Protocols And Ports

Protocol :

- A network protocol is a set of rules that govern data communication between different devices in the network.
- It determines what is being communicated, how it is being communicated, and when it is being communicated.
- It permits connected devices to communicate with each other, irrespective of internal and structural differences.

How are Protocols used in Cyber attacks ?

- Attackers can misuse the rules of how data is sent over the internet to cause problems for system.
- One common way they do this is through distributed denial of service (DDoS) attacks.

Standards :

- Standards are the sets of rules for communication that are needed for the exchange of information among devices.
- It is important to follow standards which are created by various Standard Organization like IEEE , ISO , ANSI.

Port :

- Ports is a logical address of a **16 – bits** unsigned integer that is allotted to every application on the computer that uses the internet to send or receive data.
- In the **OSI Model ports** are used in the Transport layer. In the headers of Transport layer protocols like **TCP** and **UDP,** we have a section to define port(port number).
- The network layer has to do nothing with ports, their protocols only care about **IP Addresses.**
- Ports are assigned by computer i.e. operating system to different applications. Ports help computer to differentiate between incoming and outgoing traffic.
- The port is a **16-bit** unsigned number it ranges from **0 to 65535.**

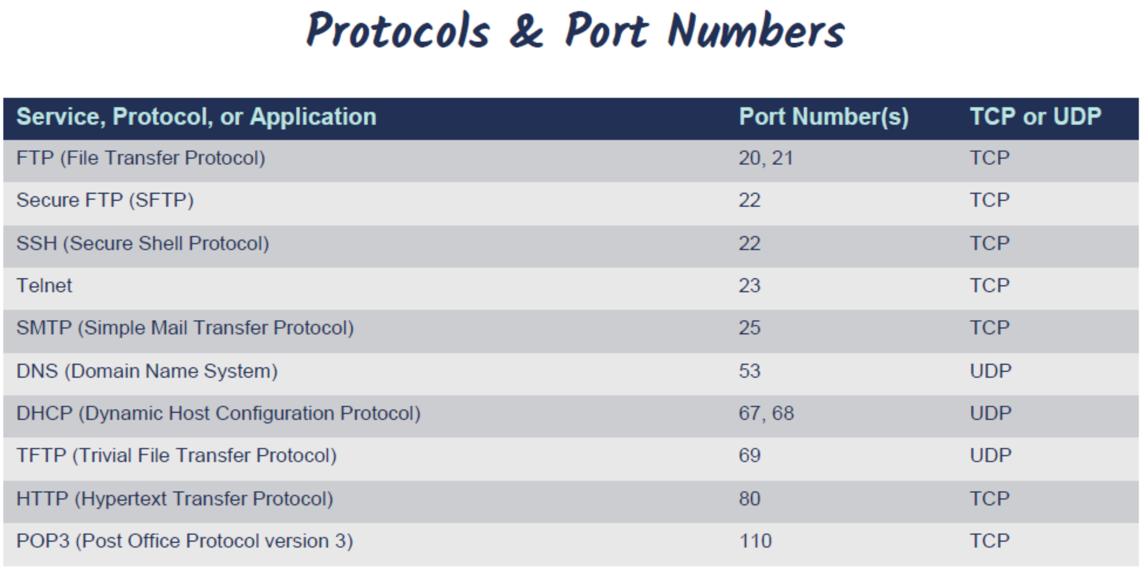
Types of Ports

Ports are further divided into three categories:

- Well Known Port
- Registered port
- Dynamic Port

1. **Well Known Port**
    - It is from the range 0 to 1023.
    - It is reserved for common and specifically used service.
    - It is used by some widely adopted protocols and services like HTTP(port 80), FTP(port 21), DNS(Port 53), SSH(port 22), etc.....

