**Computer Networking**

**Notes by MOHAMMAD EMRAN AHMED EMON**

**BSc in SOFTWARE ENGINEERING,**

**SHAHJALAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, SYLHET.**

**Registration No: 2020831040**

**Session: 2020-21**

**Organizing Secretary, SWE Society**

**Former Assistant Publication Secretary, SPORTS SUST**

**Former Executive Member, SWE Society**

**Start: 01/10/2024**

**End: 06/10/2024**

**Introduction to Networks**

**9.0 Introduction**

**9.1 Subnetting an IPv4 Network**

**9.2 Addressing Schemes**

**Subnetting**

**Subnetting** is the process of segmenting a larger network into multiple smaller networks called subnetworks or subnets.

**Reasons for Subnetting:**

Large networks must be segmented into smaller subnetworks, creating smaller groups of devices and services to:

• Control traffic by containing broadcast traffic within each subnetwork.

• Reduce overall network traffic and improve network performance.

**Communication Between Subnets**

▪ A router is necessary for devices on different networks and subnets to communicate.

▪ Each router interface must have an IPv4 host address that belongs to the network or subnet that the router interface is connected.

▪ Devices on a network and subnet use the router interface attached to their LAN as their default gateway

**Basic Subnetting**

Subnets are created by using one or more of the host bits as network bits.

▪ This is done by borrowing some of the bits from the host portion of the address.

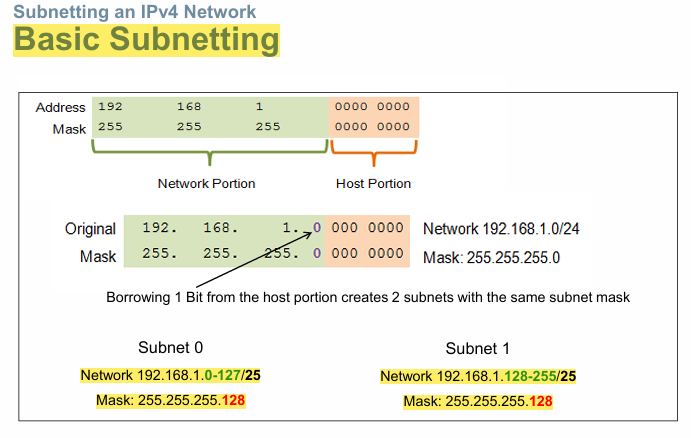
▪ The more host bits borrowed; the more subnets can be created. ▪ For each bit borrowed, the number of subnetworks available is doubled.

▪ For example, if 1 bit is borrowed, 2 subnets can be created. If 2 bits, 4 subnets are created, if 3 bits are borrowed, 8 subnets are created, and so on (2n; where n is the number of borrowed bits).

▪ However, with each bit borrowed, fewer host addresses are available per subnet

A screenshot of a computer

Description automatically generated



A computer screen shot of a network

Description automatically generated

A screenshot of a computer

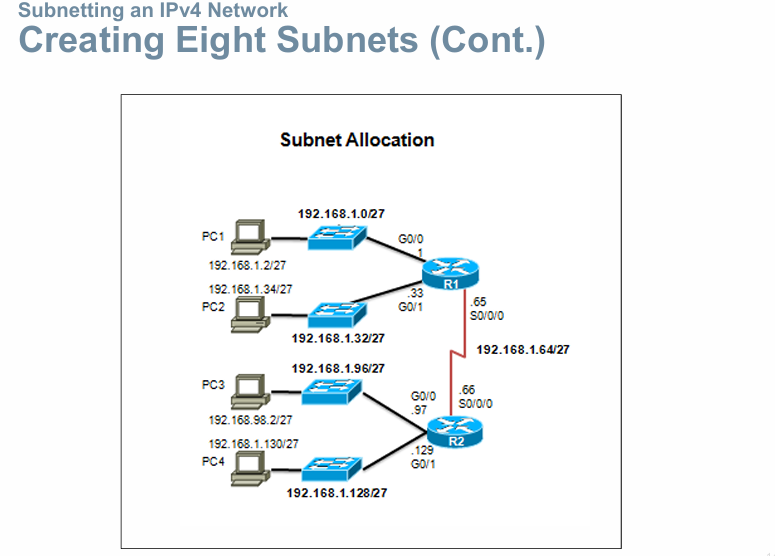
Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated



**Two considerations when planning subnets:**

▪ Number of subnets required

▪ Number of host addresses required

**Formula to determine number of usable hosts: 2n-2**

▪ 2n (where n is the number of remaining host bits) is used to calculate the number of hosts.

▪-2 (The subnetwork address and broadcast address cannot be used on each subnet.)

Calculate the number of subnets:

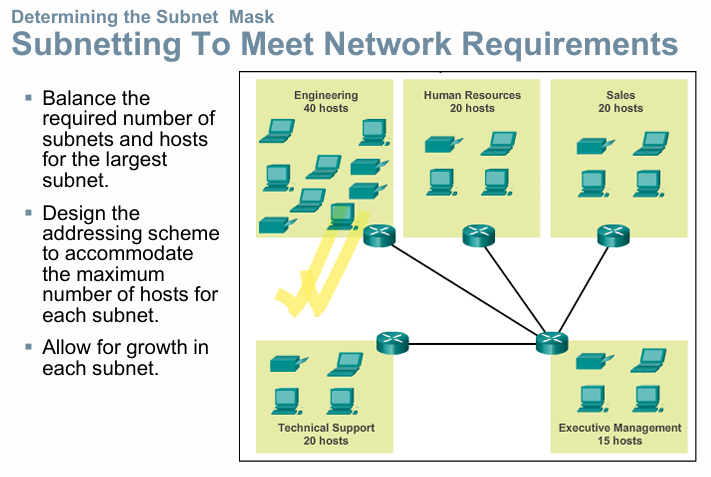
▪ 2n (where n is the number of bits borrowed)

▪ Subnet needed for each department.

