Session 6 - Protocols

Group 1: Core Cyber Security Protocols

Protocol	Abbreviation	Purpose	Port(s)	OSI Layer
HTTP	HyperText Transfer Protocol	Web browsing (insecure; no encryption)	80	Application
HTTPS	HyperText Transfer Protocol Secure	Secure web browsing using encryption (TLS/SSL)	443	Application
DNS	Domain Name System	Resolves domain names (like google.com) to IP addresses	53	Application
FTP	File Transfer Protocol	Transfers files between client and server without encryption	20 (data), 21 (control)	Application
DHCP	Dynamic Host Configuration Protocol	Automatically assigns IP address and network settings	67 (server), 68 (client)	Application
SMTP	Simple Mail Transfer Protocol	Sends outgoing emails from clients to servers	25	Application
IMAP	Internet Message Access Protocol	Accesses and manages emails stored on a mail server	143 (993 secure)	Application

Group 2: Bonus/Extended Protocols

Protocol	Abbreviation	Purpose	Port(s)	OSI Layer
POP3	Post Office Protocol v3	Downloads emails from the server to the client	110 (995 secure)	Application
SFTP	SSH File Transfer Protocol	Secure file transfer over SSH connection	22	Application
FTPS	FTP Secure	FTP with added SSL encryption for secure transfers	990	Application
SSH	Secure Shell	Secure command-line access to remote machines	22	Application
Telnet	—	Unencrypted remote terminal access (insecure)	23	Application
SNMP	Simple Network Management Protocol	Monitors and manages devices on a network	161 (requests), 162 (traps)	Application
RDP	Remote Desktop Protocol	Accesses and controls remote Windows desktops	3389	Application
NTP	Network Time Protocol	Keeps all networked systems' clocks in sync	123	Application
LDAP	Lightweight Directory Access Protocol	Authenticates and organizes user data for access control	389 (636 secure)	Application

Group 3: Supporting Protocols (Lower Layers)

Protocol	Abbreviation	Purpose	OSI Layer
TCP	Transmission Control Protocol	Provides reliable, ordered, and error-checked delivery	Transport
UDP	User Datagram Protocol	Sends fast, connectionless data with minimal overhead	Transport
IP	Internet Protocol	Determines where packets are sent across networks	Network
ARP	Address Resolution Protocol	Maps IP addresses to MAC addresses on local networks	Data Link
ICMP	Internet Control Message Protocol	Sends error messages and diagnostics (e.g., ping)	Network

Conclusion

Understanding these network protocols is essential for anyone entering cybersecurity, ethical hacking, or network defense roles. Each protocol plays a unique role in how data is sent, received, secured, or attacked across networks.

From assigning IPs (DHCP), to browsing (HTTP/HTTPS), to securing communication (SSH, SSL), and analyzing threats (DNS, ICMP), these protocols are the language of the internet.

Whether you're defending a network, analyzing packets, or detecting attacks, knowing what each protocol does—and which port and layer it operates on—gives you the edge to respond faster and smarter.

Mastering protocols isn’t just theory—it’s the real toolkit of a cyber warrior.