Living in the IT Era

MST 101d Lecture Notes

Rey Joseph Nieto

Three-Chapter Edition: 25 August 2026

Preface

These lecture notes accompany *Living in the IT Era*, taught to undergraduate biology students at Bulacan State University's San Rafael Campus. I am not trying to turn you into computer scientists or make you memorise catalogues of devices, inventors, and fashionable technologies. I want these notes to help you understand the digital systems that shape ordinary life, use those systems effectively, evaluate information critically, protect yourself and others, and recognise when specialist technical knowledge is needed.

The full course is organised into ten chapters. This edition contains the Introduction and Chapters 1–3. Each chapter is built around a central question and a practical task. Examples are drawn whenever possible from biology, health, research, and Philippine digital life.

The scope follows the general-education framework for *Living in the IT Era* in CHED Memorandum Order No. 20, series of 2013 [1]. The order places the course within the Mathematics, Science, and Technology elective domain and emphasises the science, culture, and ethics of information technology; its influence on modern life and relationships; and its use for personal, professional, and social advancement.

Reports of errors and suggestions are welcome at

`rj (at) rjnieto (dot) com`

I expect these notes to change as you use them. They inevitably reflect what I know, what I can readily bring to mind, and what I expect a class will need. You may identify a point that needs a better explanation, ask for a practical topic that I had not considered, or show that an apparently minor issue deserves more attention. I welcome those requests when they would make the course more useful.

That flexibility is deliberate. I want the module to respond both to the digital problems you face now and to those you are likely to meet later. I hope you finish the course better prepared to understand new technologies, make sensible decisions about them, and meet the IT challenges ahead.

MIT License for These Lecture Notes

Contents

Introduction

Most of you already use information technology throughout the day. A phone serves as an alarm, camera, map, notebook, bank, library, entertainment centre, and means of communication. University work may involve search engines, learning platforms, shared documents, spreadsheets, online forms, biological databases, and AI assistants. Familiarity, however, is not the same as understanding. A person can use a system every day without knowing what it does with their information, why it sometimes fails, or what risks accompany its convenience.

I do not expect you to become computer technicians. I want you to know enough to make better decisions: choosing a device or internet service, improving a home network, recognising a scam, protecting an identity, behaving responsibly and civilly online, understanding online tracking, using digital tools in scientific work, and judging claims about AI and other emerging technologies.

The organising idea is information. The usual definition of information technology can sound unnecessarily dry, but the central idea is simple: there is information, and IT is concerned with handling that information electronically. For this course, we shall define information technology as the organised use of computers, networks, and software to create, process, store, communicate, and use electronic data. This working definition is adapted from the University of Cincinnati's overview of the field [2].

I use the term broadly here. IT includes the hardware on which data are handled, the software that gives instructions to that hardware, and the networks that allow devices to exchange data. It also includes data management, cybersecurity, cloud computing, and newer applications such as artificial intelligence and machine learning [2]. These areas overlap. An online laboratory record, for example, may involve a phone or computer, a browser, a wireless network, a remote database, account permissions, and automated analysis.

IT matters because it changes what people can do with information. It can make communication faster, automate repetitive work, organise large collections of records, support decisions, and protect information from unauthorised access. In biology, these functions appear in field observations, laboratory instruments, sequence databases, statistical analysis, medical records, and collaboration between researchers. None of these systems removes the need for human judgement.

A computer can process a large data set quickly without knowing whether the measurements were sound or whether the conclusion is justified.

Data are recorded representations such as numbers, text, images, audio, and measurements. They become informative when they are interpreted in context. For example, 37.8 is only a recorded number until we learn that it is a patient's temperature in degrees Celsius. Context allows the value to answer a question or support a decision.

Most digital activities can be understood through five actions. A system receives **input**, performs some form of **processing**, may retain data in **storage**, produces **output**, and often **communicates** with another device. These actions need not occur in one machine. A student may enter information on a phone while the processing and storage take place in a distant data centre.

The Course at a Glance

The course follows a route rather than a catalogue. Chapter 1 gives us a working map of devices, connections, and software. Chapter 2 goes beneath the screen to the physical and industrial systems on which that map depends. Chapters 3–4 then show how infrastructure becomes communication and useful digital work. Chapters 5–8 follow information into platforms, human conduct, security threats, and safeguards. The final two chapters use the whole map to examine artificial intelligence and other emerging technologies.

Table 1: The ten-chapter course map.

Chapter	Question	How the course develops
1	**How IT Works and Why It Matters** What parts make up an IT system, and how should we choose among devices, connections, and software?	Establishes our working map: information flow, computer components, specification sheets, internet services, and the purposes, costs, licences, privacy, and security of software.
2	**The Physical Foundations of Computing** What material and industrial systems make digital activity possible, and how do chokepoints create power?	Goes beneath the map: electrical states, transistors, chips, infrastructure, energy, workers, and supply chains. It then uses Chinese and US leverage to ask what technological interdependence means for the Philippines.
3	**The Internet, Web, and Home Networks** How does information travel between devices and services?	Takes up the connection distinctions in Chapter 1 and the physical route introduced in Chapter 2. We distinguish the internet from the Web, follow a website request, interpret common browser messages, and diagnose provider, home-network, Wi-Fi, mesh, and VPN problems.

Continued on the next page

Chapter	Question	How the course develops
4	**Software, Cloud Services, and Digital Work** How do software and remote services turn infrastructure into useful work?	Returns to the software choices introduced in Chapter 1, now in the setting of connected systems: operating systems, applications, files, cloud storage, collaboration, reproducibility, copyright, and the control exchanged for convenience.
5	**Platforms, Algorithms, and the Information Environment** How do platforms decide what reaches us and what they learn about us?	Follows information into cookies, digital footprints, tracking, advertising, search, and recommendation systems. We then examine sources, synthetic media, and AI-generated clutter.
6	**Social Media, Attention, and Relationships** How do digital platforms shape attention, conduct, and relationships?	Moves from what platforms select to what repeated use can do: persuasive design, notifications, social comparison, disinhibition, harassment, and civility online.
7	**Cybersecurity, Identity, and Cybercrime** How are connected people and systems deceived, exploited, or attacked?	Draws together the vulnerabilities created across devices, networks, software, and platforms. We examine phishing, malicious links and downloads, scams, malware, identity theft, social engineering, and Philippine cybercrime law.
8	**Authentication, Biometrics, Privacy, and Regulation** How do we protect identity and data, and what do data collectors owe us?	Answers the threats in Chapter 7 with passwords, multi-factor authentication, one-time passwords, passwordless methods, and biometrics, then turns to privacy, responsible data collection, and the Philippine Data Privacy Act.
9	**Artificial Intelligence: How It Works and Fails** How do AI systems learn, produce outputs, and go wrong?	Uses the earlier chapters on hardware, data, networks, software, and platforms to explain machine learning and generative AI, including training, prediction, hallucination, cascading errors, bias, uncertainty, and sycophancy.
10	**Responsible AI and the Future of Computing** How should we use powerful and emerging systems without surrendering human judgement?	Brings the course together through verification, privacy, copyright, academic integrity, human oversight, and applications in biology and medicine. Quantum computing and post-quantum security show how a new technology can alter several earlier layers at once.

You are not expected to become a specialist in every field listed here. You should learn enough to ask better questions, recognise when a claim requires checking, and know when expert help is needed.

How Classes Will Work. I will not simply repeat these notes in class. Read the assigned pages before coming; I will announce them in advance. We shall use a **flipped classroom** approach: you first encounter the material through the assigned reading, and then we use class time for a bird's-eye view, questions, discussion, examples, and practical applications. The reading is part of the course, not optional preparation for it.

Chapter 1

How IT Works and Why It Matters

Learning Outcomes

By the end of this chapter, you should be able to:

1. identify the basic components of a computer and explain their roles;
2. interpret selected laptop and mobile-phone specifications without assuming that larger numbers are always better;
3. distinguish common internet connection types and interpret download rate, upload rate, latency, jitter, and packet loss;
4. classify software by purpose, delivery, payment, and licence model; and
5. select hardware, an internet service, or software using criteria suited to the user's needs rather than marketing claims alone.

Do not try to memorise every entry in the tables. I want you to learn how to read them when you actually need to compare a device, connection, or application. We will examine a few examples closely in class; you can apply the same questions to the devices and services you encounter.

1.1 A Basic Map of a Computer

A computer is a collection of components with different jobs. We begin with a basic table because you need to recognise each component's role, not memorise model numbers or become a repair technician.

Component	**Main role**	**Plain-language description**
Keyboard, mouse, camera, and microphone	Input	Allow a user or the environment to supply data to the computer.
CPU	General processing	Executes instructions and coordinates much of the computer's work. The CPU is a chip inside the computer, not the entire case.
GPU	Highly parallel processing	Produces graphics and performs many similar calculations at once; this is also useful in scientific computing and AI.
RAM	Working memory	Holds data and instructions that are being used. Its contents are normally lost when power is removed.
SSD (solid-state drive) or hard disk	Long-term storage	Retains the operating system, programs, documents, and other data when the computer is switched off.
Monitor and speakers	Output	Present visual or audio results to the user.
Ethernet and USB ports	Wired connection	Connect the computer to a network, storage device, peripheral, or other equipment.
Wi-Fi and Bluetooth	Wireless connection	Exchange data with networks or nearby devices without a cable.

The components work together. Pressing a key creates input; software assigns meaning to it; the CPU processes the instruction using data held in RAM; the result may appear on the monitor, be saved to storage, or be transmitted over a network. A more powerful component is useful only when the rest of the system and the intended task can take advantage of it.

1.2 Reading Hardware Specifications

I chose two expensive flagship devices because their specification sheets contain many of the terms that buyers encounter. I am not suggesting that you buy either of them. The same method applies to a modest laptop or phone: begin with the work it must do, then ask which figures matter for that work and which are mainly selling points.

1.2.1 Reading a Laptop Specification Sheet

A laptop specification sheet compresses a great deal of information into a small space. Before interpreting the terms, let us organise one actual example. Table 1.1 summarises specifications reported by EveryMac and Apple for a 2026 16-inch MacBook Pro [3, 4].

Table 1.1: Selected laptop specifications reported by EveryMac and Apple.

Specification	**Reported value**
Model and identifiers	Apple MacBook Pro, 16-inch, M5 Max (2026); model number A3429; model identifier Mac17,6
Processor (CPU)	Apple M5 Max with 18 CPU cores; EveryMac-reported Geekbench 6 averages of 4,307 for single-core and 28,978 for multi-core performance
Graphics (GPU) and AI hardware	Integrated 40-core Apple GPU and 16-core Neural Engine
Memory (RAM)	48 GB unified memory as standard; configurable to 64 GB or 128 GB when purchased; built into the machine and not later upgradeable
Storage	2 TB built-in SSD as standard; 4 TB or 8 TB available when purchased; not later upgradeable
Built-in display	16.2-inch Liquid Retina XDR display; 3456 by 2234 pixels; 254 pixels per inch; adaptive refresh rate up to 120 Hz
Camera and audio	12-megapixel Centre Stage camera with 1080p video and a six-speaker sound system
Wireless connections	Wi-Fi 7 and Bluetooth 6
Physical connections	Three Thunderbolt 5 ports using USB-C connectors, HDMI, an SDXC card slot, a 3.5 mm headphone socket, and MagSafe 3 charging; no built-in Ethernet port
External displays	Support for as many as four external displays, subject to limits on their resolution and refresh rate
Battery and charging	100 Wh battery; claimed maximum of 16 hours of wireless web use or 22 hours of video streaming; 140 W power adaptor
Operating system	macOS 26.3.1 originally installed; EveryMac lists no native Windows support and points instead to virtualisation
Dimensions and mass	0.66 by 14.01 by 9.77 inches; 4.7 lb (2.15 kg)

The model name tells us which machine is being described, but identifiers such as A3429 and Mac17,6 are often more reliable when checking compatibility, replacement parts, or support. Two laptops sold under similar names may belong to different generations. The date and exact identifier therefore matter.

Processor, graphics, and memory. A CPU's core count and clock speed do not by themselves establish that it is faster than another CPU. The processor generation, design, cooling, and task also matter. A **benchmark** is a standardised performance test. Its results can help, but only when the same benchmark and version are used under comparable conditions. A single-core score reflects work that depends mainly on one core; a multi-core score reflects work that can be divided among several cores. GPU core counts are likewise poor for comparisons across different designs or manufacturers. They become meaningful only with suitable tests of the work one actually intends to perform. The Neural Engine is Apple's name for hardware designed to perform certain machine-learning calculations.

RAM is the computer's short-term working space. More RAM allows more programs and larger data sets to remain readily available, but unused capacity does not make every task faster. In this machine the CPU and GPU share unified memory. The important purchasing detail is that the memory is built into the machine: its capacity must be chosen at purchase because it cannot be expanded later.

Storage and upgradeability. The 2 TB figure describes how much the built-in SSD can store, not its speed or the amount of RAM. Photographs, videos, large data sets, and applications consume storage over time. This laptop's internal storage cannot be upgraded after purchase, although external drives and network or cloud storage remain possible. A buyer should distinguish among the standard configuration, an option available when ordering, and a component that can be upgraded later; these are not the same thing.

Display and connections. Screen size is measured diagonally. Resolution gives the number of pixels, pixel density describes how closely they are packed, and refresh rate gives the maximum number of times the display can update each second. Higher values can improve particular uses, but they may also increase cost or power consumption. The software being used must be able to benefit from them.

Port descriptions require careful reading. USB-C describes the connector's shape, whereas Thunderbolt 5 describes capabilities such as data transfer, display output, and charging. Devices with the same connector need not support the same functions or speeds. The absence of built-in Ethernet does not prevent a wired network connection, but it requires a compatible adaptor or dock. Likewise, obtaining the benefits of Wi-Fi 7 requires a compatible network, not merely a compatible laptop.

Battery, portability, and software. The words "up to" mark a best-case claim measured under stated test conditions. Screen brightness, wireless activity, software, temperature, and workload can make actual battery life shorter. Mass and dimensions matter when a laptop is carried daily, while the operating system matters because required applications and laboratory equipment may support only particular platforms. A powerful computer that cannot run the required software is the wrong computer for the task.

From specifications to a sensible choice. Begin with the work the computer must perform, the software and connections it requires, the need for portability, and the available budget. Then compare machines using consistent definitions and suitable tests. Specifications cannot fully describe keyboard comfort, fan noise, repairability, reliability, warranty service, or real-world battery life, so independent reviews and first-hand inspection remain useful. The best choice is not necessarily the machine with the largest numbers; it is the one that meets the user's needs at an acceptable total cost.

The source itself also illustrates why specifications should be checked. On its page for this 40-core model, EveryMac gives two different memory-bandwidth figures, 614 GB/s and 460 GB/s. Apple's specification shows that 614 GB/s applies to the 40-core GPU configuration and 460 GB/s to the 32-core GPU configuration [4]. The 460 GB/s entry on EveryMac's 40-core page therefore appears to be an error. A polished table can organise claims, but it does not make them correct.

1.2.2 Reading a Mobile-Phone Specification Sheet

Mobile-phone specification sheets use many of the same terms as laptop sheets, but add cellular networks, SIMs, cameras, positioning, sensors, and resistance to water and dust. Table 1.2 organises selected specifications reported by GSMArena and Apple for the Apple iPhone 17 Pro Max [5–7].

Table 1.2: Selected mobile-phone specifications reported by GSMArena and Apple.

