Teah Innovative Tech (T.I.T),
Online Summer Computer Concepts
(OSCC 2026) - 10th Edition.

COMPUTER NETWORKING: FOUNDATIONS TO PRACTICE

Day 1: Internetworking

Day 2: IP Addressing & Subnetting

Day 3: Cisco Packet Tracer Practical

" A Three-Day Training Companion Guide. Five (5) years of providing FREE Tech, Academic and Productivity Skills Training with Certification."

Prepared by:

The OSCC 2026 Team

Through:

Founder & CEO: OLANO TEAH BLOH

Empower your networking career by learning to design, optimize, and troubleshoot enterprise-grade networks through the essential trifecta of IP logic, subnet calculation, and virtual simulation.

A companion reference document for participants, to keep, revisit, and use long after the training concludes.

Table of Content

How to Use This Guide

This companion guide accompanies a three-day computer networking training program designed for a mixed audience of complete beginners and more knowledgeable participants. It is written to be read from start to finish, or used as a standing reference you return to long after the training ends.

The guide follows the same three-day structure as the live sessions. Day 1 builds your mental model of how networks and the Internet are put together. Day 2 explains how every device on a network gets a unique identity through IP addressing and subnetting. Day 3 turns that theory into a hands-on skill using Cisco Packet Tracer, including a full worked example of a three-router, three-switch network.

Every concept in this guide is explained twice: once in plain, everyday language tied to something you already use, your phone, your home Wi-Fi, your streaming service, and once in the more precise technical language you will encounter in documentation, certification exams, and on the job. Technical terms are bolded on first use and also collected in the Glossary at the end of this document, so you never have to stop and search elsewhere for a definition.

[1] **Beginners:** focus on the plain-language explanations and the “Real-World Link” boxes before working through the technical detail.

[2] **Experienced participants:** look for the “Going Deeper” boxes, which extend each topic with the detail used in real deployments and certification exams.

[3] **Everyone:** The Glossary and Appendices at the end are designed as quick-reference material for use long after this training is complete.

PART I

Day 1: Internetworking

How the digital world is connected: models, devices, topologies, and transmission media.

Chapter 1: Why Networking Is a Modern Life Skill

Every day, long before most people sit down at a desk, they have already relied on a dozen invisible networks. A phone wakes up and quietly reconnects to the home Wi-Fi network. A messaging app synchronizes new messages over the household's internet connection. A weather widget silently fetches an update. A smart speaker checks whether it has new voice-assistant instructions. A commuter's maps application streams live traffic data over the mobile network. None of this requires the person to understand what a network is, and that invisibility is precisely the point of good network design.

This training exists to make that invisible infrastructure visible. Understanding computer networking today is less like learning a specialized trade and more like learning to read a map of a city you already live in. You interact with networks dozens of times per hour, whether or not you can name a single protocol. Learning how they work turns you from a passive passenger into someone who can navigate, troubleshoot, and even design that infrastructure.

The importance of this skill has only grown with the trends shaping today's digital world: remote and hybrid work depends on secure, reliable connections to company networks; smart homes now contain dozens of connected devices, from thermostats to doorbells to refrigerators; cloud computing means that the applications and data people rely on daily often live on servers thousands of miles away, reachable only through a chain of networks; and the rise of streaming, video calls, and online gaming has made network performance , not just availability , a daily concern for ordinary users.

REAL-WORLD LINK

The next time your video call freezes or your smart TV loses connection, you are experiencing a real, physical breakdown somewhere in a chain of networking equipment, not a mysterious, unexplainable glitch. By the end of this guide, you will be able to reason about where in that chain the problem most likely sits.

What You Will Be Able to Do After This Course

[1] Explain, in plain language, how data travels from your device to a website or app and back.

[2] Identify the role of every major device in a home or small office network.

[3] Read and assign IP addresses, subnet masks, and understand what they mean.

[4] Design a simple subnetted network for a small organization.

[5] Build, configure, and troubleshoot a working network topology in Cisco Packet Tracer.

[6] Speak confidently using correct networking terminology in a workplace or interview setting.

Chapter 2: What Is a Network?

At its simplest, a network is a group of two or more devices connected together so they can share information and resources. A network can be as small as a laptop connected to a single printer, or as vast as the global Internet, which links billions of devices across every country on Earth.

Three ideas sit underneath every network, no matter its size:

[1] **Nodes:** the individual devices on the network: computers, phones, printers, servers, smart devices, and the networking equipment that connects them.

[2] **Links:** the physical or wireless connections between nodes: copper cabling, fiber-optic cabling, or radio-frequency signals such as Wi-Fi and cellular data.

[3] **Addressing:** a system for uniquely identifying every node, so that information sent across the network reaches the correct destination rather than being lost or delivered to the wrong device.

The addressing idea is worth dwelling on, because it recurs constantly throughout this course. Imagine a postal system with no house numbers or street names, letters could never reliably reach their destination. Computer networks solve the same problem with numerical addresses (covered in full in Day 2). Every device that wants to communicate reliably needs a unique address on its network, in the same way every building needs a unique postal address.

Network vs. Internetwork vs. the Internet

These three related terms are often used loosely in everyday speech, but they mean specific things in networking:

[1] **A network** is one group of connected devices, such as the Wi-Fi network in your home or the wired network in an office.

[2] **An internetwork** (the origin of the term “Internetworking” used for Day 1 of this course) is what you get when you connect two or more separate networks together, so devices on one network can reach devices on another.

[3] **The Internet** (capital “I”) is the largest internetwork in existence, a global mesh of millions of interconnected networks, run by many thousands of different organizations, all agreeing to use the same addressing and communication rules so that any device, anywhere, can reach any other device that allows it.

GOING DEEPER

Technically, no single organization “owns” the Internet. It is a voluntary, cooperative agreement among Internet Service Providers (ISPs), governments, universities, and private companies to interconnect their individual networks and follow shared technical standards, most of which are maintained by international bodies such as the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN).

Chapter 3: The OSI Model, A Shared Language for Networks

Networking equipment is built by thousands of different manufacturers, in different countries, across different decades of technology. For all of this equipment to interoperate, the industry needed a shared blueprint describing exactly what job each part of the communication process is responsible for. That blueprint is the Open Systems Interconnection model, universally known as the OSI Model.

The OSI Model breaks the entire process of network communication into seven distinct layers, stacked from the most physical and concrete (the actual electrical signal or radio wave) up to the most abstract and human-facing (the application you interact with). Each layer has one job, communicates only with the layers directly above and below it, and can be understood, built, and replaced independently of the others. This separation of concerns is why, for example, you can switch from a cabled Ethernet connection to Wi-Fi without your email application needing to be rewritten, only the lower layers change.

The Seven Layers, Explained

#	Layer	What It Actually Does	Everyday Example
7	Application	The layer closest to the user, the software generating or consuming the data.	Instagram, WhatsApp, your web browser, email client.
6	Presentation	Formats, encrypts, and compresses data so the receiving system can interpret it correctly.	How a streamed video is encoded so it plays smoothly on any device.
5	Session	Opens, manages, and closes the ongoing conversation between two devices.	Staying logged in to Gmail as you move between the inbox and settings.
4	Transport	Breaks data into manageable segments and ensures reliable, ordered delivery (or prioritizes speed when reliability matters less).	TCP guarantees a file download arrives intact; UDP favors speed for live video calls and online games.
3	Network	Handles logical addressing and routing, finding the best path across multiple networks.	IP addresses; how your data finds its way across the Internet, like a GPS route.
2	Data Link	Handles addressing and delivery within a single local network segment.	MAC addresses; how a switch delivers a frame to the correct device on your LAN.

