**Lecture Notes: IP Address, Subnet Mask, Network & Host, and Subnetting**

**1. What is an IP Address?**

An **IP address (Internet Protocol Address)** is a unique identifier assigned to each device on a network to facilitate communication. It follows a structured format and consists of four octets (IPv4) separated by dots (e.g., 192.168.1.1).

**Types of IP Addresses:**

* **Public IP**: Used on the internet and assigned by ISPs. *(Example: 203.0.113.1 is a public IP assigned by an ISP.)*
* **Private IP**: Used within local networks (e.g., 192.168.x.x, 10.x.x.x, 172.16.x.x). *(Example: 192.168.1.10 in a home network.)*
* **Static IP**: Manually assigned and does not change. *(Example: A web server with 198.51.100.5.)*
* **Dynamic IP**: Assigned by DHCP and may change over time. *(Example: A home router getting 192.168.1.100 from the ISP.)*

**2. What is a Subnet?**

A **subnet (subnetwork)** is a logical division of a larger network, designed to enhance performance and security by reducing congestion. It is defined using a **subnet mask**, which separates the network and host portions of an IP address.

**Subnet Mask: Defining Network vs. Host**

A **subnet mask** determines how an IP address is split between:

* **Network Portion**: Identifies the subnet.
* **Host Portion**: Identifies individual devices within the subnet.

Example of subnet masks:

* 255.255.255.0 → /24 → 256 total IPs (254 usable hosts)
* 255.255.255.128 → /25 → 128 total IPs (126 usable hosts)
* 255.255.255.192 → /26 → 64 total IPs (62 usable hosts)

**3. Understanding Network & Host Portions**

An IP address consists of **two parts**:

1. **Network Part**: Identifies the entire network.
2. **Host Part**: Identifies individual devices (hosts) within that network.

For example, in 192.168.1.5/24:

* **Network**: 192.168.1.0
* **Host**: .5
* **Subnet Mask**: 255.255.255.0

**4. Explanation of 192.168.1.0/24**

* **192.168.1.0**: Network address (Identifies the subnet)
* **Subnet Mask (/24)**: 255.255.255.0 (First 24 bits for network, last 8 bits for host)
* **Total IPs**: 2^8 = 256
* **Usable Hosts**: 256 - 2 = 254
* **First Usable IP**: 192.168.1.1
* **Last Usable IP**: 192.168.1.254
* **Broadcast Address**: 192.168.1.255 (Sends data to all devices in the subnet)

**5. Why Are There Fewer Usable Hosts than Total Hosts?**

Each subnet has **two reserved IPs**:

1. **Network Address** (192.168.1.0): Identifies the subnet and cannot be assigned to a device.
2. **Broadcast Address** (192.168.1.255): Used to send data to all devices in the subnet.

Thus, the usable hosts = Total Hosts - 2.

**6. IP Address Classes**

| **Class** | **Range** | **Default Subnet Mask** | **Example** |
| --- | --- | --- | --- |
| **Class A** | 1.0.0.0 - 126.255.255.255 | 255.0.0.0 | 10.0.0.1 |
| **Class B** | 128.0.0.0 - 191.255.255.255 | 255.255.0.0 | 172.16.0.1 |
| **Class C** | 192.0.0.0 - 223.255.255.255 | 255.255.255.0 | 192.168.1.1 |

**7. Difference Between IPv4 and IPv6**

| **Feature** | **IPv4** | **IPv6** |
| --- | --- | --- |
| Address Length | 32-bit | 128-bit |
| Format | Dotted Decimal (192.168.1.1) | Hexadecimal (2001:db8::ff00:42:8329) |
| Total Addresses | 4.3 billion | 340 undecillion |
| Security | Limited | Built-in (IPSec) |

**8. Architecture Flow of IP Address Configuration**

**Step-by-Step Flow:**

1. **Device Requests an IP**: Using DHCP or Static Assignment.
2. **DHCP Assigns an IP** (if dynamic).
3. **Subnet Mask is Set**: Defines network and host portions.
4. **Gateway Address Configured**: Enables internet access.
5. **DNS Server Assigned**: Translates domain names to IPs.
6. **Communication Established**: Device is now online.