Specification	**Reported value**
Model and release	Apple iPhone 17 Pro Max; announced 9 September 2025 and released 19 September 2025
Regional versions	A3257 (United States and Puerto Rico); A3525 (selected markets including Canada, Japan, Mexico, and several Gulf states); A3527 (China mainland); and A3526 (other countries and regions)
Mobile networks	4G LTE and 5G, with support for older network standards
SIM arrangement	Varies by market: combinations include Nano-SIM and eSIM, eSIM only, or two Nano-SIMs
Processor and graphics	Apple A19 Pro chipset; six-core CPU and six-core Apple GPU
Memory and storage	12 GB RAM; 256 GB, 512 GB, 1 TB, or 2 TB of built-in storage; no memory-card slot
Display	6.9-inch Super Retina XDR OLED; 1320 by 2868 pixels; about 460 pixels per inch; refresh rate up to 120 Hz; Apple advertises up to 3,000 nits of peak outdoor brightness; GSMArena measured 1,000 nits under its test conditions
Rear cameras	Three 48-megapixel cameras: wide, telephoto with four-times optical zoom, and ultrawide; LiDAR depth scanner
Front camera	18-megapixel camera with an additional depth and biometrics sensor
Video	Rear-camera recording up to 4K at 120 frames per second, with available rates and formats depending on the selected mode
Wireless and positioning	Wi-Fi 7, Bluetooth 6.0, NFC, GPS, and other satellite-positioning systems
Physical connection	USB Type-C 3.2 Gen 2 with DisplayPort; no 3.5 mm headphone socket

Continued on the next page

Specification	Reported value
Sensors and authentication	Face ID, accelerometer, gyroscope, proximity sensor, compass, barometer, and second-generation Ultra Wideband support
Battery	4,823 mAh for the Nano-SIM model or 5,088 mAh for the eSIM-only model; GSMArena active-use test result of 17 hours and 58 minutes
Charging	Wired USB Power Delivery; Apple claims up to 50 per cent charge in around 20 minutes with a separately sold 40 W or higher power adaptor; up to 25 W wireless MagSafe or Qi2 charging; 4.5 W reverse wired charging
Construction and resistance	Aluminium unibody; Ceramic Shield glass; IP68 dust and water resistance, with testing to a depth of 6 m for up to 30 minutes
Performance tests	AnTuTu scores of 2,600,583 in version 10 and 2,331,417 in version 11; Geekbench 6 multi-core score of 10,118; 3DMark Wild Life Extreme score of 6,010

Start with the exact version. The product name is not enough. The model number identifies the regional version, which can affect the available SIM arrangement, battery capacity, network compatibility, and warranty service. A phone imported from another market may therefore differ from the version sold locally even when both carry the same product name. Before buying, check the exact model against the mobile operator's supported frequency bands and the manufacturer's local support terms. A label such as "5G" does not guarantee 5G service everywhere: the phone, network bands, operator, subscription, and local coverage must all be compatible. A Nano-SIM is a small physical card, whereas an eSIM is a digital SIM profile stored by the phone.

Processor, RAM, and storage. As with laptops, CPU and GPU core counts are meaningful only within the context of a particular design. Tests of real applications are more informative than a core count alone. The table also shows why benchmark versions must not be mixed: the same phone receives different AnTuTu scores under versions 10 and 11. This does not mean that its hardware changed between the two tests.

RAM supports programs while they are running; storage retains applications, photographs, videos, and other files. The storage capacity must be chosen at purchase because this phone has no memory-card slot. Cloud storage can provide additional space and synchronisation, but it may require a subscription and an internet connection and should not be confused with increasing the phone's built-in storage.

Display and cameras. Display size is measured diagonally, while resolution, pixel density, refresh rate, brightness, colour reproduction, and power use describe different properties. The sheet lists both advertised brightness levels and a separately measured result. Such figures should be compared only when the testing conditions and definitions match.

A camera's megapixel count describes the number of recorded pixels, not the overall quality of every photograph. Sensor size, lens, aperture, optical image stabilisation, focusing, image processing, lighting, and the photographer all matter. Multiple rear cameras provide different fields of view or optical capabilities; three 48-megapixel cameras should not be read as a single 144-megapixel camera. Optical zoom uses the camera's optics, whereas digital zoom enlarges or crops the recorded image and may lose detail.

Battery, charging, and durability. The two battery capacities in the table refer to different regional versions, not contradictory measurements of one battery. Capacity in milliampere-hours is useful, but it cannot by itself predict running time across phones with different displays, processors, software, and network conditions. A controlled active-use test is generally more informative, although no single test can reproduce every person's use. Fast-charging times are also conditional on a suitable charger, cable, temperature, battery state, and charging protocol.

An IP68 rating indicates performance under specified laboratory conditions; it does not mean that the phone is impossible to damage with liquid. Wear, impact, repairs, depth, time, temperature, pressure, and the type of liquid can affect resistance. Durability, repairability, spare-parts availability, and warranty conditions deserve attention alongside processor and camera figures.

Software, privacy, and cost. An operating-system version on a specification sheet is a snapshot, not a promise of support for a particular number of years. Check the manufacturer's current update policy and whether essential applications will run on the device. Face ID is convenient, but biometric authentication also raises questions about how biometric data are stored and what fallback method is used; these questions return in our study of privacy and cybersecurity.

Price is unusually unstable: it changes with storage, market, taxes, seller, promotions, and time. A sensible comparison fixes the required storage and features, checks the exact regional model, and considers the total cost of the phone, accessories, repairs, cloud services, and expected period of use. The best phone is the one that meets those requirements reliably, not simply the one with the longest specification sheet.

For your work in biology, a phone may also be a field notebook, camera, location recorder, timer, reference tool, or means of entering observations. Suitability for scientific work depends not only on the hardware but also on measurement accuracy, consistent methods, file formats, data export, privacy, and whether the work can be checked or repeated.

1.3 Internet Connection Types

A useful device still needs a suitable connection. The internet reaches homes and other premises through several technologies. The connection type affects the speeds that are possible, the consistency of those speeds, latency, reliability, installation, and cost. It also determines which services can feasibly be offered at a particular address. The table below draws on the overview by David Anders and Sean Jackson but omits its provider-specific and United States market information [8].

Connection	**How data reach the premises**	**Main characteristics**
Fibre-optic	Pulses of light travel through thin strands of glass or plastic.	Can provide very high and often similar download and upload speeds. Building the required network is costly, so service is not available everywhere.
Cable	Electrical signals travel through coaxial cable of the kind also used for cable television.	Can provide high download speeds, but upload speeds are often lower. Capacity may be shared locally, so performance can fall during busy periods.
DSL	Electrical signals travel through copper telephone lines.	Makes use of existing telephone infrastructure and, unlike dial-up, allows telephone voice service to be used at the same time. Performance depends strongly on line quality and distance from network equipment and is generally more limited than fibre or cable.
Fixed wireless	Radio signals travel between a base station and a receiver at a fixed location.	Can serve places where laying a cable is impractical. Distance, obstructions, alignment, interference, and network demand can affect performance; some systems require a mounted outdoor receiver.
Cellular home internet	A router receives a 4G LTE or 5G mobile-network signal and shares the connection with devices in the premises.	Is often quick to install, but performance varies with coverage, indoor signal strength, network load, and the router's position.
Satellite	A dish or terminal exchanges radio signals with satellites in orbit.	Can reach remote places without nearby terrestrial cables or towers. It requires a suitable view of the sky and may involve costly equipment, data limits, and greater latency. Low-Earth-orbit systems reduce the signal's travel distance compared with geostationary systems.

In the broad technical sense, cellular home internet is also a form of fixed wireless access. The table separates it because consumer plans based on mobile 4G or 5G networks are commonly discussed apart from systems using a dedicated fixed receiver.

Use these descriptions to identify broad families, not to predict a particular level of service. Two connections using the same technology may perform differently because of the local infrastructure, distance, equipment, congestion, maintenance, and plan conditions. Parts of a network may also use different media. For example, fibre may carry data across most of a provider's network while another technology completes the final connection to a building. The exact connection installed at the premises matters more than a vague marketing label.

The internet connection is not the Wi-Fi. The service provider's connection brings internet access to a modem, optical network terminal, fixed receiver, satellite terminal, or cellular router. An optical network terminal is the box at the end of a fibre connection. Wi-Fi is the short-range wireless network that a router normally uses to share the connection within the premises. A weak Wi-Fi signal in one bedroom does not necessarily mean that the internet service entering the home is slow. Conversely, an excellent Wi-Fi signal cannot make a slow external connection faster. Testing a computer over a wired Ethernet connection, where practicable, helps distinguish an internal Wi-Fi problem from a problem with the internet service itself.

What the performance figures mean. Download rate describes how quickly data travel from the internet to the user, as when loading a page or streaming a video. Upload rate describes travel in the other direction, as when sending a file, backing up photographs, joining a video call, or submitting a large data set. A connection is **symmetrical** when its download and upload rates are approximately equal; otherwise it is **asymmetrical**.

Connection rates are normally advertised in megabits per second (Mbps) or gigabits per second (Gbps), while file sizes are commonly stated in megabytes (MB) or gigabytes (GB). Since one byte contains eight bits, a rate of 100 Mbps corresponds to at most

$$\frac{100}{8} = 12.5 \text{ MB/s}$$

before overhead and other real-world limitations are considered. Here, **overhead** means the additional data and work required to manage the transmission itself. Thus, Mbps and MB/s are not interchangeable. The time required to transfer a file can be estimated by dividing its size in bits by the transfer rate in bits per second, provided that the units are first made consistent.

Rate is not the whole story. **Latency** is the time taken for data to travel between points in a network. Speed tests commonly report the round-trip time in milliseconds; a smaller value is generally better for conversation, remote control, and online games. **Jitter** is variation in that delay, while **packet loss** occurs when some transmitted data fail to arrive and may have to be recovered or sent again. A connection with a high advertised rate can still feel poor during a video call if latency, jitter, or packet loss is excessive.

Choosing a connection and plan. Begin with what is actually available at the exact address. Consider how many people and devices will use the connection at once, and distinguish download-heavy activities from tasks that need substantial upload capacity or low latency. Read whether an advertised rate is a maximum or an expected range and whether the service has a data allowance, a fair-use policy, or reduced speeds after a threshold. Account for installation charges, required equipment, contract length, post-promotional price, repair response, and the cost of ending the service.

When you compare internet plans, check these six factors. No single factor decides every case: a household that mainly streams recorded video may value different things from one that regularly joins live classes, makes calls, plays online games, or uploads large files.

Factor	**What to compare**
Total cost and budget	The installation charge, equipment charge, regular price after any promotion, data-related charges, contract terms, and the cost of cancelling must fit the household's realistic budget.
Actual needs and shared use	List the activities that matter, the number of simultaneous users and devices, and any need for reliable access at particular times. Do not pay for a headline feature that the household will not use.
Transfer capacity (download and upload)	Compare both directions of transfer, not download alone. Upload capacity matters for video calls, cloud backup, submitting work, sharing media, and sending data.
Responsiveness (latency)	Lower delay is especially important when people must interact in real time: calls, live classes, remote access, and online games.
Consistency (jitter)	Small variation in delay helps live audio and video remain smooth. A connection can have an acceptable average latency but still perform poorly if the delay changes sharply from moment to moment.
Delivery reliability (packet loss)	Lost packets can cause interruptions, garbled audio, frozen video, retries, and failed transfers. Ask about outages and test for loss at the times the service will actually be used.

When comparing plans in the Philippines, give the provider the exact service address and ask which connection will actually be installed. Availability can differ within the same municipality or city, and the advertised plan may not be offered at every address.

Once connected, test at different times and record download rate, upload rate, latency, and whether the test used Ethernet or Wi-Fi. A single result is only a snapshot. Several measurements under stated conditions provide better evidence of the service the household actually receives.

1.4 Software Selection

Hardware determines what a device is physically capable of doing, but software turns that capacity towards a particular task. Choosing software therefore begins with the task, not with whichever application happens to be popular. You must also consider compatibility, cost, privacy, security, support, and whether you will still be able to open or export your work later.

1.4.1 Types of Software by Use

Software can be grouped according to its principal purpose. These categories are convenient rather than absolute: one application may perform several kinds of work and therefore belong to more than one category.

Table 1.3: Common types of software classified by use.

Type	Principal use	Examples of tasks
System software	Operates the device and manages its hardware resources.	Running the operating system, controlling a printer, and managing files and memory.
Productivity software	Helps users create, organise, calculate, and present work.	Writing documents, using spreadsheets, preparing presentations, and taking notes.
Communication and collaboration software	Allows people to exchange messages or work together.	Email, instant messaging, video meetings, shared calendars, and collaborative editing.
Scientific and data software	Collects, manages, analyses, models, or visualises data.	Statistical analysis, database work, programming, bioinformatics, mapping, and laboratory data collection.
Creative software	Produces or edits visual, audio, and multimedia material.	Drawing, photography, page layout, animation, audio recording, and video editing.
Utility software	Maintains, organises, diagnoses, or extends a computer system.	Backing up data, compressing files, managing storage, and monitoring system performance.
Security software	Helps protect devices, accounts, networks, or data.	Malware detection, password management, encryption, firewalls, and secure authentication.
Educational software	Supports teaching, learning, practice, or assessment.	Learning platforms, simulations, tutorials, reference tools, and quizzes.
Entertainment software	Provides recreation or access to media.	Games, media players, streaming, and digital reading.

The intended use determines which features deserve attention. A spreadsheet may be entirely adequate for a small table but awkward or unsafe for a large, shared research data set. A sophisticated statistical package may be powerful but unnecessarily difficult for a simple calculation. Software should be proportionate to the task and the consequences of error.

1.4.2 How Software Is Supplied and Paid For

The labels used for software do not all describe the same thing. Some describe how software is delivered, some describe how payment works, and others describe what its licence permits. A single product may therefore carry several labels. For example, an online service can be SaaS, subscription-funded, and partly open source at the same time. **Proprietary software** is software whose owner does not normally supply the source code or grant users permission to inspect, modify, and redistribute it.

Table 1.4: Common ways in which software is supplied, licensed, or funded.

Model	**What it means**	**Important qualification**
Perpetual licence (often sold as a one-time purchase)	The licence allows the user to keep using a particular product or version without a scheduled expiry.	The payment may not include future major versions, continuing support, cloud storage, or compatibility with future devices. The user normally buys a licence, not ownership of the code.
Subscription licence	Continued use or access requires payment at regular intervals.	Updates and services may be included, but access to the software or some features may end when the subscription ends.
Software as a Service (SaaS)	The provider operates the software as an online service, commonly accessed through a browser or application.	SaaS describes delivery, not necessarily price. It may be subscription-funded, free to the user, advertising-funded, or paid for by an institution. Internet access and the provider's continued operation may be essential.
Freeware	In this chapter, the term means proprietary software supplied without a monetary charge.	A zero price does not normally grant permission to inspect, modify, or redistribute the source code. Other costs may include advertising, data collection, or paid companion services.
Free and open-source software (FOSS)	The source code is available under a licence that grants rights to use, inspect, modify, and redistribute it subject to stated conditions.	Open source does not necessarily mean that every service, copy, or form of support is free of charge. Its licence obligations still apply.
Freemium	A basic version is free, while additional features, capacity, or convenience require payment.	The free version may impose storage, export, collaboration, usage, or advertising limits.
Institutional or educational access	A university, school, or employer pays for or negotiates access on behalf of eligible users.	Access may end when the agreement expires or the user leaves the institution. Personal files should be exported before eligibility ends.
Trial or demonstration version	Use is allowed temporarily or with restricted features so that the product can be evaluated.	The software may stop working, limit saving or export, or require payment after the trial.

