CHAPTER 2: NETWORK COMMUNICATION –SECTION (NETWORK CONNECTING DEVICES)

NETWORK CONNECTING DEVICES

Router

Directs data between different networks, for example your home network and the internet.
Assigns IP addresses to devices and manages traffic so data reaches the correct destination.

Difference Between Router And Booster

Router

- ***Purpose**: Creates and manages your network, directing traffic between devices and the internet.*
- ***Function**: Assigns IP addresses, routes data packets to the correct destination, and often includes firewall/security features.*
- ***Connections**: Usually connects directly to your modem (or has a built-in modem) and then to devices via Ethernet or Wi-Fi.*
- ***Range**: Limited to the router's built-in Wi-Fi coverage area.*
- ***Example Use**: Connecting your PC, phone, smart TV, and printer to the internet and to each other.*

Booster (Wi-Fi Booster / Range Extender)

- ***Purpose**: Extends your existing Wi-Fi signal to cover areas with weak or no signal.*
- ***Function**: Receives Wi-Fi from your router and re-broadcasts it, creating a wider coverage area.*
- ***Connections**: Connects wirelessly (or sometimes via Ethernet) to your existing router; does **not** replace the router.*
- ***Range**: Helps eliminate "dead zones" in larger homes or offices.*
- ***Example Use**: Making sure the Wi-Fi from your living room reaches your upstairs bedroom.*

Switch

Connects multiple devices within the same network like PCs, printers, servers.
Uses MAC addresses to send data directly to the intended device instead of broadcasting to all.

Hub

Basic device that connects multiple devices in a network.
Sends incoming data to all connected devices, less secure and less efficient than a switch.

Access Point

Extends a wired network by adding Wi Fi capability.
Allows wireless devices to connect to the network.

Modem

Converts digital data from your network into a signal type usable by your ISP such as cable, DSL, fiber.
Often combined with a router in one device for home use.

Gateway

Acts as a bridge between different types of networks such as a corporate LAN and the internet.
Can perform protocol conversion, security checks, and routing.

Firewall Appliance

Filters network traffic based on security rules.
Can be a standalone device or built into routers.

Gateway Better Explanation

A gateway is like a translator and border guard for networks. It connects two networks that use different protocols, architectures, or data formats, making sure they can communicate.

Key functions

Protocol conversion changes data from one communication protocol to another, for example translating between IPv4 and IPv6, or between HTTP and MQTT in IoT.
Traffic control decides what data can pass between the two networks, often including security checks.
Network integration allows devices in different network environments to work together.

Real world examples

Home internet gateway your ISP modem router combo that connects your home network with private IP addresses to the ISP public internet network.
Enterprise gateway connects a company LAN to the public internet while enforcing security rules.
IoT gateway converts data from sensors using Zigbee, Bluetooth, or LoRaWAN into standard internet protocols so cloud services can understand it.
Email gateway scans, filters, and routes emails between your organization mail system and the internet.

Why it is important

Without a gateway, two networks with different languages or rules could not communicate.

Implementation
Hardware gateways dedicated devices such as VoIP gateways, industrial IoT gateways, and network gateway routers. Software is built in as firmware and you configure it via web interface or command line.

Software gateways programs like Asterisk, Kamailio, FreeSWITCH, Azure IoT Gateway SDK, pfSense or OPNsense that you install on a server or virtual machine.

Built in features home routers with NAT and IPv4 IPv6 translation, smartphone hotspot acting as Wi Fi to cellular gateway, Windows or Linux configured for Internet Connection Sharing or routing.

Rule of thumb

If you buy a dedicated gateway device, the software is built in.
If you use a general purpose computer or server, install gateway software unless the OS already provides the needed feature.

HUB

How it works:

Think of a hub like a loudspeaker in a room.

When one device sends data, the hub copies it to all ports, so every connected device gets it — even if it's meant for only one.

The destination device accepts the data; others just discard it.

Effects:

Slower overall speed – Because all devices share the same bandwidth.