**Summary**

| **Concept** | **Explanation** |
| --- | --- |
| **IP Address** | Unique identifier for devices in a network. |
| **Subnet** | A division of a network for better management. |
| **Subnet Mask** | Defines the network and host portions of an IP. |
| **Network Address** | First IP in the subnet, used to identify the network. |
| **Usable Hosts** | All assignable IPs (Total IPs - 2). |
| **Broadcast Address** | Last IP in the subnet, used for sending messages to all hosts. |
| **Total Hosts Formula** | 2^(Number of Host Bits) |
| **Usable Hosts Formula** | Total Hosts - 2 |
| **Subnet Example (/24)** | 192.168.1.0/24 → 256 total IPs, 254 usable hosts. |
| **IP Classes** | Class A, B, C with different address ranges. |
| **IPv4 vs IPv6** | Differences in structure, security, and capacity. |
| **IP Configuration Flow** | DHCP/static assignment → Subnet mask → Gateway → DNS → Communication. |

**DIFFERENCE BETWEEN IP ADDRESS AND SUBNET**

An **IP address** and a **subnet** are related but serve different purposes in networking. Here’s how they differ:

**1. IP Address**

* An **IP address (Internet Protocol address)** is a unique numerical label assigned to each device connected to a network.
* It helps in identifying a device on a network (like a home computer, smartphone, or a server).
* IP addresses are of two types:
  + **IPv4** (e.g., 192.168.1.1) - 32-bit, written in dotted decimal format.
  + **IPv6** (e.g., 2001:db8::ff00:42:8329) - 128-bit, written in hexadecimal format.

**2. Subnet (Subnet Mask)**

* A **subnet (subnetwork)** is a segment of a larger network, created by dividing an IP network into smaller parts.
* A **subnet mask** determines which part of the IP address is the **network** portion and which part is the **host** portion.
* Example:
  + IP Address: 192.168.1.10
  + Subnet Mask: 255.255.255.0
  + This means:
    - 192.168.1 is the **network portion**.
    - .10 is the **host portion**.

**Key Differences**

| **Feature** | **IP Address** | **Subnet** |
| --- | --- | --- |
| **Purpose** | Identifies a device on a network | Defines network boundaries by dividing IP ranges |
| **Format** | IPv4 (192.168.1.10), IPv6 (2001:db8::1) | Subnet mask (255.255.255.0) or CIDR (/24) |
| **Function** | Used to locate devices in a network | Helps in segmenting a network into smaller parts |
| **Analogy** | Like a house number | Like defining neighborhoods in a city |

**How They Work Together**

* The **IP address** combined with the **subnet mask** helps determine if two devices are on the same network or need a router to communicate.
* Example:
  + 192.168.1.10/24 and 192.168.1.20/24 are in the same subnet.
  + 192.168.2.10/24 is in a different subnet and needs a router to communicate with 192.168.1.10/24.

**IP Address Classes and Network vs. Host Portion Allocation**

Each IP address consists of two parts:

1. **Network Portion** – Identifies the network.
2. **Host Portion** – Identifies individual devices (hosts) within that network.

The number of bits allocated to the **network** and **host** portions varies by class. Here's the detailed breakdown:

**Class A**

* **First Octet Range**: 1.0.0.0 to 126.255.255.255
* **Default Subnet Mask**: 255.0.0.0 (/8)
* **Network Bits**: **8 bits** (First octet)
* **Host Bits**: **24 bits** (Remaining three octets)
* **Total Networks**: 27−2=1262^7 - 2 = 126 (excluding 0.0.0.0 and 127.x.x.x reserved)
* **Total Hosts per Network**: 224−2=16,777,2142^{24} - 2 = 16,777,214 (subtracting network and broadcast addresses)

✅ **Example:**

* **Network Address**: 10.0.0.0
* **First Usable Host**: 10.0.0.1
* **Last Usable Host**: 10.255.255.254
* **Broadcast Address**: 10.255.255.255

