



Gurukul Technicals Institute

Computer education · Robotics · Science projects · Delhi

FREE EBOOK

HARDWARE, NETWORKING AND REPAIR

Computer Networking Study Book

The complete study notes, practice questions and glossary for
Computer Networking

INSIDE THIS BOOK

- Networks, network types and topologies
- Network devices: NIC, hub, switch, router and access point
- Cables, connectors and Wi-Fi
- IPv4 addresses, private ranges and subnet masks
- DNS and DHCP
- ...and 2 more chapters, practice questions and a glossary

Beginner

Students learning how computers connect and share

engineergurukul.com

+91 97116 99511

Computer Networking Study Book

Learn how computers connect and talk to each other, from network types, topologies, devices, cables and Wi-Fi to IPv4 addressing, DNS, DHCP, the OSI and TCP/IP models, common ports and basic troubleshooting.

WHO IT IS FOR	Students learning how computers connect and share
LEVEL	Beginner
SUBJECT AREA	Hardware, networking and repair
WHAT IS INSIDE	7 chapters, practice questions with answers, and a glossary

CONTENTS

1	Networks, network types and topologies	3
2	Network devices: NIC, hub, switch, router and access point	5
3	Cables, connectors and Wi-Fi	7
4	IPv4 addresses, private ranges and subnet masks	9
5	DNS and DHCP	11
6	The OSI and TCP/IP models and common ports	14
7	Troubleshooting with ping and ipconfig	16
	Practice questions	18
	Answers	22
	Glossary	24

Free ebook: you may read, print and share it for learning; it may not be sold or changed. © 2026 Gurukul Technicals Institute. First edition, October 2026. Contact details are on the back cover.

Networks, network types and topologies

What is a computer network?

A **computer network** is two or more devices connected so that they can share data and resources. In a cyber café, all the computers share one internet connection and one printer; in an office, staff share files on a server; at home, phones, laptops and a smart TV share the Wi-Fi. Each connected device is called a **node** or **host**.

Networks let people:

- share files, printers and a single internet connection;
- communicate by email, chat and video calls;
- keep important data on a central server that is backed up in one place.

Client-server and peer-to-peer

In a **client-server** network, central computers called **servers** provide services such as files, email or websites, and the other computers, the **clients**, use those services. Most offices and every website work this way. In a **peer-to-peer** network, every computer is equal and shares its own files directly with the others. That suits a few computers in a small shop, but it becomes hard to manage and secure as the network grows.

Types of network by size

Type	Full form	Covers	Example
PAN	Personal Area Network	a few metres around one person	a phone connected to Bluetooth earbuds
LAN	Local Area Network	a room, building or campus	a school's computer lab
MAN	Metropolitan Area Network	a city	a cable operator's network across one city
WAN	Wide Area Network	states, countries or the world	a bank linking its branches across India

A LAN is usually owned by one organisation and is fast. A WAN often runs over lines rented from telecom companies. The **internet** is the largest WAN of all: a worldwide network of networks.

Topologies

A **topology** is the layout in which devices are connected.

- **Bus:** every device connects to one main cable, the backbone, with a terminator at each end. It is cheap, but a break in the backbone stops the whole network, and only one device can send at a time.
- **Star:** every device has its own cable to a central device, today a switch. A broken cable affects only one computer and new devices are easy to add, but if the central device fails, the whole network stops. Almost all modern wired LANs use a star.
- **Ring:** each device connects to the two next to it, forming a closed loop, and data passes around the ring from device to device. In a simple ring, a single failure can break the loop.
- **Mesh:** devices connect to many others, so data has several possible paths. In a full mesh every device connects to every other one, which needs $n(n-1)/2$ links for n devices: 10 links for 5 devices. It is very reliable but expensive.
- **Tree:** several stars joined in a hierarchy, such as one switch on each floor connected to a main switch.
- **Hybrid:** a mix of two or more topologies.

Physical topology is how the cables actually run; logical topology is how the data flows. The two are not always the same.

KEY POINTS

- A network connects devices so they can share data, printers and an internet connection.
- In a client-server network, servers provide services to clients; in a peer-to-peer network all computers are equal.
- By size, networks are PAN, LAN (building or campus), MAN (city) and WAN (countries); the internet is the largest WAN.
- Star is the usual LAN topology: a broken cable affects one device, but a failed central device stops them all.
- A full mesh of n devices needs $n(n-1)/2$ links.

TRY THESE EXERCISES

1. Walk round your home, school lab or computer centre and list every networked device you can find, such as computers, a printer, the router, phones and a smart TV, then decide whether the setup is client-server or peer-to-peer and write one reason.
2. Write one real example each of a PAN, a LAN, a MAN and a WAN from your own life, such as earbuds paired to a phone or a bank linking its branches, and note roughly how far each one stretches and who is likely to own it.
3. On paper, draw bus, star, ring, full mesh and tree layouts for six computers, mark what happens in each when one cable breaks, and use $n(n-1)/2$ to work out how many links a full mesh of 4, 6 and 8 devices needs.

