
- WiFi protocol governs the rules to connect to the Internet without a direct line from your PC to the ISP. For WiFi to work, you need:
- 1. A broadband Internet connection.
- B. A wireless router, which relays your Internet connection from the “wall” (the ISP) to the PC.
- C. A laptop or desktop with a wireless internet card or external wireless adapter.

BASIC NETWORK TOOLS

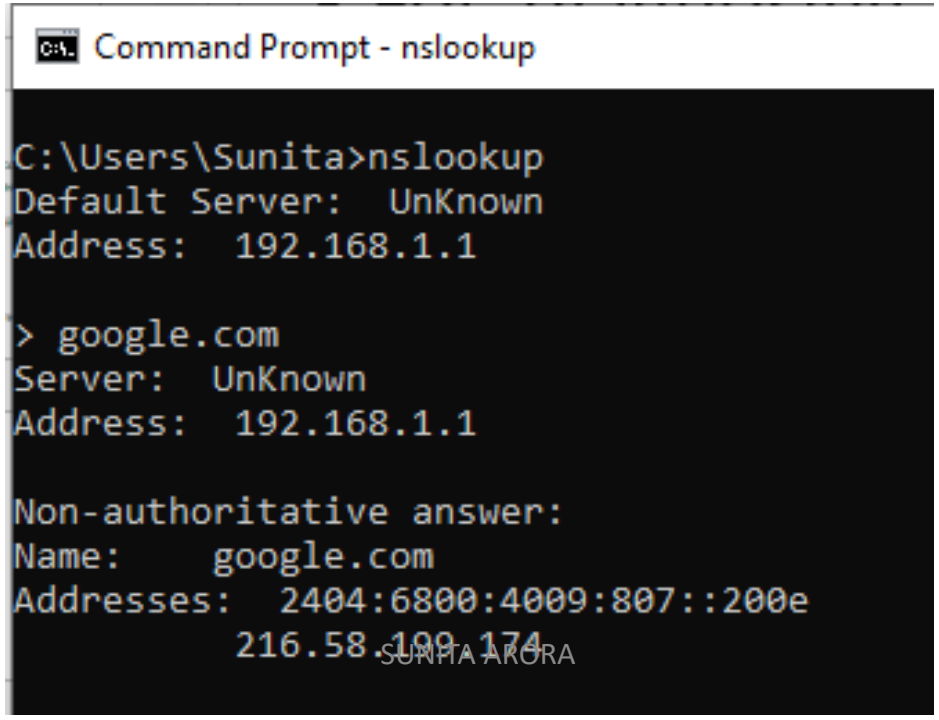
- **1. PING:**
- To test the connectivity between two hosts, you can use the PING command.
- PING determines whether the remote machine (website, server, etc) can receive the test packet and reply.
- It is determined by finding how much time it takes to get the response from the remote machine.
- Ping serves two purposes:
- A. To ensure that a network connection can be established.
- B. timing information as to the speed of the connection.
- You can use PING as per the format: ping <domain name or ip address).
- Ping command will work when you are connected to Internet.


Command Prompt
C:\Users\Sunita>ping google.com
Pinging google.com [216.58.199.174] with 32 bytes of data:
Reply from 216.58.199.174: bytes=32 time=8ms TTL=57
Reply from 216.58.199.174: bytes=32 time=3ms TTL=57
Reply from 216.58.199.174: bytes=32 time=4ms TTL=57
Reply from 216.58.199.174: bytes=32 time=4ms TTL=57
Ping statistics for 216.58.199.174:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 8ms, Average = 4ms
C:\Users\Sunita>