#	Layer	What It Actually Does	Everyday Example
1	Physical	The actual transmission of raw bits as electrical signals, light pulses, or radio waves.	The Wi-Fi signal itself, an Ethernet cable, or a fiber-optic line.

REAL-WORLD LINK

A simple mailing-a-letter analogy maps neatly onto all seven layers: writing the letter (Application), choosing the language and sealing the envelope (Presentation/Session), the postal service's delivery guarantee and tracking number (Transport), the national sorting and routing system (Network), the local mail carrier who only needs to know your street (Data Link), and the truck or plane that physically carries the letter (Physical).

Encapsulation: How Data Actually Moves Through the Layers

As data travels down through the layers on the sending device, each layer wraps the data from the layer above it with its own control information, a process called encapsulation. This is similar to placing a letter (Application data) inside an envelope (Transport), then into a mail sack bound for a specific regional hub (Network), then loading that sack onto a specific delivery truck (Data Link). At each layer, the data unit gets its own name: Data at the Application/Presentation/Session layers, a Segment at the Transport layer, a Packet at the Network layer, and a Frame at the Data Link layer, before finally becoming raw Bits at the Physical layer. On the receiving device, the exact reverse process, de-encapsulation, strips away each layer's wrapper in turn until the original application data is recovered.

GOING DEEPER

Experienced network engineers often diagnose problems by “walking the model”: checking the Physical layer first (is the cable plugged in, is the light on the switch active?), then Data Link (is the device on the right VLAN, does it have a valid MAC address entry?), then Network (does it have a correct IP address and route?), and only then moving upward to Transport and Application. This layered troubleshooting approach is one of the most transferable skills in all of IT support, and it is put into direct practice during the Day 3 troubleshooting lab.

Chapter 4: The TCP/IP Model, The Version the Real World Actually Runs On

While the OSI Model is the standard teaching and reference framework, the actual set of protocols running the Internet today is described by a simpler, four-layer model: the TCP/IP Model, named after its two most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

TCP/IP Layer	Roughly Equivalent OSI Layers	Purpose
Application	Application, Presentation, Session (7–6–5)	The software and protocols end users interact with: HTTP/HTTPS (web), SMTP (email), DNS (name lookup), FTP (file transfer).
Transport	Transport (4)	End-to-end communication and reliability, via TCP (reliable) or UDP (fast, best-effort).
Internet	Network (3)	Logical addressing and routing between networks, via IP (IPv4/IPv6).
Network Access	Data Link, Physical (2–1)	Delivery of data across the physical medium of the local network.

Notice that the TCP/IP model simply merges OSI's top three layers into a single Application layer, and its bottom two layers into a single Network Access layer, while keeping Transport and Network (renamed Internet) largely intact. This is why both models are taught together: OSI gives you the precise vocabulary for troubleshooting and reference, while TCP/IP describes what is actually implemented in every operating system and router in use today.

TCP vs. UDP: Reliability vs. Speed

At the Transport layer, two protocols dominate, and the choice between them is a trade-off every application developer must make:

[1] **TCP (Transmission Control Protocol)** establishes a connection, numbers every segment of data, confirms receipt, and retransmits anything lost, guaranteeing complete, ordered, error-free delivery. It is used for web browsing, email, and file downloads, where a missing piece of data would corrupt the result.

[2] **UDP (User Datagram Protocol)** sends data with no connection setup, no guarantee of delivery, and no retransmission. It is used for live video calls, online gaming, and voice-over-IP, where a dropped packet causing a tiny glitch is far less disruptive than the delay TCP's guarantees would introduce.

REAL-WORLD LINK

This is exactly why a video call sometimes shows a brief pixelated glitch but keeps going, while a file download that loses connection simply stalls until the connection is restored. The application's chosen protocol, UDP for the call, TCP for the download, determines that behavior.

Chapter 5: Core Networking Devices

Behind every network connection sits physical hardware, each piece responsible for a specific job. Understanding what each device does, and, just as importantly, does not do, is one of the most immediately useful skills from Day 1, because it directly explains what to check when something goes wrong.

Modem

A modem (short for modulator-demodulator) converts the signal format used by your Internet Service Provider, over cable, fiber, or telephone lines, into a format your home network equipment can use, and back again. Historically this meant converting between analog and digital signals; today it more often means converting between the ISP's specific transmission technology and standard Ethernet. Without a modem, your home network has no way to communicate with the ISP's infrastructure at all.

Router

A router is the traffic director of a network. It examines the destination address of incoming data and decides the best path to send it onward, and it connects otherwise separate networks together, most commonly, your private home network and the public Internet. A home router also typically performs several additional jobs bundled into one device: assigning IP addresses to your devices (DHCP, covered in Day 2), providing Wi-Fi, and performing Network Address Translation (also Day 2) so multiple devices can share one Internet connection.

Switch

A switch connects multiple devices within a single local network and intelligently forwards data only to the specific device it is addressed to, based on that device's hardware (MAC) address. This is far more efficient than the hub it replaced (see below). Switches are the backbone of office networks, where dozens or hundreds of desktop computers, printers, and phones all need to communicate on the same local network.

Access Point

A wireless access point (AP) extends network connectivity to Wi-Fi devices, effectively acting as a bridge between the wired network and the airwaves. A home router usually has a basic access point built in; larger homes and offices add additional or mesh access points to eliminate Wi-Fi dead zones.

Firewall

A firewall is a security device (or software feature) that inspects incoming and outgoing traffic and decides, based on a defined set of rules, what is allowed to pass and what is blocked. Nearly every

home router includes a basic firewall by default, and most operating systems include a software firewall as an additional layer of defense.

Hub (Legacy Device)

A hub is the historical predecessor to the switch. Rather than intelligently forwarding data only to its intended recipient, a hub simply repeats every incoming signal out to every connected device, forcing all devices to share the same available bandwidth and increasing the chance of data collisions. Hubs are now largely obsolete, having been replaced almost entirely by switches, but understanding the difference clarifies why switches were such an important advance.

Device	Primary Job	OSI Layer
Modem	Translates ISP signal to/from a usable network format	Physical (1)
Hub (legacy)	Repeats signal to all connected ports	Physical (1)
Switch	Forwards data to the correct device on the local network	Data Link (2)
Router	Directs traffic between separate networks; assigns IP addresses	Network (3)
Access Point	Bridges wired network to Wi-Fi devices	Data Link (2)
Firewall	Filters traffic according to security rules	Varies (3–7)

REAL-WORLD LINK

A typical home setup chains these devices together: the ISP's cable or fiber line enters a modem, which connects to a router (often combined into a single “modem-router” box today), which provides Wi-Fi to phones and laptops and wired Ethernet ports for a smart TV or games console. You can see every device currently connected by logging into your router's administration page, commonly found at an address like 192.168.1.1.