**Class B**

* **First Octet Range**: 128.0.0.0 to 191.255.255.255
* **Default Subnet Mask**: 255.255.0.0 (/16)
* **Network Bits**: **16 bits** (First two octets)
* **Host Bits**: **16 bits** (Remaining two octets)
* **Total Networks**: 214=16,3842^{14} = 16,384 (since first two bits are fixed as 10)
* **Total Hosts per Network**: 216−2=65,5342^{16} - 2 = 65,534

✅ **Example:**

* **Network Address**: 172.16.0.0
* **First Usable Host**: 172.16.0.1
* **Last Usable Host**: 172.16.255.254
* **Broadcast Address**: 172.16.255.255

**Class C**

* **First Octet Range**: 192.0.0.0 to 223.255.255.255
* **Default Subnet Mask**: 255.255.255.0 (/24)
* **Network Bits**: **24 bits** (First three octets)
* **Host Bits**: **8 bits** (Last octet)
* **Total Networks**: 221=2,097,1522^{21} = 2,097,152 (since first three bits are fixed as 110)
* **Total Hosts per Network**: 28−2=2542^8 - 2 = 254

✅ **Example:**

* **Network Address**: 192.168.1.0
* **First Usable Host**: 192.168.1.1
* **Last Usable Host**: 192.168.1.254
* **Broadcast Address**: 192.168.1.255

**Class D (Multicast)**

* **First Octet Range**: 224.0.0.0 to 239.255.255.255
* **Purpose**: Used for multicast communications (not assigned to individual hosts)
* **No Host Allocation**: This class is not used for traditional networking.

✅ **Example:**

* 224.0.0.1 – Used for all hosts on a local network.
* 239.255.255.250 – UPnP discovery.

**Class E (Experimental)**

* **First Octet Range**: 240.0.0.0 to 255.255.255.255
* **Purpose**: Reserved for experimental and future use.
* **Not Usable for Public or Private Networks**

✅ **Example:**

* 250.1.2.3 – An experimental IP address.

**Comparison of Network and Host Allocation in Each Class**

| **Class** | **Network Bits** | **Host Bits** | **Total Networks** | **Total Hosts per Network** |
| --- | --- | --- | --- | --- |
| **A** | 8 | 24 | 126 | 16,777,214 |
| **B** | 16 | 16 | 16,384 | 65,534 |
| **C** | 24 | 8 | 2,097,152 | 254 |
| **D** | - | - | Multicast | N/A |
| **E** | - | - | Reserved | N/A |

| **Class** | **IP Range** | **Default Subnet Mask** | **Representation** | **Preferred Scenario Example** |
| --- | --- | --- | --- | --- |
| **A** | 1.0.0.0 - 126.255.255.255 | 255.0.0.0 (/8) | **N.H.H.H** | Large networks with many hosts (e.g., ISP networks, large enterprises). Example: 10.0.0.0 (Private Network) |
| **B** | 128.0.0.0 - 191.255.255.255 | 255.255.0.0 (/16) | **N.N.H.H** | Medium-sized organizations, universities, or government institutions. Example: 172.16.0.0 (Private Network) |
| **C** | 192.0.0.0 - 223.255.255.255 | 255.255.255.0 (/24) | **N.N.N.H** | Small networks like home, small business, or LAN segments. Example: 192.168.1.0 (Wi-Fi Router Network) |
| **D** | 224.0.0.0 - 239.255.255.255 | No Subnetting | **Multicast** | Used for sending data to multiple destinations simultaneously. Example: 224.0.0.1 (Multicast for all hosts) |
| **E** | 240.0.0.0 - 255.255.255.255 | Reserved | **Experimental** | Reserved for future use or research. Example: 250.1.2.3 (Experimental IP) |

**Explanation of Representation**

* **N.N.N.H** → Preferred when more networks are needed, and fewer hosts per network (e.g., Class C).
* **N.N.H.H** → Preferred when medium-sized networks are required with a balanced number of hosts (e.g., Class B).
* **N.H.H.H** → Preferred when fewer networks but a large number of hosts are needed (e.g., Class A).
* Class A has the fewest networks but the most hosts per network.
* Class C has the most networks but the fewest hosts per network.
* Subnetting allows dividing larger networks into smaller segments, optimizing usage.
* IPv4 exhaustion led to the creation of IPv6, which provides significantly more address space.

