TCP/IP NETWORKING

(CET 06102)

UNIT 3

IP Address Configuration for the Public and Private Network

- **IP address** consists of four octets separated by periods, such as 129.79.123.156.
- **Each octet** designates either a *network address* or a *host address* on that network. *Which octets are used to designate the network and host address depends on the network class*.
- **There are three network classes; A, B, and C.**

The *subnet-mask* defines which bytes of the IP address represent the subnet and the host. *If no number is specified a default value is set according to the class of network that the machine is on*. The subnet-mask is conventionally given in hexadecimal.

The IU subnet-mask is *0xffffff00*, or *255.255.255.0*. The *first two characters are not part of the number*. They indicate that what follows is a hexadecimal number.

In any network, when we need to send data to a host device connected to the network, a router uses a broadcast address. Moreover, every network has one unique broadcast address.

Broadcast Address is an address that enables transmission to every node in a local network. The address is the highest numeric value of the address format being used.

We can simply replace the last bits of a network address by 1, and that would turn into a broadcast address. Therefore, we can determine the broadcast address of any network using the subnet mask and the IP address of that network.

Let's take a class C IP address: 192.168.1.0. It's a network address. Accordingly, the broadcast address for the given network address would be 192.168.1.255.

An Ethernet network is type of broadcast network. In a broadcast network any system can send information and all systems receive every message, *although* they discard messages that are not addressed to them.

Broadcasting is accomplished via the broadcast address. This is the address to use for reaching all other addresses on a network.

Any address with the host octet set to all 1's, or 255, is by default interpreted as a broadcast address.

So the **broadcast address** is the address of the subnet, *plus* 255. If a hosts IP address is 129.79.149.145, it's subnet address is 129.79.149 and it's broadcast address would be 129.79.149.255.

There are **two types** of IP addresses (in terms of *accessibility*, *uniqueness* & *naming conventions*): Public and Private.

An **IP address** is a number used to identify a host on an IP (Internet Protocol) network.

In order to successfully communicate on the Internet or any other computer network, a machine must have a network interface and an IP address assigned to it that is unique to that network.

- **Public IP address** is an IP address that is unique to the entire Internet. Public IPs can be accessed globally; therefore, *they are often used by publicly accessible entities such as websites*, *DNS* and *VPN servers*, etc.

➢Static IP address

Public static - some times called Dedicated - means the IP address never changes and is tied to a single user, device, server or website.

➢Dynamic IP address

Public dynamic - means the IP address can change from time-to-time (for example, when you lose connection and re-connect or the ISP might change the address periodically).

▪ Private IP address

Private IP address (Internal) is only used by devices communicating to each other on the same network. Devices with private IP addresses cannot connect to the Internet directly. Likewise, computers or other devices outside the local network cannot connect directly to a device with a private IP.

An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks.

The following are the three blocks of the IP address space for private networks:-

i. 10.0.0.0 - 10.255.255.255

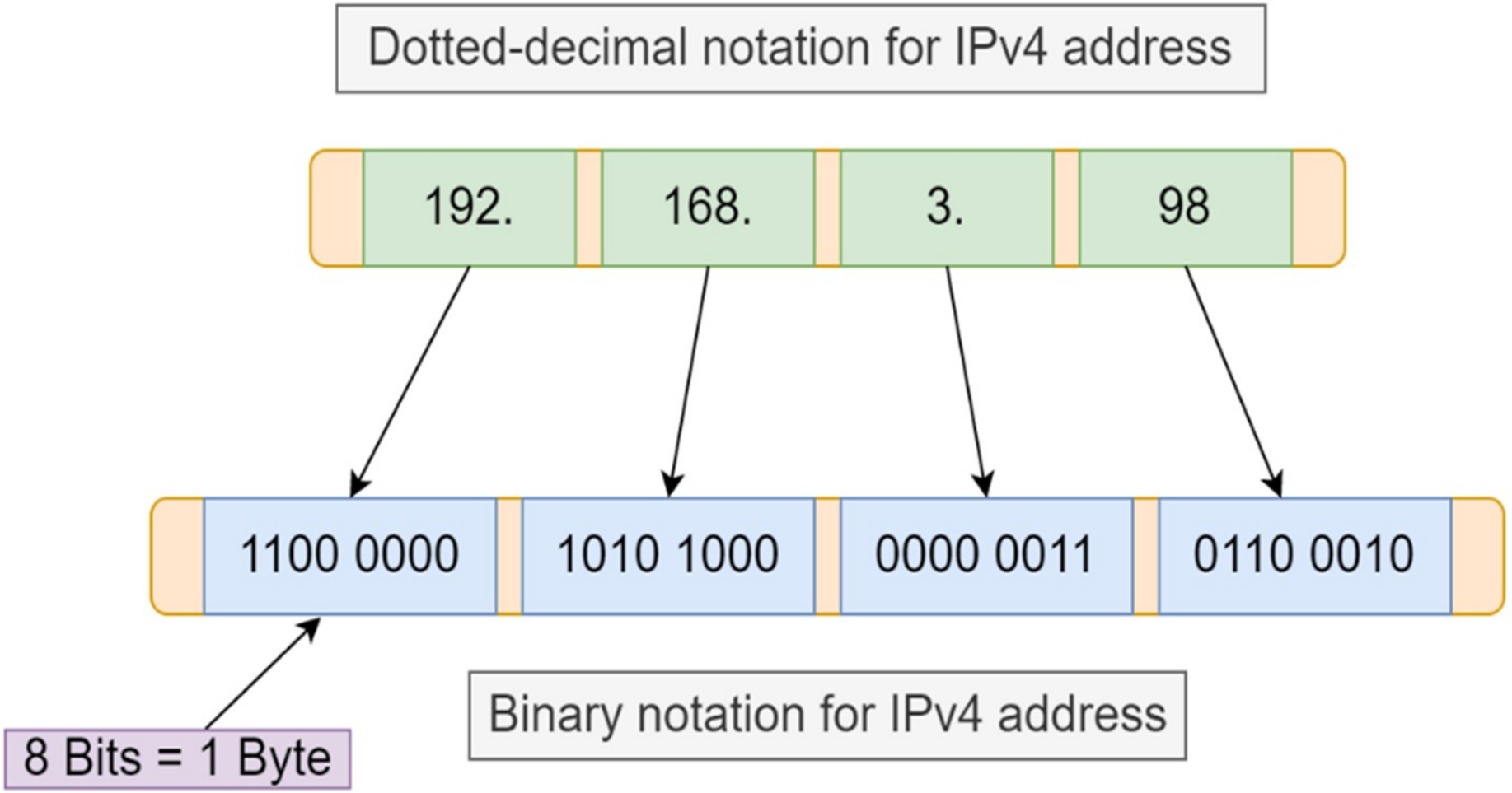
ii. 172.16.0.0 - 172.31.255.255

iii. 192.168.0.0 - 192.168.255.255

IP Address Types/ Categories

- ✓IPV4
- ✓IPV6

- IPv4 has a 32 bit long address and has 4 octets and each octet contains 8 bits.



IP Address Classes

A class - 0 to 126 with default mask of 255.0.0.0

B class - 128 to 191 with default mask of 255.255.0.0

C class - 192 to 223 with default mask of 255.255.255.0

D class - 224 to 247 (Reserved)

E class - 248 to 255 (Reserved)

APIPA(Automatic Private IP Address)is a mechanism by which a system assign the IP address by itself after the DHCP fail to assign the IP address to it. This IP address range is 169.254.0.0-169.254.255.255, with a subnet mask of 255.255.0.0.It easier to configure and support small local area networks (LANs).

NOTE: 127 (It is known as loopback address) is kept for testing internal devices in the motherboard.

Sub-Netting

A **subnet mask** is used in a process known as subnetting, in which a large network is divided into smaller networks. It's like dividing a network into several contiguous network groups, and each group is known as a subnet.

Moreover, this process is implemented to reduce the wastage of IP addresses due to classful addressing.

A **subnet mask** is used to determine the network address and host address:

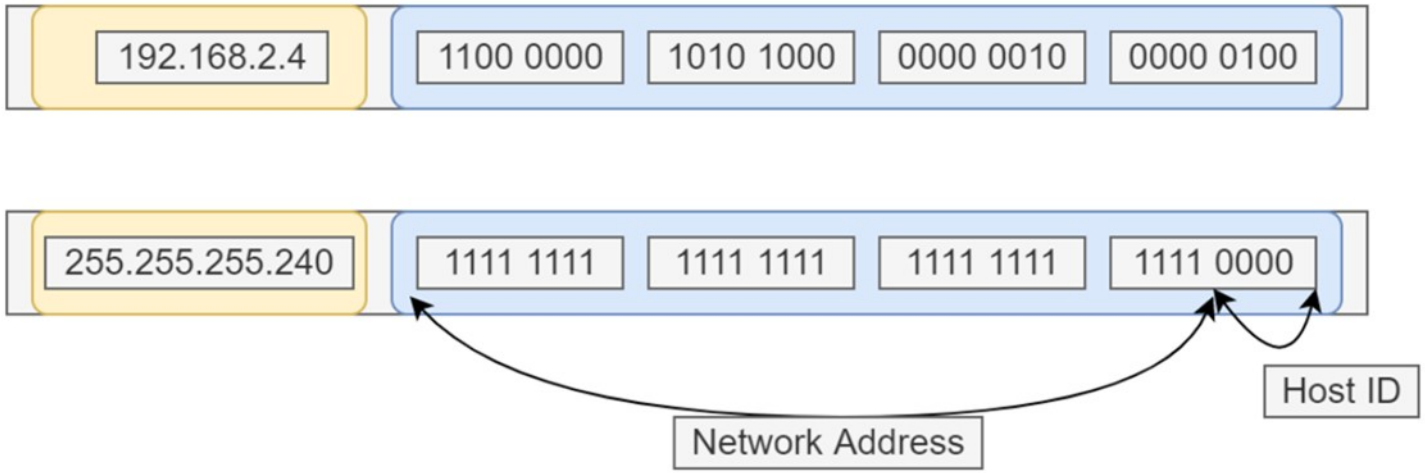
Class	Default Subnet mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Sub-netting is a division of the network in to small parts so as to simplify troubleshooting, make better use of IP address and Security purposes.