CHAPTER 2

Network devices: NIC, hub, switch, router and access point

Network interface card and MAC address

Every device on a network needs a **network interface card (NIC)**, also called a network adapter. Laptops and phones have it built in, often as both an Ethernet port and Wi-Fi. Each NIC has a **MAC address** (Media Access Control address): a 48-bit number written as 12 hexadecimal digits, such as `3C-52-82-1A-7F-09`. The manufacturer assigns it, and the first half identifies the manufacturer. Phones and Windows can also use a random MAC address on Wi-Fi for privacy. A MAC address identifies a device on its local network, while an IP address, covered later, identifies it across networks.

Hub

A **hub** is a simple box with several ports. Whatever arrives on one port, it repeats out of every other port, to all devices, whether they need the data or not. All the devices share the bandwidth, and when two send at once their signals collide. A hub works at the physical layer (layer 1). Hubs are obsolete now; switches have replaced them.

Switch

A **switch** also connects the devices of a LAN, but it is intelligent. It reads the destination MAC address of each frame and sends the frame only out of the port where that device is connected. It learns which device is on which port by noting the source MAC address of every frame it receives, and stores this in its **MAC address table**. Each port gets its full speed, and devices can send and receive at the same time (full duplex). A switch works at the data link layer (layer 2).

Router

A **router** connects different networks and forwards **packets** between them using **IP addresses**. It keeps a **routing table** and chooses the path towards each destination. A router works at the network layer (layer 3). A home router connects the home LAN to the internet service provider's network, and the internet itself is held together by routers.

Access point

A **wireless access point (AP)** lets Wi-Fi devices join a wired network. Large offices and colleges fix several access points on ceilings, all cabled back to switches, so that people can move around and stay connected.

Modem and ONT

A **modem** (modulator-demodulator) converts a computer's digital signals into signals that can travel over a telephone or cable line, and back again. A fibre broadband connection uses an **ONT** (Optical Network Terminal) instead, which converts light signals into electrical ones.

The home Wi-Fi router

The box most homes call a "Wi-Fi router" combines several devices in one: a router, a small switch with a few LAN ports, a wireless access point, a DHCP server that hands out addresses, and a firewall. Some models also contain the modem or ONT.

Device	Works with	OSI layer	Job
Hub	signals (bits)	1, Physical	repeats data out of every port
Switch	MAC addresses (frames)	2, Data link	sends data only to the right port
Router	IP addresses (packets)	3, Network	joins networks and picks paths

A repeater simply regenerates a weak signal so that it can travel further.

KEY POINTS

- Every networked device has a NIC with a 48-bit MAC address, written as 12 hexadecimal digits.
- A hub repeats data out of every port; a switch learns MAC addresses and sends data only to the right port.
- A router connects different networks and forwards packets using IP addresses.
- An access point lets wireless devices join a wired network.
- A home Wi-Fi router combines a router, a switch, an access point, a DHCP server and a firewall.

TRY THESE EXERCISES

1. On a Windows computer, open Command Prompt, run `ipconfig /all` and write down the Physical Address of each Ethernet and Wi-Fi adapter, count its 12 hexadecimal digits, and check in Wi-Fi settings whether Random hardware addresses is turned on, because then the Wi-Fi address will not identify the manufacturer.
2. Look at a home or office Wi-Fi router and its label: find the internet (WAN) port, the LAN ports and the power socket, note whether a separate modem or ONT is connected to it, and write which parts show it working as a router, a switch and an access point.
3. Draw a network diagram for a small office with an ONT, a router, an eight-port switch, a wireless access point, four wired computers, a network printer and phones on Wi-Fi, and label the switch and the router with the OSI layer each works at and whether it forwards data by MAC address or by IP address.

CHAPTER 3

Cables, connectors and Wi-Fi

Twisted-pair cable

The blue or grey "LAN cable" in most offices is **twisted-pair** copper cable. Inside are eight wires in four pairs, each pair twisted together; the twisting reduces interference from nearby cables and equipment. Most cable is **UTP** (unshielded twisted pair); **STP** (shielded twisted pair) adds foil shielding for electrically noisy places such as factories. The plug on each end is an **RJ45** connector, which is wider than the RJ11 plug on a telephone cable.

Category	Typical Ethernet speed
Cat5e	1 Gbps
Cat6	1 Gbps, or 10 Gbps on runs up to about 55 m
Cat6a	10 Gbps up to 100 m

For Ethernet over twisted pair, a single cable run should be no longer than **100 metres**. Beyond that the signal becomes too weak, so a switch is placed in between.

Traditionally, a **straight-through** cable connects a computer to a switch, and a **crossover** cable connects two similar devices, such as two computers. Most modern network ports detect the cable type automatically, a feature called Auto MDI-X, so the difference rarely matters today.

Coaxial cable

Coaxial cable has a single copper core, a layer of insulation, a braided metal shield and an outer jacket. It is used for cable TV and set-top boxes, and early bus networks used it too.

Optical fibre

Optical fibre carries data as pulses of light through thin strands of glass or plastic. It supports very high speeds over long distances, many kilometres, and electrical interference does not affect it, but it costs more and needs care when it is laid and joined. **Single-mode** fibre has a very thin core and carries signals over long distances, such as between cities. **Multimode** fibre has a wider core and suits shorter links inside buildings and campuses. Fibre-to-the-home broadband brings a fibre right into the house.

