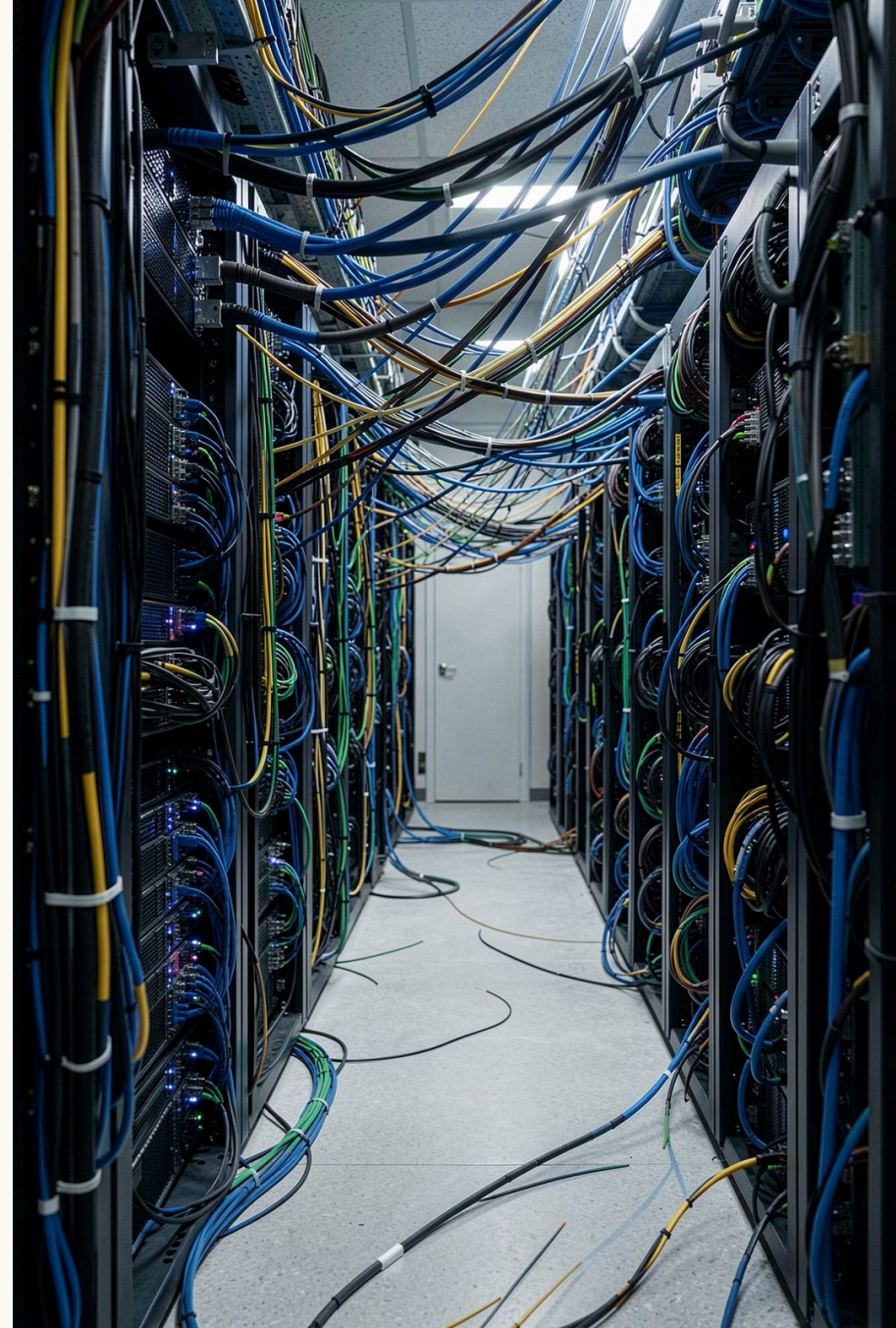


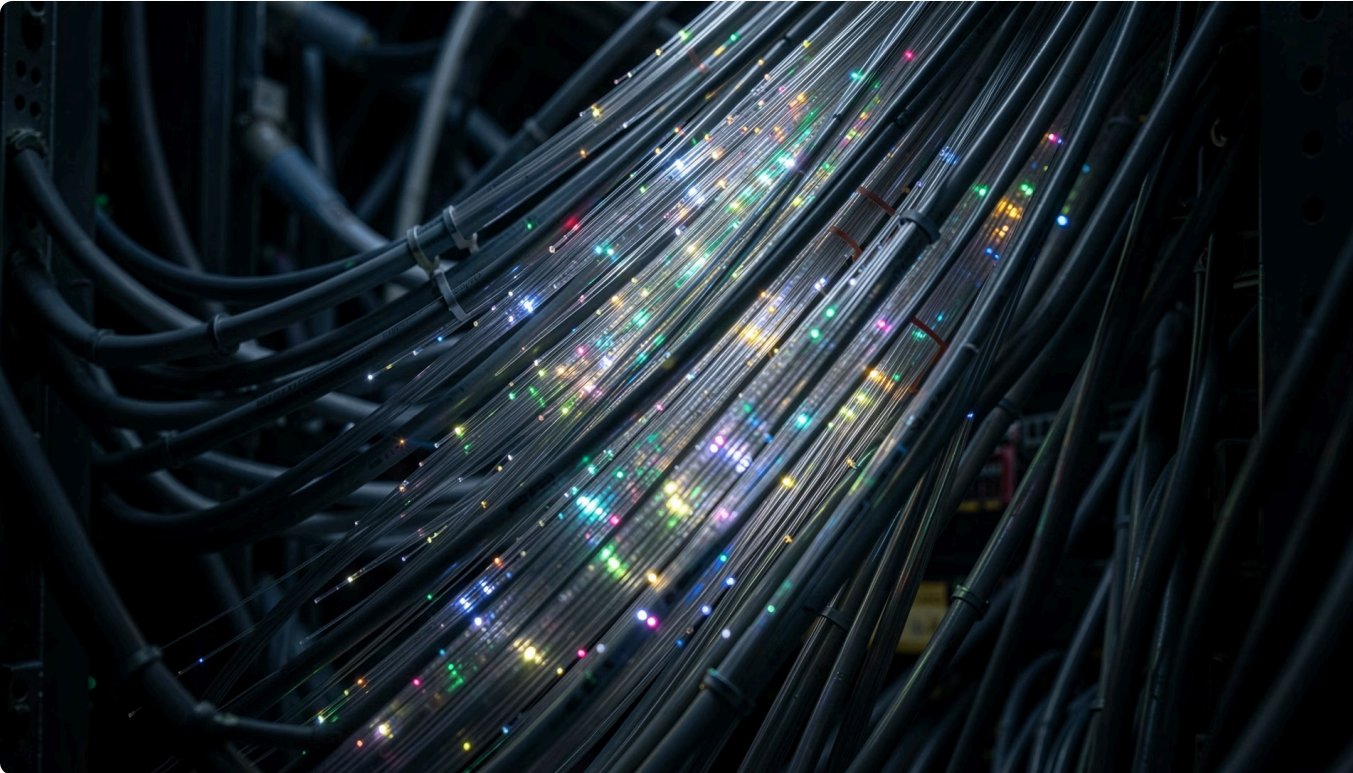
Computer Network Transmission

Security, Integrity, and the Foundations of Data Communication

SESSION 1



What Is Transmission?



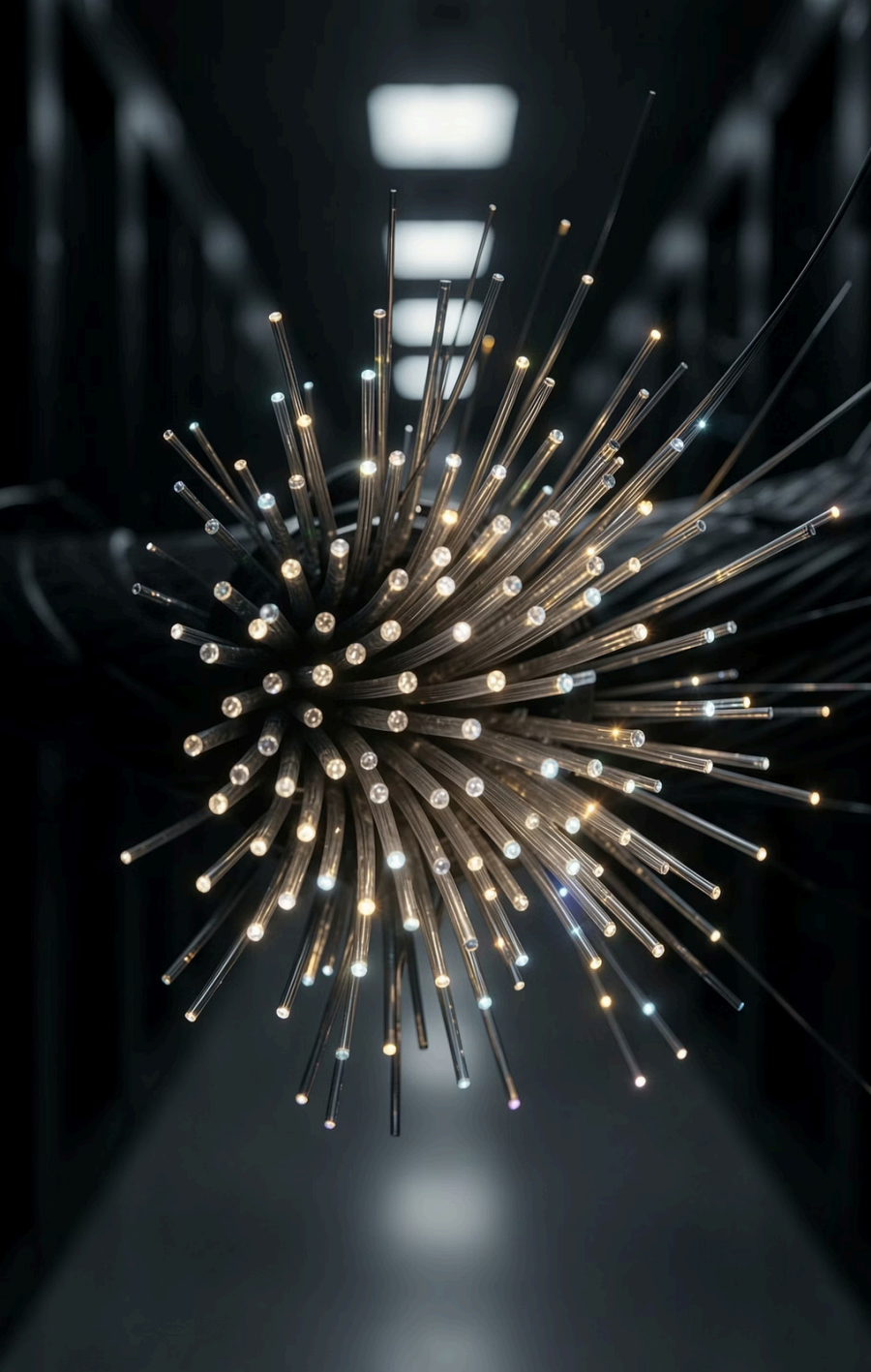
In telecommunications, **transmission (Tx)** is the process of sending and propagating an analog or digital information signal over a physical medium — wired, optical fiber, or wireless.

Examples

Data packets, phone calls, emails

Digital Communication

Transmission of a digital or digitized analog signal



Transmission Technologies & Protocols

Modulation & Demodulation

Converting signals for transmission and back

Line Coding & Equalization

Encoding data and compensating for signal distortion

Error Control & Sync

Bit synchronization and error detection/correction

Multiplexing

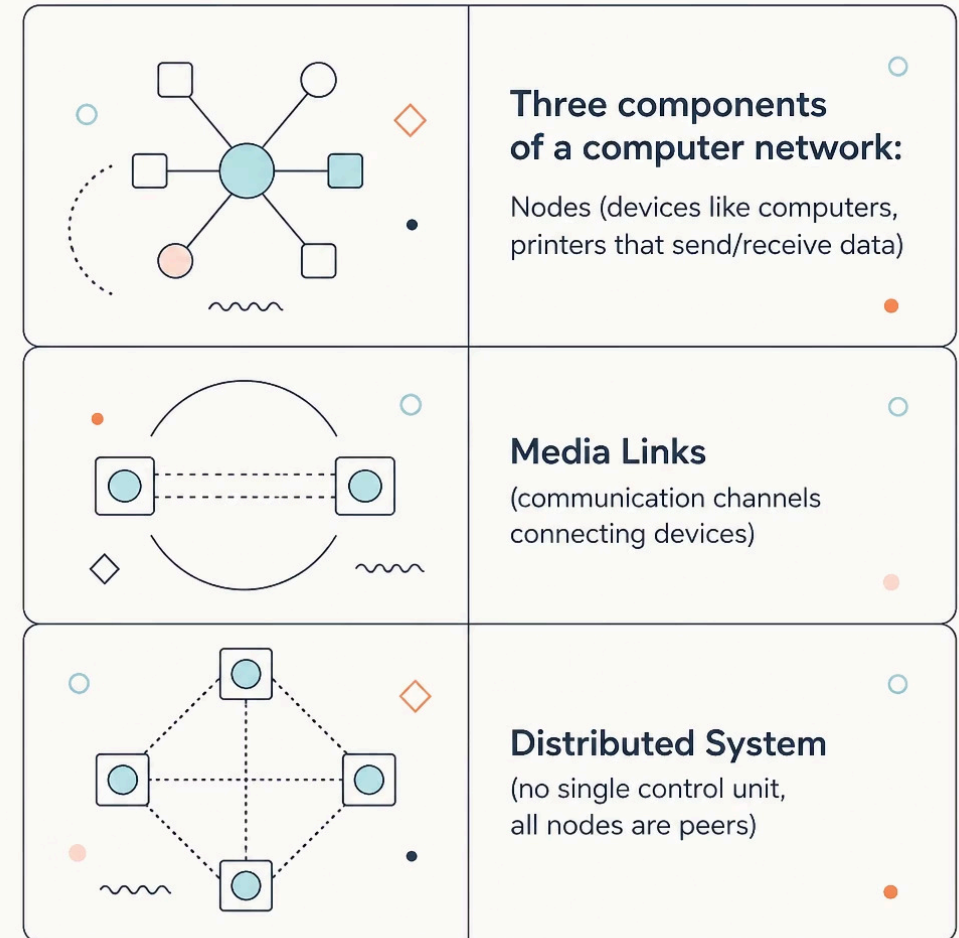
Combining multiple signals over one medium

What Is a Computer Network?

A **network** is a set of devices (nodes) connected by communication channels (media links). A node can be any device capable of sending or receiving data — a computer, printer, etc.

📄 A computer network is a **distributed system** — not a master-slave architecture.

The best example of a computer network is the **Internet**.





Network Criteria

Every network must meet three core criteria:



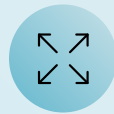
Performance

How fast and efficiently data is transmitted



Reliability

Consistent, fault-tolerant delivery of data



Scalability

Ability to grow and handle increased load

Transmission Media

Transmission media is the pathway that carries information from sender to receiver. Data travels as **electrical or electromagnetic signals** through various mediums.



Electrical Signal

Transmitted as current through copper wires

Electromagnetic Signal

Series of energy pulses at various frequencies — travels through fiber, atmosphere, water, or vacuum

Wired (Guided) Media



Bound transmission media are physical cables limited by geography. Each type has distinct characteristics for speed, noise, cost, and installation.

→ Twisted Pair Cable

Common, cost-effective for short distances

→ Coaxial Cable

Higher bandwidth, better noise resistance

→ Fiber Optic Cable

Highest speed, immune to electromagnetic interference



Wireless (Unguided) Media

Unbound transmission media transmit data without cables — not limited by physical geography. Wireless communication is increasingly popular in offices, campuses, and homes.



Radio Waves

Long-range, used in broadcast and Wi-Fi



Microwave

High-frequency, point-to-point links

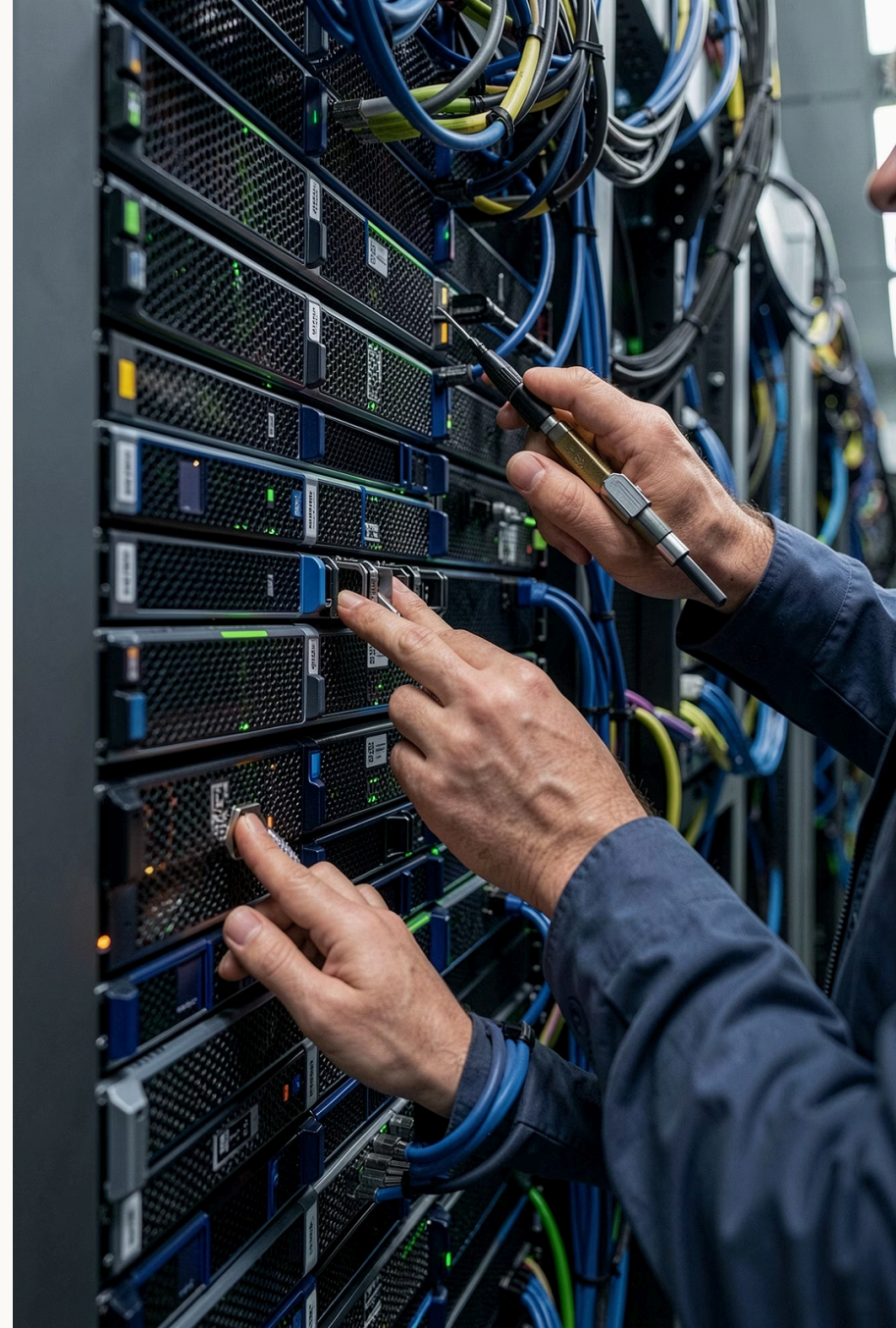


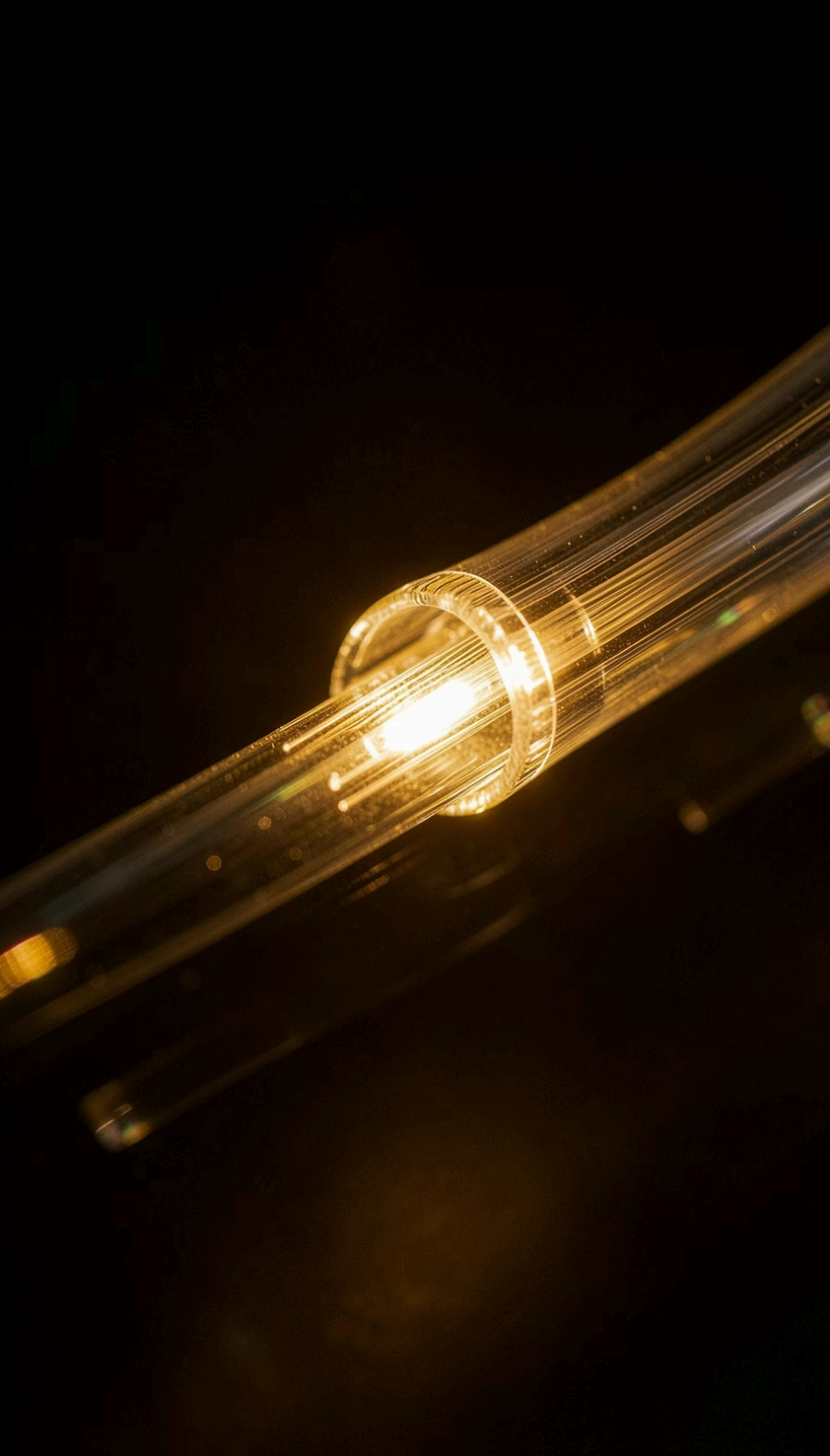
Infrared

Short-range, line-of-sight communication

Network Problems & Troubleshooting

Understanding common network errors, performance degradation, and security issues — and how to resolve them efficiently.