Let’s examine the animation in 9.1.4.1

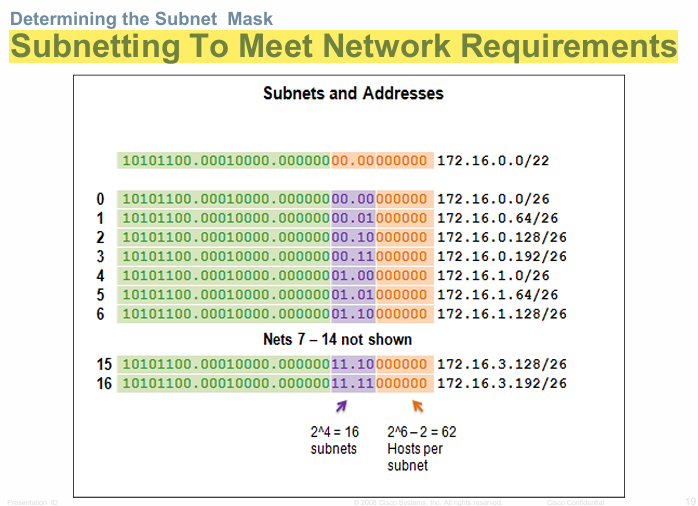
A diagram of a cloud

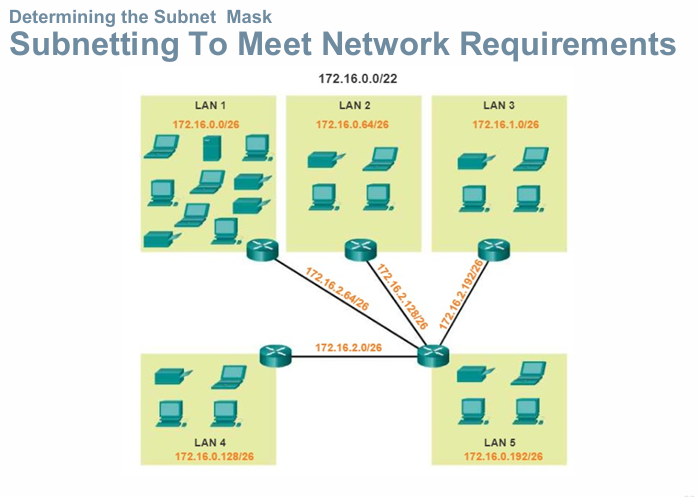
Description automatically generated



A diagram of a network

Description automatically generated





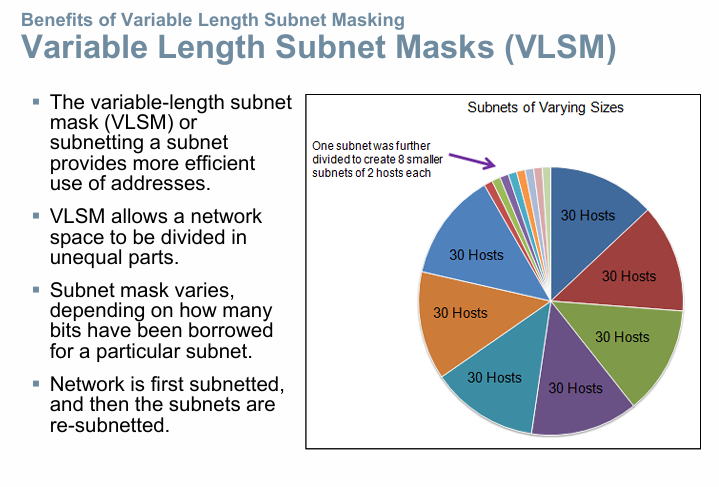
A pie chart with different colors and numbers

Description automatically generated

A diagram of a network

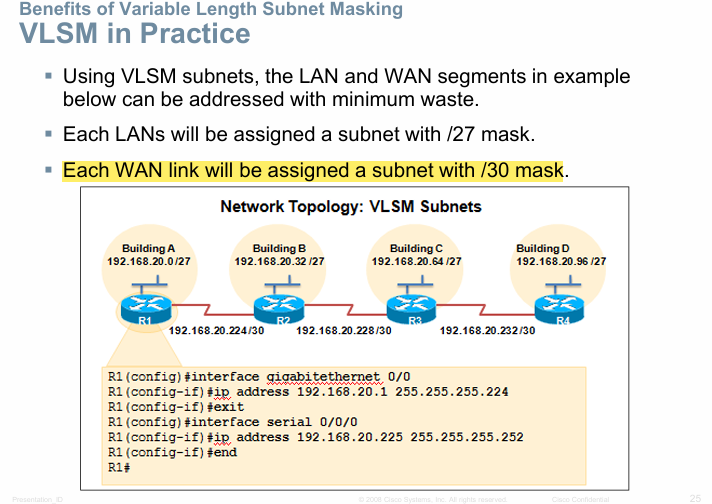
Description automatically generated with medium confidence

**Variable Length Subnet Masks (VLSM)**



A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

A table with numbers and letters

Description automatically generated with medium confidence

**IP Addressing**

[An IP address (Internet Protocol address) is a numerical label assigned to a device connected to a computer networ](https://www.bing.com/ck/a?!&&p=14a2b2829bafac3ad7d1cf6b5b24cb141394f71b0fcb20102f02a6feb1831575JmltdHM9MTczMDU5MjAwMA&ptn=3&ver=2&hsh=4&fclid=32a5eee7-1480-6593-2bd2-fbf1151b6403&psq=what+is+ip+address&u=a1aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvSVBfYWRkcmVzcw&ntb=1)k that uses the [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) for communication.

IP addresses serve two main functions:

network interface [identification](https://en.wikipedia.org/wiki/Identification_(information)),

and location [addressing](https://en.wikipedia.org/wiki/Network_address).