Wi-Fi

Wi-Fi is wireless LAN technology based on the IEEE 802.11 family of standards. Recent generations have simple names:

Name	Standard
Wi-Fi 4	802.11n
Wi-Fi 5	802.11ac
Wi-Fi 6 and 6E	802.11ax
Wi-Fi 7	802.11be

Wi-Fi uses these radio bands:

- **2.4 GHz** reaches further and passes through walls better, but it is slower and more crowded, sharing the air with Bluetooth devices and microwave ovens.
- **5 GHz** is faster and has less interference, but its range is shorter.
- **6 GHz** is used by Wi-Fi 6E and Wi-Fi 7 devices where a country's rules allow it.

The name of a Wi-Fi network is its **SSID**. Protect every network with **WPA3**, or **WPA2** where older devices need it, and a strong password. WEP and the original WPA are outdated and easy to break.

A cable is usually faster and more stable than Wi-Fi, so connect a desktop computer that never moves with a cable.

KEY POINTS

- Twisted-pair LAN cable has four twisted pairs to reduce interference and uses RJ45 connectors.
- A single twisted-pair Ethernet run should be no longer than 100 metres.
- Optical fibre carries light, covers long distances at high speed and is immune to electrical interference.
- 2.4 GHz Wi-Fi reaches further; 5 GHz is faster with a shorter range.
- Secure Wi-Fi with WPA3 or WPA2; WEP is outdated and unsafe.

TRY THESE EXERCISES

1. Examine a LAN cable: read the category printed on its jacket, such as Cat5e or Cat6, look through the clear RJ45 plug to identify the eight wires in four colour pairs, and compare the plug's width with an RJ11 telephone plug.
2. Estimate the cable length from a lab switch to the farthest computer and check it is within 100 metres, then choose a cable for each of these and give a reason: a 10 Gbps run of 80 metres on one floor, a link between two buildings on the same campus, and a link between two cities.
3. In Windows Settings, open the properties of the Wi-Fi network you are connected to and note its SSID, protocol (such as Wi-Fi 5 or Wi-Fi 6), security type and network band, then write whether the security is WPA3 or WPA2 and whether a 5 GHz band would be better in that room.

CHAPTER 4

IPv4 addresses, private ranges and subnet masks

What an IP address is

Every device on an IP network needs an **IP address**, a number that identifies it so that data can be delivered to it, much like a postal address with a PIN code. The common version, **IPv4**, uses 32 bits, written as four decimal numbers separated by dots, such as `192.168.1.25`. Each part is called an **octet** because it holds 8 bits, so each can be from 0 to 255. An address such as `192.168.1.300` is therefore invalid.

32 bits allow about 4.3 billion addresses, which is not enough for the world's devices. **IPv6** uses 128 bits, written as hexadecimal groups separated by colons, such as `2001:db8::1`, and gives an almost unlimited supply. Both versions are in use side by side.

Network part and host part

An IPv4 address has two parts: the **network part**, shared by every device on the same network, and the **host part**, which identifies one device on it. The **subnet mask** shows where the split falls. In binary, a mask is a run of 1s for the network bits followed by 0s for the host bits.

Mask	Prefix	Network bits	Usable host addresses
255.0.0.0	/8	8	16,777,214
255.255.0.0	/16	16	65,534
255.255.255.0	/24	24	254

The **prefix** form writes the number of network bits after a slash, so `192.168.1.25/24` means the mask is 255.255.255.0. Older textbooks group addresses into classes A, B and C with these three masks as defaults; modern networks can use any prefix length.

Working out a /24 network

For `192.168.1.25/24`:

- The first three octets, `192.168.1`, are the network part and the last octet is the host part.
- The **network address**, with all host bits 0, is `192.168.1.0`. It names the network itself.
- The **broadcast address**, with all host bits 1, is `192.168.1.255`. Data sent to it reaches every device on the network.
- Usable addresses run from `192.168.1.1` to `192.168.1.254`, which is 254 addresses. With h host bits a network has $2^h - 2$ usable addresses, because the network and broadcast addresses cannot be given to devices.

A computer compares the network part of the destination with its own. If they match, it sends the data directly across the LAN; if not, it sends the data to its **default gateway**, the router, which forwards it. So `192.168.1.40/24` is on the same network as `192.168.1.25/24`, but `192.168.2.40` is not.

Private and public addresses

Three ranges are reserved for **private** networks such as homes, offices and labs. Anyone may use them, and they are never routed on the internet:

Range	Prefix
10.0.0.0 to 10.255.255.255	10.0.0.0/8
172.16.0.0 to 172.31.255.255	172.16.0.0/12
192.168.0.0 to 192.168.255.255	192.168.0.0/16

Devices with private addresses reach the internet through a router that performs **NAT** (Network Address Translation), translating their private addresses into a **public** address so that they can share it.

127.0.0.1 is the loopback address, which always means "this computer itself".

KEY POINTS

- An IPv4 address is 32 bits, written as four octets from 0 to 255; IPv6 uses 128 bits.
- The subnet mask divides an address into a network part and a host part; /24 means 255.255.255.0.
- A /24 network has 254 usable addresses; the first is the network address and the last is the broadcast address.
- The private ranges are 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16, and NAT lets them share a public address.
- Traffic for another network goes to the default gateway, which is the router.

