Understanding IPv4 and IPv6 Addressing

1. The Need for IP Addressing

1.1 The Analogy: Sending a Letter

- **The Message:** The data you want to send.
- **Source Address:** Your IP address. Without it, the recipient cannot reply.
- **Destination Address:** The recipient's IP address. Without it, network devices (routers) cannot deliver the message.
- **Conclusion:** An **IP Address** is a **Layer 3 logical address** essential for communication between networks.

Think of the IP header as an envelope. The data is the letter inside. The source IP is the "return address," and the destination IP is the "delivery address." If either is missing or incorrect, the postal service (the network) cannot function.

1.2 The Governing Bodies

- **IANA (Internet Assigned Numbers Authority):** The global coordinator for IP address allocation.
- **RIRs (Regional Internet Registries):** IANA delegates address distribution to five RIRs based on geography.
    - African Network Information Center (AFRINIC): Supports the continent of Africa
    - Asia-Pacific Network Information Centre (APNIC): Supports regions of Asia and the Pacific
    - American Registry for Internet Numbers (ARIN): Supports regions of Canada, the USA, and parts of the Caribbean
    - Latin America and Caribbean Network Information Centre (LACNIC): Supports Latin America and parts of the Caribbean regions
    - Réseaux IP Européens Network Coordination Centre (RIPE NCC): Supports Europe, the Middle East, and Central Asia

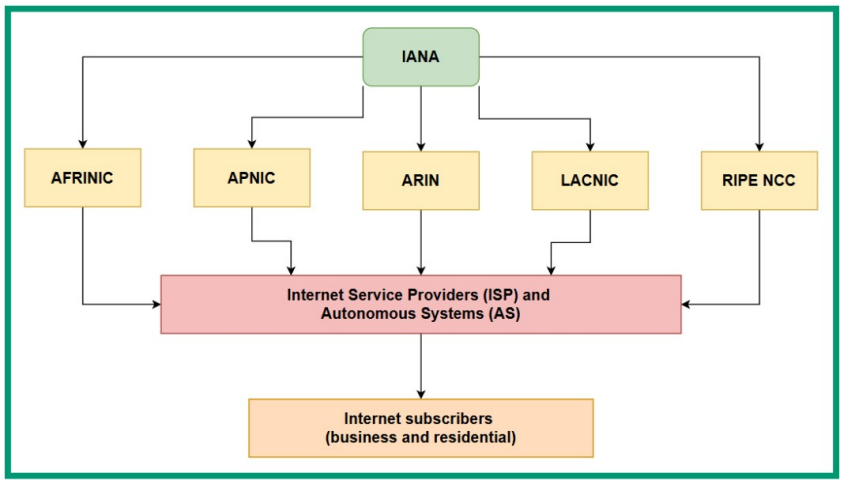

Figure 1: IP network blocks delegation

An Autonomous System (AS) is simply any organization that is responsible for managing a large number of internet routing networks such as an ISP within a country or region. IANA assigns AS numbers to the various RIRs around the world. Then, the RIRs allocate these AS numbers to network operators such as ISPs. The ISPs use their AS numbers to share their network routing prefixes with other ISPs using the Border Gateway Protocol (BGP).

This hierarchical system prevents chaos. It ensures that two different ISPs in different parts of the world don't assign the same public IP address to different customers, which would cause routing conflicts.

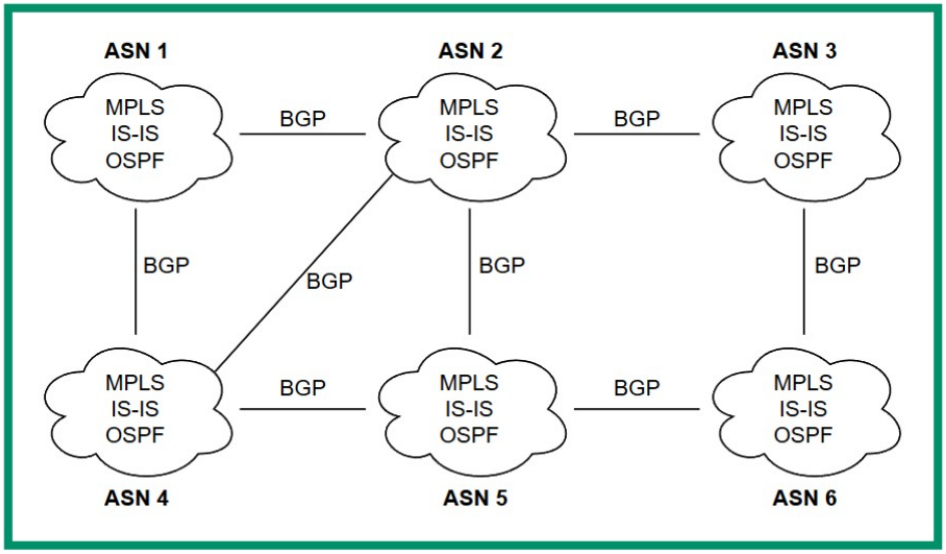

Figure 2: Interconnected ISPs sharing network routes

1.3 The Core Problem: Address Exhaustion

- **IPv4:** Deployed in 1983. It is a **32-bit** address, providing ~4.3 billion addresses.
- **IPv6:** Developed in 1999. It is a **128-bit** address, providing a virtually limitless number.

The explosion of internet-connected devices (computers, phones, IoT sensors) meant that 4.3 billion was not enough. IPv6 was created as a long-term solution.

2. Public vs. Private Address Spaces

To combat IPv4 exhaustion, IANA created two separate address spaces.

