Report

Title of the Report: Core Network Terms
Name: Dinesh Babu R S
Registration No: 2460360
Subject: Ethical Hacking (Cyber Security)
Department: Computer Science and Engineering
Email: dinesh.babu@btech.christuniversity.in
Date: August 13, 2025

INDEX

Core Network Terms

NAT (Network Address Translation)

In simple terms: NAT lets lots of devices in your home share one public IP address.

Why you should care: It helps protect your devices and saves valuable internet address space.

Imagine your router as a receptionist at a busy office, directing calls to the right desk:

[Internet]
  |
Public IP: 123.45.67.89
  |
Router → Laptop (.10), Phone (.11), Smart TV (.12)

NAT keeps outsiders from directly seeing your devices and reduces direct exposure to the internet.

ARP (Address Resolution Protocol)

In simple terms: ARP is how your computer finds the “house number” (MAC address) for a given IP.

Why you should care: Without ARP, your devices wouldn’t know exactly where to send data locally.

"Who has 192.168.1.20?" → Device replies: "Me! My MAC is XX:XX:XX."

It’s like asking around the neighborhood for someone’s exact address.

MAC Address

In simple terms: A MAC address is a unique ID for your device’s network adapter.

Why you should care: It helps your network recognize devices, like a name badge at a conference.

MAC: AA:BB:CC:DD:EE:FF
Manufacturer: Apple Inc.
Device ID: Unique to your gadget

IPv4 - Internet Addressing

In simple terms: IPv4 is the old but still common way of giving addresses to devices online.

Why you should care: We're running out — there are only 4.3 billion IPv4 addresses.

192.168.1.10 → Network, Subnet, Host, Device

IPv6 - The Future of Internet Addressing

In simple terms: IPv6 gives us an almost unlimited number of addresses.

Why you should care: More devices, better performance, and no NAT needed.

IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
IPv4 vs IPv6: 4.3 billion vs 340 undecillion addresses

How They Work Together

When you visit a website:

1. You type the URL.
2. DNS finds the site's IP.
3. ARP finds the MAC address of your gateway.
4. NAT translates your request into a public one.
5. Data returns and is sent to your device.

Common Network Attacks

- **MAC Spoofing:** Pretending to be a trusted device.
- **ARP Poisoning:** Sending fake ARP messages.
- **IP Scanning:** Looking for vulnerable devices.
- **NAT Exploits:** Confusing IP translations.

Quick Recap

- **MAC:** The device's unique ID.
- **ARP:** Finds MAC from IP.
- **IPv4:** Old system, almost full.
- **IPv6:** Future-ready, limitless.
- **NAT:** Shares one public IP.