TRY THESE EXERCISES

1. Write valid or invalid with a reason for each address, and say whether each valid one is private or public: 192.168.1.25, 10.0.0.300, 172.16.5.1, 256.1.1.1, 8.8.8.8 and 192.168.1.
2. For 192.168.10.77/24, work out the network address, the broadcast address, the first and last usable addresses and the number of usable hosts, then decide whether 192.168.10.200 and 192.168.11.5 are on the same network.
3. Run ipconfig on your computer and write down its IPv4 address, subnet mask and default gateway, write the mask in prefix form and in binary, say whether the address is private, and check that the gateway is on the same network as the computer.

CHAPTER 5

DNS and DHCP

DNS: the internet's phone book

People remember names such as `www.example.com`, but computers connect using IP addresses. The **Domain Name System (DNS)** translates names into IP addresses. When you type a website name into a browser:

1. The computer checks its own cache, in case it looked the name up recently.
2. If not, it asks its **DNS resolver**, usually run by the internet service provider or by a public service such as `8.8.8.8` (Google) or `1.1.1.1` (Cloudflare).

3. If the resolver does not already know the answer, it asks the DNS hierarchy in turn: a **root server** points it to the servers for the top-level domain, such as `.com` or `.in`, and those point it to the domain's **authoritative** server, which gives the final answer.
4. The resolver returns the IP address, and both the resolver and the computer cache it for a time set in the record, called its TTL.
5. The browser connects to that IP address.

DNS normally uses port 53, mostly over UDP for quick queries. Common record types are:

Record	Holds
A	an IPv4 address for a name
AAAA	an IPv6 address for a name
CNAME	an alias that points to another name
MX	the mail server for a domain

A domain name is read from right to left. In `www.example.co.in`, `in` is the top-level domain for India, `co.in` is the level under it that businesses commonly use, `example` is the registered name and `www` is a host within it.

DHCP: automatic addresses

Every device needs an IP address, a subnet mask, a default gateway and DNS server addresses. Typing these by hand into every laptop and phone would be slow and error-prone, and two devices given the same address would clash. The **Dynamic Host Configuration Protocol (DHCP)** hands them out automatically. In a home or small office, the router is usually the DHCP server.

A new device gets its settings in four steps, remembered as **DORA**:

1. **Discover**: the device broadcasts a message looking for a DHCP server.
2. **Offer**: a server offers an address and settings.
3. **Request**: the device asks to use the offered address.
4. **Acknowledge**: the server confirms, and the device starts using the address.

The address is given on a **lease** for a set time, and the device renews the lease before it runs out. After a device leaves, its address can later go to another device. DHCP uses UDP ports 67 (server) and 68 (client).

Static or dynamic?

Laptops and phones use DHCP. Printers, servers and network cameras need an address that never changes, so that other devices can always find them. They get either a **static** address entered by hand, outside the range that DHCP hands out, or a **DHCP reservation**, where the server always gives the same address to that device's MAC address.

If a Windows PC shows an address starting with 169.254, it gave itself that address because it could not reach a DHCP server. Check the cable or Wi-Fi and the router.

KEY POINTS

- DNS translates domain names such as `www.example.com` into IP addresses, and answers are cached.
- A lookup goes from the resolver to a root server, then the top-level domain servers, then the domain's authoritative server.
- DHCP gives a device its IP address, subnet mask, default gateway and DNS servers automatically.
- DHCP works in four steps, Discover, Offer, Request and Acknowledge (DORA), and addresses are leased.
- Printers and servers need a fixed address: a static address or a DHCP reservation.

TRY THESE EXERCISES

1. In Command Prompt, run `nslookup` followed by the name of a website you use often, note the IPv4 address, any IPv6 addresses and the DNS server that answered, run it again with `1.1.1.1` added after the name to ask that server instead, and then run `ipconfig /displaydns` to see the names your computer has cached (nslookup asks the DNS server directly, so its own lookups do not appear there, but sites you opened in the browser do).
2. Run `ipconfig /all` and find the DHCP Enabled line, the DHCP Server address, the DNS Servers and the Lease Obtained and Lease Expires times, then write the four DORA steps that gave your computer its address.
3. With the owner's permission, sign in to a home Wi-Fi router's settings page, find the DHCP address range, the lease time and the list of connected devices, and plan a fixed address for a printer either outside that range or as a DHCP reservation tied to its MAC address.

The OSI and TCP/IP models and common ports

Why use layers?

Sending data across a network involves many jobs, from turning bits into signals to choosing a route and handing the data to the right application. Network models divide these jobs into **layers**. Each layer does one job and serves the layer above it, so a change in one layer, such as moving from a cable to Wi-Fi, does not affect the others.

The OSI model

The **OSI** (Open Systems Interconnection) reference model has seven layers:

No.	Layer	Job	Examples
7	Application	network services for applications	HTTP, DNS, SMTP
6	Presentation	data formats, encryption and compression	JPEG, ASCII
5	Session	setting up, managing and ending sessions	NetBIOS, RPC
4	Transport	end-to-end delivery, ports, reliability	TCP, UDP
3	Network	logical addressing and routing	IP, routers
2	Data link	frames and MAC addresses on one link	Ethernet, switches
1	Physical	bits as electrical, light or radio signals	cables, hubs

A popular memory aid, from layer 1 upwards, is "Please Do Not Throw Sausage Pizza Away". As data moves down the layers on the sending computer, each layer adds its own header; this is called **encapsulation**, and the receiver removes the headers on the way up. The unit of data has a different name at each layer: **bits** at layer 1, **frames** at layer 2, **packets** at layer 3, and **segments** at layer 4 for TCP (UDP sends **datagrams**).