Class	Range	Default Subnet Mask
A	0.0.0.1 - 127.255.255.255	255.0.0.0
B	128.0.0.1 - 191.255.255.255	255.255.0.0
C	192.0.0.1 - 223.255.255.255	255.255.255.0
D	224.0.0.1 - 239.255.255.255	N/A
E	240.0.0.1 - 255.255.255.255	

Figure 3: IPv4 public address space

2.1 Public IP Address Space

- **Definition:** Addresses that are **routable on the internet**.
- **Must be unique** across the entire internet.
- Assigned to devices directly connected to the internet (e.g., web servers, your home router's external interface).

2.2 The Problem with Classful Addressing

- **Inflexible:** Organizations were forced to use the default subnet mask.
- **Massive Wastage:** A company with 2,000 devices needed a Class B block (65,534 addresses), wasting over 63,000 addresses.
- **Large Routing Tables:** Every classful network was a separate entry in a router's table, slowing down internet routing.

Class	Range	Default Subnet Mask	Number of Networks	Number of Usable IPv4 Addresses
A	0.0.0.1 - 127.255.255.255	255.0.0.0	126	16,777,214
B	128.0.0.1 - 191.255.255.255	255.255.0.0	16,384	65,534
C	192.0.0.1 - 223.255.255.255	255.255.255.0	2,097,152	254

Figure 4: Classful IPv4 addresses

2.3 Private IP Address Space (RFC 1918)

- **Definition:** Addresses that are **NOT routable on the internet**.
- **Can be reused** by any private network globally.
- **Purpose:** To conserve public IPv4 addresses.

Class	Range	Default Subnet Mask
A	10.0.0.1 - 10.255.255.255	255.0.0.0
B	172.16.0.1 - 172.31.255.255	255.255.0.0
C	192.168.0.1 - 192.168.255.255	255.255.255.0

Figure 5: Private IPv4 address space

Private IPs are like internal extension numbers in a large office building. The building has one public street address (public IP), but inside, every office has a unique extension (private IP). You can dial extension 101 (192.168.1.101) from inside, but someone outside the building cannot call 101 directly; they must call the main number (public IP) first.

A device with only a private IP cannot communicate directly with the internet. It needs a translator —**Network Address Translation (NAT)**.

3. Network Address Translation (NAT)

Network Address Translation (NAT) is an IP service that is commonly found on almost all private networks within organizations. NAT allows a private IPv4 source address to be translated into a public IPv4 address, allowing devices on a private network to communicate with devices on a public network.

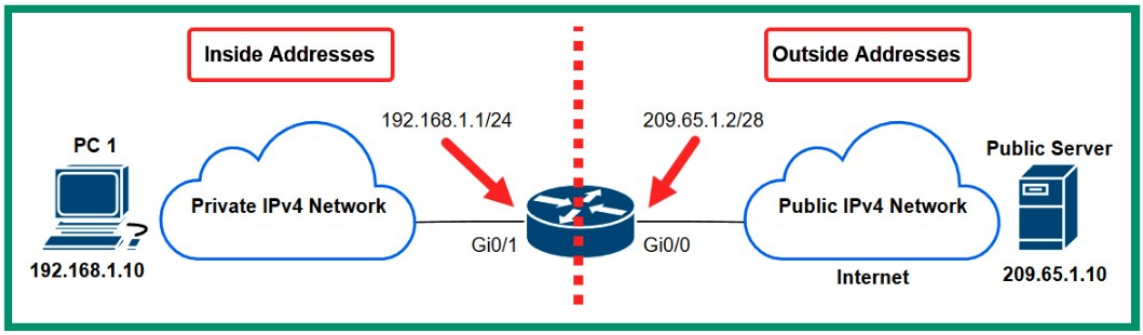

Figure 6: NAT operations

3.1 How NAT Works

1. A PC with a private IP (e.g., `192.168.1.10`) sends a packet to a web server on the internet.
2. The packet arrives at the NAT-enabled router.
3. The router **translates the source IP** from the private address (`192.168.1.10`) to its own public IP (e.g., `209.65.1.2`).
4. The web server replies to the public IP (`209.65.1.2`).
5. The router translates the destination address back to the private IP (`192.168.1.10`) and forwards the packet.

A. Advantages

- **Conserves the Public IPv4 Address Space:** The primary benefit of using NAT is to help conserve the public IPv4 address space by allowing organizations to use private IPv4 addresses on their internal networks and be assigned a single public IPv4 address on their modem/router.
- **Hides the Internal Network:** Using NAT allows an entire organization’s private network to be hidden behind a single public IPv4 address.
- **Maintains Internal Addressing Consistency:** Network professionals can maintain consistency in their private IPv4 addressing scheme within their companies.

B. Disadvantages

- **Impacts Network Performance:** As traffic is sent to the router or modem to be translated, there is some delay as the router or modem has to perform the actual translation process.
- **Incompatibility with IPsec VPNs:** Since NAT modifies the IPv4 addresses on the packet, Virtual Private Network (VPN) solutions that use IP security (IPsec) to establish a secure logical tunnel over an unsecure network does not work well.
- **Loss of End-to-End Connectivity:** NAT modifies the IPv4 addresses within the packet, so end-to-end connectivity is lost between a sender and receiver.

