Deconstructing the Network: A Penetration Tester's Blueprint

Module 02: Core Networking Principles

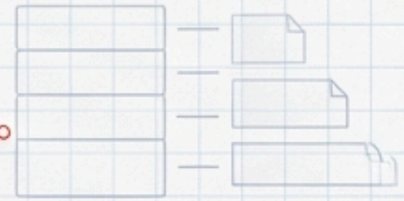
Penetration Testing Student v4

To Exploit a System, You Must First Understand Its Design

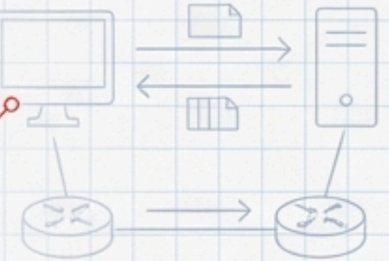
In computer network communications, every action is governed by a set of rules, or protocols.

As a penetration tester, your job is to find the flaws in that system. But you can't find the weaknesses until you know the blueprint.

This session deconstructs the architecture of modern networking. We will examine the foundational rules, the addressing schemes, and the pathways that data travels. By the end, you will understand how things work, which is the first and most critical step to exploiting them.



Deconstruct modern network protocols.



Analyze how computers communicate.

Master the principles behind sniffing and capturing network traffic.

The Packet is the Fundamental Unit of Communication

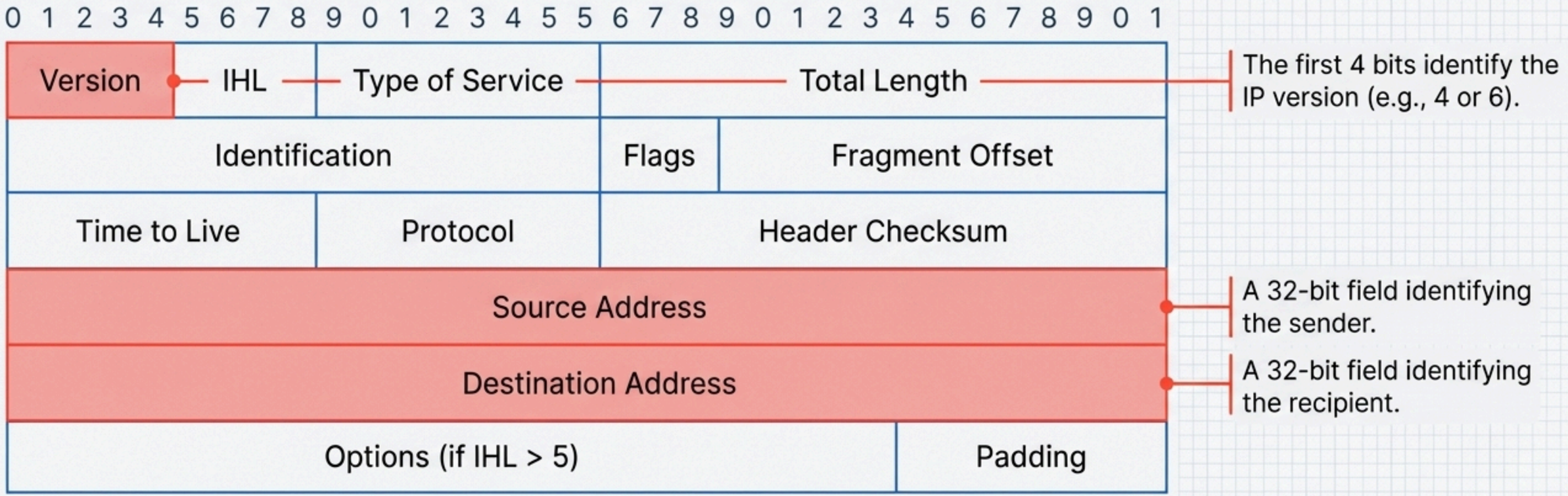
The primary goal of networking is to exchange information. This information is carried by packets—streams of bits running as electric signals over physical media like wires or airwaves.