The TCP/IP model

The OSI model is used mainly for teaching and troubleshooting. The internet actually runs on the **TCP/IP** protocol suite, whose model has four layers:

TCP/IP layer	Matching OSI layers
Application	5, 6 and 7

TCP/IP layer	Matching OSI layers
Transport	4
Internet	3
Network access (link)	1 and 2

Some textbooks split the bottom layer in two and show five layers.

TCP and UDP

- **TCP** (Transmission Control Protocol) is connection-oriented and reliable. It sets up a connection with a three-way handshake (SYN, SYN-ACK, ACK), numbers the data, resends anything lost and delivers it in order. Web pages, email and file transfers use TCP.
- **UDP** (User Datagram Protocol) is connectionless: it just sends, with no handshake and no resending. Its low overhead suits DNS lookups, live video calls and online games, where a late packet is useless anyway.

Port numbers

An IP address finds the device; a **port number**, from 0 to 65535, finds the program on that device. Ports 0 to 1023 are the **well-known ports** reserved for standard services.

Port	Protocol	Used for
80	HTTP	web pages without encryption
443	HTTPS	secure, encrypted web pages
22	SSH	secure remote login, and SFTP file transfer
25	SMTP	sending email between mail servers
53	DNS	looking up names
21	FTP	file transfer without encryption

Email apps usually send mail to their own server through port 587 or 465 instead.

KEY POINTS

- The OSI model has seven layers: Physical, Data link, Network, Transport, Session, Presentation and Application.
- The TCP/IP model has four layers: Network access, Internet, Transport and Application.
- TCP is reliable and connection-oriented; UDP is faster and connectionless.
- Well-known ports: 80 HTTP, 443 HTTPS, 22 SSH, 25 SMTP and 53 DNS.

TRY THESE EXERCISES

1. Write the seven OSI layers from 1 to 7 from memory using the memory aid, add each layer's job and one example protocol or device, mark the data unit at layers 1 to 4, and draw a second column showing the TCP/IP layer each one belongs to.
2. Sort these into TCP or UDP with a reason for each: loading a web page, sending an email, downloading a file, a DNS lookup, a live video call and an online game; then write the port numbers of HTTP, HTTPS, SSH, SMTP, DNS and FTP from memory and check them against the lesson.
3. With a few web pages open in the browser, run `netstat -n` in Command Prompt to list your computer's TCP connections, find remote addresses ending in `:443` or `:80`, and write which protocol each port belongs to and why most connections use 443.

CHAPTER 7

Troubleshooting with ping and ipconfig

ipconfig: what are my settings?

On Windows, open Command Prompt or Windows Terminal and type `ipconfig`. Part of the output looks like this:

TEXT

```
C:\> ipconfig

Wireless LAN adapter Wi-Fi:

    IPv4 Address. . . . . : 192.168.1.25
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

Command	What it does
<code>ipconfig</code>	shows the IP address, subnet mask and default gateway of each adapter
<code>ipconfig /all</code>	also shows the MAC address (as Physical Address), DHCP server, DNS servers and lease times
<code>ipconfig /release</code>	gives up the address received from DHCP
<code>ipconfig /renew</code>	asks the DHCP server for an address again
<code>ipconfig /flushdns</code>	clears the computer's DNS cache

On Linux, `ip addr` shows similar information; macOS and older Linux systems use `ifconfig`.

ping: can I reach it?

`ping` sends small test messages, called ICMP Echo Requests, to an address and waits for the replies:

TEXT

```
C:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

- `time` is the round-trip time in milliseconds; lower is better.
- On Windows, ping sends four requests and stops, and `ping -t` keeps going until you press Ctrl+C. On Linux and macOS, ping keeps going until Ctrl+C.
- "Request timed out" means no reply arrived in time. "Destination host unreachable" means your computer or a router could not deliver the request.
- You can also ping a name; ping first looks up its IP address through DNS.

A failed ping does not always mean a device is switched off. Many firewalls block ping; Windows Defender Firewall, for example, usually blocks incoming ping requests by default.

A step-by-step method

Work outwards from your own computer; the first step that fails shows where the problem lies:

1. **Check the physical connection.** Is the cable plugged in with the port light on, or is the Wi-Fi connected to the right network?
2. **Run `ipconfig`.** An address starting with 169.254 means the computer could not get an address from DHCP: try `ipconfig /release` and then `ipconfig /renew`, and check the router.
3. **Ping 127.0.0.1**, the loopback address, to test the computer's own TCP/IP software.
4. **Ping the default gateway**, for example `ping 192.168.1.1`. If this fails, check the cable, the Wi-Fi and the router.
5. **Ping an internet address by number**, such as `ping 8.8.8.8`. If this fails while the gateway replies, the problem is most likely the router's internet connection or the service provider.

6. **Ping a name**, such as `ping google.com`. If pinging by number works but the name gives "could not find host", the problem is **DNS**: check the DNS settings or run `ipconfig /flushdns`.

Two more tools

- `tracert` on Windows, or `traceroute` on Linux and macOS, lists the routers on the path to a destination and shows where delays or failures happen.
- `nslookup example.com` asks a DNS server directly for the address of a name.