Factors Affecting Data Transmission

Bandwidth

Data carrying capacity of a channel. Higher bandwidth supports higher data rates.

Radiation

Signal leakage from the medium due to undesirable electrical characteristics.

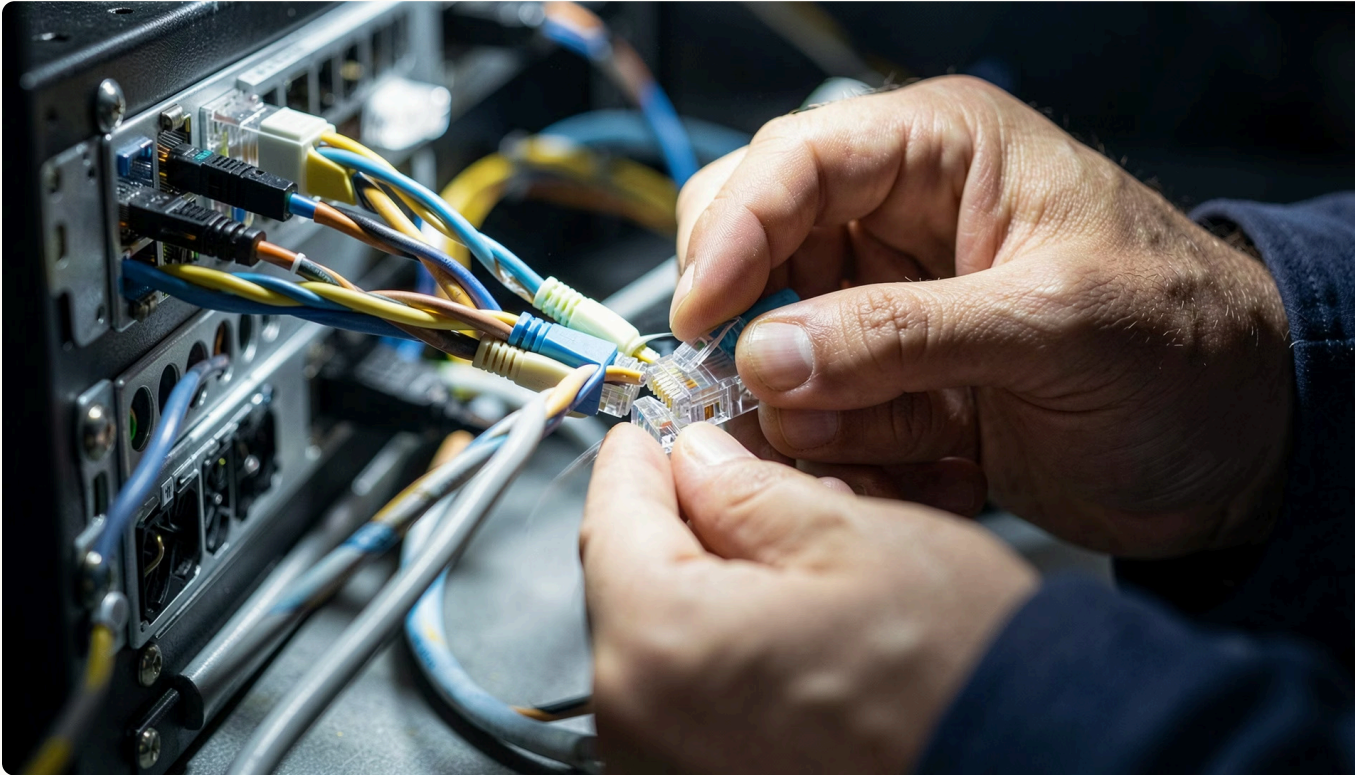
Noise Absorption

Susceptibility to external electrical noise causing signal distortion.

Attenuation

Loss of energy as signal propagates. Depends on frequency and physical media characteristics.

FCS & Alignment Errors



FCS Errors

Frames include a **File Check Sequence (FCS)** number calculated via CRC. A mismatch between sent and received FCS values signals corruption — most commonly caused by **noise on the cabling** (lights, motors, tight bends, poor terminations).

Alignment Errors

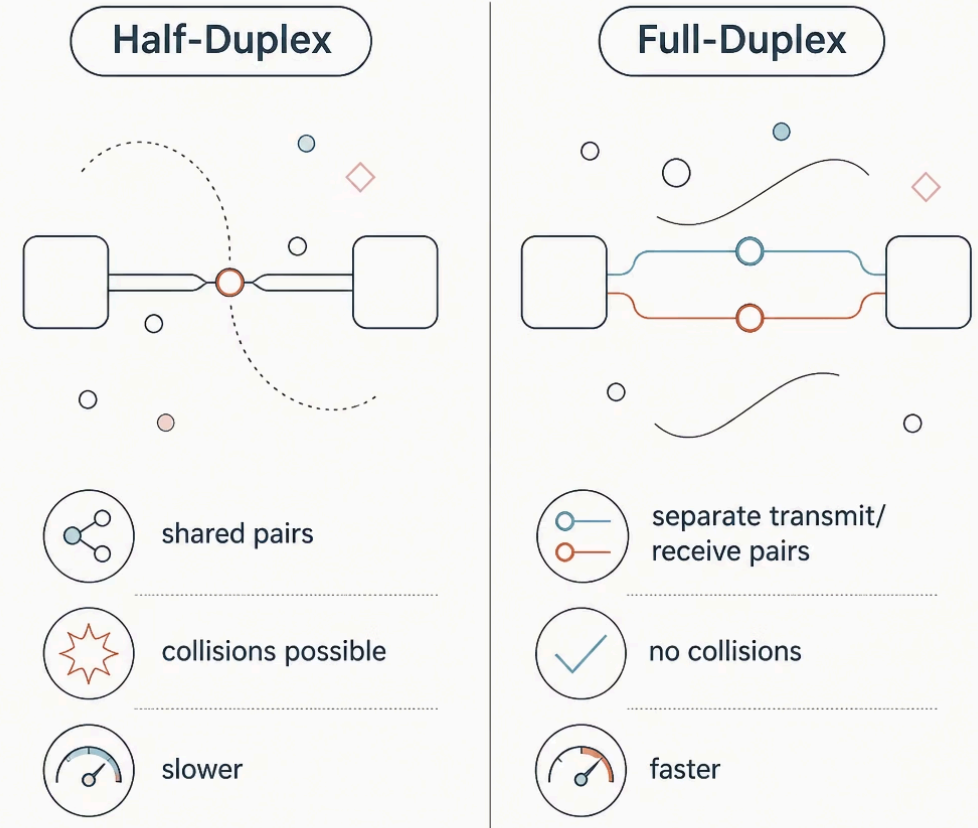
Ethernet frames must be evenly divisible by 8 bits. Misaligned frames always generate FCS errors and typically stem from cabling noise or faulty NIC hardware.

Collisions & Late Collisions

What Causes Collisions?

Collisions occur when multiple devices transmit simultaneously. Rare on modern switched networks, but happen when ports are misconfigured as **half-duplex**.

- Half-duplex ports share transmit/receive pairs → collisions
- Duplex mismatch (one end full, one end half) causes rapid error buildup
- Fix: Switch connection to **full-duplex**





Discards & Unknown Protocol Errors

Discards

Devices discard packets when low on buffer memory or when VLANs are misconfigured. Excessive discards force TCP retransmits (increasing latency) and cause UDP artifacts. Solutions: upgrade port bandwidth or split traffic across links.

Unknown Protocol Errors

A device receives a packet it cannot interpret — usually because a required protocol is disabled, or an unwanted one is enabled. Most common after new device configurations or hardware swaps.

Size Errors & Performance Degradation

Size Errors

Frames that are too short (**runts**, under 64 bytes), too long (over 1,518 bytes), or giant (over 6,000 bytes) generate errors. Almost always caused by **hardware or software stack problems** — fix by updating software or replacing hardware.

Performance Degradation

Loss of speed and data integrity, especially in large networks. Solutions: invest in quality hardware, ensure proper configuration, verify all devices routinely, and guard against rogue infected systems wasting bandwidth.



A close-up photograph of a server rack door. The door is black with a perforated metal mesh. A silver metal padlock is attached to the door handle. The padlock has the text "LMG62K" engraved on it. The background is dark and out of focus.

Host Identification & Network Security



Host Identification

Proper addressing is essential. Large networks require **DHCP servers** and domain controllers — manual addressing becomes impractical at scale.



Security Threats

Larger networks offer more vulnerable entry points. More users, passwords, and hardware mean more opportunities for intruders.



Defenses

Firewalls, proxies, strong antivirus, strict password policies, network analysis tools, physical security, and internal network segmentation.

Workstation & Server Bottlenecks

A file transfer passes through many components before leaving the system — each a potential bottleneck.



Hard drive, OS, CPU, and firewall layers are the most common performance constraints on the workstation side.

OS, CPU & Hard Drive Impact



Operating System

Driver config, CPU prioritization, and IP stack tuning affect performance. Older and Windows systems typically underperform vs. Unix equivalents.



CPU Usage

20–60 background programs run by default. One CPU-hogging process can seriously impede throughput. Compression (e.g., ZLIB) adds additional CPU load.



Hard Drive

Usually the **slowest component**. Simultaneous drive access by multiple processes drops throughput exponentially. High-end drives or RAID's help but still suffer under concurrent access.

Firewalls, Filters & Key Takeaways

Firewalls & Filters

Software firewalls inspect every packet against rules, consuming CPU and adding delay. Multiple layers (firewall + content filter + NAT) compound the problem. **Disable unnecessary rules** and allow MTP/IP traffic unfiltered where possible.

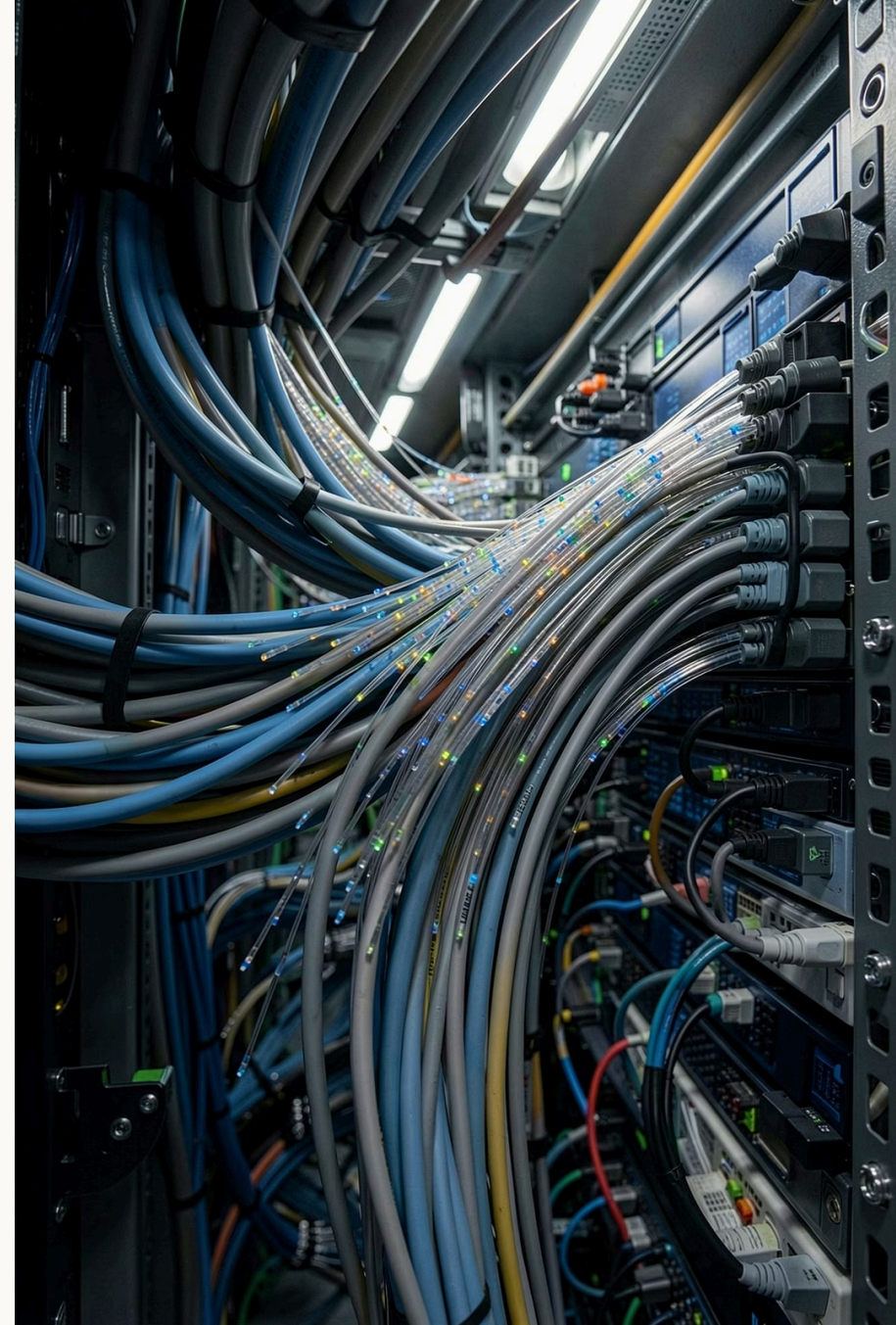
📄 See Tech Note 0002: "Configuring Firewalls"

Core Takeaways

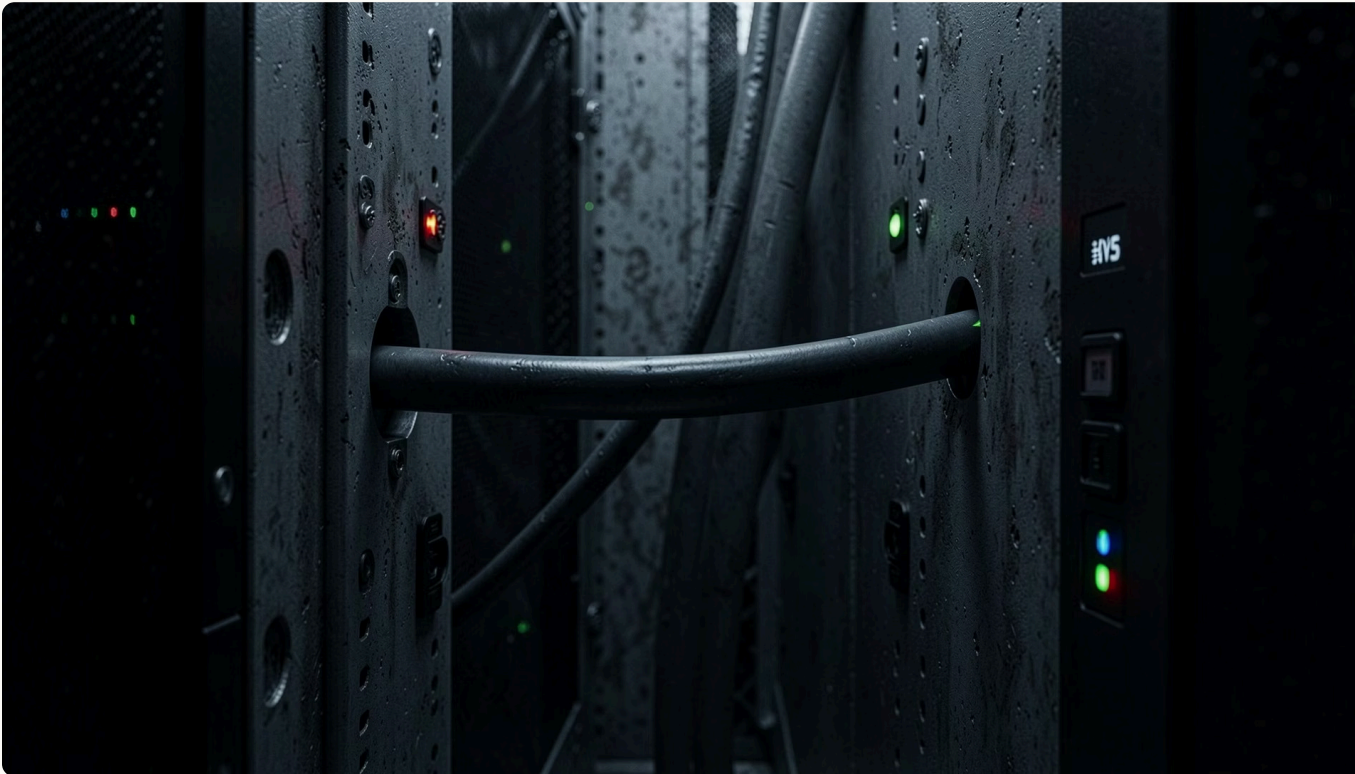
- Start with **quality hardware** — performance is only as good as its components
- Ensure **proper configuration** of all devices, VLANs, and duplex settings
- Use **SNMP tools and protocol analyzers** to diagnose errors quickly
- Secure the network with **firewalls, policies, and segmentation**

Network Performance Factors

A comprehensive guide to the hardware, software, and environmental factors that impact MTP/IP and high-speed network performance.



Virtual Private Networks



Datagram-Based VPNs (e.g., IPsec)

Process one datagram at a time with minimal overhead. May rarely cause MTU issues but unlikely to hurt performance except on very fast LANs.

