SkillNewton

Common Network Ports Cheat Sheet

Standard TCP and UDP port numbers for web, email, remote access, DNS, DHCP, management, VPN and databases, grouped by category.

This cheat sheet lists the port numbers you meet most often in networking exams, firewall rules and server troubleshooting, grouped by what the service does. Each row shows the port and transport protocol, then the service. Numbers follow the IANA registry and widely documented software defaults. Remember that a default is only a convention: services can run on other ports, so confirm with `ss -tulpn` or the service configuration.

How to use it

1. **Learn the core ports first.** Start with 22, 25, 53, 80, 443, 3389 and the email ports. They appear in almost every exam and firewall rule set.
2. **Note the transport protocol.** A rule for 53/TCP does not cover 53/UDP. Check which protocol a service uses before opening a port.
3. **Check what is really listening.** Run `ss -tulpn` on Linux or `netstat -ano` on Windows to see the ports open on your own machine.
4. **Open only what you need.** Use the list to build firewall rules that allow required services and block the rest, especially database and remote-access ports.

Web

`80/TCP`	HTTP – unencrypted web traffic. Usually only redirects to HTTPS today.
`443/TCP`	HTTPS – HTTP over TLS (HTTP/1.1 and HTTP/2).
`443/UDP`	HTTP/3 – HTTP over QUIC.
`8080/TCP`	HTTP alternate – common for development servers, proxies and application servers.
`8443/TCP`	Widely used alternative HTTPS port for admin panels and application servers (a convention, not the IANA name).
`3128/TCP`	Squid HTTP proxy – default listening port.

Email

`25/TCP`	SMTP – mail transfer between servers. Many ISPs and cloud providers block outbound 25 from ordinary hosts.
`587/TCP`	SMTP submission – mail clients sending mail, upgraded to TLS with STARTTLS and authenticated.
`465/TCP`	SMTPS submission – mail clients sending over implicit TLS (RFC 8314).
`110/TCP`	POP3 – download mail from a mailbox (unencrypted).

995/TCP	POP3S – POP3 over TLS.
143/TCP	IMAP – access and sync mail kept on the server (unencrypted or STARTTLS).
993/TCP	IMAPS – IMAP over TLS.

File transfer and remote access

20/TCP	FTP data – used for transfers in active mode.
21/TCP	FTP control – commands and login, sent in clear text.
22/TCP	SSH – encrypted remote shell; also carries SFTP and SCP.
23/TCP	Telnet – unencrypted remote shell. Replace with SSH.
69/UDP	TFTP – simple file transfer with no login; used for network boot and device configs.
445/TCP	SMB – Windows file and printer sharing. Never expose to the internet.
137–139	NetBIOS – name service (137/UDP), datagram (138/UDP) and session service (139/TCP), used by older SMB.
2049/TCP	NFS – Network File System shares (UDP also possible on older versions).
3389/TCP	RDP – Windows Remote Desktop (also uses 3389/UDP). Put it behind a VPN or gateway.
5900/TCP	VNC – remote desktop (first display; 5901 for the second, and so on).
873/TCP	rsync daemon – used when rsync runs as a service rather than over SSH.

Name and directory services

53/UDP	DNS – standard queries and responses.
53/TCP	DNS – zone transfers and large responses.
853/TCP	DNS over TLS (DoT) – encrypted DNS queries.
67/UDP	DHCP server (BOOTP server) – receives client requests.
68/UDP	DHCP client (BOOTP client) – receives offers and acknowledgements.
546/UDP and 547/UDP	DHCPv6 – client (546) and server (547).
5353/UDP	mDNS – multicast DNS for local name discovery (.local names, printers, casting).
88/TCP and UDP	Kerberos – authentication in Active Directory and other realms.
389/TCP	LDAP – directory queries (also 389/UDP for some lookups).
636/TCP	LDAPS – LDAP over TLS.

3268/TCP	Global Catalog – forest-wide LDAP searches in Active Directory (3269/TCP over TLS).

Network management, time and VPN

123/UDP	NTP – time synchronisation.
161/UDP	SNMP – manager polls an agent on a device.
162/UDP	SNMP trap – device sends alerts to the manager.
514/UDP	Syslog – traditional log forwarding (unencrypted, no delivery guarantee).
6514/TCP	Syslog over TLS.
1812/UDP	RADIUS authentication (1813/UDP for accounting).
49/TCP	TACACS+ – device administration authentication, authorisation and accounting.
179/TCP	BGP – routing information exchange between routers.
500/UDP	IKE / ISAKMP – sets up IPsec VPN tunnels.
4500/UDP	IPsec NAT traversal – IKE and ESP traffic wrapped in UDP when NAT is in the path.
1194/UDP	OpenVPN – default port (TCP can also be used).
51820/UDP	WireGuard – commonly documented default listening port (configurable).

Databases and caches

3306/TCP	MySQL and MariaDB.
5432/TCP	PostgreSQL.
1433/TCP	Microsoft SQL Server default instance.
1521/TCP	Oracle Database listener.
27017/TCP	MongoDB.
6379/TCP	Redis.
11211/TCP	Memcached.
9200/TCP	Elasticsearch and OpenSearch HTTP API (9300/TCP for node-to-node traffic).

```
# Databases should listen only where needed. Check on Linux:
sudo ss -tulpn | grep -E ':(3306|5432|6379|27017)'
# 127.0.0.1:3306  -> local only (good for a single server)
# 0.0.0.0:3306    -> all interfaces: restrict with a firewall
```

Other common services

5060/UDP and TCP	SIP – VoIP call signalling.

5061/TCP	SIP over TLS.
3478/UDP	STUN and TURN – NAT traversal for voice and video calls.
631/TCP	IPP – Internet Printing Protocol (CUPS on Linux).
9100/TCP	Raw printing (often called JetDirect or AppSocket).
1883/TCP	MQTT – lightweight IoT messaging.
8883/TCP	MQTT over TLS.
5985/TCP	WinRM over HTTP – PowerShell remoting (5986/TCP over HTTPS).
520/UDP	RIP – Routing Information Protocol (RIPng for IPv6 uses 521/UDP).
6443/TCP	Kubernetes API server – common default.

Online version, with the matching free guide: skillnewton.com/resources/cheat-sheets/common-network-ports/
Learn this hands-on: Networking & Cybersecurity: Foundation & Practical Implementation – skillnewton.com/courses/networking-foundation-course/