A blue pin with a black and white text

Description automatically generated

**Types of IP addresses**

There are several types of IP addresses, each with different purposes and characteristics. Here’s a look at each of them, what they’re used for, and how they work:

**Public IP addresses**

Public IP addresses are what devices and servers use to communicate over the internet. Your internet service provider (ISP) assigns a public IP address to your router. Then your router assigns your device and other devices connected to it with their own individual IP address.

**Private IP addresses**

A private IP address, also called a local IP address, is the IP address used to identify each device within your local network. While your public IP address is visible to devices outside your network, your private IP address is only visible within your network

**Static IP addresses**

Static IP addresses don’t change; once a device is assigned an IP address, that address remains the same. Static IP addresses are often used for large servers or other central devices

**Dynamic IP addresses**

Most devices use dynamic IP addresses, which change over time—how often varies depending on the ISP and other factors. A dynamic IP address offers security benefits, because changing IPs are harder to hack or spoof.

**IPv4 Network Addresses**

**IP Address and Address Space**

* The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet.
* An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
* The IP address is the address of the connection, not the host or the router because if the device is moved to another network, the IP address may be changed
* Address Space: An address space is the total number of addresses used by the protocol
* If a protocol uses b bits to define an address, the address space is 2b because each bit can have two different values (0 or 1)
* IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion)

**IPv4 Address Structure Binary Notation**

* Binary notation refers to the fact that computers communicate in 1s and 0s
* For ease of use by people, binary patterns representing IPv4 addresses are expressed as dotted decimals.
* This is first accomplished by separating each byte (8 bits) of the 32-bit binary pattern, called an octet, with a dot.

A computer screen shot of a computer

Description automatically generated

A diagram of a network connection

Description automatically generated

What is Subnet Mask?

[A subnet mask is a 32-bit number that defines a range of IP addresses available within a network](https://www.bing.com/ck/a?!&&p=90acd301c7046d353b3c2990d7e7a47dab601324cbea37fdc615baa75e7dbb65JmltdHM9MTczMDY3ODQwMA&ptn=3&ver=2&hsh=4&fclid=32a5eee7-1480-6593-2bd2-fbf1151b6403&psq=what+is+subnet+mask&u=a1aHR0cHM6Ly90ZWNodGVybXMuY29tL2RlZmluaXRpb24vc3VibmV0X21hc2s&ntb=1). [It distinguishes the network address and the host address within an IP address](https://www.bing.com/ck/a?!&&p=9f9ca0cbb60086711e74b91278775697a69f7cc3176a2a1d5d505ea5915ba520JmltdHM9MTczMDY3ODQwMA&ptn=3&ver=2&hsh=4&fclid=32a5eee7-1480-6593-2bd2-fbf1151b6403&psq=what+is+subnet+mask&u=a1aHR0cHM6Ly93d3cuaXB4by5jb20vYmxvZy93aGF0LWlzLXN1Ym5ldC1tYXNrLw&ntb=1). [It is made by setting network bits to all "1"s and setting host bits to all "0"s](https://www.bing.com/ck/a?!&&p=a718161c58ecf5ed3c5ae6cf2a031a42068772d84a3a30c905e651433b609d0cJmltdHM9MTczMDY3ODQwMA&ptn=3&ver=2&hsh=4&fclid=32a5eee7-1480-6593-2bd2-fbf1151b6403&psq=what+is+subnet+mask&u=a1aHR0cHM6Ly93d3cuaXBsb2NhdGlvbi5uZXQvc3VibmV0LW1hc2s&ntb=1)

