Week 2

Key Points

- IP addressing uses IPv4 (32-bit, limited) and IPv6 (128-bit, vast) for device identification.
- Subnetting divides networks into smaller parts, using natural masks, subnet masks, and CIDR for IPv4, and prefix lengths for IPv6.
- MAC addressing provides unique hardware identifiers, essential for local network communication.
- ARP maps IP to MAC addresses, while RARP maps MAC to IP, both crucial for network operations.

IP Addressing Overview

- IP addressing is like a postal system for the internet, giving each device a unique address. IPv4, with its 32-bit format (e.g., 192.168.1.1), has about 4.3 billion addresses, but we're running out due to more devices. IPv6, with 128 bits (e.g., 2001:db8::1), offers trillions of addresses, ensuring future growth. Research suggests IPv6 is becoming essential as IPv4 depletes, though adoption varies by region.

Subnetting Explained

- Subnetting is dividing a network into smaller, manageable pieces, like splitting a city into neighborhoods. For IPv4, you use natural masks (e.g., 255.255.255.0 for /24), subnet masks (e.g., 255.255.255.192 for /26), and CIDR notation (/24 means first 24 bits for network). IPv6 uses prefix lengths like /64, simpler due to its vast address space. It seems likely that subnetting enhances network efficiency and security, though complexity can vary by setup.

MAC Addressing Basics

- MAC addresses are like fingerprints for network hardware, 48-bit identifiers (e.g., 00:1A:2B:3C:4D:5E) assigned by manufacturers. They ensure data reaches the right device on a local network, operating at Layer 2. The evidence leans toward MAC addresses being vital for local communication, though privacy concerns arise with tracking.

ARP and RARP Functionality

- ARP helps devices find a MAC address for a known IP, like asking, "Who has this IP? Tell me your MAC." RARP does the reverse, finding an IP for a known MAC, though it's less common today, replaced by DHCP. Both are crucial for network operations, with ARP widely used and RARP more historical.

IP Addressing: A Detailed Look

IP addressing is the foundation of network communication, assigning unique identifiers to devices. There are two primary versions: IPv4 and IPv6, each with distinct characteristics.

- **IPv4 Details:** IPv4 uses a 32-bit address space, represented in dotted decimal notation (e.g., 192.168.1.1). This format provides approximately 4.3 billion unique addresses, which, as noted in Understanding IP Addressing and Subnetting, is insufficient given the exponential growth of internet-connected devices. The address is divided into network and host portions, with subnetting used to manage scarcity.
- **IPv6 Details:** IPv6, developed to address IPv4 limitations, uses a 128-bit address space, written in hexadecimal with colons (e.g.,

2001:0db8:85a3:0000:0000:8a2e:0370:7334). As highlighted in IPv6 Addressing & IPv6 Subnetting Explained ► Cheat Sheet, it offers 2^128 addresses, far exceeding current needs. IPv6 includes features like multicast and anycast, enhancing network efficiency.

- **Differences:** The table below summarizes key differences, based on research from Introduction to IP addressing and subnetting | TechTarget:

"Aspect"	**"IPv4"**	**"IPv6"**
"Address Space"	"32 bits; ~4.3 billion addresses"	"128 bits; 2^128 addresses"
"Notation"	"Dotted decimal (e.g. 192.168.1.1)"	"Hexadecimal; colons (e.g. 2001:db8::1)"
"Address Conservation"	"Requires NAT; subnetting"	"No conservation needed"
"Special Addresses"	"Limited; relies on broadcast"	"Includes multicast; anycast"

This comparison underscores IPv6's role as a future-proof solution, though IPv4 remains dominant in many networks due to legacy systems.

Subnetting: Dividing Networks for Efficiency

Subnetting is the process of dividing a large network into smaller sub-networks, improving performance and security. It varies significantly between IPv4 and IPv6 due to address space differences.

- **IPv4 Subnetting:** In IPv4, subnetting involves borrowing bits from the host portion to create subnets, using natural masks, subnet masks, and CIDR notation. For instance, a /24 network (e.g., 192.168.1.0/24) can be subnetted to /26 by borrowing 2 bits, creating 4 subnets with 62 usable hosts each (total 64 - 2 for network and broadcast). Research from IPv4 Subnetting Explained details Class A, B, and C subnetting, with examples like Class A

(/8) allowing up to 16,777,214 hosts per network, reduced by subnetting.

