CS-042 · Network

Ports & Protocols

How a single IP address serves many services, and the port numbers that make it possible.

Executive Summary

Ports are numbered endpoints that let a single device run many network services at once, with each service reachable at a specific port. Protocols define the rules those services use to talk. Knowing the common port numbers and the protocols behind them is fundamental to configuring, defending, and troubleshooting networks.

What It Is

A port is a 16-bit number that identifies a specific service or process on a networked device, working alongside the IP address that identifies the device itself. If an IP address is like a building's street address, a port is like a numbered door to a particular office inside it. Ports are grouped into ranges: the well-known ports from 0 to 1023 are assigned to standard services, the registered ports from 1024 to 49151 are used by many applications, and the dynamic or ephemeral ports from 49152 to 65535 are assigned temporarily for outbound connections. A protocol is the agreed set of rules a service follows, and most services pair a protocol with a default port so that clients know where to connect.

Why It Matters

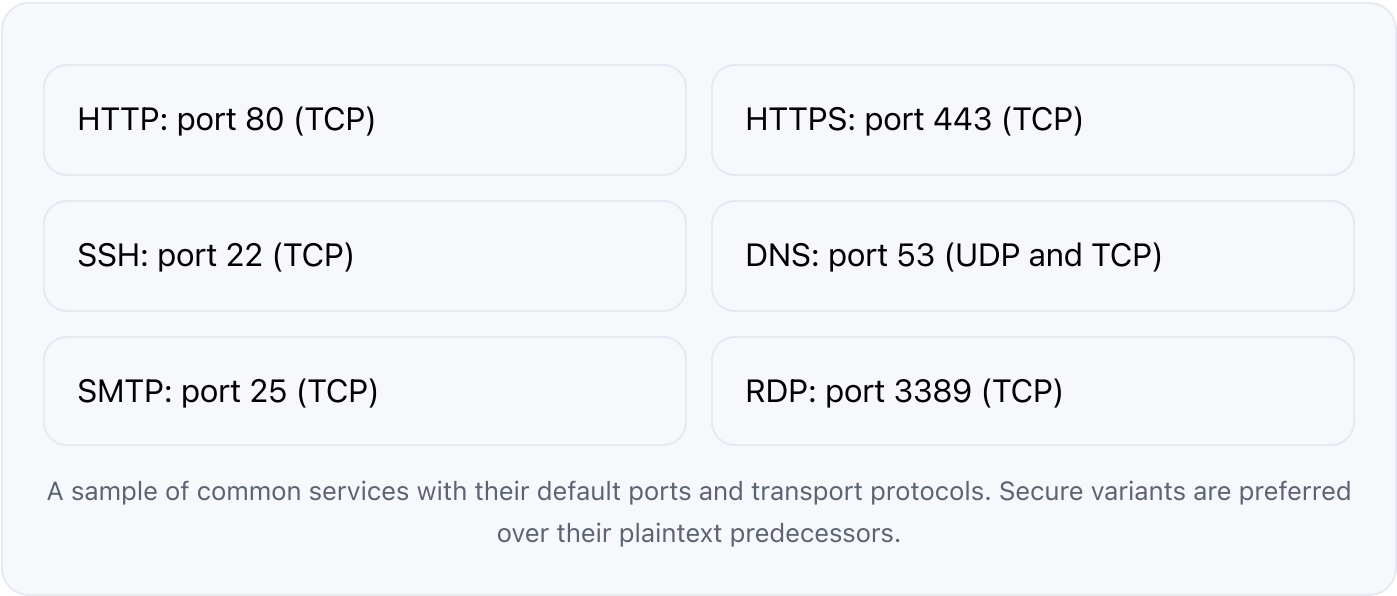
Ports and protocols are where network security becomes concrete. Firewalls decide what to allow or block largely by port and protocol, scanners map an organization's exposure by finding open ports, and attackers probe those same ports to find a way in. Every open port is a potential entrance, so knowing which services should be running and on which ports is essential to reducing attack surface. Confusing a secure protocol with its insecure predecessor, for example allowing plain FTP or Telnet, can quietly undermine an otherwise strong network. For

professionals, memorizing common ports is a baseline expectation in interviews and daily operations.