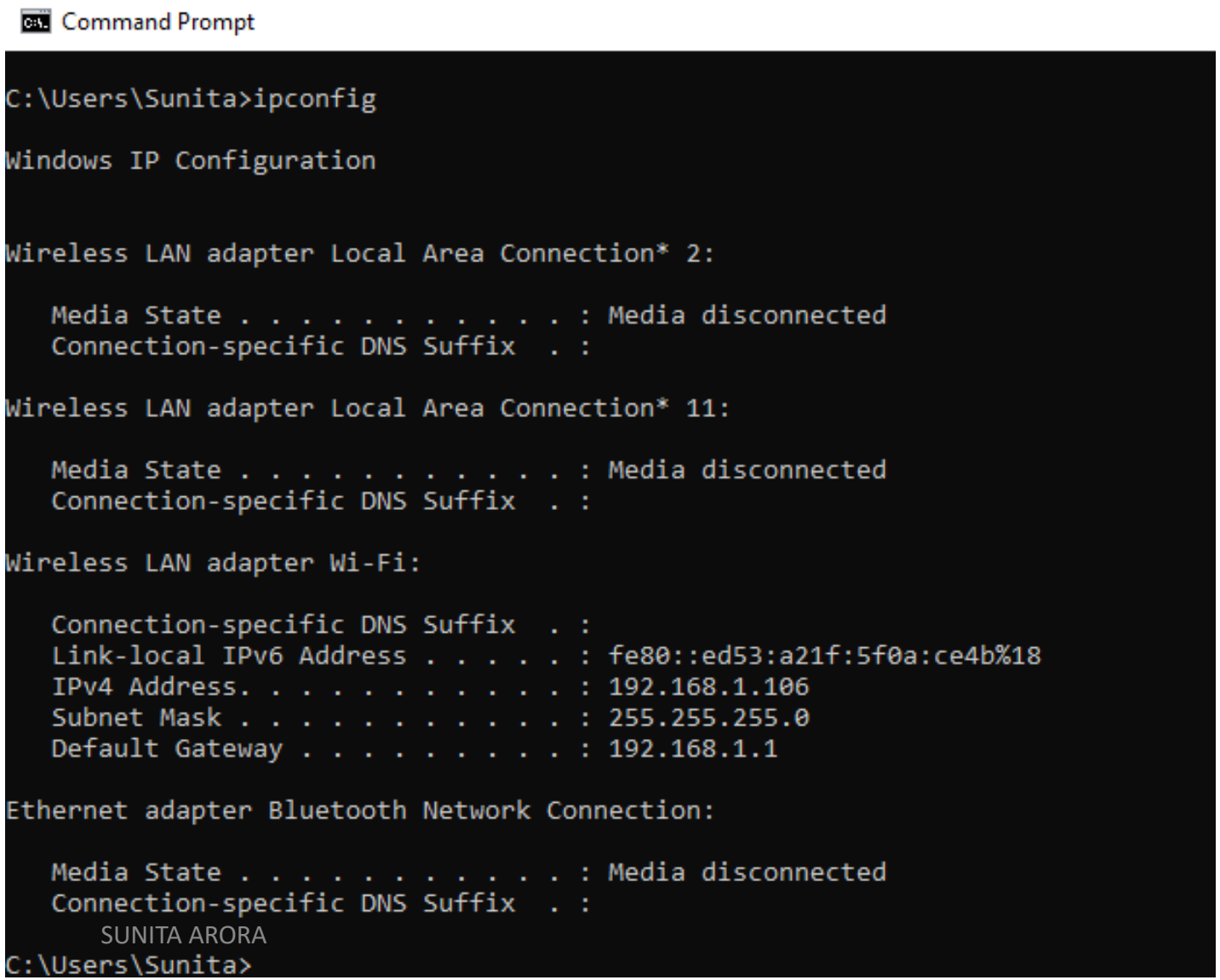
- **2. TRACEROUTE (for linux) or TRACERT (for windows):**
- Traceroute is a handy utility to view the number of hops and response time to get to a remote system or website.
- Like ping, for traceroute too, you need an Internet connection to make it work.
- You can use this command as follows: tracert <domain name or ip address>



- **3. NSLOOKUP:**
- For diagnosing DNS name resolution problems, you can use the command NSLOOKUP.
- It displays the name and IP address of your computer's default DNS server.
- It also displays a small prompt that is nslookup's own prompt. Here you can type the domain name or IP address. The result determines if your DNS server can resolve the given domain or IP address.
- Press CTRL+C to end nslookup's interactive mode.