- **IPv6 Subnetting:** IPv6 subnetting uses prefix lengths, typically /64 for end-user networks, as recommended in IPv6 Subnetting | pfSense Documentation. A /48 prefix can contain 65,536 /64 subnets, each with 2^64 addresses. The table below, derived from IPv6 Subnetting, shows subnet sizes:

"PREFIX"	"SUBNET EXAMPLE"	"TOTAL IP ADDRESSES"	"# OF /64 NETS"
"48"	"xxxx:xxxx:xxxx::"	"2^80"	"65536"
"64"	"xxxx:xxxx:xxxx:xxxx::"	"2^64"	"1"
"32"	"xxxx:xxxx::"	"2^96"	"4294967296"

This vast address space means IPv6 subnetting focuses on organization, not conservation, unlike IPv4.

- **Creating Subnets and Counting Hosts:** For IPv4, calculate subnets as 2^n (n = borrowed bits), usable hosts as 2^(host bits) - 2. For IPv6, a /64 subnet has 2^64 - 2 usable hosts, though practically 2^64 is used. Examples include subnetting 192.168.1.0/24 into /26 for 4 subnets, or dividing 2001:db8:1234::/48 into /64 subnets.

MAC Addressing: Hardware Identification

MAC addressing provides unique identifiers for network interfaces, essential for local communication. Research from MAC address - Wikipedia details:

- **Basics:** A MAC address is a 48-bit (6-byte) address, written as six groups of two hexadecimal digits (e.g., 00:1A:2B:3C:4D:5E). It operates at Layer 2, used in technologies like Ethernet and Wi-Fi.
- **Structure:** The first 24 bits are the OUI, identifying the manufacturer, while the last 24 are device-specific. Types include unicast, multicast, and broadcast (FF:FF:FF:FF:FF:FF).
- **Usage:** MAC addresses ensure data is delivered to the correct device on a local network, crucial for switches to forward frames to specific ports.

ARP and RARP: Mapping Protocols

ARP and RARP facilitate address mapping, essential for network operations. Insights from Difference between ARP and RARP | GeeksforGeeks include:

- **ARP Functionality:** ARP maps a 32-bit IP address to a 48-bit MAC address, used when a device knows the destination IP but needs the MAC. It broadcasts a request, and the target responds, as seen in How Address Resolution Protocol (ARP) Works? | GeeksforGeeks.
- **RARP Functionality:** RARP maps a 48-bit MAC to a 32-bit IP, used by devices knowing their MAC but needing an IP, typically from a server. It's less common today, replaced by DHCP, as noted in ARP vs. RARP: What's the difference? | TechTarget.

"PROTOCOL"	"FUNCTIONALITY"	"ADDRESS	"USAGE CONTEXT"

		MAPPING "	
"ARP"	"Maps IP to MAC; fetches receiver's MAC address"	"32-bit IP to 48-bit MAC"	"Sender's side; local network communication "
"RARP"	"Maps MAC to IP; fetches IP through server"	"48-bit MAC to 32-bit IP"	"Receiver's side; IP address discovery"

Practical Implications and Examples

To make these concepts easier to grasp, let's look at some real-world examples. For IPv4, imagine you have a network like 192.168.1.0/24, and you split it into smaller chunks using a /26 mask. This gives you 4 smaller networks, each with 62 usable IP addresses for devices (after reserving 2 for the network and broadcast addresses). For IPv6, take a network like 2001:db8:1234::/48—you can divide it into 65,536 smaller /64 networks, each with a massive number of IP addresses for devices. With ARP, picture a device (say, with IP 192.168.1.10) shouting across the network, "Hey, who has this IP? I need your MAC address!" The target device responds with something like 00:1A:2B:3C:4D:5E, letting communication happen. RARP is less common now, but it’s like a device knowing its MAC address and asking a server, "What’s my IP?" Nowadays, DHCP handles this job more often. These examples show how these ideas work in real networks, making communication smooth and organized.