Tunneling VPNs (SSL VPNs)

Low-quality VPNs tunnel all datagrams across a single TCP/IP connection, introducing substantial overhead and exponentially worsening TCP flow control. **MTP/IP cannot be used with SSL or tunneling VPNs.**

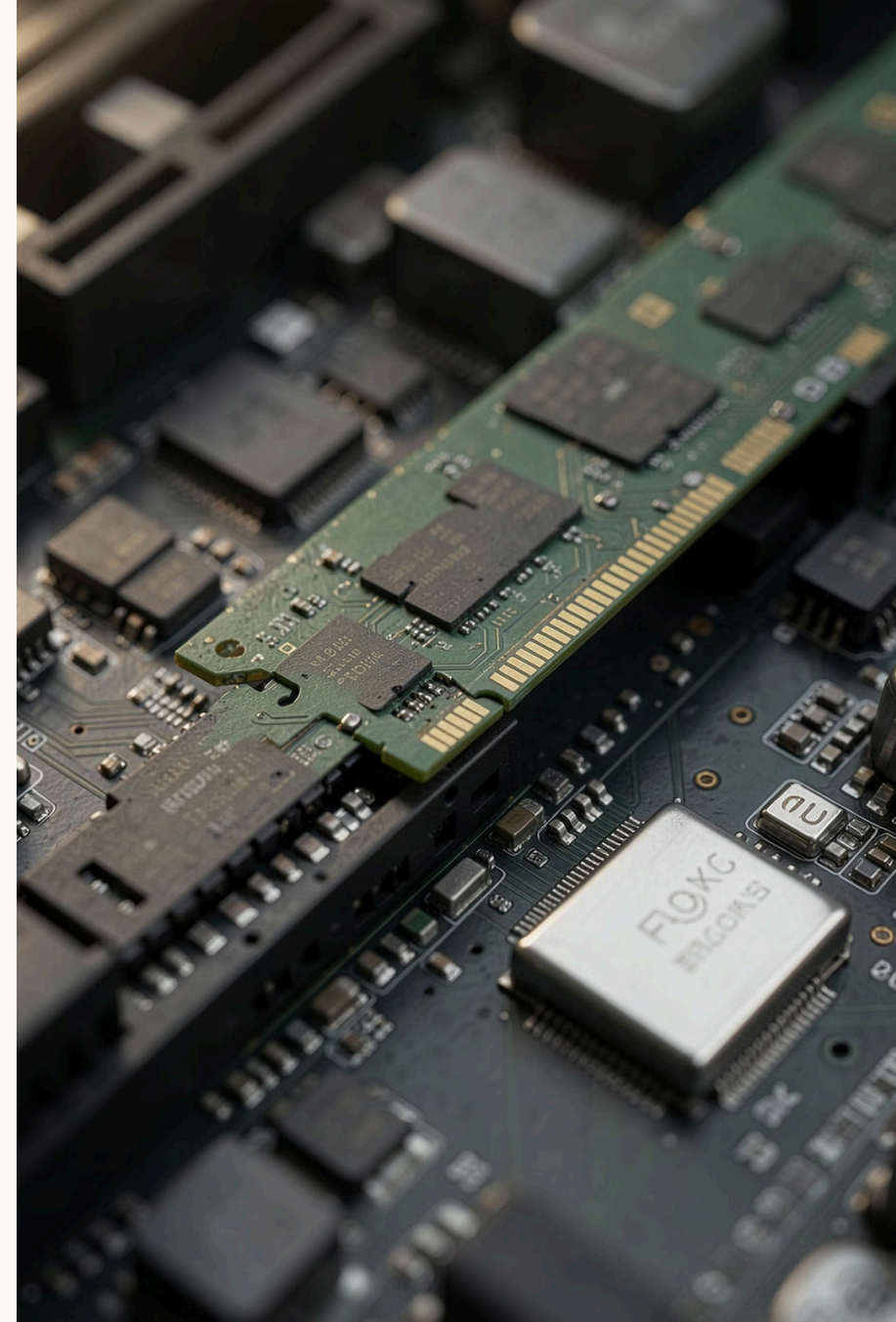
Memory & System Clock

Memory (RAM)

Inadequate memory forces disk access, degrading performance. Windows has paged pool limits — errors like *"Insufficient system resources"* may require adjustment. **Windows Server 2012+** is recommended for speeds above a few hundred Mbps.

System Clock

MTP/IP depends on accurate timing. Radical clock changes, sleep mode, failing motherboard batteries, or misconfigured NTP can cause transactions to fail. Battery failure is a risk on hardware over five years old.



HARDWARE

Network Interface Card (NIC)

Speed Matching

A 1 Gbps NIC on a 10 Gbps network caps throughput at 1 Gbps.
Multigigabit paths require matching NIC speeds.

IP Offloading

Offloads checksum calculations to NIC hardware. Requires compatible drivers — test with offloading both enabled and disabled when troubleshooting.

MTU Settings

Set MTU to at least **1500** for sub-gigabit Ethernet, and **9000 (Jumbo)** for true multigigabit paths.

User Interaction & Virtual Machines

User Activity

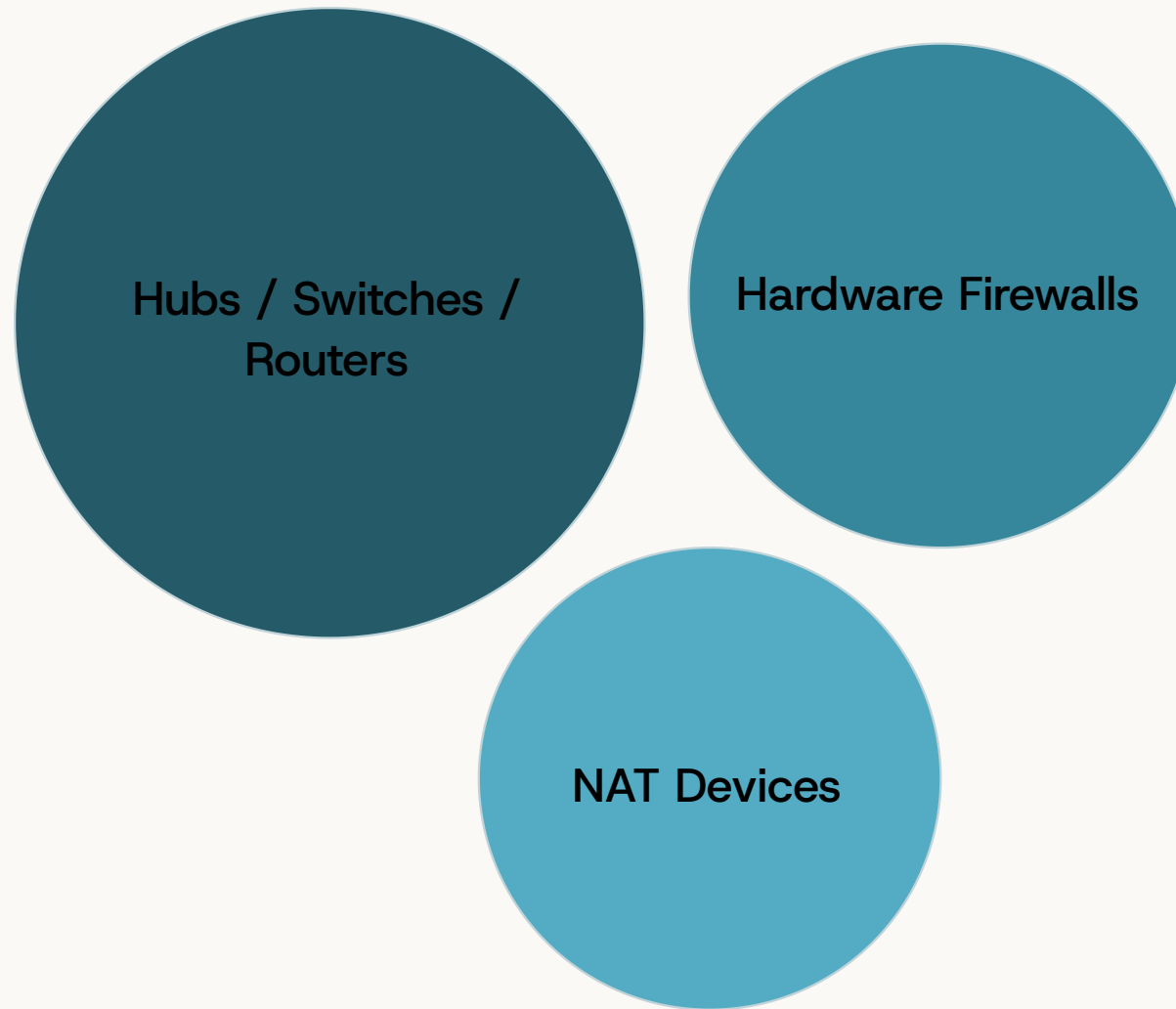
Any UI activity disrupts performance. Windows prioritizes user actions — clicking the desktop once per second in an RDP session can drop throughput by **25%**. The Activity Monitor can cause up to **50%** drop. During testing, all users should log out and disconnect from RDP.

Virtual Machines

Virtualization more than doubles processing per datagram. Multiple guests contend for limited CPU, memory, and disk. Performance costs are substantial — test in the **host** system rather than the guest whenever possible.



Network Devices & Firewalls



A typical Internet path involves 10–20 hops. Firewalls must be explicitly configured to allow MTP/IP traffic — some may allow traffic initially, then reduce or cut it off after several minutes. See Tech Note 0002 for firewall configuration guidance.

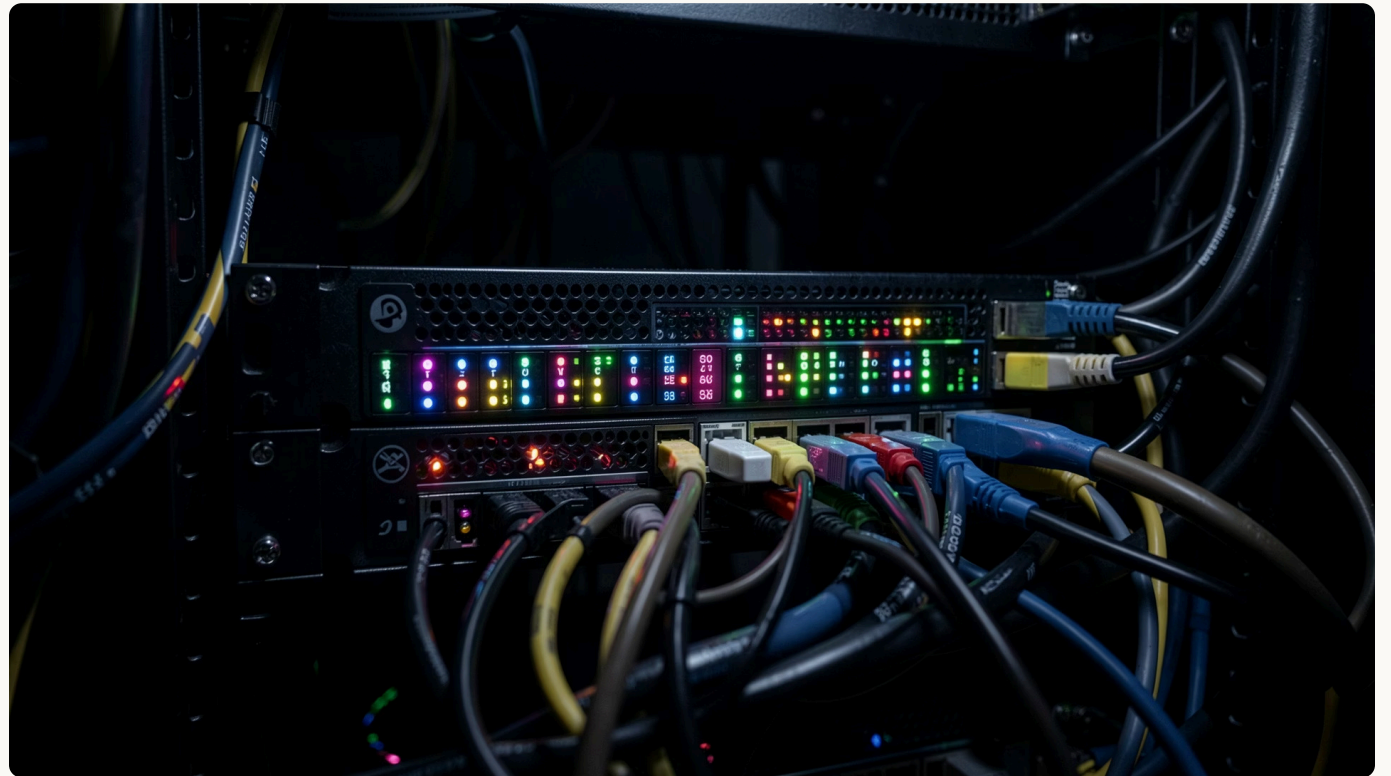
Hardware VPNs & NAT

Hardware VPNs

Encapsulate packets within other packets, often adding authentication and encryption. Datagram-based VPNs (IPsec) add minimal overhead. Tunneling VPNs (SSL) introduce substantial overhead – **MTP/IP cannot be used with them.**

NAT (Network Address Translation)

NAT devices map private IPs to a shared public IP. Some may forget session state, causing transactions to fail after several minutes. Servers behind NAT require explicit port mapping.



Maximum Transmit Unit (MTU)

1

Default MTP/IP Limit

MTP/IP limits datagrams to **1480 bytes** (including headers), leaving 20 bytes for MPLS, PPPoE, or IPsec overhead.

2

Troubleshooting with VPNs

If using MTP/IP with VPN or PPPoE and performance is poor, set **MaxDatagram to 1280**, then increase in increments of 16 until performance stops improving.

3

Jumbo Frames

Where all devices support Jumbo frames (9000 MTU), set **MinDatagram to 8192** for substantial gains. 10 Gbps+ equipment supports Jumbo frames; paths fragmenting above 1500 bytes likely cannot achieve 10 Gbps speeds.

Wireless, Bonded Lines & WAN Appliances



Wireless

Subject to variable conditions. Some media correct errors (causing delays); others drop data. Disabling hardware error correction may improve MTP/IP performance. TCP-tunneled wireless (some satellite/cellular) performs very poorly.



Bonded Lines

Bonded lines are not equivalent to a single line of the same speed. For best MTP/IP performance, all lines must converge to one IP address with round-robin UDP/IP distribution.



WAN Acceleration

Devices that modify UDP datagrams (e.g., SilverPeak) may corrupt packets. **Bypass WAN acceleration appliances for MTP/IP traffic** unless tests show clear benefit.

Bandwidth Management & Other Traffic

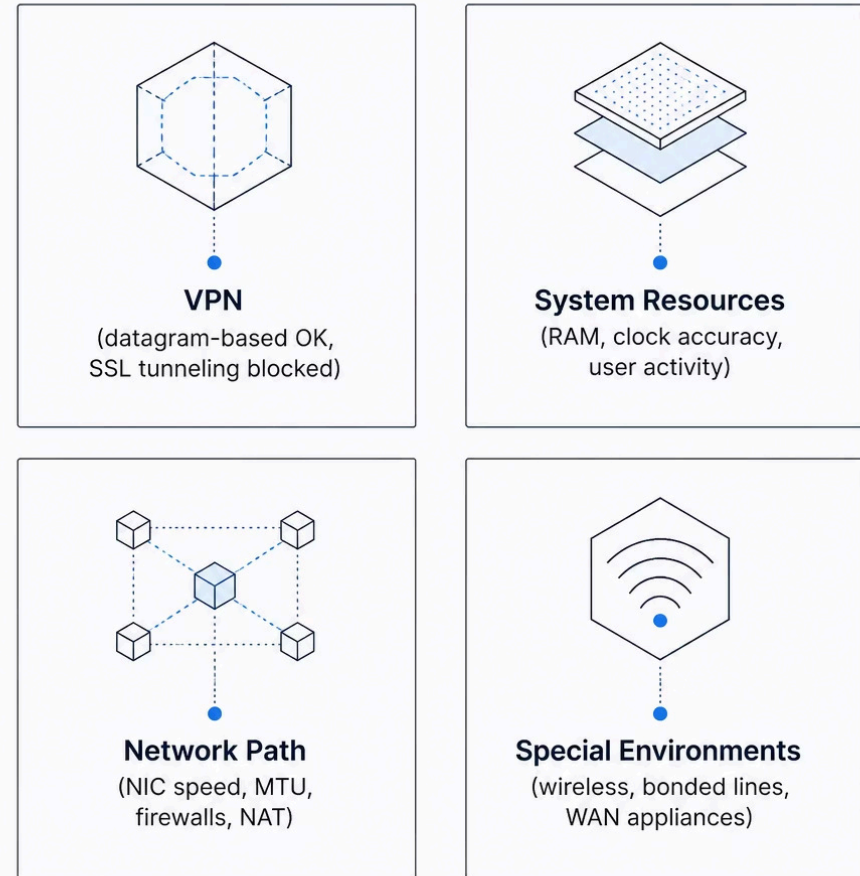
Bandwidth Management Devices

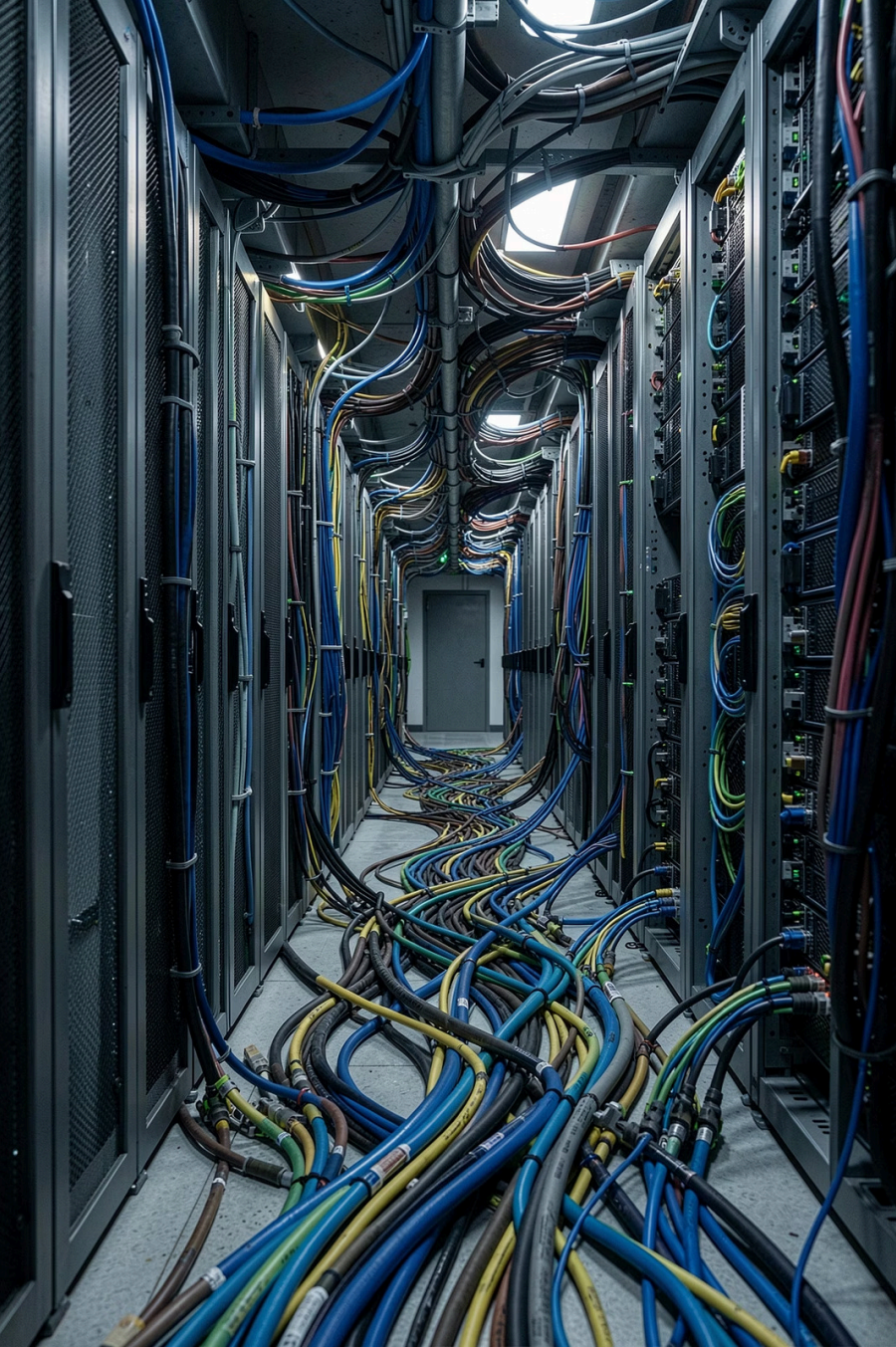
These prioritize, compress, or cache traffic. MTP/IP works well with correctly configured, standards-compliant devices — but misconfigured devices can severely degrade performance.

Other Traffic

Third-party traffic on the same path has the **largest impact** on performance. Oscillations in traffic flows can cause disproportionate interference.

- Key takeaway: Test in real-world environments whenever possible. Avoid SSL VPNs, ensure NIC and MTU are properly configured, and minimize competing traffic during performance testing.





Network Troubleshooting Guide

Identifying requirements and strategies to resolve common business network problems — from connectivity failures to configuration issues.

IT REFERENCE

SECTION 1.3

Wireless Signal but No Connection

Diagnose

Move the computer next to the router. If it connects, the network card receives signal but may not transmit effectively — a hardware issue.

Fix

Update the network card's drivers first. If that fails, the hardware may need to be replaced entirely.



Network Outages & IP Conflicts

NetBIOS Conflicts

Unpredictable outages or inaccessible files may signal a NetBIOS conflict — common on older Windows systems, especially after service pack upgrades. **Fix:** Disable WINS/NetBT name resolution (unless required) or rename the computer/domain.

Duplicate IP Addresses

Two devices assigned the same IP can block access and cause network-wide lag. **Fix:** Reconfigure DHCP to exclude static IPs from the pool, ensuring all machines receive proper addresses.



Slow Applications & Poor VoIP

Slow App Response

Usually caused by high bandwidth use — streaming or large downloads. Monitor employee usage and enforce proper network policies. If usage is fine, consider a bandwidth upgrade.

VoIP Stutters & Delays

Install **jitter buffers** to cache VoIP packets for smooth playback. Also update codecs and drivers — packet loss is a major cause of stuttering audio and video.

