LESSON 69

# Network Protocols and Infrastructure

80 minutes (2 periods) | Computer Systems and Networks | Outcome 2.15 | Outcome 2.14 | Outcome 1.11 | Outcome 1.12 | Outcome 1.13

## WHAT THIS LESSON DOES

In this lesson, you'll explore the essentials of network protocols and infrastructure. Learn about HTTP, TCP/IP, and VOIP, understand the client-server model, packet transmission, and sockets, and engage in a discussion on network security challenges.

## CURRICULUM OUTCOMES

| Outcome | What the specification asks for |
|---|---|
| **2.15** | explain what is meant by the World Wide Web (WWW) and the Internet, including the client server model, hardware components and communication protocols |
| **2.14** | describe the difference between digital and analogue input |
| **1.11** | discuss the complex relationship between computing technologies and society including issues of ethics |
| **1.12** | compare the positive and negative impacts of computing on culture and society |
| **1.13** | identify important computing developments that have taken place in the last 100 years and consider emerging trends that could shape future computing technologies |

## WHAT STUDENTS SHOULD BE ABLE TO DO

- Understand the fundamental roles and functions of key network protocols like HTTP, TCP/IP, and VOIP in data communication.
- Grasp the principles of the client-server model and the process of packet transmission in networking.
- Recognise the purpose and operation of sockets as endpoints for network communication.
- Identify critical security risks in network infrastructure and explore protective measures.
- Develop an awareness of the balance between network security and usability in real-world applications.

### BEFORE THE LESSON

- This is a theory and discussion lesson, so no environment or install is needed. Have a way to project the interactives.
- Have a couple of concrete Irish examples ready to anchor abstractions: streaming on a phone, a WhatsApp call, opening a .ie website.
- Decide how you will run the security discussion in step 9: whole class, or small groups reporting back.

# Network Protocols and Infrastructure

### HOW THE LESSON RUNS

| |
|---|
| Introduction |
| Understanding Network Protocols |
| HTTP |
| TCP/IP |
| VOIP |
| The Client-Server Model |
| Packet Transmission |
| Sockets in Networking |
| Network Security Discussion |
| Wrap Up |

### TEACHING MOVES

- 2. Understanding Network Protocols. Land the core idea with the traffic-rules analogy before naming any protocol. Stress that protocols are agreements, not devices, so both ends must follow the same rules or nothing is understood.
- 3. HTTP. Emphasise stateless: each request is treated independently with no memory of the last. Walk through one request-response cycle aloud, naming GET and POST and what each is for.
- 4. TCP/IP. Do not drown them in the four layers. Fix on TCP's job (reliable, ordered delivery) versus IP's job (addressing and routing), so the split of responsibilities is clear.
- 5. VOIP. Show the pipeline: analogue voice, digitised, compressed, packetised, sent over IP. Name Zoom or WhatsApp calls so they see they already use it daily.
- 6. The Client-Server Model. Use the Netflix example, then ask who is the client and who is the server when they message a friend. Draw out that one machine can be both at different times.
- 7. Packet Transmission. Ask why break data into packets at all. Draw the answer out: efficiency and reliability over unstable links. Name the header parts (addresses, sequence numbers, error checks) by their purpose.
- 8. Sockets in Networking. Use the building-address plus door-number analogy. Nail why the port matters: it lets several applications on one device communicate at once. Point to port 80 (HTTP) and 443 (HTTPS).
- 9. Network Security Discussion. Frame threats concretely: eavesdropping, interception, DoS, man-in-the-middle. Then push the harder question, the trade-off between locking a network down and keeping it usable, and ask for real examples.

**WHAT TO WATCH FOR**

- Students think HTTP or a protocol is a physical thing, a cable or a device, rather than a set of rules both ends agree to follow. Return to the traffic-rules analogy: the rules are not the road or the car. Ask what would happen if the browser and server used different rules for the same request.
- Students assume an IP address alone is enough to reach the right program, missing why a port number is needed. Ask how one laptop can run a browser and a video call at the same time and keep the traffic separate. The port is the door number that answers this.
- Students believe packets always travel together in order along one path. Point to the sequence numbers in the header and ask why they exist. If order were guaranteed, no reassembly would be needed.

**DIFFERENTIATION**

- Emerging: Give one running example, a single web request, and trace it through every step of the lesson so the abstractions attach to one concrete story. Let them use the analogies (traffic rules, building and door) in their own words rather than the formal definitions.
- Developing: Ask them to explain the division of labour between TCP and IP back to you, in their own words, before moving on. Have them classify each security threat in step 9 as an attack on confidentiality, integrity or availability.
- Proficient: Push toward Higher Level detail: describe the request-response cycle including more HTTP methods, or the well-known port ranges and why they are reserved. Ask them to argue one side of the security versus usability trade-off with a specific scenario, the kind of reasoning useful as evidence in an Applied Learning Task.