



SuperNovaSchool®
L E A R N T O B E D I S T I N C T

Computing

Grade 6

(Instructional Resource)

UNIT/STRAND	Networks and data communication
Session	2025-26
Prepared By	Tanawish Ishrat



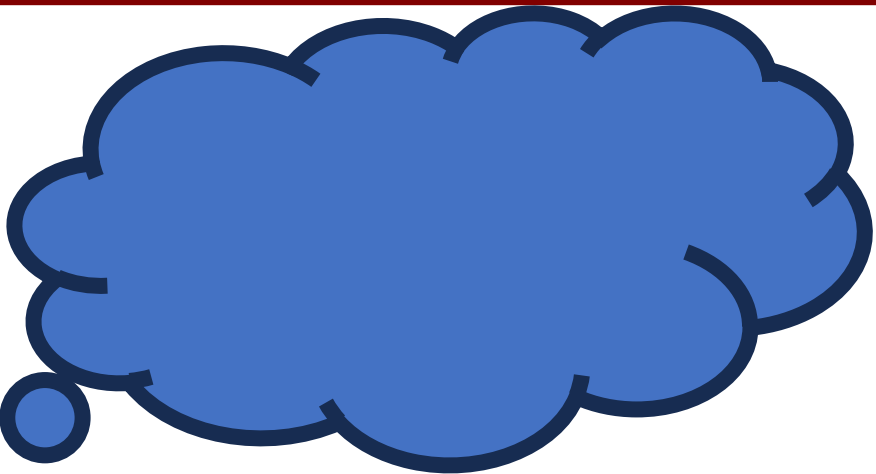
Digital Communication

- **Digital communication is the electronic exchange of information between devices.**
- **Purpose: Allows people to connect, share, and access information quickly.**
- **Examples: Sending an email, video calls, watching a live stream.**