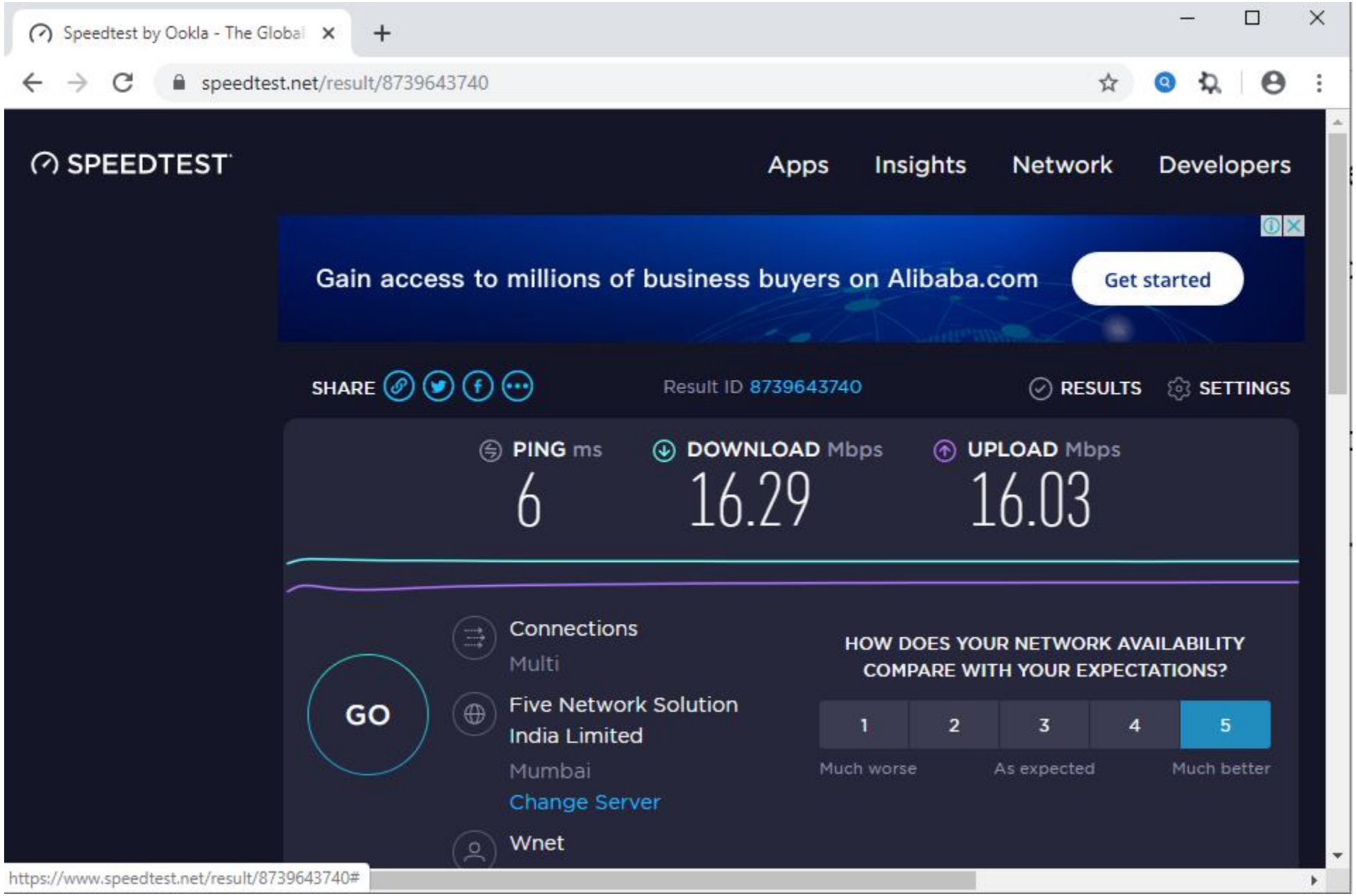


- **4. IPCONFIG:**
- The IPCONFIG command displays detailed information about the network you are connected to.
- It is used as follows: ipconfig



- **5. WHOIS command:**
- WHOIS command is used to get some information on a specific domain name, such as who registered it, when was it registered, and when the domain will expire etc.
- This command is used as follows: whois –H <domain name>

- **6. Speed test:**
- To check the download and upload speeds of your network connections, you can use a speed-test utility.
- To check the speed of your network, go to site speedtest.net while you are online and then click go.