Calculating network and broadcast addresses using a subnet mask.

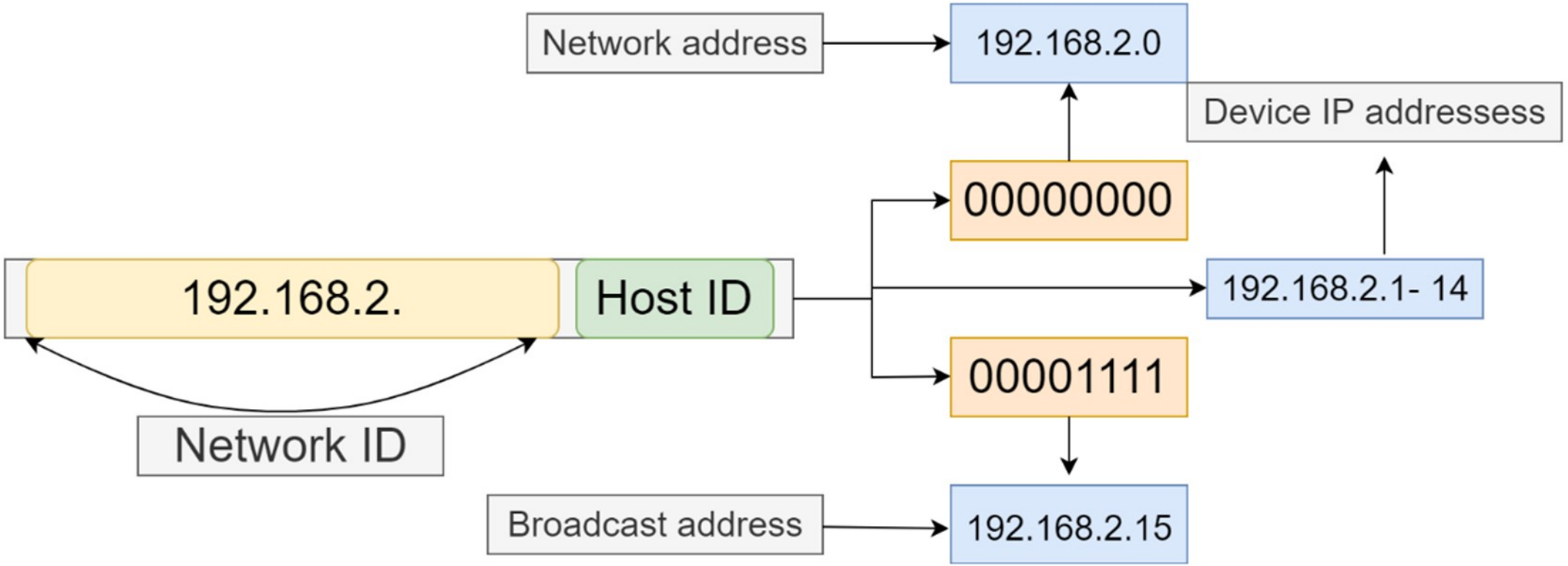
Given: IP address is 192.168.2.4 and the subnet mask is 255.255.255.240.

The first step is to write down the IP address and subnet mask in binary:



Bits in the subnet mask which are 1 denotes the network address. Similarly, the bits which are 0 will be used for the broadcast address.

In this example, we can see that the last 4 bits of the subnet mask are 0. Hence, this means we can connect 14 devices (192.168.2.1 - 192.168.2.14) and the broadcast IP address will be 192.168.2.15. Therefore, the network address will be 192.168.2.0



Hence, we can also rewrite the above IP address: 192.168.2.4/28. Here, 28 refers to the 28 bits of the subnet mask, *which are 1*.

Moreover, the IP address 192.168.2.4 belongs to class C. Hence, we know that in class C, the first 24 bits of the IP address is used for the network address, and the rest is used for the host address. In contrast, *there's a case in subnet mask where network addresses can exceed 24 bits*.

The division of the first 24 bits for network and host addresses is the default configuration for the class C IP address.

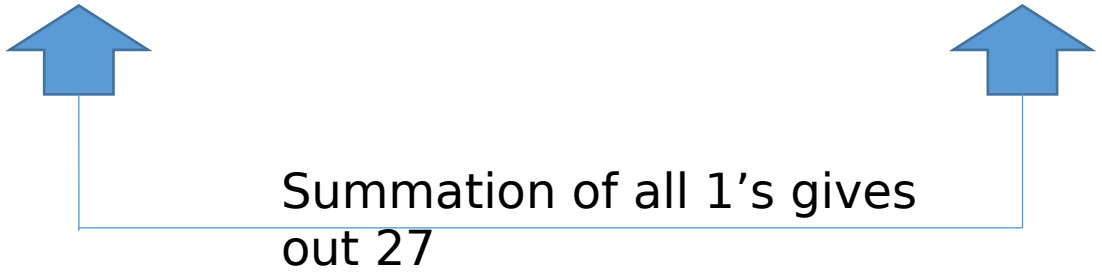
Hence, we can change that by changing the number of 1 in the subnet mask. Moreover, we know that the *default subnet mask for class C is 255.255.255.0*.

Example

We can change some bits of the subnet mask:

IP Address = 192.168.2.4 = 1100 0000. 1010 1000. 0000 0010. 0000 0100

Subnet mask = 255.255.255.224 = 1111 1111. 1111 1111. 1111 1111. 1110 0000



Hence, the IP address with this subnet mask will be in a different network. This is the way we can divide a network using the subnet mask. Therefore, now we can rewrite the IP address as 192.168.2.0/27.

Subnet Mask

In the IPV4 addressing scheme, a 32-bits number is selected for any IP address. The IP address is divided into the following two parts:

- Network Address(network identification, network ID, net Id or netid field)
- Host Address (host identification, host ID, or hostid field)

The network address is common to all hosts within a given network, the network designer assigns a unique network address to a given network, and the hosts are then assigned values for the host part of the IP address.

This setup results in all hosts within the network having a common network address prefix.

The number of bits used in the network address prefix depends on the format of the IP address.

Class A address format, 8 bits are used for the network address, and 24 bits are used for the host address.

Class B address format, 16 bits are used for the network address, and 16 bits are used for the host address.

Class C address format, 24 bits are used for the network address, and 8 bits are used for the host address.

The advantage of using a two-part scheme of network address and host address for IP address has the advantage of minimizing the number of entries in a routers' routing table.

Instead of having routing table entry for each host on a network, you can now summarize all the host in a network by using a single routing table entry.

This routing table entry contains only the network address part, which is the common prefix for all hosts in the network.

A subnet mask is a 32-bit number created by setting host bits to all 0s and setting network bits to all 1s. In this way, the subnet mask separates the IP address *into* the network and host addresses.

The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address.

Neither can be assigned to hosts, as they are reserved for these special purposes.

When organizations need additional subnetworking, subnetting divides the host element of the IP address further into a subnet.

The goal of subnet masks are simply to enable the subnetting process. The phrase “mask” is applied because the subnet mask essentially uses its own 32-bit number to mask the IP address.

IP Address and Subnet Mask

A 32-bit IP address uniquely identifies a single device on an IP network. The 32 binary bits are divided into the host and network sections by the subnet mask but they are also broken into four 8-bit octets.

Because binary is challenging, we convert each octet so they are expressed in dot decimal. This results in the characteristic dotted decimal format for IP addresses for example, 172.16.254.1.

The range of values in decimal is 0 to 255 because that represents 00000000 to 11111111 in binary.

IP Address Classes and Subnet Masks

A **Class A** subnet mask reflects the network portion in the first octet and leaves octets 2, 3, and 4 for the network manager to divide into hosts and subnets as needed.

Class A is for networks with more than 65,536 hosts.

A **Class B** subnet mask claims the first two octets for the network, leaving the remaining part of the address, the 16 bits of octets 3 and 4, for the subnet and host part.

Class B is for networks with 256 to 65,534 hosts.

A **Class C** subnet mask, the network portion is the first three octets with the hosts and subnets in just the remaining 8 bits of octet 4.

Class C is for smaller networks with fewer than 254 hosts.

Class A, B, and C networks have natural masks, or default subnet masks:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

You can determine the number and type of IP addresses any given local network requires based on its default subnet mask.

How Does Subnetting Work?