**Understanding Host and Network in IP Addressing**

An **IP address** is divided into two parts:

1. **Network Portion** - Identifies the network.
2. **Host Portion** - Identifies a specific device (host) within that network.

**1. What is a Network?**

* A **network** is a group of connected devices that share resources.
* The **network portion** of an IP address is the part that remains **the same** for all devices in the same subnet.
* It helps in identifying which network a device belongs to.
* Example:
  + IP: 192.168.1.10
  + Subnet Mask: 255.255.255.0
  + **Network Portion:** 192.168.1.0
  + All devices with IPs 192.168.1.x are in the same network.

**2. What is a Host?**

* A **host** is a device (computer, server, smartphone, etc.) connected to a network.
* The **host portion** of an IP address is the unique identifier for that device within the network.
* Example:
  + IP: 192.168.1.10
  + **Host Portion:** .10
  + Another host in the same network might be 192.168.1.20.

**Example Breakdown**

| **IP Address** | **Subnet Mask** | **Network Portion** | **Host Portion** |
| --- | --- | --- | --- |
| 192.168.1.10 | 255.255.255.0 | 192.168.1 | .10 |
| 192.168.1.20 | 255.255.255.0 | 192.168.1 | .20 |
| 192.168.2.5 | 255.255.255.0 | 192.168.2 | .5 |

* **Network = Group of connected devices sharing the same network prefix.**
* **Host = A specific device within the network.**
* Devices in the **same network** can communicate directly.
* Devices in **different networks** need a router to communicate.

**Understanding Network and Host in IP Addressing with a Detailed Example**

In **IP addressing**, an IP address is divided into two parts:

1. **Network Portion** – Identifies the network.
2. **Host Portion** – Identifies a specific device (host) within that network.

**Example: Office Network Scenario**

Imagine a company office with multiple computers, printers, and servers connected to the same network.

**Step 1: Assigning IP Addresses**

Each device in the office is assigned an **IP address**. Let’s say the office network uses the following range of IP addresses:

* **Network Address:** 192.168.1.0/24
* **Subnet Mask:** 255.255.255.0

This means:

* The **first three octets (192.168.1)** represent the **network**.
* The **last octet (X)** represents the **host** (individual device).

Here’s how the devices in the office are assigned IPs:

| **Device** | **IP Address** | **Network Portion** | **Host Portion** |
| --- | --- | --- | --- |
| **Router** | 192.168.1.1 | 192.168.1 | .1 |
| **Employee Laptop 1** | 192.168.1.10 | 192.168.1 | .10 |
| **Employee Laptop 2** | 192.168.1.20 | 192.168.1 | .20 |
| **Printer** | 192.168.1.30 | 192.168.1 | .30 |
| **Server** | 192.168.1.50 | 192.168.1 | .50 |

**Step 2: Understanding Network and Host**

* **Network Portion (192.168.1)**:
  + This remains the **same** for all devices in the office network.
  + It tells devices that they belong to the same group and can communicate **without needing a router**.
* **Host Portion (.X)**:
  + This is **different** for each device.
  + It uniquely identifies each device in the network.

**Step 3: Communication Within the Same Network**

* If **Laptop 1 (192.168.1.10)** wants to **print a document**, it sends a request to the **Printer (192.168.1.30)**.
* Since **both devices share the same network (192.168.1)**, they can communicate directly.

**Step 4: Communication Between Different Networks**

* Suppose an employee **accesses a website on the internet**.
* The website’s server has an IP like **"203.0.113.5"**, which is **outside** the 192.168.1.0 network.
* Since the website is on a different network, the request is sent to the **router (192.168.1.1)**, which **routes** the data to the internet.