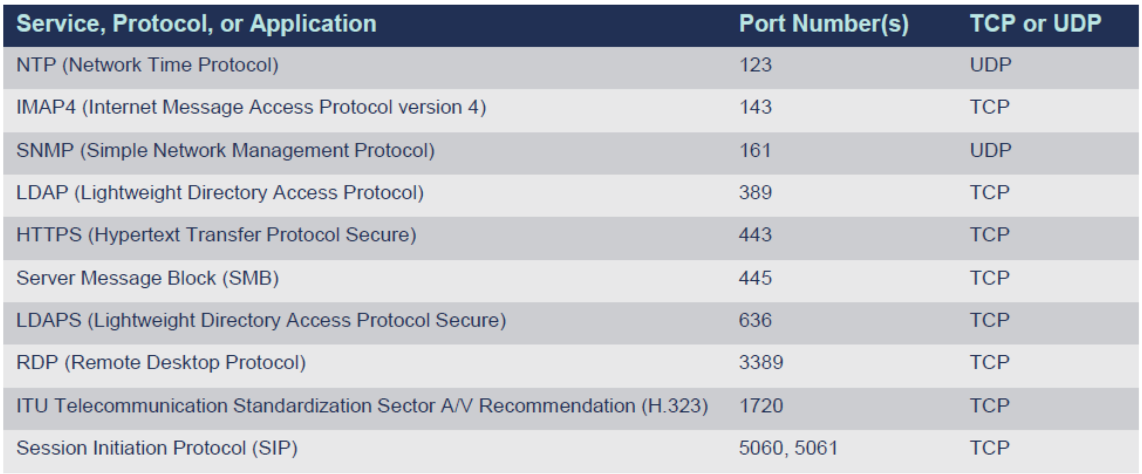
2. **Registered Port**
    - It is from range 1024 to 49151.
    - These are used by applications or services that are not as common.
    - But it is used by those applications or services which require its specific port.
    - Organizations can ask IANA(Internet Assigned Number Authority) for any specific port number within this range.
3. **Dynamic Port**
    - It is from range 49152 to 65535.
    - It is also known as Ephemeral or Private Port.
    - It is used for those connections that are temporary or short-lived.
    - It is not registered or assigned and can be used by any process.



Protocols & Port Numbers

Service, Protocol, or Application	Port Number(s)	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
Secure FTP (SFTP)	22	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System)	53	UDP
DHCP (Dynamic Host Configuration Protocol)	67, 68	UDP
TFTP (Trivial File Transfer Protocol)	69	UDP
HTTP (Hypertext Transfer Protocol)	80	TCP
POP3 (Post Office Protocol version 3)	110	TCP

Protocols & Port Numbers



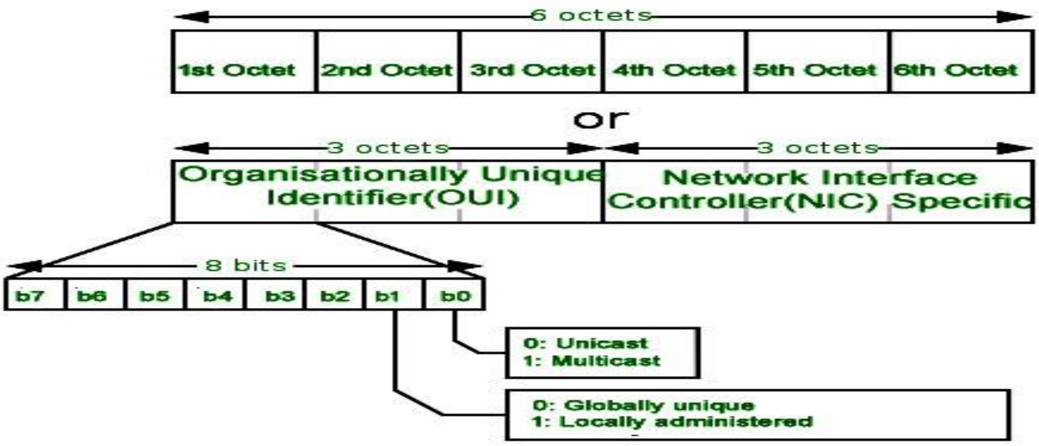
Service, Protocol, or Application	Port Number(s)	TCP or UDP
NTP (Network Time Protocol)	123	UDP
IMAP4 (Internet Message Access Protocol version 4)	143	TCP
SNMP (Simple Network Management Protocol)	161	UDP
LDAP (Lightweight Directory Access Protocol)	389	TCP
HTTPS (Hypertext Transfer Protocol Secure)	443	TCP
Server Message Block (SMB)	445	TCP
LDAPS (Lightweight Directory Access Protocol Secure)	636	TCP
RDP (Remote Desktop Protocol)	3389	TCP
ITU Telecommunication Standardization Sector A/V Recommendation (H.323)	1720	TCP
Session Initiation Protocol (SIP)	5060, 5061	TCP