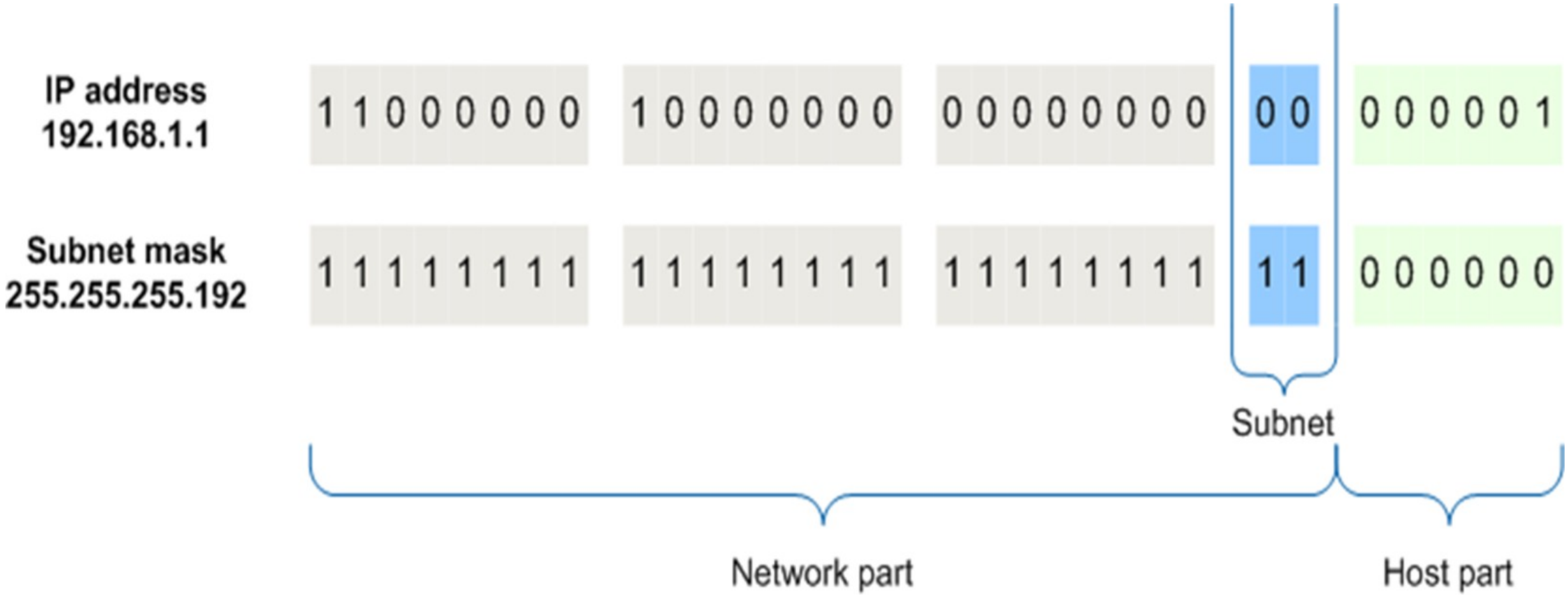
Subnetting is the technique for logically partitioning a single physical network into multiple smaller sub-networks or subnets.

Subnetting enables an organization to conceal network complexity and reduce network traffic by adding subnets without a new network number.

When a single network number must be used across many segments of a local area network (LAN), subnetting is essential.

The benefits of subnetting include:

i. Reducing broadcast volume and thus network traffic
ii. Enabling work from home
iii. Allowing organizations to surpass LAN constraints such as maximum number of hosts


IP address
192.168.1.1
1 1 0 0 0 0 0 0
1 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0
0 0 0 0 0 1
Subnet mask
255.255.255.192
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
1 1
0 0 0 0 0 0
Subnet
Network part
Host part

Formulas used in Different Calculations

Number of Hosts $= 2^n$-2

Where n is number of *remaining bits to make total of 32-bits*

Number of IPs $= 2^n$

Where n is the number of *remaining bits to make total of 32-bits*

Number of Networks $= 2^n$

Where n is number of *borrowed bits after the default of 24-bits for network address of class C.*

NOTE: The number of Hosts are the number of usable IPs. Meaning, after deduction of the network address and broadcast address the remaining will be the usable IPs/ Hosts.

Example

Use the given IP address 192.55.12.120/28 Find the following

i. Subnet mask
ii. Number of IPs
iii. Number of Hosts
iv. Network address
v. Broadcast address
vi. Number of Network(s)

Use the given IP address 192.55.12.6 and the subnet mask 255.255.255.252 Find the following

vii. Number of IPs
viii. Number of Hosts
ix. Network address
x. Broadcast address
xi. Number of Network(s)
xii. Rewrite the IP address

Definition of Terms

Network ID is the First IP address in each Sub-network

Broadcast IP is the Last IP address in each sub-network

First Host IP is the address after the Network ID

Last Host IP is the address before the Broadcast IP

Next Network is the Next ID of the next sub-network

Super-netting

Supernetting is the process of summarizing a bunch of contiguous Subnetted networks back in a single large network. Supernetting is also known as route summarization and route aggregation.

Supernetting is about aggregating networks together to form a larger network (a super network or supernet).

For **subnetting**, we "borrow" bits from the Host ID to create smaller networks. On the other hand, for **supernetting**, we take bits from the Network portion to create bigger networks.

In subnetting, we break a single subnet into many subnets. **In supernetting**, we join multiple subnets into a single subnet.

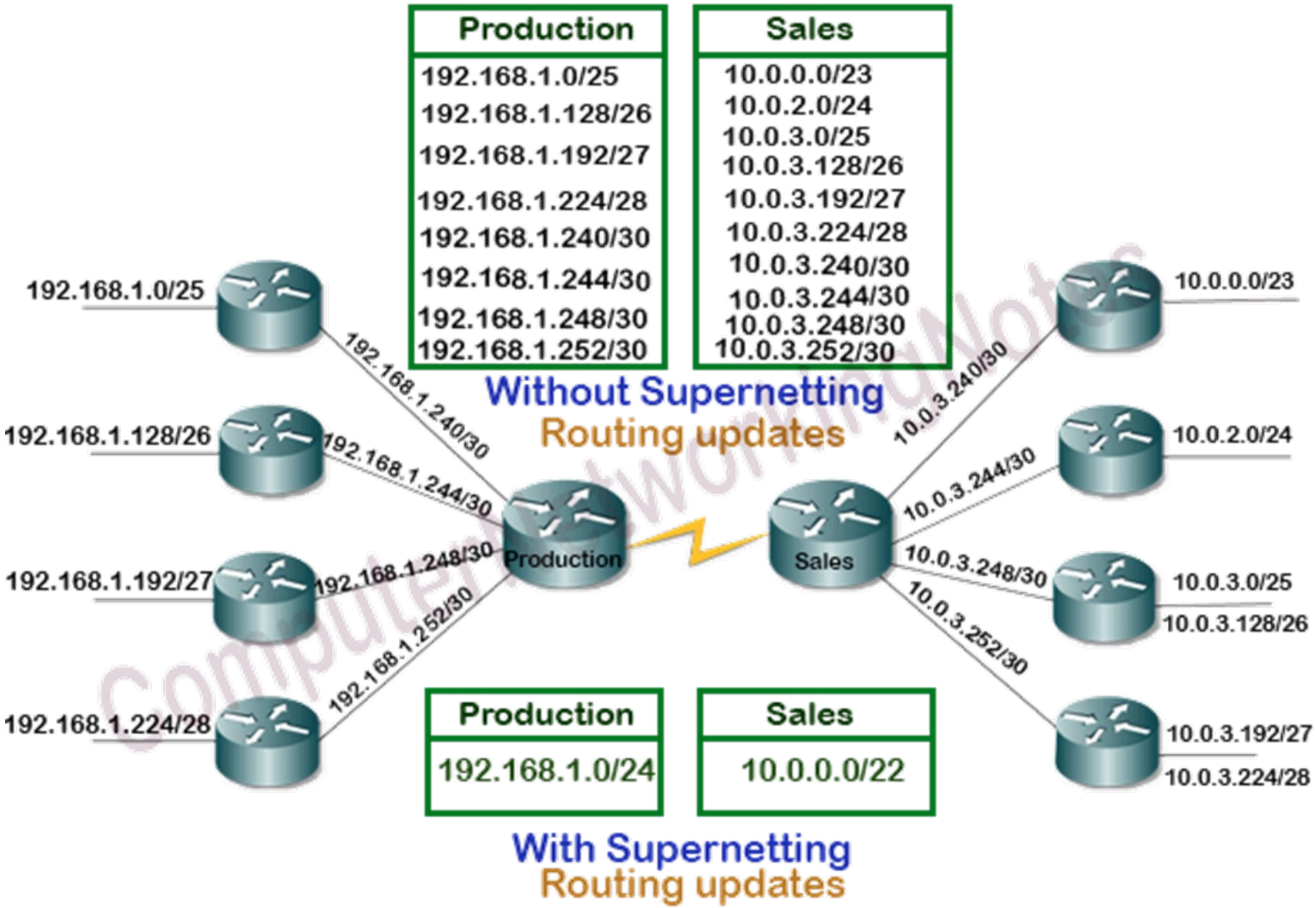
The network address and block size are two main elements of supernetting. We can perform supernetting only on the subnets having the same network address.

1. Network Address

If subnets have different network addresses, we cannot combine them through the supernetting.

When matching network addresses, we need to take care of two things. The *default network address of all subnets must be the same*. The *default network address is the address we get from default network bits*.