Digital Communication



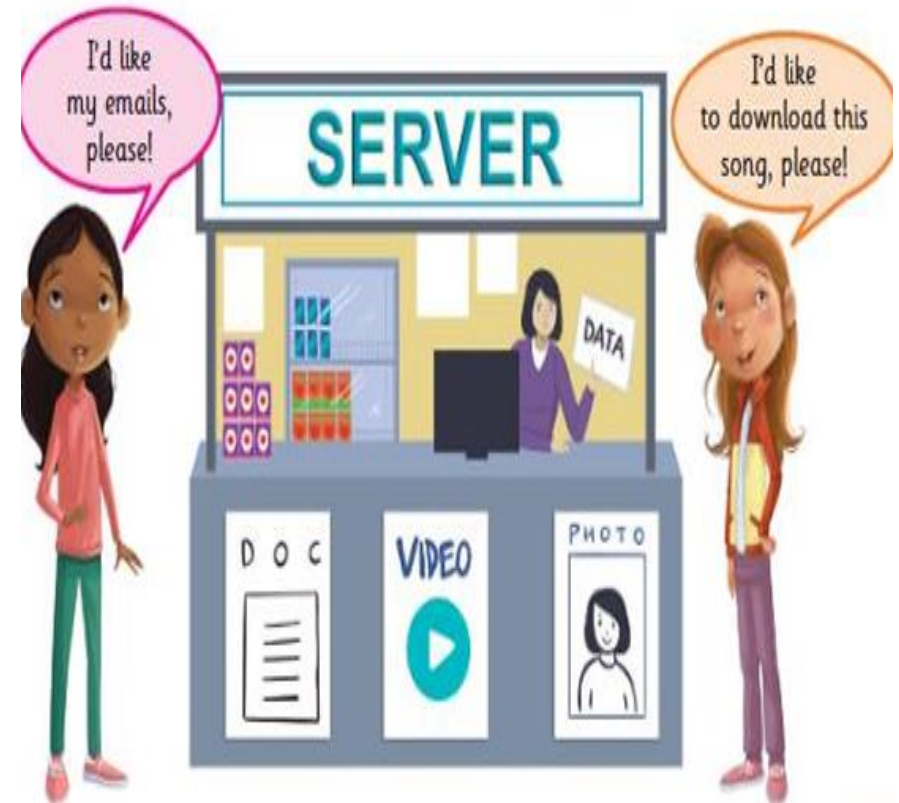
Think – Pair –
Share

Give 5 example of digital communication



Sorting Data on Server

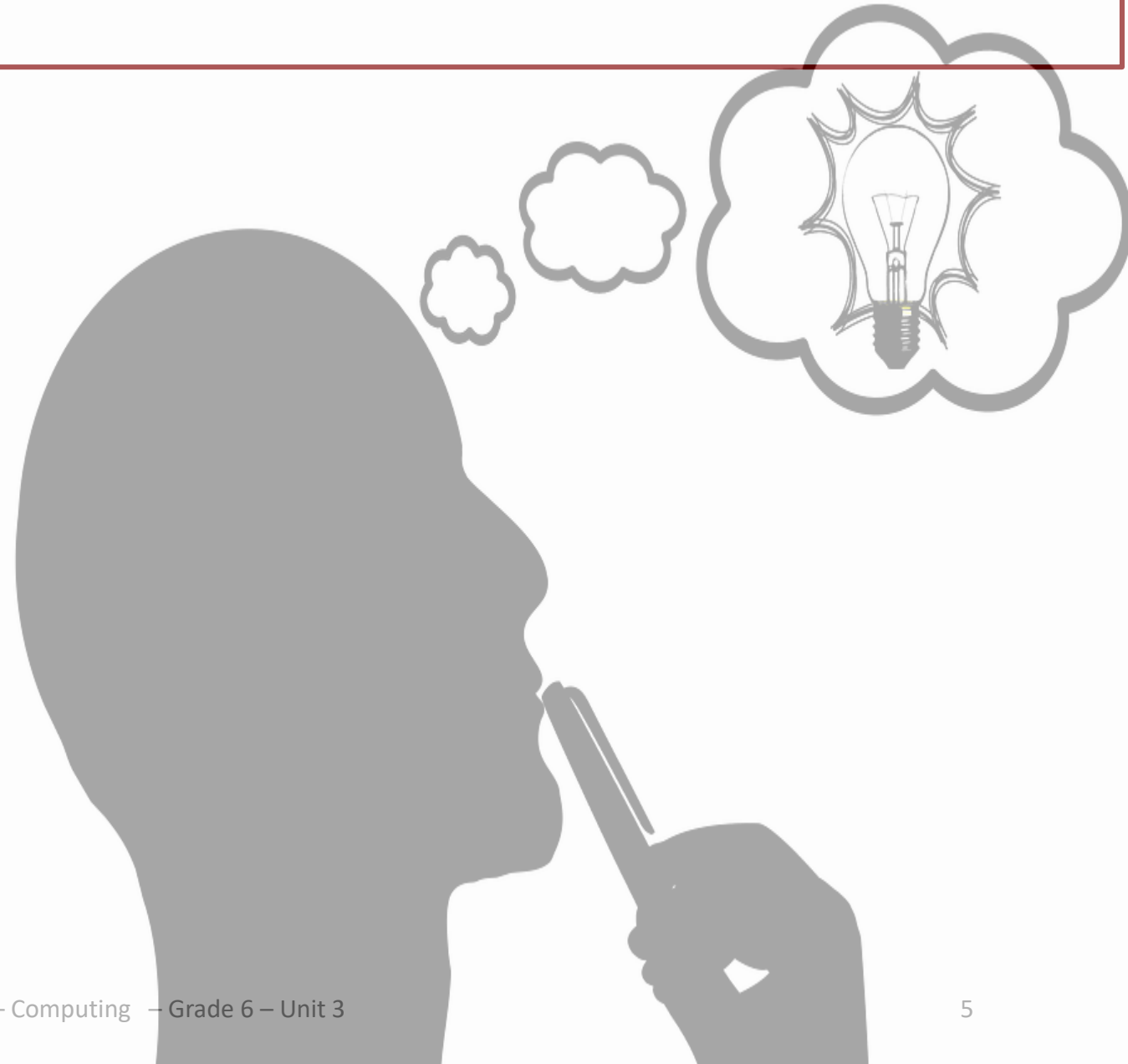
- **Servers** are special computers that store and manage data for users.
- Purpose: Centralized access to files, videos, and services from anywhere.
- Examples: Streaming Services - Netflix, YouTube; Managing Services - Google Drive, Dropbox, Twitch.





Sorting Data on Server

- What is the purpose of a server?
- Name one streaming and one managing service.





Transferring Data – Cellular Network

- A network that uses mobile towers to send data wirelessly.
- Phones use GPS and the internet to help us find our way—like a digital compass that shows us where to go when we're lost!
- Purpose: Allows data transfer while moving (e.g., in a car or outside).
- Examples: Making calls, using mobile data to browse.
- Q. What does a cellular network use to transfer data?



Did you know?

Over 85% of the world's population have a mobile phone.
That's over 7 billion people!



