# Networking Fundamentals for Cybersecurity

*By Lucio Rodrigues*

---

## 📖 Abbreviation Summary

- **IP** - Internet Protocol
- **LAN** - Local Area Network
- **WAN** - Wide Area Network
- **DNS** - Domain Name System
- **DHCP** - Dynamic Host Configuration Protocol
- **NAT** - Network Address Translation
- **TCP** - Transmission Control Protocol
- **UDP** - User Datagram Protocol
- **VPN** - Virtual Private Network
- **IDS/IPS** - Intrusion Detection/Prevention System
- **OSI Model** - Open Systems Interconnection Model

---

## 🚀 Introduction

Networking is the **backbone of cybersecurity**. Every cyberattack, defense mechanism, and investigation relies on how devices communicate. From securing corporate infrastructures to analysing suspicious traffic, **strong networking fundamentals are essential** for any cybersecurity professional.

This page highlights key networking concepts with practical relevance, explained clearly so both technical and non-technical readers can follow.

---

# 🔑 Core Networking Concepts

## 🧩 1. The OSI Model

The **OSI Model** describes how data travels through **seven layers**.

- **Physical** - Cables, signals, hardware.
- **Data Link** - Device-to-device communication (MAC addresses).
- **Network** - IP addressing, routing.
- **Transport** - TCP/UDP, ensuring delivery.
- **Session / Presentation / Application** - Connections, formatting, user interaction.

🔒 ***Cybersecurity Insight***: Knowing the OSI layers helps identify where attacks happen, like packet sniffing at the network layer or man-in-the-middle attacks at the transport layer.

---

## 🌍 2. IP Addressing & Subnetting

- **IPv4 vs IPv6** - IPv6 expands the limited IPv4 address space.
- **Subnetting** - Splitting networks for efficiency and security.
- **Public vs Private IPs** - Internet-facing vs internal addresses.

🔒 ***Cybersecurity Insight***: Subnetting isolates sensitive systems, reducing the impact of intrusions.

---

## 📡 3. DNS & DHCP

- **DNS** - Converts names into IPs. Vulnerable to **DNS poisoning**.
- **DHCP** - Assigns IPs automatically. Vulnerable to **rogue DHCP attacks**.

🔒 ***Cybersecurity Insight***: Monitoring DNS logs can reveal malicious redirects or malware callbacks.

---

## 🔀 4. Routing, NAT & Firewalls

- **Routers** - Direct traffic between networks.
- **NAT** - Masks private IPs for security.
- **Firewalls** - Gatekeepers that filter allowed traffic.

🔒 ***Cybersecurity Insight***: Misconfigured firewalls often create open doors for attackers.

---

## 📦 5. TCP & UDP Protocols

- **TCP** - Reliable, used for web traffic and email.
- **UDP** - Faster, used for DNS and streaming.

🔒 ***Cybersecurity Insight***: Attackers exploit **UDP floods** in DDoS attacks or hijack TCP sessions.

---

## 🔐 6. VPNs & Secure Connections

VPNs encrypt communications, protecting users from eavesdropping.

🔒 ***Cybersecurity Insight***: VPN misconfigurations can create vulnerabilities just as dangerous as unencrypted traffic.

---

## 👀 7. Monitoring & Intrusion Detection

- **IDS/IPS** - Detect and sometimes block malicious traffic.
- **SIEM tools** - Correlate logs and alerts across the network.

🔒 ***Cybersecurity Insight***: Spotting unusual outbound traffic can reveal compromised machines communicating with attackers.

---

## 💡 Why Networking Matters in Cybersecurity

Cybersecurity isn’t only about tools, it’s about **understanding how data flows**. Networking knowledge helps professionals:

✔ Identify abnormal traffic patterns.

✔ Configure firewalls to stop intrusions.

✔ Secure DNS, DHCP, and IP addressing.

✔ Investigate attacks with packet analysis.

---

## Final Thoughts

Networking and cybersecurity are inseparable. By mastering fundamentals like **IP addressing, routing, firewalls, and monitoring**, professionals gain the ability to see both the strengths and vulnerabilities in any system.

For me, developing these skills has been a cornerstone of my cybersecurity journey, turning theory into practical security defense.