Class	Default Network bits	Default host bits	Subnet mask in decimal notation	Subnet mask in slash notation (CIDR)
Class A	8	24	255.0.0.0	/8
Class B	16	16	255.255.0.0	/16
Class C	24	8	255.255.255.0	/24


Production
192.168.1.0/25
192.168.1.128/26
192.168.1.192/27
192.168.1.224/28
192.168.1.240/30
192.168.1.244/30
192.168.1.248/30
192.168.1.252/30
Sales
10.0.0.0/23
10.0.2.0/24
10.0.3.0/25
10.0.3.128/26
10.0.3.192/27
10.0.3.224/28
10.0.3.240/30
10.0.3.244/30
10.0.3.248/30
10.0.3.252/30
Without Supernetting
Routing updates
192.168.1.0/25
192.168.1.128/26
192.168.1.192/27
192.168.1.224/28
192.168.1.240/30
192.168.1.244/30
192.168.1.248/30
192.168.1.252/30
Production
Sales
10.0.3.240/30
10.0.3.244/30
10.0.3.248/30
10.0.3.252/30
10.0.0.0/23
10.0.2.0/24
10.0.3.0/25
10.0.3.128/26
10.0.3.192/27
10.0.3.224/28
Production
192.168.1.0/24
Sales
10.0.0.0/22
With Supernetting
Routing updates

2. Block size

Block size refers to the increment between the starting addresses of consecutive networks in a subnet or supernet.

It can be calculated from the subnet mask as:

Block Size=256−Value of the changing octet in the subnet mask.

It tells you:

- Where a network starts
- Where the next network begins
- The range of IP addresses in a network

Formula to find Block Size

Block Size=256−Subnet Mask Value (in the changing octet)

Step-by-step: How to find block size

Step 1: Convert prefix to subnet mask

Example:/23 → 255.255.254.0

Step 2: Identify the changing octet

The octet not equal to 255 or 0.

Step 3: Apply the formula

256−254=2

Block size = 2

Example 1:

Supernet mask with /22 find the block size and number of usable host

Solution:

/22 → 255.255.252.0

Then 256-252=4

Block size is 4

ii. Number of usable host

First find total number of IP

Total IP number= 2^(32- number of network)

So, 2^32-22= 2^10

So, the total host is 1024 addresses. However, **2 addresses (network and broadcast) are reserved, leaving 1022 usable addresses**

How block size helps find network ranges

Example: 205.16.32.0/21

- Mask = 255.255.248.0
- Block size = **8**
- Network range:

205.16.32.0 → 205.16.39.255

- Next network:

205.16.40.0

Example 2: 192.168.4.5/25

- Mask=255.255.255.128
- Block size :256-128=128
- Network range:

192.168.4.0 →192.168.4.127

Route Summarization Steps

Following points should be important while supernetting;

Step1.

All IP address should be **contiguous**(neighbors).

Step2.

Size of all the small should be **equal**

Step 3.

First IP address should be **exactly divisible** by whole size of supernet**.**

Example:

199.10.5.0/24

199.10.6.0/24

199.10.7.0/24

- All network are continues all having 256 hosts. The range of the first address is 199.10.5.255,so the 2nd condition satisfied.

- All IP address are belongs to Class C, all are equal so 2nd condition is satisfied.
- Whole size of supernet 3*24=72

If last 8 bits of first IP address are zero then IP will be divisible

199.10.5.0

11000111.00001010.00000101.00000000

so 3rd condition is satisfied.

Example;

Networks:

I. 192.168.4.0/24

II. 192.168.5.0/24

III. 192.168.6.0/24

IV. 192.168.7.0/24

- **Step-by-Step Supernetting:**

Now from above example,we know 1st ,2nd & 4th octet are same for above IP address but the 3rd octet different.

Default mask,255,255. ?.0

Binary form of the addresses:

- 192.168.4.0 = 11000000.10101000.00000100.00000000
- 192.168.5.0 = 11000000.10101000.00000101.00000000
- 192.168.6.0 = 11000000.10101000.00000110.00000000
- 192.168.7.0 = 11000000.10101000.00000111.00000000

- **Find common bits:** The first 22 bits (11000000.10101000.000001) are common, so the new subnet mask will be /22.
- **Create the supernet:** The new supernet would be 192.168.4.0/22, which covers IP ranges from 192.168.4.0 to 192.168.7.255
- So supernet mask we will put all one in the common bits (11000000.10101000.000001) and will be (11111111.11111111.111111) thes is equal to 255.255.252.0

Supernet mask is 255.255.252.0

NOTE:

- One of the biggest reasons we use supernetting is to reduce the size of routing tables.

BENEFIT OF SUPERNETTING

1.Improve routing efficiency by increasing the speed at which routing decisions are made

2.Decrease the size and frequency of routing updates

3.Free up memory and reduce processing power needs

4.Reduce network traffic

5.Help manage your network more effectively

6.It allows you to expand how many available addresses are on a single network.

Connection and Connectionless Oriented Services

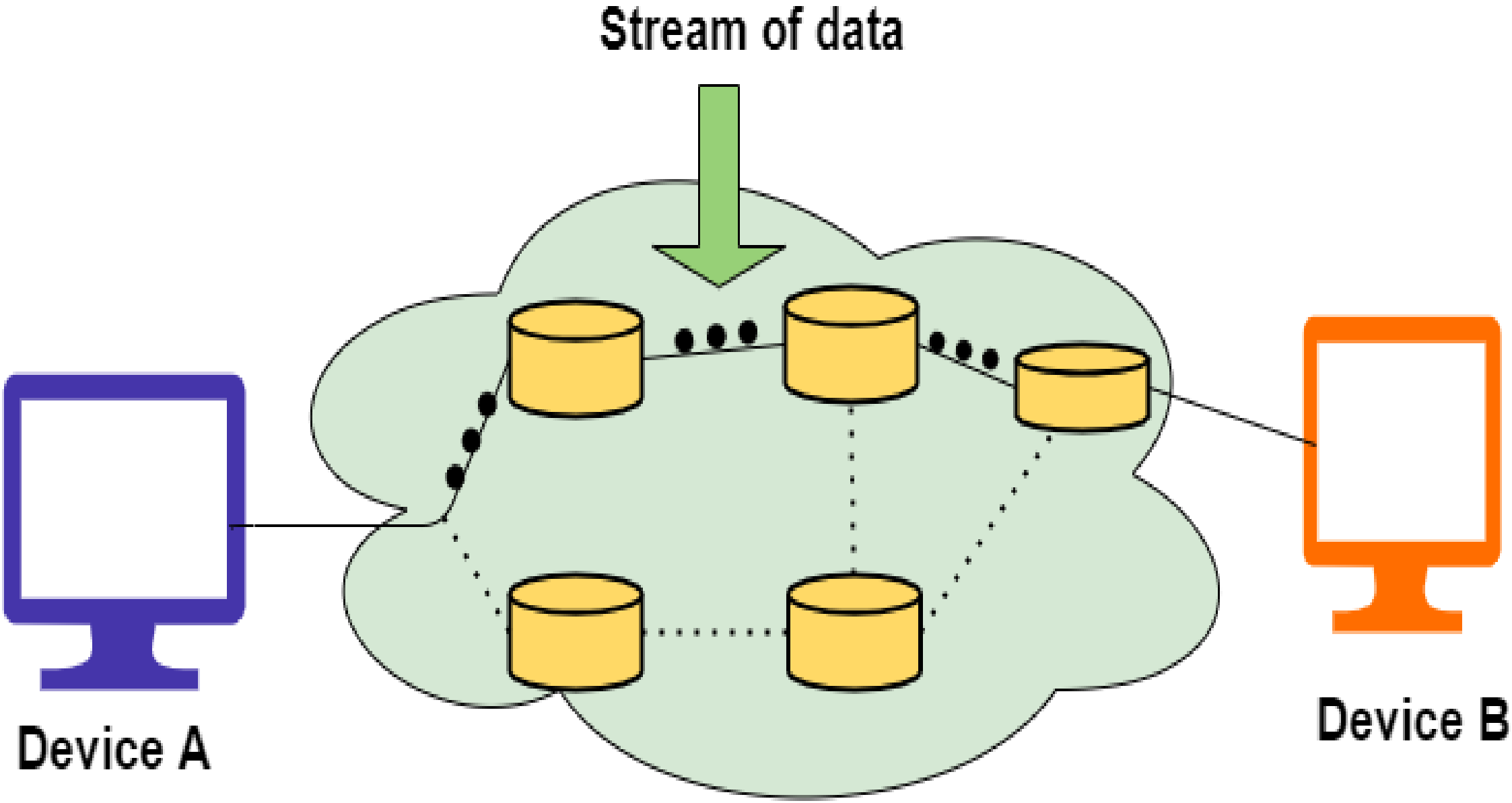
- In order to establish a connection between two or more devices, there are services in Computer Networks. There are two services that are given by the layers to layers above them. These services are as follows:

1.Connection-Oriented Service

2.Connectionless Services

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection.

- Connection-Oriented Service is basically a technique that is typically used to transport an send data at session layer. Whenever a network implements this service, it sends d transfers data or message from sender or source to receiver or destination in correct orde and manner.
- This connection service is generally done in Transport layer and for some technology lik ATM and Frame Relay in datalink layer.


Stream of data
Device A
Device B

- An example of connection-oriented is **TCP (Transmission Control Protocol) protocol**.
- (Transmission Control Protocol) is a connection-oriented protocol that allows two or more computer devices to communicate by creating connections in the same or separate networks.
- It is the most significant protocol for transferring data from one end to the other over the internet protocol.

Connection-Oriented Service

- There is a sequence of operation to be followed by the users of connection oriented service.

These are:

1. Establishing Connection

- It generally requires a session connection to be established just before any data is transported or sent with a direct physical connection among sessions.

2. Transferring Data or Message

- When this session connection is established, then we transfer or send message or data.

3. Releasing the Connection

After sending or transferring data, we release connection.

