Module 3: Attacking the Foundation – IPv4 & IPv6

ENDPOINT SECURITY | CISCO NETWORKING ACADEMY

PREPARED BY: KUDZAISHE MAJEZA

Agenda

- Introduction to IPv4 and IPv6
- IPv4 Overview
- IPv4 Packet Header
- IPv4 Security Weaknesses
- IPv4 Real-Life Scenario
- IPv6 Overview
- IPv6 Packet Header
- IPv6 Security Strengths & Weaknesses
- IPv6 Real-Life Scenario
- IPv4 vs IPv6 Comparison
- IPv4 vs IPv6 in Attacks
- Summary & Key Takeaways

Introduction

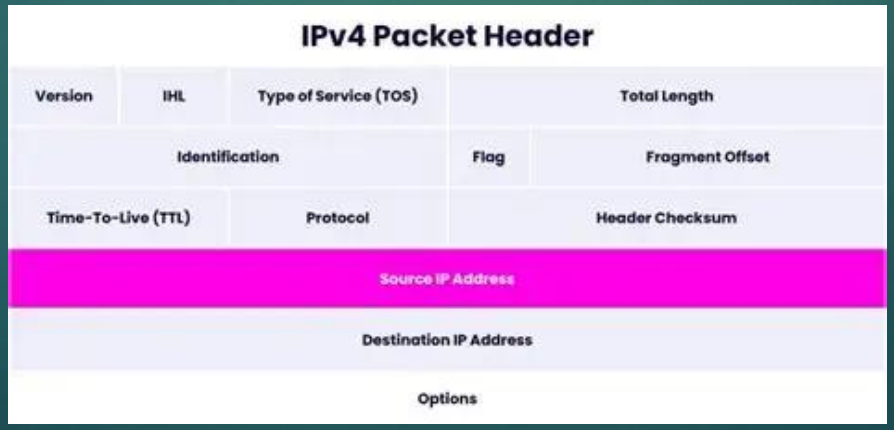
- IPv4 and IPv6 are the core protocols that move data across networks.
- Attackers often target weaknesses at this foundational layer.
- Understanding how packets work helps defend against attacks.

IPv4 Overview

- Uses 32-bit addresses (example: 192.168.1.1).
- Limited to about 4.3 billion addresses.
- Still widely used on most networks today.
- Relies heavily on NAT to conserve addresses.

IPv4 Packet Header (How an IPv4 Packet Looks)

- Version – identifies IPv4.
- Source IP Address – sender of the packet.
- Destination IP Address – receiver of the packet.
- TTL (Time to Live) – prevents infinite looping.
- Protocol – identifies TCP, UDP, or ICMP.
- Header Checksum – checks for errors.



IPv4 Security Weaknesses

- No built-in authentication.
- Susceptible to IP spoofing.
- Broadcast traffic increases attack surface.
- NAT can hide malicious activity.

Real-Life IPv4 Incident: Dyn DNS DDoS Attack (2016)