Collisions happen – If two devices send data at the same time, packets collide, and both must resend (CSMA/CD in Ethernet).

No intelligence – The hub doesn't know who is connected where.

SWITCH

How it works:

A switch is more like a post office.

When data (Ethernet frame) arrives, the switch looks at the destination MAC address.

It checks its switching table (also called MAC address table or CAM table) to see which port that MAC is connected to.

Then it sends the data only to that specific port, not to everyone.

Switching Table Explained

What it is:
A list inside the switch mapping each MAC address to the port number where that device was last seen.

Example table inside a switch:

MAC Address	*Port*
00:A1:2B:3C:4D:5E	*1*
14:CF:92:88:3A:1B	*3*
7F:19:45:2B:4E:99	*5*

How it's built:

When a frame enters, the switch reads the source MAC and records which port it came from. Over time, it learns the network layout.

Why it matters for speed:

Since data is sent only where it's needed, bandwidth is not shared between all devices — fewer collisions, faster transfers.

Port & Device Connection Questions

Do we need to connect the same device to the same port every time?

No. If you move a device to another port, the switch will update its switching table automatically after it sees new traffic.

However, if a device is connected to two different ports at once (same MAC on two ports), the switch may get confused or block one link unless special configurations like link aggregation are used.

Can we connect the same device in different ports for faster speed?

Not automatically. To combine ports for higher bandwidth, both the device and switch must support LACP (Link Aggregation Control Protocol) or similar. Otherwise, it can cause network loops, which will flood the network unless Spanning Tree Protocol (STP) is enabled.

NEPALI SECTION

अध्याय २: नेटवर्क सञ्चार – खण्ड (नेटवर्क कनेक्सन गर्ने उपकरणहरू)

नेटवर्क कनेक्सन गर्ने उपकरणहरू

राउटर (Router)
फरक–फरक नेटवर्कहरूबीच डाटा पठाउने र प्राप्त गर्ने काम गर्छ, जस्तै तपाईंको घरको नेटवर्क र इन्टरनेट बीच। उपकरणहरूलाई IP ठेगाना दिन्छ र ट्राफिक व्यवस्थापन गर्छ ताकि डाटा सही गन्तव्यमा पुग्छ।

राउटर र बुस्टरबीचको अन्तर

राउटर (Router)
• उद्देश्य: तपाईंको नेटवर्क बनाउने र व्यवस्थापन गर्ने, उपकरणहरू र इन्टरनेटबीचको ट्राफिकको दिशा दिने।
• कार्य: IP ठेगाना दिने, डाटा प्याकेटहरू सही गन्तव्यमा पठाउने, र धेरैजसो अवस्थामा फायरवाल वा सुरक्षा सुविधा दिने।
• जडान: साधारणतया मोडेमसँग सीधा जडान हुन्छ (वा मोडेम इनबिल्ट हुन्छ) अनि उपकरणहरूलाई इथरनेट वा वाइ-फाइमार्फत जडान गर्छ।
• दायरा: राउटरको आफ्नै वाइ-फाइको दायरासम्म मात्र।
• प्रयोग उदाहरण: तपाईंको कम्प्युटर, फोन, स्मार्ट टिभी र प्रिन्टरलाई इन्टरनेट र एक-अर्कासँग जडान गर्नु।

बुस्टर (Wi-Fi Booster / Range Extender)
• उद्देश्य: भएको वाइ-फाइ सिग्नललाई कमजोर वा नपुग्ने स्थानसम्म पुर्‍याउनु।
• कार्य: राउटरबाट वाइ-फाइ सिग्नल लिन्छ र फेरि प्रसारण गर्छ, जसले कभरेज बढाउँछ।
• जडान: हालको राउटरसँग वाइ-फाइ (वा कहिलेकाहीँ इथरनेट) मार्फत जडान हुन्छ; राउटरलाई बदल्दैन।
• दायरा: ठूलो घर वा अफिसमा "डेड जोन" हटाउन मद्दत गर्छ।
• प्रयोग उदाहरण: बैठक कोठाको वाइ-फाइलाई माथिल्लो तल्लाको कोठासम्म पुर्‍याउनु।