Example of Connection Oriented Services (Client – Server Model)

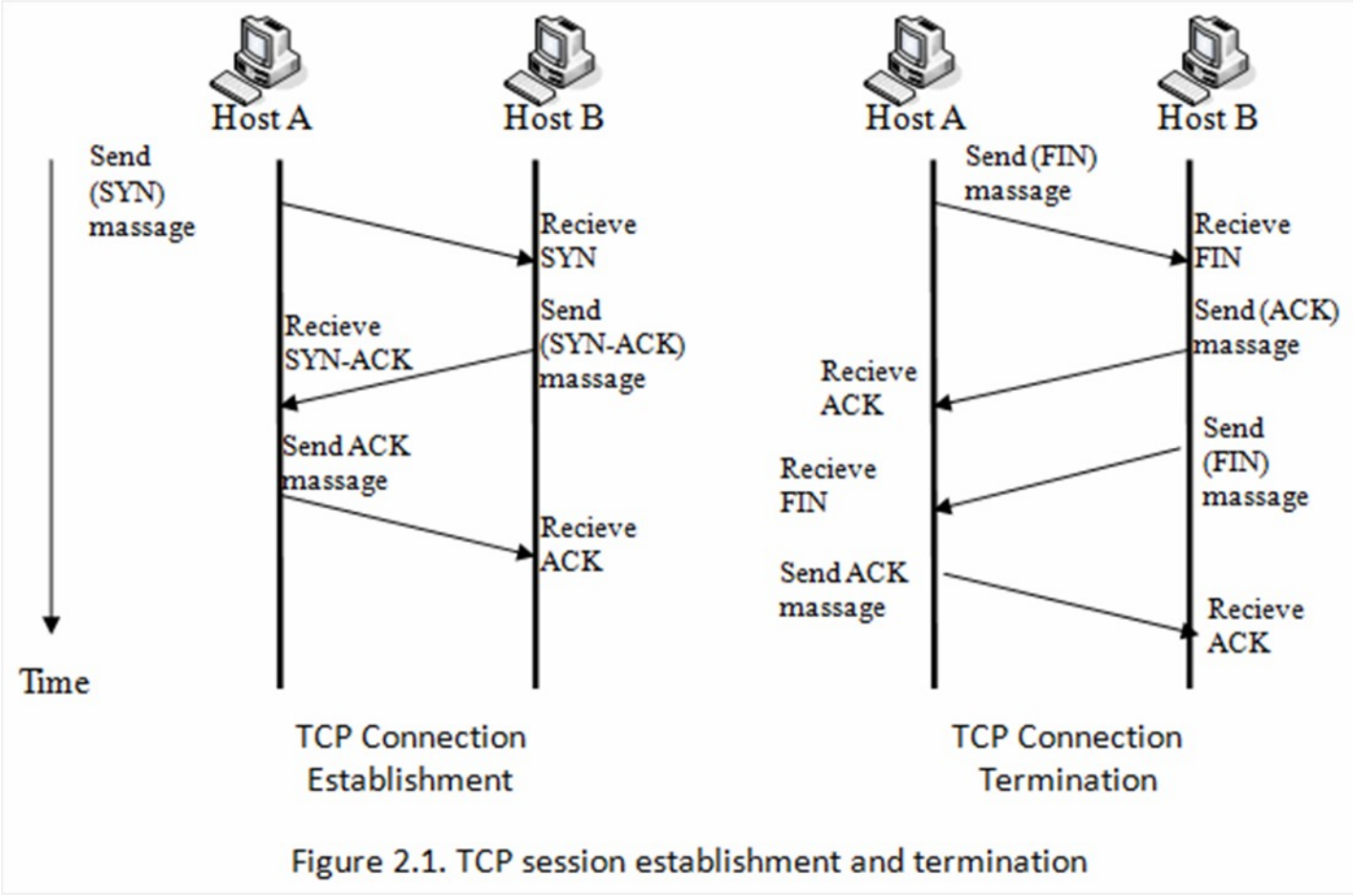


Figure 2.1. TCP session establishment and termination

Advantages

Benefits of Connection-Oriented Services are as follows:

1. Connection-Oriented Services are reliable.
2. There is no duplication of data packets.
3. There are no chances of Congestion
4. These are Suitable for long connections.
5. Sequencing of data packets is guaranteed.

Disadvantages

Drawbacks of Connection-Oriented Service are as follows:

6. This allocation of resources is mandatory before communication.
7. The speed of connection is slower. As much time is taken for establishing and relinquishing the connection.
8. In the case of Network Congestion or router failures, there are no alternative ways to continue with communication.

Connectionless Service

A Connectionless Service is technique that is used in data communications to send or transfer data or message at Layer 4 i.e., Transport Layer of Open System Interconnection model.

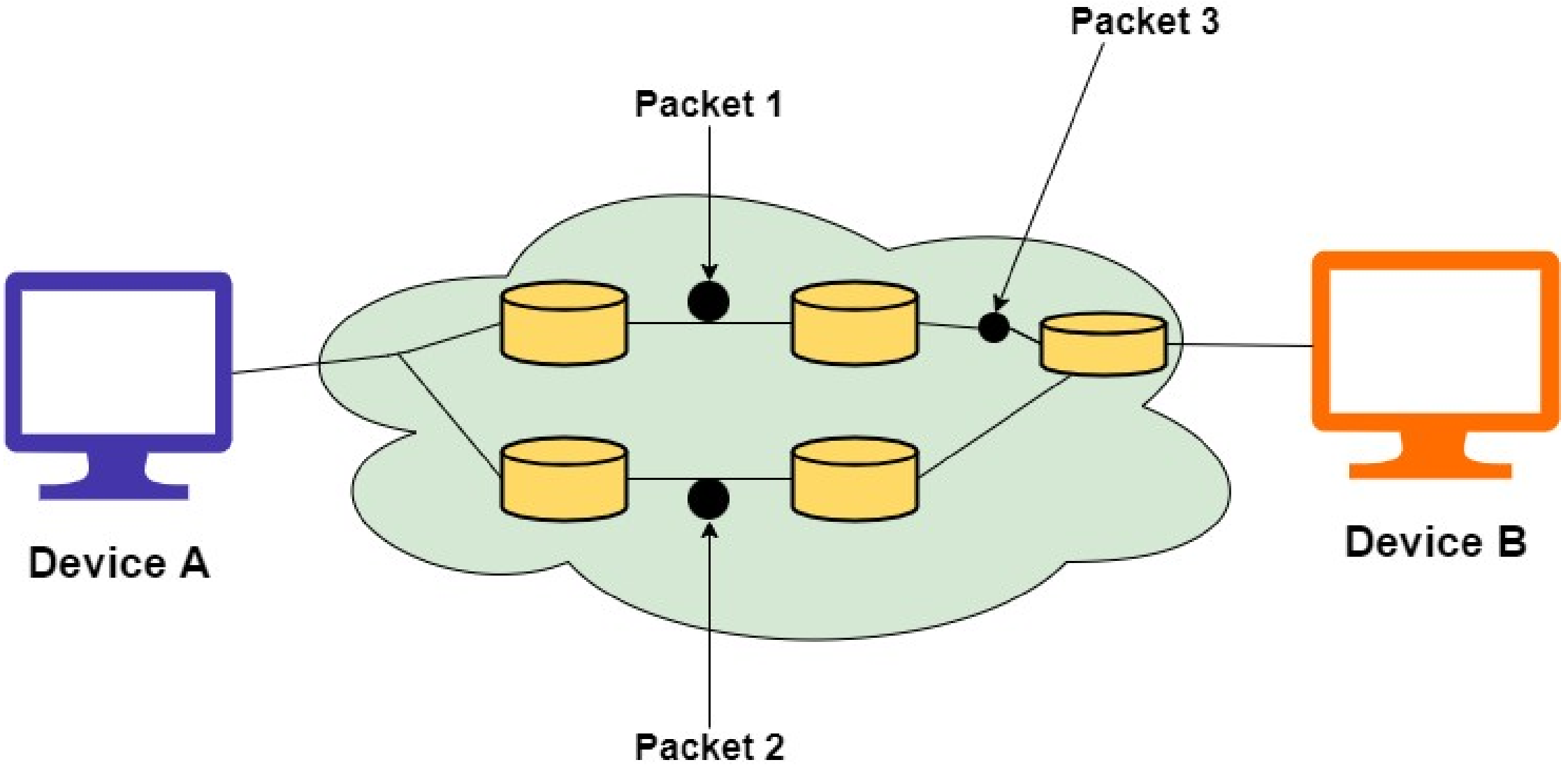
This service does not require session connection among sender or source and receiver or destination. Sender starts transferring or sending data or messages to destination.

In other words, we can say that connectionless service simply means that node can transfer or send data packets or messages to its receiver even without session connection to receiver.

Message is sent or transferred without prior arrangement. This usually works due to error handling protocols that allow and give permission for correction of errors just like requesting retransmission.

Connection Less Services.

- It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of messages sent can be different from the order received.
- In connectionless the data is transferred in one direction from source to destination without checking the destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. An example of a Connectionless service is **UDP (User Datagram Protocol) protocol**.
- The UDP (User Datagram Protocol) is a connectionless protocol that allows two or more devices to communicate without creating a connection
- In this service, network sends each packet of data to sender one at a time, independently of other packets
- It is also similar to that of postal services, as it also carries full address of destination where message is to send
- Data is also sent in one direction from source to destination without checking that destination is still present there or not or if receiver or destination is prepared to accept message


Packet 3
Packet 1
Device A
Device B
Packet 2

Advantages

Benefits of Connection Less Services are as follows:

1. There are usually low overheads.
2. Connection-Oriented services help to broadcast or multicast messages to multiple recipients.
3. In this, there is no circuit setup. Thus it takes a fraction of a minute in order to establish a connection.
4. In the case of Network congestion or router failures, it has an alternative path of data transmission.