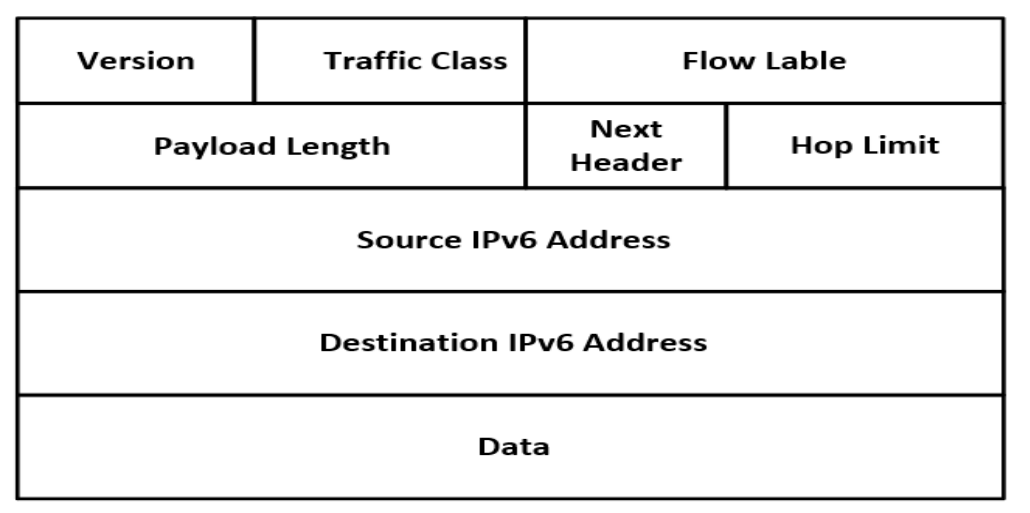
- A well-known real-world IPv4 attack happened in 2016 and targeted a company called **Dyn**, which provided **Domain Name System (DNS)** services. The Domain Name System is like the internet's phonebook it translates website names, such as *twitter.com*, into IPv4 addresses that computers can understand.
- In this attack, cybercriminals launched a **Distributed Denial of Service (DDoS)** attack using IPv4. A Distributed Denial of Service attack works by overwhelming a system with massive amounts of traffic so that legitimate users can no longer access it.
- The attackers used thousands of compromised **Internet of Things (IoT)** devices, such as cameras and routers, that were infected with malware. These devices sent huge volumes of traffic to Dyn's servers. Because IPv4 does not have built-in authentication, attackers were able to use **IP spoofing**, which means they forged fake source IPv4 addresses to hide where the traffic was really coming from.
- As a result, Dyn's DNS infrastructure became overloaded and stopped responding. This caused major websites like Twitter, Netflix, GitHub, and Reddit to go offline for hours across large parts of the world. This incident clearly shows how weaknesses in IPv4 especially spoofing and lack of authentication can be exploited to disrupt large parts of the internet.

IPv6 Overview

- Uses 128-bit addresses (example: 2001:db8::1).
- Provides nearly unlimited address space.
- Eliminates need for NAT.
- Designed with security improvements.

IPv6 Packet Header (How an IPv6 Packet Looks)

- Version – identifies IPv6.
- Source IPv6 Address.
- Destination IPv6 Address.
- Next Header – identifies protocol type.
- Hop Limit – prevents looping.
- Simplified header for faster routing.



IPv6 Security Strengths & Weaknesses

- Built-in support for IPsec.
- No broadcast traffic.
- Larger address space reduces scanning attacks.
- Misconfiguration introduces vulnerabilities.

Real-Life IPv6 Incident: Rogue Router Advertisement Attacks

- A real-life IPv6 incident commonly seen in enterprise networks involves Rogue Router Advertisement (RA) attacks.
- Between 2020 and 2022, several organizations reported incidents where attackers exploited IPv6 being enabled by default on operating systems like Windows and Linux, even when companies were not actively using IPv6.
- In these attacks, the attacker connected to the internal network and sent fake IPv6 Router Advertisement messages. These messages told devices on the network that the attacker's system was the "best router."
- Because IPv6 devices often automatically trust router advertisements, computers began sending all their traffic through the attacker's machine.
- This allowed the attacker to:

- Intercept traffic (Man-in-the-Middle attack)

- Redirect users to fake websites

- Monitor sensitive data

- The attack worked without breaking encryption or passwords, purely by abusing how IPv6 is designed to automatically configure itself.

IPv4 vs IPv6 Comparison

Feature	IPv4	IPv6
Address size	32-bit	128-bit
NAT	Required	Not needed
Security	Optional (Ipsec)	Built-in
Broadcast	Yes	No (uses multicast)
Address Space	Limited	Virtually infinitive

IPv4 vs IPv6 in Attacks

- IPv4 attacks rely on spoofing and broadcast abuse.
- IPv6 attacks target misconfigurations.
- Dual-stack environments increase risk.
- Both require strong security controls.

Summary & Key Takeaways

- IPv4 and IPv6 are foundational to networking.
- Attackers exploit weaknesses at this layer.
- Understanding headers improves security awareness.
- Correct configuration is essential.