3.2 Types of NAT

A. Static NAT

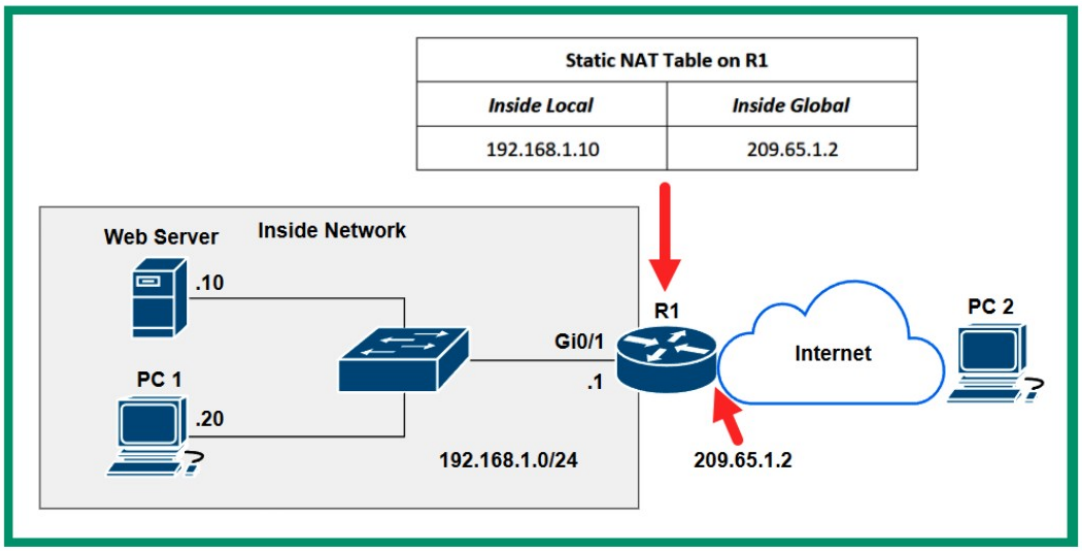

Figure 7: Static NAT

- **One-to-One** mapping. A single private IP is permanently mapped to a single public IP.
- **Use Case:** Hosting an internal server (e.g., a web or email server) that needs to be accessible from the internet.

  Like having a dedicated public phone line for the CEO's office. All calls to that public number go directly to one specific internal extension.

B. Dynamic NAT

- **Many-to-Many** mapping. A pool of public IPs is shared by many private IPs on a first-come, first-served basis.
- **Use Case:** Less common. Used when you have a limited number of public IPs and a larger number of internal devices that need occasional internet access.

  Like a company with 10 external phone lines for 50 salespeople. The first 10 salespeople to make a call get a line. The 11th must wait until a line is free.

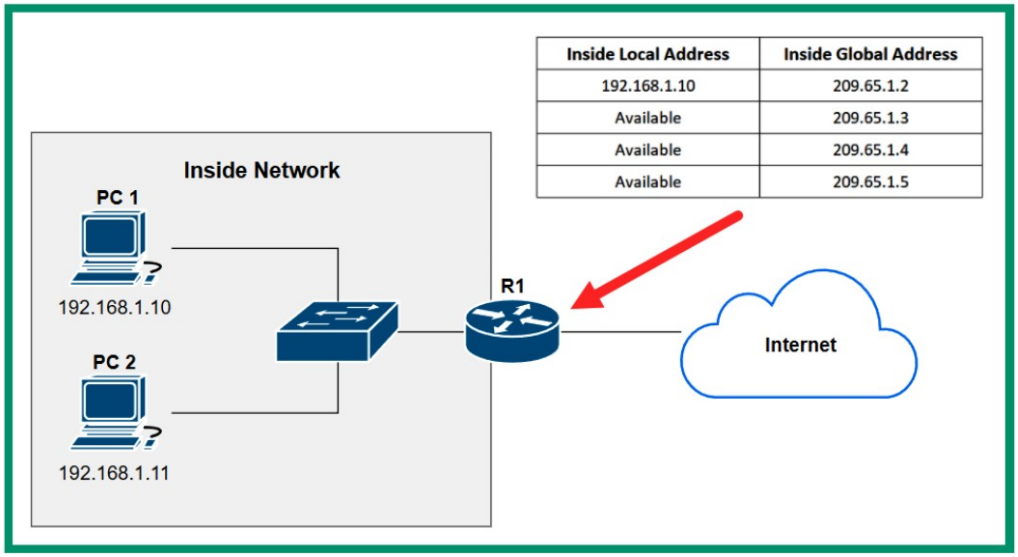

Figure 8: Dynamic NAT

C. Port Address Translation (PAT) / NAT Overload

- **Many-to-One** mapping. **This is the most common type**, used in every home router.
- It uses **source port numbers** to track thousands of internal connections using a single public IP.

  This is like the receptionist using a different "department code" for each employee's outgoing mail. All mail leaves with the same return address (`209.65.1.2`), but with a unique department code (e.g., `209.65.1.2:15001`, `209.65.1.2:15002`). When replies come back addressed to a specific department code, the receptionist knows exactly which employee to deliver it to.