Chapter 6: Network Types and Topologies

Network Types, by Scale

Networks are classified partly by their physical or geographic scale. Each type below appears constantly in daily digital life, even if the terminology is unfamiliar:

Type	Full Name	Typical Scale	Everyday Example
PAN	Personal Area Network	A few meters, around one person	Bluetooth earbuds or a smartwatch pairing with a phone
LAN	Local Area Network	One building or floor	Your home Wi-Fi network; an office network
WLAN	Wireless Local Area Network	One building or floor, wireless	The Wi-Fi portion of a LAN specifically
CAN	Campus Area Network	Several buildings, one organization	A university campus or corporate office park
MAN	Metropolitan Area Network	A city or large town	City-wide public Wi-Fi or municipal fiber networks
WAN	Wide Area Network	Regional, national, or global	The Internet itself; a bank's network linking branches nationwide

REAL-WORLD LINK

Cloud services such as Google Drive, Netflix, and Microsoft 365 are WAN-scale applications: the servers you connect to may be located on a different continent from you, reached through dozens of interconnected networks you never see.

Network Topologies, by Shape

Topology describes the physical or logical arrangement of the connections between devices on a network. The choice of topology affects cost, reliability, and how easy the network is to expand or troubleshoot.

[1] **Star Topology:** every device connects to one central device (typically a switch or router). This is the most common topology today, including nearly every home network. A single

cable failure only affects one device; if the central device fails, however, the whole network goes down.

[2] **Mesh Topology:** devices interconnect with several or all other devices, providing multiple possible paths for data and strong resilience against a single failure. Modern mesh Wi-Fi systems (such as Google Nest Wifi, Amazon Eero, or TP-Link Deco) bring this once purely enterprise concept into ordinary homes.

[3] **Bus Topology**: all devices share a single central cable. Simple and inexpensive, but a single break in the cable can bring down the entire network; this design is now mostly historical.

[4] **Ring Topology:** devices are connected in a closed loop, with data passing from device to device around the ring. Largely historical today, though the concept persists in some resilient fiber backbone designs.

[5] **Hybrid Topology:** a combination of two or more topology types, which describes most real-world corporate networks, for example, a mesh backbone connecting multiple star-topology office floors.

Chapter 7: Transmission Media, What Actually Carries the Signal

Every network link ultimately relies on a physical medium to carry its signal, even wireless ones (which use the electromagnetic spectrum, a physical resource governed by the laws of physics and by regulatory agreement between countries).

[1] **Twisted-Pair Copper Cabling (Ethernet cable):** the familiar cable with a clear plastic connector (technically called RJ45) used to connect a computer, games console, or smart TV directly to a router or switch. Twisted-pair cabling is inexpensive, easy to install, and sufficient for most home and office needs, typically supporting speeds from 100 Mbps up to 10 Gbps depending on the cable category.

[2] **Fiber-Optic Cabling:** transmits data as pulses of light through thin strands of glass or plastic rather than electrical signals through copper. Fiber supports vastly higher speeds and much longer distances without signal loss, making it the backbone of Internet Service Provider networks and increasingly common for direct-to-home Internet connections (“fiber Internet”).

[3] **Wireless (Radio Frequency):** Wi-Fi and cellular data both transmit information as radio waves through the air. Wireless offers convenience and mobility at the cost of typically lower reliability and speed compared to a direct cabled connection, and it is more susceptible to interference from physical obstacles and competing signals.

GOING DEEPER

Wi-Fi standards are named with version numbers that map to specific IEEE 802.11 specifications, for example, Wi-Fi 6 corresponds to 802.11ax. Each new generation improves speed, capacity for simultaneous devices, and efficiency, which is why a home with many connected smart devices benefits noticeably from upgrading to a newer Wi-Fi standard even without an internet speed increase from the ISP.

Chapter 8: Day 1 Summary

Day 1 built the mental model that everything else in this course rests on. In summary:

[1] A network is simply devices sharing a way to communicate, with every device given a unique address so information reaches the right destination.

[2] The OSI Model's seven layers, and the simplified four-layer TCP/IP Model, give the entire networking industry a shared language and a clean separation of responsibilities.

[3] Data is wrapped (encapsulated) with control information as it moves down through the layers on its way out, and unwrapped (de-encapsulated) as it moves back up on arrival.

[4] Modems, routers, switches, access points, and firewalls each perform a distinct, non-overlapping job in a typical network.

[5] Networks are classified by scale (PAN, LAN, MAN, WAN) and by topology (star, mesh, bus, ring, hybrid).

[6] Every network link, wired or wireless, ultimately depends on a physical transmission medium.

With this foundation in place, Day 2 turns to a question this chapter raised but did not fully answer: how, exactly, does every device get its unique address, and how do organizations design and manage those addresses at scale?

PART II

Day 2: IP Addressing & Subnetting

How every device earns a unique identity, and how networks are organized, secured, and scaled.

Chapter 9: What Is an IP Address?

An IP address (Internet Protocol address) is a numerical label assigned to every device on a network, uniquely identifying it so that data can be correctly routed to and from it. It is the modern, digital equivalent of the postal address analogy introduced in Day 1: just as a letter needs a specific street address to arrive at the correct house, a piece of network data needs a specific IP address to arrive at the correct device.

The version of IP addressing in most common use today is IPv4 (Internet Protocol version 4). An IPv4 address is written as four numbers separated by periods, called octets, such as 192.168.1.15. Each octet represents a value from 0 to 255, because each octet is actually 8 binary bits underneath the familiar decimal notation, a distinction explained fully later in this chapter.

Public IP Addresses vs. Private IP Addresses

Not every IP address is visible to the entire Internet. Addressing is split into two categories:

[1] **Public IP addresses** are globally unique and reachable from anywhere on the Internet. Your Internet Service Provider assigns one public IP address to your home router, representing your household to the outside world.

[2] **Private IP addresses** are only meaningful inside your own local network and are not directly reachable from the Internet. Every device inside your home, your phone, laptop, smart TV, receives its own private IP address from your router.

Certain address ranges are permanently reserved for private use and will never be assigned as a public address on the Internet:

Private Range	Typical Use
10.0.0.0 – 10.255.255.255	Large organizations and enterprise networks
172.16.0.0 – 172.31.255.255	Medium-sized networks
192.168.0.0 – 192.168.255.255	Home and small office networks (most common default)

REAL-WORLD LINK

Public and private addressing works like an apartment building: the building itself has one street address that couriers and visitors use to find it (your public IP), while each individual apartment has its own unit number that only matters once you are already inside the building (each device's private IP).

Chapter 10: Binary Numbers and IPv4 Structure

Although IPv4 addresses are written in familiar decimal notation for human convenience, computers and networking equipment work with them in binary, base-2 numbers made up entirely of 0s and 1s. Understanding this underlying binary structure is the key that unlocks subnetting later in this chapter.

Each of the four octets in an IPv4 address is exactly 8 bits, and each bit position represents a power of 2, counting from left to right: 128, 64, 32, 16, 8, 4, 2, 1. A bit set to 1 means that value is included in the total; a bit set to 0 means it is not. Adding up every position with a 1 gives you the decimal value of that octet.

Bit position value	128	64	32	16	8	4	2	1	= Decimal
Example A	1	1	0	0	0	0	0	0	= 192
Example B	1	0	0	0	0	0	0	0	= 128
Example C	1	1	1	1	1	1	1	1	= 255
Example D	0	0	0	0	0	0	0	0	= 0

This is why every octet in an IPv4 address can range only from 0 (all eight bits off) to 255 (all eight bits on), there are no other possible values with 8 bits. A full IPv4 address is therefore 32 bits long in total (4 octets × 8 bits), which is also why IPv4's total address space is fixed at 2^{32}, or roughly 4.3 billion possible addresses, a number that becomes important later in this chapter when we discuss IPv6.