Disadvantages

5. These are susceptible to congestion in the network.
6. It is not reliable as there is the possibility of a loss of data packets, wrong delivery of packets or duplication is high.
7. In this, each data packet needs lengthy fields because these are supposed to hold all the destination addresses and the routing information.

Connectionless Protocols :

These protocols simply allow data to be transferred without any link among processes. Some Of data packets may also be lost during transmission.

Some of protocols for connectionless services are given below:

- Internet Protocol (IP)

This protocol is connectionless. In this protocol, all packets in IP network are routed independently. They might not go through same route.

- User Datagram Protocol (UDP)

This protocol does not establish any connection before transferring data. It just sends data that's why UDP is known as connectionless.

- Internet Control Message Protocol (ICMP)

ICMP is called connectionless simply because it does not need any hosts to handshake before establishing any connection.

Internetwork Packet Exchange (IPX)

IPX is called connectionless as it doesn’t need any consistent connection that is required to be maintained while data packets or messages are being transferred from one system to another.

Service	Example
Unreliable Datagram	Electronic Junk Mail, etc.
Acknowledged Datagram	Registered mail, text messages along with delivery report, etc.
Request Reply	Queries from remote databases, etc.

TCP/IP Sockets

A TCP/IP **socket** is used for communications between two computers. The socket includes the Internet protocol (IP) address, as well as the host or port that the computers are using to transmit the data.

All applications that take part in the transmission use the socket to send and receive information.

The purpose of a TCP/IP socket is to identify the computer or network server's unique IP address, along with its port number.

Port numbers are sometimes referred to as hosts, and they tell the receiving computer where to send the requested data.

Together, the IP address and port number make up a socket.

A port address is the number of the port that will be used to send and receive data. Each computer device has several different ports that it uses to send and receive communications.

Since some of those ports may be used by certain devices such as printers, the computer needs to tell other devices where to send information.

In Internet communication, the port may be an Ethernet port assigned to a specific device or the port address of a server that is connected to several individual computers.

A **computer socket**, including a **TCP/IP socket**, is used to facilitate communication between two separate devices. *It provides instructions for where that communication should be sent*.

The IP address and port address contained in the TCP/IP socket tells the receiving computer where to send the requested data.

It also *helps establish some sort of uniform language between the machines*.

When a socket is created, the sender and receiver both test the communication port to ensure that the data is going through.

The sender may send a request that tells the receiver what its identity is. A response is then sent back to the sender confirming the sender's identity, while also communicating the identity of the receiver.

As long as the communications go through and the socket is confirmed to be working, further data requests continue.

Sockets are created each time a communication protocol is established between two or more devices. Once the communication process has ended, the TCP/IP socket is closed.

If for some reason the port requested is not available, the socket will not be created. An error message will usually prompt both the sender and receiver that the socket has failed.

Applications that are used in communications, including web browsers, also use TCP/IP sockets to send and receive data.

During the time that the socket is in use, all communications and applications are bound to the port address that is identified in the socket.

As applications send and receive data, they look for the socket's specific port address or host.

Transport Layer

The **transport Layer** is the second layer in the TCP/IP model and the fourth layer in the OSI model. It is an end-to-end layer used to deliver messages to a host.

It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably.

The unit of data encapsulation in the Transport Layer is a segment.

Working of Transport Layer

The transport layer takes services from the Application layer and provides services to the Network layer.

At the sender's side: The transport layer receives data (message) from the Application layer and then performs Segmentation, divides the actual message into segments, adds the source and destination's port numbers into the header of the segment, and transfers the message to the Network layer.

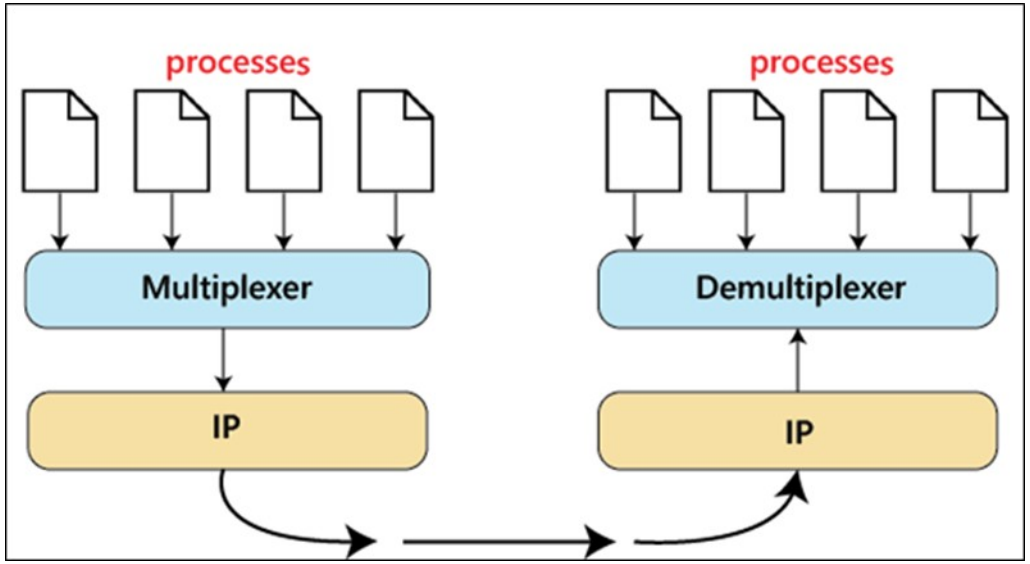
At the receiver's side: The transport layer receives data from the Network layer, reassembles the segmented data, reads its header, identifies the port number, and forwards the message to the appropriate port in the Application layer.

Responsibilities of a Transport Layer

1. The Process to Process Delivery

While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source-destination hosts to correctly deliver a frame and the Network layer requires the IP address for appropriate routing of packets, in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host.

A port number is a 16-bit address used to identify any client-server program uniquely.

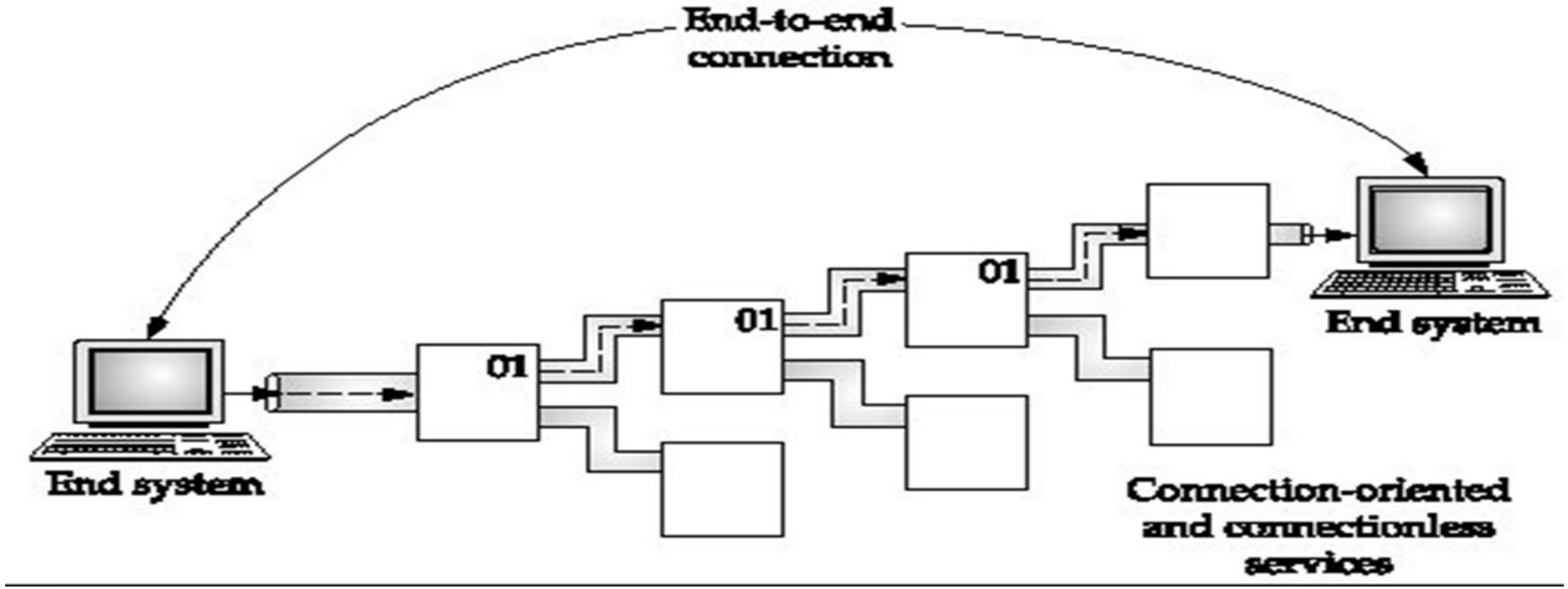


2. End-to-end Connection between Hosts

The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection-orientated protocol that uses a handshake protocol to establish a robust connection between two end hosts.

TCP ensures the reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol that ensures best-effort delivery.

It is suitable for applications that have little concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocols.



