

Computer Networks

Connect with me: [Youtube](#) | [LinkedIn](#) | [WhatsApp Channel](#) | [Web](#) | [Facebook](#) | [Twitter](#)

- [Download PDF](#)
- To access the updated handouts, please click on the following link: <https://yasirbhutta.github.io/cs-407-computer-networks/docs/computer-networks.html>

Contents:

- [What is Private IP Address](#)
- [What is Public IP address](#)
- [GigabitEthernet0/0](#)
- [Ports in networking](#)
- [What is VLAN?](#)

1. What is a Private IP Address?

A **private IP address** is an IP address reserved for internal use within a network (such as a home, office, or enterprise) that is **not routable** on the global internet. These addresses are used to identify devices within a private network and are translated to public IP addresses when communicating outside the network (via technologies like NAT, Network Address Translation).

Private IP Range for Class C Networks

In **Class C networks**, the range of private IP addresses is:

- **192.168.0.0 to 192.168.255.255**

This gives a total of **256 Class C networks**, with each network having **256 addresses** (from **192.168.0.0/24** to **192.168.255.255/24**).

Breakdown of Class C Private IP Range:

- **Starting Address:** 192.168.0.0
- **Ending Address:** 192.168.255.255
- **Subnet Mask:** 255.255.255.0

The first IP (**192.168.x.0**) is typically reserved as the **network address**, and the last IP (**192.168.x.255**) is usually reserved as the **broadcast address**.

Examples:

- Network: 192.168.1.0/24
 - Usable IP range: 192.168.1.1 to 192.168.1.254
- Network: 192.168.100.0/24
 - Usable IP range: 192.168.100.1 to 192.168.100.254

Other Private IP Ranges (for reference):

- **Class A:** 10.0.0.0 to 10.255.255.255
- **Class B:** 172.16.0.0 to 172.31.255.255
- **Class C:** 192.168.0.0 to 192.168.255.255

These IP ranges are reserved for internal network use and will not be routed on the public internet, ensuring that devices in these ranges cannot directly access or be accessed from the global internet without proper configuration (e.g., using NAT).

2. What is Public IP address

A **public IP address** is an IP address that is accessible over the internet. It is assigned to a network device, like a router, by an Internet Service Provider (ISP) and allows devices on that network to communicate with devices outside of it. This IP address is globally unique, meaning that no two devices connected directly to the internet will have the same public IP address at the same time.

Key Points

- **Uniqueness:** Each public IP is unique and can be traced to the region, ISP, or sometimes the specific organization that owns it.
- **Uses:** Public IPs are necessary for hosting web servers, allowing users to access online resources, and enabling remote access to a device on a network.
- **Types:** Public IPs can be static (permanently assigned to a device) or dynamic (changes periodically).

Most devices connected to the internet via a home network have a private IP address within the network, which is then mapped to the public IP of the router or modem when accessing the internet.

3. GigabitEthernet0/0

GigabitEthernet0/0 refers to a specific network interface on a Cisco router or switch. Let's break down the term in parts:

1. GigabitEthernet:

- **GigabitEthernet** refers to the interface type and its speed capability.
- It supports **gigabit speeds** (1 Gbps or 1000 Mbps) for data transmission.
- GigabitEthernet interfaces are commonly used in modern networking devices for faster data transfer compared to FastEthernet (100 Mbps).

2. 0/0:

- The numbers **0/0** represent the **slot/port** number:
 - **0/0** means the interface is in **slot 0, port 0**.
 - Cisco routers and switches often have multiple slots and ports where interfaces (Ethernet, Serial, etc.) are located.

Here's what it means:

- The first **0** refers to the **slot number**. Many Cisco devices have modular slots where different types of network modules can be installed.

- The second **0** refers to the **port number** within that slot. Port 0 is typically the first physical interface on that module.

Example:

On a router with **GigabitEthernet0/0**, it refers to:

- **GigabitEthernet**: The interface type supporting speeds of 1 Gbps.
- **0/0**: The first port (port 0) in the first slot (slot 0).

Usage of GigabitEthernet0/0

When configuring a Cisco router, you often interact with this interface to assign IP addresses, enable or disable the interface, and define routing settings.

Example Command:

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

In this example:

- You access the **GigabitEthernet0/0** interface on the router.
- Assign the IP address **192.168.1.1** with a subnet mask of **255.255.255.0**.
- Use **no shutdown** to enable the interface.

Common Features of GigabitEthernet Interfaces:

- **Speed**: 1 Gbps (1000 Mbps).
- **Duplex**: Full-duplex communication, meaning data can be sent and received simultaneously.
- **Usage**: Often used for **backbone connections** or **high-speed LAN segments**.
- **Physical Interface**: Uses **RJ-45 connectors** or **fiber** connectors depending on the type of GigabitEthernet port (copper or fiber).

4. Ports in networking

Each port is associated with a specific process or service, allowing computers to differentiate between different types of traffic. For example, emails use a different port than webpages, even though both reach a computer over the same internet connection

192.168.1.0/24

The IP address **192.168.1.0/24** represents a **subnet** in the world of IP addressing.

Let's break it down:

Components of **192.168.1.0/24**:

1. **192.168.1.0 (Network Address):**

- This is the **base IP address** of the subnet.
- It's a **private IP address** reserved for internal use within local networks (it won't be routed on the public internet).
- **192.168.x.x** is a common range for home and small business networks.