Speedtest by Ookla - The Global
speedtest.net/result/8739643740
SPEEDTEST
Apps
Insights
Network
Developers
Gain access to millions of business buyers on Alibaba.com
Get started
SHARE
Result ID 8739643740
RESULTS
SETTINGS
PING ms
6
DOWNLOAD Mbps
16.29
UPLOAD Mbps
16.03
GO
Connections
Multi
Five Network Solution India Limited
Mumbai
Change Server
Wnet
HOW DOES YOUR NETWORK AVAILABILITY COMPARE WITH YOUR EXPECTATIONS?
1
2
3
4
5
Much worse
As expected
Much better
https://www.speedtest.net/result/8739643740#

VARIOUS PROTOCOLS USED ON NETWORKS

- **A protocol refers to a set of rules.**
- **1. HTTP (HyperText Transfer Protocol):**
- It is an application-level protocol.
- It is a generic, stateless protocol which can be used for many tasks.
- Messages are passed to HTTP in a format similar to that used by Internet Mail and Multipurpose Internet Mail Extensions (MIME).
- The HTTP consists of two fairly distinct items: the set of requests from browsers to servers and the set of responses going back to the other way.
- HTTP has various built-in request methods which allow users to read a web page, or to read a web page's header, or to store a webpage, or to remove the web page or to connect two existing resources or to break an existing connection between two resources.

- **2. FTP (File Transfer Protocol):**
- FTP is a standard for the exchange of files across internet.
- Files of any type can be transferred, although you many have to specify whether the file is an ASCII or binary file.
- It is very useful to transfer files from one network in an organization to another.
- It is a potent and popular way to share information over the Internet.
- FTP works as a client/server process. You give the command ftp using a remote address such as the following: FTP newday.horizon.com
- The above command means that the ftp running on your system is client to an FTP process that acts as server on newday.horizon.com.
- This protocol is mainly concerned with the transfer of files.

- **3. POP (Post Office Protocol):**
- POP3 that is Post Office Protocol version 3 has become a standard mail protocol.
- The POP3 defines the rules about receiving emails from a remote server to a local email client.
- It also makes it possible for the users to download their received email messages onto their local computer so that they can read them even when they are not connected to the Internet (offline reading).
- POP3 protocol is suitable if you are accessing your emails using a single application or from a single location.
- By default, POP3 deletes emails on the server after downloading them to your local email client.
- By default, the POP3 protocol works on two ports:
- Port 110: the default POP3 non-encrypted port, used for unsecured email communication.
- Port 995: the encrypted port used for secure email communication using POP3.

- **4. IMAP (Internet Message Access Protocol):**
- The IMAP is another mail protocol used in conjunction with POP3 protocol for accessing emails on a remote web server and downloads them to a local client.
- Contrary to POP3 that assumes that single application will access the email, IMAP supports multiple applications, even multiple clients and multiple locations.
- By default, the IMAP protocol works on two ports:
- Port 143 – the default, non-encrypted port (unsecure communication).
- Port 993 – encrypted port used for secure communication.

- **5. SMTP (Simple Mail Transfer Protocol):**
- While POP3 and IMAP protocols are used for fetching emails from the email servers to client application, the SMTP is used for sending emails across the Internet.
- By default, the SMTP protocol works on these ports:
- Port 25 – the default, SMTP non-encrypted port (unsecure)
- Port 465 – encrypted port (secure communication)