Contains protocol-specific structural information. This ensures the receiving information. This ensures the receiving host can correctly interpret the message.

The actual information being sent, The actual information being sent, like part of an email or file content.

Anatomy of a Blueprint: The IPv4 Header

The IP protocol header is a minimum of 20 bytes long and contains critical information for routing and interpretation. Understanding these fields is essential for analyzing and manipulating traffic.



Layers Organize the Blueprint for Communication

PROBLEM

Networking involves many distinct challenges: making applications work, transporting data between processes, identifying hosts, and using physical media. How are these problems managed without chaos?

SOLUTION

Through layering. Protocols are organized into a stack, where each layer provides a service to the one above it and doesn't need to know the details of the layers below it.

Application Layer

Makes applications (browsers, email clients) work.

Transport Layer

Transports data between processes (server/client programs).

Network Layer

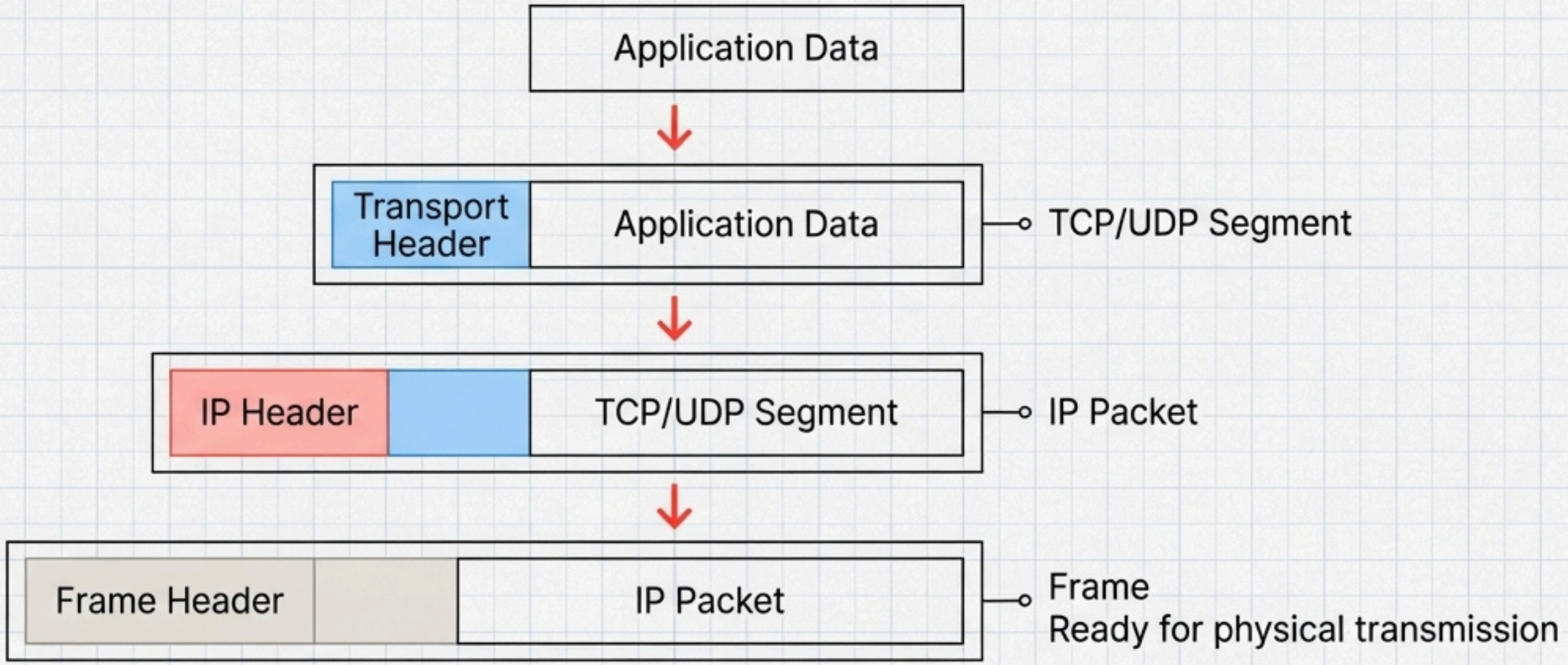
Identifies and locates hosts (IP Addressing).