Keep two questions separate: how software is paid for and where it runs. Installed software can require a subscription, while a web-based service can be provided without charge. Likewise, "freeware" is not a synonym for "open source": in this chapter the first concerns price, whereas the second concerns licence permissions.

1.4.3 Choosing Software

Begin by stating what the software must accomplish and which file formats, devices, operating systems, and collaborators it must support. Test whether it can import existing work and export data in a form that other applications can read. A convenient tool can become a trap if all of the user's work is held in a proprietary format that cannot be moved elsewhere.

Look beyond the price shown on the first day. Add renewals, storage, additional users, paid extensions, training, accessories, and the cost of moving data to another system. A one-time purchase is not automatically cheaper than a subscription, nor is free software automatically the better choice. The answer depends on the task and the period over which the software will be needed.

Privacy and security matter whenever software handles personal, academic, financial, health, or research data. Before using it, check what data it collects, where those data are stored, who can access them, whether suitable backups and encryption are available, and how the provider responds to security problems. Software should come from a dependable source and receive appropriate updates. Open source permits inspection of the code, but that fact alone does not guarantee that a particular program is secure or well maintained.

Also consider usability, accessibility, documentation, technical support, offline operation, and the ability of collaborators to use the same files. Using an unlicensed copy of commercial software is not a sensible way to save money. An altered installer may contain malicious software, and unauthorised copying or use may violate licence terms or copyright law. A simpler legal tool that does the required job is usually the better choice.

Freeware and paid software. Freeware removes the immediate purchase cost and can make useful tools available to people who could not otherwise afford them. It may also be convenient for a small or occasional task for which buying a large commercial package would be excessive. Many freeware programs come from reputable developers and are maintained responsibly. The absence of a price is not itself a warning that software is malicious.

But do not assume that every free download is safe. A file presented as freeware may have been altered, repackaged, or imitated by someone other than the real developer. Some freeware is supported by advertising, optional bundled programs, extensive data collection, or repeated pressure to buy another product. The program itself may not contain malware, yet an advertisement or false download button may lead the user to an unsafe site. The United States Federal Trade Commission therefore advises users to avoid software-download advertisements and unfamiliar download sites and to obtain software from a source they know and trust [9].

Paid software often has funding for continued development, documentation, technical support, testing, and regular updates. An established developer also has a reputation and customer relationships to protect. These considerations can provide useful evidence of trustworthiness, but payment is not a guarantee of quality, security, or privacy. A paid product can contain a vulnerability, stop receiving updates, impose restrictive licence conditions, collect more data than the task requires, or show advertising. Payment is therefore not a privacy test. Applications and websites may use identifiers and other information for tracking and personalised advertising [10].

Software	Possible advantages	Questions to ask
Freeware	No purchase cost; easy to try; may be sufficient for a small or occasional task.	Is this the developer's official copy? How is development funded? Does it display advertisements, install extras, collect data, receive updates, and provide a way to export files?
Paid software	May provide sustained development, documentation, support, updates, and specialised features.	Is the developer dependable? What is the total cost? What happens when payment or support ends? What data are collected, and can work be moved to another product?

Treat price as one piece of evidence, not as a security test. Before installing any program, confirm the developer and exact website or official store, avoid advertisements masquerading as download buttons, check the requested permissions, and keep both the program and device updated. For important work, also confirm that files can be backed up and exported. These checks apply to free, paid, subscription, and open-source software alike.

Practical Work

List the digital systems you have used since waking up. Choose one activity and trace its input, processing, storage, output, and communication. Identify the hardware, software, data, and networks involved. For one piece of software, identify its principal use and how it is supplied or paid for. End by stating one thing about the system that you would like this course to help you understand.

1.5 Questions for Discussion and Exercises

We will use some of these questions in class. Use the others to review the chapter and test whether you can apply its ideas.

1. A student enters observations into an online form during a biology laboratory activity. Identify a possible input, processing step, form of storage, output, and act of communication. Name the main hardware and software involved.
2. Explain the difference between RAM and long-term storage. Why would a computer need both?

3. A laptop is advertised as having more CPU and GPU cores than another model. Explain why those figures alone do not prove that it will be faster for a student's work. Identify one non-upgradeable component and explain how the words "up to" should affect the interpretation of its battery claim.
4. The EveryMac source used for Table 1.1 gives two memory-bandwidth figures. Explain how the manufacturer's specification resolves the conflict and what this example teaches about apparently authoritative tables.
5. Why should a buyer check the exact regional model of a phone rather than relying on its product name alone? In your answer, use the SIM or battery differences in Table 1.2, and explain why three 48-megapixel cameras are not one 144-megapixel camera.
6. Explain the difference between the connection that brings internet service into a home and the Wi-Fi network inside it. How could you investigate which one is causing a slow connection?
7. Ignoring overhead, estimate how long a 100 Mbps connection would take to download an 800 MB file. Show the conversion between bytes and bits before calculating the time.
8. A household regularly makes video calls, uploads large files, and has several simultaneous users. Apart from advertised download rate, what features and plan conditions should it examine before subscribing?
9. Explain why SaaS, subscription software, freeware, and open-source software are not four mutually exclusive categories. Then assess the claim that freeware is probably malware whereas paid software is safe.
10. A biology group needs software for recording observations, analysing data, and sharing results. State the questions the group should ask before choosing a product. Include compatibility, cost, privacy, data export, and continued access in your answer.

Chapter 2

The Physical Foundations of Computing

Learning Outcomes

By the end of this chapter, you should be able to:

1. trace a familiar digital activity through the physical devices, connections, facilities, energy, and workers that make it possible;
2. explain, without unnecessary engineering detail, how electrical states, transistors, circuits, and software belong to different levels of a computing system;
3. describe the main stages through which chips and electronic devices are produced and the physical requirements that keep digital systems operating;
4. explain how concentration, chokepoints, substitution, and interdependence create both technological power and technological vulnerability;
5. distinguish participation in a global value chain from control of that chain; and
6. evaluate a technological policy or partnership according to stated Philippine interests rather than automatic loyalty to a foreign power.

How do physical and financial chokepoints become political leverage?

Digital activity can feel weightless. A photograph disappears into "the cloud", a video call joins people in different provinces, and a search result arrives before anyone has time to wonder where it came from. Yet every one of these actions depends on matter moving, storing, or transforming energy. There are chips, batteries, radios, routers, cables, data centres, cooling systems, ports, mines, factories, and people behind the screen.

Those physical foundations have political consequences. In November 2025, the *South China Morning Post* examined China's use of controls on rare-earth exports amid a wider dispute over access to advanced chips and chipmaking equipment [11]. A rather small amount of a specialised material can hold up the production of cars, electronics, motors, and other much more expensive goods. The dispute is not simply a contest between a powerful China and a vulnerable United States. China has material and industrial chokepoints; the United States has financial and technological ones. Both still need capabilities supplied by other countries.

So let us begin with the exact link each side can influence. How can it apply pressure? What substitutes are available, and what would using that power cost? We need some technical knowledge to answer these questions, but not a degree in electrical engineering. We need to see the system clearly enough to judge claims about it.

Before Class

1. **Read.** *How China's Rare Earth Leverage Works—Limits, Risks and Global Responses*, by Kandy Wong, *South China Morning Post*, 12 November 2025; updated 13 November 2025 [11].

2. **Read.** *Semiconductors: A Global Supply Chain Powering Modern Life*, CGTN Europe, 30 November 2024 [12].

3. **Map.** On one page, sketch the journey of a phone, laptop, router, or data-centre server from materials to use. Label the stages and places named in the sources, circle one link that appears difficult to replace, and note one simplification that the chapter helps you correct. Bring the sketch to class.

Treat both sources as starting points rather than final authorities.

2.1 A Digital Action Has a Physical Route

Suppose a biology student photographs a leaf specimen and uploads the image to a shared folder. The camera sensor responds to light. Electronics convert its output into data. The processor follows software instructions to construct an image, RAM holds material being used, and storage retains the file. The phone's battery supplies energy while its radio sends a signal to a Wi-Fi router or mobile base station.

The photograph then passes through equipment operated by several organisations. It may travel through fibre-optic cables, switching and routing equipment, and possibly submarine links before reaching a provider's data centre. There, servers check the account, storage systems retain the file, and other network equipment makes it available to authorised users. Power equipment keeps the facility running and cooling equipment carries away heat. When a classmate opens the photograph, another physical route delivers a copy to another physical device.

In Chapter 3, we will examine how networks organise and direct data. For now, keep three observations in mind. First, the user's phone is only one part of the system. Second, "wireless" normally describes only part of the journey: a radio link often leads to extensive wired infrastructure. Third, the cloud is not an immaterial place. For most everyday cloud services, it means using computers operated by another organisation in buildings somewhere else.

Part of the route	What must work	One possible interruption
Student's device	Sensor or input, processor, memory, storage, software, battery, and network interface	Full storage, a damaged battery, an application error, or a failed radio
Local connection	Router or mobile base station, power, and a usable signal	Power failure, poor coverage, interference, or an overloaded network
Provider networks	Cables, network equipment, power, maintenance, and links to other networks	A damaged cable, failed equipment, or an upstream outage
Remote service	Servers, storage, account systems, cooling, electricity, and staff	A service fault, failed storage, loss of power, or a security incident
Other user's device	A working connection, compatible software, display, and permission to access the file	No access permission, an unsupported format, or another local outage

An online activity can therefore fail even when the student's phone is in perfect condition. It can also continue when one component fails if the system has a second route, backup power, replicated storage, or another form of **redundancy**. Redundancy can look wasteful during ordinary operation, because capacity is kept in reserve. During a failure, it becomes the reason a service survives. This tension between low cost and resilience will reappear in the discussion of supply chains.

2.1.1 Keeping the Infrastructure Running

A digital system has two broad kinds of physical requirement. It has an **embodied requirement**: the materials, energy, factories, transport, and labour used to make its equipment. It also has an **operational requirement**: the electricity, cooling, connectivity, maintenance, and replacement parts needed while that equipment is in use.

Data centres make the distinction easy to see. Their servers, storage devices, network equipment, buildings, generators, batteries, and cooling systems must first be manufactured. Once installed, they need reliable electricity and temperature control. Cooling may use air, water, or a combination, depending on the facility and local conditions. Efficiency per task can improve while total demand still grows. The International Energy Agency reports rapid reductions in the energy used for individual AI tasks alongside a 17 per cent increase in global data-centre electricity demand in 2025 [13]. Equipment efficiency does not by itself make total resource use disappear.

Workers are part of this physical system. Engineers design equipment; miners and refinery workers produce materials; factory workers manufacture and test components; seafarers, drivers, and port workers move them; technicians install and repair equipment; and power, telecommunications, and data-centre workers keep services operating. A diagram that contains only boxes and arrows can hide all of them.

2.2 From Electrical States to Useful Work

At a basic level, digital electronics distinguishes physical states that can be treated as 0 and 1. The states may be represented by controlled electrical conditions. There are no tiny printed zeroes and ones travelling through a chip. A **bit** is an interpretation of a physical state.

A **transistor** is an electronic device that can control current. The first successful point-contact transistor was demonstrated at Bell Telephone Laboratories in December 1947 by John Bardeen and Walter Brattain [14].

Figure 2.1: A 1997 commemorative replica of the first point-contact transistor, demonstrated at Bell Telephone Laboratories in December 1947. The photograph is a public-domain work of the Executive Office of the President of the United States, obtained through Wikimedia Commons.

Many transistors can be connected into circuits that perform small logical and memory operations. Many such circuits can be organised into a processor that follows instructions, or into memory that holds information for rapid use. Software supplies organised instructions. An application such as a camera or spreadsheet is therefore several levels removed from the electrical conditions inside the machine, but it cannot operate without them.

Level	**Question answered at that level**
Electrical state	Which controlled physical condition is present?
Transistor and circuit	What small operation can be performed or remembered?
Processor and memory	Which instructions and data are being handled?
Operating system	How are the device's resources made available and managed?
Application	What recognisable task is being performed for the user?
Human and institution	Who chose the task, rules, data, and purpose?

These descriptions are not competing explanations. Saying that a student submitted an assignment, that an application transmitted a file, and that transistors changed electrical states can all describe the same event at different levels. Confusion results when a claim appropriate to one level is silently transferred to another. A computer can compare encoded values, for example, without understanding why a teacher imposed a deadline.

Modern chips integrate enormous numbers of transistors. Miniaturisation allows much work to be performed in a small space, but switching and moving information require energy, and some energy becomes heat. Designers must balance speed, power use, battery life, cost, and cooling. A phone becoming warm during a demanding task is therefore not mysterious. Unusual heat, swelling, a burning smell, a damaged cable, or repeated shutdowns, however, should not be ignored.

The main material in most modern chips is a **semiconductor**, whose electrical behaviour can be carefully controlled. Silicon is widely used, but a chip is not merely a polished piece of silicon. It is a manufactured arrangement of extremely small structures, layers, and connections. That observation takes us from how a chip works to the more politically important question of how a chip comes to exist.

2.3 No Country Makes a Phone by Itself

A product may carry the words "Made in" followed by one country. That label does not normally tell the full history of its materials, design, machinery, components, software, assembly, or transport. A phone is better understood as the temporary meeting point of several value chains.

2.3.1 From Design to Chip

Chip production can be understood without memorising every chemical or machine:

1. A chip is **designed**. Engineers decide what it should do and create the detailed description needed to manufacture it.
2. Semiconductor material is purified and formed into thin **wafers**.

3. A fabrication plant repeatedly forms and connects microscopic structures on those wafers. This requires specialised equipment, chemicals, gases, exceptionally clean conditions, water, electricity, and skilled work.

4. The wafer is tested to identify the parts that work as intended. It is then divided into individual pieces called **dies**.

5. Working dies are **packaged** so that they can be protected, supplied with power, cooled, and connected to other components. They are tested again before being incorporated into a larger product.

The United States Department of Commerce describes design, fabrication, assembly, testing and packaging, materials, and manufacturing equipment as distinct but connected parts of the semiconductor supply chain [15]. A firm may design chips without owning a fabrication plant. A fabrication firm may manufacture designs created elsewhere. Other firms may specialise in equipment, materials, packaging, or testing. This specialisation can improve efficiency and make extraordinary technical capability possible. It also creates dependencies.

Figure 2.2 provides a useful bird's-eye view. Design software and reusable circuit designs feed chip design; designs, manufacturing equipment, and materials then come together in wafer fabrication. Finished dies proceed to assembly, testing, and packaging before reaching customers. The geographical distribution changes from one activity to the next, and no region leads every stage. The figures are a snapshot rather than a timeless league table. Regional categories simplify multinational firms and cross-border production. Figures for different activities should be compared only when their dates, products, and measures are consistent.