[A subnet mask is used to divide a network into smaller subnets](https://www.bing.com/ck/a?!&&p=9f9ca0cbb60086711e74b91278775697a69f7cc3176a2a1d5d505ea5915ba520JmltdHM9MTczMDY3ODQwMA&ptn=3&ver=2&hsh=4&fclid=32a5eee7-1480-6593-2bd2-fbf1151b6403&psq=what+is+subnet+mask&u=a1aHR0cHM6Ly93d3cuaXB4by5jb20vYmxvZy93aGF0LWlzLXN1Ym5ldC1tYXNrLw&ntb=1). [It is not shown inside the data packets traversing the Internet](https://www.bing.com/ck/a?!&&p=5588bfb016723fe57d8a29e00034b52af590ef556decd05bef307e399931b313JmltdHM9MTczMDY3ODQwMA&ptn=3&ver=2&hsh=4&fclid=32a5eee7-1480-6593-2bd2-fbf1151b6403&psq=what+is+subnet+mask&u=a1aHR0cHM6Ly93d3cuZ3VydTk5LmNvbS9zdWJuZXR0aW5nLXN1Ym5ldC1tYXNrLmh0bWw&ntb=1)

**IPv4 Subnet Mask Network Portion and Host Portion of an IPv4 Address**

* To define the network and host portions of an address, a device uses a separate 32-bit pattern called a subnet mask
* The subnet mask does not actually contain the network or host portion of an IPv4 address, it just says where to look for these portions in a given IPv4 address

A diagram of a network portion

Description automatically generated

**Types of IPv4 Address**

**Classful Addressing**

* The whole Address space was divided into five classes (Class A, B, C, D and E)
* The unicast address classes A, B, and C defined specifically sized networks and specific address blocks for these networks.
* A company or organization was assigned an entire network from class A, class B, or class C address block.
* This use of address space is referred to as classful addressing.
* It also defined class D (multicast) and class E (experimental) addresses, as previously presented.

**Types of IPv4 Address**

**Classless Addressing**

**Limits to the Class-based System**

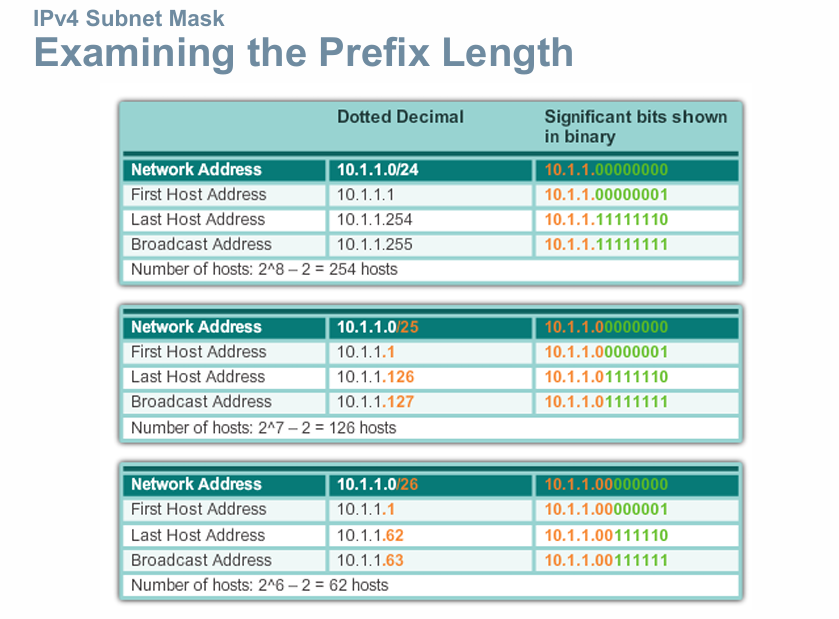
* Not all organizations' requirements fit well into one of these three classes.
* Classful allocation of address space often wasted many addresses, which exhausted the availability of IPv4 addresses.
* For example, a company that had a network with 260 hosts would need to be given a class B address with more than 65,000 addresses

**Classless Addressing/Prefix length**

* Formal name is Classless Inter-Domain Routing (CIDR, pronounced “cider”)
* Created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address

**Prefix Length**

* The prefix length is another way of expressing the subnet mask.
* The prefix length is the number of bits set to 1 in the subnet mask.
* It is written in “slash notation”, a “/” followed by the number of bits set to1.
* For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24.
* The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.