What is a MAC address?

- A **MAC (Media Access Control) address** is a hardware identifier for a network interface used at the data-link layer (OSI Layer 2).
- It's used to uniquely identify devices on the same local network segment so Ethernet/Wi-Fi frames can be delivered correctly.

Format & size

- Size: **48 bits** (6 bytes) for the common MAC (also there are 64-bit MACs but rare).
- Typical notation: 00:1A:2B:3C:4D:5E or 00-1A-2B-3C-4D-5E or 001A.2B3C.4D5E.
- Hexadecimal — each byte is two hex digits (00–FF).



Structure & meaning

- First 3 bytes (24 bits) = **OUI** (Organizationally Unique Identifier) → identifies the manufacturer/vendor.
- Last 3 bytes = device-specific identifier assigned by the vendor.
- Two important bits in the first byte:
  - **LSB (Least Significant Bit) of first octet = 1** → *multicast* MAC (frame is for multiple devices); =0 → *unicast*.
  - **Second LSB of first octet = 1** → *locally administered* (not globally unique; set by local admin or OS). =0 → *globally unique* assigned by vendor.

Where it's used :

- Layer 2 (Ethernet, Wi-Fi).
- Devices use **ARP** (Address Resolution Protocol) to map IP → MAC on IPv4 local networks.
- Switches use MAC tables to forward frames to the correct port.

What is ARP?

ARP stands for **Address Resolution Protocol**.

- It is a **network protocol** used to **map a device's IP address (Layer 3)** to its **MAC address (Layer 2)** on a local network.
- Works **only within the same LAN** (Local Area Network).
- Part of the **TCP/IP suite**.

Think of it like: You know the house number (IP), but you need the name of the person living there (MAC) to deliver a letter.

Why ARP is needed :

- When a device wants to send data to another device on the same network, it knows the **IP address** but needs the **MAC address** to send the frame at Layer 2 (Ethernet/Wi-Fi).
- ARP resolves the IP → MAC mapping.

Types of ARP :

1. **Static ARP** – Manual entry of IP ↔ MAC. Doesn't change automatically.
2. **Dynamic ARP** – Automatically resolved using ARP request/reply. Most common.

3. **Gratuitous ARP** – Device announces its own IP ↔ MAC mapping to check for conflicts or update other devices' ARP tables.

What is RARP?

RARP stands for **Reverse Address Resolution Protocol**.

- It is the **opposite of ARP**.
- While **ARP maps IP → MAC**, **RARP maps MAC → IP**.
- Used **mainly by diskless workstations or devices** that know their hardware (MAC) address but don't know their IP address yet.

Think of it like: You know the person (MAC), but you don't know their house number (IP) and you want someone to tell you.