Cable, Connectivity & Collision Issues



→ Cable Problems

Cables can be cut or shorted. Use cable testers to detect cuts, shorts, interference, and connector faults.

→ Connectivity Failures

Can occur after config changes or hardware malfunction (hub, router, switch).

→ Excessive Collisions

Caused by bad network setup, heavy data transfers, or a **jabbering NIC** (stuck in transmit mode – TX light stays on constantly).

Software & Dead Drop Symptoms

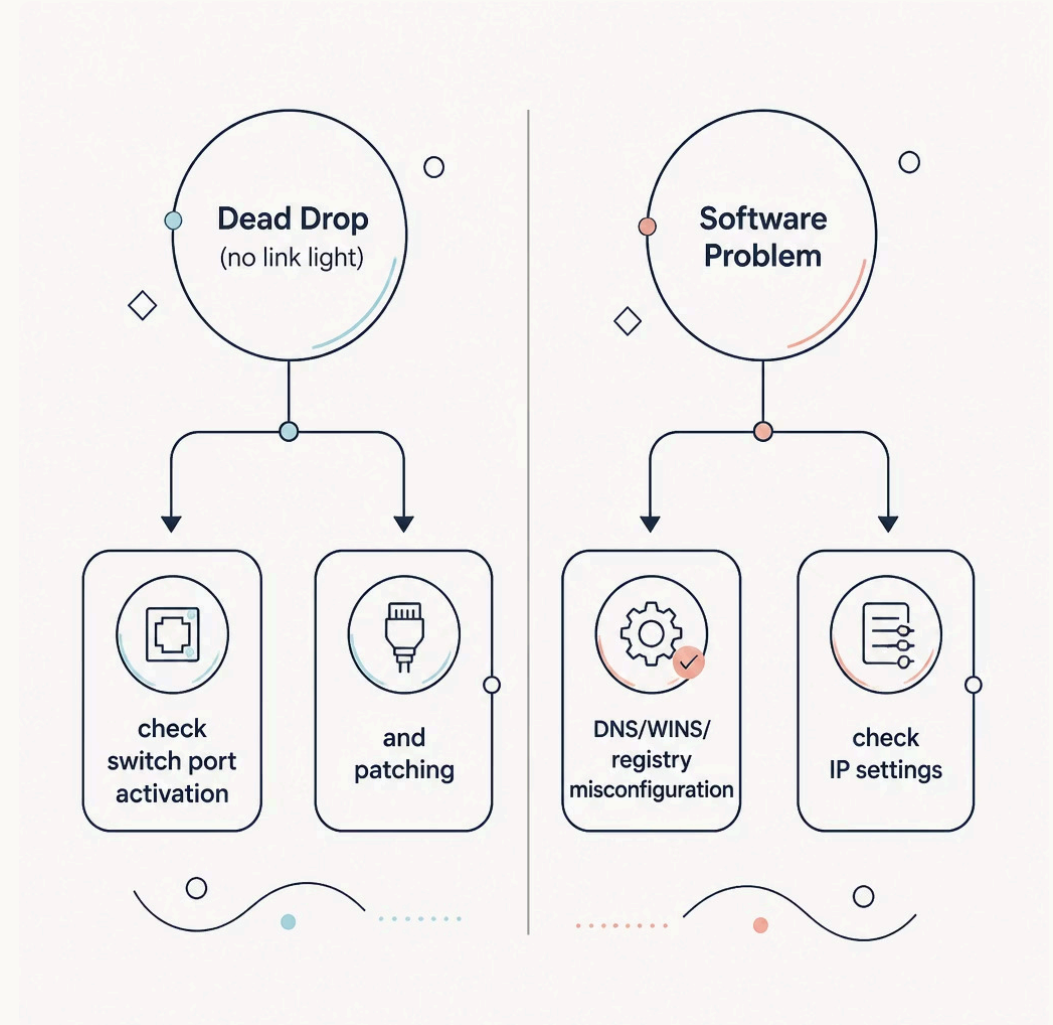
Software Problems

Network issues can often be traced to software configuration — DNS, WINS, or the registry. Duplicate IP addressing can also cause intermittent communication failures.

Dead Drop

Symptom: Device connected to wall jack shows no link light.

Cause: Connection not patched through, or switch port administratively disabled. **Fix:** Activate the switch port and verify patching; test all moved connections.



Can't Get an IP Address

01

Is it one user or many?

If one user: check NIC settings — ensure DHCP is enabled, not static.

02

Check the VLAN

Verify which VLAN the switch port belongs to. If other devices on that VLAN also fail, the router may not be forwarding DHCP requests.

03

Check the DHCP Server

If many devices across subnets are affected, the DHCP service may be down or the address pool exhausted.



Can't Connect to Application Server

Symptom

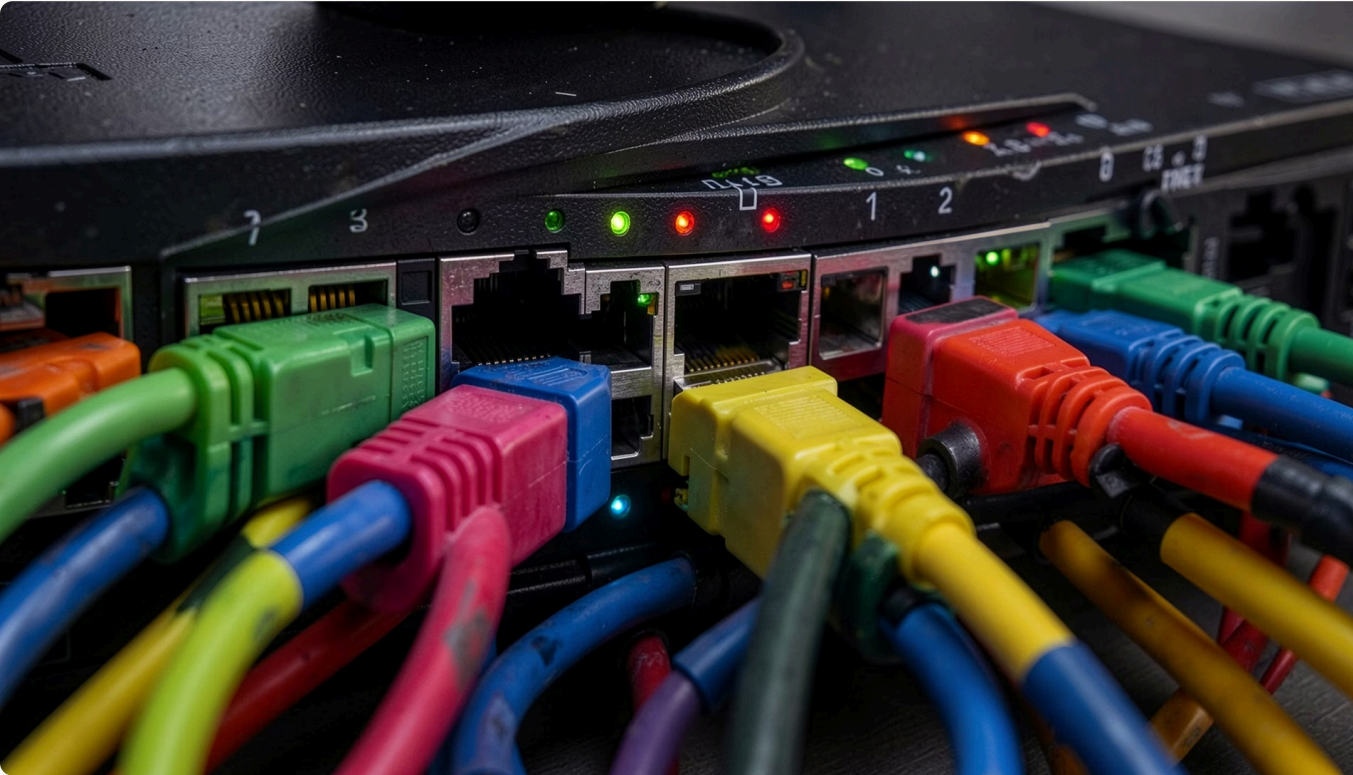
Email or CRM apps report they can't reach the server. Users often claim "the network is down" — but that's rarely the true cause.

Diagnose

Ask: is this constant or sporadic? Ping the server to check routing. If ping succeeds but issues persist, check server load (e.g., backups running) and WAN utilization with an **SNMP monitoring tool**.



Incorrect VLAN Assignment



Symptom

IP phones won't register, PCs can't reach servers, or wireless users get improper addressing — typically after deploying new services like VoIP or wireless.

Cause

Switch ports weren't reconfigured to support the new service VLANs.

Resolution

Test the port with VLAN tagging to verify which VLANs are active. Check the DHCP-assigned IP to confirm VLAN, or inspect the switch config directly.

Duplex Mismatch

Symptom

Link lights active, but throughput drops to **100 Kbps or lower**. Connection works – just very poorly.

Cause

One side forced to full duplex; the other auto-negotiates and defaults to half duplex. The full-duplex side interrupts transmissions, causing aborts and retransmissions.

Resolution

Set **all connections to auto-negotiate** unless there's a specific reason not to. For inter-switch links, statically set **both sides** to full duplex.

- ❏ These common network issues are easily resolved with a little time and effort – freeing your IT team to focus on more significant problems and boosting overall business productivity.

Printing Problems

Symptom

Printing does not consistently work on the network. A printer may appear available, but print jobs sent to it are not completed.

Cause

Determine if only one user is affected or several. If one user, the PC may not be mapped correctly to the print server. Otherwise, the network between client and printer may be to blame — packet loss or printer network connectivity issues.

Resolution

Check printer configuration for a valid IP address and print server access. Update printer drivers. Ensure traffic is flowing to and from the printer on the network and all drivers are current.



Poor or Bad Cable

Symptom & Cause

The client PC may link to the network but perform poorly, or not connect at all. Gigabit requires four pairs of cable — anything below **Category 5** will not work. In older buildings, this is a key consideration. Any untwisting of the cable (often near the RJ-45 termination or patch panel) causes signal loss and **FCS Errors** on switch ports or network adapters.

Resolution

In most cases, the cable simply needs to be **replaced**. If the problem is untwisted pairs, re-terminating the cable may resolve the errors. When supporting Gigabit or Power over Ethernet, the cable must be **Cat 5 or better**.

- ❏ FCS Errors on a switch port are a strong indicator of physical cable issues — check terminations first.

DNS Problems



Symptom

User cannot access the internet or key applications. The network appears to be down.



Cause

The client cannot resolve a server name to its IP address, so it won't send a connection request. Common causes: wrong DNS server configured, DNS requests the server doesn't have, or packet loss. DNS is UDP-based — lost packets are not retransmitted, causing failure.



Resolution

Check client DNS settings; correct via client or DHCP server. Test DNS repeatedly for delay or packet loss. Capture failing requests to check for server response. Use tools like the **EtherScope Network Assistant** for Cable Verification, Service Performance Testing, and Switch Scan to monitor printer traffic on the switch port.



Wireless Client Can't Connect

The client detects the wireless access point but cannot connect to the network. Security credentials, wireless channel interference, and dead spots can cause this. Since wireless is invisible, proper tools are essential for diagnosis.

Signal Strength

Use a wireless monitoring tool to measure signal strength from the affected area.

Site Survey

Conduct a site survey to look for rogue or unknown APs on overlapping channels that may affect known-good users.

Interference

Check for noise from surrounding APs or devices like microwaves and cordless phones.

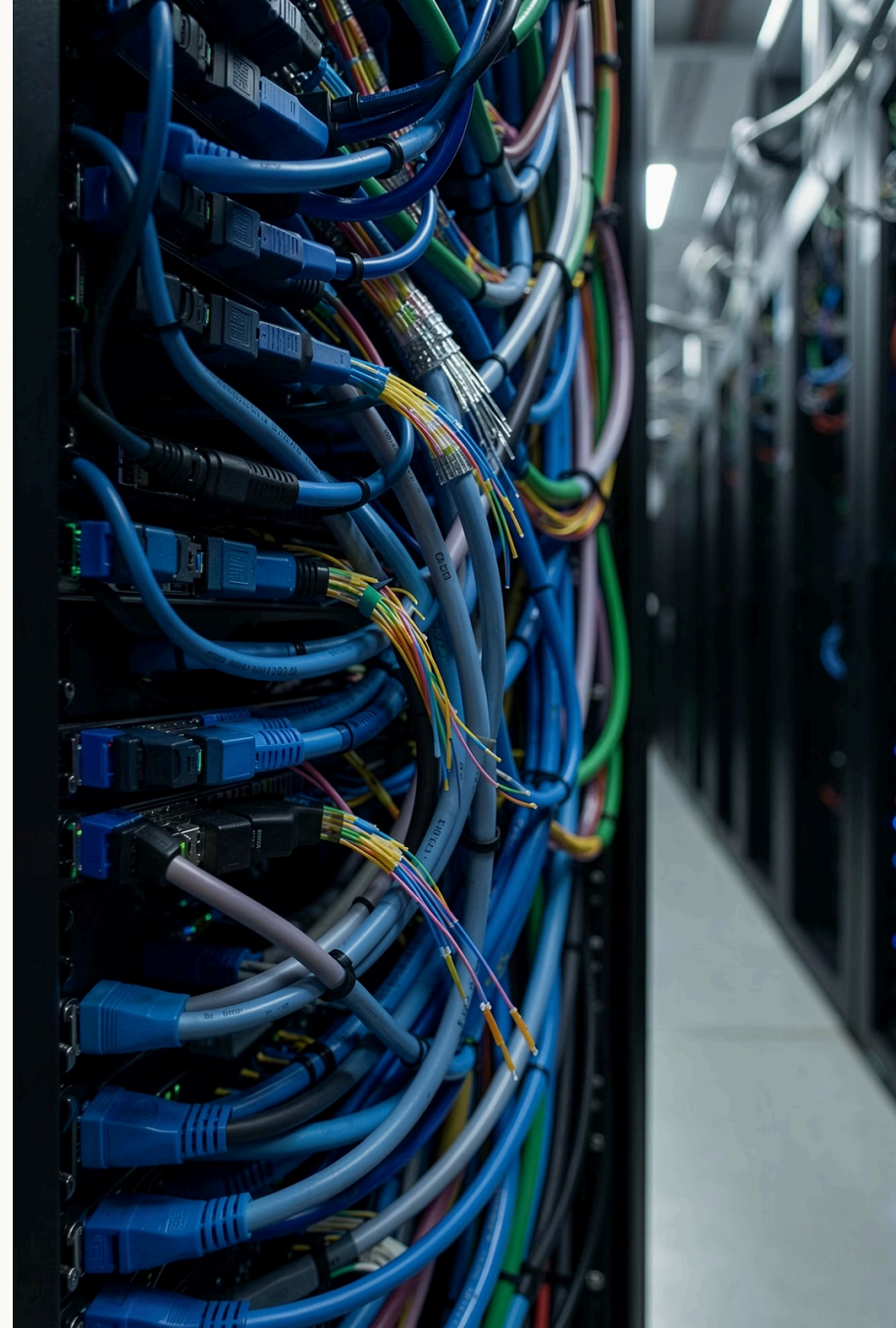
Connection Steps

Monitor the client as it attempts to connect and watch for which step fails — **association**, **authentication**, or **authorization**.

Public Switching Computer Network Protocols

Session 2 — Understanding how connected devices communicate through shared rules, packet structures, and data link layer protocols.

NETWORKING FUNDAMENTALS



What Are Network Protocols?

Assembling physical network hardware is not enough — devices need a shared communication language. **Network protocols** define the rules that let devices understand each other's signals.

Address

Route data to the correct recipient(s)

Transmit

Physically send data with security protection if needed

Respond

Receive messages and reply appropriately

- ❏ Like a postal service — but with advanced capabilities like **streaming** (constant flow to one destination) and **broadcasting** (copies to multiple destinations at once).



How Protocols Use Packets



Networks organize data into small pieces called **packets**. Larger messages are subdivided for better performance and reliability. Protocols define how packets must be formatted.

Protocols working in layers use **encapsulation** — embedding one protocol's formatted data inside another's packet.

Header

Sender/receiver addresses, sequence counters, checksums

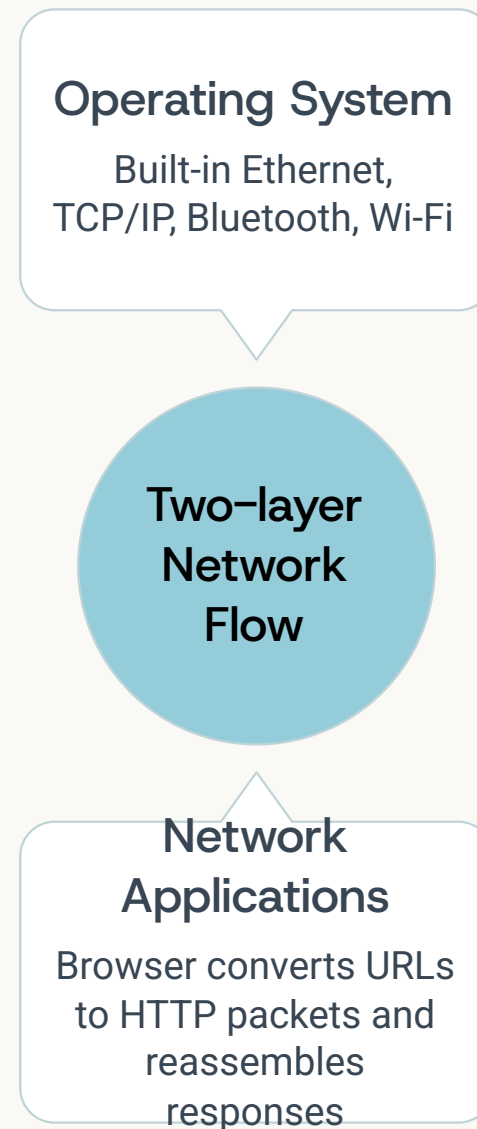
Payload

The actual data being transmitted

Footer

Error detection (not used by all protocols, e.g., IP)

How Devices Use Protocols



Operating systems provide built-in support for lower-level protocols (Ethernet, TCP/IP, Bluetooth, Wi-Fi) connected to physical network interfaces. Network applications handle higher-level protocols — for example, a web browser translates addresses like <http://lifewire.com> into HTTP packets. The receiving device strips headers/footers and concatenates packets in the correct sequence to reassemble the original message.

Data Link Layer — OSI Layer 2

The **data link layer** transfers data between adjacent nodes on a LAN or WAN segment. It detects and may correct errors from the physical layer.



Local Delivery

Frames stay within a local network — inter-network routing is a higher-layer function



Media Arbitration

Like a neighborhood traffic cop — manages access to the medium, detects and recovers from collisions



Key Protocols

Ethernet (LAN), PPP, HDLC, ADCCP (point-to-point). In TCP/IP, contained within the link layer



Bridging Features

Bridging operates at Layer 2 using **MAC addresses**. A wireless bridge maintains a MAC address table and forwards packets to the correct port.



Vendor Tip: MAC table size $\neq$ simultaneous connections. An ad claiming "supports 1,000 users" may only allow 128 concurrent connections. Always verify with the vendor.

Ethernet converters bridge one Ethernet port to a wireless WAN. **Super Ethernet converters (SEC)** support up to eight computers.

MAC Table Size

Typically 1–2,000 addresses; often larger than simultaneous connections

Simultaneous Connections

Wireless bridges support ~50 to several hundred users; more connections = higher cost

Spanning Tree (802.3)

Detects and disables routing loops in bridged networks

Switching, VLANs & MAC Sublayer

Switching

Some wireless APs include a built-in switch for Ethernet connectivity without external hardware

VLAN Tagging

Defines virtual LANs independent of geographic location

MAC Sublayer Functions

- **Error control** — Frame-exchange protocol with acknowledgments for error-free delivery
- **Congestion management** — CSMA/CA contention-based access (802.11b); polling rarely implemented
- **Packet aggregation** — Combines small packets to reduce transmit/receive switching time
- **Data protection** — WEP encryption (64-bit & 128-bit) at the MAC level

Data Link Layer Security



MAC Access Control Lists

Only MAC addresses in the ACL can connect to the AP



Protocol & Pair Filtering

Block specific Layer 2 protocols (IPX, NetBEUI, etc.) or specific MAC address pairs



Open-System Auth

Least secure — station simply identifies itself and requests access



Shared-Key (WEP)

Stations respond to AP challenge text using a distributed shared key



802.1x & Encryption Schemes

802.1x / EAP Authentication

More secure than shared-key WEP. Requires three entities:

- **Supplicant** – station requesting access
- **Authenticator** – typically the AP
- **Auth server** – e.g., RADIUS server

EAP allocates a new encryption key per session. 802.11i will evolve from 802.1x standards.

Encryption Options

DES

64-bit, user-selected key

3DES

Three 64-bit keys: encrypt
→ decrypt → re-encrypt

AES

Rijndael algorithm, 128/192/256-bit keys. Requires math coprocessor; included in 802.11i

Key Takeaways

1 **Protocols are the language of networks**
Without them, connected devices cannot communicate. They address, transmit, and respond to data.

3 **Layer 2 handles local delivery**
The data link layer manages frames, MAC addressing, collision recovery, and media arbitration on the LAN.