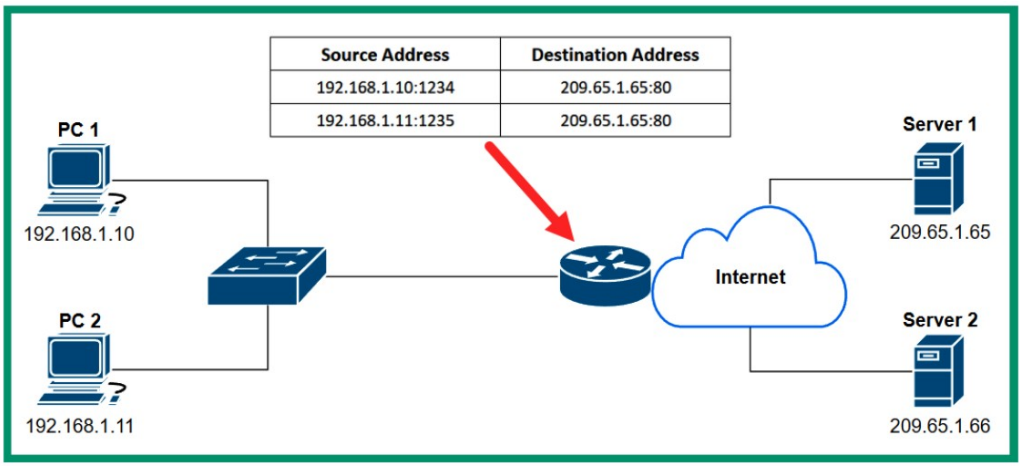

Figure 9: Port address translation

4: The Structure of IPv4 and IPv6

4.1 Fundamentals of IPv4: It's All About Binary

- **The Core Concept:** An IPv4 address is a 32-bit binary number. The dotted-decimal format (`192.168.1.1`) is just for human readability.
- **Conversion is Key:** To truly understand subnetting, you must be able to convert between decimal and binary.

Converting Binary to Decimal (The Power of Two Method):
Each octet is 8 bits. Each bit represents a power of 2, from 2^7 (128) on the left to 2^0 (1) on the right. You add the values for every bit that is a '1'.

Example: Convert `11000000` to Decimal

Radix	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary	1	1	0	0	0	0	0	0

Figure 10: Converting the first octet `11000000`

Converting Decimal into Binary:

The following are some guidelines to ensure the results are accurate:

- Always convert one octet at a time
- Always begin by subtracting the highest power of 2, which is 27 = 128, while working
- downwards to the lowest power of 2, which is 20 = 1
- If you can subtract the decimal number from the radix value, place a 1
- If you are unable to subtract the decimal number from the radix value, place a 0
- If you get a 0, then subtract the decimal number from the next lower radix value

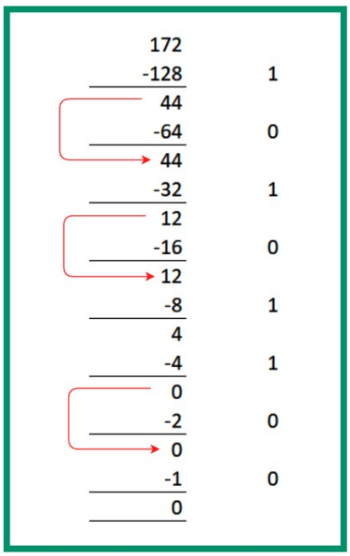

Figure 11: Converting 172 into binary

Example: Convert the IP address `192.168.1.1`

- `192` -> `128+64` -> `11000000`
- `168` -> `128+32+8` -> `10101000`
- `1` -> `1` -> `00000001`
- `1` -> `1` -> `00000001`
- **Full Binary:** `11000000.10101000.00000001.00000001`

4.2 Fundamentals of IPv6: A New Paradigm

- **Length:** 128 bits, written as eight 16-bit hexadecimal blocks.
- **Example Full Address:** `2001:0db8:85a3:0000:0000:8a2e:0370:7334`
- **Simplification Rules (Crucial for readability):**
    1. **Remove Leading Zeros:** In each block, you can remove leading zeros.
        - `0db8` -> `db8`
        - `0370` -> `370`
        - Result: `2001:db8:85a3:0000:0000:8a2e:370:7334`
    2. **Compress Successive Zero Blocks:** Replace the longest contiguous block of `0000` blocks with a double colon `::`. This can only be done once per address.
        - `2001:db8:85a3:0000:0000:8a2e:370:7334` -> `2001:db8:85a3::8a2e:370:7334`

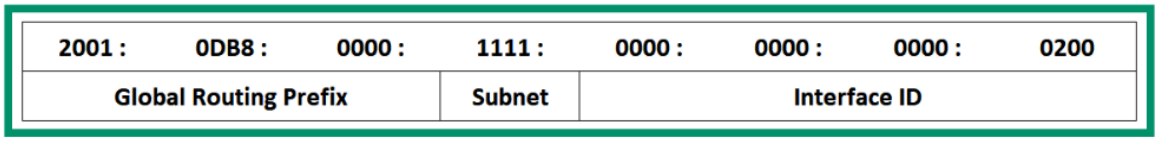

Figure 12: IPv6 address structure

As shown in the preceding snippet, the first three hextets represent the Global Routing Prefix portion, which contains the first 48 bits of the address. This portion of the IPv6 address is assigned by the service provider such as the ISP. The fourth hextet (16 bits) represents the Subnet ID, which is used by the ISP to create subnetworks of the network block. The last 64 bits represent the Interface ID portion. Combining the Global Routing Prefix, Subnet ID, and Interface ID, a client is assigned a unique 128-bit IPv6 address on its network interface card.

5. Types of IPv4 and IPv6 Addresses

5.1 Automatic Private IP Addressing (APIPA)

What is APIPA?