2. **/24 (Subnet Mask):**

- This is **CIDR (Classless Inter-Domain Routing) notation** that represents the subnet mask.
- **/24** means that the first 24 bits of the IP address are reserved for the **network portion**, and the remaining 8 bits are used for the **host portion** (devices within the network).
- In dotted decimal format, the subnet mask for **/24** is **255.255.255.0**, which is equivalent to 24 network bits.

What Does **192.168.1.0/24** Represent?

- **Network Address:** **192.168.1.0** is the **network identifier** for the subnet. It is not assigned to any device.
- **Range of Usable IP Addresses:**
 - The **usable IP range** in this subnet is from **192.168.1.1** to **192.168.1.254**.
 - **192.168.1.1** would typically be assigned to a router or gateway.
 - You can assign IP addresses from **192.168.1.2** to **192.168.1.254** to devices within the network.
- **Broadcast Address:** The **broadcast address** for this subnet is **192.168.1.255**. This address is used to send messages to all devices on the network.

Structure of an IP Address

An IPv4 address is 32 bits, and in CIDR notation, we divide this into two parts:

- **Network portion** (first 24 bits in this case): Identifies the network (e.g., 192.168.1.x).
- **Host portion** (last 8 bits in this case): Identifies individual devices within the network (e.g., **.1**, **.2**, **.3**, ... up to **.254**).

Example:

For the network **192.168.1.0/24**:

- **Network address:** 192.168.1.0
- **Subnet mask:** 255.255.255.0
- **Usable IP range:** 192.168.1.1 to 192.168.1.254
- **Broadcast address:** 192.168.1.255

This setup allows for **254 usable IP addresses** (from **.1** to **.254**) that can be assigned to hosts (e.g., computers, printers, phones) on the network.

Summary:

- **192.168.1.0** is the network identifier, and the **/24** means the first 24 bits are used for the network, leaving 8 bits for the hosts.
- **Subnet mask /24** allows for 254 devices on the network (usable IPs from **192.168.1.1** to **192.168.1.254**).

This type of subnetting is typical in home and small office networks.

5. What is VLAN?

A **Virtual Local Area Network (VLAN)** is a logical grouping of devices within a larger physical network. VLANs allow network administrators to segment networks into smaller, manageable parts, regardless of the physical location of the devices. Each VLAN operates as a separate broadcast domain, meaning that devices in different VLANs cannot communicate with each other directly without the use of a router or a Layer 3 switch.

Key Features of VLANs:

- **Logical Segmentation:** VLANs can segregate networks based on business functions, departmental needs, or security levels rather than relying on physical locations.
- **Broadcast Control:** VLANs limit broadcast traffic by ensuring that broadcast packets are sent only to devices within the same VLAN.
- **Enhanced Security:** VLANs can isolate sensitive data and devices, preventing unauthorized access from users in other VLANs.
- **Simplified Management:** VLANs allow for easier management of the network by enabling administrators to make changes to network topology without physically rewiring devices.

Why VLANs Are Important in Computer Networks

1. Improved Performance:

- By reducing broadcast traffic within a VLAN, overall network performance improves, leading to faster data transmission and reduced congestion.

2. Enhanced Security:

- VLANs provide a way to separate sensitive data from general user traffic. For example, a finance department can be placed in a different VLAN from the HR department to protect sensitive financial data.

3. Flexibility and Scalability:

- VLANs can be easily created, modified, or deleted as the organization grows or changes. This flexibility allows for efficient adaptation to new business needs without the need for physical changes to the network.

4. Simplified Troubleshooting:

- Network issues can be isolated within a specific VLAN, making troubleshooting more straightforward and less time-consuming.

5. Cost-Effectiveness:

- VLANs enable better utilization of existing network infrastructure by allowing multiple logical networks to coexist on a single physical network. This reduces the need for additional hardware and cabling.

6. **Separation of Traffic Types:**

- VLANs can be used to separate different types of traffic, such as voice, video, and data, which can improve Quality of Service (QoS) for real-time applications.

7. **Improved Network Management:**

- With VLANs, network administrators can manage network resources more effectively, applying policies and configurations at the VLAN level rather than on individual devices.

Difference Between Routers and Switches: Key Functions and Features

Routers and **switches** are essential networking devices, but they serve different purposes within a network:

1. Routers

- **Purpose:** Routers connect different networks, such as a home network to the internet or multiple office networks to each other.
- **Functionality:** They route data packets from one network to another, often directing traffic between local devices and the broader internet.
- **IP Addressing:** Routers use IP addresses to determine the best path for data packets, allowing different networks to communicate.
- **Security:** Routers often have built-in firewalls, which provide a security layer by filtering traffic.

2. Switches

- **Purpose:** Switches connect multiple devices within a single local area network (LAN), like computers, printers, and servers in an office.
- **Functionality:** Switches forward data packets within a network based on MAC addresses (not IP addresses) to ensure each device receives only the data intended for it.
- **Efficiency:** They improve network efficiency by reducing data collisions and isolating data transfers to specific devices.
- **No Routing:** Switches don't connect to the internet directly; they only manage internal network communication.

Summary Table

Feature	Router	Switch
Primary Role	Connects networks	Connects devices within a LAN
Data Handling	Routes data using IP addresses	Forwards data using MAC addresses
Scope	Operates across networks	Operates within a network
Security	Often has firewall capabilities	Typically lacks security features