2 **Data is packetized and encapsulated**
Packets have headers, payloads, and footers. Layered protocols embed one inside another.

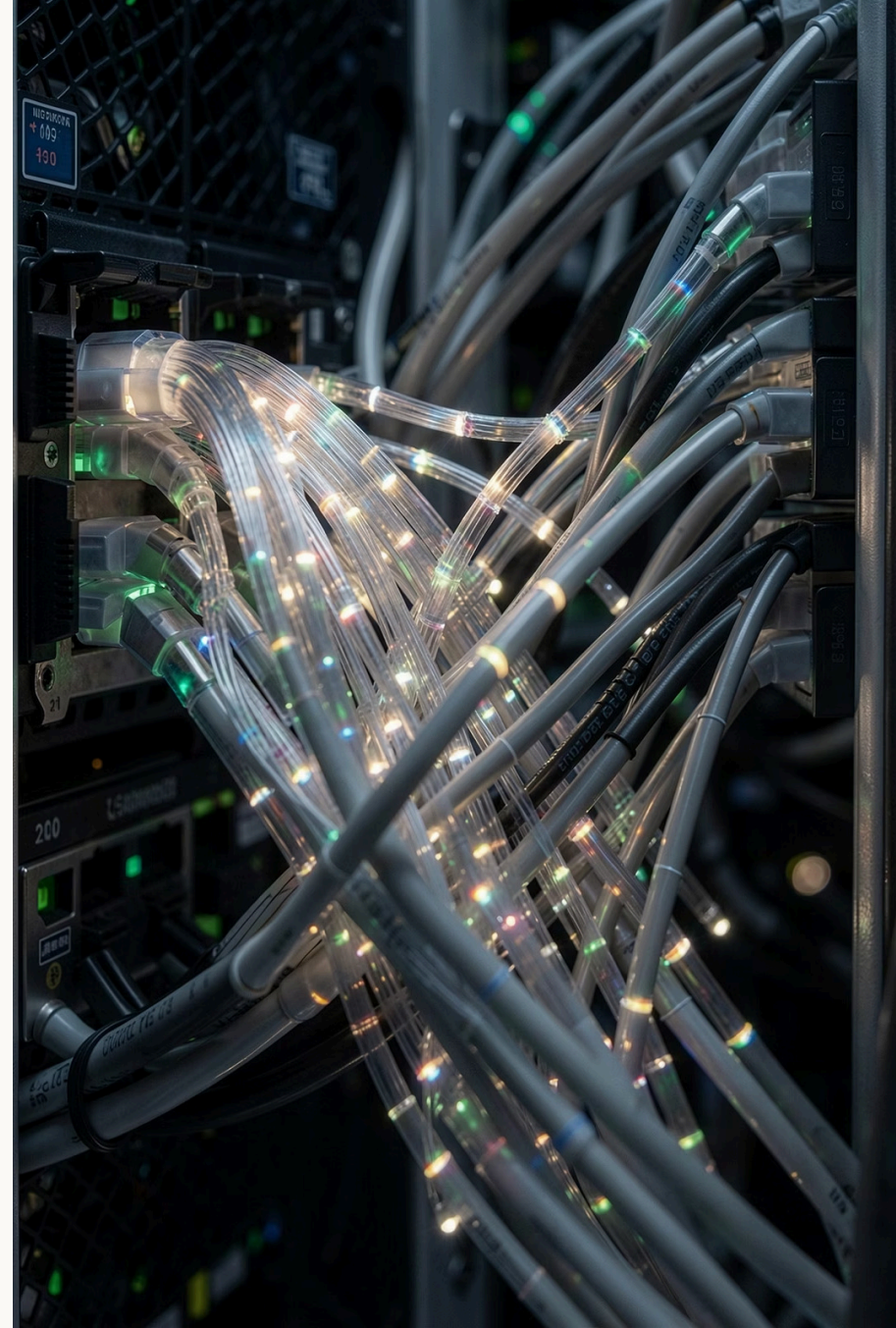
4 **Security spans access control to encryption**
From MAC ACLs and VLAN tagging to WEP, 802.1x/EAP, and AES — Layer 2 offers multiple security layers.

Data Link Protocols

Layer 2 protocols sit just above the physical layer in the OSI model, enabling communication between two devices across dedicated or shared media links.

OSI LAYER 2

NETWORKING FUNDAMENTALS



Two Types of Data Links

Dedicated Point-to-Point

A direct link between two devices — modems, bridges, or routers. Bits are always delivered in order with **no contention**.

Example: **PPP** (Point-to-Point Protocol) for dial-up Internet connections.

Shared Media Links

Multiple devices share the same cable, introducing contention for access.

Example: **Ethernet LAN**, where stations compete for the network.

Common Protocol Functions

Framing

Data broken into frames; only corrupted frames are retransmitted.

Encapsulation

Adds control info: addressing, error detection bits, and protocol control.

Fragmentation

Handles maximum packet size limits with reassembly at the receiver.

Connection Control

Connection-oriented signaling with graceful setup and teardown.



More Protocol Functions

Ordered Delivery

Handles reordering and lost packets within the DLC.

Session Control

End systems exchange status messages to set up and terminate reliable sessions.

Error Detection

Sender calculates a checksum; receiver verifies it.
Mismatch = corrupted frame → retransmit (reliable) or drop (unreliable).

Multiplexing

Multiple customers share one pipe via MAC addresses, TDM time slots, IP addresses, or socket addresses.

Addressing, Flow Control & Transmission Services



Addressing

On multipoint media (LAN), a device's address is the hardwired NIC address — e.g., MAC, link layer, IP, and socket addresses.

Flow Control

Prevents the sender from overflowing the receiver with more data than it can handle.

Transmission Services

Includes priority, security, and layer-specific services such as framing DLC.

Data Link Layer Specific Functions

The Data Link layer provides an **error-free point-to-point bit pipe** for transmitting Network Layer PDUs.



Framing

Flags — special bit patterns — mark the start and end of each frame.



Error Control & Detection

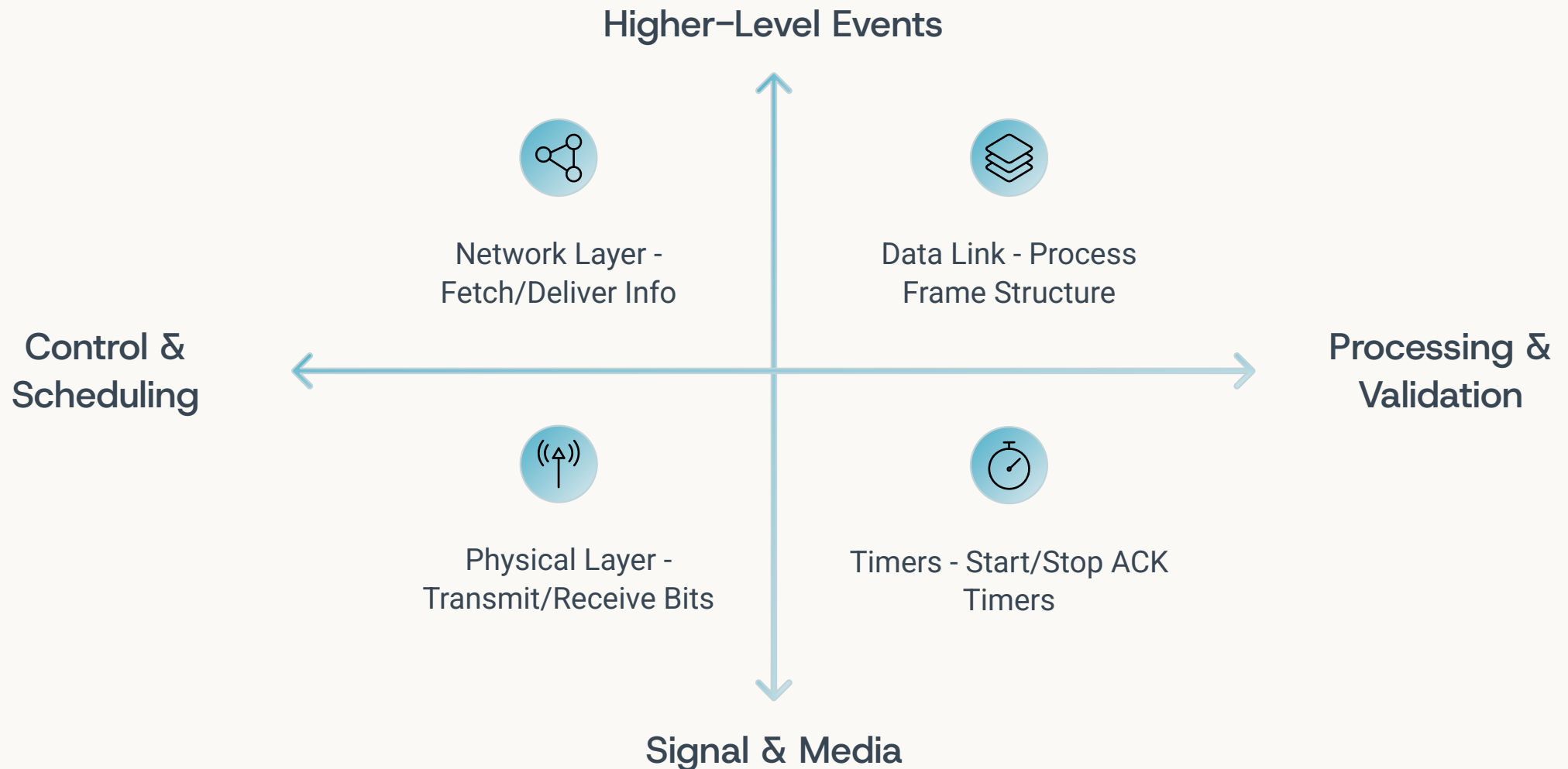
Procedures ensure frames are delivered accurately; corrupted frames trigger retransmission or are dropped.



Flow Control

Regulates data rate between sender and receiver to prevent overflow.

Layer Communication & Timers



Networks are **asynchronous** — packet and acknowledgment arrival times are unknown. Arrivals trigger protocol actions based on event type and state, such as **FrameArrival** or **CksumErr** (detected error). Timers manage flow: Start Timer, Stop Timer, Start Ack Timer, Stop Ack Timer. Enable/Disable Network Layer controls turn the flow of information on or off.

Common Data Link Protocols

SDLC

IBM's Synchronous Data Link Control for mainframe connections (point-to-point or point-to-multipoint).

HDLC

Based on SDLC; provides both reliable and best-effort service over serial interfaces (V.24, V.35).

SLIP

Transmits IP packets over dial-up links. No error detection – relies on higher layers.

PPP

More robust than SLIP; transports IP, IPX, and more. Identifies protocol type in each frame.



More Protocols: LAP & Frame Relay

LAP Variants

LAPB

Point-to-point on X.25 packet-switched networks.

LAPF

Data link for Frame Relay networks.

LAPD

Data link control over the D-channel of ISDN.

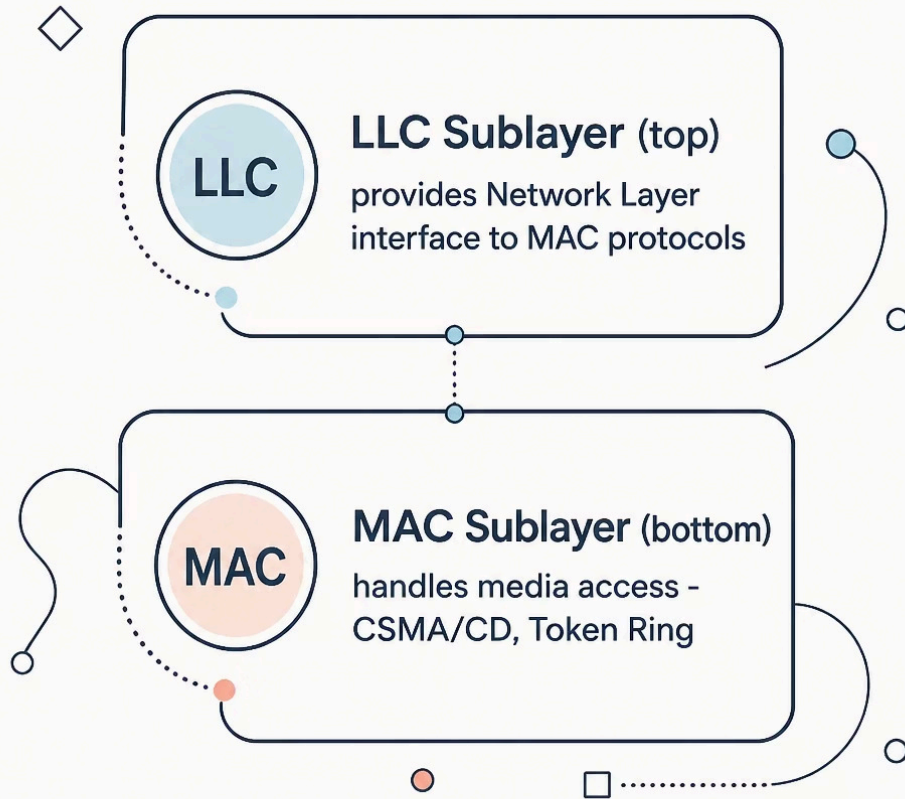
Frame Relay

Removes error-correction mechanisms from LAP/X.25 to **improve throughput** — trading reliability for speed.

LLC

IEEE 802.x family standard; also used by ANSI FDDI. A LAN data link protocol.

LAN Data Link Controls & Reliability



MAC + LLC Split

IEEE defines LAN technologies (Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring) split into:

- **MAC sublayer** – defines media access (CSMA/CD, Token Ring)
- **LLC sublayer** – lets the Network Layer communicate with MAC protocols

📄 **Reliability note:** Modern end systems handle reliability themselves (e.g., TCP). Network-level reliability is no longer essential.



Features of a Network Layer Protocol

Layer 3 of the OSI model transfers variable-length packets from source to destination, responding to the transport layer and issuing requests to the data link layer.

OSI LAYER 3

Core Functions of the Network Layer



Connectionless Communication

Packets travel without requiring acknowledgments — e.g., IP sends data without the recipient confirming receipt.



Host Addressing

Every host has a unique hierarchical address (IP address), similar to a postal address that grows more specific by location.



Message Forwarding

Routers (gateways) forward packets between networks and subnetworks for wide-area communications.



Routing (Path Selection)

Protocols like IP, IPX, and AppleTalk DDR define routing and addressing at Layer 3.

Routing: The End-to-End Logic

Routing focuses on end-to-end forwarding. For PC1 to reach PC2, data passes through $R1 \rightarrow R2 \rightarrow R3$ — each device applying its own forwarding logic.

1

PC1 → R1

Sends frame to nearby router using Layer 2 addressing

2

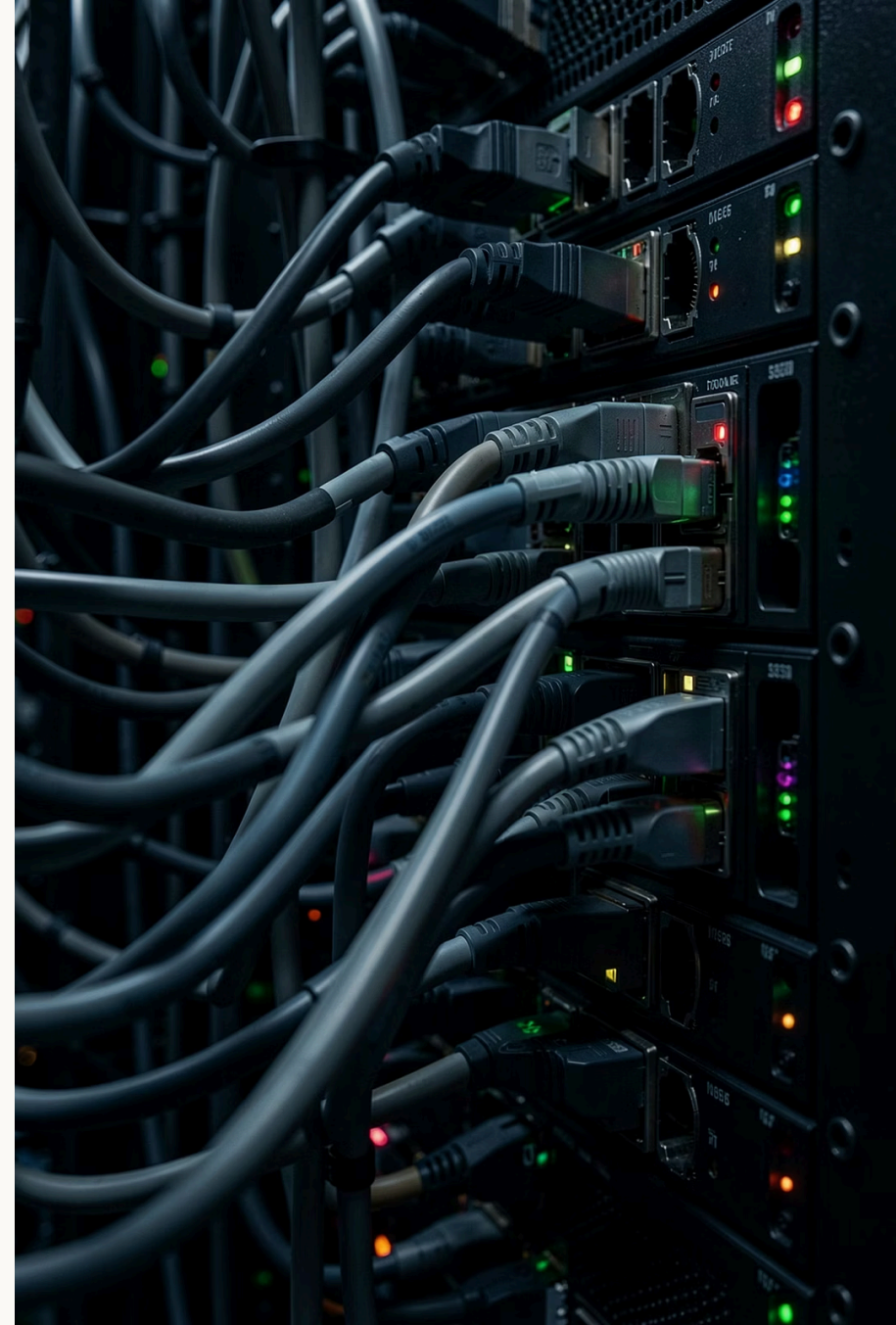
R1 & R2

Match destination address to routing table, forward to next hop

3

R3 → PC2

Final router delivers packet directly to destination host





ANALOGY

The Postal Service Model

Network layer addressing mirrors the postal system. Just as ZIP codes group addresses for efficient sorting, Layer 3 address groupings let routers forward packets without knowing every individual destination.