A table with numbers and numbers

Description automatically generated

A screenshot of a computer

Description automatically generated

**IPv4 Unicast, Broadcast, and Multicast**

In an IPv4 network, the hosts can communicate one of three different ways: **Unicast**, **Broadcast**, and **Multicast**

**#1/Unicast**

the process of sending a packet from one host to an individual host.

A diagram of a computer network

Description automatically generated

**#2 Broadcast**

the process of sending a packet from one host to all hosts in the network.

**Directed broadcast**

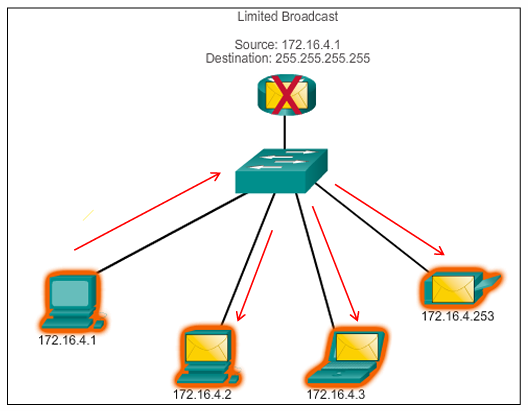
▪ Destination 172.16.4.255

▪ Hosts within the 172.16.4.0/24 network

**Limited broadcast**

▪ Destination 255.255.255.255

▪ NOTE: Routers do not forward a limited broadcast!



**#3 Multicast–**

The process of sending a packet from one host to a selected group of hosts, possibly in different networks.

▪ Reduces traffic

▪ Some examples: Video and audio broadcasts, Routing information exchange, Distribution of software, Remote gaming

▪ Reserved for addressing multicast groups – 224.0.0.0 to 239.255.255.255.

▪ Link local – 224.0.0.0 to 224.0.0.255 (Example: routing information exchanged by routing protocols)

**What is Private IP Addressing?**

Private IP Addresses are those addresses that work within the local network. These addresses are non-routable on the Internet. The address is basically assigned by the network router to your particular device. The unique private IP address is provided to every device which is on the same network. In this way, devices communicate with one another on the same network without connecting to the entire Internet. In this way, Private IP addresses are able to provide more security within a particular network. The private IP address cannot be seen on the Internet, unlike the Public IP Address. Only devices within the local network are able to see the address of one another

**Private address blocks are:**

Hosts that do not require access to the Internet can use private addresses reserved by the **Internet Assigned Numbers Authority (IANA)**

▪ 10.0.0.0 to 10.255.255.255 (10.0.0.0/8) Class-A

▪ 172.16.0.0 to 172.31.255.255 (172.16.0.0/12) Class-B

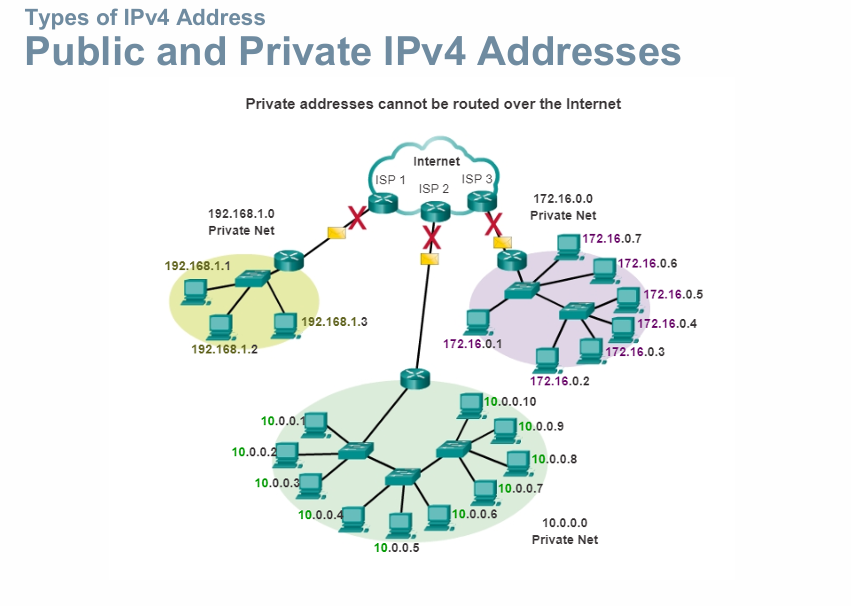
▪ 192.168.0.0 to 192.168.255.255 (192.168.0.0/16) Class-C