Data Link Layer

Uses physical media to send packets between adjacent nodes.

The ‘Russian Doll’ Principle: How Layers Work Together

How does a protocol use the one on the layer below it? The answer is **encapsulation**. The entire upper-layer packet (header and payload) becomes the payload of the lower-layer protocol.



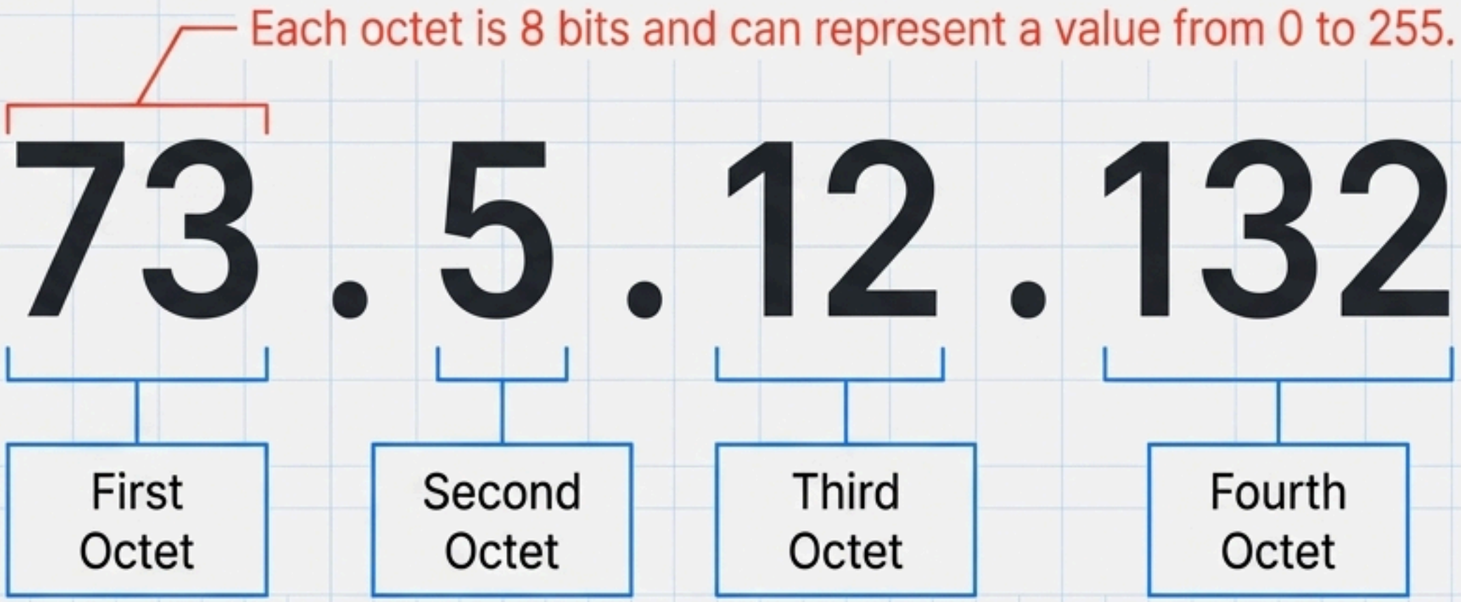
The receiving host performs this operation in reverse. This is how complexity is managed.

The Global Address: Finding Any Host on the Internet

Problem: How do you find one specific computer among billions connected to the internet?
Solution: The Internet Protocol (IP) Address.