Quick Analogy

- **ARP:** "I know the house number, who lives here?" (IP → MAC)
- **RARP:** "I know the person, what is their house number?" (MAC → IP)

Some common and useful in cybersecurity Protocols :

1. TCP/IP (Transmission Control Protocol / Internet Protocol)

- **Layer: Network / Transport**
- **Port Number: N/A (TCP/IP itself is the suite; individual protocols have ports)**
- **Purpose:**
  - **TCP ensures reliable delivery of data.**
  - **IP handles addressing and routing between devices.**
- **Cybersecurity Use:**
  - **Network mapping, packet capture, firewall configuration, pentesting network connectivity.**

---

2. HTTP (Hypertext Transfer Protocol)

- **Layer: Application**
- **Port Number: 80 (TCP)**
- **Purpose: Transfers web pages over the Internet (unencrypted).**

- Cybersecurity Use:
  - Web application testing (XSS, SQL injection).
  - Traffic inspection and vulnerability scanning.

---

3. HTTPS (Hypertext Transfer Protocol Secure)

- Layer: Application
- Port Number: 443 (TCP)
- Purpose: Encrypted web traffic using TLS/SSL.
- Cybersecurity Use:
  - Secure communication testing.
  - SSL/TLS vulnerability assessment.
  - Certificate inspection for man-in-the-middle attacks.

---

4. DNS (Domain Name System)

- Layer: Application
- Port Number: 53 (UDP/TCP)
- Purpose: Resolves domain names (e.g., www.example.com → IP address).
- Cybersecurity Use:
  - Detecting DNS tunneling or exfiltration.
  - Phishing and malware command-and-control detection.
  - Network reconnaissance.

---

5. FTP (File Transfer Protocol)

- Layer: Application
- Port Number: 21 (control), 20 (data)
- Purpose: Transfers files between client and server.
- Cybersecurity Use:
  - Checking weak or default credentials.
  - Testing file upload vulnerabilities.

- Monitoring unencrypted file transfers.

---

6. SFTP / FTPS (Secure FTP)

- **Layer: Application**
- **Port Number:**
  - SFTP → 22 (uses SSH)
  - FTPS → 990 (implicit), 21 (explicit)
- **Purpose: Secure file transfer.**
- **Cybersecurity Use:**
  - Secure auditing of file transfers.
  - Pentesting encrypted communication channels.

---

7. SSH (Secure Shell)

- **Layer: Application**
- **Port Number: 22 (TCP)**
- **Purpose: Encrypted remote administration and command execution.**
- **Cybersecurity Use:**
  - Remote administration security checks.
  - Brute-force and weak credential testing.
  - Port-forwarding attacks analysis.

---

8. ARP (Address Resolution Protocol)

- **Layer: Data Link**
- **Port Number: N/A (works at Layer 2)**
- **Purpose: Maps IP addresses to MAC addresses in a LAN.**
- **Cybersecurity Use:**
  - ARP spoofing/poisoning detection.
  - Man-in-the-middle attack analysis.
  - LAN reconnaissance.

9. RARP (Reverse ARP)

- **Layer: Data Link**
- **Port Number: N/A**
- **Purpose: Maps MAC addresses to IP addresses (obsolete, replaced by DHCP).**
- **Cybersecurity Use: Mostly historical; rarely used today.**

10. DHCP (Dynamic Host Configuration Protocol)

- **Layer: Application**
- **Port Number: 67 (server), 68 (client)**
- **Purpose: Dynamically assigns IP addresses and network settings.**
- **Cybersecurity Use:**
  - **Detect rogue DHCP servers.**
  - **Prevent IP conflicts.**
  - **Audit automatic network assignments.**

11. ICMP (Internet Control Message Protocol)

- **Layer: Network**
- **Port Number: N/A (uses IP directly)**
- **Purpose: Diagnostics and error reporting (ping, traceroute).**
- **Cybersecurity Use:**
  - **Network scanning and reconnaissance.**
  - **Detecting network devices and availability.**
  - **Ping flood / DoS attack detection.**

12. SNMP (Simple Network Management Protocol)

- **Layer: Application**
- **Port Number: 161 (agent), 162 (trap)**
- **Purpose: Monitors and manages network devices.**

- Cybersecurity Use:
    - Enumerating network devices.
    - Checking default or weak community strings.
    - Detecting misconfigured devices.