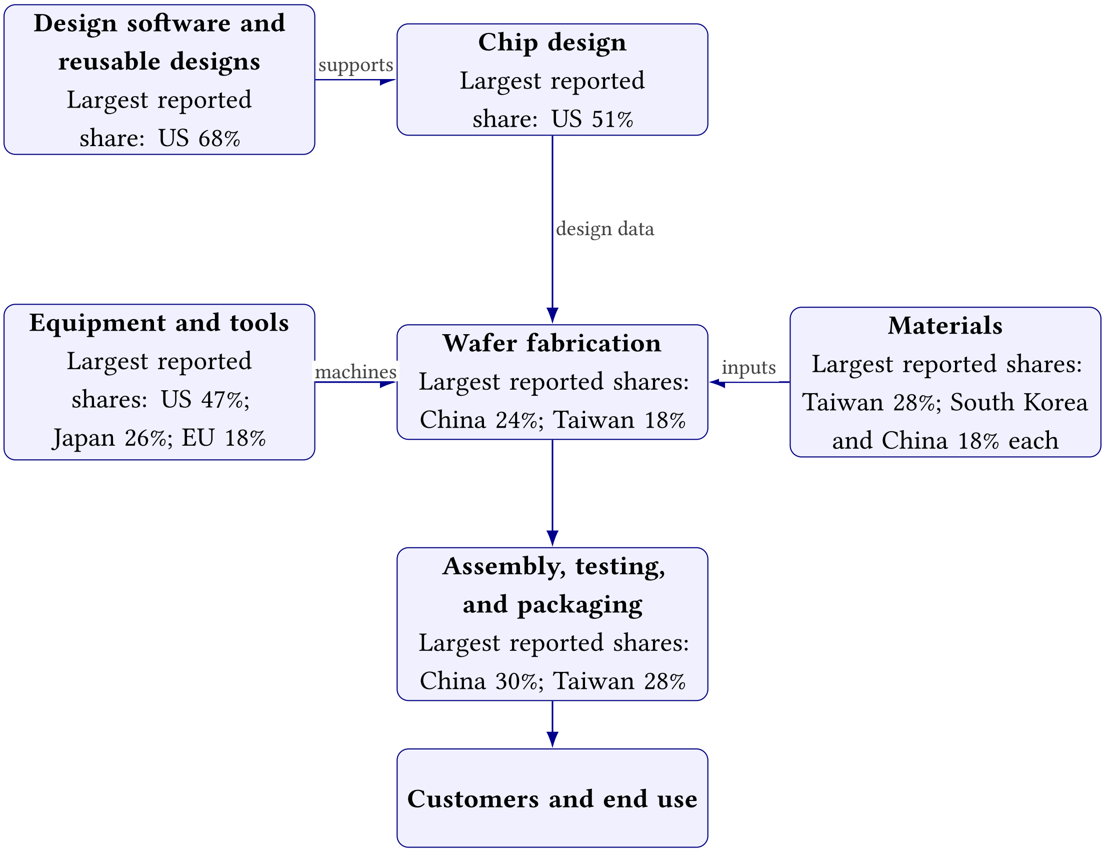

Figure 2.2: Selected geographical concentrations in the semiconductor value chain, using 2022 data from the Semiconductor Industry Association and Boston Consulting Group. Some percentages are based on company revenue and headquarters; others are based on where production capacity is located. Regions not shown complete each category [16].

Silicon is abundant in the Earth's crust, but an ordinary pile of sand is not a tray of computer processors waiting to happen. The difficult parts include purification, precise design, specialised equipment, repeated processing, quality control, packaging, knowledge, and the coordination of suppliers. A country can possess a raw material without possessing all the capabilities needed to turn it into a competitive chip.

2.3.2 Beyond the Chip

Even the most advanced processor is not a phone. A complete device also needs working memory and storage, circuit boards and connections, a display, cameras, radios, speakers, microphones, sensors, a battery, charging electronics, a case, connectors, and software. These require different materials and manufacturing processes.

Part	What it contributes	Earlier links that may be required
Chips	Processing, memory, storage, sensing, communication, and power control	Design, specialist materials and equipment, fabrication, packaging, and testing
Circuit board and connectors	Physical and electrical connections among parts	Metals, glass fibre or other substrate materials, chemicals, and precision manufacturing
Display and cameras	Visual output and image capture	Glass, electronic materials, sensors, lenses, coatings, and assembly
Battery	Portable energy	Mineral extraction, chemical refining, cell manufacture, control electronics, and safe transport
Speakers, motors, and sensors	Sound, movement, vibration, and measurement	Magnets, coils, metals, ceramics, and specialised components
Case and protective parts	Structure, durability, and heat management	Metals, glass, plastics, forming, machining, and coatings

Rare-earth elements enter this story through particular materials and components, including some high-performance permanent magnets and specialised electronic, optical, and industrial applications. They are not the principal ingredient of every chip, and the seventeen elements grouped under the term “rare earths” are not interchangeable. The relevant question is always which element, in which form, at which stage, for which use.

2.3.3 Chain, Network, and Life Cycle

The word **supply chain** is useful because it emphasises connection: if an indispensable link fails, the final product may not appear. The real arrangement is more like a network. One component has several suppliers; one refinery serves several industries; a factory depends on electricity, water, finance, transport, software, standards, and workers; used products may supply recycled material.

The broader **value chain** asks where useful capabilities and economic value are added. Its stages can be summarised as follows:

Stage	Examples	Question to ask
Extraction	Mining and recovery of raw materials	Who has usable deposits, and what are the environmental and community costs?
Processing	Separation, refining, and production of usable materials	Where does the knowledge and industrial capacity exist?
Components	Chips, batteries, displays, circuit boards, magnets, and sensors	Which parts are difficult to substitute or expand quickly?
Assembly and testing	Combining parts, checking quality, and preparing products for sale	How much capability and value are retained locally?
Distribution	Ports, shipping, warehouses, retailers, and service providers	Which routes and markets are necessary?
Operation and support	Electricity, networks, data centres, maintenance, updates, and repair	What keeps the product useful and secure?
End of life	Reuse, parts recovery, recycling, and safe disposal	Can value be recovered and harm reduced?

Participation at one stage matters, but it is not control of the whole. A country may assemble many devices while importing important components. Another may mine a mineral but send it elsewhere for refining. Another may design advanced chips while relying on foreign fabrication, packaging, customers, and materials. "We are part of the chain" and "we can command the chain" are very different claims.

Nor does price reveal strategic importance. A component costing only a few pesos can halt the sale of a product worth thousands if the component is indispensable and no qualified replacement is available. Conversely, an expensive component may provide little leverage when buyers can obtain an equivalent product from several suppliers. Power arises from the structure of dependence, not from national pride or the size of an object.

2.4 When One Link Becomes Leverage

Four concepts help explain why one participant can exert pressure on others:

1. **Concentration.** A large share of a required material, component, or capability is supplied from a small number of places.
2. **Chokepoint.** A link is sufficiently important and difficult to bypass that its interruption constrains the wider system.
3. **Substitution.** Another material, supplier, design, or process can perform the required role. Substitution may nevertheless require redesign, testing, approval, new equipment, and time.
4. **Interdependence.** A powerful supplier still depends on other participants for some combination of inputs, equipment, knowledge, finance, transport, security, and customers.

Concentration alone does not prove that an interruption will be effective. A buyer may have inventories. Other producers may possess unused capacity. The controlled input may be important in one product but irrelevant to another. Smuggling or indirect trade may weaken a restriction. A substitute may be inferior but adequate. To assess leverage, we must ask how much is controlled, at which stage, for how long, with what alternatives, and at what cost to both sides.

2.4.1 China's Rare-Earth Leverage

The advantage is not simply geological. China's position is not explained merely by the location of mines. For the magnet rare earths it examines, the International Energy Agency reports that in 2024 China accounted for 60 per cent of mined production, 91 per cent of refined output, and 94 per cent of permanent-magnet production [17]. Processing and manufacturing capability are therefore at least as important to the case as possession of deposits.

The process is difficult. Other countries can perform these activities. The difficulty is reproducing the whole system quickly, at competitive cost, and at the required quality. Rare-earth elements are reasonably plentiful in the Earth's crust, but economically useful concentrations are less common. They normally occur mixed with one another, and their similar chemical properties make them difficult to separate. Mining therefore produces an intermediate material, not a finished magnet. The useful minerals must first be concentrated from the ore, a process called **beneficiation**. Chemical treatment and separation then produce individual oxides, which must be converted into metals and alloys before a magnet can be made [17].

An industrial base. China's advantage comes from capacity across these connected stages, not just from opening mines. Its large magnet industry provides steady demand for processors farther up the chain. Scale, skilled workers, established suppliers, shared infrastructure, access to energy and other inputs, and links among refining, metal and alloy production, and magnet manufacture reinforce one another. A new project outside China often starts at smaller scale with higher capital and operating costs. It must secure permits, manage chemical and sometimes radioactive waste, obtain specialised equipment, find buyers for the valuable elements and for other elements separated at the same time, and raise money before customers have accepted its output [17].

Nor is announcing a mine the same as creating a mine-to-magnet chain. The IEA identifies refining and magnet manufacture as the slower parts of diversification. Some specialised equipment has few suppliers outside China and may take years to obtain, while industrial knowledge is partly practical knowledge developed through repeated production. A magnet for a motor or data-centre component must also meet the buyer's technical specifications and reliability requirements. Another country can build these capabilities, but money, equipment, workers, customers, environmental safeguards, and time must arrive together [17].

Controls are specific. In April 2025, China introduced controls covering seven heavy rare-earth elements and related products. Further controls announced in October were suspended for a year in November [17]. This timeline matters. "China banned rare earths" would be a misleading summary: particular controls, products, destinations, licensing arrangements, and dates must be identified.

This industrial depth is what turns concentration into leverage. A manufacturer that cannot obtain a qualified magnet cannot replace it with a bag of unprocessed ore or an announced mining project. Even a licensing delay can therefore cause uncertainty, higher prices, or interrupted production.

Leverage has limits. The leverage is not unlimited. Controls may reduce income for Chinese suppliers and impose costs on firms in China that need foreign markets or components. Customers may build inventories, support competing producers, redesign products, use substitutes, recover material through recycling, or accept higher costs in exchange for more secure supply. Aggressive use of a chokepoint can motivate other participants to weaken it. Leverage is therefore real, but conditional and capable of changing.

2.4.2 US Financial and Technological Leverage

Finance. The US dollar is widely used as a reserve asset, a currency for trade and payments, and a unit for international banking. Federal Reserve researchers report that it accounted for 58 per cent of disclosed official foreign-exchange reserves in 2024 and about half of international payments sent through SWIFT, a widely used financial-messaging network. Dollar use in trade and international banking was also much larger than the US share of world output or trade [18]. This position makes access to US banks, markets, and dollar settlement valuable even to firms and governments outside the United States.

US financial sanctions draw power from this position and from American legal authority over institutions and transactions connected to its financial system. Exclusion can make payments, borrowing, investment, and trade more difficult. The dollar is not, however, a switch that Washington can turn off for the entire world. The effect of a measure depends on its legal scope, enforcement, cooperation from other governments and financial institutions, and the target's alternatives. The US Treasury warns that alternative payment systems, digital assets, and reduced exposure to the dollar could erode the long-term effectiveness of sanctions; it also stresses clear objectives, multilateral coordination, and attention to unintended harm [19].

Technology. As Figure 2.2 illustrates, American firms occupy strong positions in chip design and electronic design automation and intellectual property. US export rules also cover high-bandwidth memory, semiconductor-manufacturing equipment, software, and technology. Under specified foreign direct product rules, certain items made outside the United States can fall within US export jurisdiction when they are produced using covered American technology or equipment [20].

An early Nvidia case makes this leverage more concrete. In August 2022, the company disclosed that the US government had imposed an immediate licensing requirement on future exports to China, including Hong Kong, of its A100 and forthcoming H100 advanced-computing chips and systems containing them. Nvidia said it would offer Chinese customers alternative products where possible and seek licences when alternatives were insufficient [21, 22]. This was not a ban on every Nvidia chip, and a licensing requirement does not mean that every application will be refused. It nevertheless showed how a government could use jurisdiction over a narrow but important class of technology to affect a foreign country's access and the commercial decisions of its own firms. The example is dated deliberately: the detailed rules and covered products have changed since 2022.

This is substantial leverage, but it is not ownership of "technology" in general. Advanced semiconductor production also relies on equipment and materials from Europe and Japan, fabrication in Taiwan and South Korea, and assembly, testing, packaging, manufacturing, and markets across Asia. China has developed major capabilities of its own and continues to invest in alternatives. The comparison here concerns particular chokepoints, not a ranking of the total scientific or technological ability of two countries.

2.5 Two Powers, Different Chokepoints

China and the United States can therefore place pressure on different parts of the same international system. We can compare these forms of leverage without pretending that the two countries' capabilities, policies, or conduct are identical.

Dimension	China	United States
Concentrated positions	Rare-earth separation, refining, and permanent-magnet production for important industrial uses	Dollar-centred finance; advanced chip design; EDA and IP; selected advanced chips, equipment, software, and technology
Means of pressure	Export licensing, delays, restrictions, and the possibility of withholding difficult-to-replace materials or components	Financial sanctions, restrictions on access to the US financial system, and export controls on specified technologies and products
Continuing dependencies	Foreign semiconductor capabilities, equipment, customers, transport, some international payment channels, and other internationally supplied inputs	Foreign fabrication, specialist equipment and materials, assembly and testing, manufacturing capacity, allied cooperation, and overseas markets
Ways leverage may weaken	New suppliers, stockpiles, recycling, substitution, redesign, and reduced reliance on Chinese processing	Alternative payment channels, reduced dollar exposure, new suppliers, technological substitution, domestic development, and weaker cooperation by other countries

China's advantage in rare-earth processing does not give it command of every electronic product. American strength in finance and semiconductor technology does not allow the United States to manufacture the whole chain alone. In both cases leverage is strongest when the controlled link is indispensable, substitutes are costly or slow, and other participants cooperate with or comply with the restriction. Using a chokepoint can also encourage customers to escape it.

When a headline says that a country "controls technology", rewrite it more precisely. Identify the stage, product, share, period, legal measure, affected users, and available alternatives. The same standard applies whether the pressure comes from Beijing, Washington, or another government.

2.6 What Does "Pro-Philippines" Require?

Public argument often treats international affairs like a basketball match: choose a team, defend every decision it makes, and jeer at the other bench. That habit is especially unhelpful for technology. The physical system just examined does not divide neatly into two self-contained camps. Materials, equipment, designs, factories, workers, shipping routes, investors, markets, and standards cross political boundaries.

Being described as "pro-US" or "pro-China" can also conceal several different decisions. A government can trade with a country, accept a particular investment, cooperate on security, use a technical standard, criticise a policy, or reject a contract. Agreement in one area does not require agreement in all the others.

The supply chains in this chapter point to a prior Philippine interest: global political stability. Philippine households and firms cannot enjoy reliable access to technology if major economies repeatedly interrupt trade, finance, shipping, or production. A conflict among them would travel through the same networks on which the Philippines depends. Interdependence gives countries practical reasons to preserve peace and predictable exchange, but it does not make peace automatic. A chokepoint can be used precisely because others depend on it. Stability therefore still requires diplomacy, predictable rules, peaceful settlement of disputes, functioning trade routes, and enough resilience that no participant can easily hold the rest hostage.

That wider stability is the condition within which the Philippines can try to tilt particular bargains in its favour. The sensible objective is neither automatic alignment nor a refusal to choose. The United States and China do not have identical institutions, capabilities, conduct, or relationships with the Philippines, and particular actions need not deserve identical judgements. The relevant test is what a proposal does to Philippine welfare, capability, security, and freedom of action. Cooperation with the United States in one area and China in another is not necessarily inconsistent. Dependence so deep that the Philippines cannot refuse either partner is the more serious problem.

"Pro-Philippines" sounds reassuring, which is precisely why it must not be allowed to do the work of an argument. Filipinos can disagree honestly about what a policy should prioritise. Consumers may want lower prices, workers may want secure employment, firms may want reliable inputs, communities may oppose pollution, and government agencies may worry about security or excessive dependence. A serious national-interest argument identifies these interests and explains its trade-offs.

