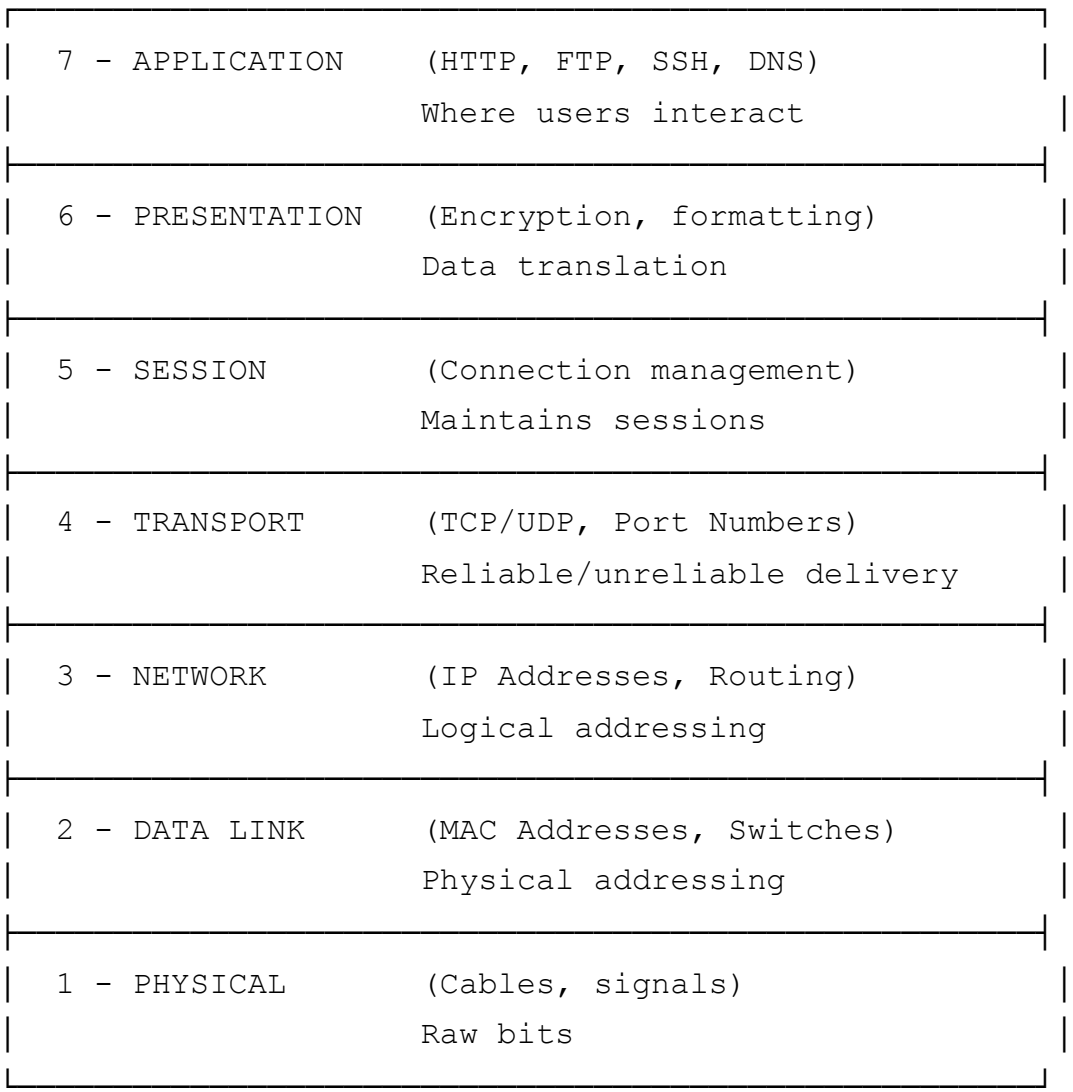
OSI Model Reference Sheet

The 7 Layers (Top to Bottom)



Mnemonic Device

"Please Do Not Throw Sausage Pizza Away"

- **P**hysical
- **D**ata Link
- **N**etwork
- **T**ransport
- **S**ession
- **P**resentation

- **A**pplication

Layer Details for Security+

Layer 7 - Application ⭐⭐⭐

What it does: User interface, where applications interact with the network

Protocols: HTTP, HTTPS, FTP, SSH, DNS, SMTP, POP3, IMAP, Telnet

Devices: Firewalls (application-level), WAF (Web Application Firewall)

Security Concerns:

- SQL injection
- Cross-site scripting (XSS)
- Application-layer DDoS attacks
- Malware downloads

Layer 6 - Presentation

What it does: Data formatting, encryption/decryption, compression

Security Concerns:

- SSL/TLS encryption happens here
- Data encoding issues

Note: Not heavily tested on Security+

Layer 5 - Session

What it does: Establishes, maintains, and terminates connections

Security Concerns:

- Session hijacking

Note: Not heavily tested on Security+

Layer 4 - Transport ⭐⭐⭐

What it does: Manages end-to-end data delivery

Protocols: TCP (reliable), UDP (fast but unreliable)

Key Concept: PORT NUMBERS live here

Devices: Firewalls (port filtering)

Security Concerns:

- SYN flood attacks
- Port scanning
- Firewall evasion

Layer 3 - Network ⭐⭐⭐

What it does: Routes packets between networks using logical addresses

Protocols: IP, ICMP, IPsec

Key Concept: IP ADDRESSES live here

Devices: Routers, Layer 3 switches, firewalls (packet filtering)

Security Concerns:

- IP spoofing
- Ping sweeps
- ICMP tunneling
- Man-in-the-middle attacks

Layer 2 - Data Link ⭐⭐

What it does: Handles physical addressing on the local network

Key Concept: MAC ADDRESSES live here

Devices: Switches, bridges, WAPs (wireless access points)

Security Concerns:

- MAC spoofing
- ARP spoofing/poisoning
- CAM table overflow
- MAC flooding

Layer 1 - Physical

What it does: Physical transmission of raw bits

Examples: Cables, fiber optics, radio waves, network cards

Security Concerns:

- Wiretapping
- Physical access attacks
- Cable cutting

TCP/IP Model (Practical Alternative)

The TCP/IP model is what's actually used in real networks:

TCP/IP Layer	OSI Equivalent	Description
Application	Layers 7, 6, 5	User-facing protocols
Transport	Layer 4	TCP/UDP
Internet	Layer 3	IP routing
Network Access	Layers 2, 1	Physical network

Security+ Quick Reference

When you hear...

- "IP address filtering" → **Layer 3**
- "Port filtering" → **Layer 4**
- "MAC address filtering" → **Layer 2**
- "SQL injection" → **Layer 7**
- "WAF" → **Layer 7**
- "Router" → **Layer 3**
- "Switch" → **Layer 2**
- "Firewall" → **Layers 3-4** (or 7 for application firewalls)

Remember: Most attacks happen at Layer 7 (Application) where users interact!