GOING DEEPER

You very rarely need to convert full addresses by hand once you have practiced subnetting; software and even mental shortcuts (covered in Chapter 12) make this fast. What matters most is understanding that a subnet mask works by marking, in binary, exactly how many of these 32 bits are reserved for identifying the network versus identifying the individual device.

Chapter 11: Static vs. Dynamic Addressing, and DHCP

Every device needs an IP address before it can communicate, but that address can be assigned in one of two ways.

Dynamic Addressing via DHCP

DHCP (Dynamic Host Configuration Protocol) allows a router or server to automatically assign an IP address to a device the moment it joins the network, along with other essential configuration information such as the subnet mask, default gateway, and DNS server addresses (all explained later in this chapter). DHCP is the default behavior for nearly every consumer device, it is why your phone or laptop simply connects and works the instant you join a Wi-Fi network, with no manual configuration required.

DHCP assigns addresses for a limited period called a lease. When the lease expires, the device must request a renewal; if it does not, the address becomes available for another device. This lease mechanism is one reason restarting a router sometimes resolves stubborn connectivity issues, it forces every device to obtain a fresh lease and configuration.

Static Addressing

A static IP address is manually configured on a device and does not change unless someone deliberately changes it. Static addressing is used for devices that other systems need to reliably find at the same address every time, servers, network printers, security cameras, and networking equipment itself.

	Dynamic (DHCP)	Static
Assigned by	Router or DHCP server, automatically	A person, manually
Changes over time?	Can change when the lease renews	Stays fixed until manually changed
Best for	Everyday devices: phones, laptops, tablets	Servers, printers, cameras, network equipment
Setup effort	None, works automatically	Requires manual configuration and record-keeping

REAL-WORLD LINK

DHCP works like a hotel assigning you a room for the length of your stay, convenient, automatic, and returned to the pool when you leave. A static IP address is like owning a permanent apartment in that same building: always the same address, but you are responsible for maintaining it yourself.

Chapter 12: Subnet Masks and CIDR Notation

A subnet mask is a 32-bit value that works alongside an IP address to divide it into two parts: the network portion (which identifies which network a device belongs to) and the host portion (which identifies that specific device within the network). It uses the same four-octet, dotted-decimal format as an IP address, but its job is entirely different, it is a mask, not a destination.

In a subnet mask, a binary 1 marks a bit position as belonging to the network portion, and a binary 0 marks a bit position as belonging to the host portion. The most common subnet mask, 255.255.255.0, is 24 ones followed by 8 zeros in binary, meaning the first three octets identify the network, and the last octet identifies individual devices, allowing up to 254 usable host addresses on that network.

CIDR Notation: A Shorthand Everyone Uses

Writing out a full subnet mask like 255.255.255.0 is precise but cumbersome. CIDR notation (Classless Inter-Domain Routing) abbreviates it by simply stating how many bits are set to 1, written as a slash followed by that number directly after the IP address, for example, 192.168.1.0/24. You will see CIDR notation used almost universally in real-world network documentation, router configuration, and cloud platforms.

CIDR	Subnet Mask	Host bits	Usable Hosts per Network
/24	255.255.255.0	8	254
/25	255.255.255.128	7	126
/26	255.255.255.192	6	62
/27	255.255.255.224	5	30
/28	255.255.255.240	4	14
/29	255.255.255.248	3	6
/30	255.255.255.252	2	2 (used for point-to-point router links)

Why Organizations Subnet Their Networks

Subnetting, dividing one larger network into several smaller ones, is not just an academic exercise. Real organizations subnet their networks for concrete, practical reasons:

[1] **Security segmentation:** keeping a Finance department's traffic separate from a Guest Wi-Fi network, so guests cannot reach sensitive internal systems even if they are on the same building's network.

[2] **Performance:** smaller networks mean less broadcast traffic competing for the same bandwidth, keeping each segment responsive.

[3] **Organization and manageability:** subnets often mirror a company's physical or departmental structure, making the network easier to document, secure, and troubleshoot.

[4] **Efficient use of address space:** allocating only as many addresses as a segment actually needs, rather than wasting an entire large block on a small department.

REAL-WORLD LINK

Subnetting an office network is much like dividing a single large office building into departments or floors: everyone still belongs to the same overall building, but Sales cannot casually wander into Finance's server room, and if Sales has a problem, it does not slow down Engineering's network traffic.

Chapter 13: Subnetting Step by Step: Worked Examples

This chapter walks through the actual calculations behind subnetting, building from a simple example to a slightly more advanced one. The goal is pattern recognition: once you have worked through a handful of examples, the math becomes fast and mechanical.

Worked Example 1: 192.168.10.0 /26

A /26 network uses 26 bits for the network portion, leaving 6 bits for hosts. Six host bits give $2^6 = 64$ total addresses in the block, of which the very first (the network address) and the very last (the broadcast address) cannot be assigned to a device, leaving 62 usable host addresses.

Element	Value	Explanation
Subnet mask	255.255.255.192	/26 in dotted-decimal form
Network address	192.168.10.0	Identifies the subnet itself; not assignable to a device
First usable host	192.168.10.1	The first assignable address, often given to the router/gateway
Last usable host	192.168.10.62	The last assignable address
Broadcast address	192.168.10.63	Used to send data to every device on the subnet; not assignable
Usable hosts	62	2^6 total addresses, minus 2 reserved

Worked Example 2: Subnetting a Small Business Network

Consider a small business that has been allocated the network 192.168.20.0/24 and needs to create three separate subnets: a staff network (up to 50 devices), a point-of-sale till system (up to 10 devices), and a guest Wi-Fi network (up to 25 devices). Rather than using one flat /24 network, dividing it into appropriately sized subnets keeps each segment isolated and avoids wasting address space.

Segment	Devices Needed	Suggested Subnet	Usable Hosts
Staff network	up to 50	192.168.20.0/26	62
Point-of-sale system	up to 10	192.168.20.64/28	14
Guest Wi-Fi	up to 25	192.168.20.80/27	30

Each subnet is sized just large enough to comfortably fit its devices with some room for growth, without wastefully allocating a full /24 (254 addresses) to a segment that only needs ten.

GOING DEEPER

This technique of using different-sized subnets across one address block, rather than one uniform size everywhere, is called VLSM (Variable Length Subnet Masking). VLSM is standard practice in real-world enterprise networks and is directly tested on certification exams such as CompTIA Network+ and Cisco's CCNA.

A Quick Method for Everyday Subnetting

A practical shortcut many networks professionals use: the “block size” of a subnet mask's interesting octet is 256 minus the mask value in that octet. For example, a /27 network has a mask of 255.255.255.224, so the block size is 256 − 224 = 32. That means every subnet boundary falls on a multiple of 32 in the final octet: 0, 32, 64, 96, 128, 160, 192, 224. This single trick lets you quickly identify network addresses, broadcast addresses, and usable ranges without working through full binary conversions every time.

Chapter 14: NAT: Network Address Translation

A typical household today may have ten, twenty, or more Internet-connected devices, yet an ISP issues only a single public IP address per household. Network Address Translation (NAT) is the technology that resolves this mismatch, allowing every private device behind a router to share that one public address when communicating with the outside Internet.

When a device on your private network sends a request to the Internet, your router rewrites the source address from the device's private IP to the router's own public IP, and keeps a temporary record of which internal device made that request. When the response comes back, the router consults that record and forwards the reply to the correct internal device. A specific variant of this process, PAT (Port Address Translation), also tracks port numbers so that many internal devices can share the single public IP simultaneously without their traffic being confused with one another.