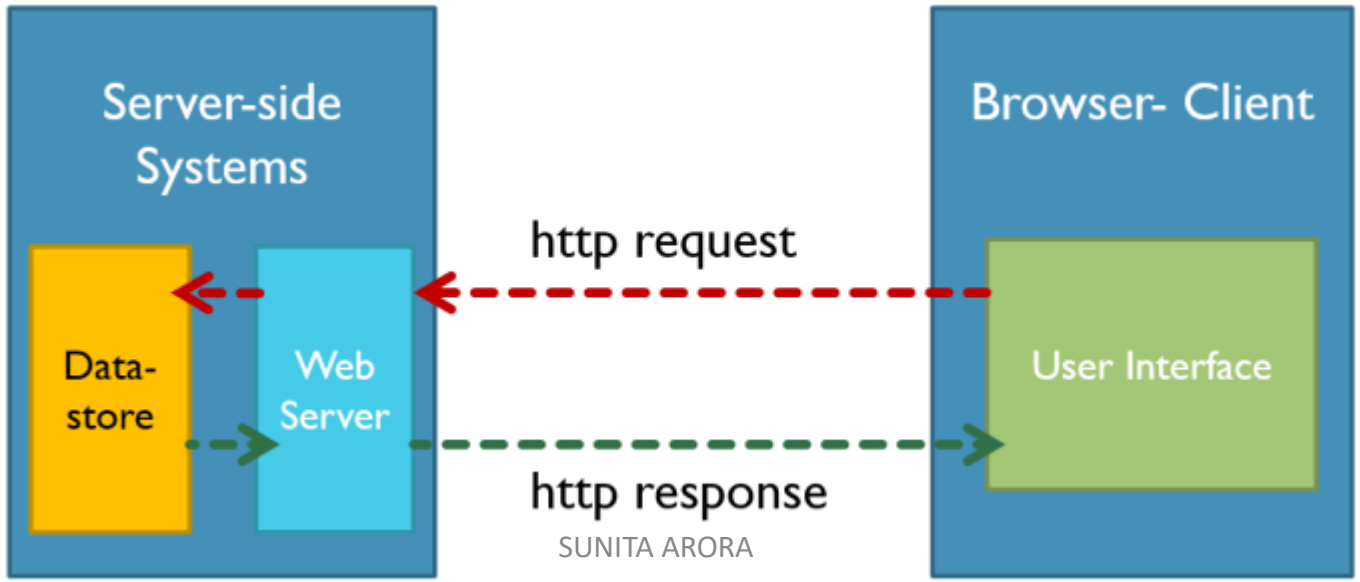
- **6. VoIP (Voice over Internet Protocol):**
- VoIP is a technology that enables voice communications over the Internet through the compression of voice into data packets that can be efficiently transmitted over data networks and then converted back into voice at the other end.

- **7. NFC (Near Field Communications):**
- NFC protocol is used to provide short-range wireless connectivity between two electronic devices that within the distance of 4-5 centimetres.
- It does not require special set-up like other type of wireless communication and establishes a two-way contactless connection between two electronic devices.
- Once NFC connection is established, the two connected device can share the digital content.
- NFC connection is inherently more secure because it is established only when two NFC supporting devices come closer to one another.

HOW HTTP WORKS – A BASIC IDEA

- Whenever we enter a URL in the address box of the browser, the web browser displays the intended URL's website or sometimes an error message.
- Internally, the web browser translates the URL into a request message according to the specified protocol; and sends the request message to the server.
- The web browser is the HTTP client here.
- The HTTP protocol uses a client-server communication model to facilitate the exchange of information on the web.
- There are HTTP clients that makes requests via HTTP protocol and HTTP servers that respond to HTTP requests.
- In other words, the web communication between a host and a client occurs, via an HTTP request/response pair.
- HTTP is a stateless protocol. In other words, the current request does not know what has been done in the previous requests.