KEY POINTS

- `ipconfig` shows a Windows computer's IP address, subnet mask and default gateway; `ipconfig /all` adds the MAC address and the DHCP and DNS servers.
- `ping` checks whether an address replies and shows the round-trip time in milliseconds.
- An address starting with 169.254 means the computer could not get one from DHCP.
- Troubleshoot outwards: loopback, then the default gateway, then an internet address, then a name.
- If an IP address replies but a name cannot be found, the problem is DNS.

TRY THESE EXERCISES

1. Follow the lesson's step-by-step method on your own computer: check the connection, run `ipconfig`, `ping 127.0.0.1`, `ping` your default gateway, `ping 8.8.8.8` and `ping` a website by its name, writing down the reply time or the error message at each step.
2. On your own computer or with your instructor's permission, unplug the LAN cable or turn off Wi-Fi, run `ipconfig` and `ping` the gateway and note the messages, then reconnect, run `ipconfig /release` followed by `ipconfig /renew`, and check whether the address changed.
3. Run `tracert 8.8.8.8` and count the routers on the path, noting any hop that is slow or shows Request timed out; then run `ping -t` to your default gateway for a minute, stop it with Ctrl+C and read the summary of packets sent, received and lost.

CHECK YOURSELF

Practice questions

Choose the best answer for each question. The answers, with a short explanation, are in the next chapter.

1. Which type of network usually covers a single building or campus, such as a school's computer lab?

- | | |
|--------|--------|
| a) WAN | b) LAN |
| c) MAN | d) PAN |

- 2. In which topology does every device have its own cable to a central switch?**
- a) Bus
 - b) Ring
 - c) Star
 - d) Full mesh
- 3. In a bus topology, what happens if the main backbone cable breaks?**
- a) Only the computer nearest the break is affected
 - b) Data automatically takes another path
 - c) The whole network stops working
 - d) The network keeps working at a slower speed
- 4. How many links are needed to connect 5 computers in a full mesh?**
- a) 5
 - b) 20
 - c) 10
 - d) 25
- 5. In which kind of network do central computers provide files and other services to the rest of the computers?**
- a) Peer-to-peer
 - b) Personal area network
 - c) Client-server
 - d) Ad hoc wireless
- 6. How is a MAC address made up?**
- a) 48 bits, written as 12 hexadecimal digits
 - b) 32 bits, written as four decimal numbers
 - c) 128 bits, written in groups separated by colons
 - d) 16 bits, written as a single number up to 65535
- 7. What does a hub do with data that arrives on one of its ports?**
- a) Sends it only to the port of the destination device
 - b) Sends it out of every other port
 - c) Forwards it to another network using IP addresses
 - d) Stores it until the destination asks for it
- 8. How does a switch decide which port to send a frame out of?**
- a) It sends every frame out of every port
 - b) It looks up the destination MAC address in its MAC address table
 - c) It asks a DNS server for the right port
 - d) It picks a port at random
- 9. Which device connects different networks, such as a home LAN and the internet, and forwards packets using IP addresses?**
- a) Hub
 - b) Switch
 - c) Repeater
 - d) Router
- 10. Which device lets laptops and phones join a wired network over Wi-Fi?**
- a) Hub
 - b) Patch panel
 - c) Modem
 - d) Wireless access point
- 11. Which connector is used on standard twisted-pair Ethernet cables?**
- a) RJ45
 - b) RJ11
 - c) BNC
 - d) HDMI

- 12. What is the maximum recommended length of a single twisted-pair Ethernet cable run?**
- a) 10 metres
 - b) 500 metres
 - c) 100 metres
 - d) 2 kilometres
- 13. Which type of cable carries data as pulses of light and is not affected by electrical interference?**
- a) Optical fibre
 - b) Coaxial cable
 - c) UTP cable
 - d) STP cable
- 14. Compared with the 5 GHz band, what is true of 2.4 GHz Wi-Fi?**
- a) It is always faster
 - b) It works only with Wi-Fi 7 devices
 - c) It cannot pass through walls at all
 - d) It usually reaches further but is slower and more crowded
- 15. Which security setting should you choose when setting up a new Wi-Fi network?**
- a) WEP
 - b) WPA3, or WPA2 where older devices need it
 - c) An open network with no password
 - d) A hidden network name with no password
- 16. How many bits are in an IPv4 address?**
- a) 48
 - b) 32
 - c) 64
 - d) 128
- 17. Which of these is a valid IPv4 address?**
- a) 192.168.10.254
 - b) 192.168.1.256
 - c) 10.0.300.1
 - d) 172.16.1
- 18. Which of these addresses is in a private range?**
- a) 192.168.0.10
 - b) 8.8.8.8
 - c) 172.32.0.5
 - d) 11.0.0.1
- 19. A computer has the address 192.168.1.25 with the subnet mask 255.255.255.0. What is its network address?**
- a) 192.168.1.255
 - b) 192.168.0.0
 - c) 192.168.1.0
 - d) 255.255.255.0
- 20. How many usable host addresses does a /24 network have?**
- a) 254
 - b) 256
 - c) 255
 - d) 24
- 21. What does DNS do?**
- a) Translates domain names into IP addresses
 - b) Hands out IP addresses to devices automatically
 - c) Joins two networks and chooses paths between them
 - d) Checks downloaded files for viruses
- 22. Which DNS record type holds the IPv4 address for a name?**
- a) A
 - b) MX
 - c) CNAME
 - d) AAAA