**Another Example: Apartment Analogy**

Think of an apartment building:

* The **apartment complex name** = **Network (192.168.1)**
* The **apartment number** = **Host (.10, .20, .30, etc.)**
* All apartments **inside the same complex** can communicate easily.
* If someone **from another complex** (192.168.2.x) wants to visit, they need to go **through the main gate (router)**.

| **Feature** | **Network** | **Host** |
| --- | --- | --- |
| **Definition** | Identifies a group of devices sharing the same network. | Identifies a specific device within that network. |
| **Example (IP Address: 192.168.1.10)** | 192.168.1 (Same for all devices in that network) | .10 (Unique for each device) |
| **Analogy** | Apartment Complex Name | Apartment Number |
| **Devices in the Same Network** | Communicate directly | Unique identification |
| **Devices in Different Networks** | Need a **router** to communicate | Belong to different groups |

**Understanding IP Address and Subnet Mask with a Detailed Example**

An **IP address** and a **subnet mask** work together to define network boundaries. Let's break it down step by step with a real-world example.

**1. What is an IP Address?**

An **IP address (Internet Protocol Address)** is a unique identifier for a device on a network. It helps devices communicate with each other.

**Example:**

Imagine a **company office** with computers, printers, and a router. Each device needs a unique **IP address** to communicate.

| **Device** | **IP Address** |
| --- | --- |
| Router | 192.168.1.1 |
| Employee PC 1 | 192.168.1.10 |
| Employee PC 2 | 192.168.1.20 |
| Printer | 192.168.1.30 |
| Server | 192.168.1.50 |

Here, **each device has a unique IP address** but is part of the same network.

**Structure of an IP Address (IPv4)**

An IPv4 address consists of **4 numbers** separated by dots (.), each ranging from 0 to 255.

Example:

* **192.168.1.10**
  + 192 → First octet
  + 168 → Second octet
  + 1 → Third octet
  + 10 → Fourth octet

**2. What is a Subnet Mask?**

A **subnet mask** determines which part of an IP address is the **network portion** and which part is the **host portion**.

**Example:**

A common subnet mask is:

**255.255.255.0**

This means:

* **255.255.255** → **Network portion** (Fixed for all devices in this network)
* **0** → **Host portion** (Unique for each device)

**Applying it to Our Office Example:**

| **Device** | **IP Address** | **Subnet Mask** | **Network Portion** | **Host Portion** |
| --- | --- | --- | --- | --- |
| Router | 192.168.1.1 | 255.255.255.0 | 192.168.1 | .1 |
| Employee PC 1 | 192.168.1.10 | 255.255.255.0 | 192.168.1 | .10 |
| Employee PC 2 | 192.168.1.20 | 255.255.255.0 | 192.168.1 | .20 |
| Printer | 192.168.1.30 | 255.255.255.0 | 192.168.1 | .30 |
| Server | 192.168.1.50 | 255.255.255.0 | 192.168.1 | .50 |

Since all devices share the **same network portion (192.168.1)**, they can communicate **without needing a router**.

**3. How IP Address and Subnet Mask Work Together**

Let’s take **192.168.1.10** with a **255.255.255.0** subnet mask.

**Subnet mask (255.255.255.0) means:**

* First **3 octets (192.168.1)** → **Network Portion** (same for all devices).
* Last **octet (.X)** → **Host Portion** (unique for each device).

This tells the computer:  
✅ **“If I need to talk to another device in 192.168.1.X, I can do it directly.”**  
❌ **“If I need to talk to 192.168.2.X, I must go through a router.”**

**Example of Different Networks**

If another department in the company uses **192.168.2.X** instead of **192.168.1.X**, the two networks cannot communicate **directly**. They need a **router** to bridge the networks.

| **Device** | **IP Address** | **Subnet Mask** | **Network** |
| --- | --- | --- | --- |
| Employee PC 1 | 192.168.1.10 | 255.255.255.0 | 192.168.1.0/24 |
| Employee PC 2 | 192.168.2.20 | 255.255.255.0 | 192.168.2.0/24 |

Since they belong to **different networks**, they need a **router** to communicate.