**Shared address space addresses**:

▪ Not globally routable

▪ Intended only for use in service provider networks

▪ Address block is 100.64.0.0/10



**Public address:**

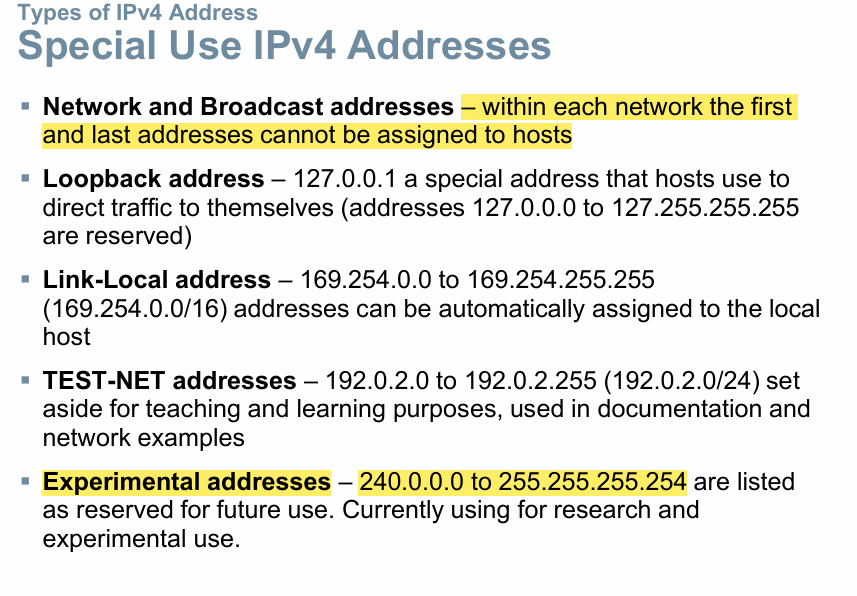
▪ Public IP address of a system is the IP address which is used to communicate outside the network.

▪ Public IP address is basically assigned by the **ISP (Internet Service Provider).**

▪ Besides private IP addresses, rest are public

**What is a Public IP Address?**

In a computer network, a Public IP address is defined as a unique numerical value that is assigned to the particular device connected in the network that makes use of internet protocol for communication and transmission.



why the first and last address cannot be assigned in network?

In a network, the first and last IP addresses are reserved for special purposes and cannot be assigned to individual devices:

1. **Network Address**: The first address in a subnet is known as the network address. It identifies the entire network and **is used by routers to determine the destination network** for data packets. [This address has all zeros in the host part of the IP address](https://dev.to/codexam/how-to-find-the-first-and-last-address-in-a-block-of-ip-addresses-and-understand-subnetting-53f4).
2. **Broadcast Address**: The last address in a subnet is the broadcast address. It is **used to send data to all devices on the network simultaneously**. [This address has all ones in the host part of the IP address](https://community.cisco.com/t5/switching/why-is-the-first-address-on-a-subnet-reserved/td-p/1896044).

[These reservations help in managing and routing network traffic efficiently, ensuring that data packets reach their intended destinations without confusion](https://community.cisco.com/t5/routing/ip-address-rejection/td-p/4731108).