The Philippines is not merely a spectator in electronics. According to the Philippine Statistics Authority, electronic products accounted for 54.3 per cent of the country's merchandise export earnings in 2025 [23]. The Board of Investments describes Philippine strengths in semiconductor assembly, testing, and packaging and in electronics manufacturing services, alongside efforts to develop design and higher-value capabilities [24]. These activities provide jobs, exports, experience, and infrastructure. They do not mean that the Philippines controls chip design, fabrication equipment, raw materials, transport, or overseas demand. Participation matters, but it does not amount to complete control.

When you consider a technological investment, restriction, contract, or partnership, give "pro-Philippines" some content by asking these questions.

Table 2.1: Questions for evaluating a technological proposal from a Philippine perspective.

Concern	**Questions to investigate**
Access and cost	Will useful technology, components, or services remain available at a price Philippine households, schools, firms, and government can afford? Who receives a subsidy, guarantee, or exclusive advantage?

Continued on the next page

Concern	**Questions to investigate**
Employment and income	How many jobs are likely to be created, what kinds of jobs are they, how secure are they, and who captures the resulting income?
Capability	Will Filipino workers, researchers, and firms acquire knowledge, design ability, equipment, intellectual property, or decision-making power? Or will the activity remain easy to move elsewhere?
Resilience	Does the proposal reduce dependence on one supplier or merely replace one dependency with another? Are alternative suppliers, routes, parts, and emergency arrangements available?
Security and control	Who owns and operates critical equipment? Who can access important data? Can Philippine institutions inspect, regulate, repair, or replace the system?
Law and public institutions	Is the arrangement consistent with Philippine law, rights, procurement rules, transparency, and accountable decision-making? What disputes or failures would be difficult to remedy?
Environment and communities	Who uses the land, water, and electricity? Who is exposed to pollution, waste, unsafe work, displacement, or other costs? What obligations remain after a facility closes?
Future choice	Does the proposal leave the Philippines with more skills, partners, and bargaining power, or make withdrawal prohibitively costly? What happens when the contract, political relationship, or technology changes?
Distribution	Which Filipinos gain, which Filipinos pay, and are the promised national benefits actually shared?

No partner will score perfectly on every question. A proposal may create jobs but consume scarce electricity; reduce immediate prices but deepen dependence; improve security but restrict access; or transfer some knowledge while leaving the most valuable decisions elsewhere. Compare the benefits, costs, alternatives, safeguards, and time horizons openly.

Diversification is often part of the answer, but it is not magic. Maintaining several suppliers can cost more. Stockpiles can become obsolete or prove too small. Domestic production may require subsidies and still depend on imported equipment. Recycling cannot immediately meet all demand. Substitution may reduce performance. Resilience is not the absence of trade; it is the ability to continue, adapt, and choose when one relationship or link is disrupted.

2.7 The Point of the Chain

The physical foundations of computing lead to a political lesson, but not to a party line. A phone works only because many layers of technology and many parts of the world meet inside it. A country that controls an indispensable link can gain leverage, yet it normally continues to depend on other links. Attempts to use that leverage can succeed, impose costs on the user, and provoke efforts to escape it—all at the same time.

Strategic independence cannot mean manufacturing every mineral, chip, cable, application, and server within Philippine borders. That is neither a realistic description of modern technology nor an intelligent use of limited resources. It means knowing where the Philippines is vulnerable, developing capabilities that improve its position, maintaining alternatives where the consequences of failure are serious, and negotiating with enough knowledge to say both yes and no.

Being pro-Philippines therefore does not require hostility to the United States, China, or anyone else. It requires refusing to outsource judgement to them.

2.8 Questions for Discussion and Exercises

We will work through selected exercises in class. Use the remaining questions to check your understanding of the chapter.

1. Trace what happens physically when a student uploads a laboratory photograph and a classmate opens it. Include the two devices, local connections, provider networks, remote service, electricity, and cooling. Identify two points at which the activity could fail even if both phones work.

2. Explain how the statements "the student submitted an assignment", "an application transmitted a file", and "transistors changed electrical states" can all describe the same event. Why would it be a mistake to say that the transistors understood the deadline?

3. A phone is labelled "Made in Country A". Construct a plausible value chain involving at least four countries or regions. What can the label establish, and what can it not establish? Use concentration, substitution, and interdependence to explain how one inexpensive link could nevertheless become a chokepoint.

4. Compare China's leverage in rare-earth processing and magnet production with US leverage in finance and advanced semiconductor technology. Identify the mechanism, dependencies, and limits on each side, and explain why the comparison does not establish that either country controls technology as a whole.

5. A foreign company proposes to build a large data centre in the Philippines. Use at least six concerns in Table 2.1 to recommend acceptance, rejection, or renegotiation. State what evidence is missing and which safeguards you would seek.

Chapter 3

The Internet, Web, and Home Networks

Learning Outcomes

By the end of this chapter, you should be able to:

1. distinguish the internet, the Web, Wi-Fi, mobile data, and cloud services;
2. explain in practical terms how a website name, DNS, an IP address, a router, and a server work together;
3. interpret HTTPS indicators and common browser messages such as 403, 404, and 503;
4. use simple comparisons and status-checking tools to distinguish a device or home-network problem from a provider or website problem;
5. design and test a local network whose wired and wireless parts suit the access connection, building, users, and activities; and
6. recommend a usable and reasonably secure home-network arrangement while explaining what a virtual private network can and cannot protect.

How does information travel between devices and services?

Imagine a household with two students, a parent who sometimes works from home, four phones, one laptop, and a television. The internet plan is advertised as fast, yet a video call freezes in a bedroom while streaming works in the living room. One person recommends a faster plan, another wants a new router, and a third says that a virtual private network will solve the problem.

Each proposal could be useful, but only for the right problem. Before buying anything, locate the failure along the route. Is the laptop struggling? Is the Wi-Fi signal weak in the room? Is the household filling the connection? Is the provider congested? Is the remote service unavailable?

Chapter 1 introduced internet connection types and measures such as download rate, upload rate, latency, jitter, and packet loss. Chapter 2 followed a digital action through physical devices, cables, data centres, energy, and workers. We now examine how networks organise that physical route and how a household can make sensible choices about it.

Before Class

1. **Map.** Sketch the network through which you most often reach the internet. Include your device, any Wi-Fi access point or router, the equipment that connects the premises to a provider, and one remote service that you use. If you rely on mobile data, draw the mobile base station instead of inventing a home router.

2. **Observe.** Mark where performance is good and where it is poor. Record the time, place, device, activity, and whether you used Wi-Fi, Ethernet, or mobile data. Do not record or share a network password.

3. **Diagnose.** Write two competing explanations for the poor result and one safe test that would help distinguish them. Bring the map to class.

3.1 Five Things That Are Not the Same

Everyday speech often compresses several systems into the word "internet". That is convenient until something fails. The distinctions in Table 3.1 tell us which organisation, device, or connection to examine.

Term	What it describes	What it is not
Internet	Interconnected networks that exchange data using shared technical rules, called protocols.	A single company, one cable, or the collection of websites.
Web	A system of interlinked resources that browsers request from web servers, normally using HTTP or HTTPS.	The whole internet; email, online games, and many other services also use the internet.
Wi-Fi	A family of technologies that connects nearby devices to a local network by radio.	Internet service. A Wi-Fi network can exist when its internet connection has failed.
Mobile data	Internet access supplied through a mobile operator's radio and core networks.	Wi-Fi, even though a phone can share mobile data by creating a Wi-Fi hotspot.
Cloud service	Storage, processing, or an application supplied through remote computers operated by a provider.	An immaterial place or an automatic backup of everything on a device.

Table 3.1: Related but distinct parts of connected computing.

The internet is commonly described as a *network of networks*. A university, mobile operator, household, government agency, and cloud provider can each operate a network. Agreed technical rules allow data to cross the boundaries between them. No single organisation owns the whole internet, even though a small number of organisations may control important facilities or services within it.

The Web is one useful system built on that foundation. A browser requests a resource identified by a web address, and a web server returns a response. Following a link is therefore a Web action carried over the internet. Sending email and joining an online game also use the internet, but neither action is simply “browsing the Web”.

3.2 Following a Web Request

Suppose a student enters a course website’s domain name in a browser and opens a laboratory guide. The details vary among networks, but the following route provides a useful model.

1. The device first needs a working connection through Wi-Fi, Ethernet, or mobile data.
2. The browser asks DNS to resolve the website name into an IP address. This lets people enter a name such as `example.com` instead of remembering a numerical address [25].
3. The device sends the request through the home router or mobile network and then the internet provider. The request travels in small pieces called *packets*; routers use the address to move them towards the website.
4. The website’s server receives the request and sends a response. When HTTPS is working correctly, it protects the information exchanged while it travels between the browser and that website.
5. The browser puts the response together and displays the requested content.

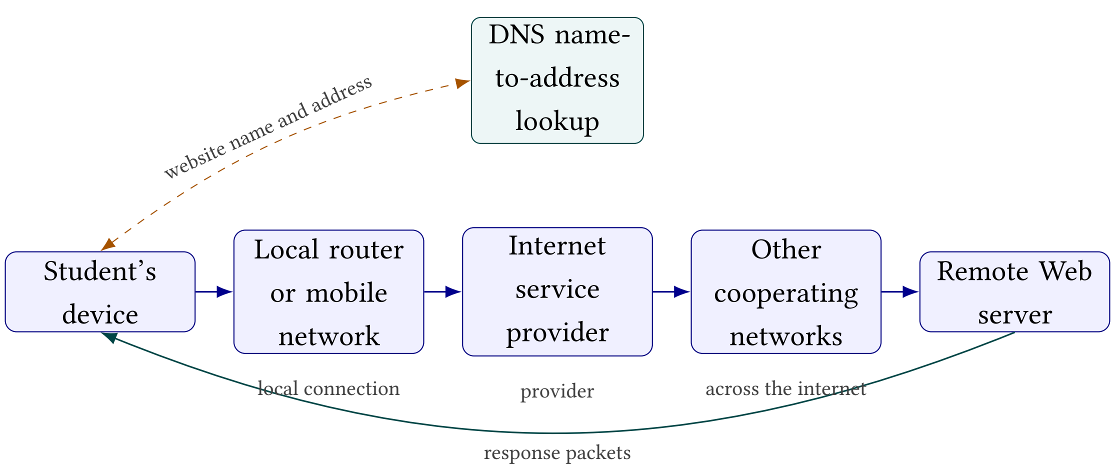

Figure 3.1: A simplified route for a Web request. DNS helps obtain an address; routers then forward request and response packets across several networks.

This is a useful model rather than a fixed itinerary. The networks may choose a different path when conditions change, but users normally do not need to manage that choice.

3.2.1 Names and Addresses

A domain name is the readable part people normally use, such as `example.com`. DNS *resolves* that name to one or more IP addresses: the numerical addresses computers use to deliver the request. It works rather like looking up a contact's name before placing a call, although the technical arrangement is different. If DNS fails, the website may be operating normally but the browser cannot learn which address to contact.

An IP address is a numerical address that networks use to deliver data. It should not be treated as a permanent name for a human being. A household's public address may change; several people and devices may share one public address; and a person may use different addresses at home, on campus, and through mobile data.

Devices on a home network commonly receive addresses used only inside that network. The router lets them share one or more public addresses supplied by the provider.

The address returned for a name can change when a service moves, distributes work among several servers, or sends users to a nearby copy. Users normally do not need to manage this process. They do need to recognise that a "server address not found" or similar DNS message is different from a 404 page: in the first case the browser did not find an address; in the second, it reached a server and received a reply.

3.2.2 What the S in HTTPS Is For

HTTP is the set of rules a browser and website use to exchange requests and responses. HTTPS adds a protected connection. The practical point of the **S** is that data travelling between the browser and the named website is protected against reading or alteration while in transit, and the browser checks a certificate for that website. This matters when sending passwords, messages, payments, or personal information.

HTTPS protects the *connection*; it does not guarantee that the website is honest, that its claims are true, or that it will handle information responsibly. Check the domain name in the address bar. Do not enter sensitive information after a certificate or "connection is not private" warning, and do not bypass such a warning merely because the page looks familiar. Browser symbols vary, so learn the security indicator used by your browser. Google Chrome's guidance similarly distinguishes a private connection from trust in the site itself (Check if a site's connection is secure).

3.2.3 Common Browser Messages

An error message is a clue about how far the request travelled. The exact wording varies, but the distinctions in Table 3.2 are useful in ordinary browsing.

Message	What it usually tells you	A sensible first response
404 Not Found	The browser reached a server, but that server could not find the requested page.	Check the spelling and the end of the address. Open the site's home page and search for a page that may have moved.
403 Forbidden	The server understood the request but refuses access.	Check that you are signed in to the correct account and have permission. Repeatedly refreshing the same request usually changes nothing.
500 Internal Server Error or 503 Service Unavailable	The website reports a problem on its side; 503 often indicates a temporary outage, maintenance, or overload.	Wait and try again, check the service's official status page, or use another channel to contact the organisation.
Server address not found or DNS error	The browser could not turn the domain name into an IP address.	Check the spelling, try unrelated websites, compare another device or connection, and check the provider's status.
Connection timed out	No useful reply arrived in time; the cause could be the device, connection, route, or website.	Compare another site, device, time, and connection before deciding which part failed.
Certificate or private-connection warning	The browser could not establish the expected protected HTTPS connection.	Do not enter sensitive information or bypass the warning. Check the address, device date and time, and network; then wait or contact the site owner.

Table 3.2: Common browser clues and proportionate first responses.

The numbers are HTTP *status codes*: short replies from a server about a request. A 403 or 404 therefore shows that some connection to a server worked; it does not mean that the whole internet is down. The Internet Engineering Task Force defines these codes in the HTTP standard (official HTTP standard).

3.3 When Online Activity Is Slow or Fails

A browser message can show how far one request travelled. Slowness, freezing, and intermittent failure are less tidy. To investigate them, compare activities and parts of the route rather than treating every symptom as "bad internet".

3.3.1 Why a Call Can Fail While a Download Works

Messages, videos, updates, and other users share the same connections. A download can wait for missing data and continue when it arrives. A live call cannot wait long without freezing or becoming difficult to understand.

Limited capacity, delay, interference, or lost data can therefore disturb a call even when messages and downloads still work. The comparison does not identify the cause by itself, but it shows why one successful activity does not prove that the connection suits every other activity.

3.3.2 Why a Nearby Website Can Still Be Slow

The student's provider is only the first large network in the route. Data may then pass through networks operated by other organisations before reaching the website. A provider can manage its own connection, but it cannot guarantee every part of the journey or the availability of the website itself.

Physical distance is therefore only part of performance. A nearby service may still be reached through a busy route, while a service that keeps a copy of popular material inside the Philippines may respond quickly. Current demand, the route, the website's own capacity, and its design all matter.

When a Website Will Not Open

Use comparisons that change one thing at a time:

1. Check the address for a typing error, especially the domain name.
2. Open two unrelated, well-known sites. If neither opens, suspect the device, DNS, local network, or provider before blaming the original website.
3. Try the same site on another device using the same Wi-Fi. Then, if available, turn Wi-Fi off on a phone and try through mobile data. This changes the connection and may also change the DNS service.
4. Look for the service's official status page. An independent checker such as Down for Everyone or Just Me can also test from elsewhere. Never enter a site password into a checker.
5. Record the exact message, address, and time. "It did not work" removes the clues needed to distinguish a 404, DNS failure, timeout, or wider outage.