**4. Real-World Analogy: Apartment System**

Think of a **city with apartment buildings**.

| **Concept** | **Real-World Example** | **IP Equivalent** |
| --- | --- | --- |
| **Network** | Apartment Complex | 192.168.1 |
| **Host** | Apartment Number | .10, .20, .30 |
| **Subnet Mask** | Defines building size | Tells which part is network vs. host |

* If two people live in **the same apartment complex**, they can **visit each other directly**.
* If someone lives in **another apartment complex**, they must go **through the main gate (router)**.

**5. Key Differences Between IP Address and Subnet Mask**

| **Feature** | **IP Address** | **Subnet Mask** |
| --- | --- | --- |
| **Purpose** | Identifies a device on a network | Defines network boundaries |
| **Example** | 192.168.1.10 | 255.255.255.0 |
| **Parts** | Network + Host | Only determines network portion |
| **Analogy** | House Number | Defines the neighborhood |

**Understanding 192.168.1.0/24 in Detail**

The notation **192.168.1.0/24** is a **CIDR (Classless Inter-Domain Routing) notation** that represents a **network address with a subnet mask**. Let’s break it down step by step.

**1. Breaking Down 192.168.1.0/24**

The given **IP address and subnet mask** notation has two parts:

* **192.168.1.0** → This is the **network address**.
* **/24** → This is the **subnet mask in prefix length format** (meaning the first 24 bits are reserved for the network).

**Step 1: Convert /24 into Subnet Mask**

* /24 means **24 bits** are for the **network portion**, and the remaining **8 bits** are for the **host portion**.
* The subnet mask for /24 is:

**Binary Representation:**

11111111.11111111.11111111.00000000

**Decimal Representation:**

255.255.255.0

This tells us:

* + The **first 24 bits (192.168.1)** define the **network**.
  + The **last 8 bits (.X)** define **hosts** (devices within the network).

**2. Network Address, Usable IPs, and Broadcast Address**

Using /24, we can determine key details:

| **Item** | **Value** |
| --- | --- |
| **Network Address** | 192.168.1.0 |
| **Subnet Mask** | 255.255.255.0 |
| **First Usable IP** | 192.168.1.1 |
| **Last Usable IP** | 192.168.1.254 |
| **Broadcast Address** | 192.168.1.255 |
| **Total Hosts** | 2^8 = 256 (Including network & broadcast) |
| **Usable Hosts** | 256 - 2 = 254 |

**Explanation**

1. **Network Address (192.168.1.0)**
   * This is the **identifier** for the subnet.
   * Devices cannot use this address.
2. **First Usable IP (192.168.1.1)**
   * The first assignable IP to a device (e.g., a router or computer).
3. **Last Usable IP (192.168.1.254)**
   * The last IP that can be assigned to a device.
4. **Broadcast Address (192.168.1.255)**
   * Used to send data to **all devices** in the subnet.

**3. How /24 Affects Network Communication**

Let’s consider two different IPs:

* **192.168.1.10/24**
* **192.168.1.50/24**

Since both IPs belong to **the same network (192.168.1.0/24)**, they can communicate **directly** without needing a router.

However, consider another device:

* **192.168.2.10/24**

Now, the network is **192.168.2.0/24**, which is different. Communication with **192.168.1.10/24** requires a **router**.

**4. Real-World Analogy**

Think of an **apartment building**:

* 192.168.1.0 → **Building Address (Network ID)**
* 192.168.1.1 - 192.168.1.254 → **Apartments (Hosts)**
* 192.168.1.255 → **Common Announcement System (Broadcast Address)**

People **inside the same building** (same subnet) can talk easily.  
To talk to people in **another building** (different subnet), you need **a phone (router)**.

**5. Summary**

* 192.168.1.0/24 defines a **network with 256 IPs (0-255)**.
* The **first (.0) is the network address**.
* The **last (.255) is the broadcast address**.
* **Usable IPs:** 192.168.1.1 - 192.168.1.254 (254 total).
* Devices **in the same subnet** can communicate **directly**.
* Different subnets **require a router**.

**Why Is There a Difference Between Usable Hosts and Total Hosts?**

When you calculate the number of **total hosts** in a subnet, you use the formula:

Total Hosts=2Number of Host Bits\text{Total Hosts} = 2^{\text{Number of Host Bits}}

However, not all of these IP addresses can be assigned to devices. This is because **two addresses are reserved in every subnet**:

1. **Network Address** → Identifies the subnet (first IP).
2. **Broadcast Address** → Used for broadcasting messages to all hosts (last IP).