- A failover mechanism built into Microsoft Windows operating systems

- **Range:** `169.254.0.1` to `169.254.255.254` with subnet mask `255.255.0.0`
- Automatically activates when DHCP client cannot locate a DHCP server

How APIPA Works:

1. **DHCP Discovery Failure:** Device boots up and broadcasts DHCP Discover messages
2. **Timeout Period:** Device waits for DHCP Offer (typically 30-60 seconds)
3. **Self-Assignment:** If no DHCP server responds, the device automatically assigns itself an IP from the APIPA range
4. **Conflict Detection:** Device performs duplicate address detection (DAD) to ensure the selected IP isn't already in use on the local network

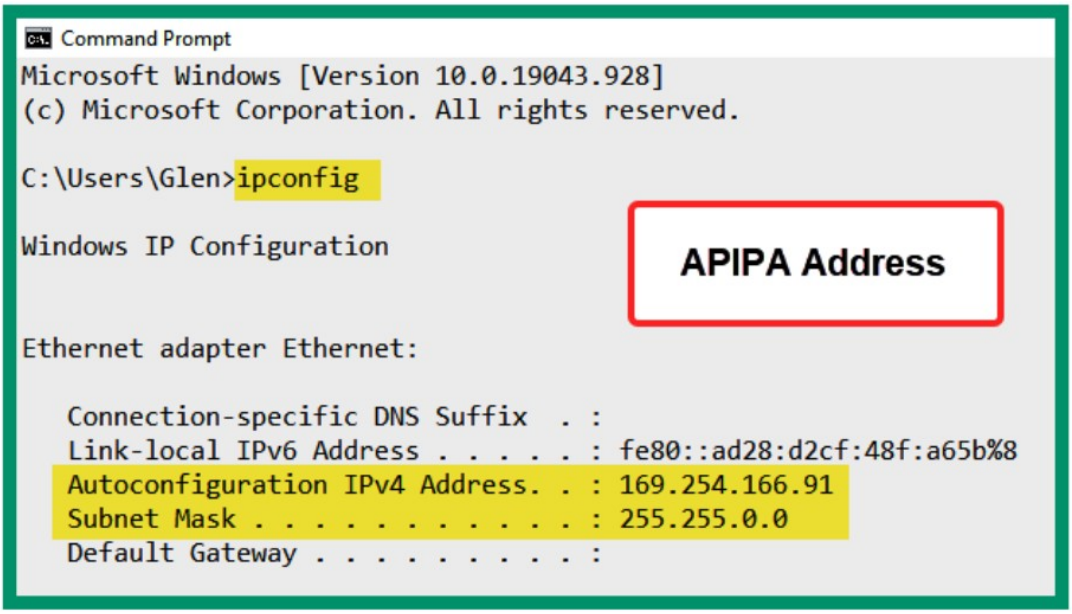

Figure 13: APIPA address on a client

5.2. EUI-64 (Extended Unique Identifier) Fundamentals

What is EUI-64?

Definition:

- A standard method defined by IEEE for creating 64-bit interface identifiers
- Converts 48-bit MAC addresses into 64-bit interface identifiers
- Primarily used in IPv6 Stateless Address Autoconfiguration (SLAAC)

Purpose in IPv6:

- Provides automatic generation of unique interface IDs
- Ensures global uniqueness when combined with IPv6 network prefix
- Enables devices to self-configure IPv6 addresses without DHCP

The following steps describe the EUI-64 process of converting a 48-bit MAC address of a network adapter to create a 64-bit address that will be used as the interface ID portion to create a unique

IPv6 address:

1. First, split the 48-bit MAC address into half, separating the Organizational Unique Identifier (OUI) and the device portions, as shown in the following diagram:

FC	99	47	75	CE	E0
11111100	10011001	01000111	01110101	11001110	11100000

Figure 14: EUI-64 process step 1

2. Next, insert the hexadecimal value, FFFE, in the middle of the 48-bit MAC address, as shown in the following diagram:

FC	99	47	**FF**	**FE**	75	CE	E0
11111100	10011001	01000111	**11111111**	**11111110**	01110101	11001110	11100000

Figure 15: EUI-64 process step 2

3. Next, flip the seventh bit within the first byte so that a 0 will become a 1 or a 1 will become a 0. This bit indicates if the NIC is administered locally (0) or is globally unique (1), as shown in the following diagram:

11111110	10011001	01000111	**11111111**	**11111110**	01110101	11001110	11100000

Figure 16: EUI-64 process step 3

4. Next, convert the binary into hexadecimal to view the EUI-64 portion of the address, as shown in the following diagram:

FE	99	47	**FF**	**FE**	75	CE	E0

Figure 17: EUI-64 process step 4

5. Lastly, putting it all together, the EUI-64 bit IPv6 address that will be assigned to the device's network adapter is 2001:DB8:0:1111:FE99:47FF:FE75:CEE0.

5.3. Unicast

- Unicast addresses can be IPv4 and IPv6 addresses that are uniquely assigned to the network adapter of a device.
- Using a unicast address allows one-to-one communication between a sender and receiver device over a network.
- As shown in the diagram, each device is assigned a unique IPv4 address on the network.
- Additionally, the IP address that's configured on each device is a unique unicast address, which allows any device to communicate with another device.