No single checker is conclusive. It observes from another location and may not see a regional, account-specific, or intermittent problem. Use its result with the comparisons above rather than treating it as a verdict.

3.4 Inside a Home Network

The comparisons above move from the remote service back towards the household. The local network is the first part of that route the household can inspect, reposition, or replace directly. Its equipment is often combined into one box, which makes the separate jobs easy to confuse.

Part	Main job	Important qualification
Modem or optical network terminal (ONT)	Connects the provider's line to the network equipment inside the premises.	Fibre commonly uses an ONT; other services use different equipment. The provider may combine this function with a router.
Router	Connects the local network to other networks and forwards traffic between them.	A home router commonly also assigns local settings, lets devices share a public address, and includes security functions.
Wi-Fi access point	Connects nearby wireless devices to the local network.	It may be built into the router or supplied by separate mesh units.
Ethernet switch	Connects several wired devices within the local network.	A small switch is often built into the home router; extra switches can add wired ports.

Table 3.3: Common parts of a home network.

Equipment can be arranged in several valid ways. A provider might install an ONT and a separate household router. Another provider might supply one all-in-one device, often called a *gateway*, that connects the provider's line, wired devices, and Wi-Fi devices. A more complex home might use the provider's equipment plus separate access points. When troubleshooting, identify functions rather than assuming that every box with antennas performs the same job.

Finding the Router's Settings Safely

First connect to the household router by Wi-Fi or Ethernet. Its settings page often uses a private local address such as `192.168.0.1`, `192.168.1.1`, or `10.0.0.1`, but these are examples rather than universal addresses. An address labelled *router* or *default gateway* in the device's network details is often the first one to try. The correct address may also appear on the equipment label, in the provider's instructions, or in the manufacturer's app. For example, TP-Link documents both `192.168.0.1` and `192.168.1.1` for many models (How to find your router's IP address).

Enter the address in the browser's address bar, not a search box. The router's administration login may differ from the password used to join Wi-Fi. Change any default administration password, change the default username too if the router allows it, store the new details safely, and sign out when finished. Do not change unfamiliar provider or network settings, or perform a factory reset, unless you understand the effect and know how to restore the service. A model may instead require a named address or provider app, so consult its own manual.

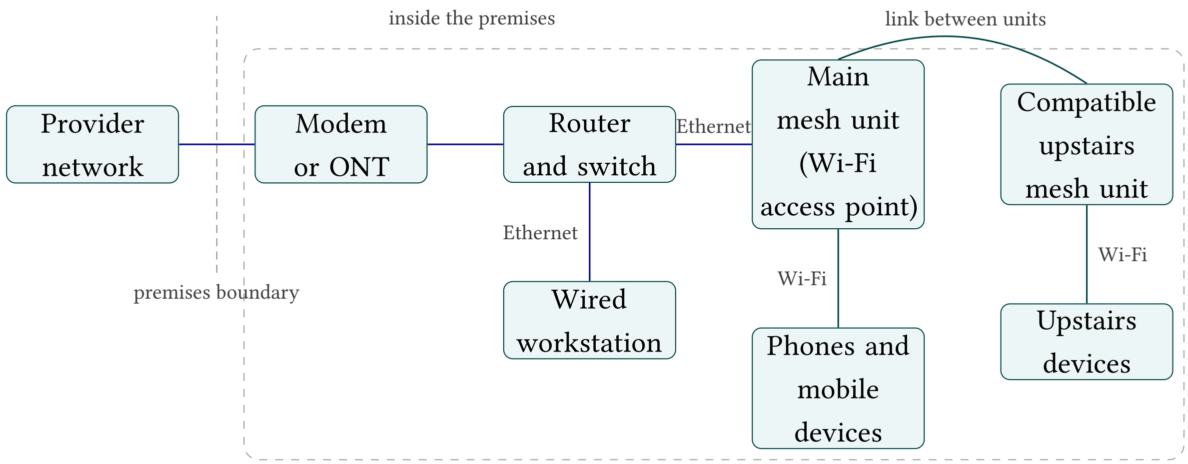

Figure 3.2: One possible home-network arrangement. The functions may be combined in fewer boxes. The two mesh units must be compatible, and their link remains distinct from wired device links and Wi-Fi coverage within each room.

3.4.1 Read the Lights Before Restarting

Indicator names, colours, and blinking patterns vary by model, so the label and manual matter more than a generic colour rule. Before unplugging anything, photograph the lights and note which ones are steady, blinking, or off. The usual clues are summarised in Table 3.4.

Table 3.4: Typical equipment lights; the model's own manual takes priority.

Light	**Usual clue**	**Practical implication**
Power	The light pattern should normally settle after startup; a changing pattern can be normal while the unit starts or updates.	If the light never comes on, check the socket, adaptor, and power switch. Do not interrupt a documented software update.
Internet or WAN	Often shows whether the router has a connection towards the provider; blinking commonly indicates traffic.	If local Wi-Fi works but this light shows no connection, investigate the modem or ONT, provider link, and outage status.
Wi-Fi or WLAN	Usually shows that the wireless radio is enabled; blinking often means traffic.	If it is off, wired internet may still work even though devices cannot join by Wi-Fi. Check whether Wi-Fi was disabled.
LAN or Ethernet	Usually shows that a powered device has a working cable link; blinking commonly means traffic.	An off light for a connected computer points first to the cable, port, or computer rather than the wider internet.
PON	On a fibre ONT or combined gateway, a steady PON light commonly means the unit has registered with the provider's fibre network.	Blinking during startup may mean that it is still trying to connect; for a persistent abnormal pattern, check the model's manual or contact the provider.

Continued on the next page

Light	Usual clue	Practical implication
LOS	Means *loss of signal* on fibre equipment and should normally be off. Red or blinking LOS commonly means that the optical signal is missing or too weak.	Check that the fibre lead has not been loosened, crushed, or sharply bent. Do not factory-reset the unit; record the lights and contact the provider if the condition persists.
WPS	Indicates temporary push-button pairing, not general internet health.	A WPS light does not show that the provider connection is working.

For this Huawei model, steady PON with LOS off means that its fibre link is established. PON off with LOS slowly blinking red means that the ONT is not connected to the fibre line or is not receiving an optical signal (ONT indicator description). The pattern is useful evidence for the provider; it is not a reason to stare into, disconnect, or attempt to repair a fibre connector.

3.4.2 Ethernet and Wi-Fi

Chapter 1 used Ethernet as a point of comparison because a suitable cable removes radio distance and interference from the test. Ethernet also has a design role: it can give a fixed computer a stable link or provide the link that carries traffic between an access point and the main router.

Wi-Fi provides mobility and avoids running a cable to every device, but its capacity is shared and its radio conditions vary. Walls, floors, furniture, distance, neighbouring networks, and other equipment can affect performance. The highest number printed on a router's box is not a guaranteed internet rate in every room. It may combine theoretical capacities under conditions that a particular device, channel, and internet plan cannot reproduce.

The 2.4 GHz Wi-Fi band usually reaches farther and passes through obstacles better, but it can be crowded and offers less capacity than newer alternatives. The 5 GHz band can provide higher rates with compatible equipment but generally has shorter reach. The United States Federal Communications Commission's home Wi-Fi guidance similarly recommends central router placement and notes that a direct Ethernet connection can remove Wi-Fi congestion from a test [26]. These physical trade-offs apply in the Philippines even though radio regulations and available channels differ by country.

3.4.3 Placement, Extenders, and Mesh Networks

Begin with placement before buying more equipment. A router hidden on the floor behind a television, placed at one end of a concrete house, or surrounded by obstacles must overcome conditions that a more central and elevated position could avoid. Place it where important devices can reach it, while respecting the provider cable, power, safety, and household layout.

Avoid enclosing a Wi-Fi router in a metal cabinet: the metal can act like a partial Faraday cage and weaken the radio signal the household is trying to use.

Keep the Wi-Fi Equipment Clear

Do not hide a router or mesh unit behind a television, refrigerator, large mirror, aquarium, water cooler, thick concrete wall, or metal shelving. These objects can absorb, reflect, or block radio signals. Give the equipment open space and ventilation rather than stacking it with game consoles, amplifiers, or other warm electronics.

Microwave ovens, baby monitors, older cordless-phone bases, wireless cameras, and other devices using the crowded 2.4 GHz band can also cause intermittent interference. They do not ruin every Wi-Fi network merely by existing nearby. If performance changes when one operates, move the router or affected device and repeat the same test. NETGEAR's placement guidance gives similar examples (Wi-Fi access-point placement).

A range extender receives and sends Wi-Fi traffic again. It may improve coverage cheaply, but repeating traffic over the same radio connection can reduce usable capacity and add delay. Its own link to the main router must be good; placing it inside the dead zone merely gives it a weak signal to repeat.

A mesh system uses several coordinated access points. It can make movement and management easier and may cover a difficult layout better. Mesh is not a synonym for unlimited speed. Wireless mesh units still require good links to one another, and a wired Ethernet link between units can provide a stronger connection where cabling is practical. A small home with good central coverage may gain little from an expensive mesh kit.

When One Router Is Not Enough

A mesh system is reasonable when tests show good service near the main router but persistent weak coverage in important distant rooms. Consumer systems such as Linksys Velop provide guided setup through an app (Linksys Velop setup guidance). This can be easier for a beginner than configuring unrelated access points separately, but it does not remove the need for sensible placement.

Place an additional unit where it still receives a good link from the main unit, not at the centre of a dead zone. Use Ethernet between units where practical, buy units that the manufacturer confirms are compatible, and test a real call or download in each important room after setup. A mesh redistributes the incoming connection; it cannot repair a provider outage or make a slow plan faster.

3.5 Diagnose the Route Before Buying a Solution

Names matter when they help locate a fault. Change one factor at a time and record the conditions. Running many speed tests without noting the room, device, connection method, server, or time produces numbers without a diagnosis.

Figure 3.3 gives the overall logic. Each answer identifies where to investigate first; it does not prove that the named part is faulty.

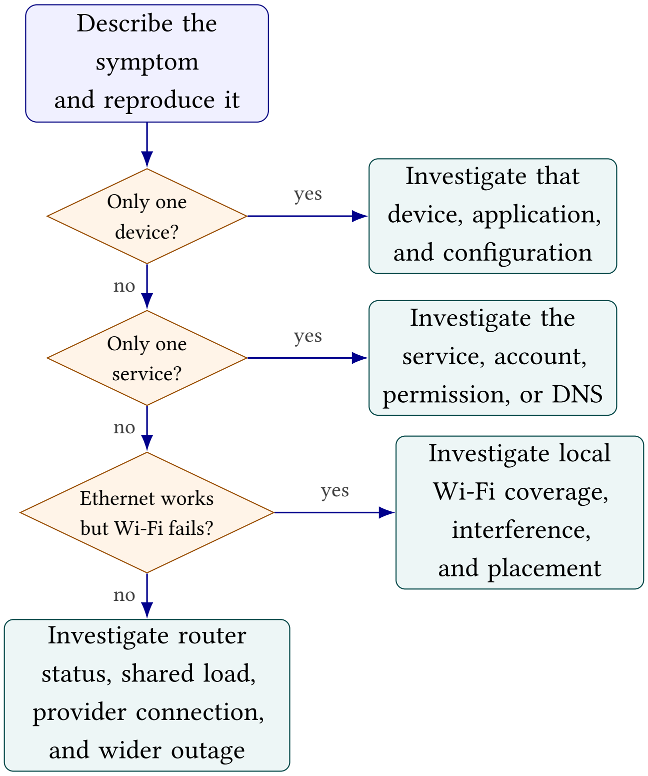

Figure 3.3: A diagnostic flow for deciding which part to investigate first. Comparisons narrow the possibilities; repeated measurements and supporting evidence are still required.

1. **Define the symptom.** Does every service fail, or only one? Is the problem a low data rate, delay, disconnection, failure to join Wi-Fi, or poor quality in one application? When and where does it occur?
2. **Compare devices.** If one phone struggles beside another working phone, examine the first device's settings, Wi-Fi capability, software, and background activity. If all devices fail together, look farther along the route.
3. **Compare places.** Test beside the access point and in the problem room. A large difference suggests local Wi-Fi coverage or interference rather than insufficient capacity in the provider's plan.
4. **Compare Wi-Fi with Ethernet where possible.** Good Ethernet performance and poor Wi-Fi performance point towards the local wireless network. Poor results on both leave the provider connection, router, shared household demand, remote test server, and device as possibilities.
5. **Compare times and activities.** A problem that appears during busy evening hours may involve household use, provider congestion, or remote service demand. A large upload can fill

the connection's limited upload capacity and interfere with a call even when a plan advertises an impressive download rate.

6. **Check the relevant part of the route.** Router status information and the provider's outage notice may help. Test another reputable remote service. If most sites work but one does not, the household's entire connection is unlikely to be the only explanation.
7. **Make the smallest justified change.** Reposition equipment, replace a damaged cable, stop an unintended transfer, update a device, or ask the provider to investigate before purchasing a faster plan or an elaborate mesh system without evidence.

Restarting equipment can clear a temporary fault, but it is not a diagnosis. Repeatedly needing to restart it is itself evidence to record. Do not press a factory-reset button casually: that operation can erase provider and household settings and may require passwords, provider details, or assistance to restore.

3.6 Fit the Local Network to the Access Connection

Diagnosis narrows the problem; design matches the parts to the work. Chapter 1 explained how to compare access technologies and plans. Once a household has selected or inherited a service, the next problem is to connect its users to that service without confusing the incoming connection with the local network. A fast access link cannot compensate for a weak radio link in a bedroom, while excellent local Wi-Fi cannot increase the capacity entering the premises.

The place where the provider's line enters may not be the best place for Wi-Fi coverage. An ONT might have to remain near the fibre entry, while equipment that receives fixed-wireless service by radio may need the part of the building with the best external signal. Where the provider's setup permits, Ethernet can carry the connection from that entry equipment to a centrally placed router. Ethernet from the router can also feed a separate access point closer to users. Where cabling is impractical, a mesh system can extend coverage, provided that its units still have good links to one another. The design should follow measurements rather than the convenience of putting every function in one box.

The incoming connection and local network must also share their capacity among the household's activities. A stable wired connection may suit a fixed workstation or a device making important calls. Mobile devices need useful coverage in the rooms where they are used. Equipment that keeps remote copies in sync or uploads large files can affect other traffic if it fills a limited link. The purpose is not to give every device its theoretical maximum at once, but to keep the household's important activities usable together.

A backup works only if its route remains available during the failure being planned for. Mobile data may back up a fixed connection, but only if it has a usable indoor signal, sufficient data, available power, and a working way to share the connection. If both services depend on the same damaged provider facility or unpowered household equipment, the apparent backup may fail with the main connection. Test the changeover before an emergency.

3.7 A Reasonably Secure Home Network

Good coverage does not make a network secure or easy to maintain. Once the basic arrangement works, concentrate on avoidable weaknesses that the household can manage:

1. Change the router's default administration password and protect the new one. Change the default administration username too if the router supports it. The administration password controls settings; it need not be the same as the password that devices use to join Wi-Fi. The United States Cybersecurity and Infrastructure Security Agency includes changing default login details among its basic protections because published or widely known defaults allow unauthorised changes [27].

2. Use the strongest current Wi-Fi security mode supported by the router and household devices, with a strong, non-default passphrase (a long Wi-Fi password). Consult the model's manual if the choice is unclear.

3. Install router and device security updates. If the router no longer receives updates, replacement may be justified even when its advertised radio speed remains adequate.