**IPv6 Network Addresses**

A screenshot of a computer code

Description automatically generated

**why IPv6 does not have broadcast addresses?**

IPv6 does not have broadcast addresses because it was designed to be more efficient and scalable than IPv4, addressing the limitations and inefficiencies of IPv4 broadcasts. Here’s why IPv6 omits broadcast addresses:

1. **Reduced Network Traffic with Multicast**
2. **Improved Network Efficiency**
3. **Enhanced Security and Control**
4. **Alternative IPv6 Addressing Types for Specific Purposes**

**what happens when a packet arrives on router interface?**

When a packet arrives on a router interface, the router examines the packet's header, particularly the destination IP address, and uses its routing table to determine the best path to forward the packet towards its intended destination network, essentially deciding where to send the packet next based on its configured routes; if the destination is on the same network, the packet is directly delivered, otherwise, it's forwarded to the next hop in the path

1. **Check the IP header**

The router looks at the packet's IP header to find the destination IP address.

1. **Check the routing table**

The router uses the routing table to see if the destination is on one of its attached networks or if it needs to be forwarded to another router.

1. **Send the packet**

The router sends the packet to the next system in the path to the destination

**1. Receiving the Packet at the Interface**

* The router interface receives the packet, which arrives as a series of bits over a physical or wireless link.
* The interface converts the bits into a complete packet and examines the **link-layer header** to see where it’s coming from.

**2. Decapsulating the Link-Layer Header**

* The router removes (decapsulates) the **link-layer header** from the packet, which contains information about the physical network.
* Once this header is removed, the router is left with the **network-layer packet** (usually an IP packet).

**3. Inspecting the Destination IP Address**

* The router then checks the **destination IP address** in the IP header of the packet.
* This destination address determines where the packet is ultimately supposed to go.

**4. Looking Up the Routing Table**

* The router consults its **routing table**, which contains paths and next-hop information for different destination networks.
* The router looks for the **longest prefix match** for the destination IP in its routing table, meaning it finds the most specific entry that matches the destination address.

**5. Making a Forwarding Decision**

* Based on the routing table, the router decides on the **next hop** (the next router or destination network) for the packet.
* If the packet’s destination matches a **directly connected network**, the router forwards the packet directly to the device on that network.
* If the destination is on a different network, the router forwards it to the next hop specified in the routing table.

**6. Re-Encapsulating the Packet in a New Link-Layer Header**

* The router re-encapsulates the packet with a new link-layer header for the next hop.
* This new header includes the **MAC address** of the next hop if it’s on the same data link, ensuring it reaches the correct next device in the chain.

**7. Sending the Packet Out the Correct Interface**

* The router sends the re-encapsulated packet out through the interface specified in the routing table entry.
* The packet leaves the router on this outbound interface, heading towards its next destination (either the next router or the final device if it’s on the destination network).

**Computer Networking Lab Practices**

**Connection Types:**

Ethernet Stright Through Cable-> for connecting two different devices

Ethernet Crossover-cable-> for connecting same type of devices

**1. Copper Straight-Through Cable**

* **Purpose**: Used to connect different types of devices, such as PCs to switches or routers to switches.
* **Connects**:
  + End devices to network devices (e.g., PC to switch).
  + Different types of devices.
* **Cable Type**: Ethernet (e.g., Cat5/Cat6).
* **Port**: Ethernet ( FastEthernet or GigabitEthernet ).

**2. Copper Crossover Cable**

* **Purpose**: Used to connect similar types of devices, such as PC to PC or switch to switch.
* **Connects**:
  + Router to router.
  + PC to PC.
  + Switch to switch (when interconnecting).
* **Cable Type**: Ethernet crossover cable.
* **Port**: Ethernet.

**Command Prompt:**

* ipconfig -just ip address
* ipconfig /all - ip+physical address
* ping 192.168.0.1 -will check the connection
* show mac-address-table

**SOME BASICS FACTS**-

* **SWITCH/HUBS**-> connects multiple devices in LAN
* **Hubs** connects all devices of a LAN network, that means it is STAR TOPOLOGY.