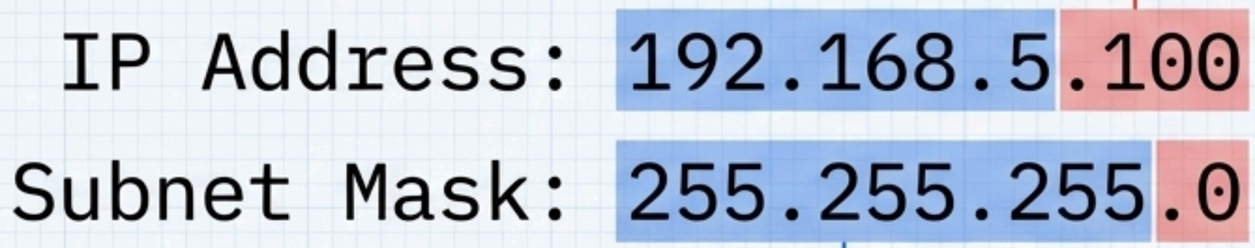
Any host on a computer network is identified by a unique IP address. The vast majority of networks still run on IP version 4 (IPv4).

An IPv4 address consists of four bytes, or octets (32 bits total), represented in “dotted-decimal” notation.



Defining the Neighborhood: IP Addresses and Subnet Masks

An IP address alone isn't enough. You also need a **subnet mask** to distinguish the two parts of the address.



Host Part: "The House Number". This uniquely identifies a specific house on the street.

Network Part: "The Street Name". All hosts on this street share this part of the address.

The subnet mask (e.g., 255.255.255.0) tells you which part is the network and which is the host.

A bitwise AND operation between the IP address and the subnet mask reveals the network address (the "street name").

The Local Address: Finding the Next Hop

Problem: An IP address can get a packet to the correct destination network (e.g., your office LAN), but how does it find the specific printer or server on that local network?
Solution: The Media Access Control (MAC) Address.

A MAC address, or physical address, uniquely identifies a network card at Layer 2.

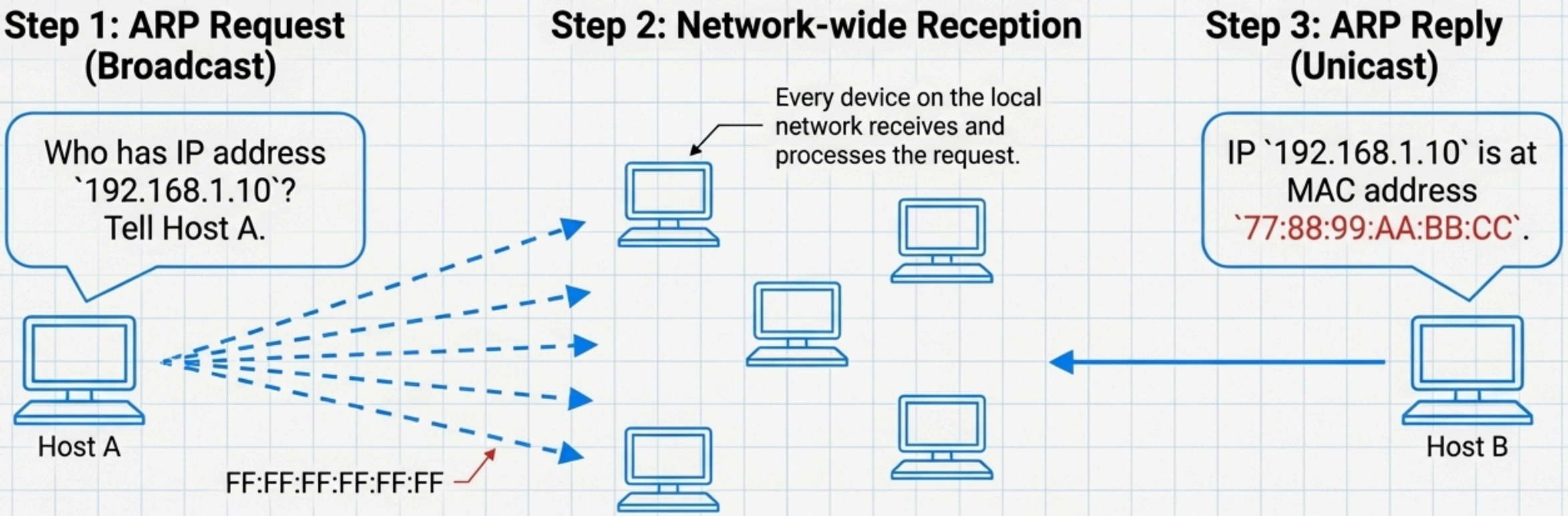
They are 48 bits (6 bytes) long and are expressed in hexadecimal form.