स्विच (Switch)
एउटै नेटवर्कभित्र धेरै उपकरणहरूलाई जडान गर्छ, जस्तै कम्प्युटर, प्रिन्टर, सर्भर।
MAC ठेगानाको आधारमा डाटा लक्षित उपकरणमा मात्र पठाउँछ, सबैमा प्रसारण गर्दैन।

हब (Hub)
मूलभूत उपकरण जसले नेटवर्कका धेरै उपकरणहरूलाई जडान गर्छ।
आएको डाटा सबै पोर्टमा पठाउँछ — स्विचभन्दा कम सुरक्षित र कम प्रभावकारी।

एक्सेस पोइन्ट (Access Point)
वायर्ड नेटवर्कमा वाइ-फाइ सुविधा थप्छ।
वायरलेस उपकरणहरूलाई नेटवर्कमा जडान गर्न अनुमति दिन्छ।

मोडेम (Modem)
नेटवर्कको डिजिटल डाटालाई तपाईंको ISP ले प्रयोग गर्नसक्ने सिग्नलमा रूपान्तरण गर्छ (जस्तै केबल, DSL, फाइबर)।
धेरैजसो अवस्थामा राउटरसँगै एउटै उपकरणमा मिसाइएको हुन्छ।

गेटवे (Gateway)
फरक प्रकारका नेटवर्कबीच पुलको रूपमा काम गर्छ (जस्तै अफिसको LAN र इन्टरनेट बीच)।
प्रोटोकल रूपान्तरण, सुरक्षा जाँच, र राउटिङ गर्न सक्छ।

फायरवाल उपकरण (Firewall Appliance)
सुरक्षा नियमको आधारमा नेटवर्क ट्राफिक फिल्टर गर्छ।
स्वतन्त्र उपकरण वा राउटरभित्र नै हुन सक्छ।

गेटवे (विस्तृत व्याख्या)
गेटवे नेटवर्कहरूको अनुवादक र सीमा सुरक्षा जस्तै हो। यसले फरक प्रोटोकल, संरचना, वा डाटा ढाँचावाला दुई नेटवर्कबीच सञ्चार सम्भव बनाउँछ।

मुख्य कार्यहरू

- **प्रोटोकल रूपान्तरण**: एउटा सञ्चार प्रोटोकलबाट अर्कोमा डाटा रूपान्तरण, जस्तै IPv4 र IPv6 बीच, वा HTTP र MQTT बीच।
- **ट्राफिक नियन्त्रण**: दुई नेटवर्कबीच कुन डाटा जान दिने भन्ने निर्णय र सुरक्षा जाँच।

- **नेटवर्क एकीकरण**: फरक नेटवर्क वातावरणका उपकरणलाई एउटै प्रणाली जस्तो काम गर्न सक्षम बनाउने।

वास्तविक उदाहरणहरू

- **घरको इन्टरनेट गेटवे**: ISP को मोडेम/राउटर संयन्त्र जसले निजी IP भएको LAN लाई सार्वजनिक इन्टरनेटसँग जोड्छ।
- **उद्यम गेटवे**: कम्पनीको LAN लाई इन्टरनेटसँग जोडेर सुरक्षा नियम लागू गर्ने।
- **IoT गेटवे**: Zigbee, Bluetooth, LoRaWAN जस्ता सेन्सर प्रोटोकलको डाटा IP आधारित सेवामा रूपान्तरण गर्ने।
- **इमेल गेटवे**: संस्थाको मेल प्रणाली र इन्टरनेटबीच इमेल स्क्यान, फिल्टर, र रुटिङ गर्ने।

किन आवश्यक छ
गेटवे बिना फरक नियम र भाषावाला नेटवर्कहरू एक-अर्कासँग कुरा गर्न सक्दैनन्।