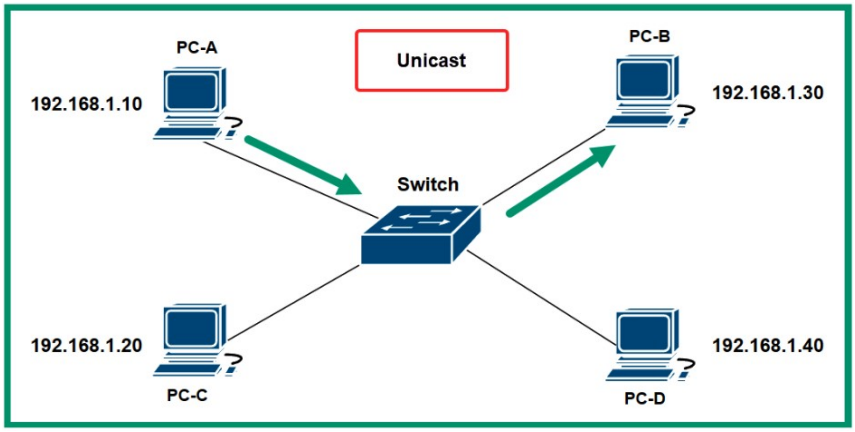

Figure 18: Unicast communication

5.4. Multicast

- Multicast addresses exist within both the IPv4 and IPv6 address spaces. Multicast allows one-to-many communication between devices on a network.
- Enterprise-grade routers within a large organization are usually configured with a dynamic routing protocol, which allows each router to automatically learn new networks and maintain an up-to-date routing table by exchanging routing information between themselves.
- These routers send and receive messages to a multicast address group, which is only used by devices running the same dynamic routing protocol.

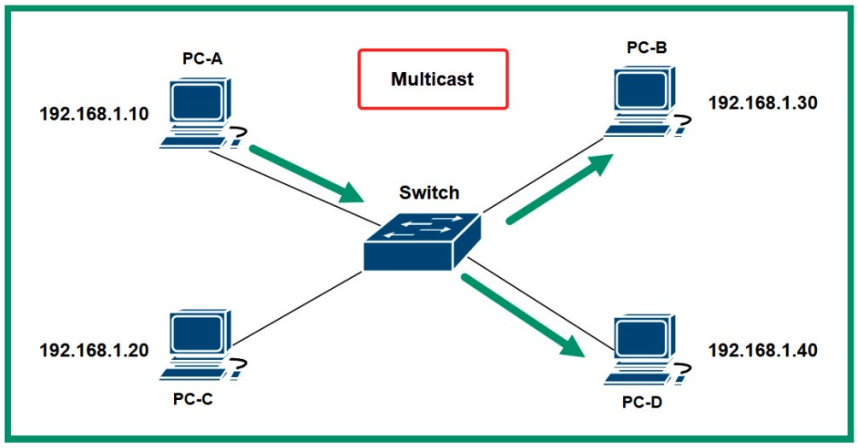

Figure 19: Multicast communication

5.5. Broadcast

- Broadcast allows one-to-all communication over an IPv4 network. Unlike IPv4 networks, IPv6 does not use broadcast addresses.
- Simply put, a computer that’s connected to a network can send a single message to the network’s broadcast address, which allows all devices within the same IP network to receive the message from the sender.
- Within a network that uses a Network ID of 192.168.1.0 and has a subnet mask of 255.255.255.0, the broadcast IP address will be 192.168.1.255.

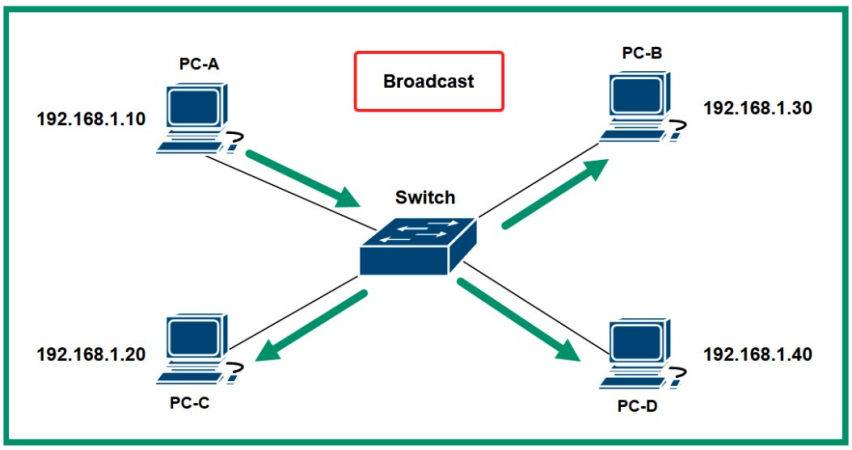

Figure 20: Broadcast communication

5.6. Anycast

- Anycast addresses exist on IPv6 networks and are used for one-to-nearest communication between devices over a network.
- Anycast allows the same unicast IPv6 address to be shared between multiple devices, such as servers on the internet.
- When a client such as a computer sends a message to an anycast IPv6 address, the message is delivered to the geographically nearest server that's configured with the anycast address.

5.7. Link-local

- On an IPv6 network, each device is assigned two IPv6 addresses on its network adapter. One of the addresses is the IPv6 unicast address, which is used by the device when communicating with other hosts outside its local network.
- If the computer on an internal network within an organization wants to communicate with a server on the internet, the IPv6 unicast address will be used for this type of communication.
- Additionally, an IPv6 Link-Local address is assigned to the same network adapter with the IPv6 unicast address.
- A **Link-Local address** is an **IP address automatically assigned to a device** for communication **within a single local network segment (link)** — when no external configuration (like DHCP or manual setup) is available.

5.8. Loopback

- A loopback address is a special IP address used by a device to test its own network stack — that is, to verify that TCP/IP is properly installed and functioning on the local host.
- It allows a computer to send and receive network traffic to itself, without using any physical network interface or external device.
- The IPv4 loopback address ranges from 127.0.0.1 to 127.255.255.254 and has a default subnet mask of 255.0.0.0 (/8). However, it's quite common for network professionals to identify 127.0.0.1 as the loopback address as it's the first IPv4 address within the range, and it's mostly used when testing the loopback connectivity on a device.