How It Works

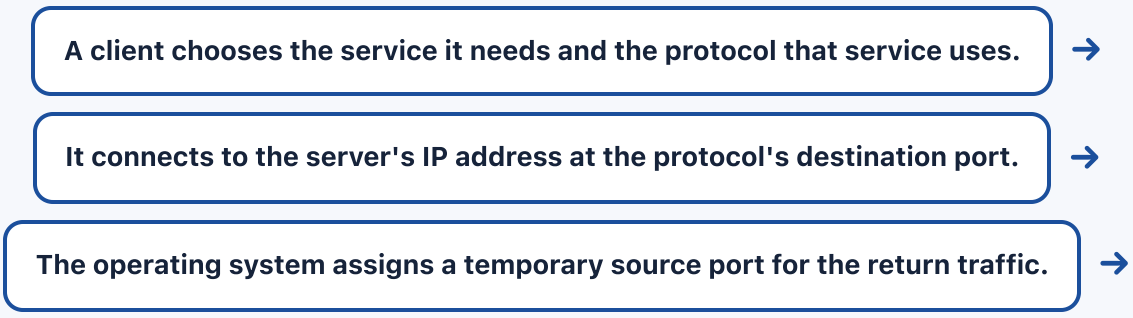
When a client connects to a service, it targets the server's IP address and a destination port, while the operating system assigns the client a temporary source port for the reply. The combination of source IP, source port, destination IP, and destination port uniquely identifies the connection. Services listen on their assigned ports: a web server listens on 80 for HTTP and 443 for HTTPS, a mail server listens on ports for SMTP, and so on. Some protocols run over TCP for reliability, some over UDP for speed, and a few use both. Administrators can change default ports, but standard assignments keep the internet interoperable and are coordinated by the Internet Assigned Numbers Authority.

Architecture Diagram



A sample of common services with their default ports and transport protocols. Secure variants are preferred over their plaintext predecessors.

Visual Workflow



The server, listening on that port, accepts the connection and responds. →

The four-part tuple of source and destination IP and port uniquely tracks the session.

Common Attacks

- Port scanning to discover which services a target exposes
- Exploiting services on open ports that are unpatched or misconfigured
- Abusing plaintext protocols like Telnet and FTP to capture credentials
- Brute-force attacks against exposed remote access ports such as SSH or RDP
- Using nonstandard ports to hide malicious traffic and command-and-control

Common Mistakes

- Leaving unused services and their ports open to the internet
- Allowing insecure protocols instead of their encrypted replacements
- Believing that changing a service to a nonstandard port is real security
- Exposing remote access ports like RDP directly to the public internet
- Not documenting which ports and services are expected on each host

Best Practices

- Close every port that does not serve a documented business need
- Prefer encrypted protocols such as HTTPS, SSH, and SFTP over their plaintext versions
- Restrict remote access ports behind a VPN or allow-list, never open to all
- Scan regularly to detect unexpected open ports and drifting configurations
- Keep services on their standard ports and document any deliberate exceptions

Quick Checklist

- [x] Can recall the default ports for HTTP, HTTPS, SSH, DNS, and RDP
- [x] Knows which common protocols use TCP, UDP, or both

- [x] Every open port on critical hosts maps to a documented service
- [x] Insecure protocols are disabled or replaced with encrypted versions
- [x] Remote access ports are not directly exposed to the public internet

Recommended Tools

Port scanner
Discovers open TCP and UDP ports and the services behind them

netstat or ss
Lists local listening ports and active connections

Firewall management console
Controls which ports and protocols are allowed or blocked

Service banner grabber
Identifies the software and version listening on a port

Industry Standards

IANA Service Name and Port Number Registry
Authoritative list of assigned port numbers

RFC 6335
Governs the procedures for port number assignment

CIS Benchmarks
Recommend disabling unneeded services and ports per platform

Career Relevance

Knowing ports and protocols cold is expected of network security engineers, SOC analysts, security engineers, and cloud security engineers. Analysts triage alerts by the ports and protocols involved, engineers write firewall and segmentation rules around them, and penetration testers map exposure by scanning them. It is one of the most frequently tested fundamentals in the interviews for roles that AI-Governance-Jobs.com serves.

Interview Questions

- What port does HTTPS use, and how does it differ from HTTP?
- Which transport protocol does DNS use, and why can it use both TCP and UDP?
- What are the three port ranges, and what is each used for?
- Why is exposing RDP directly to the internet risky, and what is a safer approach?
- How does a firewall use ports and protocols to make allow or deny decisions?

Related Certifications

CompTIA Network+ **CompTIA Security+** **Cisco CCNA**

Further Reading

- IANA Service Name and Port Number Registry
- NIST Computer Security Resource Center Glossary
- CISA: Securing Network Infrastructure Devices

Key Takeaways

- Ports let one IP address serve many services, each at a numbered endpoint.
- Well-known ports (0 to 1023) map to standard services like HTTP, HTTPS, and SSH.
- Protocols define the rules a service uses, usually paired with a default port.
- Every open port is attack surface, so close what you do not need.
- Prefer encrypted protocols over their plaintext predecessors.

FAQ

▶ **What is the difference between a port and a protocol?**

▶ **Does changing a service to a nonstandard port make it secure?**

▶ **Why do some protocols use both TCP and UDP?**

Related Careers

RELATED ROLES

Network Security Engineer

Soc Analyst | Security Engineer

RELATED CERTIFICATIONS

CompTIA Network+

CompTIA Security+ | Cisco CCNA

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps

Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Ports & Protocols**
3. Go deeper: TCP/IP
4. Go deeper: Firewalls
5. Validate it: work toward **CompTIA Network+**
6. Find the role: browse current openings

RELATED SHEETS

CS-041 TCP/IP | CS-043 Firewalls | CS-044 DNS Security | CS-051 Nmap

CS-001 Cybersecurity