---

13. Telnet

- Layer: Application
- Port Number: 23 (TCP)
- Purpose: Remote terminal access (unencrypted).
- Cybersecurity Use:
    - Checking for legacy services.
    - Brute-force testing.
    - Security risk assessment (unencrypted credentials).

---

14. SMTP (Simple Mail Transfer Protocol)

- Layer: Application
- Port Number: 25 (TCP), 465 (SSL), 587 (TLS)
- Purpose: Sending emails.
- Cybersecurity Use:
    - Phishing detection.
    - Email server security auditing.

---

15. IMAP / POP3 (Email Receiving Protocols)

- Layer: Application
- Port Number:
    - IMAP → 143 (unencrypted), 993 (SSL)
    - POP3 → 110 (unencrypted), 995 (SSL)
- Purpose: Retrieving emails from servers.
- Cybersecurity Use:

  - Email server security checks.
  - Phishing or malware email analysis.

---

16. NTP (Network Time Protocol)

- Layer: Application
- Port Number: 123 (UDP)
- Purpose: Synchronizes system clocks over the network.
- Cybersecurity Use:
  - Detect DDoS amplification (via open NTP servers).
  - Forensic timeline analysis in attacks.

---

17. SSL / TLS (Secure Sockets Layer / Transport Layer Security)

- Layer: Presentation / Application
- Port Number: 443 (HTTPS), 465 (SMTPS), 993 (IMAPS)
- Purpose: Encrypts data in transit.
- Cybersecurity Use:
  - Man-in-the-middle attack prevention.
  - Certificate validation and security auditing.

---

18. VPN Protocols (IPSec, OpenVPN, WireGuard)

- Layer: Network / Transport
- Port Number:
  - IPSec → 500, 4500
  - OpenVPN → 1194
  - WireGuard → 51820
- Purpose: Secure remote access and encrypted tunnels.
- Cybersecurity Use:
  - Secure remote administration.
  - Penetration testing of VPN access.

- Bypass testing for restricted networks.

---

19. LDAP (Lightweight Directory Access Protocol)

- **Layer: Application**
- **Port Number: 389 (unencrypted), 636 (SSL/TLS)**
- **Purpose: Access and manage directory services (like Microsoft Active Directory).**
- **Cybersecurity Use:**
  - User enumeration attacks.
  - Checking for weak credentials.
  - Directory and permission auditing.

---

20. Kerberos

- **Layer: Application**
- **Port Number: 88 (TCP/UDP)**
- **Purpose: Authentication protocol for secure network login.**
- **Cybersecurity Use:**
  - Brute-force or pass-the-ticket attacks.
  - Authentication auditing in Active Directory environments.

---

21. SNTP (Simple Network Time Protocol)

- **Layer: Application**
- **Port Number: 123 (UDP, like NTP)**
- **Purpose: Lightweight version of NTP for clock synchronization.**
- **Cybersecurity Use:**
  - Detect inaccurate clocks affecting log correlation in security analysis.

---

22. TFTP (Trivial File Transfer Protocol)

- **Layer: Application**
- **Port Number: 69 (UDP)**

- **Purpose: Simple, unencrypted file transfer protocol.**
- **Cybersecurity Use:**
    - **Often used by network devices for firmware updates.**
    - **Risk: Default or misconfigured TFTP servers can expose files.**

---

23. SNTP / NFS / SMB / CIFS (File & Sharing Protocols)

- **SMB/CIFS:**
    - **Layer: Application**
    - **Port: 445 (TCP)**
    - **Purpose: Windows file and printer sharing.**
    - **Cybersecurity Use: Exploited by ransomware (like WannaCry), network enumeration.**
- **NFS:**
    - **Layer: Application**
    - **Port: 2049 (TCP/UDP)**
    - **Purpose: UNIX/Linux file sharing.**
    - **Cybersecurity Use: File access control audits, misconfigured shares.**