REAL-WORLD LINK

NAT functions like a company receptionist: every outside call reaches the same published main number, and the receptionist privately routes each call to the correct internal extension. Callers outside never need to know each employee's direct line, they only ever see the one public number.

NAT also provides an incidental security benefit: because internal private addresses are never directly exposed to the Internet, devices on the outside cannot initiate a connection directly to a device inside your home network unless you deliberately configure the router to allow it (a practice called port forwarding).

GOING DEEPER

NAT was originally introduced as a stop-gap measure to slow the exhaustion of the limited IPv4 address space, and it succeeded well beyond its original expectations, it remains standard on virtually every home and business router today, even as IPv6 (which does not require NAT, due to its enormous address space) becomes more widespread.

Chapter 15: The Default Gateway and DNS

The Default Gateway

A default gateway is the address of the device, almost always a router, that a device sends its traffic to whenever the destination is outside its own local network. Every device on a network is configured (usually automatically, via DHCP) with a default gateway address, typically the router's own private IP address, such as 192.168.1.1.

When your laptop wants to reach a website, it first checks whether the destination address is on its own local network. If not, it hands the traffic to its default gateway, which then takes responsibility for routing that traffic onward toward its destination, potentially through many other routers along the way.

DNS: The Internet's Phone Book

Computers communicate using numerical IP addresses, but humans remember names far more easily than numbers. DNS (Domain Name System) is the service that translates human-friendly domain names, such as www.example.com, into the numerical IP address the underlying network actually needs to establish a connection.

Every time you type a website address into a browser, your device sends a DNS query, usually to a DNS server operated by your ISP or a public provider, asking for the IP address associated with that name. Only once it receives that numerical answer can your device actually initiate the connection to the website's server.

REAL-WORLD LINK

DNS is precisely why you can type “youtube.com” instead of memorizing a string of numbers, and it is also a common source of everyday connectivity confusion: if DNS fails but the underlying network connection is fine, you may see a browser error even though your Internet connection technically still works, a distinction that helps explain why “the Wi-Fi” and “the Internet” are not always the same problem.

Chapter 16: IPv6: The Future, Already Here

IPv4's roughly 4.3 billion possible addresses seemed inexhaustible when the protocol was designed in the early 1980s. It has not kept pace with a world of billions of smartphones, and an ever-growing universe of connected televisions, wearables, vehicles, and household appliances. IPv6 (Internet Protocol version 6) was developed specifically to solve this scarcity, permanently.

An IPv6 address is 128 bits long, compared to IPv4's 32 bits, written as eight groups of four hexadecimal digits separated by colons, for example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. This provides approximately 340 undecillion addresses (340 followed by 36 zeros), for practical purposes, an inexhaustible supply, enough to assign a vast number of unique addresses to every person on Earth many times over.

	IPv4	IPv6
Address length	32 bits	128 bits
Written as	Decimal (e.g., 192.168.1.1)	Hexadecimal (e.g., 2001:0db8::1)
Total address space	~4.3 billion	~340 undecillion
NAT typically required?	Yes, in most home/business networks	No, enough addresses for every device directly

IPv6 is not a future technology still being rolled out, it is already active today across most major mobile carriers and cloud providers, and increasingly on home ISP connections. Most modern devices support both IPv4 and IPv6 simultaneously (called dual-stack), quietly using whichever is available without any visible difference to the end user.

GOING DEEPER

Because IPv6 provides such an enormous address space, it eliminates the practical need for NAT, every device can have its own true, globally unique address. This actually restores the original end-to-end design principle of the early Internet, though it also means network security design must rely more heavily on firewalls rather than NAT's incidental address-hiding effect.

Chapter 17: Day 2 Summary

Day 2 gave every device on a network its own identity, and gave you the tools to design that identity system deliberately. In summary:

[1] **An IP address** is a unique numerical identifier for a device; public IPs face the Internet; private IPs live inside your own network.

[2] **IPv4 addresses** are 32-bit numbers written in decimal; understanding the underlying binary is the foundation of subnetting.

[3] **DHCP** automatically leases IP addresses to devices; static addresses are manually and permanently assigned.

[4] **A subnet mask** (or its CIDR shorthand, like /24) divides an address into a network portion and a host portion, and organizations subnet their networks for security, performance, and manageability.

[5] **NAT** allows many private devices to share one public IP address; the default gateway routes traffic leaving the local network; DNS translates human-friendly names into IP addresses.

[6] **IPv6** permanently solves IPv4's address scarcity with a 128-bit address space, and is already in widespread use today.

With addressing and subnetting now understood conceptually and mathematically, Day 3 puts every idea from the first two days into practice, building and configuring real network topologies inside Cisco Packet Tracer.

PART III

Day 3: Cisco Packet Tracer Practical

From theory to hands-on practice: building, configuring, and troubleshooting real network topologies.

Chapter 18: From Theory to Practice

Everything covered across Day 1 and Day 2, layers, devices, IP addresses, subnets, has, until now, been invisible and conceptual. Day 3 changes that. Using Cisco Packet Tracer, a free network simulation tool, you will build real network topologies, assign real addressing schemes, configure real router and switch commands, and watch data packets travel across your own network step by step.

REAL-WORLD LINK

Packet Tracer plays the same role for network engineers that a flight simulator plays for pilots: a safe, realistic environment to practice on before touching real, live infrastructure that could disrupt an actual business network if misconfigured.

What Is Cisco Packet Tracer?

Packet Tracer is a network simulation and visualization tool developed by Cisco, freely available through the Cisco Networking Academy. It allows you to drag and drop realistic virtual routers, switches, PCs, servers, and cabling onto a workspace, configure them using the same command-line syntax as real Cisco hardware, and then simulate live network traffic to see exactly how it behaves. It is used in classrooms and certification training worldwide, precisely because it removes both the cost and the risk of practicing on physical equipment.

Chapter 19: Orientation to the Packet Tracer Interface

Before building anything, it helps to understand the workspace itself.

[1] **Device categories**, along the bottom-left of the screen: End Devices (PCs, laptops, servers, printers), Switches, Routers, and Connections (the cables used to link devices together).

[2] **The workspace**, the large central canvas where you place and arrange devices by dragging them from the device categories.

[3] **Realtime Mode**, the default mode, where the simulated network behaves continuously, just as a real network would.

[4] **Simulation Mode**, which pauses time and lets you step through individual packets of data one event at a time, watching exactly how they move through the network and are handled at each device, an extraordinarily useful way to see the OSI Model's encapsulation process happen visually, rather than just reading about it.

Cabling: Connecting Devices Correctly

Packet Tracer, like real networking equipment, offers different cable types for different jobs: copper straight-through cables (used to connect dissimilar devices, such as a PC to a switch), copper crossover cables (historically used to connect similar devices, such as switch to switch, though most modern hardware auto-detects and no longer requires this distinction), and serial cables (used for the point-to-point WAN-style links between routers, such as in the case study later in this chapter). If you select the wrong cable, Packet Tracer will typically indicate the connection is not valid, giving you immediate, safe feedback, something a real production network would not so gently forgive.

Chapter 20: Building Your First Simple Network

Before attempting the full three-router case study later in this chapter, it is worth building a minimal network first, to become comfortable with the workflow.