23. What does DHCP give a device that joins a network?

- a) An IP address, subnet mask, default gateway and DNS servers, automatically
- b) The IP address of every website it will visit
- c) A new MAC address for its network card
- d) A faster connection to the internet

24. What are the four steps of DHCP, in order?

- a) Request, Offer, Discover, Acknowledge
- b) Discover, Request, Offer, Acknowledge
- c) Offer, Discover, Acknowledge, Request
- d) Discover, Offer, Request, Acknowledge

25. How many layers does the OSI reference model have?

- a) 4
- b) 5
- c) 7
- d) 6

26. Which OSI layer deals with IP addresses and routing?

- a) Data link layer (layer 2)
- b) Transport layer (layer 4)
- c) Physical layer (layer 1)
- d) Network layer (layer 3)

27. Which protocol sets up a connection with a three-way handshake and resends any data that is lost?

- a) UDP
- b) TCP
- c) ICMP
- d) ARP

28. Which port does HTTPS use by default?

- a) 80
- b) 443
- c) 22
- d) 25

29. Which service uses port 22 by default?

- a) SMTP
- b) DNS
- c) HTTP
- d) SSH

30. Which protocol uses port 25 to send email between mail servers?

- a) FTP
- b) SMTP
- c) HTTP
- d) SSH

31. Which service uses port 53?

- a) DHCP
- b) HTTPS
- c) DNS
- d) RDP

32. Which Windows command shows a computer's IP address, subnet mask and default gateway?

- a) ping
- b) tracert
- c) ipconfig
- d) nslookup

33. Which command shows the MAC address of a Windows computer's network adapters?

- a) ipconfig /renew
- b) ipconfig /all
- c) ipconfig /flushdns
- d) ping -t

34. ping 8.8.8.8 gets replies, but pinging a website name says it could not find the host. What is the most likely problem?
- a) The network cable is unplugged
 - b) The computer has no IP address
 - c) The network card is faulty
 - d) DNS is not working
35. ipconfig on a Windows PC shows the address 169.254.12.7. What does this most likely mean?
- a) The PC is connected directly to the internet
 - b) The PC is using the loopback address
 - c) The PC has a public address from the service provider
 - d) The PC could not get an address from a DHCP server

ANSWER KEY

Answers

1. **(b) LAN.** A Local Area Network covers a room, building or campus; a WAN spans states or countries.
2. **(c) Star.** In a star topology all devices connect to a central device, which today is usually a switch.
3. **(c) The whole network stops working.** All devices share the single backbone cable, so a break in it stops communication across the network.
4. **(c) 10.** A full mesh of n devices needs $n(n-1)/2$ links, and $5 \times 4 / 2 = 10$.
5. **(c) Client-server.** In a client-server network, servers provide services and clients use them; in peer-to-peer every computer is equal.
6. **(a) 48 bits, written as 12 hexadecimal digits.** A MAC address is a 48-bit hardware address shown as 12 hex digits; 32 bits describes IPv4 and 128 bits IPv6.
7. **(b) Sends it out of every other port.** A hub simply repeats incoming data out of all its other ports, unlike a switch, which sends it only where it needs to go.
8. **(b) It looks up the destination MAC address in its MAC address table.** A switch learns which MAC address is on which port and forwards each frame only to the matching port.
9. **(d) Router.** A router works at the network layer, joining networks and choosing paths for packets by IP address.
10. **(d) Wireless access point.** An access point bridges wireless devices onto the wired LAN.
11. **(a) RJ45.** Ethernet cables use the 8-pin RJ45 connector; RJ11 is the smaller telephone plug and BNC is used with coaxial cable.
12. **(c) 100 metres.** Ethernet over twisted pair is specified for runs of up to 100 metres; longer distances need a switch in between or fibre.
13. **(a) Optical fibre.** Optical fibre carries light through glass or plastic strands, so electrical noise does not affect it.
14. **(d) It usually reaches further but is slower and more crowded.** 2.4 GHz travels further and through walls better, but it carries less data and shares the air with many other devices.