4. Disable the option to manage the router from outside the home unless it is genuinely needed and can be configured safely. Making its settings page reachable from the internet creates a different risk from allowing a household device to browse the Web.

5. Use a guest network for visitors or less-trusted connected devices when the equipment can actually keep them separate from household devices. Check the manual rather than assuming that a differently named Wi-Fi network does so.

6. Record essential settings and know who can contact the provider. Do not share passwords or publish photographs that expose labels, quick response (QR) codes, account numbers, or administrative information.

These precautions do not replace security on the devices and accounts. A safe router cannot stop a user from giving a password to a convincing fake site. Likewise, a device that has been taken over or no longer receives security updates can create risk inside a carefully configured network. The full course returns to these issues in its cybersecurity and privacy units.

3.7.1 Public Wi-Fi: Useful, but Not Yours

A public hotspot is operated by someone else and shared with people the user does not know. Someone may join a fake hotspot with a convincing name, send data through an unencrypted service, bypass a certificate warning, or leave file sharing and automatic reconnection enabled. A login page for the hotspot—called a *captive portal*—can also be imitated to collect email addresses, passwords, or payment details.

Modern HTTPS protects most ordinary website traffic much better than in the early years of public Wi-Fi. The United States Federal Trade Commission notes that public Wi-Fi is usually safe when websites use encryption, while still advising users to check HTTPS, keep devices updated, and recognise fake sites (Are public Wi-Fi networks safe?). Practical precautions remain worthwhile:

1. Confirm the exact network name with the venue. A name such as "Free Airport Wi-Fi" is not proof that the airport operates it.
2. Disable automatic joining and unnecessary file or printer sharing. Mark the connection as public or untrusted if the operating system asks.
3. Prefer mobile data or a personal hotspot for especially sensitive work when it is available. On any connection, check the domain and HTTPS before signing in, and never dismiss a certificate warning casually.
4. If an employer or school supplies a VPN, follow its instructions. A reputable consumer VPN can also keep the hotspot operator or nearby users from reading traffic carried through the VPN tunnel, but it creates a new provider that must be trusted.

The safest summary is not "public Wi-Fi is always dangerous" or "a VPN makes it safe". HTTPS, careful choice of network and website, current software, and a suitable VPN each address different risks.

3.7.2 What a VPN Changes

A virtual private network (VPN) creates a protected path, often called a *tunnel*, over existing networks. An employee may use one to reach an organisation's internal systems. A consumer VPN instead commonly sends device traffic through a commercial provider's server before it continues towards other destinations.

On an untrusted local network, a correctly configured VPN protects traffic between the device and the VPN server. People and organisations carrying data on that part of the route cannot read the protected contents. The tunnel ends at the VPN server. Remote services may then see the VPN provider's public address rather than the household's usual one.

A VPN does not make the device anonymous or the user invulnerable. Its provider becomes a new intermediary that handles the traffic and must itself be trusted. Accounts, browser cookies, identifying details from the device, payments, and behaviour can still connect activity to a person. A VPN cannot make a fraudulent website honest, correct false information, remove malware already on the device, or prevent a user from disclosing a password. It also cannot repair weak Wi-Fi; the encrypted traffic must still cross the weak radio link and may incur extra delay.

VPN traffic can look unusual even when the user is doing nothing wrong. Many customers may share the same public VPN address, and the apparent country may differ from the user's location. A site may ask for checks intended to distinguish a person from a bot, or it may block the address. Streaming services may restrict VPN use because of plan, live-event, or location rules; Netflix, for example, tells affected users to turn the VPN off and retry (Netflix VPN or proxy guidance). Google likewise notes that traffic from a shared VPN can trigger its "unusual traffic" response (Google unusual-traffic guidance). If a trusted site fails only while a consumer VPN is active, temporarily disconnecting it is a useful comparison. Do not disable an organisation-required VPN while accessing its internal systems.

HTTPS and a VPN protect different portions of a route. HTTPS protects data exchanged between the browser and the HTTPS website. A consumer VPN protects traffic between the device and the VPN server; after that server, protection such as HTTPS still matters. Neither technology guarantees that the recipient will use the disclosed data responsibly.

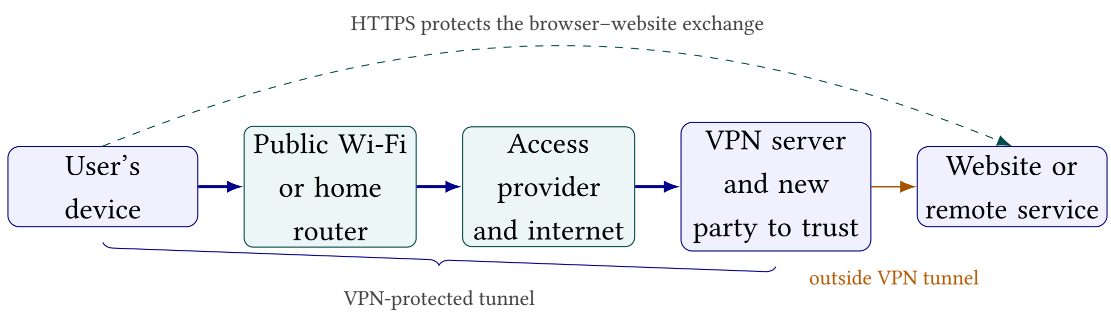

Figure 3.4: A consumer VPN changes one portion of the route. By itself, it does not protect traffic beyond the VPN server, replace HTTPS, or make the destination trustworthy.

3.8 Recommend an Arrangement, Not a Shopping List

Return to the household at the beginning of the chapter. Suppose tests show that video calls work well by Ethernet and over Wi-Fi near the router, but fail in a distant bedroom. Buying a faster provider plan is not the first justified response. Repositioning the access point, adding a properly placed access point or mesh unit, or providing a wired link addresses the evidence more directly.

Suppose instead that Ethernet and nearby Wi-Fi both deteriorate every evening while the same devices work properly through another connection. The household should document the times and measurements, check simultaneous use, and ask the provider to investigate. A new mesh system would redistribute the same poor incoming connection.

The third proposal, a VPN, answers a different question. It may protect one part of the route or provide access to an organisation's internal systems, but it cannot repair weak coverage, shared congestion, or a provider outage. It may also add delay or cause a service to challenge or block the connection. Use it for the protection or access it actually provides, not as a general cure for a slow network.

A sound recommendation should state:

1. the activities, users, rooms, devices, and budget that matter;
2. the evidence about the present bottleneck;
3. the proposed arrangement, expected benefit, and remaining limitation; and
4. the security, maintenance, and test procedures that will show whether the change worked.

The household should end up with an arrangement that suits its work and is simple enough to investigate when something fails.

3.9 Questions for Discussion and Exercises

We will work through selected exercises in class. Use the remaining questions to check your understanding of the chapter.

1. A login page uses HTTPS. Explain what the S changes, what students should check in the address bar, and why HTTPS does not prove that the page is honest.
2. Messaging works, but every website name entered in a browser produces a DNS error. Explain what DNS was trying to do and give comparisons that would help locate the problem.
3. Explain what 403, 404, and 503 usually mean. For each message, state one sensible action and one conclusion that the message does *not* justify.
4. A university website will not open. Design a short checking procedure using another site, device, connection, the university's official status page, or an independent checker. What should the student record, and why is one checker result not conclusive?
5. Compare a range extender, wireless mesh, and a wired access point for a concrete or multi-storey home. Recommend one, stating the layout, budget, cabling options, and measurements on which the choice depends.

6. A household's 300/100 Mbps fibre service delivers its advertised rates over Ethernet, but its ONT and router occupy one corner of a concrete two-storey home and upstairs calls fail. In plain language, recommend what the household should test, move, cable, or buy—and in what order. Include budget, security, backup access, and a way to verify the result. Explain how an authorised household member could find the router's settings without assuming that `192.168.1.1` is always correct.
7. A fibre connection fails. Power is on, Wi-Fi is on, PON is off, and LOS blinks red. What does this combination suggest? State what the household can check safely, what evidence it should record, and why neither a factory reset nor a new mesh system is the first response.
8. A café lists one public Wi-Fi name, but a student's phone shows two similar names. What should the student check and disable before connecting? Then assess this claim: "A VPN makes public Wi-Fi safe, hides everything I do, blocks scams and malware, and fixes a slow signal." What can a VPN protect, where does that protection end, why might it trigger a streaming error or a bot check, and what requires other safeguards?

Plain-Language Glossary

Use this glossary when a service advertisement, browser message, router label, or troubleshooting guide introduces an unfamiliar term.

Term	What it means in practice
Access point	The part that lets nearby devices join a local network by Wi-Fi; it may be built into a router, supplied as a separate unit, or form part of a mesh system.
Bandwidth or capacity	How much data a connection can carry in a given time; all users and activities sharing that connection compete for it.
Default gateway	The local router address used to reach the internet or other networks; it is often the first address to try when opening router settings.
DNS (Domain Name System)	Resolves a readable website name into the IP address needed to contact it.
Domain name	The readable name in an address, such as `example.com`; check it carefully before signing in or sending sensitive information.
Ethernet	A wired local-network connection, useful for stable device links and for comparing internet service with Wi-Fi performance.
GHz (gigahertz)	A unit used in Wi-Fi band names such as 2.4 GHz and 5 GHz; the bands differ in reach, capacity, and susceptibility to interference.
HTTP (Hypertext Transfer Protocol)	The rules a browser and Web server use to exchange ordinary Web requests and responses.
HTTPS (Hypertext Transfer Protocol Secure)	HTTP over a protected connection; it protects data in transit but does not prove that the website is honest.
IP (Internet Protocol) address	A numerical address networks use to deliver data; it can change and may be shared, so it is not a permanent identity.
ISP (internet service provider)	The company or organisation that connects the premises or mobile device to the wider internet.
IT (information technology)	The computers, software, networks, and related systems used to create, store, process, and exchange information.
LAN (local area network)	The network within a limited place such as a home; on equipment, a LAN light or port normally refers to a wired local connection.
Latency, jitter, and packet loss	Delay, variation in delay, and missing data; all three can disrupt a live call even when a download-rate test looks good.
LOS (loss of signal)	A fibre-equipment warning; red or blinking LOS commonly means that the optical signal is missing or too weak.
Mbps (megabits per second)	A unit commonly used for internet data rates; it is not the same as megabytes per second.
Modem	Equipment that converts signals for a service such as cable or a telephone-line connection; the provider may combine it with a router.
ONT (optical network terminal)	The box at the end of a fibre provider's line; it may be separate from the household router.

Continued on the next page

Term	What it means in practice
Packet	One of the small pieces in which data travels across networks; the receiving device puts the pieces together for the application.
PON (passive optical network)	The fibre network serving the ONT; a steady PON light commonly indicates that the equipment has registered with the provider.
QR (quick response) code	A square machine-readable code that can contain a network password, address, or other data; do not expose one in a photograph.
Range extender and mesh	An extender repeats an existing Wi-Fi connection; a mesh coordinates several units. Both still need good links and placement.
Router	The part that connects the local network to other networks and sends traffic in the appropriate direction; a home unit often includes Wi-Fi.
Status codes	Server replies such as 403 (access refused), 404 (page not found), and 503 (service temporarily unavailable).
VPN (virtual private network)	A protected path to a VPN server; it changes who carries and appears to send the traffic, but does not guarantee anonymity, trustworthiness, or speed.
WAN (wide area network)	On a home router, the label for the connection towards the provider rather than connections inside the premises.
Wi-Fi	A radio connection to a nearby local network. Wi-Fi is a name, not an acronym; strong Wi-Fi does not prove that internet service is working.
WLAN (wireless local area network)	Another label for the local Wi-Fi network or its indicator light.
WPS (Wi-Fi Protected Setup)	A button or code method for joining a device to Wi-Fi; its light indicates pairing, not general internet health.

Appendix A

Sample Answers to Exercises

Your answer need not match mine word for word. Several questions allow more than one answer because circumstances, priorities, and equipment differ. What matters is that your answer is accurate, relevant to the question, and clearly justified.

A.1 Chapter 1: How IT Works and Why It Matters

1. The observations entered by the student are the input. The online form may check whether required fields have been completed or convert an entered date into a standard format; this is processing. The responses may be stored in a remote database or spreadsheet. A confirmation message or summary table is an output. Sending the responses from the device to the remote system is an act of communication. The hardware may include a phone or laptop, router, network equipment, and server. The software may include the operating system, browser, online form, and database.
2. RAM holds data and instructions that programs are using at the moment. It is fast working space, and its contents are normally lost when the device is switched off. Long-term storage, such as an SSD, retains applications and files when power is removed. A computer needs RAM for active work and storage for keeping work between sessions.
3. Core counts cannot be compared in isolation because processor design, generation, cooling, software, and the kind of work all affect performance. Suitable benchmarks or tests of the student's actual applications would provide better evidence. In the example laptop, the RAM and internal SSD cannot be upgraded after purchase. The words *up to* indicate a best-case battery result under stated test conditions, not the running time that every user will obtain.
4. Apple's specification assigns 614 GB/s to the M5 Max configuration with a 40-core GPU and 460 GB/s to the configuration with a 32-core GPU. EveryMac's page for the 40-core model nevertheless gives both figures, so its 460 GB/s entry appears to be an error. The example

shows that a detailed table can still be wrong. Important specifications should be checked against a primary source and the exact model being considered.

5. Regional models may differ in SIM arrangement, battery capacity, supported network bands, and warranty coverage. In the table, some versions accept a physical Nano-SIM while another is eSIM-only, and the listed battery capacities also differ. The exact model therefore matters even when the product name is unchanged. The three rear cameras perform different optical roles. Their 48-megapixel figures cannot be added together as though they formed one 144-megapixel camera.

6. The provider's connection carries data between the home and the wider internet. Wi-Fi distributes that connection wirelessly within the home. To investigate a slow connection, test a computer through Ethernet and compare the result with Wi-Fi tests made near and far from the router. A good Ethernet result but poor distant Wi-Fi result suggests an internal wireless problem. Poor results on both may point to the service, modem or router, congestion, or another shared-network problem.

7. First convert the file size from megabytes to megabits:

   $$800\text{ MB} \times 8 = 6{,}400\text{ Mb}.$$

   The estimated download time is therefore

   $$\frac{6{,}400\text{ Mb}}{100\text{ Mb/s}} = 64\text{ s}.$$

   The actual transfer would usually take longer because of overhead, congestion, Wi-Fi conditions, and other limitations.

8. The household should examine upload rate, latency, jitter, packet loss, and performance during busy periods. It should also check whether the advertised rate is a maximum or expected range, whether capacity is shared, and whether the plan has a data allowance or fair-use threshold. Other relevant matters include availability at the exact address, installation and equipment charges, contract length, later price increases, reliability, and repair response. The importance assigned to each factor may vary among households.

9. SaaS describes how software is delivered; subscription describes how access is paid for; in these notes, freeware means software supplied without charge; and open source describes licence permissions. One product can fit several of these descriptions at once. The claim that freeware is probably malware while paid software is safe is too broad. Either can be secure or unsafe. Better evidence includes the identity and reputation of the developer, the official download

source, permissions, update history, privacy practices, independent reviews, and the ability to export files.

10. The group should begin by defining what must be recorded, which analyses are required, and how results will be shared. It should check compatibility with members' devices and required file formats; the full cost over the project; ease of use, documentation, and support; offline access; backup and recovery; and whether data can be exported in a usable form. Because biological work may involve personal, health, location, or unpublished research data, the group should also examine permissions, storage location, access controls, encryption, privacy terms, and what happens to the files when payment or institutional access ends.