1. Place two PCs and one switch onto the workspace, and use straight-through cables to connect each PC to the switch.
2. Click each PC, open its Desktop tab, and assign a static IP address in the same subnet to each, for example, 192.168.1.10/24 and 192.168.1.11/24, applying the addressing knowledge from Day 2.
3. Open a Command Prompt on one PC and test connectivity to the other using the ping command, for example: ping 192.168.1.11. A series of successful replies confirms the two devices can communicate.
4. Add a router to the workspace, and connect a second switch and pair of PCs on a second subnet, such as 192.168.2.0/24, to simulate two separate departments or office branches.
5. Configure an IP address on each of the router's connected interfaces, matching each attached subnet, and enable each interface, covered step by step in the case study that follows.
6. Set each PC's default gateway to its router interface's address, then test connectivity across the two subnets with ping. Successful replies confirm that the router is correctly forwarding traffic between the two separate networks.

GOING DEEPER

At every step, notice which Day 1 concept is in play: the switch operates using MAC addresses at the Data Link layer, while the router uses the IP addressing scheme from Day 2 to forward traffic at the Network layer. Building the network makes this layered division of labor concrete rather than abstract.

Chapter 21: Case Study: A Three-Router, Three-Switch Network

This case study is the centerpiece of Day 3. It brings together everything from Days 1 and 2 into a single, realistic small-enterprise topology: three routers, each serving its own local network through its own switch, with the three routers fully interconnected so that every device on every network can reach every other device, exactly the kind of design used by a small business with three branch locations, or three departments each requiring their own subnet.

Topology Overview

Router1, Router2, and Router3 are connected to one another in a triangle, using three separate point-to-point serial links. Each router additionally connects, through its own switch, to a small local area network of end devices. This gives the topology three separate LANs and three WAN links between the routers, for six network segments in total.

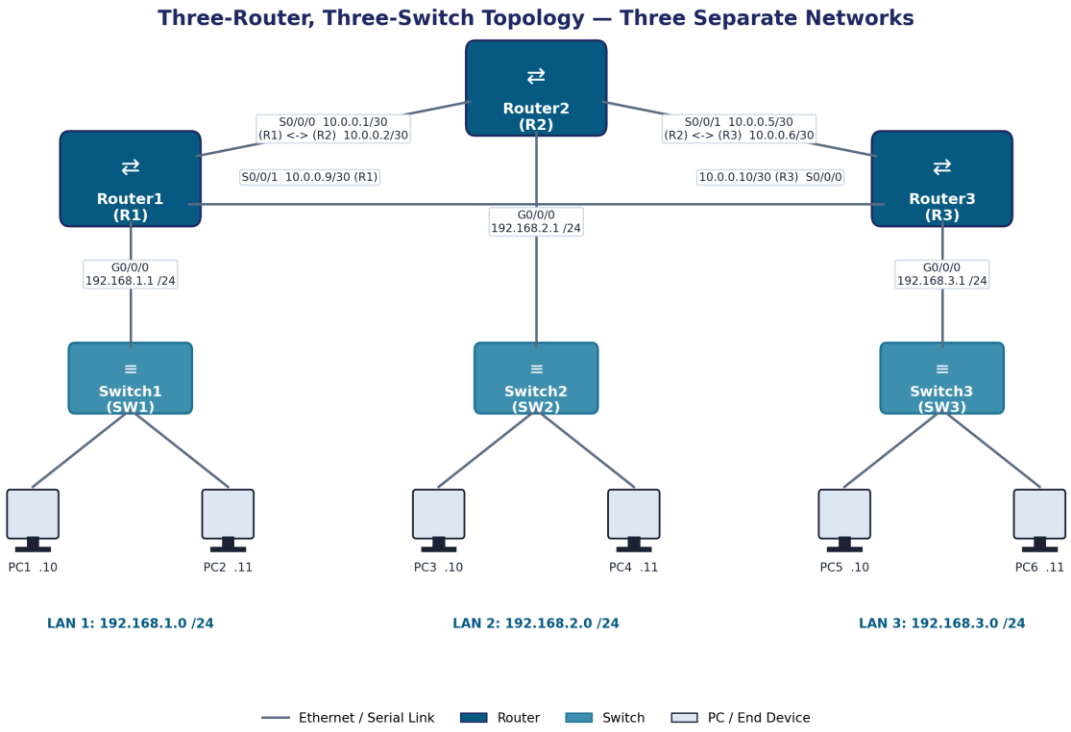

Figure 21.1, Three-router, three-switch topology with three separate LANs, fully interconnected by point-to-point links between routers.

The IP Addressing Plan

Following Day 2's subnetting principles, this design uses two different address blocks for two different purposes: a /24 network for each LAN (which needs to comfortably support many end devices), and small /30 networks for each router-to-router link (which, as covered in Chapter 12, needs exactly two usable addresses, one for each end of the point-to-point connection).

Segment	Network	Assigned Addresses
LAN 1 (behind Router1)	192.168.1.0/24	R1 G0/0/0: .1 - PC1: .10 - PC2: .11
LAN 2 (behind Router2)	192.168.2.0/24	R2 G0/0/0: .1 - PC3: .10 - PC4: .11
LAN 3 (behind Router3)	192.168.3.0/24	R3 G0/0/0: .1 - PC5: .10 - PC6: .11
Link R1 – R2	10.0.0.0/30	R1 S0/0/0: 10.0.0.1 - R2 S0/0/0: 10.0.0.2
Link R2 – R3	10.0.0.4/30	R2 S0/0/1: 10.0.0.5 - R3 S0/0/0: 10.0.0.6
Link R1 – R3	10.0.0.8/30	R1 S0/0/1: 10.0.0.9 - R3 S0/0/1: 10.0.0.10

GOING DEEPER

Notice that each router's LAN-facing interface (G0/0/0) is given the first usable address in its subnet (.1), a common real-world convention that makes documentation and troubleshooting easier, anyone reading the plan can immediately guess that a .1 address is likely a gateway. Each PC is then assigned the default gateway matching its own router's LAN interface.

Step-by-Step Build in Packet Tracer

1. Place three routers, three switches, and six PCs (two per switch) onto the workspace, arranged as shown in Figure 21.1.
2. Connect each router to its own switch using a straight-through copper cable, and connect each switch to its two PCs, also with straight-through copper cables.
3. Connect the three routers to one another using serial cables (Router1 to Router2, Router2 to Router3, and Router1 to Router3), matching the WAN links in the addressing plan.
4. Open each router's Command Line Interface (CLI) tab and configure its interfaces, using the commands in the configuration reference below.
5. Assign each PC a static IP address, subnet mask, and default gateway matching the addressing plan table.
6. Configure routing between the three routers so that each router knows how to reach the other two LANs (see the routing section below).
7. Verify full connectivity: every PC should be able to successfully ping every other PC, on every LAN, across the entire topology.

Router Configuration Reference (Router1 Example)

The following commands, entered in Packet Tracer's router CLI (accessed by clicking a router, then its CLI tab), configure Router1's interfaces. The same pattern applies to Router2 and Router3, substituting each router's own addresses from the addressing plan table.

```
Router> enable
Router# configure terminal
Router(config)# hostname Router1
Router1(config)# interface GigabitEthernet0/0/0
Router1(config-if)# ip address 192.168.1.1 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial0/0/0
Router1(config-if)# ip address 10.0.0.1 255.255.255.252
Router1(config-if)# clock rate 64000
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial0/0/1
Router1(config-if)# ip address 10.0.0.9 255.255.255.252
Router1(config-if)# no shutdown
Router1(config-if)# exit
```

A short explanation of each command: enable moves from user mode into privileged mode, unlocking configuration access. configure terminal enters global configuration mode. hostname simply renames the router for clarity. interface selects a specific physical port to configure. ip address assigns that interface's IP address and subnet mask. no shutdown activates the interface (Cisco interfaces are administratively disabled by default until this command is issued). clock rate is required only on one end of a serial link in a simulated environment, to provide timing for the connection.