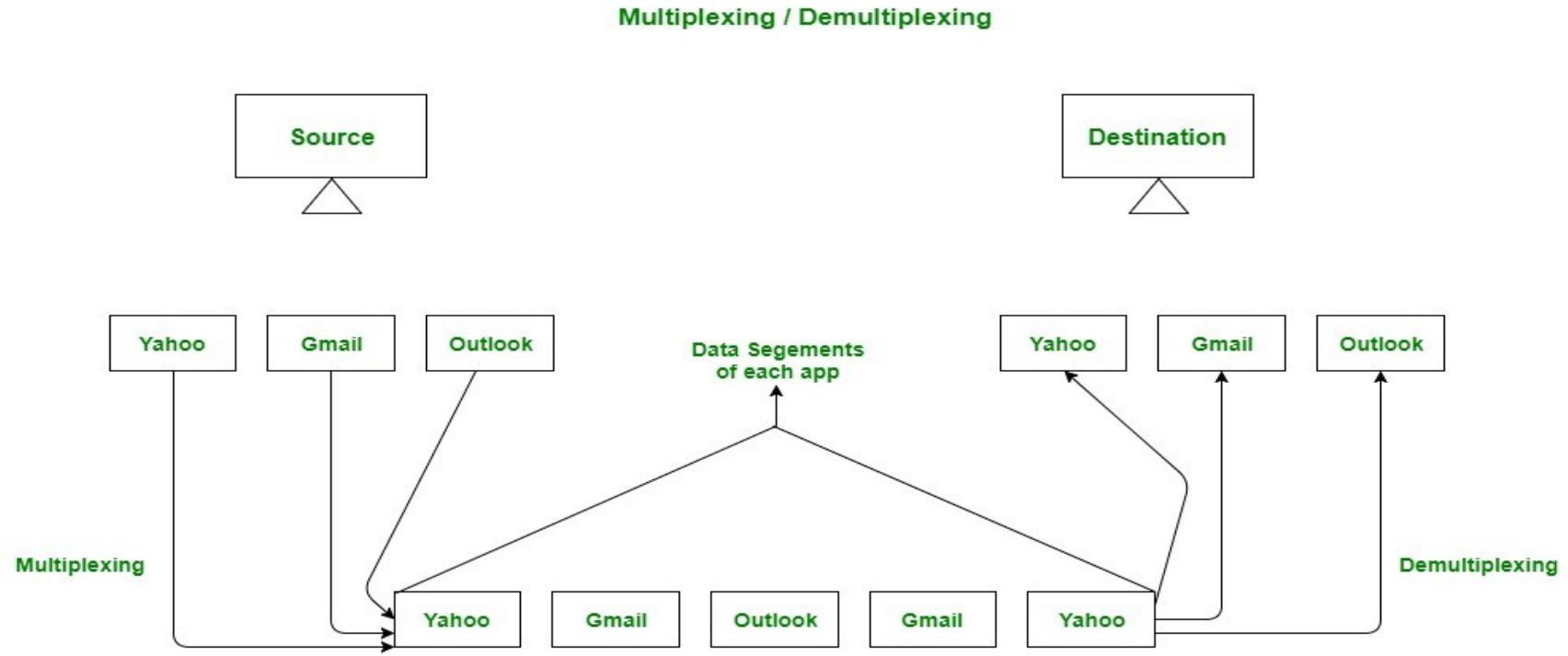
3. Multiplexing and Demultiplexing

Multiplexing(many to one) is when data is acquired from several processes from the sender and merged into one packet along with headers and sent as a single packet.

Multiplexing allows the simultaneous use of different processes over a network that is running on a host. The processes are differentiated by their port numbers.

Similarly, Demultiplexing(one to many is required at the receiver side when the message is distributed into different processes.

Transport receives the segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.



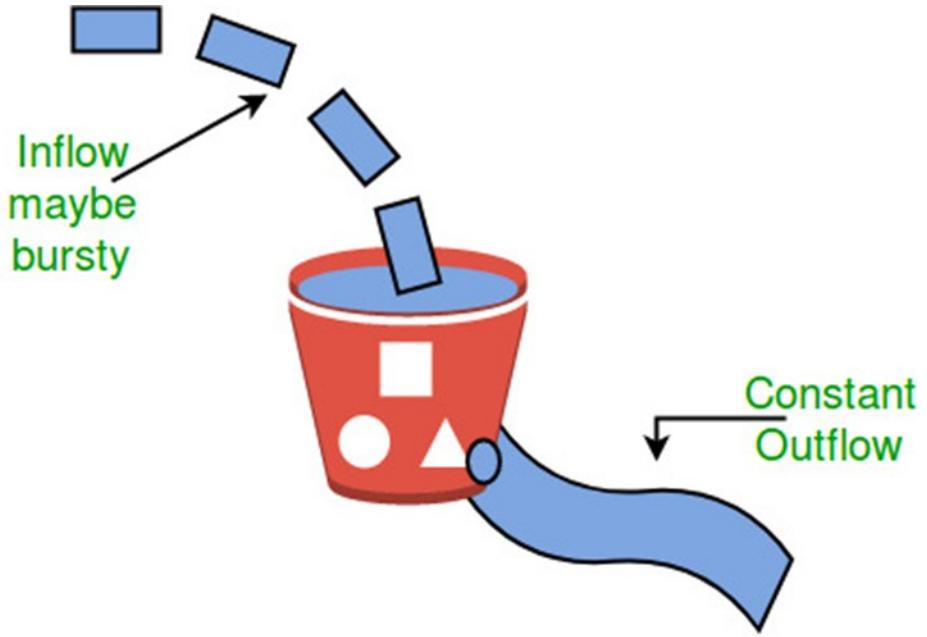
4. Congestion Control

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occurs.

As a result, the retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways.

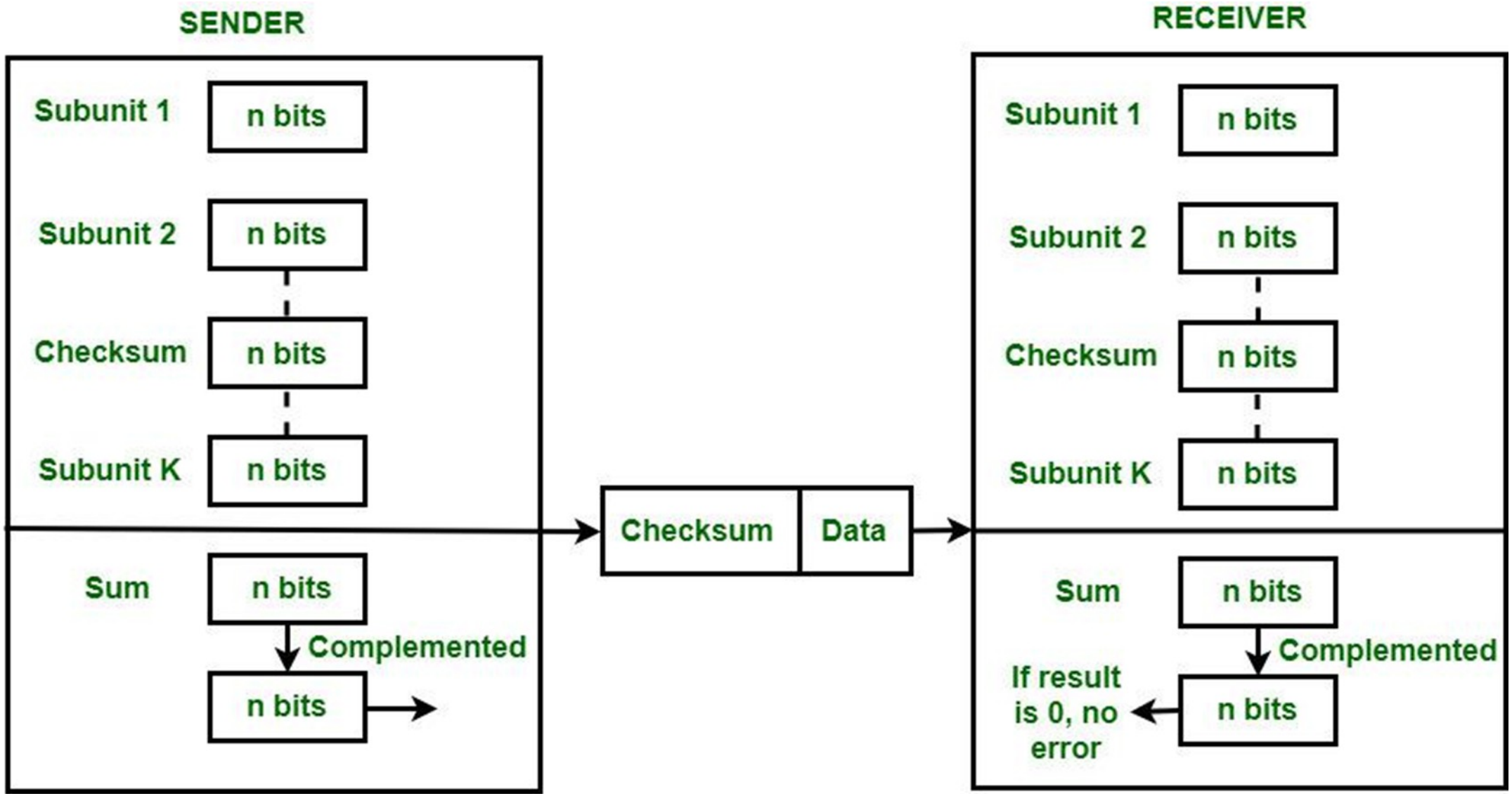
It uses open-loop congestion control to prevent congestion and closed-loop congestion control to remove the congestion in a network once it occurred.

TCP provides AIMD (additive increases multiplicative decrease) and leaky bucket technique for congestion control.