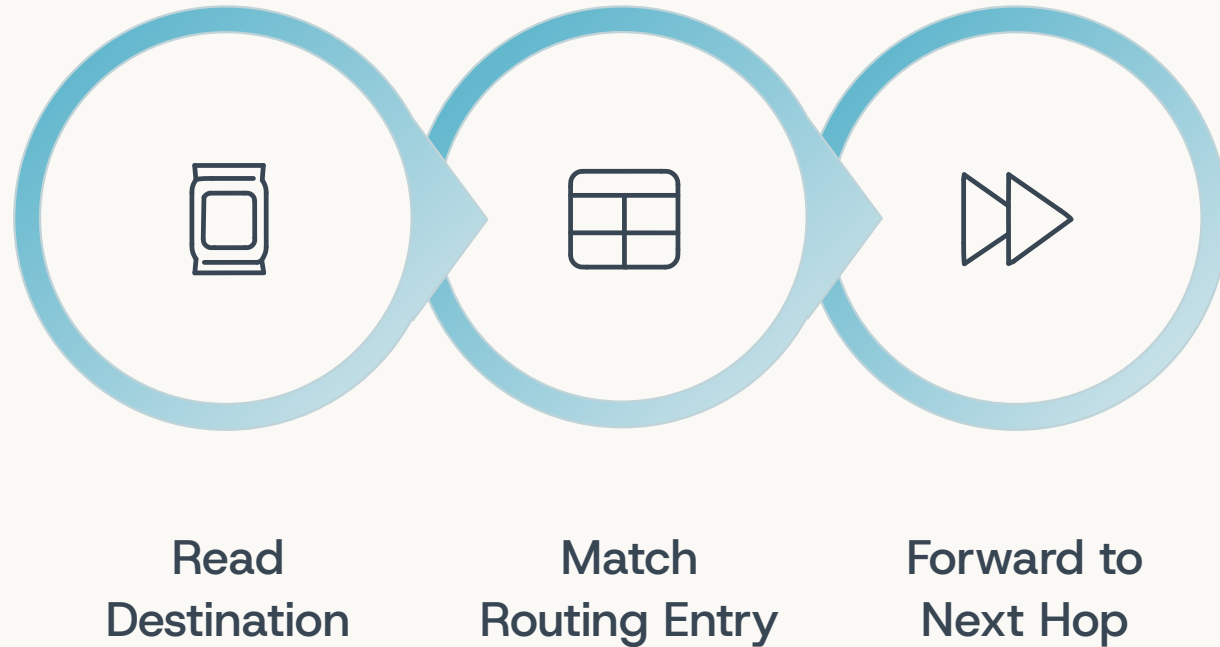
ZIP Code = Network/Subnet

One routing table entry covers an entire group

Street Address = Host Address

Unique within its group, like a house on a street

How Routers Forward Packets



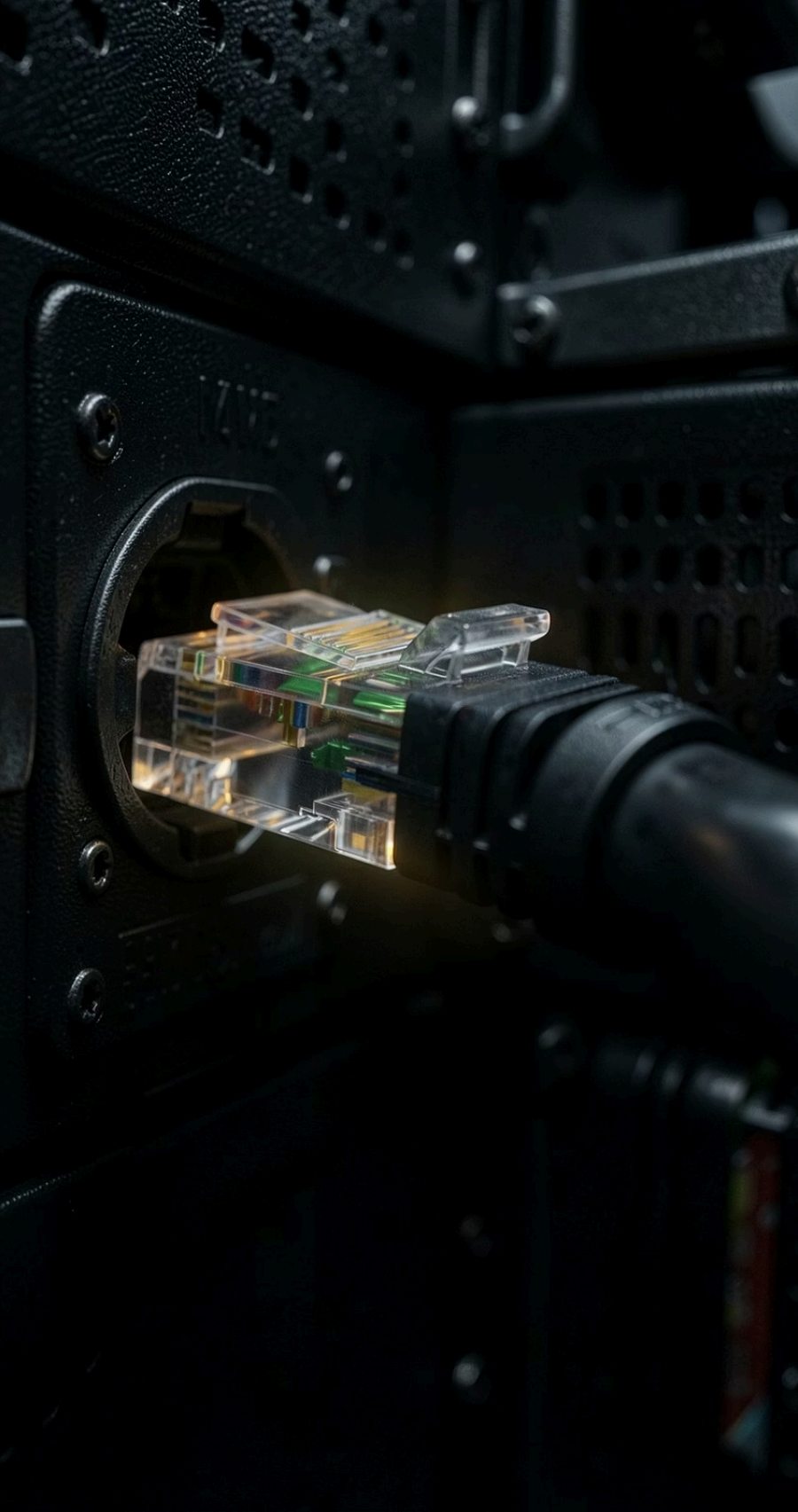
Routers compare the destination Layer 3 address to grouped entries in the routing table — not individual addresses. This grouping is what allows routers to scale to hundreds of thousands of devices efficiently.

Layer 3 Addressing Structures

Each Layer 3 address has two parts: a **grouping field** (like a ZIP code) and a **local address field** (unique within the group).

Protocol	Address Size	Grouping Field	Local Address Field
IP	32 bits	Network/Subnet (8–30 bits)	Host (2–24 bits)
IPX	80 bits	Network (32 bits)	Node (48 bits)
AppleTalk	24 bits	Network* (16 bits)	Node (8 bits)
OSI	Variable	Many formats	DSP (~56 bits)

*Consecutively numbered network values can be combined into a **cable range**.



Network Layer & Data Link Layer Interaction

The network layer decides *where* to send a packet; the data link layer handles *how* to transmit it across each physical link.

01

Network Layer selects interface

Routes packet out the appropriate network interface

02

Handoff to Data Link Layer

Data link adds header and trailer, creating a frame

03

Physical Layer transmits

Bits are placed onto the physical medium

04

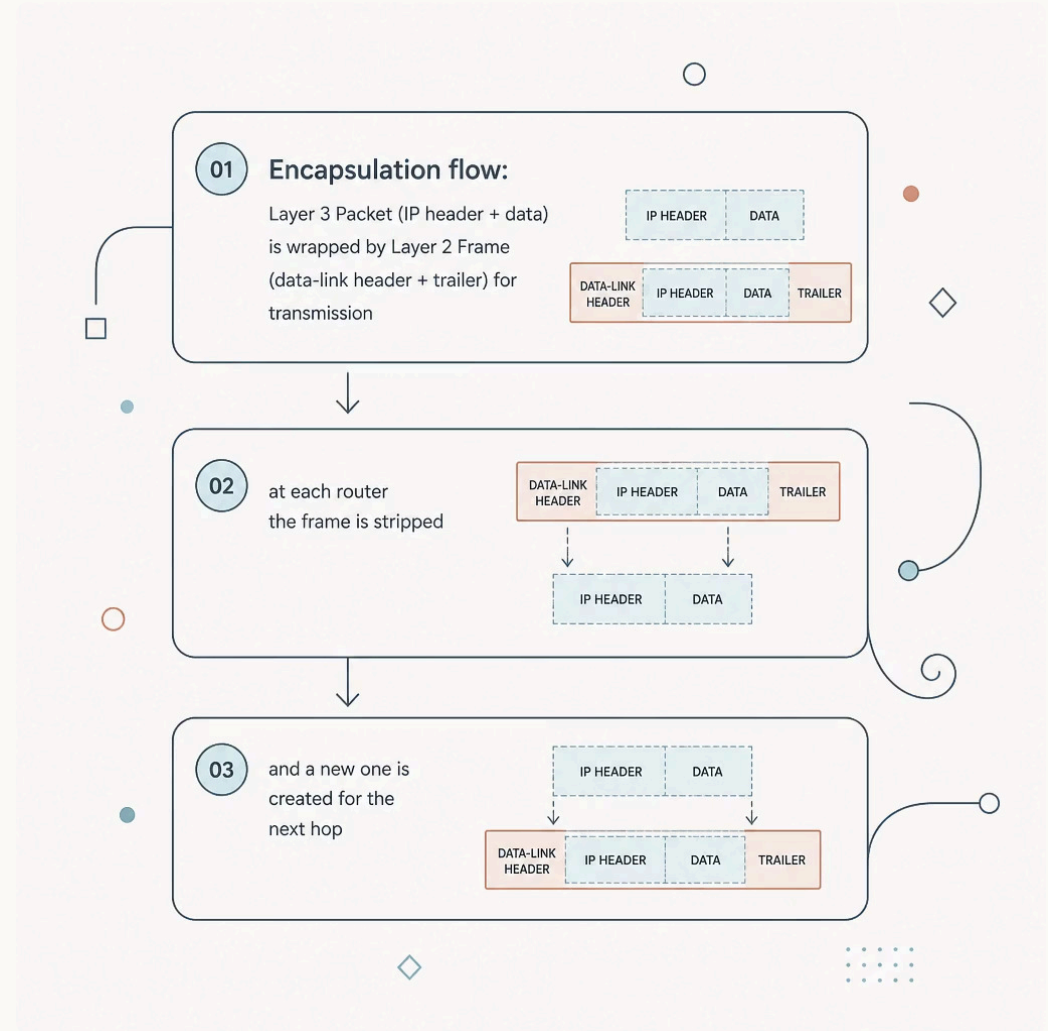
Headers discarded at each hop

Only the Layer 3 packet is forwarded end-to-end

Encapsulation & ARP

Routers build **new data-link headers and trailers** at each hop. To determine which data-link address to use, devices rely on **ARP (Address Resolution Protocol)**, which dynamically learns the Layer 2 address of an IP host on a LAN.

- ❏ Routing forwards Layer 3 packets (L3 PDUs) using successive Layer 2 frames — each frame only carries the packet to the *next* device in the path.



Routing Protocols vs. Routed Protocols

Routing Protocol

Learns routes and populates the routing table dynamically.

Example: **RIP** advertises network group locations so each router builds a complete routing table.

Routed Protocol

The **type of packet forwarded** through the network.

Example: **IP packets** are the routed protocol when RIP is the routing protocol.

Key design goals for Layer 3 addressing: large address space, unique assignment, implied grouping, and dynamic address assignment for clients.

Key Takeaways

Layer 3 provides end-to-end packet delivery

Using connectionless communication, hierarchical addressing, and message forwarding via routers.

Address grouping enables scalability

One routing table entry covers an entire group — just like a ZIP code covers many addresses.

Data link layer handles per-hop delivery

Layer 3 packets are encapsulated in Layer 2 frames; headers are rebuilt at each router.

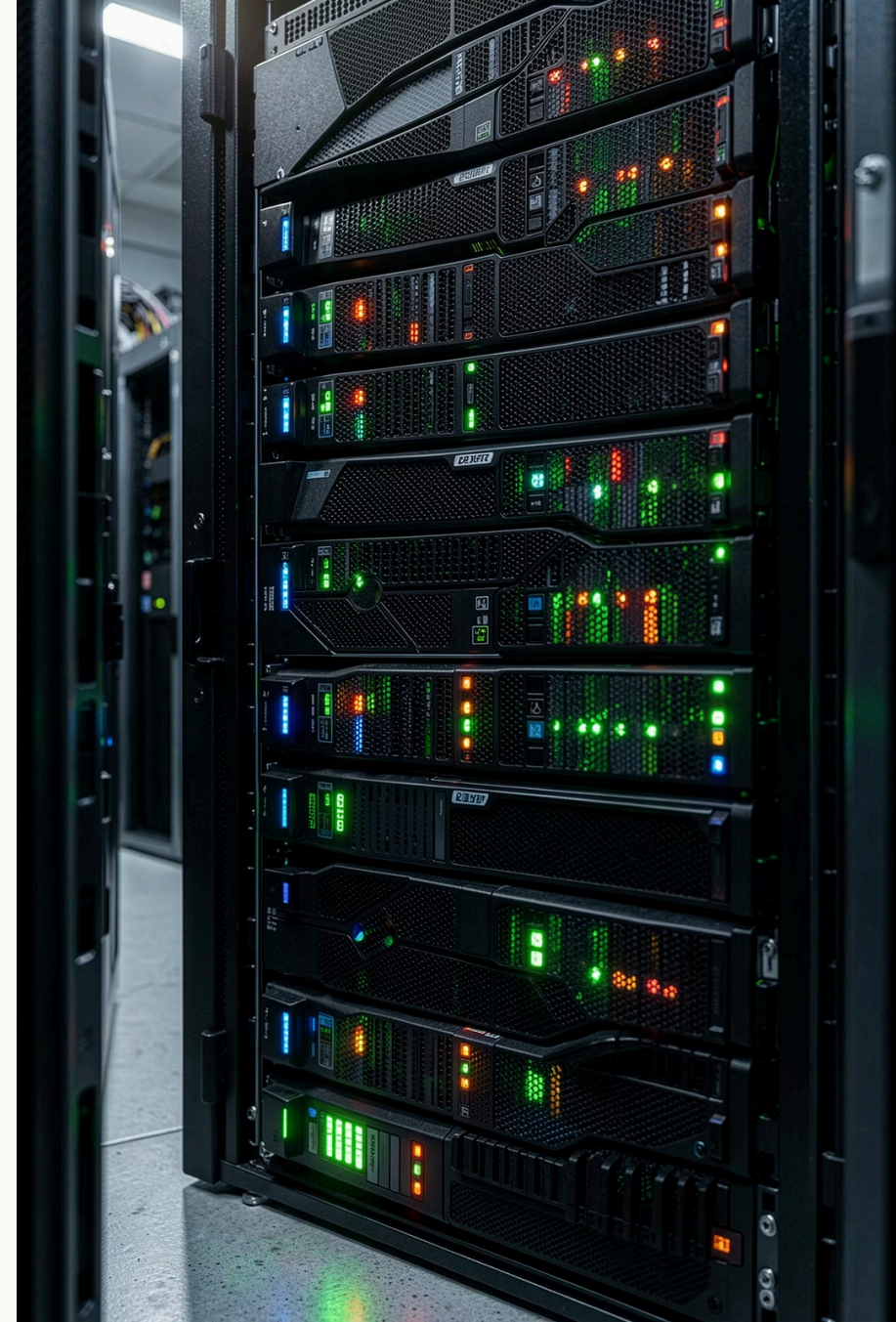
Routing protocols build tables dynamically

Routed protocols (e.g., IP) are forwarded; routing protocols (e.g., RIP) learn the paths.



Monitor a Computer Network

Session 3 — Understanding network monitoring: the systematic practice of overseeing network operations to ensure availability, detect failures, and maintain performance.



What Is Network Monitoring?



Network monitoring is the practice of **overseeing a computer network** using specialized software to ensure availability and performance of hosts, routers, switches, firewalls, and servers.

Detect Failures

Identifies overloaded, crashed, or frozen devices and alerts the network administrator.

Subset of Network Management

Focused on problems – distinct from intrusion detection, which targets external threats.

Key Metrics & Monitored Parameters

Throughput

Data transmission rate across network links

Uptime / Downtime

Availability and use-time percentages

Response Time

Speed of replies to user and automated requests

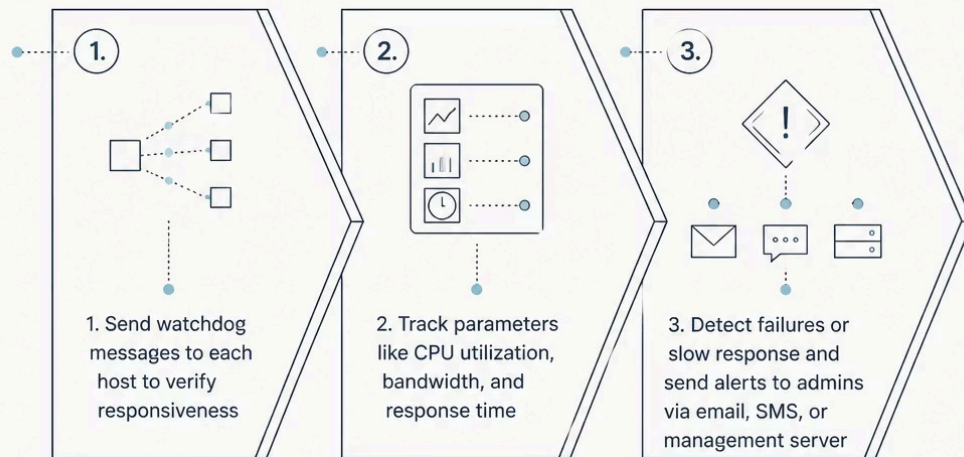
Error Rates

Frequency of transmission or connection failures

- ❑ When thresholds are exceeded, alarms are triggered and fault management processes begin – via SMS, email, or automatic failover systems.



Key Features & How It Works



Core Capabilities

- Measures **CPU utilization** of hosts and **bandwidth** of links
- Sends **watchdog messages** to verify host responsiveness
- Detects failures, slow responses, and unexpected behavior
- Notifies admins via **alerts** to management servers, email, or phone
- Tests web servers via **HTTP**; email servers via **SMTP/IMAP/POP3**

Network Monitoring Tools



Ping

A basic tool available on most computers. Sends IP test messages to verify connections and measure performance between two hosts.



HP BTO & LANDesk

Sophisticated software packages designed for professional administrators managing large computer networks.



Monitis

A web-based service for monitoring globally distributed web server pools, quickly detecting problems at any location.



Computer Network Monitoring

Collecting, analyzing, and acting on network data to ensure a properly working IT infrastructure — before problems become crises.

SECTION 3.2

The Cost of Reactive IT

The Problem

Damaged hard disks, connection failures, malware – hardware and software problems occur constantly in medium-sized companies.

The Cost

Work interruptions lead to higher costs. IT support departments must quickly limit damage, but chasing problems is expensive.

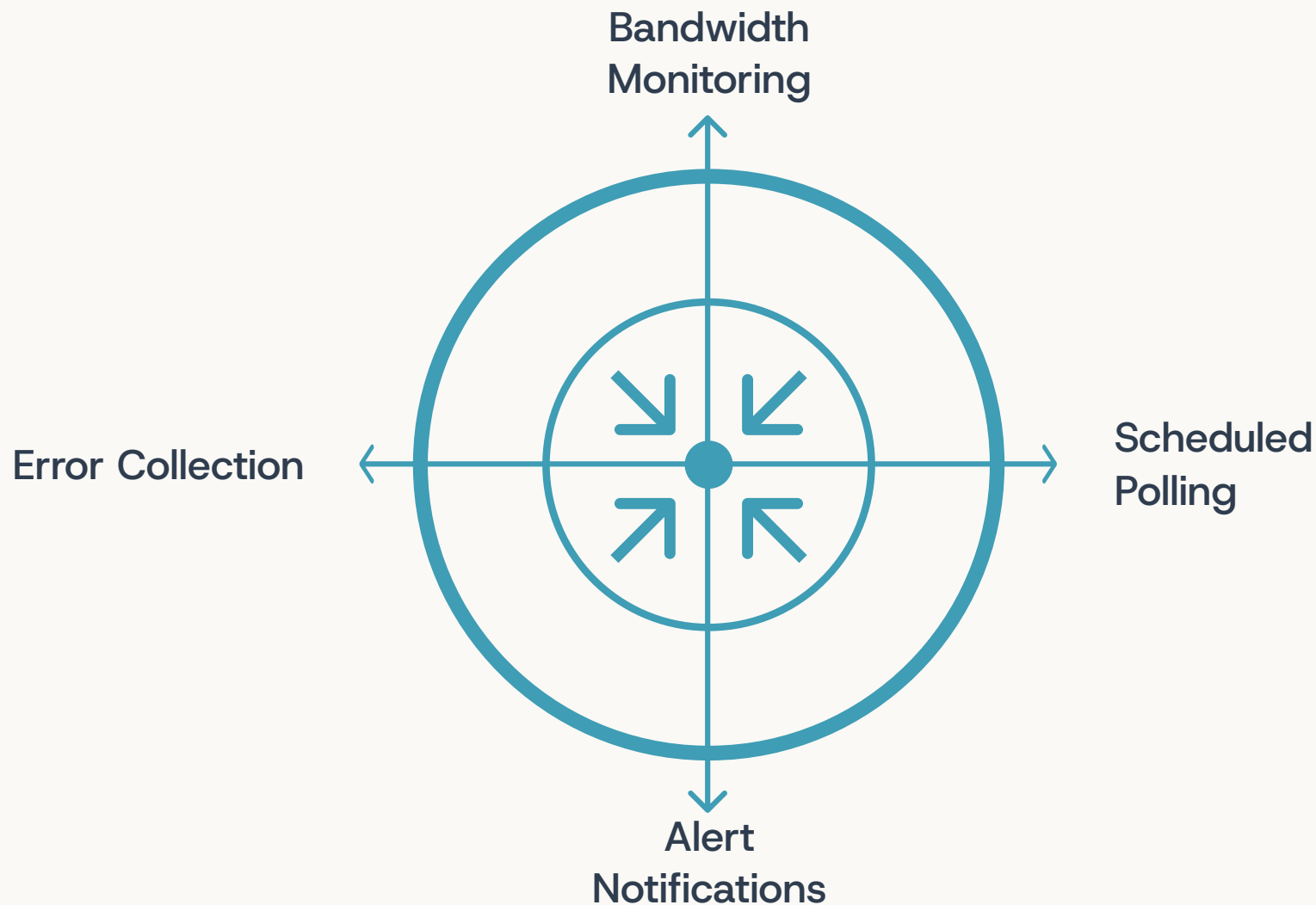
The Solution

Central monitoring spots problems **before** they happen and sends alerts quickly – take precautionary measures instead of reacting.