- In the IPv6 space, the loopback address is ::1/128, which allows network professionals to perform the same loopback testing on the TCP/IP network model on the local device.

5.9. Unique local address

- A unique Local address exists within the IPv6 addressing space and ranges from FC00::/7 to FDFF::/7.
- These unique local addresses have similarities to private IPv4 addresses on a network; they are unique to a private network within an organization and are non-routable on the internet.
- These unique local addresses are used for local addressing only and can be assigned to devices that do not need access to another network.

5.10. Default gateway

- **A default gateway is the network device (usually a router) that acts as an access point or exit for a host to communicate with devices outside its local network (subnet).**
- If a device tries to send packets to an IP address **not in its own network**, the packet is forwarded to the **default gateway**, which determines where it should go next.

Primary Function:

- Routes traffic from the local network to remote networks
- Acts as the forwarding point for all non-local destination traffic
- Essential for internet access and inter-network communication

Key Characteristics

Network Boundary Device:

- Resides on the same IP subnet as the local devices
- Has interfaces connected to multiple networks
- Makes routing decisions based on destination IP addresses

Mandatory for External Communication:

- Required for accessing resources outside the local subnet
- Without a default gateway, devices can only communicate locally
- Critical for internet connectivity

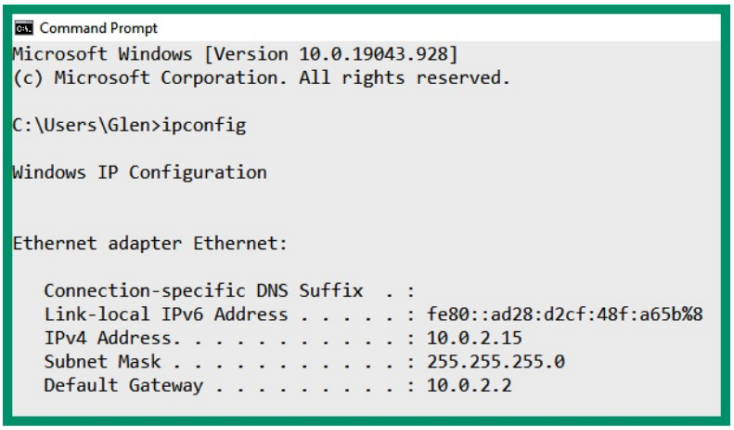

Figure 21: Default gateway address of a Windows 10 client

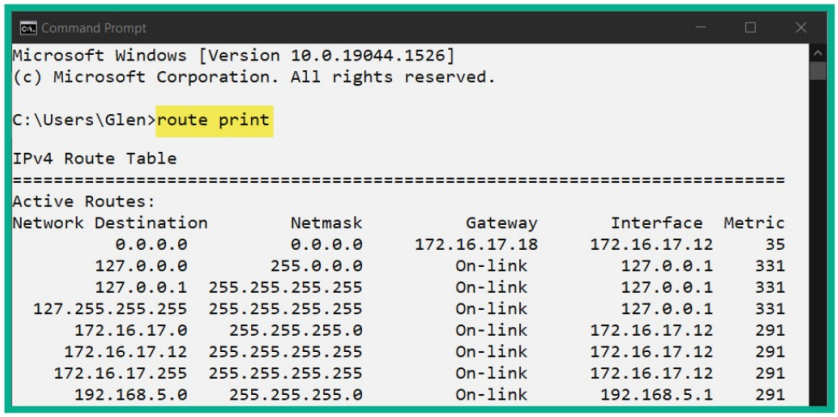

Figure 22: Routing table of a Windows device

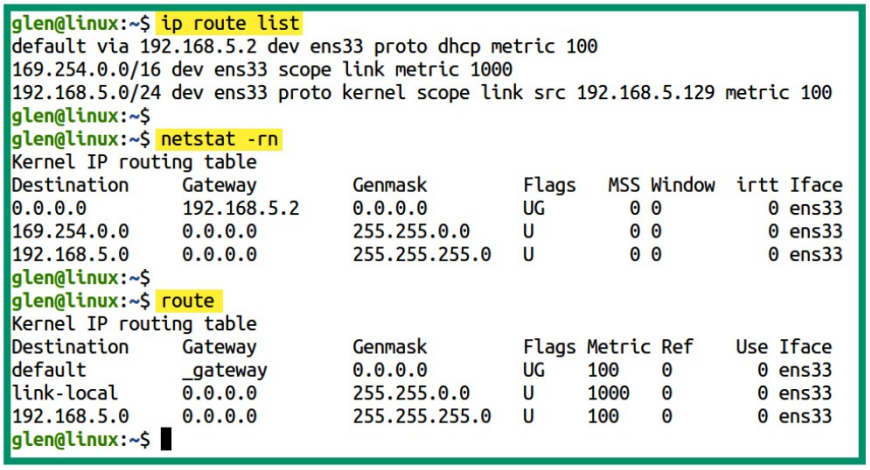

Figure 23: Routing table of a Linux-based device

6. Delving into IPv6 Concepts

- IPv4 and IPv6 addresses exist within different spaces and cannot natively communicate with each other.
- To help ensure devices that exist on both IPv4 and IPv6 networks can communicate with each other, various IPv6 technologies allow both versions of IP to coexist.

6.1. Tunneling

- IPv4 is still the dominant protocol across most of the internet.
- However, **IPv6 public networks** are increasingly being implemented worldwide.
- The transition phase between IPv4 and IPv6 creates **compatibility issues**, as both protocols **cannot communicate directly**.
- **Tunneling** provides a **bridge** between IPv4 and IPv6 networks.
- It works by **encapsulating packets** of one protocol version inside packets of another version, allowing them to traverse incompatible networks.
- When an **IPv6 packet** needs to travel across an **IPv4 network**, it is **encapsulated** inside an IPv4 packet.
- The **forwarding router** performs this encapsulation.

