



Networking

Network Services
Protocols



Network Services Protocols

- Guiding Question: How do network service protocols facilitate communication, management, and security across a network?
- Students will:
 - Explain the role of network service protocols in automating and managing network functions.
 - Identify key protocols, their port numbers, and their primary functions.
 - Describe how DHCP dynamically assigns IP addresses to devices.



Network Service Protocols.

- **Network Service Protocols** are protocols that help devices talk to each other, stay in sync and stay secure.
- Used for:
 - Getting IP addresses
 - Sharing files
 - Logging in securely
 - Monitoring devices
 - Keeping accurate time



DHCP & NTP

Dynamic Host Configuration Protocol (DHCP) – Port 67 & 68

- Gives devices an IP address automatically.
- Port 67 server – giving out IP addresses.
- Port 68 client – requesting an IP address.

Network Time Protocol (NTP) – Port 123

- NTP syncs the clocks on all devices to within a millisecond of each other.
- Accurate time is key for logs or troubleshooting or some types of encryption
- Requires a server which can be a network device or an external one.



SNMP

Simple Network Management Protocol (SNMP) – 161 & 162

- Checks on devices automatically and provides reports or alerts to an admin.
- Port 161 - Send out SNMP queries like “What’s the temperature of this PC?” or “How much memory is this application using on the device?”
- Port 162 – Incoming “traps” which are alerts or notifications when something goes wrong.



Syslog & SIP

Syslog

- Collects logs from all devices and stores them in one place
- Great too for identifying problems or unusual behavior on the network.

Session Initiation Protocol (SIP) – Port 5060

- Starts and ends Voice over IP (VoIP) calls and video chats.
- SIPS is the encrypted secure version – Port 5061



LDAP & SMB

Lightweight Directory Access Protocol (LDAP) – Port 389

- Checks your username and password when you log in.
- LDAPS is the secure encrypted version of LDAP – Port 636

Server Message Block (SMB) – Port 445

- Allows computers to share files and printers.
- Primarily used by Windows OS devices.



Port Scanners

- Port scanning software is used by admins to check whether services are configured properly across the network.
- The scanner sends test packets to a device's ports to gather information including:
 - Port status – open, closed or filtered by firewall.
 - Services running on the device – SSH, RDP, SMB, etc.
 - What version service – Example: OpenSSHv2
- Nmap is the most popular port scanning software.
 - It is free and works on most operating systems.
 - The GUI version is Zenmap.