कार्यान्वयन

- **हार्डवेयर गेटवे**: VoIP गेटवे, औद्योगिक IoT गेटवे, नेटवर्क गेटवे राउटर। फर्मवेयर पहिल्यै हुन्छ र वेब इन्टरफेस वा कमान्ड लाइनबाट कन्फिगर हुन्छ।
- **सफ्टवेयर गेटवे**: Asterisk, Kamailio, FreeSWITCH, Azure IoT Gateway SDK, pfSense, OPNsense जस्ता सफ्टवेयर जसलाई सर्भर वा VM मा इन्स्टल गर्नुपर्छ।
- **इनबिल्ट सुविधा**: घरको राउटरमा NAT, IPv4/IPv6 रूपान्तरण, मोबाइल हटकुनाले Wi-Fi बाट सेल्युलरमा रूपान्तरण, Windows/Linux मा Internet Connection Sharing वा राउटिङ।

साधारण नियम
समर्पित गेटवे उपकरणमा सफ्टवेयर फर्मवेयरमै हुन्छ।
सामान्य कम्प्युटर प्रयोग गर्दा आवश्यक सुविधा नभए सफ्टवेयर इन्स्टल गर्नुपर्छ।

हब (Hub)
कसरी काम गर्छ:
हबलाई ठूलो स्पिकर जस्तो सोच्न सकिन्छ। एउटा उपकरणले डाटा पठाउँदा हबले सबै पोर्टमा पठाउँछ, चाहे त्यो एउटा उपकरणका लागि मात्र किन नहोस्।
गन्तव्य उपकरणले मात्र प्रयोग गर्छ, बाँकीले फाल्छ।

प्रभाव:

- सबैले एउटै ब्यान्डविड्थ प्रयोग गर्ने भएकाले गति कम हुन्छ।
- दुई उपकरणले एउटै समयमा पठाउँदा टक्कर (collision) हुन्छ र पुन: पठाउनुपर्छ।
- कुन उपकरण कहाँ छ थाहा नहुने भएकाले बुद्धिमत्ता हुँदैन।

स्विच (Switch)
कसरी काम गर्छ:
स्विचलाई हुलाकखाना जस्तो सम्झन सकिन्छ। डाटा आएपछि गन्तव्य MAC ठेगाना हेर्छ, Switching Table मा कुन पोर्टमा छ खोज्छ र त्यही पोर्टमा पठाउँछ।

Switching Table के हो:
MAC ठेगाना र त्यसको पोर्ट नम्बरको सूची हो।
उदाहरण:
MAC Address | पोर्ट
00:A1:2B:3C:4D:5E | 1
14:CF:92:88:3A:1B | 3
7F:19:45:2B:4E:99 | 5

बनाउने तरिका:
फ्रेम भित्रिँदा स्रोत MAC र पोर्ट नम्बर टिपिन्छ, र स्विचले बिस्तारै नेटवर्कको लेआउट सिक्छ।

गतिको कारण:
आवश्यक पोर्टमा मात्र पठाउने भएकाले टक्कर कम हुन्छ र गति बढ्छ।

पोर्ट र उपकरण जडान सम्बन्धी प्रश्न

के एउटै उपकरण सधैं एउटै पोर्टमै जडान गर्नुपर्छ?

- होइन। नयाँ पोर्टमा जडान गर्दा केही ट्राफिक देखेपछि स्विचले तालिका अपडेट गर्छ।
  तर एउटै उपकरणलाई दुई पोर्टमा एउटै MAC सहित जडान गर्दा समस्या आउन सक्छ, जबसम्म LACP जस्तो प्रविधि प्रयोग भएको छैन।

के एउटै उपकरणलाई फरक पोर्टमा जडान गरेर गति बढाउन सकिन्छ?

- स्वचालित रूपमा होइन। दुवैपट्टि LACP वा Link Aggregation समर्थन हुनुपर्छ, नत्र नेटवर्क लुप (loop) बन्छ र ट्राफिक बढ्छ।