00:11:AA:22:EE:FF

Key Distinction: While an IP address is logical and can change, a MAC address is burned into the hardware and is (typically) permanent.

The Network's Directory: Bridging IP and MAC with ARP

Problem: A host wants to send a packet to `192.168.1.10`, but it only knows the IP. To create the Layer 2 frame, it needs the destination's MAC address. How does it find it?
Solution: The Address Resolution Protocol (ARP).



Pentester's Insight: Weaponizing the Link Layer

Understanding the mechanics of ARP and MAC addressing is not academic. It is the foundation for some of the most common and effective network attacks.

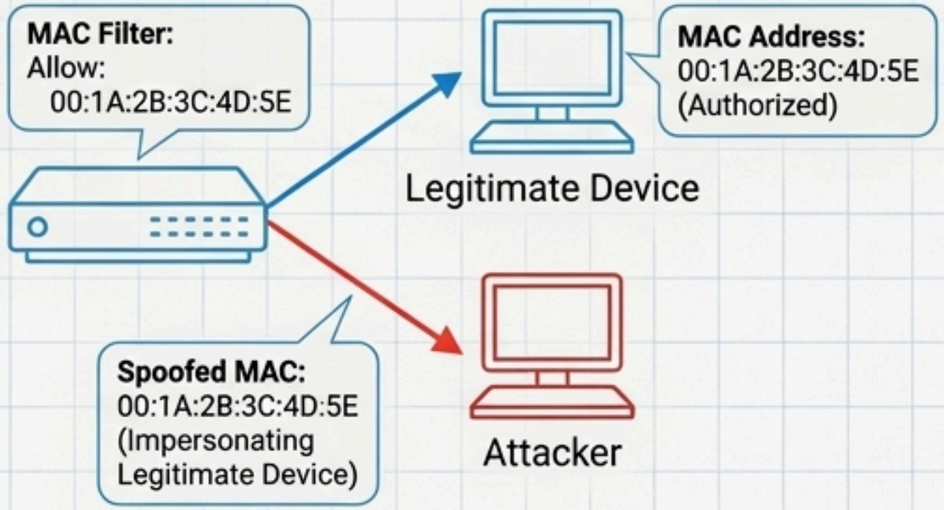
Attack Vector 1: ARP Spoofing (Poisoning)

Because ARP is a trusting protocol, an attacker can send unsolicited ARP replies. They can tell the gateway that the attacker's MAC address belongs to the victim's IP, and tell the victim that the attacker's MAC belongs to the gateway's IP.

Result: The attacker sits in the middle of the communication, able to read, modify, or block all traffic. This is a classic Man-in-the-Middle (MitM) attack.

Attack Vector 2: MAC Spoofing

An attacker can change their network card's MAC address to impersonate another device. This can be used to bypass MAC address filtering on a network or to hijack a session.



Crossing Boundaries: How Packets Navigate Between Networks

When the destination IP address is on a different network, a host sends its packet to a designated **router** (or **default gateway**). The router's job is to forward the packet to the next network on the path to the final destination.

How does a router decide where to send a packet? It consults its **routing table**. This table is a set of rules that maps destination networks to a specific outgoing interface.