15. **(b) WPA3, or WPA2 where older devices need it.** WPA3 and WPA2 are current security standards; WEP is outdated and easily broken, and an open network has no protection.
16. **(b) 32.** IPv4 addresses are 32 bits long, written as four 8-bit octets; IPv6 addresses are 128 bits.
17. **(a) 192.168.10.254.** Each of the four octets must be from 0 to 255; 256 and 300 are too large and 172.16.1 has only three octets.
18. **(a) 192.168.0.10.** 192.168.0.0/16 is a private range; the private 172 range ends at 172.31.255.255, so 172.32.0.5 is public.
19. **(c) 192.168.1.0.** With a /24 mask the first three octets are the network part, and setting the host part to 0 gives 192.168.1.0.
20. **(a) 254.** 8 host bits give 256 addresses, minus the network address and the broadcast address, which leaves 254.
21. **(a) Translates domain names into IP addresses.** DNS looks up the IP address for a name such as www.example.com so that a computer can connect to it.
22. **(a) A.** An A record holds an IPv4 address; AAAA holds an IPv6 address and MX names a mail server.
23. **(a) An IP address, subnet mask, default gateway and DNS servers, automatically.** DHCP automatically configures a device's network settings so that nobody has to type them in by hand.
24. **(d) Discover, Offer, Request, Acknowledge.** The device discovers a server, the server offers an address, the device requests it and the server acknowledges: DORA.
25. **(c) 7.** The OSI model has seven layers, from Physical (1) up to Application (7); the TCP/IP model is usually shown with four.
26. **(d) Network layer (layer 3).** The network layer handles logical addressing and routing between networks, which is where routers work.
27. **(b) TCP.** TCP is connection-oriented and reliable; UDP sends without a handshake and does not resend lost data.
28. **(b) 443.** HTTPS uses port 443; port 80 is plain HTTP.
29. **(d) SSH.** Port 22 is SSH, used for secure remote login and SFTP file transfer.
30. **(b) SMTP.** SMTP, the Simple Mail Transfer Protocol, uses port 25 between mail servers.
31. **(c) DNS.** DNS uses port 53, mostly over UDP; DHCP uses ports 67 and 68.
32. **(c) ipconfig.** ipconfig displays the IP settings of each network adapter.
33. **(b) ipconfig /all.** ipconfig /all adds details such as the Physical Address (MAC), DHCP server and DNS servers.
34. **(d) DNS is not working.** Replies from an IP address prove the connection works, so a failure only with names points to DNS.
35. **(d) The PC could not get an address from a DHCP server.** Windows gives itself a 169.254 address when no DHCP server answers, which points to a connection or DHCP problem.

Glossary

Access point

A device that lets Wi-Fi devices join a wired network, usually connected by cable to a switch.

Broadcast address

The last address of an IPv4 network, with all host bits set to 1, such as 192.168.1.255, which delivers data to every device on that network.

Default gateway

The router address a device sends traffic to when the destination is on a different network, such as the internet.

DHCP

Dynamic Host Configuration Protocol, which automatically gives a device its IP address, subnet mask, default gateway and DNS servers on a lease.

DNS

Domain Name System, the service that translates domain names such as `www.example.com` into the IP addresses computers use to connect.

Hub

An obsolete network device that repeats every signal it receives out of all its other ports, working at OSI layer 1.

IP address

A number that identifies a device on an IP network so that data can be delivered to it, written as four octets in IPv4 or hexadecimal groups in IPv6.

ipconfig

A Windows command that shows a computer's IP address, subnet mask and default gateway, with `ipconfig /all` adding the MAC address, DHCP and DNS details.

LAN

Local Area Network, a network covering a room, building or campus, usually owned by one organisation.

MAC address

The 48-bit hardware address of a network interface, written as 12 hexadecimal digits, that identifies a device on its local network.

NAT

Network Address Translation, done by a router so that devices with private addresses can share one public address on the internet.

NIC

Network Interface Card, the built-in or added hardware that connects a device to a wired or wireless network.

Optical fibre

Cable that carries data as pulses of light through thin strands of glass or plastic, giving high speeds over long distances without electrical interference.

OSI model

A seven-layer reference model, from Physical up to Application, used to teach and troubleshoot how data travels across a network.

Ping

A command that sends ICMP Echo Requests to an address and reports whether replies arrive and how long each round trip takes.

Port number

A number from 0 to 65535 that identifies which program on a device should receive the data, such as 443 for HTTPS.

Private IP address

An address in the ranges 10.0.0.0/8, 172.16.0.0/12 or 192.168.0.0/16, used inside homes, offices and labs and never routed on the internet.

Router

A device that connects different networks and forwards packets between them using IP addresses, working at OSI layer 3.

SSID

The name of a Wi-Fi network, which devices see when they look for networks to join.

Subnet mask

A number such as 255.255.255.0 that shows which part of an IPv4 address is the network part and which is the host part.

Switch

A LAN device that learns which MAC address is on each port and sends each frame only to the port of its destination, working at OSI layer 2.

TCP

Transmission Control Protocol, a connection-oriented transport protocol that sets up a connection, resends lost data and delivers it in order.

Topology

The layout in which the devices of a network are connected, such as bus, star, ring, mesh or tree.

UDP

User Datagram Protocol, a connectionless transport protocol that sends data with no handshake and no resending, which suits DNS lookups, video calls and games.

WAN

Wide Area Network, a network spanning states, countries or the world, often over lines rented from telecom companies; the internet is the largest WAN.



Gurukul Technicals Institute

Computer education institute in Delhi, with authorised member centres, robotics classes and science projects, working models and DIY kits.

COURSES

Computer & Office Skills · Accounting & Business Software · Programming & Web Development · Design & Digital Skills · Hardware & Networking · Robotics & Coding · Other Programmes

PROJECTS AND KITS

Ready-made school projects · DIY and STEM kits · Robotics and coding · Components and spares · Engineering projects

CONTACT

Head office: A-10, Chief Commissioner Colony, opposite Rana Pratap Bagh, Delhi 110007

Phone: 011 2721 1512 · **Mobile and WhatsApp:** +91 97116 99511

Email: engineergurukul@yahoo.co.in

Website: engineergurukul.com · **Instagram:** [@science_projects_club](https://www.instagram.com/science_projects_club)

More free ebooks for computer courses, robotics and science projects: engineergurukul.com/resources/ebooks/

Free to read, print and share. Not for sale.