Transferring Data – Wi-Fi

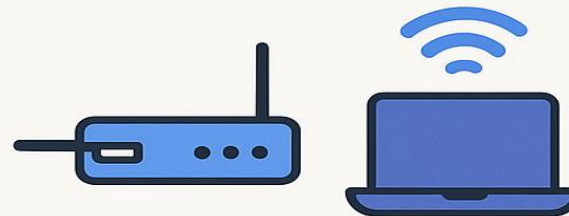
- A wireless network using a router to connect to the internet.
- Purpose: Provides internet access at home, school, and offices.
- Examples: Browsing on a laptop, streaming on a smart TV.
- Let's have a look at the image for more clarification.



- Wi-Fi uses radio waves to connect devices to the internet without wires.



Most homes use a router to connect to the internet.



- Devices can connect to the router using cables or wirelessly.



Packets can be stolen

Packets can be stolen if they are not protected.

Encryption helps keep packets safe by making them hard to read.

- Data is split into small pieces called packets before sent.

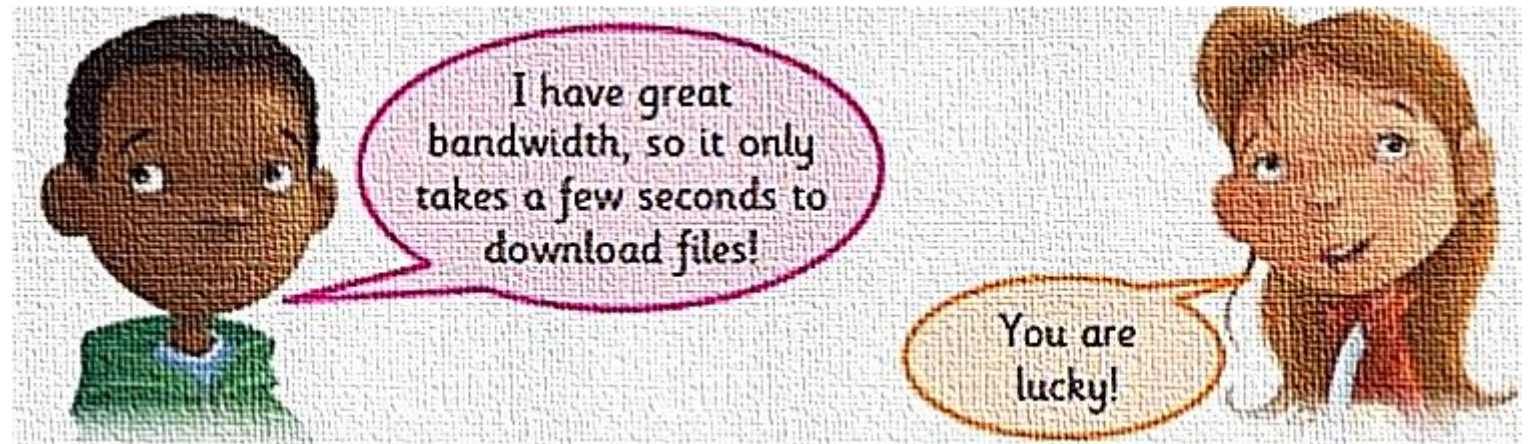


What Is
Full Form Of
WIFI?



Effect of Bandwidth on a Network

- **Definition:** Bandwidth is the maximum amount of data that can be transmitted in a given time.
- **Purpose:** Determines the speed of internet and data transfers.
- **Examples:** High bandwidth = smooth video streaming; Low bandwidth = buffering.





Effects of bandwidth

Bandwidth is a bit like a straw. If you have a narrow straw, you won't be able to drink as quickly as you would with a really wide straw. It would take someone with a wide straw a lot less time to drink the same amount as someone with the thin straw!





Network Overload

- Too many devices using the internet at once can slow everything down.
- This is called *network overload*, and it makes data move very slowly.
- Pictures may not load properly, and apps might show error messages.



Examples of Bandwidth Use



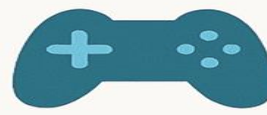
Streaming
a movie
25%



Three smart
bulbs
8%



Smart
fridge
10%



Online
video games
40%

Overload Scenario

All devices together = 103% of the network = Overload!



Solution

If streaming stops, usage drops to 78% = Network works fine!



Can you think any 2 real-life scenarios that can relate with the Network Overload.



Securing Data

- **Definition:** Protecting digital data from unauthorized access or theft.
- **Purpose:** Keeps personal, school, or work data safe.
- **Examples:** Passwords, antivirus software, encryption.

Did you know?