Routing Between the Three Networks

Configuring IP addresses on each interface alone is not enough, each router also needs to know how to reach the LANs that are not directly connected to it. For a small, stable topology like this one, static routes (manually defined paths) are simple and effective. On Router1, for example, static routes are needed to reach LAN 2 and LAN 3:

```
Router1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
Router1(config)# ip route 192.168.3.0 255.255.255.0 10.0.0.9
```

Each static route tells Router1: “to reach this destination network, send the traffic to this next-hop address.” The equivalent routes must be added on Router2 and Router3 as well, so that every router knows a path to both of the LANs it does not directly serve.

GOING DEEPER

In real enterprise networks with many routers, administrators typically use a dynamic routing protocol, such as OSPF (Open Shortest Path First), instead of static routes, so that routers automatically learn and adjust paths as the network changes, without requiring manual updates. Static routing, used here, is the clearest way to first learn the underlying concept before adding that additional layer of automation.

Verifying the Network

Once every router is configured, connectivity should be verified methodically, from the bottom up, directly echoing the layered troubleshooting approach introduced in Day 1:

[1] On each router, use show ip interface brief to confirm every interface shows a status of “up/up” and the correct IP address.

[2] From each PC, ping its own default gateway first, to confirm the local LAN connection is working.

[3] From each PC, ping a PC on a different LAN, to confirm end-to-end routing across the entire topology.

[4] Switch to Simulation Mode and send a single ping between two PCs on different LANs, then step through its event by event, watching the packet pass from PC to switch to router, across the correct serial link, to the destination router, switch, and finally PC, a direct, visual payoff of the OSI encapsulation process covered in Chapter 3.

Chapter 22: DHCP and NAT Inside Packet Tracer

The three-router case study used static IP addressing throughout, which is appropriate for routers, switches, and servers. In a real deployment, however, end-user devices on each LAN would typically receive their addresses automatically. Packet Tracer lets you configure a router as a DHCP server for its attached LAN, using commands such as the following on Router1:

```
Router1(config)# ip dhcp pool LAN1-POOL
Router1(dhcp-config)# network 192.168.1.0 255.255.255.0
Router1(dhcp-config)# default-router 192.168.1.1
Router1(dhcp-config)# dns-server 8.8.8.8
Router1(dhcp-config)# exit
Router1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
```

Once configured, any PC on that LAN set to “obtain an IP address automatically” in its Desktop settings will immediately receive an address, gateway, and DNS server from the router, the same automatic process covered conceptually in Chapter 11, now made visible in the simulator.

NAT can similarly be simulated by connecting one router to an outside “Internet” cloud or ISP-representing router, then configuring NAT/PAT so that internal, private LAN addresses are translated to a single outside-facing address before leaving the network, directly demonstrating the receptionist analogy from Chapter 14.

REAL-WORLD LINK

This is exactly the process that occurred automatically on your own phone this morning when it joined a Wi-Fi network and instantly had Internet access. Having now configured it yourself, line by line, that automatic process is no longer a mystery.

Chapter 23: Troubleshooting Methodology

Diagnosing a broken network is, day to day, the single most common task for junior IT and network support staff, and it is a skill directly transferable to fixing problems on your own home or small-office network. A structured troubleshooting lab, using a deliberately broken version of a network such as the case study above, is one of the most valuable exercises in this entire course.

Typical faults introduced in a training exercise, and the layer each corresponds to, include:

Fault	OSI Layer	How to Detect It
Cable unplugged or wrong port used	Physical (1)	Interface status shows “down/down” in show ip interface brief
Interface left administratively disabled	Physical (1)	Interface status shows “administratively down”; fixed with no shutdown
Incorrect VLAN or switchport configuration	Data Link (2)	Devices on the same physical switch cannot reach each other
Wrong IP address or subnet mask	Network (3)	Device believes a reachable host is on a different network
Missing or incorrect default gateway	Network (3)	Local network works, but nothing outside it is reachable
Missing static route	Network (3)	One specific remote network is unreachable while others work fine

The recommended approach, directly echoing Day 1's “walk the model” principle, is to check strictly from the bottom up: confirm the physical connection and interface status first, then addressing and local delivery, then routing between networks, and only then consider anything higher up the stack. Working top-down, or jumping straight to guesses, wastes far more time than this disciplined, layer-by-layer method.

Chapter 24: Capstone Project and Real-World Pathways

Suggested Capstone Scenarios

To consolidate every skill from all three days, participants are encouraged to design and build one of the following scenarios independently, applying the full workflow demonstrated in the case study: plan the addressing scheme, build the topology, configure every device, and verify connectivity end to end.

[1] A small retail shop, with staff PCs, a point-of-sale system, staff Wi-Fi, and guest Wi-Fi, each isolated on its own subnet.

[2] A small office with two departments requiring segmented, routed networks, plus a shared network printer reachable from both.

[3] An expanded version of this chapter's three-router case study, adding a fourth router and LAN, and switching from static routes to a dynamic routing protocol such as OSPF.

Where These Skills Lead

The concepts and hands-on skills built across these three days form the direct foundation for several practical paths, whether the goal is purely personal or professional:

[1] **Everyday life:** confidently setting up, securing, and troubleshooting your own home network and the growing number of smart devices in it.

[2] **IT and helpdesk support:** diagnosing and resolving connectivity issues is one of the most common responsibilities in entry-level IT roles.

[3] **Cybersecurity:** a solid understanding of addressing, traffic flow, and network segmentation is the foundation on which all network defense is built.

[4] **Formal certification:** this course's content maps directly onto the foundational knowledge assessed by CompTIA Network+ and the early modules of Cisco's CCNA (Cisco Certified Network Associate) certification, for those who wish to continue their study formally.

Chapter 25: Day 3 and Course Summary

Day 3 closed the loop opened on Day 1: the OSI Model, IP addressing, and subnetting were no longer abstract diagrams, but working configuration commands on real (simulated) routers, moving real (simulated) traffic between real, correctly subnetted networks.

[1] Cisco Packet Tracer provides a safe, realistic environment to build, configure, and break networks without any of the cost or risk of physical hardware.

[2] A working network requires correct cabling, correct interface addressing, and, when multiple networks are involved, correct routing between them, static routes for small, stable topologies, dynamic protocols such as OSPF for larger ones.

[3] The three-router, three-switch case study in this chapter demonstrated a complete, realistic small-enterprise design, from addressing plan through configuration to verification.

[4] Structured, layer-by-layer troubleshooting is the single most transferable skill from this entire course, applicable to any network problem you will ever encounter, at any scale.

Across all three days, this course has aimed to make the invisible infrastructure behind every day digital life visible, understandable, and , above all , usable. The Glossary and Appendices that follow are intended as a lasting reference, to be revisited long after this training concludes, whenever a term needs a quick refresher or a subnetting calculation needs to be double-checked.

Glossary of Networking Terms

Every technical term introduced across the three days of this course, collected here for quick reference.