**Example: 192.168.1.0/24**

* **Total Hosts Calculation**
  + /24 means **8 bits** for hosts.
  + Total Hosts=28=256\text{Total Hosts} = 2^8 = 256.
* **Reserved Addresses**
  + **Network Address**: 192.168.1.0
  + **Broadcast Address**: 192.168.1.255
* **Usable Hosts Calculation**
  + **Usable Hosts** = **Total Hosts - 2**
  + 256−2=254256 - 2 = 254

**Why Are These Two Addresses Reserved?**

**1. Network Address (192.168.1.0)**

* Defines the entire subnet.
* Used by routers to understand routing and subnetting.
* Devices cannot be assigned this address.

**2. Broadcast Address (192.168.1.255)**

* Used to send messages to **all devices** in the subnet.
* When a device sends a packet to the broadcast address, every device in that subnet receives it.
* Assigning this to a single device would break network communication.

**Key Takeaways**

| **Item** | **Address Example (/24)** | **Usage** |
| --- | --- | --- |
| **Network Address** | 192.168.1.0 | Identifies the subnet (Not assignable). |
| **First Usable Host** | 192.168.1.1 | Can be assigned to a device. |
| **Last Usable Host** | 192.168.1.254 | Can be assigned to a device. |
| **Broadcast Address** | 192.168.1.255 | Sends data to all devices in the subnet. |
| **Total Hosts** | 256 (2⁸) | Includes all possible addresses. |
| **Usable Hosts** | 254 | Assignable to devices. |

Here’s your **detailed lecture note** with **step-by-step instructions** to:

✅ **Connect a Private EC2 Instance using a Public EC2 (Bastion Host)**  
✅ **Set up NAT Gateway for internet access in a Private Subnet**  
✅ **Configure VPC Peering for cross-VPC communication**

**📌 Lecture Notes: IP Addressing, Subnetting & AWS VPC with NAT Gateway and VPC Peering (Hands-On Guide)**

**🔹 Section 1: Understanding IP Addressing and Subnetting**

(📌 Same as the previous lecture note, explaining IP addresses, subnetting, and AWS private IP ranges.)

**🔹 Section 2: AWS VPC Setup**

We are going to:  
1️. **Create a Custom VPC with Public and Private Subnets**  
2️. **Set up an Internet Gateway (IGW) for public internet access**  
3️. **Configure Route Tables for Subnet Communication**  
4️. **Launch a Public EC2 (Bastion Host) & Private EC2**  
5️. **Use NAT Gateway to allow private EC2 to access the internet**  
6️. **Configure VPC Peering for cross-VPC communication**

**🔹 Section 3: Hands-on AWS VPC Setup**

**3.1 Creating a Custom VPC**

📌 **Step 1:** Login to AWS Console → Open **VPC Dashboard**  
📌 **Step 2:** Click **Create VPC**

* **Name:** MyCustomVPC
* **IPv4 CIDR:** 10.0.0.0/16
* **IPv6 CIDR:** Disable
* **Tenancy:** Default
* Click **Create VPC**

**3.2 Creating Subnets**

📌 **Step 1:** Go to **Subnets** → Click **Create Subnet**

| **Subnet Name** | **CIDR Block** | **Availability Zone** | **Subnet Type** |
| --- | --- | --- | --- |
| Public-Subnet | 10.0.1.0/24 | us-east-1a | Public |
| Private-Subnet | 10.0.2.0/24 | us-east-1b | Private |

* Click **Create Subnets**

**3.3 Creating an Internet Gateway (IGW)**

📌 **Step 1:** Go to **Internet Gateways** → Click **Create IGW**  
📌 **Step 2:** Name it MyIGW, click **Create**  
📌 **Step 3:** Attach to MyCustomVPC