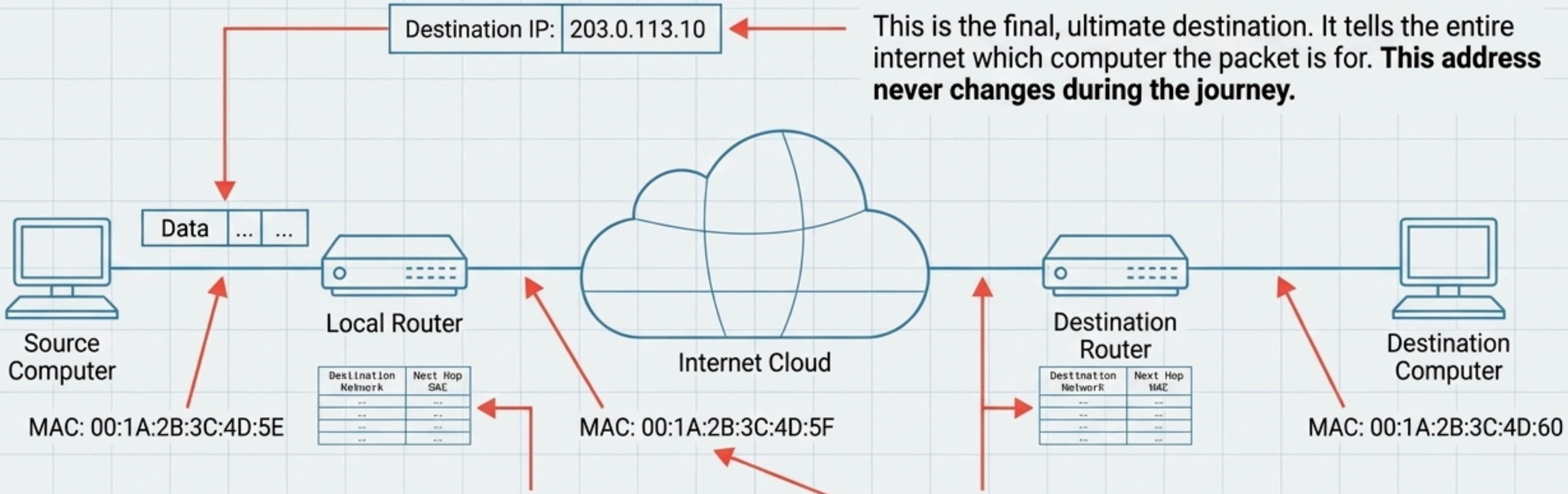
Destination Network	Netmask	Interface
228.72.0.0	255.255.0.0	1
192.168.5.0	255.255.255.0	2
0.0.0.0 (default)	0.0.0.0	3

Default Route: If no specific network matches, the packet is sent to the default route, which typically points towards the broader internet.

A Tale of Three Addresses: The Complete Journey

1. The Destination IP Address: The Home Address

This is the final, ultimate destination. It tells the entire internet which computer the packet is for. **This address never changes during the journey.**



2. The Destination MAC Address: The Next Local Hop

This is the address of the very next device in the chain (either the destination host itself or the next router). **This address changes at every hop.** Think of it as passing the letter from one postal worker to the next.

3. The Routing Table: The Map

This is the 'GPS' used by each router. It looks at the Destination IP Address (the 'Home Address') and uses its map to decide which MAC Address (the 'Next Local Hop') to send the packet to.

The Future of the Blueprint: IPv6

Problem: IPv4's 32-bit address space (~4.3 billion addresses) is nearly exhausted due to the explosion of internet-connected devices.

Solution: IPv6 uses a 128-bit address, providing 2^{128} possible addresses—an almost incomprehensibly large number.

Key Structural Differences:

- **Notation**: Consists of eight 16-bit hexadecimal blocks separated by colons (e.g., 2001:0db8:0020:130F:0000:0000:087C:140B).
- **Compression**: Zeros can be compressed for brevity (e.g., 2001:db8:20:130F::87C:140B).
- **Built-in Subnetting**: The address structure has a dedicated 16-bit space for subnets, simplifying network management.

IPv4 (32-bit)

73.5.12.132

IPv6 (128-bit)

2001:0db8:0020:130F::087C:140B

IPv6 Address Structure

You Now Have the Blueprint. Go Find the Flaws.

You've deconstructed the architecture of network communication.

You understand the rules (Protocols & Layers), the global and local addresses (IP & MAC), and the mechanisms that connect them (ARP & & Routing).

Every protocol, every header, and every address exists to solve a specific problem. They were designed by humans, and no design is perfect. Your task, as a penetration tester, is to find the assumptions, the oversights, and the weaknesses in that design.

The blueprint is in your hands.