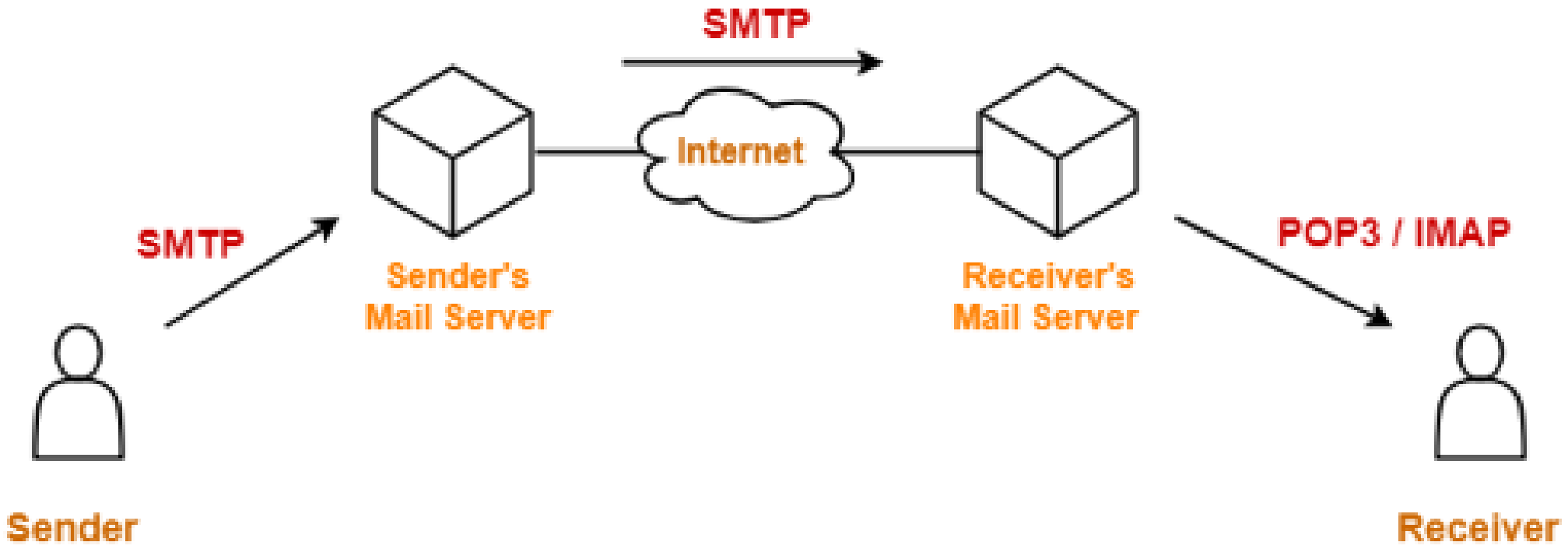
- HTTP working process:
- 1. The request message (HTTP request), is sent to an HTTP server in the form of URLs by the HTTP client.
- 2. The HTTP server receives the HTTP request, fetches the information as per the request and sends it to the HTTP client. This is called the response message from HTTP server.
- 3. The HTTP client (the browser) receives the response message, interprets the message and displays the contents of the message on the browser's window.

