
WEEK 1 – NETWORKING FOUNDATIONS

DAY 6 – COMMON PROTOCOLS

---

1. Why Protocols Are Important

In networking, protocols define **how devices communicate**.

- Without protocols, devices cannot understand each other
- They define:
  - Data format
  - Communication rules
  - Error handling

Think of it like:

Languages in which two people communicate—English, French, etc.

Every application uses a **specific protocol** suited for its purpose.

---

2. HTTP / HTTPS

HTTP – Hypertext Transfer Protocol

- Layer: **Application (OSI Layer 7)**
- Purpose: **Transfer web pages (text, images, videos)**
- Port: **80**
- Stateless protocol → each request is independent

How it works (simplified):

1. Client (browser) sends HTTP request to server
2. Server responds with requested resource

Problem with HTTP: Data is sent in **plain text** → insecure

HTTPS – Secure HTTP

- Layer: **Application (with encryption)**
- Uses **TLS/SSL encryption** → ensures confidentiality
- Port: **443**

Benefits:

- Data cannot be sniffed
- Server identity verified (certificates)
- Prevents man-in-the-middle attacks

Interview line:

“HTTPS secures HTTP traffic using TLS/SSL encryption to ensure data confidentiality and integrity.”

---

3. FTP / SFTP – File Transfer

FTP – File Transfer Protocol

- Port: **21** (control), **20** (data)
- Unencrypted → insecure
- Used for transferring files

Interview line:

“FTP allows file transfer but is insecure because credentials and data are sent in plain text.”

SFTP – Secure File Transfer Protocol

- Uses **SSH encryption** → secure channel
- Port: **22**
- Ensures confidentiality and authentication

Interview line:

“SFTP securely transfers files using SSH, encrypting both credentials and data.”

---

4. Email Protocols – SMTP, POP3, IMAP

SMTP – Simple Mail Transfer Protocol

- Layer: Application
- Port: **25 (standard), 587 (submission)**
- Purpose: **Sending emails**
- Works only **from client to server or server to server**

POP3 – Post Office Protocol v3

- Layer: Application
- Port: **110**

- Purpose: **Download emails from server to local device**
- Emails are **usually deleted from server after download**

IMAP – Internet Message Access Protocol

- Layer: Application
- Port: **143 (non-secure), 993 (secure)**
- Purpose: **Access emails while keeping them on server**
- Sync across multiple devices

Interview line:

“SMTP sends emails, POP3 downloads emails, and IMAP allows synchronized access across devices.”

---

5. DNS Basics – Domain Name System

What DNS Does

- Converts **human-readable domain names** into **IP addresses**
- Example: www.google.com → 142.250.190.132

DNS Lookup Process (Step-by-Step)

1. Client checks **local cache**
2. If not found, queries **recursive resolver**
3. Resolver queries **root server → TLD server → authoritative server**
4. IP returned to client → website loads

Interview line:

“DNS translates domain names into IP addresses so computers can route traffic correctly.”

---

6. Security Focus – DNS Spoofing (DNS Cache Poisoning)

What is DNS Spoofing?

- Attacker **injects fake DNS entries** into client or resolver cache
- Redirects users to **malicious websites** instead of legitimate ones

Example

- User types www.bank.com
- Attacker redirects to fake page → steals credentials

Mitigation

- Use **DNSSEC (DNS Security Extensions)**
- Use **trusted DNS servers**
- Monitor DNS logs for anomalies

Interview line:

"DNS spoofing is an attack where fake DNS records redirect users to malicious sites, which can be mitigated using DNSSEC and trusted resolvers."

---

7. Quick Reference Table – Common Protocols

Protocol	Purpose	Port	Security
HTTP	Web browsing	80	Plain text
HTTPS	Secure web	443	TLS/SSL
FTP	File transfer	21	Plain text
SFTP	Secure file transfer	22	SSH encryption
SMTP	Send email	25/587	Can use TLS
POP3	Download email	110	Can use SSL
IMAP	Access email	143/993	Can use SSL/TLS
DNS	Name resolution	53	Vulnerable without DNSSEC

---

8. Real-Life Analogy

- HTTP/HTTPS → Sending letters online
- FTP/SFTP → Moving files between two computers
- SMTP → Mailman sending letters
- POP3 → Collecting letters from mailbox
- IMAP → Reading letters without removing them
- DNS → Phone book mapping names → addresses

---

9. Day 6 Revision Checklist

You should be able to:

1. Explain HTTP vs HTTPS and why HTTPS is secure
2. Explain FTP vs SFTP with port numbers and security

3. Explain SMTP, POP3, IMAP differences
4. Explain DNS lookup process
5. Explain DNS spoofing and mitigation
6. Give real-life analogies for all protocols