5. Data integrity and Error Correction

The transport layer checks for errors in the messages coming from the application layer by using error detection codes, and computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.


SENDER
Subunit 1
n bits
Subunit 2
n bits
Checksum
n bits
Subunit K
n bits
Sum
n bits
Complemented
n bits
Checksum
Data
RECEIVER
Subunit 1
n bits
Subunit 2
n bits
Checksum
n bits
Subunit K
n bits
Sum
n bits
Complemented
If result is 0, no error
n bits

6. Flow Control

The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model.

TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques.

It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

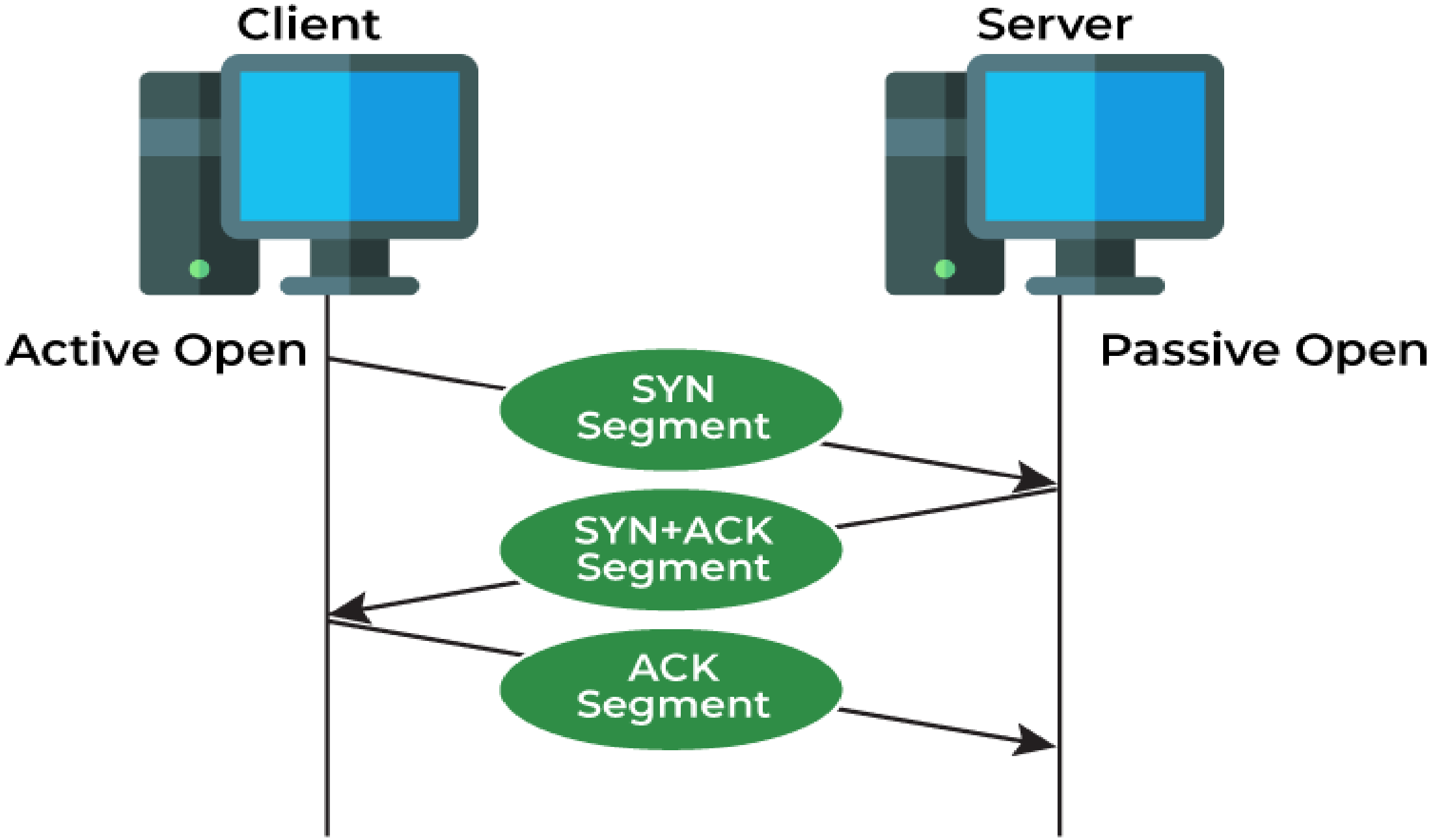
Transport Layer Protocols

The two most important protocols in the Transport Layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

TCP provides reliable data delivery service with end-to-end error detection and correction. UDP provides low-overhead, connectionless datagram delivery service.

What is Transmission Control Protocol (TCP)?

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.


Client
Server
Active Open
Passive Open
SYN
Segment
SYN+ACK
Segment
ACK
Segment

Features of TCP

- TCP keeps track of the segments being transmitted or received by assigning numbers to every single one of them.
- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- TCP implements an error control mechanism for reliable data transfer.
- TCP takes into account the level of congestion in the network.

Applications of TCP

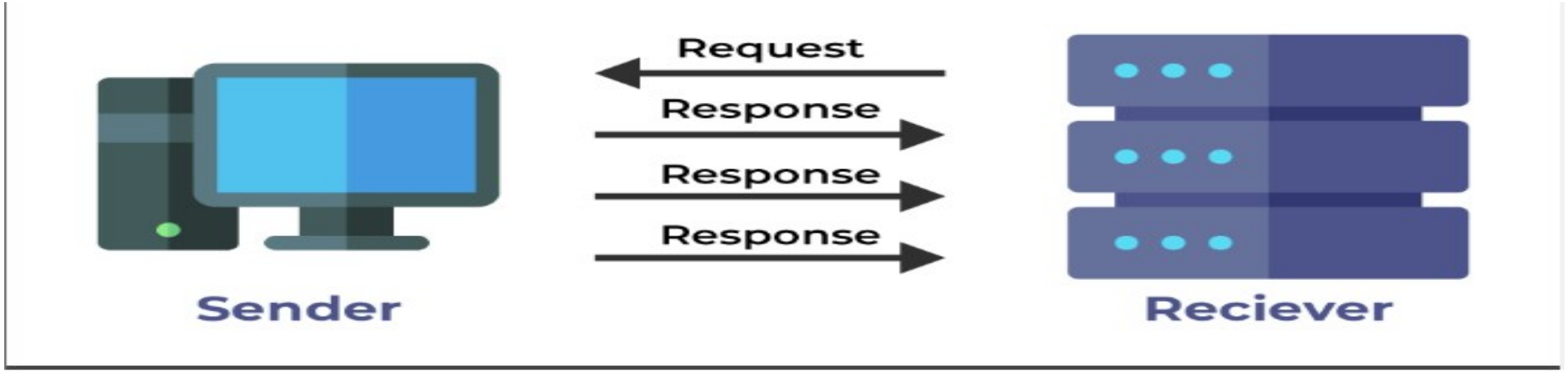
- **World Wide Web (WWW)** : When you browse websites, TCP ensures reliable data transfer between your browser and web servers.
- **Email** : TCP is used for sending and receiving emails. Protocols like **SMTP** (Simple Mail Transfer Protocol) handle email delivery across servers.
- **File Transfer Protocol (FTP)** : FTP relies on TCP to transfer large files securely. Whether you're uploading or downloading files, TCP ensures data integrity.
- **Secure Shell (SSH)** : SSH sessions, commonly used for remote administration, rely on TCP for encrypted communication between client and server.
- **Streaming Media** : Services like Netflix, YouTube, and Spotify use TCP to stream videos and music. It ensures smooth playback by managing data segments and retransmissions.

Advantages of TCP

- It is reliable for maintaining a connection between Sender and Receiver.
- It is responsible for sending data in a particular sequence.
- Its operations are not dependent on Operating System
- It allows and supports many routing protocols.
- It can reduce the speed of data based on the speed of the receiver.
- **Disadvantages of TCP**
- It is slower than UDP and it takes more bandwidth.
- Slower upon starting of transfer of a file.
- Not suitable for LAN and PAN Networks.
- It does not have a multicast or broadcast category.
- It does not load the whole page if a single data of the page is missing.

What is User Datagram Protocol (UDP)?

- User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.



Features of UDP

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching
- UDP is used for some routing update protocols like RIP(Routing Information Protocol)
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.

Application of UDP

- **Real-Time Multimedia Streaming** : UDP is ideal for streaming audio and video content. Its low-latency nature ensures smooth playback, even if occasional data loss occurs.
- **Online Gaming** : Many online games rely on UDP for fast communication between players.
- **DNS (Domain Name System) Queries** : When your device looks up domain names (like converting “www.example.com” to an IP address), UDP handles these requests efficiently ·
- **Network Monitoring** : Tools that monitor network performance often use UDP for lightweight, rapid data exchange.
- **Multicasting** : UDP supports packet switching, making it suitable for multicasting scenarios where data needs to be sent to multiple recipients simultaneously.
- **Routing Update Protocols** : Some routing protocols, like RIP (Routing Information Protocol), utilize UDP for exchanging routing information among routers.

Advantages of UDP

- It does not require any connection for sending or receiving data.
- Broadcast and Multicast are available in UDP.
- UDP can operate on a large range of networks.
- UDP has live and real-time data.
- UDP can deliver data if all the components of the data are not complete.

Disadvantages of UDP

- We can not have any way to acknowledge the successful transfer of data.
- UDP cannot have the mechanism to track the sequence of data.
- UDP is connectionless, and due to this, it is unreliable to transfer data.
- In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.
- UDP can drop packets in case of detection of errors.