- When the encapsulated packet reaches the destination network, the IPv4 header is **removed (decapsulated)**, and the **original IPv6 packet** is delivered to its IPv6 destination.
- Tunneling enables **coexistence** of IPv4 and IPv6 during the transition phase.
- **6to4 tunneling** is the most common technique during IPv6 deployment.
- **4to6 tunneling** works in reverse, enabling IPv4 traffic to pass through IPv6 environments.

6.2. Dual stack

- As the world transitions from **IPv4** to **IPv6**, not all networks or devices have been upgraded to support the new protocol.
- To ensure smooth communication during this migration period, many systems operate in **dual-stack mode**, allowing both IPv4 and IPv6 to coexist on the same device or network.
- Dual stack is a transition mechanism that allows a device, such as a computer, router, or server, to run both IPv4 and IPv6 protocols simultaneously.
- Each device interface is configured with **both an IPv4 address and an IPv6 address**.
- The device maintains **two protocol stacks** — one for IPv4 and one for IPv6.

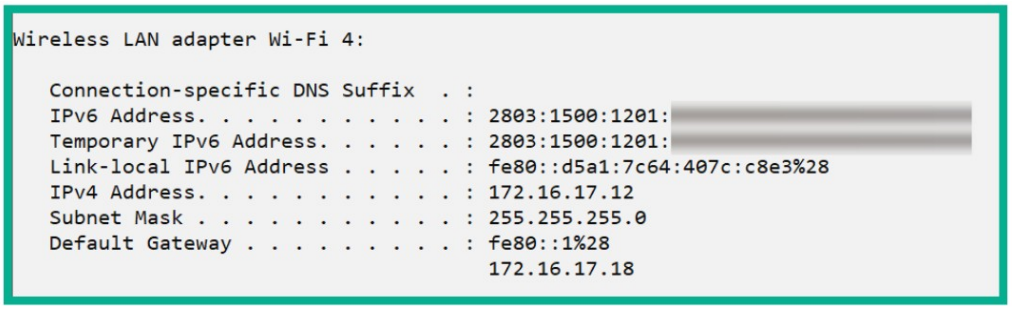

Figure 24: Dual stack NIC

6.3. Translation

- In IPv4 networks, Network Address Translation (NAT) is commonly used to convert private IPv4 addresses into public IPv4 addresses before packets are sent out to the internet.
- As networks transition to IPv6, a similar mechanism is needed to enable communication between IPv6 and IPv4 systems that cannot talk directly.
- **NAT64 (Network Address Translation 64)** is a **translation mechanism** that allows **IPv6-only devices** to communicate with **IPv4-only hosts**.
- It works by **translating IPv6 addresses into IPv4 addresses** — and vice versa — similar to how traditional NAT converts private IPv4 addresses into public IPv4 addresses.

6.3. Router advertisement

- In IPv6 networks, devices can **automatically configure their own addresses** and obtain essential network information **without manual configuration** or a traditional DHCP server.

- This automatic configuration is made possible through **ICMPv6 (Internet Control Message Protocol for IPv6)** messages — specifically **Router Solicitation (RS)** and **Router Advertisement (RA)** messages.

Router Solicitation (RS) and Router Advertisement (RA)

1. When an **IPv6-enabled host** (like a computer) connects to a network, it first sends a **Router Solicitation (RS)** message.
    - Purpose: To discover if there are any IPv6 routers on the local link.
2. The **IPv6 router** replies with a **Router Advertisement (RA)** message.
    - Purpose: To provide the host with configuration information needed to obtain a **Global Unicast Address (GUA)**.

What Is a Router Advertisement (RA)?

- A **Router Advertisement (RA)** message is an **ICMPv6 message** sent periodically or in response to an RS message.
- It informs IPv6 hosts about:
    - **How to obtain an IPv6 address**, and
    - **Important network configuration parameters.**

6.4. Stateless Address Autoconfiguration (SLAAC)

- SLAAC allows devices on a network to be configured with a GUA IPv6 address without the need for a Dynamic Host Configuration Protocol v6 (DHCPv6) server.

Process of Obtaining an IPv6 GUA Address:

1. **Router Solicitation (RS)** –
   The client sends an **RS message** to discover any IPv6 routers on the network.
2. **Router Advertisement (RA)** –
   The router responds with an **RA message**, providing the **network prefix** and **prefix length** (for example, `2001:db8:acad::/64`).
3. **Address Creation Using EUI-64** –
    - The client takes its **48-bit MAC address** from its network interface card (NIC).
    - It uses the **EUI-64 process** to convert it into a **64-bit Interface ID**.
    - The **Interface ID** is then **appended** to the 64-bit network prefix, forming a complete **128-bit IPv6 address** (GUA).
4. **Address Creation Using SLAAC with stateless DHCPv6** –
    - First, use SLAAC to create its own GUA IPv6 address.
    - Second, use the router's IPv6 Link-Local address as the default gateway for the network.
    - Lastly, use the stateless DHCPv6 server to obtain the DNS server addresses.

5. **Address Creation Using Stateful DHCPv6** –

    - A stateful DHCPv6 server has similar functionalities to a traditional DHCP server on an Ipv4 network as it provides the following configurations to clients: GUA IPv6 address, Prefix length, DNS server addresses.