Simple Network Management Protocol (SNMP)

SNMP is the **most widely used** network monitoring and management protocol. It includes monitored devices, agent software on those devices, and a Network Management System (NMS) – a toolset on a server that monitors each device and communicates information to an IT administrator.



Administrators use SNMP to gather bandwidth usage, actively poll devices at set intervals, receive failure notifications via text or email (e.g., low disk space alerts), and collect error reports for troubleshooting.

The Evolving Threat Landscape

Growing Attack Surface

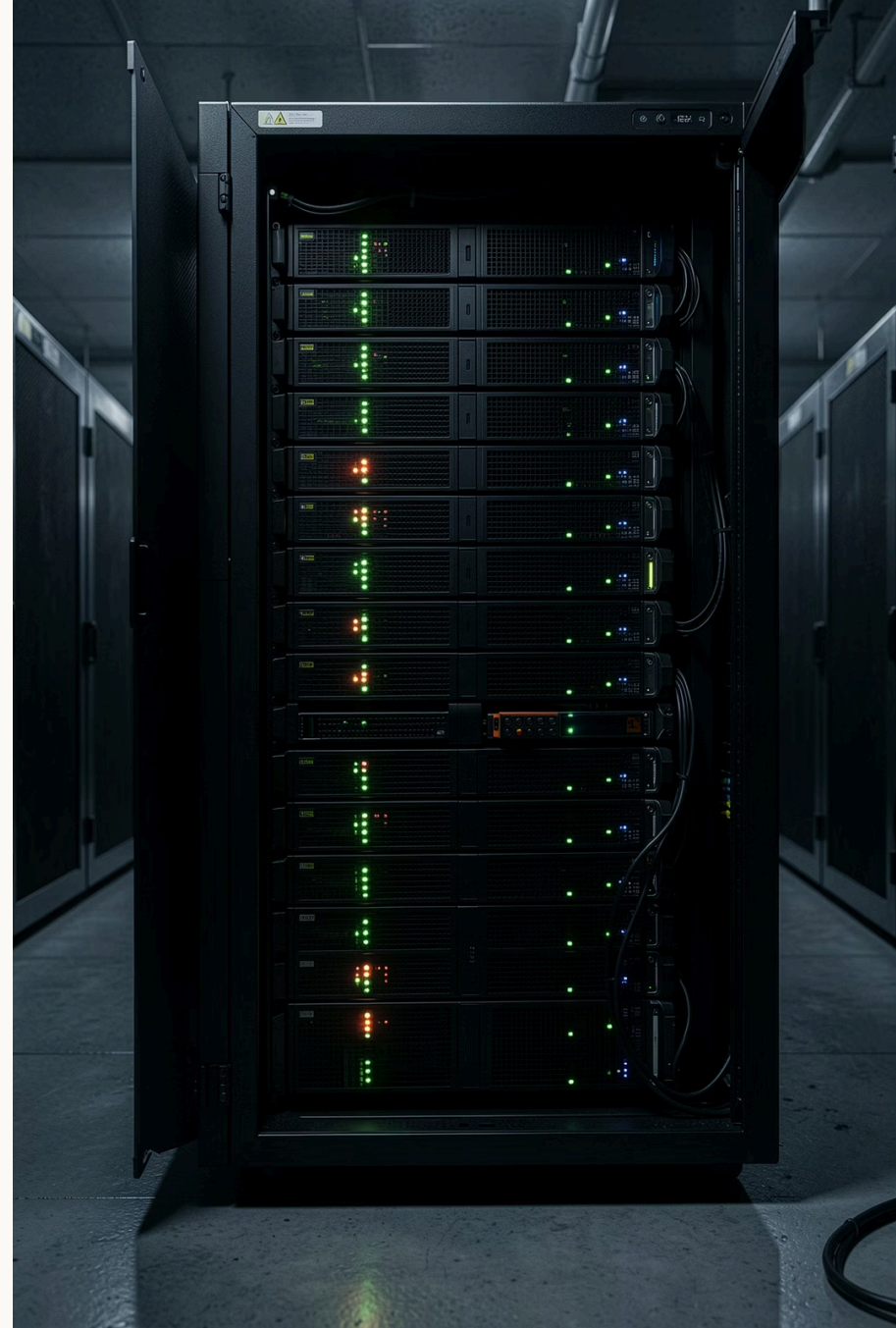
Businesses rely on IoT, BYOD, and BYOC — all exposed to network-borne threats **24/7**. The number of new threats is escalating.

Manual Response Can't Scale

It's unrealistic to block all attacks manually. From Heartbleed to FREAK, criminals exploit low-hanging fruit in widely deployed software.

What's Required

More **pervasive, automated, and intelligent** network security monitoring to improve situational awareness and drive timely threat response.



File Integrity Monitoring (FIM)



What Is FIM?

FIM establishes a baseline state of files and monitors for changes in real time. It creates cryptographic checksums of files – if something changes, you get an alert.

What It Tracks

- **Who** initiated the change
- **When** it was made
- **What** function or application made it
- **Before-and-after** state of the file
- Whether the change was **authorized**

7 FIM Features to Look For

01

Multiple Platform Support

Monitor Windows, Linux, Solaris, AIX, HP-UX without incompatibility.

02

Easy Integration

Correlate change data with event and log data; complement anti-virus as a last line of defense.

03

Extended Perimeter Protection

Include firewalls, routers, switches, and VPN concentrators.

04

Smarter Change Detection

Go beyond hash changes — detect owner, permissions, and metadata shifts.

05

Multi-Level Logging & Reporting

Integrated network-wide view with drill-down dashboards.

06

Simplified Rule Configuration

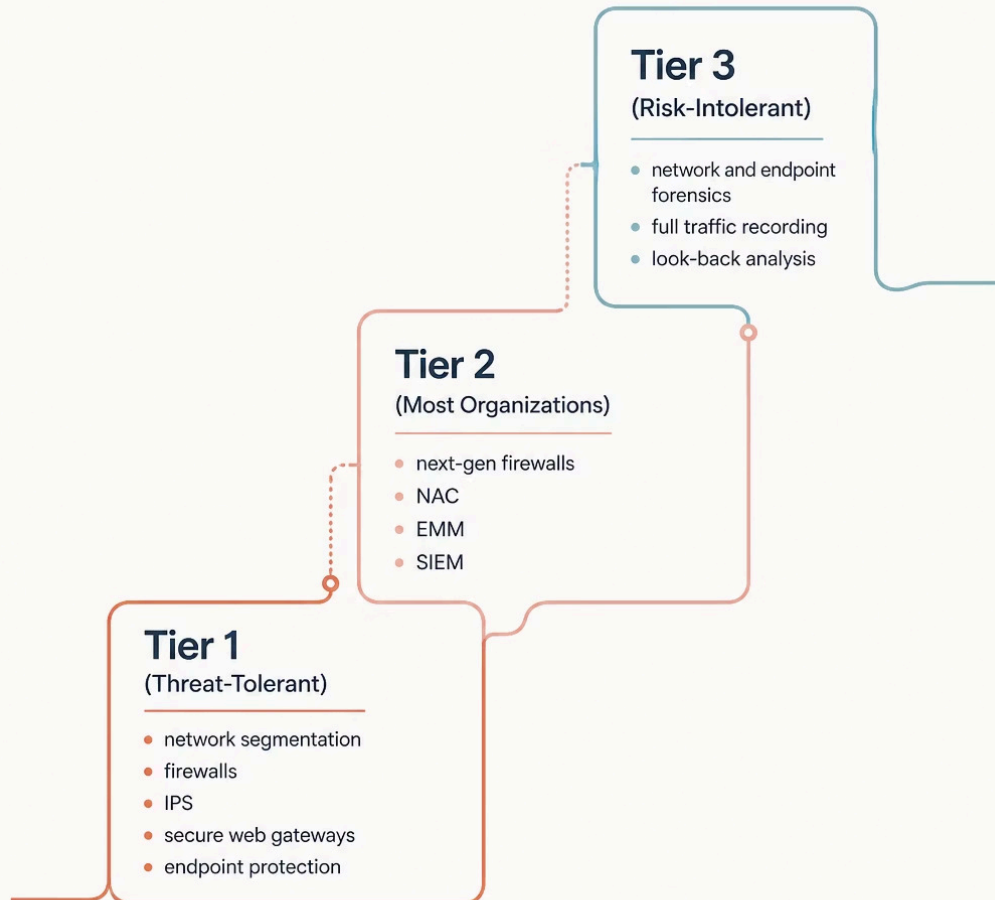
Define monitoring rules and replicate across devices.

07

Real-Time Monitoring

Compare misconfigurations against standards in real time. Per Verizon's 2015 DBIR, exfiltration can begin within minutes — a narrow window to stop threats.

Network Threat Visibility



Deploy Based on Risk

Perkins recommends deploying network security monitoring technologies based on risk. At minimum, segment networks and defend assets with firewalls, IPS, secure web gateways, and endpoint protection.

Most organizations need deeper tools — next-gen firewalls, NAC, EMM, SIEM — that broaden visibility and produce actionable intelligence. Risk-intolerant organizations should add forensics to record all activity and enable look-back analysis.

❏ Ponemon Institute: DoS attacks, malicious insiders, and malicious code account for **55%** of all cyberattack costs.

Advanced Monitoring Tools

Next-Gen Firewalls

Application-aware – identify apps even over SSL, apply user-specific policies, and learn via machine-readable threat feeds.

Wireless IPS & EMM

Scan 24/7 for rogue IoT and BYOD threats. EMMs assess mobile device integrity, alerting on jailbroken or malware-infected devices.

SIEM Evolution

Now combs data with contextual info on users, assets, and threats. Breach detection has overtaken compliance as the primary driver (Gartner).



Breach Detection & Network Forensics

Breach Detection Systems (BDS)

A new market segment applying big data analytics to profile user and device behavior. Per NSS Labs, BDS can identify pre-existing breaches and side-channel malware — a "**last line of defense**" for risk-intolerant enterprises plagued by persistent threats.

Network Forensics Appliances

Like a network DVR, these passive appliances record all ingress/egress traffic. They enable full-packet replay, cybercrime investigation, and impact assessment — making it possible to go back and find what real-time monitoring missed.

Key Takeaways

→ Monitor Proactively

Central monitoring catches problems before they escalate
— reducing downtime and cost.

→ Deploy FIM for Change Control

Detect unauthorized file changes in real time across all
platforms and network devices.

→ Use SNMP as Your Foundation

The most widely adopted protocol for bandwidth, status
polling, and alerting.

→ Scale Security to Your Risk Profile

From firewalls to SIEM to forensics — match your toolset
to your organization's risk tolerance.



Computer Monitoring: Data & User Surveillance

A comprehensive guide to tracking system performance and monitoring user activity across your network.

What Kind of Data Is Gathered?

Computer monitoring collects key metrics across your IT infrastructure — from CPU health to disk space — giving you full visibility into network performance.



CPU & Temperature

Track utilization, temperature, and performance to catch problems before they become critical.



Memory Usage

Use WMI, SNMP, or SSH sensors to monitor memory and avoid network bottlenecks.



Bandwidth

Measure real-time download/upload speeds and detect bandwidth overloads instantly.



Disk Space

Visualize all storage capacities on one dashboard to prevent failed backups and missing files.



System Information

See connected hardware, installed software, and running processes for every device at a glance.



PERFORMANCE MONITORING

CPU, Memory & Bandwidth

CPU Utilization & Temperature

Monitoring informs you about CPU utilization, temperature, and performance – helping identify possible problems before they become critical.

Memory Usage

Preconfigured sensors like WMI Memory, SNMP Memory, or SSH Meminfo make it easy to track memory usage and avoid bottlenecks.

Bandwidth Requirements

Track available bandwidth and real-time data such as download and upload speeds. Detect overloads instantly and prevent network strain.

Disk Space & System Information



Free Hard Disk Space

Aborting installations, failing backups, or disappearing files often stem from low disk space. Monitoring visualizes all memory capacities in one dashboard, ensuring smooth business processes.

System Information

Gather complete details about your IT infrastructure. View connected hardware, installed software, and running processes for every device you add.

Ways to Monitor What Your Users Are Doing

From file auditing to screen capture, there are 10 proven methods to track and control user activity on your network.

1

File Auditing

2

Browser Cache

3

Firewall Monitoring

4

URL Filtering

5

Keyword Filtering

6

Email Monitoring

7

IM Monitoring

8

Keyloggers

9

Screen Capture

10

Software Control

METHODS 1-2

File Auditing & Browser Cache

#1: Audit File Access

On Windows networks, use the built-in **audit policy** (enabled via Group Policy) to track which files employees open — including failed access attempts. Set auditing on specific files, folders, or printers.

#2: Examine Cached Web Files

Browser caches (Temporary Internet Files) store copies of visited pages. Savvy users may clear the cache, but on Windows XP you can restrict access to Internet Options using Microsoft's **Shared Computer Toolkit**.



METHODS 3–5

Firewall Monitoring & Web Filtering

#3: Monitor at the Firewall

Configure enterprise firewalls (ISA Server, Cisco PIX, CheckPoint) to report websites accessed by user and computer. Add-ons: **SurfControl**, **Websense**, **GFI WebMonitor**.

#4: Filter by URL

Block undesirable sites — pornographic, malicious, or recreational — to prevent harassment liability and time-wasting. Options range from NetNanny to enterprise packages.

#5: Filter by Keywords

URL blacklists can't cover everything. Keyword-based filtering catches undesirable content even on unknown or newly created sites.

Email & Instant Message Monitoring

#6: Monitor Email

Tools like **Spector CNE** capture sent and received messages, set word/phrase alerts, and also log IM, web browsing, and keystrokes with snapshot recording.

#7: Monitor Instant Messages

IMs are a common source of security breaches. Block IM ports at the firewall, or use **Akonix Enterprise** or **Symantec IM Manager** to control and monitor communications by group — for example, allowing chat but blocking file-sharing.

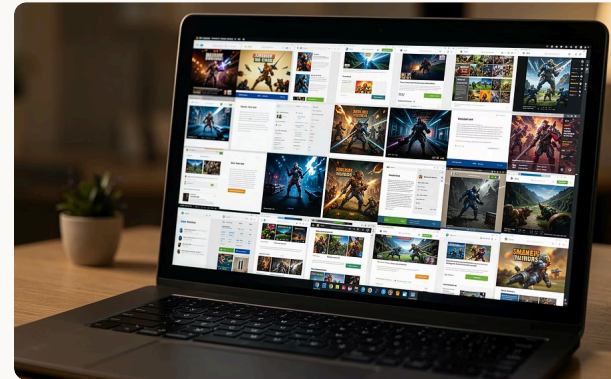


Keyloggers & Screen Capture



#8: Keyloggers

Record all typed data. **Hardware** keyloggers (e.g., KeyGhost) plug between keyboard and port. **Software** keyloggers send captured keystrokes remotely and are often bundled with tools like Spector CNE or SpyRecon.



#9: Screen Capture

Unlike keyloggers, screen capture shows exactly what employees see — websites visited, documents opened, games played — not just what they type. Often included in monitoring packages.

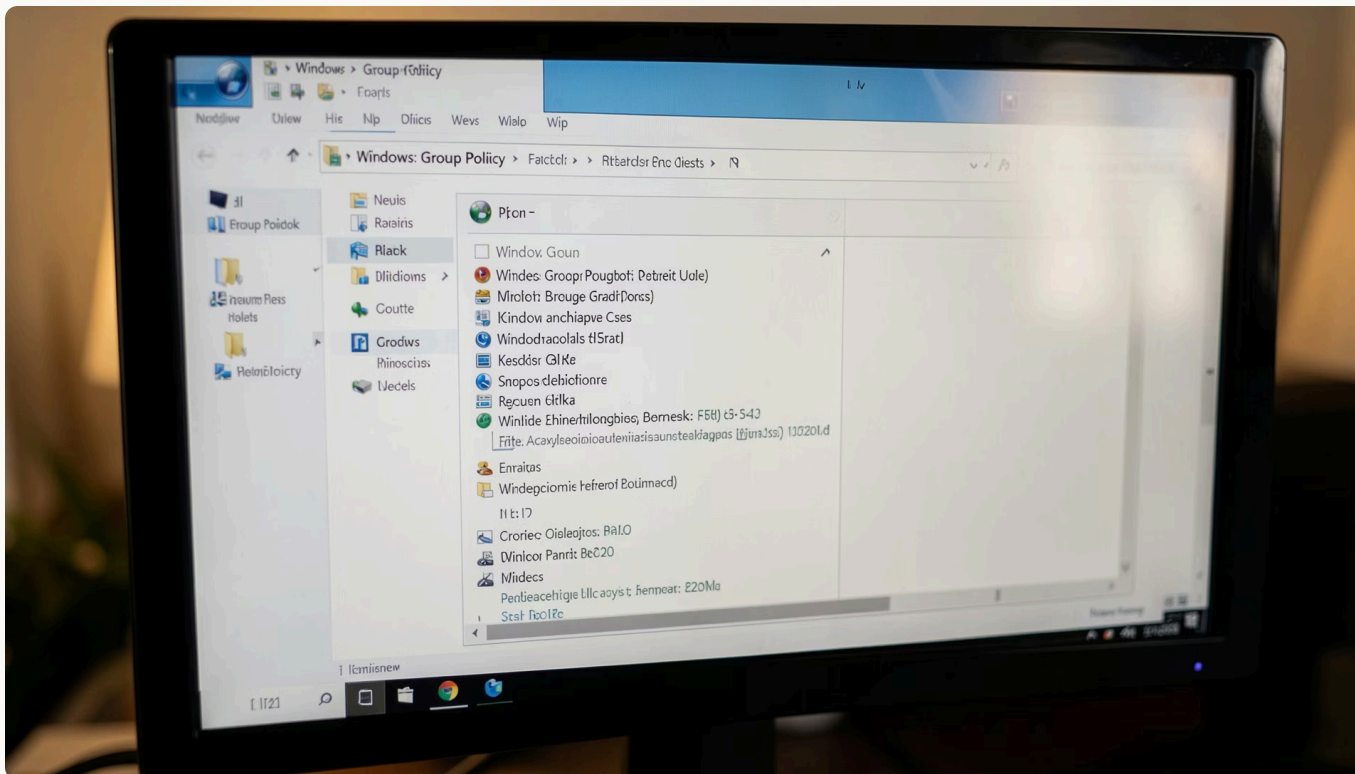
Control Software Installation & Execution

#10: Software Restriction Policies

Use built-in Windows XP and Server 2003 tools to control what employees can install or run:

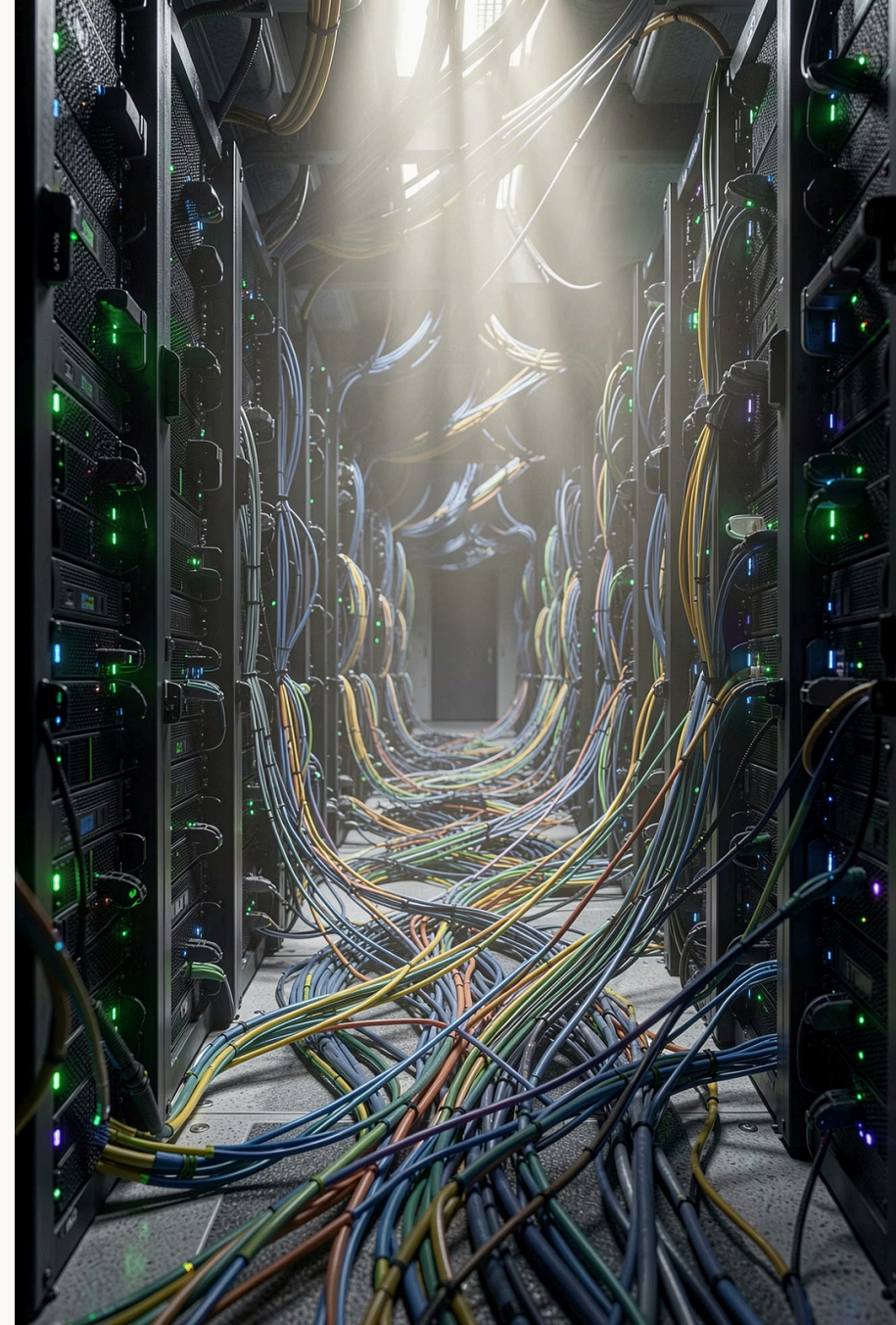
- Prevent program installation via **Group Policy User Rights**
- Manage software distribution with the **Software Installation** feature
- Control which programs can run using **Software Restriction Policies**

 Combining all 10 methods gives you complete visibility and control over your network's security and productivity.