---

24. SIP (Session Initiation Protocol)

- **Layer: Application**
- **Port Number: 5060 (unencrypted), 5061 (TLS)**
- **Purpose: Voice over IP (VoIP) signaling protocol.**
- **Cybersecurity Use:**
    - **VoIP eavesdropping, toll fraud testing.**
    - **SIP enumeration for reconnaissance.**

---

25. RTP / RTCP (Real-time Transport Protocol / Control Protocol)

- **Layer: Application / Transport**
- **Port Number: Dynamic UDP ports (usually 1024–65535)**

- Purpose: Transports real-time audio/video (VoIP, streaming).
- Cybersecurity Use:
  - Voice sniffing in insecure VoIP setups.
  - Network performance auditing.

---

26. MQTT (Message Queuing Telemetry Transport)

- Layer: Application
- Port Number: 1883 (unencrypted), 8883 (TLS)
- Purpose: Lightweight IoT messaging protocol.
- Cybersecurity Use:
  - IoT device enumeration and security testing.
  - Preventing unauthorized device communication.

---

27. CoAP (Constrained Application Protocol)

- Layer: Application
- Port Number: 5683 (UDP)
- Purpose: IoT protocol for low-power devices.
- Cybersecurity Use:
  - IoT penetration testing.
  - Detect misconfigured or exposed sensors/devices.

---

28. RDP (Remote Desktop Protocol)

- Layer: Application
- Port Number: 3389 (TCP)
- Purpose: Remote desktop access to Windows machines.
- Cybersecurity Use:
  - Brute-force attacks and credential testing.
  - RDP exploitation in network intrusions.

---

29. VNC (Virtual Network Computing)

- **Layer: Application**
- **Port Number: 5900 (TCP, default), 5901+ for multiple sessions**
- **Purpose: Remote desktop access (cross-platform).**
- **Cybersecurity Use:**
  - **Password brute-forcing.**
  - **Detect open VNC servers in networks.**

---

30. NetBIOS / NetBIOS over TCP/IP

- **Layer: Application**
- **Port Number: 137–139 (UDP/TCP)**
- **Purpose: Windows name resolution, file sharing, network browsing.**
- **Cybersecurity Use:**
  - **Enumeration of hosts and shared resources.**
  - **Checking for misconfigured or exposed shares.**

---

31. LDAP over SSL (LDAPS)

- **Layer: Application**
- **Port Number: 636 (TCP)**
- **Purpose: Secure version of LDAP for directory services (encrypted).**
- **Cybersecurity Use:**
  - **Secure user enumeration.**
  - **Prevent interception of credentials.**
  - **Auditing Active Directory securely.**

---

32. Kerberos over TCP/UDP

- **Layer: Application**
- **Port Number: 88**
- **Purpose: Secure authentication protocol for Windows/Linux networks.**

- **Cybersecurity Use:**
    - **Detect weak tickets or replay attacks.**
    - **Brute-force password attacks (Kerberoasting).**

---

33. S/MIME (Secure/Multipurpose Internet Mail Extensions)

- **Layer: Application**
- **Port Number: Uses email protocols like SMTP (25, 465, 587), IMAP (143/993)**
- **Purpose: Encrypt and digitally sign email messages.**
- **Cybersecurity Use:**
    - **Secure email communication.**
    - **Phishing prevention.**

---

34. SIP-TLS (Secure VoIP)

- **Layer: Application**
- **Port Number: 5061 (TCP)**
- **Purpose: Encrypted VoIP signaling over TLS.**
- **Cybersecurity Use:**
    - **VoIP security testing.**
    - **Prevent eavesdropping on calls.**

---

35. MQTT over TLS

- **Layer: Application**
- **Port Number: 8883**
- **Purpose: Secure IoT messaging.**
- **Cybersecurity Use:**
    - **IoT device secure communication.**
    - **Penetration testing for IoT networks.**

---

36. CoAP over DTLS

- **Layer: Application**
- **Port Number: 5684 (UDP)**
- **Purpose: Secure CoAP (IoT devices).**
- **Cybersecurity Use:**
    - **Secure IoT communication testing.**
    - **Detect exposed IoT devices.**