**3.4 Configuring Route Tables**

📌 **Step 1:** Go to **Route Tables** → Click **Create Route Table**

| **Route Table Name** | **Subnet Association** | **Routes** |
| --- | --- | --- |
| Public-RT | Public Subnet | 0.0.0.0/0 → **IGW** |
| Private-RT | Private Subnet | No internet access initially |

* Click **Create**

**3.5 Launching a Public EC2 (Bastion Host)**

📌 **Step 1:** Go to **EC2 Dashboard** → Click **Launch Instance**  
📌 **Step 2:** Select **Amazon Linux 2 AMI**  
📌 **Step 3:** Choose t2.micro instance type  
📌 **Step 4:**

* **VPC:** MyCustomVPC
* **Subnet:** Public-Subnet
* **Auto-assign Public IP:** **Enable**
* **Security Group:** PublicSG
  + Allow **SSH (22)** from **your IP**
  + Allow **HTTP (80)** from **Anywhere**  
    📌 **Step 5:** Click **Launch**

**3.6 Launching a Private EC2 Instance**

📌 **Step 1:** Go to **EC2 Dashboard** → Click **Launch Instance**  
📌 **Step 2:** Select **Amazon Linux 2 AMI**  
📌 **Step 3:** Choose t2.micro instance type  
📌 **Step 4:**

* **VPC:** MyCustomVPC
* **Subnet:** Private-Subnet
* **Auto-assign Public IP:** **Disable**
* **Security Group:** PrivateSG
  + Allow **SSH (22)** only from **Public EC2 (Bastion Host)**  
    📌 **Step 5:** Click **Launch**

**🔹 Section 4: Connecting Private EC2 using Bastion Host**

📌 **Step 1:** Connect to **Public EC2**

ssh -i mykey.pem ec2-user@<Public-EC2-IP>

📌 **Step 2:** From the Bastion Host, SSH into **Private EC2**

ssh -i mykey.pem ec2-user@<Private-EC2-Private-IP>

🎉 **Now, you have accessed the private EC2 via the Public Bastion Host!**

**🔹 Section 5: Setting Up NAT Gateway (For Private EC2 Internet Access)**

**5.1 Create a NAT Gateway**

📌 **Step 1:** Go to **VPC Dashboard → NAT Gateways → Create NAT Gateway**  
📌 **Step 2:**

* **Subnet:** Public-Subnet
* **Elastic IP:** Allocate a new one  
  📌 **Step 3:** Click **Create**

**5.2 Modify Private Route Table**

📌 **Step 1:** Go to **Route Tables**  
📌 **Step 2:** Select Private-RT, click **Edit Routes**  
📌 **Step 3:** Add 0.0.0.0/0 → **NAT Gateway**  
📌 **Step 4:** Click **Save**

🎉 **Now, the Private EC2 instance can access the internet but is not publicly accessible!**

**🔹 Section 6: VPC Peering (Connecting Two VPCs)**

**6.1 Create Second VPC**

📌 **Step 1:** Go to **VPC Dashboard** → Create **Second VPC**

* Name: VPC-2
* CIDR: 192.168.0.0/16 📌 **Step 2:** Create **Subnet (192.168.1.0/24)**

**6.2 Create VPC Peering Connection**

📌 **Step 1:** Go to **VPC Peering** → Click **Create Peering Connection**  
📌 **Step 2:**

* **VPC 1 (Requester):** MyCustomVPC
* **VPC 2 (Accepter):** VPC-2  
  📌 **Step 3:** Accept the request in VPC-2

**6.3 Modify Route Tables for Communication**

📌 **Step 1:** Edit MyCustomVPC Route Table

* Add 192.168.0.0/16 → **Target: VPC Peering Connection**  
  📌 **Step 2:** Edit VPC-2 Route Table
* Add 10.0.0.0/16 → **Target: VPC Peering Connection**

🎉 **Now, both VPCs can communicate with each other!**

**🚀 Final Summary**

✅ **Public EC2 can SSH into Private EC2 (Bastion Host Approach)**  
✅ **Private EC2 can access the internet via NAT Gateway**  
✅ **VPC Peering allows cross-VPC communication**

💡 **This setup is widely used for private workloads, secure backend processing, and multi-VPC architectures.**