

Lesson 08 — Networking Infrastructure

Streets, highways, and addressing — the physical + logical layer that everything else rides on.

IT Landscape

Module 2

Networks are roads

A network is just a road system. Data travels in packets — think envelopes in a postal truck.

- **Street** — the Ethernet cable from your laptop to the wall.
 - **Motorway** — the fiber-optic trunk line from your city to the next.
 - **Address** — every device has one (IP address). Every intersection has one too (MAC address).
 - **Post office** — the router. It reads the destination and forwards the packet along the best route.
-

Wired vs wireless

Type	Medium	You see it when...
Ethernet	Copper cable (Cat5/6/7)	Plugging a laptop into an office wall port
Fiber	Glass / light pulses	Your ISP digs up the street to install it
Wi-Fi	Radio waves (2.4 / 5 / 6 GHz)	The router in your living room
Cellular	Radio (4G / 5G towers)	Mobile data on your phone
Satellite	Microwave to orbit	Starlink in remote areas

Two kinds of address

MAC address

Burned into the hardware at the factory.

Like a serial number on a piece of furniture.

Works only on your **local network** (one room / one office floor).

IP address

Assigned by the network. Can change.

Like a postal address — move house, change address.

Private (192.168.x.x / 10.x.x.x) inside your home; **public** (your ISP's IP) facing the internet.

*Your home has **one** public IP but possibly dozens of private IPs. NAT (Network Address Translation) is the bouncer who manages traffic between them.*

Three network worlds

World	Typical size	Who manages it
SOHO	1–20 devices	You — after watching a YouTube tutorial
Enterprise	Hundreds → thousands of devices	A dedicated network team
Data Center	Tens of thousands of servers	NetOps team + custom firmware + 24/7 NOC

The physics are the same. The requirements — speed, redundancy, management — are wildly different.

What changes at scale

- **SOHO:** one router does everything. 1 Gbps is plenty. A 30-minute outage is annoying but survivable.
- **Enterprise:** dedicated switches, VLANs (logical segmentation), redundant uplinks, 24-hour SLA to fix failures.
- **Data center:** 100 Gbps links per rack, N+2 redundancy everywhere, fully meshed spine-leaf topology, no single cable break can drop anything.

At SOHO scale, "the router rebooted" is a root cause. At DC scale, a single reboot in a 10,000-server cluster isn't even a ticket.

VPN — what it actually is

A VPN is an encrypted tunnel punched through a public network so you can act as if you were physically inside a private one.

- **Corporate VPN** (WireGuard, Cisco AnyConnect): you connect from a coffee shop, and your laptop is “inside” the office — same resources, same firewall rules.
 - **Consumer “VPN” services** (NordVPN, ExpressVPN): reroute traffic through their servers. Hides your IP from websites; does not make you anonymous. Your VPN provider sees everything instead.
-

Tor — the real anonymizer

Tor bounces your traffic through **three volunteer relays** worldwide before it exits.

- Each relay strips one layer of encryption — like peeling an onion (hence the logo).
- No single relay knows both who you are *and* where you're going.
- Trade-off: **very slow** (3 relays, often 300 ms round-trip).

A consumer VPN moves trust from your ISP to the VPN vendor. Tor moves trust from any single party to the assumption that at least two of three relays are honest.

SD-WAN — software-defined wide area networks

The problem it solves: corporations used to buy expensive private MPLS lines to link branch offices. SD-WAN uses the public internet instead — with software that intelligently routes traffic.

- Same reliability guarantees, at a fraction of the cost.
 - Branch in a new city? Buy an SD-WAN box, plug it in, configure from a cloud dashboard in minutes.
 - Brands: **Cisco Viptela, VMware VeloCloud, Palo Alto Prisma SD-WAN.**
-

Watching the pipes

Networks are living things. Someone has to watch them.

- **NMS** (Network Management System) — polls every device for its health.
 - **SNMP** — the 1988-era protocol that reports metrics (CPU, port up/down, error counts) to the NMS. Still ubiquitous.
 - **NetFlow / sFlow** — samples actual traffic to show who's talking to whom, in how much volume.
 - **Observability tools** (Grafana + Prometheus, PRTG, SolarWinds) — dashboards, alerts, historical charts.
-

A day in NetOps

- 09:00 — review overnight NMS alerts. One switch port on Floor 3 flapping; open a ticket.
 - 10:30 — help a developer who says “something is slow”. Pull NetFlow data; show it's a misconfigured firewall rule, not the network.
 - 13:00 — push a new SD-WAN config to the new branch in Warsaw.
 - 15:00 — capacity review: two uplinks trending toward 70% utilisation; order an upgrade for next quarter.
 - 17:00 — patch firmware on edge routers in a maintenance window.
-

The mental model

Three network worlds on one canvas — see Theory page for the labeled diagram

Layer	SOHO	Enterprise	Data Center
Link speed	1 Gbps	10 Gbps	100 Gbps+
Redundancy	None (reboot to fix)	Dual uplinks	N+2, fully meshed
Management	Browser UI	CLI + dashboards	API-driven, scripted
Downtime tolerance	Minutes OK	Seconds, SLA-bound	Zero, 99.999% SLA

Common misconceptions

- **"VPN = anonymity."** No. A consumer VPN moves trust from your ISP to the VPN vendor. Tor is the closer approximation to anonymity.
 - **"Wi-Fi = internet."** Wi-Fi is the last-meter radio link. The internet is the vast public network your router connects to.
 - **"Fiber is fast because of magic."** It's fast because glass conducts light, and light doesn't heat up like copper, so you can push much more signal without signal degradation over long distances.
 - **"The network is someone else's problem."** Every application developer eventually hits a network constraint. Knowing the basics saves weeks of blaming the wrong layer.
-

Recap

- Networks are road systems. Packets are envelopes. Routers are post offices.
- Every device has two addresses: a hardware MAC and a logical IP.
- SOHO, enterprise, and data-center networks use the same physics but completely different operational disciplines.
- A VPN is an encrypted tunnel, not an anonymizer. Tor is closer to an anonymizer.
- SD-WAN replaced expensive MPLS leases with software-managed public internet links.
- Network operations means constant monitoring, alerting, and capacity planning — not just “plugging in cables.”

Coming up: Lesson 09 — Security Fundamentals (or the next lesson in Module 2).