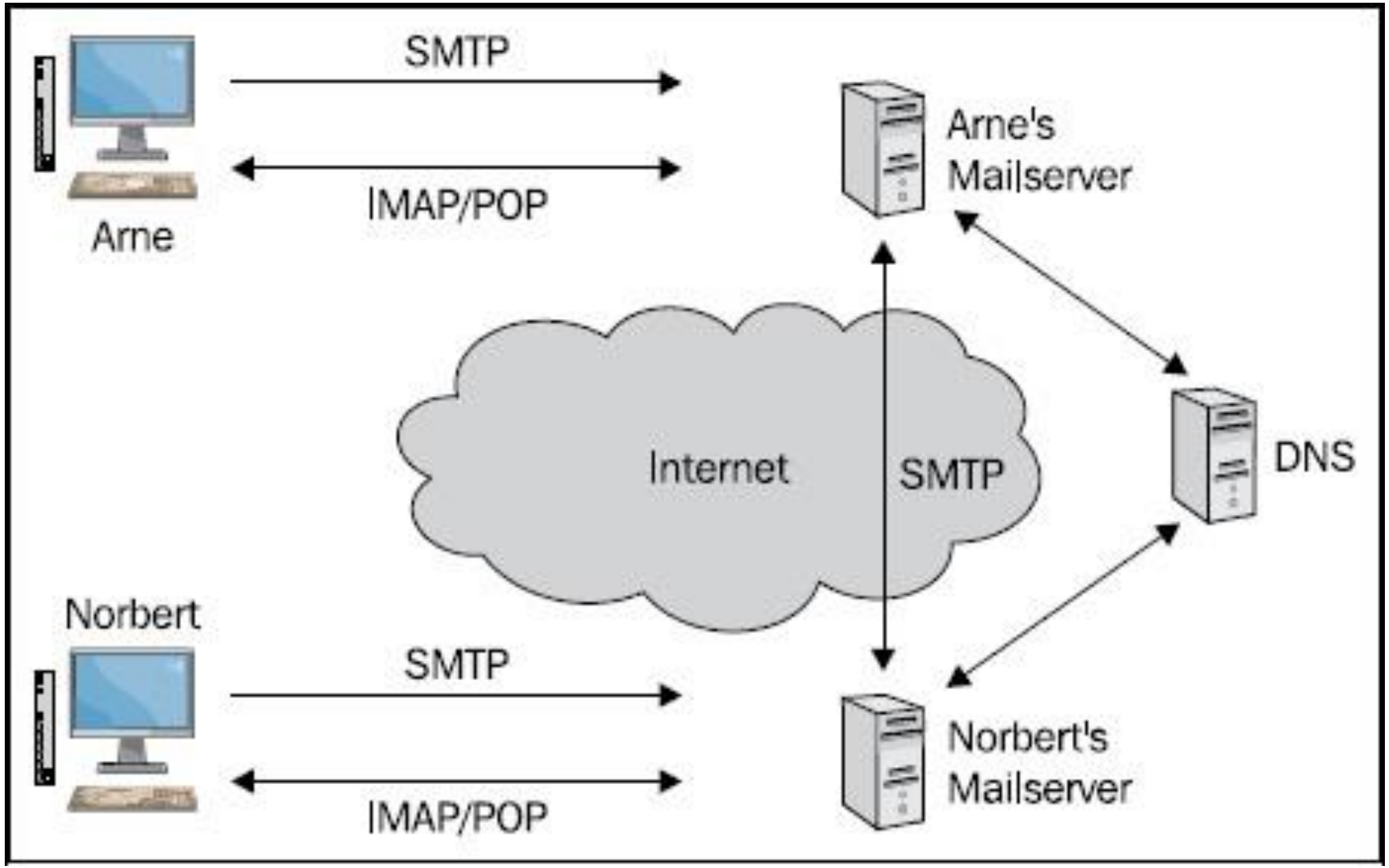


WORKING OF EMAIL

- General steps:
- i. You compose and send an email from your email client. Your email has the recipient’s email address along the email message.
- ii. Now your email client connects to the Outgoing SMTP server and hands over the email message in the required format.
- iii. The Outgoing SMTP first validates the sender details and if valid processes the message for sending and places it in Outgoing queue.
- iv. Next DNS loop up takes place. The SMTP server based on the domain details in the recipient address, looks up the DNS server of the domain and retrieves the recipient server information (such as MX records) of the recipient domain.
- Mail Exchange (MX) records are DNS records that are necessary for delivering email to the recipient’s address.

- v. Then the SMTP server connects with the recipient email server and sends the email through SMTP protocol.
- vi. The recipient server in turn validates the recipient account and delivers the email to the users mail account.
- vii. The user logs into own account and views the received email using email client that will use POP3/IMAP protocols.




SMTP
IMAP/POP
Arne
Arne's
Mailserver
Internet
SMTP
DNS
Norbert
SMTP
IMAP/POP
Norbert's
Mailserver

- For example, you have sent an email from your email account abc@gmail.com to xyz@yahoo.com. Once you clicked send button:
- A. Your email client contacts SMTP server of gmail.
- B. The SMTP server at gmail checks your email for recipient's email address and the recipient's address xyz@yahoo.com is extracted.
- C. The gmail SMTP server looks fort the MX (mail exchange) record of yahoo.com from DNS.
- D. The gmail SMPT server will retrieve the address of SMTP server of yahoo.com from its MX record and sends the email to SMTP server of yahoo.com.
- E. The SMTP server of yahoo.com receives the email message.
- F. The SMTP server of yahoo.com checks if the "xyz" recipient exists on that server (yahoo.com).
- G. If the account exists on that server, it forwards the email to its own IMAP/POP3 server (mail delivery agent) to store this email.

SECURE COMMUNICATION

- To ensure the safety of the information being transmitted over the web, many Internet security measures are employed.
- Encryption is one of such measures and is highly recommended too.
- Encryption is a technique that translates the original data into a form which is not a usable form of data.
- The encrypted data must be decoded or decrypted to bring it back to the original form.
- To decrypt the data, a specific code called the decryption key is required.
- Only the people that have access to this secret code (the decryption key) can decode and read the actual data.
- Crucial data's safety is ensured by the use of a protocol called HTTPS (HTTP Secure), which transfers the data in encryption form so that eavesdropping cannot make use of it.

- **HTTPS:**
- HTTPS stands for HyperText Transfer Protocol Secure and is a combination of HTTP and SSL/TSL protocols.
- HTTPS provides encrypted communication and secure identification of a network web server.
- HTTPS encrypts your data and establishes a secure channel over a non-secure network to ensure protected data-transfer.
- Thus data is protected from eavesdroppers and hackers who want to intercept and access your data.
- That is why most banks apply HTTPS because HTTPS connections are more secure for online payment transactions compared to HNTTP connections.