---

37. RDP over TLS

- **Layer: Application**
- **Port Number: 3389**
- **Purpose: Secure Remote Desktop access.**
- **Cybersecurity Use:**
    - **Brute-force and credential testing.**
    - **Detect misconfigured remote access servers.**

---

38. VNC over TLS / SSL

- **Layer: Application**
- **Port Number: 5900+ (TCP)**
- **Purpose: Secure VNC sessions.**
- **Cybersecurity Use:**
    - **Remote access security audits.**
    - **Prevent unauthorized access.**

---

39. NetBIOS over TCP/IP

- **Layer: Application**
- **Port Number: 137–139**
- **Purpose: Windows legacy name resolution and file sharing.**
- **Cybersecurity Use:**
    - **Enumeration of Windows shares.**

- Detect open or misconfigured file shares.

---

40. SMB over TCP (Direct Hosting)

- Layer: Application
- Port Number: 445
- Purpose: File sharing and network resource access in Windows.
- Cybersecurity Use:
    - Ransomware attack surface (WannaCry, NotPetya).
    - File share auditing and pentesting.

---

41. IPsec (Internet Protocol Security)

- Layer: Network / Transport
- Port Number: 500 (IKE), 4500 (NAT traversal)
- Purpose: Secure VPN tunnels.
- Cybersecurity Use:
    - VPN security auditing.
    - Detect weak encryption or misconfigurations.

---

42. OpenVPN

- Layer: Network / Transport
- Port Number: 1194 (UDP/TCP)
- Purpose: Secure VPN protocol.
- Cybersecurity Use:
    - Penetration testing of remote access.
    - Check for open and misconfigured VPN servers.

---

43. WireGuard

- Layer: Network / Transport
- Port Number: 51820 (UDP)

- Purpose: Modern lightweight VPN protocol.
- Cybersecurity Use:
  - IoT and small network VPN security audits.
  - Test for misconfigured or exposed endpoints.

---

44. SNMPv3 (Secure)

- Layer: Application
- Port Number: 161/162 (TCP/UDP)
- Purpose: Secure network monitoring (authentication + encryption).
- Cybersecurity Use:
  - Check for misconfigured SNMP access.
  - Network device auditing and enumeration.

---

45. NFSv4 (Network File System)

- Layer: Application
- Port Number: 2049 (TCP/UDP)
- Purpose: UNIX/Linux file sharing.
- Cybersecurity Use:
  - Audit exported directories.
  - Detect insecure NFS shares.

---

46. TFTP (Trivial FTP)

- Layer: Application
- Port Number: 69 (UDP)
- Purpose: Simple file transfer without authentication.
- Cybersecurity Use:
  - Exploitation of misconfigured servers.
  - Firmware and device file exposure testing.

---

47. H.323

- Layer: Application
- Port Number: 1720 (TCP)
- Purpose: VoIP and video conferencing.
- Cybersecurity Use:
  - VoIP security auditing.
  - Detect open and unencrypted H.323 services.

---

48. RTP / RTCP

- Layer: Application / Transport
- Port Number: Dynamic (1024–65535 UDP)
- Purpose: Real-time audio/video streaming.
- Cybersecurity Use:
  - Voice sniffing for unencrypted VoIP streams.
  - Media streaming security analysis.

---

49. SIP (Session Initiation Protocol)

- Layer: Application
- Port Number: 5060 (unencrypted), 5061 (TLS)
- Purpose: VoIP signaling.
- Cybersecurity Use:
  - Enumerate SIP endpoints.
  - Test for insecure VoIP configuration.

---

50. MQTT / CoAP (IoT Protocols)

- Layer: Application
- Port Number: MQTT → 1883, 8883 (TLS); CoAP → 5683, 5684 (DTLS)
- Purpose: Messaging for IoT devices.
- Cybersecurity Use:

- **Test for exposed IoT devices.**
- **Security auditing of communication channels.**