A.2 Chapter 2: The Physical Foundations of Computing

1. The first phone's camera sensor records the specimen. Its processor and software construct an image, RAM holds current work, storage retains the file, and the battery powers these operations. The phone's radio sends the file through Wi-Fi or a mobile connection. Provider equipment and physical links carry it to a data centre, where account systems authorise the upload and servers and storage systems retain the file. Electricity and cooling keep that equipment operating. When the classmate opens the file, a corresponding route delivers it to the second phone. The activity could fail because the provider's cable is damaged, the remote service is unavailable, the data centre loses power, or access permission is incorrectly set, even if both phones work.
2. The three statements describe different levels of the same event. At the human and institutional level, the action fulfils an academic requirement. At the application level, software prepares and transmits a file. At the circuit level, organised changes in physical states implement the instructions. The transistors have no representation of the course rules or the social meaning of a deadline; saying they understood it would incorrectly transfer a human description to the physical level.
3. One plausible chain has minerals extracted in Countries B and C, materials refined in Country D, chips designed in Country E and fabricated in Country F, displays and batteries made elsewhere, final assembly in Country A, and sales and network services in the Philippines. Depending on the applicable labelling rule, "Made in Country A" may establish where final manufacture or a substantial transformation occurred. It does not by itself establish the origin of every material, component, design, machine, item of software, or source of economic value. Concentration occurs when one of these stages has few suppliers. It becomes a chokepoint when interruption would constrain the whole chain and substitution is slow or costly. The suppliers themselves remain interdependent because they need inputs, transport, customers, and other stages. An

inexpensive qualified connector could therefore matter more strategically than an expensive display if the connector has one supplier while several interchangeable displays are available.

4. China's leverage in this case comes from concentrated rare-earth separation, refining, and permanent-magnet production. Export licensing or restrictions can delay inputs for industries that cannot qualify another supplier quickly. China nevertheless depends on foreign semiconductor capabilities, equipment, customers, some international payment channels, and other inputs. Its leverage can weaken through new suppliers, inventories, recycling, redesign, and substitution.

   US financial leverage comes from the international use of the dollar and access to American banks and markets. Its semiconductor leverage comes from strong positions in areas such as advanced chip design, EDA and IP, together with export jurisdiction over specified chips, equipment, software, and technology. The United States still depends on foreign fabrication, specialist equipment and materials, assembly and testing, manufacturing, markets, and cooperation from other governments. Alternative payments, reduced dollar exposure, new technologies, and weaker cooperation can reduce its leverage. These are comparisons of particular links, not proof that one country controls finance, materials, or technology in every form.

5. Answers will depend on the proposed facility. A recommendation to renegotiate might require evidence about expected electricity and water demand, the source of power, jobs and training, tax concessions, ownership, data access, network resilience, environmental effects, community consultation, security review, and obligations when the facility closes. Possible safeguards include clear service and environmental standards, independent audits, Philippine legal jurisdiction, emergency and exit arrangements, worker training, transparent incentives, limits on exclusive dealing, and plans for equipment and waste. An answer recommending acceptance or rejection can also be sound if it states the evidence, alternatives, affected groups, and trade-offs rather than relying on the investor's nationality.

A.3 Chapter 3: The Internet, Web, and Home Networks

1. The S indicates that the browser is using a protected HTTPS connection. Data exchanged with the named website is encrypted while it travels, and the browser checks a certificate for that domain. The student should read the actual domain in the address bar, not rely on the page's logo or appearance, and should stop if the browser reports a certificate or private-connection warning.

   HTTPS does not certify that the organisation is honest, that its statements are true, or that it will use submitted data responsibly. A convincing scam page can also use HTTPS. The protection concerns the connection to the named site, so checking the name remains essential.

2. DNS was trying to resolve a readable website name, such as `example.com`, to an IP address that the network can contact. If the messaging application can send and receive new messages over the same connection, the device is still exchanging some data across the internet, so "the whole internet is down" is too broad a conclusion.

   Try several unrelated website names, another browser on the same device, and another device on the same Wi-Fi. Then, if available, turn Wi-Fi off on a phone and try through mobile data. If all devices on the first network show DNS errors while mobile data works, the local or provider-supplied DNS path becomes more plausible. If only one browser fails, examine that browser. If only one domain fails, the problem may belong to that service or its DNS records.

3. A 403 means that the server understood the request but refuses access. Check the account and permission or ask the owner; repeated refreshing is unlikely to help. It does not show that the entire website or connection is down.

   A 404 means that the server could not find the requested page. Check the address, open the site's home page, and search for moved material. It does not show that the whole website is unavailable.

   A 503 means that the service reports itself temporarily unavailable, often because of maintenance or overload. Wait, retry later, and check the official status page. It does not prove permanent failure or that every user and region is affected.

4. First record the exact address, browser message, and time. Check the spelling and open two unrelated sites. Try the university site on another device using the same Wi-Fi. Then try it through mobile data, which changes the local network and provider route, and may also change DNS. Check the university's official status page or announcements. If another connection is available, an independent service such as Down for Everyone or Just Me can test from elsewhere without receiving the student's login details.

   If unrelated sites also fail, investigate the device, Wi-Fi, DNS, or provider. If the university site fails on several connections and its status page or checker reports an outage, a service-side problem is more plausible. One checker result is not conclusive because it observes from a different place and may miss a regional, intermittent, or account-specific problem.

5. The recommendation depends on the building. For a concrete two-storey home that already has an Ethernet route between floors, I would use a wired access point on the second floor. The cable gives it a stable connection instead of relying on the weak Wi-Fi link between floors. Its location should be chosen from tests in the rooms where access matters.

   If cabling is impossible but a mesh unit can be placed where it still has a strong connection to the main unit, a mesh system may provide easier roaming and management. A simple extender may be the least expensive choice for one lightly used room, but it can reduce usable capacity and will not help if it is placed inside the dead zone. Before choosing, I would need the floor plan, wall materials, present signal and speed measurements, device locations, possible cabling paths, and the household's budget.

6. The Ethernet result shows that the fibre plan is already delivering its advertised rate, so buying a faster plan is not the first step. I would first test calls near the router and upstairs at several positions. If possible, I would move the Wi-Fi equipment to a more central, open location. If the ONT must remain where the fibre enters, I would use Ethernet to place the router centrally if the provider's setup permits it. If the router must remain too, Ethernet from the router can feed a centrally placed or upstairs access point.

   If cabling between floors is impossible, I would next try a mesh unit placed where it still has a good connection to the main unit. I would not place it inside the dead zone or buy several units before testing one sensible location. The budget should address the measured coverage gap rather than increase the already adequate fibre rate.

   An authorised household member can find the router address under *router* or *default gateway* in a connected device's network details, or consult the equipment label, provider instructions, or model manual. Addresses such as `192.168.0.1` and `192.168.1.1` are common examples, not guarantees. The address belongs in the browser address bar. The administration login may differ from the Wi-Fi joining password, and settings should be recorded before making a justified change.

   The household should change administrative defaults, use current Wi-Fi protection, install updates, protect the joining passphrase, and use a separated guest network if the equipment supplies real isolation. Tested mobile data could provide backup, subject to indoor signal, data allowance, battery, and household power. After installation, I would test Ethernet and Wi-Fi in every work area, repeat calls and uploads at busy times, record the observed speed and call stability, and practise changing to the backup connection.

7. Power and Wi-Fi lights show that the equipment is powered and its local radio is enabled; they do not prove that the fibre service is working. PON off with LOS blinking red commonly points to a missing or weak optical signal between the premises and provider. The household can check for an outage notice and visually check that the fibre lead has not been loosened, crushed, or sharply bent. It should record the time and photograph the light pattern before contacting the provider. It should not inspect the end of a fibre connector.

   A factory reset would erase settings without restoring a missing optical signal. A mesh system changes Wi-Fi coverage inside the premises and likewise cannot repair the provider's fibre signal. Neither change addresses the evidence.

8. The student should confirm the exact network name with café staff rather than choose the strongest or most convincing name. Before connecting, disable automatic joining and unnecessary file or printer sharing, mark the network as public if prompted, and keep the device and browser updated. For sensitive work, mobile data or a personal hotspot may be the better choice. On any connection, the student should check the website's exact domain and HTTPS and should not bypass a certificate warning.

   The claim combines several different problems. A correctly configured VPN can encrypt protected traffic between the device and the VPN server. On public Wi-Fi, this can prevent other parties on that local route from reading the protected contents, and a consumer VPN can make destinations see the VPN server's outgoing address instead of the user's usual public address.

   Protection ends at the VPN server unless another protection such as HTTPS continues it. The VPN operator must be trusted to handle the traffic, and accounts, cookies, device identifiers, payments, and disclosed personal data can still identify the user. A VPN cannot make a scam site honest, stop the user from surrendering a password, remove malware, verify information, or repair a weak Wi-Fi radio signal. Those problems require measures such as careful source and link checking, current device protection and updates, sound authentication, and better local-network coverage. A VPN may add processing and route distance, so it can sometimes make performance slightly worse rather than better. Because many customers can share one VPN address, a site may also mistake their combined traffic for automated activity and demand a bot check or block access. Streaming services may reject a VPN when its apparent location or use conflicts with their rules. If a trusted service works without the consumer VPN, that comparison identifies the likely cause; it does not show that the device or entire internet connection has failed.

Bibliography

[1] Commission on Higher Education. General education curriculum: Holistic understandings, intellectual and civic competencies. Technical Report CHED Memorandum Order No. 20, Series of 2013, Commission on Higher Education, 2013. URL https://ched.gov.ph/wp-content/uploads/2017/10/CMO-No.20-s2013.pdf.

[2] University of Cincinnati Online. What is information technology? an in-depth guide. University of Cincinnati, n.d. URL https://www.online.uc.edu/blog/what-is-information-technology.html.

[3] EveryMac.com. Apple macbook pro "m5 max" 18 cpu/40 gpu 16-inch specs. EveryMac.com, 2026. URL https://everymac.com/systems/apple/macbook_pro/specs/macbook-pro-m5-max-18-core-cpu-40-core-gpu-16-2026-specs.html.

[4] Apple Inc. Macbook pro: Technical specifications. Apple, 2026. URL https://www.apple.com/macbook-pro/specs/.

[5] GSMArena. Apple iphone 17 pro max: Full phone specifications. GSMArena.com, 2025. URL https://www.gsmarena.com/apple_iphone_17_pro_max-13964.php.

[6] Apple Inc. iphone 17 pro and iphone 17 pro max: Technical specifications. Apple Philippines, 2025. URL https://www.apple.com/ph/iphone-17-pro/specs/.

[7] Apple Inc. Identify your iphone model. Apple Support, May 2026. URL https://support.apple.com/en-gb/108044. Published 15 May 2026.

[8] David Anders and Sean Jackson. Home internet 101: Which internet connection is the best? CNET, July 2025. URL https://www.cnet.com/home/internet/internet-connection-types-explained/. Published 12 July 2025.

[9] United States Federal Trade Commission. Malware: How to protect against, detect, and remove it. Consumer Advice, April 2025. URL https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it.

[10] United States Federal Trade Commission. How websites and apps collect and use your information. Consumer Advice, September 2023. URL https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information.

[11] Kandy Wong. How china's rare earth leverage works—limits, risks and global responses. South China Morning Post, November 2025. URL https://www.scmp.com/economy/global-economy/article/3332513/how-chinas-rare-earth-leverage-works-limits-risks-and-global-responses. Published 12 November 2025; updated 13 November 2025.

[12] CGTN Europe. Semiconductors: A global supply chain powering modern life. CGTN Europe, November 2024. URL https://newseu.cgtn.com/news/2024-11-30/Semiconductors-A-global-supply-chain-powering-modern-life-1yXlImgjCPC/p.html. Published 30 November 2024.

[13] International Energy Agency. Key questions on energy and AI. Technical report, International Energy Agency, Paris, April 2026. URL https://www.iea.org/reports/key-questions-on-energy-and-ai. Published 16 April 2026.

[14] Computer History Museum. 1947: Invention of the point-contact transistor. Computer History Museum, The Silicon Engine, n.d. URL https://www.computerhistory.org/siliconengine/invention-of-the-point-contact-transistor/.

[15] United States Department of Commerce. Review of semiconductor manufacturing and advanced packaging. Technical report, United States Department of Commerce, June 2021. URL https://media.bis.gov/media/documents/100-day-supply-chain-review-report.pdf. In *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017*, pp. 21–82.

[16] Semiconductor Industry Association and Boston Consulting Group. Emerging resilience in the semiconductor supply chain. Technical report, Semiconductor Industry Association and Boston Consulting Group, May 2024. URL https://www.semiconductors.org/wp-content/uploads/2024/05/Report_Emerging-Resilience-in-the-Semiconductor-Supply-Chain.pdf.

[17] International Energy Agency. Rare earth elements: Pathways to secure and diversified supply chains. Technical report, International Energy Agency, Paris, April 2026. URL https://www.iea.org/reports/rare-earth-elements.

[18] Carol Bertaut, Bastian von Beschwitz, and Stephanie Curcuru. The international role of the U.S. dollar—2025 edition. FEDS Notes, Board of Governors of the Federal Reserve System, July 2025. URL https://www.federalreserve.gov/econres/notes/feds-notes/the-international-role-of-the-u-s-dollar-2025-edition-20250718.html. Published 18 July 2025.

[19] United States Department of the Treasury. The treasury 2021 sanctions review. Technical report, United States Department of the Treasury, October 2021. URL https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf.

[20] United States Department of Commerce, Bureau of Industry and Security. Commerce strengthens export controls to restrict China's capability to produce advanced semiconductors for military applications. Press release, December 2024. URL https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military. Published 2 December 2024.

[21] Reuters. Nvidia says U.S. has imposed new license requirement for future exports of some chips to China. Reuters, August 2022. URL https://www.reuters.com/technology/nvidia-says-us-has-imposed-new-license-requirement-future-exports-china-2022-08-31/. Published 31 August 2022.

[22] NVIDIA Corporation. Current report on form 8-K. United States Securities and Exchange Commission, August 2022. URL https://www.sec.gov/Archives/edgar/data/1045810/000104581022000146/nvda-20220826.htm. Filed 31 August 2022; date of earliest event 26 August 2022.

[23] Philippine Statistics Authority. International merchandise trade statistics of the philippines 2025. Statistical release, reference no. 2026-SSO-037, March 2026. URL https://psa.gov.ph/statistics/export-import/annual/node/1684083140.

[24] Philippine Board of Investments. DTI-BOI, NGAs eye 128k workers in PH's semiconductor industry by 2028; vow to upskill filipino workforce. Philippine Board of Investments, August 2024. URL https://boi.gov.ph/dti-boi-ngas-eye-128k-workers-in-phs-semiconductor-industry-by-2028-vow-to-upskill-filipino-workforce/. Published 6 August 2024.

[25] Internet Corporation for Assigned Names and Numbers. The domain name system. ICANN, September 2022. URL https://www.icann.org/resources/pages/dns-2022-09-13-en.

[26] United States Federal Communications Commission. Home network tips for the coronavirus pandemic. Consumer guide, March 2020. URL https://docs.fcc.gov/public/attachments/DOC-363362A1.pdf. Posted 26 March 2020.

[27] Cybersecurity and Infrastructure Security Agency. Take the first steps towards better cybersecurity with these four goals. Cybersecurity and Infrastructure Security Agency, July 2023. URL https://www.cisa.gov/news-events/news/take-first-steps-towards-better-cybersecurity-these-four-goals. Released 21 July 2023.