Network Monitoring & Diagnostics

Understanding network reports, monitoring tools, and common network problems — essential knowledge for every network administrator.





A Fast-Growing Market

\$1.6B

Market Size

Network performance monitoring & diagnostics segment

20.7%

CAGR

Compound annual growth rate (Gartner)

Leaders are innovating around cloud-based monitoring, software-defined environments, and flexible deployment models. This market is a segment of the larger network management space.

Types of Network Reports

1

Processor Utilization

CPU usage of a network device over time

2

Memory Utilization

Percentage of free memory on a device over time

3

Interface Traffic Volume

Inbound and outbound traffic rate through a selected port

4

Interface Error Packet Analysis

Percentage of error or discarded packets, inbound and outbound

5

Interface Packet Analysis

Types of packets (unicast or non-unicast) traversing a port

6

Custom Performance Report

Displays performance counter values



WHY USE A NETWORK REPORTING TOOL?

Stay in Control

Tools like **PRTG Network Monitor** help administrators:

- Identify network and bandwidth usage trends
- Monitor availability and uptime of devices
- Check performance metrics (CPU, RAM) of servers
- View data in easy-to-read reports and graphs

Advantages of Network Reporting Tools



Cost-Effective

Powerful monitoring with detailed reports for admins and summary views for managers



Historic Comparison

Compare current data to historic trends for resource planning and troubleshooting



200+ Sensor Types

Complete network overview — Hyper-V, VoIP, bandwidth, IP usage, and more



Share & Mobile

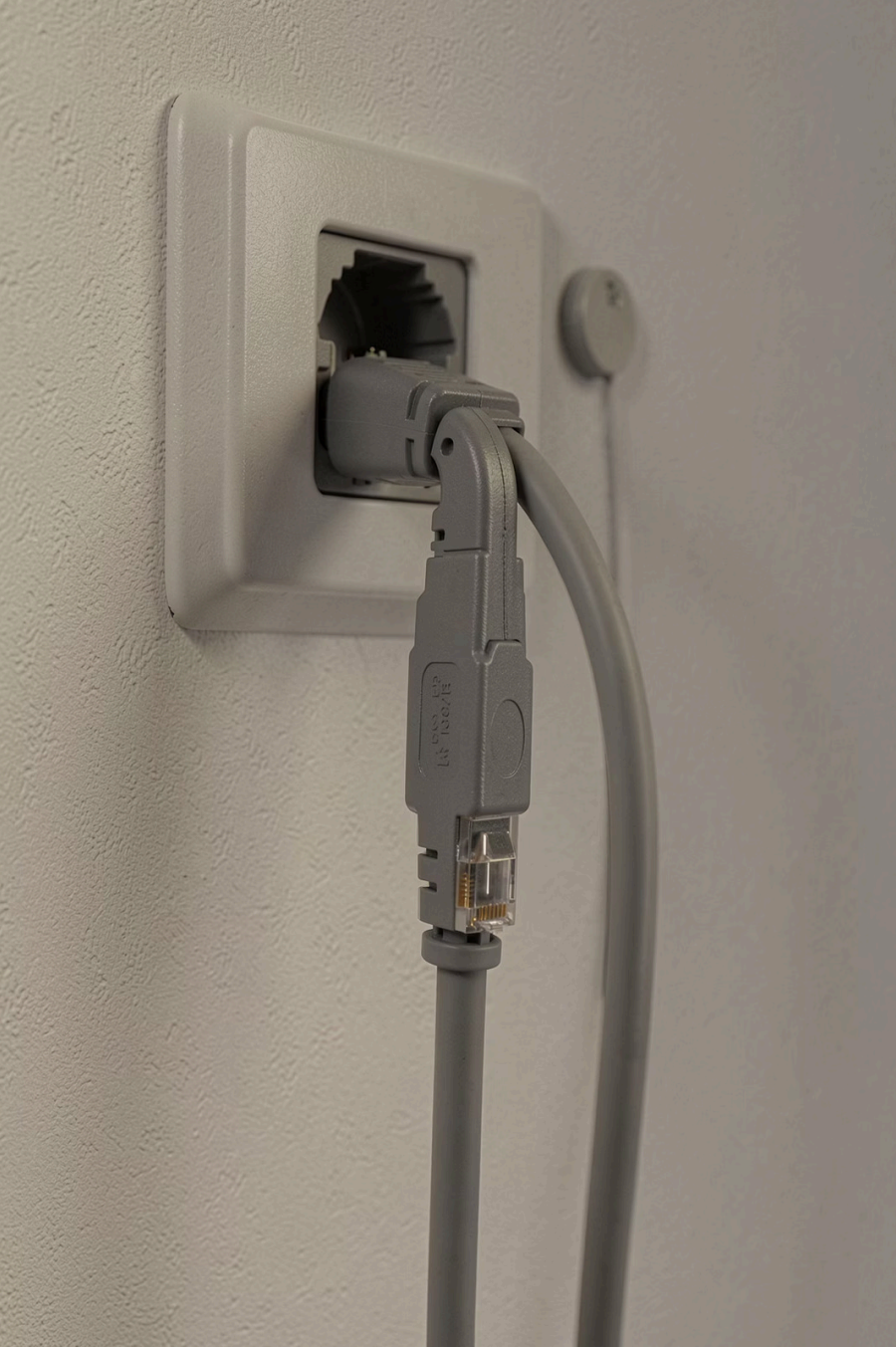
Publish graphs to intranet/website; iPhone interface for mobile monitoring



Actionable Intelligence

It is the tool's ability to provide immediate, intelligent reports that makes the difference in running a well-planned and optimized IT infrastructure.

Network monitoring tools accumulate gigabytes of data, but the real value lies in generating **actionable reports** for capacity planning, device upgrades, and SLA verifications — especially when upper management needs to make critical decisions.



Common Network Problems

When networks fail, the impact is immediate: increased congestion, slow application response, loss of productivity, and chaos for IT managers. Monitoring provides helpful clues to the nature of the issue.

"Network Cable Unplugged"

Adapter, cable, or driver failures

IP Address Conflicts

Two devices sharing the same IP

Path Not Found Errors

Invalid paths or sharing misconfigurations

"Network Cable Unplugged" — Causes & Fixes

Possible Causes

- Malfunctioning network adapter
- Bad Ethernet cable
- Outdated or corrupt device drivers
- Issue after Windows 10 upgrade

How to Resolve

- **Power cycle** the device (full shutdown, remove battery on laptops)
- **Disable** unused Ethernet adapter
- **Check or replace** the Ethernet cable
- **Update or reinstall** the network driver
- **Change Duplex settings** to Half/Full Duplex
- **Re-seat or replace** removable adapter hardware

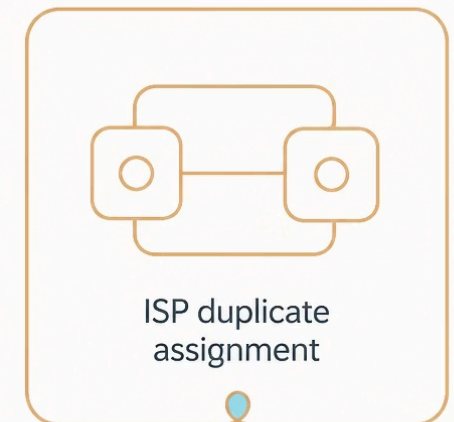
IP Address Conflicts

How They Happen

- Admin assigns two devices the same **static IP**
- Static IP falls within the **DHCP range**
- **DHCP server malfunction** assigns duplicate addresses
- ISP accidentally assigns the same IP to two customers

How to Resolve

- Ensure all static IPs are **unique**
- **Release and renew** dynamic IP addresses
- **Upgrade router firmware** if DHCP is faulty



Other Common Errors & Key Takeaways

Path Not Found (Error 0x80070035)

Ensure valid shared resource paths, enable File/Printer Sharing, and verify user permissions on the remote device

Clock Synchronization

Unsynchronized clocks cause network errors — use **NTP** to keep Windows devices in sync

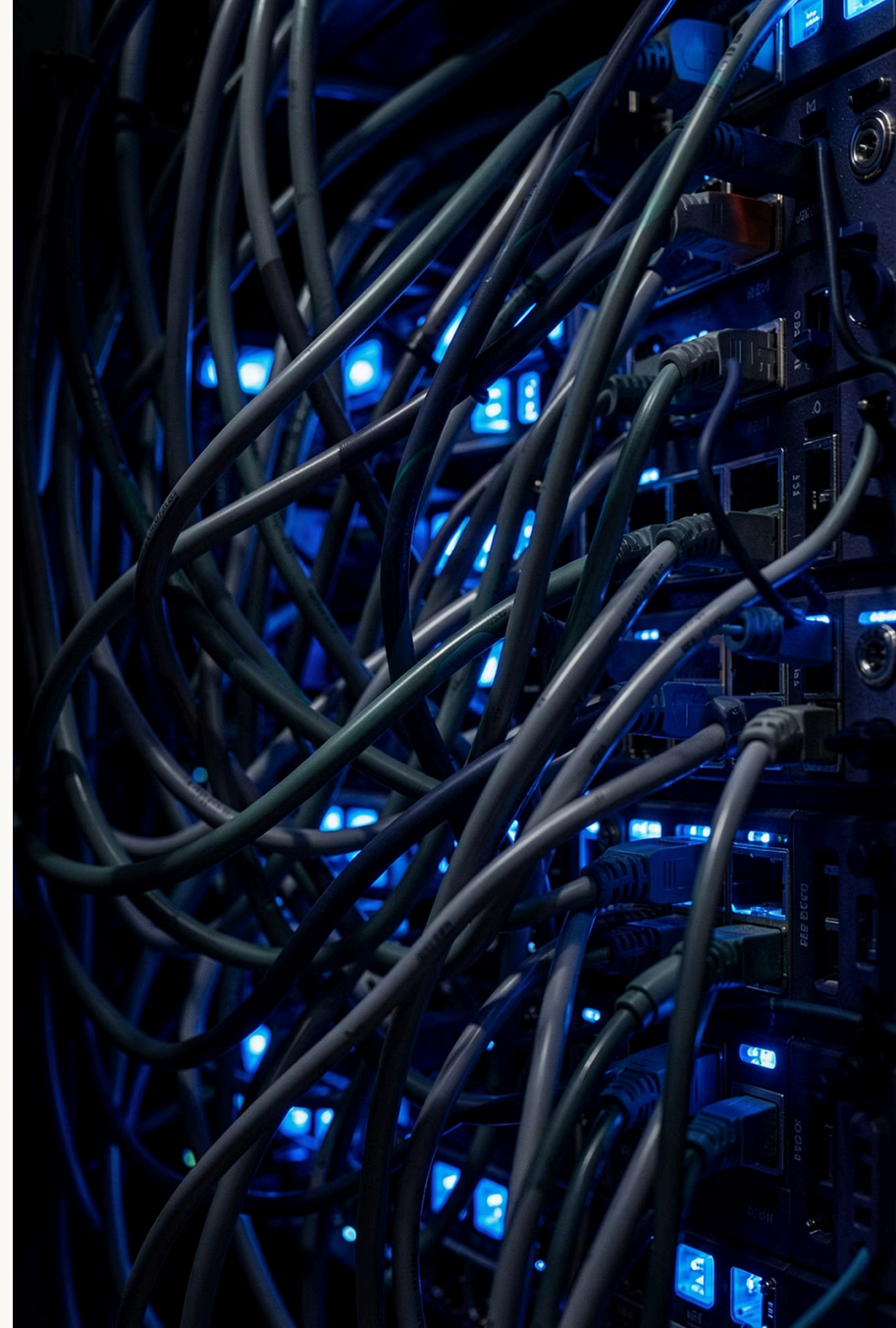
Service Failures

If Microsoft File/Printer Sharing services fail, **reboot** to restore normal functionality

- ❏ **Key Takeaway:** Proactive monitoring, accurate reporting, and systematic troubleshooting are the foundations of a well-optimized IT infrastructure.

Network Troubleshooting Guide

From firewall conflicts to VPN errors — a practical reference for diagnosing and resolving common network issues across Windows, iOS, and home infrastructure.



Disable Local Firewalls



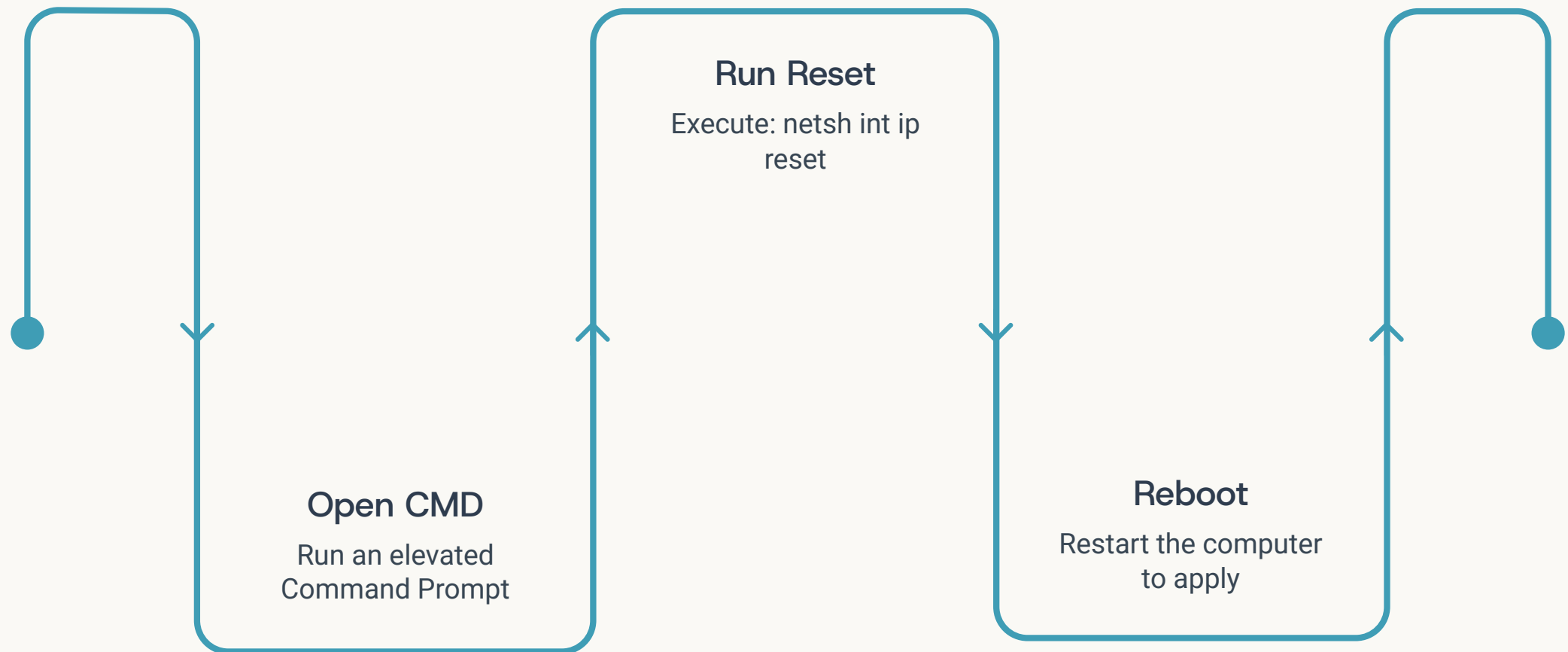
A misconfigured software firewall on a Windows device can cause connection errors. Temporarily disable the built-in Windows Firewall or third-party firewall software to test whether it's the culprit.

- ❏ Home desktops behind a broadband router firewall don't need their own firewall. Mobile devices should keep theirs active.

If disabling resolves the issue, adjust firewall settings to allow the connection, then re-enable protection.

Reset TCP/IP

Resetting TCP/IP components can resolve occasional Windows networking glitches. Open an elevated Command Prompt and run `netsh` commands, then reboot.



On Windows 8/8.1, run `netsh int ip reset` and reboot. For full details, see Microsoft KB 299357.

"A Duplicate Name Exists on the Network"

Why It Happens

This error prevents a Windows PC from joining the network. It occurs on networks with Windows XP or Server 2003 when two devices share the same name.

- Two PCs share the same Computer Name
- Workgroup name matches another device (e.g., router SSID)
- A server has two network names

Cause 1 -
Two Windows computers share the same Computer Name (most common)

Cause 2 -
Windows Workgroup name matches a router or access point SSID

Cause 3 -
Windows Server configured with two different network names (least common)

Resolving Duplicate Name Errors

01

Check Workgroup Name

Ensure the workgroup name differs from any router or access point SSID.

03

Rename & Reboot

Change one device's name to something unique, then reboot it.

05

Fix Server Error 52

Ensure the Windows server has only one network name configured.

02

Find Duplicate Devices

Check each computer name in Control Panel to identify the conflict.

04

Update WINS Database

On devices where the error persists, remove lingering references to the old name.

06

Upgrade Old Systems

Strongly consider upgrading any Windows XP devices to a newer OS.

Limited or No Connectivity

Try these steps in order if your Windows PC shows limited or no network connectivity.

1

Restart Computer & Router

Reboot both — a simple restart often resolves software-level network issues.

2

Check Ethernet Cable

Unplug and reattach, or swap with a known-good cable.

3

Reset TCP/IP Stack

Run `netsh int ip reset C:\logreset.txt` in an elevated Command Prompt, then reboot.

4

Disable Wi-Fi Power Saving

In adapter Properties → Power Management, uncheck "allow computer to turn off this device."

5

Verify DHCP Settings

Ensure the adapter obtains an IP automatically. If the IP starts with 169.254, run `ipconfig /release` then `ipconfig /renew`.

6

Update Drivers & Run Troubleshooter

Update the network adapter driver and run Windows Network Troubleshooter.

Limited Connectivity — Advanced Steps

TCP Advanced Commands

In an elevated Command Prompt, run these in order:

```
netsh int tcp set heuristics disabled  
netsh int tcp set global autotuninglevel=disabled  
netsh int tcp set global rss=enabled  
netsh int tcp show global
```

Then reboot.

Additional Checks

- **WPA Security Key:** Verify your wireless security key matches the router's settings.
- **Bypass Router:** Connect directly to the modem. If it works, the router may be faulty.
- **Contact ISP:** If the error persists, the issue may lie with your internet service provider.

iPhone Error -3 & VPN Error 800



iPhone "Unable to Join Network (Error -3)"

- Verify the SSID matches the access point (case-sensitive).
- Confirm WEP/WPA encryption keys or passphrases match (passphrases are case-sensitive).
- Troubleshoot the access point's security settings if needed.

VPN Error 800 — "Unable to Establish Connection"

- Confirm the local network connection is active; ping the server.
- Verify the VPN server name or IP address is correct.
- Temporarily disable the firewall; allow TCP port 1723 and IP port 47.
- Update router firmware if you've never connected through it before.

Bandwidth Saturation & Wireless Interference

Sawtooth Pattern

A strong indicator of bandwidth saturation. Latency and packet loss spike abruptly at a bandwidth-limited point (often the ISP link), then drop — repeating in a sawtooth pattern.

Solutions: Use less bandwidth, buy more, or implement throttling for heavy consumers.



- ❑ Bandwidth saturation can come from overuse or under-supply. Correlate network activity with PingPlotter results to identify the cause.

Hardware Failures & Unreachable Destinations



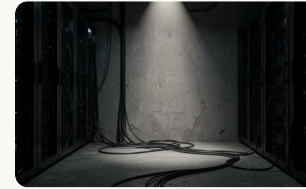
Bad Local Hardware

Packet loss at hop 1 (your router) points to a faulty cable, switch, NIC, or power supply. Check everything between you and the router.



ISP Bad Hardware

Consistent packet loss starting inside your provider's network suggests noise on the line or failing hardware — e.g., water in a junction box or a bad splitter.



Destination Unreachable

This doesn't always mean the target is down. A router may be blocking ICMP. Try switching to TCP or UDP packets in PingPlotter.