- How to check if your connection is secure?
- Before keying in any personal/financial information on any website, make sure that the URL starts with “HTTPS” and that there is a padlock sign on the navigation bar footer of your browser.

- **Secure Socket Layer (SSL):**
- SSL stands for Secure Socket Layer protocol.
- It is a mechanism of data transfer over Internet to provide a safe passage for the transmission of data – like transferring a message inside a locked safe.
- It encrypts (i.e., converts into un-understandable form) the data so that a third party cannot eavesdrop on the transmission and view the data being transmitted.

- How SSL works?
- The working of SSL requires that the website has SSL certificate installed which ensures its authenticity.
- Once installed, the sensitive information (such as credit card details, Login and password details etc.) is obtained from the user through a secure connection over Internet.
- Without SSL, the attackers can try to steal personal information given to site.


Requests secure SSL session
Sends certificate
Customer
Sends one-time encryption key for session
Server
Server decrypts session key using private key and establishes a secure session

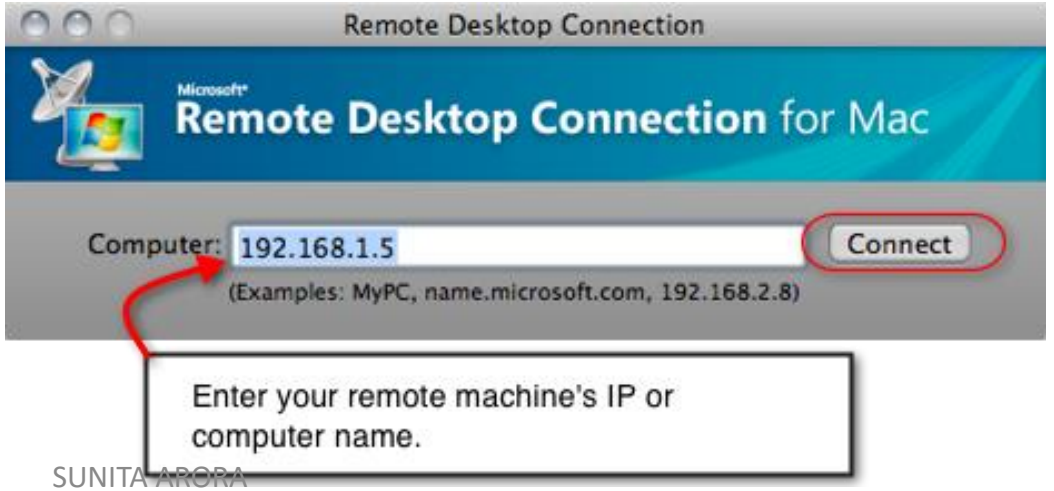
How does HTTPS work: SSL explained

This presumes that SSL has already been issued by SSL issuing authority.

NETWORK APPLICATIONS

- Computer networks have connected computers all over the world in a way that it is now possible to work on a computer even if you are not physically present next to it.
- Two network applications that make such an access possible are:
- **1. Remote Desktop**
- **2. Remote Login**

- **1. Remote Desktop:**
- Remote desktop connection is a technology that allows you to sit at a computer (the client computer) and connect to a remote computer (the host computer) in a different location.
- For instance, you are working on an important project when you fell ill. The doctor has advised you not to travel, but you can work from home. This time, you would want to connect to your work computer (the host computer) while sitting at your home, working on your home laptop (the client computer) using the remote desktop application.
- The remote desktop application displays the desktop of the host computer on the screen of the client computer, and the user can work on it as if it is his/her computer.



- **2. Remote Login:**
- A remote login facility permits a user to work on a program on a distant computer based on valid login credentials.
- The work access to a program is granted by login concept wherein users having authorized login and password to work on that program are allowed access.
- There are two login programs: TELNET and SSH that facilitate remote login on the Internet.
- You specify the remote machine on which you want to work, and these programs will help you connect to it.
- After entering valid login details, you are allowed access to the application program you want to work on.
- Whatever keystrokes and mouse movements you perform on the client program, it sends them to the remote device, and the remote computer sends the output as per sent keystrokes/mouse movements.
- The output received is then displayed on the screen of the client.