Term	Definition
Access Point (AP)	A device that extends network connectivity to Wi-Fi devices, bridging the wired network and wireless signals.
Bandwidth	The maximum rate at which data can be transferred across a network link, usually measured in bits per second (Mbps, Gbps).
Bit	The smallest unit of digital data, either a 0 or a 1.
Broadcast Address	The last address in a subnet, used to send data to every device on that subnet simultaneously; not assignable to a single device.
CIDR (Classless Inter-Domain Routing)	A shorthand notation for subnet masks, written as a slash followed by the number of network bits, e.g., /24.
Data Link Layer	OSI Layer 2, responsible for delivering data within a single local network segment using MAC addresses.
Default Gateway	The router address a device sends traffic to when the destination is outside its own local network.
DHCP (Dynamic Host Configuration Protocol)	A protocol that automatically assigns IP addresses and network configuration to devices joining a network.
DNS (Domain Name System)	The service that translates human-readable domain names into numerical IP addresses.
Encapsulation	The process of wrapping data with additional control information as it moves down through the OSI layers before transmission.
Ethernet	The dominant standard for wired local area networking, defining cabling, connectors, and how devices share the medium.
Firewall	A device or software feature that filters network traffic according to a defined set of security rules.
Frame	The unit of data at the Data Link layer, including MAC address information.
Gateway	See Default Gateway.

Term	Definition
Hub	A legacy Physical-layer device that repeats incoming signals to every connected port, now largely replaced by switches.
Internet	The global internetwork connecting millions of individually operated networks using shared addressing and communication standards.
Internetwork	Two or more separate networks connected together so that devices on each can communicate.
IP Address	A numerical label uniquely identifying a device on a network, used for routing data to the correct destination.
IPv4	Internet Protocol version 4; uses 32-bit addresses written in dotted-decimal notation, e.g., 192.168.1.1.
IPv6	Internet Protocol version 6; uses 128-bit addresses written in hexadecimal, providing a vastly larger address space than IPv4.
LAN (Local Area Network)	A network confined to a small physical area, such as a home or single office building.
Lease (DHCP)	The limited time period for which a DHCP-assigned IP address remains valid before it must be renewed.
MAC Address	A hardware address permanently assigned to a network interface, used for local delivery at the Data Link layer.
Mesh Topology	A network design in which devices interconnect with several or all other devices, providing multiple paths and strong resilience.
Modem	A device that translates an ISP's transmission signal into a format usable by home network equipment, and vice versa.
NAT (Network Address Translation)	A technique allowing multiple private devices to share a single public IP address for Internet access.
Network	A group of two or more devices connected to share information and resources.
Network Address	The first address in a subnet, identifying the subnet itself; not assignable to a single device.
Network Layer	OSI Layer 3, responsible for logical addressing and routing between networks, primarily via IP.
Node	Any individual device connected to a network.

Term	Definition
OSI Model	A conceptual seven-layer framework describing the distinct responsibilities involved in network communication.
Packet	The unit of data at the Network layer, including source and destination IP addresses.
Packet Tracer	A free network simulation tool developed by Cisco, used to build, configure, and test virtual network topologies.
PAN (Personal Area Network)	A very short-range network, typically around a single person, such as Bluetooth-connected devices.
PAT (Port Address Translation)	A variant of NAT that also tracks port numbers, allowing many devices to share one public IP simultaneously.
Physical Layer	OSI Layer 1, responsible for the transmission of raw bits as electrical signals, light, or radio waves.
Port (Networking)	A numbered endpoint used to distinguish multiple simultaneous connections or services on the same device.
Port Forwarding	A router configuration that allows a specific external request to reach a specific device inside a private network.
Presentation Layer	OSI Layer 6, responsible for formatting, encrypting, and compressing data between systems.
Private IP Address	An IP address valid only within a local network, not directly reachable from the public Internet.
Protocol	An agreed-upon set of rules governing how devices communicate.
Public IP Address	A globally unique IP address reachable from anywhere on the Internet.
Ring Topology	A largely historical network design in which devices are connected in a closed loop.
Router	A device that directs traffic between separate networks and determines the best path for data to travel.
Session Layer	OSI Layer 5, responsible for opening, managing, and closing an ongoing conversation between two devices.
Star Topology	A network design in which every device connects to one central device, such as a switch; the most common topology today.

Term	Definition
Static IP Address	An IP address manually and permanently assigned to a device, rather than automatically leased.
Subnet	A smaller network created by dividing a larger network's address space.
Subnet Mask	A 32-bit value that, paired with an IP address, defines which portion identifies the network and which identifies the host.
Subnetting	The practice of dividing one network into multiple smaller networks.
Switch	A device that connects multiple devices within a local network and forwards data to the correct device based on MAC address.
TCP (Transmission Control Protocol)	A Transport-layer protocol providing reliable, ordered, error-checked delivery of data.
TCP/IP Model	A four-layer practical networking model (Application, Transport, Internet, Network Access) describing the protocols actually in use today.
Topology	The physical or logical arrangement of connections between devices on a network.
Transport Layer	OSI Layer 4, responsible for end-to-end communication and reliability between devices.
UDP (User Datagram Protocol)	A Transport-layer protocol offering fast, connectionless, best-effort delivery, favoring speed over guaranteed delivery.
VLSM (Variable Length Subnet Masking)	The practice of using differently sized subnets within the same address block to match each segment's actual needs.
WAN (Wide Area Network)	A network spanning a large geographic area, such as a region, country, or the entire Internet.
Wi-Fi	The common name for wireless local area networking based on the IEEE 802.11 family of standards.

Appendix A: Subnetting Cheat Sheet

CIDR	Subnet Mask	Total Addresses	Usable Hosts	Common Use
/24	255.255.255.0	256	254	Standard LAN (office, home)
/25	255.255.255.128	128	126	Medium LAN segment
/26	255.255.255.192	64	62	Department or floor
/27	255.255.255.224	32	30	Small team or guest Wi-Fi
/28	255.255.255.240	16	14	Small device group
/29	255.255.255.248	8	6	Very small device group
/30	255.255.255.252	4	2	Point-to-point router link

Appendix B: Common Port Numbers

Port	Protocol	Service
20 / 21	TCP	FTP (File Transfer Protocol)
22	TCP	SSH (Secure Shell)
23	TCP	Telnet (unencrypted remote access, legacy)
25	TCP	SMTP (outgoing email)
53	TCP/UDP	DNS (Domain Name System)
67 / 68	UDP	DHCP (address assignment)
80	TCP	HTTP (unencrypted web traffic)
110	TCP	POP3 (incoming email, legacy)
143	TCP	IMAP (incoming email)
443	TCP	HTTPS (encrypted web traffic)
3389	TCP	RDP (Remote Desktop Protocol)

Appendix C: Essential Cisco IOS Command Reference

Command	Purpose
enable	Enter privileged EXEC mode
configure terminal	Enter global configuration mode
hostname <name>	Set the device's name
interface <name>	Select a specific interface to configure
ip address <addr> <mask>	Assign an IP address and subnet mask to an interface
no shutdown	Administratively enable an interface
ip route <network> <mask> <next-hop>	Add a static route
ip dhcp pool <name>	Create a DHCP address pool
show ip interface brief	Display a summary of all interfaces and their IP/status
show running-config	Display the device's current active configuration
ping <address>	Test reachability to another device
traceroute <address>	Show the path taken to reach a destination, hop by hop
copy running-config startup-config	Save the current configuration permanently

Thanks for attending Teah innovative Tech (T.I.T) OSCC 2026 – 10th Edition