Around 333.2 billion emails are sent each day. This works out at about 47 per person, though some people might send 100, but others might send 0. Over 85% of all sent emails are **spam** (junk mail) or phishing attempts. The more active you are online, the more spam emails you may receive.





Securing Data

- **Fraud** – Tricking people to steal money.
- **Identity Theft** – Pretending to be someone else using their personal information.
- **Phishing** – Fooling someone into giving away personal data like passwords or account details.
- **Account Takeover** – Breaking into someone's account and locking them out.



User Authentication

- **Verifying a user's identity before giving access to data.**
- **Purpose: Protects devices and online accounts.**
- **Examples: Username and Password, Fingerprint scanner, Facial recognition.**





Username & Password

- A username is your unique ID used to log into an account.
- A password keeps your account safe by making sure only you can access it.
- It is a two-factor authentication and also the most common way to secure your data.

Username

Password

☐ Remember Me





Username & Password

- At least 8 characters long
- A mix of uppercase and lowercase letters
- Includes numbers and symbols (like !, #, @)
- Not easy to guess (avoid names, birthdates, or “123456”)
- Use a different password for each account



Fingerprint Authentication

Scan your finger: Your phone or device has a fingerprint sensor that scans the unique patterns on your finger.

- **Match with stored data:** The sensor compares your fingerprint with the one saved on your device to see if they match.

- **Unlock access:** If they match, the device unlocks, allowing you to use it.

Did you know?

Our fingerprints are made up of three different types of pattern: loops, whirls and arches. These patterns are what make each fingerprint unique. Even identical twins have different fingerprints. However, there are some rare genetic conditions which cause people to have no fingerprints.



How fingerprint authentication Works



Fingerprints are a good way of authentication because every person has a unique set of fingerprints. This means that no two people have the same fingerprint. It is very difficult to hack this type of authentication.



Facial Recognition

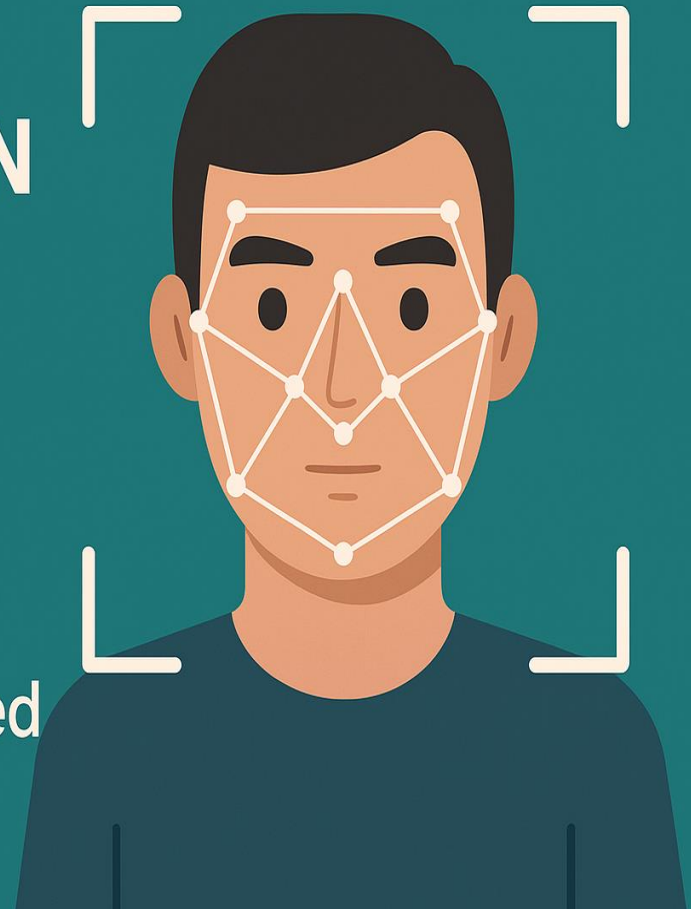
Why it's Secure ?

Unique to you: Your face is unique, so it's hard for others to trick the system.

• **Hands-free:** No need for passwords or fingerprints—just look at your device.

FACIAL RECOGNITION

- Camera scans your face
- Facial features are analyzed
- Match with stored data





Final Recap

- Digital communication helps us share and access information.
- Servers store data for streaming and managing.
- Data is transferred using cellular networks or Wi-Fi.
- Bandwidth affects network speed.
- Data must be secured.
- Authentication helps protect our accounts.
- Username & password, fingerprint , facial recognition are the most famous ways of authentication these days.





Let's Discuss!

- Which method of authentication do you think is most secure? Why?
- What could happen if we didn't protect our data?
- What safety precautions can you take to keep your data secure?

